Algebraische Zahlentheorie

Wolfgang M. Ruppert

Wintersemester 2002/2003

13. März 2003[1]

[1] Im Wintersemester 2002/2003 am Mathematischen Institut der Universität Erlangen abgehaltene Vorlesung

Inhaltsverzeichnis

Vorwort

Die Algebraische Zahlentheorie beschäftigt sich mit algebraischen Zahlen, das sind komplexe Zahlen α, die einer Gleichung $\alpha^n + q_{n-1}\alpha^{n-1} + \cdots + q_1\alpha + q_0 = 0$ mit rationalen Zahlen $q_{n-1}, \ldots, q_1, q_0$ genügen. Man versucht dabei, zahlentheoretische Eigenschaften der natürlichen Zahlen auf algebraische Zahlen zu übertragen, wie z.B. die eindeutige Zerlegung von natürlichen Zahlen in ein Produkt von Primzahlen. Dies führt zur Entwicklung vieler Begriffe, wie sie in einer Algebra-Vorlesung behandelt werden, wie 'Ring', 'Ideal', 'Einheit', 'Modul'.

Das vorliegende Skript ist zu Vorlesungen im Sommersemester 2000 und im Wintersemester 2002/2003 entstanden. Es versucht, in die grundlegenden Begriffe einzuführen und zwar möglichst konstruktiv. So sollten zur Vorlesung Beispiele gerechnet werden, was zur Entwicklung einiger einfacher Maple-Programme führte. Allerdings ist die Vorlesung von einer 'Algorithmischen Algebraischen Zahlentheorie' bzw. 'Computational Algebraic Number Theory' noch deutlich entfernt.
Es gibt schöne abstrakte Darstellungen der Algebraischen Zahlentheorie, wie das Buch von J. Neukirch, Algebraische Zahlentheorie, oder S. Lang, Algebraic Number Theory. Bereits mehr konstruktive Ausrichtung findet sich dann bei S. I. Borewics, I. R. Šafarevič, Zahlentheorie. Will man allerdings ersthafter rechnen, muss man zu Darstellungen der 'Computational Algebraic Number Theory' greifen, wie H. Cohen, A Course in Computational Algebraic Number Theory, oder M. E. Pohst, Computational Algebraic Number Theory.
Das vorliegende Skript versuchte hier, eine gewisse Brücke zu schlagen, was die Gesamtdarstellung noch etwas unausgereift bzw. unvollendet macht.

Historisch tauchten algebraische Zahlen beim Lösen diophantischer Gleichungen auf. Will man z.B. die ganzzahligen Lösungen der Gleichung $y^2 + 2 = x^3$ bestimmen, so kommt man schnell zum Ziel, wenn man zerlegt $(y + \sqrt{-2})(y - \sqrt{-2}) = x^3$ und dann den Ansatz $y + \sqrt{-2} = (u + v\sqrt{-2})^3$ macht. Das Skript behandelt als Anwendung die diophantischen Gleichungen $x^3 + 3y^3 + dz^3 = 0$ und $x^3 + y^3 = z^3$.

An aktuellen Anwendungen der Algebraischen Zahlentheorie sei noch das Zahlkörpersieb (number field sieve) genannt, eine Faktorisierungsmethode, mit der man zur Zeit große natürliche Zahlen am schnellsten faktorisieren kann. Diese wird in einem Kapitel vorgestellt.

Für die Beispiele wurden kleine Programme in Maple 6 geschrieben. Zur Behandlung der diophantischen Gleichung $x^3+3y^3+dz^3 = 0$ wurden das Computeralgebrasystem KANT/KASH 2.2 und das Maple-Paket APECS 6.1 benutzt.

KAPITEL 1

Einführung

1. Rationale und irrationale Zahlen

In der Schule lernt man zunächst die rationalen Zahlen kennen, dann die reellen, später vielleicht noch die komplexen. Man hat die Inklusionen von Körpern

$$\mathbf{Q} \subseteq \mathbf{R} \subseteq \mathbf{C}.$$

Die rationalen Zahlen ergeben sich durch eine einfache algebraische Konstruktion aus den natürlichen Zahlen $\mathbf{N}$. Eine komplexe Zahl $\alpha \in \mathbf{C} \setminus \mathbf{Q}$ wird auch als irrational bezeichnet.
Als erstes Beispiel einer irrationalen Zahl lernt man $\sqrt{2}$ kennen.
Die Irrationalität von e und π ist schon nicht mehr offensichtlich.

SATZ. *$e = 2.71828\ldots$ ist irrational.*

Beweis: Angenommen, e ist rational, d.h. $e = \frac{a}{b}$ mit natürlichen Zahlen a und b. Wir betrachten

$$a!e^{-1} = a!\sum_{n=0}^{\infty} \frac{(-1)^n}{n!} = \sum_{n=0}^{a} \frac{(-1)^n a!}{n!} + \sum_{n=a+1}^{\infty} \frac{(-1)^n a!}{n!}.$$

Offensichtlich ist $\sum_{n=0}^{a} \frac{(-1)^n a!}{n!}$ eine ganze Zahl. Nun ist

$$(-1)^{a+1} \sum_{n=a+1}^{\infty} \frac{(-1)^n a!}{n!} = \frac{1}{a+1} - \frac{1}{(a+1)(a+2)} + \frac{1}{(a+1)(a+2)(a+3)} - + \ldots$$

eine alternierende Reihe mit streng monoton fallenden Folgengliedern, so dass bekanntlich gilt

$$0 < \frac{1}{a+1} - \frac{1}{(a+1)(a+2)} < (-1)^{a+1} \sum_{n=a+1}^{\infty} (-1)^n \frac{a!}{n!} < \frac{1}{a+1} < 1,$$

insbesondere ist $a!\sum_{n=a+1}^{\infty}(-1)^n\frac{1}{n!}$ keine ganze Zahl. Dies müßte aber wegen der Annahme der Fall sein. Wir haben einen Widerspruch: e kann nicht rational sein. ■

Bemerkungen:

1. Ein Beweis für die Irrationalität von π ist in Aufgabe 1 skizziert.
2. Es gibt (viele) Zahlen, von denen man bis jetzt nicht weiß, ob sie rational oder irrational sind, z.B.
$$2^e, \quad \pi^e, \quad \pi^{\sqrt{2}}.$$
3. Es ist nicht bekannt, ob $e + \pi$ oder $e\pi$ irrational sind. (Vergleiche Aufgabe 7.) Nesterenko bewies 1996 einen Satz, aus dem die Irrationalität von $\pi + e^\pi$ folgt.
4. Untersucht werden auch die Werte der ζ-Funktion
$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$
für $s \in \mathbf{N}$. Für gerade natürliche Zahlen s sind die Werte irrational:
$$\zeta(2) = \frac{\pi^2}{6}, \quad \zeta(4) = \frac{\pi^4}{90}, \quad \zeta(6) = \frac{\pi^6}{945}, \quad \ldots$$

Version vom 17.2.2003

Für ungerade natürliche Zahlen s ist wenig bekannt. 1978 wurde von Apéry bewiesen, dass $\zeta(3) = \sum_{n=1}^{\infty} \frac{1}{n^3}$ irrational ist. 2001 bewies Rivoal, dass mindestens eine der Zahlen $\zeta(5), \zeta(7), \ldots, \zeta(21)$ irrational ist.

2. Algebraische und transzendente Zahlen

Eine komplexe Zahl $\alpha \in \mathbf{C}$ heißt algebraisch, wenn sie einer polynomialen Gleichung mit rationalen Koeffizienten genügt, d.h. wenn

$$\alpha^n + a_1\alpha^{n-1} + a_2\alpha^{n-2} + \cdots + a_{n-1}\alpha + a_n = 0$$

gilt mit $a_1, \ldots, a_n \in \mathbf{Q}$. Ist n minimal gewählt, so heißt n der Grad der algebraischen Zahl α. (Multipliziert man mit dem gemeinsamen Nenner aller a_i's durch, so kann man auch

$$a_0\alpha^n + a_1\alpha^{n-1} + a_2\alpha^{n-2} + \cdots + a_{n-1}\alpha + a_n = 0$$

mit $a_i \in \mathbf{Z}$, $\mathrm{ggT}(a_0, a_1, \ldots, a_n) = 1$, $a_0 > 0$ erreichen.)

Beispiele:

1. Jede rationale Zahl q ist algebraisch, denn $q - q = 0$.
2. $\sqrt{2}$ ist algebraisch, denn $(\sqrt{2})^2 - 2 = 0$.
3. Die Nullstellen des Polynoms $x^3 + x + 1 = 0$ sind algebraische Zahlen (Näherungswerte: -0.6823, $0.3412 \pm 1.1615i$)

Satz. *Die Menge $A \subseteq \mathbf{C}$ der algebraischen Zahlen ist abzählbar.*

Eine komplexe Zahl $\alpha \in \mathbf{C}$, die nicht algebraisch ist, heißt transzendent.

Da die Menge der komplexen Zahlen überabzählbar ist, die algebraischen Zahlen aber abzählbar sind, ist klar, dass die 'meisten' komplexen Zahlen transzendent sind. Man kann im allgemeinen einer komplexen Zahl aber nicht gleich ansehen, ob sie algebraisch oder transzendent ist.

Satz. 1. *(Hermite 1873) e ist transzendent.*
2. *(Lindemann 1882) π ist transzendent.*

Die Ergebnisse von Hermite und Lindemann lassen sich wie folgt verallgemeinern:

Satz (Hermite-Lindemann). *Ist $\alpha \in \mathbf{C} \setminus \{0\}$ algebraisch, so ist e^α transzendent.*

Eine weitere Verallgemeinerung ist:

Satz (Gelfond-Schneider (1934)). *Seien $b, c \in \mathbf{C}$ mit $b \notin \mathbf{Q}$, $c \neq 0$. Dann ist wenigstens eine der drei Zahlen*

$$a = e^c, \quad b, \quad a^b = e^{bc}$$

transzendent.

Beispiele:

1. $2^{\sqrt{2}}$ ist transzendent.
2. e^π ist transzendent (Gelfond 1929), über die Zahl π^e weiß man aber nichts.
3. 1999 bewies Nesterenko, daß für $d \in \mathbf{Z} \setminus \{0\}$ die Zahl $e^{\pi\sqrt{d}}$ transzendent ist.

3. Approximationseigenschaften algebraischer Zahlen

Satz (Dirichlet (1842)). *Sei α eine reelle Zahl. Zu $Q \in \mathbf{N}$ lassen sich dann $p, q \in \mathbf{Z}$ finden mit*

$$1 \leq q \leq Q \quad \text{und} \quad |\alpha - \frac{p}{q}| < \frac{1}{qQ}.$$

Beweis: Bestimme für $0 \leq i \leq Q$ ein $a_i \in \mathbf{Z}$ mit $0 \leq i\alpha - a_i < 1$. Sei $b_i = i\alpha - a_i$. Von den $Q+1$ Zahlen b_i muß es mindestens zwei geben, die einen Abstand $\leq \frac{1}{Q}$ haben: $|(i\alpha - a_i) - (j\alpha - a_j)| \leq \frac{1}{Q}$. O.E. $i > j$. Mit $q = i - j$ und $p = a_i - a_j$ folgt die Behauptung. ■

FOLGERUNG. *Ist α reell und irrational, so gibt es unendlich viele Lösungen der Ungleichung*

$$|\alpha - \frac{p}{q}| < \frac{1}{q^2}.$$

Beweis: Man starte mit $i = 1$ und z.B. $Q_1 = 1$.

1. Nach Dirichlet findet man bei gegebenem $Q_i \geq 1$ ganze Zahlen p_i, q_i mit $1 \leq q_i \leq Q_i$ und $|q_i\alpha - p_i| \leq \frac{1}{Q_i}$. Es folgt
$$|\alpha - \frac{p_i}{q_i}| \leq \frac{1}{q_i Q_i} \leq \frac{1}{q_i^2}.$$
2. Nun wähle man ein Q_{i+1} mit
$$\frac{1}{Q_{i+1}} < |q_i\alpha - p_i|$$
und beginne mit Q_{i+1} statt Q_i.
3. Man erhält so eine Folge $\frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots$ rationaler Zahlen, die nach Konstruktion alle verschieden sind. ■

Bemerkung: Durch Kettenbruchentwicklung einer reellen Zahl erhält man Approximationen wie in der Folgerung beschrieben.

Beispiel: Die Paare ganzer Zahlen (p, q) mit $1 \leq q \leq 100$ und $|\pi - \frac{p}{q}| < \frac{1}{q^2}$ sind

$$(p,q) = (3,1), \quad (6,2), \quad (19,6), \quad (22,7), \quad (44,14), \quad (66,21), \quad (88,28).$$

Es ist

$$\pi - 3 = 0.141593, \quad \pi - \frac{19}{6} = -0.02507, \quad \pi - \frac{22}{7} = -0.00126$$

und zum Vergleich

$$\frac{1}{2^2} = 0.25, \quad \frac{1}{6^2} = 0.02778, \quad \frac{1}{28^2} = 0.00128.$$

Man sieht, dass die Approximation $\frac{22}{7}$ in diesem Bereich eine herausragende Rolle spielt.

Roth konnte 1955 nach langem Bemühen zeigen, dass der Approximationssatz von Dirichlet für algebraische Zahlen nicht wesentlich verschärft werden kann. Roth erhielt dafür 1958 die Fields Medal.

SATZ (Roth (1955)). *Sei α eine reelle algebraische Zahl vom Grad ≥ 2. Dann hat für jedes $\varepsilon > 0$ die Ungleichung*

$$|\alpha - \frac{p}{q}| < \frac{1}{q^{2+\varepsilon}}$$

nur endlich viele Lösungen $\frac{p}{q} \in \mathbf{Q}$.

In den Übungen findet man auch eine Anwendung des Satzes für diophantische Gleichungen.

Die Approximation algebraischer Zahlen begann mit folgendem Satz von Liouville:

SATZ (Liouville (1844)). *Sei α eine irrationale algebraische reelle Zahl vom Grad n. Dann gibt es eine Konstante $c(\alpha) > 0$, so dass für alle rationalen Zahlen $\frac{p}{q}$ gilt ($p, q \in \mathbf{Z}$, $q > 0$):*

$$|\alpha - \frac{p}{q}| \geq \frac{c(\alpha)}{q^n}.$$

Beweis:

1. Sei $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \in \mathbf{Z}[x]$ ein Polynom minimalen Grades mit $f(\alpha) = 0$. Insbesondere ist $f(x)$ irreduzibel, $n \geq 2$ und $f'(\alpha) \neq 0$. Definiere
$$c(\alpha) = \min(1, \frac{1}{\sum_{k=1}^{n} \frac{1}{k!}|f^{(k)}(\alpha)|}).$$
Dann gilt
$$c(\alpha) \leq \frac{1}{\sum_{k=1}^{n} \frac{1}{k!}|f^{(k)}(\alpha)|} \quad \text{und} \quad \sum_{k=1}^{n} \frac{1}{k!}|f^{(k)}(\alpha)| \leq \frac{1}{c(\alpha)}.$$

Wegen $c(\alpha) \leq 1$ folgt die Behauptung sofort im Fall $|\alpha - \frac{p}{q}| > 1$. Wir können im folgenden also $|\alpha - \frac{p}{q}| \leq 1$ voraussetzen.

2. Die Taylorreihenentwicklung von f um α ist

$$f(x) = \sum_{k=1}^{n} \frac{f^{(k)}(\alpha)}{k!}(x-\alpha)^k$$

und ergibt wegen $|\alpha - \frac{p}{q}| \leq 1$

$$|f(\frac{p}{q})| \leq \sum_{k=1}^{n} \frac{1}{k!}|f^{(k)}(\alpha)||\frac{p}{q} - \alpha|^k \leq \frac{1}{c(\alpha)}|\alpha - \frac{p}{q}|.$$

3. Da $f(x)$ irreduzibel vom Grad ≥ 2 ist, gilt $f(\frac{p}{q}) \neq 0$. Nun ist

$$f(\frac{p}{q}) = \frac{a_0 p^n + a_1 p^{n-1} q + a_2 p^{n-2} q^2 + \cdots + a_n q^n}{q^n}.$$

Da $a_0 p^n + \cdots + a_n q^n$ eine ganze Zahl $\neq 0$ ist, folgt

$$|a_0 p^n + a_1 p^{n-1} q + a_2 p^{n-2} q^2 + \cdots + a_n q^n| \geq 1$$

und damit

$$|f(\frac{p}{q})| = |\frac{a_0 p^n + a_1 p^{n-1} q + a_2 p^{n-2} q^2 + \cdots + a_n q^n}{q^n}| \geq \frac{1}{q^n},$$

was verbunden mit obiger Ungleichung

$$\frac{1}{q^n} \leq |f(\frac{p}{q})| \leq \frac{1}{c(\alpha)}|\alpha - \frac{p}{q}|$$

ergibt, was zu zeigen war. ■

Algebraische Zahlen lassen sich also nicht zu gut approximieren. Das kann man zur Konstruktion transzendenter Zahlen benutzen:

Beispiel: Die Zahl $\sum_{k=1}^{\infty} \frac{1}{2^{k!}}$ ist transzendent.

4. Beispiele zur Motivation

Die Algebraische Zahlentheorie hat ihren Ursprung in konkreten Fragestellungen, die mit ganzen Zahlen zu tun haben. Im folgenden sollen dafür ein paar Beispiele gegeben werden.

Aufgabe: Bestimme alle ganzzahligen Lösungen der Gleichung

$$y^2 = x^3 - 2.$$

(Diese Aufgabe geht bereits auf Diophant (um 250) zurück.)

Dazu ein paar Anmerkungen:

1. Fermat (1601–1655) stellt englischen Mathematikern die Aufgabe, zu zeigen, daß es außer $x = 3, y = \pm 5$ keine weiteren Lösungen gibt. Er schreibt[i]:
Ob sich jedoch außer 25 noch ein anderes Quadrat in ganzen Zahlen finden läßt, das, um 2 vermehrt, einen Kubus ergibt, das zu untersuchen scheint auf den ersten Blick sehr schwierig. Ich kann aber dennoch einen ganz sicheren Beweis dafür erbringen...
Leider fehlt eine Ausführung der Behauptung.

[i] Pierre de Fermat, Bemerkungen zu Diophant, Ostwald's Klassiker der exakten Wissenschaften, Nr. 234, Akademische Verlagsanstalt, Leipzig, 1932, S. 30 und S. 47

2. Euler (1707-1783) geht in seinem Algebra-Buch[ii] wie folgt vor: Man faktorisiert die Gleichung $y^2+2=x^3$ und erhält:
$$(y+\sqrt{-2})(y-\sqrt{-2})=x^3.$$
Da rechts eine dritte Potenz steht, muß auch $(y+\sqrt{-2})$ eine sein, d.h.
$$y+\sqrt{-2}=(a+b\sqrt{-2})^3$$
mit ganzen Zahlen a und b. Nun ist $(a+b\sqrt{-2})^3=a^3+3a^2b\sqrt{-2}+3ab^2(-2)+b^3(-2)\sqrt{-2}$ und durch Koeffizientenvergleich erhält man
$$\begin{aligned} y &= a^3-6ab^2=a(a^2-6b^2)\\ 1 &= 3a^2b-2b^3=b(3a^2-2b^2)\end{aligned}$$
Aus der letzten Gleichung folgt $b=\pm 1$. Der Fall $b=-1$ führt auf $3a^2=1$, was nicht geht, der Fall $b=1$ auf $a^2=1$ und damit schließlich auf die zwei Lösungen $x=3$ und $y=\pm 5$.
3. Ist Eulers Argument richtig? Eulers Vorgehensweise setzt voraus, dass der Ring
$$R=\{u+v\sqrt{-2}:u,v\in\mathbf{Z}\}$$
ähnliche Eigenschaften hat wie der Ring der ganzen Zahlen $\mathbf{Z}$. In $\mathbf{Z}$ gilt die Aussage: Sind $a,b,c\in\mathbf{N}$ mit $a^3=bc$ und $\mathrm{ggT}(b,c)=1$, so gibt es natürliche Zahlen $\widetilde{b}$ und $\widetilde{c}$ mit $b=\widetilde{b}^3$, $c=\widetilde{c}^3$. Eine analoge Aussage im Ring R wird von Euler benutzt. Aber ist klar, dass man das so ohne weiteres darf?

Aufgabe: Bestimme alle ganzzahligen Lösungen der Gleichung
$$y^2=x^3-26.$$

1. Wir gehen wie bei der letzten Aufgabe wie Euler vor: Wir faktorisieren
$$x^3=y^2+26=(y+\sqrt{-26})(y-\sqrt{26}).$$
Wir setzen an
$$y+\sqrt{-26}=(a+b\sqrt{-26})^3=(a^3-78ab^2)+b(3a^2-26b^2)\sqrt{-26},$$
was durch Koeffizientenvergleich
$$y=a(a^2-78b^2)\quad\text{ und }\quad 1=b(3a^2-26b^2)$$
liefert. Also folgt sofort $b=\pm 1$. Der Fall $b=-1$ führt auf $3a^2=25$, was nicht geht, der Fall $b=1$ führt auf $a=\pm 3$, und damit auf die Lösunge $y=\pm 207$, $x=35$.
2. Sieht man sich die Gleichung kurz an, so erkennt man, dass auch $x=3$, $y=\pm 1$ eine Lösung ist.
3. Mit dem Eulerschen Ansatz haben wir also nicht alle Lösungen gefunden. Dies zeigt, dass sich Eigenschaften des Ringes $\mathbf{Z}$ nicht so ohne weiteres auf den Ring
$$R=\{u+v\sqrt{-26}:u,v\in\mathbf{Z}\}$$
übertragen.
4. In der Algebraischen Zahlentheorie wird untersucht, welche Eigenschaften Ringe des Typs $\{u+v\sqrt{d}:u,v\in\mathbf{Z}\}$ haben.

Aufgabe: Man bestimme alle ganzzahligen Lösungen der Gleichung
$$x^3-2x^2y-xy^2+2y^3=720.$$

Es gilt
$$x^3-2x^2y-xy^2+2y^3=(x+y)(x-y)(x-2y),$$
also haben wir die Gleichung
$$(x+y)(x-y)(x-2y)=720$$

[ii] Leonhard Euler, Algebra, Reclam 1959

zu lösen. Lösen $x, y \in \mathbf{Z}$ die Gleichung, so sind $x+y$, $x-y$ und $x-2y$ ganzzahlige Teiler der Zahl 720, deren Produkt 720 ergibt. Da in $\mathbf{Z}$ die Faktorzerlegung eindeutig ist, kann man leicht alle ganzen Zahlen t_1, t_2, t_3 angeben, deren Produkt 720 ergibt. Es gibt 1080 Möglichkeiten:

$$(t_1, t_2, t_3) = (-720, -1, 1), (-720, 1, -1), (-360, -2, 1), (-360, -1, 2), (-360, 1, -2), \ldots, (720, 1, 1).$$

Setzt man jetzt an

$$x + y = t_1, \quad x - y = t_2, \quad x - 2y = t_3,$$

so erhält man

$$x = \frac{1}{2}(t_1 + t_2), \quad y = \frac{1}{2}(t_1 - t_2)$$

mit der Bedingung $t_3 = x - 2y = \frac{1}{2}(t_1 + t_2) - 2 \cdot \frac{1}{2}(t_1 - t_2)$ bzw.

$$t_1 - 3t_2 + 2t_3 = 0.$$

Man kann jetzt alle Lösungen der Gleichung auflisten:

x	y	t_1	t_2	t_3
-19	-11	-30	-8	3
-16	-14	-30	-2	12
-2	7	5	-9	-16
-1	7	6	-8	-15
8	-2	6	10	12
11	13	24	-2	-15
17	7	24	10	3

Aufgabe: Bestimme alle ganzahligen Lösungen der Gleichung

$$x^3 - 3xy^2 - y^3 = 17.$$

Definiert man eine algebraische Zahl α durch $\alpha^3 - 3\alpha - 1 = 0$, so faktorisiert die Gleichung wie folgt:

$$(x - \alpha y)(x - 2y + \alpha^2 y)(x + 2y + \alpha y - \alpha^2 y) = 17.$$

Wir finden Lösungen durch Probieren:

x	y	$x - \alpha y$	$x - 2y + \alpha^2 y$	$x + 2y + \alpha y - \alpha^2 y$
-15	-8	$-15 + 8\alpha$	$1 - 8\alpha^2$	$-31 - 8\alpha + 8\alpha^2$
-8	23	$-8 - 23\alpha$	$-54 + 23\alpha^2$	$38 + 23\alpha - 23\alpha^2$
-4	3	$-4 - 3\alpha$	$-10 + 3\alpha^2$	$2 + 3\alpha - 3\alpha^2$
-3	-2	$-3 + 2\alpha$	$1 - 2\alpha^2$	$-7 - 2\alpha + 2\alpha^2$
-2	5	$-2 - 5\alpha$	$-12 + 5\alpha^2$	$8 + 5\alpha - 5\alpha^2$
1	-4	$1 + 4\alpha$	$9 - 4\alpha^2$	$-7 - 4\alpha + 4\alpha^2$
3	1	$3 - \alpha$	$1 + \alpha^2$	$5 + \alpha - \alpha^2$
5	-3	$5 + 3\alpha$	$11 - 3\alpha^2$	$-1 - 3\alpha + 3\alpha^2$
23	-15	$23 + 15\alpha$	$53 - 15\alpha^2$	$-7 - 15\alpha + 15\alpha^2$

Allerdings ist nicht klar, dass wir alle Lösungen gefunden haben.
Wie könnte man weiter vorgehen? Die Menge

$$R = \mathbf{Z} + \mathbf{Z}\alpha + \mathbf{Z}\alpha^2$$

bildet einen kommutativen Ring (mit Eins). Hätte man jetzt Aussagen darüber, welche Faktorisierungen

$$17 = \tau_1 \tau_2 \tau_3 \quad \text{mit} \quad \tau_1, \tau_2, \tau_3 \in R$$

möglich sind, könnte man wie bei der letzten Aufgabe versuchen, damit alle Lösungen der Ausgangsgleichung zu bestimmen. Mit solchen Fragestellungen beschäftigt sich die Algebraische Zahlentheorie.

KAPITEL 2

Algebraische Zahlkörper

1. Definition

Ein algebraischer Zahlkörper K ist eine endliche Körpererweiterung von $\mathbf{Q}$. Der Grad der Körpererweiterung $[K : \mathbf{Q}]$, d.h. die Dimension von K als $\mathbf{Q}$-Vektorraum, wird auch als Grad des Zahlkörpers bezeichnet.

SATZ. *Sei K ein Zahlkörper vom Grad n.*

1. *Es gibt ein $\alpha \in K$ mit $K = \mathbf{Q}(\alpha)$.*
2. *$1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ bilden eine $\mathbf{Q}$-Basis von K, insbesondere*
$$\mathbf{Q}(\alpha) = \mathbf{Q} + \mathbf{Q}\alpha + \mathbf{Q}\alpha^2 + \cdots + \mathbf{Q}\alpha^{n-1},$$
und es gibt $a_0, a_1, \ldots, a_{n-1} \in \mathbf{Q}$ mit
$$\alpha^n = -a_0 - a_1\alpha - \cdots - a_{n-1}\alpha^{n-1}.$$
3. *Das Polynom $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbf{Q}[x]$ ist irreduzibel über $\mathbf{Q}$, und der durch*
$$\mathbf{Q}[x] \to \mathbf{Q}(\alpha) = K, \quad x \mapsto \alpha$$
definierte Ringhomomorphismus liefert eine Isomorphismus
$$\mathbf{Q}[x]/(f(x)) \simeq \mathbf{Q}(\alpha) = K$$
von Körpern.

Beweis:

1. Dies folgt aus zwei Sätzen der Algebra: i) In Charakteristik 0 ist jede Körpererweiterung separabel. ii) Eine endliche separable Körpererweiterung wird von einem Element (wie oben) erzeugt.
2. Sei $f(x) \in \mathbf{Q}[x]$ das Minimalpolynom von α. In der Algebra lernt man: $f(x)$ ist irreduzibel, und der durch $\mathbf{Q}[x] \to \mathbf{Q}(\alpha)$, $x \mapsto \alpha$ definierte Ringhomomorphismus induziert einen Isomorphismus
$$\mathbf{Q}[x]/(f(x)) \simeq \mathbf{Q}(\alpha).$$
Ist $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, so folgt durch Einsetzen
$$0 = f(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0,$$
was die Behauptungen 2 und 3 zeigt. ■

Bemerkungen:

1. Sei K ein Zahlkörper und $\alpha \in K$, nicht notwendig $K = \mathbf{Q}(\alpha)$. Das Minimalpolynom von α (über $\mathbf{Q}$) ist ein Polynom $f(x) \in \mathbf{Q}[x]$ kleinsten Grades mit $f(\alpha) = 0$. Ist $g(x) \in \mathbf{Q}[x]$ ein Polynom mit $g(\alpha) = 0$, so teilt f das Polynom g, d.h. es gibt ein Polynom $h(x) \in \mathbf{Q}[x]$ mit $f(x) = g(x)h(x)$.
2. Es gibt mehrere Möglichkeiten, das Minimalpolynom zu normieren. Die in der Algebra gängige Methode ist es zu verlangen, dass der höchste Koeffizient 1 ist. In der Zahlentheorie verwendet man auch die Normierung
$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$
mit $a_i \in \mathbf{Z}$ und $\mathrm{ggT}(a_0, a_1, \ldots, a_n) = 1$.
3. Das Minimalpolynom von $\frac{1}{2}\sqrt{3}$ kann man so als $x^2 - \frac{3}{4}$ oder als $4x^2 - 3$ nehmen.

Rechnen in $\mathbf{Q}(\alpha) \simeq \mathbf{Q}[x]/(f(x))$: Sei $f(x)$ das Minimalpolynom von α.

1. Ist $g(x) \in \mathbf{Q}[x]$, so liefert Division durch $f(x)$ in $\mathbf{Q}[x]$ die (eindeutige) Zerlegung
$$g(x) = h(x)f(x) + \widetilde{g}(x) \quad \text{mit} \quad \text{grad}\widetilde{g} < \text{grad}f.$$
(Maple hat dafür die Funktionen $\widetilde{g} = \text{rem}(g, f, x)$ und $h = \text{quo}(g, f, x)$.) Wegen $f(\alpha) = 0$ folgt sofort $g(\alpha) = \widetilde{g}(\alpha)$, also werden die Elemente von K durch Polynome $g \in \mathbf{Q}[x]$ mit $\text{grad}g < n = \text{grad}f$ repräsentiert, d.h.
$$K = \{g(\alpha) : g(x) \in \mathbf{Q}[x], \text{grad}g < \text{grad}f\}.$$
2. Die Summe von $g_1(\alpha)$ und $g_2(\alpha)$ mit $\text{grad}g_1 < \text{grad}f$, $\text{grad}g_2 < \text{grad}f$ wird durch das Polyom $g_1 + g_2$ repräsentiert, da $\text{grad}(g_1 + g_2) < \text{grad}f$ gilt.
3. Wie multipliziert man zwei Elemente $g_1(\alpha)g_2(\alpha)$? Wir dividieren $g_1(x)g_2(x)$ in $\mathbf{Q}[x]$ durch $f(x)$:
$$g_1(x)g_2(x) = q(x)f(x) + g(x) \quad \text{mit} \quad \text{grad}g < \text{grad}f.$$
Dann ist $g_1(\alpha)g_2(\alpha) = g(\alpha)$, da $f(\alpha) = 0$ gilt.
4. Wie findet man $\frac{1}{g(\alpha)}$, wenn $g(x)$ ein Polynom $\neq 0$ und mit $\text{grad}g < \text{grad}f$ ist? Eine Möglichkeit ergibt sich mit dem erweiterten euklidischen Algorithmus: zu den Polynomen $f(x)$ und $g(x)$ findet man (konstruktiv) Polynome $h(x), r(x) \in \mathbf{Q}[x]$ mit
$$g(x)h(x) + f(x)r(x) = \text{ggT}(g(x), f(x)).$$
(Praktisch liefert dies die Maple-Funktion $\text{gcdex}(g, f, x, 'h', 'r')$.) Da $f(x)$ irreduzibel über $\mathbf{Q}$ ist, ist $\text{ggT}(g, f)$ (bis auf eine Konstante) 1 oder f. Wegen $\text{grad}g < \text{grad}f$, $g \neq 0$ bleibt nur der Fall $\text{ggT}(g, f) = 1$ und damit
$$g(x)h(x) + f(x)r(x) = 1.$$
Dann ist $g(\alpha)h(\alpha) = 1$, also $\frac{1}{g(\alpha)} = h(\alpha)$.

Beispiel: Das Polynom $f(x) = 2x^3 + 3x^2 + 5x + 7$ ist irreduzibel über $\mathbf{Q}$. Wir betrachten den Zahlkörper $K = \mathbf{Q}(\alpha) \simeq \mathbf{Q}[x]/(f)$ mit $f(\alpha) = 0$. Wir wählen
$$g_1(x) = 11 + 13x + 17x^2, \quad g_2(x) = 19 + 23x + 29x^2$$
und $\beta = g_1(\alpha)$, $\gamma = g_2(\alpha)$. Wir dividieren g_1g_2 durch f und finden
$$g_1g_2 = 209 + 500x + 941x^2 + 768x^3 + 493x^4 = (\frac{493}{2}x + \frac{57}{4})f + (\frac{437}{4} - \frac{5187}{4}x - \frac{1337}{4}x^2),$$
woraus sich sofort
$$\beta\gamma = \frac{437}{4} - \frac{5187}{4}\alpha - \frac{1337}{4}\alpha^2$$
ergibt. Mit dem erweiterten euklidischen Algorithmus findet man eine Darstellung
$$f(x)(\frac{10009}{71130} - \frac{6341}{71130}x) + g_1(x)(\frac{97}{71130} - \frac{629}{71130}x + \frac{373}{35565}x^2) = 1,$$
woraus sich sofort
$$\frac{1}{\beta} = \frac{97}{71130} - \frac{629}{71130}\alpha + \frac{373}{35565}\alpha^2$$
ergibt.

Bemerkung: Für einen Zahlkörper K ist die Darstellung als $K = \mathbf{Q}(\alpha) \simeq \mathbf{Q}[x]/(f)$ nicht eindeutig. Daher ergeben sich ganz natürlich ein paar Fragen:

1. Wann definieren zwei (irreduzible) Polynome $f, g \in \mathbf{Q}[x]$ (gleichen Grades) den gleichen Zahlkörper, d.h. wann gilt
$$\mathbf{Q}[x]/(f) \simeq \mathbf{Q}[x]/(g)?$$
2. Kann man bestimmte Elemente eines Zahlkörpers auszeichnen oder gibt es eine Normalform für Zahlkörper, die eine Identifikation erleichtern?

Ein Zahlkörper K heißt quadratisch, falls $[K:\mathbf{Q}]=2$ gilt, kubisch, falls $[K:\mathbf{Q}]=3$ gilt, biquadratisch, falls $[K:\mathbf{Q}]=4$ gilt.

Quadratische Zahlkörper: Sei K ein quadratischer Zahlkörper. Dann gibt es ein irreduzibles Polynom $f(x)=x^2+ax+b\in\mathbf{Q}[x]$ mit $K=\mathbf{Q}(\alpha)$ und $f(\alpha)=0$. Es ist

$$\alpha^2+a\alpha=-b,\quad (\alpha+\frac{a}{2})^2=\frac{a^2-4b}{4}.$$

Nun findet man eine Zerlegung

$$a^2-4b=c^2d,$$

wo $c\in\mathbf{Q}^*$ und $d\in\mathbf{Z}$ quadratfrei ist, d.h.

$$d\in\{-1,\pm2,\pm3,\pm5,\pm6,\pm7,\pm10,\ldots\}.$$

Dann ist

$$(\frac{2\alpha+a}{c})^2=d.$$

Mit $\beta=\frac{2\alpha+a}{c}$ gilt $K=\mathbf{Q}(\beta)$ und $\beta^2=d$. Man schreibt auch $K=\mathbf{Q}(\sqrt{d})$. Es ist nicht schwer zu sehen, dass d durch K eindeutig bestimmt ist. Also werden die quadratischen Zahlkörper durch die quadratfreien ganzen Zahlen

$$d\in\{-1,\pm2,\pm3,\pm5,\pm6,\pm7,\pm10,\pm11\}$$

charakterisiert.

2. Die rationale Darstellung

Sei K ein Zahlkörper vom Grad n. Betrachtet man K als $\mathbf{Q}$-Vektorraum, so liefert jedes Element $\alpha\in K$ durch Multiplikation einen $\mathbf{Q}$-Vektorraum-Endomorphismus $f_\alpha\in\mathrm{End}_{\mathbf{Q}}(K)$:

$$f_\alpha(\omega)=\alpha\omega.$$

Aus

$$\begin{aligned} f_{\alpha+\beta}(\omega) &= (\alpha+\beta)\omega=\alpha\omega+\beta\omega=f_\alpha(\omega)+f_\beta(\omega)=(f_\alpha+f_\beta)(\omega),\\ f_{\alpha\beta}(\omega) &= \alpha\beta\omega=f_\alpha(\beta\omega)=f_\alpha(f_\beta(\omega))=(f_\alpha\circ f_\beta)(\omega), \end{aligned}$$

d.h.

$$f_{\alpha+\beta}=f_\alpha+f_\beta,\quad f_{\alpha\beta}=f_\alpha\circ f_\beta,$$

sieht man (nach Definition der Ringstruktur in Endomorphismenringen), dass durch

$$K\to\mathrm{End}_{\mathbf{Q}}(K),\quad \alpha\mapsto f_\alpha$$

ein $\mathbf{Q}$-linearer Ringhomomorphismus definiert wird.
Wir wollen jetzt eine Matrixdarstellung von f_α gewinnen. Sei dazu $\omega_1,\ldots,\omega_n$ eine $\mathbf{Q}$-Basis von K. Dann gibt es $A(\alpha)_{ij}\in\mathbf{Q}$ mit

$$\alpha\omega_i=\sum_{j=1}^{n}A(\alpha)_{ij}\omega_j.$$

Die Matrix $A(\alpha)=(A(\alpha)_{ij})$ ist also eine Matrixdarstellung von f_α. Man kann dies auch noch so schreiben:

$$\alpha\begin{pmatrix}\omega_1\\ \vdots\\ \omega_n\end{pmatrix}=A(\alpha)\begin{pmatrix}\omega_1\\ \vdots\\ \omega_n\end{pmatrix}.$$

Die Abbildung

$$K\to M_n(\mathbf{Q}),\quad \alpha\mapsto A(\alpha)$$

ein $\mathbf{Q}$-linearer Ringhomomorphismus. Damit ist K ein Teilkörper des Matrizenrings $M_n(\mathbf{Q})$.

Beispiel: $K=\mathbf{Q}(\sqrt{d})$ bzw. $K=\mathbf{Q}(\omega)$ mit $\omega^2=d$. Als $\mathbf{Q}$-Basis wählen wir $1,\omega$. Aus

$$(a+b\omega)\begin{pmatrix}1\\ \omega\end{pmatrix}=\begin{pmatrix}a & b\\ db & a\end{pmatrix}\begin{pmatrix}1\\ \omega\end{pmatrix}$$

ergibt sich als Matrixdarstellung von $a + b\omega$:

$$A(a + b\omega) = \begin{pmatrix} a & b \\ db & a \end{pmatrix}.$$

Eine weitere Interpretation:

$$\{\begin{pmatrix} a & b \\ db & a \end{pmatrix} \in M_2(\mathbf{Q}) : a, b \in \mathbf{Q}\}$$

ist ein Körper, der zu $\mathbf{Q}(\omega)$ isomorph ist.

DEFINITION. Ist K ein Zahlkörper vom Grad n, $\alpha \in K$, so wird das charakteristische Polynom von α, die Spur $\mathrm{Sp}(\alpha)$, die Norm $\mathrm{N}(\alpha)$ als charakteristisches Polynom von f_α, als Spur $\mathrm{Sp}(f_\alpha)$, als Determinante $\det(f_\alpha)$ definiert. Hat man f_α in einer Matrixdarstellung $A(\alpha) \in M_n(\mathbf{Q})$ gegeben, so ist das charakteristische Polynom von α das charakteristische Polynom $\det(xI_n - A(\alpha)) \in \mathbf{Q}[x]$ von $A(\alpha)$ und weiter $\mathrm{Sp}(\alpha) = \mathrm{Sp}(A(\alpha))$ und $\mathrm{N}(\alpha) = \det(A(\alpha))$.

Die folgenden Eigenschaften von Spur und Norm folgen sofort aus den entsprechenden Eigenschaften für Spur und Determinante von Matrizen:

SATZ. *Die Spur* $\mathrm{Sp} : K \to \mathbf{Q}$ *ist* $\mathbf{Q}$*-linear, d.h. für* $\alpha, \beta \in K$ *und* $q \in \mathbf{Q}$ *gilt*

$$\mathrm{Sp}(\alpha + \beta) = \mathrm{Sp}(\alpha) + \mathrm{Sp}(\beta) \quad \textit{und} \quad \mathrm{Sp}(q\alpha) = q\mathrm{Sp}(\alpha), \quad \mathrm{Sp}(0) = 0,$$

die Norm ist multiplikativ, d.h. für $\alpha, \beta \in K$ *gilt*

$$\mathrm{N} : K \to \mathbf{Q} \quad \textit{mit} \quad \mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta), \quad \mathrm{N}(1) = 1.$$

Beispiel: Für den quadratischen Zahlkörper $K = \mathbf{Q}(\omega)$ mit $\omega^2 = d$ ergibt sich dann aus obiger Darstellung sofort

$$\mathrm{Sp}(a + b\omega) = 2a, \quad \mathrm{N}(a + b\omega) = a^2 - db^2.$$

Das charakteristische Polynom von $a + b\omega$ ist $x^2 - 2ax + (a^2 - db^2)$.

Bemerkung: Spur und Norm hängen natürlich vom gewählten Zahlkörper K ab. (Hat ein Zahlkörper Grad n, so ist $A(1)$ die $n \times n$-Einheitsmatrix, also $\mathrm{Sp}(1) = n$.) Daher schreibt man bei Unklarheiten auch $\mathrm{Sp} = \mathrm{Sp}_K$ und $\mathrm{N} = \mathrm{N}_K$.

LEMMA. *Sei* K *ein Zahlkörper und* $\alpha \in K$ *mit* $K = \mathbf{Q}(\alpha)$*. Dann stimmen Minimalpolynom von* α *und charakteristisches Polynom von* α *(bis auf eine Konstante) überein.*

Beweis: K habe Grad n, $f(x)$ sei das Minimalpolynom von α, $g(x)$ das charakteristische Polynom von α, d.h. von $A(\alpha) \in M_n(\mathbf{Q})$. Beide Polynome haben Grad n. Aus der Linearen Algebra weiß man, dass $g(A(\alpha)) = 0$ gilt. Da die rationale Darstellung $K \to M_n(\mathbf{Q})$ ein (injektiver) Ringhomomorphismus ist, folgt $A(g(\alpha)) = 0$ und damit $g(\alpha) = 0$. Nach Konstruktion des Minimalpolynoms teilt $f(x)$ das Polynom $g(x)$, d.h. es gibt ein Polynom $h(x) \in \mathbf{Q}[x]$ mit $g(x) = f(x)h(x)$. Aus Gradgründen muß $h(x)$ konstant sein. ■

Bemerkungen:

1. Mit dem Lemma kann man das Minimalpolynoms eines Elements $\beta \in K$ berechnen, falls $\mathbf{Q}(\beta) = K$ gilt.
2. Im allgemeinen Fall $\beta \in K$ kann man zeigen, dass das charakteristische Polynom von β eine Potenz des Minimalpolynoms ist.
3. Sei $K = \mathbf{Q}(\alpha)$ und $f(x) \in \mathbf{Q}[x]$ das Minimalpolynom von α und $\beta \in K$ mit $\beta = g(\alpha)$ und $g(x) \in \mathbf{Q}[x]$, $\mathrm{grad} g < \mathrm{grad} f$. Bildet man die Resultante

   $$h(X) = \mathrm{Resultante}_x(X - g(x), f(x)),$$

   so ist $h(x)$ das Minimalpolynom von β über $\mathbf{Q}$. (In Maple hat man dafür die Funktion resultant$(X - g, f, x)$ zur Verfügung.)

Beispiel: Wir betrachten wieder den kubischen Zahlkörper $K = \mathbf{Q}(\alpha)$ mit $f(\alpha) = 0$, wo $f = 2x^2 + 3x^2 + 5x + 7$ ist. Für $\beta = 11 + 13\alpha + 17\alpha^2$ gilt:

$$\begin{aligned}(11 + 13\alpha + 17\alpha^2) \cdot 1 &= 11 + 13\alpha + 17\alpha^2 \\ (11 + 13\alpha + 17\alpha^2) \cdot \alpha &= -\frac{119}{2} - \frac{63}{2}\alpha - \frac{25}{2}\alpha^2 \\ (11 + 13\alpha + 17\alpha^2) \cdot \alpha^2 &= \frac{175}{4} - \frac{113}{4}\alpha - \frac{51}{4}\alpha^2\end{aligned}$$

Dies liefert die Darstellung

$$\beta \mapsto \begin{pmatrix} 11 & 13 & 17 \\ -\frac{119}{2} & -\frac{63}{2} & -\frac{25}{2} \\ \frac{175}{4} & -\frac{113}{4} & -\frac{51}{4} \end{pmatrix}.$$

Das charakteristische Polynom der Matrix und damit das Minimalpolynom von β ist

$$x^3 + \frac{133}{4}x^2 - \frac{817}{2}x - 35565.$$

3. Die Einbettungen von K in $\mathbf{C}$

LEMMA. *Ein Zahlkörper K vom Grad n hat genau n Einbettungen $\sigma_i : K \to \mathbf{C}$, $i = 1, \ldots, n$ in $\mathbf{C}$. Explizit: Ist $K = \mathbf{Q}(\alpha)$, $f(x)$ das Minimalpolynom von α, sind $\alpha_1, \ldots, \alpha_n \in \mathbf{C}$ die komplexen Nullstellen von $f(x)$, so werden die Einbettungen beschrieben durch*

$$\sigma_i(\alpha) = \alpha_i$$

bzw.

$$\sigma_i(\sum_j x_j \alpha^j) = \sum_j x_j \alpha_i^j,$$

wenn $x_j \in \mathbf{Q}$ ist.

Beweis: Da $f(\alpha_i) = 0$ ist, folgt, dass $\sigma_i : \mathbf{Q}(\alpha) \simeq \mathbf{Q}[x]/(f(x)) \to \mathbf{C}$ ein Körperhomomorphismus ist. Da f in $\mathbf{C}$ n verschiedene Nullstellen hat, sind alle σ_i verschieden. Sei umgekehrt $\sigma : K \to \mathbf{C}$ ein Körperhomomorphismus. Dann folgt aus $f(\alpha) = 0$ sofort $f(\sigma(\alpha)) = 0$, also gibt es ein i mit $\sigma(\alpha) = \alpha_i$ und damit $\sigma = \sigma_i$. ■

Bezeichnungen:

1. Ist $\alpha_i \in \mathbf{R}$, so gilt $\sigma_i(K) \subseteq \mathbf{R}$. Man nennt dann σ_i eine reelle Einbettung. Die Anzahl der reellen Einbettungen wird historisch mit r_1 bezeichnet.
2. Ist $\alpha_i \in \mathbf{C} \notin \mathbf{R}$, so heißt σ_i eine komplexe Einbettung. Da $f(x)$ ein reelles Polynom ist, ist auch $\overline{\alpha_i}$ eine Nullstelle von $f(x)$, d.h. es gibt einen Index $j \neq i$ mit $\alpha_j = \overline{\alpha_i}$. Die Einbettung σ_j ist dann konjugiert komplex zu σ_i. Komplexe Einbettungen treten also immer paarweise auf. Ihre Anzahl wird historisch mit $2r_2$ bezeichnet.
3. Mit diesen Bezeichnungen werden die Einbettungen manchmal auch so aufgezählt:

   $$\sigma_1, \ldots, \sigma_{r_1}, \sigma_{r_1+1}, \overline{\sigma_{r_1+1}}, \ldots \sigma_{r_1+r_2}, \overline{\sigma_{r_1+r_2}}.$$

   Insbesondere gilt die Formel:

   $$r_1 + 2r_2 = n.$$

Beispiel: Sei $K = \mathbf{Q}(\alpha)$, $\alpha^2 = d$, $d \in \mathbf{Z}$ quadratfrei. Wir unterscheiden zwei Fälle:

1. $d > 0$. Es gibt zwei reelle Einbettungen. Bezeichne $\sqrt{d}$ die positive reelle Wurzel von d:

   $$\sigma_1(a + b\alpha) = a + b\sqrt{d}, \quad \sigma_2(a + b\alpha) = a - b\sqrt{d}.$$

   K heißt dann reellquadratisch.
2. $d < 0$. Ist $\sqrt{d}$ eine komplexe Wurzel, so ist

   $$\sigma(a + b\alpha) = a + b\sqrt{d}$$

   eine komplexe Einbettung von K, die zweite ist dann $\overline{\sigma}$. Der Zahlkörper K wird als imaginärquadratisch bezeichnet.

Beispiel: $K = \mathbf{Q}(\alpha)$ mit $f(\alpha) = 0$ und $f = 2x^3 + 3x^2 + 5x + 7$. Die drei komplexen Nullstellen von f sind

$$\alpha_1 \approx -1.45, \quad \alpha_2 \approx -0.03 - 1.56i, \quad \alpha_3 \approx -0.03 + 1.56i,$$

wir haben also eine reelle Einbettung und zwei konjugiert komplexe.

SATZ. *Sei K ein Zahlkörper vom Grad n mit den Einbettungen $\sigma_i : K \to \mathbf{C}$, $i = 1, \ldots, n$. Sei $\omega_1, \ldots, \omega_n$ eine $\mathbf{Q}$-Basis von K und $A(\alpha) \in M_n(\mathbf{Q})$ die zugehörige Matrixdarstellung von $\alpha \in K$. Dann gibt es eine komplexe Matrix S mit*

$$A(\alpha) = S^{-1} \begin{pmatrix} \sigma_1(\alpha) & & \\ & \ldots & \\ & & \sigma_n(\alpha) \end{pmatrix} S$$

für alle $\alpha \in K$.

Beweis: Wir wählen $\alpha \in K$ fest mit $K = \mathbf{Q}(\alpha)$. Dann stimmt das Minimalpolynom $f(x)$ von α mit dem charakteristischen Polynom von $A(\alpha)$ überein. Seien $\alpha_1, \ldots, \alpha_n$ die n verschiedenen komplexen Wurzeln von $f(x)$ mit $\sigma_i(\alpha) = \alpha_i$. Da das charakteristische Polynom von $A(\alpha)$ die n verschiedenen Wurzeln α_i hat, ist $A(\alpha)$ über $\mathbf{C}$ diagonalisierbar, d.h. es gibt eine komplexe Matrix S mit

$$A(\alpha) = S^{-1} \begin{pmatrix} \alpha_1 & & \\ & \ldots & \\ & & \alpha_n \end{pmatrix} S = S^{-1} \begin{pmatrix} \sigma_1(\alpha) & & \\ & \ldots & \\ & & \sigma_n(\alpha) \end{pmatrix} S.$$

Nun folgt schnell mit $x_j \in \mathbf{Q}$ die Beziehung

$$A(\sum_j x_j \alpha^j) = \sum_j x_j A(\alpha)^j = S^{-1} \begin{pmatrix} \sigma_1(\sum_j x_j \alpha^j) & & \\ & \ldots & \\ & & \sigma_n(\sum_j x_j \alpha^j) \end{pmatrix} S.$$

Da man alle Elemente von K als $\sum x_j \alpha^j$ schreiben kann, folgt die Behauptung. ■

Aus dem Satz ergibt sich sofort:

FOLGERUNG. *Sei K ein Zahlkörper vom Grad n und $\sigma_1, \ldots, \sigma_n$ die verschiedenen komplexen Einbettungen. Dann gilt*

$$\mathrm{Sp}(\alpha) = \sigma_1(\alpha) + \cdots + \sigma_n(\alpha), \quad \mathrm{N}(\alpha) = \sigma_1(\alpha) \ldots \sigma_n(\alpha).$$

Beispiel: Wir wollen die rationale Darstellung für einen quadratischen Zahlkörper $K = \mathbf{Q}(\sqrt{d})$ diagonalisieren. Als $\mathbf{Q}$-Basis wählen wir $1, \sqrt{d}$. Aus

$$\sqrt{d} \begin{pmatrix} 1 \\ \sqrt{d} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ d & 0 \end{pmatrix} \begin{pmatrix} 1 \\ \sqrt{d} \end{pmatrix}$$

folgt, dass wir die Matrix

$$A(\sqrt{d}) = \begin{pmatrix} 0 & 1 \\ d & 0 \end{pmatrix}$$

diagonalisieren müssen. Das charakteristische Polynom ist

$$\det(xI - A(\sqrt{d}) = x^2 - d$$

mit den Nullstellen $\pm\sqrt{d}$. Die Eigenwertgleichung $A(\sqrt{d})v_{pm} = \pm\sqrt{d}v_{\pm}$ wird gelöst von

$$v_{\pm} = \begin{pmatrix} 1 \\ \pm\sqrt{d} \end{pmatrix}.$$

Als Transformationsmatrix setzen wir daher

$$S = \begin{pmatrix} 1 & 1 \\ \sqrt{d} & -\sqrt{d} \end{pmatrix}$$

an und erhalten dann

$$S^{-1} A(\sqrt{d}) S = \begin{pmatrix} \sqrt{d} & 0 \\ 0 & -\sqrt{d} \end{pmatrix}.$$

Dies liefert sofort

$$S^{-1}A(a+b\sqrt{d})S = \begin{pmatrix} a+b\sqrt{d} & 0 \\ 0 & a-b\sqrt{d} \end{pmatrix}.$$

4. Spurform und Diskriminanten

LEMMA. *Sei K ein Zahlkörper. Durch*

$$(\alpha,\beta) \mapsto \mathrm{Sp}(\alpha\beta)$$

wird eine symmetrische nichtausgeartete $\mathbf{Q}$*-Bilinearform auf K definiert, die auch als Spurform bezeichnet wird.*

Beweis: Sei $\omega_1,\ldots,\omega_n$ eine $\mathbf{Q}$-Basis von K. Für $\alpha = x_1\omega_1+\cdots+x_n\omega_n$, $\beta = y_1\omega_1+\cdots+y_n\omega_n$ mit $x_i, y_i \in \mathbf{Q}$ gilt dann

$$\begin{aligned} \mathrm{Sp}(\alpha\beta) &= \mathrm{Sp}((x_1\omega_1+\cdots+x_n\omega_n)(y_1\omega_1+\cdots+y_n\omega_n)) = \mathrm{Sp}(\sum_{i,j} x_iy_j\omega_i\omega_j) = \\ &= \sum_{i,j} x_i\mathrm{Sp}(\omega_i\omega_j)y_j = (x_1\ldots x_n)(\mathrm{Sp}(\omega_i\omega_j))_{i,j}\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}. \end{aligned}$$

Aus dieser Darstellung sieht man sofort mit $\omega_i\omega_j = \omega_j\omega_i$, dass die Spurform eine symmetrische $\mathbf{Q}$-Bilinearform ist. Wäre die Bilinearform ausgeartet, so gäbe es ein $\alpha \in K$, $\alpha \neq 0$, so dass für alle $\beta \in K$ die Beziehung $\mathrm{Sp}(\alpha\beta) = 0$ bestände. Nun ist aber $\mathrm{Sp}(\alpha\cdot\frac{1}{\alpha}) = \mathrm{Sp}(1) = n \neq 0$, also ist die Spurform nicht ausgeartet. (Äquivalent dazu ist, dass die Determinante der darstellenden Matrix $\neq 0$ ist.) ■

Beispiel: Wählt man bei einem quadratischen Zahlkörper $\mathbf{Q}(\sqrt{d})$ die Elemente $1, \sqrt{d}$ als $\mathbf{Q}$-Basis, so wird die Matrix der Spurform

$$\begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix}.$$

Beispiel: Wir betrachten $K = \mathbf{Q}(\alpha)$ mit $f(\alpha) = 0$ und $f = 2x^3+3x^2+5x+7$. Bezüglich der Basis $1, \alpha, \alpha^2$ wird die Matrix der Spurform

$$(\mathrm{Sp}(\alpha^i\alpha^j))_{i,j=0,1,2} = \begin{pmatrix} 3 & -\frac{3}{2} & -\frac{11}{4} \\ -\frac{3}{2} & -\frac{11}{4} & -\frac{21}{8} \\ -\frac{11}{4} & -\frac{21}{8} & \frac{257}{16} \end{pmatrix}.$$

DEFINITION. Für einen Zahlkörper vom Grad n und $\alpha_1,\ldots,\alpha_n \in K$ wird

$$\mathrm{disc}\,(\alpha_1,\ldots,\alpha_n) = \det(\mathrm{Sp}(\alpha_i\alpha_j)_{i,j})$$

als Diskriminante des n-Tupels $\alpha_1,\ldots,\alpha_n$ bezeichnet.

SATZ. *Sind $\sigma_1,\ldots,\sigma_n$ die komplexen Einbettungen des Zahlkörpers K, so gilt für $\alpha_1,\ldots,\alpha_n \in K$:*

$$\mathrm{disc}\,(\alpha_1,\ldots,\alpha_n) = (\det(\sigma_i\alpha_j)_{i,j})^2.$$

Beweis: Matrizenmultiplikation ergibt:

$$\begin{aligned} ((\sigma_i\alpha_k)_{i,k})^t\cdot(\sigma_l\alpha_j)_{l,j} &= (\sigma_k\alpha_i)_{i,k}\cdot(\sigma_l\alpha_j)_{l,j} = (\sum_k \sigma_k(\alpha_i)\cdot\sigma_k(\alpha_j))_{i,j} = (\sum_k \sigma_k(\alpha_i\alpha_j))_{i,j} = \\ &= (\mathrm{Sp}(\alpha_i\alpha_j))_{i,j}, \end{aligned}$$

woraus man durch Determinantenbildung sofort die Behauptung erhält. ■

SATZ. *Für einen Zahlkörper K vom Grad n und $\alpha_1,\ldots,\alpha_n \in K$ gilt:*

$$\mathrm{disc}\,(\alpha_1,\ldots,\alpha_n) = 0 \quad\Longleftrightarrow\quad \alpha_1,\ldots,\alpha_n \textit{ sind linear abhängig über } \mathbf{Q}.$$

Beweis: Für $x_1, \ldots, x_n \in \mathbf{Q}$ gilt:

$$(\sigma_i\alpha_j)_{i,j}\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0 \quad \Longleftrightarrow \quad \sigma_i(\sum_j x_j\alpha_j) = 0 \text{ für alle } i \quad \Longleftrightarrow \quad \sum_j x_j\alpha_j = 0.$$

Da die nichttriviale Lösbarkeit des Gleichungssystems $(\sigma_i\alpha_j)_{i,j}(x_j)_j = 0$ äquivalent mit $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = 0$ ist, folgt die Behauptung. ■

SATZ. *Ist $K = \mathbf{Q}(\alpha)$, $f \in \mathbf{Q}[x]$ das (normierte) Minimalpolyom von α, sind $\sigma_1, \ldots, \sigma_n$ die komplexen Einbettungen von K, so gilt:*

$$\operatorname{disc}(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) = \prod_{i<j}(\sigma_i(\alpha) - \sigma_j(\alpha))^2 = (-1)^{\frac{n(n-1)}{2}}\mathrm{N}(f'(\alpha)) = \operatorname{disc}(f),$$

wo $\operatorname{disc}(f)$ *die Diskriminante des Polynoms f bezeichnet.*

Beweis: $\operatorname{disc}(1, \alpha, \ldots, \alpha^{n-1})$ ist das Quadrat der Determinante von

$$\begin{pmatrix} \sigma_1 1 & \sigma_1\alpha & \ldots & \sigma_1\alpha^{n-1} \\ \vdots & \vdots & \ldots & \vdots \\ \sigma_n 1 & \sigma_n\alpha & \ldots & \sigma_n\alpha^{n-1} \end{pmatrix}.$$

Nach Vandermonde folgt damit das erste =-Zeichen der Behauptung.
Die Diskriminante des Polynoms f ist nach Definition das Produkt $\prod_{i<j}(\sigma_i(\alpha)-\sigma_j(\alpha))^2$, da $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ die verschiedenen Nullstellen von f in $\mathbf{C}$ sind.
Wir haben die Faktorisierung

$$f(x) = (x - \sigma_1\alpha)\ldots(x - \sigma_n\alpha) = \prod_j(x - \sigma_j\alpha)$$

und damit nach der Produktformel für das Differenzieren

$$f'(x) = \sum_i \prod_{j\neq i}(x - \sigma_j\alpha),$$

was

$$f'(\sigma_i\alpha) = \prod_{j\neq i}(\sigma_i\alpha - \sigma_j\alpha)$$

ergibt. Nun folgt:

$$\begin{aligned} \mathrm{N}(f'(\alpha)) &= \prod_i \sigma_i(f'(\alpha)) = \prod_i f'(\sigma_i\alpha) = \prod_i\prod_{j\neq i}(\sigma_i\alpha - \sigma_j\alpha) = \prod_{i\neq j}(\sigma_i\alpha - \sigma_j\alpha) = \\ &= \prod_{i<j}(\sigma_i\alpha - \sigma_j\alpha)\cdot\prod_{i>j}(\sigma_i\alpha - \sigma_j\alpha) = \prod_{i<j}(\sigma_i\alpha - \sigma_j\alpha)\cdot\prod_{i<j}(\sigma_j\alpha - \sigma_i\alpha) = \\ &= \prod_{i<j}(\sigma_i\alpha - \sigma_j\alpha)\cdot\prod_{i<j}(-1)(\sigma_i\alpha - \sigma_j\alpha) = \prod_{1\leq i<j\leq n}(-1)\cdot\prod_{i<j}(\sigma_i\alpha - \sigma_j\alpha)^2. \end{aligned}$$

Da die Menge $\{1 \leq i < j \leq n\}$ (als obere Dreiecksseite einer quadratischen $n\times n$-Matrix) $\frac{n(n-1)}{2}$ Elemente enthält, folgt schließlich die letzte Behauptung. ■

LEMMA. *Ist K ein Zahlkörper vom Grad n, sind $\alpha_1, \ldots, \alpha_n \in K$, $x_{ij} \in \mathbf{Q}$ und $\beta_i = \sum_j x_{ij}\alpha_j$, so ist*

$$\operatorname{disc}(\beta_1, \ldots, \beta_n) = (\det(x_{ij}))^2 \cdot \operatorname{disc}(\alpha_1, \ldots, \alpha_n).$$

Beweis:

$$\mathrm{Sp}(\beta_i\beta_j) = \mathrm{Sp}((\sum_k x_{ik}\alpha_k)(\sum_l x_{jl}\alpha_l)) = \sum_{k,l} x_{ik}\mathrm{Sp}(\alpha_k\alpha_l)x_{jl}.$$

Liest man dies als Matrizenprodukt, so folgt die Behauptung durch Determinantenbildung. ■

SATZ. *Ist $\alpha_1, \ldots, \alpha_n$ eine $\mathbf{Q}$-Basis des Zahlkörpers K, so gibt es eine $\mathbf{Q}$-Basis $\beta_1, \ldots, \beta_n$ von K mit*

$$\mathrm{Sp}(\alpha_i \beta_j) = \begin{cases} 1 \text{ für } i = j \\ 0 \text{ für } i \neq j \end{cases}.$$

$\beta_1, \ldots, \beta_n$ heißt die zu $\alpha_1, \ldots, \alpha_n$ duale Basis. Explizit: Ist $X = (\mathrm{Sp}(\alpha_i \beta_i)_{1 \leq i,j \leq n})^{-1}$, so gilt $\beta_i = \sum_j x_{ij} \alpha_j$ mit $X = (x_{ij})_{1 \leq i,j \leq n}$.

Beweis: Dies ist aus der Linearen Algebra bekannt. Wir geben aber noch einen expliziten Beweis. Wir setzen an $\beta_j = \sum_k x_{jk} \alpha_k$ mit einer Matrix $X = (x_{jk})$. Nun ist

$$\mathrm{Sp}(\alpha_i \beta_j) = \mathrm{Sp}(\alpha_i \sum_k x_{jk} \alpha_k) = \sum_k \mathrm{Sp}(\alpha_i \alpha_k) x_{jk}.$$

Wir müssen also die Matrixgleichung

$$1 = (\mathrm{Sp}(\alpha_i \alpha_k)_{ik}) X^t$$

lösen, was sofort durch $X = (\mathrm{Sp}(\alpha_i \alpha_j))^{-1}$ geschieht, weil $\mathrm{Sp}(\alpha_i \alpha_j)$ symmetrisch ist. ■

Beispiel: Sei $K = \mathbf{Q}(\alpha)$ mit $f(\alpha) = 0$ und $f = 2x^3 + 3x^2 + 5x + 7$. Wir wollen die Dualbasis zu $1, \alpha, \alpha^2$ bestimmen. Wir berechnen

$$(\mathrm{Sp}(\alpha^i \alpha^j))_{i,j=0,1,2} = \begin{pmatrix} 3 & -\frac{3}{2} & -\frac{11}{4} \\ -\frac{3}{2} & -\frac{11}{4} & -\frac{21}{8} \\ -\frac{11}{4} & -\frac{21}{8} & \frac{257}{16} \end{pmatrix}$$

und erhalten

$$X = (\mathrm{Sp}(\alpha^i \alpha^j))^{-1} = \frac{1}{3043} \begin{pmatrix} 817 & -501 & 58 \\ -501 & -650 & -192 \\ 58 & -192 & 168 \end{pmatrix},$$

so dass sich als Dualbasis β_i ergibt

$$\begin{aligned} \beta_0 &= \frac{817}{3043} - \frac{501}{3043}\alpha + \frac{58}{3043}\alpha^2 \\ \beta_1 &= -\frac{501}{3043} - \frac{650}{3043}\alpha - \frac{192}{3043}\alpha^2 \\ \beta_2 &= \frac{58}{3043} - \frac{192}{3043}\alpha + \frac{168}{3043}\alpha^2 \end{aligned}$$

Ein Test zeigt, dass tatsächlich $\mathrm{Sp}(\alpha^i \beta_j) = \delta_{ij}$ für $i, j = 0, 1, 2$ gilt.

SATZ. *Sei $K = \mathbf{Q}(\alpha)$, $f(x)$ das Minimalpolynom von α. Faktorisiert man*

$$\frac{f(x)}{x - \alpha} = \gamma_0 + \gamma_1 x + \cdots + \gamma_{n-1} x^{n-1},$$

so ist

$$\frac{\gamma_0}{f'(\alpha)}, \frac{\gamma_1}{f'(\alpha)}, \ldots, \frac{\gamma_{n-1}}{f'(\alpha)}$$

die zu $1, \alpha, \ldots, \alpha^{n-1}$ duale Basis.

Beweis:

1. Seien $\sigma_1, \ldots, \sigma_n$ die Einbettungen von K in $\mathbf{C}$ und abkürzend $g(x) = \gamma_0 + \gamma_1 x + \cdots + \gamma_{n-1} x^{n-1}$. Wir haben dann
$$f(x) = \prod_j (x - \sigma_j \alpha), \quad f'(x) = \sum_i \prod_{j \neq i} (x - \sigma_j \alpha), \quad f'(\sigma_i \alpha) = \prod_{j \neq i} (\sigma_i \alpha - \sigma_j \alpha).$$
2. Aus $(x - \alpha) g(x) = f(x)$ folgt
$$(x - \sigma_i \alpha)(\sigma_i g)(x) = f(x) = (x - \sigma_1 \alpha) \ldots (x - \sigma_n \alpha)$$
und
$$(\sigma_i g)(x) = \prod_{j \neq i} (x - \sigma_j \alpha).$$

Dies liefert

$$(\sigma_i g)(\sigma_j \alpha) = \begin{cases} f'(\sigma_i\alpha) \text{ für } i = j \\ 0 \text{ für } i \neq j \end{cases}.$$

3. Wir betrachten jetzt für $0 \leq k \leq n-1$ das Polynom

$$h(x) = \sum_{i=1}^{n} (\sigma_i g)(x) \frac{\sigma_i \alpha^k}{f'(\sigma_i \alpha)} - x^k.$$

Dann ist

$$h(\sigma_j \alpha) = \sigma_j \alpha^k - \sigma_j \alpha^k = 0$$

für alle k. Da andererseits $\text{grad} g \leq n-1$ gilt, ein Polynom $\neq 0$ vom Grad $\leq n-1$ höchstens $n-1$ Nullstellen hat, folgt $h(x) = 0$, d.h.

$$\begin{aligned} x^k &= \sum_{i=1}^{n} (\sigma_i g)(x) \frac{\sigma_i \alpha^k}{f'(\sigma_i \alpha)} = \sum_{i=1}^{n} (\sum_{l=0}^{n-1} \sigma_i \gamma_l x^l) \frac{\sigma_i \alpha^k}{f'(\sigma_i \alpha)} = \sum_{l=0}^{n-1} (\sum_{i=1}^{n} \sigma_i \alpha^k \frac{\sigma_i \gamma_l}{f'(\sigma_i \alpha)}) x^l = \\ &= \sum_{l=0}^{n-1} (\sum_{i=1}^{n} \sigma_i (\alpha^k \frac{\gamma_l}{f'(\alpha)})) x^l = \sum_{l=0}^{n-1} \text{Sp}(\alpha^k \cdot \frac{\gamma_l}{f'(\alpha)}) x^l \end{aligned}$$

Koeffizientenvergleich liefert nun

$$\text{Sp}(\alpha^k \cdot \frac{\gamma_l}{f'(\alpha)}) = \delta_{kl},$$

was die Behauptung zeigt. ■

Beispiel: Sei $K = \mathbf{Q}(\alpha)$ mit $f(\alpha) = 0$, $f = 2x^3 + 3x^2 + 5x + 7$. Wir wollen mit dem Satz die Dualbasis zu $1, \alpha, \alpha^2$ bestimmen. Mit Maple finden wir

$$f(x) = ((5 + 3t + 2t^2) + (3 + 2t)x + 2x^2)(x - t) + f(t),$$

woraus sich sofort

$$\frac{f(x)}{x - \alpha} = \gamma_0 + \gamma_1 x + \gamma_2 x^2 \quad \text{mit} \quad \gamma_0 = 5 + 3\alpha + 2\alpha^2, \quad \gamma_1 = 3 + 2\alpha, \quad \gamma_2 = 2$$

ergibt. Nun ist $f'(x) = 5 + 6x + 6x^2$ und

$$\frac{1}{f'(\alpha)} = \frac{29}{3043} - \frac{96}{3043}\alpha + \frac{84}{3043}\alpha^2,$$

woraus man dann durch Multiplikation die Dualbasis $\beta_i = \frac{\gamma_i}{f'(\alpha)}$ erhält:

$$\begin{aligned} \beta_0 &= \frac{817}{3043} - \frac{501}{3043}\alpha + \frac{58}{3043}\alpha^2 \\ \beta_1 &= -\frac{501}{3043} - \frac{650}{3043}\alpha - \frac{192}{3043}\alpha^2 \\ \beta_2 &= \frac{58}{3043} - \frac{192}{3043}\alpha + \frac{168}{3043}\alpha^2 \end{aligned}$$

Tatsächlich liefert ein Test, dass $\text{Sp}(\alpha^i \beta_j) = \delta_{ij}$ gilt $(i, j = 0, 1, 2)$.

Das Lemma zeigt, wie man die Koeffienten eines Elements $\alpha \in K$ bzgl. einer $\mathbf{Q}$-Basis mit Hilfe der komplexen Zahlen $\sigma_1\alpha, \ldots, \sigma_n\alpha$ abschätzen kann.

LEMMA. *Sei $\omega_1, \ldots, \omega_n$ eine $\mathbf{Q}$-Basis des Zahlkörpers K, $\delta_1, \ldots, \delta_n$ die dazu duale Basis, $\sigma_1, \ldots, \sigma_n : K \to \mathbf{C}$ die komplexen Einbettungen und $M = \max(|\sigma_i \delta_j| : 1 \leq i, j \leq n)$. Ist $\alpha \in K$ mit $\alpha = \sum_i x_i \omega_i$, $x_i \in \mathbf{Q}$, so gilt*

$$x_i = \text{Sp}(\alpha \delta_i) \quad \textit{und} \quad |x_i| \leq nM \max(|\sigma_j \alpha| : 1 \leq j \leq n).$$

Beweis: Es gilt

$$\mathrm{Sp}(\alpha\delta_i) = \mathrm{Sp}(\sum_j x_j\omega_j\delta_i) = \sum_j x_j \mathrm{Sp}(\omega_j\delta_i) = x_i$$

und damit

$$x_i = \mathrm{Sp}(\alpha\delta_i) = \sum_j \sigma_j(\alpha\delta_i) = \sum_j \sigma_j(\alpha)\sigma_j(\delta_i),$$

also

$$|x_i| \leq \sum_j |\sigma_j(\alpha)||\sigma_j(\delta_i)| \leq \sum_j |\sigma_j(\alpha)| \cdot M \leq nM \max(|\sigma_j(\alpha)| : 1 \leq j \leq n),$$

was gezeigt werden sollte. ■

KAPITEL 3

Faktorisierung von Polynomen über Zahlkörpern

1. Einführung

Ist K ein Körper, so macht die Polynomdivision den Polynomring $K[x]$ zu einem euklidischen Ring: Zu $f(x), g(x) \in K[x]$ mit $g(x) \neq 0$ gibt es $q(x), r(x) \in K[x]$ mit

$$f(x) = q(x)g(x) + r(x) \quad \text{mit} \quad \operatorname{grad}(r(x)) < \operatorname{grad}(g(x)) \quad \text{oder} \quad r(x) = 0.$$

Dabei sind der Quotient $q(x)$ und der Rest $r(x)$ eindeutig bestimmt. Der euklidische Algorithmus liefert den ggT zweier Polynome, den wir immer als normiertes Polynom annehmen (außer im Fall $\operatorname{ggT}(0,0)$). Jeder euklidische Ring ist auch faktoriell, d.h. jedes Polynom $f(x) \in K[x] \setminus \{0\}$ hat eine eindeutige Primfaktorzerlegung

$$f(x) = c \cdot p_1(x)^{e_1} \cdot \cdots \cdot p_r(x)^{e_r}$$

mit $c \in K^*$ und (paarweise verschiedenen) normierten irreduziblen Polynomen $p_i(x)$ (vom Grad ≥ 1).

Die explizite Primfaktorzerlegung von Polynomen aus $\mathbf{F}_p[x]$ oder $\mathbf{Q}[x]$ ist eine wichtige Aufgabe und wird in der Algebra behandelt. Maple stellt dafür die Funktionen 'Factor(f) mod p' bzw. 'factor(f)' zur Verfügung.

Wir wollen hier zeigen, wie man Polynome über Zahlkörpern K faktorisieren kann, wenn man Polynome aus $\mathbf{Q}[x]$ faktorisieren kann.

2. Die Normabbildung für Polynome

Sei K ein Zahlkörper vom Grad n über $\mathbf{Q}$. Ist $\omega_1, \ldots, \omega_n$ eine $\mathbf{Q}$-Basis von K, so liefert jedes $\alpha \in K$ eine Matrix $A(\alpha) \in M_n(\mathbf{Q})$ vermöge

$$\alpha \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = A(\alpha) \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix}.$$

Die Zuordnung

$$K \to M_n(\mathbf{Q}), \quad \alpha \mapsto A(\alpha)$$

ist ein (injektiver) Ringhomomorphismus, der sich natürlich zu einem Ringhomorphismus

$$A : K[x] \to M_n(\mathbf{Q}[x]), \quad \sum_{i=0}^{m} \alpha_i x^i \mapsto \sum_{i=0}^{m} A(\alpha_i) x^i$$

fortsetzt. Durch Determinantenbildung erhalten wir eine Fortsetzung der (multiplikativen) Normabbildung:

$$\mathrm{N} : K[x] \to \mathbf{Q}[x], \quad F(x) \mapsto \det A(F(x)).$$

(Man sieht leicht, dass die Norm nicht von der gewählten $\mathbf{Q}$-Basis von K abhängt.)
Seien $\sigma_1, \ldots, \sigma_n : K \hookrightarrow \mathbf{C}$ die komplexen Einbettungen der Zahlkörpers. Durch

$$\sigma_i : K[x] \to \mathbf{C}[x], \quad \sum_{j=0}^{m} \alpha_j x^j \mapsto \sum_{j=0}^{m} (\sigma_i \alpha_j) x^j$$

wird eine Fortsetzung auf Polynome definiert. Es gilt der Satz:

Version vom 18.2.2003

SATZ.

$$\mathrm{N}(F(x)) = (\sigma_1 F(x)) \cdot \cdots \cdot (\sigma_n F(x)).$$

Beweis: Wir wissen, dass es eine Matrix $S \in GL_n(\mathbf{C})$ gibt, sodass für alle $\alpha \in K$ gilt

$$A(\alpha) = S^{-1} \begin{pmatrix} \sigma_1(\alpha) & & \\ & \ddots & \\ & & \sigma_n(\alpha) \end{pmatrix} S.$$

Dann folgt aber sofort für alle $F(x) \in K[x]$

$$A(F(x)) = S^{-1} \begin{pmatrix} \sigma_1(F(x)) & & \\ & \ddots & \\ & & \sigma_n(F(x)) \end{pmatrix} S.$$

Determinantenbildung liefert die Behauptung. ■

Unmittelbar sieht man:

FOLGERUNG. *Ist K ein Zahlkörper vom Grad n über $\mathbf{Q}$, so gilt für $F(x) \in K[x]$:*

$$\mathrm{grad}(\mathrm{N}(F(x)) = n \cdot \mathrm{grad}(F(x)).$$

Ist $f(x) \in \mathbf{Q}[x]$, so gilt

$$\mathrm{N}(f(x)) = f(x)^n.$$

Ein wichtiges Beispiel für die Norm von Polynomen gibt der folgende Satz:

SATZ. *Ist $K = \mathbf{Q}(\alpha)$ und $f(x)$ das (normierte) Minimalpolynom von α, so gilt*

$$\mathrm{N}(x - \alpha) = f(x).$$

Beweis: Sind $\alpha_1, \ldots, \alpha_n \in \mathbf{C}$ die komplexen Nullstellen des Polynoms $f(x)$, d.h. $f(x) = (x-\alpha_1) \ldots (x-\alpha_n)$ in $\mathbf{C}[x]$, so sind die komplexen Einbettungen $\sigma_i : K \hookrightarrow \mathbf{C}$ gegeben durch $\sigma_i(\alpha) = \alpha_i$. Dann gilt

$$\mathrm{N}(x-\alpha) = \sigma_1(x-\alpha) \ldots \sigma_n(x-\alpha) = (x-\sigma_1(\alpha)) \ldots (x-\sigma_n(\alpha)) = (x-\alpha_1) \ldots (x-\alpha_n) = f(x),$$

was gezeigt werden sollte. ■

LEMMA. *Für $F(x) \in K[x]$ gilt*

$$F(x) | \mathrm{N}(F(x)).$$

Beweis: Wir dividieren in $K[x]$ das Polynom $\mathrm{N}(F(x))$ durch $F(x)$ mit Rest:

$$\mathrm{N}(F(x)) = G(x)F(x) + R(x) \quad \text{mit} \quad \mathrm{grad}R(x) < \mathrm{grad}F(x).$$

Wir wenden σ_i an und erhalten (unter Verwendung von $\sigma_i \mathrm{N}(F(x)) = \mathrm{N}(F(x))$):

$$\mathrm{N}(F(x)) = (\sigma_i G)(x)(\sigma_i F)(x) + (\sigma_i R)(x).$$

Mit $\mathrm{N}(F(x)) = \prod_j (\sigma_j F)(x)$ folgt $(\sigma_i F)(x) | (\sigma_i R)(x)$, was sofort $(\sigma_i R)(x) = 0$, also $R(x) = 0$ impliziert. Damit folgt die Behauptung. ■

Wir erhalten nun den ersten Zerlegungssatz:

SATZ. *Sei $F(x) \in K[x]$ ein normiertes Polynom und $\mathrm{N}(F(x)) = g_1(x)g_2(x)$ eine nichttriviale Zerlegung der Norm in $\mathbf{Q}[x]$ mit $\mathrm{ggT}(g_1(x), g_2(x)) = 1$. Dann ist auch*

$$F(x) = \mathrm{ggT}(F(x), g_1(x)) \cdot \mathrm{ggT}(F(x), g_2(x))$$

eine nichttriviale Zerlegung von $F(x)$ in $K[x]$.

Beweis: Da $F(x)$ normiert ist und $F(x)|\mathrm{N}(F(x))$ gilt, folgt

$$F(x) = \mathrm{ggT}(F(x), \mathrm{N}(F(x))) = \mathrm{ggT}(F(x), g_1(x)g_2(x)) = \mathrm{ggT}(F(x), g_1(x)) \cdot \mathrm{ggT}(F(x), g_2(x)).$$

Wäre die Zerlegung trivial, so hätte man (nach eventueller Vertauschung von $g_1(x)$ und $g_2(x)$) o.E. $\mathrm{ggT}(F(x), g_1(x)) = F(x)$, also $F(x)|g_1(x)$. Normbildung ergäbe $\mathrm{N}(F(x))|g_1(x)^n$, also $g_1(x)g_2(x)|g_1(x)^n$, daher $g_2(x)|g_1(x)^{n-1}$, ein offensichtlicher Widerspruch. Daher ist die angegebene Zerlegung nicht trivial. ■

Beispiel: $K = \mathbf{Q}(\alpha)$ mit $\alpha^2 = 2$ und $F = x^3 + (\alpha - 2)x - 2 \in K[x]$. Berechnung und Faktorisierung der Norm liefert

$$\mathrm{N}(F) = x^6 - 4x^4 - 4x^3 + 2x^2 + 8x + 4 = (x^2 - 2)(x^4 - 2x^2 - 4x - 2).$$

Nun berechnet man

$$\mathrm{ggT}(F, x^2 - 2) = x - \alpha$$

und erhält die Zerlegung

$$F = (x - \alpha)(x^2 + \alpha x + \alpha).$$

Läßt sich die Norm eines Polynoms $F(x) \in K[x]$ in zwei teilerfremde Teile zerlegen, erhält man also eine nichttriviale Faktorisierung. Daraus ergibt sich unmittelbar:

LEMMA. *Für ein Polynom $F(x) \in K[x]$ gilt:*

$$F(x) \text{ irreduzibel in } K[x] \quad \Longrightarrow \quad \mathrm{N}(F(x)) \text{ Potenz eines irreduziblen Polynoms aus } \mathbf{Q}[x],$$
$$F(x) \text{ irreduzibel in } K[x] \quad \Longleftarrow \quad \mathrm{N}(F(x)) \text{ irreduzibel in } \mathbf{Q}[x].$$

Das folgende Beispiel zeigt, dass das Lemma nicht wesentlich verschärft werden kann.

Beispiel: $K = \mathbf{Q}(\alpha)$ mit $\alpha^2 = 2$.

1. $F = x^2 + 1$ hat Norm $(x^2 + 1)^2$, F ist irreduzibel in $K[x]$.
2. $F = (x - \alpha)(x + \alpha)$ hat Norm $(x^2 - 2)^2$, F ist reduzibel in $K[x]$.

Bevor wir die Faktorisierung von Polynomen aus $K[x]$ allgemein angehen können, müssen wir noch einige allgemeine Eigenschaften von Polynomen zusammenstellen.

3. Wie macht man ein Polynom quadratfrei?

LEMMA. *Sei K ein Körper der Charakteristik 0 und $f(x) \in K[x]$. Ist*

$$f(x) = c \cdot p_1(x)^{e_1} \dots p_r(x)^{e_r}$$

die Primfaktorzerlegung von $f(x)$ mit $c \in K^*$ und (paarweise verschiedenen) normierten irreduziblen Polynomen $p_i(x)$ und $e_i \geq 1$, so gilt

$$\mathrm{ggT}(f(x), f'(x)) = p_1(x)^{e_1 - 1} \dots p_r(x)^{e_r - 1} \quad \text{und} \quad \frac{f(x)}{\mathrm{ggT}(f(x), f'(x))} = c \cdot p_1(x) \dots p_r(x).$$

Beweis: Wir schreiben $f(x) = c \cdot p_i(x)^{e_i} r_i(x)$ mit $p_i(x) \nmid r_i(x)$. Dann ist

$$f'(x) = ce_i p_i(x)^{e_i - 1} p_i'(x) r_i(x) + cp_i(x)^{e_i} r_i'(x) = cp_i(x)^{e_i - 1}[e_i p_i'(x) r_i(x) + p_i(x) r_i'(x)].$$

Da K Charakteristik 0 hat, teil $p_i(x)$ das Polynom $e_i p_i'(x)$ nicht, also teilt $p_i(x)$ das Polynom $f'(x)$ genau $(e_i - 1)$ mal. Also folgt für die Primfaktorzerlegung von $f'(x)$:

$$f'(x) = p_1(x)^{e_1 - 1} \dots p_r(x)^{e_r - 1} \cdot r(x) \quad \text{mit} \quad p_i(x) \nmid r(x).$$

Damit folgt

$$\mathrm{ggT}(f(x), f'(x)) = p_1(x)^{e_1 - 1} \dots p_r(x)^{e_r - 1} \quad \text{und} \quad \frac{f(x)}{\mathrm{ggT}(f(x), f'(x))} = c \cdot p_1(x) \dots p_r(x),$$

wie behauptet. ■

Wir formulieren das Lemma für die Anwendung:

FOLGERUNG. *Sei K ein Körper der Charakteristik 0 und $f(x) \in K[x]$ ein Polynom vom Grad ≥ 1.*

1. *Das Polynom* $\frac{f(x)}{\mathrm{ggT}(f(x),f'(x))}$ *ist quadratfrei.*
2. *Hat das Polynom* $\frac{f(x)}{\mathrm{ggT}(f(x),f'(x))}$ *die Primfaktorzerlegung*

$$\frac{f(x)}{\mathrm{ggT}(f(x),f'(x))} = c \cdot p_1(x) \dots p_r(x),$$

so gilt

$$f(x) = c \cdot p_1(x)^{e_1} \dots p_r(x)^{e_r} \quad \textit{mit} \quad e_i \geq 1.$$

Die e_i*'s kann man bestimmen, indem man testet, wie oft* $p_i(x)$ *das Polynom* $f(x)$ *teilt.*

Die Folgerung zeigt, wie man sich beim Faktorisieren von Polynomen leicht auf quadratfreie Polynome zurückziehen kann.

Eine weitere Folgerung aus unserem Lemma:

FOLGERUNG. *Sei* K *ein Körper der Charakteristik* 0 *und* $f(x) \in K[x]$ *ein Polynom. Dann gilt:*

$$f(x) \textit{ quadratfrei} \quad \Longleftrightarrow \quad \mathrm{ggT}(f(x), f'(x)) = 1.$$

4. Faktorisierung von Polynomen über Zahlkörpern

Der folgende Satz zeigt, wie man durch eine einfache Variablentransformation erreichen kann, dass die Norm eines quadratfreien Polynoms quadratfrei wird:

SATZ. *Ist* $F(x) \in K[x]$ *quadratfrei,* $\mathrm{grad} F(x) \geq 1$, $K = \mathbf{Q}(\alpha)$, *so ist die Norm* $\mathbf{N}(F(x - k\alpha)) \in \mathbf{Q}[x]$ *für alle bis auf endliche viele* $k \in \mathbf{Z}$ *quadratfrei.*

Beweis: Sei

$$\sigma_i F(x) = c_i \prod_{r=1}^{d} (x - u_{ir}) \quad \text{mit} \quad c_i, u_{ir} \in \mathbf{C}.$$

Da $F(x)$ als quadratfrei vorausgesetzt ist, gilt $u_{ir} \neq u_{is}$ für $r \neq s$. Wir erhalten aus

$$\sigma_i(F(x - k\alpha)) = (\sigma_i F)(x - k\sigma_i\alpha) = c_i \prod_{r=1}^{d} (x - k\sigma_i\alpha - u_{ir})$$

durch Produktbildung

$$\mathrm{N}(F(x - k\alpha)) = \prod_{i=1}^{d} \sigma_i(F(x - k\alpha)) = \prod_{i=1}^{n} c_i \prod_{r=1}^{d} (x - k\sigma_i\alpha - u_{ir}).$$

Nun gelten die Äquivalenzen:

$$\begin{aligned}
& \mathrm{N}(F(x - k\alpha)) \text{ nicht quadratfrei} \\
\Longleftrightarrow \quad & x - k\sigma_i\alpha - u_{ir} = x - k\sigma_j\alpha - u_{js} \text{ für Indizes } i,j,r,s \text{ mit } (i,r) \neq (j,s) \\
\Longleftrightarrow \quad & k(\sigma_i\alpha - \sigma_j\alpha) = u_{ir} - u_{js} \text{ für Indizes } i,j,r,s \text{ mit } (i,r) \neq (j,s) \\
& (\text{Aus } \sigma_i\alpha = \sigma_j\alpha \text{ würde } i = j \text{ und } u_{ir} = u_{js} \text{ und damit } (i,r) = (j,s) \text{ folgen.}) \\
\Longleftrightarrow \quad & k(\sigma_i\alpha - \sigma_j\alpha) = u_{ir} - u_{js} \text{ für Indizes } i,j,r,s \text{ mit } i \neq j \\
\Longleftrightarrow \quad & k = \frac{u_{ir} - u_{js}}{\sigma_i\alpha - \sigma_j\alpha} \text{ für Indizes } i,j,r,s \text{ mit } i \neq j \\
\Longleftrightarrow \quad & k \in \{\frac{u_{ir} - u_{js}}{\sigma_i\alpha - \sigma_j\alpha} : 1 \leq i,j \leq n, 1 \leq r,s \leq d \text{ mit } i \neq j\}.
\end{aligned}$$

Dies liefert sofort die Behauptung. ■

Wir stellen unsere Ergebnisse zusammen:

SATZ. *Sei* $K = \mathbf{Q}(\alpha)$ *ein Zahlkörper und* $F(x) \in K[x]$ *ein Polynom vom Grad* d *mit* $F(x) = cx^d + \dots$.

1. *Das Polynom*
$$G(x) = \frac{F(x)}{c \cdot \mathrm{ggT}(F(x), F'(x))} \in K[x]$$
ist normiert und quadratfrei.
2. *Für* $k \in \mathbf{Z}$ *ist*
$$g_k(x) = \mathrm{N}(G(x - k\alpha)) \in \mathbf{Q}[x]$$
normiert. (Für alle bis auf endlich viele $k \in \mathbf{Z}$ *ist* $g_k(x)$ *quadratfrei, d.h.* $\mathrm{ggT}(g_k(x), g_k'(x)) = 1$*.)*
3. *Gilt* $\mathrm{ggT}(g_k(x), g_k'(x)) = 1$ *und ist*
$$g_k(x) = p_1(x) \dots p_r(x)$$
die Primfaktorzerlegung von $g_k(x)$ *in* $\mathbf{Q}[x]$*, so sind*
$$P_i(x) = \mathrm{ggT}(G(x), p_i(x + k\alpha)), \quad i = 1, \dots, r$$
die Primteiler von $F(x)$*, d.h. es gibt eine Faktorisierung*
$$F(x) = c \cdot P_1(x)^{e_1} \dots P_r(x)^{e_r}$$
mit $e_i \geq 1$*.*

Beweis: Aus $P_i(x) = \mathrm{ggT}(G(x), p_i(x + k\alpha))$ folgt durch Variablentransformation
$$P_i(x - k\alpha) = \mathrm{ggT}(G(x - k\alpha), p_i(x)).$$
(Wie zuvor sieht man, dass P_i nicht konstant ist.) Zunächst gilt $P_i(x - k\alpha) | G(x - k\alpha)$, also
$$\mathrm{N}(P_i(x - k\alpha)) | \mathrm{N}(G(x - k\alpha)) = p_1(x) \dots p_r(x).$$
Aus $P_i(x - k\alpha) | p_i(x)$ folgt
$$\mathrm{N}(P_i(x - k\alpha)) | p_i(x)^n,$$
was wegen der paarweisen Teilerfremdheit der $p_i(x)$'s
$$\mathrm{N}(P_i(x - k\alpha)) | \mathrm{ggT}(p_1(x) \dots p_r(x), p_i(x)^n) = p_i(x), \quad \text{also} \quad \mathrm{N}(P_i(x - k\alpha)) | p_i(x)$$
liefert. Nun ist $\mathrm{N}(P_i(x - k\alpha)) \in \mathbf{Q}[x]$ normiert, nichtkonstant und $p_i(x) \in \mathbf{Q}[x]$ normiert und irreduzibel, daher ergibt sich
$$\mathrm{N}(P_i(x - k\alpha)) = p_i(x).$$
Hieraus folgt sofort die Irreduzibilität von $P_i(x - k\alpha)$ und damit die von $P_i(x)$. Wir haben weiter
$$\begin{aligned} G(x - k\alpha) &= \mathrm{ggT}(G(x - k\alpha), \mathrm{N}(G(x - k\alpha))) = \mathrm{ggT}(G(x - k\alpha), g_k(x)) = \\ &= \mathrm{ggT}(G(x - k\alpha), p_1(x) \dots p_r(x)) = \\ &= \mathrm{ggT}(G(x - k\alpha), p_1(x)) \dots \mathrm{ggT}(G(x - k\alpha), p_r(r)) = \\ &= P_1(x - k\alpha) \dots P_r(x - k\alpha), \end{aligned}$$
was sofort $G(x) = P_1(x) \dots P_r(x)$ liefert. Da $F(x)$ und $G(x)$ die gleichen Primteiler besitzen, folgt die Behauptung. ■

Bemerkung: Um den Satz anzuwenden, muss man in 3. nur solange probieren, bis man ein $k \in \mathbf{Z}$ findet mit $\mathrm{ggT}(g_k(x), g_k'(x)) = 1$.

Beispiel: Wir betrachten $K = \mathbf{Q}(\alpha)$ mit $\alpha^2 = 2$ und $F(x) = x^2 - 2$. Dann ist $G(x) = F(x) = x^2 - 2$.

$g_0 = (x^2 - 2)^2$	$\mathrm{ggT}(g_0, g_0') = x^2 - 2$	nicht quadratfrei
$g_1 = x^4 - 8x^2$	$\mathrm{ggT}(g_1, g_1') = x$	nicht quadratfrei
$g_2 = x^4 - 20x^2 + 36$	$\mathrm{ggT}(g_2, g_2') = 1$	quadratfrei

Wir erhalten in $\mathbf{Q}[x]$ die Faktorisierung $g_2(x) = p_1(x)p_2(x)$ mit $p_1(x) = x^2 - 2$, $p_2(x) = x^2 - 18$ und berechnen daraus
$$\begin{aligned} P_1(x) &= \mathrm{ggT}(G(x), p_1(x + 2\alpha)) = \mathrm{ggT}(x^2 - 2, x^2 + 4\alpha x + 6) = x + \alpha, \\ P_2(x) &= \mathrm{ggT}(G(x), p_2(x + 2\alpha)) = \mathrm{ggT}(x^2 - 2, x^2 + 4\alpha x - 10) = x - \alpha. \end{aligned}$$
Dies führt zur Primfaktorzerlegung $f(x) = (x + \alpha)(x - \alpha)$ in $K[x]$.

5. Anwendungen

Wir geben ein paar einfache Anwendungsbeispiele für das Faktorisierungsverfahren. Sei $K = \mathbf{Q}(\alpha)$ ein Zahlkörper und $f(x) \in \mathbf{Q}[x]$ das Minimalpolynom von α.

Wurzelziehen: Will man testen, ob $\beta \in K^*$ eine m-te Potenz ist, faktorisiert man $x^m - \beta$ über K. Genau dann gibt es ein $\gamma \in K$ mit $\gamma^m = \beta$, wenn $x^m - \beta$ einen Faktor $x - \gamma$ besitzt.

Einheitswurzeln: Welche m-ten Einheitswurzeln liegen in K? Zu diesem Zweck faktorisiert man einfach $x^m - 1$ über K.

Galoissche Körpererweiterung: $K = \mathbf{Q}(\alpha)$ ist genau dann eine galoissche Körpererweiterung von $\mathbf{Q}$, wenn das Polynom das Minimalpolynom $f(x)$ von α in lauter Linearfaktoren über K zerfällt.

Beispiel: Wir betrachten $K = \mathbf{Q}(\alpha)$ mit $f(\alpha) = 0$ und $f(x) = x^4 - 2x^2 + 9$. Faktorisieren von $x^8 - 1$ ergibt

$$\begin{aligned} x^8 - 1 \;=\; & (x-1)(x+1)(x + \frac{5}{12}\alpha - \frac{1}{12}\alpha^3 - \frac{1}{4} + \frac{1}{4}\alpha^2)(x + \frac{5}{12}\alpha - \frac{1}{12}\alpha^3 + \frac{1}{4} - \frac{1}{4}\alpha^2) \\ & \cdot(x - \frac{5}{12}\alpha + \frac{1}{12}\alpha^3 - \frac{1}{4} + \frac{1}{4}\alpha^2)(x + \frac{1}{4} + \frac{1}{12}\alpha^3 - \frac{1}{4}\alpha^2 - \frac{5}{12}\alpha) \\ & \cdot(x - \frac{1}{6}\alpha - \frac{1}{6}\alpha^3)(x + \frac{1}{6}\alpha + \frac{1}{6}\alpha^3), \end{aligned}$$

also enthält K alle 8-ten Einheitswurzeln. Faktorisieren des Minimalpolynoms von α liefert

$$f = (x - \alpha)(x + \alpha)(x - (\frac{1}{3}\alpha^3 - \frac{2}{3}\alpha))(x - (-\frac{1}{3}\alpha^3 + \frac{2}{3}\alpha)),$$

d.h. f zerfällt über K in Linearfaktoren, K ist also galoissch über $\mathbf{Q}$. Die Konjugierten von α sind

$$\alpha, \quad -\alpha, \quad \frac{1}{3}\alpha^3 - \frac{2}{3}\alpha, \quad -\frac{1}{3}\alpha^3 + \frac{2}{3}\alpha.$$

Beispiel: $K = \mathbf{Q}(\alpha)$ mit $\alpha^3 - 3\alpha - 1 = 0$. Das Minimalpolynom $f(x) = x^3 - 3x - 1$ von α faktorisiert über K als

$$f(x) = (x - \alpha)(x + \alpha^2 - 2)(x - \alpha^2 + \alpha + 2),$$

also ist K galoissch über $\mathbf{Q}$.

Das Teilkörperproblem: Wie kann man für zwei Zahlkörper K und L entscheiden, ob K ein Teilkörper von L ist? Etwas präziser stellen wir die Frage: Gibt es einen Körperhomorphismus $K \hookrightarrow L$? Eine notwendige Bedingung ist natürlich die Gradbedingung $[K : \mathbf{Q}] | [L : \mathbf{Q}]$. Ein präzises Kriterium gibt der folgende Satz.

SATZ. *Seien $K = \mathbf{Q}(\alpha)$, $L = \mathbf{Q}(\beta)$ Zahlkörper mit $f(\alpha) = 0$, $g(\beta) = 0$, $f(x)$ und $g(x)$ die Minimalpolynome von α bzw. β. Dann gilt:*

1. *Gibt es einen Körperhomomorphismus $\phi : K \hookrightarrow L$, dann ist $f(\phi(\alpha)) = 0$, d.h. $f(x)$ spaltet in $L[x]$ den Linearfaktor $x - \phi(\alpha)$ ab.*
2. *Gibt es ein $\widetilde{\alpha} \in L$ mit $f(\alpha) = 0$, d.h. spaltet $f(x)$ in $L[x]$ einen Linearfaktor $x - \widetilde{\alpha}$ ab, so definiert*

$$\phi : K \hookrightarrow L, \quad \alpha \mapsto \widetilde{\alpha}$$

einen Körperhomomorphismus.

Beweis:

1. Ist $\phi : K \to L$ ein Körperhomomorphismus, so folgt

$$f(\phi(\alpha)) = \phi(f(\alpha)) = \phi(0) = 0,$$

d.h. das Polynom $f(x) \in \mathbf{Q}[x]$ spaltet in $L[x]$ einen Linearfaktor $x - \phi(\alpha)$ ab.

2. Spaltet umgekehrt $f(x)$ in $L[x]$ einen Linearfaktor $x - \widetilde{\alpha}$ ab, so liegt $f(x)$ im Kern der Abbildung

$$\mathbf{Q}[t] \to L, \quad t \mapsto \widetilde{\alpha},$$

also erhalten wir einen Homomorphismus

$$\phi : K \simeq \mathbf{Q}[t]/(f(t)) \to L,$$

wie behauptet. ■

Bemerkung: Wendet man das Kriterium im Fall $[K : \mathbf{Q}] = [L : \mathbf{Q}]$ an, so kann man damit entscheiden, ob die Zahlkörper K und L isomorph sind.

KAPITEL 4

Moduln

1. Definition

Sei K ein Zahlkörper vom Grad n. Eine Teilmenge $U \subseteq K$ heißt ein Modul, wenn es $\alpha_1, \ldots, \alpha_m \in K$ gibt mit

$$U = \mathbf{Z}\alpha_1 + \cdots + \mathbf{Z}\alpha_m = \{x_1\alpha_1 + \cdots + x_m\alpha_m : x_1, \ldots, x_m \in \mathbf{Z}\} \quad \text{und} \quad \mathbf{Q}\alpha_1 + \cdots + \mathbf{Q}\alpha_m = K.$$

Durch die Addition in K ist U also eine abelsche Gruppe. U wird als abelsche Gruppe von endlich vielen Elementen erzeugt (U ist ein endlich erzeugter $\mathbf{Z}$-Modul), und U enthält eine $\mathbf{Q}$-Basis von K. Die Elemente $\alpha_1, \ldots, \alpha_m$ werden auch ein Erzeugendensystem von U genannt.

Überlegung: Sei K ein Zahlkörper mit $\mathbf{Q}$-Basis $\omega_1, \ldots, \omega_n$ und

$$U = \mathbf{Z}\alpha_1 + \cdots + \mathbf{Z}\alpha_m$$

ein Modul in K. Dann gibt es $x_{ij} \in \mathbf{Q}$ mit

$$\alpha_i = \sum_j x_{ij}\omega_j \quad \text{bzw.} \quad \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} = M \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} \quad \text{mit} \quad M = (x_{ij}) \in M(m \times n, \mathbf{Q}).$$

Die Tatsache, dass U als Modul eine $\mathbf{Q}$-Basis von K enthält, ist gleichwertig damit, dass die Matrix M Rang n hat.
Mit folgenden Operationen kann man das Erzeugendensystem abändern ohne den Modul U zu ändern:

- Ersetzen von α_i durch $-\alpha_i$.
- Vertauschung von α_i und α_j.
- Ersetzen von α_j durch $\alpha_j + k\alpha_i$ für $i \neq j$ und $k \in \mathbf{Z}$. (Denn: $\mathbf{Z}\alpha_i + \mathbf{Z}\alpha_j = \mathbf{Z}\alpha_i + \mathbf{Z}(\alpha_j + k\alpha_i)$.)

Für die Matrix M übersetzt sich dies in folgende **elementare Zeilenumformungen:**

- Multiplikation einer Zeile mit -1.
- Vertauschung zweier Zeilen.
- Addition des k-fachen einer Zeile zu einer davon verschiedenen Zeile für $k \in \mathbf{Z}$.

Welche Normalform kann man erhalten?

Beispiel: In $K = \mathbf{Q}(\omega)$ mit $\omega^2 = d$, $d \in \mathbf{Z}$ quadratfrei $\neq 0, 1$, betrachten wir

$$U = \mathbf{Z}(2 + 3\omega) + \mathbf{Z}(4 + 5\omega) + \mathbf{Z}(6 + 7\omega).$$

Die beschreibende Matrix erhalten wir aus

$$\begin{pmatrix} 2 + 3\omega \\ 4 + 5\omega \\ 6 + 7\omega \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 4 & 5 \\ 6 & 7 \end{pmatrix} \begin{pmatrix} 1 \\ \omega \end{pmatrix},$$

die sich durch elementare Zeilenoperationen leicht in

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}$$

transformieren läßt. Damit erhalten wir

$$U = \mathbf{Z} \cdot 2 + \mathbf{Z}\omega,$$

was insbesondere zeigt, dass U ein Modul in K ist.

Beispiel: In $K = \mathbf{Q}(\alpha)$ mit $f(\alpha) = 0$ und $f = x^3 + 7x + 20$ betrachten wir für $\beta = \frac{1}{2}\alpha + \frac{1}{2}\alpha^2$ den Modul $U = \mathbf{Z} + \mathbf{Z}\beta + \mathbf{Z}\beta^2$. Nun ist

$$\begin{pmatrix} 1 \\ \beta \\ \beta^2 \end{pmatrix} = \begin{pmatrix} 1 \\ \frac{1}{2}\alpha + \frac{1}{2}\alpha^2 \\ -10 - \frac{17}{2}\alpha - \frac{3}{2}\alpha^2 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 1 \\ -20 & -17 & -3 \end{pmatrix}\begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \end{pmatrix}.$$

Durch elementare Zeilenoperationen transformiert man obige Matrix in

$$\frac{1}{2}\begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 14 \end{pmatrix},$$

so dass wir jetzt schreiben können

$$U = \mathbf{Z} + \mathbf{Z}(\frac{1}{2}\alpha + \frac{1}{2}\alpha^2) + \mathbf{Z} \cdot 7\alpha^2.$$

Was in den Beispielen gemacht wurde, läßt sich nun leicht allgemein machen.

2. Die Hermitesche Normalform von Matrizen

Wir haben jetzt folgende Situation: Gegeben ist eine Matrix $M \in M(m \times n, \mathbf{Q})$ vom Rang n. Wir wollen durch elementare Zeilenumformungen eine Normalform erreichen.
Bevor wir einen allgemeinen Algorithmus zur Normalisierung einer Matrix formulieren, betrachten wir noch kurz Nenner von rationalen Zahlen.

Nenner: Ist $s \in \mathbf{Q}$, so kann man eindeutig schreiben

$$s = \frac{a}{d} \quad \text{mit } a \in \mathbf{Z}, \quad d \in \mathbf{N}, \quad \mathrm{ggT}(a, d) = 1.$$

d heißt der Nenner von s. Der Nenner läßt sich auch durch $d = \min\{x \in \mathbf{N} : xs \in \mathbf{Z}\}$ charakterisieren. Sind $s_1, \ldots, s_m \in \mathbf{Q}$ und ist $d \in \mathbf{N}$ mit

$$s_1 = \frac{a_1}{d}, \ldots, s_m = \frac{a_m}{d} \quad \text{und} \quad a_i \in \mathbf{Z},$$

so heißt d ein gemeinsamer Nenner von $s_1, \ldots, s_m$.

Lemma. *Seien* $s_1 = \frac{a_1}{d_1}, \ldots, s_m = \frac{a_m}{d_m} \in \mathbf{Q}$ *mit* $a_i \in \mathbf{Z}$, $d_i \in \mathbf{N}$ *und* $\mathrm{ggT}(a_i, d_i) = 1$. *Dann ist*

$$d = \mathrm{kgV}(d_1, \ldots, d_m)$$

der kleinste gemeinsame Nenner von $s_1, \ldots, s_m$, *d.h.*

$$d = \min\{\widetilde{d} \in \mathbf{N} : \widetilde{d}s_1, \ldots, \widetilde{d}s_m \in \mathbf{Z}\}.$$

Schreibt man $s_i = \frac{b_i}{d}$, *so gilt* $\mathrm{ggT}(d, b_1, \ldots, b_m) = 1$.

Beweis: Für $\widetilde{d} \in \mathbf{N}$ gilt (unter Benutzung von $\mathrm{ggT}(d_i, a_i) = 1$)

$$\begin{aligned} \widetilde{d}s_1, \ldots, \widetilde{d}s_m \in \mathbf{Z} \quad &\Longleftrightarrow \quad \frac{\widetilde{d}a_1}{d_1}, \ldots, \frac{\widetilde{d}a_m}{d_m} \in \mathbf{Z} \quad \Longleftrightarrow \quad d_1|\widetilde{d}a_1, \ldots, d_m|\widetilde{d}a_m \quad \Longleftrightarrow \\ &\Longleftrightarrow \quad d_1|\widetilde{d}, \ldots, d_m|\widetilde{d} \quad \Longleftrightarrow \quad \mathrm{kgV}(d_1, \ldots, d_m)|\widetilde{d}, \end{aligned}$$

was die erste Behauptung beweist. Die Aussage $\mathrm{ggT}(d, b_1, \ldots, b_m) = 1$ ist klar, denn andernfalls wäre $\frac{d}{\mathrm{ggT}(d, b_1, \ldots, b_m)}$ einen kleinerer gemeinsamer Nenner. ■

Angeregt durch die Beispiele stellen wir folgenden Algorithmus auf um eine Matrix mit elementaren Zeilentransformationen zu normalisieren:

Algorithmus: Sei $M = (b_{ij})$ eine $m \times n$-Matrix mit Koeffizienten in $\mathbf{Q}$ mit $\mathbf{Q}$-Rang n. Durch elementare Zeilentransformationen wird M in eine Matrix

$$\frac{1}{d}(c_{ij})_{i=1,\dots,m,j=1,\dots,n} = \frac{1}{d}\begin{pmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ & c_{22} & \dots & c_{2n} \\ & & \dots & \dots \\ & & & c_{nn} \\ & & & \end{pmatrix}$$

transformiert mit den Eigenschaften:

1. $d \in \mathbf{N}$ ist der kleinste gemeinsame Nenner der Einträge von M, $c_{ij} \in \mathbf{Z}$.
2. $c_{ii} > 0$ für alle i.
3. $c_{ij} = 0$ für $i > j$.
4. $0 \leq c_{ij} < c_{jj}$ für $1 \leq i < j$, d.h. die Einträge in der Spalte über c_{ii} liegen zwischen 0 und $c_{ii} - 1$.

Dazu gehen wir wie folgt vor:

1. Sei $d \geq 1$ der kleinste gemeinsame Nenner aller Zahlen b_{ij}. Dann ist $b_{ij} = \frac{a_{ij}}{d}$ mit $a_{ij} \in \mathbf{Z}$. Wir transformieren die Matrix $A = (a_{ij})$.
2. Für $k = 1, \dots, n$ führt man folgende Schritte durch: (Beginnt man den k-ten Schritt, haben die Spalten $1, 2, \dots, k-1$ bereits die gewünschte Form.)
   (a) Durch eventuelle Multiplikation der i-ten Zeile mit -1 erreicht man $a_{ik} \geq 0$ für $i = k, \dots, m$.
   (b) Durch Zeilenvertauschungen erreicht man, dass a_{kk} minimal $\neq 0$ unter den Zahlen a_{kk}, $a_{k+1,k}$, $a_{k+2,k}$, $\dots$, a_{mk} ist, d.h. es gilt dann für $i = k+1, \dots, m$:
   $$a_{ik} = 0 \quad \text{oder} \quad a_{kk} \leq a_{ik}.$$
   (c) Für $i = k+1, \dots, m$ subtrahiert man im Fall $a_{ik} > 0$ von der i-ten Zeile das $[\frac{a_{ik}}{a_{kk}}]$-fache der k-ten Zeile, d.h. man ersetzt für $j = k, \dots, n$ den Eintrag a_{ij} durch
   $$\widetilde{a}_{ij} = a_{ij} - [\frac{a_{ik}}{a_{kk}}]a_{kj}.$$
   (Dann ist $\widetilde{a}_{ik} = a_{ik} \bmod a_{kk}$ und somit $0 \leq \widetilde{a}_{ik} < a_{kk}$. Insbesondere verkleinert sich bei jedem solchen Schritt die Summe $\sum_{i=k+1}^{m} a_{ik} \geq 0$.)
   (d) Man wiederholt nun die Schritte (b) und (c), bis man $a_{ik} = 0$ für $i = k+1, \dots, m$ erreicht hat.
   (e) Für $i = 1, \dots, k-1$ subtrahiert man im Fall $a_{ik} > 0$ von der i-ten Zeile das $[\frac{a_{ik}}{a_{kk}}]$-fache der k-ten Zeile, d.h. man ersetzt für $j = k, \dots, n$ den Eintrag a_{ij} durch
   $$\widetilde{a}_{ij} = a_{ij} - [\frac{a_{ik}}{a_{kk}}]a_{kj}.$$
   (Dann ist $\widetilde{a}_{ik} = a_{ik} \bmod a_{kk}$ und somit $0 \leq \widetilde{a}_{ik} < a_{kk}$.)

Die erhaltene Matrix $\frac{1}{d}(c_{ij})$ wird auch als Hermitesche Normalform der Matrix M bezeichnet. (Die Eindeutigkeit wird später gezeigt werden.)

Beispiel: Wir wenden den Normalisierungsprozeß auf die Matrix

$$\begin{pmatrix} 2 & 3 & 5 \\ 7 & 11 & 13 \\ 17 & 19 & 23 \end{pmatrix}$$

an und erhalten nacheinander folgende Matrizen:

$$\begin{pmatrix} 2 & 3 & 5 \\ 1 & 2 & -2 \\ 1 & -5 & -17 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & -2 \\ 2 & 3 & 5 \\ 1 & -5 & -17 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & -2 \\ 0 & -1 & 9 \\ 0 & -7 & -15 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & -2 \\ 0 & 1 & -9 \\ 0 & 7 & 15 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 16 \\ 0 & 1 & -9 \\ 0 & 0 & 78 \end{pmatrix} \to$$

$$\begin{pmatrix} 1 & 0 & 16 \\ 0 & 1 & 69 \\ 0 & 0 & 78 \end{pmatrix},$$

wobei die letzte Matrix die Hermitesche Normalform der Ausgangsmatrix ist.

Bemerkung: In Maple gibt es die Funktion 'linalg[ihermite]', die zu einer Matrix die Hermitesche Normalform bestimmt.

Bevor wir den hermiteschen Normalisierungsprozess durch Matrizen beschreiben, erinnern wir an die Definition der Gruppe $GL_m(\mathbf{Z})$:

$$GL_m(\mathbf{Z}) = \{M \in M_m(\mathbf{Z}) : \text{ es gibt eine Matrix } \widetilde{M} \text{ mit } M\widetilde{M} = \widetilde{M}M = I_m\}.$$

Bezüglich Matrizenmultiplikation ist dann $GL_m(\mathbf{Z})$ offensichtlich eine Gruppe.

SATZ. *Es ist*

$$GL_m(\mathbf{Z}) = \{M \in M_m(\mathbf{Z}) : \det M = \pm 1\}.$$

Beweis: Ist $M \in GL_m(\mathbf{Z})$, so gibt es eine Matrix $\widetilde{M} \in M_m(\mathbf{Z})$ mit $M\widetilde{M} = I_m$. Damit folgt $\det(M)\det(\widetilde{M}) = 1$. Wegen $\det(M), \det(\widetilde{M}) \in \mathbf{Z}$ folgt $\det(M) = \pm 1$. Sei umgekehrt $\det(M) = \pm 1$. Streicht man in M die Zeile i und die Spalte j, so gilt für die zugehörige Determinante $M_{ij} \in \mathbf{Z}$. In der Linearen Algebra wird die Formel

$$M^{-1} = \frac{1}{\det M}((-1)^{i+j}M_{ji})_{ij}$$

gezeigt. Damit ist aber M^{-1} eine Matrix mit Einträgen aus $\mathbf{Z}$ und es folgt die Behauptung. ■

Wir definieren nun für vorgegebenes $m \in \mathbf{N}$ drei Typen von $m \times m$-Matrizen: $R(k)$, $S(k,l)$, $T(k,l,c)$.

- Für $1 \le k \le m$ wird die $m \times m$-Matrix $R(k)$ definiert durch

$$R(k)_{ij} = \begin{cases} -1 & \text{für } i = j = k \\ 1 & \text{für } i = j \neq k \\ 0 & \text{sonst} \end{cases} \quad \text{bzw.} \quad R(k) = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & -1 & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}.$$

  Ist M eine $m \times n$-Matrix, so ist $R(k)M$ die Matrix, die aus M durch Multiplikation der k-ten Zeile mit -1 entsteht.
- Für $1 \le k, l \le m$ wird die $m \times m$-Matrix $S(k,l)$ definiert durch

$$S(k,l)_{ij} = \begin{cases} 1 & \text{für } (i,j) = (k,l), (l,k) \\ 1 & \text{für } i = j \neq k, l \\ 0 & \text{sonst} \end{cases} \quad \text{bzw.} \quad S(k,l) = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 0 & & 1 & & \\ & & & \ddots & & & \\ & & 1 & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}.$$

  $S(k,l)M$ ist die Matrix, die aus M durch Vertauschen der Zeilen k und l entsteht.
- Für $1 \le k, l \le m$, $k \neq l$, $c \in \mathbf{Z}$ wird die $m \times m$-Matrix $T(k,l,c)$ definiert durch

$$T(k,l,c)_{ij} = \begin{cases} 1 & \text{für } i = j \\ c & \text{für } (i,j) = (l,k) \\ 0 & \text{sonst} \end{cases} \quad \text{bzw.} \quad T(k,l,c) = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & c & & \\ & & & \ddots & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}.$$

  Die Matrix $T(k,l,c)M$ ist genau die Matrix, die entsteht, wenn man die k-te Zeile von M mit c multipliziert und zur l-ten Zeile addiert.

Die elementaren Zeilenumformungen, die wir für die Herleitung der Hermiteschen Normalform benutzt haben, lassen sich also auch die Multiplikation der Matrix M mit eine der Matrizen $R(k), S(k,l), T(k,l,c)$ beschreiben. Offensichtlich gilt: $R(k), S(k,l), T(k,l,c) \in GL_m(\mathbf{Z})$.

Sei M eine $m \times n$-Matrix (vom Rang n). Wir bringen M auf Hermitesche Normalform $\frac{1}{d}(c_{ij})_{i,j}$. Dann gibt es also Matrizen $U_i \in \{R(k), S(k,l), T(k,l,c)\}$ mit

$$U_r U_{r-1} \dots U_2 U_1 M = \frac{1}{d}(c_{ij}).$$

(Wendet man die entsprechenden elementaren Umformungen gleichzeitig auf die Einheitsmatrix I_m an, so erhält man daraus am Schluß die Matrix $U_r U_{r-1} \dots U_2 U_1$.)

SATZ. *Die Matrizen $R(k)$, $S(k,l)$ und $T(k,l,m)$ erzeugen die Gruppe $GL_m(\mathbf{Z})$, d.h. die Linksmultiplikation von $G \in GL_m(\mathbf{Z})$ an eine $m \times n$-Matrix M läßt sich auch durch elementare Zeilenumformungen erreichen.*

Beweis: Wir haben bereits bemerkt, dass $R(k), S(k,l), T(k,l,c) \in GL_m(\mathbf{Z})$ gilt. Sei nun umgekehrt $G \in GL_m(\mathbf{Z})$ gegeben. Durch elementare Zeilenumformungen bringen wir G auf Hermitesche Normalform (c_{ij}), d.h. es gibt Matrizen $U_i \in \{R(k), S(k,l), T(k,l,c)\}$ mit

$$U_r U_{r-1} \dots U_2 U_1 G = (c_{ij}).$$

Die Matrix (c_{ij}) liegt wieder in $GL_m(\mathbf{Z})$, also folgt $c_{11} \dots c_{nn} = \det(c_{ij}) = \pm 1$, was wegen $c_{ii} > 0$ dann $c_{ii} = 1$ ergibt. Für $i < j$ ist $0 \le c_{ij} < c_{jj} = 1$, also $c_{ij} = 0$. Daher ist $(c_{ij}) = I_m$ und somit

$$G = U_1^{-1} U_2^{-1} \dots U_{r-1}^{-1} U_r^{-1},$$

was die Behauptung beweist. ■

SATZ. *Die Hermitesche Normalform einer Matrix $M \in M(m \times n, \mathbf{Q})$ vom Rang n ist eindeutig bestimmt.*

Beweis: Sei d der kleinste gemeinsame Nenner der Einträge von M und seien $\frac{1}{d}C$, $\frac{1}{d}D$ zwei Hermitesche Normalformen von M. D.h. $C = (c_{ij})$ und $D = (d_{ij})$ sind obere Dreiecksmatrizen mit Einträgen aus $\mathbf{N}_0$, so dass gilt: $c_{ij} < c_{jj}$ und $d_{ij} < d_{jj}$ für $i < j$. Nun gibt es Matrizen $G_1, G_2 \in GL_m(\mathbf{Z})$ mit $\frac{1}{d}C = G_1 M$ und $\frac{1}{d}D = G_2 M$. Mit $G = (g_{ij}) = G_2 G_1^{-1} \in GL_m(\mathbf{Z})$ gilt daher:

$$(d_{ij}) = D = dG_2 M = G_2 G_1^{-1} C = GC = (g_{ij})(c_{ij}).$$

Da C und D obere Dreiecksmatrizen sind, ist es auch G. Daher gilt für $i \le j$:

$$d_{ij} = \sum_k g_{ik} c_{kj} = \sum_{i \le k \le j} g_{ik} c_{kj}.$$

Insbesondere $d_{ii} = g_{ii} c_{ii}$, also $g_{ii} > 0$. Nun ist $\pm 1 = \det(g_{ij}) = g_{11} \dots g_{nn}$, also folgt $g_{ii} = 1$. Dies liefert $d_{ii} = c_{ii}$. Wir zeigen nun für festes i, dass $g_{ij} = 0$ für $j > i$ gilt. Für $j = i+1$ ist

$$d_{i,i+1} = g_{ii} c_{i,i+1} + g_{i,i+1} c_{i+1,i+1} = c_{i,i+1} + g_{i,i+1} c_{i+1,i+1}.$$

Wegen $c_{i+1,i+1} = d_{i+1,i+1}$ und $0 \le c_{i,i+1} < c_{i,i+1}$, $0 \le d_{i,i+1} < d_{i,i+1}$ folgt $g_{i,i+1} = 0$. Es gelte nun bereits

$$g_{i,i+1} = \dots = g_{i,j-1} = 0.$$

Mit obiger Formel folgt

$$d_{ij} = g_{ii} c_{ij} + g_{ij} d_{jj} = c_{ij} + g_{ij} d_{jj}.$$

Wegen $0 \le d_{ij}, c_{ij} < d_{jj} = c_{jj}$ folgt $g_{ij} = 0$, was wir zeigen wollten. Damit ist G die Einheitsmatrix und $D = C$. ■

Bemerkung: Maple liefert bei Aufruf von 'linalg[ihermite]'(M, U) die Hermitesche Normalform von M, die Matrix U wird so bestimmt, dass UM die Hermitesche Normalform ist.

3. Die Hermitesche Normalform von Moduln

Wir wenden jetzt die Hermitesche Normalform für Matrizen auf Moduln eines Zahlkörpers an.

SATZ. *Sei K ein Zahlkörper, $\omega_1, \ldots, \omega_n \in K$ eine $\mathbf{Q}$-Basis von K und $U = \mathbf{Z}\beta_1 + \cdots + \mathbf{Z}\beta_m$ ein Modul in K. Die Matrix $M \in M(m \times n, \mathbf{Q})$ werde definiert durch*

$$\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_m \end{pmatrix} = M \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix}.$$

Sei $\frac{1}{d}(c_{ij})_{1 \le i \le m, 1 \le j \le n}$ die Hermitesche Normalform von M, also insbesondere $d \in \mathbf{N}$, $c_{ij} \in \mathbf{Z}$ mit $\mathrm{ggT}(d, c_{11}, c_{12}, \ldots, c_{nn}) = 1$ und $0 \le c_{ij} < c_{jj}$ für alle $i < j$, und

$$\alpha_i = \frac{1}{d} \sum_{j=i}^{n} c_{ij}\omega_j \quad \text{für} \quad i = 1, \ldots, n.$$

Dann gilt

$$U = \mathbf{Z}\alpha_1 + \cdots + \mathbf{Z}\alpha_n$$

und $\alpha_1, \ldots, \alpha_n$ ist eine $\mathbf{Q}$-Basis von K. Die Darstellung $U = \mathbf{Z}\alpha_1 + \cdots + \mathbf{Z}\alpha_n$ heißt die Hermitesche Normalform von U bzgl. $\omega_1, \ldots, \omega_n$. Sie ist eindeutig bestimmt.

Beweis: Seien $U_1, \ldots, U_r \in \{R(k), S(k,l), T(k,l,c)\}$ die Matrizen, die den elementaren Umformungen von M entsprechen, d.h.

$$U_r U_{r-1} \ldots U_2 U_1 M = \frac{1}{d}(c_{ij}).$$

Wir haben anfangs überlegt: Sind die Einträge von

$$\begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_m \end{pmatrix} \text{ ein Erzeugendensystem von } U, \text{ so auch die Einträge von } U_i \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_m \end{pmatrix}.$$

Also bilden auch die Einträge der folgenden Spalte ein Erzeugendensystem von U:

$$U_r U_{r-1} \ldots U_2 U_1 \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_m \end{pmatrix} = U_r U_{r-1} \ldots U_2 U_1 M \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = \frac{1}{d}(c_{ij})_{1 \le i \le m, 1 \le j \le n} \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Die 0-Einträge der rechten Spalte kommen daher, dass (c_{ij}) eine obere Dreiecksmatrix vom Rang n ist. Mit $\omega_1, \ldots, \omega_n$ ist natürlich auch $\alpha_1, \ldots, \alpha_n$ eine $\mathbf{Q}$-Basis von K. Die Eindeutigkeit der Hermiteschen Normalform folgt sofort aus der Eindeutigkeit der Hermiteschen Normalform für Matrizen. ■

Bemerkung: Der Satz zeigt, dass jeder Modul in K die Gestalt $U = \mathbf{Z}\alpha_1 + \cdots + \mathbf{Z}\alpha_n$ hat, wobei $\alpha_1, \ldots, \alpha_n$ eine $\mathbf{Q}$-Basis von K ist. U ist ein sogenannter freier $\mathbf{Z}$-Modul vom Rang n. Insbesondere kann man Koeffizientenvergleich machen, d.h. $\sum_i x_i\alpha_i = \sum_i y_i\alpha_i$ impliziert $x_i = y_i$.

SATZ. *Sei $K = \mathbf{Q}(\alpha)$ ein Zahlkörper vom Grad n und U ein Modul in K. Ist $U = \mathbf{Z}\beta_1 + \cdots + \mathbf{Z}\beta_n$ die Hermitesche Normalform von U bzgl. der $\mathbf{Q}$-Basis $\alpha^{n-1}, \ldots, \alpha, 1$, d.h.*

$$\beta_i = \frac{1}{d} \sum_{j=1}^{n} c_{ij}\alpha^{n-j} \quad \text{für} \quad i = 1, \ldots, n,$$

mit

$$d \in \mathbf{N}, \quad c_{ij} \in \mathbf{Z} \quad \mathrm{ggT}(d, c_{11}, c_{12}, \ldots, c_{nn}) = 1 \quad \text{und} \quad 0 \le c_{ij} < c_{jj} \text{ für alle } i < j,$$

dann gilt

$$U \cap \mathbf{Q} = \mathbf{Z}\frac{c_{nn}}{d}.$$

Beweis: Es gilt für $x_i \in \mathbf{Q}$

$$x_1\alpha^{n-1} + x_2\alpha^{n-2} + \cdots + x_{n-1}\alpha + x_n \in \mathbf{Q} \quad \Longleftrightarrow \quad x_1 = \cdots = x_{n-1} = 0.$$

Seien nun $y_i \in \mathbf{Z}$ mit $\omega = y_1\beta_1 + \cdots + y_n\beta_n \in U \cap \mathbf{Q}$, o.E. $\omega \neq 0$. Wählt man $r \geq 1$ mit $y_1 = y_2 = \cdots = y_{r-1} = 0$, $y_r \neq 0$, so gilt

$$\begin{aligned}
\omega &= y_r\beta_r + y_{r+1}\beta_{r+1} + \cdots + y_n\beta_n = \\
&= y_r\left(\frac{c_{rr}}{d}\alpha^{n-r} + \frac{c_{r,r+1}}{d}\alpha^{n-r-1} + \ldots\right) + y_{r+1}\left(\frac{c_{r+1,r+1}}{d}\alpha^{n-r-1} + \ldots\right) + \cdots = \\
&= \frac{y_r c_{rr}}{d}\alpha^{n-r} + \frac{y_r d_{r,r+1} + y_{r+1}c_{r+1,r+1}}{d}\alpha^{n-r-1} + \ldots
\end{aligned}$$

Wäre $r < n$, so wäre der Koeffizient bei α^{n-r} von 0 verschieden, also $\omega \notin \mathbf{Q}$. Daher bleibt nur die Möglichkeit $r = n$, was dann die Behauptung liefert. ■

Beispiel: Im Fall $K = \mathbf{Q}$ besagt der vorangegangene Satz, dass jeder von Modul in $\mathbf{Q}$ die Gestalt

$$U = \mathbf{Z} \cdot \frac{c}{d} \quad \text{mit} \quad c, d \in \mathbf{N}, \mathrm{ggT}(c, d) = 1$$

hat. Dabei sind c und d eindeutig bestimmt.

Die folgende Aussage folgt sofort aus der Eindeutigkeit der Hermiteschen Normalform. Wir schreiben sie hier auf, da sie für die praktische Anwendung sehr wichtig ist.

Folgerung. *Seien U und V Moduln eines Zahlkörpers K mit Hermiteschen Normalformen $U = \mathbf{Z}\alpha_1 + \cdots + \mathbf{Z}\alpha_n$ bzw. $V = \mathbf{Z}\beta_1 + \cdots + \mathbf{Z}\beta_n$ bzgl. einer $\mathbf{Q}$-Basis $\omega_1, \ldots, \omega_n$ von K. Dann gilt:*

$$U = V \quad \Longleftrightarrow \quad \alpha_1 = \beta_1, \ldots, \alpha_n = \beta_n.$$

Definition. Sei U ein Modul eines Zahlkörpers K. Ist $\alpha_1, \ldots, \alpha_n$ eine $\mathbf{Q}$-Basis von K und $U = \mathbf{Z}\alpha_1 + \cdots + \mathbf{Z}\alpha_n$, so heißt $\alpha_1, \ldots, \alpha_n$ eine $\mathbf{Z}$-Basis von U.

Mit Hilfe der Hermiteschen Normalform erhalten wir sofort folgenden Satz:

Satz. *Jeder Modul eines Zahlkörpers K besitzt eine $\mathbf{Z}$-Basis.*

Satz. *Sei K ein Zahlkörper vom Grad n, seien U_1 und U_2 zwei Moduln in K mit $\mathbf{Z}$-Basen $\alpha_1, \ldots, \alpha_n$ bzw. $\beta_1, \ldots, \beta_n$. Schreibt man $\beta_i = \sum_j x_{ij}\alpha_j$ mit $x_{ij} \in \mathbf{Q}$, d.h.*

$$\begin{pmatrix} \beta_1 \\ \ldots \\ \beta_n \end{pmatrix} = X \begin{pmatrix} \alpha_1 \\ \ldots \\ \alpha_n \end{pmatrix},$$

mit $X = (x_{ij})$, so gilt:

1. *$U_2 \subseteq U_1$ genau dann, wenn $X \in M_n(\mathbf{Z})$ gilt.*
2. *$U_1 = U_2$ genau dann, wenn $X \in GL_n(\mathbf{Z})$ gilt. Insbesondere unterscheiden sich zwei $\mathbf{Z}$-Basen eines $\mathbf{Z}$-Moduls nur um eine Matrix aus $GL_n(\mathbf{Z})$.*

Beweis: Da $\alpha_1, \ldots, \alpha_n$ und $\beta_1, \ldots, \beta_n$ auch $\mathbf{Q}$-Basen von K sind, sind die Koeffizienten $x_{ij} \in \mathbf{Q}$ natürlich eindeutig bestimmt. Damit ist 1. sofort klar. Um 2. zu zeigen schreiben wir $\alpha_i = \sum_j y_{ij}\beta_j$ mit $y_{ij} \in \mathbf{Q}$. Mit $Y = (y_{ij})$ folgt dann aus

$$\beta_i = \sum_j x_{ij}\alpha_j = \sum_{j,k} x_{ij}y_{jk}\beta_k$$

sofort $XY = I_n$ und analog $YX = I_n$. Nun gilt mit 1.

$$U_1 = U_2 \quad \Longleftrightarrow \quad U_2 \subseteq U_1, U_1 \subseteq U_2 \quad \Longleftrightarrow \quad X, Y \in M_n(\mathbf{Z}) \quad \Longleftrightarrow \quad X \in GL_n(\mathbf{Z}),$$

also die Behauptung. ■

Lemma. *Sind U und V zwei Moduln eines Zahlkörpers K, so gibt es eine natürliche Zahl d mit $dV \subseteq U$.*

Beweis: Sei $U = \mathbf{Z}\alpha_1 + \cdots + \mathbf{Z}\alpha_n$ und $V = \mathbf{Z}\beta_1 + \cdots + \mathbf{Z}\beta_n$ mit $\mathbf{Z}$-Basen $\alpha_1, \ldots, \alpha_n$ bzw. $\beta_1, \ldots, \beta_n$. Dann gibt es $x_{ij} \in \mathbf{Q}$ mit $\beta_i = \sum_j x_{ij}\alpha_j$. Sei d der kleinste gemeinsame Nenner der x_{ij}'s. Dann ist $x_{ij} = \frac{a_{ij}}{d}$ mit $a_{ij} \in \mathbf{Z}$. Aus $d\beta_i = \sum_j a_{ij}\alpha_j \in U$ folgt $dV \subseteq U$, was wir zeigen wollten. ■

DEFINITION. Sind

$$U = \mathbf{Z}\alpha_1 + \cdots + \mathbf{Z}\alpha_r \quad \text{und} \quad V = \mathbf{Z}\beta_1 + \cdots + \beta_s$$

Moduln eines Zahlkörpers K, so wird die Summe $U + V$ und das Produkt UV definiert durch

$$U + V = \mathbf{Z}\alpha_1 + \cdots + \mathbf{Z}\alpha_r + \mathbf{Z}\beta_1 + \cdots + \mathbf{Z}\beta_s \quad \text{und} \quad UV = \{\sum_{i,j} x_{ij}\alpha_i\beta_j : x_{ij} \in \mathbf{Z}\}.$$

Summe und Produkt sind wieder Moduln in K.

Bemerkungen:

1. $U + V = \{u + v : u \in U, v \in V\}$.
2. Natürlich gilt $UV \supseteq \{uv : u \in U, v \in V\}$. Gleichheit muß aber nicht gelten.

Beispiel: Wir betrachten $K = \mathbf{Q}(\omega)$ mit $\omega^2 = -6$ und wählen als

$$U = \mathbf{Z} \cdot 2 + \mathbf{Z}\omega \quad \text{und} \quad V = \mathbf{Z} \cdot 3 + \mathbf{Z}\omega.$$

Nach Definition wird UV von den Produkten $2 \cdot 3, 2 \cdot \omega, 3 \cdot \omega, \omega^2$ erzeugt, woraus man sofort

$$UV = \mathbf{Z} \cdot 6 + \mathbf{Z}\omega$$

erhält. Offensichtlich enthält UV das Element ω. Wir wollen sehen, dass ω sich nicht als Produkt uv mit $u \in U$, $v \in V$ schreiben läßt. Die Norm von $x + y\omega$ ist $\mathrm{N}(x + y\omega) = x^2 + 6y^2$. Ist $u \in U \setminus \{0\}$, d.h. $u = 2a + b\omega$ mit $a, b \in \mathbf{Z}$, so gilt für die Norm $\mathrm{N}(u) = 4a^2 + 6b^2 \geq 4$. Entsprechend erhält man für $v = 3c + d\omega \in V \setminus \{0\}$ die Beziehung $\mathrm{N}(v) = 9c^2 + 6d^2 \geq 6$. Gäbe es eine Darstellung $\omega = uv$, so würde folgen $6 = \mathrm{N}(\omega) = \mathrm{N}(u)\mathrm{N}(v) \geq 4 \cdot 6$, ein offensichtlicher Widerspruch.

Wir geben eine weitere Anwendung der Hermiteschen Normalform, die insbesondere zeigt, dass auch der Durchschnitt von Moduln eines Zahlkörpers wieder ein Modul ist.

SATZ. *Sei K ein Zahlkörper mit $\mathbf{Q}$-Basis $\omega_1, \ldots, \omega_n$. Seien $\mathfrak{a}, \mathfrak{b} \subseteq K$ Moduln mit $\mathbf{Z}$-Basen $\alpha_1, \ldots, \alpha_n$ bzw. $\beta_1, \ldots, \beta_n$. Schreibt man*

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = A \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix}, \quad \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = B \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} \quad \text{mit } A, B \in M_n(\mathbf{Q}),$$

bestimmt man

$$U = \begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix} \in GL_{2n}(\mathbf{Z}) \text{ mit } U_{ij} \in M_n(\mathbf{Z}),$$

sodass

$$U \begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix} \begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} U_{11}A + U_{12}B \\ U_{21}A + U_{22}B \end{pmatrix}$$

die Hermitesche Normalform von $\begin{pmatrix} A \\ B \end{pmatrix}$ ist, so ist $U_{11}A + U_{12}B$ eine Matrix vom Rang n in Hermitescher Normalform, $U_{21}A + U_{22}B = 0$ und

$$\mathfrak{a} \cap \mathfrak{b} = \mathbf{Z}\gamma_1 + \cdots + \mathbf{Z}\gamma_n \quad \text{mit} \quad \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix} = U_{21}A \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix}.$$

$\mathfrak{a} \cap \mathfrak{b}$ ist ein Modul in K mit $\mathbf{Z}$-Basis $\gamma_1, \ldots, \gamma_n$.

Beweis: Da A und B Rang n haben, hat auch $\begin{pmatrix} A \\ B \end{pmatrix}$ Rang n, woraus sofort die Aussagen über $U_{11}A + U_{12}B$ und $U_{21}A + U_{22}B$ folgen. Wir zeigen nun $\mathfrak{a} \cap \mathfrak{b} = \mathbf{Z}\gamma_1 + \cdots + \mathbf{Z}\gamma_n$.
$\supseteq$: Zu $\lambda \in \mathbf{Z}\gamma_1 + \cdots + \mathbf{Z}\gamma_n$ gibt es $u \in \mathbf{Z}^n$ mit

$$\lambda = u \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix} = uU_{21}A \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = uU_{21} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = -uU_{22}B \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = -uU_{22} \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix},$$

was sofort $\lambda \in \mathfrak{a} \cap \mathfrak{b}$ zeigt.
$\subseteq$: Sei $\lambda \in \mathfrak{a} \cap \mathfrak{b}$. Dann gibt es $x, y \in \mathbf{Z}^n$ mit

$$\lambda == x \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = y \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = xA \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = yB \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix},$$

was sofort $xA - yB = 0$ liefert. Wir definieren $u, v \in \mathbf{Z}^n$ durch $(v, u)U = (x, -y)$. Dann gilt

$$\begin{aligned} 0 &= xA - yB = (x, -y) \begin{pmatrix} A \\ B \end{pmatrix} = (v, u)U \begin{pmatrix} A \\ B \end{pmatrix} = (v, u) \begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix} \begin{pmatrix} A \\ B \end{pmatrix} = \\ &= (v, u) \begin{pmatrix} U_{11}A + U_{12}B \\ U_{21}A + U_{22}B \end{pmatrix} = v(U_{11}A + U_{12}B) + u(U_{21}A + U_{22}B) = v(U_{11}A + U_{12}B). \end{aligned}$$

Da $U_{11}A + U_{12}B$ Rang n hat, folgt $v = 0$ und damit

$$(x, -y) = (0, u)U = (0, u) \begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix} = (uU_{21}, uU_{22}),$$

also $x = uU_{21}$ und damit

$$\lambda = x \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = xA \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = uU_{21}A \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = u \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix},$$

was die Inklusion $\subseteq$ zeigt.
Wählt man $d \in \mathbf{N}$ mit $d\mathfrak{b} \subseteq \mathfrak{a}$, so folgt $d\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$. Da $d\mathfrak{b}$ eine $\mathbf{Q}$-Basis von K enthält, gilt dies auch für $\mathfrak{a} \cap \mathfrak{b}$, d.h. $\gamma_1, \ldots, \gamma_n$ ist eine $\mathbf{Q}$-Basis von K und $\mathfrak{a} \cap \mathfrak{b}$ damit ein Modul in K. ■

Beispiel: Sei $K = \mathbf{Q}\omega_1 + \mathbf{Q}\omega_2$ zweidimensional über $\mathbf{Q}$. Wir betrachten die Moduln

$$\mathfrak{a} = \mathbf{Z} \cdot (2\omega_1 + 5\omega_2) + \mathbf{Z} \cdot 8\omega_2, \quad \mathfrak{b} = \mathbf{Z} \cdot (2\omega_1 + 3\omega_2) + \mathbf{Z} \cdot 8\omega_2.$$

Wir wählen

$$A = \begin{pmatrix} 2 & 5 \\ 0 & 8 \end{pmatrix}, \quad B = \begin{pmatrix} 2 & 3 \\ 0 & 8 \end{pmatrix}$$

und erhalten mit

$$U = \begin{pmatrix} -1 & 0 & 2 & 0 \\ 1 & 0 & -1 & 0 \\ -4 & 1 & 4 & 0 \\ -4 & 0 & 4 & 1 \end{pmatrix} \text{ die hermitesche Normalform } U \begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 0 & 2 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Mit

$$U_{21} = \begin{pmatrix} -4 & 1 \\ -4 & 0 \end{pmatrix}$$

folgt

$$U_{21}A = \begin{pmatrix} -8 & -12 \\ -8 & -20 \end{pmatrix}$$

mit der hermiteschen Normalform

$$\begin{pmatrix} 8 & 4 \\ 0 & 8 \end{pmatrix}.$$

Daher folgt

$$\mathfrak{a} \cap \mathfrak{b} = \mathbf{Z} \cdot (8\omega_1 + 4\omega_2) + \mathbf{Z} \cdot 8\omega_2.$$

Unter Zuhilfenahme der Durchschnittsbildung für Moduln können wir eine weitere Moduloperation einführen:

SATZ. *Sind $\mathfrak{a}$ und $\mathfrak{b}$ Moduln eines Zahlkörpers K mit $\mathbf{Z}$-Basen $\alpha_1, \ldots, \alpha_n$ bzw. $\beta_1, \ldots, \beta_n$, so ist auch*

$$(\mathfrak{a} : \mathfrak{b}) = \{\lambda \in K : \lambda\mathfrak{b} \subseteq \mathfrak{a}\}$$

ein Modul, nämlich

$$(\mathfrak{a} : \mathfrak{b}) = \bigcap_{i=1}^{n} (\mathbf{Z}\frac{\alpha_1}{\beta_i} + \cdots + \mathbf{Z}\frac{\alpha_n}{\beta_i}).$$

Beweis: Es genügt die angegebene Formel zu beweisen, da Durchschnitte von Moduln wieder Moduln sind. Aus

$$\begin{aligned} \lambda \in (\mathfrak{a} : \mathfrak{b}) &\iff \lambda\mathfrak{b} \subseteq \mathfrak{a} \\ &\iff \lambda\beta_i \in \mathbf{Z}\alpha_1 + \cdots + \mathbf{Z}\alpha_n \text{ für alle } i \\ &\iff \lambda \in \mathbf{Z}\frac{\alpha_1}{\beta_i} + \cdots + \mathbf{Z}\frac{\alpha_n}{\beta_i} \text{ für alle } i \\ &\iff \lambda \in \cap_{i=1}^{n} (\mathbf{Z}\frac{\alpha_1}{\beta_i} + \cdots + \mathbf{Z}\frac{\alpha_n}{\beta_i}) \end{aligned}$$

folgt nun die Behauptung. ■

4. Faktorgruppen und die Smithsche Normalform

Erinnerung: Seien $U \supseteq V$ abelsche Gruppen. Dann definiert man auf U durch

$$u_1 \equiv u_2 \bmod V \quad \iff \quad u_1 - u_2 \in V$$

eine Äquivalenzrelation, die mit der Addition verträglich ist. Die Menge der Äquivalenzklassen wird mit U/V bezeichnet, die Äquivalenzklasse von $u \in U$ mit $\overline{u}$. Dann ist also $\overline{u_1} = \overline{u_2}$ genau dann, wenn $u_1 - u_2 \in V$ gilt. Man definiert nun durch

$$\overline{u_1} + \overline{u_2} = \overline{u_1 + u_2}$$

eine Addition auf U/V, die U/V zu einer abelschen Gruppe macht. U/V wird die Faktorgruppe von U nach V genannt.

LEMMA. *Seien $V \subseteq U$ Moduln eines Zahlkörpers K. Sei $\alpha_1, \ldots, \alpha_n$ eine $\mathbf{Z}$-Basis von U und $V = Z\beta_1 + \cdots + \mathbf{Z}\beta_n$ die Hermitesche Normalform von V bzgl. $\alpha_1, \ldots, \alpha_n$, d.h.*

$$\beta_i = \sum_{j=i}^{n} c_{ij}\alpha_j, \quad c_{ii} > 0, \quad 0 \le c_{ij} < c_{jj} \text{ für } i < j.$$

Dann ist

$$\{x_1\alpha_1 + \cdots + x_n\alpha_n : x_i \in \mathbf{Z}, 0 \le x_i < c_{ii}\}$$

ein Repräsentantensystem der Faktorgruppe U/V und insbesondere $\#U/V = c_{11} \ldots c_{nn}$.

Beweis: Sei $u = x_1\alpha_1 + \cdots + x_n\alpha_n \in U$ gegeben. Wir addieren oder subtrahieren β_1 sooft, bis wir $0 \le x_1 < c_{11}$ erreicht haben. Nun ändern wir den Koeffizienten x_2 durch Addition oder Subtraktion von β_2, usw. Schließlich können wir $0 \le x_i < c_{ii}$ annehmen. Die Eindeutigkeit eines solchen reduzierten Elements überlegt man sich analog: man zeigt zunächst die Eindeutigkeit von x_1, dann die von x_2, etc. ■

Beispiele:

1. Sei $U = \mathbf{Z}\alpha + \mathbf{Z}\beta$ und $V = \mathbf{Z} \cdot 2\alpha + \mathbf{Z} \cdot 2\beta$. Die Repräsentanten von U/V sind $0, \alpha, \beta, \alpha + \beta$. Offensichtlich ist U/V eine Kleinsche Vierergruppe, d.h. $U/V \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$.
2. Sei $U = \mathbf{Z}\alpha + \mathbf{Z}\beta$ und $V = \mathbf{Z} \cdot (2\alpha + \beta) + \mathbf{Z} \cdot 2\beta$. Ein Repräsentantensystem von U/V ist wieder $0, \alpha, \beta, \alpha + \beta$. Nun ist $2\beta \equiv 0$ und damit

   $$\alpha \equiv \alpha, \quad 2\alpha \equiv -\beta \equiv \beta, \quad 3\alpha \equiv 2\alpha + \alpha \equiv \alpha + \beta.$$

   α erzeugt also die ganze Gruppe, d.h. U/V ist eine zyklische Gruppe der Ordnung 4.

SATZ. *Seien $V \subseteq U$ Moduln eines Zahlkörpers K. Sei $S \subseteq U$ ein Repräsentantensystem von U/V, insbesondere $\#S = \#U/V$.*

1. *Ist $W \subseteq K$ eine abelsche Gruppe mit $V \subseteq W \subseteq U$, so ist auch W ein Modul. Außerdem gilt:*
$$W = V + \sum_{w \in W \cap S} \mathbf{Z}w.$$
2. *Es gibt nur endlich viele Moduln W in K mit $V \subseteq W \subseteq U$.*

Beweis:

1. Da V eine $\mathbf{Q}$-Basis von K enthält, gilt dies auch für W. Wir müssen nur noch zeigen, dass W als abelsche Gruppe von endlich vielen Elementen erzeugt wird. Dazu genügt es die behauptete Gleichung zu zeigen, da auch V endlich erzeugt ist.
   $\supseteq$ Da W eine abelsche Gruppe ist, folgt dies aus $V \subseteq W$ und $\{s \in W \cap S\} \subseteq W$.
   $\subseteq$ Sei $w \in W$. Dann gibt es ein $s \in S$ mit $w \equiv s \bmod V$, d.h. es gibt ein $v \in V$ mit $w = s + v$. Aus $s = w - v \in W \cap S$ folgt $w = v + s \in V + \mathbf{Z}s \subseteq V + \sum_{t \in W \cap S} \mathbf{Z}t$, was zu zeigen war.
2. Nach 1. ist jeder Modul W mit $V \subseteq W \subseteq U$ durch $S \cap W \subseteq S$ bestimmt. Da S endlich ist, besitzt S auch nur endlich viele Teilmengen, daher kann es auch nur endlich viele Moduln W geben. ■

Die Struktur der Faktorgruppe U/V läßt sich aus der Hermiteschen Normalform noch nicht ablesen. Wir erwähnen daher kurz eine andere Normalform in Form eines Satzes. Ein Beweis wird normalerweise in der Algebra gegeben.

SATZ. *Zu jeder Matrix $M \in M(m \times n, \mathbf{Z})$ gibt es Matrizen $S \in GL_m(\mathbf{Z})$, $T \in GL_n(\mathbf{Z})$, sodass für $D = SMT$ gilt*

$$D = \begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & d_{\min(m,n)} \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix} \quad \textit{mit} \quad d_i \in \mathbf{N}_0 \quad \textit{und} \quad d_1 | d_2 | d_3 | \dots | d_{\min(m,n)}.$$

D heißt die Smitsche Normalform von M, $d_1, \dots, d_{\min(m,n)}$ heißen die Elementarteiler von M. Die Smithsche Normalform ist eindeutig bestimmt.

Bemerkung: Die Maple-Funktion 'linalg[ismith](M, S, T)' liefert die Smithsche Normalform von M zusammen mit den im Satz angegebenen Matrizen S und T.

SATZ. *Seien $V \subseteq U$ Moduln eines Zahlkörpers K mit $\mathbf{Z}$-Basen $\beta_1, \dots, \beta_n$ bzw. $\alpha_1, \dots, \alpha_n$. Sei $M \in M_n(\mathbf{Z})$ definiert durch*

$$\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = M \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}.$$

Seien $S, T \in GL_n(\mathbf{Z})$, sodass SMT in Smithscher Normalform ist, d.h.

$$SMT = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix} \quad \textit{mit} \quad d_i \in \mathbf{N} \quad \textit{und} \quad d_1 | d_2 | \dots | d_n.$$

Definiert man $\gamma_1, \dots, \gamma_n$ durch

$$\begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix} = T^{-1} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix},$$

so gilt

$$U = \mathbf{Z}\gamma_1 + \cdots + \mathbf{Z}\gamma_n, \quad V = \mathbf{Z}d_1\gamma_1 + \cdots + \mathbf{Z}d_n\gamma_n$$

und

$$U/V \to \mathbf{Z}/\mathbf{Z}d_1 \oplus \cdots \oplus \mathbf{Z}/\mathbf{Z}d_n, \quad \overline{x_1\gamma_1 + \cdots + x_n\gamma_n} \mapsto (x_1 \bmod d_1, \ldots, x_n \bmod d_n)$$

ist ein Gruppenisomorphismus.

Beweis: Natürlich ist $\gamma_1, \ldots, \gamma_n$ wegen $T, T^{-1} \in GL_n(\mathbf{Z})$ eine $\mathbf{Z}$-Basis von U. Aus

$$\begin{pmatrix} d_1\gamma_1 \\ \vdots \\ d_n\gamma_n \end{pmatrix} = SMT \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix} = SMT \cdot T^{-1} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = SM \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = S \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}$$

folgt wegen $S \in GL_n(\mathbf{Z})$, dass $d_1\gamma_1, \ldots, d_n\gamma_n$ eine $\mathbf{Z}$-Basis von V ist. Da $\gamma_1, \ldots, \gamma_n$ eine $\mathbf{Q}$-Basis von K ist, ist die Abbildung

$$\phi : U \to \mathbf{Z}/\mathbf{Z}d_1 \oplus \cdots \oplus \mathbf{Z}/\mathbf{Z}d_n, \quad x_1\gamma_1 + \cdots + x_n\gamma_n \mapsto (x_1 \bmod d_1, \ldots, x_n \bmod d_n)$$

wohldefiniert. Natürlich ist ϕ surjektiv. Der Kern ist offensichtlich V, was dann den Isomorphismus $U/V \simeq \mathbf{Z}/\mathbf{Z}d_1 \oplus \cdots \oplus \mathbf{Z}/\mathbf{Z}d_n$ liefert. ■

5. Indexberechnungen

Sei K ein Zahlkörper vom Grad n und U_1, U_2 zwei Moduln in K. Sind $\alpha_1, \ldots, \alpha_n$ und $\beta_1, \ldots, \beta_n$ $\mathbf{Z}$-Basen von U_1 und U_2, also

$$U_1 = \mathbf{Z}\alpha_1 + \ldots \mathbf{Z}\alpha_n, \quad U_2 = \mathbf{Z}\beta_1 + \cdots + \mathbf{Z}\beta_n,$$

so gibt es genau eine Matrix $M \in M_n(\mathbf{Q})$ mit

$$\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = M \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}.$$

M ist also die Übergangsmatrix von $\alpha_1, \ldots, \alpha_n$ zu $\beta_1, \ldots, \beta_n$. Man definiert den Index $[U_1 : U_2]$ von U_2 in U_1 durch

$$[U_1 : U_2] = |\det M|.$$

Der Index ist eine positive rationale Zahl. Wir zeigen nun, dass der Index nicht von der Wahl der $\mathbf{Z}$-Basen für U_1 und U_2 abhängt. Sind $\alpha_1', \ldots, \alpha_n'$ und $\beta_1', \ldots, \beta_n'$ weitere $\mathbf{Z}$-Basen von U_1 und U_2, so gibt es Matrizen $S, T \in GL_n(\mathbf{Z})$ mit

$$\begin{pmatrix} \alpha_1' \\ \vdots \\ \alpha_n' \end{pmatrix} = S \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} \beta_1' \\ \vdots \\ \beta_n' \end{pmatrix} = T \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}, \quad \text{also} \quad \begin{pmatrix} \beta_1' \\ \vdots \\ \beta_n' \end{pmatrix} = TMS^{-1} \begin{pmatrix} \alpha_1' \\ \vdots \\ \alpha_n' \end{pmatrix}.$$

Wegen $\det S = \det T = \pm 1$ folgt $|\det M| = |\det(TMS^{-1})|$, d.h. der Index ist tatsächlich unabhängig von den gewählten Basen.

Durch einfache Matrizenmultiplikation erhält man folgenden Satz:

Satz. *Seien U_1, U_2, U_3 Moduln in K. Dann gilt:*

1. $[U_1 : U_2] \cdot [U_2 : U_1] = 1$.
2. $[U_1 : U_3] = [U_1 : U_2] \cdot [U_2 : U_3]$.

Satz. *Seien $V \subseteq U$ Moduln eines Zahlkörpers K. Dann gilt:*

1. $[U : V] \in \mathbf{N}$.
2. $U = V \iff [U : V] = 1$.
3. $[U : V] = \#U/V$, *wenn U/V die Faktorgruppe von U nach V bezeichnet.*
4. $[U : V] \cdot U \subseteq V$.

Beweis: Wir nutzen die Smithsche Normalform und können dann schreiben

$$U = \mathbf{Z}\gamma_1 + \cdots + \mathbf{Z}\gamma_n, \quad V = \mathbf{Z}d_1\gamma_1 + \cdots + \mathbf{Z}d_n\gamma_n \quad \text{mit} \quad d_i \in \mathbf{N} \quad \text{und} \quad d_1|d_2|\ldots|d_n.$$

Die Übergangsmatrix von $\gamma_1, \ldots, \gamma_n$ zu $d_1\gamma_1, \ldots, d_n\gamma_n$ ist die Diagonalmatrix M mit den Diagonalelementen $d_1, \ldots, d_n$, was sofort

$$[U : V] = d_1 \ldots d_n$$

ergibt, insbesondere $[U : V] \in \mathbf{N}$. Andererseits haben wir gesehen, dass für die Faktorgruppe

$$U/V \simeq \mathbf{Z}/\mathbf{Z}d_1 \oplus \cdots \oplus \mathbf{Z}/\mathbf{Z}d_n, \quad \text{also} \quad \#U/V = d_1 \ldots d_n$$

gilt. Dies zeigt die 3. Behauptung. Die 2. Aussage folgt sofort aus der 3. Die 4. Aussage folgt sofort aus den angegebenen Formeln. ■

6. Die Diskriminante eines Moduls

Sei K ein Zahlkörper vom Grad n. Die Diskriminante eines n-Tupels $\alpha_1, \ldots, \alpha_n \in K$ war definiert durch

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \det(\operatorname{Sp}(\alpha_i\alpha_j))_{i,j}.$$

(Die Diskriminante war genau dann 0, wenn $\alpha_1, \ldots, \alpha_n$ $\mathbf{Q}$-linear abhängig waren.) Ist $\alpha_1, \ldots, \alpha_n$ eine $\mathbf{Q}$-Basis von K, sind $\beta_1, \ldots, \beta_n \in K$ und schreibt man $\beta_i = \sum_j x_{ij}\alpha_j$ mit $x_{ij} \in \mathbf{Q}$, so hatten wir die Formel

$$\operatorname{disc}(\beta_1, \ldots, \beta_n) = (\det(x_{ij}))^2 \cdot \operatorname{disc}(\alpha_1, \ldots, \alpha_n)$$

gezeigt.
Sei jetzt U ein Modul in K mit zwei Basisdarstellungen $U = \mathbf{Z}\alpha_1 + \cdots + \mathbf{Z}\alpha_n = \mathbf{Z}\beta_1 + \cdots + \mathbf{Z}\beta_n$ und $\beta_i = \sum_j x_{ij}\beta_j$. Ist $\beta_i = \sum_j x_{ij}\alpha_j$, so folgt $(x_{ij}) \in GL_n(\mathbf{Z})$ und damit

$$\operatorname{disc}(\beta_1, \ldots, \beta_n) = \operatorname{disc}(\alpha_1, \ldots, \alpha_n).$$

Daher ist die folgende Definition unabhängig von der ausgewählten Basis:

DEFINITION. Ist U ein Modul eines Zahlkörpers K mit einer einer $\mathbf{Z}$-Basis $\alpha_1, \ldots, \alpha_n$, so definiert man die Diskriminante von U durch

$$\operatorname{disc}(U) = \operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \det(Sp(\alpha_i\alpha_j)).$$

Die folgende Formel spielt eine wichtige Rolle in der Algebraischen Zahlentheorie:

SATZ. *Sind U, V Moduln eines Zahlkörpers K, so gilt*

$$\operatorname{disc}(V) = [U : V]^2 \cdot \operatorname{disc}(U).$$

Beweis: Wir schreiben $U = \mathbf{Z}\alpha_1 + \cdots + \mathbf{Z}\alpha_n$ und $V = \mathbf{Z}\beta_1 + \cdots + \mathbf{Z}\beta_n$. Durch $\beta_i = \sum_j x_{ij}\alpha_j$ mit $x_{ij} \in \mathbf{Q}$ wird die Übergangsmatrix (x_{ij}) gegeben, sodass für den Index gilt $[U : V] = |\det(x_{ij})|$. Die obige Diskriminantenformel liefert nun

$$\operatorname{disc}(V) = \operatorname{disc}(\beta_1, \ldots, \beta_n) = (\det(x_{ij})_{i,j})^2 \cdot \operatorname{disc}(\alpha_1, \ldots, \alpha_n) = [U : V]^2 \cdot \operatorname{disc}(U),$$

was zu zeigen war. ■

Bemerkung: Ist $K = \mathbf{Q}(\alpha)$ mit $f(\alpha) = 0$, wobei f das normierte Minimalpolynom von f von α ist, so haben wir früher die Beziehung

$$\operatorname{disc}(1, \alpha, \ldots, \alpha^{n-1}) = \operatorname{disc}(f)$$

gesehen. Ist nun U ein Modul in K mit $\mathbf{Z}$-Basis $\gamma_1, \ldots, \gamma_n$, ist $\gamma_i = \sum_{j=0}^{n-1} c_{ij}\alpha^j$, so folgt

$$\operatorname{disc}(U) = (\det(c_{ij})_{i,j})^2 \cdot \operatorname{disc}(f).$$

Mit dieser Formel kann man praktische Diskriminanten berechnen, wenn man $\operatorname{disc}(f)$ kennt.

KAPITEL 5

Ordnungen

1. Ordnungen und ganze algebraische Zahlen

Die ganzen Zahlen $\mathbf{Z}$ bilden einen Modul in $\mathbf{Q}$ und sind gleichzeitig ein Unterring von $\mathbf{Q}$. Die Verallgemeinerung auf algebraische Zahlkörper findet sich in folgender Definition:

DEFINITION. Sei K ein algebraischer Zahlkörper vom Grad n. Eine Teilmenge $R \subseteq K$ heißt Ordnung, wenn folgende beiden Eigenschaften erfüllt sind:

1. R ist ein Modul in K, d.h. es gibt eine $\mathbf{Q}$-Basis $\omega_1, \ldots, \omega_n \in K$ mit
$$R = \mathbf{Z}\omega_1 + \cdots + \mathbf{Z}\omega_n.$$
2. R ist ein Unterring von K, d.h. $1 \in R$ und $x, y \in R$ impliziert $xy \in R$.

(Für Ordnungen ist auch die Bezeichnung $\mathfrak{o}$ gebräuchlich.)

Bemerkung: Um die Ringeigenschaft in der Definition der Ordnung zu überprüfen kann man sich natürlich auf die Bedingungen
$$1 \in R \quad \text{und} \quad \omega_i\omega_j \in R$$
beschränken.

Beispiel: Jeder Modul U in $\mathbf{Q}$ hat eine eindeutige Darstellung $U = \mathbf{Z}\frac{c}{d}$ mit $c, d \in \mathbf{N}$ und $\mathrm{ggT}(c, d) = 1$. Es gilt:
$$1 \in U \iff 1 = \frac{c}{d}k \text{ für ein } k \in \mathbf{Z} \iff d = ck \text{ für ein } k \in \mathbf{Z} \iff c = 1$$
und
$$(\frac{c}{d})^2 \in U \iff \frac{c^2}{d^2} = \frac{c}{d}k \text{ für ein } k \in \mathbf{Z} \iff \frac{c}{d} \in \mathbf{Z} \iff d = 1.$$
Also ist die einzige Ordnung in $\mathbf{Q}$ der Ring der ganzen Zahlen $\mathbf{Z}$.

Beispiel: $K = \mathbf{Q}(\sqrt{d})$, $d \in \mathbf{Z}$ quadratfrei $\neq 0, 1$. Dann ist
$$R = \mathbf{Z} + \mathbf{Z}\sqrt{d} = \{x + y\sqrt{d} : x, y \in \mathbf{Z}\}$$
eine Ordnung in K.

Beispiel: Sei $K = \mathbf{Q}(\alpha)$ mit $\alpha^3 = 2$. Dann ist
$$R = \mathbf{Z} + \mathbf{Z}\alpha + \mathbf{Z}\alpha^2$$
eine Ordnung in K, denn $\alpha^i \cdot \alpha^j = 2^k\alpha^l$, wenn $i + j = 3k + l$ mit $0 \leq l \leq 2$ gilt.

Ist K ein Zahlkörper, $\alpha \in K$, so ist (nach Definition) $\mathbf{Z}[\alpha]$ der kleinste Unterring von K, der $\mathbf{Z}$ und α enthält, also
$$\mathbf{Z}[\alpha] = \mathbf{Z} + \mathbf{Z}\alpha + \mathbf{Z}\alpha^2 + \mathbf{Z}\alpha^3 + \ldots$$

Beispiel: In $\mathbf{Q}$ gilt
$$\mathbf{Z}[\frac{1}{2}] = \{\frac{a}{2^n} \in \mathbf{Q} : a \in \mathbf{Z}, n \in \mathbf{N}_0\}.$$

Um zu charakterisieren, wann $\mathbf{Z}[\alpha]$ eine Ordnung ist, kommt man schnell auf folgenden Begriff:

DEFINITION. Ein Element α eines Zahlkörpers K heißt ganz über $\mathbf{Z}$ (oder auch ganz algebraisch), wenn es einer Gleichung

$$\alpha^m + a_1\alpha^{m-1} + \cdots + a_{m-1}\alpha + a_m = 0$$

mit $a_i \in \mathbf{Z}$ genügt. (Man beachte, dass der Koeffizient bei α^m die Zahl 1 ist.)

Die folgende Aussage ist als Lemma von Gauss bekannt, das normalerweise in einer Algebra-Vorlesung bewiesen wird.

SATZ. *Seien $f, g, h \in \mathbf{Q}[x]$ normierte Polynome mit $f = gh$. Gilt dann $f \in \mathbf{Z}[x]$, so folgt $g, h \in \mathbf{Z}[x]$. D.h. jeder normierte Teiler eines normierten Polynoms aus $\mathbf{Z}[x]$ ist wieder in $\mathbf{Z}[x]$.*

Damit erhalten wir eine andere Charakterisierung ganzer algebraischer Elemente:

LEMMA. *Genau dann ist $\alpha \in K$ ganz algebraisch, wenn sein normiertes Minimalpolynom Koeffizienten in $\mathbf{Z}$ hat.*

Beweis: Sei $g(x) \in \mathbf{Q}[x]$ das normierte Minimalpolynom von $\alpha \in K$. Ist $g(x) \in \mathbf{Z}[x]$, so ist α nach Definition ganz algebraisch. Ist umgekehrt α ganz algebraisch, so gibt es ein normiertes Polynom $f(x) \in \mathbf{Z}[x]$ mit $f(\alpha) = 0$. Nach Eigenschaft des Minimalpolynoms teilt $g(x)$ das Polynom $f(x)$, nach dem Lemma von Gauss gilt also $g(x) \in \mathbf{Z}[x]$, was zu zeigen war. ■

LEMMA. *Sei K ein Zahlkörper und $\alpha \in K$ mit normiertem Minimalpolynom $f(x) = x^m + a_1x^{m-1} + \cdots + a_m$. Ist $d \in \mathbf{N}$ mit*

$$da_1, \quad d^2a_2, \quad \ldots, \quad d^m a_m \in \mathbf{Z},$$

so ist $d\alpha$ ganz algebraisch. Insbesondere läßt sich jedes $\alpha \in K$ darstellen als $\alpha = \frac{\beta}{d}$ mit $d \in \mathbf{N}$ und β ganz algebraisch.

Beweis: Aus $\alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0$ folgt durch Multiplikation mit d^m die Gleichung $(d\alpha)^m + da_1(d\alpha)^{m-1} + \cdots + d^m a_m = 0$, und daraus die Behauptung. ■

Nach diesen Vorbereitungen erhalten wir jetzt folgenden Satz:

SATZ. *Genau dann ist $\mathbf{Z}[\alpha] \subseteq K$ eine Ordnung in K, wenn α ganz über $\mathbf{Z}$ ist und $K = \mathbf{Q}(\alpha)$ gilt.*

Beweis:

1. Sei $\mathbf{Z}[\alpha]$ eine Ordnung mit $\mathbf{Z}$-Basis $\omega_1, \ldots, \omega_n$, die wir auch als $\mathbf{Q}$-Basis von K wählen können. Wegen $\alpha\omega_i \in \mathbf{Z}\omega_1 + \cdots + \mathbf{Z}\omega_n$ hat die darstellende Matrix $A(\alpha)$ Einträge aus $\mathbf{Z}$, also hat das charakteristische Polynom
$$f(x) = \det(xI_n - A(\alpha)) = x^n + a_1x^{n-1} + \cdots + a_n$$
Koeffizienten a_i in $\mathbf{Z}$. Mit $f(\alpha) = 0$ folgt, dass α ganz über $\mathbf{Z}$ ist. Wegen $\mathbf{Q}(\alpha) = \mathbf{Q}\omega_1 + \cdots + \mathbf{Q}\omega_n = K$ folgt auch $K = \mathbf{Q}(\alpha)$.
2. Sei α ganz über $\mathbf{Z}$ mit $K = \mathbf{Q}(\alpha)$. Dann hat das Minimalpolynom $f = x^n + a_1x^{n-1} + \cdots + a_n$ Koeffizienten in $\mathbf{Z}$, d.h. $a_i \in \mathbf{Z}$. Da $1, \alpha, \ldots, \alpha^{n-1}$ eine $\mathbf{Q}$-Basis von K ist, ist
$$U = \mathbf{Z} + \mathbf{Z}\alpha + \cdots + \mathbf{Z}\alpha^{n-1}$$
ein Modul in K. Mit
$$\alpha^n = -a_n - a_{n-1}\alpha - \cdots - a_1\alpha^{n-1}$$
sieht man, dass $\alpha U \subseteq U$ gilt, was dann $\alpha^i U \subseteq U$ für alle $i \geq 0$ liefert. Also ist U ein Unterring von K und somit eine Ordnung. Die Behauptung folgt nun aus $U = \mathbf{Z}[\alpha]$. ■

Bemerkung: Ist K ein Zahlkörper, so kann man sich mit Hilfe des Lemmas leicht Ordnungen in K konstruieren: man wählt $\alpha \in K$ mit $K = \mathbf{Q}(\alpha)$ und $d \in \mathbf{N}$, sodass $d\alpha$ ganz algebraisch ist. Dann ist $\mathbf{Z}[d\alpha]$ eine Ordnung.

Beispiel: Sei $K = \mathbf{Q}(\alpha)$ mit $f(\alpha) = 0$ und $f = 2x^3 + 3x^2 + 5x + 7$. Das Element α ist nicht ganz algebraisch. Aus $2\alpha^3 + 3\alpha^2 + 5\alpha + 7 = 0$ folgt durch Multiplikation mit 4

$$(2\alpha)^3 + 3(2\alpha)^2 + 10(2\alpha) + 28 = 0,$$

also ist das Element 2α ganz algebraisch und damit $\mathbf{Z}[2\alpha]$ eine Ordnung in K.

Beispiel: $K = \mathbf{Q}(\alpha)$ mit $f(\alpha) = 0$ und $f = x^3 + 7x + 20$. Wir betrachten ein paar Ordnungen:

1. $\beta = \frac{1}{2}\alpha + \frac{1}{2}\alpha^2$ ist ganz algebraisch mit Minimalpolynom $x^3 + 7x^2 + 29x - 30$ und Diskriminante -149107. Es gilt
$$\begin{pmatrix} 1 \\ \beta \\ \beta^2 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 1 \\ -20 & -17 & -3 \end{pmatrix}\begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \end{pmatrix}.$$
Die Hermitesche Normalform der Übergangsmatrix ist
$$\frac{1}{2}\begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 14 \end{pmatrix},$$
woraus man die Hermitesche Normalform des Moduls $\mathbf{Z}[\beta]$ bzgl. der $\mathbf{Q}$-Basis $1, \alpha, \alpha^2$ erhält:
$$\mathbf{Z}[\beta] = \mathbf{Z} + \mathbf{Z}\beta + \mathbf{Z}\beta^2 = \mathbf{Z} + \mathbf{Z}(\frac{1}{2}\alpha + \frac{1}{2}\alpha^2) + \mathbf{Z}\cdot 7\alpha^2.$$
Für den Index gilt $[\mathbf{Z}[\alpha] : \mathbf{Z}[\beta]] = \frac{7}{2}$.
2. $\gamma = \frac{3}{2}\alpha - \frac{1}{2}\alpha^2$ ist ganz algebraisch mit Minimalpolynom $x^3 - 7x^2 - 17x + 170$ und Diskriminante -149107. Es ist
$$\begin{pmatrix} 1 \\ \gamma \\ \gamma^2 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & -1 \\ 60 & 11 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \end{pmatrix}.$$
Die Hermitesche Normalform der Übergangsmatrix ist
$$\frac{1}{2}\begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 9 \\ 0 & 0 & 14 \end{pmatrix},$$
was zur Hermiteschen Normalform des Moduls $\mathbf{Z}[\gamma]$ führt:
$$\mathbf{Z}[\gamma] = \mathbf{Z} + \mathbf{Z}(\frac{1}{2}\alpha + \frac{9}{2}\alpha^2) + \mathbf{Z}\cdot 7\alpha^2.$$
Für den Index gilt wieder $[\mathbf{Z}[\alpha] : \mathbf{Z}[\gamma]] = \frac{7}{2}$.
3. Mit den Formeln zur Indexberechnung ergibt sich
$$[\mathbf{Z}[\beta] : \mathbf{Z}[\gamma]] = [\mathbf{Z}[\beta] : \mathbf{Z}[\alpha]][\mathbf{Z}[\alpha] : \mathbf{Z}[\gamma]] = [\mathbf{Z}[\alpha] : \mathbf{Z}[\beta]]^{-1}[\mathbf{Z}[\alpha] : \mathbf{Z}[\gamma]] = 1.$$
Andererseits zeigt unsere Normalformdarstellung aber sofort, dass
$$\mathbf{Z}[\beta] \neq \mathbf{Z}[\gamma]$$
gilt.

Der folgende Satz gibt eine wichtige Eigenschaft von Ordnungen an:

SATZ. *Sei R eine Ordnung in K und $\alpha \in R$. Dann hat das normierte charakteristische Polynom von α Koeffizienten in $\mathbf{Z}$. Insbesondere ist α ganz algebraisch und es gilt* $\mathrm{Sp}(\alpha), \mathrm{N}(\alpha) \in \mathbf{Z}$.

Beweis: Sei $\omega_1, \ldots, \omega_n$ eine $\mathbf{Z}$-Basis von R, d.h.
$$R = \mathbf{Z}\omega_1 + \cdots + \mathbf{Z}\omega_n.$$
Da R eine Ordnung ist, ist $\alpha\omega_i \in R$, d.h. es gibt $a_{ij} \in \mathbf{Z}$ mit $\alpha\omega_i = \sum_j a_{ij}\omega_j$. Die α darstellende Matrix ist also $A(\alpha) = (a_{ij}) \in M_n(\mathbf{Z})$. Das charakteristische Polynom von α hat dann natürlich ganzzahlige Koeffizienten. Da α eine Nullstelle des charakteristischen Polynoms ist, ist α ganz algebraisch. Ebenso folgt $\mathrm{Sp}(\alpha) = \mathrm{Sp}(A(\alpha)), \mathrm{N}(\alpha) = \det A(\alpha) \in \mathbf{Z}$. ■

Der folgende Satz spielt eine zentrale Rolle beim Studium der Ordnungen eines Zahlkörpers:

SATZ. *Ist R eine Ordnung in K, so ist* $\mathrm{disc}\,(R) \in \mathbf{Z}$.

Beweis: Sei $\omega_1, \ldots, \omega_n$ eine $\mathbf{Z}$-Basis von R. Der vorangegangene Satz liefert $\mathrm{Sp}(\omega_i\omega_j) \in \mathbf{Z}$, was natürlich auch

$$\mathrm{disc}\,(R) = \mathrm{disc}\,(\omega_1, \ldots, \omega_n) = \det(\mathrm{Sp}(\omega_i\omega_j)) \in \mathbf{Z}$$

impliziert. ■

Beispiel: $K = \mathbf{Q}(\alpha)$ mit $f(\alpha) = 0$ und $f = 2x^3 + 3x^2 + 5x + 7$. Das Element $\beta = 1 + 2\alpha$ hat dann das Minimalpolynom $g = x^3 + 7x + 20$, also ist $\mathbf{Z}[\beta]$ eine Ordnung in K. Für die Diskriminante gilt

$$\mathrm{disc}\,(\mathbf{Z}[\beta]) = \mathrm{disc}\,(g) = -12172 = -2^2 \cdot 17 \cdot 179.$$

Auch das folgende Lemma ist hilfreich beim Studium von Ordnungen:

LEMMA. *Ist R Ordnung eines Zahlkörper K, so gibt es immer eine $\mathbf{Z}$-Basis von R, die 1 enthält, d.h.*

$$R = \mathbf{Z} + \mathbf{Z}\omega_2 + \cdots + \mathbf{Z}\omega_n.$$

Beweis: Sei $\alpha_1, \ldots, \alpha_n$ eine $\mathbf{Z}$-Basis von R. Wegen $1 \in R$ gibt es $x_1, \ldots, x_n \in \mathbf{Z}$ mit

$$1 = x_1\alpha_1 + \cdots + x_n\alpha_n.$$

Es ist $\mathrm{ggT}(x_1, \ldots, x_n) = 1$, denn wäre $d = \mathrm{ggT}(x_1, \ldots, x_n) > 1$, so ergäbe sich durch Division $\frac{1}{d} \in R$, was aber wegen $\mathrm{N}(\frac{1}{d}) = \frac{1}{d^n}$ und $\mathrm{N}(R) \subseteq \mathbf{Z}$ einen Widerspruch ergäbe. Bringt man also die (einspaltige) Matrix $(x_1 \ldots x_n)^t$ durch elementare Zeilenumformungen auf Hermitesche Normalform, so erhält man die Matrix $(1\,0 \ldots 0)^t$, d.h. es gibt eine Matrix $G \in GL_n(\mathbf{Z})$ mit

$$G \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Sei $H = (G^{-1})^t \in GL_n(\mathbf{Z})$. Dann ist

$$(x_1\, x_2 \ldots x_n) = (1\,0 \ldots, 0)H.$$

Wir definieren jetzt eine neue $\mathbf{Z}$-Basis $\omega_1, \ldots, \omega_n$ von R durch

$$\begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = H \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}.$$

Dann ist

$$\omega_1 = (1\,0 \ldots 0) \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = (1\,0 \ldots 0)H \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = (x_1 \ldots x_n) \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = 1,$$

was wir zeigen wollten. ■

Wir geben eine alternative Formulierung:

LEMMA. *Sei $K = \mathbf{Q}(\alpha)$ ein Zahlkörper vom Grad n und R eine Ordnung in K. Ist dann $R = \mathbf{Z}\omega_1 + \cdots + \mathbf{Z}\omega_n$ die Hermitesche Normalform von R bzgl. der $\mathbf{Q}$-Basis $\alpha^{n-1}, \ldots, \alpha, 1$ von K, so gilt $\omega_n = 1$.*

Beweis: Es gibt (mit den früheren Bezeichnungen) $c_{nn}, d \in \mathbf{N}$ mit $\omega_n = \frac{c_{nn}}{d}$. Außerdem haben wir gezeigt, dass

$$R \cap \mathbf{Q} = \mathbf{Z}\frac{c_{nn}}{d}$$

gilt. Da $R \cap \mathbf{Q}$ eine Ordnung in $\mathbf{Q}$, folgt $R \cap \mathbf{Q} = \mathbf{Z}$, also $\frac{c_{nn}}{d} = 1$ und damit die Behauptung. ■

Die Ordnungen eines quadratischen Zahlkörpers lassen sich einfach beschreiben:

SATZ. *Sei $d \in \mathbf{Z}$ quadratfrei $\neq 0, 1$ und $K = \mathbf{Q}(\sqrt{d})$. Definiere*

$$\omega = \begin{cases} \frac{1+\sqrt{d}}{2} \text{ für } d \equiv 1 \bmod 4 \\ \sqrt{d} \text{ für } d \equiv 2 \bmod 4 \text{ oder } d \equiv 3 \bmod 4 \end{cases}.$$

1. *Für jede natürliche Zahl f ist*

$$R_f = \mathbf{Z}[f\omega] = \mathbf{Z} + \mathbf{Z} \cdot f\omega$$

eine Ordnung in K mit Diskriminante

$$\operatorname{disc}(R_f) = \begin{cases} f^2 d \text{ für } d \equiv 1 \bmod 4 \\ f^2 \cdot 4d \text{ für } d \equiv 2 \bmod 4 \text{ oder } d \equiv 3 \bmod 4. \end{cases}$$

2. *Jede Ordnung in K stimmt mit einer Ordnung R_f überein.*

Beweis:

1. Im Fall $d \equiv 1 \bmod 4$ ist $\operatorname{Sp}(f\omega) = f \in \mathbf{Z}$ und mit $d - 1 = 4m$ gilt

$$\operatorname{N}(f\omega) = f^2 \frac{1+\sqrt{d}}{2}\frac{1-\sqrt{d}}{2} = f^2 \frac{1-d}{4} = -f^2 m,$$

das charakteristische Polynom von $f\omega$ ist also

$$x^2 - fx - f^2 m \in \mathbf{Z},$$

$f\omega$ ist also ganz algebraisch und damit

$$R_f = \mathbf{Z}[f\omega] = \mathbf{Z} + \mathbf{Z} \cdot f\omega$$

eine Ordnung. Die Diskriminante von R_f berechnet sich als

$$\operatorname{disc}(R_f) = \operatorname{disc}(\mathbf{Z}[f\omega]) = \operatorname{disc}(x^2 - fx - f^2 m) = f^2 - 4(-f^2 m) = f^2(1 + 4m) = f^2 d,$$

wie behauptet. Im Fall $d \equiv 2 \bmod 4$ oder $d \equiv 3 \bmod 4$ ist das charakteristische Polynom von $f\omega$ das Polynom $x^2 - f^2 d$, $f\omega$ ist also offensichtlich ganz über $\mathbf{Z}$ und damit $R_f = \mathbf{Z}[f\omega]$ eine Ordnung. Die Diskriminante berechnet sich als Diskriminante des Minimalpolynoms von $f\omega$ zu $4f^2 d$.

2. Sei nun R eine Ordnung in K. Nach dem vorangegangenen Lemma können wir schreiben $R = \mathbf{Z} + \mathbf{Z}\alpha = \mathbf{Z}[\alpha]$ und $\alpha = u + v\sqrt{d}$ mit $u, v \in \mathbf{Q}$. Nun muss gelten: $\operatorname{Sp}(\alpha) = 2u \in \mathbf{Z}$ und $\operatorname{N}(\alpha) = u^2 - dv^2 \in \mathbf{Z}$. Insbesondere gilt dann $4(u^2 - dv^2) = (2u)^2 - d(2v)^2 \in \mathbf{Z}$. Da $(2u) \in \mathbf{Z}$ ist, muss auch $d(2v)^2 \in \mathbf{Z}$ gelten. Da d quadratfrei ist, folgt $2v \in \mathbf{Z}$. Schaut man genauer, so sieht man, dass aus $u^2 - dv^2 \in \mathbf{Z}$ natürlich $(2u)^2 - d(2v)^2 \equiv 0 \bmod 4$ folgt. Durch einfaches Ausprobieren findet man für $x, y \in \mathbf{Z}$:

$$x^2 - dy^2 \equiv 0 \bmod 4 \quad \Longleftrightarrow \quad \begin{cases} x \equiv y \bmod 2 & \text{für } d \equiv 1 \bmod 4, \\ x \equiv y \equiv 0 \bmod 2 & \text{für } d \equiv 2 \bmod 4 \text{ oder } d \equiv 3 \bmod 4. \end{cases}$$

Ist $d \equiv 1 \bmod 4$, so gibt es also $m \in \mathbf{Z}$ mit $2u - 2v = 2m$ und es folgt

$$\alpha = u + v\sqrt{d} = (u - v) + 2v\frac{1+\sqrt{d}}{2} = m + 2v\omega,$$

was mit der Abkürzung $f = 2v$ sofort $R = R_f$ liefert.
Ist $d \equiv 2, 3 \bmod 4$, so folgt $u, v \in \mathbf{Z}$ und damit $R = R_v$. ■

Beispiel: Sei $K = \mathbf{Q}(\alpha)$ mit $\alpha^3 = 2$. Wir betrachten die Ordnung

$$R = \mathbf{Z}[\alpha] = \mathbf{Z} + \mathbf{Z}\alpha + \mathbf{Z}\alpha^2.$$

Sei $S \subseteq R$ ebenfalls eine Ordnung. In Hermitescher Normalform können wir ansetzen

$$S = \mathbf{Z} + \mathbf{Z}\beta + \mathbf{Z}\gamma \quad \text{mit} \quad \beta = a\alpha + b\alpha^2, \quad \gamma = c\alpha^2, \quad \text{d.h.} \quad \begin{pmatrix} 1 \\ \beta \\ \gamma \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & 0 & c \end{pmatrix} \begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \end{pmatrix}$$

mit $a, b, c \in \mathbf{Z}$, $a, c \geq 1$, $0 \leq b < c$. Für den Index gilt $[R : S] = ac$. Wir wollen nun nur annehmen, dass $S \subseteq R$ ein Untermodul obiger Bauart ist, und untersuchen, wann S eine Ordnung ist. Nun leitet man leicht folgende Beziehungen her:

$$\begin{aligned} \beta^2 &= 4ab + \frac{2b^2}{a}\beta + \frac{a^3 - 2b^3}{ac}\gamma, \\ \beta\gamma &= 2ac + \frac{2bc}{a}\beta - \frac{2b^2}{a}\gamma, \\ \gamma^2 &= \frac{2c^2}{a}\beta - \frac{2bc}{a}\gamma. \end{aligned}$$

Also gilt:

$$S \text{ ist eine Ordnung} \quad \Longleftrightarrow \quad 2b^2 \equiv 2bc \equiv 2c^2 \equiv 0 \bmod a, \quad a^3 - 2b^3 \equiv 0 \bmod ac.$$

Wir wollen nun sämtliche Ordnungen S mit $1 \leq [R : S] \leq 9$ auflisten. Dazu bestimmen wir zunächst sämtliche Lösungen (a, b, c) obiger Gleichungen mit $1 \leq ac \leq 9$:

$$(1,0,1), (2,0,1), (1,2,3), (2,0,2), (1,2,5), (2,1,3), (2,0,4), (2,2,4), (3,0,3).$$

Dies ergibt folgende Ordnungen:

$$\begin{aligned} R_1 &= \mathbf{Z} + \mathbf{Z}\alpha + \mathbf{Z}\alpha^2 \\ R_2 &= \mathbf{Z} + \mathbf{Z} \cdot 2\alpha + \mathbf{Z}\alpha^2 \\ R_3 &= \mathbf{Z} + \mathbf{Z}(\alpha + 2\alpha^2) + \mathbf{Z} \cdot 3\alpha^2 \\ R_4 &= \mathbf{Z} + \mathbf{Z} \cdot 2\alpha + \mathbf{Z} \cdot 2\alpha^2 \\ R_5 &= \mathbf{Z} + \mathbf{Z}(\alpha + 2\alpha^2) + \mathbf{Z} \cdot 5\alpha^2 \\ R_6 &= \mathbf{Z} + \mathbf{Z}(2\alpha + \alpha^2) + \mathbf{Z} \cdot 3\alpha^2 \\ R_{8a} &= \mathbf{Z} + \mathbf{Z} \cdot 2\alpha + \mathbf{Z} \cdot 4\alpha^2 \\ R_{8b} &= \mathbf{Z} + \mathbf{Z}(2\alpha + 2\alpha^2) + \mathbf{Z} \cdot 4\alpha^2 \\ R_9 &= \mathbf{Z} + \mathbf{Z} \cdot 3\alpha + \mathbf{Z} \cdot 3\alpha^2 \end{aligned}$$

Wir beobachten zunächst: Es gibt keine Ordnung vom Index 7, es gibt 2 Ordnungen vom Index 8.
Wir betrachten jetzt Ordnungen der Form $\mathbf{Z}[\omega]$ mit $\omega \in R$, also o.E. $\omega = u\alpha + v\alpha^2$, $u \geq 1$ oder $u = 0, v \geq 1$. Man findet

$$\mathbf{Z}[\omega] = \mathbf{Z} + \mathbf{Z}\omega + \mathbf{Z}\omega^2 = \mathbf{Z} + \mathbf{Z}(u\alpha + v\alpha^2) + \mathbf{Z}(4uv + 2v^2\alpha + u^2\alpha^2) = \mathbf{Z} + \mathbf{Z}(u\alpha + v\alpha^2) + \mathbf{Z}(2v^2\alpha + u^2\alpha^2),$$

es gilt $[R : \mathbf{Z}[\omega]] = |u^3 - 2v^3|$. Wir suchen jetzt numerisch alle u, v mit $-9 \leq u^3 - 2v^3 \leq 9$ und beschränken uns auf $|u|, |v| \leq 1000$. Die (nichttrivialen) Lösungen sind (bis aufs Vorzeichen):

$$(u, v, u^3 - 2v^3) = (1,0,1), (1,1,-1), (0,1,-2), (1,-1,3), (5,4,-3), (2,1,6), (2,0,8), (2,2,-8).$$

Durch Bestimmung der Hermiteschen Normalform von $\mathbf{Z}[\omega]$ findet man zugehörig:

$$\mathbf{Z}[\alpha + \alpha^2] = \mathbf{Z}[\alpha] = R_1, \quad \mathbf{Z}[\alpha^2] = R_2, \quad \mathbf{Z}[\alpha - \alpha^2] = \mathbf{Z}[5\alpha + 4\alpha] = R_3, \quad \mathbf{Z}[2\alpha + \alpha^2] = R_6,$$

$$\mathbf{Z}[2\alpha] = R_{8a}, \quad \mathbf{Z}[2\alpha + 2\alpha^2] = R_{8b}.$$

Man sieht leicht: $u^3 - 2v^3 = \pm 4$ hat keine ganzzahligen Lösungen; dies liefert sofort, dass die Ordnung R_4 sich nicht in der Form $\mathbf{Z}[\omega]$ schreiben läßt.

Bemerkung: Das vorangegangene Beispiel zeigt, dass nicht jede Ordnung eines Zahlkörpers die Gestalt $\mathbf{Z}[\alpha]$ haben muss.

Wir erinnern noch kurz an einen wichtigen ringtheoretischen Begriff:

DEFINITION. Sei R ein Ring (mit Eins 1). $\alpha \in R$ heißt Einheit, wenn ein $\beta \in R$ existiert mit $\alpha\beta = \beta\alpha = 1$. Die Menge der Einheiten $R^* = \{\alpha \in R : \alpha \text{ Einheit}\}$ bildet dann bzgl. der Multiplikation eine Gruppe, die sogenannte Einheitengruppe von R.

Ist R Ordnung eines Zahlkörpers, so gilt für $\alpha \in R$, $\alpha \neq 0$ offensichtlich

$$\alpha \in R^* \quad \Longleftrightarrow \quad \frac{1}{\alpha} \in R.$$

Für eine weitere Charakterisierung stellen wir folgendes Lemma vor:

LEMMA. *Ist R Ordnung eines Zahlkörpers und $\alpha \in R$, $\alpha \neq 0$, so gilt*

$$\frac{1}{\alpha} \in \frac{1}{\mathrm{N}\alpha} R.$$

Beweis: α ist eine Nullstelle des charakteristischen Polynoms von α, d.h. es gibt $a_1, \ldots, a_n \in \mathbf{Z}$ mit

$$\alpha^n - a_1\alpha^{n-1} + a_2\alpha^{n-2} + \cdots + (-1)^{n-1}a_{n-1}\alpha + (-1)^n a_n = 0 \quad \text{und} \quad a_n = \mathrm{N}\alpha.$$

Aus

$$\alpha(\alpha^{n-1} - a_1\alpha^{n-2} + \cdots + (-1)^{n-1}a_{n-1}) = \pm\mathrm{N}\alpha$$

folgt dann die Behauptung. ■

LEMMA. *Sei R Ordnung eines Zahlkörpers K. Dann gilt für $\alpha \in R$:*

$$\alpha \in R^* \quad \Longleftrightarrow \quad \mathrm{N}\alpha = \pm 1.$$

Beweis: $\Longrightarrow$ Ist α Einheit, so gibt es $\beta \in R$ mit $\alpha\beta = 1$. Wegen $\mathrm{N}(R) \subseteq \mathbf{Z}$ folgt aus $\mathrm{N}(\alpha)\mathrm{N}(\beta) = 1$ dann $\mathrm{N}(\alpha) = \pm 1$.
$\Longleftarrow$ Das vorangegangene Lemma zeigt im Fall $\mathrm{N}\alpha = \pm 1$ sofort $\frac{1}{\alpha} \in R$, also $\alpha \in R^*$. ■

2. Die Maximalordnung – der Ring der ganzen Zahlen

LEMMA. *Sei K ein Zahlkörper.*

1. *Sind R_1, R_2 Ordnungen in K, so ist auch R_1R_2 eine Ordnung.*
2. *Ist R eine Ordnung in K und $\alpha \in K$ ganz über $\mathbf{Z}$, so ist auch $R[\alpha]$ eine Ordnung.*

Beweis:

1. Sei $R_1 = \mathbf{Z}\alpha_1 + \cdots + \mathbf{Z}\alpha_n$ und $R_2 = \mathbf{Z}\beta_1 + \cdots + \mathbf{Z}\beta_n$. Dann ist
$$R_1R_2 = \mathbf{Z}\alpha_1\beta_1 + \mathbf{Z}\alpha_1\beta_2 + \cdots + \mathbf{Z}\alpha_n\beta_n.$$
Ist $\alpha_1, \ldots, \alpha_n$ eine $\mathbf{Q}$-Basis von K, so auch $\alpha_1\beta_1, \ldots, \alpha_n\beta_1$, was zeigt, dass R_1R_2 ein Modul ist. Da $1 \in R_1$ und $1 \in R_2$, folgt $1 \in R_1R_2$. Weiter folgt aus
$$\alpha_i\alpha_j = \sum_k a_{ijk}\alpha_k \quad \text{und} \quad \beta_r\beta_s = \sum_t b_{rst}\beta_t \quad \text{mit} \quad a_{ijk}, b_{rst} \in \mathbf{Z}$$
die Beziehung
$$(\alpha_i\beta_r)(\alpha_j\beta_s) = \sum_{k,t} a_{ijk}b_{rst}\alpha_k\beta_t$$
und damit die Abgeschlossenheit von R_1R_2 bzgl. Multiplikation. Also ist R_1R_2 eine Ordnung.
2. Sei $R = \mathbf{Z}\omega_1 + \cdots + \mathbf{Z}\omega_n$. Hat α Grad m über $\mathbf{Q}$, so gibt es eine Gleichung $\alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0$ mit $a_i \in \mathbf{Z}$, also ist $\mathbf{Z}[\alpha] = \mathbf{Z} + \mathbf{Z}\alpha + \cdots + \mathbf{Z}\alpha^{m-1}$. Wie im ersten Teil zeigt man nun, dass
$$R[\alpha] = \sum_{i=1}^{n} \sum_{j=0}^{m-1} \mathbf{Z} \cdot \omega_i\alpha^j$$
eine Ordnung ist. ■

LEMMA. *Sind α und β ganze algebraische Elemente eines Zahlkörpers K, so sind auch $\alpha + \beta$ und $\alpha\beta$ ganz algebraisch.*

Beweis: Sei $R \subseteq K$ eine Ordnung. Dann ist auch $S = R[\alpha][\beta]$ eine Ordnung. Wegen $\alpha, \beta \in S$ gilt $\alpha + \beta, \alpha\beta \in S$, also sind $\alpha + \beta$ und $\alpha\beta$ ganz algebraisch. ■

Das Lemma impliziert sofort folgenden Satz:

SATZ. *Für einen Zahlkörper K ist*

$$\mathbf{Z}_K = \{\alpha \in K : \alpha \text{ ist ganz über } \mathbf{Z}\}$$

ein Ring. $\mathbf{Z}_K$ wird der Ring der ganzen Zahlen von K oder der Ganzheitsring von K genannt.

Wir erinnern an folgende wichtige Tatsache: Sind $R \subseteq S$ Ordnungen eines Zahlkörpers, so gilt die Formel

$$\operatorname{disc} R = [S : R]^2 \cdot \operatorname{disc} S.$$

Dabei sind $\operatorname{disc} R$ und $\operatorname{disc} S$ ganze Zahlen $\neq 0$.

LEMMA. *Sei K ein Zahlkörper, R eine Ordnung in K mit $\mathbf{Z}$-Basis $\omega_1, \ldots, \omega_n$ und Diskriminante $\operatorname{disc} R = m^2 d$, d quadratfrei. Sei*

$$A = \{\frac{1}{m}(z_1\omega_1 + \cdots + z_n\omega_n) : 0 \leq z_i < m\} \cap \mathbf{Z}_K.$$

Dann gilt:

$$\mathbf{Z}_K = \sum_i \mathbf{Z}\omega_i + \sum_{\alpha \in A} \mathbf{Z}\alpha,$$

insbesondere ist $\mathbf{Z}_K$ ein Modul in K.

Beweis: Da $\mathbf{Z}_K$ ein Ring ist, folgt sofort die Inklusion $\supseteq$. Sei umgekehrt $\alpha \in \mathbf{Z}_K$. Dann ist $R[\alpha]$ eine Ordnung und es gilt

$$m^2 d = \operatorname{disc} R = [R[\alpha] : R]^2 \cdot \operatorname{disc} R[\alpha].$$

Es folgt $[R[\alpha] : R] | m$ und daher $mR[\alpha] \subseteq R$, also $m\alpha \in R$, d.h. es gibt $x_i \in \mathbf{Z}$ mit $m\alpha = \sum_i x_i\omega_i$. Wir zerlegen nun $x_i = my_i + z_i$ mit $y_i, z_i \in \mathbf{Z}$ und $0 \leq z_i < m$. Es folgt

$$\alpha = \frac{1}{m}\sum_i x_i\omega_i = \sum_i y_i\omega_i + \frac{1}{m}\sum_i z_i\omega_i, \quad \text{also} \quad \frac{1}{m}\sum_i z_i\omega_i = \alpha - \sum_i y_i\omega_i \in \mathbf{Z}_K.$$

Dies zeigt die Inklusion $\subseteq$. ■

Wir können jetzt folgenden zentralen Satz formulieren:

SATZ. *Sei K ein Zahlkörper. Dann gilt:*

1. *$\mathbf{Z}_K$ ist eine Ordnung.*
2. *Jede Ordnung R von K ist in $\mathbf{Z}_K$ enthalten: $R \subseteq \mathbf{Z}_K$.*

Man nennt daher $\mathbf{Z}_K$ auch die Maximalordnung von K. Eine andere übliche Bezeichnung ist $\mathfrak{o}_K$. Eine $\mathbf{Z}$-Basis von $\mathbf{Z}_K$ wird auch als Ganzheitsbasis von K bezeichnet.

Beweis: Wir haben bereits gezeigt, dass $\mathbf{Z}_K$ ein Ring und ein Modul ist, also ist $\mathbf{Z}_K$ eine Ordnung. Wir wissen auch, dass alle Elemente einer Ordnung R ganz über $\mathbf{Z}$ sind, d.h. es gilt $R \subseteq \mathbf{Z}_K$. ■

Bemerkungen:

1. Wir werden später sehen, dass die Maximalordnung $\mathbf{Z}_K$ eines Zahlkörpers K auch ringtheoretisch unter den Ordnungen ausgezeichnet ist.
2. Die praktische Bestimmung der Maximalordnung ist eine wichtige und nichttriviale Aufgabe in der *Computational Algebraic Number Theory*.
3. Ist R Ordnung eines Zahlkörpers K, so gilt

$$\operatorname{disc} R = [\mathbf{Z}_K : R]^2 \operatorname{disc} \mathbf{Z}_K.$$

4. Die Diskriminante eines Zahlkörpers K wird definiert als Diskriminante der Maximalordnung $\mathbf{Z}_K$, d.h. $\operatorname{disc} K = \operatorname{disc} \mathbf{Z}_K$.

3. Ansätze zur Bestimmung einer Ganzheitsbasis

Wir benutzen zunächst das Lemma, mit dem wir gezeigt haben, dass $\mathbf{Z}_K$ als abelsche Gruppe endlich erzeugt ist:

1. Verfahren: Gegeben sei ein Zahlkörper K vom Grad n über $\mathbf{Q}$.

1. Man wählt sich eine Ordnung R, berechnet die Diskriminante $\operatorname{disc} R$ und zerlegt die Diskriminante als $\operatorname{disc} R = m^2 d$ mit $d \in \mathbf{Z}$ quadratfrei und $m \in \mathbf{N}$.
2. Man bestimmt
$$A = \{\frac{1}{m}(z_1\omega_1 + \cdots + z_n\omega_n) : 0 \le z_i < m\} \cap \mathbf{Z}_K$$
indem man z.B. testet, für welche Elemente $\frac{1}{m}\sum z_i\omega_i$ das charakteristische Polynom ganzzahlige Koeffizienten hat. Allerdings kann dies wegen $\#\{\frac{1}{m}\sum z_i\omega_i : 0 \le z_i < m\} = m^n$ sehr aufwendig sein.
3. Man hat nun eine Darstellung
$$\mathbf{Z}_K = \sum_i \mathbf{Z}\omega_i + \sum_{\alpha \in A} \mathbf{Z}\alpha,$$
wendet man den Hermiteschen Normalisierungsprozess darauf an, erhält man eine $\mathbf{Z}$-Basis von $\mathbf{Z}_K$.

Beispiel: Sei $K = \mathbf{Q}(\omega)$ mit $\omega^2 = d$ und $d \in \mathbf{Z}$ quadratfrei $\neq 0, 1$. (Wir haben bereits früher alle Ordnungen von K bestimmt. Dieses Beispiel dient nur zur Illustration des obigen Verfahrens.) Wir starten mit der Ordnung $R = \mathbf{Z}[\omega]$. Da ω das Minimalpolynom $x^2 - d$ hat, gilt $\operatorname{disc}(R) = 4d = 2^2 d$. Wir haben hier also $m = 2$ und
$$A = \{0, \frac{1}{2}, \frac{\omega}{2}, \frac{1+\omega}{2}\} \cap \mathbf{Z}_K.$$
Wir gehen die Kandidaten für A durch: 0 ist trivial, $\frac{1}{2}$ und $\frac{\omega}{2}$ sind nicht ganz, also bleibt nur $\frac{1+\omega}{2}$ zu untersuchen. Das Minimalpolynom von $\frac{1+\omega}{2}$ ist
$$x^2 - x + \frac{1-d}{4}.$$
Fall: $d \equiv 1 \bmod 4$*:* Dann ist $\frac{1+\omega}{2}$ ganz über $\mathbf{Z}$ und damit
$$\mathbf{Z}_K = \mathbf{Z} + \mathbf{Z}\omega + \mathbf{Z}\frac{1+\omega}{2} = \mathbf{Z} + \mathbf{Z}\frac{1+\omega}{2} = \mathbf{Z}[\frac{1+\omega}{2}].$$
Fall: $d \equiv 2, 3 \bmod 4$*:* Das Element $\frac{1+\omega}{2}$ ist nicht ganz über $\mathbf{Z}$ und damit ist
$$\mathbf{Z}_K = \mathbf{Z} + \mathbf{Z}\omega = \mathbf{Z}[\omega].$$
Wir fassen zusammen:
$$\mathbf{Z}_K = \begin{cases} \mathbf{Z}[\frac{1+\sqrt{d}}{2}] & \text{für } d \equiv 1 \bmod 4, \\ \mathbf{Z}[\sqrt{d}] & \text{für } d \equiv 2, 3 \bmod 4 \end{cases} \quad \text{und} \quad \operatorname{disc}(K) = \begin{cases} d & \text{für } d \equiv 1 \bmod 4, \\ 4d & \text{für } d \equiv 2, 3 \bmod 4. \end{cases}$$

Beispiel: Wir betrachten $K = \mathbf{Q}(\alpha)$ mit $\alpha^3 + \alpha^2 - 2\alpha + 8 = 0$. Es ist $\operatorname{disc}(\mathbf{Z}[\alpha]) = -2^2 \cdot 503$. Wir müssen also
$$A = \{0, \frac{1}{2}, \frac{\alpha}{2}, \frac{\alpha^2}{2}, \frac{1+\alpha}{2}, \frac{1+\alpha^2}{2}, \frac{\alpha+\alpha^2}{2}, \frac{1+\alpha+\alpha^2}{2}\} \cap \mathbf{Z}_K$$

bestimmen. Die Minimalpolynome der Kandidaten sind:

Element	Minimalpolynom
$\frac{1}{2}$	$x - \frac{1}{2}$
$\frac{\alpha}{2}$	$x^3 + \frac{1}{2}x^2 - \frac{1}{2}x + 1$
$\frac{\alpha^2}{2}$	$x^3 - \frac{5}{2}x^2 - 3x - 8$
$\frac{1+\alpha}{2}$	$x^3 - x^2 - \frac{1}{4}x + \frac{5}{4}$
$\frac{1+\alpha^2}{2}$	$x^3 - 4x^2 + \frac{1}{4}x - \frac{29}{4}$
$\frac{\alpha+\alpha^2}{2}$	$x^3 - 2x^2 + 3x - 10$
$\frac{1+\alpha+\alpha^2}{2}$	$x^3 - \frac{7}{2}x^2 + \frac{23}{4}x - \frac{97}{8}$

Nur $\frac{\alpha+\alpha^2}{2}$ ist von diesen Elementen ganz über $\mathbf{Z}$. Daher folgt

$$\mathbf{Z}_K = \mathbf{Z}[\alpha] + \mathbf{Z}\frac{\alpha+\alpha^2}{2} = \mathbf{Z} + \mathbf{Z}\alpha + \mathbf{Z}\frac{\alpha+\alpha^2}{2} \quad \text{und} \quad \operatorname{disc} K = -503.$$

Wir betrachten nun Ordnungen der Form $\mathbf{Z}[\beta]$, wobei wir

$$\beta = u + v\alpha + w\frac{\alpha+\alpha^2}{2} \quad \text{mit} \quad u, v, w \in \mathbf{Z}$$

ansetzen können. Man berechnet

$$\operatorname{disc} \mathbf{Z}[\beta] = -503(2v^3 + v^2w - vw^2 + 2w^3)^2.$$

Nun gilt modulo 2:

$$2v^3 + v^2w - vw^2 + 2w^3 \equiv vw(v-w) \equiv 0 \bmod 2,$$

d.h. $2^2 \cdot 503 | \operatorname{disc} \mathbf{Z}[\beta]$. Dies zeigt, dass der Index $[\mathbf{Z}_K : \mathbf{Z}[\beta]]$ immer gerade ist. Insbesondere gilt $\mathbf{Z}_K \neq \mathbf{Z}[\beta]$, d.h. die Maximalordnung $\mathbf{Z}_K$ hat nicht die Gestalt $\mathbf{Z}[\beta]$. Außerdem gilt

$$2 \nmid \operatorname{disc} \mathbf{Z}_K, \quad \text{aber} \quad 2 | \operatorname{disc} \mathbf{Z}[\beta] \quad \text{für alle Ordnungen } \mathbf{Z}[\beta],$$

d.h. 2 teilt die Diskriminante des Zahlkörpers nicht, aber alle Elementdiskriminanten $\operatorname{disc} \mathbf{Z}[\beta]$. Man nennt die Primzahl 2 hier einen außerwesentlichen Diskriminantenteiler. (Das Beispiel geht auf Dedekind zurück.)

Beispiel: Ist K ein Zahlkörper und hat man eine Ordnung R, so dass $\operatorname{disc}(R)$ quadratfrei ist, so ist R die Maximalordnung, denn aus

$$\operatorname{disc}(R) = [\mathbf{Z}_K : R]^2 \cdot \operatorname{disc}(\mathbf{Z}_K)$$

folgt $[\mathbf{Z}_K : R] = 1$.

Beispiel: $K = \mathbf{Q}(\alpha)$ mit $f(\alpha) = 0$ und $f = x^3 + 7x + 20$. Die Ordnung $\mathbf{Z}[\alpha]$ hat Diskriminante

$$\operatorname{disc}(\mathbf{Z}[\alpha]) = -12172 = -2^2 \cdot 17 \cdot 179.$$

Wir wollen die Maximalordnung $\mathbf{Z}_K$ bestimmen und betrachten dazu

$$A = \{\frac{1}{2}(u + v\alpha + w\alpha^2) : 0 \leq u, v, w \leq 1\} \cap \mathbf{Z}_K.$$

Ist $\beta = \frac{1}{2}(u + v\alpha + w\alpha^2) \in A$, so gilt

$$\operatorname{Sp}(\beta) = \frac{3}{2}u - 7w \in \mathbf{Z},$$

also $u = 0$. Es bleiben noch 3 nichttriviale Möglichkeiten: $\frac{1}{2}\alpha$ hat das Minimalpolynom $x^3 + \frac{7}{4}x + \frac{5}{2}$, $\frac{1}{2}\alpha^2$ hat das Minimalpolynom $x^3 + 7x^2 + \frac{49}{4}x - 50$, $\frac{1}{2}\alpha + \frac{1}{2}\alpha^2$ hat das Minimalpolynom $x^3 + 7x^2 + 29x - 30$ (mit Diskriminante $-7^2 \cdot 17 \cdot 179$). Also ist $A = \{0, \frac{1}{2}\alpha + \frac{1}{2}\alpha^2\}$ und damit

$$\mathbf{Z}_K = \mathbf{Z} + \mathbf{Z}\alpha + \mathbf{Z}\alpha^2 + \mathbf{Z}(\frac{1}{2}\alpha + \frac{1}{2}\alpha^2) = \mathbf{Z} + \mathbf{Z}(\frac{1}{2}\alpha + \frac{1}{2}\alpha^2) + \mathbf{Z}\alpha^2 \quad \text{mit} \quad \operatorname{disc} K = -17 \cdot 179 = -3043.$$

Frage: Gibt es ein $\beta \in K$ mit $\mathbf{Z}_K = \mathbf{Z}[\beta]$? Wegen $\beta \in \mathbf{Z}_K$ können wir ansetzen

$$\beta = u + v(\frac{1}{2}\alpha + \frac{1}{2}\alpha^2) + w\alpha^2 \quad \text{mit} \quad u, v, w \in \mathbf{Z}.$$

Nun gilt

$$\operatorname{disc}\mathbf{Z}[\beta] = \operatorname{disc}(u + v(\frac{1}{2}\alpha + \frac{1}{2}\alpha^2) + w\alpha^2) = -3043(7v^3 + 37v^2w + 67vw^2 + 40w^3)^2.$$

Sei $\lambda(v,w) = 7v^3+37v^2w+67vw^2+40w^3$. Genau dann gilt $\mathbf{Z}_K = \mathbf{Z}[\beta]$, wenn $\lambda(v,w) = \pm 1$ ist. Wir listen die Tripel $(v,w,\lambda(v,w))$ auf mit $(v,w) \neq 0$, $0 \leq v \leq 10000$, $-10000 \leq w \leq 10000$ und $|\lambda(v,w)| < 10$:

$$(2,-1,2),(1,-1,3),(4,-3,4),(1,0,7),(3,-2,7),(17,-13,-7).$$

Vermutung: Es gibt kein $\beta \in K$ mit $\mathbf{Z}_K = \mathbf{Z}[\beta]$.

Bemerkung: Das vorgestellte Verfahren funktioniert, wenn in der Zerlegung $\operatorname{disc} R = m^2 d$ die Zahl m nicht zu groß ist um die Menge

$$A = \{\frac{1}{m}(z_1\omega_1 + \cdots + z_n\omega_n) : 0 \leq z_i < m\} \cap \mathbf{Z}_K$$

explizit zu bestimmen. Wir werden jetzt diesen Ansatz etwas verfeinern.

LEMMA. *Sei R Ordnung eines Zahlkörpers K mit einer $\mathbf{Z}$-Basis $\omega_1,\ldots,\omega_n$, $\operatorname{disc} R = m^2 d$ mit $d \in \mathbf{Z}$ quadratfrei, $m \in \mathbf{N}$. Für eine Primzahl p wird definiert*

$$A_p = \{\frac{1}{p}(z_1\omega_1 + \cdots + z_n\omega_n) : 0 \leq z_i \leq p-1\} \cap \mathbf{Z}_K.$$

Dann gilt:

1. *Ist $\alpha \in A_p \setminus \{0\}$, so ist $R[\alpha]$ eine Ordnung und es gilt*
$$[R[\alpha] : R] = p^l \quad \text{für ein} \quad l \geq 1.$$
Außerdem gilt $p|[\mathbf{Z}_K : R]$ und $p^2|\operatorname{disc} R$.
2. *$v_p(\operatorname{disc}\mathbf{Z}_K) < v_p(\operatorname{disc} R) \iff A_p \neq \{0\}$.*
3. *Gilt $A_p = \{0\}$ für alle Primzahlen p mit $p^2|\operatorname{disc} R$, so ist bereits $R = \mathbf{Z}_K$.*
4. *Durch*
$$\mathbf{F}_p \times A_p \to A_p, \quad (c, \frac{1}{p}\sum_i z_i\omega_i) \mapsto \frac{1}{p}\sum_i (cz_i \bmod p)\omega_i$$
wird A_p zu einem $\mathbf{F}_p$-Vektorraum.
5. *Definiert man*
$$\begin{aligned}\widetilde{A}_p \quad = \quad & \{\frac{1}{p}(z_1\omega_1 + \cdots + z_n\omega_n) : 0 \leq z_i \leq p-1,\\ & z_1 = \cdots = z_{i-1} = 0, z_i = 1 \text{ für ein } i \text{ mit } 1 \leq i \leq n\} \cap \mathbf{Z}_K,\end{aligned}$$
so gilt
$$A_p \neq \{0\} \quad \iff \quad \widetilde{A}_p \neq \emptyset.$$

Beweis:

1. Sei $\alpha \in A_p \setminus \{0\}$. Wegen $\alpha \in \mathbf{Z}_K$ ist $R[\alpha]$ eine Ordnung in K, wegen $\alpha \neq 0$ gilt $R \neq R[\alpha]$. Aus $p\alpha \in R$ folgt $p^i\alpha^i \in R$, sodass wegen $R[\alpha] = R + R\alpha + \cdots + R\alpha^{n-1}$ gilt $p^{n-1}R[\alpha] \subseteq R$. Also annulliert p^{n-1} die Faktorgruppe $R[\alpha]/R$, was zeigt, dass $[R[\alpha] : R] = \#R[\alpha]/R$ eine p-Potenz ist. Wegen $R \subseteq R[\alpha] \subseteq \mathbf{Z}_K$ erhält man aus $[\mathbf{Z}_K : R] = [\mathbf{Z}_K : R[\alpha]] \cdot [R[\alpha] : R]$ sofort $p|[\mathbf{Z}_K : R]$ und aus $\operatorname{disc} R = [\mathbf{Z}_K : R]^2 \operatorname{disc}\mathbf{Z}_K$ dann $p^2|\operatorname{disc} R$.
2. $\Longrightarrow$ Sei $v_p(\operatorname{disc}\mathbf{Z}_K) < v_p(\operatorname{disc} R)$. Wegen $\operatorname{disc} R = [\mathbf{Z}_K : R]^2 \operatorname{disc}\mathbf{Z}_K$ folgt $p|[\mathbf{Z}_K : R]$. Unter Verwendung der Smithschen Normalform können wir schreiben
$$\mathbf{Z}_K = \mathbf{Z}\alpha_1 + \cdots + \mathbf{Z}\alpha_n, \quad R = \mathbf{Z}d_1\alpha_1 + \cdots + \mathbf{Z}d_n\alpha_n$$
mit $d_1|d_2|\ldots|d_n$, $d_i \in \mathbf{N}$ und $[\mathbf{Z}_K : R] = d_1 d_2 \ldots d_n$. Es folgt $p|d_n$. Schreiben wir $d_n = d_n' p$ und $\alpha = d_n'\alpha_n$, so gilt $\alpha \in \mathbf{Z}_K$, $p\alpha \in R$, $\alpha \notin R$. Es gibt eine Darstellung $p\alpha = \sum_i x_i\omega_i$ mit $x_i \in \mathbf{Z}$. Wir zerlegen $x_i = y_i p + z_i$ mit $y_i, z_i \in \mathbf{Z}$, $0 \leq z_i \leq p-1$ und $(z_1,\ldots,z_n) \neq (0,\ldots,0)$. Dann ist
$$\frac{1}{p}\sum_i z_i\omega_i = \alpha - \sum_i y_i\omega_i \in \mathbf{Z}_K, \quad \text{also} \quad \frac{1}{p}\sum_i z_i\omega_i \in A_p \setminus \{0\}.$$

$\Longleftarrow$ Gilt $A_p \neq \{0\}$, so folgt mit 1. $p|[\mathbf{Z}_K : R]$, was wegen $\operatorname{disc} R = [\mathbf{Z}_K : R]^2 \operatorname{disc} \mathbf{Z}_K$ sofort die Behauptung liefert.

3. Wäre $R \neq \mathbf{Z}_K$, so gäbe es eine Primzahl p mit $p|[\mathbf{Z}_K : R]$, was mit $\operatorname{disc} R = [\mathbf{Z}_K : R]^2 \operatorname{disc} \mathbf{Z}_K$ die Beziehungen $p^2|\operatorname{disc} R$ und $v_p(\operatorname{disc} \mathbf{Z}_K) < v_p(\operatorname{disc} R)$ zeigt. Nach 2. gilt dann $A_p \neq \{0\}$. Damit folgt die Behauptung.
4. Sei $c \in \mathbf{Z}$ und $\alpha = \frac{1}{p}\sum_i z_i\omega_i \in A_p$, d.h. $0 \leq z_i \leq p-1$. Wir zerlegen $cz_i = s_ip+t_i$ mit $0 \leq t_i \leq p-1$. Dann ist
$$\frac{1}{p}\sum_i t_i\omega_i = c \cdot \frac{1}{p}\sum_i z_i\omega_i - \sum_i s_i\omega_i \in \mathbf{Z}_K, \quad \text{also} \quad \frac{1}{p}\sum_i t_i\omega_i \in A_p.$$
Mit $t_i \equiv cz_i \bmod p$ folgt sofort die Behauptung.
5. Die Richtung $\Longleftarrow$ ist trivial. Sei umgekehrt $\alpha = \frac{1}{p}\sum_i z_i\omega_i \in A_p \setminus \{0\}$. Dann gibt es einen Index $i \in \{1, \ldots, n\}$ mit $z_1 = z_2 = \cdots = z_{i-1} = 0$ und $1 \leq z_i \leq p-1$. Wählt man $c \in \mathbf{Z}$ mit $cz_i \equiv 1 \bmod p$, so liefert das Bild von $c \cdot \alpha$ in A_p ein Element von $\widetilde{A}_p$. ■

Das Lemma führt jetzt zu folgender Vorgehensweise:

2. Verfahren zur Bestimmung von $\mathbf{Z}_K$: Gegeben sei ein Zahlkörper K vom Grad n über $\mathbf{Q}$.

1. Man wählt eine Ordnung R und berechnet $\operatorname{disc} R = m^2d$ mit $d \in \mathbf{Z}$ quadratfrei, $m \in \mathbf{N}$. Sei P die Menge der Primzahlen, die m teilen.
2. Man wählt eine $\mathbf{Z}$-Basis $\omega_1, \ldots, \omega_n$ für R und definiert
$$\begin{aligned} A_p &= \{\frac{1}{p}(z_1\omega_1 + \cdots + \omega_n) : 0 \leq z_i \leq p-1\} \cap \mathbf{Z}_K \quad \text{und} \\ \widetilde{A}_p &= \{\frac{1}{p}(z_1\omega_1 + \cdots + z_n\omega_n) : 0 \leq z_i \leq p-1, \\ &\qquad z_1 = \cdots = z_{i-1} = 0, z_i = 1 \text{ für ein } i \text{ mit } 1 \leq i \leq n\} \cap \mathbf{Z}_K. \end{aligned}$$
(Es gilt $\#\widetilde{A}_p \leq p^{n-1} + p^{n-2} + \cdots + p + 1 = \frac{p^n-1}{p-1}$.)
3. Ist $P = \emptyset$, so gilt $R = \mathbf{Z}_K$ und man ist fertig. Andernfalls wählt man eine Primzahl $p \in P$ und versucht, ein Element in $\widetilde{A}_p$ zu bestimmen.
4. Ist $\widetilde{A}_p = \emptyset$, so streicht man p aus der Liste P und geht zurück zu 3.
5. Hat man ein $\alpha \in \widetilde{A}_p$ gefunden, so ersetzt man R durch $R[\alpha]$ und geht zurück zu 2.

Beispiel: Wir betrachten $K = \mathbf{Q}(\alpha)$ mit $\alpha^4 + 12 = 0$.

- Wir starten mit $R = \mathbf{Z}[\alpha] = \mathbf{Z}\alpha^3 + \mathbf{Z}\alpha^2 + \mathbf{Z}\alpha + \mathbf{Z}$. Es gilt
$$\operatorname{disc} R = 442368 = 2^{14} \cdot 3^3 = (2^7 \cdot 3)^2 \cdot 3.$$
Daher setzen wir $P = \{2, 3\}$.
- Für $p = 3$ finden wir $\widetilde{A}_3 = \emptyset$, also müssen wir nur noch die Primzahl $p = 2$ betrachten.
- Ausgehend von der Ordnung R finden wir
$$\alpha_1 = \frac{1}{2}\alpha^3 \in \widetilde{A}_2, \quad \text{damit} \quad R_1 = R[\alpha_1] = \mathbf{Z}\frac{1}{2}\alpha^3 + \mathbf{Z}\alpha^2 + \mathbf{Z}\alpha + \mathbf{Z}.$$
- Wir gehen jetzt von R_1 aus und finden
$$\alpha_2 = \frac{1}{4}\alpha^3 + \frac{1}{2}\alpha \quad \text{und damit} \quad R_2 = R_1[\alpha_2] = \mathbf{Z}(\frac{1}{4}\alpha^3 + \frac{1}{2}\alpha) + \mathbf{Z}\frac{1}{2}\alpha^2 + \mathbf{Z}\alpha + 1.$$
- Für R_2 finden wir
$$\alpha_3 = \frac{1}{4}\alpha^2 + \frac{1}{2} \quad \text{und} \quad R_3 = R_2[\alpha_3] = \mathbf{Z}(\frac{1}{4}\alpha^3 + \frac{1}{2}\alpha) + \mathbf{Z}(\frac{1}{4}\alpha^2 + \frac{1}{2}) + \mathbf{Z}\alpha + \mathbf{Z}.$$
- Für R_3 gilt $\widetilde{A}_2 = \emptyset$ und daher schließlich
$$\mathbf{Z}_K = R_3 = \mathbf{Z}(\frac{1}{4}\alpha^3 + \frac{1}{2}\alpha) + \mathbf{Z}(\frac{1}{4}\alpha^2 + \frac{1}{2}) + \mathbf{Z}\alpha + \mathbf{Z}.$$
Für die Indizes gilt
$$[R_1 : R] = 2, \quad [R_2 : R_1] = 4, \quad [R_3 : R_2] = 2 \quad \text{und} \quad \operatorname{disc} \mathbf{Z}_K = \operatorname{disc} R_3 = 2^6 \cdot 3^3 = 1728.$$

Beispiel: Wir betrachten $K = \mathbf{Q}(\alpha)$ mit $\alpha^3 = d$, wobei $d \geq 2$ kubikfrei sein soll. Es ist $\operatorname{disc}\mathbf{Z}[\alpha] = -27d^2 = (3d)^2 \cdot (-3)$, daher müssen wir die Primteiler von $3d$ anschauen. Wir haben

$$\widetilde{A}_p = \{\frac{\alpha^2 + v\alpha + w}{p}, \frac{\alpha + w}{p}, \frac{1}{p} : 0 \leq v, w \leq p-1\} \cap \mathbf{Z}_K,$$

wobei wir natürlich $\frac{1}{p}$ sofort weglassen können. Wir stellen die zugehörigen Minimalpolynome zusammen:

$$\begin{aligned}
\text{Minimalpolynom}\,(\frac{1}{p}(\alpha^2 + v\alpha + w)) &= x^3 - \frac{3w}{p}x^2 - \frac{3(dv - w^2)}{p^2}x - \frac{d^2 + dv^3 - 3dvw + w^3}{p^3}, \\
\text{Minimalpolynom}\,(\frac{1}{p}(\alpha + w)) &= x^3 + \frac{3w}{p}x^2 - \frac{3w^2}{p^2}x + \frac{d + w^3}{p^3}, \\
\text{Minimalpolynom}\,(\frac{1}{p}) &= x - \frac{1}{p}.
\end{aligned}$$

Wir betrachten zunächst die Primzahl $p = 3$. Wäre $\frac{1}{3}(\alpha + w)$ mit $w \in \{0, 1, 2\}$ ganz über $\mathbf{Z}$, so wäre $3w^2 \equiv 0 \bmod 9$ und $d + w^3 \equiv 0 \bmod 27$. Die erste Kongruenz liefert $w = 0$, dann den Widerspruch $d \equiv 0 \bmod 27$ ergeben würde. Wir betrachten nun $\beta = \frac{1}{3}(\alpha^2 + v\alpha + w)$. Die Ganzheit ist äquivalent mit $dv \equiv w^2 \bmod 3$ und $d^2 + dv^3 - 3dvw + w^3 \equiv 0 \bmod 27$. Durch Ausprobieren findet man

$$\widetilde{A}_3 = \begin{cases} \{\frac{\alpha^2}{3}\} & \text{für } d \equiv 0 \bmod 9, \\ \{\frac{\alpha^2+\alpha+1}{3}\} & \text{für } d \equiv 1 \bmod 9, \\ \{\frac{\alpha^2+2\alpha+1}{3}\} & \text{für } d \equiv 8 \bmod 9. \end{cases}$$

Für $p \neq 3$, $p|d$ erhält man analog

$$\widetilde{A}_p = \begin{cases} \emptyset & \text{für } p^2 \nmid d, \\ \{\frac{\alpha^2}{p}\} & \text{für } p^2|d. \end{cases}$$

Als einfache Folgerung erhalten wir: Ist d quadratfrei und $d \not\equiv \pm 1 \bmod 9$, so ist $\mathbf{Z}_K = \mathbf{Z}[\alpha]$.

Beispiel: Wir betrachten $K = \mathbf{Q}(\alpha)$ mit $\alpha^4 - 10\alpha^2 + 1 = 0$ und starten mit $R = \mathbf{Z}[\alpha]$. Es gilt $\operatorname{disc} R = 147456 = 2^{14} \cdot 3^2 = (2^7 \cdot 3)^2$, daher müssen wir die Primzahlen 2 und 3 anschauen.

- Für R findet man durch Ausprobieren, dass $\widetilde{A}_3 = \emptyset$ gilt. Also ist $v_3(\operatorname{disc}\mathbf{Z}_K) = v_3(\operatorname{disc} R) = 2$ und somit $[\mathbf{Z}_K : R]|2^7$. Wir müssen nur noch die Primzahl 2 anschauen.
- Für R findet man
$$\alpha_1 = \frac{1}{2}\alpha^3 + \frac{1}{2}\alpha \in \widetilde{A}_2 \quad \text{und damit} \quad R_1 = R[\alpha_1] = \mathbf{Z}(\frac{1}{2}\alpha^3 + \frac{1}{2}\alpha) + \mathbf{Z}(\frac{1}{2}\alpha^2 + \frac{1}{2}) + \mathbf{Z}\alpha + \mathbf{Z}.$$
- Wir setzen $\widetilde{A}_2$ für R_2 an und finden
$$\alpha_2 = \frac{1}{4}\alpha^3 + \frac{1}{4}\alpha^2 + \frac{3}{4}\alpha + \frac{3}{4} \in \widetilde{A}_2.$$
Nun berechnen wir
$$R_2 = R_1[\alpha_2] = \mathbf{Z}(\frac{1}{4}\alpha^3 + \frac{1}{4}\alpha^2 + \frac{3}{4}\alpha + \frac{3}{4}) + \mathbf{Z}(\frac{1}{2}\alpha^2 + \frac{1}{2}) + \mathbf{Z}\alpha + \mathbf{Z}.$$
- Setzen wir $\widetilde{A}_2$ für R_2 an, so erhalten wir nun $\widetilde{A}_2 = \emptyset$. Damit gilt $\mathbf{Z}_K = R_2$. Wir haben
$$[R_1 : R] = 4, \quad [R_2 : R_1] = 2, \quad \operatorname{disc}\mathbf{Z}_K = \operatorname{disc} R_2 = 2304 = 2^8 \cdot 3^2.$$

Bemerkung: Gilt $p^2|\operatorname{disc} R$, so enthält $\widetilde{A}_p$

$$p^{n-1} + p^{n-2} + \cdots + p + 1 = \frac{p^n - 1}{p - 1}$$

Kandidaten. Für größere p ist dann die Bestimmung von $\widetilde{A}_p$ eventuell sehr aufwendig, in jedem Fall dann, wenn $\widetilde{A}_p = \emptyset$ gilt. Wir werden später ein weiteres Verfahren vorstellen, das diese Schwierigkeiten meidet.

Wir werden jetzt einen Satz beweisen, der ausgehend von einer Ordnung $\mathbf{Z}[\alpha]$ die Gestalt von $\mathbf{Z}_K$ beschreibt.

LEMMA. *Sei* $\mathbf{Z}[\alpha]$ *Ordnung in einem Zahlkörper* K, $M \subseteq K$ *ein endlich erzeugter* $\mathbf{Z}$*-Modul maximalen Rangs in* K, *so dass gilt* $\alpha M \subseteq M$. *Dann besitzt* M *eine* $\mathbf{Z}$*-Basis* $\omega_0, \omega_1, \ldots, \omega_{n-1}$ *mit folgenden Eigenschaften:*

1. *Es gibt* $d, c \in \mathbf{N}$, $d_i \in \mathbf{N}$, $b_{ij} \in \mathbf{N}_0$ *mit*

$$1 = d_0 | d_1 | d_2 | \ldots | d_{n-1} | c, \quad b_{ij} < \frac{d_i}{d_j} \text{ für } i > j$$

und

$$\omega_i = \frac{c}{d}\frac{1}{d_i}(\alpha^i + \sum_{0 \le j < i} b_{ij}\alpha^j),$$

also

$$\omega_0 = \frac{c}{d}, \quad \omega_1 = \frac{c}{d}\frac{1}{d_1}(\alpha + b_{10}), \quad \omega_2 = \frac{c}{d}\frac{1}{d_2}(\alpha^2 + b_{21}\alpha + b_{20}), \quad \ldots$$

2. $M \cap \mathbf{Q} = \frac{c}{d}\mathbf{Z}$.

Beweis:

1. Wir bestimmen die Hermitesche Normalform von M bzgl. $\alpha^{n-1}, \ldots, \alpha, 1$, die wir in der Form

$$\begin{pmatrix} \omega_{n-1} \\ \vdots \\ \omega_1 \\ \omega_0 \end{pmatrix} = \frac{1}{d} \begin{pmatrix} c_{n-1,n-1} & c_{n-1,n-2} & \cdots & c_{n-1,0} \\ & c_{n-2,n-2} & \cdots & c_{n-2,0} \\ & & & \\ & & c_{11} & c_{10} \\ & & & c_{00} \end{pmatrix} \begin{pmatrix} \alpha^{n-1} \\ \vdots \\ \alpha \\ 1 \end{pmatrix}$$

schreiben mit $d = \min\{\widetilde{d} : \widetilde{d}M \subseteq \mathbf{Z}[\alpha], \widetilde{d} \in \mathbf{N}\}$, $c_{ij} \in \mathbf{N}_0$, $0 \le c_{ij} < c_{jj}$ für $j < i$. Für die folgenden Aussagen können wir o.E. $d = 1$ annehmen.

2. Wir zeigen jetzt durch Induktion, dass gilt

$$c_{ii} | c_{kl} \text{ für alle } k, l \text{ mit } k \le i.$$

Die Aussage ist trivial im Fall $i = 0$. Wir setzen jetzt voraus, dass gilt $c_{i-1,i-1} | c_{kl}$ für alle k, l mit $k \le i-1$. Dies heißt insbesondere

$$\omega_0, \ldots, \omega_{i-1} \in c_{i-1,i-1}\mathbf{Z}[\alpha] = \mathbf{Z} \cdot c_{i-1,i-1}\alpha^{n-1} + \cdots + \mathbf{Z} \cdot c_{i-1,i-1}\alpha + \mathbf{Z} \cdot c_{i-1,i-1}.$$

Nun ist

$$\alpha\omega_{i-1} = c_{i-1,i-1}\alpha^i + c_{i-1,i-2}\alpha^{i-1} + \cdots + c_{i-1,0}\alpha.$$

Wegen der Voraussetzung $\alpha\omega_i \in M$ gibt es $m_i, \ldots, m_0 \in \mathbf{Z}$ mit

$$\alpha\omega_{i-1} = m_i\omega_i + m_{i-1}\omega_{i-1} + \cdots + m_1\omega_1 + m_0\omega_0.$$

Nun ist

$$m_i\omega_i = m_i c_{ii}\alpha^i + m_i c_{i,i-1}\alpha^{i-1} + \cdots + m_i c_{i,1}\alpha + m_i c_{i,0}.$$

Durch Koeffizientenvergleich bei α^i findet man $c_{i-1,i-1} = m_i c_{ii}$, was bereits $c_{ii} | c_{i-1,i-1}$ liefert, und weiter

$$m_i\omega_i \in c_{i-1,i-1}\mathbf{Z}[\alpha] = m_i c_{ii}\mathbf{Z}[\alpha],$$

was dann $c_{ii} | c_{ij}$ für alle j liefert.

3. Wir definieren jetzt

$$b_{ij} = \frac{c_{ij}}{c_{ii}}, \quad d_i = \frac{c_{00}}{c_{ii}}, \quad c = c_{00}.$$

   (a) Dann ist $c_{ij} = \frac{c}{d_i}b_{ij}$, was die bedeutete Form liefert.
   (b) Die Aussage $c_{ij} < c_{jj}$ übersetzt sich in $b_{ij} < \frac{d_i}{d_j}$ für $j < i$.
   (c) Die Teilbarkeit $c_{jj} | c_{ii}$ für $i < j$ liefert $d_i | d_j$.
   (d) Nach Definition gilt $d_0 = 1$ und $d_i | c$. ■

SATZ. *Sei* $\mathbf{Z}[\alpha]$ *Ordnung eines Zahlkörpers* K *vom Grad* n. *Sei* R *eine weitere Ordnung mit* $\alpha \in R$. *Dann besitzt* R *eine* $\mathbf{Z}$*-Basis* $1, \omega_1, \ldots, \omega_{n-1}$ *folgender Form:*

1. *Mit* $d_0 = 1$, $d_1, \ldots, d_{n-1} \in \mathbf{N}$, $b_{ij} \in \mathbf{N}_0$ *gilt*
$$\omega_i = \frac{1}{d_i}(\alpha^i + b_{i,i-1}\alpha^{i-1} + \cdots + b_{i,1}\alpha + b_{i,0}).$$
2. $d_1|d_2|d_3|\ldots|d_{n-1}$, $b_{ij} < \frac{d_i}{d_j}$ *für* $i > j$.
3. $[R : \mathbf{Z}[\alpha]] = d_1 \ldots d_{n-1}$ *und daher* $(d_1 d_2 \ldots d_{n-1})^2 | \mathrm{disc}\,(\mathbf{Z}[\alpha])$.
4. *Für* $i_1 + \cdots + i_r < n$ *gilt* $d_{i_1} \ldots d_{i_r} | d_{i_1+\cdots+i_r}$.

Beweis:

1. Wir wenden das vorangegangene Lemma im Fall $M = R$ an. Wegen $R \cap \mathbf{Z} = \mathbf{Z}$ folgt $d = c$ und damit der Hauptteil der Aussagen.
2. Die Formel für den Index ist klar, aus
$$\mathrm{disc}\,(\mathbf{Z}[\alpha]) = [R : \mathbf{Z}[\alpha]]^2 \mathrm{disc}\,(R)$$
und $\mathrm{disc}\,(R), \mathrm{disc}\,(\mathbf{Z}[\alpha]) \in \mathbf{N}$ folgt der andere Teil.
3. Sei $i = i_1 + \cdots + i_r$. Da R ein Ring ist, ist $\omega_{i_1} \ldots \omega_{i_r}$ in R, also gibt es $m_i, m_{i-1}, \ldots, m_0 \in \mathbf{Z}$ mit
$$\omega_{i_1} \ldots \omega_{i_r} = m_i\omega_i + m_{i-1}\omega_{i-1} + \cdots + m_1\omega_1 + m_0.$$
Koeffzientenvergleich bei α^i ergibt
$$\frac{1}{d_{i_1} \ldots d_{i_r}} = m_i \frac{1}{d_i}$$
und damit die Behauptung. ■

Beispiel: Wir wollen mit Hilfe des vorangegangenen Satzes für $K = \mathbf{Q}(\alpha)$ mit $\alpha^3 = 2$ eine Ganzheitsbasis bestimmen. Wir können schreiben
$$\mathbf{Z}_K = \mathbf{Z} + \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2 \text{ mit } \omega_1 = \frac{1}{d_1}(\alpha + b_{10}), \omega_2 = \frac{1}{d_2}(\alpha^2 + b_{21}\alpha + b_{20}) \text{ mit } \ldots$$
Für die Diskriminante gilt $\mathrm{disc}\,(\mathbf{Z}[\alpha]) = -27 \cdot 4 = -6^2 \cdot 3$, also folgt $d_1 d_2 | 6$. Mit $d_1^2 | d_2$ folgt $d_1^3 | 6$, so dass nur $d_1 = 1$ und damit $b_{10} = 0$ möglich ist. Es bleiben jetzt die Beziehungen
$$d_2 | 6, \quad b_{21} < d_2, \quad b_{20} < d_2.$$
Das Minimalpolynom von ω_2 ist
$$x^3 - \frac{3b_{20}}{d_2}x^2 + \frac{3(b_{20}^2 - 2b_{21})}{d_2^2}x - \frac{b_{20}^3 - 6b_{21}b_{20} + 4 + 2b_{21}^3}{d_2^3}.$$
Durch Ausprobieren der (endlich vielen) Möglichkeiten $d_2 = 6, 3, 2$ sieht man, dass nur der Fall $d_2 = 1$ und damit $b_{21} = b_{20} = 0$ übrig bleibt. D.h. $\omega_2 = \alpha^2$ und damit gilt
$$\mathbf{Z}_K = \mathbf{Z}[\alpha].$$

Beispiel: Wir betrachten $K = \mathbf{Q}(\sqrt{2}, \sqrt{3})$. Aus
$$(\sqrt{2} + \sqrt{3}) \begin{pmatrix} 1 \\ \sqrt{2} \\ \sqrt{3} \\ \sqrt{6} \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 2 & 0 & 0 & 1 \\ 3 & 0 & 0 & 1 \\ 0 & 3 & 2 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ \sqrt{2} \\ \sqrt{3} \\ \sqrt{6} \end{pmatrix}$$
berechnet sich das Minimalpolynom von $\alpha = \sqrt{2} + \sqrt{3}$ zu
$$f = x^4 - 10x^2 + 1 \quad \text{und} \quad \mathrm{disc}\,(\mathbf{Z}[\alpha]) = \mathrm{disc}\,(f) = 147456 = 2^{14} \cdot 3^2 = (2^7 \cdot 3)^2.$$
Wir wollen mit Hilfe des letzten Satzes eine Ganzheitsbasis von K bestimmen. Wir setzen an $\mathbf{Z}_K = \mathbf{Z} + \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2 + \mathbf{Z}\omega_3$ mit
$$\omega_1 = \frac{1}{d_1}(\alpha + b_{10}), \quad \omega_2 = \frac{1}{d_2}(\alpha^2 + b_{21}\alpha + b_{20}), \quad \omega_3 = \frac{1}{d_3}(\alpha^3 + b_{32}\alpha^2 + b_{31}\alpha + b_{30})$$
und
$$d_1^2 | d_2, \quad d_1^3 | d_3, \quad d_1 d_2 | d_3, \quad b_{ij} < \frac{d_i}{d_j} \text{ für } i > j, \quad d_1 d_2 d_3 = [\mathbf{Z}_K : \mathbf{Z}[\alpha]] | 2^7 \cdot 3.$$

Wir betrachten ω_1: Aus $d_1^6 = d_1 \cdot d_1^2 \cdot d_1^3 | d_1 d_2 d_3 | 2^7 \cdot 3$ folgt $d_1 | 2$. Im Fall $d_1 = 2$ ist für $b_{10} \in \{0, 1\}$ das Minimalpolynom von ω_1 nicht ganzzahlig, also bleibt nur $d_1 = 1$, $b_{10} = 0$ übrig:

$$\omega_1 = \alpha.$$

Wir betrachten ω_2: Aus $d_2 | d_3$ und $d_2 d_3 | 2^7 \cdot 3$ folgt $d_2^2 | 2^7 \cdot 3$, also gibt es nur die Möglichkeiten $d_2 \in \{1, 2, 4, 8\}$. Durch Ausprobieren aller Möglichkeiten findet man $d_2 = 2$, $b_{21} = 0$, $b_{20} = 1$, d.h.

$$\omega_2 = \frac{1}{2}(\alpha^2 + 1) = 3 + \sqrt{6}.$$

Wir kommen nun zu ω_3: Wir wissen $2 | d_3$ und $2 d_3 | 2^7 \cdot 3$, also $d_3 | 2^6 \cdot 3$ und damit

$$d_3 \in \{2, 4, 8, 16, 32, 64\} \cup \{6, 12, 24, 48, 96, 192\} = \{2, 4, 6, 8, 12, 16, 24, 32, 48, 64, 96, 192\}.$$

Weiter

$$b_{32} < \frac{d_3}{2}, \quad b_{31} < d_3, \quad b_{30} < d_3.$$

Wir berechnen das charakteristische Polynom von ω_3 und untersuchen numerisch, wann die Koeffizienten ganzzahlig sind. Wir finden (mit Maple) als einzige Lösungen

$$(d_3, b_{32}, b_{31}, b_{30}) = (2, 0, 1, 0), (4, 1, 3, 3).$$

Daher müssen wir

$$\omega_3 = \frac{1}{4}(\alpha^3 + \alpha^2 + 3\alpha + 3)$$

wählen und erhalten $[\mathbf{Z}_K : \mathbf{Z}[\alpha]] = 8$, was schließlich für die Diskriminante

$$\operatorname{disc}(K) = \operatorname{disc}(\mathbf{Z}_K) = 2^8 \cdot 3^2$$

ergibt. Gibt es ein Element β mit $\mathbf{Z}_K = \mathbf{Z}[\beta]$? Wir setzen an

$$\beta = u\omega_1 + v\omega_2 + w\omega_3$$

und erhalten für die Diskriminante

$$\operatorname{disc}(\mathbf{Z}[\beta]) = 2304(2u^2+8uw+5w^2)^2(-2u^2+4v^2-12uw+4vw-17w^2)^2(-2u^2+6v^2-14uw+6vw-23w^2)^2.$$

Durch Ausprobieren findet man, dass z.B.

$$\omega_1 - \omega_2 - \omega_3 \quad \text{und} \quad -2 - 3\omega_1 + \omega_3 = \frac{1}{2}(\sqrt{2} + \sqrt{6})$$

Diskriminante 2304 haben. (Die Minimalpolynome sind $x^4 + 20x^3 + 74x^2 + 100x + 46$ bzw. $x^4 - 4x^2 + 1$.) Also gilt:

$$\mathbf{Z}_K = \mathbf{Z}[\frac{1}{2}(\sqrt{2} + \sqrt{6})].$$

KAPITEL 6

Ideale

1. Einführung

Die natürlichen Zahlen $\mathbf{N}$ bzw. die ganzen Zahlen $\mathbf{Z}$ haben einige wichtige Eigenschaften:

- Jede natürliche Zahl läßt sich (eindeutig) als Produkt von Primzahlen darstellen, der Ring $\mathbf{Z}$ ist also faktoriell.
- In $\mathbf{N}$ gibt es den euklidischen Algorithmus, der gerade für die Anwendung von fundamentaler Bedeutung ist. Dies macht $\mathbf{Z}$ zu einem euklidischen Ring.

Leider gelten die entsprechenden Aussagen für Ordnungen in Zahlkörpern im allgemeinen nicht.

Beispiel: In $\mathbf{Z}[\sqrt{-5}]$ hat die Zahl 6 die Faktorisierungen

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

die nicht miteinander verträglich sind. Um das Phänomen zu erklären, kann man mit *idealen* Zahlen ansetzen

$$2 = \alpha_1\alpha_2, \quad 3 = \alpha_3\alpha_4, \quad 1 + \sqrt{-5} = \alpha_1\alpha_3, \quad 1 - \sqrt{-5} = \alpha_2\alpha_4,$$

was die Faktorisierung erklären würde. Allerdings gibt es solche Zahlen in $\mathbf{Z}[\sqrt{-5}]$ nicht. Wir werden sehen, dass sich die Beziehungen klären, wenn man $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ als Ideale in $\mathbf{Z}[\sqrt{-5}]$ deutet.

2. Ideale

Wir sind hauptsächlich an dem Fall interessiert, dass R eine Ordnung eines Zahlkörpers K ist. Allerdings gelten viele Eigenschaften auch allgemeiner für kommutative Ringe.

Ein Ideal $\mathfrak{a}$ eines kommutativen Rings R ist eine Teilmenge $\mathfrak{a} \subseteq R$ mit folgenden Eigenschaften:

- $\mathfrak{a}$ ist eine Untergruppe der additiven Gruppe von R, d.h. $0 \in \mathfrak{a}$ und $x, y \in \mathfrak{a}$ impliziert $x + y \in \mathfrak{a}$, $-x \in \mathfrak{a}$.
- $R\mathfrak{a} \subseteq \mathfrak{a}$, d.h. $r \in R$ und $x \in \mathfrak{a}$ liefert $rx \in \mathfrak{a}$.

Trivialerweise ist $\{0\}$ ein Ideal, das auch einfach mit 0 bezeichnet wird. Sind $\alpha_1, \ldots, \alpha_m \in R$, so ist offensichtlich

$$R\alpha_1 + \cdots + R\alpha_m = \{r_1\alpha_1 + \cdots + r_m\alpha_m : r_1, \ldots, r_n \in R\}$$

ein Ideal, das auch mit $(\alpha_1, \ldots, \alpha_m)$ bezeichnet wird. Ideale, die sich so schreiben lassen, nennt man endlich erzeugt.

LEMMA. *Ist $\mathfrak{a} \neq 0$ ein Ideal einer Ordnung R eines Zahlkörpers K, so ist $\mathfrak{a}$ ein Modul in K, d.h. es gibt eine $\mathbf{Q}$-Basis $\alpha_1, \ldots, \alpha_n$ von K mit*

$$\mathfrak{a} = \mathbf{Z}\alpha_1 + \cdots + \mathbf{Z}\alpha_n.$$

Insbesondere ist der Index $[R : \mathfrak{a}]$ definiert, den man auch als Idealnorm bezeichnet:

$$\mathrm{N}(\mathfrak{a}) = [R : \mathfrak{a}].$$

Beweis: Sei $\omega_1, \ldots, \omega_n$ eine $\mathbf{Z}$-Basis von R und $\alpha \in \mathfrak{a}$, $\alpha \neq 0$. Dann ist

$$R\alpha = \mathbf{Z}\alpha\omega_1 + \cdots + \mathbf{Z}\alpha\omega_n$$

ein Modul und $R\alpha \subseteq \mathfrak{a} \subseteq R$. Da $\mathfrak{a}$ eine abelsche Gruppe ist und zwischen zwei Moduln liegt, ist $\mathfrak{a}$ ebenfalls ein Modul. ■

Ringe, bei denen jedes Ideal endlich erzeugt ist, heißen noetherisch. Das Lemma liefert also insbesondere:

FOLGERUNG. *Ordnungen in Zahlkörpern sind noethersche Ringe.*

Wir wollen unsere Kenntnisse über Moduln in Zahlkörpern noch zu einer genaueren Beschreibung von Idealen benutzen:

LEMMA. *Sei R Ordnung eines Zahlkörpers K und $\omega_1, \ldots, \omega_n$ eine festgewählte $\mathbf{Z}$-Basis von R. Jedem $\alpha \in K$ wird vermöge der rationalen Darstellung $\alpha\omega_i = \sum_j a_{ij}\omega_j$ eine Matrix $A(\alpha) = (a_{ij}) \in M_n(\mathbf{Q})$ zugeordnet. Die von 0 verschiedenen Ideale $\mathfrak{a}$ von R stehen dann in Bijektion zu den Matrizen $C = (c_{ij}) \in M_n(\mathbf{Z})$ in Hermitescher Normalform vom Rang n (d.h. $c_{ij} \in \mathbf{Z}$, $c_{ii} \geq 1$, $c_{ij} = 0$ für $i > j$, $0 \leq c_{ij} < c_{jj}$ für $i < j$) mit der Eigenschaft*

$$CA(\omega_1)C^{-1}, \ldots, CA(\omega_n)C^{-1} \in M_n(\mathbf{Z})$$

vermöge der Beziehung

$$C \quad \mapsto \quad \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} c_{11} & c_{12} & \ldots & c_{1n} \\ & c_{22} & \ldots & c_{2n} \\ & & & \vdots \\ & & & c_{nn} \end{pmatrix} \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} \quad \mapsto \quad \mathfrak{a} = \mathbf{Z}\alpha_1 + \cdots + \mathbf{Z}\alpha_n.$$

(Ist $R = \mathbf{Z}[\alpha]$, so kann man sich auf die Bedingung $CA(\alpha)C^{-1} \in M_n(\mathbf{Z})$ beschränken.)

Beweis:

1. Jedes ω_k liefert vermöge $\omega_k\omega_i = \sum_j m_{kij}\omega_j$ eine Matrix $A(\omega_k) = (m_{kij})_{ij} \in M_n(\mathbf{Z})$. Anders geschrieben:
$$\omega_k \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = A(\omega_k) \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix}.$$
2. Die in R enthaltenen Moduln von K stehen in Bijektion zu den $n \times n$-Matrizen $C = (c_{ij})$ (in Hermitescher Normalform) vermöge:
$$C \quad \mapsto \quad \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} c_{11} & c_{12} & \ldots & c_{1n} \\ & c_{22} & \ldots & c_{2n} \\ & & & \vdots \\ & & & c_{nn} \end{pmatrix} \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} \quad \mapsto \quad \mathbf{Z}\alpha_1 + \cdots + \mathbf{Z}\alpha_n,$$
wobei $c_{ij} \in \mathbf{Z}$, $c_{ii} \geq 1$, $0 \leq c_{ij} < c_{jj}$ für $i < j$, $c_{ij} = 0$ für $i > j$ gilt.
3. Wir berechnen:
$$\omega_k \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \omega_k C \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = C\omega_k \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = CA(\omega_k) \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = CA(\omega_k)C^{-1} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}.$$
Daher gilt
$$\begin{aligned} \mathbf{Z}\alpha_1 + \cdots + \mathbf{Z}\alpha_n \text{ ist Ideal} \quad &\iff \quad \omega_k\alpha_i \in \mathbf{Z}\alpha_1 + \cdots + \mathbf{Z}\alpha_n \text{ für alle } i,k \\ &\iff \quad CA(\omega_1)C^{-1}, \ldots, CA(\omega_n)C^{-1} \in M_n(\mathbf{Z}), \end{aligned}$$
was wir zeigen wollten. Im Fall $R = \mathbf{Z}[\alpha]$ kann man sich natürlich wegen $A(\alpha^k) = A(\alpha)^k$ auf die Bedingung auf $CA(\alpha)C^{-1} \in M_n(\mathbf{Z})$ beschränken. ■

Bemerkungen: (mit den Bezeichnungen des Lemmas)

1. Entsprechen die Ideale $\mathfrak{a}_1$ und $\mathfrak{a}_2$ den Matrizen C_1 und C_2, so rechnet man ähnlich wie eben nach, daß gilt
$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \quad \Longleftrightarrow \quad C_1 C_2^{-1} \in M_n(\mathbf{Z}).$$
2. Hat man $\omega_n = 1$ gewählt, entspricht dem Ideal $\mathfrak{a}$ die Matrix $C = (c_{ij})$, so sieht man sofort, daß
$$\mathfrak{a} \cap \mathbf{Q} = \mathfrak{a} \cap \mathbf{Z} = \mathbf{Z} c_{nn}$$
gilt.

Beispiel: Wir betrachten den Zahlkörper $K = \mathbf{Q}(\alpha)$ mit $f(\alpha) = 0$, wobei $f = x^3 + 7x + 20$ ist. Die Diskriminante ist $\operatorname{disc}(K) = \operatorname{disc}(\mathbf{Z}_K) = -3043 = -17 \cdot 179$. Eine $\mathbf{Z}$-Basis des Ganzheitsrings $\mathbf{Z}_K$ ist
$$\omega_1 = \frac{\alpha^2 + \alpha}{2}, \quad \omega_2 = \alpha, \quad \omega_3 = 1.$$
Mit Hilfe des Lemmas wollen wir wir alle Ideale mit Norm ≤ 15 auflisten.
Es ist
$$A(\omega_1) = \begin{pmatrix} -3 & -7 & -10 \\ 1 & -4 & -10 \\ 1 & 0 & 0 \end{pmatrix}, \quad A(\omega_2) = \begin{pmatrix} 1 & -4 & -10 \\ 2 & -1 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad A(\omega_3) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$
Ein Ideal $\mathfrak{a}$ wird angesetzt als
$$\mathfrak{a} = \mathbf{Z}\alpha_1 + \mathbf{Z}\alpha_2 + \mathbf{Z}\alpha_3 \quad \text{mit} \quad \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} = \begin{pmatrix} c_{11} & c_{12} & c_{13} \\ 0 & c_{22} & c_{23} \\ 0 & 0 & c_{33} \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \\ \omega_3 \end{pmatrix}$$
mit
$$c_{11}, c_{22}, c_{33} \geq 1, \quad c_{12} \leq c_{22}, \quad c_{13}, c_{23} \leq c_{33} - 1.$$
Wir betrachten alle Möglichkeiten mit $[\mathbf{Z}_K : \mathfrak{a}] = c_{11}c_{22}c_{33} \leq 15$ und testen jeweils, ob
$$CA(\omega_1)C^{-1} \in M_n(\mathbf{Z}) \text{ und } CA(\omega_2)C^{-1} \in M_n(\mathbf{Z})$$
erfüllt ist. Wir erhalten folgende Liste:
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \to \mathfrak{a}_1 = \mathbf{Z}_K, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix} \to \mathfrak{a}_2, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 3 \end{pmatrix} \to \mathfrak{a}_3,$$
$$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 4 \end{pmatrix} \to \mathfrak{a}_{4a}, \quad \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix} \to \mathfrak{a}_{4b}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 5 \end{pmatrix} \to \mathfrak{a}_5, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 4 \\ 0 & 0 & 6 \end{pmatrix} \to \mathfrak{a}_6,$$
$$\begin{pmatrix} 1 & 0 & 4 \\ 0 & 1 & 3 \\ 0 & 0 & 7 \end{pmatrix} \to \mathfrak{a}_{7a}, \quad \begin{pmatrix} 1 & 0 & 4 \\ 0 & 1 & 5 \\ 0 & 0 & 7 \end{pmatrix} \to \mathfrak{a}_{7b}, \quad \begin{pmatrix} 1 & 0 & 6 \\ 0 & 1 & 6 \\ 0 & 0 & 7 \end{pmatrix} \to \mathfrak{a}_{7c},$$
$$\begin{pmatrix} 1 & 0 & 6 \\ 0 & 1 & 4 \\ 0 & 0 & 8 \end{pmatrix} \to \mathfrak{a}_{8a}, \quad \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} \to \mathfrak{a}_{8b}, \quad \begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & 9 \end{pmatrix} \to \mathfrak{a}_{9a}, \quad \begin{pmatrix} 1 & 2 & 1 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix} \to \mathfrak{a}_{9b},$$
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 10 \end{pmatrix} \to \mathfrak{a}_{10}, \quad \begin{pmatrix} 1 & 0 & 6 \\ 0 & 1 & 4 \\ 0 & 0 & 12 \end{pmatrix} \to \mathfrak{a}_{12a}, \quad \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 6 \end{pmatrix} \to \mathfrak{a}_{12b},$$
$$\begin{pmatrix} 1 & 0 & 4 \\ 0 & 1 & 10 \\ 0 & 0 & 14 \end{pmatrix} \to \mathfrak{a}_{14a}, \quad \begin{pmatrix} 1 & 0 & 4 \\ 0 & 1 & 12 \\ 0 & 0 & 14 \end{pmatrix} \to \mathfrak{a}_{14b}, \quad \begin{pmatrix} 1 & 0 & 6 \\ 0 & 1 & 6 \\ 0 & 0 & 14 \end{pmatrix} \to \mathfrak{a}_{14c}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 10 \\ 0 & 0 & 15 \end{pmatrix} \to \mathfrak{a}_{15}.$$
Das Ideal $\mathfrak{a}_{14a}$ ist dann also
$$\mathfrak{a}_{14a} = \mathbf{Z}(\omega_1 + 4\omega_3) + \mathbf{Z}(\omega_2 + 10\omega_3) + \mathbf{Z} \cdot 14\omega_3.$$

Beispiel: Wir betrachten $K = \mathbf{Q}(\alpha)$ mit $\alpha^2 = -11$ und die Ordnung $R = \mathbf{Z}[\alpha]$, die nicht die Maximalordnung ist. Als $\mathbf{Z}$-Basis wählen wir $\alpha, 1$. Dann ist die darstellende Matrix

$$A(u\alpha + v) = \begin{pmatrix} v & -11u \\ u & v \end{pmatrix}.$$

Wendet man das Lemma an, so findet man, daß sich Ideale $\mathfrak{a} \neq 0$ eindeutig durch Matrizen

$$C = \begin{pmatrix} a & ab \\ 0 & ac \end{pmatrix} \text{ mit } a, c \in \mathbf{N}, b \in \mathbf{N}_0, b < c, b^2 + 11 \equiv 0 \bmod c$$

vermöge

$$C \quad \mapsto \quad \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} = C \begin{pmatrix} \alpha \\ 1 \end{pmatrix} \quad \mapsto \quad \mathfrak{a} = \mathbf{Z}\alpha_1 + \mathbf{Z}\alpha_2$$

beschreiben lassen. Wir listen die Ideale mit Norm $2 \leq N\mathfrak{a} \leq 10$ auf:

$$\begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \to \mathfrak{a}_2, \quad \begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix} \to \mathfrak{a}_{3a}, \quad \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} \to \mathfrak{a}_{3b},$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 4 \end{pmatrix} \to \mathfrak{a}_{4a}, \quad \begin{pmatrix} 1 & 3 \\ 0 & 4 \end{pmatrix} \to \mathfrak{a}_{4b}, \quad \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \to \mathfrak{a}_{4c},$$

$$\begin{pmatrix} 1 & 2 \\ 0 & 5 \end{pmatrix} \to \mathfrak{a}_{5a}, \quad \begin{pmatrix} 1 & 3 \\ 0 & 5 \end{pmatrix} \to \mathfrak{a}_{5b}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 6 \end{pmatrix} \to \mathfrak{a}_{6a}, \quad \begin{pmatrix} 1 & 5 \\ 0 & 6 \end{pmatrix} \to \mathfrak{a}_{6b},$$

$$\begin{pmatrix} 2 & 2 \\ 0 & 4 \end{pmatrix} \to \mathfrak{a}_8, \quad \begin{pmatrix} 1 & 4 \\ 0 & 9 \end{pmatrix} \to \mathfrak{a}_{9a}, \quad \begin{pmatrix} 1 & 5 \\ 0 & 9 \end{pmatrix} \to \mathfrak{a}_{9b}, \quad \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} \to \mathfrak{a}_{9c},$$

$$\begin{pmatrix} 1 & 3 \\ 0 & 10 \end{pmatrix} \to \mathfrak{a}_{10a}, \quad \begin{pmatrix} 1 & 7 \\ 0 & 10 \end{pmatrix} \to \mathfrak{a}_{10b}.$$

Wir bemerken, daß gilt

$$\mathfrak{a}_8 \subseteq \mathfrak{a}_{4a,b,c} \subseteq \mathfrak{a}_2.$$

LEMMA. *Sei $\mathfrak{a} \neq 0$ Ideal einer Ordnung R (in einem Zahlkörper K vom Grad n). Dann gibt es ein $\ell(\mathfrak{a}) \in \mathbf{N}$ mit*

$$\mathfrak{a} \cap \mathbf{Z} = \mathfrak{a} \cap \mathbf{Q} = \mathbf{Z}\ell(\mathfrak{a})$$

und es gilt

$$\ell(\mathfrak{a}) | \mathrm{N}(\mathfrak{a}) | \ell(\mathfrak{a})^n.$$

Beweis: $\mathfrak{a} \cap \mathbf{Q}$ ist ein Modul in $\mathbf{Q}$, also gibt es eine rationale Zahl $\ell(\mathfrak{a}) > 0$ mit $\mathfrak{a} \cap \mathbf{Q} = \mathbf{Z}\ell(\mathfrak{a})$. Wegen $\mathfrak{a} \subseteq R$ folgt $\mathbf{Z}\ell(\mathfrak{a}) = \mathfrak{a} \cap \mathbf{Q} \subseteq R \cap \mathbf{Q} = \mathbf{Z}$ und damit $\mathfrak{a} \cap \mathbf{Q} = \mathfrak{a} \cap \mathbf{Z} = \mathbf{Z}\ell(\mathfrak{a})$ und $\ell(\mathfrak{a}) \in \mathbf{N}$. Aus der Indexformel $[R : \mathfrak{a}] \cdot R \subseteq \mathfrak{a}$ folgt wegen $1 \in R$ die Beziehung $\mathrm{N}(\mathfrak{a}) = [R : \mathfrak{a}] \cdot 1 \in \mathfrak{a}$, also $\mathrm{N}(\mathfrak{a}) \in \mathbf{Z}\ell(\mathfrak{a})$ und damit $\ell(\mathfrak{a}) | \mathrm{N}(\mathfrak{a})$. Aus $\ell(\mathfrak{a}) \in \mathfrak{a}$ folgt $R\ell(\mathfrak{a}) \subseteq \mathfrak{a} \subseteq R$. Ist $\omega_1, \ldots, \omega_n$ eine $\mathbf{Z}$-Basis von R, so ist $\ell(\mathfrak{a})\omega_1, \ldots, \ell(\mathfrak{a})\omega_n$ eine $\mathbf{Z}$-Basis von $R\ell(\mathfrak{a})$, was sofort $[R : R\ell(\mathfrak{a})] = \ell(\mathfrak{a})^n$ liefert. Es folgt

$$\ell(\mathfrak{a})^n = [R : R\ell(\mathfrak{a})] = [R : \mathfrak{a}] \cdot [\mathfrak{a} : R\ell(\mathfrak{a})] = \mathrm{N}(\mathfrak{a}) \cdot [\mathfrak{a} : R\ell(\mathfrak{a})]$$

und daraus $\mathrm{N}(\mathfrak{a}) | \ell(\mathfrak{a})^n$, was alles beweist. ■

Operationen mit Idealen: Da Ideale von Ordnungen Moduln sind, kann man sie wie Moduln addieren und multiplizieren: Sind

$$\mathfrak{a} = \mathbf{Z}\alpha_1 + \cdots + \mathbf{Z}\alpha_r, \quad \mathfrak{b} = \mathbf{Z}\beta_1 + \cdots + \mathbf{Z}\beta_s$$

Ideale in R, so ist die Summe

$$\mathfrak{a} + \mathfrak{b} = \mathbf{Z}\alpha_1 + \cdots + \mathbf{Z}\alpha_r + \mathbf{Z}\beta_1 + \cdots + \mathbf{Z}\beta_s$$

und das Produkt

$$\mathfrak{a}\mathfrak{b} = \mathbf{Z}\alpha_1\beta_1 + \cdots + \mathbf{Z}\alpha_r\beta_1 + \cdots + \mathbf{Z}\alpha_1\beta_s + \cdots + \mathbf{Z}\alpha_r\beta_s.$$

Mit unserem Hermiteschen Normalisierungsverfahren für Moduln erhält man dann daraus leicht wieder eine Darstellung als Modul mit einer $\mathbf{Z}$-Basis als Erzeugendensystem.

Beispiel: Für $K = \mathbf{Q}(\alpha)$ mit $\alpha^3 + 7\alpha + 20 = 0$ betrachten wir die Ideale

$$\mathfrak{a}_2 = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2 + \mathbf{Z} \cdot 2\omega_3, \quad \mathfrak{a}_{4a} = \mathbf{Z}(\omega_1 + 2\omega_3) + \mathbf{Z}\omega_2 + \mathbf{Z} \cdot 4\omega_3, \quad \mathfrak{a}_{4b} = \mathbf{Z} \cdot 2\omega_1 + \mathbf{Z}(\omega_2 + \omega_3) + \mathbf{Z} \cdot 2\omega_3.$$

Mit dem Hermiteschen Normalisierungsverfahren erhalten wir

$$\mathfrak{a}_2 + \mathfrak{a}_{4a} = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2 + \mathbf{Z}\cdot 2\omega_3 = \mathfrak{a}_2 \quad \text{und} \quad \mathfrak{a}_2 + \mathfrak{a}_{4b} = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2 + \mathbf{Z}\omega_3 = R$$

und

$$\begin{aligned}
\mathfrak{a}_2\mathfrak{a}_{4b} &= \mathbf{Z}\cdot 2\omega_1^2 + \mathbf{Z}\omega_1(\omega_2+\omega_3) + \mathbf{Z}\cdot 2\omega_1\omega_3 + \\
&\quad + \mathbf{Z}\cdot 2\omega_1\omega_2 + \mathbf{Z}\omega_2(\omega_2+\omega_3) + \mathbf{Z}\cdot 4\omega_2\omega_3 + \\
&\quad + \mathbf{Z}\cdot 4\omega_1\omega_3 + \mathbf{Z}\cdot 2\omega_3(\omega_2+\omega_3) + \mathbf{Z}\cdot 4\omega_3^2 = \\
&= \mathbf{Z}(-6\omega_1 - 14\omega_2 - 20\omega_3) + \mathbf{Z}(2\omega_1 - 4\omega_2 - 10\omega_3) + \mathbf{Z}(2\omega_1) + \\
&\quad + \mathbf{Z}(2\omega_1 - 8\omega_2 - 20\omega_3) + \mathbf{Z}(2\omega_1) + \mathbf{Z}(2\omega_2) + \\
&\quad + \mathbf{Z}(4\omega_1) + \mathbf{Z}(2\omega_2 + 2\omega_3) + \mathbf{Z}(4\omega_3) = \\
&= \mathbf{Z}\cdot 2\omega_1 + \mathbf{Z}\cdot 2\omega_2 + \mathbf{Z}\cdot 2\omega_3 = R\cdot 2 = (2) = \mathfrak{a}_{8b}
\end{aligned}$$

und

$$\begin{aligned}
\mathfrak{a}_2\mathfrak{a}_2 &= \mathbf{Z}\omega_1^2 + \mathbf{Z}\omega_1\omega_2 + \mathbf{Z}\omega_1\cdot 2\omega_3 + \mathbf{Z}\omega_2^2 + \mathbf{Z}\omega_2\cdot 2\omega_3 + \mathbf{Z}\cdot 4\omega_3^2 = \\
&= \mathbf{Z}(-3\omega_1 - 7\omega_2 - 10\omega_3) + \mathbf{Z}(\omega_1 - 4\omega_2 - 10\omega_3) + \mathbf{Z}(2\omega_1) + \mathbf{Z}(2\omega_1 - \omega_2) + \mathbf{Z}(2\omega_2) + \mathbf{Z}(4\omega_3) = \\
&= \mathbf{Z}(\omega_1 + 2\omega_3) + \mathbf{Z}\omega_2 + \mathbf{Z}\cdot 4\omega_3 = \mathfrak{a}_{4a}.
\end{aligned}$$

Beispiel: $K = \mathbf{Q}(\alpha)$ mit $\alpha^2 = -11$. Wir betrachten wieder die Ordnung $R = \mathbf{Z}[\alpha]$. Für das Ideal $\mathfrak{a}_2 = \mathbf{Z}(\alpha+1) + \mathbf{Z}\cdot 2$ gilt

$$\mathfrak{a}_2^2 = \mathbf{Z}(\alpha+1)^2 + \mathbf{Z}\cdot 2(\alpha+1) + \mathbf{Z}\cdot 4 = \mathbf{Z}(2\alpha - 10) + \mathbf{Z}(2\alpha + a) + \mathbf{Z}\cdot 4 = \mathbf{Z}(2\alpha+2) + \mathbf{Z}\cdot 4 = \mathfrak{a}_8.$$

Faktorringe: Sei $\mathfrak{a}$ ein Ideal eines kommutativen Rings R. Dann definiert man eine Äquivalenzrelation auf R durch

$$x \equiv y \bmod \mathfrak{a} \quad \Longleftrightarrow \quad x - y \in \mathfrak{a}.$$

Die Äquivalenzrelation ist mit Addition und Multiplikation verträglich, sodass die Menge der Äquivalenzklassen $R/\mathfrak{a}$ in natürlicher Weise eine Ringstruktur hat und $R \to R/\mathfrak{a}$ ein Ringhomormorphismus ist.

Gilt für Ideale $\mathfrak{a}$, $\mathfrak{b}$ eines Rings R die Beziehung

$$\mathfrak{a} + \mathfrak{b} = (1) = R,$$

so nennt man sie teilerfremd.
Wir erinnern in diesem Zusammenhang an den chinesischen Restsatz für Ringe:

Satz. *Sind $\mathfrak{a}$ und $\mathfrak{b}$ teilerfremde Ideale eines kommutativen Rings R, so gilt:*

1. $\mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}$.
2. *Sind $a, b \in R$ gegeben, so gibt es ein $x \in R$ mit*

   $$x \equiv a \bmod \mathfrak{a} \quad \textit{und} \quad x \equiv b \bmod \mathfrak{b}.$$

   Ist x' eine weitere Lösung der Kongruenzen, so gilt $x \equiv x' \bmod \mathfrak{a}\mathfrak{b}$.
3. *Die natürlichen Ringhomomorphismen $R \to R/\mathfrak{a}$ und $R \to R/\mathfrak{b}$ induzieren einen Ringisomorphismus*

   $$R/\mathfrak{a}\mathfrak{b} \to R/\mathfrak{a} \oplus R/\mathfrak{b}.$$

Beweis: Wegen $\mathfrak{a} + \mathfrak{b} = R$ gibt es $a_1 \in \mathfrak{a}$ und $b_1 \in \mathfrak{b}$ mit $a_1 + b_1 = 1$. Dann ist

$$a_1 \equiv \begin{cases} 0 & \bmod \mathfrak{a}, \\ 1 & \bmod \mathfrak{b}, \end{cases}, \quad b_1 \equiv \begin{cases} 1 & \bmod \mathfrak{a}, \\ 0 & \bmod \mathfrak{b}. \end{cases}$$

1. Aus $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a}$ und $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{b}$ folgt $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$. Sei umgekehrt $x \in \mathfrak{a} \cap \mathfrak{b}$. Dann sind $xa_1, xb_1 \in \mathfrak{a}\mathfrak{b}$ und damit $x = xa_1 + xb_1 \in \mathfrak{a}\mathfrak{b}$. Dies zeigt $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a}\mathfrak{b}$ und damit die Behauptung.

2. Für $x = ab_1 + ba_1$ gilt
$$x \equiv \begin{cases} ab_1 \equiv a \bmod \mathfrak{a}, \\ ba_1 \equiv b \bmod \mathfrak{b}. \end{cases}$$
Ist x' mit $x' \equiv a \bmod \mathfrak{a}$, $x' \equiv b \bmod \mathfrak{b}$ gegeben, so folgt $x - x' \in \mathfrak{a}$, $x - x' \in \mathfrak{b}$, also $x - x' \in \mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$, also $x \equiv x' \bmod \mathfrak{ab}$, wie behauptet.
3. Dies ist nur eine ringtheoretische Formulierung der 2. Aussage. ■

Bemerkung: Der chinesische Restsatz läßt sich leicht auf mehrere Ideale ausdehnen: Sind $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ paarweise teilerfremde Ideale, so gilt
$$\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_r = \mathfrak{a}_1 \ldots \mathfrak{a}_r \quad \text{und} \quad R/\mathfrak{a}_1 \ldots \mathfrak{a}_r \simeq R/\mathfrak{a}_1 \oplus \cdots \oplus R/\mathfrak{a}_r.$$

3. Hauptideale

Ein Ideal $\mathfrak{a}$ eines Rings R ist ein Hauptideal, wenn es sich in der Form $\mathfrak{a} = (\alpha) = R\alpha$ mit einem Element $\alpha \in R$ schreiben läßt. Wir erinnern kurz an folgende wichtige Eigenschaft der Erzeuger von Hauptidealen:

LEMMA. *Sei R Ordnung eines Zahlkörpers und $\alpha, \beta \in R \setminus \{0\}$. Dann gilt*
$$R\alpha = R\beta \quad \Longleftrightarrow \quad \beta = \varepsilon\alpha \text{ für ein } \varepsilon \in R^*,$$
d.h. Erzeuger von Hauptidealen unterscheiden sich nur um eine Einheit.

Beweis: $\Longrightarrow$ Aus $\alpha \in R\beta$ folgt $\alpha = u\beta$ für ein $u \in R$. Analog gibt es ein $v \in R$ mit $\beta = v\alpha$. Daher ist $\beta = v\alpha = vu\beta$, was wegen $\beta \neq 0$ sofort $uv = 1$ liefert, d.h. $u, v \in R^*$.
$\Longleftarrow$ Zunächst ist $\beta = \varepsilon\alpha \in R\alpha$, also $R\beta \subseteq R\alpha$. Wegen $\varepsilon^{-1} \in R$ gilt $\alpha = \varepsilon^{-1}\beta \in R\beta$, also $R\alpha \subseteq R\beta$, was schließlich $R\alpha = R\beta$ beweist. ■

SATZ. *Ist R eine Ordnung, so gilt für $\alpha \in R$:*
$$|N(\alpha)| = [R : R\alpha] = N((\alpha)),$$
d.h. die Norm von α als Element ist bis aufs Vorzeichen die Norm des von α erzeugten Hauptideals.

Beweis: Sei $\omega_1, \ldots, \omega_n$ eine $\mathbf{Z}$-Basis von R. Die Multiplikation mit α liefert dann vermöge
$$\alpha\omega_i = \sum_j a_{ij}\omega_j$$
eine Matrix $A(\alpha) = (a_{ij})$, deren Determinante die Norm liefert:
$$N(\alpha) = \det A(\alpha).$$
Nun ist andererseits $\alpha\omega_1, \ldots, \alpha\omega_n$ eine $\mathbf{Z}$-Basis des Hauptideals $R\alpha$. Die Matrix $A(\alpha)$ transformiert die Basis $\omega_1, \ldots, \omega_n$ in die Basis $\alpha\omega_1, \ldots, \alpha\omega_n$, also folgt nach Definition
$$[R : R\alpha] = |\det A(\alpha)|,$$
was die Behauptung ergibt. ■

Ist jedes Ideal eines Integritätsrings R Hauptideal, so nennt man R einen Hauptidealring. In der Algebraischen Zahlentheorie stellen sich in diesem Zusammenhang zwei wichtige (nichttriviale) Fragen:

1. Kann man einem Ideal $\mathfrak{a}$ einer Ordnung R ansehen, ob es ein Hauptideal ist?
2. Wie kann man sehen, ob eine Ordnung R ein Hauptidealring ist?

Beispiel: Wir betrachten wieder den Zahlkörper $K = \mathbf{Q}(\alpha)$ mit $\alpha^3 + 7\alpha + 20 = 0$. Als Ganzheitsbasis wählen wir
$$\omega_1 = \frac{\alpha^2 + \alpha}{2}, \quad \omega_2 = \alpha, \quad \omega_3 = 1.$$
Bezüglich dieser Basis wird dann
$$A(u\omega_1 + v\omega_2 + w\omega_3) = \begin{pmatrix} -3u + v + w & -7u - 4v & -10u - 10v \\ u + 2v & -4u - v + w & -10u \\ u & v & w \end{pmatrix}.$$

Das Hauptideal $R(u\omega_1 + v\omega_2 + w\omega_3)$ wird dann durch die Matrix $A(u\omega_1 + v\omega_2 + w\omega_3)$ beschrieben, durch Normalisierung erhält man die zugehörige Matrix in Normalform. Wir haben nun numerisch alle $u\omega_1 + v\omega_2 + w\omega_3$ mit $|u|, |v|, |w| \leq 100$ getestet. Auf diese Weise sieht man, dass alle Ideale mit Norm ≤ 15 Hauptideale sind:

$$\begin{aligned}
\mathfrak{a}_2 &= (\omega_2 + 2\omega_3) \\
\mathfrak{a}_3 &= (\omega_1 + \omega_2 + \omega_3) \\
\mathfrak{a}_{4a} &= (2\omega_1 + 3\omega_2 + 4\omega_3) \\
\mathfrak{a}_{4b} &= (2\omega_1 - 3\omega_2 + 11\omega_3) = (40\omega_1 + 67\omega_2 + 93\omega_3) \\
\mathfrak{a}_5 &= (21\omega_1 + 12\omega_2 + 5\omega_3) = (18\omega_1 - 26\omega_2 + 95\omega_3) \\
\mathfrak{a}_6 &= (5\omega_1 - 2\omega_2 - 8\omega_3) \\
\mathfrak{a}_{7a} &= (\omega_1 + 2\omega_2 + 3\omega_3) \\
\mathfrak{a}_{7b} &= (9\omega_1 + 13\omega_2 + 17\omega_3) \\
\mathfrak{a}_{7c} &= (\omega_1 - \omega_3) \\
\mathfrak{a}_{8a} &= (12\omega_1 - \omega_2 - 12\omega_3) \\
\mathfrak{a}_{8b} &= (2\omega_3) \\
\mathfrak{a}_{9a} &= (3\omega_1 - 14\omega_2 - 29\omega_3) \\
\mathfrak{a}_{9b} &= (7\omega_1 - 10\omega_2 + 37\omega_3) \\
\mathfrak{a}_{10} &= (2\omega_1 - 3\omega_2 + 10\omega_3) \\
\mathfrak{a}_{12a} &= (11\omega_1 - 30\omega_2 - 66\omega_3) \\
\mathfrak{a}_{12b} &= (\omega_2 + \omega_3) \\
\mathfrak{a}_{14a} &= (7\omega_1 + \omega_2 - 4\omega_3) \\
\mathfrak{a}_{14b} &= (9\omega_1 - 13\omega_2 + 48\omega_3) = (53\omega_1 - 6\omega_2 - 56\omega_3) \\
\mathfrak{a}_{14c} &= (3\omega_1 - 5\omega_2 - 12\omega_3) \\
\mathfrak{a}_{15} &= (\omega_1 - \omega_2 + 5\omega_3)
\end{aligned}$$

Die Hauptideale mit zwei Erzeugern liefern dann natürlich Einheiten von R:

$$\alpha_1 = 2\omega_1 - 3\omega_2 + 11\omega_3, \quad \beta_1 = 40\omega_1 + 67\omega_2 + 93\omega_3$$

liefert

$$\frac{\beta_1}{\alpha_1} = 127\omega_1 - 107\omega_3, \quad \frac{\alpha_1}{\beta_1} = -78105\omega_1 + 112903\omega_2 - 413023\omega_3.$$

(Die andern beiden Relationen liefern bis aufs Vorzeichen die gleiche Einheit.) Kann man mit diesen Ergebnissen schon vermuten, dass $\mathbf{Z}_K$ ein Hauptidealring ist?

Beispiel: $R = \mathbf{Z}[\alpha]$ mit $\alpha^2 = -11$. Es ist $N(u\alpha + v) = 11u^2 + v^2$. Die einzigen Hauptideale mit Norm ≤ 10 sind daher (1), (2) und (3). Es gibt also Ideale mit Norm ≤ 10, die keine Hauptideale sind, z.B. $\mathfrak{a}_2 = \mathbf{Z}(\alpha + 1) + \mathbf{Z} \cdot 2$. Insbesondere ist R kein Hauptidealring.

4. Maximale Ideale

Ein Ideal $\mathfrak{m} \subseteq R$ heißt maximal, wenn es ein maximales Element in der bezüglich Inklusion geordneten Menge

$$\{\mathfrak{a} : \mathfrak{a} \text{ ist Ideal in } R \text{ und } \mathfrak{a} \neq R\}$$

ist, d.h. wenn die folgenden zwei Bedingungen erfüllt sind:

1. $\mathfrak{m} \neq R$.
2. Ist $\mathfrak{a}$ ein Ideal mit $\mathfrak{m} \subseteq \mathfrak{a} \subseteq R$, so folgt $\mathfrak{a} = \mathfrak{m}$ oder $\mathfrak{a} = R$.

Äquivalent dazu ist die Forderung, dass der Faktorring $R/\mathfrak{m}$ ein Körper sein soll.

Der folgende Satz wird in der Algebra mit Hilfe des Zornschen Lemmas bewiesen:

SATZ. *Jedes Ideal $\mathfrak{a} \neq R$ eines kommutativen Rings R ist in einem maximalen Ideal $\mathfrak{m}$ enthalten.*

Beweis: Wir beweisen den Satz für Ordnungen R eines Zahlkörpers: Nach unseren Überlegungen ist die Menge

$$\{\mathfrak{b} : \mathfrak{b} \text{ Ideal in R}, \mathfrak{a} \subseteq \mathfrak{b}, \mathfrak{b} \neq R\}$$

endlich, also enthält sie sicher mindestens ein maximales Element. ■

Bemerkung: Die Ordnung R habe eine festgewählte $\mathbf{Z}$-Basis $\omega_1, \ldots, \omega_n$. Das Ideal $\mathfrak{a}$ habe eine $\mathbf{Z}$-Basis $\alpha_1, \ldots, \alpha_n$, das Ideal $\mathfrak{b}$ eine $\mathbf{Z}$-Basis $\beta_1, \ldots, \beta_n$. Dann gibt es Matrizen $A, B \in M_n(\mathbf{Z})$ mit

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = A \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = B \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix},$$

was dann

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = AB^{-1} \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}$$

ergibt. Daher gilt:

$$\mathfrak{a} \subseteq \mathfrak{b} \quad \Longleftrightarrow \quad AB^{-1} \in M_n(\mathbf{Z}).$$

Eine notwendige Bedingung für $\mathfrak{a} \subseteq \mathfrak{b}$ ist natürlich außerdem $[R : \mathfrak{b}] | [R : \mathfrak{a}]$.

Bemerkung: Ist $\mathfrak{a}$ Ideal einer Ordnung R, so daß $N\mathfrak{a}$ eine Primzahl ist, so ist $\mathfrak{a}$ ein maximales Ideal, denn $\mathfrak{a} \subseteq \mathfrak{b} \subseteq R$ impliziert

$$N\mathfrak{a} = [R : \mathfrak{a}] = [R : \mathfrak{b}] \cdot [\mathfrak{b} : \mathfrak{a}]$$

und damit $\mathfrak{b} = R$ oder $\mathfrak{b} = \mathfrak{a}$.

Beispiel: Wir betrachten die Ordnung $R = \mathbf{Z}[\alpha]$ mit $\alpha^3 = 2$ und wählen als $\mathbf{Z}$-Basis $\alpha^2, \alpha, 1$. Es gibt zwei Ideale $\mathfrak{a}_1$ und $\mathfrak{a}_2$ mit Index 25, die den Matrizen

$$A_1 = \begin{pmatrix} 1 & 0 & 16 \\ 0 & 1 & 22 \\ 0 & 0 & 25 \end{pmatrix} \quad \text{und} \quad A_2 = \begin{pmatrix} 1 & 3 & 4 \\ 0 & 5 & 0 \\ 0 & 0 & 5 \end{pmatrix}$$

entsprechen. Es gibt nur ein Ideal $\mathfrak{m}$ mit Index 5, das der Matrix

$$M = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 5 \end{pmatrix}$$

entspricht. Nun rechnet man nach: $A_1 M^{-1} \in M_3(\mathbf{Z})$, $A_2 M^{-1} \notin M_3(\mathbf{Z})$, d.h. $\mathfrak{a}_1 \subseteq \mathfrak{m}$ und $\mathfrak{a}_2 \not\subseteq \mathfrak{m}$. Also ist $\mathfrak{a}_2$ selbst schon ein maximales Ideal.

5. Primideale

Ein Ideal $\mathfrak{p}$ eines kommutativen Rings R nennt man Primideal, wenn folgende zwei Bedingungen erfüllt sind:

1. $\mathfrak{p} \neq R$.
2. Gilt $ab \in \mathfrak{p}$, so folgt $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$, wo $a, b \in R$ sind.

Äquivalent damit ist die Bedingung, dass der Faktorring $R/\mathfrak{p}$ ein Integritätsring ist.

SATZ. *Jedes maximale Ideal $\mathfrak{m}$ ist ein Primideal.*

Beweis: Dies folgt sofort aus der Tatsache, daß für ein maximales Ideal $\mathfrak{m}$ der Faktorring $R/\mathfrak{m}$ ein Körper und damit auch ein Integritätsring ist. ■

Die Definitionseigenschaft von Primidealen kann man auch auf Idealebene hochheben:

LEMMA. *Ist $\mathfrak{p}$ ein Primideal und gilt für Ideale $\mathfrak{a}_i$ die Beziehung $\mathfrak{a}_1 \mathfrak{a}_2 \ldots \mathfrak{a}_r \subseteq \mathfrak{p}$, so gibt es einen Index i mit $\mathfrak{a}_i \subseteq \mathfrak{p}$.*

Beweis: Wir können uns auf den Fall $r = 2$ beschränken, der Rest folgt durch Induktion. Angenommen, es würde gelten $\mathfrak{a}_1 \not\subseteq \mathfrak{p}$, $\mathfrak{a}_2 \not\subseteq \mathfrak{p}$. Dann gäbe es $a_1 \in \mathfrak{a}_1$, $a_1 \notin \mathfrak{p}$, $a_2 \in \mathfrak{a}_2$, $a_2 \notin \mathfrak{p}$. Die Konsequenz wäre

$$a_1 a_2 \in \mathfrak{a}_1 \mathfrak{a}_2 \subseteq \mathfrak{p},$$

ein Widerspruch zur Primidealeigenschaft von $\mathfrak{p}$. ■

In jedem Integritätsring ist 0 ein Primideal, insbesondere also in den Ordnungen von Zahlkörpern.

Der folgende Satz gilt im Allgemeinfall nicht:

SATZ. *Jedes Primideal $\mathfrak{p} \neq 0$ einer Ordnung eines Zahlkörpers ist ein maximales Ideal.*

Beweis: Wir zeigen, dass $R/\mathfrak{p}$ ein Körper ist, dadurch, dass wir zu $a \in R/\mathfrak{p}$, $a \neq 0$ ein Inverses konstruieren. Wir betrachten die Abbildung

$$f : R/\mathfrak{p} \to R/\mathfrak{p}, \quad x \mapsto ax.$$

Da $R/\mathfrak{p}$ Integritätsring ist, ist f injektiv. Da $R/\mathfrak{p}$ endlich ist (mit Mächtigkeit $\#R/\mathfrak{p} = N\mathfrak{p} = [R : \mathfrak{p}]$), ist damit f auch surjektiv, d.h. es gibt $b \in R/\mathfrak{p}$ mit $ab = 1$, was wir zeigen wollten. ■

FOLGERUNG. *Sei R eine Ordnung und $\mathfrak{p}, \mathfrak{p}_1, \ldots, \mathfrak{p}_r$ von 0 verschiedene Primideale mit*

$$\mathfrak{p}_1 \ldots \mathfrak{p}_r \subseteq \mathfrak{p}.$$

Dann gibt es einen Index i mit $\mathfrak{p} = \mathfrak{p}_i$.

Beweis: Es gibt zunächst einen Index i mit $\mathfrak{p}_i \subseteq \mathfrak{p}$. Da aber alle Primideale $\neq 0$ maximal sind, folgt bereits $\mathfrak{p}_i = \mathfrak{p}$. ■

Bemerkung: Die von 0 verschiedenen Primideale in $\mathbf{Z}$ sind genau die Ideale $\mathbf{Z}p = (p)$, wo p eine Primzahl ist. Primideale verallgemeinern also die Primzahlen. Sie spielen für die Arithmetik in Ordnungen von Zahlkörpern eine ähnlich wichtige Rolle wie die Primzahlen in $\mathbf{Z}$. Daher wollen wir uns zunächst einen gewissen Überblick über die Primideale in Ordnungen verschaffen.

Der folgende Satz gibt einige wesentliche Eigenschaften von Primidealen in Ordnungen an.

SATZ. *Sei R Ordnung eines Zahlkörpers K vom Grad n und $\mathfrak{p} \subseteq R$ ein Primideal $\neq 0$. Dann gibt es eine Primzahl $p \in \mathbf{N}$ mit folgenden Eigenschaften:*

1. *$p \in \mathfrak{p}$, also $(p) \subseteq \mathfrak{p}$.*
2. *$\mathfrak{p} \cap \mathbf{Z} = \mathfrak{p} \cap \mathbf{Q} = \mathbf{Z}p$.*
3. *$\mathrm{N}\mathfrak{p} = p^f$ mit $1 \leq f \leq n$.*

Beweis:

1. Sei $\mathrm{N}\mathfrak{p} = p_1 p_2 \ldots p_r$ die Primfaktorzerlegung der Norm von $\mathfrak{p}$ mit (nicht notwendig verschiedenen) Primzahlen p_i. Wegen $\mathrm{N}\mathfrak{p} = [R : \mathfrak{p}] = \#R/\mathfrak{p}$ gilt $\mathrm{N}\mathfrak{p} \cdot R \subseteq \mathfrak{p}$ und damit $p_1 \ldots p_r = \mathrm{N}\mathfrak{p} \in \mathfrak{p}$. Aus der Primidealeigenschaft folgt, dass es einen Index i gibt mit $p_i \in \mathfrak{p}$. Wir setzen $p = p_i$.
2. Da $\mathfrak{p}$ nur ganze algebraische Zahlen enthält, gilt $\mathfrak{p} \cap \mathbf{Q} = \mathfrak{p} \cap \mathbf{Z}$. Nun ist $\mathfrak{p} \cap \mathbf{Z}$ ein Ideal in $\mathbf{Z}$, also von der Form $\mathfrak{p} \cap \mathbf{Z} = \mathbf{Z}a$ mit einer natürlichen Zahl a. Wegen $p \in \mathfrak{p} \cap \mathbf{Z} = \mathbf{Z}a$ gilt $a = 1$ oder $a = p$. Der Fall $a = 1$ kann aber wegen $1 \notin \mathfrak{p}$ nicht eintreten. Also bleibt $a = p$, wie behauptet.
3. Aus $Rp = (p) \subseteq \mathfrak{p}$ ergibt sich

   $$p^n = [R : Rp] = [R : \mathfrak{p}] \cdot [\mathfrak{p} : Rp],$$

   also gibt es ein f mit $N\mathfrak{p} = [R : \mathfrak{p}] = p^f$ und $1 \leq f \leq n$. ■

Bemerkung: Der Satz verschafft eine erste Übersicht über die Primideale einer Ordnung R:

$$\{\text{Primideal } \mathfrak{p} \subseteq R\} = \{0\} \cup \bigcup_{p \text{ Primzahl}} \{\text{Primideal } \mathfrak{p} \subseteq R \text{ mit } p \in \mathfrak{p}\}.$$

Aus $p \in \mathfrak{p}$ folgt $Rp \subseteq \mathfrak{p} \subseteq R$. Da es zwischen Rp und R nur endlich viele Moduln gibt, gibt es auch nur endlich viele Primideale $\mathfrak{p}$, die p enthalten. Da das Ideal Rp in (mindestens) einem maximalen Ideal enthalten ist, gibt es auch tatsächlich Primideale, die p enthalten.

Beispiel: Wir betrachten den Zahlkörper $K = \mathbf{Q}(\alpha)$ mit $\alpha^3+\alpha^2-2\alpha+8 = 0$. Wir wollen alle Primideale in $\mathbf{Z}_K$ bestimmen, die 2 enthalten.
Eine $\mathbf{Z}$-Basis von $R = \mathbf{Z}_K$ ist

$$\omega_1 = \frac{\alpha^2+\alpha}{2}, \quad \omega_2 = \alpha, \quad \omega_3 = 1.$$

Die rationale Darstellung von ω_1 und ω_2 wird dann durch die Matrizen

$$A(\omega_1) = \begin{pmatrix} 1 & -2 & -2 \\ 0 & 1 & -4 \\ 1 & 0 & 0 \end{pmatrix} \quad \text{und} \quad A(\omega_2) = \begin{pmatrix} 0 & 1 & -4 \\ 2 & -1 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

beschrieben. Für ein Primideal $\mathfrak{p}$ mit $2 \in \mathfrak{p}$ können wir die zugehörige Matrix in Hermitescher Normalform dann in der Form

$$C = \begin{pmatrix} c_{11} & c_{12} & c_{13} \\ 0 & c_{22} & c_{23} \\ 0 & 0 & 2 \end{pmatrix}$$

ansetzen mit $N\mathfrak{p} = 2^f = 2c_{11}c_{22}$, $1 \le f \le 3$, $0 \le c_{12} \le c_{22}-1$, $0 \le c_{13}, c_{23} \le 1$. (Es ist $c_{33} = 2$ wegen $\mathbf{Z}2 = \mathbf{Z} \cap \mathfrak{p} = \mathbf{Z}c_{33}$.)
Wir bestimmen zunächst alle Ideale $\mathfrak{p}$ mit Norm 2. Dann muß gelten $c_{11} = c_{22} = 1$, $c_{12} = 0$. Es bleiben wegen $0 \le c_{13}, c_{23} \le 1$ also nur noch vier Möglichkeiten. Testet man in allen Fällen nun die Idealbedingung $CA(\omega_1)C^{-1}, CA(\omega_2)C^{-1} \in M_3(\mathbf{Z})$, so findet man, daß genau drei Matrizen übrigbleiben:

$$P_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}, \quad P_2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}, \quad P_3 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix},$$

so daß die zugehörigen Primideale also

$$\mathfrak{p}_1 = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2 + \mathbf{Z}2, \quad \mathfrak{p}_2 = \mathbf{Z}(\omega_1+1) + \mathbf{Z}\omega_2 + \mathbf{Z}2, \quad \mathfrak{p}_3 = \mathbf{Z}(\omega_1+1) + \mathbf{Z}(\omega_2+1) + \mathbf{Z}2$$

sind. Explizites Nachrechnen zeigt die Idealgleichung

$$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 = (2).$$

Ist $\mathfrak{p}$ nun irgendein Primideal mit $2 \in \mathfrak{p}$, so folgt $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 \subseteq \mathfrak{p}$, also gibt es ein i mit $\mathfrak{p} = \mathfrak{p}_i$. Damit haben wir gezeigt, daß $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ die einzigen Primideale von $\mathbf{Z}_K$ sind, die 2 enthalten.

Der im letzten Beispiel gezeigte Weg zur Bestimmung von Primidealen ist im allgemeinen sehr aufwendig. Wir wollen jetzt einfachere Möglichkeiten aufzeigen, die allerdings eine spezielle Situation voraussetzen. Wir schicken ein Lemma voraus:

LEMMA. *Sei R Ordnung eines Zahlkörpers, $\alpha \in R$ ein Element, p eine Primzahl und $g(x), h(x) \in \mathbf{Z}[x]$ Polynome, die modulo p teilerfremd sind. Dann gelten die Idealgleichungen*

$$(p, g(\alpha)h(\alpha)) = (p, g(\alpha)) \cdot (p, h(\alpha)) \quad \textit{und} \quad R = (p, g(\alpha)) + (p, h(\alpha)).$$

Beweis: Nach Voraussetzung sind die modulo p reduzierten Polynome $\overline{g}(x), \overline{h}(x) \in \mathbf{F}_p[x]$ teilerfremd. Mit dem erweiterten euklidischen Algorithmus in $\mathbf{F}_p[x]$ findet man Polynome $\overline{a}(x), \overline{b}(x) \in \mathbf{F}_p[x]$ mit

$$\overline{a}(x)\overline{g}(x) + \overline{b}(x)\overline{h}(x) = \overline{1}.$$

Seien $a(x), b(x) \in \mathbf{Z}[x]$ irgendwelche Repräsentanten von $\overline{a}(x)$ und $\overline{b}(x)$. Dann gibt es ein Polynom $c(x) \in \mathbf{Z}[x]$ mit

$$a(x)g(x) + b(x)h(x) = 1 + pc(x).$$

Damit ist

$$1 = a(\alpha)g(\alpha) + b(\alpha)h(\alpha) - pc(\alpha).$$

Dies liefert sofort

$$1 \in (p, g(\alpha)) + (p, h(\alpha))$$

und damit die Teilefremdheit der Ideale $(p, g(\alpha))$ und $(p, h(\alpha))$. Für das Produkt gilt:

$$(p, g(\alpha)) \cdot (p, h(\alpha)) = (p^2, pg(\alpha), ph(\alpha), g(\alpha)h(\alpha)) \subseteq (p, g(\alpha)h(\alpha)).$$

Für die umgekehrte Inklusion müssen wir nur noch zeigen, daß p im Produkt der Ideale enthalten ist. Multipliziert man aber obige Beziehung mit p, so erhält man

$$p = a(\alpha) \cdot pg(\alpha) + b(\alpha) \cdot ph(\alpha) - c(\alpha) \cdot p^2 \in (p, g(\alpha)) \cdot (p, h(\alpha)),$$

was noch zu zeigen war. ■

SATZ. *Sei $R = \mathbf{Z}[\alpha]$ Ordnung eines Zahlkörpers K vom Grad n und f das Minimalpolynom von α. Sei p eine Primzahl und*

$$f(x) \equiv g_1(x)^{e_1} \dots g_r(x)^{e_r} \bmod p$$

die Primfaktorzerlegung von $f(x)$ modulo p, d.h. $g_i(x) \in \mathbf{Z}[x]$ sind normierte Polynome vom Grad $f_i \geq 1$, $g_i(x)$ ist irreduzibel modulo p, je zwei Polynome $g_i(x)$ sind verschieden modulo p und $e_i \geq 1$. (Insbesondere ist dann $\sum_i e_i f_i = n$.) Dann gilt:

1. *$\mathfrak{p}_i = (p, g_i(\alpha))$ ist ein Primideal mit Norm p^{f_i}.*
2. *$\mathfrak{p}_i \neq \mathfrak{p}_j$ für $i \neq j$.*
3. *Man hat die Zerlegung*
$$(p) = (p, g_1(\alpha)^{e_1}) \dots (p, g_r(\alpha)^{e_r}) \supseteq \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}.$$
4. *$\mathfrak{p}_1, \dots, \mathfrak{p}_r$ sind alle Primideale von R, die p enthalten.*
5. *Genau dann gilt $e_1 = \dots = e_r = 1$, wenn $\operatorname{disc}(f) \not\equiv 0 \bmod p$ gilt. In diesem Fall hat man*
$$(p) = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_r.$$

Beweis:

1. Wegen $\mathbf{Z}[\alpha] = \mathbf{Z}[x]/(f(x))$ gilt für den Faktorring modulo $\mathfrak{p}_i$:
$$\mathbf{Z}[\alpha]/\mathfrak{p}_i = \mathbf{Z}[\alpha]/(p, g_i(x)) \simeq \mathbf{Z}[x]/(f(x), p, g_i(x)) \simeq \mathbf{F}_p[x]/(\overline{f}(x), \overline{g_i}(x)) = \mathbf{F}_p[x]/(\overline{g_i}(x)).$$
Da $\overline{g_i}(x)$ in $\mathbf{F}_p[x]$ irreduzibel sein sollte, ist der Quotient $\mathbf{F}_p[x]/(\overline{g_i}(x))$ ein Körper, also $\mathfrak{p}_i$ ein Primideal.
2. Aus dem letzten Lemma folgt $\mathfrak{p}_i + \mathfrak{p}_j = R$, was natürlich die Behauptung beweist.
3. Wir schreiben
$$f(x) = g_1(x)^{e_1} g_2(x)^{e_2} \dots g_r(x)^{e_r} + ph(x)$$
und erhalten mit $f(\alpha) = 0$ die Beziehung
$$g_1(x)^{e_1}(\alpha) \dots g_r(\alpha)^{e_r} = -ph(\alpha).$$
Da die Polynome $g_i(x)^{e_i}$ modulo p paarweise teilerfremd sind, erhält man mit dem letzten Lemma nun
$$(p) = (p, -ph(\alpha)) = (p, g_1(\alpha)^{e_1} \dots g_r(\alpha)^{e_r}) = (p, g_1(\alpha)^{e_1}) \dots (p, g_r(\alpha)^{e_r}),$$
was bereits das $=$-Zeichen beweist. Mit
$$\mathfrak{p}_i^{e_i} = (p, g_i(\alpha))^{e_i} = (p^{e_i}, p^{e_i-1} g_i(\alpha), p^{e_i-2} g_i(\alpha)^2, \dots p g_i(\alpha)^{e_i-1}, g_i(\alpha)^{e_i}) \subseteq (p, g_i(\alpha)^{e_i})$$
folgt auch das $\supseteq$-Zeichen.
4. Ist $\mathfrak{p}$ ein Primideal mit $p \in \mathfrak{p}$, so folgt aus 3.
$$\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r} \subseteq (p) \subseteq \mathfrak{p}.$$
Die Primidealeigenschaft von $\mathfrak{p}$ liefert $\mathfrak{p}_i \subseteq \mathfrak{p}$ für ein i und damit $\mathfrak{p} = \mathfrak{p}_i$, da alle Primideale $\neq 0$ maximal sind.
5. Bekanntlich ist die Diskriminante eines Polynoms f genau dann $\neq 0$, wenn alle Nullstellen von f im algebraischen Abschluß einfach sind. Ist nun $\operatorname{disc}(f) \not\equiv 0 \bmod p$, so gilt also $e_1 = \dots = e_r = 1$. Sei umgekehrt $e_1 = \dots = e_r = 1$. Da endliche Körper vollkommen sind, d.h. jedes irreduzible Polynom ist separabel, hat auch $f \bmod p$ nur einfache Nullstellen im algebraischen Abschluß und somit ist $\operatorname{disc}(f) \not\equiv 0 \bmod p$. Die Zerlegung von (p) folgt nun sofort aus 3. ■

Bemerkungen:

1. Um den Satz anzuwenden, muß man die Primfaktorzerlegung von Polynomen aus $\mathbf{F}_p[x]$ bestimmen. Dafür gibt es effektive Algorithmen. In Maple hat man dazu die Funktion Factor(f) mod p.

2. Da die Diskriminante disc (f) eines irreduziblen Polynoms $f \in \mathbf{Z}[x]$ nur endlich viele Primteiler p hat, hat man also für fast alle Primzahlen p eine Zerlegung $(p) = \mathfrak{p}_1 \dots \mathfrak{p}_r$ mit Exponenten $e_i = 1$.
3. Beim Auftreten von Exponenten $e_i > 1$ muß nicht mehr
$$(p) = \mathfrak{p}_1^{e_1} \cdots = \mathfrak{p}_r^{e_r} = (p, g_1(\alpha))^{e_1} \dots (p, g_r(\alpha))^{e_r}$$
gelten - außer im Fall $R = \mathbf{Z}_K$, wie wir später zeigen werden.

Beispiel: Wir wollen für den Zahlkörper $K = \mathbf{Q}(i)$ (mit $i^2 = -1$) die Primideale der Ordnung $R = \mathbf{Z}[i]$ bestimmen. Jedes von 0 verschiedene Primideal $\mathfrak{p}$ enthält eine Primzahl p. Zur Bestimmung aller Primideale $\mathfrak{p} \subseteq R$, die p enthalten, faktorisieren wir das Minimalpolynom $f(x) = x^2 + 1$ von $i \in R$ modulo p.
Für $p = 2$ ist $f(x) \equiv (x+1)^2 \bmod 2$, also $\mathfrak{p}_2 = (2, i+1)$ das einzige Primideal, das 2 enthält. Man kann explizit nachrechnen, dass $\mathfrak{p}_2^2 = (2)$ gilt.
Sei nun $p > 2$. Da $f(x)$ Grad 2 hat, ist $f(x)$ genau dann reduzibel modulo p, wenn es eine Nullstelle a_p modulo p hat. Dies führt zu folgenden beiden Möglichkeiten:

- Gibt es $a_p \in \mathbf{Z}$ mit $f(a_p) \equiv 0 \bmod p$, d.h. $a_p^2 \equiv -1 \bmod p$, so ist
$$f(x) \equiv (x - a_p)(x + a_p) \bmod p$$
und
$$\mathfrak{p}_{pa} = (p, i - a_p) \quad \text{und} \quad \mathfrak{p}_{pb} = (p, i + a_p)$$
sind genau die Primideale, die p enthalten. Außerdem gilt $\mathfrak{p}_{pa}\mathfrak{p}_{pb} = (p)$.
- Gibt es kein $a_p \in \mathbf{Z}$ mit $a_p^2 \equiv -1 \bmod p$, so ist $f(x)$ irreduzibel modulo p und
$$\mathfrak{p}_p = (p)$$
das einzige Primideal von R, das p enthält.

Wir können jetzt explizit die ersten Primideale auflisten:

p	Faktorisierung von $f(x) \bmod p$	p enthaltende Primideale
2	$f(x) \equiv (x+1)^2 \bmod 2$	$\mathfrak{p}_2 = (2, i+1)$
3	$f(x)$ irreduzibel modulo 3	$\mathfrak{p}_3 = (3)$
5	$f(x) \equiv (x-2)(x+2) \bmod 5$	$\mathfrak{p}_{5a} = (5, i-2)$, $\mathfrak{p}_{5b} = (5, i+2)$
7	$f(x)$ irreduzibel modulo 7	$\mathfrak{p}_7 = (7)$
11	$f(x)$ irreduzibel modulo 11	$\mathfrak{p}_{11} = (11)$
13	$f(x) \equiv (x-5)(x+5) \bmod 13$	$\mathfrak{p}_{13a} = (13, i-5)$, $\mathfrak{p}_{5b} = (13, i+5)$
17	$f(x) \equiv (x-4)(x+4) \bmod 17$	$\mathfrak{p}_{17a} = (17, i-4)$, $\mathfrak{p}_{5b} = (17, i+4)$
19	$f(x)$ irreduzibel modulo 19	$\mathfrak{p}_{19} = (19)$

Wir suchen nun nach einem von p abhängigen Kriterium, wann ein $a_p \in \mathbf{Z}$ mit $a_p^2 \equiv -1 \bmod p$ existiert bzw. nicht existiert. Wir setzen $p > 2$ voraus.
Wir betrachten zunächst den Fall, dass $a_p \in \mathbf{Z}$ existiert mit $a_p^2 \equiv -1 \bmod p$. Dann ist $a_p^4 \equiv 1 \bmod p$, also hat $\overline{a_p}$ Ordnung 4 in der multiplikativen Gruppe $\mathbf{F}_p^*$. Da die Elementordnung immer ein Teiler der Gruppenordnung ist, folgt $4 | \#\mathbf{F}_p^*$, also $4 | p-1$, und damit $p \equiv 1 \bmod 4$.
Sei nun umgekehrt $p \equiv 1 \bmod 4$. Dann gilt $4 | p-1$, d.h. 4 teilt die Gruppenordnung $\#\mathbf{F}_p^* = p - 1$. Da die multiplikative Gruppe $\mathbf{F}_p^*$ zyklisch ist, gibt es zu jedem Teiler d der Gruppenordnung $p-1$ (mindestens) ein Element der Ordnung d. Also gibt es $a_p \in \mathbf{Z}$ mit $a_p^4 \equiv 1 \bmod p$, aber $a_p^2 \not\equiv 1 \bmod p$. Dann folgt aber mit $p | (a_p^2 - 1)(a_p^2 + 1)$ sofort $a_p^2 \equiv -1 \bmod p$.
Damit haben wir für Primzahlen $p > 2$ gezeigt, dass genau dann ein $a_p \in \mathbf{Z}$ mit $a_p^2 \equiv -1 \bmod p$ existiert, wenn $p \equiv 1 \bmod 4$ gilt.
Wir fassen das Ergebnis nochmals für die Primideale zusammen:

- Ist $p \equiv 1 \bmod 4$, so gibt es $a_p \in \mathbf{Z}$ mit $a_p^2 \equiv -1 \bmod 4$, also gilt $f(x) \equiv (x - a_p)(x + a_p) \bmod p$ und damit gibt es genau zwei p enthaltende Primideale, nämlich
$$\mathfrak{p}_{pa} = (p, i - a_p) \quad \text{und} \quad \mathfrak{p}_{pb} = (p, i + a_p),$$
wobei die Gleichung $\mathfrak{p}_{pa}\mathfrak{p}_{pb} = (p)$ gilt.

- Ist $p \equiv 3 \bmod 4$, so gibt es kein $a_p \in \mathbf{Z}$ mit $a_p^2 \equiv -1 \bmod p$, also ist $f(x)$ irreduzibel modulo p und damit ist
$$\mathfrak{p}_p = (p)$$
das einzige p enthaltende Primideal.

Für $p \equiv 1 \bmod 4$ gibt es also genau zwei Primideale $\mathfrak{p}_{pa}, \mathfrak{p}_{pb}$, die p enthalten, sonst genau eines, nämlich $\mathfrak{p}_2 = (2, i+1)$ im Fall $p = 2$ und $\mathfrak{p}_p = (p)$ im Fall $p \equiv 3 \bmod 4$.

Beispiel: Wir betrachten $K = \mathbf{Q}(\alpha)$ mit $f(\alpha) = 0$, wo $f(x) = x^3 + 7x + 20$ ist, und darin die (nichtmaximale) Ordnung $R = \mathbf{Z}[\alpha]$. Die Primfaktorzerlegung von $f(x)$ modulo p liefert die folgenden Primideale:

p	Primfaktorzerlegung von $f \bmod p$	Primideale
2	$x(x+1)^2$	$\mathfrak{p}_{2a} = (2, \alpha)$, $\mathfrak{p}_{2b} = (2, \alpha+1)$
3	$(x+1)(x^2+2x+2)$	$\mathfrak{p}_{3a} = (3, \alpha+1)$, $\mathfrak{p}_{3b} = (3, \alpha^2+2\alpha+2)$
5	$x(x^2+2)$	$\mathfrak{p}_{5a} = (5, \alpha)$, $\mathfrak{p}_{5b} = (5, \alpha^2+2)$
7	$(x+3)(x+5)(x+6)$	$\mathfrak{p}_{7a} = (7, \alpha+3)$, $\mathfrak{p}_{7b} = (7, \alpha+5)$, $\mathfrak{p}_{7c} = (7, \alpha+6)$
11	irreduzibel	$\mathfrak{p}_{11} = (11)$
13	irreduzibel	$\mathfrak{p}_{13} = (13)$
17	$(x+6)(x+14)^2$	$\mathfrak{p}_{17a} = (17, \alpha+6)$, $\mathfrak{p}_{17b} = (17, \alpha+14)$
19	irreduzibel	$\mathfrak{p}_{19} = (19)$

Wählt man als $\mathbf{Z}$-Basis $\alpha^2, \alpha, 1$, so findet man für nachfolgende Ideale wie üblich die entsprechenden Matrizen in Hermitescher Normalform:

$$\mathfrak{p}_{2a} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}, \quad \mathfrak{p}_{2b} \to \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix}, \quad \mathfrak{p}_{2b}^2 \to \begin{pmatrix} 1 & 0 & 3 \\ 0 & 2 & 2 \\ 0 & 0 & 4 \end{pmatrix}, \quad \mathfrak{p}_{2a}\mathfrak{p}_{2b}^2 \to \begin{pmatrix} 2 & 0 & 2 \\ 0 & 2 & 2 \\ 0 & 0 & 4 \end{pmatrix},$$

was insbesondere $(2) \neq \mathfrak{p}_{2a}\mathfrak{p}_{2b}^2$ zeigt.

Leider haben nicht alle Ordnungen eines Zahlkörpers die Gestalt $\mathbf{Z}[\alpha]$, so daß man den letzten Satz zur Primidealbestimmung direkt anwenden könnte. In jeder Ordnung R ist aber eine Ordnung der Gestalt $\mathbf{Z}[\alpha]$ enthalten. Daher liegt es nahe, die Primideale verschiedener Ordnungen in Beziehung zu setzen.

Seien $R \subseteq S$ Ordnungen eines Zahlkörpers. Man kann leicht natürliche Abbildungen zwischen R- und S-Idealen angeben:

1. Ist $\mathfrak{a} \subseteq R$ ein R-Ideal (mit $\mathfrak{a} = R\alpha_1 + \cdots + R\alpha_r$), so ist
$$S\mathfrak{a} = S(R\alpha_1 + \cdots + R\alpha_r) = S\alpha_1 + \cdots + S\alpha_r$$
ein S-Ideal.
2. Ist $\mathfrak{A} \subseteq S$ ein S-Ideal, so ist $R \cap \mathfrak{A} \subseteq R$ offensichtlich ein R-Ideal.

Allerdings ist nicht klar, dass die angebenen Abbildungen invers zueinander sind.

Wir geben zunächst einen allgemeinen Satz für Primideale an:

LEMMA. *Sind $R \subseteq S$ zwei kommutative Ringe, ist $\mathfrak{P} \subseteq S$ ein Primideal in S, so ist $\mathfrak{P} \cap R$ ein Primideal in R.*

Beweis: Man überprüft einfach die in der Definition geforderten Eigenschaften eines Primideals. Alternativ: Der (natürliche) Homomorphismus $R \to S/\mathfrak{P}$ hat als Kern das Ideal $R \cap \mathfrak{P}$, so daß der Homomorphiesatz eine Einbettung
$$R/\mathfrak{P} \cap R \hookrightarrow S/\mathfrak{P}$$
liefert. Da $S/\mathfrak{P}$ Integritätsring ist, ist auch $R/R \cap \mathfrak{P}$ Integritätsring und damit $R \cap \mathfrak{P}$ ein Primideal in R. ■

SATZ. *Seien $R \subseteq S$ Ordnungen eines Zahlkörpers K und p eine Primzahl, die den Index $f = [S : R]$ nicht teilt, d.h. $f \not\equiv 0 \bmod p$. Dann gibt es eine Bijektion der p enthaltenden Primideale von R und S:*

$$\begin{array}{ccc} \textit{Primideale in } R & & \textit{Primideale in } S \\ \mathfrak{p} & \mapsto & S\mathfrak{p} \\ R \cap \mathfrak{P} & \leftarrow & \mathfrak{P} \end{array}$$

Außerdem stimmen die Idealnormen überein: $N(\mathfrak{p}) = N(S\mathfrak{p})$, wobei $N(\mathfrak{p}) = [R : \mathfrak{p}]$ und $N(S\mathfrak{p}) = [S : S\mathfrak{p}]$ ist.

Beweis:

1. Da f und p nach Voraussetzung teilerfremd sind, gibt es eine Darstellung $1 = af + bp$ mit ganzen Zahlen $a, b \in \mathbf{Z}$. Da f die Ordnung der abelschen Faktorgruppe S/R ist, gilt $fS \subseteq R$.
2. Sei im folgenden $\mathfrak{p}$ ein Primideal von R, das die Primzahl p enthält.
3. Wir zeigen zunächst, dass $S = S\mathfrak{p} + R$ gilt. Die Inklusion $S \supseteq S\mathfrak{p} + R$ ist trivial. Sei jetzt $s \in S$. Dann ist
$$s = s \cdot 1 = s(af + bp) = (bs)p + a(fs) \in S\mathfrak{p} + R \quad \text{wegen} \quad fs \in R,$$
was auch $S \subseteq S\mathfrak{p} + R$ zeigt.
4. Wir zeigen nun $R \cap S\mathfrak{p} = \mathfrak{p}$, wobei $R \cap S\mathfrak{p} \supseteq \mathfrak{p}$ wieder trivial ist. Sei $r = \sum s_i \pi_i \in R \cap S\mathfrak{p}$ mit $r \in R$, $s_i \in S$, $\pi_i \in \mathfrak{p}$. Dann ist
$$r = r(af + bp) = af \cdot r + rbp = af \sum s_i \pi_i + rbp = a \sum (fs_i)\pi_i + rbp \in \mathfrak{p} \quad \text{wegen} \quad fs_i \in R,$$
was $R \cap S\mathfrak{p} \subseteq \mathfrak{p}$ und damit die behauptete Gleichung zeigt.
5. Über die Inklusion $R \subseteq S$ definieren wir einen Ringhomomorphismus
$$\psi : R \to S/S\mathfrak{p}, \quad x \mapsto x \bmod S\mathfrak{p}.$$
Wegen $S = S\mathfrak{p} + R$ ist ψ surjektiv. Der Kern von ψ ist $R \cap S\mathfrak{p} = \mathfrak{p}$. Der Homomorphiesatz für Ringhomomorphismen liefert nun einen Isomorphismus
$$R/\mathfrak{p} \simeq S/S\mathfrak{p}.$$
Mit $\mathfrak{p}$ ist daher auch $S\mathfrak{p}$ ein Primideal. Außerdem folgt $\mathrm{N}\mathfrak{p} = \#R/\mathfrak{p} = \#S/S\mathfrak{p} = \mathrm{N}(S\mathfrak{p})$.
6. Wegen $R \cap S\mathfrak{p} = \mathfrak{p}$ ist die Zuordnung $\mathfrak{p} \mapsto S\mathfrak{p}$ injektiv.
7. Ist $\mathfrak{P}$ ein Primideal in S mit $p \in S$, so ist $\mathfrak{P} \cap R$ ein Primideal $\mathfrak{p}$ in R, das p enthält, d.h. $\mathfrak{P} \cap R = \mathfrak{p}$. Aus $\mathfrak{p} \subseteq \mathfrak{P}$ folgt nun $S\mathfrak{p} \subseteq \mathfrak{P}$ und wegen der Maximalität der Primideale $S\mathfrak{p} = \mathfrak{P}$. Damit ist alles gezeigt. ■

Anwendung: Sei R Ordnung eines Zahlkörpers K und p eine Primzahl, zu der wir alle Primideale $\mathfrak{p} \subseteq R$ mit $p \in \mathfrak{p}$ bestimmen wollen. Wir wählen ein $\alpha \in R$ mit $K = \mathbf{Q}(\alpha)$ und bestimmen das Minimalpolynom $f(x)$. Teilt nun p den Index $[R : \mathbf{Z}[\alpha]]$ nicht, so bestimmen wir die Primfaktorzerlegung von $f(x)$ modulo p:
$$f(x) \equiv g_1(x)^{e_1} \ldots g_r(x)^{e_r} \bmod p.$$
Dann sind $\mathfrak{p}_i = (p, g_i(\alpha)) \subseteq R$, $i = 1, \ldots, r$ die Primideale von R, die p enthalten. (Ist die Indexbedingung nicht erfüllt, kann man versuchen ein anderes α zu finden.)

Beispiel: Sei $K = \mathbf{Q}(\alpha)$ mit $\alpha^2 = -2$. Wir betrachten die Ordnungen $R = \mathbf{Z}[3\alpha]$ und $S = \mathbf{Z}[\alpha]$ mit Index $[S : R] = 3$. Sei $\beta = 3\alpha$. Das Minimalpolynom von β ist $x^2 + 18$. Aus $x^2 + 18 \equiv x^2 \bmod 3$ folgt, dass
$$\mathfrak{p} = (3, \beta)$$
das einzige Primideal in R ist, das die Primzahl 3 enthält. Das Minimalpolynom von α ist $x^2 + 2$, aus $x^2 + 2 \equiv (x + 1)(x + 2) \bmod 3$ folgt, dass
$$\mathfrak{P}_1 = (3, \alpha + 1) \quad \text{und} \quad \mathfrak{P}_2 = (3, \alpha + 2)$$
die Primideale von S sind, die 3 enthalten. Also gibt es keine Bijektion zwischen den 3-enthaltenden Primidealen von R und S. Wir bemerken noch, dass
$$S\mathfrak{p} = S \cdot 3 + S \cdot \beta = S \cdot 3 + S \cdot 3\alpha = S \cdot 3$$
kein Primideal in S ist.

Beispiel: Wir betrachten $K = \mathbf{Q}(\alpha)$ mit $\alpha^3 + 7\alpha + 20 = 0$. Die Ordnung $R = \mathbf{Z}[\alpha]$ hat Index 2 in der Maximalordnung $\mathbf{Z}_K$, als Ganzheitsbasis können wir

$$\omega_1 = \frac{\alpha^2 + \alpha}{2}, \quad \omega_2 = \alpha, \quad \omega_3 = 1$$

wählen. Die Primideale aus $\mathbf{Z}[\alpha]$, die 3 enthalten, sind:

$$\mathfrak{p}_{3a} = (3, \alpha + 1), \quad \mathfrak{p}_{3b} = (3, \alpha^2 + 2\alpha + 2).$$

Nun wird über $\mathbf{Z}_K$:

$$\mathbf{Z}_K 3 + \mathbf{Z}_K(\alpha + 1) \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 3 \end{pmatrix}, \quad \mathbf{Z}_K 3 + \mathbf{Z}_K(\alpha^2 + 2\alpha + 2) \to \begin{pmatrix} 1 & 2 & 1 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix},$$

was den früher bestimmten Idealen $\mathfrak{a}_3$ und $\mathfrak{a}_{9b}$ entspricht.
Die 2 enthaltenden Primideale von $\mathbf{Z}[\alpha]$ sind

$$\mathfrak{p}_{2a} = (2, \alpha) \quad \text{und} \quad \mathfrak{p}_{2b} = (2, \alpha + 1)$$

mit

$$\mathrm{N}(\mathfrak{p}_{2a}) = 2 \quad \text{und} \quad \mathrm{N}(\mathfrak{p}_{2b}) = 2.$$

Nimmt man das Erzeugnis in $\mathbf{Z}_K$, so erhält man

$$\mathbf{Z}_K \mathfrak{p}_{2a} = \mathbf{Z}_K 2 + \mathbf{Z}_K \alpha \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}, \quad \mathbf{Z}_K \mathfrak{p}_{2b} = \mathbf{Z}_K 2 + \mathbf{Z}_K(\alpha + 1) \to \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix},$$

was den Idealen $\mathfrak{a}_2$ und $\mathfrak{a}_{4b}$ entspricht, die in diesem Fall auch prim sind. Hier gilt

$$\mathrm{N}(\mathbf{Z}_K \mathfrak{p}_{a2}) = 2 = \mathrm{N}(\mathfrak{p}_{2a}) \quad \text{und} \quad \mathrm{N}(\mathbf{Z}_K \mathfrak{p}_{2b}) = 4 \neq 2 = \mathrm{N}(\mathfrak{p}_{2b}),$$

also muß die Idealnorm nicht erhalten bleiben, wenn man zu einer größeren Ordnung übergeht und die Primzahl den Index der Ordnungen teilt.

Beispiel: Wir betrachten wieder $K = \mathbf{Q}(\alpha)$ mit $f(\alpha) = 0$, wo $f = x^3 + x^2 - 2x + 8$ ist. Aus $f \equiv x^2(x + 1) \bmod 2$ folgt, daß $(2, \alpha)$ und $(2, \alpha + 1)$ die Primideale in $\mathbf{Z}[\alpha]$ sind, die 2 enthalten. Durch Übergang zu den Normalformen kann man sehen, daß in $\mathbf{Z}_K$ das Ideal $(2, \alpha + 1)$ weiterhin prim ist, es stimmt mit $\mathfrak{p}_3$ überein, allerdings hat $(2, \alpha)$ die Normalform

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix},$$

insbesondere Norm 4, und kann daher nicht prim sein, da alle 2 enthaltenden Primideale von $\mathbf{Z}_K$ Norm 2 haben. (Bei diesem Beispiel kann man auch bei Wahl einer anderen Ordnung $\mathbf{Z}[\beta]$ nichts erreichen.)

Die Aussagen des folgenden Satzes werden später mehrfach benutzt werden.

Satz. *Sei R Ordnung eines Zahlkörpers K vom Grad n, p eine Primzahl und $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ die p enthaltenden Primideale von R. Definiert man*

$$I_p(R) = \{\alpha \in R : \alpha^m \equiv 0 \bmod p \text{ für ein } m \geq 1\},$$

so gilt

$$I_p(R) = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r = \mathfrak{p}_1 \ldots \mathfrak{p}_r \quad \text{und} \quad I_p(R)^n = (\mathfrak{p}_1 \ldots \mathfrak{p}_r)^n \subseteq Rp.$$

Insbesondere ist $I_p(R)$ ein Ideal und es gilt

$$I_p(R) = \{\alpha \in R : \alpha^n \equiv 0 \bmod p\}.$$

Beweis: Da die Ideale $\mathfrak{p}_i$ maximal sind, gilt $\mathfrak{p}_i+\mathfrak{p}_j = R$ für $i \neq j$. Im Zusammenhang mit dem chinesischen Restsatz haben wir dann die Gleichung $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r = \mathfrak{p}_1 \ldots \mathfrak{p}_r$ bewiesen. Sei jetzt $\alpha \in I_p(R)$. Dann gibt es ein $m \geq 1$ mit $\alpha^m \in Rp$. Es folgt $\alpha^m \in \mathfrak{p}_i$ und damit $\alpha \in \mathfrak{p}_i$. Dies liefert $\alpha \in \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$, also $I_p(R) \subseteq \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$. Sei nun $\alpha \in \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$. Wir haben

$$R \supseteq R\alpha + Rp \supseteq R\alpha^2 + Rp \supseteq \cdots \supseteq R\alpha^m + Rp \supseteq R\alpha^{m+1} + Rp \supseteq Rp.$$

Da es zwischen R und Rp nur endlich viele Moduln gibt, existiert ein $m \in \mathbf{N}$ mit $R\alpha^m+Rp = R\alpha^{m+1}+Rp$. Dann gibt es $u, v \in R$ mit $\alpha^m = u\alpha^{m+1} + vp$, also $\alpha^m(1-u\alpha) = vp$. Wegen $\alpha, p \in \mathfrak{p}_i$ und der Tatsache, dass $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ die einzigen p enthaltenden Primideale sind, folgt $R(1-u\alpha)+Rp = R$, d.h. es gibt $w, x \in R$ mit $1 = w(1-u\alpha) + xp$ und damit

$$\alpha^m = \alpha^m(1-u\alpha)w + \alpha^m xp = vwp + \alpha^m xp = p(vw + \alpha^m x) \in Rp.$$

Dies beweist $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r \subseteq I_p(R)$ und damit die Gleichheit $I_p(R) = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$.
Sei nun $\omega_1, \ldots, \omega_n$ eine $\mathbf{Z}$-Basis von R. Wir betrachten die rationale Darstellung bzgl. der $\mathbf{Q}$-Basis $\omega_1, \ldots, \omega_n$, d.h. jedes $\alpha \in K$ liefert eine Matrix $A(\alpha)$ vermöge

$$\alpha \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = A(\alpha) \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix}.$$

Es gilt für $\alpha \in R$:

$$\begin{aligned} \alpha \in I_p(R) &\iff \alpha^m \in Rp \text{ für ein } m \geq 1 \iff A(\alpha^m) \equiv 0 \bmod p \text{ für ein } m \geq 1 \iff \\ &\iff \overline{A(\alpha)} \text{ ist nilpotent in } M_n(\mathbf{F}_p) \iff \\ &\iff \text{das charakteristische Polynom von } \overline{A(\alpha)} \text{ ist } x^n \iff \alpha^n \equiv 0 \bmod p. \end{aligned}$$

Dies beweist $I_p(R)^n = (\mathfrak{p}_1 \ldots \mathfrak{p}_r)^n \subseteq Rp$ und $I_p(R) = \{\alpha \in R : \alpha^n \equiv 0 \bmod p\}$. ■

Wir erwähnen noch eine weitere allgemeine Eigenschaft von Primidealen:

LEMMA. *Sei $\mathfrak{p} \neq 0$ Primideal einer Ordnung R eines Zahlkörpers K. Dann gilt:*

1. $\mathfrak{p} \neq \mathfrak{p}^2$.
2. $\mathfrak{p}/\mathfrak{p}^2$ *ist ein* $R/\mathfrak{p}$*-Vektorraum.*
3. $[\mathfrak{p} : \mathfrak{p}^2] = (\mathrm{N}\mathfrak{p})^\mu$ *für ein* $\mu \geq 1$ *und damit* $\mathrm{N}\mathfrak{p}^2 = (\mathrm{N}\mathfrak{p})^{\mu+1}$.

Beweis:

1. Wir nehmen an, es würde $\mathfrak{p} = \mathfrak{p}^2$ gelten. Sei $\mathfrak{p} = (\pi_1, \ldots, \pi_r)$. Jedes Element aus $\mathfrak{p}^2$ läßt sich schreiben als $\sum_{j=1}^r \mu_j\pi_j$ mit $\mu_j \in \mathfrak{p}$, also erhält man mit der Annahme $\mathfrak{p} = \mathfrak{p}^2$ eine Darstellung

$$\pi_i = \sum_{j=1}^r \mu_{ij}\pi_j \quad \text{mit } \mu_{ij} \in \mathfrak{p}.$$

In Matrizenschreibweise ergibt sich

$$\begin{pmatrix} \pi_1 \\ \vdots \\ \pi_r \end{pmatrix} = \begin{pmatrix} \mu_{11} & \cdots & \mu_{1r} \\ \vdots & & \vdots \\ \mu_{r1} & \cdots & \mu_{rr} \end{pmatrix} \begin{pmatrix} \pi_1 \\ \vdots \\ \pi_r \end{pmatrix}.$$

Setzt man $M = (\mu_{ij})_{ij}$, so wird

$$(I_r - M) \begin{pmatrix} \pi_1 \\ \vdots \\ \pi_r \end{pmatrix} = 0.$$

Nun gilt $I_r - M \equiv I_r \bmod \mathfrak{p}$, also $\det(I_r - M) \equiv 1 \bmod \mathfrak{p}$, insbesondere $\det(I_r - M) \neq 0$. Durch Multiplikation mit der inversen Matrix aus $GL_r(K)$ folgt

$$\begin{pmatrix} \pi_1 \\ \vdots \\ \pi_r \end{pmatrix} = 0,$$

also $\mathfrak{p} = R\pi_1 + \cdots + R\pi_r = 0$, ein Widerspruch zur Voraussetzung $\mathfrak{p} \neq 0$. Damit folgt $\mathfrak{p} \neq \mathfrak{p}^2$.

2. Sind $r_1, r_2 \in R$ mit $r_2 - r_1 = x \in \mathfrak{p}$, $\pi_1, \pi_2 \in \pi$ mit $\pi_2 - \pi_1 = y_2 \in \mathfrak{p}^2$, so folgt modulo $\mathfrak{p}^2$

$$r_2\pi_2 = r_2(\pi_1 + y_2) = r_2\pi_1 + r_2y_2 \equiv r_2\pi_1 = (r_1 + x)\pi_1 = r_1\pi_1 + x\pi_1 \equiv r_1\pi_1 \bmod \mathfrak{p}^2,$$

daher ist

$$R/\mathfrak{p} \times \mathfrak{p}/\mathfrak{p}^2 \to \mathfrak{p}/\mathfrak{p}^2, \quad (\overline{r}, \overline{\pi}) \mapsto \overline{r\pi}$$

wohldefiniert und liefert offensichtlich eine Vektorraumstruktur auf $\mathfrak{p}/\mathfrak{p}^2$ bzgl. des Körpers $R/\mathfrak{p}$.

3. Ist μ die Dimension von $\mathfrak{p}/\mathfrak{p}^2$ über $R/\mathfrak{p}$, so gilt $\#\mathfrak{p}/\mathfrak{p}^2 = (\#R/\mathfrak{p})^\mu$. Wegen $\mathfrak{p} \neq \mathfrak{p}^2$ folgt $\mu \geq 1$. Damit gilt

$$[\mathfrak{p} : \mathfrak{p}^2] = \#\mathfrak{p}/\mathfrak{p}^2 = (\#R/\mathfrak{p})^\mu = (\mathrm{N}\mathfrak{p})^\mu \quad \text{und} \quad \mathrm{N}(\mathfrak{p}^2) = [R : \mathfrak{p}^2] = [R : \mathfrak{p}] \cdot [\mathfrak{p} : \mathfrak{p}^2] = (\mathrm{N}\mathfrak{p})^{\mu+1},$$

was zu zeigen war. ■

6. Gebrochene Ideale

Beim Rechnen mit ganzen Zahlen ist es manchmal nützlich, auch Nenner zuzulassen, d.h. mit rationalen Zahlen zu rechnen. Ebenso erweist es sich in manchen Situationen als vorteilhaft, Ideale mit Nennern zuzulassen:

DEFINITION. Sei R eine Ordnung eines Zahlkörpers. Ein gebrochenes Ideal $\mathfrak{a}$ von R ist ein Modul des Zahlkörpers, für den $R\mathfrak{a} \subseteq \mathfrak{a}$ gilt.

Das folgende Lemma gibt eine alternative Definition:

LEMMA. *Sei R Ordnung eines Zahlkörpers K. Eine Teilmenge $\mathfrak{a} \subseteq K$, $\mathfrak{a} \neq \{0\}$ ist genau dann ein gebrochenes Ideal von R, wenn es $\alpha_1, \ldots, \alpha_r \in K$ gibt mit*

$$\mathfrak{a} = R\alpha_1 + \cdots + R\alpha_r.$$

(In algebraischer Sprache: Ein gebrochenes Ideal ist ein endlich erzeugter R-Untermodul von K.)

Beweis: Sei $\mathfrak{a}$ ein gebrochenes Ideal und $\alpha_1, \ldots, \alpha_n$ eine $\mathbf{Z}$-Basis von $\mathfrak{a}$. Wegen $R\mathfrak{a} \subseteq \mathfrak{a}$ folgt

$$\mathfrak{a} = \mathbf{Z}\alpha_1 + \cdots + \mathbf{Z}\alpha_n \subseteq R\alpha_1 + \cdots + R\alpha_n = \mathbf{Z}\alpha_1 + \cdots + \mathbf{Z}\alpha_n = \mathfrak{a},$$

was die eine Richtung beweist. Sei umgekehrt $\mathfrak{a} \neq \{0\}$ mit $\mathfrak{a} = R\alpha_1 + \cdots + R\alpha_r$. Offensichtlich gilt dann $R\mathfrak{a} \subseteq \mathfrak{a}$. Ist $\omega_1, \ldots, \omega_n$ eine $\mathbf{Z}$-Basis von R, so folgt

$$\mathfrak{a} = \sum_{i=1}^{r} \sum_{j=1}^{n} \mathbf{Z}\alpha_i\omega_j,$$

also ist $\mathfrak{a}$ ein Modul in K. ■

Bemerkungen:

1. Jedes Ideal $\neq 0$ einer Ordnung R ist auch ein gebrochenes Ideal. Ist $\mathfrak{a}$ ein gebrochenes Ideal von R und $\mathfrak{a} \subseteq R$, so ist R ein Ideal von R.
2. Ein gebrochenes Ideal $\mathfrak{a}$ einer Ordnung R läßt sich eindeutig durch eine Hermitesche Normalform (mit Nenner) beschreiben. Ist also $\omega_1, \ldots, \omega_n$ eine $\mathbf{Z}$-Basis von R, so gibt es $d \in \mathbf{N}$, $c_{ij} \in \mathbf{Z}$ mit $c_{ii} > 0$, $0 \leq c_{ij} < c_{jj} - 1$ für $i < j$, $c_{ij} = 0$ für $i > j$, $\mathrm{ggT}(d, c_{11}, c_{12}, \ldots, c_{nn}) = 1$ und

$$\mathfrak{a} = \frac{1}{d} \sum_{i=1}^{n} \mathbf{Z}(\sum_{j=i}^{n} c_{ij}\omega_j).$$

   Insbesondere ist $d\mathfrak{a}$ ein Ideal $\neq 0$ in R.
3. Um die (gewöhnlichen) Ideale von R auch sprachlich von den gebrochenen Ideale von R abzugrenzen, nennt man sie manchmal auch ganze Ideale von R.

Beispiele: Sei R Ordnung eines Zahlkörpers.

1. Ist $\alpha \in K$, $\alpha \neq 0$, so ist $R\alpha$ ein gebrochenes Ideal.
2. Ist $\mathfrak{a} \subseteq R$ ein Ideal, $d \in \mathbf{N}$, so ist $\frac{1}{d}\mathfrak{a}$ ein gebrochenes Ideal.

Gebrochene Ideale kann man (als Moduln des Zahlkörpers) addieren und multiplizieren, die Idealnorm wird durch $\mathrm{N}\mathfrak{a} = [R : \mathfrak{a}]$ auch für gebrochene Ideale definiert.

Beispiel: Ist $\alpha \in K$, $\alpha \neq 0$, so ist $R\alpha = (\alpha)$ ein gebrochenes Ideal mit Norm $|\mathrm{N}(\alpha)|$. (Der Beweis unterscheidet sich nicht von dem Beweis für $\alpha \in R$.)

Für Moduln $\mathfrak{a} = \mathbf{Z}\alpha_1 + \cdots + \mathbf{Z}\alpha_n$ und $\mathfrak{b} = \mathbf{Z}\beta_1 + \cdots + \mathbf{Z}\beta_n$ eines Zahlkörpers K hatten wir gesehen, dass auch

$$(\mathfrak{a} : \mathfrak{b}) = \{\lambda \in K : \lambda\mathfrak{b} \subseteq \mathfrak{a}\}$$

ein Modul ist, nämlich

$$(\mathfrak{a} : \mathfrak{b}) = \bigcap_{i=1}^{n} (\mathbf{Z}\frac{\alpha_1}{\beta_i} + \cdots + \mathbf{Z}\frac{\alpha_n}{\beta_i}).$$

LEMMA. *Sind $\mathfrak{a}$ und $\mathfrak{b}$ gebrochene Ideale einer Ordnung R, so ist auch $(\mathfrak{a} : \mathfrak{b})$ ein gebrochenes Ideal von R.*

Beweis: Es bleibt nur noch $R \cdot (\mathfrak{a} : \mathfrak{b}) \subseteq (\mathfrak{a} : \mathfrak{b})$ zu zeigen. Sei $\lambda \in (\mathfrak{a} : \mathfrak{b})$, d.h. $\lambda\mathfrak{b} \subseteq \mathfrak{a}$. Dann gilt $R\lambda \cdot \mathfrak{b} \subseteq R\mathfrak{a} \subseteq \mathfrak{a}$, also $R\lambda \subseteq (\mathfrak{a} : \mathfrak{b})$ und damit $R(\mathfrak{a} : \mathfrak{b}) \subseteq (\mathfrak{a} : \mathfrak{b})$, wie behauptet. ■

Bemerkung: Eigentlich muss man im letzten Lemma für $\mathfrak{b}$ nur voraussetzen, dass $\mathfrak{b}$ ein Modul ist.

Wir werden später Aussagen über gebrochene Ideale der Gestalt $(R : \mathfrak{a})$ benötigen, die wir hier zusammenstellen:

LEMMA. *Sei R Ordnung eines Zahlkörpers und $\mathfrak{a}$ ein gebrochenes Ideal von R.*

1. *Ist $\mathfrak{a} = R\alpha_1 + \cdots + R\alpha_r \subseteq K$ mit $\alpha_i \in K^*$, so gilt*
$$(R : \mathfrak{a}) = \bigcap_{i=1}^{r} R\frac{1}{\alpha_r}.$$
2. $\mathfrak{a} \cdot (R : \mathfrak{a}) \subseteq R$.
3. *Für $\omega \in K$, $\omega \neq 0$ ist*
$$(R : \omega\mathfrak{a}) = \frac{1}{\omega}(R : \mathfrak{a}).$$
4. *Ist $\mathfrak{a}$ ein ganzes Ideal und $d \in \mathbf{N}$ mit $d \in \mathfrak{a}$, so gilt:*
$$R \subseteq (R : \mathfrak{a}) \subseteq \frac{1}{d}R.$$

Beweis:

1. Für $\lambda \in K$ gilt:
$$\begin{aligned} \lambda \in (R : \mathfrak{a}) &\iff \lambda\mathfrak{a} \subseteq R \iff \lambda\alpha_1 \in R, \ldots, \lambda\alpha_r \in R \\ &\iff \lambda \in R\frac{1}{\alpha_r}, \ldots, \lambda \in R\frac{1}{\alpha_r} \iff \lambda \in (R\frac{1}{\alpha_1}) \cap \cdots \cap (R\frac{1}{\alpha_r}), \end{aligned}$$
was die Behauptung beweist.
2. Klar.
3. Für $\lambda \in K$ gilt:
$$\lambda \in (R : \omega\mathfrak{a}) \iff \lambda\omega\mathfrak{a} \subseteq R \iff \lambda\omega \in (R : \mathfrak{a}) \iff \lambda \in \frac{1}{\omega}(R : \mathfrak{a}),$$
was die Behauptung zeigt.
4. Wegen $R\mathfrak{a} \subseteq \mathfrak{a} \subseteq R$ folgt die erste Inklusion. Ist $\lambda \in (R : \mathfrak{a})$, so muss wegen $d \in \mathfrak{a}$ gelten: $\lambda d \in R$, also $\lambda \in \frac{1}{d}R$, was die zweite Inklusion zeigt. ■

Beispiel: Wir betrachten $K = \mathbf{Q}(\alpha)$ mit $\alpha^3 + \alpha^2 - 2\alpha + 8 = 0$. Es gilt $\mathbf{Z}_K = \mathbf{Z} \cdot \frac{\alpha^2+\alpha}{2} + \mathbf{Z}\alpha + \mathbf{Z}$. Wir hatten gesehen, dass das Ideal $\mathfrak{p} = (2, \alpha + 1)$ ein Primideal mit Norm 2 ist. Mit obiger Formel gilt:

$$\begin{aligned}
(R : \mathfrak{p}) &= (\mathbf{Z}_K \cdot \frac{1}{2}) \cap (\mathbf{Z}_K \cdot \frac{1}{\alpha+1}) = \\
&= (\mathbf{Z} \cdot \frac{\alpha^2+\alpha}{4} + \mathbf{Z} \cdot \frac{\alpha}{2} + \mathbf{Z} \cdot \frac{1}{2}) \cap (\mathbf{Z} \cdot \frac{\alpha^2+\alpha}{2(\alpha+1)} + \mathbf{Z} \cdot \frac{\alpha}{\alpha+1} + \mathbf{Z} \cdot \frac{1}{\alpha+1}) = \\
&= (\mathbf{Z} \cdot (\frac{1}{4}\alpha^2 + \frac{1}{4}\alpha) + \mathbf{Z} \cdot \frac{1}{2}\alpha + \mathbf{Z} \cdot \frac{1}{2}) \cap (\mathbf{Z} \cdot \frac{1}{2}\alpha + \mathbf{Z} \cdot (\frac{1}{10}\alpha^2 + \frac{4}{5}) + \mathbf{Z} \cdot (-\frac{1}{10}\alpha^2 + \frac{1}{5})) = \\
&= \frac{1}{20}\left((\mathbf{Z} \cdot (5\alpha^2 + 5\alpha) + \mathbf{Z} \cdot 10\alpha + \mathbf{Z} \cdot 10) \cap (\mathbf{Z} \cdot 10\alpha + \mathbf{Z} \cdot (2\alpha^2 + 16) + \mathbf{Z} \cdot (-2\alpha^2 + 4))\right) = \\
&= \frac{1}{20}\left((\mathbf{Z} \cdot (5\alpha^2 + 5\alpha) + \mathbf{Z} \cdot 10\alpha + \mathbf{Z} \cdot 10) \cap (\mathbf{Z} \cdot (2\alpha^2 + 16) + \mathbf{Z} \cdot 10\alpha + \mathbf{Z} \cdot 20)\right) = \\
&= \frac{1}{20}(\mathbf{Z} \cdot 10\alpha^2 + \mathbf{Z} \cdot 10\alpha + \mathbf{Z} \cdot 20) = \mathbf{Z} \cdot \frac{1}{2}\alpha^2 + \mathbf{Z} \cdot \frac{1}{2}\alpha + \mathbf{Z}.
\end{aligned}$$

7. Invertierbare Ideale

DEFINITION. Ein gebrochenes Ideal $\mathfrak{a}$ einer Ordnung R eines Zahlkörpers heißt invertierbar, wenn es ein gebrochenes Ideal $\mathfrak{b}$ gibt mit

$$\mathfrak{a}\mathfrak{b} = R.$$

Beispiel: Gebrochene Hauptideale $R\alpha$ sind invertierbar, denn

$$R\alpha \cdot R\frac{1}{\alpha} = R.$$

Da die Idealmultiplikation kommutativ und assoziativ ist, ist folgender Satz sofort klar:

SATZ. *Sei R Ordnung eines Zahlkörpers und I_R die Menge der gebrochenen invertierbaren Ideale von R. Dann wird I_R durch Multiplikation zu einer abelschen Gruppe. Das Inverse zu $\mathfrak{a} \in I_R$ wird mit $\mathfrak{a}^{-1}$ bezeichnet. Die Hauptideale $H_R = \{R\alpha : \alpha \in K, \alpha \neq 0\}$ sind eine Untergruppe von I_R. Die Faktorgruppe I_R/H_R heißt die Klassengruppe von R und wird mit $C\ell(R)$ bezeichnet.*

(Die Bedeutung dieses Satzes wird erst später sichtbar werden. An dieser Stelle sollte nur gezeigt werden, was man aus der Definition des Begriffs *invertierbares Ideal* sofort folgern kann.)

LEMMA. *Ein gebrochenes Ideal $\mathfrak{a}$ einer Ordnung ist genau dann invertierbar, wenn gilt*

$$\mathfrak{a} \cdot (R : \mathfrak{a}) = R.$$

In diesem Fall ist $\mathfrak{a}^{-1} = (R : \mathfrak{a})$.

Beweis: Gilt $\mathfrak{a} \cdot (R : \mathfrak{a}) = R$, so ist $\mathfrak{a}$ nach Definition invertierbar. Sei umgekehrt $\mathfrak{a}$ invertierbar, d.h. $\mathfrak{a}\mathfrak{b} = R$ mit einem gebrochenen Ideal $\mathfrak{b}$. Nach Definition von $(R : \mathfrak{a})$ gilt dann $\mathfrak{b} \subseteq (R : \mathfrak{a})$ und damit $R = \mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a}(R : \mathfrak{a}) \subseteq R$, also $\mathfrak{a}(R : \mathfrak{a}) = R$, wie behauptet. ■

Beispiel: $K = \mathbf{Q}(\alpha)$ mit $\alpha^2 = -11$ und $R = \mathbf{Z}[\alpha]$.

- Wir betrachten das Ideal $\mathfrak{a}_2 = \mathbf{Z}(\alpha + 1) + \mathbf{Z} \cdot 2$ mit Norm 2. Man berechnet

  $$(R : \mathfrak{a}_2) = \mathbf{Z}\frac{\alpha+1}{2} + \mathbf{Z} = \frac{1}{2}\mathfrak{a}_2 \quad \text{und damit} \quad \mathfrak{a}_2 \cdot (R : \mathfrak{a}_2) = \frac{1}{2}\mathfrak{a}_2^2 = \frac{1}{2}\mathfrak{a}_8 = \mathfrak{a}_2.$$

  Also ist $\mathfrak{a}_2$ nicht invertierbar.
- Für die Ideale $\mathfrak{a}_{3a} = (3, \alpha + 1)$, $\mathfrak{a}_{3b} + (3, \alpha + 2)$ gilt

  $$\mathfrak{a}_{3a}\mathfrak{a}_{3b} = (\alpha + 1, 3) \cdot (\alpha + 2, 3) = (3)$$

  und damit $\frac{1}{3}\mathfrak{a}_{3a}\mathfrak{a}_{3b} = R$, d.h. $\mathfrak{a}_{3a}$ und $\mathfrak{a}_{3b}$ sind invertierbare Ideale.

Wir stellen jetzt einige einfache Eigenschaften invertierbarer Ideale zusammen:

LEMMA. *Sei R Ordnung eines Zahlkörpers K.*

1. *Für gebrochene Ideale $\mathfrak{a}_i$ von R gilt:*

$$\mathfrak{a}_1\mathfrak{a}_2\dots\mathfrak{a}_r \text{ invertierbar} \iff \mathfrak{a}_i \text{ invertierbar für alle } i=1,\dots,r.$$

2. *Sind $\mathfrak{a},\mathfrak{b},\mathfrak{c}$ gebrochene Ideale von R und ist $\mathfrak{a}$ invertierbar, so gilt:*

$$\begin{aligned}\mathfrak{b}\subseteq\mathfrak{c} &\iff \mathfrak{ab}\subseteq\mathfrak{ac},\\ \mathfrak{b}\subsetneq\mathfrak{c} &\iff \mathfrak{ab}\subsetneq\mathfrak{ac},\\ \mathfrak{b}=\mathfrak{c} &\iff \mathfrak{ab}=\mathfrak{ac}.\end{aligned}$$

Beweis:

1. Ist $\mathfrak{a}_1\dots\mathfrak{a}_r$ invertierbar, so gibt es ein gebrochenes Ideal $\mathfrak{b}$ mit $\mathfrak{a}_1\dots\mathfrak{a}_r\mathfrak{b}=R$, also ist
$$\mathfrak{a}_i(\mathfrak{a}_1\dots\mathfrak{a}_{i-1}\mathfrak{a}_{i+1}\dots\mathfrak{a}_r\mathfrak{b})=R,$$
was die Invertierbarkeit von $\mathfrak{a}_i$ zeigt. Sind umgekehrt alle $\mathfrak{a}_i$ invertierbar, so gibt es gebrochene Ideale $\mathfrak{b}_i$ mit $\mathfrak{a}_i\mathfrak{b}_i=R$ und damit $(\mathfrak{a}_1\dots\mathfrak{a}_r)(\mathfrak{b}_1\dots\mathfrak{b}_r)=R$, was die Behauptung zeigt.
2. Aus $\mathfrak{b}\subseteq\mathfrak{c}$ folgt durch Multiplikation mit $\mathfrak{a}$ sofort $\mathfrak{ab}\subseteq\mathfrak{ac}$. Umgekehrt folgt aus $\mathfrak{ab}\subseteq\mathfrak{ac}$ durch Multiplikation mit $\mathfrak{a}^{-1}$ wegen $\mathfrak{aa}^{-1}=R$ sofort $\mathfrak{b}=\mathfrak{a}^{-1}\mathfrak{ab}\subseteq\mathfrak{a}^{-1}\mathfrak{ac}=\mathfrak{c}$. Die anderen Aussagen ergeben sich genauso durch Multiplikation mit $\mathfrak{a}$ bzw. $\mathfrak{a}^{-1}$ und der Beziehung $\mathfrak{aa}^{-1}=R$. ■

Das folgende Lemma führt eine gebräuchliche Sprechweise ein:

LEMMA. *Sei R Ordnung eines Zahlkörpers, seien $\mathfrak{a},\mathfrak{b}$ Ideale mit*

$$\mathfrak{b}\subseteq\mathfrak{a}\subseteq R \quad \textit{und} \quad \mathfrak{a} \quad \textit{invertierbar.}$$

Dann ist $\mathfrak{c}=\mathfrak{ba}^{-1}$ ein ganzes Ideal mit

$$\mathfrak{b}=\mathfrak{ca}=(\mathfrak{ba}^{-1})\mathfrak{a}.$$

Man sagt, $\mathfrak{a}$ teilt $\mathfrak{b}$, und schreibt $\mathfrak{a}|\mathfrak{b}$.

Beweis: Aus $\mathfrak{b}\subseteq\mathfrak{a}$ folgt durch Multiplikation mit $\mathfrak{a}^{-1}$ die Beziehung

$$\mathfrak{c}=\mathfrak{ba}^{-1}\subseteq\mathfrak{aa}^{-1}=R,$$

also ist $\mathfrak{c}$ ein ganzes Ideal und $\mathfrak{a}=\mathfrak{ca}$, wie behauptet. ■

8. Die Multiplikativität der Norm

Wir beginnen mit ein paar einfachen Bemerkungen.

LEMMA. *Sind $\mathfrak{a}$ und $\mathfrak{b}$ teilerfremde Ideale einer Ordnung R, so gilt:*

$$\mathrm{N}(\mathfrak{ab})=\mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b}).$$

Beweis: Der chinesische Restsatz liefert

$$R/\mathfrak{ab}\simeq R/\mathfrak{a}\oplus R/\mathfrak{b},$$

was sofort

$$\mathrm{N}(\mathfrak{ab})=[R:\mathfrak{ab}]=\#R/\mathfrak{ab}=\#R/\mathfrak{a}\cdot\#R/\mathfrak{b}=[R:\mathfrak{a}]\cdot[R:\mathfrak{b}]=\mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b})$$

liefert. ■

LEMMA. *Ist $\mathfrak{a}$ Ideal einer Ordnung R und $\mathrm{N}\mathfrak{a}=bc$ mit $b,c\in\mathbf{N}$ und $\mathrm{ggT}(b,c)=1$, so gilt für $\mathfrak{b}=\mathfrak{a}+Rb$, $\mathfrak{c}=\mathfrak{a}+Rc$*

$$\mathfrak{a}=\mathfrak{bc},\quad \mathfrak{a}+\mathfrak{b}=R,\quad \mathrm{N}\mathfrak{b}=b,\quad \mathrm{N}\mathfrak{c}=c.$$

Beweis: Wegen $bc = \mathrm{N}\mathfrak{a} \in \mathfrak{a}$ gilt

$$\mathfrak{bc} = (\mathfrak{a} + Rb)(\mathfrak{a} + Rc) = \mathfrak{a}^2 + b\mathfrak{a} + c\mathfrak{a} + Rbc \subseteq \mathfrak{a} + R\mathrm{N}\mathfrak{a} \subseteq \mathfrak{a}.$$

Wegen $\mathrm{ggT}(b, c) = 1$ gibt es $u, v \in \mathbf{Z}$ mit $1 = bu + cv$. Daher gilt für $\lambda \in \mathfrak{a}$ zunächst $\lambda bu \in \mathfrak{ab} \subseteq \mathfrak{bc}$, $\lambda vc \in \mathfrak{ac} \subseteq \mathfrak{bc}$, also

$$\lambda = \lambda bu + \lambda cv \in \mathfrak{bc},$$

was $\mathfrak{a} \subseteq \mathfrak{bc}$ und damit die Gleichheit $\mathfrak{a} = \mathfrak{bc}$ beweist. Aus $1 = bu + cv$ folgt natürlich sofort $\mathfrak{b} + \mathfrak{c} = R$. Das letzte Lemma liefert daher

$$bc = \mathrm{N}\mathfrak{a} = \mathrm{N}\mathfrak{b} \cdot \mathrm{N}\mathfrak{c}.$$

Nun folgt aus $Rb \subseteq \mathfrak{b}$

$$b^n = [R : Rb] = [R : \mathfrak{b}][\mathfrak{b} : Rb] = \mathrm{N}\mathfrak{b} \cdot [\mathfrak{b} : Rb], \quad \text{also} \quad \mathrm{N}\mathfrak{b} | b^n.$$

Analog erhält man $\mathrm{N}\mathfrak{c} | c^n$. Wegen $\mathrm{ggT}(b, c) = 1$ folgt hieraus sofort $\mathrm{N}\mathfrak{b} = b$ und $\mathrm{N}\mathfrak{c} = c$, wie behauptet. ■

Mit dem letzten Lemma erhält man durch Induktion sofort folgenden Zerlegungssatz für Ideale:

Satz. *Sei $\mathfrak{a} \neq 0$ Ideal einer Ordnung R und*

$$\mathrm{N}\mathfrak{a} = p_1^{e_1} \dots p_r^{e_r}$$

die Primfaktorzerlegung der Norm. Dann gilt mit $\mathfrak{q}_i = \mathfrak{a} + Rp_i^{e_i}$

$$\mathfrak{a} = \mathfrak{q}_1 \dots \mathfrak{q}_r, \quad \mathrm{N}(\mathfrak{q}_i) = p_i^{e_i} \quad \textit{und} \quad \mathfrak{q}_i + \mathfrak{q}_j = R \textit{ für } i \neq j.$$

Leider muss die Idealnorm im Allgemeinen nicht multiplikativ sein, wie folgendes Beispiel zeigt:

Beispiel: In der Ordnung $\mathbf{Z}[\alpha]$ mit $\alpha^2 = -11$ gilt für das Ideal $\mathfrak{a}_2 = (2, \alpha + 1)$ die Beziehung

$$\mathfrak{a}_2^2 = \mathfrak{a}_8 = 2\mathfrak{a}_2 \quad \text{und} \quad \mathrm{N}(\mathfrak{a}_2) = 2, \quad \mathrm{N}(\mathfrak{a}_8) = 8, \quad \text{also} \quad \mathrm{N}(\mathfrak{a}_2\mathfrak{a}_2) \neq \mathrm{N}(\mathfrak{a}_2)N(\mathfrak{a}_2).$$

Allerdings erhält man die Multiplikativität unter einer zusätzlichen Voraussetzung:

Satz. *Sei R Ordnung eines Zahlkörpers und seinen $\mathfrak{a}, \mathfrak{b}$ gebrochene Ideale in R. Ist $\mathfrak{a}$ invertierbar, so gilt für die Idealnormen*

$$\mathrm{N}(\mathfrak{ab}) = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b}).$$

Wir benötigen zum Beweis des Satzes ein Lemma:

Lemma. *Sei R eine Ordnung, $\mathfrak{a}$ ein gebrochenes invertierbares Ideal, $\mathfrak{b} \subsetneq \mathfrak{c}$ gebrochene Ideale mit*

$$\{\mathfrak{d} \textit{ gebrochenes Ideal } : \mathfrak{b} \subsetneq \mathfrak{d} \subsetneq \mathfrak{c}\} = \emptyset,$$

(d.h. zwischen $\mathfrak{b}$ und $\mathfrak{c}$ gibt es keine weiteren gebrochenen Ideale). Dann gilt

$$\mathfrak{c}/\mathfrak{b} \simeq \mathfrak{ac}/\mathfrak{ab}, \quad \textit{also insbesondere} \quad [\mathfrak{c} : \mathfrak{b}] = [\mathfrak{ac} : \mathfrak{ab}].$$

Beweis:

1. Man wähle $c \in \mathfrak{c} \setminus \mathfrak{b}$. Dann ist $\mathfrak{b} \subsetneq \mathfrak{b} + Rc \subseteq \mathfrak{c}$ und daher nach Voraussetzung $\mathfrak{c} = \mathfrak{b} + Rc$. Also ist die Abbildung

   $$f : R \to \mathfrak{c}/\mathfrak{b}, \quad \lambda \mapsto \lambda c \bmod \mathfrak{b}$$

   surjektiv. Definiert man ein Ideal $(\mathfrak{b} : \mathfrak{c})_R$ durch

   $$(\mathfrak{b} : \mathfrak{c})_R = \{\lambda \in R : \lambda\mathfrak{c} \subseteq \mathfrak{b}\},$$

   so folgt für den Kern von f für $\lambda \in R$:

   $$\lambda \in Kern(f) \iff \lambda c \in \mathfrak{b} \iff \lambda(\mathfrak{b} + Rc) \subseteq \mathfrak{b} \iff \lambda\mathfrak{c} \subseteq \mathfrak{b} \iff \lambda \in (\mathfrak{b} : \mathfrak{c})_R.$$

   Der Homomorphiesatz liefert nun

   $$R/(\mathfrak{b} : \mathfrak{c})_R \simeq \mathfrak{c}/\mathfrak{b}.$$

2. Da $\mathfrak{a}$ invertierbar ist, gilt auch für $\mathfrak{ab}$ und $\mathfrak{ac}$ die Beziehung $\mathfrak{ab} \subsetneq \mathfrak{ac}$ und
$$\{\mathfrak{d} \text{ gebrochenes Ideal } : \mathfrak{ab} \subsetneq \mathfrak{d} \subsetneq \mathfrak{ac}\} = \emptyset.$$
Also folgt wie in 1. die Aussage
$$R/(\mathfrak{ab} : \mathfrak{ac})_R \simeq \mathfrak{ac}/\mathfrak{ab}.$$
3. Nun gilt wegen der Invertierbarkeit von $\mathfrak{a}$ für $\lambda \in R$:
$$\lambda \in (\mathfrak{b} : \mathfrak{c})_R \iff \lambda\mathfrak{c} \subseteq \mathfrak{b} \iff \lambda\mathfrak{ac} \subseteq \mathfrak{ab} \iff \lambda \in (\mathfrak{ab} : \mathfrak{ac})_R,$$
also $(\mathfrak{ab} : \mathfrak{ac})_R = (\mathfrak{b} : \mathfrak{c})_R$. Mit den Aussagen aus 1. und 2. folgt die Behauptung. ■

LEMMA. *Sei R eine Ordnung, $\mathfrak{a}$ ein gebrochenes invertierbares Ideal, $\mathfrak{b}, \mathfrak{c}$ gebrochene Ideale mit $\mathfrak{b} \subseteq \mathfrak{c}$. Dann gilt für die Indizes:*
$$[\mathfrak{ac} : \mathfrak{ab}] = [\mathfrak{c} : \mathfrak{b}].$$

Beweis: Da es nur endlich viele abelsche Gruppen zwischen $\mathfrak{b}$ und $\mathfrak{c}$ gibt, kann man eine Kette von gebrochenen Idealen
$$\mathfrak{b} = \mathfrak{b}_0 \subsetneq \mathfrak{b}_1 \subsetneq \mathfrak{b}_2 \subsetneq \cdots \subsetneq \mathfrak{b}_r = \mathfrak{c}$$
wählen mit
$$\{\mathfrak{d} \text{ gebrochenes Ideal } : \mathfrak{b}_i \subsetneq \mathfrak{d} \subsetneq \mathfrak{b}_{i+1}\} = \emptyset.$$
Das letzte Lemma ergibt also $[\mathfrak{ab}_{i+1} : \mathfrak{ab}_i] = [\mathfrak{b}_{i+1} : \mathfrak{b}_i]$ und damit
$$[\mathfrak{ac} : \mathfrak{ab}] = [\mathfrak{ab}_r : \mathfrak{ab}_{r-1}] \ldots [\mathfrak{ab}_2 : \mathfrak{ab}_1][\mathfrak{ab}_1 : \mathfrak{ab}_0] = [\mathfrak{b}_r : \mathfrak{b}_{r-1}] \ldots [\mathfrak{b}_2 : \mathfrak{b}_1][\mathfrak{b}_1 : \mathfrak{b}_0] = [\mathfrak{c} : \mathfrak{b}],$$
wie behauptet. ■

Wir können nun den Satz über die Multiplikativität der Norm beweisen:

Beweis des Satzes über die Multiplikativität der Norm: Es gilt mit dem letzten Lemma
$$N(\mathfrak{ab}) = [R : \mathfrak{ab}] = [R : \mathfrak{a}][\mathfrak{a} : \mathfrak{ab}] = N(\mathfrak{a})[\mathfrak{a}R : \mathfrak{ab}] = N(\mathfrak{a})[R : \mathfrak{b}] = N(\mathfrak{a})N(\mathfrak{b}),$$
wie behauptet. ■

Bemerkung: Sind $\mathfrak{b} \subseteq \mathfrak{c}$ Ideale einer Ordnung R, so muß nicht
$$R/(\mathfrak{b} : \mathfrak{c})_R \simeq \mathfrak{c}/\mathfrak{b}$$
gelten.

9. Invertierbarkeit von Primidealen

Motivation: Ist $a = a_0$ eine natürliche Zahl und p_1 eine Primzahl mit $p_1 | a_0$, dann kann man schreiben $a = a_1 p_1$ mit der natürlichen Zahl $a_1 = a_0 p_1^{-1}$. Iteriert man diesen Prozess, so findet man eine Darstellung $a = a_r p_1 p_2 \ldots p_r$ mit Primzahlen p_i und $1 \leq a_r < a_{r-1} < \cdots < a_1 < a$. Nach endlichen vielen Schritten hat man dann $a_r = 1$ und damit die Primfaktorzerlegung von a.
Ähnlich wollen wir nun mit Idealen in Ordnungen von Zahlkörpern vorgehen: Ist $\mathfrak{a}$ ein Ideal, $\mathfrak{p}$ ein invertierbares Primideal mit $\mathfrak{p} | \mathfrak{a}$, d.h. $\mathfrak{a} \subseteq \mathfrak{p}$, so ist $\mathfrak{b} = \mathfrak{ap}^{-1}$ ein ganzes Ideal mit $\mathfrak{a} = \mathfrak{bp}$ und $\mathrm{N}(\mathfrak{a}) = \mathrm{N}(\mathfrak{b})\mathrm{N}(\mathfrak{p}) > \mathrm{N}(\mathfrak{b})$. Durch Iteration kann man versuchen, $\mathfrak{a}$ als Produkt von Primidealen darzustellen.

Das folgende Beispiel zeigt, wie man leicht an invertierbare Primideale kommt.

Beispiel: Sei R Ordnung eines Zahlkörpers K und $\alpha \in R$ mit Minimalpolynom $f(x) \in \mathbf{Z}[x]$, so dass $K = \mathbf{Q}(\alpha)$ gilt. Sei p eine Primzahl mit $\mathrm{disc}\,(f) \not\equiv 0 \bmod p$. Ist dann
$$f(x) \equiv g_1(x) \ldots g_r(x) \bmod p$$
die Primfaktorzerlegung von $f(x)$ modulo p, so sind $\mathfrak{p}_i = (p, g_i(\alpha))$ die p enthaltenden Primideale von R und es gilt
$$(p) = \mathfrak{p}_1 \ldots \mathfrak{p}_r, \quad \text{also} \quad \frac{1}{p}\mathfrak{p}_1 \ldots \mathfrak{p}_r = R,$$

was sofort die Invertierbarkeit der $\mathfrak{p}_i$ zeigt zusammen mit der Darstellung

$$\mathfrak{p}_i^{-1} = \frac{1}{p}\prod_{j\neq i}\mathfrak{p}_i.$$

Leider ist man nicht immer in der schönen Situation des Beispiels. Wir werden im folgenden einige Hilfsaussagen für den Allgemeinfall zusammenstellen.

LEMMA. *Ist $\mathfrak{p}$ ein die Primzahl p enthaltendes Primideal einer Ordnung R, so gilt*

$$R \subsetneq (R:\mathfrak{p}) \subseteq \frac{1}{p}R,$$

d.h. es gibt $\lambda \in K$ mit

$$\lambda \notin R \quad \textit{und} \quad \lambda\mathfrak{p} \subseteq R.$$

Beweis: Aus $p\cdot(R:\mathfrak{p}) \subseteq \mathfrak{p}\cdot(R:\mathfrak{p}) \subseteq R$ folgt die zweite Inklusion. Sind $\mathfrak{p},\mathfrak{p}_2,\ldots,\mathfrak{p}_r$ die p enthaltenden Primideale, so haben wir gesehen, dass $(\mathfrak{p}\mathfrak{p}_2\ldots\mathfrak{p}_r)^n \subseteq Rp$ gilt, wenn n den Grad des Zahlkörpers bezeichnet. Also gibt es eine Darstellung

$$\mathfrak{p}^e\mathfrak{p}_2^{e_2}\ldots\mathfrak{p}_r^{e_r} \subseteq Rp \quad \text{mit} \quad e,e_2,\ldots,e_r \geq 0.$$

Wir wählen eine Darstellung mit minimalem Wert $e+e_2+\cdots+e_r$. Wegen $p\in\mathfrak{p}$ folgt $\mathfrak{p}^e\mathfrak{p}_2^{e_2}\ldots\mathfrak{p}_r^{e_r} \subseteq \mathfrak{p}$ und damit $e\geq 1$. Die Minimalität liefert $\mathfrak{p}^{e-1}\mathfrak{p}_2^{e_2}\ldots\mathfrak{p}_r^{e_r} \not\subseteq Rp$. Wir wählen $\alpha \in \mathfrak{p}^{e-1}\mathfrak{p}_2^{e_2}\ldots\mathfrak{p}_r^{e_r}$, $\alpha\notin Rp$. Es folgt $\frac{\alpha}{p}\notin R$ und dann $\alpha\mathfrak{p} \subseteq \mathfrak{p}^e\mathfrak{p}_2^{e_2}\ldots\mathfrak{p}_r^{e_r} \subseteq Rp$, also $\frac{\alpha}{p}\mathfrak{p}\subseteq R$, d.h. $\frac{\alpha}{p}\in(R:\mathfrak{p})$. Mit $\lambda=\frac{\alpha}{p}$ folgt die Behauptung. ■

SATZ. *Sei $\mathfrak{p}\neq 0$ Primideal einer Ordnung R eines Zahlkörpers K und $\lambda\in K$ mit $\lambda\notin R$, $\lambda\mathfrak{p}\subseteq R$. Dann sind folgende Aussagen äquivalent:*

1. *$\mathfrak{p}$ ist invertierbar, d.h. $\mathfrak{p}\cdot(R:\mathfrak{p}) = R$. (Dann ist $\mathfrak{p}^{-1} = (R:\mathfrak{p}) = R+\lambda R$.)*
2. *$\lambda\mathfrak{p} \not\subseteq \mathfrak{p}$.*
3. *Es gibt $\pi\in\mathfrak{p}$ und $s\in R\setminus\mathfrak{p}$ mit $\mathfrak{p}\subseteq R\frac{\pi}{s}$.*
4. *Es gibt $\pi\in\mathfrak{p}$ mit $\mathfrak{p} = R\pi+\mathfrak{p}^2$.*
5. *$\mathfrak{p}/\mathfrak{p}^2$ ist 1-dimensionaler $R/\mathfrak{p}$-Vektorraum.*
6. *$\mathrm{N}(\mathfrak{p}^2) = (\mathrm{N}\mathfrak{p})^2$.*

Beweis:

$1\Longrightarrow 2$: Aus $R\subsetneq R+\lambda R$ folgt durch Multiplikation mit dem invertierbaren Primideal $\mathfrak{p}$ die Inklusion

$$\mathfrak{p} = \mathfrak{p}\cdot R \subsetneq \mathfrak{p}\cdot(R+\lambda R) = \mathfrak{p}+\lambda\mathfrak{p},$$

was sofort $\lambda\mathfrak{p}\not\subseteq\mathfrak{p}$ impliziert.

$2\Longrightarrow 1$: Es gilt

$$\mathfrak{p} \subsetneq \mathfrak{p}+\lambda\mathfrak{p} = \mathfrak{p}\cdot(R+\lambda R) \subseteq R.$$

Da $\mathfrak{p}$ maximales Ideal ist, folgt

$$\mathfrak{p}\cdot(R+\lambda R) = R,$$

also ist $\mathfrak{p}$ invertierbar und es gilt die Formel

$$\mathfrak{p}^{-1} = (R:\mathfrak{p}) = R+\lambda R.$$

$2\Longrightarrow 3$: Wegen $\lambda\mathfrak{p}\subseteq R$, $\lambda\mathfrak{p}\not\subseteq\mathfrak{p}$ gibt es ein $\pi\in\mathfrak{p}$ mit $\lambda\pi\notin\mathfrak{p}$, aber $\lambda\pi\in R$. Setze $s=\lambda\pi$. Dann ist $s\in R\setminus\mathfrak{p}$ und

$$\mathfrak{p} = \frac{\pi}{s}\lambda\mathfrak{p} \subseteq \frac{\pi}{s}R.$$

$3\Longrightarrow 2$: Die Inklusion $\mathfrak{p}\subseteq R\frac{\pi}{s}$ liefert $\frac{s}{\pi}\mathfrak{p}\subseteq R$. Aus $\frac{s}{\pi}\pi = s\notin\mathfrak{p}$ folgt $\frac{s}{\pi}\mathfrak{p}\not\subseteq\mathfrak{p}$. Dann gilt aber

$$\mathfrak{p} \subsetneq \mathfrak{p}+\frac{s}{\pi}\mathfrak{p} = \mathfrak{p}(R+R\frac{s}{\pi}) \subseteq R,$$

also $\mathfrak{p}(R+R\frac{s}{\pi}) = R$, d.h. $\mathfrak{p}$ ist invertierbar.

$3 \Longrightarrow 4$: $\mathfrak{p} \subseteq R\frac{\pi}{s}$ liefert $s\mathfrak{p} \subseteq R\pi$. Da $R/\mathfrak{p}$ ein Körper ist, gibt es wegen $s \not\equiv 0 \bmod \mathfrak{p}$ ein $t \in R$ mit $1 \equiv st \bmod \mathfrak{p}$, also $1 = st + \widetilde{\pi}$ mit $\widetilde{\pi} \in \mathfrak{p}$. Wir haben nun

$$R\pi + \mathfrak{p}^2 \subseteq \mathfrak{p} = (st + \widetilde{\pi})\mathfrak{p} \subseteq ts\mathfrak{p} + \widetilde{\pi}\mathfrak{p} \subseteq tR\pi + \mathfrak{p}^2 \subseteq R\pi + \mathfrak{p}^2,$$

was sofort $\mathfrak{p} = R\pi + \mathfrak{p}^2$ zeigt.

$4 \Longrightarrow 3$: Sei $\mathfrak{p} = (\pi_1, \ldots, \pi_r)$. Jedes Element aus $\mathfrak{p}^2$ läßt sich schreiben als $\sum_{j=1}^{r} \mu_j \pi_j$ mit $\mu_j \in \mathfrak{p}$, also erhält man wegen $\mathfrak{p} = R\pi + \mathfrak{p}^2$ eine Darstellung

$$\pi_i = a_i \pi + \sum_{j=1}^{r} \mu_{ij} \pi_j \quad \text{mit} \quad a_i \in R, \mu_{ij} \in \mathfrak{p}.$$

In Matrizenschreibweise ergibt sich

$$\begin{pmatrix} \pi_1 \\ \vdots \\ \pi_r \end{pmatrix} = \begin{pmatrix} a_1 \\ \vdots \\ a_r \end{pmatrix} \pi + \begin{pmatrix} \mu_{11} & \cdots & \mu_{1r} \\ \vdots & & \vdots \\ \mu_{r1} & \cdots & \mu_{rr} \end{pmatrix} \begin{pmatrix} \pi_1 \\ \vdots \\ \pi_r \end{pmatrix}.$$

Setzt man $M = (\mu_{ij})_{ij}$, so wird

$$(I_r - M) \begin{pmatrix} \pi_1 \\ \vdots \\ \pi_r \end{pmatrix} = \begin{pmatrix} a_1 \\ \vdots \\ a_r \end{pmatrix} \pi.$$

Sei $(I_r - M)[i,j]$ die Untermatrix von $I_r - M$, die durch Streichen der i-ten Zeile und j-ten Spalte entsteht. Definiert man eine Matrix N durch

$$N = \left((-1)^{i+j} \det((I_r - M)[i,j])\right)_{i,j=1,\ldots,r},$$

so gilt

$$N^t(I_r - M) = \det(I_r - M) \cdot I_r.$$

Natürlich hat N Einträge aus R. Definiert man $s = \det(I_r - M)$, so folgt sofort $s \equiv 1 \bmod \mathfrak{p}$ wegen $\mu_{ij} \in \mathfrak{p}$, also $s \in R \setminus \mathfrak{p}$. Multiplikation obiger Matrizengleichung mit N^t ergibt dann

$$s \begin{pmatrix} \pi_1 \\ \vdots \\ \pi_r \end{pmatrix} = N^t \begin{pmatrix} a_1 \\ \vdots \\ a_r \end{pmatrix} \pi$$

und damit $s\pi_i \in R\pi$, also $s\mathfrak{p} \subseteq R\pi$, wie behauptet.

$4 \Longrightarrow 5$: Aus $\mathfrak{p} = R\pi + \mathfrak{p}^2$ folgt, dass $\overline{\pi} = \pi + \mathfrak{p}^2$ den $R/\mathfrak{p}$-Vektorraum $\mathfrak{p}/\mathfrak{p}^2$ erzeugt, also ist $\mathfrak{p}/\mathfrak{p}^2$ höchstens 1-dimensional. Wegen $\mathfrak{p} \neq \mathfrak{p}^2$ ist $\mathfrak{p}/\mathfrak{p}^2$ tatsächlich 1-dimensional.

$5 \Longrightarrow 4$: Wählt man $\pi \in \mathfrak{p}$ mit $\mathfrak{p}/\mathfrak{p}^2 = R/\mathfrak{p} \cdot \overline{\pi}$ (als R/pp-Vektorraum), so folgt sofort $\mathfrak{p} = R\pi + \mathfrak{p}^2$.

$5 \iff 6$: Dies folgt mit $\#R/\mathfrak{p} = \mathrm{N}\mathfrak{p}$ sofort aus der Beziehung

$$\mathrm{N}(\mathfrak{p}^2) = [R : \mathfrak{p}^2] = [R : \mathfrak{p}][\mathfrak{p} : \mathfrak{p}^2] = \mathrm{N}(\mathfrak{p}) \cdot \#\mathfrak{p}/\mathfrak{p}^2. \quad \blacksquare$$

Beispiel: In $R = \mathbf{Z}[\alpha]$ mit $\alpha^2 = -11$ betrachten wir das Primideal $\mathfrak{p} = (2, \alpha + 1)$ mit Norm 2. Wir wählen $\lambda = \frac{\alpha+1}{2} \notin R$ und erhalten

$$\lambda \cdot 2 = \alpha + 1, \quad \lambda \cdot \alpha = -5 + \alpha,$$

also $\lambda\mathfrak{p} \subseteq \mathfrak{p}$, d.h. $\mathfrak{p}$ ist nicht invertierbar.

Für Anwendungen ist es wichtig, für ein Primideal $\mathfrak{p} \neq 0$ ein $\lambda_\mathfrak{p}$ zu finden mit $\lambda_\mathfrak{p} \in K \setminus R$, $\lambda_\mathfrak{p}\mathfrak{p} \subseteq R$. Wir geben dafür zwei Methoden an:

SATZ. *Sei R Ordnung eines Zahlkörpers K und p eine Primzahl. Sei weiter $\mathbf{Z}[\alpha] \subseteq R$ eine Ordnung, sodass p teilerfremd zum Index von $\mathbf{Z}[\alpha]$ in R ist, d.h.* $\mathrm{ggT}(p, [R : \mathbf{Z}[\alpha]) = 1$. *Faktorisiert man das Minimalpolynom $f(x)$ von α modulo p*

$$f(x) \equiv g_1(x)^{e_1} \ldots g_r(x)^{e_r} \bmod p$$

(mit normierten modulo p paarweise teilerfremden und modulo p irreduziblen Polynomen $g_i(x)$), so sind die p enthaltenden Primideale von R durch

$$\mathfrak{p}_i = (p, g_i(\alpha)), \quad i = 1, \ldots, r$$

gegeben. Definiert man

$$h_i(x) = g_1(x)^{e_1} \ldots g_{i-1}(x)^{e_{i-1}} g_i(x)^{e_i - 1} g_{i+1}(x)^{e_{i+1}} \ldots g_r(x)^{e_r} = \frac{1}{g_i(x)} \prod_{j=1}^{r} g_j(x)^{e_j}$$

und setzt man

$$\lambda_i = \frac{h_i(\alpha)}{p} \in K,$$

so gilt

$$\lambda_i \notin R, \quad \lambda_i \mathfrak{p}_i \subseteq R.$$

Beweis: Die Aussagen über die Primideale $\mathfrak{p}_i$ wurden bereits früher gezeigt.

1. Sei n der Grad des Zahlkörpers. Dann ist $h_i(x)$ ein normiertes Polynom vom Grad $< n$, also gilt $\lambda_i = \frac{h_i(\alpha)}{p} \notin \mathbf{Z}[\alpha]$, aber natürlich $p\lambda_i \in \mathbf{Z}[\alpha]$. Wäre $\lambda_i \in R$, so würde $[R : \mathbf{Z}[\alpha]] \cdot \lambda_i \in \mathbf{Z}[\alpha]$ folgen, was mit $p\lambda_i \in \mathbf{Z}[\alpha]$ und $\mathrm{ggT}(p, [R : \mathbf{Z}[\alpha]) = 1$ den Widerspruch $\lambda_i \in \mathbf{Z}[\alpha]$ liefern würde. Also muss $\lambda_i \notin R$ gelten.
2. Es gibt ein Polynom $h(x) \in \mathbf{Z}[x]$ mit
$$f(x) = g_1(x)^{e_1} \ldots g_r(x)^{e_r} + ph(x) = g_i(x)h_i(x) + ph(x),$$
was mit $f(\alpha) = 0$ sofort $g_i(\alpha)h_i(\alpha) \in pR$, also $\lambda_i \cdot g_i(\alpha) \in R$ liefert. Da auch $\lambda_i \cdot p = h_i(\alpha) \in R$ gilt, folgt schließlich $\lambda_i \mathfrak{p}_i \subseteq R$. ■

LEMMA. *Sei R Ordnung eines Zahlkörpers mit $\mathbf{Z}$-Basis $\omega_1, \ldots, \omega_n$ und $\mathfrak{p} = (\alpha_1, \ldots, \alpha_r) \neq 0$ ein Primideal in R, das die Primzahl p enthält. Seien $A_{ijk} \in \mathbf{Z}$ mit*

$$\omega_i \alpha_j = \sum_{k=1}^{n} A_{ijk} \omega_k \quad \textit{für alle } i, j.$$

Dann gibt es ein $(x_1, \ldots, x_n) \in \{0, 1, \ldots, p-1\}^n \setminus \{(0, \ldots, 0\}$ mit

$$\sum_{i=1}^{n} x_i A_{ijk} \equiv 0 \bmod p \quad \textit{für} \quad j = 1, \ldots, r, \quad k = 1, \ldots, n.$$

Setzt man

$$\lambda = \frac{1}{p} \sum_{i=1}^{n} x_i \omega_i \quad \textit{mit} \quad x_i \in \{0, 1, \ldots, p-1\},$$

so gilt

$$\lambda \notin R, \quad \lambda \mathfrak{p} \subseteq R.$$

Beweis: Wir wissen, dass ein $\lambda \in K$ existiert mit $\lambda \notin R$, $\lambda \mathfrak{p} \subseteq R$. Wegen $p \in \mathfrak{p}$ gilt $\lambda \cdot p \in R$, d.h. man kann ansetzen $\lambda = \frac{1}{p} \sum_{i=1}^{n} x_i \omega_i$. Da man λ um Elemente aus R abändern kann, kann man o.E. $0 \leq x_i \leq p-1$ annehmen. Wegen

$$\lambda \alpha_j = \frac{1}{p} \sum_{i=1}^{n} x_i \omega_i \alpha_j = \frac{1}{p} \sum_{i=1}^{n} \sum_{k=1}^{n} x_i A_{ijk} \omega_k = \frac{1}{p} \sum_{k=1}^{n} \left(\sum_{i=1}^{n} x_i A_{ijk} \right) \omega_k = \sum_{k=1}^{n} \left(\frac{1}{p} \sum_{i=1}^{n} x_i A_{ijk} \right) \omega_k$$

ist die Bedingung $\lambda \mathfrak{p} \subseteq R$ äquivalent mit

$$\sum_{i=1}^{n} x_i A_{ijk} \equiv 0 \bmod p \quad \text{für} \quad j = 1, \ldots, r, \quad k = 1, \ldots, n.$$

Da wir bereits allgemein bewiesen haben, dass ein λ existiert, folgt, dass das angegebene Gleichungssystem wegen $\lambda \notin R$ eine nichttriviale Lösung hat und damit die Behauptung. ■

Nach diesen etwas länglichen technischen Vorbereitungen kommen wir zu einem zentralen Punkt: Wir imitieren das Herausdividieren einer Primzahl aus einer natürlichen Zahl:

SATZ. *Sei $\mathfrak{a}$ ein von 0 verschiedenenes Ideal einer Ordnung R. Ist $\mathfrak{p}$ ein invertierbares Primideal von R, so gibt es eine eindeutige Zerlegung*

$$\mathfrak{a} = \mathfrak{b}\mathfrak{p}^v,$$

wo $\mathfrak{b}$ ein Ideal ist mit $\mathfrak{b} \not\subseteq \mathfrak{p}$ und $v \in \mathbf{N}_0$. Der Exponent v wird auch mit $v_\mathfrak{p}(\mathfrak{a})$ bezeichnet und als Bewertung von $\mathfrak{a}$ in $\mathfrak{p}$ bezeichnet.

Beweis: Existenz: Gilt $\mathfrak{a} \not\subseteq \mathfrak{p}$, so setzen wir $\mathfrak{b} = \mathfrak{a}$, $v = 0$. Es gelte jetzt $\mathfrak{a} \subseteq \mathfrak{p}$. Da $\mathfrak{p}$ invertierbar ist, können wir schreiben $\mathfrak{a} = \mathfrak{a}_1\mathfrak{p}$ mit dem ganzen Ideal $\mathfrak{a}_1 = \mathfrak{a}\mathfrak{p}^{-1}$. Außerdem gilt $\mathrm{N}(\mathfrak{a}) = \mathrm{N}(\mathfrak{a}_1)\mathrm{N}(\mathfrak{p}) > \mathrm{N}(\mathfrak{a}_1)$. Man macht nun mit $\mathfrak{a}_1$ weiter und erhält sukzessive

$$\mathfrak{a} = \mathfrak{a}_1\mathfrak{p} = \mathfrak{a}_2\mathfrak{p}^2 = \mathfrak{a}_3\mathfrak{p}^3 = \cdots = \mathfrak{a}_v\mathfrak{p}^v \quad \text{und} \quad \mathrm{N}(\mathfrak{a}) > \mathrm{N}(\mathfrak{a}_1) > \mathrm{N}(\mathfrak{a}_2) > \mathrm{N}(\mathfrak{a}_3) > \cdots > \mathrm{N}(\mathfrak{a}_v).$$

Da die Norm echt abnimmt, muss der Prozess aufhören, d.h. wir erhalten irgendwann $\mathfrak{a}_v \not\subseteq \mathfrak{p}$ und damit die gewünschte Darstellung.
Eindeutigkeit: Es gelte

$$\mathfrak{a} = \mathfrak{b}\mathfrak{p}^v = \mathfrak{c}\mathfrak{p}^w \quad \text{mit} \quad \mathfrak{b} \not\subseteq \mathfrak{p}, \mathfrak{c} \not\subseteq \mathfrak{p}.$$

Sei o.E. $v \le w$. Wir multiplizieren zuerst mit $\mathfrak{p}^{-v} = (\mathfrak{p}^{-1})^v$ und erhalten

$$\mathfrak{b} = \mathfrak{c}\mathfrak{p}^{w-v}.$$

Nun ist $\mathfrak{b} \not\subseteq \mathfrak{p}$ und damit $\mathfrak{c}\mathfrak{p}^{w-v} \not\subseteq \mathfrak{p}$, was sofort $w = v$ und $\mathfrak{b} = \mathfrak{c}$ liefert. ■

LEMMA. *Sei $\mathfrak{p}$ ein invertierbares Primideal einer Ordnung R. Dann gilt für von 0 verschiedene Ideale $\mathfrak{a}$ und $\mathfrak{b}$ in R:*

1. $v_\mathfrak{p}(\mathfrak{a}\mathfrak{b}) = v_\mathfrak{p}(\mathfrak{a}) + v_\mathfrak{p}(\mathfrak{b})$.
2. $v_\mathfrak{p}(\mathfrak{a} + \mathfrak{b}) = \min(v_\mathfrak{p}(\mathfrak{a}), v_\mathfrak{p}(\mathfrak{b}))$.
3. $v_\mathfrak{p}(\mathfrak{a} \cap \mathfrak{b}) = \max(v_\mathfrak{p}(\mathfrak{a}), v_\mathfrak{p}(\mathfrak{b}))$.

Beweis: Wir schreiben $\mathfrak{a} = \mathfrak{a}_0\mathfrak{p}^v$ und $\mathfrak{b} = \mathfrak{b}_0\mathfrak{p}^w$ mit $v = v_\mathfrak{p}(\mathfrak{a})$ und $w = v_\mathfrak{p}(\mathfrak{b})$, insbesondere $\mathfrak{a}_0 \not\subseteq \mathfrak{p}$ und $\mathfrak{b}_0 \not\subseteq \mathfrak{p}$.

1. Es ist
$$\mathfrak{a}\mathfrak{b} = \mathfrak{a}_0\mathfrak{b}_0\mathfrak{p}^{v+w}.$$
Die Primidealeigenschaft von $\mathfrak{p}$ liefert $\mathfrak{a}_0\mathfrak{b}_0 \not\subseteq \mathfrak{p}$ und damit $v_\mathfrak{p}(\mathfrak{a}\mathfrak{b}) = v + w$.
2. Sei o.E. $v \le w$. Dann ist
$$\mathfrak{a} + \mathfrak{b} = (\mathfrak{a}_0 + \mathfrak{b}_0\mathfrak{p}^{w-v})\mathfrak{p}^v,$$
wegen $\mathfrak{a}_0 \not\subseteq \mathfrak{p}$ folgt $\mathfrak{a}_0 + \mathfrak{b}_0\mathfrak{p}^{w-v} \not\subseteq \mathfrak{p}$ und damit $v_\mathfrak{p}(\mathfrak{a} + \mathfrak{b}) = v$.
3. Da $\mathfrak{p}$ das einzige Primideal ist, das $\mathfrak{p}^v$ enthält, sind $\mathfrak{a}_0$ und $\mathfrak{p}^v$ teilerfremd. Dann ist aber $\mathfrak{a} = \mathfrak{a}_0\mathfrak{p}^v = \mathfrak{a}_0 \cap \mathfrak{p}^v$ und analog $\mathfrak{b} = \mathfrak{b}_0 \cap \mathfrak{p}^w$. Es gilt auch $\mathfrak{a}_0 \cap \mathfrak{b}_0 \not\subseteq \mathfrak{p}$, denn andernfalls hätte man $\mathfrak{a}_0\mathfrak{b}_0 \subseteq \mathfrak{a}_0 \cap \mathfrak{b}_0 \subseteq \mathfrak{p}$, was zu dem Widerspruch $\mathfrak{a}_0 \subseteq \mathfrak{p}$ oder $\mathfrak{b}_0 \subseteq \mathfrak{p}$ führen würde. Es folgt
$$\mathfrak{a} \cap \mathfrak{b} = (\mathfrak{a}_0 \cap \mathfrak{b}_0) \cap (\mathfrak{p}^v \cap \mathfrak{p}^w) = (\mathfrak{a}_0 \cap \mathfrak{b}_0) \cap \mathfrak{p}^{\max(v,w)} = (\mathfrak{a}_0 \cap \mathfrak{b}_0)\mathfrak{p}^{\max(v,w)},$$
woraus die Behauptung folgt. ■

Die Bewertung $v_\mathfrak{p}$ kann man mit Hilfe des folgenden Lemmas berechnen:

LEMMA. *Sei $\mathfrak{p}$ ein invertierbares Primideal einer Ordnung R und $\lambda \in K \setminus R$ mit $\lambda\mathfrak{p} \subseteq R$. Dann ist*

$$v_\mathfrak{p}(\mathfrak{a}) = \max\{v \in \mathbf{N}_0 : \lambda^v\mathfrak{a} \subseteq R\}.$$

Beweis: Wir schreiben $\mathfrak{a} = \mathfrak{a}_0\mathfrak{p}^w$ mit $w = v_\mathfrak{p}(\mathfrak{a})$. Nach Voraussetzung ist $\mathfrak{b} = \lambda\mathfrak{p}$ ein ganzes Ideal. Da $\mathfrak{p}$ invertierbar ist, gilt $\mathfrak{b} = \lambda\mathfrak{p} \not\subseteq \mathfrak{p}$, also $v_\mathfrak{p}(\mathfrak{b}) = 0$. Damit gilt:

$$\lambda^v\mathfrak{a} \subseteq R \iff (\lambda\mathfrak{p})^v\mathfrak{a} \subseteq \mathfrak{p}^v \iff \mathfrak{b}^v\mathfrak{a}_0\mathfrak{p}^w \subseteq \mathfrak{p}^v \iff w \ge v \iff v_\mathfrak{p}(\mathfrak{a}) \ge v,$$

woraus sofort die Behauptung folgt. ■

Beispiel: $K = \mathbf{Q}(\alpha)$ mit $\alpha^3 + \alpha^2 - 2\alpha + 8 = 0$. Dann ist

$$\mathbf{Z}_K = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2 + \mathbf{Z}\omega_3 \quad \text{mit} \quad \omega_1 = \frac{\alpha^2 + \alpha}{2}, \quad \omega_2 = \alpha, \quad \omega_3 = 1.$$

Die 2 enthaltenden Primideale sind

$$\mathfrak{p}_1 = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2 + \mathbf{Z}2, \quad \mathfrak{p}_2 = \mathbf{Z}(\omega_1+1) + \mathbf{Z}\omega_2 + \mathbf{Z}2, \quad \mathfrak{p}_3 = \mathbf{Z}(\omega_1+1) + \mathbf{Z}(\omega_2+1) + \mathbf{Z}2,$$

alle mit Norm 2 und $(2) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$. Daher sind die $\mathfrak{p}_i$'s invertierbar. Mit dem Ansatz $\lambda_i = \frac{1}{2}(u_1\omega_1 + u_2\omega_2 + u_3)$, $u_i = 0, 1$ und $\lambda_i \notin \mathbf{Z}_K$, $\lambda_i\mathfrak{p}_i \subseteq \mathbf{Z}_K$ findet man Elemente

$$\lambda_1 = \frac{1}{2}(\omega_1+1) = \frac{1}{4}\alpha^2 + \frac{1}{4}\alpha + \frac{1}{2}, \quad \lambda_2 = \frac{1}{2}(\omega_1+\omega_2) = \frac{1}{4}\alpha^2 + \frac{3}{4}\alpha, \quad \lambda_3 = \frac{1}{2}\omega_2 = \frac{1}{2}\alpha.$$

Wir betrachten nun (bis aufs Vorzeichen) alle Elemente $\beta = u_1\omega_1 + u_2\omega_2 + u_3$ mit $|u_i| \le 1$ und bestimmen $v_{\mathfrak{p}_i}(\beta)$:

(u_1, u_2, u_3)	Norm	$(v_{\mathfrak{p}_1}(\beta), v_{\mathfrak{p}_2}(\beta), v_{\mathfrak{p}_3}(\beta))$
(0, 0, 1)	1	(0, 0, 0)
(0, 1, -1)	-2^3	(0, 0, 3)
(0, 1, 0)	-2^3	(2, 1, 0)
(0, 1, 1)	$-2 \cdot 5$	(0, 0, 1)
(1, -1, -1)	$2^2 \cdot 5$	(0, 2, 0)
(1, -1, 0)	2^3	(1, 0, 2)
(1, -1, 1)	2	(0, 1, 0)
(1, 0, -1)	2^3	(0, 1, 2)
(1, 0, 0)	$2 \cdot 5$	(1, 0, 0)
(1, 0, 1)	2^4	(0, 3, 1)
(1, 1, -1)	-2^4	(0, 4, 0)
(1, 1, 0)	-2^2	(1, 0, 1)
(1, 1, 1)	$2 \cdot 5$	(0, 1, 0)

FOLGERUNG. *Sei R eine Ordnung und P eine Menge von invertierbaren Primidealen. Dann hat jedes von 0 verschiedene Ideal $\mathfrak{a}$ von R eine eindeutige Zerlegung*

$$\mathfrak{a} = \mathfrak{a}_0 \prod_{\mathfrak{p}\in P} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})} \quad \textit{mit} \quad \mathfrak{a}_0 \not\subseteq \mathfrak{p} \textit{ für alle } \mathfrak{p} \in P.$$

(Da $\mathfrak{a}$ nur in endlich vielen maximalen Idealen enthalten ist, ist das Produkt endlich.)

Beweis: Dies beweist man genauso wie den letzten Satz indem man nacheinander aus $\mathfrak{a}$ alle möglichen Primideale $\mathfrak{p} \in P$ herausteilt. ■

Beispiel: Wir wollen nun das Beispiel

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

in $R = \mathbf{Z}[\sqrt{-5}]$ verstehen. Das Minimalpolynom von $\alpha = \sqrt{-5}$ ist $f = x^2 + 5$. Aus

$$f \equiv (x+1)^2 \bmod 2, \quad f \equiv (x+1)(x+2) \bmod 3$$

erhält man daher die Primideale, die 2 und 3 erhalten:

$$\mathfrak{p}_2 = (2, \alpha+1), \quad \mathfrak{p}_{3a} = (3, \alpha+1), \quad \mathfrak{p}_{3b} = (3, \alpha+2),$$

die bezüglich der Basis $\alpha, 1$ durch folgende Matrizen dargestellt werden:

$$\mathfrak{p}_2 \to \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}, \quad \mathfrak{p}_{3a} \to \begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix}, \quad \mathfrak{p}_{3b} \to \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}.$$

Nun berechnet man:

$$\mathfrak{p}_2^2 = (2), \quad \mathfrak{p}_{3a}\mathfrak{p}_{3b} = (3).$$

Außerdem haben $\mathfrak{p}_2\mathfrak{p}_{3a}$ und $(1+\alpha)$ die gleiche Normalformdarstellung $\begin{pmatrix} 1 & 1 \\ 0 & 6 \end{pmatrix}$, ebenso wie $\mathfrak{p}_2\mathfrak{p}_{3b}$ und $(1-\alpha)$: $\begin{pmatrix} 1 & 5 \\ 0 & 6 \end{pmatrix}$. Also folgt

$$\mathfrak{p}_2\mathfrak{p}_{3a} = (1+\alpha), \quad \mathfrak{p}_2\mathfrak{p}_{3b} = (1-\alpha),$$

was die obige Faktorisierung auf Idealebene erklärt.

Natürlich stellt sich nun die Frage, ob jedes Primideal einer Ordnung R invertierbar ist oder nicht. Wir wissen bereits, bis auf endlich viele sind alle Primideale invertierbar. Für die Maximalordnung $\mathbf{Z}_K$ können wir nun eine einfache Antwort geben. (Der Allgemeinfall folgt später.)

SATZ. *Jedes Primideal $\mathfrak{p} \neq 0$ der Maximalordnung $\mathbf{Z}_K$ ist invertierbar.*

Beweis: Wir wählen ein $\lambda \in K \setminus \mathbf{Z}_K$ mit $\lambda\mathfrak{p} \subseteq \mathbf{Z}_K$. Wir nehmen an, $\mathfrak{p}$ wäre nicht invertierbar. Dann gilt $\lambda\mathfrak{p} \subseteq \mathfrak{p}$. Sei $\alpha_1, \ldots, \alpha_n$ eine $\mathbf{Z}$-Basis von $\mathfrak{p}$. Wir schauen die rationale Darstellung bezüglich der Basis $\alpha_1, \ldots, \alpha_n$ an: Jedes $\omega \in K$ liefert über $\omega\alpha_i = \sum_j A(\omega)_{ij}\alpha_j$ eine Matrix $A(\omega) \in M_n(\mathbf{Q})$. Nach unserer Annahme $\lambda\mathfrak{p} \subseteq \mathfrak{p}$ folgt $A(\lambda) \subseteq M_n(\mathbf{Z})$. Dann gilt aber für das charakteristische Polynom von λ:

$$\det(xI_n - A(\lambda)) \in \mathbf{Z}[x],$$

also ist λ ganz über $\mathbf{Z}$ und damit $\lambda \in \mathbf{Z}_K$, ein Widerspruch zur Annahme. Also ist $\mathfrak{p}$ doch invertierbar. ■

10. Eindeutige Primidealzerlegung in $\mathbf{Z}_K$

Der folgende Satz ergibt sich nun unmittelbar aus den letzten Überlegungen.

SATZ. *Jedes von 0 verschiedene Ideal $\mathfrak{a}$ in $\mathbf{Z}_K$ hat eine eindeutige Faktorisierung*

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})}$$

als Produkt von Primidealen. (Natürlich gilt $v_{\mathfrak{p}}(\mathfrak{a}) = 0$ für fast alle $\mathfrak{p}$.)

Zur Illustration betrachten wir ein Beispiel:

Beispiel: Wir betrachten $K = \mathbf{Q}(\alpha)$ mit $f(\alpha) = 0$, wo $f = x^3 + 7x + 20$ ist. Als $\mathbf{Z}$-Basis von $\mathbf{Z}_K$ wählen wir

$$\omega_1 = \frac{\alpha^2 + \alpha}{2}, \quad \omega_2 = \alpha, \quad \omega_3 = 1.$$

Wir wollen die Primidealzerlegung des (zufällig gewählten) Hauptideals

$$\mathfrak{a} = (427419669081\omega_1 + 321110693270\omega_2 + 343633073697\omega_3)$$

bestimmen. Die zu den Idealen gehörigen Matrizen in Hermitescher Normalform werden alle bezüglich der Basis $\omega_1, \omega_2, \omega_3$ berechnet. Zum Ideal $\mathfrak{a}$ gehört dann die Matrix

$$\mathfrak{a} \leftrightarrow A = \begin{pmatrix} 1 & 0 & 32330541596902171497871369274842042 \\ 0 & 1 & 23935786203039022000120025873473 2729 \\ 0 & 0 & 92590650302762406161103143748245 7923 \end{pmatrix}.$$

Gilt $\mathfrak{a} = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_r^{e_r}$, so folgt natürlich $N\mathfrak{a} = (N\mathfrak{p}_1)^{e_1} \ldots (N\mathfrak{p}_r)^{e_r}$. Daher bestimmen wir die Primfaktorzerlegung der Norm von $\mathfrak{a}$:

$$N\mathfrak{a} = 92590650302762406161103143748245 7923 = p_1p_2p_3p_4p_5 \quad \text{mit}$$

$$p_1 = 7, \quad p_2 = 3299, \quad p_3 = 21521, \quad p_4 = 9680839171, \quad p_5 = 192447080070865421.$$

Um die p_i enthaltenden Primideale zu bestimmen, bestimmen wir die Primfaktorzerlegung von $f \bmod p_i$:

$$\begin{aligned} f &\equiv (x+3)(x+5)(x+6) \bmod p_1 \\ f &\equiv (x+1113)(x+2654)(x+2831) \bmod p_2 \\ f &\equiv (x+7931)(x^2+13590x+16406) \bmod p_3 \\ f &\equiv (x+4647764309)(x+5284952662)(x+9428961371) \bmod p_4 \\ f &\equiv (x+81377350823052079)(x^2+111069729247813342x+24689123917554875) \bmod p_5 \end{aligned}$$

Dies führt dann zu folgenden Primidealen:

$$\mathfrak{p}_{1a} = (7, \alpha+3), \quad \mathfrak{p}_{1b} = (7, \alpha+5), \quad \mathfrak{p}_{1c} = (7, \alpha+6), \quad \mathfrak{p}_{2a} = (3299, \alpha+1113), \quad \mathfrak{p}_{2b} = (3299, \alpha+2654),$$
$$\mathfrak{p}_{2c} = (3299, \alpha+2831), \quad \mathfrak{p}_{3a} = (21521, \alpha+7931), \quad \mathfrak{p}_{3b} = (21521, \alpha^2+13590\alpha+16406),$$
$$\mathfrak{p}_{4a} = (9680839171, \alpha+4647764309), \quad \mathfrak{p}_{4b} = (9680839171, \alpha+5284952662),$$
$$\mathfrak{p}_{4c} = (9680839171, \alpha+9428961371), \quad \mathfrak{p}_{5a} = (192447080070865421, \alpha+81377350823052079),$$

$$\mathfrak{p}_{5b} = (192447080070865421, \alpha^2 + 111069729247813342\alpha + 24689123917554875).$$

Die zugehörigen Matrizen sind

$$P_{1a} = \begin{pmatrix} 1 & 0 & 4 \\ 0 & 1 & 3 \\ 0 & 0 & 7 \end{pmatrix}, \quad P_{1b} = \begin{pmatrix} 1 & 0 & 4 \\ 0 & 1 & 5 \\ 0 & 0 & 7 \end{pmatrix}, \quad P_{1c} = \begin{pmatrix} 1 & 0 & 6 \\ 0 & 1 & 6 \\ 0 & 0 & 7 \end{pmatrix},$$

$$P_{2a} = \begin{pmatrix} 1 & 0 & 1384 \\ 0 & 1 & 1113 \\ 0 & 0 & 3299 \end{pmatrix}, \quad P_{2b} = \begin{pmatrix} 1 & 0 & 2801 \\ 0 & 1 & 2654 \\ 0 & 0 & 3299 \end{pmatrix}, \quad P_{2c} = \begin{pmatrix} 1 & 0 & 2420 \\ 0 & 1 & 2831 \\ 0 & 0 & 3299 \end{pmatrix},$$

$$P_{3a} = \begin{pmatrix} 1 & 0 & 17287 \\ 0 & 1 & 7931 \\ 0 & 0 & 21521 \end{pmatrix}, \quad P_{3b} = \begin{pmatrix} 1 & 17555 & 8203 \\ 0 & 21521 & 0 \\ 0 & 0 & 21521 \end{pmatrix},$$

$$P_{4a} = \begin{pmatrix} 1 & 0 & 6491190138 \\ 0 & 1 & 4647764309 \\ 0 & 0 & 9680839171 \end{pmatrix}, \quad P_{4b} = \begin{pmatrix} 1 & 0 & 989553069 \\ 0 & 1 & 5284952662 \\ 0 & 0 & 9680839171 \end{pmatrix}, \quad P_{4c} = \begin{pmatrix} 1 & 0 & 2200095971 \\ 0 & 1 & 9428961371 \\ 0 & 0 & 9680839171 \end{pmatrix},$$

$$P_{5a} = \begin{pmatrix} 1 & 0 & 124567653488181316 \\ 0 & 1 & 81377350823052079 \\ 0 & 0 & 192447080070865421 \end{pmatrix}, \quad P_{5b} = \begin{pmatrix} 1 & 151758404659339381 & 1085681019942101 48 \\ 0 & 192447080070865421 & 0 \\ 0 & 0 & 192447080070865421 \end{pmatrix}.$$

Nun gilt $\mathfrak{a} \subseteq \mathfrak{p}_\lambda$ genau dann, wenn $AP_\lambda^{-1} \in M_3(\mathbf{Z})$ gilt. Durch Berechnen aller AP_λ^{-1} findet man, daß $\mathfrak{a}$ genau in den Primidealen

$$\mathfrak{p}_{1b}, \quad \mathfrak{p}_{2c}, \quad \mathfrak{p}_{3a}, \quad \mathfrak{p}_{4a}, \quad \mathfrak{p}_{5a}$$

enthalten ist. Da wegen der Normen keine höheren Potenzen vorkommen können, folgt sofort

$$\mathfrak{a} = \mathfrak{p}_{1b}\mathfrak{p}_{2c}\mathfrak{p}_{3a}\mathfrak{p}_{4a}\mathfrak{p}_{5a}.$$

(Zum Test haben wir die Gleichung nochmals explizit nachgerechnet.)

Beispiel: Wir wollen die Primidealzerlegung von

$$101 + 103\sqrt{2} + 107\sqrt{3} + 109\sqrt{6}$$

in der Maximalordnung des Zahlkörpers $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ bestimmen. Wir wissen bereits, dass $K = \mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\alpha)$ mit $f(\alpha) = 0$, $f(x) = x^4 - 4x^2 + 1$, $\mathbf{Z}_K = \mathbf{Z}[\alpha]$ und $(3\alpha - \alpha^3)^2 = 2$, $(2 - \alpha^2)^2 = 3$ gilt. Mit

$$\omega_2 = 3\alpha - \alpha^3, \quad \omega_3 = 2 - \alpha^2, \quad \omega_6 = \omega_2\omega_3 = 5\alpha - \alpha^3$$

gilt $\omega_2^2 = 2$, $\omega_3^2 = 3$ und

$$\beta = 101 + 103\omega_2 + 107\omega_3 + 109\omega_6 = 315 + 854\alpha - 212\alpha^3 - 107\alpha^2$$

bestimmen. Die Norm (zusammen mit der Primfaktorzerlegung) ist

$$\mathrm{N}\beta = 671946628 = 2^2 \cdot 19^2 \cdot 465337.$$

Wir bestimmen also die Primideale mit Norm 2, 19, $p = 465337$ und faktorisieren dafür f modulo der angegebenen Primzahlen:

$$\begin{aligned} f &\equiv (x+1)^4 \bmod 2, \\ f &\equiv (x^2 + 5x + 1)(x^2 + 14x + 1) \bmod 19, \\ f &\equiv (x + 107194)(x + 144892)(x + 320445)(x + 358143) \bmod p. \end{aligned}$$

Damit erhalten wir folgende Primideale $\mathfrak{p}$, zusammen mit Elementen $\lambda_\mathfrak{p}$, für die $\lambda_\mathfrak{p} \notin \mathbf{Z}_K$, $\lambda_\mathfrak{p}\mathfrak{p} \subseteq \mathbf{Z}_K$ und

$$v_\mathfrak{p}(\beta) = \max\{v \geq 0 : \lambda_\mathfrak{p}^v \beta \in \mathbf{Z}_K\}$$

gilt.

$\mathfrak{p}$	$\lambda_\mathfrak{p}$
$\mathfrak{p}_2 = (2, \alpha+1)$	$\lambda_2 = \frac{(\alpha+1)^3}{2}$
$\mathfrak{p}_{19a} = (19, \alpha^2+5\alpha+1)$	$\lambda_{19a} = \frac{\alpha^2+14\alpha+1}{19}$
$\mathfrak{p}_{19b} = (19, \alpha^2+14\alpha+1)$	$\lambda_{19b} = \frac{\alpha^2+5\alpha+1}{19}$
$\mathfrak{p}_{pa} = (p, \alpha+107194)$	$\lambda_{pa} = \frac{(\alpha+144892)(\alpha+320445)(\alpha+358143)}{p}$
$\mathfrak{p}_{pb} = (p, \alpha+144892)$	$\lambda_{pb} = \frac{(\alpha+107194)(\alpha+320445)(\alpha+358143)}{p}$
$\mathfrak{p}_{pc} = (p, \alpha+320445)$	$\lambda_{pc} = \frac{(\alpha+107194)(\alpha+144892)(\alpha+358143)}{p}$
$\mathfrak{p}_{pd} = (p, \alpha+358143)$	$\lambda_{pd} = \frac{(\alpha+107194)(\alpha+144892)(\alpha+320445)}{p}$

Da $\mathfrak{p}_2$ das einzige Primideal ist, das 2 enthält, und $\mathrm{N}\mathfrak{p}_2 = 2$ gilt, folgt $v_{\mathfrak{p}_2}(\beta) = 2$.

$$\begin{aligned}
\lambda_{19a}\cdot\beta &= \frac{3390}{19} + \frac{5476}{19}\alpha - \frac{136}{19}\alpha^2 - \frac{1704}{19}\alpha^3 \notin \mathbf{Z}[\alpha],\\
\lambda_{19b}\cdot\beta &= 78 + 139\alpha - 10\alpha^2 - 39\alpha^3 \in \mathbf{Z}[\alpha],\\
\lambda_{19b}^2\cdot\beta &= \frac{283}{19} + \frac{568}{19}\alpha - 3\alpha^2 - \frac{106}{19}\alpha^3 \notin \mathbf{Z}[\alpha],
\end{aligned}$$

was sofort $v_{\mathfrak{p}_{19a}}(\beta) = 0$, $v_{\mathfrak{p}_{19b}}(\beta) = 1$ liefert. Genauso findet man

$$\lambda_{pa}\beta \notin \mathbf{Z}[\alpha], \quad \lambda_{pb}\beta \in \mathbf{Z}[\alpha], \quad \lambda_{pb}^2\beta \notin \mathbf{Z}[\alpha], \quad \lambda_{pc}\beta \notin \mathbf{Z}[\alpha], \quad \lambda_{pd}\beta \notin \mathbf{Z}[\alpha],$$

also $v_{\mathfrak{p}_{pa}}(\beta) = 0$, $v_{\mathfrak{p}_{pb}}(\beta) = 1$, $v_{\mathfrak{p}_{pc}}(\beta) = 0$, $v_{\mathfrak{p}_{pd}}(\beta) = 0$. (Natürlich braucht man aus Normgründen nur $\lambda_{pb}\beta \in \mathbf{Z}[\alpha]$ zu finden.) Damit erhalten wir die Primidealzerlegung

$$(\beta) = \mathfrak{p}_2^2 \cdot \mathfrak{p}_{19b} \cdot \mathfrak{p}_{pb}.$$

Wir wenden jetzt unsere Kenntnisse auf gebrochene Ideale an:

Satz. *Jedes von* 0 *verschiedene gebrochene Ideal* $\mathfrak{a}$ *der Maximalordnung hat eine eindeutige Darstellung*

$$\mathfrak{a} = \prod_\mathfrak{p} \mathfrak{p}^{w_\mathfrak{p}} \qquad \textit{mit} \qquad w_\mathfrak{p} \in \mathbf{Z}.$$

Fast alle Exponenten $w_\mathfrak{p}$ *sind* 0. *Man definiert dann die Bewertung* $v_\mathfrak{p}$ *als Fortsetzung auf die gebrochenen Ideale durch* $v_\mathfrak{p}(\mathfrak{a}) = w_\mathfrak{p}$.

Beweis: Existenz: Sei $d \in \mathbf{N}$ mit $\mathfrak{b} = d\mathfrak{a} \subseteq R$. Dann haben wir für die ganzen Ideale (d) und $\mathfrak{b}$ die Darstellungen

$$(d) = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}((d))} \qquad \text{und} \qquad \mathfrak{b} = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{b})},$$

was sofort

$$\mathfrak{a} = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{b}) - v_\mathfrak{p}((d))}$$

liefert.
Eindeutigkeit: Sei

$$\mathfrak{a} = \prod_\mathfrak{p} \mathfrak{p}^{w_\mathfrak{p}} = \prod_\mathfrak{p} \mathfrak{p}^{u_\mathfrak{p}}.$$

Dann erhält man durch Multiplikation mit $\prod_\mathfrak{p} \mathfrak{p}^{|\min(w_\mathfrak{p}, u_\mathfrak{p})|}$ das ganze Ideal

$$\prod_\mathfrak{p} \mathfrak{p}^{|\min(w_\mathfrak{p}, u_\mathfrak{p})|}\mathfrak{a} = \prod_\mathfrak{p} \mathfrak{p}^{w_\mathfrak{p} + |\min(w_\mathfrak{p}, u_\mathfrak{p})|} = \prod_\mathfrak{p} \mathfrak{p}^{u_\mathfrak{p} + |\min(w_\mathfrak{p}, u_\mathfrak{p})|}.$$

Die Eindeutigkeitsaussage für ganze Ideale liefert

$$w_\mathfrak{p} + |\min(w_\mathfrak{p}, u_\mathfrak{p})| = u_\mathfrak{p} + |\min(w_\mathfrak{p}, u_\mathfrak{p})|,$$

woraus $w_\mathfrak{p} = u_\mathfrak{p}$ und damit die Behauptung folgt. ■

FOLGERUNG. *Die Gruppe der invertierbaren Ideale von $\mathbf{Z}_K$ ist eine freie abelsche Gruppe, wobei als Basis die Primideale $\neq 0$ genommen werden können.*

SATZ. *Sei $R = \mathbf{Z}_K$ die Maximalordnung eines Zahlkörpers K und seien $\mathfrak{a}$ und $\mathfrak{b}$ gebrochene Ideale. Dann gilt:*

1. $v_\mathfrak{p}(\mathfrak{a}^{-1}) = -v_\mathfrak{p}(\mathfrak{a})$.
2. $v_\mathfrak{p}(\mathfrak{ab}) = v_\mathfrak{p}(\mathfrak{a}) + v_\mathfrak{p}(\mathfrak{b})$.
3. $v_\mathfrak{p}(\mathfrak{a}+\mathfrak{b}) = \min(v_\mathfrak{p}(\mathfrak{a}), v_\mathfrak{p}(\mathfrak{b}))$.
4. $v_\mathfrak{p}(\mathfrak{a}\cap\mathfrak{b}) = \max(v_\mathfrak{p}(\mathfrak{a}), v_\mathfrak{p}(\mathfrak{b}))$.
5. $\mathfrak{a} \subseteq \mathfrak{b} \iff v_\mathfrak{p}(\mathfrak{a}) \geq v_\mathfrak{p}(\mathfrak{b})$ *für alle* $\mathfrak{p}$.
6. $\mathfrak{a} \subseteq R \iff v_\mathfrak{p}(\mathfrak{a}) \geq 0$ *für alle* $\mathfrak{p}$.

Beweis: 1. ist klar. Man wähle jetzt eine natürliche Zahl d mit $d\mathfrak{a}, d\mathfrak{b} \subseteq R$. Die Aussagen 2., 3., und 4. folgen dann aus den entsprechenden Eigenschaften von $v_\mathfrak{p}$ für ganze Ideale. Wir beweisen 6.: Aus

$$\mathfrak{a} = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})}$$

sieht man $\Leftarrow$, die Richtung $\Rightarrow$ ist bereits bekannt. Zu 5.: Mit 6. gelten die Äquivalenzen:

$$\mathfrak{a} \subseteq \mathfrak{b} \iff \mathfrak{a}\mathfrak{b}^{-1} \subseteq R \iff 0 \leq v_\mathfrak{p}(\mathfrak{a}\mathfrak{b}^{-1}) = v_\mathfrak{p}(\mathfrak{a}) - v_\mathfrak{p}(\mathfrak{b}) \text{ für alle } \mathfrak{p},$$

was die Behauptung beweist. ■

Bemerkung: Ist $R \subsetneq \mathbf{Z}_K$, so muss I_R keine freie abelsche Gruppe sein, wie nachfolgendes Beispiel zeigt.

Beispiel: Für $R = \mathbf{Z}[\sqrt{-11}]$ und $\mathfrak{a} = (4, 1+\sqrt{-11})$ gilt $\mathfrak{a}^3 = (8)$ und daher $(\frac{1}{2}\mathfrak{a})^3 = R$, also ist $\frac{1}{2}\mathfrak{a}$ Torsionselement in I_R, I_R kann also keine freie abelsche Gruppe sein.

11. Primidealzerlegung der Primzahlen $p \in \mathbf{N}$ in $\mathbf{Z}_K$

Sei K ein Zahlkörper und p eine Primzahl. Das von p im Ganzheitsring $\mathbf{Z}_K$ erzeugte Ideal zerlegt sich dann in eindeutiger Weise in ein Produkt von Primidealen:

$$(p) = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_r^{e_r}$$

mit paarweise verschiedenen Primidealen $\mathfrak{p}_i$, die die Primzahl p enthalten. Ist $\mathrm{N}\mathfrak{p}_i = [\mathbf{Z}_K : \mathfrak{p}] = \#\mathbf{Z}_K/\mathfrak{p}_i = p^{f_i}$, so folgt durch Normbildung $p^n = p^{f_1 e_1} \ldots p^{f_r e_r}$ und damit

$$n = \sum_i e_i f_i.$$

f_i heißt der Grad des Primideals $\mathfrak{p}_i$, also $\mathbf{Z}_K/\mathfrak{p}_i \simeq \mathbf{F}_{p^{f_i}}$, der Exponent e_i wird der Verzweigungsindex von $\mathfrak{p}_i$ genannt.
Weitere Sprechweisen sind:

1. $\mathfrak{p}_i$ heißt verzweigt, falls $e_i > 1$ gilt.
2. p heißt verzweigt, falls $e_i > 1$ für ein i gilt.
3. p heißt träge, falls $(p) = \mathfrak{p}_1$ gilt.
4. p heißt voll zerlegt, falls $e_i = f_i = 1$ für alle i gilt. Insbesondere ist $R/\mathfrak{p}_i \simeq \mathbf{F}_p$.

SATZ. *Sei $\alpha \in \mathbf{Z}_K$ mit Minimalpolynom f vom Grad des Zahlkörpers K. Ist p eine Primzahl, die den Index $[\mathbf{Z}_K : \mathbf{Z}[\alpha]]$ nicht teilt, ist*

$$f(x) \equiv g_1(x)^{e_1} \ldots g_r(x)^{e_r} \bmod p$$

die Primfaktorzerlegung von f modulo p, so ist

$$(p) = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_r^{e_r} \quad \textit{mit} \quad \mathfrak{p}_i = (p, g_i(\alpha))$$

die Primfaktorzerlegung von (p) in $\mathbf{Z}_K$.

Beweis: Wir wissen bereits, dass $\mathfrak{p}_i = (p, g_i(\alpha))$ die einzigen p enthaltenden Primideale in $\mathbf{Z}_K$ sind, dass $\mathrm{N}\mathfrak{p}_i = p^{f_i}$ mit $f_i = \mathrm{grad} g_i$, $\sum_i e_i f_i = n$ und

$$(p) \supseteq \mathfrak{p}^{e_1} \dots \mathfrak{p}_r^{e_r}$$

gilt. Nun ist

$$\mathrm{N}((p)) = p^n \quad \text{und} \quad \mathrm{N}(\prod_i \mathfrak{p}^{e_i}) = \prod_i p^{f_i e_i} = p^n,$$

also sind die beiden Ideale gleich, wie behauptet. ■

Nach dem Satz ist klar, dass es nur endlich viele verzweigte Primzahlen gibt. Eine genauere Aussage macht der folgende Satz:

Satz. *Für die Maximalordnung eines Zahlkörpers K und eine Primzahl p gilt:*

$$p \text{ verzweigt in } K \iff p | \mathrm{disc}\,(K).$$

Beweis: Wir haben in $R = \mathbf{Z}_K$ die Zerlegung $Rp = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$. Also ist nach dem chinesischen Restsatz:

$$R/Rp \simeq R/\mathfrak{p}_1^{e_1} \oplus \dots \oplus R/\mathfrak{p}_r^{e_r}.$$

Nun gilt $\mathrm{disc}\,(K) \equiv 0 \bmod p$ genau dann, wenn die Spurform des $\mathbf{F}_p$-Vektorraums R/Rp ausgeartet ist. Da aber R/Rp offensichtlich die orthogonale Summe der $R/\mathfrak{p}_i^{e_i}$ ist, ist also $\mathrm{disc}\,(K) \equiv 0 \bmod p$ genau dann, wenn für ein i die Spurform auf $R/\mathfrak{p}_i^{e_i}$ ausgeartet ist.

- Ist $e_i \geq 2$, so liefert $\alpha \in \mathfrak{p}_i^{e_i - 1} \setminus \mathfrak{p}_i^{e_i}$ ein nilpotentes Element $\overline{\alpha} \in R/\mathfrak{p}_i^{e_i}$. Dann ist aber für alle $\overline{\omega} \in R/\mathfrak{p}_i^{e_i}$ auch $\overline{\alpha\omega}$ nilpotent, also auch die zugehörige Matrix, die dann natürlich Spur 0 hat, d.h. $Sp(\alpha\omega) = 0$, so daß also die Spurform ausgeartet ist.
- Ist $e_i = 1$, so ist $R/\mathfrak{p}_i$ ein endlicher Körper: $R/\mathfrak{p}_i \simeq \mathbf{F}_p[x]/(g(x))$, wo $g \in \mathbf{F}_p[x]$ ein irreduzibles Polynom ist. Die Determinante der Spurform ist dann die Diskriminante des Polynoms, wie wir gesehen haben, also $\neq 0$, d.h. die Spurform ist nicht ausgeartet.

Daraus ergibt sich die Behauptung. ■

Beispiel: Wir betrachten den Zahlkörper $K = \mathbf{Q}(\alpha)$ mit $f(\alpha) = 0$ und $f = 2 + 3x + 5x^2 + 7x^3 + x^4$. Es ist

$$\mathrm{disc}\,(\mathbf{Z}[\alpha]) = \mathrm{disc}\,(f) = -80876 = -2^2 \cdot 20219.$$

Wegen $[\mathbf{Z}_K : \mathbf{Z}[\alpha]] \in \{1, 2\}$ überzeugt man sich schnell, daß $\mathbf{Z}_K = \mathbf{Z}[\alpha]$ gilt. Die Zerlegung von (p) in $\mathbf{Z}_K$ erhält man also durch Faktorisierung von $f \bmod p$.
Die verzweigten Primzahlen sind 2 und 20219 mit der Zerlegung

$$(2) = (2, \alpha) \cdot (2, \alpha + 1)^3 \quad \text{und} \quad (20219) = (20219, \alpha + 7919) \cdot (20219, \alpha + 12250) \cdot (20219, \alpha + 10138)^2.$$

Alle anderen Primzahlen sind unverzweigt. Hier ist das Zerlegungsverhalten der ersten 100 Primzahlen (> 2) aufgelistet, wobei $\mathfrak{p}_f^?$ ein Primideal vom Grad f bezeichnet.

$\mathbf{Z}_K p$	p	
$\mathfrak{p}_1\mathfrak{p}_1'\mathfrak{p}_1''\mathfrak{p}_1'''$	263, 401, 449	3
$\mathfrak{p}_1\mathfrak{p}_1'\mathfrak{p}_2$	23, 31, 43, 47, 53, 61, 157, 229, 277, 313, 373, 379, 383, 397, 443, 461, 503, 523, 541	19
$\mathfrak{p}_1\mathfrak{p}_3$	3, 5, 7, 13, 19, 71, 73, 79, 83, 97, 101, 103, 107, 113, 163, 173, 193, 199, 211, 223, 233, 239, 241, 251, 257, 269, 271, 283, 331, 337, 349, 353, 389, 409, 421, 431, 433, 463, 467, 479, 487, 491, 509	43
$\mathfrak{p}_2\mathfrak{p}_2'$	29, 67, 89, 149, 191, 367, 521	7
$\mathfrak{p}_4$	11, 17, 37, 41, 59, 109, 127, 131, 137, 139, 151, 167, 179, 181, 197, 227, 281, 293, 307, 311, 317, 347, 359, 419, 439, 457, 499, 547	28

In der letzten Spalte der Tabelle ist die Anzahl der Primzahlen $2 < p < 500$ mit einem entsprechenden Zerlegungsverhalten angegeben. (Kann man sich dieses unterschiedliche Verteilungsverhalten erklären?)

Beispiel: Wir wollen die Gleichung $y^2 = x^3 - 26$ mit den nun zur Verfügung stehenden Methoden untersuchen.

1. Der Zahlkörper $K = \mathbf{Q}(\alpha)$ mit $\alpha^2 = -26$ hat den Ganzheitsring $\mathbf{Z}_K = \mathbf{Z}[\alpha]$. Die 2 und 13 enthaltenden Primideale von $\mathbf{Z}_K$ sind
$$\mathfrak{p}_2 = (2, \alpha) \quad \text{und} \quad \mathfrak{p}_{13} = (13, \alpha).$$
2. Seien $x, y \in \mathbf{Z}$ mit $y^2 = x^3 - 26$. Dann gilt
$$x^3 = y^2 + 26 = (y + \alpha)(y - \alpha).$$
3. Angenommen, es gäbe ein Primideal $\mathfrak{p}$ mit $\mathfrak{p} | y + \alpha$, $\mathfrak{p} | y - \alpha$. Dann ist $y + \alpha, y - \alpha \in \mathfrak{p}$, also $2\alpha \in \mathfrak{p}$ und $2 \cdot 13 = (-\alpha) \cdot 2\alpha \in \mathfrak{p}$. Daher folgt $\mathfrak{p} = \mathfrak{p}_2$ oder $\mathfrak{p} = \mathfrak{p}_{13}$.
Fall $\mathfrak{p} = \mathfrak{p}_2$*:* Es folgt $2 | y$ und damit
$$v_{\mathfrak{p}_2}(y + \alpha) = v_{\mathfrak{p}_2}(y - \alpha) = 1, \quad 3v_{\mathfrak{p}_2}(x) = v_{\mathfrak{p}_2}(x^3) = v_{\mathfrak{p}_2}((y + \alpha)(y - \alpha)) = 2,$$
also $v_{\mathfrak{p}_2}(x) = \frac{2}{3}$, was Unsinn ist.
Fall $\mathfrak{p} = \mathfrak{p}_{13}$*:* Auch hier erhält man $v_{\mathfrak{p}_{13}}(y + \alpha) = 1, \ldots$, dann den Widerspruch $v_{\mathfrak{p}_{13}}(x) = \frac{2}{3}$.
Also sind $y + \alpha$ und $y - \alpha$ teilerfremd.
4. Sei
$$(y + \alpha) = \mathfrak{p}_1^{a_1} \ldots \mathfrak{p}_r^{a_r}$$
die Primidealzerlegung von $(y + \alpha)$. Da $y + \alpha$ und $y - \alpha$ teilerfremd sind, folgt $v_{\mathfrak{p}_i}(y - \alpha) = 0$ und damit
$$3v_{\mathfrak{p}_i}(x) = v_{\mathfrak{p}_i}(x^3) = v_{\mathfrak{p}_i}(y + \alpha) + v_{\mathfrak{p}_i}(y - \alpha) = v_{\mathfrak{p}_i}(y + \alpha) = a_i,$$
was sofort zu
$$(y + \alpha) = \prod_i \mathfrak{p}_i^{a_i} = \prod_i \mathfrak{p}_i^{3v_{\mathfrak{p}_i}(x)} = \left(\prod_i \mathfrak{p}_i^{v_{\mathfrak{p}_i}(x)} \right)^3$$
führt. Mit $\mathfrak{a} = \prod_i \mathfrak{p}_i^{v_{\mathfrak{p}_i}(x)}$ folgt also
$$(y + \alpha) = \mathfrak{a}^3,$$
d.h. $(y + \alpha)$ ist 3-te Potenz eines Ideals $\mathfrak{a}$.
5. Ist das Ideal $\mathfrak{a}$ ein Hauptideal, d.h. $\mathfrak{a} = (a + b\alpha)$ mit $a, b \in \mathbf{Z}$ so folgt
$$(y + \alpha) = ((a + b\alpha)^3)$$
und da sich die beiden Erzeuger nur um eine Einheit ± 1 unterscheiden können, gilt $y + \alpha = \pm(a + b\alpha)^3$, o.E. also
$$y + \alpha = (a + b\alpha)^3.$$
Koeffizientenvergleich liefert die Gleichungen
$$1 = b(3a^2 - 26b^2), \quad y = a(a^2 - 78b^2),$$
und damit die Lösungen $b = 1$, $a^2 = 9$, $y = -69a$, $x = 35$.
6. Die Lösung $x = 3$, $y = 1$ haben wir auf dem vorher beschriebenen Weg nicht gefunden. Es gilt $\mathrm{N}(1 + \alpha) = 27$. Es gibt 2 Primideale mit Norm 3, nämlich $\mathfrak{p}_3 = (3, \alpha + 1)$ und $\mathfrak{q}_3 = (3, \alpha + 2)$. Man findet schnell die Primidealzerlegung
$$(1 + \alpha) = \mathfrak{p}_3^3.$$
Nun ist $\mathfrak{p}_3$ kein Hauptideal, also ist klar, dass man auf dem zuvor beschriebenen Weg keinen Erfolg haben konnte.

12. Ideale in $\mathbf{Z}_K$ lassen sich von zwei Elementen erzeugen

LEMMA. *Seien endlich viele Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ in $\mathbf{Z}_K$ gegeben, dazu Zahlen $w_i \in \mathbf{N}_0$. Dann gibt es dazu $\alpha \in \mathbf{Z}_K$ mit*
$$v_{\mathfrak{p}_1}(\alpha) = w_1, \ldots, v_{\mathfrak{p}_r}(\alpha) = w_r.$$

Beweis: Wegen $\mathfrak{p}_i^{w_i+1} \subsetneq \mathfrak{p}_i^{w_i}$ gibt es ein $\alpha_i \in \mathfrak{p}_i^{w_i} \setminus \mathfrak{p}_i^{w_i+1}$. Der chinesische Restsatz liefert ein $\alpha \in R$ mit $\alpha \equiv \alpha_i \bmod \mathfrak{p}_i^{w_i+1}$ für alle i, d.h. $\alpha = \alpha_i + \beta_i$ mit $\beta_i \in \mathfrak{p}_i^{w_i+1}$. Offensichtlich ist $\alpha \in \mathfrak{p}_i^{w_i}$, aber $\alpha \notin \mathfrak{p}_i^{w_i+1}$, da andernfalls auch $\alpha_i \in \mathfrak{p}_i^{w_i+1}$ gelten würde. Damit folgt $v_{\mathfrak{p}_i}(\alpha) = w_i$, wie behauptet. ■

SATZ. *Sei $\mathfrak{a}$ ein von 0 verschiedenes Ideal der Maximalordnung $\mathbf{Z}_K$ eines Zahlkörpers K und $\alpha \in \mathfrak{a}$ mit $\mathfrak{a} \neq 0$. Dann gibt es ein $\beta \in \mathfrak{a}$ mit*

$$\mathfrak{a} = (\alpha, \beta) = R\alpha + R\beta.$$

(In $\mathbf{Z}_K$ kann also jedes Ideal von zwei Elementen erzeugt werden.)

Beweis: Sei $\mathfrak{a} = \prod_i \mathfrak{p}_i^{c_i}$ und $(\alpha) = \prod_i \mathfrak{p}_i^{a_i}$. Dann ist $a_i \geq c_i$. Wir setzen an $(\beta) = \prod_i \mathfrak{p}_i^{b_i}$. Genau dann gilt $\beta \in \mathfrak{a}$, wenn $b_i \geq a_i$ gilt. Weiter ist

$$(\alpha, \beta) = R\alpha + R\beta = \prod_i \mathfrak{p}_i^{\min(a_i, b_i)},$$

also haben wir die Bedingung $\min(a_i, b_i) = c_i$ für alle i. Wir legen jetzt b_i wie folgt fest:

$$b_i = \begin{cases} c_i, \text{ falls } c_i > 0, \\ 0, \text{ falls } c_i = 0 \text{ und } a_i > 0. \end{cases}$$

Dies sind endlich viele Bedingungen, also gibt es nach dem letzten Lemma ein zugehöriges β, mit dem dann $\mathfrak{a} = (\alpha, \beta)$ gilt. ■

FOLGERUNG. *Jedes Primideal $\mathfrak{p} \neq 0$ der Maximalordnung $\mathbf{Z}_K$ eines Zahlkörpers K läßt sich in der Form*

$$\mathfrak{p} = (p, \alpha) = \mathbf{Z}_K p + \mathbf{Z}_K \alpha$$

mit einer Primzahl p und einem Element $\alpha \in \mathfrak{p}$ darstellen.

Beispiel: Wir betrachten wieder $K = \mathbf{Q}(\alpha)$ mit $\alpha^3 + \alpha^2 - 2\alpha + 8 = 0$ und die 3 Primideale

$$\mathfrak{p}_1 = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2 + \mathbf{Z}2, \quad \mathfrak{p}_2 = \mathbf{Z}(\omega_1 + 1) + \mathbf{Z}\omega_2 + \mathbf{Z}2, \quad \mathfrak{p}_3 = \mathbf{Z}(\omega_1 + 1) + \mathbf{Z}(\omega_2 + 1) + \mathbf{Z}2,$$

alle mit Norm 2 und $(2) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$. Wir betrachten die Anteile von $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ mit der früher erstellten Liste:

$$\begin{aligned} (2) &= \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3, \\ (\omega_2 + 1) &= \mathfrak{p}_3 \cdot \ldots, \\ (\omega_1) &= \mathfrak{p}_1 \cdot \ldots, \\ (\omega_1 + \omega_2 + 1) &= \mathfrak{p}_2 \cdot \ldots \end{aligned}$$

und erhalten daher

$$\mathfrak{p}_1 = (2, \omega_1), \quad \mathfrak{p}_2 = (2, \omega_1 + \omega_2 + 1), \quad \mathfrak{p}_3 = (2, \omega_2 + 1).$$

Die Darstellungen sind natürlich nicht eindeutig. So ist z.B. $(\omega_2 - 1) = \mathfrak{p}_3^3 \cdot \ldots$ und damit $\mathfrak{p}_3 = (2, \omega_2 - 1)$.

FOLGERUNG. *Sei $\mathfrak{p}$ ein die Primzahl p enthaltendes Primideal der Maximalordnung $\mathbf{Z}_K$ des Zahlkörpers K. Dann gibt es eine Ordnung $\mathbf{Z}[\alpha]$ und ein Primideal $(p, g(\alpha)) \subseteq \mathbf{Z}[\alpha]$ mit $\mathfrak{p} = \mathbf{Z}_K(p, g(\alpha))$.*

Beweis: Man wähle $\alpha \in \mathbf{Z}_K$ mit $\mathfrak{p} = (p, \alpha)$ und o.E. $K = \mathbf{Q}(\alpha)$. Sei $f(x)$ das Minimalpolynom von α. Dann ist $\mathbf{Z}[\alpha]/(p, \alpha) \simeq \mathbf{Z}/p\mathbf{Z}$, d.h. (p, α) ist in $\mathbf{Z}[\alpha]$ ein Primideal. Dies beweist die Behauptung. ■

Schon im Beweis wird sichtbar, dass die Primideale $(p, g(\alpha)) \subseteq \mathbf{Z}[\alpha]$ und $\mathfrak{p} = \mathbf{Z}_K(p, g(\alpha)) \subseteq \mathbf{Z}_K$ unterschiedliche Grade haben können.

Beispiel: Wir betrachten $K = \mathbf{Q}(\alpha)$ mit $\alpha^3 = 2$ und $\mathbf{Z}_K = \mathbf{Z}[\alpha]$. Die 5 enthaltenden Primideale sind $\mathfrak{p}_5 = (5, \alpha + 2)$ und $\mathfrak{p}_{25} = (5, \beta)$ mit $\beta = \alpha^2 + 3\alpha + 4$ vom Grad 1 bzw. 2. Das Minimalpolynom von β ist $g(x) = x^3 - 12x^2 + 30x - 50$. Aus $g(x) \equiv x^2(x + 3) \bmod 5$ folgt, dass $(5, \beta)$ und $(5, \beta + 3)$ die 5 enthaltenden Primideale von $\mathbf{Z}[\beta]$ sind. Es gilt

$$\mathbf{Z}_K(5, \beta) = \mathfrak{p}_{25}, \quad \mathbf{Z}_K(5, \beta + 3) = \mathfrak{p}_5.$$

13. Hauptidealringe und faktorielle Ringe

Erinnerung an faktorielle Ringe: Ein Integritätsring R mit Quotientenkörper K ist ein faktorieller Ring, wenn es eine Menge $\{\pi_i : i \in I\}$ von Nichteinheiten gibt, so dass sich jedes Element $\alpha \neq 0$ aus R eindeutig schreiben läßt als $\alpha = \varepsilon \prod_{i\in I} \pi_i^{a_i}$ mit einer Einheit $\varepsilon \in R^*$ und $a_i \in \mathbf{N}_0$. Jedes $\beta \in K^*$ hat dann eine eindeutige Darstellung $\beta = \eta \prod_{i\in I} \pi_i^{b_i}$ mit einer Einheit $\eta \in R^*$ und $b_i \in \mathbf{Z}$. Genau dann ist $\beta \in R$, wenn alle $b_i \geq 0$ sind.

LEMMA. *Ist eine Ordnung R eines Zahlkörpers ein faktorieller Ring, so ist R die Maximalordnung, d.h. $R = \mathbf{Z}_K$.*

Beweis: Sei R faktoriell mit den Bezeichnungen von eben. Sei $f = [\mathbf{Z}_K : R]$. Dann ist $\mathbf{Z}_K f \subseteq R$. Wir schreiben $f = \varepsilon \prod_{i\in I} \pi_i^{a_i}$ mit $\varepsilon \in R^*$ und $a_i \geq 0$. Sei $\beta \in \mathbf{Z}_K$ beliebig. Wir schreiben $\beta = \eta \prod_{i\in I} \pi_i^{b_i}$ mit $\eta \in R^*$ und $b_i \in \mathbf{Z}$. Dann ist für alle $m \geq 0$ auch $\beta^m \in \mathbf{Z}_K$ und damit $\beta^m f \in R$. Aus

$$\beta^m f = \varepsilon \eta^m \prod_{i\in I} \pi_i^{a_i + m b_i} \in R$$

folgt dann $a_i + m b_i \geq 0$ für alle $m \geq 0$ und damit $b_i \geq 0$. Daher ist $\beta \in R$. Es folgt $\mathbf{Z}_K = R$, wie behauptet. ■

LEMMA. *Ist $\mathbf{Z}_K$ faktoriell, so ist $\mathbf{Z}_K$ schon ein Hauptidealring.*

Beweis: Sei $R = \mathbf{Z}_K$ mit den Bezeichungen von oben. Die Eindeutigkeit der Darstellung zeigt, daß $(\pi_i) = R\pi_i$ ein Primideal ist. Ist $\mathfrak{p} \neq 0$ irgendein Primideal von R, so gibt es also ein Element $\varepsilon \prod_{i\in I} \pi_i^{a_i} \in \mathfrak{p}$. Ausnutzen der Primidealeigenschaft von $\mathfrak{p}$ liefert einen Index i mit $\pi_i \in \mathfrak{p}$, also $(\pi_i) \subseteq \mathfrak{p}$ und wegen der Maximalität aller Primideale $\neq 0$ in R die Gleichheit $\mathfrak{p} = (\pi_i)$. Also sind die (π_i), $i \in I$, schon alle Primideale $\neq 0$. Da sich jedes Ideal $\neq 0$ als Produkt von Primidealen darstellen läßt, ist jedes Ideal Hauptideal und damit R Hauptidealring. ■

14. Dedekindringe

Eine schöne, kurze, prägnante Einführung in Dedekindringe findet sich bei J.-P. Serre, Local Fields.

DEFINITION. Ein Integritätsring R heißt ganz abgeschlossen (in seinem Quotientenkörper K), wenn gilt:

$$\alpha \in K \text{ ganz über } R \quad \Rightarrow \quad \alpha \in R,$$

gilt für $\alpha \in R$ eine Relation $\alpha^m + a_1\alpha^{m-1} + \cdots + a_{m-1}\alpha + a_m = 0$ mit $a_i \in R$, so ist schon $\alpha \in R$.

LEMMA. *Die Maximalordnung $\mathbf{Z}_K$ eines Zahlkörpers K ist ganz abgeschlossen.*

Beweis: Sei $\alpha \in K$ ganz über $\mathbf{Z}_K$, d.h. $\alpha^m + a_{m-1}\alpha^{m-1} + \cdots + a_0 = 0$ mit $a_i \in \mathbf{Z}_K$. Angenommen, es gibt ein Primideal $\mathfrak{p}$ mit $v_\mathfrak{p}(\alpha) = w < 0$. Für $i \leq m-1$ gilt $v_\mathfrak{p}(a_i\alpha^i) \geq -wi$, somit

$$v_\mathfrak{p}(Ra_{m-1}\alpha^{m-1} + \cdots + Ra_0) \geq -w(m-1),$$

was

$$v_\mathfrak{p}(a_{m-1}\alpha^{m-1} + \cdots + a_0) \geq -w(m-1)$$

impliziert und damit den Widerspruch

$$-w(m-1) \leq v_\mathfrak{p}(\alpha^m) = -wm.$$

Also gilt für alle Primideale $\mathfrak{p}$ die Aussage $v_\mathfrak{p}(\alpha) \geq 0$ und damit $\alpha \in R$, was zu zeigen war. ■

Bemerkung: Ist R Ordnung eines Zahlkörpers und $R \neq \mathbf{Z}_K$, so ist R natürlich nicht ganz abgeschlossen, denn alle Elemente von $\mathbf{Z}_K$ sind ganz über $\mathbf{Z}$ und damit erst recht über R.

DEFINITION. Ein Dedekindring ist ein 1-dimensionaler ganz abgeschlossener noetherscher Integritätsring. (1-dimensional bedeutet: es gibt mindestens ein Primideal $\neq 0$, jedes Primideal $\neq 0$ ist maximal.)

Beispiel: Die Maximalordnung $\mathbf{Z}_K$ eines Zahlkörpers ist ein Dedekindring.

SATZ. *In einem Dedekindring ist jedes von* 0 *verschiedene Ideal eindeutig (bis auf die Reihenfolge) als Produkt von Primidealen darstellbar.*

Beweis: Man verallgemeinert einfach den entsprechenden Beweis für $\mathbf{Z}_K$, wobei Argumente mit dem Index $[\mathfrak{a} : \mathfrak{b}]$ durch Argumente mit noetherschen Ringen ersetzt werden müssen. ■

15. Invertierbarkeit von Primidealen in Ordnungen

Wir haben bewiesen, dass jedes Primideal $\neq 0$ der Maximalordnung $\mathbf{Z}_K$ eines Zahlkörpers K invertierbar ist. Wir wollen jetzt charakterisieren, welche Primideale einer Ordnung $R \subseteq K$ invertierbar sind. Wir beginnen mit einem etwas allgemeineren Satz.

SATZ. *Seien $R \subsetneq S$ Ordnungen eines Zahlkörpers K und*

$$\mathfrak{f} = \{\lambda \in K : \lambda S \subseteq R\}.$$

$\mathfrak{f}$ *heißt der Führer von R in S. Dann gilt:*

1. $\mathfrak{f} \subsetneq R$, $\mathfrak{f}$ *ist ein R-Ideal, also $R\mathfrak{f} = \mathfrak{f}$. Außerdem ist $[S : R] \in \mathfrak{f}$.*
2. $\mathfrak{f}$ *ist ein S-Ideal, also $S\mathfrak{f} = \mathfrak{f}$.*
3. *Es gibt eine normerhaltende Bijektion zwischen den Primidealen von R und S, die $\mathfrak{f}$ nicht enthalten:*

$$\begin{array}{rcll} \{\mathfrak{p} \subseteq R : \mathfrak{f} \not\subseteq \mathfrak{p}\} & \leftrightarrow & \{\mathfrak{P} \subseteq S : \mathfrak{f} \not\subseteq \mathfrak{P}\} & \\ \mathfrak{p} & \to & S\mathfrak{p} & \textit{mit } \mathrm{N}(\mathfrak{p}) = \mathrm{N}(S\mathfrak{p}) \\ R \cap \mathfrak{P} & \leftarrow & \mathfrak{P} & \textit{mit } \mathrm{N}(\mathfrak{P}) = \mathrm{N}(R \cap \mathfrak{P}) \end{array}$$

   Außerdem gilt:

$$\mathfrak{p} \textit{ invertierbares } R\textit{-Ideal} \iff S\mathfrak{p} \textit{ invertierbares } S\textit{-Ideal.}$$

4. $\mathfrak{f}$ *ist als R-Ideal nicht invertierbar.*
5. *Ist $\mathfrak{p} \subseteq R$ ein Primideal mit $\mathfrak{f} \subseteq \mathfrak{p}$, so ist $\mathfrak{p}$ nicht invertierbar.*

Beweis:

1. Wir haben $\mathfrak{f}S \subseteq R$. Wegen $1 \in S$ folgt daraus $\mathfrak{f} \subseteq R$. Wäre $\mathfrak{f} = R$, so würde $1 \in \mathfrak{f}$ sofort $S \subseteq R$, also $S = R$ liefern, was ausgeschlossen war. Dass $\mathfrak{f}$ ein R-Ideal ist, sieht man sofort, also $R\mathfrak{f} \subseteq \mathfrak{f}$ und damit $R\mathfrak{f} = \mathfrak{f}$. Wegen $[S : R] = \#S/R$ folgt $[S : R] \cdot S \subseteq R$ und somit $[S : R] \in \mathfrak{f}$.
2. Man sieht auch sofort, dass $\mathfrak{f}$ ein S-Ideal ist, also $S\mathfrak{f} \subseteq \mathfrak{f}$ und damit $S\mathfrak{f} = \mathfrak{f}$.
3. (a) Sei $\mathfrak{p}$ ein Primideal von R mit $\mathfrak{f} \not\subseteq \mathfrak{p}$. Da $\mathfrak{p}$ maximales Ideal ist, folgt $\mathfrak{f} + \mathfrak{p} = R$. Multiplikation mit S ergibt
$$S = S\mathfrak{f} + S\mathfrak{p} = \mathfrak{f} + S\mathfrak{p}.$$
Dies impliziert auch $R + S\mathfrak{p} = S$.
   (b) Wegen $\mathfrak{p} + \mathfrak{f} = R$ gibt es $\pi \in \mathfrak{p}$ und $\varphi \in \mathfrak{f}$ mit $\pi + \varphi = 1$. Ein Element von $S\mathfrak{p} \cap R$ läßt sich schreiben als $r = \sum s_i \pi_i$ mit $r \in R$, $s_i \in S$, $\pi_i \in \mathfrak{p}$. Es folgt mit $\varphi s_i \in R$
$$r = r(\pi + \varphi) = r\pi + r\varphi = r\pi + \sum \varphi s_i \pi_i = r\pi + \sum (\varphi s_i)\pi_i \in \mathfrak{p},$$
also $S\mathfrak{p} \cap R \subseteq \mathfrak{p}$. Da die umgekehrte Inklusion trivial ist, folgt $S\mathfrak{p} \cap R = \mathfrak{p}$.
   (c) Wegen $R + S\mathfrak{p} = S$ ist jedes Element von S kongruent zu einem Element von R modulo $S\mathfrak{p}$, d.h. der natürliche Ringhomomorphismus $R \to S/S\mathfrak{p}$ ist surjektiv. Der Kern ist $R \cap S\mathfrak{p} = \mathfrak{p}$, also erhalten wir einen Isomorphismus
$$R/\mathfrak{p} \simeq S/S\mathfrak{p}.$$
Damit ist auch $S\mathfrak{p}$ ein Primideal und $\mathrm{N}\mathfrak{p} = \#R/\mathfrak{p} = \#S/S\mathfrak{p} = \mathrm{N}(S\mathfrak{p})$.
   (d) $\mathfrak{p} \to S\mathfrak{p}$ definiert also eine Abbildung zwischen den Primidealen von R und S, die $\mathfrak{f}$ nicht enthalten. Wegen $R \cap S\mathfrak{p} = \mathfrak{p}$ ist die Abbildung injektiv.
   (e) Sei $\mathfrak{P}$ ein Primideal von S mit $\mathfrak{f} \not\subseteq \mathfrak{P}$. Dann ist $\mathfrak{p} = R \cap \mathfrak{P}$ ein Primideal in R mit $\mathfrak{f} \not\subseteq \mathfrak{p}$. Aus $\mathfrak{p} \subseteq \mathfrak{P}$ folgt $S\mathfrak{p} \subseteq S\mathfrak{P} = \mathfrak{P}$. Da $S\mathfrak{p}$ ein Primideal ist, folgt $S\mathfrak{p} = \mathfrak{P}$. Also ist die Zuordnung $\mathfrak{p} \to S\mathfrak{p}$ auch surjektiv.

(f) Ist $\mathfrak{p}$ invertierbares R-Ideal, so gibt es ein gebrochenes R-Ideal $\widetilde{\mathfrak{p}}$ mit $\mathfrak{p}\widetilde{\mathfrak{p}} = R$, was durch Multiplikation mit S sofort $(S\mathfrak{p})(S\widetilde{\mathfrak{p}}) = S$ liefert, d.h. $S\mathfrak{p}$ ist invertierbares S-Ideal.

(g) Sei $S\mathfrak{p}$ ein invertierbares S-Ideal. Wähle $\varphi \in \mathfrak{f} \setminus \mathfrak{p}$. Dann ist $\varphi \notin \mathfrak{p} = S\mathfrak{p} \cap R$, also $\varphi \notin S\mathfrak{p}$ und damit $v_{S\mathfrak{p}}(\varphi) = 0$. Wähle ein $\lambda \in K$ mit $v_{S\mathfrak{p}}(\lambda) = -1$, d.h. ein $\lambda \notin S$ mit $\lambda(S\mathfrak{p}) \subseteq S$. Dann ist $v_{S\mathfrak{p}}(\varphi\lambda) = -1$, also $\varphi\lambda \notin S$, $\varphi\lambda \notin R$. Es gilt

$$\varphi\lambda\mathfrak{p} \subseteq \varphi\lambda(S\mathfrak{p}) \subseteq \varphi S \subseteq R.$$

Wäre $\mathfrak{p}$ nicht invertierbar, so hätte man nun $\varphi\lambda\mathfrak{p} \subseteq \mathfrak{p}$, was sofort $\varphi\lambda S\mathfrak{p} \subseteq S\mathfrak{p}$, also die Nichtinvertierbarkeit von $S\mathfrak{p}$ liefern würde, ein Widerspruch zur Voraussetzung. Also ist auch $\mathfrak{p}$ invertierbares R-Ideal.

4. Wäre $\mathfrak{f}$ ein invertierbares R-Ideal, so würde wegen $\mathfrak{f}\mathfrak{f}^{-1} = R$ durch Multiplikation mit $\mathfrak{f}^{-1}$ aus $S\mathfrak{f} = \mathfrak{f}$ der Widerspruch $S = R$ folgen.
5. Wäre $\mathfrak{p}$ invertierbares R-Ideal, so wäre wegen $\mathfrak{f} \subseteq \mathfrak{p}$ dann $\mathfrak{f}\mathfrak{p}^{-1} \subseteq R$. Aus $S\mathfrak{f} = \mathfrak{f}$ ergäbe sich

$$(\mathfrak{f}\mathfrak{p}^{-1})S = \mathfrak{f}\mathfrak{p}^{-1} \subseteq R,$$

nach Definition von $\mathfrak{f}$ dann $\mathfrak{f}\mathfrak{p}^{-1} \subseteq \mathfrak{f}$, also $\mathfrak{f} \subseteq \mathfrak{f}\mathfrak{p}$, was aber nicht sein kann, wie man durch Normbildung sofort sieht. ■

Wir erhalten jetzt unmittelbar den gewünschten Satz:

SATZ. *Sei R Ordnung eines Zahlkörpers K mit $R \subsetneq \mathbf{Z}_K$ und*

$$\mathfrak{f} = \{\lambda \in K : \lambda\mathbf{Z}_K \subseteq R\}$$

der Führer von R in $\mathbf{Z}_K$. Dann gilt: Genau dann ist ein Primideal $\mathfrak{p} \subseteq R$ invertierbares R-Ideal, wenn $\mathfrak{f} \not\subseteq \mathfrak{p}$ gilt.

Beispiel: Sei $d \in \mathbf{Z} \setminus \{0, 1\}$ quadratfrei und $K = \mathbf{Q}(\sqrt{d})$. Mit

$$\omega = \begin{cases} \frac{1+\sqrt{d}}{2} & \text{für } d \equiv 1 \bmod 4, \\ \sqrt{d} & \text{für } d \equiv 2, 3 \bmod 4 \end{cases} \qquad \text{gilt} \quad \mathbf{Z}_K = \mathbf{Z}[\omega] = \mathbf{Z} + \mathbf{Z}\omega.$$

ω genügt der Gleichung $\omega^2 = \omega + \frac{d-1}{4}$ bzw. $\omega^2 = d$. Die Ordnungen von K sind

$$R_f = \mathbf{Z}[f\omega] = \mathbf{Z} + \mathbf{Z}f\omega \quad \text{mit} \quad f \in \mathbf{N}.$$

Schreiben wir $\alpha = f\omega$, so genügt α der Gleichung $\alpha^2 = f\alpha + f^2\frac{d-1}{4}$ bzw. $\alpha^2 = f^2 d$. Wir wollen den Führer $\mathfrak{f}$ von R_f in $\mathbf{Z}_K$ bestimmen. Wegen $\mathfrak{f} \subseteq R_f$ setzen wir an $\lambda = x + y\alpha$ mit $x, y \in \mathbf{Z}$ und erhalten

$$\begin{aligned} \lambda = x + y\alpha \in \mathfrak{f} \quad &\Longleftrightarrow \quad \lambda\mathbf{Z}[\omega] \subseteq \mathbf{Z}[\alpha] \quad \Longleftrightarrow \quad \lambda(\mathbf{Z} + \mathbf{Z}\omega) \subseteq \mathbf{Z}[\alpha] \quad \Longleftrightarrow \quad \lambda\omega \in \mathbf{Z} + \mathbf{Z}\alpha \\ &\Longleftrightarrow \quad (x + y\alpha)\frac{\alpha}{f} \in \mathbf{Z} + \mathbf{Z}\alpha \\ &\Longleftrightarrow \quad \begin{cases} yf\frac{d-1}{4} + (\frac{x}{f} + y)\alpha \in \mathbf{Z} + \mathbf{Z}\alpha & \text{für } d \equiv 1 \bmod 4 \\ yfd + \frac{x}{f}\alpha \in \mathbf{Z} + \mathbf{Z}\alpha & \text{für } d \equiv 2, 3 \bmod 4 \end{cases} \\ &\Longleftrightarrow \quad x | f \quad \Longleftrightarrow \quad x \in \mathbf{Z}f. \end{aligned}$$

Damit folgt für das Führerideal

$$\mathfrak{f} = \mathbf{Z}f + \mathbf{Z}\alpha = \mathbf{Z}f + \mathbf{Z}f\alpha = \mathbf{Z}_K f.$$

Als R-Ideal hat $\mathfrak{f}$ Norm f. Wir wollen nun die nichtinvertierbaren Primideale $\mathfrak{p}$ in R bestimmen. Es muss gelten $\mathfrak{f} \subseteq \mathfrak{p}$ und damit $p | f$, wenn p die in $\mathfrak{p}$ enthaltene Primzahl ist. Das Minimalpolynom $g(x)$ von α ist

$$g(x) = \begin{cases} x^2 - fx - f^2\frac{d-1}{4} & \text{für } d \equiv 1 \bmod 4, \\ x^2 - f^2 d & \text{für } d \equiv 2, 3 \bmod 4. \end{cases}$$

Für $p | f$ ersieht man aus $g(x) \equiv x^2 \bmod p$, dass $\mathfrak{p} = (p, \alpha)$ das einzige Primideal in R ist, das p enthält. Es gilt

$$\mathfrak{p} = \mathbf{Z}p + \mathbf{Z}\alpha,$$

$\mathfrak{p}$ hat Norm p und offensichtlich gilt $\mathfrak{f} \subseteq \mathfrak{p}$. Damit sehen wir, dass die nichtinvertierbaren Primideale von R genau die Ideale

$$\mathfrak{p} = \mathbf{Z}p + \mathbf{Z}\alpha \quad \text{mit} \quad p|f$$

sind.

FOLGERUNG. *Seien $\mathbf{Z}[\alpha] \subseteq R$ Ordnungen eines Zahlkörpers K, $f(x)$ das Minimalpolynom von α, p eine Primzahl und*

$$f(x) \equiv g_1(x)^{e_1} \dots g_r(x)^{e_r} \bmod p$$

die Primfaktorzerlegung von $f(x)$ modulo p. Gilt $e_i = 1$, so ist $\mathfrak{p}_i = (p, g_i(\alpha))$ ein invertierbares Primideal in R.

Beweis: Wir haben früher die Zerlegung

$$(p) = (p, g_1(\alpha)^{e_1}) \dots (p, g_r(\alpha)^{e_r})$$

bewiesen. Im Fall $e_i = 1$ sieht man daraus, dass in $\mathbf{Z}[\alpha]$ das Primideal $\mathfrak{p}_i = (p, g_i(\alpha))$ invertierbar ist. Dies impliziert $\mathfrak{f} \not\subseteq \mathfrak{p}_i$. Also ist $R\mathfrak{p}_i$ Primideal in R und ebenfalls invertierbar. ■

Das folgende Beispiel zeigt nochmals, dass die Situation im Fall von nichtinvertierbaren Idealen anders ist als im Fall invertierbarer Ideale.

Beispiel: Wir wollen in der Ordnung $R = \mathbf{Z}[\sqrt{-3}]$ alle Ideale mit Norm 2^m bestimmen.

- Wir schreiben $R = \mathbf{Z}[\omega]$ mit $\omega^2 = -3$. Als $\mathbf{Z}$-Basis von R wählen für $\omega, 1$. Die rationale Darstellung von ω ist dann $A(\omega) = \begin{pmatrix} 0 & -3 \\ 1 & 0 \end{pmatrix}$.
- Ideale $\mathfrak{a}$ entsprechen bijektiv (auf die Basis $\omega, 1$ bezogen) Matrizen C in Hermitescher Normalform, die der Bedingung $CA(\omega)C^{-1} \in M_2(\mathbf{Z})$ genügen. Dies sind genau die Matrizen

  $$C = \begin{pmatrix} a & ab \\ 0 & ac \end{pmatrix} \text{ mit } a, b, c \in \mathbf{Z}, a, c \geq 1, 0 \leq b \leq c-1 \text{ und } b^2 \equiv -3 \bmod c.$$

  Die Norm ist $N\mathfrak{a} = a^2 c$. Soll die Norm eine 2-Potenz sein, müssen sowohl a als auch c Potenzen von 2 sein, d.h. $a = 2^k$, $c = 2^l$.
- Wir bestimmen die Lösungen der Gleichung $b^2 \equiv -3 \bmod 2^l$ mit $0 \leq b \leq 2^l - 1$.
  - Für $l = 0$ findet man $b = 0$, für $l = 1$ dann $b = 1$, für $l = 2$ weiter $b = 1$ und $b = 3$.
  - Ist $l \geq 3$ und $b^2 \equiv -3 \bmod 2^l$, so folgt $b^2 \equiv 5 \bmod 8$, was aber nicht geht. Also gibt es für $l \geq 3$ keine Lösungen.
- Dies führt auf folgende Ideale:

  $$R = (1) \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathfrak{p}_2 \leftrightarrow \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}, \quad \mathfrak{a}_{4a} \leftrightarrow \begin{pmatrix} 1 & 1 \\ 0 & 4 \end{pmatrix}, \quad \mathfrak{a}_{4b} \leftrightarrow \begin{pmatrix} 1 & 3 \\ 0 & 4 \end{pmatrix}.$$

  Damit können wir alle Ideale mit Norm 2^m angeben: Ist m ungerade, also $m = 2k+1$, so ist

  $$2^k \mathfrak{p}_2$$

  das einzige Ideal mit Norm 2^m. Ist m gerade, $m = 2k$, mit $m \geq 2$, so gibt es drei Ideale mit Norm 2^m:

  $$(2^k), \quad 2^{k-1}\mathfrak{a}_{4a}, \quad 2^{k-1}\mathfrak{a}_{4b}.$$

  Wir bemerken noch, daß $\mathfrak{a}_{4a,b} \subseteq \mathfrak{p}_2$ gilt, d.h. $\mathfrak{p}_2$ ist das einzige Primideal von R, das 2 enthält.
- Wir stellen eine Multiplikationstabelle der Ideale $\mathfrak{p}_2$, $\mathfrak{a}_{4a}$, $\mathfrak{a}_{4b}$ auf:

  $$\mathfrak{p}_2^2 = \mathfrak{p}_2\mathfrak{a}_{4a} = \mathfrak{p}_2\mathfrak{a}_{4b} = 2\mathfrak{p}_2, \quad \text{außerdem} \quad \mathfrak{p}_2^2 \subseteq \mathfrak{a}_{4a,b} \subseteq \mathfrak{p}_2,$$

  $$\mathfrak{a}_{4a}^2 = 2\mathfrak{a}_{4b}, \quad \mathfrak{a}_{4b}^2 = 2\mathfrak{a}_{4a}, \quad \mathfrak{a}_{4a}\mathfrak{a}_{4b} = (4).$$

- Die Maximalordnung ist $\mathbf{Z}_K = \mathbf{Z}[\frac{1+\omega}{2}]$. Der Führer ist

$$\begin{aligned}\mathfrak{f} &= \{u+v\omega \in K : (u+v\omega)\mathbf{Z}[\frac{1+\omega}{2} \subseteq \mathbf{Z}[\omega]\} = \{u+v\omega \in R : (u+v\omega)\frac{1+\omega}{2} \in R\} = \\ &= \{u+v\omega \in R : \frac{u-3v}{2} + \frac{u+v}{2}\omega \in R\} = \{u+v\omega \in R : u \equiv v \bmod 2\} = \\ &= \mathbf{Z}(1+\omega) + \mathbf{Z}2 = \mathfrak{p}_2.\end{aligned}$$

In $\mathbf{Z}_K$ wird

$$\mathbf{Z}_K\mathfrak{p}_2 = \mathbf{Z}_K\mathfrak{a}_{4a} = \mathbf{Z}_K\mathfrak{a}_{4b} = (2).$$

16. Eine praktische Möglichkeit zur Bestimmung von $\mathbf{Z}_K$

Für eine Ordnung R eines Zahlkörpers K und eine Primzahl p haben wir definiert

$$I_p(R) = \{\alpha \in R : \alpha^m \equiv 0 \bmod p \text{ für ein } m \geq 1\}$$

und gezeigt, dass

$$I_p(R) = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r = \mathfrak{p}_1 \ldots \mathfrak{p}_r \quad \text{und} \quad I_p(R)^n \subseteq Rp, \quad I_p(R) = \{\alpha \in R : \alpha^n \equiv 0 \bmod p\}$$

gilt, wenn $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ die p enthaltenden Primideale von R sind.

LEMMA. *Sei R Ordnung eines Zahlkörpers K vom Grad n und p eine Primzahl. Sei k mit $p^{k-1} < n \leq p^k$. Dann ist*

$$\phi : R/Rp \to R/Rp, \quad x \mapsto x^{p^k} \mod p$$

eine $\mathbf{F}_p$-lineare Abbildung. Seien $\alpha_1, \ldots, \alpha_r \in R$, sodass $\overline{\alpha_1}, \ldots, \overline{\alpha_r}$ eine Basis des Kerns von ϕ ist. Dann gilt

$$I_p(R) = Rp + \mathbf{Z}\alpha_1 + \cdots + \mathbf{Z}\alpha_r.$$

Beweis: R/Rp ist ein n-dimensionaler $\mathbf{F}_p$-Vektorraum. Wegen

$$(\alpha+\beta)^{p^k} \equiv \alpha^{p^k} + \beta^{p^k} \bmod p$$

ist ϕ ein Vektorraumhomomorphismus. Wir beweisen nun $I_p(R) = Rp + \mathbf{Z}\alpha_1 + \cdots + \mathbf{Z}\alpha_r$.
$\subseteq$ Sei $\alpha \in I_p(R)$. Dann gilt $\alpha^n \equiv 0 \bmod p$ und wegen $n \leq p^k$ auch $\alpha^{p^k} \equiv 0 \bmod p$. Also ist $\phi(\overline{\alpha}) = 0$, d.h. es gibt $x_1, \ldots, x_r \in \mathbf{Z}$ mit

$$\alpha \equiv x_1\alpha_1 + \cdots + x_r\alpha_r \bmod p,$$

was die Behauptung zeigt.
$\supseteq$ Dies ist klar, da $I_p(R)$ eine abelsche Gruppe ist und $\alpha_i^{p^k} \equiv 0 \bmod p$ gilt. ■

Bemerkung: Das Lemma zeigt, wie man $I_p(R)$ praktisch berechnen kann. Mit Hilfe des folgenden Lemmas kann man den Kern bestimmen.

LEMMA. *Sei R Ordnung eines Zahlkörpers vom Grad n mit $\mathbf{Z}$-Basis $\omega_1, \ldots, \omega_n$ und p eine Primzahl, sowie k mit $p^{k-1} < n \leq p^k$. Die Matrix $M \in M_n(\mathbf{Z})$ werde definiert durch*

$$\begin{pmatrix} \omega_1^{p^k} \\ \vdots \\ \omega_n^{p^k} \end{pmatrix} = M \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix}.$$

Seien $S, T \in GL_n(\mathbf{Z})$ mit

$$SMT = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix} \quad \text{und} \quad d_i \in \mathbf{N}, \quad d_1|d_2|\ldots|d_n.$$

Bezeichnet S_i die i-te Zeile von S, so gilt

$$I_p(R) = \sum_{i=1}^{n} \mathbf{Z}p\omega_i + \sum_{i \text{ mit } p|d_i} S_i \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix}.$$

Beweis: Für $x_1,\dots,x_n \in \mathbf{Z}$ setzen wir $(y_1,\dots,y_n) = (x_1,\dots,x_n)S^{-1}$ und erhalten dann:

$$\begin{aligned}
\sum x_i\omega_i \in I_p(R) &\iff (\sum x_i\omega_i)^{p^k} \equiv 0 \bmod p \iff \sum x_i\omega_i^{p^k} \equiv 0 \bmod p \iff \\
&\iff \sum_{i,j} x_i m_{ij}\omega_j \equiv 0 \bmod p \iff \sum_j (\sum_i x_i m_{ij})\omega_j \equiv 0 \bmod p \iff \\
&\iff \sum_i x_i m_{ij} \equiv 0 \bmod p \text{ für alle } j \iff (x_1,\dots,x_n)M \equiv 0 \bmod p \iff \\
&\iff (x_1,\dots,x_n)S^{-1}SMTT^{-1} \equiv 0 \bmod p \iff \\
&\iff (y_1,\dots,y_n)SMT \equiv 0 \bmod p \iff \\
&\iff (d_1y_1,\dots,d_ny_n) = (y_1,\dots,y_n)\begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix} \equiv 0 \bmod p \iff \\
&\iff y_i \equiv 0 \bmod p \text{ für } d_i \not\equiv 0 \bmod p \iff \\
&\iff (x_1,\dots,x_n) = (y_1,\dots,y_n)S = \sum_{i=1}^n y_iS_i \text{ und } y_i \equiv \mathrm{mod}0 \text{ für } d_i \not\equiv 0 \bmod p \iff \\
&\iff (x_1,\dots,x_n) \equiv \sum_{i \text{ mit } d_i\equiv 0 \bmod p} y_iS_i \bmod p \iff \\
&\iff \sum_i x_i\omega_i \in \sum_i \mathbf{Z}p\omega_i + \sum_{i \text{ mit } d_i\equiv 0 \bmod p} \mathbf{Z}S_i \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix},
\end{aligned}$$

was die Behauptung beweist. ■

LEMMA. *Ist $\mathfrak{a} \neq 0$ Ideal einer Ordnung R eines Zahlkörpers K, so ist $R' = (\mathfrak{a} : \mathfrak{a})$ eine Ordnung des Zahlkörpers mit $R \subseteq R'$.*

Beweis: Wir wissen bereits, dass R' ein Modul ist. Aus der Definition

$$R' = \{\lambda \in K : \lambda\mathfrak{a} \subseteq \mathfrak{a}\}$$

sieht man $R \subseteq R'$ und die Abgeschlossenheit von R' bzgl. Multiplikation. Daher ist R' eine Ordnung. ■

LEMMA. *Für eine Ordnung R eines Zahlkörpers K und eine Primzahl p sei*

$$R_p = \{\alpha \in \mathbf{Z}_K : p^k\alpha \in R \text{ für ein } r \geq 0\}.$$

Dann ist R_p eine Ordnung und es gibt ein $r \geq 0$ mit

$$R \subseteq R_p \subseteq \frac{1}{p^r}R.$$

Außerdem gilt $\mathrm{ggT}(p, [\mathbf{Z}_K : R_p]) = 1$.

Beweis: Offensichtlich ist R_p abgeschlossen gegenüber Addition und Multiplikation. Wegen $R \subseteq R_p \subseteq \mathbf{Z}_K$ ist daher R_p eine Ordnung. Es gibt dann ein $r \geq 0$ mit $R_p \subseteq \frac{1}{p^r}R$. Würde $p|[\mathbf{Z}_K : R_p]$ gelten, so gäbe es ein $\alpha \in \mathbf{Z}_K \setminus R_p$ mit $p\alpha \in R_p$, wie man mit Hilfe der Smithschen Normalform sehen kann. Es würde $p^{r+1}\alpha \in R$, also $\alpha \in R_p$ folgen, ein Widerspruch. Daher gilt $\mathrm{ggT}(p, [\mathbf{Z}_K : R_p]) = 1$. ■

SATZ. *Sei R Ordnung eines Zahlkörpers K und p eine Primzahl.*

1. *$(I_p(R) : I_p(R))$ ist eine Ordnung mit*

$$R \subseteq (I_p(R) : I_p(R)) \subseteq \frac{1}{p}R \cap \mathbf{Z}_K \subseteq R_p,$$

insbesondere erhält man für den Index

$$[(I_p(R) : I_p(R)) : R] = p^l \text{ für ein } l \text{ mit } 0 \leq l \leq n.$$

2. *Weiter gilt*

$$(I_p(R) : I_p(R)) = R \quad \Longleftrightarrow \quad R = R_p \quad \Longleftrightarrow \quad \mathrm{ggT}(p, [\mathbf{Z}_K : R]) = 1.$$

Beweis:

1. Wir wissen bereits, dass $(I_p(R) : I_p(R))$ eine Ordnung ist, was insbesondere $(I_p(R) : I_p(R)) \subseteq \mathbf{Z}_K$ impliziert. Wegen $p \in I_p(R)$ folgt für $\lambda \in (I_p(R) : I_p(R))$ sofort $\lambda \cdot p \in I_p(R) \subseteq R$, also $\lambda \in \frac{1}{p}R$, und damit $(I_p(R) : I_p(R)) \subseteq \frac{1}{p}R \cap \mathbf{Z}_K \subseteq R_p$. Aus $R \subseteq (I_p(R) : I_p(R)) \subseteq \frac{1}{p}R$ und $[\frac{1}{p}R : R] = p^n$ folgen die Aussagen für den Index.
2. Wir zeigen $\Longrightarrow$. Wir setzen voraus, dass $(I_p(R) : I_p(R)) = R$ gilt.
   (a) Wir wissen, dass $I_p(R)^n \subseteq Rp$ gilt. Daher folgt
   $$I_p(R)^{nr} R_p \subseteq (Rp)^r R_p = p^r R_p \subseteq R.$$
   (b) Sei jetzt $i \geq 1$ mit $I_p(R)^i R_p \subseteq R$. ($i = nr$ erfüllt diese Bedingung.) Sei $\alpha \in I_p(R)^{i-1} R_p \subseteq RR_p = R_p$. Dann ist
   $$\alpha I_p(R) \subseteq I_p(R)^i R_p \subseteq R.$$
   Ist $\beta \in I_p(R)$, so gilt zunächst
   $$\alpha\beta \subseteq \alpha I_p(R) \subseteq R,$$
   und dann weiter:
   $$\begin{aligned} (\alpha\beta)^n &= \alpha^n \beta^n \in R_p^n I_p(R)^n \subseteq R_p \cdot pR = pR_p, \\ (\alpha\beta)^{n(r+1)} &\in p^{r+1} R_p = p \cdot p^r R_p \subseteq p \cdot R, \end{aligned}$$
   also $\alpha\beta \in I_p(R)$. Da $\beta \in I_p(R)$ beliebig war, folgt
   $$\alpha I_p(R) \subseteq I_p(R), \quad \text{d.h.} \quad \alpha \in (I_p(R) : I_p(R)).$$
   Mit der Voraussetzung $(I_p(R) : I_p(R)) = R$ folgt $\alpha \in R$, also schließlich
   $$I_p(R)^{i-1} R_p \subseteq R.$$
   Daher gilt die Implikation
   $$I_p(R)^i R_p \subseteq R \quad \Longrightarrow \quad I_p(R)^{i-1} R_p \subseteq R.$$
   (c) Wendet man die letzte Formel ausgehend von $i = nr$ an, so erhält man durch sukzessive Anwendung schließlich $I_p(R)^0 R_p \subseteq R$, d.h. $R_p \subseteq R$ und damit $R_p = R$.

   Die Richtung $\Longleftarrow$ folgt sofort aus 1. ■

Aus den angestellten Überlegungen erhalten wir nun ein Verfahren zu Bestimmung der Maximalordnung $\mathbf{Z}_K$ (Round-Two-Method von Zassenhaus):

Verfahren zur Bestimmung von $\mathbf{Z}_K$: Gegeben sei ein Zahlkörper K vom Grad n.

1. Man wählt eine Ordnung R und berechnet $\operatorname{disc} R = m^2 d$ mit $m \in \mathbf{N}$ und $d \in \mathbf{Z}$ quadratfrei. Die Primteiler von m schreibt man in eine Liste p.
2. Ist $P = \emptyset$, so ist man fertig und es gilt $\mathbf{Z}_K = R$. Andernfalls wählt man eine Primzahl $p \in P$.
3. Man berechnet $R' = (I_p(R) : I_p(R))$.
4. Gilt $R' = R$, so streicht man p aus der Liste P und geht zurück zu 2.
5. Ist $R' \neq R$, so setzt man $R := R'$ und geht zurück zu 3.

Zu dem Verfahren haben wir eine Maple-Funktion 'ord_max(R,K)' geschrieben.

KAPITEL 7

Gitter — Geometrische Methoden

1. Einführendes Beispiel

Wir betrachten für $d \in \mathbf{N}$ einen Ring der Gestalt

$$R = \mathbf{Z}[\sqrt{-d}] \quad \text{oder} \quad R = \mathbf{Z}[\frac{1+\sqrt{-d}}{2}] \text{ für } d \equiv 3 \bmod 4.$$

R ist Unterring von $\mathbf{C}$, zeichnet man die Elemente von R in der komplexen Zahlenebene, so erhält man ein Gitter. Die Norm des zugehörigen Zahlkörpers ist

$$N : \mathbf{Q}(\sqrt{-d}) \to \mathbf{Q}, \quad N(u+v\sqrt{-d}) = (u+v\sqrt{-d})\overline{(u+v\sqrt{-d})} = u^2 + dv^2 = |u+v\sqrt{-d}|^2.$$

Da R aus ganzen algebraischen Zahlen besteht, gilt $N(R) \subseteq \mathbf{N}_0$.
R ist euklidischer Ring bzgl. der Norm, wenn es zu $a, b \in R$ mit $b \neq 0$ Elemente $q, r \in R$ gibt mit

$$a = qb + r \quad \text{und} \quad N(r) < N(b).$$

Die Bedingung kann man auch so formulieren: zu $a, b \in R$ mit $b \neq 0$ gibt es $q \in R$ mit $N(a-bq) < N(b)$. Division durch b ergibt die Äquivalenz mit

$$|\frac{a}{b} - q|^2 = \frac{N(a-bq)}{N(b)} < 1, \quad \text{also} \quad |\frac{a}{b} - q| < 1.$$

Da die Elemente von $\mathbf{Q}(\sqrt{-d})$ dicht in $\mathbf{C}$ liegen, folgt dann unmittelbar das

Kriterium: Genau dann ist R euklidischer Ring bzgl. der Norm, wenn es zu jedem $z \in \mathbf{C}$ ein $q \in R$ gibt mit

$$|z - q| < 1.$$

Wir betrachten $R = \mathbf{Z}[\frac{1+\sqrt{-d}}{2}]$. Man überlegt sich, dass der schlimmste Fall für den Mittelpunkt des von $0, 1, \frac{1+\sqrt{-d}}{2}, \frac{3+\sqrt{-d}}{2}$ gebildeten Parallelogramms auftritt. Der Mittelpunkt ist $\frac{3+\sqrt{-d}}{4}$ und

$$|\frac{3+\sqrt{-d}}{4} - 1| = |\frac{-1+\sqrt{-d}}{4}| = \sqrt{\frac{1+d}{16}}.$$

Also ist in diesem Fall R euklidisch, falls $d \equiv 3 \bmod 4$ und $1 + d < 16$ gilt, d.h. für $d = 3, 7, 11$.

Für $R = \mathbf{Z}[\sqrt{-d}]$ tritt der schlimmste Fall für den Mittelpunkt des von $0, 1, \sqrt{-d}, 1+\sqrt{-d}$ gebildeten Parallelogramms auf. Der Mittelpunkt ist $\frac{1+\sqrt{-d}}{2}$ und der Abstand

$$|\frac{1+\sqrt{-d}}{2} - 0| = \sqrt{\frac{1+d}{4}}.$$

Also ist R genau dann euklidisch, wenn $1 + d < 4$ gilt, d.h. für $d = 1, 2$.

Damit haben wir folgenden Satz bewiesen:

Satz. *Die einzigen Ordnungen imaginärquadratischer Zahlkörper, die euklidisch bzgl. der Norm sind, sind*

$$\mathbf{Z}[\sqrt{-1}], \quad \mathbf{Z}[\sqrt{-2}], \quad \mathbf{Z}[\frac{1+\sqrt{-3}}{2}], \quad \mathbf{Z}[\frac{1+\sqrt{-7}}{2}], \quad \mathbf{Z}[\frac{1+\sqrt{-11}}{2}].$$

(Insbesondere sind diese Ringe dann auch Hauptidealringe und faktoriell.)

Version vom 25.2.2003

2. Gitter

Wir legen im folgenden den reellen Vektorraum $\mathbf{R}^n$ zugrunde, zusammen mit einem Skalarprodukt $v \cdot w$. Die zugehörige Norm schreiben wir als $\|v\| = \sqrt{v \cdot v}$. Wenn nichts anderes gesagt wird, verwenden wir das Standardskalarprodukt:

$$(v_1, \ldots, v_n) \cdot (w_1, \ldots, w_n) = v_1 w_1 + \cdots + v_n w_n \quad \text{und} \quad \|(v_1, \ldots, v_n)\| = \sqrt{v_1^2 + \cdots + v_n^2}.$$

Eine Teilmenge $M \subseteq \mathbf{R}^n$ nennt man diskret, wenn jede beschränkte Menge, also z.B. jede Kugel $\{x \in \mathbf{R}^n : \|x\| \leq r\}$, nur endlich viele Elemente von M enthält.

DEFINITION. Ein Gitter in $\mathbf{R}^n$ ist eine diskrete Teilmenge von $\mathbf{R}^n$, die gleichzeitig Untergruppe der additiven Gruppe von $\mathbf{R}^n$ ist.

Beispiel: $\mathbf{Z}^n$ ist ein Gitter in $\mathbf{R}^n$.

LEMMA. *Sind $v_1, \ldots, v_r \in \mathbf{R}^n$ linear unabhängig, so gibt es eine Konstante $\mu > 0$ mit*

$$\|x_1 v_1 + \cdots + x_r v_r\| \geq \mu \max(|x_1|, \ldots, |x_r|) \text{ für alle } x_i \in \mathbf{R}.$$

Beweis: Da die Menge $Q = \{(x_1, \ldots, x_r) : \max(|x_1|, \ldots, |x_r|) = 1\}$ im $\mathbf{R}^r$ kompakt ist, nimmt die stetige Funktion $(x_1, \ldots, x_r) \mapsto \|x_1 v_1 + \cdots + x_r v_r\|$ dort ihr Minimum μ an; es ist $\mu > 0$, da $v_1, \ldots, v_r$ linear unabhängig sind. Sei jetzt $(x_1, \ldots, x_r) \neq 0$ gegeben. Mit $t = \max(|x_1|, \ldots, |x_r|)$ ist $(\frac{x_1}{t}, \ldots, \frac{x_r}{t})$ ein Punkt von Q und somit folgt $\|\frac{x_1}{t} v_1 + \cdots + \frac{x_r}{t} v_r\| \geq \mu$, was durch Multiplikation mit t die Behauptung liefert. (Der Fall $t = 0$ ist trivial.) ■

SATZ. *Genau dann ist $\Gamma \subseteq \mathbf{R}^n$ ein Gitter, wenn es $\mathbf{R}$-linear unabhängige Elemente $v_1, \ldots, v_r \in \mathbf{R}^n$ gibt mit*

$$\Gamma = \mathbf{Z}v_1 + \cdots + \mathbf{Z}v_r = \{x_1 v_1 + \cdots + x_r v_r : x_i \in \mathbf{Z}\}.$$

Beweis:

1. Sei $\Gamma = \mathbf{Z}v_1 + \cdots + \mathbf{Z}v_r$ mit linear unabhängigen $v_1, \ldots, v_r$ gegeben. Wir müssen zeigen, dass Γ diskret ist. Nach dem letzten Lemma gibt es ein $\mu > 0$ mit $\|x_1 v_1 + \cdots + x_r v_r\| \geq \mu \max(|x_1|, \ldots, |x_r|)$ für alle $x_i \in \mathbf{R}$. Dann ist aber für jedes $H > 0$ die Menge

$$\begin{aligned} \Gamma \cap \{x \in \mathbf{R}^n : \|x\| \leq H\} &= \{x_1 v_1 + \cdots + x_r v_r : x_i \in \mathbf{Z} \text{ und } \|x_1 v_1 + \cdots + x_r v_r\| \leq H\} \\ &\subseteq \{x_1 v_1 + \cdots + x_r v_r : x_i \in \mathbf{Z}, |x_i| \leq \frac{H}{\mu}\} \end{aligned}$$

   endlich, was die Diskretheit beweist.

2. Sei Γ eine diskrete Untergruppe von $\mathbf{R}^n$, sei V der von Γ aufgespannte $\mathbf{R}$-Untervektorraum und $v_1, \ldots, v_r \in \Gamma$ eine $\mathbf{R}$-Basis von V. Nach 1. ist dann $\Gamma_0 = \mathbf{Z}v_1 + \cdots + \mathbf{Z}v_r$ ein Gitter in $\mathbf{R}^n$. Die Menge

$$F = \{x_1 v_1 + \cdots + x_r v_r : 0 \leq x_i < 1\}$$

   ist ein Repräsentantensystem der Faktorgruppe V/Γ_0. (Jedes $x_1 v_1 + \cdots + x_r v_r \in V$ hat $(x_1 - \lfloor x_1 \rfloor)v_1 + \cdots + (x_r - \lfloor x_r \rfloor)v_r \in F$ als eindeutigen Repräsentanten.) Also ist $F \cap \Gamma$ ein Repräsentantensystem der Faktorgruppe Γ/Γ_0. Da die Menge $F \subseteq \mathbf{R}^n$ beschränkt ist, ist $F \cap \Gamma$ endlich. Mit $m = \#\Gamma/\Gamma_0 = \#F \cap \Gamma$ ist dann $m\Gamma \subseteq \Gamma_0$ und daher

$$\mathbf{Z}v_1 + \cdots + \mathbf{Z}v_r \subseteq \Gamma \subseteq \frac{1}{m}(\mathbf{Z}v_1 + \cdots + \mathbf{Z}v_r).$$

   Mit unserem Normalisierungsverfahren findet man

$$\Gamma = \mathbf{Z}w_1 + \cdots + \mathbf{Z}w_r$$

   mit

$$\begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_r \end{pmatrix} = \frac{1}{m} \begin{pmatrix} c_{11} & c_{12} & \ldots & c_{1r} \\ & c_{22} & \ldots & c_{2r} \\ & & \ddots & \vdots \\ & & & c_{rr} \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_r \end{pmatrix}$$

   und (c_{ij}) in Hermitescher Normalform. Dies zeigt die Behauptung. ■

Ist $\Gamma = \mathbf{Z}v_1 + \cdots + \mathbf{Z}v_r \subseteq \mathbf{R}^n$ ein Gitter mit $\mathbf{R}$-linear unabhängigen $v_1, \ldots, v_r$, so heißt $v_1, \ldots, v_r$ eine Gitterbasis und r der Rang des Gitters. Nach unseren Überlegungen bei endlich erzeugten $\mathbf{Z}$-Moduln ist klar, dass $w_1, \ldots, w_r \in \mathbf{R}^n$ genau dann eine Gitterbasis von Γ ist, wenn es eine Matrix $M \in GL_r(\mathbf{Z})$ gibt mit

$$\begin{pmatrix} w_1 \\ \vdots \\ w_r \end{pmatrix} = M \begin{pmatrix} v_1 \\ \vdots \\ v_r \end{pmatrix}.$$

Die von der Gitterbasis abhängige Menge

$$F = \{\lambda_1 v_1 + \cdots + \lambda_r v_r \in \mathbf{R}^n : 0 \leq \lambda_i < 1\}$$

wird als Fundamentalparallelotop oder Grundmasche des Gitters oder Gittermasche bezeichnet. Die Determinante oder das Volumen des Gitters wird durch eine Gramsche Determinante definiert:

$$\operatorname{vol}(\Gamma) = \det(\Gamma) = \sqrt{\det(v_i \cdot v_j)}.$$

Spannt Γ den ganzen $\mathbf{R}^n$ auf, so ist

$$\operatorname{vol}(\Gamma) = \det(\Gamma) = |\det(v_1, \ldots, v_n)| = \operatorname{vol}(F),$$

also das Volumen einer Grundmasche.

Beispiele:

1. $\mathbf{Z}^n$ ist ein Gitter im $\mathbf{R}^n$ mit Determinante 1.
2. $\mathbf{Z} + \mathbf{Z}\sqrt{2}$ ist kein Gitter in $\mathbf{R}$. Warum?

3. Die additive Einbettung eines Zahlkörpers in $\mathbf{R}^n$

Sei K ein Zahlkörper vom Grad n, seien $\sigma_1, \ldots, \sigma_{r_1} : K \hookrightarrow \mathbf{R}$ die reellen und $\sigma_{r_1+1}, \overline{\sigma_{r_1+1}}, \ldots, \sigma_{r_1+r_2}, \overline{\sigma_{r_1+r_2}} : K \hookrightarrow \mathbf{C}$ die komplexen Einbettungen von K. Dann definieren wir die additive Einbettung $\phi : K \to \mathbf{R}^n$ durch:

$$\phi(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_{r_1}(\alpha), \operatorname{Re}\sigma_{r_1+1}(\alpha), \operatorname{Im}\sigma_{r_1+1}(\alpha), \ldots, \operatorname{Re}\sigma_{r_1+r_2}(\alpha), \operatorname{Im}\sigma_{r_1+r_2}(\alpha)).$$

Beispiele:

1. Für einen imaginärquadratischen Zahlkörper $K = \mathbf{Q}(\sqrt{-d})$ mit $d \in \mathbf{N}$ ist

$$\phi : K \to \mathbf{R}^2, \quad u + v\sqrt{-d} \mapsto (u, v\sqrt{d}).$$

2. Für einen reellquadratischen Zahlkörper $K = \mathbf{Q}(\sqrt{d})$ mit $d \in \mathbf{N}$, d kein Quadrat, ist

$$\phi : K \to \mathbf{R}^2, \quad u + v\sqrt{d} \mapsto (u + v\sqrt{d}, u - v\sqrt{d}).$$

LEMMA. *Ist $\mathfrak{a}$ ein freier $\mathbf{Z}$-Modul vom maximalem Rang in K, so ist $\phi(\mathfrak{a})$ ein Gitter vom Rang n in $\mathbf{R}^n$ mit*

$$\det(\phi(\mathfrak{a})) = \frac{1}{2^{r_2}}\sqrt{|\operatorname{disc}(\mathfrak{a})|}.$$

Beweis: Sei $\alpha_1, \ldots, \alpha_n$ eine $\mathbf{Z}$-Basis von $\mathfrak{a}$. Wir schreiben

$$\sigma_k\alpha_j = x_{jk} \text{ für } k = 1, \ldots, r_1 \quad \text{und} \quad \sigma_{r_1+l}\alpha_j = y_{jl} + iz_{jl} \text{ für } l = 1, \ldots, r_2$$

mit reellen Zahlen x_{jk}, y_{jl}, z_{jl}. Wir wissen, dass $\operatorname{disc}(\mathfrak{a}) = |\det(\sigma_k\alpha_j)_{jk}|^2$ gilt. Wir formen die Determinante mit Spaltenumformungen um, wobei wir jeweils nur die j-te Zeile angeben:

$$\begin{aligned}
\pm\sqrt{|\operatorname{disc}\mathfrak{a}|} &= \det(\sigma_1(\alpha_j),\ldots,\sigma_n(\alpha_j)) = \\
&= \det(x_{jr_1},\ldots,x_{jr_1},y_{j1}+iz_{j1},y_{j1}-iz_{j1},\ldots,y_{jr_2}+iz_{jr_2},y_{jr_2}-iz_{jr_2}) = \\
&= \det(x_{jr_1},\ldots,x_{jr_1},y_{j1}+iz_{j1},2y_{j1},\ldots,y_{jr_2}+iz_{jr_2},2y_{jr_2}) = \\
&= 2^{r_2}\det(x_{jr_1},\ldots,x_{jr_1},y_{j1}+iz_{j1},y_{j1},\ldots,y_{jr_2}+iz_{jr_2},y_{jr_2}) = \\
&= 2^{r_2}\det(x_{jr_1},\ldots,x_{jr_1},iz_{j1},y_{j1},\ldots,iz_{jr_2},y_{jr_2}) = \\
&= (2i)^{r_2}\det(x_{jr_1},\ldots,x_{jr_1},z_{j1},y_{j1},\ldots,z_{jr_2},y_{jr_2}) = \\
&= (-2i)^{r_2}\det(x_{jr_1},\ldots,x_{jr_1},y_{j1},z_{j1},\ldots,y_{jr_2},z_{jr_2}) = \\
&= (-2i)^{r_2}\det(\phi(\alpha_j)).
\end{aligned}$$

Wegen $\operatorname{disc}\mathfrak{a} \neq 0$ sind die Vektoren $\phi(\alpha_1),\ldots,\phi(\alpha_n)$ also $\mathbf{R}$-linear unabhängig, d.h. $\phi(\mathfrak{a})$ ist ein Gitter vom Rang n. Außerdem folgt nach Definition der Gitterdeterminante sofort

$$\det(\phi(\mathfrak{a})) = |\det(\phi(\alpha_j))| = (\frac{1}{2})^{r_2}\sqrt{|\operatorname{disc}\mathfrak{a}|},$$

was gezeigt werden sollte. ■

4. Der Gitterpunktsatz von Minkowski

Wir erinnern an zwei Bezeichnungen: Eine Teilmenge $X \subseteq \mathbf{R}^n$ nennt man zentralsymmetrisch (bzgl. des Nullpunkts), wenn gilt:

$$x \in X \quad\Longrightarrow\quad -x \in X.$$

Eine Teilmenge X heißt konvex, wenn mit zwei Punkten x, y aus X auch deren Verbindungsstrecke in X liegt, also

$$x, y \in X \quad\Longrightarrow\quad tx + (1-t)y \in X \text{ für alle } 0 \leq t \leq 1.$$

Über die Existenz von Gitterpunkten in Teilmengen $X \subseteq \mathbf{R}^n$ macht der folgende Gitterpunktsatz von Minkowski Aussagen:

SATZ. *Ist Γ ein Gitter vom Rang n in $\mathbf{R}^n$ und X eine symmetrische, konvexe Teilmenge, sodass für das Volumen die Abschätzung*

$$\operatorname{vol}(X) > 2^n\det(\Gamma)$$

gilt, so enthält X einen von 0 verschiedenen Punkt von Γ.

Beweis:

- Angenommen, es gilt für alle $\gamma_1, \gamma_2 \in \Gamma$ mit $\gamma_1 \neq \gamma_2$

$$(\frac{1}{2}X + \gamma_1) \cap (\frac{1}{2}X + \gamma_2) = \emptyset.$$

Ist F eine Grundmasche es Gitters Γ, so ist $\mathbf{R}^n$ die disjunkte Vereinigung der Mengen $F+\gamma$, $\gamma \in \Gamma$ und somit

$$\begin{aligned}
\frac{1}{2^n}\operatorname{vol}(X) &= \operatorname{vol}(\frac{1}{2}X) = \operatorname{vol}(\frac{1}{2}X \cap (\bigcup_{\gamma\in\Gamma}(F+\gamma))) = \operatorname{vol}(\bigcup_{\gamma\in\Gamma}(\frac{1}{2}X \cap (F+\gamma))) = \\
&= \sum_{\gamma\in\Gamma}\operatorname{vol}(\frac{1}{2}X \cap (F+\gamma)) = \sum_{\gamma\in\Gamma}\operatorname{vol}((\frac{1}{2}X-\gamma)\cap F) = \\
&= \operatorname{vol}(\bigcup_{\gamma\in\Gamma}\left((\frac{1}{2}X-\gamma)\cap F\right)) = \operatorname{vol}(\left(\bigcup_{\gamma\in\Gamma}(\frac{1}{2}X-\gamma)\right)\cap F) \leq \\
&\leq \operatorname{vol}(F) = \det(\Gamma),
\end{aligned}$$

was unserer Voraussetzung widerspricht.

- Somit gibt es $\gamma_1, \gamma_2 \in \Gamma$, $\gamma_1 \neq \gamma_2$, mit
$$(\frac{1}{2}X + \gamma_1) \cap (\frac{1}{2}X + \gamma_2) \neq \emptyset,$$
d.h. es gibt $x_1, x_2 \in X$ mit
$$\frac{1}{2}x_1 + \gamma_1 = \frac{1}{2}x_2 + \gamma_2,$$
also ist
$$0 \neq \gamma_1 - \gamma_2 = \frac{1}{2}x_1 + \frac{1}{2}(-x_2) \in \Gamma \cap X,$$
da mit x_1, x_2 auch $-x_2$ und $\frac{x_1+(-x_2)}{2}$ in X liegt. Dies beweist die Behauptung. ■

Bemerkung: Der Koeffizient 2^n im Minkowskischen Gitterpunktsatz kann nicht verbessert werden. Man wähle
$$X = \{(x_1, \ldots, x_n) \in \mathbf{R}^n : |x_i| < 1\} \quad \text{und} \quad \Gamma = \mathbf{Z}^n.$$
X ist konvex, symmetrisch und $\mathrm{vol}\,(X) = 2^n$, aber X enthält als einzigen Gitterpunkt den Nullpunkt.

5. Elemente kleiner Norm in Idealen

Sei K ein Zahlkörper vom Grad n über $\mathbf{Q}$. Wir verwenden die additive Einbettung $\phi : K \to \mathbf{R}^n$ mit
$$\phi(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_{r_1}(\alpha), \mathrm{Re}\,\sigma_{r_1+1}(\alpha), \mathrm{Im}\,\sigma_{r_1}(\alpha), \ldots, \mathrm{Re}\,\sigma_{r_1+r_2}(\alpha), \mathrm{Im}\,\sigma_{r_1+r_2}(\alpha)).$$
Um den Minkowskischen Gitterpunktsatz anzuwenden, brauchen wir die Aussage des folgenden Lemmas. Wir verwenden auf $\mathbf{R}^n$ die Koordinaten $x_1, \ldots, x_{r_1}, y_1, z_1, \ldots, y_{r_2}, z_{r_2}$.

LEMMA. *Die Menge*
$$S_t = \{(x_1, \ldots, x_{r_1}, y_1, z_1, \ldots, y_{r_2}, z_{r_2}) \in \mathbf{R}^n : \sum_{i=1}^{r_1} |x_i| + 2\sum_{j=1}^{r_2} \sqrt{y_j^2 + z_j^2} \leq t\} \subseteq \mathbf{R}^n$$
ist konvex, zentralsymmetrisch und hat Volumen
$$\mathrm{vol}\,(S_t) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t^n}{n!}.$$

Beweis: Die Eigenschaft zentralsymmetrisch ist klar, die Eigenschaft konvex sieht man aus der Darstellung
$$S_t = \{(x_1, \ldots, x_{r_1}, y_1, z_1, \ldots, y_{r_2}, z_{r_2}) \in \mathbf{R}^n : \sum_{i=1}^{r_1} |x_i| + 2\sum_{j=1}^{r_2} |y_j + iz_j| \leq t\}$$
zusammen mit $|\lambda a + (1-\lambda)b| \leq \lambda|a| + (1-\lambda)|b|$ für $0 \leq \lambda \in \mathbf{R}$ und $a, b \in \mathbf{C}$.
Nun zur Volumenberechnung: Für y_j und z_j führen wir Polarkoordinaten u_j und φ_j ein: $y_j = u_j \cos\varphi_j$ und $z_j = u_j \sin\varphi_j$. Dann folgt wie üblich $dy_j dz_j = u_j du_j d\varphi_j$ und damit
$$\begin{aligned}
\mathrm{vol}\,(S_t) &= \int_{S_t} dx_1 \ldots dx_{r_1} dy_1 dz_1 \ldots dy_{r_2} dz_{r_2} = \\
&= \int_{\substack{\sum_i |x_i| + 2\sum_j u_j \leq t \\ u_j \geq 0, 0 \leq \varphi_j \leq 2\pi}} u_1 \ldots u_{r_2} dx_1 \ldots dx_{r_1} du_1 \ldots du_{r_2} d\varphi_1 \ldots d\varphi_{r_2} = \\
&= 2^{r_1}(2\pi)^{r_2} \int_{\substack{\sum x_i + 2\sum u_j \leq t \\ x_i \geq 0, u_j \geq 0}} u_1 \ldots u_{r_2} dx_1 \ldots dx_{r_1} du_1 \ldots du_{r_2}.
\end{aligned}$$
Zu zeigen ist also
$$(*) \qquad \int_{\substack{\sum x_i + 2\sum u_j \leq t \\ x_i \geq 0, u_j \geq 0}} u_1 \ldots u_{r_2} dx_1 \ldots dx_{r_1} du_1 \ldots du_{r_2} = \frac{1}{4^{r_2}} \frac{t^n}{n!}.$$
Wir beweisen dies durch Induktion nach r_2.
Im Fall $r_2 = 0$ lautet die Behauptung
$$\int_{\sum x_i \leq t, 0 \leq x_i} dx_1 \ldots dx_n = \frac{t^n}{n!},$$

die wir durch Induktion nach n zeigen: Der Fall $n = 1$ ist klar. Der Rest folgt mit

$$\begin{aligned}\int_{\sum x_i \le t, 0 \le x_i} dx_1 \dots dx_n &= \int_{x_n=0}^{t} \left[\int_{\sum x_i \le t - x_n, x_i \ge 0} dx_1 \dots dx_{n-1} \right] dx_n = \\ &= \int_{x_n=0}^{t} \frac{(t-x_n)^{n-1}}{(n-1)!} dx_n \overset{x_n = t-y}{=} \int_{y=0}^{t} \frac{y^{n-1}}{(n-1)!} dy = \frac{t^n}{n!}.\end{aligned}$$

Wir beweisen nun die Gleichung $(*)$ für r_2, wobei wir $(*)$ für $r_2 - 1$ voraussetzen:

$$\begin{aligned}&\int_{\substack{\sum x_i + 2 \sum u_j \le t \\ x_i \ge 0, u_j \ge 0}} u_1 \dots u_{r_2} dx_1 \dots dx_{r_1} du_1 \dots du_{r_2} = \\ = &\int_{u_{r_2}=0}^{t/2} [\int_{\sum x_i + 2 \sum u_j \le t - 2u_{r_2}} u_1 \dots u_{r_2 - 1} dx_1 \dots dx_{r_1} du_1 \dots du_{r_2 - 1}] u_{r_2} du_{r_2} = \\ = &\int_{u_{r_2}=0}^{t/2} \frac{1}{4^{r_2 - 1}} \frac{(t - 2u_{r_2})^{n-2}}{(n-2)!} u_{r_2} du_{r_2} \overset{u_{r_2} = v/2}{=} \frac{1}{4^{r_2}} \int_{v=0}^{t} \frac{(t-v)^{n-2} v dv}{(n-2)!} \overset{v = t-z}{=} \\ = &\frac{1}{4^{r_2}(n-2)!} \int_{z=0}^{t} z^{n-2}(t-z) dz = \frac{1}{4^{r_2}(n-2)!} \left[t \int_{z=0}^{t} z^{n-2} dz - \int_{z=0}^{t} z^{n-1} dz \right] = \\ = &\frac{1}{4^{r_2}(n-2)!} \left[t \frac{t^{n-1}}{n-1} - \frac{t^n}{n} \right] = \frac{1}{4^{r_2}} \frac{t^n}{n!},\end{aligned}$$

was die Behauptung schließlich beweist. ■

Lemma.

$$|\mathrm{N}(\alpha)| \le \frac{1}{n^n} \left(\sum_{j=1}^{r_1} |\sigma_j(\alpha)| + 2 \sum_{k=1}^{r_2} |\sigma_{r_1 + k}(\alpha)| \right)^n.$$

Anders ausgedrückt:

$$\phi(\alpha) \in S_t \quad \Longrightarrow \quad |\mathrm{N}(\alpha)| \le \left(\frac{t}{n} \right)^n.$$

Beweis: Mit der Ungleichung zwischen arithmetischem und geometrischem Mittel ergibt sich

$$\sqrt[n]{|\mathrm{N}(\alpha)|} = \sqrt[n]{|\sigma_1(\alpha)| \cdot \dots \cdot |\sigma_n(\alpha)|} \le \frac{|\sigma_1(\alpha)| + \dots + |\sigma_n(\alpha)|}{n} = \frac{1}{n} (\sum_{j=1}^{r_1} |\sigma_j(\alpha)| + 2 \sum_{k=1}^{r_2} |\sigma_{r_1 + k}(\alpha)|),$$

was die erste Aussage liefert. Die zweite Aussage folgt mit

$$\phi(\alpha) = (\sigma_1(\alpha), \dots, \sigma_{r_1}(\alpha), \mathrm{Re}\,(\sigma_{r_1+1}(\alpha)), \mathrm{Im}\,(\sigma_{r_1+1}(\alpha)), \dots, \mathrm{Re}\,(\sigma_{r_1+r_2}(\alpha)), \mathrm{Im}\,(\sigma_{r_1+r_2}\alpha)))$$

und

$$\sqrt{\mathrm{Re}\,(\sigma_{r_1+k}(\alpha))^2 + \mathrm{Im}\,(\sigma_{r_1+k}(\alpha))^2} = |\sigma_{r_1+k}(\alpha)| \text{ (für } k = 1, \dots, r_2)$$

aus der Definition von S_t. ■

Wir kommen nun zu der zentralen Aussage:

Satz. *Ist $\mathfrak{a}$ ein gebrochenes Ideal einer Ordnung R von K, so gibt es ein Element $\alpha \neq 0$ in $\mathfrak{a}$ mit*

$$|\mathrm{N}(\alpha)| \le \left(\frac{4}{\pi} \right)^{r_2} \frac{n!}{n^n} \sqrt{|\mathrm{disc}\,(R)|} \mathrm{N}\mathfrak{a}.$$

Beweis: $\phi(\mathfrak{a})$ ist ein Gitter vom Rang n in $\mathbf{R}^n$. Gilt nun $\mathrm{vol}\,(S_t) > 2^n \mathrm{vol}\,(\phi(\mathfrak{a}))$, so gibt es nach dem Gitterpunktsatz ein $\alpha \in \mathfrak{a}$, $\alpha \neq 0$ mit $\phi(\alpha) \in S_t$. Wir haben (wegen $\mathrm{disc}\,(\mathfrak{a}) = [R : \mathfrak{a}]^2 \mathrm{disc}\,(R) = (\mathrm{N}\mathfrak{a})^2 \mathrm{disc}\,(R)$)

$$\mathrm{vol}\,(\phi(\mathfrak{a})) = (\frac{1}{2})^{r_2} \sqrt{|\mathrm{disc}\,(\mathfrak{a})|} = (\frac{1}{2})^{r_2} \sqrt{|\mathrm{disc}\,(R)|} \mathrm{N}\mathfrak{a} \quad \text{und} \quad \mathrm{vol}\,(S_t) = 2^{r_1} \left(\frac{\pi}{2} \right)^{r_2} \frac{t^n}{n!}.$$

Damit gilt:

$$\begin{aligned}\mathrm{vol}\,(S_t) > 2^n \mathrm{vol}\,(\phi(\mathfrak{a})) \quad &\Longleftrightarrow \quad 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{t^n}{n!} > 2^n\cdot(\frac{1}{2})^{r_2}\sqrt{\mathrm{disc}\,(R)|}\mathrm{N}\mathfrak{a} \iff \\ &\Longleftrightarrow \quad \left(\frac{t}{n}\right)^n > \left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}\sqrt{|\mathrm{disc}\,(R)|}\mathrm{N}\mathfrak{a}.\end{aligned}$$

Wir wählen nun ein $\varepsilon > 0$ mit

$$\left\lfloor\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}\sqrt{|\mathrm{disc}\,(R)|}\right\rfloor = \left\lfloor\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}\sqrt{|\mathrm{disc}\,(R)|}+\varepsilon\right\rfloor$$

und $t > 0$ mit

$$\left(\frac{t}{n}\right)^n = \left[\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}\sqrt{|\mathrm{disc}\,(R)|}+\varepsilon\right]\mathrm{N}\mathfrak{a}.$$

Dann gibt es nach dem Minkowskischen Gitterpunktsatz ein $\alpha \in \mathfrak{a}$, $\alpha \neq 0$ mit $\phi(\alpha) \in S_t$ und damit

$$|\mathrm{N}(\alpha)| \leq \left(\frac{t}{n}\right)^n = \left[\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}\sqrt{|\mathrm{disc}\,(R)|}+\varepsilon\right]\mathrm{N}\mathfrak{a}.$$

Wegen $\mathrm{N}\mathfrak{a}|\mathrm{N}(\alpha)$ folgt

$$\frac{|\mathrm{N}(\alpha)|}{\mathrm{N}\mathfrak{a}} \leq \left\lfloor\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}\sqrt{|\mathrm{disc}\,(R)|}+\varepsilon\right\rfloor = \left\lfloor\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}\sqrt{|\mathrm{disc}\,(R)|}\right\rfloor \leq \left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}\sqrt{|\mathrm{disc}\,(R)|},$$

was zu zeigen war. ■

6. Die Minkowskische Diskriminantenabschätzung

SATZ. *Ist K ein Zahlkörper vom Grad n mit r_1 reellen und $2r_2$ komplexen Einbettungen ($n = r_1 + 2r_2$), dann gilt*

$$|\mathrm{disc}\,\mathbf{Z}_K| \geq (\frac{\pi}{4})^{2r_2}\frac{n^{2n}}{(n!)^2}.$$

Beweis: Wir haben gezeigt, dass jedes gebrochene Ideal $\mathfrak{a}$ einer Ordnung R ein Element $\alpha \neq 0$ enthält mit

$$|\mathrm{N}(\alpha)| \leq \left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}\sqrt{|\mathrm{disc}\,(R)|}\mathrm{N}\mathfrak{a}.$$

Wählt man nun $R = \mathbf{Z}_K$, $\mathfrak{a} = \mathbf{Z}_K$, so folgt die Behauptung wegen $|\mathrm{N}\alpha| \geq 1$. ■

Bemerkung: Die folgende Tabelle enthält explizite Werte für die Abschätzung $M(n, r_1, r_2) = (\frac{\pi}{4})^{2r_2}\frac{n^{2n}}{(n!)^2}$, sowie in den kleinsten Fällen die Zahlkörper mit den kleinsten Diskriminanten.

n	r_1	r_2	$M(n, r_1, r_2)$	
1	1	0	1.00	$\mathrm{disc}\,\mathbf{Q} = 1$
2	2	0	4.00	$\mathrm{disc}\,\mathbf{Q}(\sqrt{5}) = 5$
2	0	1	2.47	$\mathrm{disc}\,\mathbf{Q}(\sqrt{-3}) = -3$
3	3	0	20.25	
3	1	1	12.49	
4	4	0	113.78	
4	2	1	70.18	
4	0	2	43.29	
5	5	0	678.17	
5	3	1	418.33	
5	1	2	258.05	

Eine schlechte, wenn auch für unsere Zwecke hinreichende Abschätzung macht folgende Folgerung:

FOLGERUNG. *Für die Diskriminante* $\mathrm{disc}\,(K)$ *eines Zahlkörpers K vom Grad n gilt*

$$|\mathrm{disc}\,(K)| \geq 3^{n-1}.$$

Beweis: Wir setzen

$$d_n = (\frac{\pi}{4})^n \frac{n^{2n}}{n!^2}$$

und erhalten dann wegen $n = r_1 + 2r_2 \geq 2r_2$

$$|\mathrm{disc}\,(K)| \geq (\frac{\pi}{4})^{2r_2} \frac{n^{2n}}{n!^2} \geq (\frac{\pi}{4})^n \frac{n^{2n}}{n!^2} = d_n.$$

Es gilt

$$\frac{d_{n+1}}{d_n} = \frac{\pi}{4} \cdot \frac{(n+1)^{2n+2}}{(n+1)!^2} \cdot \frac{n!^2}{n^{2n}} = \frac{\pi}{4} \cdot \frac{(n+1)^{2n}}{n!^2} \cdot \frac{n!^2}{n^{2n}} = \frac{\pi}{4}(1+\frac{1}{n})^{2n}.$$

Nun ist

$$\ln(1+\frac{1}{n}) = \frac{1}{n} - \frac{1}{2n^2} + \frac{1}{3n^3} - \frac{1}{4n^4} + - \ldots,$$

woraus man bekanntlich die Abschätzung

$$\ln(1+\frac{1}{n}) \geq \frac{1}{n} - \frac{1}{2n^2}, \quad \text{also} \quad \ln(1+\frac{1}{n})^{2n} = 2n\ln(1+\frac{1}{n}) \geq 2 - \frac{1}{n}$$

und damit

$$\frac{d_{n+1}}{d_n} \geq \frac{\pi}{4} e^{2-\frac{1}{n}} \geq 3.5 \text{ für } n \geq 2$$

erhält. Es ist $d_3 \approx 9.8 \geq 9$ und damit für $n \geq 3$:

$$d_n \geq 3d_{n-1} \geq 3^2 d_{n-2} \geq 3^{n-3} d_3 \geq 3^{n-3} \cdot 3^2 = 3^{n-1}.$$

Damit folgt für $n \geq 3$ die zweite Abschätzung. Für $n = 2$ ist $d_2 \approx 2.5$ und damit $|\mathrm{disc}\,(K)| \geq 3$, was schließlich auch die letzte Behauptung zeigt. ■

Folgerung. **Q** *besitzt keine unverzweigten Erweiterungen, d.h. ist K ein Zahlkörper $\neq \mathbf{Q}$, so gibt es immer Primzahlen, die in $\mathbf{Z}_K$ verzweigen.*

Beweis: Ist K ein Zahlkörper vom Grad $n \geq 2$, so folgt aus unserer Abchätzung $|\mathrm{disc}\,(K)| \geq 3^{n-1} \geq 3$. Also gibt es eine Primzahl p mit $p|\mathrm{disc}\,(K)$, die somit in $\mathbf{Z}_K$ verzweigt. ■

7. Die Endlichkeit der Klassengruppe $C\ell(R)$

Sei R Ordnung eines Zahlkörpers K. Die Gruppe I_R der invertierbaren gebrochenen Ideale von R enthält als Untergruppe die Gruppe der Hauptideale. Die Faktorgruppe $C\ell(R) = I_R/H_R$ wird durch folgende Äquivalenzrelation definiert:

$$\mathfrak{a} \sim \mathfrak{b} \iff \mathfrak{a}\mathfrak{b}^{-1} \in H_R \iff \mathfrak{a} = \lambda\mathfrak{b} \text{ für ein } \lambda \in K^*.$$

Die Gruppe $C\ell(R)$ wird Klassengruppe von R genannt. Man sagt, die Ideale $\mathfrak{a}$ und $\mathfrak{b}$ liegen in der gleichen Klasse, wenn $\mathfrak{a} \sim \mathfrak{b}$ gilt.
Eine wesentliche Folgerung des Minkowskischen Gitterpunktsatzes ist nun:

Satz. *In jeder Idealklasse von R gibt es ein ganzes Ideal $\mathfrak{a}$ mit*

$$\mathrm{N}\mathfrak{a} \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|\mathrm{disc}\,(R)|}.$$

Beweis: Sei $c \in C\ell(R)$ und $\mathfrak{b}$ ein Repräsentant von c. Dann gibt es ein $\alpha \in \mathfrak{b}^{-1}$, $\alpha \neq 0$ mit

$$\mathrm{N}(\alpha) \leq (\frac{4}{\pi})^{r_2} \frac{n!}{n^n} \sqrt{|\mathrm{disc}\,(R)|}\mathrm{N}\mathfrak{b}^{-1}.$$

Wir setzen $\mathfrak{a} = \alpha\mathfrak{b}$. Dann ist $\mathfrak{a}$ ein ganzes Ideal wegen $\mathfrak{a} = \alpha\mathfrak{b} \subseteq \mathfrak{b}^{-1}\mathfrak{b} = R$, offensichtlich $\mathfrak{a} \sim \mathfrak{b}$, also $\overline{\mathfrak{a}} = c$ und

$$\mathrm{N}\mathfrak{a} = \frac{|\mathrm{N}\alpha|}{\mathrm{N}\mathfrak{b}^{-1}} \leq (\frac{4}{\pi})^{r_2} \frac{n!}{n^n} \sqrt{|\mathrm{disc}\,(R)|},$$

wie behauptet. ■

Die Zahl $(\frac{4}{\pi})^{r_2} \frac{n!}{n^n} \sqrt{|\mathrm{disc}\,(K)|}$ wird auch als Minkowski-Schranke für K bezeichnet.

FOLGERUNG. *Die Klassengruppe $C\ell(R)$ ist endlich. Die Ordnung $\#C\ell(R)$ wird als Klassenzahl h_R bezeichnet. Im Fall $R = \mathbf{Z}_K$ schreibt man auch h_K.*

Beweis: Da es nur endlich viele ganze Ideale mit Norm $\leq (\frac{4}{\pi})^{r_2} \frac{n!}{n^n} \sqrt{|\mathrm{disc}\,(R)|}$ gibt, folgt die Aussage aus dem letzten Satz. ■

Bemerkung: Im Fall $R = \mathbf{Z}_K$ ist jedes Ideal $\neq 0$ invertierbar. Also gilt:

$$\mathbf{Z}_K \text{ Hauptidealring} \iff h_K = 1.$$

FOLGERUNG. *Die Klassengruppe $C\ell(\mathbf{Z}_K)$ wird von den Primidealen $\mathfrak{p} \subseteq \mathbf{Z}_K$ mit*

$$N\mathfrak{p} \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|\mathrm{disc}\,(K)|}$$

erzeugt. Genau dann ist $\mathbf{Z}_K$ ein Hauptidealring, wenn jedes dieser Primideale ein Hauptideal ist.

Beweis: In $\mathbf{Z}_K$ ist jedes Ideal $\neq 0$ Produkt von Primidealen:

$$\mathfrak{a} = \prod_i \mathfrak{p}_i^{v_{\mathfrak{p}}(\mathfrak{a})} \quad \text{und} \quad \mathrm{N}\mathfrak{a} = \prod_i p_i^{f_i v_{\mathfrak{p}}(\mathfrak{a})} \text{ mit } \mathrm{N}\mathfrak{p}_i = p_i^{f_i}.$$

Da jede Idealklasse ein ganzes Ideal mit Norm $\leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|\mathrm{disc}\,(K)|}$ enthält, folgt die Behauptung. ■

Wir wollen nun für einige einfache Beispiele die Klassengruppe $C\ell(R)$ explizit bestimmen.

Beispiel: Für $K = \mathbf{Q}(\sqrt[3]{2})$ ist $\mathbf{Z}_K = \mathbf{Z}[\sqrt[3]{2}]$ mit $\mathrm{disc}\,(\mathbf{Z}_K) = -108$. Jede Idealklasse enthält ein ganzes Ideal mit Norm $\leq \frac{4}{\pi} \frac{3!}{3^3} \sqrt{108} \leq 2.95$. Nun ist

$$(2) = (\sqrt[3]{2})^3$$

die Primidealzerlegung von 2, also ist $(\sqrt[3]{2})$ das einzige Ideal mit Norm 2 und Hauptideal. Somit ist $h_K = 1$ und $\mathbf{Z}_K$ Hauptidealring.

Beispiel: Für $K = \mathbf{Q}(\sqrt{-23})$ ist $\mathbf{Z}_K = \mathbf{Z}[\frac{1+\sqrt{-23}}{2}]$ mit Diskriminante -23. Wir schreiben $\alpha = \frac{1+\sqrt{-23}}{2}$ (mit Minimalpolynom $f = x^2 - x + 6$). Jede Idealklasse enthält ein ganzes Ideal mit Norm $\leq \frac{2}{\pi}\sqrt{23} \leq 3.06$. Die Ideale mit Norm ≤ 3 sind

$$(1), \quad \mathfrak{p}_{2a} = (2, \alpha), \quad \mathfrak{p}_{2b} = (2, \alpha + 1), \quad \mathfrak{p}_{3a} = (3, \alpha), \quad \mathfrak{p}_{3b} = (3, \alpha + 2).$$

Man findet leicht die Relationen:

$$\mathfrak{p}_{2a}\mathfrak{p}_{2b} = (2), \quad \mathfrak{p}_{3a}\mathfrak{p}_{3b} = (3), \quad \mathfrak{p}_{2a}\mathfrak{p}_{3a} = (\alpha).$$

Für das Hauptideal $(u\alpha + v)$ gilt

$$\mathrm{N}(u\alpha + v) = 6u^2 + uv + v^2 = \frac{23}{4}u^2 + (\frac{1}{2}u + v)^2 = 5.75u^2 + (0.5u + v)^2,$$

woraus man sofort sieht, dass es kein Hauptideal mit Norm 2 oder 4 gibt. Also sind $\mathfrak{p}_{2a}$ und $\mathfrak{p}_{2a}^2$ keine Hauptideale. Nun ist

$$\mathfrak{p}_{2a}^3 = (\alpha - 2),$$

d.h. $\mathfrak{p}_{2a}$ hat Ordnung 3 in der Klassengruppe. Mit den obigen Relationen erhält man

$$\mathfrak{p}_{2b} = \frac{\alpha + 1}{4}\mathfrak{p}_{2a}^2, \quad \mathfrak{p}_{3a} = \frac{\alpha - 3}{4}\mathfrak{p}_{2a}^2, \quad \mathfrak{p}_{3b} = \frac{\alpha - 1}{2}\mathfrak{p}_{2a}.$$

Daher ist $C\ell(\mathbf{Z}_K)$ zyklisch von Ordnung 3, also $h_K = 3$.

Beispiel: $K = \mathbf{Q}(\sqrt{-163})$ hat Ganzheitsring $\mathbf{Z}_K = \mathbf{Z}[\frac{1+\sqrt{-163}}{2}]$ mit Diskriminante -163. Jede Idealklasse enthält ein ganzes Ideal mit Norm ≤ 8.13. Das Minimalpolynom von $\frac{1+\sqrt{-163}}{2}$ ist $f = x^2 - x + 41$. Für $p = 2, 3, 5, 7$ ist $f \bmod p$ irreduzibel, d.h. (2), (3), (5), (7) sind Primideale, das einzige Primideal mit Norm ≤ 8 ist also (2). Somit ist $h_K = 1$ und $\mathbf{Z}[\frac{1+\sqrt{-163}}{2}]$ Hauptidealring.

Beispiel: Für $K = \mathbf{Q}(\alpha)$ mit $\alpha^3 + 7\alpha + 20 = 0$ ist

$$\mathbf{Z}_K = \mathbf{Z}\frac{\alpha^2 + \alpha}{2} + \mathbf{Z}\alpha + \mathbf{Z} \quad \text{mit} \quad \mathrm{disc}\,(\mathbf{Z}_K) = -3043.$$

Jede Idealklasse enthält ein ganzes Ideal mit Norm $\leq \frac{4}{\pi}\frac{3!}{3^3}\sqrt{3043} \leq 15.61$. Nun haben wir früher sämtliche Ideale von $\mathbf{Z}_K$ mit Norm ≤ 15 aufgelistet und gesehen, dass sie Hauptideale sind. Also ist $h_K = 1$ und $\mathbf{Z}_K$ Hauptidealring.

Beispiel: $K = \mathbf{Q}(\alpha)$ mit $\alpha^3 + \alpha^2 - 2\alpha + 8 = 0$ hat Diskriminante -503, eine $\mathbf{Z}$-Basis von $\mathbf{Z}_K$ ist

$$\omega_1 = \frac{\alpha^2 + \alpha}{2}, \quad \omega_2 = \alpha, \quad \omega_3 = 1.$$

Die Minkowskischranke liefert, dass jede Idealklasse ein ganzes Ideal mit Norm ≤ 6.35 enthält. Nun ist

$$\mathfrak{p}_1 = (3\omega_1 - 4\omega_2 + 4\omega_3), \quad \mathfrak{p}_2 = (\omega_1 - \omega_2 + \omega_3), \quad \mathfrak{p}_3 = (2\omega_1 - 3\omega_2 + 3\omega_3) \quad \text{mit} \quad \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 = (2).$$

(3) ist Primideal. $f(x) \equiv (x+1)(x^2+3) \bmod 5$ liefert, dass es genau ein Primideal mit Norm 5 gibt, nämlich

$$\mathfrak{q}_5 = (5, \alpha + 1) = (2\omega_1 - 5\omega_3).$$

Die einzigen Primideale mit Norm ≤ 6 sind also Hauptideale, $\mathbf{Z}_K$ ist damit Hauptidealring und $h_K = 1$.

Beispiel: $K = \mathbf{Q}(\sqrt{2}, \sqrt{3})$. Dann ist $\mathbf{Z}_K = \mathbf{Z}[\alpha]$ mit $f = x^4 - 4x^2 + 1$ und $f(\alpha) = 0$. Die Diskriminante ist $2^8 \cdot 3^2$, die Minkowskischranke ≤ 4.5. Nun erhält man durch Faktorisierung von $f \bmod p$ die 2 und 3 enthaltenden Primideale:

$$\mathfrak{p}_2 = (2, \alpha + 1) \text{ mit } \mathfrak{p}_2^4 = (2), \quad \mathfrak{p}_{3^2} = (3, \alpha^2 + 1) \text{ mit } \mathfrak{p}_{3^2}^2 = (3).$$

Das einzige Primideal mit Norm ≤ 4.5 ist $\mathfrak{p}_2$, das wegen $\mathrm{N}(\alpha + 1) = -2$ das Hauptideal $(\alpha + 1)$ ist. Also ist $h_K = 1$ und $\mathbf{Z}_K$ ein Hauptidealring.

Beispiel: Wir betrachten die nichtmaximale Ordnung $R = \mathbf{Z}[\sqrt{-3}]$, die Diskriminante -12 hat. Die Minkowski-Schranke ist ≤ 2.21. Das einzige Ideal $\neq (1)$ mit Norm ≤ 2 ist $\mathfrak{p} = (2, 1 + \sqrt{-3})$, das aber wegen $\mathfrak{p}^2 = 2\mathfrak{p}$ nicht invertierbar ist. Daher ist (1) das einzige ganze invertierbare Ideal mit Norm ≤ 2 und somit $C\ell(R) = 1$ und $h_R = 1$.

8. Elemente kleiner Norm II

Der folgende Satz zeigt, wie man im Prinzip Elemente kleiner Norm in Idealen finden kann:

SATZ. *Sei $\mathfrak{a} \neq 0$ ein gebrochenes Ideal einer Ordnung R, $\alpha_1, \ldots, \alpha_n$ eine $\mathbf{Z}$-Basis von $\mathfrak{a}$ und $\beta_1, \ldots, \beta_n$ die duale Basis, d.h. $\mathrm{Sp}(\alpha_i\beta_j) = \delta_{ij}$. Dann gilt:*

1. $$\lambda = x_1\alpha_1 + \cdots + x_n\alpha_n \in \mathfrak{a} \text{ mit } \phi(\lambda) \in S_t \quad \Longrightarrow \quad |x_i| \leq \max_{1\leq j\leq n} |\sigma_j\beta_i| \cdot t.$$
   (Daher kann man alle Elemente $\lambda \in \mathfrak{a}$ mit $\phi(\lambda) \in S_t$ explizit aufzählen.)
2. *Es gibt ein $\lambda = x_1\alpha_1 + \cdots + x_n\alpha_n \in \mathfrak{a}$, $\lambda \neq 0$, mit*
$$\frac{|\mathrm{N}(\lambda)|}{N\mathfrak{a}} \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}\sqrt{|\mathrm{disc}\,(R)|} \quad \text{und} \quad |x_i| \leq \max_{1\leq j\leq n} |\sigma_j\beta_i| \cdot \left[\left(\frac{4}{\pi}\right)^{r_2} n!\sqrt{|\mathrm{disc}\,(R)|}\mathrm{N}\mathfrak{a}\right]^{1/n}.$$

Beweis: Ist $\lambda = x_1\alpha_1 + \cdots + x_n\alpha_n$, so gilt wegen $\mathrm{Sp}(\alpha_k\beta_i) = \delta_{ki}$

$$x_i = \sum_k x_k \mathrm{Sp}(\alpha_k\beta_i) = \mathrm{Sp}(\lambda\beta_i) = \sum_j \sigma_j\lambda\sigma_j\beta_i \quad \text{und somit} \quad |x_i| \leq \max_j |\sigma_j\beta_i| \cdot \sum_j |\sigma_j\lambda|.$$

Nun ist $\phi(\alpha) \in S_t$ gleichwertig mit $\sum_j |\sigma_j\lambda| \leq t$, also folgt

$$|x_i| \leq \max_j |\sigma_j\beta_i| \cdot t,$$

wie behauptet. Wählt man nun

$$t = \left[\left(\frac{4}{\pi}\right)^{r_2} n!\sqrt{|\mathrm{disc}\,(R)|}\mathrm{N}\mathfrak{a}\right]^{1/n},$$

so ist man genau in der Situation des Hauptsatzes, d.h. es existiert ein $\lambda \in \mathfrak{a} \setminus \{0\}$ mit $\phi(\lambda) \in S_t$. Wie früher folgt die Normabschätzung, der Rest folgt aus 1. ■

Beispiel: Wir betrachten $K = \mathbf{Q}(\alpha)$ mit $\alpha^3+7\alpha+20 = 0$. Der Ganzheitsring $\mathbf{Z}_K$ hat die Ganzheitsbasis $\omega_1 = \frac{\alpha^2+\alpha}{2}$, $\omega_2 = \alpha$, $\omega_3 = 1$ und Diskriminante -3043. Es ist

$$\sigma_1(\alpha) \approx -1.89106, \quad \sigma_2(\alpha) \approx 0.94553 - 3.11160i, \quad \sigma_3(\alpha) \approx 0.94553 + 3.11160i,$$

also $r_1 = r_2 = 1$. Nach Minkowski enthält jedes Ideal $\mathfrak{a} \neq 0$ ein Element $\lambda \neq 0$ mit $\frac{|N(\lambda)|}{N\mathfrak{a}} \leq 15$.

1. Wir betrachten das Ideal $\mathfrak{a}_5 = (5, \alpha)$, das als (normalisierte) $\mathbf{Z}$-Basis

$$\alpha_1 = \omega_1 = \frac{\alpha^2+\alpha}{2}, \quad \alpha_2 = \omega_2 = \alpha, \quad \alpha_3 = 5\omega_3 = 5$$

hat. Die Dualbasis ist

$$\beta_1 = \frac{21}{3043}\alpha^2 - \frac{90}{3043}\alpha + \frac{98}{3043}, \quad \beta_2 = -\frac{111}{6086}\alpha^2 + \frac{41}{6086}\alpha - \frac{259}{3043}, \quad \beta_3 = \frac{49}{15215}\alpha^2 - \frac{42}{3043} + \frac{1243}{15215}$$

und

$$\max_{1\leq j\leq 3} |\sigma_j\beta_i| \leq 0.11282, \quad 0.16308, \quad 0.11932 \quad \text{für} \quad i = 1, 2, 3.$$

Wie im letzten Satz wählen wir

$$t = \left[\left(\frac{4}{\pi}\right)^{r_2} n!\sqrt{|\mathrm{disc}\,(\mathbf{Z}_K)|}\mathrm{N}\mathfrak{a}\right]^{1/n} \approx 12.82018$$

und erhalten dann für Elemente $\lambda = x_1\alpha_1 + x_2\alpha_2 + x_3\alpha_3 \in \mathfrak{a}_5$ mit $\phi(\lambda) \in S_t$ die Abschätzungen

$$|x_1| \leq 1, \quad |x_2| \leq 2, \quad |x_3| \leq 1.$$

Wir bestimmen nun alle solchen λ's mit $\frac{|\mathrm{N}(\lambda)|}{\mathrm{N}\mathfrak{a}} \leq 15$ und erhalten folgende Liste:

λ	$\frac{N(\lambda)}{N\mathfrak{a}_5}$	$\sum_j \lvert\sigma_i\lambda\rvert$	$\phi(\lambda) \in S_t$?
α_2	-4	8.39	ja
$\alpha_1 - 2\alpha_2 - \alpha_3$	-9	22.27	nein
$\alpha_1 - 2\alpha_2 + \alpha_3$	7	13.44	nein
$\alpha_1 - \alpha_2$	14	12.85	nein
$\alpha_1 - \alpha_2 + \alpha_3$	3	10.52	ja
α_1	6	12.78	ja
$\alpha_1 + \alpha_2$	-14	17.39	nein

Allerdings haben wir keinen Erzeuger des Hauptideals $\mathfrak{a}_5 = (21\alpha_1 + 12\alpha_2 + \alpha_3)$ gefunden.

2. Wir betrachten das einzige Primideal $\mathfrak{p}$ mit Norm

$$p = 2^{128} - 173 = 340282366920938463463374607431768211283.$$

Man kann schreiben

$$\mathfrak{p} = (p, \alpha + 264268547492017156591560000458929396806).$$

Als normalisierte $\mathbf{Z}$-Basis von $\mathfrak{p}$ findet man

$$\begin{aligned}
\alpha_1 &= \frac{\alpha^2+\alpha}{2} + 272220783624752510100293485520492691 47, \\
\alpha_2 &= \alpha + 264268547492017156591560000458929396806, \\
\alpha_3 &= 340282366920938463463374607431768211283
\end{aligned}$$

Wendet man den Satz an, um ein Element $\lambda = x_1\alpha_1 + x_2\alpha_2 + x_3\alpha_3$ mit $|\mathrm{N}(\lambda)| \leq 15 \cdot \mathrm{N}\mathfrak{p}$ zu finden, so erhält man die Abschätzungen

$$|x_1| \leq 7439728834064, \quad |x_2| \leq 10754339754498, \quad |x_3| \leq 7756819398913.$$

Wir haben nicht versucht, ein solches Element λ auf diesem Weg zu finden.

Bemerkungen:

1. Bei obigem Verfahren erhält man nicht notwendig ein Element $\lambda \in \mathfrak{a} \setminus \{0\}$ mit minimaler Norm. Insbesondere kann man nicht sicher sein, ob $\mathfrak{a}$ Hauptideal ist oder nicht, falls man kein Element $\lambda \in \mathfrak{a}$ mit $|\mathrm{N}(\lambda)| = \mathrm{N}\mathfrak{a}$ gefunden hat.
2. Bei größeren Zahlen kann man das Verfahren praktisch nicht mehr durchführen.

9. LLL-Reduktion

Ist $\Gamma \subseteq \mathbf{R}^n$ ein Gitter vom Rang m, das durch eine Gitterbasis $b_1, \ldots, b_m$ gegeben ist, so ist im Allgemeinfall nicht klar, wie man daraus eine 'schöne' Gitterbasis gewinnen kann, wobei z.B. $\|b_1\|$ ein Vektor kürzester Länge ist.
Auf L. Lovász, H.W. Lenstra und A.K. Lenstra (1982) geht der im folgenden beschriebene LLL-Algorithmus zurück, der zwar nicht unbedingt eine 'beste' Gitterbasis liefert, dafür aber eine mit überblickbaren Eigenschaften. Außerdem ist der LLL-Algorithmus praktikabel.

Wir erinnern zunächst an das Gram-Schmidt-Orthogonalisierungsverfahren für linear unabhängige Vektoren $b_1, \ldots, b_m \in \mathbf{R}^n$. Man definiert rekursiv:

$$\begin{aligned} b_1^* &= b_1, \\ b_i^* &= b_i - \sum_{j=1}^{i-1} \mu_{ij} b_j^* \text{ für } i = 2, \ldots, r \text{ mit } \mu_{ij} = \frac{b_i \cdot b_j^*}{\|b_j^*\|^2} \end{aligned}$$

Wir geben einige einfache Eigenschaften an:

1. $\mathbf{R}b_1 + \cdots + \mathbf{R}b_i = \mathbf{R}b_1^* + \cdots + \mathbf{R}b_i^*$ für $i = 1, \ldots, m$ und $b_i^* \cdot b_j^* = 0$ für $i > j$.
2. $\|b_i\|^2 = \|b_i^*\|^2 + \sum_{j<i} \mu_{ij}^2 \|b_j^*\|^2$, insbesondere $\|b_i^*\| \leq \|b_i\|$.
3. Bei Basiswechsel $v_i = \sum_k a_{ij} w_j$ gilt mit $A = (a_{ij})$ für die Gramschen Matrizen $(v_i \cdot v_j) = A(w_i \cdot w_j)A^t$, insbesondere $\det(v_i \cdot v_j) = (\det A)^2 \det(w_i \cdot w_j)$, was hier sofort

$$\operatorname{vol}(\mathbf{Z}b_1 + \cdots + \mathbf{Z}b_r) = \sqrt{\det(b_i \cdot b_j)} = \sqrt{\det(b_i^* \cdot b_j^*)} = \prod_i \|b_i^*\| \leq \prod_i \|b_i\|$$

liefert. Im Fall $m = n$ folgt daraus die Hadamardsche Determinantenabschätzung:

$$|\det(b_1, \ldots, b_n)| \leq \|b_1\| \cdots \|b_n\|.$$

1. Idee: Seien $i_0 > j_0$ Indizes und $k \in \mathbf{Z}$. Ersetzt man b_{i_0} durch

$$b'_{i_0} = b_{i_0} + k b_{j_0},$$

so bleibt die Gram-Schmidt-Orthogonalisierung gleich, die μ_{ij}'s ändern sich wie folgt:

$$\mu'_{ij} = \begin{cases} \mu_{ij} & \text{für } i \neq i_0, \\ \mu_{i_0 j} & \text{für } i = i_0, j > j_0, \\ \mu_{i_0 j_0} + k & \text{für } i = i_0, j = j_0, \\ \mu_{i_0 j} + k\mu_{j_0 j} & \text{für } i = i_0, j < j_0. \end{cases}$$

Ersetzt man nacheinander für $i = 2, 3, \ldots, m$, für $j = i-1, i-2, \ldots, 1$ den Gittervektor b_i durch

$$b'_i = b_i - \lfloor \mu_{ij} \rceil b_j,$$

so gilt bei der neuen Gitterbasis

$$|\mu_{ij}| \leq \frac{1}{2}.$$

2. Idee: Wir vertauschen zwei benachbarte Gittervektoren b_i und b_{i-1}. Bei der Gram-Schmidt-Orthogonalisierung ändern sich nur b_i^* und b_{i-1}^*, z.B. ${b'_{i-1}}^* = \mu_{i,i-1} b_{i-1}^* + b_i^*$. Wegen

$$\operatorname{vol}(\Gamma) = \prod_{i=1}^{r} \|b_i^*\| = \prod_{i=1}^{r} \|{b'_i}^*\|$$

bleibt das Produkt $\|b_{i-1}^*\|\|b_i^*\|$ gleich. $\|b_{i-1}^*\|^2$ ändert sich um folgenden Faktor:

$$c_{i,i-1} = \frac{\|{b'_{i-1}}^*\|^2}{\|b_{i-1}^*\|^2} = \frac{\|b_i^*\|^2}{\|b_{i-1}^*\|^2} + \mu_{i,i-1}^2.$$

Die Idee ist nun, b_i mit b_{i-1} zu vertauschen, wenn dann $\|{b'_{i-1}}^*\|^2 < \frac{3}{4}\|b^*_{i-1}\|^2$ gilt. (Statt $\frac{3}{4}$ kann man auch eine andere Konstante c wählen.) Wir haben

$$\begin{aligned} \|{b'_{i-1}}^*\|^2 < \frac{3}{4}\|b^*_{i-1}\|^2 \quad &\Longleftrightarrow \quad \|\mu_{i,i-1}b^*_{i-1} + b^*_i\|^2 < \frac{3}{4}\|b^*_{i-1}\|^2 \\ &\Longleftrightarrow \quad \mu^2_{i,i-1}\|b^*_{i-1}\|^2 + \|b^*_i\|^2 < \frac{3}{4}\|b^*_{i-1}\|^2 \\ &\Longleftrightarrow \quad \|b^*_i\|^2 < (\frac{3}{4} - \mu^2_{i,i-1})\|b^*_{i-1}\|^2. \end{aligned}$$

Kann man eine Gitterbasis $b_1, \ldots, b_m$ durch die 1. oder 2. Idee nicht mehr abändern, so spricht man von einer LLL-reduzierten Basis:

DEFINITION. Sei $\Gamma \subseteq \mathbf{R}^n$ ein Gitter vom Rang m und $b_1, \ldots, b_m$ eine Gitterbasis. Seien $b^*_1, \ldots, b^*_m$ (wie oben) rekursiv definiert durch

$$b^*_1 = b_1, \quad b^*_i = b_i - \sum_{1 \le j < i} \mu_{ij} b^*_j \quad \text{mit} \quad \mu_{ij} = \frac{b_i \cdot b^*_j}{b^*_j \cdot b^*_j}.$$

Die Gitterbasis $b_1, \ldots, b_m$ heißt LLL-reduziert, wenn gilt

$$|\mu_{ij}| \le \frac{1}{2} \text{ für } 1 \le j < i \le m \quad \text{und} \quad \|b^*_i\|^2 \ge (\frac{3}{4} - \mu^2_{i,i-1})\|b^*_{i-1}\|^2 \text{ für } 1 < i \le m \text{ (Lovász-Bedingung)}.$$

Wir geben zunächst die schönen Eigenschaften von LLL-reduzierten Gitterbasen an:

SATZ. *Sei $b_1, \ldots, b_m$ eine LLL-reduzierte Basis des Gitters Γ. Dann gilt:*

1. $$\operatorname{vol}(\Gamma) \le \prod_{i=1}^{m} ||b_i|| \le 2^{\frac{m(m-1)}{4}} \operatorname{vol}(\Gamma).$$
2. $$||b_1|| \le 2^{\frac{m-1}{4}} \operatorname{vol}(\Gamma)^{\frac{1}{m}}.$$
3. *Sind $x_1, \ldots, x_t \in \Gamma$ linear unabhängig, so gilt*
$$||b_1||, ||b_2||, \ldots, ||b_t|| \le 2^{\frac{m-1}{2}} \max(||x_1||, ||x_2||, \ldots, ||x_t||).$$
4. *Für jedes $x \in \Gamma \setminus \{0\}$ gilt*
$$||b_1|| \le 2^{\frac{m-1}{2}} ||x||.$$

Beweis:

- Wegen $|\mu_{i,i-1}| \le \frac{1}{2}$ folgt aus der Lovasz-Bedingung
$$\|b^*_j\|^2 \ge (\frac{3}{4} - \mu^2_{i,i-1})\|b^*_{i-1}\|^2 \ge \frac{1}{2}\|b^*_{j-1}\|^2$$
und daher durch Induktion
$$\|b^*_j\|^2 \le 2^{i-j}\|b^*_i\|^2 \text{ für } j \le i.$$
Mit $|\mu_{ij}| \le \frac{1}{2}$ ergibt sich dann damit
$$\begin{aligned} \|b_i\|^2 &= \|b^*_i\|^2 + \mu^2_{i,i-1}\|b^*_{i-1}\|^2 + \cdots + \mu^2_{i,1}\|b^*_1\|^2 \le \|b^*_i\|^2 + \frac{1}{4}\|b^*_{i-1}\|^2 + \cdots + \frac{1}{4}\|b^*_1\|^2 \le \\ &\le \left[1 + \frac{1}{4}(2 + 2^2 + \cdots + 2^{i-1})\right] \|b^*_i\|^2 = \frac{2^{i-1}+1}{2}\|b^*_i\|^2 \le 2^{i-1}\|b^*_i\|^2. \end{aligned}$$
Für $j \le i$ folgt
$$\|b_j\|^2 \le 2^{j-1}\|b^*_j\|^2 \le 2^{j-1} \cdot 2^{i-j}\|b^*_i\|^2 = 2^{i-1}\|b^*_i\|^2.$$
- Die 1. Behauptung ergibt sich aus
$$\operatorname{vol}(\Gamma) = \prod_{i=1}^{m} \|b^*_i\| \le \prod_{i=1}^{m} \|b_i\| \le \prod_{i=1}^{m} 2^{\frac{i-1}{2}}\|b^*_i\| = 2^{\frac{m(m-1)}{4}} \prod_{i=1}^{m} \|b^*_i\| = 2^{\frac{m(m-1)}{4}} \operatorname{vol}(\Gamma).$$

- Die 2. Behauptung folgt durch Wurzelziehen aus

$$\|b_1\|^m \leq \prod_{i=1}^{m} 2^{\frac{i-1}{2}} \|b_i^*\| = 2^{\frac{m(m-1)}{4}} \prod_{i=1}^{m} \|b_i^*\| = 2^{\frac{m(m-1)}{4}} \operatorname{vol}(\Gamma).$$

- Wähle k minimal mit $x_1, \ldots, x_t \in \mathbf{R}b_1 + \cdots + \mathbf{R}b_k$. (Natürlich ist $k \geq t$.) Wir erhalten eine Darstellung

$$x_i = \sum_{j=1}^{k} r_{ij} b_j = \sum_{j=1}^{k} s_{ij} b_j^* \text{ mit } r_{ij} \in \mathbf{Z}, s_{ij} \in \mathbf{R} \text{ und } r_{ik} = s_{ik}.$$

  Wähle i mit $r_{ik} \neq 0$. Dann ist

$$\|x_i\|^2 = \sum_{j=1}^{k} s_{ij}^2 \|b_j^*\|^2 \geq s_{ik}^2 \|b_k^*\|^2 = r_{ik}^2 \|b_k^*\|^2 \geq \|b_k^*\|^2.$$

  Daher folgt für $j \leq k$ (und damit auch für $j \leq t$)

$$\|b_j\|^2 \leq 2^{k-1} \|b_k^*\|^2 \leq 2^{k-1} \|x_i\|^2 \leq 2^{m-1} \max(\|x_1\|^2, \ldots, \|x_t\|^2),$$

  was die 3. Behauptung beweist. Die 4. Aussage ist ein Spezialfall der 3. Aussage. ■

Wie erhält man eine LLL-reduzierte Gitterbasis? Man wendet die 1. und 2. Idee wiederholt an, wobei auf die Reihenfolge der Indizes zu achten ist. Eine einfache Version des LLL-Algorithmus geht wie folgt:

LLL-Algorithmus: Gegeben sei ein Gitter Γ im $\mathbf{R}^n$ durch eine Gitterbasis $b_1, \ldots, b_m$.

1. Setze $i := 1$. Sei T die $m \times m$-Einheitsmatrix mit den Zeilen $T_1, \ldots, T_m$.
2. Ist $i > m$ beende das Verfahren, ansonsten führe folgende Schritte aus:
   (a) Ist $i = 1$, setze $b_1^* = b_1$ und $i := 2$.
   (b) Setze $b_i^* := 0$.
   (c) Für $j = i-1, i-2, \ldots, 1$:
      (i) $\mu_{ij} := \frac{b_i \cdot b_j^*}{b_j^* \cdot b_j^*}$.
      (ii) $k := \lfloor \mu_{ij} \rceil$.
      (iii) Ist $k \neq 0$, setze $b_i := b_i - kb_j$, $T_i := T_i - kT_j$, $\mu_{ij} := \mu_{ij} - k$.
      (iv) $b_i^* := b_i^* - \mu_{ij} b_j^*$.
   (d) $b_i^* := b_i + b_i^*$.
   (e) $c_{i,i-1} := \frac{b_i^* \cdot b_i^*}{b_{i-1}^* \cdot b_{i-1}^*} + \mu_{i,i-1}^2$.
   (f) Ist $c_{i,i-1} < c$, vertausche b_i mit b_{i-1} und T_i mit T_{i-1}, setze $i := i - 1$. Ansonsten setze $i := i + 1$.

Am Ende ist $b_1, \ldots, b_m$ LLL-reduziert. Die Matrix T gibt die Transformation an, die die Ausgangsbasis in die LLL-reduzierte Basis überführt.

Bemerkungen:

1. Zu Beginn von Schritt 2.b ist $b_1, \ldots, b_{i-1}$ LLL-reduziert. Nach 2.e gilt $|\mu_{ij}| \leq \frac{1}{2}$ für alle $j = 1, 2, \ldots, i-1$. Im Schritt 2.f wird getestet, ob auch $b_1, \ldots, b_{i-1}, b_i$ LLL-reduziert ist. Wenn ja, wird der Index i um 1 erhöht. Wenn nein, dann wird b_i mit b_{i-1} vertauscht und i durch $i-1$ ersetzt.
2. Die Maple-Funktion 'lattice' führt obiges Verfahren aus. (Mit 'infolevel[lattice]:=3' kann man einzelne Schritte des Verfahrens sehen.)
3. Wir haben eine Maple-Funktion 'lll' geschrieben, die nach dem dargestellten Verfahren funktioniert.

Beispiel:

```
b_anfang=[[63, 57, -59], [45, -8, -93], [92, 43, -62]]
i=1
i=2
  mu_21=.735209
  Ersetze b_2 durch b_2-(1)b_1 (neues mu_21=-.264791)
```

```
c_21=.533227
Vertausche b_2 und b_1
Ersetze i=2 durch i=1
i=1
i=2
  mu_21=-.496582
c_21=1.875372
Ersetze i=2 durch i=3
  mu_32=1.155973
  Ersetze b_3 durch b_3-(1)b_2 (neues mu_32=.155973)
  mu_31=.085890
c_32=.108039
Vertausche b_3 und b_2
Ersetze i=3 durch i=2
  mu_21=.085890
c_21=.183348
Vertausche b_2 und b_1
Ersetze i=2 durch i=1
i=1
i=2
  mu_21=.468451
c_21=5.454111
Ersetze i=2 durch i=3
  mu_32=-.620579
  Ersetze b_3 durch b_3-(-1)b_2 (neues mu_32=.379421)
  mu_31=1.621415
  Ersetze b_3 durch b_3-(2)b_1 (neues mu_31=-.378585)
c_32=1.458888
Ersetze i=3 durch i=4
b_ende=[[29, -14, -3], [-18, -65, -34], [-13, 20, -87]]
```

10. Elemente kleiner Norm III

Wir legen wie üblich einen Zahlkörper K vom Grad n zugrunde. Durch Anwendung von LLL-Reduktion auf das Gitter $\phi(\mathfrak{a}) \subseteq \mathbf{R}^n$ kann man versuchen, Elemente kleiner Norm in einem Ideal $\mathfrak{a}$ zu finden.

Lemma.

$$|\mathrm{N}(\alpha)| \le \frac{2^{r_2}}{n^{n/2}} \|\phi(\alpha)\|^n.$$

Beweis: Wir schreiben

$$\begin{aligned} u_j &= |\sigma_j(\alpha)| \text{ für } 1 \le j \le r_1 \text{ und} \\ v_k &= |\sigma_{r_1+k}(\alpha)| = |\overline{\sigma_{r_1+k}}(\alpha)| = \sqrt{|\mathrm{Re}\,\sigma_{r_1+k}(\alpha)|^2 + |\mathrm{Im}\,\sigma_{r_1+k}(\alpha)|^2} \text{ für } 1 \le k \le r_2 \end{aligned}$$

und erhalten für $\alpha \neq 0$

$$\frac{|\mathrm{N}(\alpha)|}{\|\phi(\alpha)\|^n} = \frac{\prod_{j=1}^{r_1} |\sigma_j(\alpha)| \cdot \prod_{k=1}^{r_2} |\sigma_{r_1+k}(\alpha)| \cdot \prod_{k=1}^{r_2} |\overline{\sigma_{r_1+k}}(\alpha)|}{\sqrt{\sum_{j=1}^{r_1} |\sigma_j(\alpha)| + \sum_{k=1}^{r_2} ((\mathrm{Re}\,(\sigma_{r_1+k}(\alpha))^2 + (\mathrm{Im}\,(\sigma_{r_1+k}(\alpha))^2)}^n} = f(u_1, \ldots, u_{r_1}, v_1, \ldots, v_{r_2})$$

mit der reellen Funktion

$$f(u_1, \ldots, u_{r_1}, v_1, \ldots, v_{r_2}) = \frac{u_1 \cdot \cdots \cdot u_{r_1} \cdot v_1^2 \cdot \cdots \cdot v_{r_2}^2}{\sqrt{u_1^2 + \cdots + u_{r_1}^2 + v_1^2 + \cdots + v_{r_2}^2}^n},$$

die wir für $u_j \ge 0$, $v_k \ge 0$ betrachten. Bekanntlich nimmt das Produkt $u_1 \ldots u_{r_1}$ unter der Nebenbedingung $x^2 = u_1^2 + \cdots + u_{r_1}^2$ für $u_1 = \cdots = u_{r_1} = \frac{1}{\sqrt{r_1}} x$ an, also $u_1 \ldots u_r \le r_1^{-r_1/2} x^{r_1}$. Analog erhält man,

dass unter der Bedingung $y^2 = v_1^2 + \cdots + v_{r_2}^2$ die Abschätzung $v_1^2 \ldots v_{r_2}^2 \leq r_2^{-r_2} y^{2r_2}$ gilt. Somit folgt

$$\frac{|N(\alpha)|}{\|\phi(\alpha)\|^n} = f(u_1, \ldots, u_{r_1}, v_1, \ldots, v_{r_2}) \leq \frac{r_1^{-r_1/2} x^{r_1} \cdot r_2^{-r_2} y^{2r_2}}{\sqrt{x^2+y^2}^n}.$$

Setzt man $R^2 = x^2 + y^2$, so folgt durch Extremwertbestimmung in Abhängigkeit von x

$$\frac{x^{r_1} y^{2r_2}}{x^2+y^2} = \frac{x^{r_1}(R^2-x^2)^{r_2}}{R^2} \leq (\frac{r_1}{n})^{r_1/2}(1-\frac{r_1}{n})^{r_2} = \frac{r_1^{r_1/2}(2r_2)^{r_2}}{n^{n/2}},$$

was durch Einsetzen dann die Behauptung ergibt. ■

SATZ. *Ist $\phi(\alpha_1), \ldots, \phi(\alpha_n)$ eine LLL-reduzierte Basis des gebrochenen R-Ideals $\mathfrak{a}$, so gilt*

$$|\mathrm{N}(\alpha_1)| \leq \frac{2^{n(n-1)/4}}{n^{n/2}} \sqrt{|\mathrm{disc}\,(R)|}\mathrm{N}\mathfrak{a}.$$

Beweis: Zunächst ist

$$\mathrm{vol}\,(\phi(\mathfrak{a})) = 2^{-r_2}\sqrt{|\mathrm{disc}\,(R)|}\mathrm{N}\mathfrak{a}.$$

Da $\phi(\alpha_1), \ldots, \phi(\alpha_n)$ eine LLL-reduzierte Basis von $\phi(\mathfrak{a})$ ist, gilt

$$\|\phi(\alpha_1)\| \leq 2^{(n-1)/4}\mathrm{vol}\,(\phi(\mathfrak{a}))^{1/n},$$

das letzte Lemma liefert schließlich

$$|\mathrm{N}(\alpha_1)| \leq \frac{2^{r_2}}{n^{n/2}}\|\phi(\alpha_1)\|^n.$$

Wir setzen nun die drei Aussagen zusammen:

$$|\mathrm{N}(\alpha_1)| \leq \frac{2^{r_2}}{n^{n/2}}\left[2^{(n-1)/4}\mathrm{vol}\,(\phi(\mathfrak{a}))^{1/n}\right]^n = \frac{2^{r_2+n(n-1)/4}}{n^{n/2}} 2^{-r_2}\sqrt{|\mathrm{disc}\,(R)|}\mathrm{N}\mathfrak{a},$$

woraus die Behauptung folgt. ■

Bemerkung: Ist $\mathfrak{a}$ gebrochenes Ideal einer Ordnung R eines Zahlkörpers K, so gibt es ein $\alpha \in \mathfrak{a} \setminus \{0\}$ mit folgenden Eigenschaften

$$\begin{aligned} |\mathrm{N}\alpha| &\leq (\frac{4}{\pi})^{r_2}\frac{n!}{n^n} \cdot \mathrm{N}\mathfrak{a} \cdot \sqrt{|\mathrm{disc}\,R|} \quad \text{(Minkowski-Abschätzung)} \\ |\mathrm{N}\alpha| &\leq \frac{2^{n(n-1)/4}}{n^{n/2}} \cdot \mathrm{N}\mathfrak{a} \cdot \sqrt{|\mathrm{disc}\,R|} \text{ (LLL-Reduktion).} \end{aligned}$$

In der folgenden Tabelle werden die beiden Abschätzungen verglichen:

n	r_1	r_2	$(\frac{4}{\pi})^{r_2}\frac{n!}{n^n}$	$\frac{2^{n(n-1)/4}}{n^{n/2}}$
2	2	0	0.500000	0.707107
2	0	1	0.636620	0.707107
3	3	0	0.222222	0.544331
3	1	1	0.282942	0.544331
4	4	0	0.093750	0.500000
4	2	1	0.119366	0.500000
4	0	2	0.151982	0.500000
5	5	0	0.038400	0.572433
5	3	1	0.048892	0.572433
5	1	2	0.062252	0.572433
6	6	0	0.015432	0.838052
6	4	1	0.019649	0.838052
6	2	2	0.025018	0.838052
6	0	3	0.031853	0.838052

Wir wollen sehen, dass LLL-Reduktion für die Zahlentheorie recht nützlich sein kann.

Beispiel: Wir betrachten $K = \mathbf{Q}(\sqrt{-163})$ mit $Z_K = \mathbf{Q}(\frac{1+\sqrt{-163}}{2})$. Das Element $\alpha = \frac{1+\sqrt{-163}}{2}$ hat das Minimalpolynom $f = x^2 - x + 41$. Es gibt zwei Primideale mit Norm $p = 10007$. Eines davon ist

$$\mathfrak{p} = (10007, \alpha + 4301) = \mathbf{Z} \cdot (\alpha + 4301) + \mathbf{Z} \cdot 10007.$$

K besitzt bis auf Konjugation eine komplexe Einbettung, z.B. $\sigma\alpha \approx 0.5000 + 6.3836i$. Für die additive Einbettung gilt dann

$$\begin{pmatrix} \phi(\alpha + 4301) \\ \phi(10007) \end{pmatrix} \approx \begin{pmatrix} 4301.5000 & 6.3836 \\ 10007.0000 & 0.0000 \end{pmatrix}.$$

Wir wenden nun LLL-Reduktion an (mit der Maple-Funktion 'lattice') und erhalten

$$\begin{pmatrix} \phi(\beta_1) \\ \phi(\beta_2) \end{pmatrix} \approx \begin{pmatrix} 89.5000 & 44.6852 \\ 330.0000 & -548.9896 \end{pmatrix}.$$

Die Übergangsmatrix zur neuen Basis ist dabei

$$T = \begin{pmatrix} 7 & -3 \\ -86 & 37 \end{pmatrix}.$$

Also erhält man

$$\begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix} = T \begin{pmatrix} \alpha + 4301 \\ 10007 \end{pmatrix} = \begin{pmatrix} 7\alpha + 86 \\ -86\alpha + 373 \end{pmatrix}.$$

Dabei gilt

$$\mathrm{N}(7\alpha + 86) = 10007, \quad \mathrm{N}(-86\alpha + 373) = 41 \cdot 10007.$$

Insbesondere gilt $\mathfrak{p} = (7\alpha + 86)$. (Ändert man die Rechengenauigkeit, können sich andere reduzierte Basen ergeben.)

Beispiel: Wir betrachten wieder den Zahlkörper $K = \mathbf{Q}(\alpha)$ mit $\alpha^3 + 7\alpha + 20 = 0$. Es gilt

$$\mathbf{Z}_K = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2 + \mathbf{Z}\omega_3 \quad \text{mit} \quad \omega_1 = \frac{\alpha^2 + \alpha}{2}, \quad \omega_2 = \alpha, \quad \omega_3 = 1 \quad \text{und} \quad \operatorname{disc} \mathbf{Z}_K = -3043.$$

Wir wissen auch, dass $\mathbf{Z}_K$ Hauptidealring ist.

1. Es gibt genau ein Primideal $\mathfrak{p}$ mit Norm

$$p = 2^{128} - 173 = 340282366920938463463374607431768211283,$$

nämlich

$$\mathfrak{p} = (340282366920938463463374607431768211283, \alpha + 264268547492017156591560000458929396806).$$

Wir wollen $\mathfrak{p}$ als Hauptideal schreiben. Die Hermitesche Normalform von $\mathfrak{p}$ bzgl. der $\mathbf{Z}$-Basis $\omega_1, \omega_2, \omega_3$ ist $\mathfrak{p} = \mathbf{Z}\alpha_1 + \mathbf{Z}\alpha_2 + \mathbf{Z}\alpha_3$ mit

$$\begin{aligned} \alpha_1 &= \omega_1 + 272220783624752510100293485520492691 47, \\ \alpha_2 &= \omega_2 + 264268547492017156591560000458929396806, \\ \alpha_3 &= 340282366920938463463374607431768211283. \end{aligned}$$

Wir wenden jetzt LLL-Reduktion auf $\phi(\alpha_1), \phi(\alpha_2), \phi(\alpha_3)$ an und erhalten (nach 66 Vertauschungen benachbarter Basisvektoren) eine LLL-reduzierte Basis $\phi(\beta_1), \phi(\beta_2), \phi(\beta_3)$ mit

$$\begin{aligned} \beta_1 &= -1517733606726\omega_1 + 2179167368524\omega_2 - 12385744120593, \\ \beta_2 &= -194866083130\omega_1 - 4135642325165\omega_2 - 9594152173926, \\ \beta_3 &= -4135642325165\omega_1 - 271701595538\omega_2 + 5771406502613. \end{aligned}$$

Dabei ist nun

$$\mathrm{N}(\beta_1) = -p, \quad \mathrm{N}(\beta_2) = -2p, \quad \mathrm{N}(\beta_3) = 7p,$$

was insbesondere $\mathfrak{p} = (\beta_1)$ zeigt. Wir haben also mit LLL-Reduktion einen Erzeuger des Hauptideals $\mathfrak{p}$ gefunden.

2. Für (zufällig gewähltes)

$$\beta = 427419669081\omega_1 + 321110693270\omega_2 + 343633073697\omega_3$$

hatten wir die Primidealzerlegung des Hauptideals (β) bestimmt, nämlich

$$(\beta) = \mathfrak{p}_{1b}\mathfrak{p}_{2c}\mathfrak{p}_{3a}\mathfrak{p}_{4a}\mathfrak{p}_{5a}$$

mit

$$p_1 = 7, \quad p_2 = 3299, \quad p_3 = 21521, \quad p_4 = 9680839171, \quad p_5 = 192447080070865421,$$

$$\begin{aligned}
\mathfrak{p}_{1b} &= (7, \alpha+5) = (\pi_{1b}) \text{ mit } \pi_{1b} = 9\omega_1 + 13\omega_2 + 17 \text{ mit } \mathrm{N}(\pi_{1b}) = -7,\\
\mathfrak{p}_{2c} &= (3299, \alpha+2831) = \mathbf{Z}(\omega_1 + 2420) + \mathbf{Z}(\omega_2 + 2831) + \mathbf{Z}\cdot 3299,\\
\mathfrak{p}_{3a} &= (21521, \alpha+7931) = \mathbf{Z}(\omega_1 + 17287) + \mathbf{Z}(\omega_2 + 7931) + \mathbf{Z}\cdot 21521,\\
\mathfrak{p}_{4a} &= (9680839171, \alpha+4647764309) =\\
&= \mathbf{Z}(\omega_1 + 6491190138) + \mathbf{Z}(\omega_2 + 4647764309) + \mathbf{Z}\cdot 9680839171,\\
\mathfrak{p}_{5a} &= (192447080070865421, \alpha+81377350823052079) =\\
&= \mathbf{Z}(\omega_1 + 124567653488181316) + \mathbf{Z}(\omega_2 + 81377350823052079) + \mathbf{Z}\cdot 192447080070865421.
\end{aligned}$$

Wir wollen die $\mathfrak{p}_i$'s als Hauptideale darstellen. Wir wenden LLL-Reduktion auf $\phi(\mathfrak{p}_i)$ an und erhalten neue $\mathbf{Z}$-Basen (Anzahl der Vertauschungen benachbarter Basisvektoren: 6, 7, 16, 36):

$$\begin{aligned}
\mathfrak{p}_{2c} &= \mathbf{Z}(7\omega_2 + 23) + \mathbf{Z}(8\omega_1 - 8\omega_2 + 11) + \mathbf{Z}(-\omega_1 + 9\omega_2 - 34),\\
\mathfrak{p}_{3a} &= \mathbf{Z}(-4\omega_1 + 6\omega_2 - 41) + \mathbf{Z}(19\omega_2 + 42) + \mathbf{Z}(-23\omega_1 + 4\omega_2 - 20),\\
\mathfrak{p}_{4a} &= \mathbf{Z}(-849\omega_1 + 1117\omega_2 - 1366) + \mathbf{Z}(-268\omega_1 - 1015\omega_2 - 3562) + \mathbf{Z}(-1015\omega_1 - 230\omega_2 + 3121),\\
\mathfrak{p}_{5a} &= \mathbf{Z}(-159345\omega_1 + 28074\omega_2 - 757504) + \mathbf{Z}(131271\omega_1 + 60062\omega_2 - 417973)\\
&\quad + \mathbf{Z}(279469\omega_1 - 1091255\omega_2 - 137233).
\end{aligned}$$

Wir bestimmen die Normen der neuen Basisvektoren für $\mathfrak{p}_i = \mathbf{Z}\alpha_{1i} + \mathbf{Z}\alpha_{2i} + \mathbf{Z}\alpha_{3i}$:

$\mathfrak{p}_i$	$\mathrm{N}(\alpha_{1i})$	$\mathrm{N}(\alpha_{2i})$	$\mathrm{N}(\alpha_{3i})$
$\mathfrak{p}_{2c}$	$2^2 \cdot 3299$	$3^2 \cdot 3299$	$-2^4 \cdot 3299$
$\mathfrak{p}_{3a}$	-21521	$2 \cdot 21521$	$-2 \cdot 3 \cdot 5 \cdot 21521$
$\mathfrak{p}_{4a}$	$-2^2 \cdot 9680839171$	$-2 \cdot 3 \cdot 9680839171$	$3 \cdot 7 \cdot 9680839171$
$\mathfrak{p}_{5a}$	$-2 \cdot 192447080070865421$	$-3 \cdot 192447080070865421$	$109 \cdot 192447080070865421$

Wir bemerken zunächst, dass die Primidealzerlegung von 2

$$(2) = (\alpha+2) \cdot (\alpha^2 - 2\alpha + 11)$$

ist, wobei $\mathrm{N}(\alpha+2) = 2$ und $\mathrm{N}(\alpha^2 - 2\alpha + 11) = 4$ gilt. Wir betrachten den ersten Basisvektor von $\mathfrak{p}_{2c}$. Er ist nicht durch $\alpha+2$ teilbar, also teilen wir $\alpha^2 - 2\alpha + 11$ heraus und erhalten

$$\pi_{2c} = 7\omega_1 + 15\omega_2 + 23 \quad \text{mit} \quad \mathrm{N}(\pi_{2c}) = 3299.$$

Bei $\mathfrak{p}_{3a}$ ist der erste Basisvektor bereits Primelement:

$$\pi_{3a} = -41 + 4\alpha - 2\alpha^2 \quad \text{mit} \quad \mathrm{N}(\pi_{3a}) = -21521.$$

Für $\mathfrak{p}_{4a}$ dividieren wir aus dem ersten Basisvektor $(\alpha+2)^2$ heraus und erhalten

$$\pi_{4a} = -39875\omega_1 + 57588\omega_2 - 210839 \quad \text{mit} \quad \mathrm{N}(\pi_{4a}) = -9680839171.$$

Bei $\mathfrak{p}_{5a}$ dividieren wir aus dem ersten Basisvektor $\alpha+2$ heraus und erhalten

$$\pi_{5a} = -972997\omega_1 + 1379823\omega_2 - 5243737.$$

Tatsächlich findet man nun

$$\beta = \pi_{1b}\pi_{2c}\pi_{3a}\pi_{4a}\pi_{5a},$$

eine Faktorisierung von β in Primelemente.

Beispiel: Für $K = \mathbf{Q}(\alpha)$ mit $2 + 3\alpha + 5\alpha^2 + 7\alpha^3 + \alpha^4 = 0$ betrachten wir in $\mathbf{Z}_K = \mathbf{Z}[\alpha]$ für

$$p = 340282366920938463463374607431768211297$$

das Primideal

$$\mathfrak{p} = (340282366920938463463374607431768211297, \alpha + 209347000537071323670817353923549650293)$$

mit Norm p. Eine normalisierte $\mathbf{Z}$-Basis von $\mathfrak{p}$ ist

$$\begin{aligned}
\alpha_1 &= \alpha^3 + 52333425093305383492022171817273555465,\\
\alpha_2 &= \alpha^2 + 22652324134956339789218060644632480339,\\
\alpha_3 &= \alpha + 20934700053707132367081735392354965029 3,\\
\alpha_4 &= 34028236692093846346337460743176821129 7.
\end{aligned}$$

Wir machen LLL-Reduktion und finden (nach 96 Vertauschungen benachbarter Basisvektoren) eine neue $\mathbf{Z}$-Basis:

$$\begin{aligned}
\beta_1 &= -654494764\alpha^3 + 4279528383 - 4315754383\alpha^2 + 9579475\alpha,\\
\beta_2 &= -6658900589\alpha^2 - 5496906961 - 1263184053\alpha^3 + 7940788002\alpha,\\
\beta_3 &= -14202959627\alpha - 4371139333 + 2306464616\alpha^3 + 12008356060\alpha^2,\\
\beta_4 &= -12819426199 - 30029150681\alpha - 4279528383\alpha^3 - 31265688209\alpha^2.
\end{aligned}$$

Für die Normen gilt:

$$\mathrm{N}(\beta_1) = -p, \quad \mathrm{N}(\beta_2) = 9p, \quad \mathrm{N}(\beta_3) = -78p, \quad \mathrm{N}(\beta_4) = -8p.$$

Daher ist β_1 Erzeuger des Hauptideals $\mathfrak{p}$.

KAPITEL 8

Einheiten

1. Einführung

Wir wollen uns in diesem Kapitel mit den Einheiten der Ordnung R eines algebraischen Zahlkörpers K beschäftigen. Die Einheiten bilden bzgl. der Multiplikation eine Gruppe, die mit R^* bezeichnet wird. Das folgende grundlegende Kriterium haben wir bereits früher bewiesen: Für $\alpha \in R$ gilt:

$$\alpha \in R^* \quad \Longleftrightarrow \quad \mathrm{N}\alpha = \pm 1.$$

Ganz elementar lassen sich mit Hilfe dieses Kriteriums die Einheiten im imaginärquadratischen Fall bestimmen:

Satz. *Sei R Ordnung eines imaginärquadratischen Zahlkörpers. Dann ist $R^* = \{\pm 1\}$ außer für $R = \mathbf{Z}[\sqrt{-1}]$ und $R = \mathbf{Z}[\frac{1+\sqrt{-3}}{2}]$. In diesen Fällen hat man*

$$\mathbf{Z}[\sqrt{-1}]^* = \{\pm 1, \pm\sqrt{-1}\} \quad \textit{und} \quad \mathbf{Z}[\frac{1+\sqrt{-3}}{2}]^* = \{\pm 1, \pm\frac{1+\sqrt{-3}}{2} \pm \frac{1-\sqrt{-3}}{2}\}.$$

Beweis: Natürlich gilt immer $\{\pm 1\} \subseteq R^*$. Sei jetzt $\alpha \in R^*$, $\alpha \neq \pm 1$. Dann ist $\mathrm{N}\alpha = \sigma_1(\alpha) \cdot \overline{\sigma_1(\alpha)} = 1$, $s = \mathrm{Sp}(\alpha) \in \mathbf{Z}$ und $\alpha^2 - s\alpha + 1 = 0$. Also gilt (in einer komplexen Einbettung)

$$\sigma_i(\alpha) = \frac{s \pm \sqrt{s^2-4}}{2}.$$

Da $s^2 - 4 < 0$ gelten muß, gibt es nur zwei Fälle:

- $|s| = 0$. Dann ist $\sigma_i(\alpha) = \pm\sqrt{-1}$ und $R = \mathbf{Z}[\sqrt{-1}]$.
- $|s| = 1$. Dann ist $\sigma_i(\alpha) = \frac{\pm 1 \pm \sqrt{-3}}{2}$ und somit $R = \mathbf{Z}[\frac{1+\sqrt{-3}}{2}]$. (Da das charakteristische Polynom ansatzgemäß konstanten Term 1 hat, handelt es sich auch um Einheiten.) ■

Im allgemeinen ist nicht so klar, wie (nichttriviale) Einheiten aussehen und wie man an Einheiten kommt.

Beispiel: In der Maximalordnung $\mathbf{Z}_K$ des Zahlkörpers $K = \mathbf{Q}(\alpha)$ mit $\alpha^3+7\alpha+20 = 0$ und Ganzheitsbasis $\omega_1 = \frac{\alpha^2+\alpha}{2}$, $\omega_2 = \alpha$, $\omega_3 = 1$ hatten wir (zufällig) Elemente

$$\alpha_1 = 2\omega_1 - 3\omega_2 + 11\omega_3, \quad \beta_1 = 40\omega_1 + 67\omega_2 + 93\omega_3$$

gefunden, die das gleiche Ideal erzeugen. Also ist $\frac{\beta_1}{\alpha_1}$ eine Einheit:

$$\frac{\beta_1}{\alpha_1} = 127\omega_1 - 107\omega_3 \quad \text{und} \quad \left(\frac{\beta_1}{\alpha_1}\right)^{-1} = \frac{\alpha_1}{\beta_1} = -78105\omega_1 + 112903\omega_2 - 413023\omega_3.$$

Die Struktur der Einheitengruppe R^* ist Inhalt des folgenden Satzes von Dirichlet, der in diesem Kapitel bewiesen werden wird:

Satz (Dirichlet). *Es gibt eine Einheitswurzel $\zeta \in R^*$ einer Ordnung m (d.h. $m \in \mathbf{N}$ ist minimal mit $\zeta^m = 1$) und Einheiten $\varepsilon_1, \ldots, \varepsilon_{r_1+r_2-1} \in R^*$, so daß sich jede Einheit $\varepsilon \in R^*$ eindeutig schreiben läßt als*

$$\varepsilon = \zeta^l \varepsilon_1^{m_1} \ldots \varepsilon_{r_1+r_2-1}^{m_{r_1+r_2-1}} \quad \textit{mit} \quad 0 \leq l < m \quad \textit{und} \quad m_i \in \mathbf{Z}.$$

2. Die logarithmische Abbildung

Wir legen einen algebraischen Zahlkörper K vom Grad n zugrunde mit reellen Einbettungen $\sigma_i : K \hookrightarrow \mathbf{R}$, $i = 1, \ldots, r_1$ und komplexen Einbettungen $\sigma_{r_1+j}, \overline{\sigma_{r_1+j}} : K \hookrightarrow \mathbf{C}$, $j = 1, \ldots, r_2$. Sei weiter R eine Ordnung des Zahlkörpers. Wir definieren die logarithmische Abbildung durch

$$\ell : R^* \to \mathbf{R}^{r_1+r_2}, \quad \alpha \mapsto (\ln|\sigma_1\alpha|, \ldots, \ln|\sigma_{r_1}\alpha|, 2\ln|\sigma_{r_1+1}\alpha|, \ldots, 2\ln|\sigma_{r_1+r_2}\alpha|).$$

Offensichtlich ist ℓ ein Gruppenhomomorphismus:

$$\ell(\alpha_1\alpha_2) = \ell(\alpha_1) + \ell(\alpha_2).$$

Ist α Einheit in R, so gilt $\pm 1 = N\alpha = \prod_i \sigma_i\alpha = (\sigma_1\alpha)\ldots(\sigma_{r_1}\alpha)(\sigma_{r_1+1}\alpha)(\overline{\sigma_{r_1+1}\alpha})\ldots(\sigma_{r_1+r_2}\alpha)(\overline{\sigma_{r_1+r_2}\alpha})$, also $1 = \prod_{i=1}^{r_1}|\sigma_i\alpha| \cdot \prod_{j=1}^{r_2}|\sigma_{r_1+j}\alpha|^2$ und damit $\sum_{i=1}^{r_1}\ln|\sigma_i\alpha| + 2\sum_{j=1}^{r_2}\ln|\sigma_{r_2+j}\alpha| = 0$, was die Inklusion

$$\ell(R^*) \subseteq \{(z_1, \ldots, z_{r_1+r_2}) \in \mathbf{R}^{r_1+r_2} : \sum_i z_i = 0\}$$

liefert.

LEMMA. *Sei $\alpha_1, \ldots, \alpha_n$ eine $\mathbf{Z}$-Basis von R, $\beta_1, \ldots, \beta_n$ die duale Basis, d.h. $\mathrm{Sp}(\alpha_j\beta_i) = \delta_{ji}$. Sind $c_1, \ldots, c_{r_1+r_2} \in \mathbf{R}$ gegeben, so gilt für $\alpha = x_1\alpha_1 + \cdots + x_n\alpha_n \in R$ ($x_i \in \mathbf{Z}$) mit $\alpha \in R^*$:*

$$\ell(\alpha) \in \{(z_1, \ldots, z_{r_1+r_2}) \in \mathbf{R}^{r_1+r_2} : z_i \le c_i\} \quad \Longrightarrow \quad |x_i| \le \sum_{j=1}^{r_1}|\sigma_j\beta_i|e^{c_j} + 2\sum_{j=1}^{r_2}|\sigma_{r_1+j}\beta_i|e^{c_{r_1+j}/2}.$$

Insbesondere gibt es nur endlich viele solcher α's.

Beweis: Für $1 \le j \le r_1$ gilt $\ln|\sigma_j\alpha| \le c_j$, also $|\sigma_j\alpha| \le e^{c_j}$, für $1 \le j \le r_2$ gilt $2\ln|\sigma_{r_1+j}\alpha| \le c_{r_1+j}$ und damit $|\sigma_{r_1+j}\alpha| \le e^{c_{r_1+j}/2}$. Wegen $\mathrm{Sp}(\alpha_j\beta_i) = \delta_{ij}$ gilt

$$x_i = \mathrm{Sp}(\alpha\beta_i) = \sum_{i=j}^{r_1}\sigma_j(\alpha\beta_i) + \sum_{j=1}^{r_2}(\sigma_{r_1+j}(\alpha\beta_i) + \overline{\sigma_{r_1+j}(\alpha\beta_i)})$$

und damit

$$|x_i| \le \sum_{j=1}^{r_1}|\sigma_j\alpha||\sigma_j\beta_i| + 2\sum_{j=1}^{r_2}|\sigma_{r_1+j}\alpha||\sigma_{r_1+j}\beta_i| \le \sum_{j=1}^{r_1}|\sigma_j\beta_i|e^{c_j} + 2\sum_{j=1}^{r_2}|\sigma_{r_1+j}\beta_i|e^{c_{r_1+j}/2}. \quad \blacksquare$$

Das Lemma zeigt, daß $\ell(R^*) \subseteq \mathbf{R}^n$ diskret ist. Da $\ell(R^*)$ eine Untergruppe des (r_1+r_2-1)-dimensionalen Raums $\{(z_1, \ldots, z_{r_1+r_2}) : \sum z_i = 0\}$ ist, folgt nun sofort:

FOLGERUNG. *$\ell(R^*)$ ist ein Gitter vom Rang $\le r_1 + r_2 - 1$.*

3. Der Kern der logarithmischen Abbildung — Einheitswurzeln

Erinnerung:

1. Eine Einheitswurzel eines Zahlkörpers K ist ein Element $\zeta \in K$, so daß $m \in \mathbf{N}$ existiert mit $\zeta^m = 1$. Ist m minimal gewählt, so ist m also die Ordnung von ζ in der multiplikativen Gruppe K^*. Man nennt dann ζ eine primitive m-te Einheitswurzel.
2. Sei $\zeta \in K$ eine primitive m-te Einheitswurzel. Das Minimalpolynom von ζ ist das sogenannte m-te Kreisteilungspolynom $\Phi_m(x) \in \mathbf{Z}[x]$. Da ζ Nullstelle von $x^m - 1$ ist, teilt $\Phi_m(x)$ das Polynom $x^m - 1$, außerdem sieht man sofort, daß $\zeta \in \mathbf{Z}_K$ gilt. Man hat weiter die Darstellung

$$\Phi_m(x) = \prod_{\substack{0 \le l < m \\ \mathrm{ggT}(l,m)=1}} (x - \zeta^l).$$

Dies zeigt

$$\mathrm{grad}\Phi_m(x) = [\mathbf{Q}(\zeta) : \mathbf{Q}] = \varphi(m)$$

mit der Eulerschen φ-Funktion φ, die sich bei gegebener Primfaktorzerlegung $m = \prod p_i^{e_i}$ so berechnen läßt:

$$\varphi(m) = \prod p_i^{e_i-1}(p_i - 1).$$

Ist n der Körpergrad $[K : \mathbf{Q}]$, so gilt insbesondere

$$\prod_i p_i^{e_i-1}(p_i-1)|n,$$

also kommen auch nur endlich viele Werte für m in Frage.

3. Die Menge der in K enthaltenen Einheitswurzeln wird mit $\mu(K)$ bezeichnet und ist eine endliche zyklische Gruppe. Ist $\#\mu(K) = m$ und $\zeta \in \mu(K)$ ein Erzeuger, so ist ζ eine primitive m-te Einheitswurzel und
$$\mu(K) = \{\zeta^l : 0 \le l \le m-1\}.$$
ζ^l ist genau dann ebenfalls primitive m-te Einheitswurzel, wenn $\mathrm{ggT}(m,l) = 1$ gilt.
4. Die m-ten Einheitswurzel in K erhält man durch Faktorisieren des Polynom $x^m - 1$ in $K[x]$. Die Einheitswurzeln ζ entsprechen den Linearfaktoren $x - \zeta$.

Die einzigen Einheitswurzeln in $\mathbf{R}$ sind ± 1. Hat man also eine Einbettung $\sigma : K \hookrightarrow \mathbf{R}$ und ist ζ eine primitive m-te Einheitswurzel, so folgt $(\sigma(\zeta))^m = \sigma(\zeta^m) = 1$, also $\sigma(\zeta) = \pm 1$ und damit $\zeta = \pm 1$. Dies liefert die nützliche Bemerkung:

LEMMA. *Ist $r_1 > 0$, so gilt $\mu(K) = \{\pm 1\}$.*

Ist $\sigma : K \hookrightarrow \mathbf{C}$ eine komplexe Einbettung und $\zeta \in K$ eine primitive m-te Einheitswurzel, so ist

$$\sigma(\zeta) = e^{\frac{2\pi i}{m}l} \quad \text{für ein } l \text{ mit } 0 \le l \le m-1 \text{ und } \mathrm{ggT}(m,l) = 1.$$

Insbesondere folgt $\ln|\sigma(\zeta)| = 0$ und damit

$$\mu(R) = R \cap \mu(K) \subseteq Kern(\ell).$$

Setzt man in das erste Lemma $c_1 = \cdots = c_{r_1+r_2} = 0$ ein, so erhält man:

LEMMA. *Ist $\alpha_1, \ldots, \alpha_n$ eine $\mathbf{Z}$-Basis von R und $\beta_1, \ldots, \beta_n$ die duale Basis, dann hat man für $\alpha = x_1\alpha_1 + \cdots + x_n\alpha_n \in R^*$ mit $\ell(\alpha) = 0$ die Abschätzung*

$$|x_i| \le \sum_{i=1}^{n} |\sigma_j \beta_i|.$$

Wir werden das Lemma konkret anwenden, aber zunächst damit folgenden Satz beweisen:

SATZ. *$Kern(\ell) = \mu(R)$.*

Beweis: Nach dem letzten Lemma ist $Kern(\ell)$ endlich, damit eine endliche (abelsche) Gruppe. Jedes Element hat also endliche Ordnung und ist damit eine Einheitswurzel. Also $Kern(\ell) \subseteq \mu(R)$. Die Umkehrung $\mu(R) \subseteq Kern(\ell)$ hatten wir schon gesehen. ■

Beispiel: Wir betrachten $K = \mathbf{Q}(i, \sqrt{2})$. Das Element $\alpha = i + \sqrt{2}$ hat das Minimalpolynom $f = x^4 - 2x^2 + 9$, das man durch Ausmultiplizieren von $(x-(i+\sqrt{2})(x-(i-\sqrt{2})(x-(-i+\sqrt{2})(x-(-i-\sqrt{2})$ erhält. Eine $\mathbf{Z}$-Basis von $\mathbf{Z}_K$ ist

$$\alpha_1 = \frac{\alpha^3 + 3\alpha^2 + 7\alpha + 9}{12}, \quad \alpha_2 = \frac{\alpha^2+1}{2}, \quad \alpha_3 = \alpha, \quad \alpha_4 = 1.$$

Wendet man das Lemma an, so erhält man für $\lambda = x_1\alpha_1 + \cdots + x_4\alpha_4 \in \mathbf{Z}_K^* \cap Kern(\ell)$ die Abschätzungen

$$|x_1| \le 2, \quad |x_2| \le 1, \quad |x_3| \le 1, \quad |x_4| \le 1.$$

Folgende Liste enthält alle Elemente λ mit Norm ± 1, die diesen Ungleichungen genügen.

λ	charakteristisches Polynom von λ	$\sum_i \lvert\sigma_i\lambda\rvert$	$\ell(\lambda)$	$\lambda = \zeta^l$
1	$(x-1)^4$	4.00	$(0,0)$	ζ^0
-1	$(x+1)^4$	4.00	$(0,0)$	ζ^4
$2\alpha_1-\alpha_2-\alpha_3-1$	$(x^2+1)^2$	4.00	$(0,0)$	ζ^2
$-2\alpha_1+\alpha_2+\alpha_3+1$	$(x^2+1)^2$	4.00	$(0,0)$	ζ^6
$\alpha_1-\alpha_2-\alpha_3$	x^4+1	4.00	$(0,0)$	ζ
$\alpha_1-\alpha_3-1$	x^4+1	4.00	$(0,0)$	ζ^7
$-\alpha_1+\alpha_2+\alpha_3$	x^4+1	4.00	$(0,0)$	ζ^5
$-\alpha_1+\alpha_3+1$	x^4+1	4.00	$(0,0)$	ζ^3
$\alpha_1-\alpha_2-1$	$x^4+4x^3+8x^2+4x+1$	5.66	$(-0.88,0.88)$	
$-\alpha_1$	$x^4+4x^3+8x^2+4x+1$	5.66	$(0.88,-0.88)$	
$-\alpha_1+\alpha_2+1$	$x^4-4x^3+8x^2-4x+1$	5.66	$(-0.88,0.88)$	
α_1	$x^4-4x^3+8x^2-4x+1$	5.66	$(0.88,-0.88)$	
$-\alpha_1-\alpha_2-\alpha_3$	$x^4+8x^3+32x^2-8x+1$	12.00	$(1.76,-1.76)$	
$\alpha_1+\alpha_2+\alpha_3$	$x^4-8x^3+32x^2+8x+1$	12.00	$(1.76,-1.76)$	

Also ist $\mu(K)$ eine Gruppe mit 8 Elementen, ein Erzeugendes ist z.B. $\zeta = \alpha_1-\alpha_2-\alpha_3$. Da ζ Grad 4 hat, gilt natürlich auch $K = \mathbf{Q}(\zeta)$. (Bei dem Verfahren sind wir auch noch auf weitere Einheiten gestoßen.)

4. Ein erster Struktursatz

Da wir bereits wissen, daß $\ell(R^*)$ ein Gitter vom Rang $\le r_1+r_2-1$ ist, erhalten wir leicht eine erste Strukturaussage:

Satz. *Seien $\varepsilon_1,\dots,\varepsilon_r \in R^*$, so daß $\ell(\varepsilon_1),\dots,\ell(\varepsilon_r)$ eine Gitterbasis von $\ell(R^*)$ bilden ($r \le r_1+r_2-1$). Dann läßt sich jede Einheit $\varepsilon \in R^*$ eindeutig in der Form*

$$\varepsilon = \zeta\cdot\varepsilon^{m_1}\dots\varepsilon_r^{m_r}$$

mit $\zeta\in\mu(R)$ und $m_i\in\mathbf{Z}$ schreiben. Also hat man einen Gruppenisomorphismus

$$R^*\simeq \mathbf{Z}/|\mu(R)|\mathbf{Z}\oplus\mathbf{Z}^r.$$

Beweis: Sei $\varepsilon\in R^*$. Dann gibt es (eindeutig bestimmte) $m_i\in\mathbf{Z}$ mit

$$\ell(\varepsilon) = m_1\ell(\varepsilon_1)+\dots+m_r\ell(\varepsilon_r).$$

Es folgt

$$\ell(\varepsilon\cdot\prod_i \varepsilon_i^{-m_i}) = 0,$$

also ist $\zeta = \varepsilon\cdot\prod_i\varepsilon_i^{-m_i}\in\mu(R)$ und somit

$$\varepsilon = \zeta\prod_i\varepsilon_i^{m_i}.$$

Wendet man ℓ auf eine solche Darstellung an, sieht man, daß die Exponenten m_i eindeutig bestimmt sind, also auch ζ. ■

Um den Satz von Dirichlet zu beweisen, müssen wir noch zeigen, daß das Gitter $\ell(R^*)$ Rang r_1+r_2-1 hat. Dazu genügt es, Einheiten $\varepsilon_1,\dots,\varepsilon_{r_1+r_2-1}$ zu konstruieren, so daß $\ell(\varepsilon_1),\dots,\ell(\varepsilon_{r_1+r_2-1})$ linear unabhängig sind.

5. Existenz von unabhängigen Einheiten

Den Minkowskischen Gitterpunktsatz kann man auf das Einheitenproblem nicht direkt anwenden. Der Trick besteht darin, viele Elemente mit beschränkter Norm zu konstruieren, dann muß es dabei welche geben, die sich nur um eine Einheit voneinander unterscheiden, wie das folgende Lemma zeigt:

Lemma. *Sind $\alpha,\beta\in R$ mit $|\mathrm{N}\alpha| = |\mathrm{N}\beta| = c$ und $\alpha\equiv\beta \bmod Rc$, dann ist $\frac{\alpha}{\beta}\in R^*$.*

Beweis: Ist $g = x^n + b_1 x^{n-1} + \cdots + b_n \in \mathbf{Z}[x]$ das charakteristische Polynom von β, so ist $b_n = \pm c$. Aus $\beta(\beta^{n-1} + b_1\beta^{n-2} + \cdots + b_{n-1}) = \pm c$ folgt dann, daß $\frac{c}{\beta} \in R$ ist. Es gibt nach Voraussetzung $\gamma \in R$ mit $\alpha = \beta + \gamma c$, was

$$\frac{\alpha}{\beta} = 1 + \gamma \cdot \frac{c}{\beta} \in R$$

liefert. Aus Symmetriegründen gilt auch $\frac{\beta}{\alpha} \in R$, was zeigt, daß $\frac{\alpha}{\beta}$ Einheit in R ist. ■

Mit dem folgenden Lemma kann man (theoretisch) viele Elemente mit beschränkter Norm konstruieren:

LEMMA. *Seien $c_1, \ldots, c_{r_1}, d_1, \ldots, d_{r_2}, \varepsilon$ positive reelle Zahlen mit*

$$c_1 \ldots c_{r_1} d_1^2 \ldots d_{r_2}^2 = (\frac{2}{\pi})^{r_2} \sqrt{|\mathrm{disc}\,(R)|} + \varepsilon.$$

Dann gibt es ein $\alpha \in R$, $\alpha \neq 0$ mit

$$|\sigma_i \alpha| < c_i \quad \textit{für} \quad 1 \leq i \leq r_1 \quad \textit{und} \quad |\sigma_{r_1+j}\alpha| < d_j \quad \textit{für} \quad 1 \leq j \leq r_2.$$

Insbesondere gilt

$$|\mathrm{N}\alpha| < (\frac{2}{\pi})^{r_2} \sqrt{|\mathrm{disc}\,(R)|} + \varepsilon.$$

Konkret: Ist $\alpha_1, \ldots, \alpha_n$ eine $\mathbf{Z}$-Basis von R, $\beta_1, \ldots, \beta_n$ die duale Basis, so kann man ein α wie oben in der (endlichen) Menge

$$\{x_1\alpha_1 + \cdots + x_n\alpha_n \in R : |x_i| < \sum_{j=1}^{r_1} |\sigma_j\beta_i| c_j + 2\sum_{j=1}^{r_2} |\sigma_{r_1+j}\beta_i| d_j \textit{ für alle } i\}$$

finden.

Beweis: Wir betrachten wieder die additive Einbettung $\phi : K \to \mathbf{R}^n$ mit

$$\phi(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_{r_1}(\alpha), \mathrm{Re}\,\sigma_{r_1+1}(\alpha), \mathrm{Im}\,\sigma_{r_1+1}(\alpha), \ldots, \mathrm{Re}\,\sigma_{r_1+r_2}(\alpha), \mathrm{Im}\,\sigma_{r_1+r_2}(\alpha)).$$

Man sieht (ähnlich wie früher), daß die Menge

$$Q = \{(x_1, \ldots, x_{r_1}, y_1, z_1, \ldots, y_{r_2}, z_{r_2}) \in \mathbf{R}^n : |x_i| < c_i \text{ für } 1 \leq i \leq r_1 \text{ und } \sqrt{y_j^2 + z_j^2} < d_j \text{ für } 1 \leq j \leq r_2\}$$

konvex und symmetrisch ist und das Volumen $\mathrm{vol}\,(Q) = 2^{r_1}\pi^{r_2} c_1 \ldots c_{r_1} d_1^2 \ldots d_{r_2}^2$ hat. Nun gilt nach Wahl von c_i und d_j mit $\mathrm{vol}\,(\phi(R)) = 2^{-r_2}\sqrt{|\mathrm{disc}\,(R)|}$

$$\mathrm{vol}\,(Q) = 2^{r_1}\pi^{r_2}\left[(\frac{2}{\pi})^{r_2}\sqrt{|\mathrm{disc}\,(R)|} + \varepsilon\right] = 2^n \cdot (\frac{1}{2})^{r_2}\sqrt{|\mathrm{disc}\,(R)|} + 2^{r_1}\pi^{r_2}\varepsilon > 2^n \cdot \mathrm{vol}\,(\phi(R)).$$

Also liefert der Minkowskische Gitterpunktsatz ein $\alpha \in R$, $\alpha \neq 0$ mit $\phi(\alpha) \in Q$. Das bedeutet aber

$$|\sigma_i\alpha| < c_i \text{ für } 1 \leq i \leq r_1 \quad \text{und} \quad |\sigma_{r_1+j}\alpha| < d_j \text{ für } 1 \leq j \leq r_2,$$

was zusammen mit

$$|\mathrm{N}\alpha| = \prod_{i=1}^{r_1} |\sigma_i\alpha| \cdot \prod_{j=1}^{r_2} |\sigma_{r_1+j}\alpha|^2$$

die Behauptung liefert. Setzt man α als $\alpha = x_1\alpha_1 + \cdots + x_n\alpha_n$ an, so folgt wie üblich

$$x_i = \mathrm{Sp}(\alpha\beta_i) = \sum_{j=1}^{r_1} \sigma_j(\beta_i)\sigma_j(\alpha) + \sum_{j=1}^{r_2} (\sigma_{r_1+j}(\beta_i)\sigma_{r_1+j}(\alpha) + \overline{\sigma_{r_1+j}(\beta_i)\sigma_{r_1+j}(\alpha)})$$

und damit

$$|x_i| \leq \sum_{j=1}^{r_1} |\sigma_j\beta_i||\sigma_j\alpha| + 2\sum_{j=1}^{r_2} |\sigma_{r_1+j}\beta_i||\sigma_{r_1+j}\alpha| < \sum_{j=1}^{r_1} |\sigma_j\beta_i| c_j + 2\sum_{j=1}^{r_2} |\sigma_{r_1+j}\beta_i| d_j,$$

was zu zeigen war. ■

Wir wenden die vorangegangenen Überlegungen nun zur Konstruktion von Einheiten an:

LEMMA. *Sei $1 \leq k \leq r_1 + r_2$. Es gibt eine Einheit $\varepsilon_k \in R^*$ mit*

$$|\sigma_k \varepsilon_k| > 1 \text{ und } |\sigma_i \varepsilon_k| < 1 \text{ für } i \neq k, 1 \leq i \leq r_1 + r_2.$$

Beweis:

1. Wir konstruieren eine Folge $\lambda_m \in R \setminus \{0\}$ mit $|\mathrm{N}\lambda_m| \leq (\frac{2}{\pi})^{r_2} \sqrt{|\mathrm{disc}\,(R)|} + 1$ und

   $$|\sigma_i \lambda_m| < |\sigma_i \lambda_{m-1}| \text{ für } 1 \leq i \leq r_1 + r_2, i \neq k \text{ und für alle } m \geq 1$$

   wie folgt: Wir starten mit $\lambda_0 = 1$. Seien jetzt $\lambda_0, \ldots, \lambda_{m-1}$ bereits konstruiert. Setze

   $$c_i = |\sigma_i \lambda_{m-1}| \text{ für } 1 \leq i \leq r_1, i \neq k \quad \text{und} \quad d_j = |\sigma_{r_1+j} \lambda_{m-1}| \text{ für } 1 \leq j \leq r_2, j \neq k.$$

   Wähle c_k bzw. d_k geeignet, so daß die Voraussetzungen des letzten Lemmas für $\varepsilon = 1$ erfüllt sind. Dann findet man dazu ein λ_m, das die gewünschten Bedingungen erfüllt.
2. Da die Normen der λ_m's beschränkt sind und die Faktorringe $R/|\mathrm{N}\lambda_m|R$ endlich sind, gibt es Indizes $m_1 < m_2$ mit

   $$|\mathrm{N}\lambda_{m_1}| = |\mathrm{N}\lambda_{m_2}| \quad \text{und} \quad \lambda_{m_1} \equiv \lambda_{m_2} \bmod |\mathrm{N}\lambda_{m_1}|.$$

   Wie wir im Lemma gezeigt haben, ist dann $\varepsilon = \frac{\lambda_{m_2}}{\lambda_{m_1}}$ eine Einheit. Nach Konstruktion gilt

   $$|\sigma_i \varepsilon| = \frac{|\sigma_i \lambda_{m_2}|}{|\sigma_i \lambda_{m_1}|} < 1 \text{ für } 1 \leq i \leq r_1 + r_2, i \neq k.$$

   Wegen $1 = |N\varepsilon|$ muß dann $|\sigma_k \varepsilon| > 1$ gelten. ■

LEMMA. *Sei $1 \leq k \leq r_1 + r_2$ fest gewählt. Die $r_1 + r_2 - 1$ Vektoren $\ell(\varepsilon_i)$, $1 \leq i \leq r_1 + r_2, i \neq k$ sind* **R**-*linear unabhängig, wobei ε_i wie im letzten Lemma gewählt ist.*

Beweis: Wir schreiben die Vektoren $\ell(\varepsilon_i)$, $i \neq k$, als Zeilen in eine Matrix A, d.h. wir bilden die $(r_1 + r_2 - 1) \times (r_1 + r_2)$-Matrix

$$A = (a_{ij})_{\substack{1 \leq i \leq r_1+r_2, i \neq k \\ 1 \leq j \leq r_1+r_2}} \quad \text{mit} \quad \ell(\varepsilon_i) = (a_{i1}, \ldots, a_{i,r_1+r_2}).$$

Nach Wahl der ε_i's gilt $a_{ij} < 0$ für $i \neq j$ und $a_{ii} > 0$. Wir müssen zeigen, daß A den Rang $r_1 + r_2 - 1$ hat. Dazu bestimmen wir alle Relationen $\sum_j a_{ij} x_j = 0$, $i \neq k$. Wir wissen, daß $\sum_j a_{ij} = 0$ gilt. Sei $\sum_j a_{ij} x_j = 0$, $i \neq k$, eine weitere Relation. Da dann für $v, w \in \mathbf{R}$ auch $\sum_{j=1}^{r_1+r_2} a_{ij}(vx_j + w) = 0$ gilt, können wir (nach Übergang von x_j zu $vx_j + w$) annehmen, daß es einen Index $l \neq k$ gibt mit $x_l \geq x_j$ für alle j. Nun gilt für $l \neq j$: $a_{lj} < 0$ und daher $a_{lj}(x_l - x_j) \leq 0$. Es folgt

$$\sum_{j \neq l} a_{lj}(x_l - x_j) = \sum_j a_{lj}(x_l - x_j) = x_l \sum_j a_{lj} - \sum_j a_{lj} x_j = 0,$$

was wegen $a_{lj} < 0$ dann $x_l = x_j$ liefert. Es gibt also im wesentlichen nur eine Relation, d.h. der Kern der Matrix A hat Dimension 1. Also hat die Matrix A Rang $r_1 + r_2 - 1$, was wir zeigen wollten. ■

Es ergibt sich unmittelbar:

FOLGERUNG. *$\ell(R^*)$ ist ein Gitter vom Rang $r_1 + r_2 - 1$.*

Zusammen mit unserem ersten Struktursatz liefert das den Beweis des Satzes von Dirichlet.

Ein System von Grundeinheiten von R ist eine Menge von Einheiten $\varepsilon_1, \ldots, \varepsilon_{r_1+r_2-1} \in R^*$, so daß $\ell(\varepsilon_1), \ldots, \ell(\varepsilon_{r_1+r_2-1})$ eine Gitterbasis von $\ell(R^*)$ bilden.

6. Der Regulator

LEMMA. *Sei $\varepsilon_1, \ldots, \varepsilon_{r_1+r_2-1} \in R^*$ ein System von Grundeinheiten von R. Sei A die Matrix mit den Zeilen $\ell(\varepsilon_i)$, also*

$$A = \begin{pmatrix} \ln|\sigma_1\varepsilon_1| & \ldots & 2\ln|\sigma_{r_1+r_2}\varepsilon_1| \\ \vdots & & \vdots \\ \ln|\sigma_1\varepsilon_{r_1+r_2-1}| & \ldots & 2\ln|\sigma_{r_1+r_2}\varepsilon_{r_1+r_2-1}| \end{pmatrix}$$

und A_k die Matrix, die durch Streichen der k-ten Spalte aus A entsteht. Dann ist $|\det(A_k)|$ unabhängig von k und von der Wahl der Grundeinheiten und wird der Regulator von R genannt: $\operatorname{Reg}(R) = |\det A_k|$.

Beweis:

- Wir vergrößern obige Matrix A durch eine erste Zeile $(1\,1\ldots1)$ und deuten in der Mitte die k-te Spalte an, also

$$B = \begin{pmatrix} 1 & \ldots & 1 & \ldots & 1 \\ \ln|\sigma_1\varepsilon_1| & \ldots & u\ln|\sigma_k\sigma_1| & \ldots & 2\ln|\sigma_{r_1+r_2}\varepsilon_1| \\ \vdots & & \vdots & & \vdots \\ \ln|\sigma_1\varepsilon_{r_1+r_2-1}| & \ldots & u\ln|\sigma_k\varepsilon_{r_1+r_2-1}| & \ldots & 2\ln|\sigma_{r_1+r_2}\varepsilon_{r_1+r_2-1}| \end{pmatrix}$$

  mit $u = 1$ für $k \le r_1$ und $u = 2$ für $k > r_1$. Nun addieren wir die anderen Spalten zur k-ten Spalte und erhalten

$$\widetilde{B} = \begin{pmatrix} 1 & \ldots & r_1+r_2 & \ldots & 1 \\ \ln|\sigma_1\varepsilon_1| & \ldots & 0 & \ldots & 2\ln|\sigma_{r_1+r_2}\varepsilon_1| \\ \vdots & & \vdots & & \vdots \\ \ln|\sigma_1\varepsilon_{r_1+r_2-1}| & \ldots & 0 & \ldots & 2\ln|\sigma_{r_1+r_2}\varepsilon_{r_1+r_2-1}| \end{pmatrix}.$$

  Natürlich gilt $\det\widetilde{B} = \det B$. Entwicklung nach der k-te Spalte liefert dann

$$\det\widetilde{B} = \pm(r_1+r_2)\det A_k.$$

  Dies beweist, daß $|\det A_k|$ unabhängig von k ist.
- Hat man eine andere Gitterbasis von $\ell(R^*)$, so entsteht die zugehörige Matrix A durch elementare Zeilenumformungen aus der Ausgangsmatrix A. Die entsprechenden Determinanten ändern sich höchstens um ±1. ■

Für praktische Bedürfnisse verkürzen wir die logarithmische Abbildung

$$\ell : R^* \to \mathbf{R}^{r_1+r_2}, \quad \alpha \mapsto (\ln|\sigma_1\alpha|, \ldots, \ln|\sigma_{r_1}\alpha|, 2\ln|\sigma_{r_1+1}\alpha|, \ldots, 2\ln|\sigma_{r_1+r_2}\alpha|)$$

zu einer Abbildung $\ell_1 : R^* \to \mathbf{R}^{r_1+r_2-1}$, indem wir einen Spaltenindex k auswählen und dann k-te Spalte herausstreichen:

$$\ell_1(\alpha) = \begin{cases} (\ln|\sigma_1\alpha|, \ldots, \ln|\sigma_{k-1}\alpha|, \ln|\sigma_{k+1}\alpha|, \ldots, \ln|\sigma_{r_1}\alpha|, \ldots, 2\ln|\sigma_{r_1+1}\alpha|, \ldots, 2\ln|\sigma_{r_1+r_2}\alpha|) \text{ bzw.} \\ (\ln|\sigma_1\alpha|, \ldots, \ln|\sigma_{r_1}\alpha|, 2\ln|\sigma_{r_1+1}\alpha|, \ldots, 2\ln|\sigma_{k-1}\alpha|, 2\ln|\sigma_{k+1}\alpha|, \ldots, 2\ln|\sigma_{r_1+r_2}\alpha|). \end{cases}$$

Nach Definition des Regulators gilt dann

$$\operatorname{Reg}(R) = |\det\begin{pmatrix} \ell_1(\varepsilon_1) \\ \vdots \\ \ell_1(\varepsilon_{r_1+r_2-1}) \end{pmatrix}|,$$

wenn $\varepsilon_1, \ldots, \varepsilon_{r_1+r_2-1}$ ein System von Grundeinheiten für R ist. Wir haben gezeigt, dass der Regulator nicht davon abhängt, welche Spalte man streicht.

Bemerkung: Gegeben sei eine Ordnung R eines Zahlkörpers K mit Invarianten $r_1 + 2r_2 = n$. Will man die Einheitengruppe R^* beschreiben, so stellen sich zwei Aufgaben:

- Bestimme die in K bzw. R gelegenen Einheitswurzeln.
- Bestimme ein System von Grundeinheiten $\varepsilon_1, \ldots, \varepsilon_{r_1+r_2-1}$ für R.

Die Bestimmung der Einheitswurzeln ist im Allgemeinen nicht zu problematisch, wie wir bereits gesehen haben. Die Konstruktion von Grundeinheiten teilt man meist wie folgt auf:

1. Konstruiere genügend viele Einheiten $\varepsilon_1, \varepsilon_2, \ldots$, d.h.
$$\mathbf{R}\ell_1(\varepsilon_1) + \mathbf{R}\ell_1(\varepsilon_2) + \cdots = \mathbf{R}^{r_1+r_2-1}$$
bzw.
$$\operatorname{Rang} \begin{pmatrix} \ell_1(\varepsilon_1) \\ \ell_1(\varepsilon_2) \\ \vdots \end{pmatrix} = r_1 + r_2 - 1.$$
2. Konstruiere aus den gefundenen Einheiten ein System von Grundeinheiten.

Das erste Problem wird im nächsten Kapitel behandelt. Dabei werden Einheiten als Nebenprodukt bei der Bestimmung der Klassengruppe anfallen. Das zweite Problem werden wir im Folgenden angehen.

7. Reduktion von vielen Einheiten auf ein System von unabhängigen Einheiten

Sei R Ordnung eines Zahlkörpers K mit Invarianten $r_1 + 2r_2 = n$ und $r = r_1 + r_2 - 1$. Nach dem Satz von Dirichlet gibt es ein System von Grundeinheiten $\eta_1, \ldots, \eta_r$, d.h.
$$\ell_1(R^*) = \mathbf{Z}^r \cdot \begin{pmatrix} \ell_1(\eta_1) \\ \vdots \\ \ell_1(\eta_r) \end{pmatrix} \quad \text{und} \quad \operatorname{Reg}(R) = |\det \begin{pmatrix} \ell_1(\eta_1) \\ \vdots \\ \ell_1(\eta_r) \end{pmatrix}|.$$
Leider kennen wir nicht einmal $\operatorname{Reg}(R)$.

Sind $\varepsilon_1, \ldots, \varepsilon_r$ Einheiten, so setzen wir
$$\operatorname{Reg}(\varepsilon_1, \ldots, \varepsilon_r) = |\det \begin{pmatrix} \ell_1(\varepsilon_1) \\ \vdots \\ \ell_1(\varepsilon_r) \end{pmatrix}|.$$
Gilt
$$\varepsilon_i = \zeta_i \prod_{j=1}^{r} \eta_j^{m_{ij}} \quad \text{mit} \quad \zeta_i \in \mu(K), \quad m_{ij} \in \mathbf{Z},$$
so folgt
$$\begin{pmatrix} \ell_1(\varepsilon_1) \\ \vdots \\ \ell_1(\varepsilon_r) \end{pmatrix} = (m_{ij}) \cdot \begin{pmatrix} \ell_1(\eta_1) \\ \vdots \\ \ell_1(\eta_r) \end{pmatrix}, \quad \text{also} \quad \operatorname{Reg}(\varepsilon_1, \ldots, \varepsilon_r) = |\det(m_{ij})| \cdot \operatorname{Reg}(R).$$

Wir nehmen nun an, wir haben genügend viele Einheiten $\varepsilon_1, \varepsilon_2, \ldots$ gefunden, sodass
$$\operatorname{Rang} \begin{pmatrix} \ell_1(\varepsilon_1) \\ \ell_1(\varepsilon_2) \\ \vdots \end{pmatrix} = r_1 + r_2 - 1$$
gilt. Wir wollen sie so abändern, dass
$$\ell_1(\varepsilon_i) \in \mathbf{Z}^r \begin{pmatrix} \ell_1(\varepsilon_1) \\ \ell_1(\varepsilon_2) \\ \vdots \end{pmatrix} \quad \text{für alle } i$$
gilt.

1. Nach eventueller Vertauschung von Indizes können wir annehmen, dass $\ell_1(\varepsilon_1), \ldots, \ell_1(\varepsilon_r)$ linear unabhängig über $\mathbf{R}$ sind.
2. Haben wir alle gefundenen Einheiten auf $\varepsilon_1, \ldots, \varepsilon_r$ zurückgeführt, sind wir fertig.

3. Wir betrachten ε_{r+1}. Wir haben Darstellungen

$$\ell_1(\varepsilon_{r+1}) = v \cdot \begin{pmatrix} \ell_1(\eta_1) \\ \vdots \\ \ell_1(\eta_r) \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} \ell_1(\varepsilon_1) \\ \vdots \\ \ell_1(\varepsilon_r) \end{pmatrix} = M \cdot \begin{pmatrix} \ell_1(\eta_1) \\ \vdots \\ \ell_1(\eta_r) \end{pmatrix}$$

mit $v \in \mathbf{Z}^r$, $M \in M_r(\mathbf{Z})$, $\det M \neq 0$. also

$$\ell_1(\varepsilon_{r+1}) = v \cdot M^{-1} \cdot \begin{pmatrix} \ell_1(\varepsilon_1) \\ \vdots \\ \ell_1(\varepsilon_r) \end{pmatrix}.$$

Es gibt also $c_1, \ldots, c_r \in \mathbf{Z}$ und $d \in \mathbf{N}$ mit $\mathrm{ggT}(d, c_1, \ldots, c_r) = 1$ und

$$\ell_1(\varepsilon_{r+1}) = \frac{1}{d}(c_1, \ldots, c_r) \cdot \begin{pmatrix} \ell_1(\varepsilon_1) \\ \vdots \\ \ell_1(\varepsilon_r) \end{pmatrix}.$$

Wir bestimmen nun $d, c_1, \ldots, c_r$. Das Problem sieht rechnerisch allerdings eher so aus

$$\ell_1(\varepsilon_{r+1}) \approx \frac{1}{d}(c_1, \ldots, c_r) \cdot \begin{pmatrix} \ell_1(\varepsilon_1) \\ \vdots \\ \ell_1(\varepsilon_r) \end{pmatrix},$$

da man mit reellen Zahlen rechnet. Allerdings kann man leicht testen, ob die gemutmaßten Zahlen $d, c_1, \ldots, c_r$ passen, indem man algebraisch testet, ob

$$\varepsilon_1^{c_1} \ldots \varepsilon_r^{c_r} \cdot \varepsilon_{r+1}^{-d}$$

eine Einheitswurzel ist.

4. Mit dem Hermiteschen Normalisierungsprozess bestimmen wir $S \in GL(\mathbf{Z})$ und $c \in \mathbf{N}$ mit

$$S \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_r \end{pmatrix} = \begin{pmatrix} c \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \text{also} \quad (c_1, \ldots, c_r) S^t = (c, 0, \ldots, 0).$$

Dabei gilt natürlich weiter $\mathrm{ggT}(c, d) = 1$. Mit $T = (S^t)^{-1} \in GL(\mathbf{Z})$ definieren wir

$$\varepsilon_i' = \prod_j \varepsilon_j^{t_{ij}}$$

und erhalten

$$\begin{aligned} \ell_1(\varepsilon_{r+1}) &= \frac{1}{d}(c_1, \ldots, c_r) \cdot \begin{pmatrix} \ell_1(\varepsilon_1) \\ \vdots \\ \ell_1(\varepsilon_r) \end{pmatrix} = \frac{1}{d}(c_1, \ldots, c_r) \cdot T^{-1} \cdot \begin{pmatrix} \ell_1(\varepsilon_1') \\ \vdots \\ \ell_1(\varepsilon_r') \end{pmatrix} = \\ &= \frac{1}{d}(c, 0, \ldots, 0) \cdot \begin{pmatrix} \ell_1(\varepsilon_1') \\ \vdots \\ \ell_1(\varepsilon_r') \end{pmatrix} = \frac{c}{d} \ell_1(\varepsilon_1'), \end{aligned}$$

also $\ell_1(\varepsilon_{r+1}^d) = \ell_1({\varepsilon_1'}^c)$. Es gibt also eine Einheitswurzel $\zeta \in \mu(K) \cap R$ mit

$$\varepsilon_{r+1}^d = \zeta {\varepsilon_1'}^c.$$

Mit dem erweiterten euklidischen Algorithmus findet man $a, b \in \mathbf{Z}$ mit

$$ac + bd = 1.$$

Wir setzen

$$\varepsilon_1'' = {\varepsilon_1'}^b \varepsilon_{r+1}^a$$

und erhalten

$$\begin{aligned} \varepsilon_1''^{\,c} &= \varepsilon_1'^{\,bc} \cdot \varepsilon_{r+1}^{ac} = (\varepsilon_1'^{\,c})^b \cdot \varepsilon_{r+1}^{ac} = (\zeta^{-1}\varepsilon_{r+1}^{d})^b \cdot \varepsilon_{r+1}^{ac} = \zeta^{-b} \cdot \varepsilon_{r+1}, \\ \varepsilon_1''^{\,d} &= \varepsilon_1'^{\,bd} \cdot \varepsilon_{r+1}^{ad} = \varepsilon_1'^{\,bd} \cdot (\varepsilon_{r+1}^{d})^a = \varepsilon_1'^{\,bd} \cdot (\zeta\varepsilon_1'^{\,c})^a = \zeta^a \cdot \varepsilon_1', \end{aligned}$$

also

$$\varepsilon_1' = \zeta^{-a} \cdot \varepsilon_1''^{\,d} \quad \text{und} \quad \varepsilon_{r+1} = \zeta^b \cdot \varepsilon_1''^{\,c}.$$

Wir haben damit

$$\ell_1(\varepsilon_1), \ldots, \ell_1(\varepsilon_{r+1}) \in \mathbf{Z}^r \cdot \begin{pmatrix} \ell_1(\varepsilon_1'') \\ \ell_1(\varepsilon_2') \\ \vdots \\ \ell_1(\varepsilon_r') \end{pmatrix} \quad \text{und} \quad \operatorname{Reg}(\varepsilon_1'', \varepsilon_2', \ldots, \varepsilon_r') = \frac{1}{d}\operatorname{Reg}(\varepsilon_1, \ldots, \varepsilon_r).$$

Wählen wir daher $\varepsilon_1'', \varepsilon_2', \ldots, \varepsilon_r'$ statt $\varepsilon_1, \ldots, \varepsilon_r$, so haben wir ε_{r+1} auf die ersten Einheiten zurückgeführt und wir können es streichen.

Beispiel: Wir betrachten den Zahlkörper $K = \mathbf{Q}(\alpha)$ mit $f(\alpha) = 0$ und $f = x^4 - 3x - 5$ und wollen ein System von Grundeinheiten für die Ordnung $\mathbf{Z}[\alpha]$ bestimmen.

1. Beim Versuch, die Klassengruppe zu bestimmen, traten als Nebenprodukt die angegebenen 12 Einheiten $e_1, \ldots, e_{12}$ auf.

$$
\begin{aligned}
e_1 &= 826342587286\alpha^3 - 931834427970\alpha^2 + 1050793469999\alpha - 3663966727459\\
e_2 &= -1171359538776826321 6\alpha^3 + 1320896640116173957 5\alpha^2\\
&\quad -14895238192127956934\alpha + 51937567536048219454\\
e_3 &= 3347178144931746165362 8\alpha^3 + 6008775650376289043227 6\alpha^2\\
&\quad +10786813026735760051201 7\alpha + 9322699153534813393164 4\\
e_4 &= -1562898461025860093864756553\alpha^3 - 2805678637344909541598670128\alpha^2\\
&\quad -5036688442886206923163701271\alpha - 4353049502826435537154711751\\
e_5 &= 8294385026985041095454078099972\alpha^3 - 9353255726602182156262201150437\alpha^2\\
&\quad +1054730307341618547925212976190 1\alpha - 3677693895410358291598318630991 6\\
e_6 &= -3503198129570110707640154871342196705\alpha^3\\
&\quad -6288859065143627127433354959761252443\alpha^2\\
&\quad -1128961219960815038149314729031429405 0\alpha\\
&\quad -9757252474494148121818358410593189791\\
e_7 &= -4513077290175096726850201268840287258 9\alpha^3\\
&\quad -8101770433262464996061582447571587085 1\alpha^2\\
&\quad -1454410814017750714132946266510637246 47\alpha\\
&\quad -1257000972495609881003998136401860245 14\\
e_8 &= 2846049848695580822854074861049213317213915224428 5\alpha^3\\
&\quad +5109161894025167751137345481726286894857893167787 5\alpha^2\\
&\quad +9171847524498832396401100361336864887935535758499 1\alpha\\
&\quad +7926935874485168413143255830483476331046467864690 1\\
e_9 &= 1018200395315922945025426089823685020754910049550 0\alpha^3\\
&\quad +1827849453379657877828648771225528296459005174878 5\alpha^2\\
&\quad +3281312440645509873308696710500758598398887992909 0\alpha\\
&\quad +2835933897905553688016125381365051227271917616940 1\\
e_{10} &= -1726048178930205402014165465977896295839875023327 7\alpha^3\\
&\quad -3098561181942601077021887635134152717798887453782 8\alpha^2\\
&\quad -5562464313245429364865739901469828235860257215818 1\alpha\\
&\quad -4807460852072771785152346314438210487754784468917 9\\
e_{11} &= 6215416352483949214717489280386978494828241554126 39\alpha^3\\
&\quad +1115776956547908049531394985570551576773723966827166\alpha^2\\
&\quad +2003016606064971230894548023461470246860260163633757\alpha\\
&\quad +1731143496377905590050200627788003039518012725404256\\
e_{12} &= 1384132319475662164245379388362390293590112101867531101921 3\alpha^3\\
&\quad +2484761855522275445288398772506536474500983708359767528374 6\alpha^2\\
&\quad +4460586167800312134323754370319597783005795821636273451897 7\alpha\\
&\quad +3855142643869964033124192763776038589085191884200728573810 4
\end{aligned}
$$

2. Die komplexen Nullstellen von f sind

$$\alpha_1 \approx -1.1277, \quad \alpha_2 \approx 1.7952, \quad \alpha_3 \approx -0.3338 + 1.5358i, \quad \alpha_4 = \overline{\alpha_3}.$$

Daher ist $r_1 = 2$, $r_2 = 1$. Die einzigen Einheitswurzeln in K sind also ± 1 und es gibt $r_1 + r_2 - 1 = 2$ unabhängige Grundeinheiten in $\mathbf{Z}[\alpha]$. Wir betrachten folgende logarithmische Abbildung

$$\ell_1 : K^* \to \mathbf{R}^2, \quad \beta \mapsto (\ln|\sigma_1\beta|, \ln|\sigma_2\beta|).$$

3. Wir beginnen mit $e_a = e_1$ und $e_b = e_2$ und erhalten (Rechengenauigkeit: 100 Stellen)

$$\begin{pmatrix} \ell_1(e_a) \\ \ell_1(e_b) \end{pmatrix} \approx \begin{pmatrix} 29.6077 & -49.7283 \\ 46.0747 & -57.9514 \end{pmatrix} \quad \text{mit} \quad \operatorname{Reg}(e_a, e_b) \approx 575.41$$

Wir betrachten jetzt e_3:

$$\ell_1(e_3) \approx (-39.8996, 54.8677) \quad \text{und} \quad \ell(e_3) \begin{pmatrix} \ell_1(e_a) \\ \ell_1(e_b) \end{pmatrix}^{-1} \approx (-0.3750, -0.6250).$$

Dies sieht aus wie $\frac{1}{8}(-3,-5)$. Tatsächlich überprüft man: $e_a^{-3}e_b^{-5} = -e_3^8$. Wir setzen also $d = 8$, $(c_1, c_2) = (-3, -5)$. Mit

$$S = \begin{pmatrix} -2 & 1 \\ -5 & 3 \end{pmatrix}$$

gilt $(c_1, c_2)S^t = (1, 0)$.

$$T = \begin{pmatrix} -3 & -5 \\ 1 & 2 \end{pmatrix} = (S^t)^{-1}.$$

Mit $a = 1, b = 0$, $ac + bd = 1$ erhalten wir

$$e'_a = e_a^{-3}e_b^{-5}, \quad e'_b = e_a e_b^2, \quad e''_a = e_3.$$

Wir setzen $e_a := e''_a$, $e_b := e'_b$ und erhalten

$$\begin{aligned} e_a &= 33471781449317461653628\alpha^3 + 60087756503762890432276\alpha^2 + \\ &\quad 10786813026735760051201 7\alpha + 9322699153534813393 1644, \\ e_b &= 865263444006705251423493252981763987083864379744 5500\alpha^3 \\ &\quad -975723967038579850508785936343972194549291700155 3173\alpha^2 \\ &\quad +110028600705119580234555457672921170198846556490463 52\alpha \\ &\quad -383654011188567086351840273657030678555575001594230 69. \end{aligned}$$

(Nun Rechengenauigkeit: 1000 Stellen) $\operatorname{Reg}(e_a, e_b) \approx 71.93$.

4. Für e_4 findet man

$$\ell_1(e_4) \begin{pmatrix} \ell_1(e_a) \\ \ell_1(e_b) \end{pmatrix}^{-1} \approx (23.3333, 7.3333) \approx \frac{1}{3}(70, 22).$$

Tatsächlich gilt $e_a^{70}e_b^{22} = -e_4^3$. Wir wählen also $d = 3$, $(c_1, c_2) = (70, 22)$.

$$S = \begin{pmatrix} 6 & -19 \\ 11 & -35 \end{pmatrix} \quad \text{mit} \quad (c, 0) = (2, 0), \quad T = (S^t)^{-1} = \begin{pmatrix} 35 & 11 \\ -19 & -6 \end{pmatrix}.$$

Damit $(c = 2, d = 3, a = -1, b = 1)$

$$e'_a = e_a^{35}e_b^{11}, \quad e'_b = e_a^{-19}e_b^{-6}, \quad e''_a = e'_a e_4^{-1}$$

Die neuen Werte für e_a und e_b sind

$$\begin{aligned} e_a &= 8808972166741\alpha^3 + 15813660094699\alpha^2 + 28388311468941\alpha + 24535113999456, \\ e_b &= +105491840684\alpha^3 - 118959042029\alpha^2 + 134145495602\alpha - 467746208971 \end{aligned}$$

mit $\operatorname{Reg}(e_a, e_b) \approx 23.98$.

5. e_5 erfüllt

$$\ell_1(e_5) \begin{pmatrix} \ell_1(e_a) \\ \ell_1(e_b) \end{pmatrix}^{-1} \approx (-40, -25),$$

und tatsächlich gilt $e_5 = e_a^{-40}e_b^{-25}$.

6. Für e_6 gilt
$$\ell_1(e_6)\begin{pmatrix}\ell_1(e_a)\\ \ell_1(e_b)\end{pmatrix}^{-1} \approx (1.6667,-0.6667)\approx\frac{1}{3}(5,-2),$$
und in der Tat ist $e_a^5e_b^{-2}=-e_6^3$. Mit $(c_1,c_2)=(5,-2)$, $d=3$, $c=1$ finden wir
$$S=\begin{pmatrix}1&2\\2&5\end{pmatrix},\quad T=\begin{pmatrix}5&-2\\-2&1\end{pmatrix}$$
und
$$e_a''=e_6,\quad e_b'=e_a^{-2}e_b.$$
Die neuen Größen sind:
$$\begin{aligned}e_a &= -350319812957011070764015487134219670 5\alpha^3\\ &\quad -628885906514362712743335495976125244 3\alpha^2\\ &\quad -112896121996081503814931473 90314294050\alpha\\ &\quad -975725247449414812181835841059318979 1,\\ e_b &= 373144233738245766839991462 8\alpha^3-420780254317355410414365642 4\alpha^2\\ &\quad +474497543884277298056978781 7\alpha-165450514542311862853572495 56\end{aligned}$$
mit $\mathrm{Reg}\,(e_a,e_b)\approx 7.99$.
7. Unter Verwendung von ℓ_1 findet man $e_7=-e_a^{-58}\cdot e_b^{-45}$, $e_8=-e_a^{-59}\cdot e_b^{-46}$, $e_9=e_a^{-80}\cdot e_b^{-62}$, $e_{10}=-e_a^{42}\cdot e_b^{31}$, $e_{11}=e_a^4\cdot e_b^2$, $e_{12}=e_a^{16}\cdot e_b^{11}$, d.h. wir haben alle 12 Einheiten e_i auf e_a und e_b zurückgeführt.
8. Um eventuell kleinere Koeffizienten für e_a und e_b zu erhalten, wenden für auf die Vektoren
$$\ell_1(e_a)\approx(-50.12,87.15),\quad \ell_1(e_b)\approx(65.65,-114.32)$$
LLL-Reduktion an. Mit der Transformationsmatrix
$$T=\begin{pmatrix}21&16\\-38&-29\end{pmatrix}$$
erhält man
$$e_a=-1-\alpha\quad\text{und}\quad e_b=4+6\alpha+3\alpha^2+2\alpha^3$$
mit Regulator 7.99.

8. Neue Einheiten durch Wurzelziehen

Seien $\varepsilon_1,\dots,\varepsilon_r$ unabhängige Einheiten einer Ordnung R und $\eta_1,\dots,\eta_r$ ein System von Grundeinheiten.
$$\mathbf{Z}\ell_1(\varepsilon_1)+\cdots+\mathbf{Z}\ell_1(\varepsilon_r)\subseteq\mathbf{Z}\ell_1(\eta_1)+\cdots+\mathbf{Z}\ell_1(\eta_r)$$
sind Gitter mit Determinanten $\mathrm{Reg}\,(\varepsilon_1,\dots,\varepsilon_r)$ bzw. $\mathrm{Reg}\,(\eta_1,\dots,\eta_r)$. Der Gitterindex ist
$$\frac{\mathrm{Reg}\,(\varepsilon_1,\dots,\varepsilon_r)}{\mathrm{Reg}\,(\eta_1,\dots,\eta_r)}.$$
Angenommen, eine Primzahl p teilt den Gitterindex. Dann gibt es eine Einheit η mit
$$\ell_1(\eta)\notin\mathbf{Z}\ell_1(\varepsilon_1)+\cdots+\mathbf{Z}\ell_1(\varepsilon_r),\quad\text{aber}\quad p\ell_1(\eta)\in\mathbf{Z}\ell_1(\varepsilon_1)+\cdots+\mathbf{Z}\ell_1(\varepsilon_r).$$
Es gibt also o.E. $c_i\in\{0,1,\dots,p-1\}$, $\zeta\in\mu(K)$ mit $(c_1,\dots,c_r)\neq(0,\dots,0)$ und
$$\eta^p=\zeta\cdot\varepsilon_1^{c_1}\dots\varepsilon_r^{c_r}.$$
d.h. das Polynom
$$x^p-\zeta\cdot\varepsilon_1^{c_1}\dots\varepsilon_r^{c_r}$$
spaltet den Linearfaktor $x-\eta$ über K ab.

Auf diese Weise kann man für kleine Primzahlen testen, ob der Regulator durch p teilbar ist und eventuell die Einheitengruppe vergrößern.

Beispiel: Wir betrachten wieder das Beispiel $K = \mathbf{Q}(\alpha)$ mit $\alpha^4 - 3\alpha - 5 = 0$. Wir gehen aus von den Einheiten

$$\begin{aligned} e_1 &= 826342587286\alpha^3 - 931834427970\alpha^2 + 1050793469999\alpha - 3663966727459, \\ e_2 &= -1171359538776826321 6\alpha^3 + 1320896640116173957 5\alpha^2 - 1489523819212795693 4\alpha \\ &\quad +51937567536048219454. \end{aligned}$$

LLL-Reduktion ergibt mit $T = \begin{pmatrix} -1 & 1 \\ 4 & -3 \end{pmatrix}$

$$\begin{aligned} e_{1s} &= 1622655\alpha^3 - 1829805\alpha^2 + 2063400\alpha - 7194781, \\ e_{2s} &= -831696551 - 1856295269\alpha - 110823495\alpha^2 + 781509404\alpha^3. \end{aligned}$$

Das Polynom $x^2 + e_{1s}$ hat eine Wurzel e_{1t}:

$$e_{1t} = 1911 - 431\alpha^3 + 486\alpha^2 - 548\alpha.$$

Das Polynom $x^2 - e_{1t}$ hat eine Wurzel e_{1u}:

$$e_{1u} = -7\alpha^3 + 8\alpha^2 - 9\alpha + 31.$$

Das Polynom $x^2 - e_{1u}$ hat eine Wurzel e_{1v}:

$$e_{1v} = -4 + a - a^2 + a^3.$$

Weitere Faktorisierungsversuche $x^2 - \ldots$ oder $x^2 + \ldots$ helfen nicht weiter, d.h. der Regulator ist nicht mehr durch 2 teilbar. Wir haben jetzt

$$\begin{aligned} e_{1v} &= -4 + \alpha - \alpha^2 + \alpha^3, \\ e_{2s} &= -831696551 - 1856295269\alpha - 110823495\alpha^2 + 781509404\alpha^3. \end{aligned}$$

Wir probieren nun mit $p = 3$. Das Polynom $x^3 - e_{1v}e_{2s}$ hat eine Wurzel e_{2t}:

$$e_{2t} = -616 - 46\alpha^3 + 335\alpha^2 - 110\alpha.$$

Das Polynom $x^3 - e_{1v}^2 e_{2t}$ hat eine Wurzel e_{2u}:

$$e_{2u} = -1 + 2\alpha + \alpha^2 - \alpha^3.$$

Der Regulator ist nun 7.99.

9. Wie weit sind unabhängige Einheiten von Grundeinheiten entfernt?

Wir sind jetzt in folgender Situation: Wir haben Einheiten $\varepsilon_1, \ldots, \varepsilon_r \in R^*$ (mit $r = r_1 + r_2 - 1$), so dass $\ell(\varepsilon_1), \ldots, \ell(\varepsilon_r)$ in $\mathbf{R}^{r_1+r_2}$ linear unabhängig sind. Kann man daraus ein System von Grundeinheiten erhalten?

Der folgende Weg zeigt eine prinzipielle Möglichkeit, die aber nur dann praktisch anwendbar ist, wenn die auftretenden Zahlen nicht zu groß sind.

Ist $\varepsilon \in R^*$ irgendeine Einheit, so gibt es $\lambda_i \in \mathbf{R}$ mit $\ell(\varepsilon) = \sum_i \lambda_i \ell(\varepsilon_i)$. Schreibt man $\lambda_i = m_i + \mu_i$ mit $|\mu_i| \leq \frac{1}{2}$, so ist $\ell(\varepsilon\varepsilon_1^{-m_1} \ldots \varepsilon_r^{-m_r}) = \sum_i \mu_i \ell(\varepsilon_i)$. Um ein System von Grundeinheiten zu erhalten, nehmen wir zu $\varepsilon_1, \ldots, \varepsilon_r$ die Einheiten ε der Menge

$$\{\varepsilon \in R^* : \ell(\varepsilon) = \sum_i \mu_i \ell(\varepsilon_i), |\mu_i| \leq \frac{1}{2}\}$$

hinzu und gewinnen dann mit dem zuvor beschriebenen Normalisierungsverfahren eine $\mathbf{Z}$-Basis. Dass man das im Prinzip effektiv machen kann, zeigt das folgende Lemma:

LEMMA. *Seien $\varepsilon_1,\dots,\varepsilon_r \in R^*$ mit $r = r_1 + r_2 - 1$, sodass $\ell(\varepsilon_1),\dots,\ell(\varepsilon_r)$ in $\mathbf{R}^{r_1+r_2}$ linear unabhängig sind. Sei $\alpha_1,\dots,\alpha_n$ eine $\mathbf{Z}$-Basis von R und $\beta_1,\dots,\beta_n$ die Dualbasis. Ist $\varepsilon = x_1\alpha_1 + \cdots + x_n\alpha_n \in R^*$ eine Einheit mit*

$$\ell(\varepsilon) = \sum_k \mu_k \ell(\varepsilon_k) \quad \text{und} \quad |\mu_k| \le \frac{1}{2},$$

so gilt

$$|x_i| \le \sum_j |\sigma_j\beta_i||\sigma_j\varepsilon| \le \sum_j |\sigma_j\beta_i| \prod_k \max(\sqrt{|\sigma_j\varepsilon_k|}, \frac{1}{\sqrt{|\sigma_j\varepsilon_k|}}).$$

Insbesondere gibt es also nur endlich viele solcher Einheiten.

Beweis: Wir haben $\ell(\varepsilon) = \sum_k \mu_k \ell(\varepsilon_k)$ und daher

$$\ln|\sigma_j\varepsilon| = \sum_k \mu_k \ln|\sigma_j\varepsilon_k|, \quad \text{also} \quad |\sigma_j\varepsilon| = \prod_k |\sigma_j\varepsilon_k|^{\mu_k},$$

was wegen $|\mu_k| \le \frac{1}{2}$ durch

$$|\sigma_j\varepsilon| \le \prod_k \max(\sqrt{|\sigma_j\varepsilon_k|}, \frac{1}{\sqrt{|\sigma_j\varepsilon_k|}})$$

abgeschätzt werden kann. Mit $x_i = \mathrm{Sp}(\varepsilon\beta_i) = \sum_j \sigma_j\beta_i\sigma_j\varepsilon$ folgt dann wie üblich

$$|x_i| \le \sum_j |\sigma_j\beta_i||\sigma_j\varepsilon| \le \sum_j |\sigma_j\beta_i| \prod_k \max(\sqrt{|\sigma_j\varepsilon_k|}, \frac{1}{\sqrt{|\sigma_j\varepsilon_k|}}),$$

was gezeigt werden sollte. ■

Beispiel: Wir betrachten wieder $K = \mathbf{Q}(\alpha)$ mit $\alpha^4 - 3\alpha - 5 = 0$. Wir haben die Einheiten

$$e_a = -1 - \alpha \quad \text{und} \quad e_b = 4 + 6\alpha + 3\alpha^2 + 2\alpha^3$$

gefunden mit Regulator 7.99. Weitere Einheiten $u = u_3\alpha^3 + u_2\alpha^2 + u_1\alpha + u_0$ erfüllen mit dem Lemma die Ungleichungen

$$|u_3| \le 1.46, \quad |u_2| \le 2.22, \quad |u_1| \le 3.46, \quad |u_0| \le 4.99.$$

findet die Einheiten

$$\pm 1, \quad \pm(\alpha+1), \quad \pm(\alpha^2+2\alpha+1), \quad \pm(\alpha^3-\alpha^2-2\alpha+1), \quad \pm(\alpha^3-\alpha-4), \quad \pm(\alpha^3-\alpha^2+\alpha-4),$$

was aber wegen

$$\alpha+1 = -e_a, \quad \alpha^2+2\alpha+1 = e_a^2, \quad \alpha^3-\alpha^2+2\alpha+1 = -e_b^{-1}, \quad \alpha^3-\alpha-4 = e_a^{-1}e_b^{-1}, \quad \alpha^3-\alpha^2+\alpha-4 = -e_a^{-1}$$

nichts Neues ergibt. Also ist $R^* = \{\pm e_a^a e_b^b : a,b \in \mathbf{Z}\}$.

Beispiel: $K = \mathbf{Q}(\alpha)$ mit $\alpha^2 = 11$. Dann ist $\mathbf{Z}_K = \mathbf{Z}[\alpha]$ und $\mu(K) = \{\pm 1\}$. Durch Probieren findet man, dass $\varepsilon = 3\alpha + 10$ eine Einheit ist. Ist ε Grundeinheit? Wir haben $\sigma_1\alpha = 3.32$, $\sigma_2\alpha = -3.22$, $\sigma_1\varepsilon = 19.95$, $\sigma_2\varepsilon = 0.05$. Damit folgt $\max(|\sigma_j\varepsilon|^{1/2}, |\sigma_j\varepsilon|^{-1/2}) \le 4.47$. Die Dualbasis zu $\alpha_1 = \alpha$, $\alpha_2 = 1$ ist $\beta_1 = \frac{1}{22}\alpha$, $\beta_2 = \frac{1}{2}$. Mit dem Satz ergibt sich $|x_k| \le 4.47(|\sigma_1\beta_k| + |\sigma_2\beta_k|)$ und damit $|x_1| \le 1.35$, $|x_2| \le 4.47$. Die einzigen Einheiten, die diesen Ungleichungen genügen, sind ± 1. Also ist ε Grundeinheit und damit $\mathrm{Reg}\,(K) = 2.9932$.

Beispiel: Wir wollen für $\mathbf{Q}(\alpha)$ mit $\alpha^3 = 2$ die Einheitengruppe $\mathbf{Z}[\alpha]^*$ bestimmen. Durch Ausprobieren findet man, daß $\varepsilon = \alpha - 1$ eine Einheit ist. Mit dem Lemma müssen wir nach Einheiten $x_2\alpha^2 + x_1\alpha + x_0$ suchen mit

$$|x_2| \le 1.01, \quad |x_1| \le 1.26, \quad |x_0| \le 1.59.$$

Als Einheiten, die dieser Abschätzung genügen findet man ± 1, $\pm(\alpha-1)$, $\pm(\alpha^2+\alpha+1)$. Nun ist aber $\alpha^2+\alpha+1 = (\alpha-1)^{-1}$, also ist ε Grundeinheit und $\mathrm{Reg}\,(K) = 1.3474$.

Beispiel: Wir betrachten $K = \mathbf{Q}(\alpha)$ mit $f(\alpha) = 0$ und $f = 2 + 3x + 5x^2 + 7x^3 + x^4$. Die Diskriminante von $\mathbf{Z}[\alpha]$ ist $-80876 = -2^2 \cdot 20219$. Mit der Faktorisierung $f \equiv x(x+1)^3 \bmod 2$ rechnet man nach $(2,\alpha)\cdot(2,\alpha+1)^3 = (2)$, also verzweigt 2 und damit folgt $\mathbf{Z}_K = \mathbf{Z}[\alpha]$. Man hat $r_1 = 2$, $r_2 = 1$, die Minkowski-Schranke ist ≤ 33.95.

Wir wollen die Einheitengruppe von $\mathbf{Z}_K$ bestimmen. Bei der Bestimmung der Klassengruppe haben wir unter anderem auch die Einheiten

$$\varepsilon_1 = 7\alpha^3 + 51\alpha^2 + 46\alpha + 9 \quad \text{und} \quad \varepsilon_2 = 98\alpha^3 + 87\alpha^2 + 53\alpha + 31$$

gefunden.
Wollte man das angegebene Lemma anwenden, müsste man nach Einheiten $\varepsilon = x_3\alpha^3 + x_2\alpha^2 + x_1\alpha + x_0$ mit

$$|x_3| \leq 2686, \quad |x_2| \leq 16817, \quad |x_1| \leq 1065, \quad |x_0| \leq 7290$$

suchen. Das ist für unsere Verhältnisse zu groß, um alle Möglichkeiten durchzuprobieren. Daher probieren wir zunächst die Faktorisierungsmethode. Tatsächlich hat $x^2 - e_1e_2$ eine Nullstelle e_{2s} mit

$$e_{2s} = 4\alpha^3 + 30\alpha^2 + 24\alpha + 3$$

mit Regulator 39.62. LLL-Reduktion führt auf

$$e_1' = 7\alpha^3 + 51\alpha^2 + 46\alpha + 9, \quad e_2' = 2\alpha^3 + \alpha^2 + \alpha + 1.$$

Mit dem Lemma suchen wir nach weiteren Einheiten $u = u_3\alpha^3 + u_2\alpha^2 + u_1\alpha + u_0$, die den Abschätzungen

$$|u_3| \leq 24, \quad |u_2| \leq 152, \quad |u_1| \leq 20, \quad |u_0| \leq 65$$

genügen. Wir finden (nach längerem Suchen) bis auf ± 1 die Einheiten

$$1, \quad 2\alpha^3 + \alpha^2 + \alpha + 1 = e_2', \quad 18\alpha^3 + 113\alpha^2 + 7\alpha + 49 = -{e_1'}^{-1}, \quad 21\alpha^3 + 16\alpha^2 + 9\alpha + 7 = -{e_1'}^{-1}e_2'.$$

Also folgt $\mathbf{Z}[\alpha]^* = \{\pm {e_1'}^a {e_2'}^b : a, b \in \mathbf{Z}\}$.

KAPITEL 9

Ansätze zur Berechnung von $C\ell(\mathbf{Z}_K)$ und $\mathbf{Z}_K^*$

1. Einführung

Wir wollen anhand eines Beispiels skizzieren, wie man für einen Zahlkörper K die Berechnung von $C\ell(\mathbf{Z}_K)$ und $\mathbf{Z}_K^*$ praktisch angehen kann.

Als Beispiel wählen wir $K = \mathbf{Q}(\alpha)$ mit $f(\alpha) = 0$ und

$$f = x^3 - 11.$$

2. Bestimmung eine Z-Basis von $\mathbf{Z}_K$

Zunächst sollte man eine $\mathbf{Z}$-Basis von $\mathbf{Z}_K$ bestimmen. In unserem Beispiel findet man $\mathbf{Z}_K = \mathbf{Z}\alpha^2 + \mathbf{Z}\alpha + \mathbf{Z}$ mit der Diskriminante: $-3267 = -3^3 \cdot 11^2$.

3. Primideale

Man bestimmt endlich viele Primideale $\mathfrak{p}_i$, $i = 1, \ldots, r$, z.B. alle deren Norm $\leq (\frac{4}{\pi})^{r_2} \frac{n!}{n^n} \sqrt{|\mathrm{disc}\,(K)|}$ (Minkowski-Schranke) ist und die nicht träge sind, zusammen mit $\lambda_{\mathfrak{p}_i} \in K \setminus \mathbf{Z}_K$ und $\lambda_{\mathfrak{p}_i}\mathfrak{p}_i \subseteq \mathbf{Z}_K$, mit deren Hilfe sich die Bewertungen $v_{\mathfrak{p}_i}$ leicht berechnen lassen. Sei weiter p_i die in $\mathfrak{p}_i$ enthaltene Primzahl.

In unserem Beispiel ist die Minkowski-Schranke ≤ 16.2. Die Primideale erhält man durch Faktorisieren von $f \bmod p$:

$$\begin{aligned}
f &\equiv (x+1)(x^2+x+1) \bmod 2,\\
f &\equiv (x+1)^3 \bmod 3,\\
f &\equiv (x+4)(x^2+x+1) \bmod 5,\\
f &\equiv x^3+3 \bmod 7,\\
f &\equiv x^3 \bmod 11,\\
f &\equiv x^3+2 \bmod 13.
\end{aligned}$$

Wir wählen die Primideale

Name	Erzeugendensystem	$\lambda_{\mathfrak{p}}$	Norm
$\mathfrak{p}_2$	$(2, \alpha+1)$	$(\alpha^2+\alpha+1)/2$	2
$\mathfrak{p}_4$	$(2, \alpha^2+\alpha+1)$	$(\alpha+1)/2$	4
$\mathfrak{p}_3$	$(3, \alpha+1)$	$(\alpha^2+2\alpha+1)/3$	3
$\mathfrak{p}_5$	$(5, \alpha+4)$	$(\alpha^2+\alpha+1)/5$	5
$\mathfrak{p}_{25}$	$(5, \alpha^2+\alpha+1)$	$(\alpha+4)/5$	25
$\mathfrak{p}_{11}$	$(11, \alpha)$	$\alpha^2/11$	11

Version vom 13.3.2003

4. Erzeugung von Relationen

Wähle $\beta \in \mathbf{Z}_K$, berechne $\mathrm{N}\beta$ und teste, ob sich $|\mathrm{N}\beta|$ als Produkt der Primzahlen $p_1, \ldots, p_r$ schreiben läßt. Wenn dies nicht der Fall ist, wählt man ein anderes $\beta \in \mathbf{Z}_K$. Andernfalls hat man eine Relation

$$(\beta) = \mathfrak{p}_1^{v_{\mathfrak{p}_1}(\beta)} \ldots \mathfrak{p}_r^{v_{\mathfrak{p}_r}(\beta)}.$$

Wir wählen einen geeigneten Index i, setzen $\alpha_i = \beta$, berechnen $v_{ij} = v_{\mathfrak{p}_j}(\beta)$ und erhalten

$$\prod_{j=1}^{r} \mathfrak{p}_j^{v_{ij}} = (\alpha_i).$$

Auf diese Weise sammeln wir einige Relationen und erhalten eine Matrix $(v_{ij})_{i=1,\ldots,m,j=1,\ldots,r}$ und Elemente $(\alpha_i)_{i=1,\ldots,m}$.

In unserem Beispiel wählen wir zunächst $\beta = 2, 3, 5, 11$, dann $\beta = \alpha, \alpha+1, \alpha-1, \alpha-2, \alpha+4$. ($\beta = \alpha+2$ geht nicht wegen $\mathrm{N}(\alpha+2) = 19$.) Wir listen dies in einer Tabelle auf:

β	$\mathrm{N}(\beta)$	$v_{\mathfrak{p}_{11}}(\beta)$	$v_{\mathfrak{p}_{25}}(\beta)$	$v_{\mathfrak{p}_5}(\beta)$	$v_{\mathfrak{p}_3}(\beta)$	$v_{\mathfrak{p}_4}(\beta)$	$v_{\mathfrak{p}_2}(\beta)$
11	11^3	3	0	0	0	0	0
5	5^3	0	1	1	0	0	0
3	3^3	0	0	0	3	0	0
2	2^3	0	0	0	0	1	1
α	11	1	0	0	0	0	0
$\alpha+1$	$2^2 \cdot 3$	0	0	0	1	0	2
$\alpha-1$	$2 \cdot 5$	0	0	1	0	0	1
$\alpha-2$	3	0	0	0	1	0	0
$\alpha+4$	$3 \cdot 5^2$	0	0	2	1	0	0

Ordnen wir die Primideale in der Reihenfolge $\mathfrak{p}_{11}$, $\mathfrak{p}_{25}$, $\mathfrak{p}_5$, $\mathfrak{p}_3$, $\mathfrak{p}_4$, $\mathfrak{p}_2$, so erhalten wir also

$$V = (v_{ij})_{i=1,\ldots,9,j=1,\ldots,6} = \begin{pmatrix} 3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 1 & 0 & 0 \end{pmatrix} \quad \text{und} \quad (\alpha_i)_{i=1,\ldots,9} = \begin{pmatrix} 11 \\ 5 \\ 3 \\ 2 \\ \alpha \\ \alpha+1 \\ \alpha-1 \\ \alpha-2 \\ \alpha+4 \end{pmatrix}.$$

5. Umformung der Relationenmatrix

Aus

$$\prod_j \mathfrak{p}_j^{v_{i_1 j}} = (\alpha_{i_1}), \quad \prod_j \mathfrak{p}_j^{v_{i_2 j}} = (\alpha_{i_2}), \quad \ell \in \mathbf{Z}$$

folgt sofort

$$\prod_j \mathfrak{p}_j^{\ell v_{i_1 j} + v_{i_2 j}} = (\alpha_{i_1}^{\ell} \alpha_{i_2}).$$

Man kann also aus gegebenen Relationen leicht neue erzeugen. Wir verallgemeinern dies wie folgt: Ist $S = (s_{ij})_{i=1,\ldots,m,j=1,\ldots,m}$ eine ganzzahlige Matrix, so gilt für $i = 1, \ldots, m$

$$(\prod_j \alpha_j^{s_{ij}}) \quad = \quad \prod_j (\alpha_j)^{s_{ij}} = \prod_j (\prod_k \mathfrak{p}_k^{v_{jk}})^{s_{ij}} = \prod_k \prod_j \mathfrak{p}_k^{s_{ij} v_{jk}} = \prod_k \mathfrak{p}_k^{\sum_j s_{ij} v_{jk}} = \prod_k \mathfrak{p}_k^{(SV)_{ik}}.$$

Gilt jetzt $m \geq r$ und hat die Matrix V Rang r, so gibt es $S \in GL_m(\mathbf{Z})$, sodass SV in Hermitescher Normalform ist.

In unserem Beispiel folgt mit

$$S = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & -1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 & -3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & -3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & -2 & -2 & 1 \end{pmatrix}$$

$$SV = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{und} \quad SA = (\prod_j \alpha_j^{s_{ij}})_{i=1,\dots,9} = \begin{pmatrix} \alpha \\ 4\alpha^2+9\alpha+19 \\ \alpha-1 \\ \alpha-2 \\ 2 \\ \alpha^2+2\alpha+5 \\ 1 \\ 18\alpha^2+40\alpha+89 \\ 18\alpha^2+40\alpha+89 \end{pmatrix}.$$

Die letzten 3 Zeilen von SV sind 0, also liefern die entsprechenden Zeilen von SA Einheiten. In unserem Beispiel ist also

$$18\alpha^2+40\alpha+89$$

eine nichttriviale Einheit.
Die ersten Zeilen der Matrix SV liefern folgende Beziehungen

$$\begin{aligned} \mathfrak{p}_{11} &= (\alpha), \\ \mathfrak{p}_{25} &= (4\alpha^2+9\alpha+19)\mathfrak{p}_2^{-1} = (4\alpha^2+9\alpha+19)\mathfrak{p}_2^{-2}\mathfrak{p}_2 = \frac{4\alpha^2+9\alpha+19}{\alpha^2+2\alpha+5}\mathfrak{p}_2 = \frac{\alpha^2+\alpha+1}{2}\mathfrak{p}_2, \\ \mathfrak{p}_5 &= (\alpha-1)\mathfrak{p}_2^{-1} = (\alpha-1)\mathfrak{p}_2^{-2}\mathfrak{p}_2 = \frac{\alpha-1}{\alpha^2+2\alpha+5}\mathfrak{p}_2 = \frac{\alpha^2+\alpha-7}{2}\mathfrak{p}_2, \\ \mathfrak{p}_3 &= (\alpha-2), \\ \mathfrak{p}_4 &= (2)\mathfrak{p}_2^{-1} = (2)\mathfrak{p}_2^{-2}\mathfrak{p}_2 = \frac{2}{\alpha^2+2\alpha+5}\mathfrak{p}_2 = \frac{\alpha^2-\alpha+3}{2}\mathfrak{p}_2, \\ \mathfrak{p}_2^2 &= (\alpha^2+2\alpha+5). \end{aligned}$$

In der Klassengruppe $C\ell(\mathbf{Z}_K)$ gilt also

$$\overline{\mathfrak{p}_{11}} = \overline{\mathfrak{p}_3} = 1, \quad \overline{\mathfrak{p}_{25}} = \overline{\mathfrak{p}_5} = \overline{\mathfrak{p}_4} = \overline{\mathfrak{p}_2} \quad \text{und} \quad \overline{\mathfrak{p}_2}^2 = 1.$$

Da wir mit den Primidealen der Norm $\leq$ Minkowski-Schranke gestartet sind, sehen wir, daß die Klassengruppe von $\mathfrak{p}_2$ erzeugt wird. Außerdem ist $\mathfrak{p}_2^2$ Hauptideal. Daher sind zwei Fälle möglich: $\mathfrak{p}_2$ ist Hauptideal und damit $h_K = 1$ oder $\mathfrak{p}_2$ ist kein Hauptideal und $h_K = 2$. (Dies wird später untersucht werden, wenn wir die Einheiten bestimmt haben.)

6. Anwendung der Smithschen Normalform

Wir betrachten wieder unsere Relationen

$$\prod_{j=1}^{r} \mathfrak{p}_j^{v_{ij}} = (\alpha_i) \quad \text{für} \quad i = 1, \dots, m,$$

wobei wir annehmen, dass $V = (v_{ij})$ Rang r hat.
Wir definieren einen Gruppenhomomorphismus

$$\psi : \mathbf{Z}^r \to C\ell(\mathbf{Z}_K), \quad (v_1, \dots, v_r) \mapsto \text{ Klasse von } \mathfrak{p}_1^{v_1} \dots \mathfrak{p}_r^{v_r}.$$

Mit den obigen Bezeichnungen gilt

$$\psi((v_{i1},\ldots,v_{ir}) = \text{Klasse von } (\alpha_i) = 1.$$

Damit liegt jede Zeile von V im Kern von ψ, also auch jede Linearkombination, d.h.

$$\mathbf{Z}^m V \subseteq Kern(\psi).$$

Da $\mathfrak{p}_1,\ldots,\mathfrak{p}_r$ die Klassengruppe erzeugen, ist $\psi : \mathbf{Z}^r \to C\ell(\mathbf{Z}_K)$ surjektiv, also haben wir eine Surjektion

$$\overline{\psi} : \mathbf{Z}^r/\mathbf{Z}^m V \to C\ell(\mathbf{Z}_K).$$

Wir setzen jetzt voraus, dass die $m \times r$-Matrix V Rang r hat, was insbesondere $m \geq r$ impliziert. Wir bestimmen die Smithsche Normalform von V, d.h. wir finden Matrizen $S \in GL_m(\mathbf{Z})$, $T \in GL_r(\mathbf{Z})$, sodass für $D = SVT$ gilt

$$D = \begin{pmatrix} d_1 & 0 & \ldots & 0 \\ 0 & d_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & d_r \\ 0 & 0 & \ldots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \ldots & 0 \end{pmatrix} \quad \text{mit} \quad d_i \in \mathbf{N} \quad \text{und} \quad d_1|d_2|d_3|\ldots|d_r.$$

Es gilt dann die Gruppenisomorphie

$$\mathbf{Z}^r/\mathbf{Z}^m V \simeq \mathbf{Z}/\mathbf{Z}d_1 \oplus \cdots \oplus \mathbf{Z}/\mathbf{Z}d_r, \quad \text{insbesondere} \quad \#\mathbf{Z}^r/\mathbf{Z}^m V = d_1 \ldots d_r.$$

Daher haben wir jetzt einen surjektiven Gruppenhomomorphismus

$$\mathbf{Z}/\mathbf{Z}d_1 \oplus \cdots \oplus \mathbf{Z}/\mathbf{Z}d_r \to C\ell(\mathbf{Z}_K).$$

Insbesondere folgt

$$h_K | d_1 \ldots d_r.$$

Haben wir genügend Relationen, so sollte gelten

$$C\ell(\mathbf{Z}_K) \simeq \mathbf{Z}/\mathbf{Z}d_1 \oplus \cdots \oplus \mathbf{Z}/\mathbf{Z}d_r \quad \text{und} \quad h_K = d_1 \ldots d_r,$$

was man an dieser Stelle aber i.a. nicht feststellen kann, es sei denn, es gilt $d_1 \ldots d_r = 1$ und damit $h_K = 1$. Wir setzen

$$\widetilde{h_K} = d_1 \ldots d_r$$

und betrachten $\widetilde{h_K}$ als vorläufige Klassenzahl. Gilt $h_K \neq \widetilde{h_K}$, wird sich dies später herausstellen. Dann muss man noch nach weiteren Relationen suchen.

Für unser Beispiel liefert die Smithsche Normalform nichts Neues, da wir bereits wissen, dass $h_K = 1$ oder $h_K = 2$ gilt. Wir setzen $\widetilde{h_K} = 2$.

7. Bestimmung von $\mathbf{Z}_K^*$

Wir nehmen an, dass wir bei der Umformung der Relationenmatrix genügend Einheiten gefunden haben um daraus eine 'Basis' $\varepsilon_1,\ldots,\varepsilon_{r_1+r_2-1}$ unabhängiger Einheiten zu erhalten. Hat man zu wenig Einheiten, sollte man nach weiteren Relationen suchen.

Sind die konstruierten Einheiten $\varepsilon_1,\ldots,\varepsilon_{r_1+r_2-1}$ nicht zu groß, kann man mit den Verfahren des letzten Kapitels versuchen, daraus tatsächlich ein System von Grundeinheiten zu konstruieren.
Im andern Fall berechnen wir aus den Einheiten $\varepsilon_1,\ldots,\varepsilon_{r_1+r_2-1}$ einen vorläufigen Regulator

$$\widetilde{\mathrm{Reg}\,(K)} = \mathrm{Reg}\,(\varepsilon_1,\ldots,\varepsilon_{r_1+r_2-1}).$$

Bilden $\varepsilon_1,\ldots,\varepsilon_{r_1+r_2-1}$ kein System von Grundeinheiten, wird sich dies später herausstellen. Dann bestimmt man noch die Menge der Einheitswurzeln $\mu(K)$.

In unserem Beispiel ist $\mu(K) = \{\pm 1\}$, da K eine reelle Einbettung besitzt. Wegen $r_1 + r_2 - 1 = 1$ ist das Gitter $\ell(\mathbf{Z}_K^*)$ eindimensional. Nun haben wir bei der Umformung der Relationenmatrix bereits eine Einheit erhalten, nämlich

$$\varepsilon = 18\alpha^2 + 40\alpha + 89.$$

Wäre ε keine Grundeinheit, gäbe es eine Einheit ε_0 mit

$$\ell(\varepsilon_0) = \lambda\ell(\varepsilon) \text{ mit } 0 < \lambda \leq \frac{1}{2}.$$

Damit erhält man die Abschätzung

$$1 \leq |\sigma_1\varepsilon_0| \leq 16.340, \quad |\sigma_2\varepsilon_0| \leq 1,$$

was mit dem Ansatz $\varepsilon_0 = x_1\alpha^2 + x_2\alpha + x_3$ auf die Ungleichungen

$$|x_1| \leq 1.25, \quad |x_2| \leq 2.76, \quad |x_3| \leq 6.13$$

führt. Als einzige Einheiten ergeben sich ± 1. Also folgt $\mathbf{Z}_K^* = \{\pm\varepsilon^m : m \in \mathbf{Z}\}$ und $\mathrm{Reg}\,(K) \approx 5.59$. (Anmerkung: $-1/\varepsilon = 2\alpha^2 - 4\alpha - 1$.)

8. Die ζ-Funktion

Für einen Zahlkörper K definiert man

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{(\mathrm{N}\mathfrak{a})^s},$$

wobei $\mathfrak{a}$ alle Ideale $\neq 0$ von $\mathbf{Z}_K$ durchläuft. Die eindeutige Primidealzerlegung liefert

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1 - \frac{1}{\mathrm{N}(\mathfrak{p})^s}},$$

wobei $\mathfrak{p}$ alle Primideale $\neq 0$ durchläuft. Die Darstellungen konvergieren für $\mathrm{Re}\,(s) > 1$ und liefern, dass $\zeta_K(s)$ dort eine analytische Funktion ist. $\zeta_K(s)$ besitzt eine meromorphe Fortsetzung auf ganz $\mathbf{C}$ mit genau einem Pol in $s = 1$. Nun gilt die Formel

$$h_K \mathrm{Reg}\,(K) = \frac{\#\mu(K)\sqrt{\mathrm{disc}\,\mathbf{Z}_K}}{2^{r_1}(2\pi)^{r_2}} \prod_p \frac{1 - \frac{1}{p}}{\prod_{\mathfrak{p}|p}(1 - \frac{1}{\mathrm{N}\mathfrak{p}})}.$$

Die verallgemeinerte Riemannsche Vermutung (GRH – Generalized Riemann Hypothesis) besagt, dass gilt

$$\zeta_K(s) = 0 \quad \Longrightarrow \quad \begin{cases} s \in \{-1, -2, -3, -4, \ldots\} (\text{triviale Nullstellen}) & \text{oder} \\ \mathrm{Re}\,(s) = \frac{1}{2} \end{cases}$$

Die Riemannsche Vermutung ist eine bisher unbewiesene Vermutung, die aber viele Auswirkungen besitzt, wie zum Beispiel folgenden Satz:

Satz (E. Bach). *Sei*

$$a_K = \frac{\#\mu(K)\sqrt{\mathrm{disc}\,\mathbf{Z}_K}}{2^{r_1}(2\pi)^{r_2}} \prod_{p \leq 12\ln^2|\mathrm{disc}\,\mathbf{Z}_K|} \frac{1 - \frac{1}{p}}{\prod_{\mathfrak{p}|p}(1 - \frac{1}{\mathrm{N}\mathfrak{p}})}.$$

Gilt GRH, so folgt

$$\frac{a_K}{\sqrt{2}} < h_K \mathrm{Reg}\,(K) < \sqrt{2} \cdot a_K.$$

Folgerung. *Gilt für die vorläufigen Werte* $\widetilde{h_K}$ *und* $\widetilde{\mathrm{Reg}\,(K)}$

$$\widetilde{h_K} \cdot \widetilde{\mathrm{Reg}\,(K)} < \sqrt{2} \cdot a_K,$$

so folgt (mit GRH)

$$h_K = \widetilde{h_K}, \quad \mathrm{Reg}\,(K) = \widetilde{\mathrm{Reg}\,(K)}.$$

(Mit den vorangegangenen Bezeichnungen ist dann $\varepsilon_1, \ldots, \varepsilon_{r_1+r_2-1}$ *ein System von Grundeinheiten und* $C\ell(\mathbf{Z}_K) \simeq \mathbf{Z}/\mathbf{Z}d_1 \oplus \cdots \oplus \mathbf{Z}/\mathbf{Z}d_r$*.) Andernfalls ist* $h_K \neq \widetilde{h_K}$ *oder* $\mathrm{Reg}\,(K) \neq \widetilde{\mathrm{Reg}\,(K)}$.

Beweis: Es gibt $c_1, c_2 \in \mathbf{N}$ mit

$$\widetilde{h_K} = c_1 h_K \quad \text{und} \quad \widetilde{\mathrm{Reg}\,(K)} = c_2 \mathrm{Reg}\,(K).$$

- *1. Fall:* $\widetilde{h_K} \cdot \widetilde{\mathrm{Reg}\,(K)} < \sqrt{2} \cdot a_K$*:* Dann folgt

$$c_1 c_2 = \frac{c_1 h_K \cdot c_2 \mathrm{Reg}\,(K)}{h_K \mathrm{Reg}\,(K)} = \frac{\widetilde{h_K} \cdot \widetilde{\mathrm{Reg}\,(K)}}{h_K \mathrm{Reg}\,(K)} < \frac{\sqrt{2} \cdot a_K}{h_K \mathrm{Reg}\,(K)} < \sqrt{2} \cdot \sqrt{2} = 2,$$

  also $c_1 = c_2 = 1$ und damit $h_K = \widetilde{h_K}$ und $\mathrm{Reg}\,(K) = \widetilde{\mathrm{Reg}\,(K)}$.
- *2. Fall:* $\widetilde{h_K} \cdot \widetilde{\mathrm{Reg}\,(K)} \geq \sqrt{2} \cdot a_K$*:* Dann ist

$$c_1 c_2 = \frac{c_1 h_K \cdot c_2 \mathrm{Reg}\,(K)}{h_K \mathrm{Reg}\,(K)} = \frac{\widetilde{h_K} \cdot \widetilde{\mathrm{Reg}\,(K)}}{h_K \cdot \mathrm{Reg}\,(K)} \geq \frac{\sqrt{2} \cdot a_K}{h_K \mathrm{Reg}\,(K)} > 1,$$

  also $c_1 c_2 \geq 2$ und damit $c_1 \geq 2$ oder $c_2 \geq 2$, d.h. $h_K \neq \widetilde{h_K}$ oder $\mathrm{Reg}\,(K) \neq \widetilde{\mathrm{Reg}\,(K)}$. ■

Mit Hilfe der Folgerung können wir also testen, ob die vorläufig ermittelten Werte für h_K und $\mathrm{Reg}\,(K)$ stimmen oder nicht.

In unserem Beispiel finden wir $a_K \approx 11.11$. Dies zeigt, dass tatsächlich $h_K = 2$, $\mathrm{Reg}\,(K) \approx 5.59$ gilt.

9. Weitere Beispiele

Beispiel: Wir betrachten den reellquadratischen Körper $K = \mathbf{Q}(\alpha)$ mit $\alpha^2 = 94$. Die Maximalordnung ist $\mathbf{Z}_K = \mathbf{Z}[\alpha]$ mit Diskriminante $4 \cdot 94$. Die Minkowski-Schranke ist ≤ 9.7. Es gibt 5 Primideale mit Norm ≤ 9: $\mathfrak{p}_2$, $\mathfrak{p}_{3a}$, $\mathfrak{p}_{3b}$, $\mathfrak{p}_{5a}$, $\mathfrak{p}_{5b}$. Wir testen als Relationen $\beta = 2, 3, 5$ und $\beta = u\alpha + v$ mit $\mathrm{ggT}(u, v) = 1$ und $|u|, |v| \leq 10$. Folgende Relationen funktionierten:

$$\alpha - 8, \alpha + 2, \alpha + 10, \alpha + 7, 2\alpha + 1, \alpha - 7, \alpha - 10, 2\alpha - 1, \alpha - 2, \alpha + 8, 1, 3, 5.$$

Dann sieht man, dass die Klassengruppe trivial ist, d.h. $h_K = 1$. An (nichttrivialen) Einheiten findet man bei dem Prozess

$$221064\alpha + 2143295, \quad 947610731760\alpha + 9187426914049.$$

Mit dem üblichen Verfahren findet man, dass

$$\varepsilon = 221064\alpha + 2143295$$

eine Grundeinheit ist.
(Das Beispiel zeigt, dass manchmal große Einheiten auftreten können, die man auf diese Weise einfach findet.)

Beispiel: Wir betrachten $K = \mathbf{Q}(\alpha)$ mit $2 + 3\alpha + 5\alpha^2 + 7\alpha^3 + \alpha^4 = 0$. Es ist $\mathbf{Z}_K = \mathbf{Z}[\alpha]$, die Minkowski-Schranke ist ≤ 33.95. Indem man alle möglichen Relationen der Form $\beta = u_3\alpha^3 + u_2\alpha^2 + u_1\alpha + u_0$ mit $|u_i| \leq 2$ benutzt, sieht man, dass $h_K = 1$ gilt. Außerdem erhält man eine Menge von Einheiten, mit deren Hilfe wir im letzten Kapitel bereits die Grundeinheiten von $\mathbf{Z}_K$ bestimmt haben.

Wir geben im Folgenden noch zwei Ansätze/Methoden an zur Bestimmung von $C\ell(\mathbf{Z}_K)$ und $\mathbf{Z}_K^*$.

1. Ansatz cl_einh_1: Gegeben sei ein Zahlkörper K mit Ganzheitsring $\mathbf{Z}_K$.

1. Wir stellen eine Liste P aller Primzahlen p auf, die $\leq$ der Minkowski-Schranke sind, d.h. für die $p \leq (\frac{4}{\pi})^{r_2} \frac{n!}{n^n}$ gilt.
2. Aus P werden alle trägen Primzahlen p gestrichen.
3. Für jede Primzahl $p \in P$ werden die zugehörigen Primideale $\mathfrak{p}_{p,1}, \ldots \mathfrak{p}_{p,r_p}$ bestimmt.

4. Man nehme die größte Primzahl p aus P und betrachte die zugehörigen Primideale $\mathfrak{p} = \mathfrak{p}_{p,i}$: Man bestimmt eine LLL-reduzierte Basis $\alpha_1, \ldots, \alpha_n$ von $\mathfrak{p}$. Dann gibt es eine Zerlegung

$$(\alpha_i) = \mathfrak{p} \cdot \mathfrak{q}_i.$$

   Tauchen in der Primfaktorzerlegung von $\mathrm{N}(\mathfrak{q}_i)$ nur Primzahlen $< p$ auf, so kann man mit der Relation $(\alpha_i) = \mathfrak{p} \cdot \mathfrak{q}_i$ das Primideal $\mathfrak{p}$ auf Primideale zu kleineren Primzahlen reduzieren. Kann man alle Primideale $\mathfrak{p}_{p,1}, \ldots, \mathfrak{p}_{p,r_p}$ auf kleinere Primzahlen reduzieren, so streicht man p aus der Liste P heraus.
5. Kann man auf diese Weise keine Primzahlen aus P mehr herausstreichen, versucht man mit den restlichen Primzahlen p bzw. den Primidealen $\mathfrak{p}_{p,1}, \ldots, \mathfrak{p}_{p,r_p}$ Relationen zu erzeugen. Dazu kann man wieder Elemente der LLL-reduzierten Basis von $\mathfrak{p}_{p,i}$ betrachten.

Beispiel: $K = \mathbf{Q}(\alpha)$ mit $\alpha^3 = 239$. Es ist $\mathbf{Z}_K = \mathbf{Z}[\alpha]$. Mit obigem Verfahren finden wir $h = 1$ und die nichttriviale Einheit

$$\begin{aligned}\varepsilon \;=\;& +42908157621410076449869458360704964555267526377321313050854537836118 7\backslash \\ & 02153610021264542653366\alpha^2 \\ & +39944966879732668842071850097008942723043276879881105023068066632242 0\backslash \\ & 40061692318413592157050 4\alpha \\ & -41314020447657499502473910302959395872043280836624623527619700273315 1\backslash \\ & 64437745191240787288412 41\end{aligned}$$

mit Regulator 431.94. (Dies passt zu den Abschätzungen mit der Riemannschen Vermutung.)

2. Ansatz cl_einh_2: Man wählt ≈ 20 der ersten Primideale und versucht wieder mit LLL-Reduktion der Primideale Relationen zu finden.

Beispiel: $K = \mathbf{Q}(\alpha)$ mit $\alpha^3 = 101$ und $\mathbf{Z}_K = \mathbf{Z}[\alpha]$. Wir finden $h|2$ und die nichttriviale Einheit

$$\varepsilon = 174631364070883307 40\alpha^2 + 8132599228388566970 8\alpha + 3787359192976369370 09$$

mit Regulator 48.48. (Dies passt zu den GRH-Abschätzungen.)

10. Große Primideale

Wir wollen an einem Beispiel zeigen, wie man mit großen Primidealen umgehen kann.

In unserem Beispiel ist das einzige Primideal mit Norm $q = 10^{100} + 949$ das Ideal $\mathfrak{q} = (q, \alpha + q_1)$ mit

$$\begin{aligned}q_1 \;=\;& 94274438529313260882796096106334705224143313447985378597473255685967806136754 11\backslash \\ & 49830944002320574312 9.\end{aligned}$$

Die Hermitesche Normalform ist $\mathfrak{q} = \mathbf{Z}\rho_1 + \mathbf{Z}\rho_2 + \mathbf{Z}\rho_3$ mit

$$\begin{aligned}\rho_1 \;=\;& \alpha^2 + 17414496041640976086330586749190008614027147020871603110313856301752039\backslash \\ & 45230677784682419237526700764, \\ \rho_2 \;=\;& \alpha + 94274438529313260882796096106334705224143313447985378597473255685967806136\backslash \\ & 75411498309440023205743129, \\ \rho_3 \;=\;& 10000000000000000000000000000000000000000000000000000000000000000000000000000000000000000\backslash \\ & 00000000000000000949\end{aligned}$$

Eine LLL-reduzierte Basis von $\mathfrak{q}$ erhält man nach 161 Vertauschungen benachbarter Basisvektoren:

$$\begin{aligned}
\lambda_1 &= 526956551500397735061240625700619\alpha^2 + 350906203038749368292789852206425\alpha \\
&\quad -3026596488322725006880071507459 56 \\
\lambda_2 &= 176050348461648366768450773494194\alpha^2 + 653565851871021868980797002952381\alpha \\
&\quad -6099181715336647586361654033452765 \\
\lambda_3 &= 590261201685709802021018814326500\alpha^2 - 28741377561489491090344320906231 70\alpha \\
&\quad +8169470921229297668824756788450 89
\end{aligned}$$

Dann ist $N(\lambda_i) = 2q, -20q, -10q$. Es folgt $(\lambda_1) = \mathfrak{p}_2\mathfrak{q}$, was $\lambda_1\mathfrak{p}_2 = (\alpha^2 + 2\alpha + 5)\mathfrak{q}$ und damit

$$\begin{aligned}
\mathfrak{q} &= \frac{\lambda_1}{\alpha^2 + 2\alpha + 5}\mathfrak{p}_2 = \\
&= (111721775318610753708225944002711 9\alpha^2 - 252323155311019974074164223841674 5\alpha \\
&\quad +514287443290657266194468528099133)/2 \cdot \mathfrak{p}_2
\end{aligned}$$

liefert. Insbesondere ist $\mathfrak{q}$ auch kein Hauptideal.

11. Das Hauptidealproblem

Der folgende Satz zeigt, dass man im Prinzip entscheiden kann, ob ein Ideal $\mathfrak{a}$ einer Ordnung R ein Hauptideal ist, wenn man die Einheitengruppe R^* kennt.

SATZ. *Sei $\varepsilon_1, \ldots, \varepsilon_r$ ein System von Grundeinheiten der Ordnung R (mit $r = r_1 + r_2 - 1$). Ist das gebrochene Ideal $\mathfrak{a}$ ein Hauptideal, so gibt es ein $\alpha \in \mathfrak{a}$ mit $\mathfrak{a} = (\alpha)$ und*

$$|\sigma_j\alpha| \le (N\mathfrak{a})^{1/(r_1+r_2)} \cdot \prod_i \max(|\sigma_j\varepsilon_i|^{1/2}, |\sigma_j\varepsilon_i|^{-1/2}).$$

Konkret: Ist $\alpha_1, \ldots, \alpha_n$ eine $\mathbf{Z}$-Basis von $\mathfrak{a}$ und $\beta_1, \ldots, \beta_n$ die Dualbasis, so hat man für $\alpha = x_1\alpha_1 + \cdots + x_n\alpha_n$ die Abschätzung

$$|x_i| \le \sum_{j=1}^{n} |\sigma_j\alpha||\sigma_j\beta_i|.$$

Beweis: Wir denken uns die logarithmische Abbildung zu $\ell : K^* \to \mathbf{R}^{r_1+r_2}$ fortgesetzt, d.h. für $\alpha \in K^*$ ist

$$\ell(\alpha) = (\ln|\sigma_1\alpha|, \ldots, \ln|\sigma_{r_1}\alpha|, 2\ln|\sigma_{r_1+1}\alpha|, \ldots, 2\ln|\sigma_{r_1+r_2}\alpha|).$$

Die Vektoren $(1, \ldots, 1), \ell(\varepsilon_1), \ldots, \ell(\varepsilon_r)$ bilden eine $\mathbf{R}$-Basis von $\mathbf{R}^{r_1+r_2}$. Zu $\alpha \in K^*$ gibt es dann (eindeutig bestimmte) reelle Zahlen $\lambda_0, \lambda_1, \ldots, \lambda_r$ mit

$$\ell(\alpha) = \lambda_0(1, \ldots, 1) + \sum_i \lambda_i\ell(\varepsilon_i).$$

Da sich die Einträge in $\ell(\varepsilon_i)$ zu 0 aufaddieren, sieht man außerdem

$$\ln|N\alpha| = \lambda_0(r_1 + r_2).$$

Wir zerlegen für $i \ge 1$ die Zahl $\lambda_i = m_i + \mu_i$ mit $m_i \in \mathbf{Z}$ und $|\mu_i| \le \frac{1}{2}$. Für $\alpha_0 = \alpha\varepsilon_1^{-m_1} \ldots \varepsilon_r^{-m_r}$ gilt

$$\ell(\alpha_0) = \frac{\ln|N\alpha|}{r_1 + r_2}(1, \ldots, 1) + \sum_i \mu_i\ell(\varepsilon_i).$$

Es folgt

$$|\sigma_j\alpha_0| \le |N\alpha|^{1/(r_1+r_2)} \prod_i \max(|\sigma_j\varepsilon_i|^{1/2}, |\sigma_j\varepsilon_i|^{-1/2}).$$

Ist $\mathfrak{a} = (\alpha)$ ein Hauptideal, so gilt auch $\mathfrak{a} = (\alpha_0)$ und $|N\alpha_0| = N\mathfrak{a}$. Für α_0 hat man dann die Abschätzung des Satzes. Die Abschätzung der x_i's ergibt sich wie üblich. ■

In der Praxis wird man allerdings eher so vorgehen: Ist $\mathfrak{a}$ Ideal von $\mathbf{Z}_K$, so bestimmt man eine LLL-reduzierte Basis $\alpha_1, \ldots, \alpha_n$ von $\mathfrak{a}$. Dann hat man Faktorisierungen $\alpha_i = \mathfrak{a}\mathfrak{b}_i$ mit Idealen $\mathfrak{b}_i$. Genau dann ist $\mathfrak{a}$ Hauptideal, wenn $\mathfrak{b}_i$ Hauptideal ist. Die Norm von $\mathfrak{b}_1$ wird durch

$$\mathrm{N}\mathfrak{b}_1 \leq \frac{2^{n(n-1)/4}}{n^{n/2}} \sqrt{|\mathrm{disc}\, \mathbf{Z}_K|}$$

beschränkt. Auf diese Weise kann man das Problem auf Ideale beschränkter Norm reduzieren.

KAPITEL 10

Die diophantische Gleichung $x^3 + 3y^3 + dz^3 = 0$

1. Einführung

Eine diophantische Gleichung kann man in der Form $f(z_1, \ldots, z_n) = 0$ schreiben, wobei $f(x_1, \ldots, x_n) \in \mathbf{Z}[x_1, \ldots, x_n]$ ein Polynom mit ganzzahligen Koeffizienten ist und wobei nach Lösungen $(z_1, \ldots, z_n) \in \mathbf{Z}^n$ gesucht wird.

Diophantische Gleichungen haben eine lange Tradition. Die Suche nach Lösungen wurde oft als Herausforderung angesehen. Mitunter sieht man leicht Lösungen, manchmal kann man einfach zeigen, dass es keine Lösungen gibt, mitunter ist überhaupt nicht klar, wie man die Gleichung angehen sollte.

Beispiele:

1. Fermat stellt in Briefen mehrfach die Aufgabe, Lösungen von Gleichungen $x^2 - dy^2 = 1$ zu bestimmen.
2. Die 'kleinste' Lösung der Gleichung $x^2 - 61y^2 = 1$ in natürlichen Zahlen ist
$$1766319049^2 - 61 \cdot 226153980^2 = 1.$$
3. Die auf Fermat (1637) zurückgehende Fermatsche Gleichung
$$x^n + y^n = z^n \quad \text{mit} \quad n \geq 3 \quad \text{und} \quad x, y, z \in \mathbf{N}$$
wurde erst $\approx$ 1994 für alle $n \geq 3$ gelöst (Taylor, Wiles).
4. Euler vermutete 1769, dass die Gleichung
$$x^4 + y^4 + z^4 = t^4$$
keine Lösung in natürlichen Zahlen besitzt. Elkies fand 1988 Lösungen, z.B.
$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4.$$

Wir wollen uns hier für $d \in \mathbf{Z}$ mit der diophantischen Gleichung
$$x^3 + 3y^3 + dz^3 = 0$$
beschäftigen. Wir bemerken zunächst ein paar

Elementare Eigenschaften:

1. Natürlich gibt es immer die triviale Lösung $(x, y, z) = (0, 0, 0)$.
2. Ist (x, y, z) eine Lösung und ist $t \in \mathbf{Z}$, so ist auch (tx, ty, tz) eine Lösung.
3. Ist (x, y, z) eine nichttriviale Lösung, so auch $(\frac{x}{\mathrm{ggT}(x,y,z)}, \frac{y}{\mathrm{ggT}(x,y,z)}, \frac{z}{\mathrm{ggT}(x,y,z)})$, also muss man nur nach Lösungen mit $\mathrm{ggT}(x, y, z) = 1$ suchen.
4. Für $d = 0$ ist die Gleichung nur durch $x = y = 0$ lösbar. Ist $d < 0$ und $x^3 + 3y^3 + dz^3 = 0$, so gilt $x^3 + 3y^3 + |d|(-z)^3 = 0$, also kann man sich auf $d \geq 1$ beschränken.
5. Sei $d \geq 1$ und $d = d_1 c^3$ so zerlegt, dass d_1 der kubikfreie Anteil von d ist.
   - Ist $x_0^3 + 3y_0^3 + dz_0^3 = 0$ mit $(x_0, y_0, z_0) \neq (0, 0, 0)$, so ist $x_0^3 + 3y_0^3 + d_1(cz_0)^3 = 0$, d.h. (x_0, y_0, cz_0) ist eine nichttriviale Lösung der Gleichung $x^3 + 3y^3 + d_1 z^3 = 0$.
   - Ist $x_1^3 + 3y_1^3 + d_1 z_1^3 = 0$ mit $(x_1, y_1, z_1) \neq (0, 0, 0)$, so folgt $(cx_1)^3 + 3(cy_1)^3 + dz_1^3 = 0$, also ist (cx_1, cy_1, z_1) eine nichttriviale Lösung der Gleichung $x^3 + 3y^3 + dz^3 = 0$.

   Die Gleichung $x^3 + 3y^3 + dz^3 = 0$ ist also genau dann nichttrivial lösbar, wenn es $x^3 + 3y^3 + d_1 z^3 = 0$ ist. Wir können uns daher auf kubikfreie d's beschränken.

Version vom 8.2.2003

6. Ist $d \geq 1$ kubikfrei und $x^3 + 3y^3 + dz^3 = 0$, so überlegt man sich leicht, dass die Äquivalenzen
$$\mathrm{ggT}(x,y,z) = 1 \iff \mathrm{ggT}(x,y) = 1 \iff \mathrm{ggT}(x,z) = 1 \iff \mathrm{ggT}(y,z) = 1$$
gelten.

Wir formulieren nun zwei Aufgaben:

Aufgaben: Sei $d \geq 1$ kubikfrei.

1. Hat die Gleichung $x^3 + 3y^3 + dz^3 = 0$ eine nichttriviale Lösung?
2. Bestimme/beschreibe alle Lösungen der Gleichung $x^3 + 3y^3 + dz^3 = 0$.

Wir wollen uns hier auf folgende konkrete Aufgabe beschränken:

Herausforderung: Untersuche für alle $d \in \{1, 2, 3, \ldots, 100\}$, ob die Gleichung $x^3 + 3y^3 + dz^3 = 0$ eine nichttriviale Lösung besitzt.

Nach den Vorüberlegungen können wir sofort die nichtkubikfreien d's ausschließen, also für $1 \leq d \leq 100$ die Zahlen, die durch 8 oder 27 teilbar sind. Dies sind genau 15 Zahlen, nämlich
$$d \in \{8, 16, 24, 27, 32, 40, 48, 54, 56, 64, 72, 80, 81, 88, 96\}.$$
Es bleiben 85 Zahlen übrig.

2. Experimentelle Suche nach Lösungen

1. Methode: Für ein vorgegebenes H betrachten wir alle $x, y \in \mathbf{Z}$ mit $|x|, |y| \leq H$, $\mathrm{ggT}(x,y) = 1$ und zerlegen dann $x^3 + 3y^3$ als $x^3 + 3y^3 = -dz^3$ mit kubikfreiem $d \geq 1$ und $z \in \mathbf{Z}$. Für dieses d hat unsere Gleichung dann die nichttriviale Lösung (x, y, z). Da mit (x, y, z) auch $(-x, -y, -z)$ eine Lösung der Gleichung ist, können wir eine Lösung normieren durch die Bedingung $\mathrm{ggT}(x, y, z) = 1$ und $x \geq 1$ oder $x = 0, y \geq 1$. Wir erhalten so alle d's, die eine nichttriviale Lösung mit $|x|, |y| \leq H$ besitzen.

Da wir uns hier nur die d's mit $1 \leq d \leq 100$ interessieren, können wir auch wie folgt vorgehen:

2. Methode: Für ein vorgegebenens H betrachten wir alle $x, y \in \mathbf{Z}$ mit $|x|, |y| \leq H$ und $\mathrm{ggT}(x,y) = 1$ und berechnen $Z = -x^3 - 3y^3$. Für die uns interessierenden d's testen wir, ob $d|Z$ gilt. Wenn ja, testen wir, ob $\frac{Z}{d}$ eine dritte Potenz ist, d.h. ob es ein $z \in \mathbf{Z}$ gibt mit $Z = dz^3$. Wenn ja, haben wir für dieses d eine nichttriviale Lösung. (Bei dieser Methode muss man im Unterschied zur 1. Methode nicht den kubikfreien Teil von Z bestimmen, sondern nur testen, ob $\frac{Z}{d}$ eine dritte Potenz ist. Dies ist wesentlich einfacher.)

Die folgende Tabelle enthält für die kubikfreien d's mit $1 \leq d \leq 100$ alle (normierten) Lösungen, die wir bei Wahl von $H = 4000$ gefunden haben.

Für 26 Zahlen $1 \leq d \leq 100$ haben wir also eine nichttriviale Lösung der Gleichung $x^3 + 3y^3 + dz^3 = 0$ gefunden:
$$d \in \{1, 2, 3, 4, 5, 10, 11, 17, 23, 25, 29, 30, 41, 44, 47, 51, 53, 59, 61, 67, 71, 73, 82, 83, 89, 94\}.$$

Für die 59 (kubikfreien) Zahlen
$$\begin{aligned} d \in \{&6, 7, 9, 12, 13, 14, 15, 18, 19, 20, 21, 22, 26, 28, 31, 33, 34, 35, 36, 37, \\ &38, 39, 42, 43, 45, 46, 49, 50, 52, 55, 57, 58, 60, 62, 63, 65, 66, 68, 69, 70, \\ &74, 75, 76, 77, 78, 79, 84, 85, 86, 87, 90, 91, 92, 93, 95, 97, 98, 99, 100\} \end{aligned}$$
haben wir keine Lösung gefunden. Für diese d's sollte wir entweder eine Lösung suchen oder beweisen, dass die Gleichung $x^3 + 3y^3 + dz^3 = 0$ nur die triviale Lösung $(0, 0, 0)$ besitzt.

Kubikfreie d's mit $1 \leq d \leq 100$, für die $x^3 + 3y^3 + dz^3 = 0$ eine nichttriviale Lösung besitzt.

d	Lösungen (x, y, z) der Gleichung $x^3 + 3y^3 + dz^3 = 0$
1	(1,0,-1)
2	(1,-1,1), (5,1,-4), (655,-253,-488)
3	(0,1,-1), (3,-2,-1), (3,-1,-2), (21,-20,17), (21,17,-20), (1314,-919,271), (1314,271,-919)
4	(1,1,-1), (7,-5,2), (2849,-1555,-1436)
5	(2,-1,-1), (4,13,-11)
10	(1,-3,2), (11,-3,-5), (13,-9,-1), (161,237,-164)
11	(2,1,-1), (28,-19,-5)
17	(4,-3,1), (392,-141,-145)
23	(1,-2,1), (47,44,-25)
25	(1,2,-1), (49,-52,23)
29	(10,-7,1)
30	(3,1,-1), (33,-19,-8)
41	(16,7,-5)
44	(5,-3,-1), (191,-141,32), (185,-507,206), (557,-387,29)
47	(1,5,-2), (751,-1885,748)
51	(3,2,-1), (9,-11,4), (6,-13,5), (75,-52,-1)
53	(7,3,-2), (3535,-2301,-524)
59	(17,-16,5)
61	(4,-1,-1), (23,-29,10), (55,-82,29), (232,125,-67), (1723,-1198,89)
67	(4,1,-1), (5,-4,1), (13,-23,8), (280,-131,-61), (925,-647,68), (1295,-232,-317), (2909,-199,-716)
71	(250,-231,67)
73	(2,-3,1), (19,-9,-4), (308,195,-89), (347,-24,-83), (409,-282,-25)
82	(1,3,-1), (163,-249,80)
83	(1867,-49,-428)
89	(2,3,-1), (340,-291,73)
94	(67,-41,-10), (73,-11,-16), (103,139,-46)

3. Kongruenzbetrachtungen

Gilt $x^3 + 3y^3 + dz^3 = 0$ mit $\mathrm{ggT}(x, y, z) = 1$, so folgt für alle $M \in \mathbf{N}$

$$x^3 + 3y^3 + dz^3 \equiv 0 \bmod M \quad \text{und} \quad \mathrm{ggT}(x, y, z) = 1,$$

insbesondere für alle Primzahlpotenzen p^m

$$x^3 + 3y^3 + dz^3 \equiv 0 \bmod p^m \quad \text{und} \quad \mathrm{ggT}(x, y, z) = 1.$$

Dies kehrt man wie folgt um: Findet man zu d eine Primzahlpotenz p^m, so dass keine $x, y, z \in \mathbf{Z}$ mit

$$x^3 + 3y^3 + dz^3 \equiv 0 \bmod p^m \quad \text{und} \quad \mathrm{ggT}(x, y, z) = 1$$

existieren, so hat die Gleichung $x^3 + 3y^3 + dz^3 = 0$ auch keine nichttriviale Lösung in ganzen Zahlen. Auf diese Weise erhält man Kriterien für die Nichtlösbarkeit der Gleichung $x^3 + 3y^3 + dz^3 = 0$ in ganzen Zahlen.

LEMMA. *Ist* $d \equiv 6, 9, 12, 15, 18, 21 \bmod 27$, *so gibt es keine* $x, y, z \in \mathbf{Z}$ *mit*

$$x^3 + 3y^3 + dz^3 \equiv 0 \bmod 27 \quad \textit{und} \quad \mathrm{ggT}(x, y, z) = 1.$$

Beweis: Seien $x, y, z, d \in \mathbf{Z}$ mit $\mathrm{ggT}(x, y, z) = 1$ und $x^3 + 3y^3 + dz^3 \equiv 0 \bmod 27$.

1. Wir wollen zuerst zeigen, dass $z \not\equiv 0 \bmod 3$ gilt. Wir nehmen an, es wäre $z \equiv 0 \bmod 3$. Dann würde modulo 3 sofort $x \equiv 0 \bmod 3$, dann $3y^3 \equiv 0 \bmod 27$ folgen, also $3 | \mathrm{ggT}(x, y, z)$, ein Widerspruch. Somit gilt $z \not\equiv 0 \bmod 3$.

2. Wegen $\mathrm{ggT}(3, z) = 1$ gibt es $t \in \mathbf{Z}$ mit $tz \equiv 1 \bmod 27$, was sofort $(tx)^3 + 3(ty)^3 + d \equiv 0 \bmod 27$ impliziert. Wählt man $u, v \in \mathbf{Z}$ mit $u \equiv -tx \bmod 27$, $v \equiv -ty \bmod 27$, so hat man
$$d \equiv u^3 + 3v^3 \bmod 27.$$
3. Lassen wir jetzt $0 \leq u, v \leq 26$ laufen, so erhalten wir folgende 21 d's mit $d \equiv u^3 + 3v^3 \bmod 27$:
$$d \in \{0, 1, 2, 3, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 24, 25, 26\}.$$
4. Ist also $d \equiv 6, 9, 12, 15, 18, 21 \bmod 27$, so gibt es keine $u, v \in \mathbf{Z}$ mit $d \equiv u^3 + 3v^3 \bmod 27$ und damit auch keine $x, y, z \in \mathbf{Z}$ mit $x^3 + 3y^3 + dz^3 \equiv 0 \bmod 27$ und $\mathrm{ggT}(x, y, z) = 1$. ■

Damit erhalten wir sofort:

Kriterium: Ist $d \equiv 6, 9, 12, 15, 18, 21 \bmod 27$, so gibt es keine $x, y, z \in \mathbf{Z}$ mit $\mathrm{ggT}(x, y, z) = 1$ und $x^3 + 3y^3 + dz^3 = 0$.

Anwendung: Für folgende 20 d's hat die Gleichung $x^3 + 3y^3 + dz^3 = 0$ keine nichttriviale Lösung, da sie keine nichttriviale Lösung modulo 27 hat:
$$d \in \{6, 9, 12, 15, 18, 21, 33, 36, 39, 42, 45, 60, 63, 66, 69, 75, 87, 90, 93, 99\}.$$

LEMMA. *Ist p ein Primteiler von d (kubikfrei) und hat die Gleichung $t^3 \equiv 3 \bmod p$ keine Lösung, so gibt es keine $x, y, z \in \mathbf{Z}$ mit*
$$x^3 + 3y^3 + dz^3 \equiv 0 \bmod p^3 \quad \textit{und} \quad \mathrm{ggT}(x, y, z) = 1.$$

Beweis: Seien $x, y, z \in \mathbf{Z}$ mit $\mathrm{ggT}(x, y, z) = 1$ und $x^3 + 3y^3 + dz^3 \equiv 0 \bmod p^3$. Wegen $d \equiv 0 \bmod p$ folgt $x^3 + 3y^3 \equiv 0 \bmod p$. Wäre $y \equiv 0 \bmod p$, so würde $x \equiv 0 \bmod p$ und damit $dz^3 \equiv 0 \bmod p^3$ folgen. Da $d \not\equiv 0 \bmod p^3$ gilt, würde der Widerspruch $z \equiv 0 \bmod p$, also $p | \mathrm{ggT}(x, y, z)$ folgen. Wählt man $u \in \mathbf{Z}$ mit $uy \equiv 1 \bmod p$, so folgt $(ux)^3 + 3 \equiv 0 \bmod p$, also $(-ux)^3 \equiv 3 \bmod p$, ein Widerspruch zu unserer Voraussetzung, dass die Gleichung $t^3 \equiv 3 \bmod p$ keine Lösung haben soll. ■

LEMMA. *Sei p eine Primzahl.*

1. *Ist $p \equiv 2 \bmod 3$, so hat die Gleichung $t^3 \equiv 3 \bmod p$ genau eine Lösung modulo p.*
2. *Hat die Kongruenz $t^3 \equiv 3 \bmod p$ keine Lösung, so ist $p \equiv 1 \bmod 6$.*
3. *Für folgende Primzahlen $p \leq 100$ hat die Gleichung $t^3 \equiv 3 \bmod p$ keine Lösung:*
$$p \in \{7, 13, 19, 31, 37, 43, 79, 97\}.$$

Beweis:

1. Wir betrachten den Gruppenhomomorphismus
$$\psi : \mathbf{F}_p^* \to \mathbf{F}_p^*, \quad t \mapsto t^3.$$
Ist s aus dem Kern von ψ, d.h. $\psi(s) = 1$, so gilt $s^3 = 1$. Da s von der Gruppenordnung $\#\mathbf{F}_p^* = p - 1$ annulliert wird, gilt auch $s^{p-1} = 1$. Wegen $p \equiv 2 \bmod 3$, also $p = 2 + 3k$ gilt
$$1 = s^{p-1} = s^{1+3k} = s \cdot (s^3)^k = s.$$
Also ist ψ injektiv, da $\mathbf{F}_p^*$ endlich ist, auch surjektiv, d.h. es gibt $t \in \mathbf{F}_p^*$ mit $t^3 = 3$.
2. In den Fällen $p = 2$ und $p = 3$ hat die Kongruenz $t^3 \equiv 3 \bmod p$ eine Lösung. Hat die Gleichung $t^3 \equiv 3 \bmod p$ keine Lösung, so ist also einerseits $p \equiv 1 \bmod 2$, andererseits erhält man aus 1. die Aussage $p \not\equiv 2 \bmod 3$, was mit $p \neq 3$ sofort $p \equiv 1 \bmod 3$ und schließlich $p \equiv 1 \bmod 6$ ergibt.
3. Die Primzahlen erhält man, indem man die Lösbarkeit der Gleichung explizit testet. ■

Bemerkung: Hat $t^3 \equiv 3 \bmod p$ keine Lösung, so gilt also $p \equiv 1 \bmod 6$. Die Umkehrung gilt allerdings nicht, wie man an den Beispielen (mit $p \leq 100$)

$$\begin{aligned} p = 61 &: 4^3 \equiv 5^3 \equiv 52^3 \equiv 3 \bmod 61, \\ p = 67 &: 18^3 \equiv 53^3 \equiv 63^3 \equiv 3 \bmod 67, \\ p = 73 &: 25^3 \equiv 54^3 \equiv 67^3 \equiv 3 \bmod 67 \end{aligned}$$

sieht.

Kriterium: Ist p ein Primteiler von d (kubikfrei) mit $p \equiv 1 \bmod 6$, sodass die die Kongruenz $t^3 \equiv 3 \bmod p$ keine Lösung hat, so gibt es keine $x, y, z \in \mathbf{Z}$ mit $\mathrm{ggT}(x, y, z) = 1$ und $x^3 + 3y^3 + dz^3 = 0$.

Anwendung: Für folgende kubikfreien d's mit $d \leq 100$ hat die Gleichung $x^3 + 3y^3 + dz^3 \equiv 0 \bmod p^3$ keine nichttriviale Lösung:

p	$d \equiv 0 \bmod p$
7	7, 14, 21, 28, 35, 42, 49, 63, 70, 77, 84, 91, 98
13	13, 26, 39, 52, 65, 78, 91
19	19, 38, 57, 76, 95
31	31, 62, 93
37	37, 74
43	43, 86
79	79
97	97

Wir stellen nun nochmals zusammen, für welche d's wir durch eine Kongruenzbetrachtung modulo p^3 gezeigt haben, dass $x^3 + 3y^3 + dz^3 = 0$ keine nichttriviale Lösung besitzt.

d	Kongruenz modulo p^3
6	K3
7	K7
9	K3
12	K3
13	K13
14	K7
15	K3
18	K3
19	K19
21	K3, K7
26	K13
28	K7
31	K31
33	K3
35	K7
36	K3
37	K37
38	K19
39	K3, K13
42	K3, K7
43	K43
45	K3
49	K7
52	K13

d	Kongruenz modulo p^3
57	K19
60	K3
62	K31
63	K3, K7
65	K13
66	K3
69	K3
70	K7
74	K37
75	K3
76	K19
77	K7
78	K13
79	K79
84	K7
86	K43
87	K3
90	K3
91	K7, K13
93	K3, K31
95	K19
97	K97
98	K7
99	K3

Durch Kongruenzbetrachtungen haben wir also gezeigt, dass für folgende 48 Werte für d die Gleichung $x^3 + 3y^3 + dz^3 = 0$ keine nichttriviale Lösung besitzt:

$$\begin{aligned} d \quad \in \quad & \{6, 7, 9, 12, 13, 14, 15, 18, 19, 21, 26, 28, 31, 33, 35, 36, 37, 38, 39, 42, 43, 45, 49, 52, \\ & 57, 60, 62, 63, 65, 66, 69, 70, 74, 75, 76, 77, 78, 79, 84, 86, 87, 90, 91, 93, 95, 97, 98, 99\}. \end{aligned}$$

Für folgende 11 Werte für d haben wir bis jetzt weder eine nichttriviale Lösung gefunden noch durch Kongruenzbetrachtung zeigen können, dass keine nichttriviale Lösung existiert:

$$d \in \{20, 22, 34, 46, 50, 55, 58, 68, 85, 92, 100\}.$$

Man kann nun fragen, ob man durch weitere Kongruenzbetrachtungen noch andere d's ausschließen kann. Dies ist aber nicht der Fall. Man kann zeigen:

LEMMA. *Sei $d \geq 2$ kubikfrei mit folgenden Eigenschaften:*

1. $d \not\equiv 6, 9, 12, 15, 18, 21 \bmod 27$.
2. *Für alle Primteiler $p \equiv 1 \bmod 6$ von d hat die Kongruenzgleichung $t^3 \equiv 3 \bmod p$ eine Lösung.*

Dann existieren für jedes $M \in \mathbf{N}$ Zahlen $x_M, y_m, z_M \in \mathbf{Z}$ mit

$$x_M^3 + 3y_M^3 + dz_M^3 \equiv 0 \bmod M \quad \text{und} \quad \mathrm{ggT}(x_M, y_M, z_M) = 1.$$

Ein Beweis wird später gegeben werden.

Für die 11 Werte

$$d \in \{20, 22, 34, 46, 50, 55, 58, 68, 85, 92, 100\}$$

muß man also nach neuen Behandlungswegen suchen.

4. Klassengruppenkriterien für $\mathbf{Q}(\sqrt[3]{d})$

Seien $x, y, z \in \mathbf{Z}$ mit $x^3 + dy^3 + 3z^3 = 0$ und $d \geq 2$ kubikfrei. Ist $K = \mathbf{Q}(\alpha)$ mit $\alpha^3 = d$, so gilt in $\mathbf{Z}_K$

$$(x + z\alpha)(x^2 - xz\alpha + z^2\alpha^2) = -3y^3 \quad \text{und} \quad \mathrm{N}(x + z\alpha) = x^3 + dz^3 = -3y^3.$$

Wir wollen die Gestalt der Primidealzerlegung von $x + z\alpha$ in $\mathbf{Z}_K$ untersuchen. Dazu stellen wir (ohne Beweis) einige Aussagen über sogenannte reine kubische Zahlkörper $\mathbf{Q}(\sqrt[3]{d})$ zusammen. (Beweise findet man zum Beispiel bei Cohen, A Course in Computational Algebraic Number Theory. Da wir aber die Aussagen nur für endliche viele explizit gegebene d's brauchen, kann man sie in diesen Fällen mit unseren Methoden auch direkt zeigen.)

SATZ. *Sei $d \geq 2$ kubikfrei, $d = ab^2$ mit a und b quadratfrei und $\mathrm{ggT}(a, b) = 1$. Dann ist*

$$\mathbf{Z}_K = \begin{cases} \mathbf{Z} \cdot \frac{\alpha^2}{b} + \mathbf{Z} \cdot \alpha + \mathbf{Z} & \text{für } a \not\equiv \pm b \bmod 9 \quad \text{und} \quad \mathrm{disc}\, \mathbf{Z}_K = -27a^2b^2 \quad \textit{(Typ 1)}, \\ \mathbf{Z} \cdot \frac{\alpha^2 + ab^2\alpha + b^2}{3b} + \mathbf{Z} \cdot \alpha + \mathbf{Z} & \text{für } a \equiv \pm b \bmod 9 \quad \text{und} \quad \mathrm{disc}\, \mathbf{Z}_K = -3a^2b^2 \quad \textit{(Typ 2)}. \end{cases}$$

SATZ. *Sei $d \geq 2$ kubikfrei, $d = ab^2$ mit a und b quadratfrei und $\mathrm{ggT}(a, b) = 1$.*

1. *Gilt $a \not\equiv \pm b \bmod 9$, so ist das einzige 3 enthaltende Primideal von $\mathbf{Z}_K$*

$$\mathfrak{p} = \begin{cases} \mathbf{Z} \cdot (\frac{\alpha^2}{b} - b) + \mathbf{Z} \cdot (\alpha - a) + \mathbf{Z} & \text{für } d \not\equiv 0 \bmod 3, \\ \mathbf{Z} \cdot \frac{\alpha^2}{b} + \mathbf{Z} \cdot \alpha + \mathbf{Z} & \text{für } d \equiv 0 \bmod 3. \end{cases}$$

   mit $\mathfrak{p}^3 = (3)$.

2. *Gilt $a \equiv \pm b \bmod 9$, so sind mit $\omega = \frac{\alpha^2 + ab^2\alpha + b^2}{3b}$ die einzigen 3 enthaltenden Primideale*

$$\begin{aligned} \mathfrak{p}_1 &= \mathbf{Z} \cdot (\omega - \frac{b(a^2 + 2)}{3}) + \mathbf{Z} \cdot (\alpha - a) + \mathbf{Z}, \\ \mathfrak{p}_2 &= \mathbf{Z} \cdot (\omega - \frac{b(a^2 - 1)}{3}) + \mathbf{Z} \cdot (\alpha - a) + \mathbf{Z} \end{aligned}$$

   und es gilt $\mathfrak{p}_1\mathfrak{p}_2^2 = (3)$.

Bemerkung: Man überlegt sich leicht, dass sich die Bedingung $a \equiv \pm b \bmod 9$ auch als $a^2 \equiv b^2 \bmod 9$ formulieren läßt. Für kubikfreies $d = ab^2 \geq 2$ und $K = \mathbf{Q}(\alpha)$ mit $\alpha^3 = d$ können wir dann nochmals die Einteilung der reinen kubischen Zahlkörper zusammenstellen:

- Typ 1: $a \not\equiv \pm b \bmod 9$, $a^2 \not\equiv b^2 \bmod 9$, $(3) = \mathfrak{p}^3$.
- Typ 2: $a \equiv \pm b \bmod 9$, $a^2 \equiv b^2 \bmod 9$, $(3) = \mathfrak{p}_1\mathfrak{p}_2^2$.

LEMMA. *Sei $d \geq 2$ kubikfrei, $K = \mathbf{Q}(\alpha)$ mit $\alpha^3 = d$ der zugehörige Zahlkörper,*

$$(3) = \mathfrak{p}^3 \quad \textit{(Typ 1)} \qquad \textit{bzw.} \qquad (3) = \mathfrak{p}_1\mathfrak{p}_2^2 \quad \textit{(Typ 2)}$$

die Faktorisierung von 3 in $\mathbf{Z}_K$. Seien $x, y, z \in \mathbf{Z}$ mit $x^3 + 3y^3 + dz^3 = 0$ und $\mathrm{ggT}(x, y, z) = 1$. Dann gibt es ein Ideal $\mathfrak{a}$ in $\mathbf{Z}_K$ mit

$$(x + z\alpha) = \mathfrak{p}^{v_\mathfrak{p}(x+z\alpha)}\mathfrak{a}^3 \qquad \textit{bzw.} \qquad (x + z\alpha) = \mathfrak{p}_1^{v_{\mathfrak{p}_1}(x+z\alpha)}\mathfrak{p}_2^{v_{\mathfrak{p}_2}(x+z\alpha)}\mathfrak{a}^3 \qquad \textit{mit} \qquad \mathrm{ggT}(3, \mathrm{N}\mathfrak{a}) = 1.$$

(Das Hauptideal $(x + z\alpha)$ ist also bis auf Anteile von 3 eine 3-te Potenz.)

Beweis: Wir haben die Zerlegung

$$(x + z\alpha)(x^2 - xz\alpha + z^2\alpha^2) = -3y^3.$$

Sei $\mathfrak{q}$ ein Primideal mit $\mathfrak{q}|x + z\alpha$, das aber 3 nicht teilt. Natürlich gilt dann auch $\mathfrak{q}|y$. Würde $\mathfrak{q}|x^2 - xz\alpha + z^2\alpha^2$ gelten, so würde mit $x \equiv -z\alpha \bmod \mathfrak{q}$ auch $0 \equiv x^2 - xz\alpha + z^2\alpha^2 \equiv 3z^2\alpha^2 \bmod \mathfrak{q}$, also $\mathfrak{q}|z\alpha$ und damit auch $\mathfrak{q}|x$ folgen, was zum Widerspruch $1 = \mathrm{ggT}(x, y) \in \mathfrak{q}$ führen würde. Damit ist $v_\mathfrak{q}(x^2 - xz\alpha + z^2\alpha^2) = 0$ und somit

$$v_\mathfrak{q}(x + z\alpha) = v_\mathfrak{q}(y^3) = 3v_\mathfrak{q}(y).$$

Definieren wir

$$\mathfrak{a} = \prod_{\mathfrak{q}|x+z\alpha, \mathfrak{q}\nmid 3} \mathfrak{q}^{v_\mathfrak{q}(y)},$$

so gilt

$$\prod_{\mathfrak{q}|x+z\alpha, \mathfrak{q}\nmid 3} \mathfrak{q}^{v_\mathfrak{q}(x+z\alpha)} = \prod_{\mathfrak{q}|x+z\alpha, \mathfrak{q}\nmid 3} \mathfrak{q}^{3v_\mathfrak{q}(y)} = \mathfrak{a}^3.$$

Dann ergibt

$$(x + z\alpha) = \mathfrak{p}^{v_\mathfrak{p}(x+z\alpha)} \prod_{\mathfrak{q}|x+z\alpha, \mathfrak{q}\nmid 3} \mathfrak{q}^{v_\mathfrak{q}(x+z\alpha)} = \mathfrak{p}^{v_\mathfrak{p}(x+z\alpha)}\mathfrak{a}^3 \quad \text{(Typ 1)} \quad \text{bzw.}$$

$$(x + z\alpha) = \mathfrak{p}_1^{v_{\mathfrak{p}_1}(x+z\alpha)}\mathfrak{p}_2^{v_{\mathfrak{p}_2}(x+z\alpha)} \prod_{\mathfrak{q}|x+z\alpha, \mathfrak{q}\nmid 3} \mathfrak{q}^{v_\mathfrak{q}(x+z\alpha)} = \mathfrak{p}_1^{v_{\mathfrak{p}_1}(x+z\alpha)}\mathfrak{p}_2^{v_{\mathfrak{p}_2}(x+z\alpha)}\mathfrak{a}^3 \quad \text{(Typ 2)}$$

sofort die Behauptung. ■

Wir wollen nun die Anteile von $\mathfrak{p}$ bzw. $\mathfrak{p}_1$ und $\mathfrak{p}_2$ in $(x + z\alpha)$ genauer studieren. Dazu berechnen wir diese bei (einigen) unserer gefundenen Lösungen $x^3 + 3y^3 + dz^3 = 0$ (mit $\mathrm{ggT}(x, y, z) = 1$). Die Ergebnisse sind in einer Tabelle zusammengestellt.
Anhand der Tabelle lassen sich einige Vermutungen aufstellen, die im folgenden bewiesen werden sollen.

LEMMA. *Sei $d = ab^2 \geq 2$ mit quadratfreien $a, b \in \mathbf{N}$ und $\mathrm{ggT}(a, b) = 1$, seien $x, y, z \in \mathbf{Z}$ mit $\mathrm{ggT}(x, y, z) = 1$ und $x^3 + 3y^3 + dz^3 = 0$. Dann gilt:*

$$a^2 \equiv b^2 \bmod 9 \quad \textit{(Typ 2)} \qquad \Longleftrightarrow \qquad y \equiv 0 \bmod 3.$$

Beweis: $\Longrightarrow$ Aus $a^2 \equiv b^2 \bmod 9$ folgt $d \equiv a^3 \bmod 9$ und damit modulo 3 die Kongruenz $0 \equiv x^3 + 3y^3 + dz^3 \equiv x^3 + a^3z^3 \equiv (x + az)^3 \bmod 3$, was $x + az \equiv 0 \bmod 3$ liefert. Es folgt $x^2 - xaz + a^2z^2 = (x + az)^2 - 3xaz \equiv 0 \bmod 3$ und damit modulo 9

$$x^3 + dz^3 \equiv x^3 + a^3z^3 = (x + az)(x^2 - xaz + a^2z^2) \equiv 0 \bmod 9,$$

Werte für $v_{\mathfrak{p}}(x + z\alpha)$ bzw. $(v_{\mathfrak{p}_1}(x + z\alpha), v_{\mathfrak{p}_2}(x + z\alpha))$

d	x	y	z	$\mathrm{N}(x + z\alpha)$	$v_{\mathfrak{p}}(x + z\alpha)$ bzw. $(v_{\mathfrak{p}_1}(x + z\alpha), v_{\mathfrak{p}_2}(x + z\alpha))$
2	655	-253	-488	$-3 \cdot 11^3 \cdot 23^3$	1
3	21	17	-20	$3 \cdot 17^3$	1
3	1314	271	-919	$3 \cdot 271^3$	1
4	2849	-1555	-1436	$-3 \cdot 5^3 \cdot 311^3$	1
5	4	13	-11	$3 \cdot 13^3$	1
10	1	-3	2	-3^4	(3,1)
10	11	-3	-5	-3^4	(3,1)
10	13	-9	-1	-3^7	(6,1)
10	161	237	-164	$3^4 \cdot 79^3$	(3,1)
11	2	1	-1	3	1
11	28	-19	-5	$-3 \cdot 19^3$	1
17	4	-3	1	-3^4	(3,1)
17	392	-141	-145	$-3^4 \cdot 47^3$	(3,1)
23	1	-2	1	$-2^3 \cdot 3$	1
23	47	44	-25	$2^6 \cdot 3 \cdot 11^3$	1
25	1	2	-1	$2^3 \cdot 3$	1
25	49	-52	23	$-2^6 \cdot 3 \cdot 13^3$	1
44	5	-3	-1	-3^4	(3,1)
44	191	-141	32	$-3^4 \cdot 47^3$	(3,1)
44	185	-507	206	$-3^4 \cdot 13^6$	(3,1)
44	557	-387	29	$-3^7 \cdot 43^3$	(6,1)
47	1	5	-2	$3 \cdot 5^3$	1
47	751	-1885	748	$-3 \cdot 5^3 \cdot 13^3 \cdot 29^3$	1

was wegen $x^3 + 3y^3 + dz^3 = 0$ sofort $3y^3 \equiv 0 \bmod 9$ und damit $y \equiv 0 \bmod 3$ liefert.
$\Longleftarrow$ Aus $3|y$ folgt $3 \nmid x$, $3 \nmid z$, $3 \nmid a$, $3 \nmid b$. Modulo 9 ergibt sich $0 = x^3 + 3y^3 + dz^3 \equiv x^3 + ab^2z^3 \bmod 9$, also $ab^2z^3 \equiv -x^3 \bmod 9$. Nun ist $\#(\mathbf{Z}/9\mathbf{Z})^* = 6$, also gilt $a^6 \equiv b^6 \equiv x^6 \equiv z^6 \equiv 1 \bmod 9$ und damit

$$a \equiv ab^6z^6 = ab^2z^3 \cdot b^4z^3 \equiv -x^3b^4z^3 \bmod 9,$$

also

$$a^2 \equiv x^6b^8z^6 \equiv b^8 = b^2 \cdot b^6 \equiv b^2 \bmod 9,$$

d.h. $a^2 - b^2 \equiv 0 \bmod 9$, was gezeigt werden sollte. ■

Wir können jetzt den 3-Anteil in der Faktorisierung von $(x + z\alpha)$ genau bestimmen:

Satz. *Sei $d = ab^2 \geq 2$ mit quadratfreien $a, b \in \mathbf{N}$ und $\mathrm{ggT}(a, b) = 1$ und $K = \mathbf{Q}(\alpha)$ mit $\alpha^3 = d$ der zugehörige Zahlkörper. Seien weiter $x, y, z \in \mathbf{Z}$ mit $x^3 + 3y^3 + dz^3 = 0$ und $\mathrm{ggT}(x, y, z) = 1$.*

1. *Gilt $a^2 \not\equiv b^2 \bmod 9$, so gilt in $\mathbf{Z}_K$ die Idealzerlegung*

$$(x + z\alpha) = \mathfrak{p}\mathfrak{a}^3, \quad \mathrm{ggT}(3, \mathrm{N}\mathfrak{a}) = 1,$$

   wobei $\mathfrak{p}^3 = (3)$ ist.
2. *Gilt $a^2 \equiv b^2 \bmod 9$, so ist $m = v_3(y) \geq 1$ und in $\mathbf{Z}_K$ hat man die Idealzerlegung*

$$(x + z\alpha) = \mathfrak{p}_1^{3m}\mathfrak{p}_2\mathfrak{a}^3 \quad \textit{mit} \quad \mathrm{ggT}(3, \mathrm{N}\mathfrak{a}) = 1,$$

   wobei $\mathfrak{p}_1\mathfrak{p}_2^2 = (3)$ gilt.

Beweis:

1. Wir wissen bereits, dass wir schreiben können $(x + z\alpha) = \mathfrak{p}^{m_0}\mathfrak{a}^3$ mit $\mathrm{ggT}(3, \mathrm{N}\mathfrak{a}) = 1$ und $m_0 \geq 0$. Normbildung liefert

$$3^{m_0}(\mathrm{N}\mathfrak{a})^3 = \mathrm{N}(\mathbf{Z}_K(x + z\alpha)) = |\mathrm{N}(x + z\alpha)| = |x^3 + dz^3| = 3|y|^3.$$

   Im Fall $a^2 \not\equiv b^2 \bmod 9$ ist $y \not\equiv 0 \bmod 3$, also folgt sofort $m_0 = 1$, wie behauptet.

2. Im Fall $a^2 \equiv b^2 \bmod 9$ wissen wir, dass
$$3|y, \quad 3\nmid x, \quad 3\nmid z, \quad 3\nmid a, \quad 3\nmid b$$
gilt. Insbesondere ist $m = v_3(y) \geq 1$. Wir können ansetzen
$$(x+z\alpha) = \mathfrak{p}_1^{m_1}\mathfrak{p}_2^{m_2}\mathfrak{a}^3 \quad \text{mit} \quad \mathrm{ggT}(3, \mathrm{N}\mathfrak{a}) = 1.$$
Normbildung liefert
$$3^{m_1+m_2}\mathrm{N}\mathfrak{a}^3 = \mathrm{N}(\mathbf{Z}_K(x+z\alpha)) = |\mathrm{N}(x+z\alpha)| = |x^3+dy^3| = |-3y^3|,$$
was sofort zu
$$m_1 + m_2 = 1 + 3m$$
führt. Wir zerlegen
$$\begin{aligned} -3y^3 &= x^3+dz^3 = (x+z\alpha)(x^2-xz\alpha+z^2\alpha^2) = (x+z\alpha)((x+z\alpha)^2-3xz\alpha) = \\ &= (x+z\alpha)^3 - 3xz\alpha(x+z\alpha) \end{aligned}$$
und erhalten
$$(x+z\alpha)^3 = 3xz\alpha(x+z\alpha) - 3y^3,$$
was sofort $\mathfrak{p}_1|x+z\alpha$ und $\mathfrak{p}_2|x+z\alpha$ liefert, also $m_1 \geq 1$ und $m_2 \geq 1$.
Wir haben die Zerlegung
$$x^2 - xz\alpha + z^2\alpha^2 = (x+z\alpha)^2 - 3xz\alpha$$
und
$$v_{\mathfrak{p}_2}(x+z\alpha)^2 = 2m_2, \quad v_{\mathfrak{p}_2}(3xz\alpha) = 2.$$
Wäre $m_2 \geq 2$, so würde folgen
$$v_{\mathfrak{p}_2}(x^2 - xz\alpha + z^2\alpha^2) = \min(2m_2, 2) = 2$$
und damit
$$2 + 6m = v_{\mathfrak{p}_2}(-3y^3) = v_{\mathfrak{p}_2}((x+z\alpha)(x^2-xz\alpha+z^2\alpha)) = m_2 + 2,$$
also $m_2 = 6m$, was natürlich der Gleichung $m_1 + m_2 = 1 + 3m$ wegen $m \geq 1$ widerspricht. Daher bleibt nur der Fall $m_2 = 1$ übrig. Daraus ergibt sich weiter $m_1 = 3m + 1 - m_2 = 3m$, d.h. wir erhalten die Zerlegung
$$(x+z\alpha) = \mathfrak{p}_1^{3m}\mathfrak{p}_2\mathfrak{a}^3,$$
was gezeigt werden sollte. ■

Wir interpretieren nun im Fall von Typ 1 die Beziehungen $(3) = \mathfrak{p}^3$ und $(x+z\alpha) = \mathfrak{p}\mathfrak{a}^3$ in der Klassengruppe.

SATZ. *Sei $d = ab^2 \geq 2$ mit quadratfreien $a, b \in \mathbf{N}$ und $\mathrm{ggT}(a,b) = 1$ sowie $a^2 \not\equiv b^2 \bmod 9$, $K = \mathbf{Q}(\alpha)$ mit $\alpha^3 = 3$ der zugehörige Zahlkörper und $\mathfrak{p}^3 = (3)$ in $\mathbf{Z}_K$. Die Klassengruppe habe die Zerlegung*
$$C\ell(\mathbf{Z}_K) \simeq Z_{d_1} \oplus \cdots \oplus Z_{d_r} \quad \text{mit} \quad d_1|d_2|\ldots|d_r.$$
Es gilt
$$\mathfrak{p} \quad \text{kein Hauptideal} \quad \Longrightarrow \quad 3|d_r.$$
Sind nun $x, y, z \in \mathbf{Z}$ mit
$$x^3 + 3y^3 + dz^3 = 0 \quad \text{und} \quad \mathrm{ggT}(x,y,z) = 1,$$
so gilt
$$9\nmid d_r \quad \Longrightarrow \quad \mathfrak{p} \quad \text{Hauptideal.}$$

Beweis: Ist $\mathfrak{p}$ kein Hauptideal, so hat wegen $\mathfrak{p}^3 = (3)$ das Ideal $\mathfrak{p}$ Ordnung 3 in der Klassengruppe, also folgt $3|\#C\ell(\mathbf{Z}_K) = d_1 \ldots d_r$ und damit $3|d_r$.
Wir haben eine Zerlegung $(x+z\alpha) = \mathfrak{p}\mathfrak{a}^3$, die sofort $(x+z\alpha)^3 = \mathfrak{p}^3\mathfrak{a}^9 = 3\mathfrak{a}^9$ liefert. Also ist $\mathfrak{a}^9$ ein Hauptideal. Da auch $\mathfrak{a}^{d_r}$ Hauptideal ist, folgt, dass $\mathfrak{a}^{\mathrm{ggT}(9,d_r)}$ Hauptideal ist. Gilt nun $9\nmid d_r$, so ist $\mathrm{ggT}(9,d_r) = 1$ oder $\mathrm{ggT}(9,d_r) = 3$, also ist $\mathfrak{a}$ oder $\mathfrak{a}^3$ ein Hauptideal, in jedem Fall also $\mathfrak{a}^3$ und damit auch $\mathfrak{p}$. ■

Bemerkungen:

1. Im Fall $C\ell(\mathbf{Z}_K) \simeq Z_{d_1} \oplus \cdots \oplus Z_{d_r}$ mit $d_1 | \ldots | d_r$ ist d_r die kleinste natürliche Zahl e mit $C\ell(\mathbf{Z}_K)^e = \{1\}$. Die Zahl d_r wird auch als Exponent der abelschen Gruppe $C\ell(\mathbf{Z}_K)$ bezeichnet.
2. Ist $\mathfrak{p}$ kein Hauptideal, so gilt $3 | d_r$, also $\mathrm{ggT}(9, d_r) \in \{3, 9\}$.
3. Die Bedingung $9 \nmid d_r$ läßt sich auch als $\mathrm{ggT}(9, d_r) \in \{1, 3\}$ formulieren.

Damit erhalten wir folgendes Klassengruppenkriterium:

Kriterium: Sei $d = ab^2 \geq 2$ mit quadratfreien $a, b \in \mathbf{N}$ und $\mathrm{ggT}(a, b) = 1$ sowie $a^2 \not\equiv b^2 \bmod 9$, $K = \mathbf{Q}(\alpha)$ mit $\alpha^3 = d$ der zugehörige Zahlkörper und $\mathfrak{p}^3 = (3)$ in $\mathbf{Z}_K$ sowie $C\ell(\mathbf{Z}_K) \simeq Z_{d_1} \oplus \cdots \oplus Z_{d_r}$ mit $d_1 | \ldots | d_r$. Sind nun folgende Bedingungen erfüllt

- $\mathrm{ggT}(9, d_r) = 3$,
- $\mathfrak{p}$ ist kein Hauptideal,

so besitzt $x^3 + 3y^3 + dz^3 = 0$ nur die triviale Lösung $x = y = z = 0$.

Anwendung: Von unseren 11 ungelösten Fällen $d \in \{20, 22, 34, 46, 50, 55, 58, 68, 85, 92, 100\}$ liefern

$$d \in \{20, 22, 34, 50, 58, 68, 85, 92\}$$

reine kubische Zahlkörper $K = \mathbf{Q}(\sqrt[3]{d})$ vom Typ 1. Für sie haben wir mit dem Computeralgebrapaket KANT/KASH die Klassengruppe $C\ell(\mathbf{Z}_K) \simeq Z_{d_1} \oplus \cdots \oplus Z_{d_r}$ bestimmt und getestet, ob $\mathfrak{p}$ ein Hauptideal ist oder nicht. Die KASH-Befehle lauteten z.B. für $d = 20$:

```
O:=OrderMaximal(Poly(Zx,[1,0,0,-20]));
OrderClassGroup(O);
a:=Factor(3*O);
pp:=a[1][1];
IdealIsPrincipal(pp,classgroup);
```

Wir erhielten das Ergebnis:

d	Invarianten $(d_1, \ldots, d_r)$ von $C\ell(\mathbf{Z}_K)$	$\mathrm{ggT}(9, d_r)$	$\mathfrak{p}$ Hauptideal?	Kriterium erfolgreich?
20	(3)	3	Nein	Ja
22	(3)	3	Nein	Ja
34	(3)	3	Nein	Ja
50	(3)	3	Nein	Ja
58	(6)	3	Nein	Ja
68	(3)	3	Nein	Ja
85	(3)	3	Nein	Ja
92	(3)	3	Nein	Ja

Also hat in den angegebenen 8 Fällen

$$d \in \{20, 22, 34, 50, 58, 68, 85, 92\}$$

die Gleichung $x^3 + 3y^3 + dz^3 = 0$ nur die triviale Lösung. Unser Klassengruppenkriterium war also in jedem Fall erfolgreich.

Achtung: Bei Aufruf von 'IdealIsPrincipal($\mathfrak{p}$)' lieferte KANT/KASH im Fall $d = 239$, dass $\mathfrak{p}$ mit $\mathfrak{p}^3 = (3)$ kein Hauptideal ist, obwohl $h_K = 1$ berechnet wurde. Dies ist natürlich Unsinn, wird aber damit erklärt, dass numerisch nicht hinreichend genau gerechnet wurde. Bei Aufruf von 'IdealIsPrincipal($\mathfrak{p}$,classgroup)' liefert KANT/KASH dagegen einen Erzeuger des Ideals $\mathfrak{p}$. Die Methode 'IdealIsPrincipal($\mathfrak{p}$,classgroup)' soll immer korrekt arbeiten - ohne Annahme über hinreichende numerische Rechengenauigkeit.

Aufgabe: Suche d's vom Typ 1 ohne Lösung, für die das Klassengruppenkriterium nicht funktioniert.

Wir müssen nun noch die 3 Fälle $d \in \{46, 55, 100\}$ untersuchen, für die der zugehörige reine kubische Zahlkörper vom Typ 2 ist.

SATZ. *Sei $d \geq 2$ kubikfrei, $K = \mathbf{Q}(\alpha)$ mit $\alpha^3 = d$ vom Typ 2, $(3) = \mathfrak{p}_1\mathfrak{p}_2^2$, $C\ell(\mathbf{Z}_K) \simeq Z_{d_1} \oplus \cdots \oplus Z_{d_r}$ mit $d_1|\ldots|d_r$. Seien $x, y, z \in \mathbf{Z}$ mit $\mathrm{ggT}(x, y, z) = 1$ und $x^3 + 3y^3 + dz^3 = 0$. Dann gilt:*

$$d_r|3 \quad \Longrightarrow \quad \mathfrak{p}_2 \text{ Hauptideal} \qquad (\text{und } \mathfrak{p}_1 \text{ Hauptideal}).$$

Beweis: Wir haben eine Darstellung

$$(x + z\alpha) = \mathfrak{p}_1^{3m}\mathfrak{p}_2\mathfrak{a}^3 = \mathfrak{p}_2(\mathfrak{p}_1^m\mathfrak{a})^3.$$

Die Voraussetzung $d_r|3$ liefert, dass $(\mathfrak{p}_1^m\mathfrak{a})^3$ ein Hauptideal ist, also ist auch $\mathfrak{p}_2$ ein Hauptideal. Wegen $\mathfrak{p}_1\mathfrak{p}_2^2 = (3)$ muss dann schließlich auch $\mathfrak{p}_1$ ein Hauptideal sein. ■

Wir erhalten nun sofort folgendes Kriterium:

Kriterium: Sei $d = ab^2 \geq 2$ mit $a, b \in \mathbf{N}$ quadratfrei, $\mathrm{ggT}(a, b) = 1$ und $a^2 \equiv b^2 \bmod 9$, $K = \mathbf{Q}(\alpha)$ mit $\alpha^3 = d$ der zugehörige reine kubische Zahlkörper (vom Typ 2) und $C\ell(\mathbf{Z}_K) \simeq d_1 \oplus \cdots \oplus d_r$ mit $d_1|\ldots|d_r$. Gilt

- $d_r = 3$,
- $\mathfrak{p}_2$ kein Hauptideal,

so hat die Gleichung $x^3 + 3y^3 + dz^3 = 0$ nur die triviale Lösung $x = y = z = 0$ in ganzen Zahlen.

Anwendung: Wir betrachten unsere verbliebenen Fälle $d \in \{46, 55, 100\}$. Folgende Tabelle wurde wieder mit KANT/KASH erstellt:

d	Invarianten $(d_1, \ldots, d_r)$ von $C\ell(\mathbf{Z}_K)$	d_r	$\mathfrak{p}_2$ Hauptideal?	Kriterium erfolgreich?
46	(1)	1	Ja	Nein
55	(1)	1	Ja	Nein
100	(1)	1	Ja	Nein

Das Kriterium hilft also hier nicht weiter. Die Fälle $d \in \{46, 55, 100\}$ bleiben weiterhin offen.
Im Fall $d = 170 = 2 \cdot 5 \cdot 17$ gibt es immer Kongruenzlösungen, aber

d	Invarianten $(d_1, \ldots, d_r)$ von $C\ell(\mathbf{Z}_K)$	d_r	$\mathfrak{p}_2$ Hauptideal?	Kriterium erfolgreich?
170	(3)	3	Nein	Ja

zeigt mit dem letzten Kriterium, dass die Gleichung $x^3 + 3y^3 + 170z^3 = 0$ keine nichttriviale Lösung besitzt.

5. Klassengruppenkriterien für $\mathbf{Q}(\sqrt[3]{9d})$ bzw. $\mathbf{Q}(\sqrt[3]{\frac{d}{3}})$

Sei $d = ab^2 \geq 2$ kubikfrei mit $a, b \in \mathbf{N}$ und $\mathrm{ggT}(a, b) = 1$. Die Gleichung $x^3 + 3y^3 + dz^3 = 0$ können wir auch in der Form

$$3y^3 + dz^3 = -x^3$$

schreiben.

- Gilt $3 \nmid d$, so folgt durch Multiplikation mit 9

  $$27y^3 + 9ab^2z^3 = -9x^3, \quad \text{also} \quad (3y)^3 + a(3b)^2z^3 = -9x^3.$$

  Wir setzen $\widetilde{d} = a(3b)^3$ und erhalten dann in $K = \mathbf{Q}(\beta)$ mit $\beta^3 = \widetilde{d}$

  $$(3y + z\beta)(9y^2 - 3yz\beta + z^2\beta^2) = -9x^3 \quad \text{und} \quad \mathrm{N}(3y + z\beta) = -3x^3.$$

  (Natürlich ist K ein reiner kubischer Zahlkörper vom Typ 1.)
- Gilt $3|d$, so ist $v_3(d) = 1$, d.h. $3|a$. Schreiben wir $a = 3\widetilde{a}$ und $\widetilde{d} = \widetilde{a}b^2 = \frac{d}{3}$, so gilt

  $$3y^3 + 3\widetilde{a}b^2z^3 = -x^3,$$

  also ist $x = 3\widetilde{x}$ und wir erhalten

  $$3y^3 + 3\widetilde{d}z^3 = -27\widetilde{x}^3, \quad \text{also} \quad y^3 + \widetilde{d}z^3 = -9\widetilde{x}^3.$$

  Setzt man $K = \mathbf{Q}(\beta)$ mit $\beta^3 = \widetilde{d}$, so folgt in K

  $$(y + z\beta)(y^2 - yz\beta + z^2\beta^2) = -9\widetilde{x}^3 \quad \text{und} \quad \mathrm{N}(y + z\beta) = -9\widetilde{x}^3.$$

Wir betrachten zunächst den Fall $3 \nmid d$. Um zu einer Vermutung zu kommen, berechnen wir in $K = \mathbf{Q}(\beta)$ mit $\beta^3 = \widetilde{d} = 9d$ für einige gefundene Lösungen (x, y, z) von $x^3 + 3y^3 + dz^3 = 0$ die Norm $\mathrm{N}(3y + z\beta)$ und $v_{\mathfrak{p}}(3y + z\beta)$:

d	$\widetilde{d}$	x	y	z	$\mathrm{N}(3y + z\beta)$	$v_{\mathfrak{p}}(3y + z\beta)$
53	477	7	3	-2	$3^2 \cdot 7^3$	2
59	531	17	-16	5	$3^2 \cdot 17^3$	2
61	549	4	-1	-1	$2^6 \cdot 3^2$	2
61	549	23	-29	10	$3^2 \cdot 23^3$	2
61	549	55	-82	29	$3^2 \cdot 5^3 \cdot 11^3$	2
61	549	232	125	-67	$2^9 \cdot 3^2 \cdot 29^3$	2
61	549	1723	-1198	89	$3^2 \cdot 1723^3$	2
67	603	4	1	-1	$2^6 \cdot 3^2$	2
67	603	5	-4	1	$3^2 \cdot 5^3$	2
67	603	13	-23	8	$3^2 \cdot 13^3$	2
67	603	280	-131	-61	$2^9 \cdot 3^2 \cdot 5^3 \cdot 7^3$	2
67	603	925	-647	68	$3^2 \cdot 5^6 \cdot 37^3$	2
67	603	1295	-232	-317	$3^2 \cdot 5^3 \cdot 7^3 \cdot 37^3$	2
67	603	2909	-199	-716	$3^2 \cdot 2909^3$	2

Wir beweisen dazu folgenden Satz:

SATZ. *Sei $d = ab^2 \in \mathbf{N}$ kubikfrei mit $a, b \in \mathbf{N}$, $\mathrm{ggT}(a, b) = 1$ und $d \not\equiv 0 \bmod 3$. Seien $x, y, z \in \mathbf{Z}$ mit $x^3 + 3y^3 + dz^3 = 0$ und $\mathrm{ggT}(x, y, z) = 1$. Setzt man $\widetilde{d} = a(3b)^2$ und $K = \mathbf{Q}(\beta)$ mit $\beta^3 = \widetilde{d}$, so gilt in $\mathbf{Z}_K$*

$$(3y + z\beta) = \mathfrak{p}^2\mathfrak{a}^3 \quad \textit{mit} \quad \mathfrak{p}^3 = (3) \quad \textit{und} \quad \mathrm{ggT}(3, \mathrm{N}\mathfrak{a}) = 1.$$

Beweis: Natürlich gilt $a^2 - (3b)^2 \not\equiv 0 \bmod 9$, d.h. K ist ein reiner kubischer Zahlkörper vom Typ 1, es gibt also genau ein Primideal $\mathfrak{p}$, das die 3 enthält. Außerdem gilt $\mathfrak{p}^3 = (3)$. Wir haben die Zerlegung

$$(3y + z\beta)(9y^2 - 3yz\beta + z^2\beta) = -9x^3 \quad \text{und} \quad \mathrm{N}(3y + z\beta) = 27z^3 + \widetilde{d}z^3 = -9x^3.$$

Wie früher zeigt man für ein Primideal $\mathfrak{q}$:

$$\mathfrak{q} | 3y + z\beta, \quad \mathfrak{q} | 9y^2 - 3yz\beta + z^2\beta \quad \Longrightarrow \quad \mathfrak{q} = \mathfrak{p}.$$

Daraus erhält man eine Zerlegung

$$(3y + z\beta) = \mathfrak{p}^m\mathfrak{a}^3 \quad \text{mit} \quad \mathrm{ggT}(3, \mathrm{N}\mathfrak{a}) = 1.$$

Normbildung liefert

$$9|x|^3 = \mathrm{N}((3y + z\beta) = 3^m(\mathrm{N}\mathfrak{a})^3.$$

Wegen $3 \nmid x$ folgt sofort $m = 2$ und damit die Behauptung. ■

Wie früher leitet man damit folgendes Kriterium her:

Kriterium: Sei $d = ab^2 \geq 2$ mit quadratfreien $a, b \in \mathbf{N}$, $\mathrm{ggT}(a, b) = 1$ und $d \not\equiv 0 \bmod 3$. Sei $\widetilde{d} = 9d$, $K = \mathbf{Q}(\beta)$ mit $\beta^3 = \widetilde{d}$ der zugehörige Zahlkörper und $\mathfrak{p}^3 = (3)$ in $\mathbf{Z}_K$ sowie $C\ell(\mathbf{Z}_K) \simeq Z_{d_1} \oplus \cdots \oplus Z_{d_r}$ mit $d_1 | \ldots | d_r$. Sind nun folgende Bedingungen erfüllt

- $\mathrm{ggT}(9, d_r) = 3$,
- $\mathfrak{p}$ ist kein Hauptideal,

so besitzt $x^3 + 3y^3 + dz^3 = 0$ nur die triviale Lösung $x = y = z = 0$.

Anwendungsversuch: Wir versuchen, das Kriterium auf unsere 11 Fälle

$$d \in \{20, 22, 34, 46, 50, 55, 58, 68, 85, 92, 100\}$$

anzuwenden, die nach den Kongruenzbetrachungen noch offen waren. Hier wird $K = \mathbf{Q}(\beta)$ mit $\beta^3 = \widetilde{d} = 9d$ zugrundegelegt.

d	$\widetilde{d}$	Invarianten $(d_1, \ldots, d_r)$ von $C\ell(\mathbf{Z}_K)$	$\mathrm{ggT}(9, d_r)$	$\mathfrak{p}$ Hauptideal?	Kriterium erfolgreich?
20	180	(3)	3	Nein	Ja
22	198	(6)	3	Nein	Ja
34	306	(3)	3	Nein	Ja
46	414	(6)	3	Ja	Nein
50	450	(3)	3	Nein	Ja
55	495	(9)	9	Nein	Nein
58	522	(3)	3	Nein	Ja
68	612	(6)	3	Nein	Ja
85	765	(3)	3	Nein	Ja
92	828	(6)	3	Nein	Ja
100	900	(3)	3	Ja	Nein

Leider werden die offenen Fälle

$$d \in \{46, 55, 100\}$$

durch das Kriterium nicht abgedeckt.

Wir betrachten nun den Fall $d \equiv 0 \bmod 3$. Um zu einer Vermutung zu kommen, berechnen wir in $K = \mathbf{Q}(\beta)$ mit $\beta^3 = \widetilde{d} = \frac{d}{3}$ für einige gefundene Lösungen (x, y, z) von $x^3 + 3y^3 + dz^3 = 0$ die Norm $\mathrm{N}(y + z\beta)$ und $v_{\mathfrak{p}}(y + z\beta)$ im Fall von Typ 1 bzw. $(v_{\mathfrak{p}_1}(y + z\beta), v_{\mathfrak{p}_2}(y + z\beta)$ im Fall von Typ 2.

d	$\widetilde{d}$	x	y	z	$\mathrm{N}(y + z\beta)$	$v_{\mathfrak{p}}(y + z\beta)$ bzw. $(v_{\mathfrak{p}_1}(3y + z\beta), v_{\mathfrak{p}_2}(3y + z\beta))$
30	10	3	1	-1	3^2	(1,1)
30	10	33	-19	-8	$3^2 \cdot 11^3$	(1,1)
51	17	3	2	-1	3^2	(1,1)
51	17	9	-11	4	3^5	(4,1)
51	17	6	-13	5	$2^3 \cdot 3^2$	(1,1)
51	17	75	-52	-1	$3^2 \cdot 5^6$	(1,1)

Wir beweisen dazu folgenden Satz:

SATZ. *Sei $d = ab^2 \in \mathbf{N}$ kubikfrei mit $a, b \in \mathbf{N}$, $\mathrm{ggT}(a, b) = 1$ und $3|d$. Seien $x, y, z \in \mathbf{Z}$ mit $\mathrm{ggT}(x, y, z) = 1$ und $x^3 + 3y^3 + dz^3 = 0$. Dann gilt $3|a$ und $3|x$. Schreibt man $x = 3\widetilde{x}$, $a = 3\widetilde{a}$ und $\widetilde{d} = \widetilde{a}b^2 = \frac{d}{3}$ und setzt man $K = \mathbf{Q}(\beta)$ mit $\beta^3 = \widetilde{d}$, so ist K ein reiner kubischer Zahlkörper vom Typ 2, d.h. die 3 zerlegt sich als $(3) = \mathfrak{p}_1\mathfrak{p}_2^2$ und es gilt*

$$(y + z\beta) = \mathfrak{p}_1^{1+3m}\mathfrak{p}_2\mathfrak{a}^3 \quad \textit{mit} \quad \mathrm{ggT}(3, \mathrm{N}\mathfrak{a}) = 1 \quad \textit{und} \quad m = v_3(\widetilde{x}).$$

Beweis: Wir haben bereits gesehen, dass gilt

$$y^3 + \widetilde{a}b^2z^3 = -9\widetilde{x}^3.$$

Außerdem gilt natürlich $3 \nmid y$, $3 \nmid z$, $3 \nmid \widetilde{a}$, $3 \nmid b$. Wegen $\#(\mathbf{Z}/9\mathbf{Z})^* = 6$ gilt dann

$$y^6 \equiv z^6 \equiv \widetilde{a}^6 \equiv b^6 \equiv 1 \bmod 9.$$

Aus $\widetilde{a}b^2z^3 \equiv -y^3 \bmod 9$ folgt also durch Quadrieren

$$\widetilde{a}^2b^4 \equiv \widetilde{a}^2b^4z^6 \equiv y^6 \equiv 1 \bmod 9,$$

Multiplikation mit b^2 ergibt

$$\widetilde{a}^2 \equiv \widetilde{a}^2b^4 \cdot b^2 \equiv b^2 \bmod 9,$$

d.h. $K = \mathbf{Q}(\beta)$ ist ein reiner kubischer Zahlkörper vom Typ 2 und 3 faktorisiert als $(3) = \mathfrak{p}_1\mathfrak{p}_2^2$.
Man faktorisiert nun

$$(y + z\beta)(y^2 - yz\beta + z^2\beta^1) = -9\widetilde{x}^3 \quad \text{und} \quad \mathrm{N}(y + z\beta) = -9\widetilde{x}^3.$$

Wie früher sieht man für ein Primideal $\mathfrak{q}$:

$$\mathfrak{q}|y + z\beta, \quad \mathfrak{q}|y^2 - yz\beta + z^2\beta^2 \quad \Longrightarrow \quad \mathfrak{q}|3 \quad \Longrightarrow \quad \mathfrak{q} = \mathfrak{p}_1 \text{ oder } \mathfrak{q} = \mathfrak{p}_2.$$

Dann muss $(y + z\beta)$ bis auf den 3-Anteil eine 3-te Potenz sein, d.h. man hat eine Zerlegung

$$(y + z\beta) = \mathfrak{p}_1^{m_1}\mathfrak{p}_2^{m_2}\mathfrak{a}^3 \quad \text{mit} \quad \mathrm{ggT}(3, \mathrm{N}\mathfrak{a}) = 1.$$

Sei nun $m = v_3(\widetilde{x})$. Die Norm liefert

$$3^{m_1+m_2}\mathrm{N}\mathfrak{a}^3 = \mathrm{N}((y + z\beta)) = 3^2|\widetilde{x}|^3,$$

woraus sofort

$$m_1 + m_2 = 2 + 3m$$

folgt. Wir haben

$$y^2 - yz\beta + z^2\beta^2 = (y + z\beta)^2 - 3yz\beta.$$

Daraus folgt zunächst $m_1 \geq 1$ und $m_2 \geq 2$, da andernfalls $\mathfrak{p}_i$ auch $y^2 + yz\beta + z^2\beta^2$ nicht teilen würde, was aber nicht sein kann, da das Produkt mit $y + z\beta$ die Zahl $-9\widetilde{x}^3$ ergibt. Wäre $m_2 \geq 2$, also $v_{\mathfrak{p}_2}(y + z\beta) \geq 2$, so würde mit $v_{\mathfrak{p}_2}(3) = 2$ sofort $v_{\mathfrak{p}_2}(y^2 - yz\beta + z^2\beta^2) = 2$ und damit

$$4 + 6m = v_{\mathfrak{p}_2}(-9\widetilde{x}^3) = v_{\mathfrak{p}_2}(y + z\beta) + v_{\mathfrak{p}_2}(y^2 - yz\beta + z^2\beta^2) = m_2 + 2$$

folgen. Also wäre $m_2 = 2 + 6m$ und damit $m_1 = 2 + 3m - m_2 = (2 + 3m) - (2 + 6m) = -3m \leq 0$, ein Widerspruch zu $m_1 \geq 1$. Damit muss nun $m_2 = 1$ gelten, was schließlich auch $m_1 = 2+3m-m_2 = 1+3m$ ergibt. ■

Der Satz führt zu folgendem Kriterium:

Kriterium: Sei $d \geq 2$ kubikfrei mit $d \equiv 0 \bmod 3$ und $\widetilde{d} = \frac{d}{3}$. Sei $K = \mathbf{Q}(\beta)$ mit $\beta^3 = \widetilde{d}$ ein reiner kubischer Zahlkörper vom Typ 2, hierin $(3) = \mathfrak{p}_1\mathfrak{p}_2^2$ und $C\ell(\mathbf{Z}_K) \simeq Z_{d_1} \oplus \cdots \oplus Z_{d_r}$ mit $d_1|\ldots|d_r$. Gilt

- $d_r = 3$,
- $\mathfrak{p}_2$ kein Hauptideal,

so hat die Gleichung $x^3 + 3y^3 + dz^3 = 0$ nur die triviale Lösung $x = y = z = 0$ in ganzen Zahlen.

Beispiel: Für $d = 510$ ist $\widetilde{d} = 170$, die zugehörige Klassengruppe $\simeq Z_3$ und $\mathfrak{p}_2$ kein Hauptideal. Also hat $x^3 + 3y^3 + 510z^3 = 0$ nur die triviale Lösung in ganzen Zahlen. (Allerdings ist in diesem Fall auch das erste Kriterium für $K = \mathbf{Q}(\sqrt[3]{510})$ anwendbar, da in diesem Fall $C\ell(\mathbf{Z}_K) \simeq Z_6 \oplus Z_6$ gilt und $\mathfrak{p}$ kein Hauptideal ist.)

Unsere bisher offenen Fälle $d \in \{46, 55, 100\}$ bleiben also weiterhin offen.

6. Arithmetik in $\mathbf{Q}(\sqrt[3]{3})$

Unsere Gleichung $x^3 + 3y^3 + dz^3 = 0$ läßt sich auch als

$$x^3 + 3y^3 = -dz^3$$

schreiben und in der Gestalt

$$(x + y\sqrt[3]{3})(x^2 - xz\sqrt[3]{3} + z^2\sqrt[3]{3}^2) = -dz^3$$

faktorisieren.

Wir legen daher im folgenden den Zahlkörper

$$K = \mathbf{Q}(\alpha) \quad \text{mit} \quad \alpha^3 = 3$$

zugrunde. Es gilt

$$\mathbf{Z}_K = \mathbf{Z}[\alpha], \quad \mathrm{disc}\,\mathbf{Z}_K = -3^5, \quad h_K = 1,$$

d.h. $\mathbf{Z}_K$ ist Hauptidealring und faktorieller Ring. (Die Minkowski-Schranke ist 4.41.) Grundeinheit ist

$$\varepsilon = \alpha^2 - 2 \quad \text{mit} \quad \mathrm{N}\varepsilon = 1.$$

Im folgenden Lemma werden die Primideale von $\mathbf{Z}_K$ beschrieben:

LEMMA. *Sei p eine Primzahl.*

1. *Für $p = 3$ ist $\mathfrak{p} = (\alpha)$ das einzige $p = 3$ enthaltende Primideal und es gilt $\mathfrak{p}^3 = (3)$.*

2. *Für* $p \equiv 2 \bmod 3$ *gibt es (modulo* p *genau) ein* $a \in \mathbf{Z}$ *mit* $a^3 \equiv 3 \bmod p$. *Die* p *enthaltenden Primideale sind*

$$\mathfrak{p} = (p, \alpha - a) \quad \textit{und} \quad \mathfrak{p}' = (p, \alpha^2 + a\alpha + a^2)$$

mit $\mathrm{grad}\mathfrak{p} = 1$, $\mathrm{grad}\mathfrak{p}' = 2$ *und* $(p) = \mathfrak{p}\mathfrak{p}'$.
3. *Ist* $p \equiv 1 \bmod 3$, *so gibt es ein* $z \in \mathbf{Z}$ *mit* $z^2 + z + 1 \equiv 0 \bmod p$.
   (a) *Gibt es ein* $a \in \mathbf{Z}$ *mit* $a^3 \equiv 3 \bmod p$, *so gibt es drei* p *enthaltende Primideale, nämlich*

$$\mathfrak{p} = (p, \alpha - a), \quad \mathfrak{p}' = (p, \alpha - za), \quad \mathfrak{p}'' = (p, \alpha - z^2 a)$$

   mit $\mathrm{grad}\mathfrak{p} = \mathrm{grad}\mathfrak{p}' = \mathrm{grad}\mathfrak{p}'' = 1$ *und* $\mathfrak{p}\mathfrak{p}'\mathfrak{p}'' = (p)$.
   (b) *Gibt es kein* $a \in \mathbf{Z}$ *mit* $a^3 \equiv 3 \bmod p$, *so ist* (p) *prim in* $\mathbf{Z}_K$.

Beweis: Sei $f = x^3 - 3$ das Minimalpolynom von α. Die p enthaltenden Primideale von $\mathbf{Z}_K$ erhält man durch Faktorzerlegung von f modulo p.

1. $f \equiv x^3 \bmod 3$ zeigt zusammen mit $3 = \alpha^3$, dass $\mathfrak{p} = (3, \alpha) = (\alpha)$ das einzige 3 enthaltende Primideal ist, und dass $\mathfrak{p}^3 = (3)$ gilt. (Natürlich kann man dies auch unmittelbar aus der Gleichung $\alpha^3 = 3$ ersehen.) Da die Diskriminante des Zahlkörpers -3^5 ist, ist 3 die einzige verzweigte Primzahl.
2. Im Fall $p \equiv 2 \bmod 3$ betrachten wir den Gruppenhomomorphismus

$$\psi : \mathbf{F}_p^* \to \mathbf{F}_p^*, \quad u \mapsto u^3.$$

   Ist $z \in \mathrm{Kern}(\psi)$, so gilt $z^3 = 1$, da $\mathbf{F}_p^*$ Ordnung $p - 1$ hat, gilt auch $z^{p-1} = 1$, also $z^{\mathrm{ggT}(3,p-1)} = 1$, was wegen $p \equiv 2 \bmod 3$ sofort $\mathrm{ggT}(3, p-1) = 1$ und damit $z = 1$ liefert. Also ist ψ injektiv, da $\mathbf{F}_p^*$ endlich ist, auch surjektiv. Es gibt also genau ein $\overline{a} \in \mathbf{F}_p^*$ mit $\overline{a}^3 = 3$, d.h. modulo p genau ein $a \in \mathbf{Z}$ mit $a^3 \equiv 3 \bmod p$. Wir haben nun modulo p

$$f = x^3 - 3 \equiv x^3 - a^3 = (x - a)(x^2 + ax + a^2) \bmod p.$$

   Wäre $x^2 + ax + a^2$ reduzibel modulo p, so hätte es eine Nullstelle $a' \not\equiv a \bmod p$, die natürlich auch ${a'}^3 \equiv 3 \bmod p$ erfüllen würde, was nicht sein kann. Daher sind

$$\mathfrak{p} = (p, \alpha - a) \quad \text{und} \quad \mathfrak{p}' = (p, \alpha^2 + a\alpha + a^2)$$

   genau die p enthaltenden Primideale. Es gilt $\mathrm{grad}\mathfrak{p} = 1$ und $\mathrm{grad}\mathfrak{p}' = 2$, $\mathfrak{p}\mathfrak{p}' = (p)$.
3. Sei nun $p \equiv 1 \bmod 3$. Dann gilt $3 | p - 1$. Da es in einer zyklischen Gruppe zu jedem Teiler der Gruppenordnung ein Element dieser Ordnung gibt, die Gruppe $\mathbf{F}_p^*$ zyklisch ist, gibt es ein $\overline{z} \in \mathbf{F}_p^*$ mit $\overline{z} \neq 1$, $\overline{z}^3 = 1$, sodass dann $\overline{z}^2 + \overline{z} + 1 = 0$ gilt. Wir wählen nun $z \in \mathbf{Z}$ mit $z^2 + z + 1 \equiv 0 \bmod p$, was dann $z \not\equiv 1 \bmod p$ und $z^3 \equiv 1 \bmod p$ erfüllt, insbesondere sind $1, z, z^2$ modulo p verschieden und die 3 Nullstellen der Gleichung $x^3 - 1 \equiv 0 \bmod p$.
   (a) Gibt es ein $a \in \mathbf{Z}$ mit $a^3 \equiv 3 \bmod p$, so folgt

$$f = x^3 - 3 \equiv (x - a)(x - za)(x - z^2 a) \bmod p,$$

   also sind

$$\mathfrak{p} = (p, \alpha - a), \quad \mathfrak{p}' = (p, \alpha - za), \quad \mathfrak{p}'' = (p, \alpha - z^2 a)$$

   die p enthaltenden Primideale mit $\mathrm{grad}\mathfrak{p} = \mathrm{grad}\mathfrak{p}' = \mathrm{grad}\mathfrak{p}'' = 1$ und $\mathfrak{p}\mathfrak{p}'\mathfrak{p}'' = (p)$.
   (b) Gibt es kein $a \in \mathbf{Z}$ mit $a^3 \equiv 3 \bmod p$, so hat $f = x^3 - 3$ keine Nullstelle modulo p, ist also irreduzibel modulo p. Dann ist aber (p) das einzige Primideal, das p enthält. ■

Bemerkung: Da $\mathbf{Z}_K$ Hauptidealring ist, können wir für jedes Primideal $\mathfrak{p}$ ein Element π finden mit $\mathfrak{p} = (\pi)$. Natürlich ist π nur bis auf Einheit bestimmt, d.h. statt π kann man auch $\pm\varepsilon^l\pi$ (mit $l \in \mathbf{Z}$)

wählen. Für die nachfolgenden Primideale vom Grad 1 mit Norm ≤ 100 haben wir folgende π's ausgewählt:

2	$\mathfrak{p}_2 = (2, \alpha + 1)$	$\pi_2 = \alpha - 1$
3	$\mathfrak{p}_3 = (3, \alpha)$	$\pi_3 = \alpha$
5	$\mathfrak{p}_5 = (5, \alpha + 3)$	$\pi_5 = -\alpha + 2$
11	$\mathfrak{p}_{11} = (11, \alpha + 2)$	$\pi_{11} = \alpha + 2$
17	$\mathfrak{p}_{17} = (17, \alpha + 10)$	$\pi_{17} = \alpha^2 + 2$
23	$\mathfrak{p}_{23} = (23, \alpha + 11)$	$\pi_{23} = 2\alpha - 1$
29	$\mathfrak{p}_{29} = (29, \alpha + 11)$	$\pi_{29} = 7\alpha - 10$
41	$\mathfrak{p}_{41} = (41, \alpha + 14)$	$\pi_{41} = \alpha^2 + 2\alpha - 4$
47	$\mathfrak{p}_{47} = (47, \alpha + 19)$	$\pi_{47} = 2\alpha^2 + \alpha + 2$
53	$\mathfrak{p}_{53} = (53, \alpha + 20)$	$\pi_{53} = 2\alpha^2 + 3\alpha + 2$
59	$\mathfrak{p}_{59} = (59, \alpha + 10)$	$\pi_{59} = -\alpha^2 + 2\alpha + 2$
61	$\mathfrak{p}_{61a} = (61, \alpha + 9)$	$\pi_{61a} = \alpha^2 + 2\alpha - 2$
61	$\mathfrak{p}_{61b} = (61, \alpha + 56)$	$\pi_{61b} = -3\alpha^2 + 2\alpha + 4$
61	$\mathfrak{p}_{61c} = (61, \alpha + 57)$	$\pi_{61c} = -\alpha + 4$
67	$\mathfrak{p}_{67a} = (67, \alpha + 4)$	$\pi_{67a} = \alpha + 4$
67	$\mathfrak{p}_{67b} = (67, \alpha + 14)$	$\pi_{67b} = -2\alpha^2 + \alpha + 4$
67	$\mathfrak{p}_{67c} = (67, \alpha + 49)$	$\pi_{67c} = 4\alpha - 5$
71	$\mathfrak{p}_{71} = (71, \alpha + 65)$	$\pi_{71} = 2\alpha^2 - 1$
73	$\mathfrak{p}_{73a} = (73, \alpha + 6)$	$\pi_{73a} = 2\alpha^2 + 1$
73	$\mathfrak{p}_{73b} = (73, \alpha + 19)$	$\pi_{73b} = \alpha^2 + 4$
73	$\mathfrak{p}_{73c} = (73, \alpha + 48)$	$\pi_{73c} = 3\alpha - 2$
83	$\mathfrak{p}_{83} = (83, \alpha + 72)$	$\pi_{83} = 2\alpha^2 + \alpha - 4$
89	$\mathfrak{p}_{89} = (89, \alpha + 60)$	$\pi_{89} = 3\alpha + 2$

LEMMA. *Seien $x, y \in \mathbf{Z}$ mit $\mathrm{ggT}(x, y) = 1$ und sei*

$$(x + y\alpha) = (\alpha)^{u_0}\mathfrak{p}_1^{u_1} \ldots \mathfrak{p}_r^{u_r} \quad \text{mit} \quad u_0 \geq 0 \quad \text{und} \quad u_1, \ldots, u_r \geq 1$$

die Primidealzerlegung von $x + y\alpha$. Sei weiter p_i die in $\mathfrak{p}_i$ enthaltene Primzahl.

1. *Es gilt $u_0 \in \{0, 1\}$.*
2. *Es gilt $\mathrm{grad}(\mathfrak{p}_i) = 1$. (Daher erfüllen die (zuvor gewählten) Primelemente π_i mit $\mathfrak{p}_i = (\pi_i)$ die Gleichung $\mathrm{N}\pi_i = p_i$.)*
3. *Für $i \neq j$ gilt $p_i \neq p_j$.*
4. *Es gibt ein $l \in \mathbf{Z}$ mit*

   $$x + y\alpha = \pm\varepsilon^l \alpha^{u_0} \pi_1^{u_1} \ldots \pi_r^{u_r}.$$

   Zerlegt man $l = m + 3n$, $u_i = v_i + 3w_i$ mit $m, v_i \in \{0, 1, 2\}$, so gilt

   $$x + y\alpha = \varepsilon^m \alpha^{u_0} \pi_1^{v_1} \ldots \pi_r^{v_r} \cdot (\pm\pi_1^{w_1} \ldots \pi_r^{w_r})^3$$

   und

   $$3^{u_0} p_1^{v_1} \ldots p_r^{v_r}$$

   ist der kubikfreie (positive) Anteil der Norm $\mathrm{N}(x + y\alpha) = x^3 + 3y^3$.
5. *Gilt $x^3 + 3y^3 + dz^3 = 0$, so ist*

   $$d = 3^{u_0} p_1^{v_1} \ldots p_r^{v_r}$$

Beweis:

1. Im Fall $u_0 = 0$ ist nichts zu zeigen. Wir betrachten den Fall $u_0 \geq 1$. Es folgt $\alpha | x + y\alpha$, also $\alpha | x$ und damit $3 | x$, was wegen $\mathrm{ggT}(x, y) = 1$ die Beziehung $3 \nmid y$ und somit $v_\alpha(x) \geq 3$, $v_\alpha(y\alpha) = 1$, also $v_\alpha(x + y\alpha) = 1$ liefert. Dies zeigt $u_0 = 1$.

2. Wegen der Voraussetzung $e_i \geq 1$ gilt $\mathfrak{p}_i | x + y\alpha$. Würde $p_i | y$ gelten, würde dies $\mathfrak{p}_i | x$, also $p_i | x$ implizieren, im Widerspruch zu $\mathrm{ggT}(x, y) = 1$. Daher gibt es ein $u \in \mathbf{Z}$ mit $1 \equiv -uy \bmod p_i$. Da dann auch $1 \equiv -uy \bmod \mathfrak{p}_i$ gilt, folgt $\alpha \equiv -uy\alpha \equiv ux \bmod \mathfrak{p}_i$ und damit auch $\alpha^2 \equiv u^2 x^2 \bmod \mathfrak{p}_i$. Wegen $\mathbf{Z}_K = \mathbf{Z}\alpha^2 + \mathbf{Z}\alpha + \mathbf{Z}$, ist somit jedes $\beta \in \mathbf{Z}_K$ modulo $\mathfrak{p}_i$ äquivalent zu einer Zahl $t_\beta \in \mathbf{Z}$, wobei man wegen $\mathfrak{p}_i | p_i$ o.E. $t_\beta \in \{0, 1, \ldots, p_i - 1\}$ annehmen kann. Es folgt $\#\mathbf{Z}_K/\mathfrak{p}_i \leq p_i$ und damit natürlich $\#\mathbf{Z}_K/\mathfrak{p}_i = p_i$, also $\mathrm{grad}\mathfrak{p}_i = 1$.
3. Wir nehmen an, es gibt zwei Primideale $\mathfrak{p}_i, \mathfrak{p}_j$ mit $p_i = p_j = p$. Dann folgt wie eben $p \nmid x$, $p \nmid y$. Wegen $\mathrm{grad}\mathfrak{p}_i = \mathrm{grad}\mathfrak{p}_j = 1$ können wir ansetzen
$$\mathfrak{p}_i = (p, \alpha - a_i) \quad \text{und} \quad \mathfrak{p}_j = (p, \alpha - a_j).$$
Aus $\mathfrak{p}_i | x + y\alpha$ folgt $0 \equiv x + y\alpha \equiv x + ya_i \bmod \mathfrak{p}_i$, also $x + ya_i \in \mathfrak{p}_i \cap \mathbf{Z} = \mathbf{Z} \cdot p$ und damit $p | x + ya_i$. Genauso sieht man $p | x + ya_j$. Dies liefert $p | y(a_i - y_j)$, wegen $p \nmid y$ folgt $a_i \equiv a_j \bmod p$ und damit $\mathfrak{p}_i = \mathfrak{p}_j$.
4. Natürlich erhalten wir jetzt sofort eine Zerlegung
$$x + y\alpha = \pm\varepsilon^l \alpha^{u_0} \pi_1^{u_1} \ldots \pi_r^{u_r}$$
mit $l \in \mathbf{Z}$. Trivial ist auch, dass nach Zerlegung
$$l = m + 3n, \quad u_i = v_i + 3w_i \quad \text{mit} \quad m, v_i \in \{0, 1, 2\}$$
die Beziehung
$$x + y\alpha = \varepsilon^m \alpha^{u_0} \pi_1^{v_1} \ldots \pi_r^{v_r} \cdot (\pm\pi_1^{w_1} \ldots \pi_r^{w_r})^3$$
gilt. Normbildung liefert nun
$$x^3 + 3y^3 = \mathrm{N}(x + y\alpha) = 3^{u_0} p_1^{v_1} \ldots p_r^{v_r} \cdot (p_1^{w_1} \ldots p_r^{w_r})^3.$$
Wegen $p_i \neq p_j$ für $i \geq j$ ist klar, dass
$$3^{u_0} p_1^{v_1} \ldots p_r^{v_r}$$
der kubikfreie (positive) Anteil von $\mathrm{N}(x + y\alpha)$ ist. (Es kann durchaus $v_i = 0$ gelten.)
5. Da $d \geq 1$ kubikfrei sein sollte, folgt aus einer Beziehung $x^3 + 3y^3 + dz^3 = 0$, dass d der kubikfreie positive Teil von dz^3 und damit der von $x^3 + 3y^3 = \mathrm{N}(x + y\alpha)$ ist, wie behauptet. ■

Aus dem gerade bewiesenen Lemma ergibt sich unmittelbar der folgende Satz:

SATZ. *Seien $x, y, z \in \mathbf{Z}$ mit $\mathrm{ggT}(x, y, z) = 1$ und $d \geq 1$ kubikfrei mit $x^3 + 3y^3 + dz^3 = 0$. Ist*
$$d = 3^{u_0} p_1^{v_1} \ldots p_r^{v_r}$$
die Primfaktorzerlegung von d (mit $u_0 \in \{0, 1, 2\}$ und $v_i \in \{1, 2\}$), so ist $u_0 \in \{0, 1\}$ und es gibt Primideale $\mathfrak{p}_i = (\pi_i)$ vom Grad 1 mit $p_i \in \mathfrak{p}_i$ und $\mathrm{N}\pi_i = p_i$, dazu $m \in \{0, 1, 2\}$, $u, v, w \in \mathbf{Z}$ mit
$$x + y\alpha = \varepsilon^m \cdot \alpha^{u_0} \pi_1^{v_1} \ldots \pi_r^{v_r} \cdot (u\alpha^2 + v\alpha + w)^3.$$

Beispiel: Für $d = 67$ haben wir für $x^3 + 3y^3 + dz^3 = 0$ unter anderem die Lösungen $(x, y, z) = (4, 1, -1)$, $(5, -4, 1)$, $(13, -23, 8)$ gefunden. Wir zerlegen $x + y\alpha$, wie im letzten Satz angegeben:

(x, y, z)	$\mathrm{N}(x + y\alpha)$	$x + y\alpha$
$(4, 1, -1)$	67	π_{67a}
$(5, -4, 1)$	-67	$-\pi_{67c} = \pi_{67c} \cdot (-1)^3$
$(13, -23, 8)$	$-2^9 \cdot 67$	$-\varepsilon^{-4}\pi_2^9\pi_{67b} = \varepsilon^2\pi_{67b} \cdot (-\varepsilon^{-2}\pi_2^3)^3$
$(280, -131, -61)$	$61^3 \cdot 67$	$\pi_{61c}^3\pi_{67a} = \pi_{67a} \cdot \pi_{61c}^3$
$(925, -647, 68)$	$-2^6 \cdot 17^3 \cdot 67$	$-\varepsilon^{-1}\pi_2^6\pi_{17}^3\pi_{67b} = \varepsilon^2\pi_{67b} \cdot (-\varepsilon^{-1}\pi_2^2\pi_{17})^3$

Wir wollen nun mit Hilfe des letzten Satzes unsere ungelösten Fälle $d \in \{46, 55, 100\}$ angehen.

Fall $d = 46$: Wir nehmen an, es gäbe $x, y, z \in \mathbf{Z}$ mit $\mathrm{ggT}(x, y, z) = 1$ und
$$x^3 + 3y^3 + 46z^3 = 0.$$
Zunächst sieht man, dass
$$2 \nmid x, \quad 2 \nmid y, \quad 3 \nmid x, \quad 3 \nmid z$$

gelten müsste. Es ist $d = 46 = 2 \cdot 23$ und es gibt jeweils ein Primideal mit Norm 2 und mit Norm 23, also gäbe es nach dem letzten Satz $u, v, w \in \mathbf{Z}$ und $m \in \{0, 1, 2\}$ mit

$$x + y\alpha = \varepsilon^m \pi_2 \pi_{23} (u\alpha^2 + v\alpha + w)^3.$$

Wir setzen nun allgemein an für $u, v, w \in \mathbf{Z}$

$$x_m + y_m\alpha + g_m\alpha^2 = \varepsilon^m \pi_2 \pi_{23} (u\alpha^2 + v\alpha + w)^3$$

und erhalten durch Koeffizientenvergleich

$$\begin{aligned}
x_0 &= w^3 - 27uw^2 + 3v^3 + 18vw^2 + 18uvw - 27v^2w + 54u^2w + 54uv^2 + 9u^3 - 81u^2v \\
y_0 &= -3w^3 + 3vw^2 + 9u^2w + 18v^2w + 9uv^2 + 18uw^2 - 54uvw - 9v^3 + 54u^2v - 27u^3 \\
g_0 &= 3v^2w + 3uw^2 + 2w^3 - 9vw^2 + 9u^2v - 27u^2w + 36uvw + 6v^3 - 27uv^2 + 18u^3 \\
x_1 &= -11w^3 + 108uw^2 - 27vw^2 - 198uvw - 33v^3 + 108v^2w - 81uv^2 + 324u^2v - 99u^3 - 81u^2w \\
y_1 &= 12w^3 - 33vw^2 - 99u^2w - 27uw^2 - 27v^2w - 99uv^2 + 216uvw + 36v^3 + 108u^3 - 81u^2v \\
g_1 &= -33v^2w - 33uw^2 - 3w^3 + 36vw^2 - 99u^2v + 108u^2w - 9v^3 + 108uv^2 - 54uvw - 27u^3 \\
x_2 &= 58w^3 - 297uw^2 - 45vw^2 + 1044uvw + 174v^3 - 297v^2w - 135uv^2 + 522u^3 - 891u^2v - 135u^2w \\
y_2 &= -33w^3 + 174vw^2 + 522u^2w - 45uw^2 - 45v^2w + 522uv^2 - 594uvw - 99v^3 - 297u^3 - 135u^2v \\
g_2 &= 174v^2w + 174uw^2 - 5w^3 - 99vw^2 + 522u^2v - 297u^2w - 15v^3 - 297uv^2 - 90uvw - 45u^3
\end{aligned}$$

Für eine angenommene Lösung gilt $g_m(u, v, w) = 0$, aber $x_m(u, v, w) \not\equiv 0 \bmod 2$, $y_m(u, v, w) \not\equiv 0 \bmod 2$, $x_m(u, v, w) \not\equiv 0 \bmod 3$. Wir bemerken nun:

- Es ist
$$y_1 \equiv (u + v)(u + w)(v + w) \bmod 2,$$
d.h. für jede Wahl von $u, v, w \in \mathbf{Z}$ ist y_1 durch 2 teilbar, was bei einer Lösung nicht sein darf. Also ist der Fall $m = 1$ nicht möglich.
- $x_2 \equiv (u + v)(u + w)(v + w) \bmod 2$ zeigt analog, dass $m = 2$ nicht möglich ist.
- Wir haben
$$x_0 \equiv w^3 \bmod 3, \quad g_0 \equiv 2w^3 \bmod 3.$$
Bei einer Lösung müsste $g_0(u, v, w) = 0$ sein, also $w \equiv 0 \bmod 3$, was aber dann den Widerspruch $x_0 \equiv 0 \bmod 3$ liefern würde. Also ist auch $m = 3$ nicht möglich.

Damit haben wir gezeigt, dass für $d = 46$ keine nichttriviale Lösung der Gleichung $x^3 + 3y^3 + dz^3 = 0$ existiert.

Fall $d = 55$**:** Es gibt jeweils ein Primideal mit Norm 5 und mit Norm 11. Hätte $x^3 + 3y^3 + 55z^3 = 0$ eine Lösung mit $\mathrm{ggT}(x, y, z) = 1$, so könnten wir ansetzen

$$x_m + y_m\alpha + g_m\alpha^2 = \varepsilon^m \pi_5 \pi_{11} (u\alpha^2 + v\alpha + w)^3$$

und es gäbe ein $m \in \{0, 1, 2\}$ und $u, v, w \in \mathbf{Z}$ mit $g_m(u, v, w) = 0$ und $3 \nmid x_m(u, v, w)$. Durch Koeffizientenvergleich erhält man:

$$\begin{aligned}
x_0 &= 4w^3 + 12v^3 - 9vw^2 + 72uvw + 36u^3 - 27uv^2 - 27u^2w \\
y_0 &= 12vw^2 - 9v^2w + 36uv^2 - 9uw^2 + 36u^2w - 27u^2v \\
g_0 &= 12v^2w - w^3 + 12uw^2 + 36u^2v - 18uvw - 3v^3 - 9u^3 \\
x_1 &= -8w^3 - 144uvw + 54vw^2 - 24v^3 + 162u^2w + 162uv^2 - 27v^2w - 27uw^2 - 72u^3 - 81u^2v \\
y_1 &= -24vw^2 - 72uv^2 - 72u^2w + 54v^2w - 3w^3 + 54uw^2 + 162u^2v - 54uvw - 9v^3 - 27u^3 \\
g_1 &= -24uw^2 - 24v^2w + 6w^3 - 9vw^2 + 18v^3 + 108uvw - 72u^2v - 27uv^2 + 54u^3 - 27u^2w \\
x_2 &= 7w^3 + 126uvw - 180vw^2 + 21v^3 - 540u^2w - 540uv^2 + 216v^2w + 216uw^2 + 63u^3 + 648u^2v \\
y_2 &= 21vw^2 + 63uv^2 + 63u^2w - 180v^2w + 24w^3 - 180uw^2 - 540u^2v + 432uvw + 72v^3 + 216u^3 \\
g_2 &= 21uw^2 + 21v^2w - 20w^3 + 72vw^2 - 60v^3 - 360uvw + 63u^2v - 180u^3 + 216uv^2 + 216u^2w
\end{aligned}$$

Wir bemerken:

- $x_0 \equiv w^3 \bmod 3$, $g_0 \equiv 2w^3 \bmod 3$.
- $x_2 \equiv w^3 \bmod 3$, $g_2 \equiv w^3 \bmod 3$.

- g_1 hat keine Nullstelle modulo 25.

Wie im Fall $d = 46$ folgt, dass $x^3 + 3y^3 + 55z^3 = 0$ nur die triviale Lösung besitzt.

Fall $d = 100$: Es gibt jeweils nur ein Primideal mit Norm 2 und mit Norm 5. Daher können wir wie zuvor ansetzen:

$$x_m + y_m\alpha + g_m\alpha^2 = \varepsilon^m \pi_2^2 \pi_5^2 (u\alpha^2 + v\alpha + w)^3$$

und erhalten durch Koeffizientenvergleich

$$\begin{aligned}
x_0 &= -14w^3 - 252uvw - 81v^2w - 42v^3 + 117vw^2 - 81uw^2 - 126u^3 + 351u^2w + 351uv^2 - 243u^2v \\
y_0 &= -42vw^2 - 9w^3 + 117v^2w - 126uv^2 + 117uw^2 - 126u^2w - 27v^3 - 162uvw + 351u^2v - 81u^3 \\
g_0 &= 13w^3 - 27vw^2 - 42uw^2 - 42v^2w + 39v^3 - 81uv^2 - 126u^2v + 234uvw - 81u^2w + 117u^3 \\
x_1 &= w^3 + 18uvw + 513v^2w + 513uw^2 + 3v^3 - 360vw^2 + 9u^3 + 1539u^2v - 1080u^2w - 1080uv^2 \\
y_1 &= 57w^3 + 3vw^2 + 9u^2w + 9uv^2 + 171v^3 - 360uw^2 - 360v^2w + 1026uvw + 513u^3 - 1080u^2v \\
g_1 &= 3uw^2 - 40w^3 + 3v^2w + 171vw^2 - 720uvw - 120v^3 + 513u^2w + 513uv^2 + 9u^2v - 360u^3 \\
x_2 &= 169w^3 + 3042uvw - 2106v^2w + 507v^3 + 729vw^2 - 2106uw^2 + 1521u^3 + 2187u^2w + 2187uv^2 \\
&\quad -6318u^2v \\
y_2 &= 507vw^2 - 234w^3 + 729v^2w + 1521uv^2 + 729uw^2 + 1521u^2w - 702v^3 - 4212uvw + 2187u^2v \\
&\quad -2106u^3 \\
g_2 &= 81w^3 - 702vw^2 + 507uw^2 + 507v^2w + 243v^3 - 2106uv^2 + 1521u^2v + 1458uvw - 2106u^2w \\
&\quad +729u^3
\end{aligned}$$

Wie zuvor zeigen die Eigenschaften

- $x_0 \equiv (u+v)(u+w)(v+w) \bmod 2$,
- $y_2 \equiv (u+v)(u+w)(v+w) \bmod 2$,
- $x_1 \equiv w^3 \bmod 3$, $g_1 \equiv 2w^3 \bmod 3$,

dass die Gleichung $x^3 + 3y^3 + 100z^3 = 0$ nur die triviale Lösung besitzt.

Damit haben wir auch die noch offen gebliebenen Fälle $d \in \{46, 55, 100\}$ erledigt.

7. Überlegungen mit elliptischen Kurven

Wir wollen hier noch ein Kriterium angeben, wann die Gleichung

$$x^3 + 3y^3 + dz^3 = 0 \quad \text{mit} \quad \mathrm{ggT}(x, y, z) = 1$$

keine Lösung haben kann. Dieses Kriterium benutzt sogenannte elliptische Kurven. (Elliptische Kurven und das Kriterium finden sich bei J. W. S. Cassels, Lectures on Elliptic Curves, Cambridge University Press 1991.) Damit läßt sich die Nichtlösbarkeit der Gleichung in einigen Fällen unabhängig von den Kriterien der Algebraischen Zahlentheorie nachprüfen.

Sind $a, b \in \mathbf{Q}$ mit $4a^3 + 27b^2 \neq 0$, so definiert die Gleichung

$$y^2 = x^3 + ax + b$$

eine elliptische Kurve $E_{a,b}$ über $\mathbf{Q}$. Die Lösungen in rationalen Zahlen

$$E_{a,b}(\mathbf{Q}) = \{(x, y) \in \mathbf{Q} \times \mathbf{Q} : y^2 = x^3 + ax + b\} \cup \{O\}$$

werden mit Hinzunahme eines (unendlich fernen) Punkten O durch eine geometrisch definierte Addition zu einer endlich erzeugten abelschen Gruppe. Unter Zuhilfenahme analytischer Hilfsmittel und unter der Annahme verschiedener plausibler, aber unbewiesener Vermutungen (Vermutung von Birch und Swinnerton-Dyer, verallgemeinerte Riemannsche Vermutung) kann man manchmal die Struktur von $E_{a,b}(\mathbf{Q})$ explizit bestimmen. Für die nachfolgenden Fälle haben wir dazu das Maple-Paket APECS (Version 6.1) verwendet.

Gilt für $u, v, w \in \mathbf{Z} \setminus \{0\}$ die Gleichung

$$u^3 + 3v^3 + dw^3 = 0,$$

so folgt für

$$\begin{aligned} U &= -27v^9 + 27dv^6w^3 + 18d^2v^3w^6 + d^3w^9, \\ V &= 27v^9 + 54dv^6w^3 + 9d^2v^3w^6 - d^3w^9, \\ W &= 3uvw(9v^6 + 3dv^3w^3 + d^2w^6) = 3uvw\left(9(v^3 + \frac{1}{6}dw^3)^2 + \frac{3}{4}d^2w^6\right) \end{aligned}$$

die Gleichung

$$U^3 + V^3 + 3dW^3 = 0,$$

wobei hier $W \neq 0$ gilt. (Die Formeln für U, V, W werden geometrisch hergeleitet, die Gültigkeit kann man aber direkt nachprüfen.) Setzt man nun

$$x = -\frac{36dW}{U+V}, \quad y = \frac{108d(U-V)}{U+V},$$

so erhält man

$$\begin{aligned} x &= \frac{4(w^6d^2 + 3v^3dw^3 + 9v^6)}{u^2w^2v^2} = \frac{4(u^6 + 3u^3v^3 + 9v^6)}{u^2w^2v^2}, \\ y &= \frac{4(-dw^3 + 3v^3)(dw^3 + 6v^3)(2dw^3 + 3v^3)}{u^3v^3w^3} = \frac{4(u^3 - 3v^3)(u^3 + 6v^3)(2u^3 + 3v^3)}{u^3v^3w^3} \end{aligned}$$

und es gilt

$$y^2 = x^3 - 3888d^2.$$

Dies ist die Gleichung einer elliptischen Kurve und damit

$$(x, y) \in E_{0,-3888d^2}(\mathbf{Q}).$$

Beispiel: Für $d = 29$ finden wir für $u^3 + 3v^3 + 29w^3 = 0$ die Lösung $(u, v, w) = (10, -7, 1)$, die zu

$$x = \frac{1029841}{1225}, \quad y = \frac{1042214111}{42875}$$

mit $y^2 = x^3 - 112752$ führt.

Das folgende Kriterium ist nun offensichtlich:

Kriterium: Gilt für $d \geq 1$

$$E_{0,-3888d^2}(\mathbf{Q}) = 0,$$

so hat die Gleichung $x^3 + 3y^3 + dz^3 = 0$ nur die triviale Lösung in ganzen Zahlen.

Anwendung: Wir testen die Fälle

$$d \in \{20, 22, 34, 46, 50, 55, 58, 68, 85, 92, 100\},$$

die nach den Kongruenzüberlegungen noch offen waren. Mit APECS finden wir:

d	$E_{0,-3888d^2}(\mathbf{Q})$
20	0
22	0
34	0
46	0
50	0
55	0
58	0
68	0
85	0
92	0
100	0

Also sieht man auch mit Hilfe von elliptischen Kurven, dass in diesen Fällen die Gleichung $x^3+3y^3+dz^3 = 0$ nur die triviale Lösung in ganzen Zahlen besitzt.

Das folgende Beispiel zeigt, dass die Umkehrung des obigen Kriteriums nicht gilt.

Beispiel: Im Fall $d = 110$ findet man mit APECS, dass die Kurve

$$E_{0,-3888\cdot 110^2}: \quad y^2 = x^3 - 3888 \cdot 110^2$$

den nichttrivialen Punkt

$$(x, y) = (364, 1088)$$

besitzt, der dem nichttrivialen Punkt

$$(U, V, W) = (1621, 1349, -273) \quad \text{auf} \quad U^3 + V^3 + 3 \cdot 110 \cdot W^3 = 0$$

entspricht. Aber $x^3 + 3y^3 + 110z^3 = 0$ hat nur die triviale Lösung in ganzen Zahlen, wie man mit Mitteln der Algebraischen Zahlentheorie zeigen kann. (Für $K = \mathbf{Q}(\sqrt[3]{110})$ gilt $C\ell(\mathbf{Z}_K) \simeq Z_3 \oplus Z_3$, aber $\mathfrak{p}$ mit $\mathfrak{p}^3 = (3)$ ist kein Hauptideal.)

8. Weitere Kongruenzbetrachtungen

Wir haben früher Kongruenzkriterien für die Nichtlösbarkeit der Gleichung

$$x^3 + 3y^3 + dz^3 = 0 \quad \text{mit} \quad \mathrm{ggT}(x, y, z) = 1$$

hergeleitet. Wir wollen in diesem Abschnitt zeigen, dass es keine weiteren Kongruenzkriterien gibt, mit denen man die Nichtlösbarkeit der Gleichung zeigen kann.

Der folgende Satz zeigt, wann und wie man von einer Nullstelle eines Polynoms modulo p^m zu Nullstellen modulo p^n für alle $n \geq m$ kommt.

Satz. *Sei $f(x) \in \mathbf{Z}[x]$ und $w \in \mathbf{Z}$ mit*

$$f(w) \equiv 0 \bmod p^m, \quad v_p(f'(w)) = \ell, \quad m > 2\ell.$$

Definiert man eine Folge ganzer Zahlen $w_m, w_{m+1}, w_{m+2}, \ldots$ rekursiv durch $w_m = w$ und für $n \geq m$

$$z_n \equiv -\frac{(f(w_n)/p^n)}{(f'(w_n)/p^\ell)} \bmod p, \quad w_{n+1} = w_n + z_n p^{n-\ell},$$

dann gilt für alle $n \geq m$

$$f(w_n) \equiv 0 \bmod p^n, \quad v_p(f'(w_n)) = \ell, \quad w_n \equiv w \bmod p^{m-\ell}.$$

Beweis: Wir beweisen die Behauptung durch Induktion nach n mit $n \geq m$, wobei $n = m$ klar ist. Sei die Behauptung jetzt bereits für n gezeigt. Die Taylorreihe von $f(x)$ um w_n hat die Gestalt

$$f(x) = f(w_n) + f'(w_n)(x - w_n) + c_{n,2}(x - w_n)^2 + c_{n,3}(x - w_n)^3 + \ldots.$$

Nach Voraussetzung können wir schreiben

$$f(w_n) = a_n p^n, \quad f'(w_n) = b_n p^\ell \quad \text{mit } b_n \not\equiv 0 \bmod p \quad \text{und} \quad z_n \equiv -\frac{a_n}{b_n} \bmod p,$$

also gilt

$$\begin{aligned} f(x) &= a_n p^n + b_n p^\ell (x - w_n) + \sum_{i \geq 2} c_{n,i}(x - w_n)^i, \\ f(x)' &= b_n p^\ell + \sum_{i \geq 2} i c_{n,i}(x - w_n)^{i-1}. \end{aligned}$$

Benutzt man nun $n - 2\ell \geq 1$, $n - \ell \geq \ell + 1$ und $n \geq \ell$, so folgt

$$\begin{aligned}
f(w_{n+1}) &= a_n p^n + b_n p^\ell (w_{n+1} - w_n) + \sum_{i\geq 2} c_{n,i}(w_{n+1} - w_n)^i = \\
&= a_n p^n + b_n p^\ell \cdot z_n p^{n-\ell} + \sum_{i\geq 2} c_{n,i} z_n^i p^{i(n-\ell)} = \\
&= p^n(a_n + z_n b_n) + p^{n+1} \sum_{i\geq 2} c_{n,i} z_n^i p^{i(n-\ell)-n-1} = \\
&= p^n(a_n + z_n b_n) + p^{n+1} \sum_{i\geq 2} c_{n,i} z_n^i p^{(i-2)(n-\ell)+(n-2\ell)-1} \equiv 0 \bmod p^{n+1}, \\
f'(w_{n+1}) &= b_n p^\ell + \sum_{i\geq 2} i c_{n,i} z_n^{i-1} p^{(i-1)(n-\ell)} = b_n p^\ell + p^{n-\ell} \sum_{i\geq 2} i c_{n,i} z_n^{i-1} p^{(i-2)(n-\ell)} \equiv \\
&\equiv b_n p^\ell \bmod p^{\ell+1}, \\
v_p(f'(w_{n+1})) &= \ell,
\end{aligned}$$

und die Behauptung folgt. ■

Eine einfache Umformulierung des Satzes ist folgende:

FOLGERUNG. *Sei $f(x) \in \mathbf{Z}[x]$ ein Polynom und p eine Primzahl. Findet man ein $w \in \mathbf{Z}$ mit $f'(w) \neq 0$ und*

$$v_p(f(w)) \geq 2v_p(f'(w)) + 1,$$

so gibt es für alle $n \in \mathbf{N}$ ein $w_n \in \mathbf{Z}$ mit

$$f(w_n) \equiv 0 \bmod p^n \quad \text{und} \quad w_n \equiv w \bmod p.$$

Bemerkung: Die Bedingung $v_p(f(w)) \geq 2v_p(f'(w)) + 1$ kann man nicht abschwächen, da man leicht Beispiele angeben kann, wo $v_p(f(w)) = 2v_p(f'(w))$ gilt, $f(x)$ aber modulo hoher p-Potenzen keine Nullstelle besitzt.

FOLGERUNG. *Sei $F(x_1, \ldots, x_n) \in \mathbf{Z}[x_1, \ldots, x_n]$ ein homogenes Polynom vom Grad $d \geq 1$ und p eine Primzahl. Findet man $w_1, \ldots, w_n \in \mathbf{Z}$ mit $\mathrm{ggT}(w_1, \ldots, w_n) = 1$ und*

$$v_p(F(w_1, \ldots, w_n)) \geq 2\min(v_p(\frac{\partial F}{\partial x_1}(w_1, \ldots, w_n)), \ldots v_p(\frac{\partial F}{\partial x_n}(w_1, \ldots, w_n))) + 1,$$

wobei die rechte Seite endlich sein sollte, so gibt es für alle $k \geq 1$ Zahlen $z_1^{(k)}, \ldots, z_n^{(k)} \in \mathbf{Z}$ mit

$$F(z_1^{(k)}, \ldots, z_n^{(k)}) \equiv 0 \bmod p^k \quad \text{und} \quad \mathrm{ggT}(z_1^{(k)}, \ldots, z_n^{(k)}) = 1.$$

Beweis: Nach eventuellem Vertauschen von Indizes kann man

$$v_p(F(w_1, \ldots, w_n)) \geq 2v_p(\frac{\partial F}{\partial x_1}(w_1, \ldots, w_n)) + 1 \quad \text{und} \quad \frac{\partial F}{\partial x_1}(w_1, \ldots, w_n) \neq 0$$

annehmen. Wir setzen

$$f(x) = F(x, w_2, \ldots, w_n)$$

und erhalten

$$f'(x) = \frac{\partial F}{\partial x_1}(x, w_2, \ldots, w_n), \quad v_p(f(w_1)) \geq 2v_p(f'(w_1)) + 1.$$

Die vorangegangene Folgerung liefert nun eine Folge ganzer Zahlen $w_1^{(k)}$ mit $w_1^{(k)} \equiv w_1 \bmod p$ und

$$f(w_1^{(k)}) \equiv 0 \bmod p^k, \quad \text{also} \quad F(w_1^{(k)}, w_2, \ldots, w_n) \equiv 0 \bmod p^k.$$

Würde nun $p | \mathrm{ggT}(w_1^{(k)}, w_2, \ldots, w_n)$ gelten, so folgte wegen $w_1^{(k)} \equiv w_1 \bmod p$ auch der Widerspruch $p | \mathrm{ggT}(w_1, \ldots, w_n)$. Wir haben daher $\mathrm{ggT}(w_1^{(k)}, w_2, \ldots, w_n) \not\equiv 0 \bmod p$. Schreiben wir jetzt

$$(w_1^{(k)}, w_2, \ldots, w_n) = \mathrm{ggT}(w_1^{(k)}, w_2, \ldots, w_n) \cdot (z_1^{(k)}, z_2^{(k)}, \ldots, z_n^{(k)}),$$

so gilt

$$F(z_1^{(k)}, z_2^{(k)}, \ldots, z_n^{(k)}) \equiv 0 \bmod p^k \quad \text{und} \quad \mathrm{ggT}(z_1^{(k)}, z_2^{(k)}, \ldots, z_n^{(k)}) = 1,$$

was die Behauptung beweist. ■

Wir wollen das Ergebnis nun auf

$$F(x,y,z) = x^3 + 3y^3 + dz^3 \quad \text{mit} \quad \frac{\partial F}{\partial x}(x,y,z) = 3x^2, \quad \frac{\partial F}{\partial y}(x,y,z) = 9y^2, \quad \frac{\partial F}{\partial z}(x,y,z) = 3dz^2$$

anwenden.
Wir betrachten zuerst den Fall $p = 3$.

SATZ. *Sei $d \in \mathbf{N}$ kubikfrei. Dann gilt:*

1. *Ist $d \equiv 6, 9, 12, 15, 18, 21 \bmod 27$, so gibt es keine $x, y, z \in \mathbf{Z}$ mit*

$$x^3 + 3y^3 + dz^3 \equiv 0 \bmod 27 \quad \textit{und} \quad \mathrm{ggT}(x,y,z) = 1.$$

2. *Ist $d \not\equiv 6, 9, 12, 15, 18, 21 \bmod 27$, so gibt es für alle $k \geq 1$ Zahlen $x_k, y_k, z_k \in \mathbf{Z}$ mit*

$$x_k^3 + 3y_k^3 + dz_k^3 \equiv 0 \bmod 3^k \quad \textit{und} \quad \mathrm{ggT}(x_k, y_k, z_k) = 1.$$

Beweis: Der 1. Teil wurde bereits früher gezeigt. Wir müssen nur noch den 2. Teil zeigen. Wir schreiben $F(x,y,z) = x^3 + 3y^3 + dz^3$ und haben dann

$$\frac{\partial F}{\partial x} = 3x^2, \quad \frac{\partial F}{\partial y} = 3^2 y^2, \quad \frac{\partial F}{\partial x} = 3dz^2.$$

1. Fall: $d \equiv 3 \bmod 27$. Wir schreiben $d = 3 + 27t$ und wählen

$$x_0 = 0, \quad y_0 = 1, \quad z_0 = -1 + 3t + 9t^2 - 9t^3.$$

Dann ist

$$F(x_0, y_0, z_0) = -3^5 t^2(-1 + 2t + 16t^2 - 30t^3 - 96t^4 + 126t^5 + 135t^6 - 234t^7 + 81t^8) \equiv 0 \bmod 3^5$$

und

$$v_3\left(\frac{\partial F}{\partial y}(x_0, y_0, z_0)\right) = v_3(3^2 y_0^2) = 2, \quad \mathrm{ggT}(x_0, y_0, z_0) = 1,$$

die Voraussetzungen unseres Satzes sind damit erfüllt und liefern die Behauptung.
2. Fall: $d \equiv 24 \bmod 27$. Wir schreiben $d = -3 + 27t$ und wählen

$$x_0 = 0, \quad y_0 = 1, \quad z_0 = 1 + 3t - 9t^2 - 9t^3.$$

Dann ist

$$F(x_0, y_0, z_0) = -3^5 t^2(-1 - 2t + 16t^2 + 30t^3 - 96t^4 - 126t^5 + 135t^6 + 234t^7 + 81t^8) \equiv 0 \bmod 3^5$$

und

$$v_3\left(\frac{\partial F}{\partial y}(x_0, y_0, z_0)\right) = 2, \quad \mathrm{ggT}(x_0, y_0, z_0) = 1,$$

die Voraussetzungen sind erfüllt und liefern die Behauptung.
3. Fall: $d \not\equiv 0 \bmod 3$. Bei nachfolgender Wahl von x_0, y_0, z_0 in Abhängigkeit von $d \bmod 27$ gilt

$$F(x_0, y_0, z_0) \equiv 0 \bmod 3^3 \quad \text{und} \quad v_3\left(\frac{\partial F}{\partial x}(x_0, y_0, z_0)\right) = 1, \quad \mathrm{ggT}(x_0, y_0, z_0) = 1.$$

$d \bmod 27$	(x_0, y_0, z_0)
1	$(1,0,8)$
2	$(1,2,1)$
4	$(1,1,8)$
5	$(1,1,4)$
7	$(1,2,2)$
8	$(1,0,4)$
10	$(1,0,2)$
11	$(1,2,4)$
13	$(1,1,2)$
14	$(1,1,7)$
16	$(1,2,5)$
17	$(1,0,7)$
19	$(1,0,5)$
20	$(1,2,7)$
22	$(1,1,5)$
23	$(1,1,1)$
25	$(1,2,8)$
26	$(1,0,1)$

Die Voraussetzungen der letzten Folgerung sind also erfüllt und liefern die Behauptung. ■

Wir kommen nun zum Fall $p \neq 3$ und $p|d$.

SATZ. *Sei $d \in \mathbf{N}$ kubikfrei und $p \neq 3$ eine Primzahl mit $p|d$.*

1. *Hat die Kongruenz $t^3 \equiv 3 \bmod p$ keine Lösung, so gibt es auch keine $x, y, z \in \mathbf{Z}$ mit*
$$x^3 + 3y^3 + dz^3 \equiv 0 \bmod p^3 \quad \textit{und} \quad \mathrm{ggT}(x,y,z) = 1.$$
2. *Gibt es ein $t \in \mathbf{Z}$ mit $t^3 \equiv 3 \bmod p$, so existieren für alle $k \in \mathbf{N}$ Zahlen $x_k, y_k, z_k \in \mathbf{Z}$ mit*
$$x_k^3 + 3y_k^3 + dz_k^3 \equiv 0 \bmod p^k \quad \textit{und} \quad \mathrm{ggT}(x_k, y_k, z_k) = 1.$$

Beweis: Der 1. Teil wurde bereits vorher gezeigt. Wir beweisen den 2. Teil. Sei also $t \in \mathbf{Z}$ mit $t^3 \equiv 3 \bmod p$. Wegen $p \neq 3$ gilt $v_p(t) = 0$. Wir betrachten $F(x,y,z) = x^3 + 3y^3 + dz^3$ und erhalten

$$F(t,-1,0) = t^3 - 3 \equiv 0 \bmod p, \quad v_p\left(\frac{\partial F}{\partial x}(t,-1,0)\right) = v_p(3t^2) = 0, \quad \mathrm{ggT}(t,-1,0) = 1,$$

die Voraussetzung der letzten Folgerung sind also erfüllt und die Behauptung folgt. ■

Für den nächsten Fall benötigen wir ein (nichttriviales) Ergebnis, das auf F. K. Schmidt zurückgeht:

SATZ. *Sei p eine Primzahl und $f(x,y,z) \in \mathbf{F}_p[x,y,z]$ ein homogenes Polynom vom Grad 3, sodass*

$$\{(x_0,y_0,z_0) \in \overline{\mathbf{F}_p}^3 : \frac{\partial f}{\partial x}(x_0,y_0,z_0) = \frac{\partial f}{\partial y}(x_0,y_0,z_0) = \frac{\partial f}{\partial z}(x_0,y_0,z_0) = 0\} = \{(0,0,0)\}$$

gilt, wobei $\overline{\mathbf{F}_p}$ den algebraischen Abschluß von $\mathbf{F}_p$ bezeichnet. Dann gibt es $(x_0,y_0,z_0) \in \mathbf{F}_p^3$ mit

$$f(x_0,y_0,z_0) = 0 \quad \textit{und} \quad (x_0,y_0,z_0) \neq (0,0,0).$$

Wir können nun folgenden Satz beweisen:

SATZ. *Sei $d \in \mathbf{N}$ kubikfrei und p eine Primzahl mit $3d \not\equiv 0 \bmod p$. Dann gibt es für alle $k \geq 1$ Zahlen $x_k, y_k, z_k \in \mathbf{Z}$ mit $\mathrm{ggT}(x_k, y_k, z_k) = 1$ und*

$$x_k^3 + 3y_k^3 + dz_k^3 \equiv 0 \bmod p^k.$$

Beweis: Für $f(x,y,z) = x^3 + 3y^3 + dz^3 \in \mathbf{F}_p[x,y,z]$ gilt

$$\frac{\partial f}{\partial x} = 3x^2, \quad \frac{\partial f}{\partial y} = 9y^2, \quad \frac{\partial f}{\partial z} = 3dz^2$$

und damit

$$\begin{aligned} & \{(x_0,y_0,z_0) \in \overline{\mathbf{F}_p}^3 : \frac{\partial f}{\partial x}(x_0,y_0,z_0) = \frac{\partial f}{\partial y}(x_0,y_0,z_0) = \frac{\partial f}{\partial z}(x_0,y_0,z_0) = 0\} = \\ = \quad & \{(x_0,y_0,z_0) \in \overline{\mathbf{F}_p}^3 : 3x_0^2 = 9y_0^2 = 3dz_0^2 = 0\} = \{(0,0,0)\}. \end{aligned}$$

Nach dem vorangegangenen Satz gibt es somit $(x_0,y_0,z_0) \in \mathbf{F}_p^3 \setminus \{(0,0,0)\}$ mit $x_0^3 + 3y_0^3 + dz_0^3 = 0$. Wählt man für (x_0,y_0,z_0) einen Repräsentanten $(x_1,y_1,z_1) \in \mathbf{Z}^3$, so folgt $(x_1,y_1,z_1) \not\equiv (0,0,0) \bmod p$, also $\mathrm{ggT}(p,x_1,y_1,z_1) = 1$, und $x_1^3 + 3y_1^3 + dz_1^3 \equiv 0 \bmod p$. Teilt man eventuell $\mathrm{ggT}(x_1,y_1,z_1)$ aus x_1,y_1,z_1 heraus, so bleibt die Kongruenz weiter bestehen und es gilt $\mathrm{ggT}(x_1,y_1,z_1) = 1$. Da natürlich

$$\min(v_p(3x_1^2), v_p(9y_1^2), v_p(3dz_1^2)) = 0$$

gilt, kann man sich wie zuvor gezeigt leicht Lösungen modulo p^k konstruieren. ■

Wir fassen zusammen:

SATZ. *Sei $d \in \mathbf{N}$ kubikfrei.*

1.
   - *Ist $d \equiv 6,9,12,15,18,21 \bmod 27$, so gilt für alle $x,y,z \in \mathbf{Z}$ mit $\mathrm{ggT}(x,y,z) = 1$*
   $$x^3 + 3y^3 + dz^3 \not\equiv 0 \bmod 27.$$
   - *Ist p ein Primteiler von d und hat die Kongruenz $t^3 \equiv 3 \bmod p$ keine Lösung, so gilt für alle $x,y,z \in \mathbf{Z}$ mit $\mathrm{ggT}(x,y,z) = 1$*
   $$x^3 + 3y^3 + dz^3 \not\equiv 0 \bmod p^3.$$

2.
   - *Ist $d \not\equiv 6,9,12,15,18,21 \bmod 27$ und*
   - *gibt es für alle Primteiler p von d ein $t_p \in \mathbf{Z}$ mit $t_p^3 \equiv 3 \bmod p$,*

   so gibt es für alle $M \in \mathbf{N}$ ganze Zahlen $x_M, y_M, z_M \in \mathbf{Z}$ mit
   $$x_M^3 + 3y_M^3 + dz_M^3 \equiv 0 \bmod M \quad \text{und} \quad \mathrm{ggT}(x_M, y_M, z_M) = 1.$$

Beweis: Der erste Teil wurde bereits gezeigt. Den zweiten Teil haben wir bereits im Fall $M = p^m$ gezeigt, der Allgemeinfall folgt mit dem chinesischen Restesatz. ■

Bemerkung: Der vorangegangene Satz gibt ein genaues Kriterium, wann man die Nichtlösbarkeit der Gleichung $x^3 + 3y^3 + dz^3 = 0$ mit Kongruenzbetrachtungen zeigen kann.

9. Zusammenfassung

Wir stellen nun die Ergebnisse für die Gleichungen $x^3 + 3y^3 + dz^3 = 0$ mit $1 \le d \le 100$ zusammen, wobei folgende Bezeichnungen verwendet werden:

- nkf: d ist nicht kubikfrei.
- Kp: die Nichtlösbarkeit folgt durch eine Kongruenzbetrachtung modulo p^3.
- AZT1: die Nichtlösbarkeit wurde mit dem Klassengruppenkriterium gezeigt.
- AZT2: die Nichtlösbarkeit wurde mit Arithmetik in $\mathbf{Q}(\sqrt[3]{3})$ gezeigt.
- (x,y,z) gibt eine Lösung an. Es sind alle (normierten) Lösungen mit $|x|, |y| \le 4000$ aufgelistet.

Wir haben also für alle kubikfreien d's mit $1 \le d \le 100$ entscheiden können, ob die Gleichung $x^3 + 3y^3 + dz^3 = 0$ eine nichttriviale Lösung besitzt oder nicht besitzt.

d	
1	(1,0,-1)
2	(1,-1,1), (5,1,-4), (655,-253,-488)
3	(0,1,-1), (3,-2,-1), (3,-1,-2), (21,-20,17), (21,17,-20), (1314,-919,271), (1314,271,-919)
4	(1,1,-1), (7,-5,2), (2849,-1555,-1436)
5	(2,-1,-1), (4,13,-11)
6	K3
7	K7
8	nkf
9	K3
10	(1,-3,2), (11,-3,-5), (13,-9,-1), (161,237,-164)
11	(2,1,-1), (28,-19,-5)
12	K3
13	K13
14	K7
15	K3
16	nkf
17	(4,-3,1), (392,-141,-145)
18	K3
19	K19
20	AZT1, EK
21	K3, K7
22	AZT1, EK
23	(1,-2,1), (47,44,-25)
24	nkf
25	(1,2,-1), (49,-52,23)
26	K13
27	nkf
28	K7
29	(10,-7,1)
30	(3,1,-1), (33,-19,-8)
31	K31
32	nkf
33	K3
34	AZT1, EK
35	K7
36	K3
37	K37
38	K19
39	K3, K13
40	nkf
41	(16,7,-5)
42	K3, K7
43	K43
44	(5,-3,-1), (191,-141,32), (185,-507,206), (557,-387,29)
45	K3
46	AZT2, EK
47	(1,5,-2), (751,-1885,748)
48	nkf
49	K7
50	AZT1, EK

d	
51	(3,2,-1), (9,-11,4), (6,-13,5), (75,-52,-1)
52	K13
53	(7,3,-2), (3535,-2301,-524)
54	nkf
55	AZT2, EK
56	nkf
57	K19
58	AZT1, EK
59	(17,-16,5)
60	K3
61	(4,-1,-1), (23,-29,10), (55,-82,29), (232,125,-67), (1723,-1198,89)
62	K31
63	K3, K7
64	nkf
65	K13
66	K3
67	(4,1,-1), (5,-4,1), (13,-23,8), (280,-131,-61), (925,-647,68), (1295,-232,-317), (2909,-199,-716)
68	AZT1, EK
69	K3
70	K7
71	(250,-231,67)
72	nkf
73	(2,-3,1), (19,-9,-4), (308,195,-89), (347,-24,-83), (409,-282,-25)
74	K37
75	K3
76	K19
77	K7
78	K13
79	K79
80	nkf
81	nkf
82	(1,3,-1), (163,-249,80)
83	(1867,-49,-428)
84	K7
85	AZT1, EK
86	K43
87	K3
88	nkf
89	(2,3,-1), (340,-291,73)
90	K3
91	K7, K13
92	AZT1, EK
93	K3, K31
94	(67,-41,-10), (73,-11,-16), (103,139,-46)
95	K19
96	nkf
97	K97
98	K7
99	K3
100	AZT2, EK

KAPITEL 11

Das Zahlkörpersieb — Number Field Sieve (NFS)

1. Einführung

Grundlegend für die Zahlentheorie ist die Tatsache, dass sich jede natürliche Zahl N eindeutig als Produkt von Primzahlen schreiben läßt:

$$N = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}.$$

Beispiel: Die 10 größten Zahlen mit 40 bzw. 50 Dezimalstellen haben folgende Primfaktorzerlegungen:

$10^{40}-1 = 3^2 \cdot 11 \cdot 41 \cdot 73 \cdot 101 \cdot 137 \cdot 271 \cdot 1676321 \cdot 5964848081 \cdot 27961 \cdot 9091 \cdot 3541$ (0.28 sec)

$10^{40}-2 = 2 \cdot 52853032071556332079876487 \cdot 94601951941577$ (328.73 sec)

$10^{40}-3 = 13 \cdot 569085301052150111 \cdot 5853526052603 \cdot 4787 \cdot 48239$ (11.46 sec)

$10^{40}-4 = 2^2 \cdot 3 \cdot 7 \cdot 9131647862473 \cdot 106852828571 \cdot 155977777 \cdot 782209$ (1.98 sec)

$10^{40}-5 = 5 \cdot 31 \cdot 645161290322580645161290322580645161 29$ (0.03 sec)

$10^{40}-6 = 2 \cdot 19 \cdot 17121977485637 \cdot 68264114230454681951 \cdot 225149$ (46.43 sec)

$10^{40}-7 = 3 \cdot 3333333333333333333333333333333333333331$ (0.05 sec)

$10^{40}-8 = 2^3 \cdot 11840289566799559 \cdot 105571742392604012369161$ (235.62 sec)

$10^{40}-9 = 23 \cdot 373 \cdot 155773 \cdot 1721071782307 \cdot 265883581 \cdot 19031 \cdot 859249$ (3.77 sec)

$10^{40}-10 = 2 \cdot 3^3 \cdot 5 \cdot 37 \cdot 53 \cdot 79 \cdot 900900900900990990990991 \cdot 265371653$ (4.76 sec)

$10^{50}-1 = 3^2 \cdot 11 \cdot 41 \cdot 251 \cdot 271 \cdot 78875943472201 \cdot 182521213001 \cdot 5051 \cdot 9091 \cdot 21401 \cdot 25601$ (2.18 sec)

$10^{50}-2 = 2 \cdot 7 \cdot 17163266078098477799929 69 \cdot 42512082058217 \cdot 3277033 \cdot 29873$ (149.30 sec)

$10^{50}-3 = 44848033061277421 \cdot 41488023184722935209 \cdot 3674333699 \cdot 14627$ (267.21 sec)

$10^{50}-4 = 2^2 \cdot 3 \cdot 29 \cdot 59 \cdot 263 \cdot 958989105371471 \cdot 921953189 \cdot 88369891 \cdot 1542089 \cdot 153701$ (18.76 sec)

$10^{50}-5 = 5 \cdot 1259 \cdot 46320316841 \cdot 115998774646597401239 \cdot 1164438729401 \cdot 2539$ (52.07 sec)

$10^{50}-6 = 2 \cdot 23 \cdot 2987996491 \cdot 337699326627790407766486 09 \cdot 739565251 \cdot 29131$ (52.93 sec)

$10^{50}-7 = 3 \cdot 3333333333333333333333333333333333333333333333333333331$ (0.11 sec)

$10^{50}-8 = 2^3 \cdot 659156682698499622938 79 \cdot 4626413859859721 \cdot 11857073 \cdot 3457$ (388.70 sec)

$10^{50}-9 = 7 \cdot 13 \cdot 100308773475776339 \cdot 14285714285714285714285 71 \cdot 7668629$ (1105.24 sec)

$10^{50}-10 = 2 \cdot 3^2 \cdot 5 \cdot 239 \cdot 19767301445981909635680 23014679333 \cdot 505885997 \cdot 4649$ (0.07 sec)

(Die Faktorisierungen wurden mit Maple 8.0 auf einer Sun-Workstation mit 1024 MB RAM erstellt, worauf sich auch auf die angegebenen Rechenzeiten beziehen.)

C. F. Gauss bemerkte 1801 in seinen Disquisitiones Arithmeticae (Art. 329):
Dass die Aufgabe, die Primzahlen von den zusammengesetzten zu unterscheiden und letztere in ihre Primfactoren zu zerlegen, zu den wichtigsten und nützlichsten der gesamten Arithmetik gehört und die Bemühungen und den Scharfsinn sowohl der alten wie auch der neueren Geometer in Anspruch genommen hat, ist so bekannt, dass es überflüssig wäre, hierüber viele Worte zu verlieren. ...
... ausserdem aber dürfte es die Würde der Wissenschaft erheischen, alle Hülfsmittel zur Lösung jenes so eleganten und berühmten Problems fleissig zu vervollkommnen.
(Carl Friedrich Gauss, Untersuchungen über höhere Arithmetik. (Disquisitiones Arithmeticae. ...) Deutsch herausgegeben von H. Maser, Berin, 1889.)

Version vom 26.2.2003

Die Schwierigkeit der Faktorzerlegung kann man auch daran erkennen, dass die Firma RSA Data Security, Inc. für die Faktorisierung sogenannter RSA Challenge Numbers Geldpreise ausgesetzt sind. Die kleinste derartige Zahl ist zur Zeit RSA-576 (mit 576 Bits bzw. 174 Dezimalstellen):

$$\begin{aligned}\text{RSA-576} \;=\; & 188198812920607963838697239461650439807163563379417382700763356422988\backslash\\ & 8597152346654853190606065047430453173880113033967161996923212057340318\backslash\\ & 7955065699622130516875930765025705 9.\end{aligned}$$

Wer als erster eine Faktorisierung einreicht, erhält \$10000.
Die größte RSA Challenge Number ist zur Zeit RSA-2048 (2048 Bits und 617 Dezimalstellen):

$$\begin{aligned}\text{RSA-2048} \;=\; & 25195908475657893494027183240048398571429282126204032027777137836043 66\backslash\\ & 20207075955562640185258807844069182906412495150821892985591491761845 02\backslash\\ & 80848912007284499268739280728777673597141834727026189637501497182469 11\backslash\\ & 65077613379859095700097330459748808428401797429100642458691817195118 74\backslash\\ & 61215151726546322822168699875491824224336372590851418654620435767984 23\backslash\\ & 38718477444792073993423658482382428119816381501067481045166037730605 62\backslash\\ & 01619676256133844143603833904414952634432190114657544454178424020924 61\backslash\\ & 65157233507787077498171257724679629263863563732899121548314381678998 85\backslash\\ & 04044536402352738195137863656439121201039712282212072035 7\end{aligned}$$

Durch Faktorisierung dieser Zahl kann \$200000 verdienen.
(Die Sicherheit des RSA-Kryptosystems beruht auf der Schwierigkeit, größere Zahlen in angemessener Zeit zu faktorisieren.)

Die Primfaktorzerlegung wird heutzutage in verschiedene Einzelaufgaben aufgeteilt:

1. **Kleine Teiler:** Man entfernt aus der zu faktorisierenden Zahl N zunächst alle kleinen Teiler, d.h. man teilt aus N z.B. alle Teiler $\leq 10^5$ heraus.
2. **Primzahltests:** Ein Primzahltest sollte schnell und einfach das Ergebnis liefern, ob eine Zahl N *zusammengesetzt* oder *wahrscheinlich prim* ist. Beispiele: Fermatscher Primzahltest, Solovay-Strassen-Primzahltest, Miller-Rabin-Test, ...
3. **Primzahlbeweise:** Ein Primzahlbeweis soll zeigen, dass eine (wahrscheinlich prime) Zahl tatsächlich eine Primzahl ist. Primzahlbeweise sind meist komplexer und aufwendiger als Primzahltests. Beispiele: Jacobi-Summen-Test, ECPP (elliptic curve primality proving), ...
4. **Faktorisierungsmethoden:** Hierbei versucht man, eine nichttriviale Faktorisierung $N = N_1 N_2$ einer (nach einem Primzahltest als zusammengesetzt erkannten) Zahl N (ohne kleine Teiler) zu finden. Beispiele: Pollardsche ρ-Methode, QS (quadratic sieve), MPQS (multiple polynomial quadratic sieve), NFS (number field sieve), ECM (elliptic curve method), ...

2. Elementare Suche nach Teilern

$N \in \mathbf{N}$ habe die Primfaktorzerlegung

$$N = p_1^{e_1} \dots p_r^{e_r} \quad \text{mit Primzahlen} \quad p_1 < \dots < p_r \quad \text{und} \quad e_1, \dots, e_r \geq 1.$$

- Dann ist p_{i+1} die kleinste natürliche Zahl t, die $\frac{N}{p_1^{e_1} \dots p_i^{e_i}}$ teilt, d.h.

$$p_{i+1} = \min\{t > p_i : t | \frac{N}{p_1^{e_1} \dots p_i^{e_i}}\}.$$

- Außerdem sieht man sofort

$$p_{i+1} > \sqrt{\frac{N}{p_1^{e_1} \dots p_i^{e_i}}} \quad \Longrightarrow \quad i+1 = r, \quad e_r = 1.$$

Solche Eigenschaften werden bei der **naiven Faktorisierungsmethode** benutzt, bei der man nacheinander testet, ob eine der Zahlen 2, 3, 5, 7, ... die Zahl N teilt, und sie dann gegebenenfalls herausteilt. Man muss dabei nur die Teiler $\leq \sqrt{N}$ (bzw. $\leq \sqrt{\frac{N}{p_1^{e_1}\cdots p_i^{e_i}}}$, wenn $p_1^{e_1}\ldots p_i^{e_i}$ die bereits gefundenen Faktoren sind) betrachten, der Rest ist dann nämlich 1 oder ein Primteiler von N.

Die naive Faktorisierungsmethode ist deterministisch, allerdings wächst die Schrittzahl (durchschnittlich) mindestens wie $\sqrt{N}$. Bräuchte man mit diesem Verfahren zum Faktorisieren von 50-stelligen Zahlen durchschnittlich 1 Sekunde, so für 60-stellige Zahlen mehr als 27 Stunden, für 70-stellige Zahlen mehr als 317 Jahre. Es ist klar, daß man mit dieser Faktorisierungsmethode schnell an Grenzen stößt.

Bevor man allerdings aufwendigere Verfahren zur Faktorisierung einer natürlichen Zahl N heranzieht, sollte man auf jeden Fall die **kleinen Teiler** herausteilen. (Dabei hängt 'klein' von den zur Verfügung stehenden rechnerischen Möglichkeiten ab.) Im allgemeinen haben nämlich zufällig gewählte große Zahlen kleine Teiler. Bezeichnet $a(T)$ den Anteil der natürlichen Zahlen, die einen Primteiler $\leq T$ haben, genauer

$$a(T) = \lim_{M\to\infty} \frac{1}{M}\#\{1 \leq N \leq M : N \text{ hat einen Primteiler } \leq T\},$$

so erhält man die Tabelle:

T	20	100	1000	10000	100000	1000000
$a(T)$	82.90%	87.97%	91.90%	93.91%	95.12%	95.94%

(Bereits Gauss bemerkte, dass ungefähr $83\% \approx \frac{5}{6}$ aller natürlichen Zahlen einen Primteiler ≤ 20 haben: *... weil sich, allgemein zu reden, unter sechs Zahlen kaum eine findet, die nicht durch eine der Zahlen 2, 3, 5, ..., 19 teilbar wäre.* (Dies findet sich ebenfalls in Art. 329 der Disquisitiones Arithmeticae.))

Daher teilt man aus einer zu faktorisierenden Zahl N zunächst alle kleinen Teiler heraus, man zerlegt also z.B.

$$N = 2^{e_2}\cdot 3^{e_3}\cdot\cdots\cdot 9973^{e_{9973}}\cdot N_1 \quad \text{oder} \quad N = 2^{e_2}\cdot 3^{e_3}\cdot\cdots\cdot 999983^{e_{999983}}\cdot N_1$$

und weiß dann, dass N_1 keinen Teiler ≤ 10000 bzw. 1000000 hat.

Ein anderer elementaren Faktorisierungsversuch ist die Fermatsche Faktorisierungsmethode. Ist N eine ungerade Zahl mit einer Faktorisierung $N = N_1N_2$, so gilt

$$N = N_1N_2 = (\frac{N_1+N_2}{2})^2 - (\frac{N_1-N_2}{2})^2,$$

also hat man

$$(\frac{N_1+N_2}{2})^2 - N = (\frac{N_1-N_2}{2})^2 \quad \text{und} \quad \frac{N_1+N_2}{2} \geq \lceil\sqrt{N}\rceil.$$

Damit erhält man die

Fermatsche Faktorisierungsmethode: Wähle $x \geq \lceil\sqrt{N}\rceil$, berechne $y_2 = x^2 - N$. Teste, ob y_2 ein Quadrat ist. Wenn ja, so erhält man mit $y = \sqrt{y_2}$ die Zerlegung $N = x^2 - y^2 = (x+y)(x-y)$.
Man probiert dies aus für

$$x = \lceil\sqrt{N}\rceil, \quad \lceil\sqrt{N}\rceil + 1, \quad \lceil\sqrt{N}\rceil + 2, \quad \ldots$$

Hat N eine Faktorisierung $N = N_1N_2$ mit $N_1 \approx N_2$, so kann man hoffen, sie mit der Fermatschen Methode zu finden.

Beispiel: Die folgenden Zahlen p und q sind Primzahlen mit 40 Dezimalstellen, die in den ersten 19 Dezimalstellen überein. Die Primfaktorzerlegung der Zahl $N = pq$ wird mit der Fermatschen Faktorisierungsmethode gleich beim ersten Schritt gefunden.

$$\begin{aligned}
p &= 8736457823642378642543234523453453452509\\
q &= 8736457823642378642807604836819268089003\\
N &= 76325695304282127165672234149236448043093990090524844325761330927581861045658527\\
\lceil\sqrt{N}\rceil &= 8736457823642378642675419680136360770756\\
\frac{p+q}{2} &= 8736457823642378642675419680136360770756
\end{aligned}$$

3. Primzahltests

Kann man einer natürlichen Zahl N leicht ansehen, ob sie prim ist oder nicht? Ein Kriterium liefert der folgende einfach zu beweisende Satz:

SATZ. *Ist N eine natürliche Zahl, so gilt:*

$$N \text{ ist Primzahl} \quad \Longleftrightarrow \quad \mathrm{ggT}(1 \cdot 2 \cdot 3 \cdot \cdots \cdot (N-1), N) = \mathrm{ggT}((N-1)! \bmod N, N) = 1.$$

Leider ist der Satz praktisch nutzlos, da man keine Methode kennt, um $(N-1)! \bmod N$ schnell zu berechnen.
Der Satz von Wilson liefert noch eine genauere Aussage, die ohne ggT-Bildung auskommt:

$$N \text{ ist Primzahl} \quad \Longleftrightarrow \quad (N-1)! \equiv -1 \bmod N.$$

(Man kann sich auch leicht überlegen, dass sich eine natürliche Zahl N schnell faktorisieren ließe, könnte man für alle natürlichen Zahlen $m \leq N$ den Wert $m! \bmod N$ schnell gerechnen.)

Während sich Fakultäten modulo N nicht schnell berechnen lassen, kann man schnell modulo N potenzieren mit der sogenannten

Square-and-multiply-Methode: Wir wollen für $a \in \mathbf{Z}$, $d, N \in \mathbf{N}$ die Potenz $a^d \bmod N$ berechnen.

- Ist
$$d = d_0 + d_1 \cdot 2 + \cdots + d_r \cdot 2^r \text{ mit } d_i \in \{0, 1\}$$
die Binärentwicklung von d, so gilt
$$a^d \equiv \prod_{j=0}^{r} (a^{2^j})^{d_j} \bmod N$$
und $r = \lfloor \log_2 d \rfloor$, falls $d_r \neq 0$ ist.
- Definiert man für $i = 0, 1, 2, \ldots, r$
$$c_i = \lfloor \frac{d}{2^i} \rfloor = d_i + d_{i+1} \cdot 2 + \cdots + d_r \cdot 2^{r-i}, \quad x_i \equiv a^{2^i} \bmod N, \quad y_i \equiv \prod_{j=0}^{i} (a^{2^j})^{d_j} \bmod N,$$
so sieht man sofort, dass c_i, d_i, x_i und y_i durch folgende Rekursionsformeln gegeben werden
$$c_0 = d, \quad d_0 \equiv c_0 \bmod 2, \quad x_0 = a, \quad y_0 = a^{d_0}$$
und
$$c_i = \lfloor \frac{c_{i-1}}{2} \rfloor, \quad d_i \equiv c_i \bmod 2, \quad x_i \equiv x_{i-1}^2 \bmod N, \quad y_i \equiv y_{i-1} x_i^{d_i} \bmod N.$$
Man hat dann
$$y_r \equiv a^d \bmod N.$$
- Man überlegt sich schnell, dass man mit den obigen Rekursionsformeln (wegen $d_i \in \{0, 1\}$)
$$\lfloor \log_2 d \rfloor \leq \log_2 d < 3.33 \log_{10} d$$
Quadratbildungen und höchstens soviele Multiplikationen modulo N braucht. Die ist ein schnelles Verfahren.
- Wir geben noch folgenden einfachen expliziten Algorithmus an:
Algorithmus: Für $N, d \in \mathbf{N}$ und $a \in \mathbf{Z}$ soll $a^d \bmod N$ berechnet werden.
  1. Setze $c := d$, $x := a$. Setze $y := 1$, falls $c \equiv 0 \bmod 2$, sonst $y := a$.
  2. Setze $c := \lfloor \frac{c}{2} \rfloor$, $x := x^2 \bmod N$.
  3. Ist $c \equiv 1 \bmod 2$, setze $y := xy \bmod N$.
  4. Ist $c = 1$, gib y als Ergebnis aus und beende das Verfahren, sonst gehe zu Schritt 2.

  Man kann den Algorithmus auch leicht modifizieren um in einer multiplikativ bzw. additiv geschriebenen Gruppe G und $a \in G$, $d \in \mathbf{N}$ die Potenz a^d bzw. das Produkt $d \cdot a$ zu berechnen.

Beispiel: Berechnung von $2^{19487190} \bmod 19487191$:

i	c_i	d_i	x_i	y_i
0	19487190	0	2	1
1	9743595	1	4	4
2	4871797	1	16	64
3	2435898	0	256	64
4	1217949	1	65536	4194304
5	608974	0	7785276	4194304
6	304487	1	18895842	12707193
7	152243	1	15484497	5384192
8	76121	1	9279458	12472249
9	38060	0	17081390	12472249
10	19030	0	7339882	12472249
11	9515	1	8253526	16737979
12	4757	1	19392852	2885849
13	2378	0	13687825	2885849
14	1189	1	14850112	2726202
15	594	0	3820594	2726202
16	297	1	19119904	11781179
17	148	0	9404267	11781179
18	74	0	18378282	11781179
19	37	1	17930990	17521259
20	18	0	10378067	17521259
21	9	1	12051623	11407692
22	4	0	16255176	11407692
23	2	0	7096585	11407692
24	1	1	10960476	1

Ergebnis: $2^{19487190} \equiv 1 \bmod 19487191$.

Ausgangspunkt ist folgender Satz:

SATZ (Kleiner Satz von Fermat). *Ist p eine Primzahl und $a \in \mathbf{Z}$ mit* $\mathrm{ggT}(a,p) = 1$, *so gilt*

$$a^{p-1} \equiv 1 \bmod p.$$

Beweis: $\mathbf{Z}/p\mathbf{Z}$ ist ein endlicher Körper mit p Elementen, die multiplikative Gruppe hat $p-1$ Elemente. Also gilt für $\overline{a} \in \mathbf{Z}/p\mathbf{Z}$

$$\overline{a}^{p-1} = \overline{1},$$

was sich sofort in die behauptete Kongruenz übersetzt. ■

Bemerkungen:

1. Findet man zu N ein a mit $\mathrm{ggT}(a,N) = 1$ und $a^{N-1} \not\equiv 1 \bmod N$, so ist N sicher keine Primzahl.
2. Die Umkehrung des kleinen Satzes von Fermat gilt nicht. So gibt es zusammengesetzte Zahlen N mit $\mathrm{ggT}(a,N) = 1$ und $a^{N-1} \equiv 1 \bmod N$. Solche Zahlen nennt man auch Fermatsche Pseudoprimzahlen zur Basis a. Sie verhalten sich im kleinen Satz von Fermat wie Primzahlen, sind aber keine Primzahlen.
3. Die einzigen Fermatschen Pseudoprimzahlen N zur Basis 2 mit $N \leq 1000$ sind
$$341 = 11 \cdot 31, \quad 561 = 3 \cdot 11 \cdot 17, \quad 645 = 3 \cdot 5 \cdot 43.$$
4. Im Vergleich zu (echten) Primzahlen gibt es allerdings nur verhältnismäßig wenige Pseudoprimzahlen. Erfüllt also eine zufällig gewählte Zahl N die Bedingung $a^{N-1} \equiv 1 \bmod N$, so ist es wahrscheinlicher, dass sie eine Primzahl ist, als dass sie eine Pseudoprimzahl zur Basis a ist.

Fermatscher Primzahltest: Sei N eine natürliche Zahl (ohne kleine Teiler), $a \geq 2$ (mit $\mathrm{ggT}(a,N) = 1$), z.B. $a = 2$.

- Gilt $a^{N-1} \not\equiv 1 \bmod N$, so ist N *zusammengesetzt.*

- Gilt $a^{N-1} \equiv 1 \bmod N$, so ist N *wahrscheinlich prim.* (Genauer: N ist eine Primzahl oder eine Fermatsche Pseudoprimzahl zur Basis a.)

Da man $a^{N-1} \bmod N$ schnell berechnen kann, erhält man so einen einfachen und schnellen Test dafür, ob eine natürliche Zahl N zusammengesetzt oder wahrscheinlich prim ist.

Bemerkungen:

1. Ähnlich wie der Fermatsche Primzahltest, sind der Solovay-Strassen-Test und der Miller-Rabin-Test aufgebaut.
2. Computeralgebrasysteme begnügen sich im allgemeinen mit wahrscheinlichen Primzahlen. Liefert z.B. die Maple-Funktion 'isprime(N)' für eine große Zahl den Wert 'true', so ist N wahrscheinlich prim, im strengen Sinn ist nicht bewiesen worden, dass N tatsächlich eine Primzahl ist.
3. Es gibt auch zusammengesetzte natürliche Zahlen N, für die
$$a^{N-1} \equiv 1 \bmod N \quad \text{für alle } a \in \mathbf{N} \text{ mit } \mathrm{ggT}(a, N) = 1$$
gilt. Man nennt solche Zahlen *Carmichael-Zahlen*. Die kleinste Carmichael-Zahl ist $561 = 3 \cdot 11 \cdot 17$.

Beispiel: Die größte 1000-stellige Dezimalzahl mit $2^{N-1} \equiv 1 \bmod N$ ist
$$N = 10^{1000} - 1769.$$
Es gilt auch noch $a^{N-1} \equiv 1 \bmod N$ für $a = 2, 3, \ldots, 10000$.

4. Primzahlbeweise

Hat eine natürliche Zahl $N \geq 2$ keinen Teiler t mit $2 \leq t \leq \sqrt{N}$, so ist N eine Primzahl. Damit kann man zeigen, dass eine Zahl N eine Primzahl ist, allerdings wächst die Schrittzahl wie $\sqrt{N}$, sodass das Verfahren für größere N nicht mehr praktikabel ist. Ein weiterer Nachteil besteht darin, dass man einen solchen Primzahlbeweis nur nachprüfen kann, wenn man ihn selbst nochmals durchführt.
Wir wollen hier eine andere Beweismethode vorstellen, die die Gruppenstruktur von $(\mathbf{Z}/p\mathbf{Z})^*$ benutzt.

LEMMA. *Sei N eine natürliche Zahl und*
$$N - 1 = q_1^{e_1} \ldots q_r^{e_r}$$
die Primfaktorzerlegung von $N-1$. Ist a eine natürliche Zahl mit
$$a^{N-1} \equiv 1 \bmod N, \quad a^{\frac{N-1}{q_i}} \not\equiv 1 \bmod N \text{ für } i = 1, \ldots, r,$$
so ist N eine Primzahl.

Beweis: Die Voraussetzung bedeutet, dass das Element $\overline{a} \in \mathbf{Z}/N\mathbf{Z}$ in der multiplikativen Gruppe $(\mathbf{Z}/N\mathbf{Z})^*$ genau Ordnung $N-1$ hat. Wegen
$$\#\mathbf{Z}/N\mathbf{Z} = N = \#\{\overline{0}\} + \#\{\overline{a}^i : 0 \leq i \leq N-2\}$$
hat dann jedes Element $\overline{b} \in \mathbf{Z}/N\mathbf{Z} \setminus \{\overline{0}\}$ die Gestalt $\overline{b} = \overline{a}^i$, ist also invertierbar. Daher ist jede Zahl $b \in \{1, 2, \ldots, N-1\}$ invertierbar modulo N, d.h. $\mathrm{ggT}(b, N) = 1$, weshalb N keinen nichttrivialen Teiler besitzen kann. N ist also prim. ■

Beispiel: Wir betrachten $p = 10^{20} + 39$ und finden, dass p wahrscheinlich prim ist. Wir faktorisieren $p - 1$ mit Maple und erhalten
$$p - 1 = 2 \cdot 3 \cdot 32839 \cdot 507526619771207$$
(mit 4 Faktoren q_i), wobei wir von der letzten Zahl nur voraussetzen können, dass sie wahrscheinlich prim ist. Durch Probieren finden wir
$$3^{p-1} \equiv 1 \bmod p, \quad 3^{\frac{p-1}{q_i}} \not\equiv 1 \bmod p \text{ für } i = 1, \ldots, 4.$$
(Für 2 gilt $2^{\frac{p-1}{2}} \equiv 1 \bmod p$.) Also ist nach dem Lemma p eine Primzahl, falls $q_4 = 507526619771207$ eine Primzahl ist.
Wir betrachten nun $q_4 = 507526619771207$: Es gilt
$$q_4 - 1 = 507526619771207 - 1 = 2 \cdot 7 \cdot 43 \cdot 5741 \cdot 146850283,$$

wobei klar ist, daß die 5 auftretenden Faktoren r_i Primzahlen sind. Durch Probieren finden wir

$$5^{q_4-1} \equiv 1 \bmod q_4, \quad 5^{\frac{q_4-1}{r_i}} \not\equiv 1 \bmod q_4 \text{ für } i = 1, \ldots, 5,$$

also folgt, das q_4 eine Primzahl ist. Damit haben wir schließlich bewiesen, dass $10^{20} + 37$ eine Primzahl ist.

Das Beispiel kann man leicht verallgemeinern:

Primzahlbeweis mit der $(p-1)$-Methode: Sei p eine wahrscheinlich prime Zahl.

1. Faktorisiere $p-1$:
$$p - 1 = q_1^{e_1} \ldots q_r^{e_r}$$
mit Primzahlen oder wahrscheinlichen Primzahlen q_i.
2. Suche eine natürliche Zahl a mit
$$a^{p-1} \equiv 1 \bmod p, \quad a^{\frac{p-1}{q_i}} \not\equiv 1 \bmod p \text{ für } i = 1, \ldots, r$$
z.B. durch Probieren von $a = 2, 3, 5, 6, 7, \ldots$.
3. p eine Primzahl ist, wenn $q_1, \ldots, q_r$ Primzahlen sind. Zeige also noch, dass alle q_i's Primzahlen sind.

Bemerkungen:

1. Bei der beschriebenen Methode hängt alles davon ab, ob sich $p-1$ faktorisieren läßt. (D.h. es hängt von der Struktur der Gruppe $(\mathbf{Z}/p\mathbf{Z})^*$ ab.) Das Finden einer Zahl a mit $a^{p-1} \equiv 1 \bmod p$ und $a^{\frac{p-1}{q_i}} \not\equiv 1 \bmod p$ ist dagegen in der Praxis unproblematisch.
2. Ein großer Vorteil der $(p-1)$-Primzahlbeweismethode ist, dass ein Beweis einfach und schnell nachzuprüfen ist.
3. Der Primzahlbeweis funktioniert also so, dass man aus der Struktur von $(\mathbf{Z}/p\mathbf{Z})^*$ schließt, dass p prim ist. Goldwasser, Kilian, Atkin und andere kamen auf die Idee, dass man ganz analog auch andere p zugeordnete Gruppen, wie elliptische Kurven $E_{a,b}(\mathbf{Z}/p\mathbf{Z})$ als Testobjekte verwenden könnte. Der Vorteil ist, dass man Parameter die a, b variieren kann, bis man eine faktorisierbare Gruppenordnung $\#E_{a,b}(\mathbf{Z}/(p))$ erhält. Das Verfahren ist als ECPP (elliptic curve primality proving) bekannt.

5. Eine Grundidee zur Faktorisierung

Vorbemerkungen:

1. Für das Faktorisierungsproblem kann man sich nach Entfernung kleiner Teiler und Durchführen von Primzahltests auf folgende Situation beschränken: N ist eine zusammengesetzte natürliche Zahl ohne kleine Teiler, insbesondere ist N ungerade. Gesucht wird nun ein nichttrivialer Teiler von N.
2. Ist a eine ganze Zahl, so gilt
$$\mathrm{ggT}(a, N) = 1 \quad \text{oder} \quad 1 < \mathrm{ggT}(a, N) < N \quad \text{oder} \quad \mathrm{ggT}(a, N) = N.$$
Im Fall $1 < \mathrm{ggT}(a, N) < N$ hat man einen nichttrivialen Teiler von N gefunden, nämlich $\mathrm{ggT}(a, N)$, und man hat das Faktorisierungsproblem gelöst. Da die ggT-Berechnung mit dem euklidischen Algorithmus sehr schnell ist, berechnet man oft zuerst $\mathrm{ggT}(a, N)$ und hat dann einen nichttrivialen Teiler von N oder $N|a$ oder $\mathrm{ggT}(N, n) = 1$.
3. Ist N eine nichttriviale Potenz, d.h. $N = m^k \geq 2$ mit $k \geq 2$, $m \geq 2$, so folgt $N = m^k \geq 2^k$, also $k \leq \frac{\ln N}{\ln 2}$. Damit erhält man folgendes praktikable Kriterium: Ist
$$N \neq \lfloor N^{\frac{1}{k}} \rfloor^k \quad \text{für} \quad k = 2, \ldots, \lfloor \frac{\ln N}{\ln 2} \rfloor,$$
so ist N keine nichttriviale Potenz. Daher kann man voraussetzen, dass N keine nichttriviale Potenz ist, da man sonst sofort eine nichttriviale Faktorisierung von N hätte.

Ein Grundansatz zur Zerlegung einer Zahl N wird in folgendem Lemma gegeben:

LEMMA. *Ist N eine ungerade natürliche Zahl, sind $x, y \in \mathbf{Z}$ mit*

$$x^2 \equiv y^2 \bmod N \quad \text{und} \quad \mathrm{ggT}(N, x) = \mathrm{ggT}(N, y) = 1,$$

so folgt

$$N = \mathrm{ggT}(N, x-y) \cdot \mathrm{ggT}(N, x+y).$$

Genau dann ist die Zerlegung trivial, d.h. $\{\mathrm{ggT}(N, x-y), \mathrm{ggT}(N, x+y)\} = \{1, N\}$, wenn $y \equiv \pm x \bmod N$ gilt.

Beweis: Wir zeigen zunächst, dass $\mathrm{ggT}(N, x-y)$ und $\mathrm{ggT}(N, x+y)$ teilerfremd sind: Wäre dies nicht der Fall, so gäbe es eine Primzahl mit $p | \mathrm{ggT}(N, x-y)$ und $p | \mathrm{ggT}(N, x+y)$, also $p | x-y, x+y, N$, was $p | 2x, 2y, N$ und wegen $N \equiv 1 \bmod 2$ sofort den Widerspruch $p | \mathrm{ggT}(N, x), \mathrm{ggT}(N, y)$ liefern würde. Also ergibt sich mit den üblichen Formeln wegen $N | x^2 - y^2$ die behauptete Zerlegung

$$N = \mathrm{ggT}(N, x^2 - y^2) = \mathrm{ggT}(N, (x-y)(x+y)) = \mathrm{ggT}(N, x-y) \cdot \mathrm{ggT}(N, x+y).$$

Wir haben

$$\mathrm{ggT}(N, x-y) = 1 \iff \mathrm{ggT}(N, x+y) = N \iff N | x+y \iff y \equiv -x \bmod N$$

und analog

$$\mathrm{ggT}(N, x-y) = N \iff \mathrm{ggT}(N, x+y) = 1 \iff y \equiv x \bmod N,$$

was auch die letzte Behauptung zeigt. ■

LEMMA. *Sei N eine zusammengesetzte ungerade natürliche Zahl, die keine Primzahlpotenz ist, und*

$$L = \{(x, y) : 1 \le x, y < N, \mathrm{ggT}(N, x) = \mathrm{ggT}(N, y) = 1, x^2 \equiv y^2 \bmod N\}.$$

Dann gilt

$$\frac{\#\{(x, y) \in L : 1 < \mathrm{ggT}(N, x-y) < N\}}{\#L} \ge \frac{1}{2}.$$

Beweis:

1. Sei
$$L_0 = \{1 \le t < n : t^2 \equiv 1 \bmod N\}.$$
Natürlich gilt $1, N-1 \in L_0$ (wegen $(N-1)^2 \equiv (-1)^2 \equiv 1 \bmod N$). Sei $N = N_1 N_2$ mit $1 < N_1, N_2 < N$ und $\mathrm{ggT}(N_1, N_2) = 1$. Mit dem chinesischen Restsatz findet man $u \in \mathbf{N}_0$ mit
$$u \equiv 1 \bmod N_1 \quad \text{und} \quad u \equiv -1 \bmod N_2.$$
O.E. $1 \le u < N$. Dann ist $u^2 \equiv 1 \bmod N_1$ und $u^2 \equiv 1 \bmod N_2$, also $u^2 \equiv 1 \bmod N_1 N_2$ und damit $u \in L_0$. Also enthält L_0 mindestens die 4 Elemente
$$1, \quad N-1, \quad u, \quad N-u.$$

2. Wir zeigen nun
$$L = \{(ty \bmod N, y) : 1 \le y < N, \mathrm{ggT}(N, y) = 1, t \in L_0\}.$$
$\supseteq$ ist klar wegen $t^2 \equiv 1 \bmod N$.
$\subseteq$: Sei $(x, y) \in L$. Da y invertierbar modulo N ist, gibt es v mit $0 \le v < N$ und $x \equiv vy \bmod N$. Nun folgt aus $x^2 \equiv y^2 \bmod N$ durch Kürzen sofort $v^2 \equiv 1 \bmod N$, also $v \in L_0$ und damit die Behauptung.
Die obige Darstellung liefert nun sofort
$$\#L = \varphi(N) \cdot \#L_0.$$

3. Sei $(x, y) = (ty \bmod N, y) \in L$ mit $t \in L_0$. Wegen $\mathrm{ggT}(N, y) = 1$ ist $\mathrm{ggT}(N, x-y) = \mathrm{ggT}(N, t-1)$. Wir betrachten ein paar Fälle:
   - Gilt $\mathrm{ggT}(N, x-y) = \mathrm{ggT}(N, t-1) = 1$, so folgt aus $N | (t-1)(t+1)$ sofort $N | t+1$, also $t \equiv -1 \bmod N$ und damit $t = N-1$.
   - Gilt $\mathrm{ggT}(N, x-y) = \mathrm{ggT}(N, t-1) = N$, so folgt $t \equiv 1 \bmod N$, also $t = 1$.
   - Ist also $t \in L$, $t \ne 1, N-1$, so gilt notwendig $1 < \mathrm{ggT}(N, x-y) < N$.

4. Wir haben jetzt also

$$\begin{aligned} & \{(x,y) \in L : 1 < \mathrm{ggT}(N, x-y) < N\} = \\ = \quad & \{(ty \bmod N, y) : 1 \leq y < N, \mathrm{ggT}(N,y) = 1, t \in L_0 \setminus \{1, N-1\}\} \end{aligned}$$

und damit

$$\#\{(x,y) \in L : 1 < \mathrm{ggT}(N, x-y) < N\} = \varphi(N) \cdot \#(L_0 \setminus \{1, N-1\}).$$

Damit ergibt sich

$$\frac{\#\{(x,y) \in L : 1 < \mathrm{ggT}(N, x-y) < N\}}{\#L} = \frac{\varphi(N) \cdot \#(L_0 \setminus \{1, N-1\})}{\varphi(N) \cdot \#L_0} = \frac{\#L_0 - 2}{\#L_0}.$$

Da L_0 mindestens 4 Elemente hat, ist $\frac{\#L_0-2}{\#L_0} \geq \frac{1}{2}$ und die Behauptung folgt. ■

Aus dem Lemma ergibt sich sofort folgende

Faktorisierungsidee: Man produziere viele 'zufällige' Kongruenzen

$$x^2 \equiv y^2 \bmod N.$$

Dann sollte man auch ab und zu mit $\mathrm{ggT}(N, x-y)$ einen nichttrivialen Teiler von N finden.

Die wesentliche Frage ist nun: Wie kommt man an Kongruenzen $x^2 \equiv y^2 \bmod n$? Die folgenden Faktorisierungsmethoden

1. CFRAC - Morrison-Brillart (Faktorisierung mit Kettenbrüchen),
2. Quadratic Sieve (QS),
3. Multiple Polynomial Quadratic Sieve (MPQS),
4. Zahlkörpersieb - Number Field Sieve (NFS)

gehen diese Frage in verschiedener Weise an. Wir wollen im folgenden das Zahlkörpersieb kurz skizzieren.

Das Zahlentheoriesieb ist die Faktorisierungsmethode, mit der man heutzutage die größten Zahlen faktorisieren kann. Allerdings hängt die Durchführung der Faktorisierung sehr stark von der zu faktorisierenden Zahl N ab. (Beispiel: RSA-155)

6. Grundschritte des Zahlkörpersiebs

Gegeben sei eine zusammengesetzte natürliche Zahl N ohne kleine Teiler. Wir suchen einen nichttrivialen Teiler von N.

6.1. Auswahl eines Polynoms. Man sucht sich ein ein irreduzibles normiertes Polynom $f(x) \in \mathbf{Z}[x]$ vom Grad d, sodass eine Zahl $m \in \mathbf{Z}$ existiert mit

$$f(m) \equiv 0 \bmod N,$$

wobei noch einige weitere Eigenschaften erfüllt sein sollen, die später angegeben werden.
Natürlich gibt es viele solcher Polynome $f(x) = x^d + a_1 x^{d-1} + \cdots + a_d$, da die a_i's variiert werden können und nur eine Gleichung der Form

$$m^d + a_1 m^{d-1} + a_2 m^{d-2} + \cdots + a_d = NN'$$

mit $N' \in \mathbf{Z}$ erfüllt sein muß.

6.2. Der Zahlkörper. Sei $K = \mathbf{Q}(\alpha)$ mit $f(\alpha) = 0$. Wir nehmen an, dass die Maximalordnung $\mathbf{Z}_K$ ein Hauptidealring ist. (Es muss nicht notwendig $\mathbf{Z}_K = \mathbf{Z}[\alpha]$ gelten.) Das Polynom $f(x)$ liegt wegen $f(m) \equiv 0 \bmod N$ im Kern des Ringhomomorphismus $\mathbf{Z}[x] \to \mathbf{Z}/N\mathbf{Z}$, $x \mapsto m \bmod N$, also kann man es herausfaktorisieren und erhält einen Ringhomomorphismus

$$\Phi : \mathbf{Z}[\alpha] \to \mathbf{Z}/N\mathbf{Z}, \quad \alpha \mapsto m \bmod N.$$

Gilt für den Index $\mathrm{ggT}(N, [\mathbf{Z}_K : \mathbf{Z}[\alpha]]) > 1$, so hätte man einen nichttrivialen (kleinen) Teiler von N, also kann man o.E. $\mathrm{ggT}(N, [\mathbf{Z}_K : \mathbf{Z}[\alpha]]) = 1$ voraussetzen. In diesem Fall läßt sich obiger Ringhomomorphismus eindeutig zu einem Ringhomomorphismus

$$\Phi : \mathbf{Z}_K \to \mathbf{Z}/N\mathbf{Z}, \quad \alpha \mapsto m \bmod N$$

fortsetzen.

6.3. Einheiten. Sei $\varepsilon_1, \ldots, \varepsilon_r$ ein System von Grundeinheiten von $\mathbf{Z}_K$ und $\zeta \in \mathbf{Z}_K$ eine Einheitswurzel, die $\mu(K)$ erzeugt.

6.4. Faktorbasen. Wir geben uns eine Konstante $B_{\mathbf{Q}}$ vor. Die Primzahlen $p \le B_{\mathbf{Q}}$ seien $p_1, \ldots, p_t$, sie bilden den ersten Teil der sogeannten Faktorbasis:

$$\mathrm{FB}_{\mathbf{Q}} = \{p_1, \ldots, p_t\}.$$

Für ein Primideal $\mathfrak{p} \subseteq \mathbf{Z}_K$ bezeichne $p_{\mathfrak{p}}$ die in $\mathfrak{p}$ enthaltene Primzahl. Wir geben uns eine Konstante B_K vor und wählen dann alle Primideale $\mathfrak{p}_i$ mit $p_{\mathfrak{p}_i} \le B_K$, die als Teiler von Ausdrücken der Gestalt $a\alpha + b$ auftreten können. Dann wählt man dazu erzeugende Primelemente π_i, d.h. $\mathfrak{p}_i = (\pi_i)$. Diese bilden jetzt den zweiten Teil der Faktorbasis:

$$\mathrm{FB}_K = \{\pi_1, \ldots, \pi_s\}.$$

6.5. Das Ziel. Wir suchen nun $a_i, b_i \in \mathbf{Z}$, sodass sich $a_i\alpha + b_i$ und $a_i m + b_i$ als Produkt der oben gewählten Primzahlen, Primelemente und Einheiten schreiben läßt:

$$\begin{aligned} a_i m + b_i &= (-1)^{c_{i0}} p_1^{c_{i1}} p_2^{c_{i2}} \ldots p_t^{c_{it}}, \\ a_i\alpha + b_i &= \zeta^{e_{i0}} \varepsilon_1^{e_{i1}} \ldots \varepsilon_r^{e_{ir}} \cdot \pi_1^{d_{i1}} \ldots \pi_s^{d_{is}}. \end{aligned}$$

(Dies erklärt auch den Namen Faktorbasis.) Hat man genügend viele Paare (a_i, b_i) gefunden, so kann man Produkte bilden:

$$\begin{aligned} \prod_{i\in I}(a_i m + b_i) &= (-1)^{\sum_i c_{i0}} p_1^{\sum_i c_{i1}} p_2^{\sum_i c_{i2}} \ldots p_t^{\sum_i c_{it}}, \\ \prod_{i\in I}(a_i\alpha + b_i) &= \zeta^{\sum_i e_{i0}} \varepsilon_1^{\sum_i e_{i1}} \ldots \varepsilon_r^{\sum_i e_{ir}} \cdot \pi_1^{\sum_i d_{i1}} \ldots \pi_s^{\sum_i d_{is}}. \end{aligned}$$

Sind alle Exponenten $\sum_i c_{i0}, \ldots, \sum_i d_{is}$ gerade, so kann man definieren

$$\begin{aligned} y_I &= (-1)^{(\sum_i c_{i0})/2} p_1^{(\sum_i c_{i1})/2} p_2^{(\sum_i c_{i2})/2} \ldots p_t^{(\sum_i c_{it})/2}, \\ \xi_I &= \zeta^{(\sum_i e_{i0})/2} \varepsilon_1^{(\sum_i e_{i1})/2} \ldots \varepsilon_r^{(\sum_i e_{ir})/2} \cdot \pi_1^{(\sum_i d_{i1})/2} \ldots \pi_s^{(\sum_i d_{is})/2} \end{aligned}$$

und erhält

$$\prod_{i\in I}(a_i m + b_i) = y_I^2 \quad \text{und} \quad \prod_{i\in I}(a_i\alpha + b_i) = \xi_I^2.$$

Es folgt

$$\Phi(\xi_I)^2 = \Phi(\xi_I^2) = \Phi(\prod_{i\in I}(a_i\alpha + b_i)) \equiv \prod_{i\in I}(a_i\Phi(\alpha) + b_i) \equiv \prod_{i\in I}(a_i m + b_i) \equiv y_I^2 \bmod N.$$

Gilt nun $\Phi(x_i) \not\equiv \pm y_I \bmod N$, so liefert

$$\mathrm{ggT}(\Phi(\xi_I) - y_I, N)$$

einen nichttrivialen Teiler von N. Hat man genügend viele geeignet I's, so sollte man auf diese Weise irgendwann einen nichttrivialen Teiler von N erhalten.
Es gibt zwei Probleme:

- Wie findet man (viele) Paare (a, b), sodass $am + b$ bzw. $a\alpha + b$ sich vollständig mit der gewählten Faktorbasis faktorisieren lassen?

- Wie kann man aus vielen Paaren (a_i, b_i) Paare $(a_i, b_i), i \in I$ auswählen, sodass $\prod_{i\in I}(a_i m + b_i)$ und $\prod_{i\in I}(a_i\alpha + b_i)$ Quadrate sind?

Die erste Frage geht man mit Siebmethoden an, die zweite mit Linearer Algebra.

6.6. Der Siebprozess. Der einfacheren Schreibweise halber sei hier $B_{\mathbf{Q}} = B_K$. Dann gilt:

$$a\alpha + b \text{ faktorisiert in der Faktorbasis } \mathrm{FB}_K \quad \Longleftrightarrow \quad \mathrm{N}(a\alpha + b) \text{ faktorisiert in der Faktorbasis } \mathrm{FB}_{\mathbf{Q}}.$$

Wir wählen $A, B \geq 1$ und betrachten die Menge

$$M_{A,B} = \{(a, b) \in \mathbf{Z} \times \mathbf{Z} : 1 \leq a \leq A, -B \leq b \leq B, \mathrm{ggT}(a, b) = 1 \text{ und } am + b \neq 0\}.$$

Für jedes Paar $(a, b) \in M_{A,B}$ können wir zerlegen

$$\begin{aligned} |am + b| &= p_1^{u_1} \dots p_t^{u_t} \cdot U_{a,b} \quad \text{mit} \quad p_i \nmid U_{a,b}, \\ |\mathrm{N}(a\alpha + b)| &= p_1^{v_1} \dots p_t^{v_t} \cdot V_{a,b} \quad \text{mit} \quad p_i \nmid V_{a,b}, \end{aligned}$$

(wobei natürliche die Exponenten u_i und v_i auch von (a, b) abhängen). Wir suchen alle Paare

$$(a, b) \in M_{A,B} \quad \text{mit} \quad U_{a,b} = V_{a,b} = 1.$$

Für solche Paare (a, b) faktorisieren nämlich $am+b$ und $a\alpha+b$ vollständig in der vorgegebenen Faktorbasis.

Naive Vorgehensweise: Man nimmt sich jedes $(a, b) \in M_{A,B}$ einzeln vor, probiert mit jeder Primzahl p_i der Faktorbasis, ob sie $|am+b|$ und $|\mathrm{N}(a\alpha+b)|$ teilt (durch Division mit Rest), und teilt sie gegebenenfalls so oft wie möglich heraus. Man Schluß bleiben $U_{a,b}$ und $V_{a,b}$ übrig. Gilt nun $U_{a,b} = V_{a,b} = 1$, so hat man ein gesuchtes Paar (a, b) gefunden, sonst nicht. Bei dieser Vorgehensweise braucht man viele Divisionen mit Rest.

Wir gehen nun anders vor: Wir überlegen zuerst für jede Primzahl der Faktorbasis, welche $(a, b) \in M_{A,B}$ die Eigenschaft

$$p^k | am + b \quad \text{bzw.} \quad p^k | \mathrm{N}(a\alpha + b)$$

erfüllen. Für $am + b$ sind die Eigenschaften in folgendem Lemma zusammengestellt:

LEMMA. *Seien $a, b, m \in \mathbf{Z}$ mit $\mathrm{ggT}(a, b) = 1$, $k \in \mathbf{N}$ und p eine Primzahl.*

1. *Es gilt:*
$$p^k | am + b \quad \Longleftrightarrow \quad \mathrm{ggT}(p, a) = 1 \quad \textit{und} \quad b \equiv -am \bmod p^k.$$
2. *Es gilt:*
$$(a, b) \in M_{A,B} \quad \textit{und} \quad p^k | am + b \quad \Longleftrightarrow \quad 1 \leq a \leq A, \quad \mathrm{ggT}(p, a) = 1, \quad b = -am + lp^k$$
$$\textit{für ein } l \textit{ mit } \lceil \frac{am - B}{p^k} \rceil \leq l \leq \lfloor \frac{am + B}{p^k} \rfloor.$$
3. *Ist $am + b \neq 0$ und gilt $p^k | am + b$, so folgt*
$$p^k \leq A|m| + B \quad \textit{und} \quad k \leq \frac{\ln(A|m| + B)}{\ln p}.$$

Beweis: Die erste Eigenschaft ist sofort klar, wenn man bedenkt, dass $p^k | am + b$ und $\mathrm{ggT}(a, b) = 1$ natürlich $\mathrm{ggT}(p, a) = 1$ implizieren. Bei der zweiten Aussage können wir b in der Form $b = -am + lp^k$ mit einem $l \in \mathbf{Z}$ ansetzen. Wir haben folgende Äquivalenzen:

$$\begin{aligned} -B \leq b \leq B \quad &\Longleftrightarrow \quad -B \leq -am + lp^k \leq B \quad \Longleftrightarrow \quad \frac{am - B}{p^k} \leq l \leq \frac{am + B}{p^k} \\ &\Longleftrightarrow \quad \lceil \frac{am - B}{p^k} \rceil \leq l \leq \lfloor \frac{am + B}{p^k} \rfloor, \end{aligned}$$

was die entsprechende Behauptung beweist. Die letzte Aussage ist trivial. ■

Bemerkung: Das Lemma zeigt, dass man die $(a, b) \in M_{A,B}$ beschreiben kann, für die $p^k | am + b$ gilt. Man kommt dabei ohne Probedivisionen aus. Wir schreiben nun noch die multiplikative Zerlegung

$$|am + b| = p_1^{u_1} \dots p_t^{u_t} U_{a,b}$$

additiv um:

$$\ln U_{a,b} = \ln|am+b| - u_1 \ln p_1 - \cdots - u_t \ln p_t.$$

1. Siebprozess:

1. Wir definieren
$$S[a,b] := \ln|am+b| \quad \text{für} \quad (a,b) \in M_{A,B}.$$
(Die Rechengenauigkeit muss nicht sehr groß sein, wie wir später sehen werden.)
2. Wir lassen nun p die Primzahlen $p_1, \ldots, p_t$ durchlaufen und in Abhängigkeit davon k die natürlichen Zahlen mit $1 \le k \le \frac{\ln(A|m|+B)}{\ln p}$ bzw. $p^k \le A|m| + B$.
3. Bei festem p und k durchlaufen wir alle a's mit $1 \le a \le A$ und $\mathrm{ggT}(p,a) = 1$, abhängig davon lassen wir l laufen mit
$$\lceil \frac{am-B}{p^k} \rceil \le l \le \lfloor \frac{am+B}{p^k} \rfloor$$
und setzen
$$b := -am + lp^k, \quad S[a,b] := S[a,b] - \ln p.$$
4. Am Schluß gilt: $S[a,b] = U_{a,b}$. Die uns interessierenden Paare $(a,b) \in M_{A,B}$ sind also genau die mit $S[a,b] = 0$.

Bemerkungen:

1. Sei $|am+b| = p_1^{u_1} \ldots p_t^{u_t} U_{a,b}$ mit $p_i \nmid U_{a,b}$. Gilt $p_i^k | am+b$, so haben wir von $S[a,b]$ den Wert $\ln p_i$ abgezogen. Da diese Eigenschaft genau für $k = 1, 2, \ldots, u_1$ erfüllt ist, haben wir insgesamt $u_i \ln p_i$ von $S[a,b]$ abgezogen. Somit ist klar, dass man Ende des Siebprozesses $S[a,b] = U_{a,b}$ übrigbleibt.
2. Wir erinnern daran, dass $p_1, \ldots, p_t$ alle Primzahlen $\le B_{\mathbf{Q}}$ waren. Gilt $U_{a,b} \ne 1$, so hat $U_{a,b}$ einen Primteiler $> B_{\mathbf{Q}}$, also folgt $\ln U_{a,b} > \ln B_{\mathbf{Q}}$. Damit ist z.B. folgende Eigenschaft klar:
$$\ln U_{a,b} = 0 \quad \Longleftrightarrow \quad \ln U_{a,b} \le \frac{1}{2} \ln B_{\mathbf{Q}}.$$
Dies zeigt, dass man beim Umgang mit den Logarithmen keine hohe Rechengenauigkeit braucht.

Wir erinnern daran, dass $f(x) \in \mathbf{Z}[x]$ das normierte Minimalpolynom von α mit $K = \mathbf{Q}(\alpha)$ war und dass der Grad von f mit d bezeichnet wurde.

LEMMA. *Seien $a, b \in \mathbf{Z}$ mit $\mathrm{ggT}(a,b) = 1$, $k \in \mathbf{N}$ und p eine Primzahl. Seien $t_{p,k,j}$, $j = 1, 2, 3, \ldots$ die Nullstellen von $f(x)$ modulo p^k, d.h. gilt für $c \in \mathbf{Z}$ die Aussage $f(c) \equiv 0 \bmod p^k$, so gibt es ein j mit $c \equiv t_{p,k,j} \bmod p^k$.*

1. *Es gilt:*
$$p^k | \mathrm{N}(a\alpha + b) \quad \Longleftrightarrow \quad \mathrm{ggT}(p,a) = 1 \quad \text{und} \quad b \equiv -t_{p,k,j} a \bmod p^k \quad \text{für ein } j.$$
2. *Es gilt:*
$$(a,b) \in M_{A,B} \text{ und } p^k | \mathrm{N}(a\alpha+b) \quad \Longleftrightarrow \quad 1 \le a \le A, \quad \mathrm{ggT}(p,a) = 1,$$
$$b = -t_{p,k,j} a + lp^k \text{ für ein } j \text{ und ein } l \text{ mit}$$
$$\lceil \frac{t_{p,k,j} a - B}{p^k} \rceil \le l \le \lfloor \frac{t_{p,k,j} a + B}{p^k} \rfloor.$$
3. *Gilt $p^k | \mathrm{N}(a\alpha+b)$, so folgt*
$$p^k \le \|f\|_1 \max(A,B)^d,$$
wobei $\|f\|_1 = \sum_i |c_i|$ für $f = \sum_i c_i x^i$ ist.

Beweis: Gilt für ein Paar $(a,b) \in \mathbf{Z}^2$ mit $\mathrm{ggT}(a,b) = 1$ die Bedingung $p^k | \mathrm{N}(a\alpha+b)$, so gilt auch $p \nmid a$, d.h. $\mathrm{ggT}(a,b) = 1$. Zwischen Minimalpolynom $f(x)$ von α und der Norm in $K[x]$ besteht folgende Identität:
$$\mathrm{N}(x - \alpha) = f(x).$$
Daher gilt
$$\mathrm{N}(a\alpha + b) = \mathrm{N}(-a)\mathrm{N}(-\frac{b}{a} - \alpha) = (-a)^d f(-\frac{b}{a}),$$

was (mit $\mathrm{ggT}(a,p)=1$) zu folgenden Äquivalenzen führt

$$\begin{aligned} p^k|\mathrm{N}(a\alpha+b) \quad &\Longleftrightarrow \quad f(-\frac{b}{a}) \equiv 0 \bmod p^k \quad \Longleftrightarrow \quad -\frac{b}{a} \equiv t_{p,k,j} \bmod p^k \text{ für ein } j \\ &\Longleftrightarrow \quad b \equiv -t_{p,k,j}a \bmod p^k \text{ für ein } j. \end{aligned}$$

Dies zeigt die erste Behauptung. Wir könnnen nun ansetzen $b=-t_{p,k,j}+lp^k$ für ein j und ein $l\in\mathbf{Z}$. Umformung von $-B\le b\le B$ führt dann wie zuvor zur zweiten Behauptung. Gilt $f(x)=\sum_i c_i x_i$, so können wir die Norm wie folgt abschätzen:

$$\begin{aligned} |\mathrm{N}(a\alpha+b)| &= |(-a)^d f(-\frac{b}{a})| = |(-a)^d \sum_{i=1}^{d} c_i(-\frac{b}{a})^i| = |\sum_{i=1}^{d} c_i(-1)^{d-i}a^{d-i}b^i| \le \sum_{i=1}^{d}|c_i||a|^{d-i}|b|^i \\ &\le \sum_i |c_i|\max(|a|,|b|)^d = \|f\|_1 \max(|a|,|b|)^d. \end{aligned}$$

Ist also $(a,b)\in M_{A,B}$ und gilt $p^k|\mathrm{N}(a\alpha+b)$, so folgt

$$p^k \le |\mathrm{N}(a\alpha+b)| \le \|f\|_1 \max(|a|,|b|)^d \le \|f\|_1 \max(A,B)^d,$$

was zu zeigen war. ■

2. Siebprozess:

1. Wir definieren
$$T[a,b] := \ln|\mathrm{N}(a\alpha+b)| \quad \text{für} \quad (a,b)\in M_{A,B}.$$
Für $a\neq 0$ gilt auch $T[a,b]=\ln|a^d f(-\frac{b}{a})|$.
2. Wir lassen p die Primzahlen $p_1,\ldots,p_t$ der Faktorbasis durchlaufen und in Abhängigkeit davon k die natürlichen Zahlen mit $p^k\le\|f\|_1\max(A,B)^d$.
3. Bei festem p und k werden alle $t_{p,k,j}$, $j=1,2,\ldots$ durchlaufen.
4. Bei festen Werten für p, k und j durchlaufen wir alle a's mit $1\le a\le A$ und $\mathrm{ggT}(p,a)=1$, abhängig davon alle l's mit
$$\lceil\frac{t_{p,k,j}a-B}{p^k}\rceil \le l \le \lfloor\frac{t_{p,k,j}a+B}{p^k}\rfloor$$
und setzen
$$b := -t_{p,k,j}a+lp^k, \quad T[a,b] := T[a,b]-\ln p.$$
5. Am Schluß gilt: $T[a,b]=V_{a,b}$. Die uns interessierenden Paare $(a,b)\in M_{A,B}$ sind also genau die mit $T[a,b]=0$.

Bemerkungen:

1. Wir haben zu Beginn des Prozesses
$$|\mathrm{N}(a\alpha+b)| = p_1^{v_1}\ldots p_t^{v_t}V_{a,b} \text{ mit } p_i\nmid V_{a,b} \quad \text{und} \quad T[a,b]=v_1\ln p_1+\cdots+v_t\ln p_t+\ln V_{a,b}.$$
Die Eigenschaft $p_i^k|\mathrm{N}(a\alpha+b)$ ist für $k=1,2,\ldots,v_i$ erfüllt, jedesmal wird von $T[a,b]$ der Wert $\ln p_i$ abgezogen, insgesamt also $v_i\ln p_i$. Damit ist klar, dass am Ende des Prozesses $T[a,b]=\ln V_{a,b}$ übrigbleibt.
2. Wie früher sieht man:
$$V_{a,b}\neq 1 \quad \Longrightarrow \quad \ln V_{a,b} > \ln B_{\mathbf{Q}},$$
was sofort zu
$$\ln V_{a,b}=0 \quad \Longleftrightarrow \quad \ln V_{a,b} \le \frac{1}{2}\ln B_{\mathbf{Q}}$$
führt.
3. Beim 2. Siebprozess kann man sich auf die Elemente $(a,b)\in M_{A,B}$ beschränken, für die $S[a,b]\approx 0$ (nach dem 1. Siebprozess) gilt.

Ergebnis: Bei Vorgabe von A und B kann man mit den beiden Siebprozessen genau die (a,b)'s mit

$$\mathrm{ggT}(a,b)=1, \quad 1\le a\le A, \quad -B\le b\le B$$

bestimmen, für die sich $am+b$ und $a\alpha+b$ vollständig mit den Elementen der vorgegebenen Faktorbasis faktorisieren lassen.

Beispiel: Wir wollen alle $(a,b)\in\mathbf{Z}^2$ bestimmen mit $\mathrm{ggT}(a,b)=1$, $1\le a\le 100$, $-100\le b\le 100$, sodass für

$$m=123456$$

eine Zerlegung

$$am+b=\pm 2^r\cdot 3^s\cdot 5^t\cdot 7^u$$

existiert. Wir wenden den 1. Siebprozess an mit $A=B=100$ und der Faktorbasis $\mathrm{FB}=\{2,3,5,7\}$. Es gibt $A(2B+1)=20100$ Paare (a,b) mit $1\le a\le A$ und $|b|\le B$. Die Menge $M_{A,B}=\{(a,b)\in\mathbf{Z}^2 : \mathrm{ggT}(a,b)=1, 1\le a\le A, |b|\le B, am+b\neq 0\}$ hat 12175 Elemente. In der folgenden Tabelle gibt $k_{\max}$ das maximale k mit $p^k\le A\cdot m+B$ an, weiter ist angegeben, bei wievielen Paaren (a,b) eine Subtraktion von $\ln p$ durchgeführt wurde.

p	$k_{\max}$	Wie oft wurde $\ln p$ subtrahiert?
2	23	8215
3	14	4576
5	10	2513
7	8	1770

Zum Schluß bleiben zwei Paare übrig: $(1,24)$ und $(81,64)$. Tatsächlich gilt:

$$1\cdot 123456+24=2^3\cdot 3^2\cdot 5\cdot 7^3 \quad \text{und} \quad 81\cdot 123456+64=2^7\cdot 5^7.$$

6.7. Lineare Algebra. Wir haben also 'viele' Paare (a_i,b_i) gefunden mit einer Faktorisierung

$$\begin{aligned} a_im+b_i &= (-1)^{c_{i0}}p_1^{c_{i1}}p_2^{c_{i2}}\ldots p_t^{c_{it}},\\ a_i\alpha+b_i &= \zeta^{e_{i0}}\varepsilon_1^{e_{i1}}\ldots\varepsilon_r^{e_{ir}}\cdot\pi_1^{d_{i1}}\ldots\pi_s^{d_{is}}.\end{aligned}$$

Wir schreiben die Exponenten in die Zeilen einer Matrix R, d.h. die i-te Zeile von R ist

$$R_i=(c_{i0}\,c_{i1}\,\ldots c_{is}\,e_{i0}\,e_{i1}\,\ldots e_{ir}\,d_{i1}\,d_{i2}\,\ldots d_{it}),$$

wobei wegen $\Phi(a_i\alpha+b_i)\equiv a_im+b_i \bmod N$ die Eigenschaft

$$(*) \qquad \Phi(\zeta^{e_{i0}}\varepsilon_1^{e_{i1}}\ldots\varepsilon_r^{e_{ir}}\cdot\pi_1^{d_{i1}}\ldots\pi_s^{d_{is}})\equiv(-1)^{c_{i0}}p_1^{c_{i1}}p_2^{c_{i2}}\ldots p_t^{c_{it}} \bmod N$$

erfüllt ist. Bei elementaren Zeilenoperationen an R bleibt die Eigenschaft $(*)$ erhalten. Wir können dann erreichen, dass die transformierte Matrix R modulo 2 in oberer Dreiecksgestalt ist. Die Matrix R hat $2+r+s+t$ Spalten. Dann stehen sicher in den letzten

$$\#(\text{Zeilen von } R)-2-r-s-t$$

Zeilen von R nur gerade Zahlen. Dies führt dann auf eine Relation $\phi(\xi_I)^2\equiv y_I^2 \bmod N$, wie zuvor beschrieben.

7. Ein kleines Beispiel

Im folgenden soll ein kleines Beispiel vorgestellt werden, das die prinzipielle Vorgehensweise beim Zahlkörpersieb demonstriert.

Wir betrachten $f(x)=x^3+7x+20$ und $K=\mathbf{Q}(\alpha)$ mit $f(\alpha)=0$. Die Maximalordnung ist

$$\mathbf{Z}_K=\mathbf{Z}\cdot\frac{\alpha^2+\alpha}{2}+\mathbf{Z}\cdot\alpha+\mathbf{Z}$$

und hat Klassenzahl $h_K=1$, eine Grundeinheit mit Norm $+1$ ist

$$\varepsilon=-\frac{127}{2}\alpha^2-\frac{127}{2}\alpha+107$$

mit Regulator $\mathrm{Reg}\,(K) = 13.44782$. Für die Primzahlen $p \le 20$ haben wir Zerlegungen

$$(2) = \mathfrak{p}_2\mathfrak{p}_4, \quad (3) = \mathfrak{p}_3\mathfrak{p}_9, \quad (5) = \mathfrak{p}_5\mathfrak{p}_{25}, \quad (7) = \mathfrak{p}_{7a}\mathfrak{p}_{7b}\mathfrak{p}_{7c}, \quad (11), \quad (13), \quad (17) = \mathfrak{p}_{17a}\mathfrak{p}_{17b}^2, \quad (19).$$

Wir stellen die benötigten Primideale $\mathfrak{p} = (\pi)$ zusammen, sodass $\mathfrak{p} = (\pi)$, $\mathrm{N}\pi = p$ bzw. (im Fall $\mathfrak{p}_4$) $\mathrm{N}\pi = p^2$ und $\lambda_\mathfrak{p}\mathfrak{p} \subseteq \mathbf{Z}_K$, $\lambda_\mathfrak{p} \notin \mathbf{Z}_K$ (zur Berechnung der Bewertungen) gilt:

$$\begin{array}{lll}
\mathfrak{p}_2 = (2, \alpha) & \pi_2 = \alpha + 2 & \lambda_2 = \frac{1}{2}(\alpha + 1) \\
\mathfrak{p}_4 = (2, \alpha + 1) & \pi_4 = \alpha^2 - 2\alpha + 11 & \lambda_4 = \frac{1}{2}\alpha \\
\mathfrak{p}_3 = (3, \alpha + 1) & \pi_3 = -\frac{1}{2}\alpha^2 - \frac{3}{2}\alpha - 1 & \lambda_3 = \frac{1}{3}(\alpha^2 + 2\alpha + 2) \\
\mathfrak{p}_5 = (5, \alpha) & \pi_5 = \frac{21}{2}\alpha^2 + \frac{45}{2}\alpha + 5 & \lambda_5 = \frac{1}{5}(\alpha^2 + 2) \\
\mathfrak{p}_{7a} = (7, \alpha + 3) & \pi_{7a} = \frac{1}{2}\alpha^2 + \frac{5}{2}\alpha + 3 & \lambda_{7a} = \frac{1}{7}(\alpha + 5)(\alpha + 6) \\
\mathfrak{p}_{7b} = (7, \alpha + 5) & \pi_{7b} = -\frac{9}{2}\alpha^2 - \frac{35}{2}\alpha - 17 & \lambda_{7b} = \frac{1}{7}(\alpha + 3)(\alpha + 6) \\
\mathfrak{p}_{7c} = (7, \alpha + 6) & \pi_{7c} = -\frac{1}{2}\alpha^2 - \frac{1}{2}\alpha + 1 & \lambda_{7c} = \frac{1}{7}(\alpha + 3)(\alpha + 5) \\
\mathfrak{p}_{17a} = (17, \alpha + 6) & \pi_{17a} = -16\alpha^2 + 2\alpha + 61 & \lambda_{17a} = \frac{1}{17}(\alpha + 14)^2 \\
\mathfrak{p}_{17b} = (17, \alpha + 14) & \pi_{17b} = -\frac{1}{2}\alpha^2 + \frac{1}{2}\alpha + 3 & \lambda_{17b} = \frac{1}{17}(\alpha + 6)(\alpha + 14)
\end{array}$$

Für die Norm von $a\alpha + b$ gilt

$$N(a\alpha + b) = b^3 + 7a^2b - 20a^3.$$

Beispiel: Wir wollen (die zusammengesetzte Zahl) $N = 29503$ in Faktoren zerlegen. Es ist $f(49) = 4N$. Wir setzen $m = 49$. Dann liefert $\mathbf{Z}[\alpha] \to \mathbf{Z}/N\mathbf{Z}$, $\alpha \mapsto m \bmod N$ einen Ringhomomorphismus, der sich zu einem Ringhomomorphismus

$$\Phi : \mathbf{Z}_K \to \mathbf{Z}/N\mathbf{Z}, \quad \alpha \mapsto m$$

fortsetzt.

Wir suchen jetzt nach $a, b \in \mathbf{Z}$ (mit $\mathrm{ggT}(a, b) = 1$), sodass wir Faktorisierungen

$$\begin{aligned}
a\alpha + b &= (-1)^r \cdot \varepsilon^s \pi_2^{c_1} \cdot \pi_4^{c_2} \cdot \pi_3^{c_3} \cdot \pi_5^{c_4} \cdot \pi_{7a}^{c_5} \cdot \pi_{7b}^{c_6} \cdot \pi_{7c}^{c_7} \cdot \pi_{17a}^{c_8} \cdot \pi_{17b}^{c_9}, \\
am + b &= (-1)^t \cdot 2^{d_1} \cdot 3^{d_2} \cdot 5^{d_3} \cdot 7^{d_4} \cdot 11^{d_5} \cdot 13^{d_6} \cdot 17^{d_7} \cdot 19^{d_8}
\end{aligned}$$

erhalten. (Die erste Bedingung ist gleichwertig damit, dass in der Primfaktorzerlegung von $|\mathrm{N}(a\alpha + b)|$ nur $2, 3, 5, 7, 17$ vorkommen.)

Wir wenden die Siebprozesse mit $A = B = 100$ an. Die Menge

$$M_{A,B} = \{(a, b) \in \mathbf{Z}^2 : \mathrm{ggT}(a, b) = 1, 1 \le a \le A, -B \le b \le B, am + b \ne 0\}$$

hat 12174 Elemente. Nach dem 1. Siebprozess bleiben 1457 Paare übrig:

$$(1, -100), (1, -99), (1, -98), \ldots, (99, 89), (100, -49), (100, 13).$$

Für den 2. Siebprozess braucht man Nullstellen von f modulo p^k, welche teilweise in folgender Tabelle aufgeführt sind:

p	$k_{\max}$	Nullstellen von $f(x)$ modulo $p^{k_{\max}}$
2	24	3158260
3	15	8188196
5	10	2480765
7	8	3548490, 5319610, 2661502
17	6	12101376

Wird jetzt der 2. Siebprozess auf die verbliebenen 1457 Elemente angewandt, so bleiben 21 Paare übrig:

$$\begin{aligned}(a,b) \;=\; & (1,-68),(1,-23),(1,-15),(1,-11),(1,-5),(1,-4),(1,-1),\\ & (1,0),(1,1),(1,2),(1,3),(1,5),(1,6),(1,31),\\ & (3,5),(5,2),(5,11),(7,20),(11,-19),(13,43),(19,4).\end{aligned}$$

Wir bestimmen die jeweiligen Faktorzerlegungen von $a_i m + b_i$ und $a_i \alpha + b_i$, wobei wir für nachfolgende Tabelle von (a_i, b_i) eventuell zu $(-a_i, -b_i)$ übergegangen sind. Außerdem haben wir noch die (trivialen) Paare $(0,-1),(0,2),(0,7),(0,17)$ hinzugenommen.

a	b	r	s	c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	t	d_1	d_2	d_3	d_4	d_5	d_6	d_7	d_8
0	-1	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
0	2	0	0	1	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
0	7	0	-1	0	0	0	0	1	1	1	0	0	0	0	0	0	1	0	0	0	0
0	17	0	-1	0	0	0	0	0	0	0	1	2	0	0	0	0	0	0	0	1	0
-1	1	0	0	0	1	0	0	0	0	1	0	0	1	4	1	0	0	0	0	0	0
-1	0	0	-1	2	0	0	1	0	0	0	0	0	1	0	0	0	2	0	0	0	0
-1	-1	0	0	0	1	1	0	0	0	0	0	0	1	1	0	2	0	0	0	0	0
1	2	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0
1	3	0	0	0	1	0	0	1	0	0	0	0	0	2	0	0	0	0	1	0	0
-1	4	0	-1	4	0	0	0	1	0	0	0	0	1	0	2	1	0	0	0	0	0
-1	5	0	-1	0	1	2	1	0	0	0	0	0	1	2	0	0	0	1	0	0	0
1	5	0	-1	0	1	0	1	0	1	0	0	0	0	1	3	0	0	0	0	0	0
-5	-2	0	-1	1	0	2	0	0	0	1	0	1	1	0	0	0	0	0	1	0	1
-3	-5	0	-1	0	1	0	2	0	0	0	0	0	1	3	0	0	0	0	0	0	1
1	6	0	-1	1	0	0	0	0	0	1	1	0	0	0	0	1	0	1	0	0	0
-1	11	0	-1	0	1	1	0	1	0	0	1	0	1	1	0	0	0	0	0	0	1
5	11	0	-1	0	1	3	0	0	1	0	0	0	0	8	0	0	0	0	0	0	0
-1	15	0	-2	0	1	0	3	0	0	1	0	0	1	1	0	0	0	0	0	1	0
-11	19	0	-2	0	1	6	0	0	0	0	1	0	1	3	0	1	0	0	1	0	0
-19	-4	0	-3	5	0	4	0	0	2	0	0	0	1	0	0	1	0	1	0	1	0
7	20	0	-3	6	0	0	3	0	0	0	0	0	0	0	1	0	0	2	0	0	0
-1	23	0	-2	0	1	2	0	0	3	0	0	0	1	1	0	0	0	0	1	0	0
1	31	0	-1	0	1	2	0	2	0	0	0	1	0	4	0	1	0	0	0	0	0
13	43	0	-1	0	1	2	0	0	0	4	0	0	0	3	0	1	0	0	0	1	0
-1	68	0	-3	4	0	9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

Wir tragen jetzt die Exponenten zeilenweise in eine Matrix R ein:

$$R = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 4 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & 2 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & -1 & 4 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & 0 & 1 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & -1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 3 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & 1 & 0 & 2 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & -1 & 0 & 1 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 1 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & -1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & -1 & 0 & 1 & 3 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -2 & 0 & 1 & 0 & 3 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & -2 & 0 & 1 & 6 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 3 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & -3 & 5 & 0 & 4 & 0 & 0 & 2 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & -3 & 6 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 2 & 0 & 0 & 0 \\
0 & -2 & 0 & 1 & 2 & 0 & 0 & 3 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & -1 & 0 & 1 & 2 & 0 & 2 & 0 & 0 & 0 & 1 & 0 & 4 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & 0 & 1 & 2 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 3 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & -3 & 4 & 0 & 9 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}$$

Bezeichnet

$$(r, s, c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8, c_9, t, d_1, d_2, d_3, d_4, d_5, d_6, d_7, d_8)$$

eine Zeile von R, so gilt also

$$(*) \qquad \Phi((-1)^r \varepsilon^s \pi_2^{c_1} \dots \pi_{17b}^{c_9}) = (-1)^t 2^{d_1} \dots 19^{d_8} \bmod N.$$

Elementare Zeilenumformungen ändern nichts an der Eigenschaft $(*)$. Elementare Zeilenumformungen lassen sich auch beschreiben durch Multiplikation der Matrix R mit einer Matrix T von links, d.h. man geht von R zu TR über. Wir bestimmen (mit Maple) eine Matrix T, die als Einträge nur 0 und 1 hat,

sodass TR modulo 2 obere Dreiecksgestalt hat. (T ist auch invertierbar modulo 2.)

$$T = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}$$

Wir erhalten:

$$TR = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 4 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 2 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 2 & 5 & 1 & 2 & 0 & 0 & 0 & 0 & 0 \\
0 & -2 & 2 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 \\
0 & -2 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 2 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & -2 & 0 & 2 & 0 & 0 & 2 & 1 & 2 & 1 & 2 & 1 & 6 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\
0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 5 & 2 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & -2 & 6 & 2 & 0 & 0 & 2 & 0 & 0 & 1 & 2 & 1 & 3 & 3 & 1 & 0 & 0 & 1 & 2 & 0 \\
0 & -2 & 6 & 2 & 2 & 0 & 2 & 0 & 2 & 0 & 1 & 3 & 6 & 4 & 1 & 0 & 0 & 2 & 1 & 1 \\
0 & -4 & 6 & 2 & 0 & 2 & 2 & 2 & 2 & 0 & 0 & 3 & 5 & 6 & 1 & 3 & 0 & 0 & 0 & 0 \\
0 & -2 & 4 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 2 & 3 & 1 & 0 & 2 & 1 & 0 & 1 & 0 \\
0 & -4 & 8 & 4 & 2 & 4 & 2 & 0 & 0 & 0 & 0 & 4 & 8 & 3 & 1 & 2 & 1 & 1 & 1 & 1 \\
0 & -6 & 2 & 4 & 2 & 4 & 2 & 2 & 2 & 2 & 2 & 2 & 8 & 4 & 1 & 1 & 2 & 1 & 2 & 1 \\
0 & -4 & 4 & 6 & 6 & 2 & 2 & 2 & 2 & 0 & 0 & 4 & 18 & 2 & 2 & 3 & 1 & 1 & 1 & 0 \\
0 & -4 & 2 & 4 & 4 & 2 & 2 & 0 & 0 & 2 & 2 & 4 & 6 & 0 & 2 & 2 & 1 & 1 & 1 & 1 \\
0 & -8 & 2 & 8 & 12 & 2 & 2 & 2 & 2 & 4 & 2 & 4 & 22 & 4 & 2 & 0 & 2 & 2 & 1 & 1 \\
0 & -10 & 8 & 6 & 6 & 8 & 2 & 2 & 2 & 2 & 0 & 6 & 16 & 6 & 2 & 2 & 2 & 0 & 2 & 2 \\
0 & -8 & 8 & 4 & 8 & 2 & 0 & 4 & 2 & 2 & 2 & 4 & 14 & 4 & 4 & 2 & 2 & 0 & 2 & 0 \\
0 & -8 & 12 & 6 & 4 & 6 & 2 & 0 & 2 & 2 & 0 & 6 & 12 & 4 & 4 & 0 & 4 & 0 & 0 & 2 \\
0 & -8 & 8 & 6 & 8 & 2 & 2 & 4 & 2 & 2 & 2 & 6 & 18 & 4 & 4 & 2 & 2 & 2 & 2 & 0 \\
0 & -6 & 2 & 4 & 10 & 2 & 2 & 0 & 2 & 2 & 4 & 4 & 14 & 2 & 2 & 0 & 0 & 2 & 2 & 2 \\
0 & -8 & 4 & 8 & 12 & 4 & 2 & 2 & 4 & 2 & 0 & 4 & 22 & 4 & 2 & 2 & 0 & 2 & 2 & 2 \\
0 & -4 & 4 & 2 & 10 & 2 & 0 & 0 & 0 & 0 & 0 & 2 & 4 & 0 & 2 & 0 & 0 & 0 & 0 & 2
\end{pmatrix}$$

Bezeichnet nun

$$(r, s, c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8, c_9, t, d_1, d_2, d_3, d_4, d_5, d_6, d_7, d_8)$$

eine Zeile i von TR, so gilt weiterhin

$$(*) \qquad \Phi((-1)^r \varepsilon^s \pi_2^{c_1} \dots \pi_{17b}^{c_9}) = (-1)^t 2^{d_1} \dots 19^{d_8} \bmod N.$$

Sind jetzt alle Einträge der Zeile i gerade, so können wir definieren

$$\begin{aligned} \xi_i &= (-1)^{r/2} \varepsilon^{s/2} \pi_2^{c_1/2} \dots \pi_{17b}^{c_9/2}, \\ y_i &= (-1)^{t/2} 2^{d_1/2} \dots 19^{d_8/2} \bmod N, \end{aligned}$$

und erhalten dann

$$\Phi(\xi_i)^2 \equiv y_i^2 \bmod N.$$

Nun berechnen wir $\mathrm{ggT}(\Phi(\xi_i) - y_i, N)$ und schauen, ob wir einen nichttrivialen Teiler von N gefunden haben.

In unserem Fälle sind sämtliche Einträge der Zeilen 19 bis 25 gerade. Wir erhalten dafür folgende Tabelle

Zeile i	$\Phi(\xi_i)$	y_i	$\mathrm{ggT}(\Phi(\xi_i) - y_i, N)$
19	29231	28145	181
20	5634	23869	1
21	26269	26269	29503
22	27441	27441	29503
23	20475	7761	163
24	18071	11432	1
25	28797	29123	163

und daraus die Faktorisierung $N = 163 \cdot 181$.

8. RSA-155

Am 22. August 1999 wurde die Zahl RSA-155 (155 Dezimalstellen, 512 Bits)

$$\begin{aligned} \text{RSA-155} = {} & 109417386415705274218097073220403576120037329454492059909138421314763\backslash \\ & 499842889347847179972578912673324976257528997818337970765372440271467\backslash \\ & 43531593354333897 \end{aligned}$$

mit dem Zahlkörpersieb erfolgreich in das Produkt der folgenden Primzahlen zerlegt:

$$\begin{aligned} p &= 10263959282974110577205419657399167590071656780803806680334193352179071130777 9, \\ q &= 10660348838016845482092722036001287867920795857598929152227060823719306280864 3. \end{aligned}$$

Zugrunde lag das Polynom

$$\begin{aligned} f = {} & 406798435423621593619137084050 64 + 74596615800717864439197430 56x - \\ & - 11816848430079521880356852x^2 - 66269852234118574445x^3 + \\ & + 80168937284997582x^4 + 119377138320x^5 \end{aligned}$$

mit

$$m = -391230797211680007713134490 81.$$

Dann gilt nämlich $f(m) \equiv 0 \bmod$ RSA-155. (Will man ein normiertes Polynom haben, so substituiert man

$$x = \frac{1}{19896189720} y$$

und erhält

$$\begin{aligned} \widetilde{f}(y) = {} & 106244798580898516451304128187717669141680935476113603152697 1848816640000 + \\ & + 97921400337192155710387520490307096131345565476563604480 00y - \\ & - 77963305056772650110395228784436823810073280 0y^2 - \\ & - 21975292546106483568894395090 0y^3 + 1336148954749959 7y^4 + y^5. \end{aligned}$$

Für

$$\widetilde{m} = -77840021656304324333915871650313564732 0$$

gilt dann wieder die Aussage $\widetilde{f}(\widetilde{m}) \equiv 0 \bmod$ RSA-155.)

- Im ersten Schritt wurde das zugrundegelegte Polynom sorgfältig gewählt. (Das brauchte 0.40 CPU-Jahre mit einem 250 MHz-Prozessor $\approx$ 100 MIPS Jahre.)
- Nach Relationen wurde 3.7 Monate lang gesucht mit $\approx$ 300 Rechner (35.7 CPU-Jahre mit Prozessoren zwischen 175 und 500 MHz). Es wurden 124722179 Relationen gesammelt.
- Aus den Relationen wurde die Matrix mit 6699181 Zeilen und 6711336 Spalten zusammengestellt. (Allerdings gab es nur 417132631 von 0 verschiedene Einträge, d.h. $\approx$ 62 Nichtnullen pro Spalte und auch pro Zeile. Um diese Matrix erfolgreich zu bearbeiten brauchte es 224 CPU-Stunden und 3.2 GBytes Arbeitsspeicher (central memory) auf einer Cray C916.
- Die Gesamtzeit betrug 7.4 Monate.

9. Beispiel für den Siebprozess

Wir führen die Siebprozesse für unser Beispiel mit den Parametern $A = 10$, $B = 6$ durch.
Die folgenden Tabellen enthalten $S[a,b]$. Zu Beginn ist $S[a,b] = \ln|am+b|$, falls $\mathrm{ggT}(a,b) = 1$ und $am + b \neq 0$ ist.
(a,b) durchlaufen 130 Elemente.

$S[a,b]$	$b=-6$	$b=-5$	$b=-4$	$b=-3$	$b=-2$	$b=-1$	$b=0$	$b=1$	$b=2$	$b=3$	$b=4$	$b=5$	$b=6$
$a=1$	3.8	3.8	3.8	3.8	3.9	3.9	3.9	3.9	3.9	4.0	4.0	4.0	4.0
$a=2$		4.5		4.6		4.6		4.6		4.6		4.6	
$a=3$		5.0	5.0		5.0	5.0		5.0	5.0		5.0	5.0	
$a=4$		5.3		5.3		5.3		5.3		5.3		5.3	
$a=5$	5.5		5.5	5.5	5.5	5.5		5.5	5.5	5.5	5.5		5.5
$a=6$		5.7				5.7		5.7				5.7	
$a=7$	5.8	5.8	5.8	5.8	5.8	5.8		5.8	5.8	5.8	5.8	5.9	5.9
$a=8$		6.0		6.0		6.0		6.0		6.0		6.0	
$a=9$		6.1	6.1		6.1	6.1		6.1	6.1		6.1	6.1	
$a=10$				6.2		6.2		6.2		6.2			

(Es bleiben 77 sinnvolle Elemente.)
$p = 2$ ausgesiebt:

$S[a,b]$	$b=-6$	$b=-5$	$b=-4$	$b=-3$	$b=-2$	$b=-1$	$b=0$	$b=1$	$b=2$	$b=3$	$b=4$	$b=5$	$b=6$
$a=1$	3.8	2.4	3.8	3.1	3.9	1.1	3.9	3.2	3.9	2.6	4.0	3.3	4.0
$a=2$		4.5		4.6		4.6		4.6		4.6		4.6	
$a=3$		4.3	5.0		5.0	4.3		3.6	5.0		5.0	2.9	
$a=4$		5.3		5.3		5.3		5.3		5.3		5.3	
$a=5$	5.5		5.5	4.8	5.5	4.1		4.8	5.5	3.4	5.5		5.5
$a=6$		5.7				5.7		5.7				5.7	
$a=7$	5.8	5.1	5.8	4.4	5.8	5.1		3.8	5.8	5.2	5.8	4.5	5.9
$a=8$		6.0		6.0		6.0		6.0		6.0		6.0	
$a=9$		4.7	6.1		6.1	4.0		5.4	6.1		6.1	5.4	
$a=10$				6.2		6.2		6.2		6.2			

$p = 3$ ausgesiebt:

$S[a,b]$	$b=-6$	$b=-5$	$b=-4$	$b=-3$	$b=-2$	$b=-1$	$b=0$	$b=1$	$b=2$	$b=3$	$b=4$	$b=5$	$b=6$
$a=1$	3.8	2.4	1.6	3.1	3.9	-.0	3.9	3.2	2.8	2.6	4.0	-.0	4.0
$a=2$		3.4		4.6		4.6		2.4		4.6		4.6	
$a=3$		4.3	5.0		5.0	4.3		3.6	5.0		5.0	2.9	
$a=4$		5.3		5.3		4.2		5.3		5.3		4.2	
$a=5$	5.5		5.5	4.8	-.0	4.1		3.7	5.5	3.4	4.4		5.5
$a=6$		5.7				5.7		5.7				5.7	
$a=7$	5.8	5.1	4.7	4.4	5.8	2.9		3.8	4.7	5.2	5.8	3.4	5.9
$a=8$		3.8		6.0		6.0		4.9		6.0		6.0	
$a=9$		4.7	6.1		6.1	4.0		5.4	6.1		6.1	5.4	
$a=10$				6.2		5.1		6.2		6.2			

$p = 5$ ausgesiebt:

$S[a,b]$	$b=-6$	$b=-5$	$b=-4$	$b=-3$	$b=-2$	$b=-1$	$b=0$	$b=1$	$b=2$	$b=3$	$b=4$	$b=5$	$b=6$
$a=1$	3.8	2.4	0.0	3.1	3.9	-.0	3.9	0.0	2.8	2.6	4.0	-.0	2.4
$a=2$		3.4		2.9		4.6		2.4		4.6		4.6	
$a=3$		4.3	5.0		3.4	4.3		3.6	5.0		5.0	2.9	
$a=4$		5.3		5.3		2.6		5.3		5.3		4.2	
$a=5$	5.5		5.5	4.8	-.0	4.1		3.7	5.5	3.4	4.4		5.5
$a=6$		5.7				5.7		4.1				5.7	
$a=7$	5.8	5.1	4.7	2.8	5.8	2.9		3.8	3.1	5.2	5.8	3.4	5.9
$a=8$		3.8		6.0		6.0		4.9		4.4		6.0	
$a=9$		4.7	6.1		6.1	2.4		5.4	6.1		4.5	5.4	
$a=10$				6.2		5.1		6.2		6.2			

$p = 7$ ausgesiebt:

$S[a,b]$	$b=-6$	$b=-5$	$b=-4$	$b=-3$	$b=-2$	$b=-1$	$b=0$	$b=1$	$b=2$	$b=3$	$b=4$	$b=5$	$b=6$
$a=1$	3.8	2.4	0.0	3.1	3.9	-.0	0.0	0.0	2.8	2.6	4.0	-.0	2.4
$a=2$		3.4		2.9		4.6		2.4		4.6		4.6	
$a=3$		4.3	5.0		3.4	4.3		3.6	5.0		5.0	2.9	
$a=4$		5.3		5.3		2.6		5.3		5.3		4.2	
$a=5$	5.5		5.5	4.8	-.0	4.1		3.7	5.5	3.4	4.4		5.5
$a=6$		5.7				5.7		4.1				5.7	
$a=7$	5.8	5.1	4.7	2.8	5.8	2.9		3.8	3.1	5.2	5.8	3.4	5.9
$a=8$		3.8		6.0		6.0		4.9		4.4		6.0	
$a=9$		4.7	6.1		6.1	2.4		5.4	6.1		4.5	5.4	
$a=10$				6.2		5.1		6.2		6.2			

$p = 11$ ausgesiebt:

$S[a,b]$	$b=-6$	$b=-5$	$b=-4$	$b=-3$	$b=-2$	$b=-1$	$b=0$	$b=1$	$b=2$	$b=3$	$b=4$	$b=5$	$b=6$
$a=1$	3.8	-.0	0.0	3.1	3.9	-.0	0.0	0.0	2.8	2.6	4.0	-.0	0.0
$a=2$		3.4		2.9		4.6		-.0		4.6		4.6	
$a=3$		4.3	2.6		3.4	4.3		3.6	5.0		5.0	2.9	
$a=4$		5.3		5.3		2.6		5.3		5.3		4.2	
$a=5$	5.5		5.5	-.0	-.0	4.1		3.7	5.5	3.4	4.4		5.5
$a=6$		5.7				5.7		4.1				5.7	
$a=7$	5.8	5.1	4.7	2.8	3.4	2.9		3.8	3.1	5.2	5.8	3.4	5.9
$a=8$		3.8		6.0		6.0		4.9		4.4		6.0	
$a=9$		4.7	6.1		6.1	-.0		5.4	6.1		4.5	5.4	
$a=10$				6.2		5.1		6.2		6.2			

$p = 13$ ausgesiebt:

$S[a,b]$	$b=-6$	$b=-5$	$b=-4$	$b=-3$	$b=-2$	$b=-1$	$b=0$	$b=1$	$b=2$	$b=3$	$b=4$	$b=5$	$b=6$
$a=1$	3.8	-.0	0.0	3.1	3.9	-.0	0.0	0.0	2.8	0.0	4.0	-.0	0.0
$a=2$		3.4		2.9		4.6		-.0		4.6		4.6	
$a=3$		4.3	0.0		3.4	4.3		3.6	5.0		5.0	2.9	
$a=4$		5.3		5.3		.0		5.3		5.3		4.2	
$a=5$	5.5		5.5	-.0	-.0	4.1		3.7	2.9	3.4	4.4		5.5
$a=6$		5.7				5.7		4.1				3.1	
$a=7$	5.8	0.0	4.7	2.8	3.4	2.9		3.8	3.1	5.2	5.8	3.4	5.9
$a=8$		3.8		6.0		6.0		4.9		4.4		6.0	
$a=9$		4.7	6.1		6.1	-.0		2.8	6.1		4.5	5.4	
$a=10$				6.2		5.1		6.2		6.2			

$p = 17$ ausgesiebt:

$S[a,b]$	$b=-6$	$b=-5$	$b=-4$	$b=-3$	$b=-2$	$b=-1$	$b=0$	$b=1$	$b=2$	$b=3$	$b=4$	$b=5$	$b=6$
$a=1$	3.8	-.0	0.0	3.1	3.9	-.0	0.0	0.0	0.0	0.0	4.0	-.0	0.0
$a=2$		3.4		2.9		4.6		-.0		4.6		4.6	
$a=3$		4.3	0.0		3.4	4.3		3.6	5.0		5.0	2.9	
$a=4$		5.3		5.3		.0		5.3		5.3		4.2	
$a=5$	5.5		5.5	-.0	-.0	4.1		3.7	2.9	3.4	4.4		5.5
$a=6$		0.0				5.7		4.1				3.1	
$a=7$	5.8	0.0	4.7	0.0	3.4	2.9		3.8	3.1	5.2	5.8	3.4	5.9
$a=8$		3.8		6.0		3.1		4.9		4.4		6.0	
$a=9$		4.7	6.1		6.1	-.0		0.0	6.1		4.5	5.4	
$a=10$				6.2		5.1		6.2		3.4			

$p = 19$ ausgesiebt:

$S[a,b]$	$b=-6$	$b=-5$	$b=-4$	$b=-3$	$b=-2$	$b=-1$	$b=0$	$b=1$	$b=2$	$b=3$	$b=4$	$b=5$	$b=6$
$a=1$	3.8	-.0	0.0	3.1	3.9	-.0	0.0	0.0	0.0	0.0	4.0	-.0	0.0
$a=2$		3.4		.0		4.6		-.0		4.6		4.6	
$a=3$		4.3	0.0		3.4	4.3		3.6	5.0		5.0	-.0	
$a=4$		5.3		5.3		.0		5.3		5.3		4.2	
$a=5$	5.5		5.5	-.0	-.0	4.1		3.7	.0	3.4	4.4		5.5
$a=6$		0.0				5.7		4.1				3.1	
$a=7$	5.8	0.0	4.7	0.0	3.4	-.0		3.8	3.1	5.2	5.8	3.4	5.9
$a=8$		3.8		6.0		3.1		4.9		4.4		6.0	
$a=9$		4.7	3.1		6.1	-.0		0.0	6.1		4.5	5.4	
$a=10$				6.2		5.1		6.2		3.4			

Am Ende des 1. Siebprozesses bleiben 23 Paare (a,b) übrig:

$$(9,-1),(9,1),(3,-4),(3,5),(4,-1),(5,-3),(5,-2),(5,2),(6,-5),(7,-5),(7,-3),(7,-1),(1,5),$$

$$(1,6),(2,-3),(2,1),(1,-5),(1,-4),(1,-1),(1,0),(1,1),(1,2),(1,3).$$

Für die verbleibenden 23 Elemente wird nun $T[a,b] = \ln|\mathrm{N}(a\alpha + b)|$ betrachtet:

$T[a,b]$	$b=-6$	$b=-5$	$b=-4$	$b=-3$	$b=-2$	$b=-1$	$b=0$	$b=1$	$b=2$	$b=3$	$b=4$	$b=5$	$b=6$
$a=1$		5.2	4.7			3.3	3.0	2.5	.7	3.3		4.9	5.5
$a=2$				5.6				4.9					
$a=3$			6.8									4.6	
$a=4$						7.2							
$a=5$				8.0	8.0				7.7				
$a=6$		8.6											
$a=7$		9.1		9.0		8.9							
$a=8$													
$a=9$						9.6		9.5					
$a=10$													

$p = 2$ ausgesiebt:

$T[a,b]$	$b=-6$	$b=-5$	$b=-4$	$b=-3$	$b=-2$	$b=-1$	$b=0$	$b=1$	$b=2$	$b=3$	$b=4$	$b=5$	$b=6$
$a=1$		3.8	1.9			1.9	1.6	1.1	0.0	1.9		3.6	4.8
$a=2$				5.6				4.9					
$a=3$			4.7									3.2	
$a=4$						7.2							
$a=5$				6.6	7.3				7.0				
$a=6$		8.6											
$a=7$		7.7		7.6		7.5							
$a=8$													
$a=9$						8.2		8.2					
$a=10$													

$p = 3$ ausgesiebt:

$T[a,b]$	$b=-6$	$b=-5$	$b=-4$	$b=-3$	$b=-2$	$b=-1$	$b=0$	$b=1$	$b=2$	$b=3$	$b=4$	$b=5$	$b=6$
$a=1$		1.6	1.9			1.9	1.6	-.0	0.0	1.9		3.6	4.8
$a=2$				5.6				4.9					
$a=3$			4.7									3.2	
$a=4$						7.2							
$a=5$				6.6	7.3				4.8				
$a=6$		8.6											
$a=7$		6.6		7.6		7.5							
$a=8$													
$a=9$						8.2		8.2					
$a=10$													

$p = 5$ ausgesiebt:

$T[a,b]$	$b=-6$	$b=-5$	$b=-4$	$b=-3$	$b=-2$	$b=-1$	$b=0$	$b=1$	$b=2$	$b=3$	$b=4$	$b=5$	$b=6$
$a=1$		-.0	1.9			1.9	0.0	-.0	0.0	1.9		1.9	4.8
$a=2$				5.6				4.9					
$a=3$			4.7									0.0	
$a=4$						7.2							
$a=5$				6.6	7.3				4.8				
$a=6$		7.0											
$a=7$		3.4		7.6		7.5							
$a=8$													
$a=9$						8.2		8.2					
$a=10$													

$p = 7$ ausgesiebt:

$T[a,b]$	$b=-6$	$b=-5$	$b=-4$	$b=-3$	$b=-2$	$b=-1$	$b=0$	$b=1$	$b=2$	$b=3$	$b=4$	$b=5$	$b=6$
$a=1$		-.0	-.0			-.0	0.0	-.0	0.0	-.0		0.0	2.8
$a=2$				5.6				4.9					
$a=3$			4.7									0.0	
$a=4$						5.3							
$a=5$				4.7	7.3				2.8				
$a=6$		5.1											
$a=7$		3.4		7.6		7.5							
$a=8$													
$a=9$						6.3		8.2					
$a=10$													

$p = 17$ ausgesiebt:

$T[a,b]$	$b=-6$	$b=-5$	$b=-4$	$b=-3$	$b=-2$	$b=-1$	$b=0$	$b=1$	$b=2$	$b=3$	$b=4$	$b=5$	$b=6$
$a=1$		-.0	-.0			-.0	0.0	-.0	0.0	-.0		0.0	0.0
$a=2$				5.6				4.9					
$a=3$			4.7									0.0	
$a=4$						5.3							
$a=5$				4.7	7.3				-.0				
$a=6$		5.1											
$a=7$		3.4		7.6		7.5							
$a=8$													
$a=9$						6.3		8.2					
$a=10$													

Es bleiben 11 Paare (a, b) uebrig:

$$(1,-5),(1,-4),(1,-1),(1,0),(1,1),(1,2),(1,3),(1,5),(1,6),(3,5),(5,2).$$

KAPITEL 12

Die diophantischen Gleichungen $x^3+y^3=z^3$ und $x^3+y^3=3^n z^3$

1. Einführung

Die Gleichung $x^3+y^3=z^3$ hat natürlich offensichtlich die Lösungen

$$(x,y,z)=(0,1,1),\quad (1,0,1),\quad (1,-1,0).$$

Wir wollen zeigen, dass keine Lösung mit $x,y,z\in\mathbf{Z}$ und $xyz\neq 0$ existiert. Beim Beweis werden wir den Zahlkörper $\mathbf{Q}(\sqrt{-3})$ benutzen. Wir stellen daher einige Aussagen über diesen Zahlkörper zusammen:

Wir betrachten $K=\mathbf{Q}(\sqrt{-3})$. Mit

$$\zeta=\frac{-1+\sqrt{-3}}{2}$$

gilt

$$\mathbf{Z}_K=\mathbf{Z}[\zeta]\quad\text{und}\quad \zeta^2+\zeta+1=0\quad\text{bzw.}\quad \zeta^2=-\zeta-1.$$

$\mathbf{Z}_K$ ist ein Hauptidealring. Für

$$\pi=1-\zeta$$

gilt

$$\pi^2=-3\zeta.$$

(π) ist das einzige 3 enthaltende Primideal von $\mathbf{Z}_K$. Die Einheitengruppe von $\mathbf{Z}_K$ ist

$$\mathbf{Z}_K^*=\{\pm 1,\pm\zeta,\pm\zeta^2\}\quad\text{mit}\quad \zeta^3=1.$$

Ziel ist der Beweis des folgenden Satzes:

SATZ. *Sei $m\geq 0$ und $\varepsilon\in\{1,\zeta,\zeta^2\}$. Genau dann gibt es $x,y,z\in\mathbf{Z}_K\setminus\{0\}$ mit*

$$x^3+y^3=\varepsilon\pi^m z^3,$$

wenn gilt

$$m\equiv 1 \bmod 3\quad\text{und}\quad \varepsilon=\zeta.$$

Als unmittelbare Folgerung erhalten wir den Satz:

SATZ. *Es gibt keine $x,y,z\in\mathbf{Z}_K\setminus\{0\}$ mit*

$$x^3+y^3=z^3.$$

SATZ. *Die Gleichungen $x^3+y^3=z^3$ und $x^3+y^3=3z^3$ haben keine Lösungen $x,y,z\in\mathbf{Z}$ mit $xyz\neq 0$. Die Gleichung $x^3+y^3=9z^3$ hat die Lösung $(x,y,z)=(1,2,1)$.*

Beweis: Wir nehmen an, es gibt $x,y,z\in\mathbf{Z}$ mit $xyz\neq 0$ und

$$x^3+y^3=3^n z^3.$$

Wegen $3=-\zeta^2\pi^2$ gilt

$$x^3+y^3=(-1)^n\zeta^{2n}\pi^{2n}z^3=\zeta^{2n}\pi^{2n}((-1)^n z)^3.$$

Der Hauptsatz impliziert $\zeta^{2n}=\zeta$ und $2n\equiv 1 \bmod 3$, was genau die Bedingung $n\equiv 2 \bmod 3$ liefert. Dies zeigt, dass $x^3+y^3=z^3$ und $x^3+y^3=3z^3$ auch keine Lösungen mit $x,y,z\in\mathbf{Z}_K\setminus\{0\}$ besitzen. Der Rest ist trivial. ■

Version vom 15.2.2003

2. Die Beweise

Das folgende Lemma stellt einige im folgenden mehrfach gebrauchte Aussagen über Kongruenzen modulo π^4 zusammen.

LEMMA. 1. *Für jedes $\alpha\in\mathbf{Z}_K$ gibt es eindeutig bestimmte $a_i\in\{0,1,-1\}$ mit*

$$\alpha\equiv a_0+a_1\pi+a_2\pi^2+a_3\pi^3 \bmod \pi^4.$$

2. *Wir haben die Entwicklungen*

$$\begin{aligned}\zeta &= 1-\pi,\\ \zeta^2 &\equiv 1+\pi+\pi^2+\pi^3 \bmod \pi^4,\\ 3 &\equiv -\pi^2-\pi^3 \bmod \pi^4,\\ 2 &\equiv -1-\pi^2-\pi^3 \bmod \pi^4\end{aligned}$$

3. *Für $\alpha=a_0+a_1\pi+a_2\pi^2+a_3\pi^3 \bmod \pi^4$ mit $a_i\in\{0,1,-1\}$ gilt*

$$\alpha^3\equiv\begin{cases}a_0 \bmod \pi^4 & \text{für } a_0=\pm1,\\ a_1\pi^3 \bmod \pi^4 & \text{für } a_0=0.\end{cases}$$

Beweis:

1. Dies folgt daraus, dass $0,1,-1$ ein Repräsentantensystem von $\mathbf{Z}_K/(\pi)$ ist.
2. Aus $\pi=1-\zeta$ und $\pi^2=-3\zeta$ folgt

$$\begin{aligned}\zeta &= 1-\pi,\\ \zeta^2 &= 1-2\pi+\pi^2=1+(1-3)\pi+\pi^2=1+\pi+\pi^2-3\pi=1+\pi+\pi^2+(-3\zeta)\zeta^2\pi=\\ &= 1+\pi+\pi^2+\pi^2\zeta^2\pi=1+\pi+\pi^2+\zeta^2\pi^3=1+\pi+\pi^2+(1+\pi+\pi^2+\zeta^2\pi^3)\pi^3\equiv\\ &\equiv 1+\pi+\pi^2+\pi^3 \bmod \pi^4,\\ 3 &= (-3\zeta)(-\zeta^2)=(-\zeta^2)\pi^2\equiv(-1-\pi-\pi^2-\pi^3)\pi^2\equiv-\pi^2-\pi^3 \bmod \pi^4,\\ 2 &= -1+3\equiv-1-\pi^2-\pi^3 \bmod \pi^4\end{aligned}$$

3. Wir setzen an $\alpha\equiv a_0+a_1\pi+a_2\pi^2+a_3\pi^3 \bmod \pi^4$ und erhalten wegen $a_i^3=a_i$ $(a_i\in\{0,1,-1\})$

$$\begin{aligned}\alpha^3 &\equiv a_0^3+3a_0^2a_1\pi+(3a_0^2a_2+3a_0a_1^2)\pi^2+(3a_0^2a_3+6a_0a_1a_2+a_1^3)\pi^3\equiv\\ &\equiv a_0+(-\pi^2-\pi^3)a_0^2a_1\pi+(-\pi^2-\pi^3)(a_0^2a_2+a_0a_1^2)\pi^2+\\ &\quad+(-\pi^2-\pi^3)(a_0^2a_3+2a_0a_1a_2)\pi^3+a_1\pi^3\\ &\equiv a_0-a_0^2a_1\pi^3+a_1\pi^3=a_0+a_1(1-a_0^2)\pi^3 \bmod \pi^4.\end{aligned}$$

Daraus folgt

$$\alpha^3\equiv\begin{cases}a_0 \bmod \pi^4 & \text{für } a_0=\pm1,\\ a_1\pi^3 \bmod \pi^4 & \text{für } a_0=0,\end{cases}$$

was die Behauptung beweist. ■

LEMMA. *Für $x,y,z\in\mathbf{Z}_K$ mit $x,y,z\not\equiv0 \bmod \pi$ und $\varepsilon\in\mathbf{Z}_K^*$ gilt*

$$x^3+y^3\not\equiv\varepsilon z^3 \bmod \pi^4.$$

Insbesondere gilt $x^3+y^3\neq\varepsilon z^3$.

Beweis: $x,y,z\not\equiv0 \bmod \pi$ impliziert $x\equiv\pm1 \bmod \pi$, $y\equiv\pm1 \bmod \pi$, $z\equiv\pm1 \bmod \pi$. Dann folgt $x^3\equiv\pm1 \bmod \pi^4$, $y^3\equiv\pm1 \bmod \pi^4$, $z^3\equiv\pm1 \bmod \pi^4$, also $x^3+y^3\equiv2,0,-2 \bmod \pi^4$. Mit $\varepsilon\in\mathbf{Z}_K^*=$

$\{\pm 1, \pm\zeta, \pm\zeta^2\}$ und den zuvor hergeleiteten Entwicklungen erhält man

$$x^3+y^3 \equiv \begin{cases} -1-\pi^2-\pi^3 \bmod \pi^4 & \text{oder} \\ 0 \bmod \pi^4 & \text{oder} \\ 1+\pi^2+\pi^3 \bmod \pi^4 & \end{cases} \quad \text{und} \quad \varepsilon z^3 \equiv \begin{cases} 1 \bmod \pi^4 & \text{oder} \\ -1 \bmod \pi^4 & \text{oder} \\ 1-\pi \bmod \pi^4 & \text{oder} \\ -1+\pi \bmod \pi^4 & \text{oder} \\ 1+\pi+\pi^2+\pi^3 \bmod \pi^4 & \text{oder} \\ -1-\pi-\pi^2-\pi^3 \bmod \pi^4, & \end{cases}$$

was sofort die Behauptung zeigt. ■

LEMMA. *Sind $x, y, z \in \mathbf{Z}_K \setminus \{0\}$, $\varepsilon \in \{1, \zeta, \zeta^2\}$, $m \geq 1$ mit*

$$x^3+y^3 = \varepsilon\pi^m z^3 \quad \textit{und} \quad v_\pi(x) = v_\pi(y) = v_\pi(z) = 0,$$

so gilt:

1. *Es ist $m \geq 4$.*
2. *Es gibt $x_1, y_1, z_1 \in \mathbf{Z}_K \setminus \{0\}$, $\eta \in \{1, \zeta, \zeta^2\}$ mit*
$$x_1^3+\eta y_1^3 = \varepsilon\eta^2\pi^{m-3} z_1^3 \quad \textit{und} \quad v_\pi(x_1) = v_\pi(y_1) = v_\pi(z_1) = 0.$$
3. *Ist $m \geq 5$, so gilt $\eta = 1$.*
4. *Ist $m = 4$, so gilt $\varepsilon = \zeta$.*

Beweis: Nach eventueller Division von x, y, z durch $\mathrm{ggT}(x, y, z)$ können wir immer $\mathrm{ggT}(x, y, z) = 1$ voraussetzen.

1. Modulo π gilt $0 \equiv x^3+y^3 \equiv (x+y)^3 \bmod \pi$, also $x+y \equiv 0 \bmod \pi$ und damit $\frac{x}{y} \equiv -1 \bmod \pi$. Dies impliziert, wie früher gezeigt wurde, $(\frac{x}{y})^3 \equiv -1 \bmod \pi^4$ und damit $x^3+y^3 \equiv 0 \bmod \pi^4$, was sofort die Behauptung $m \geq 4$ zeigt.
2. (a) Wegen $\frac{x}{y} \equiv -1 \bmod \pi$ gibt es ein $c \in \{-1, 0, 1\}$ mit $\frac{x}{y} \equiv -1 + c\pi \bmod \pi^2$. Dann ist (mit $\zeta = 1-\pi$)
$$\begin{aligned} \frac{\zeta x}{y} &\equiv (1-\pi)(-1+c\pi) \equiv -1+(1+c)\pi \bmod \pi^2, \\ \frac{\zeta^2 x}{y} &\equiv (1-2\pi)(-1+c\pi) \equiv -1+(2+c)\pi \equiv -1+(-1+c) \bmod \pi^2. \end{aligned}$$
Nun ist $-\zeta^2 \equiv -1-\pi \bmod \pi^2$. Geht man von x zu ζx oder $\zeta^2 x$ über, so ändert sich an der Ausgangsgleichung nichts. Also können wir o.E.
$$\frac{x}{y} \equiv -\zeta^2 \bmod \pi^2$$
annehmen. Dann folgt
$$x+\zeta^2 y \equiv 0 \bmod \pi^2.$$

   (b) Wir haben
$$\begin{aligned} x+y &= (x+\zeta^2 y)+(1-\zeta^2)y = (x+\zeta^2 y)+\pi(2-\pi)y, \\ x+\zeta y &= (x+\zeta^2 y)+\zeta(1-\zeta)y = (x+\zeta^2 y)+\zeta\pi y, \end{aligned}$$
was mit $v_\pi(x+\zeta^2 y) \geq 2$ sofort
$$v_\pi(x+y) = v_\pi(x+\zeta y) = 1$$
liefert. Die Zerlegung
$$(x+y)(x+\zeta y)(x+\zeta^2 y) = x^3+y^3 = \varepsilon\pi^m z^3$$
liefert nun
$$v_\pi(x+y) = 1, \quad v_\pi(x+\zeta y) = 1, \quad v_\pi(x+\zeta^2 y) = m-2.$$

(c) Wir wollen nun untersuchen, welche gemeinsamen Teiler die Faktoren auf der linken Seite folgender Gleichung haben können:

$$(x+y)(x+\zeta y)(x+\zeta^2 y)=\varepsilon\pi^m z^3.$$

Angenommen, $\mathfrak{p}|x+y$ und $\mathfrak{p}|x+\zeta y$. Dann folgt auch $\mathfrak{p}|\zeta x+\zeta y$ und durch Subtraktion $\mathfrak{p}|(1-\zeta)y$ und $\mathfrak{p}|(1-\zeta)x$, also $\mathfrak{p}|\pi x$ und $\mathfrak{p}|\pi y$. Das Primideal $\mathfrak{p}$ teilt auch die rechte Seite der Gleichung, also gilt $\mathfrak{p}|\pi z$. Da wir uns auf den Fall $\mathrm{ggT}(x,y,z)=1$ zurückgezogen haben, folgt $\mathfrak{p}|\pi$, also $\mathfrak{p}=(\pi)$. Genauso sieht man die folgenden Aussagen:

$$\mathrm{ggT}(x+y,x+\zeta y)|\pi,\quad \mathrm{ggT}(x+y,x+\zeta^2 y)|\pi,\quad \mathrm{ggT}(x+\zeta y,x+\zeta^2 y)|\pi.$$

Die Anteile von π haben wir aber bereits bestimmt.

(d) Die eindeutige Primfaktorzerlegung liefert jetzt aus

$$(x+y)\cdot(x+\zeta y)\cdot(x+\zeta^2 y)=\varepsilon\pi^m z^3$$

Darstellungen

$$x+y=u\pi x_1^3,\quad x+\zeta y=v\pi y_1^3,\quad x+\zeta^2 y=-w\pi^{m-2}z_1^3$$

mit Einheiten $u,v,w\in\mathbf{Z}_K^*$ und $x_1,y_1,z_1\in\mathbf{Z}_K$ mit $x_1,y_1,z_1\not\equiv 0 \bmod \pi$. Dabei können wir $u,v,w\in\{1,\zeta,\zeta^2\}$ annehmen. Das Vorzeichen bei z_1^3 wurde für spätere Formulierungen gewählt. Man beachte, dass $m\geq 4$ gezeigt wurde. Die Gleichung

$$\varepsilon\pi^m z^3=u\pi x_1^3\cdot v\pi y_1^3\cdot(-1)w\pi^{m-2}z_1^3$$

liefert wegen $u,v,w,\varepsilon\in\{1,\zeta,\zeta^2\}$

$$\varepsilon=uvw\quad\text{ und }\quad z=-x_1y_1z_1.$$

Es folgt sofort mit $\pi=1-\zeta$ durch Elimination

$$x=-\zeta ux_1^3+vy_1^3,\quad y=ux_1^3-vy_1^3.$$

Daraus erhalten wir

$$\begin{aligned}
-w\pi^{m-2}z_1^3 &= x+\zeta^2 y=\\
&= (-\zeta ux_1^3+vy_1^3)+\zeta^2(ux_1^3-vy_1^3)=\\
&= -\zeta(1-\zeta)ux_1^3+(1+\zeta)(1-\zeta)vy_1^3=\\
&= -\zeta(1-\zeta)ux_1^3-\zeta^2(1-\zeta)vy_1^3=-\zeta\pi ux_1^3-\zeta^2\pi vy_1^3=\\
&= -\zeta u\pi(x_1^3+\frac{\zeta v}{u}y_1^3),
\end{aligned}$$

also

$$x_1^3+\frac{\zeta v}{u}y_1^3=\frac{w}{\zeta u}\pi^{m-3}z_1^3.$$

Es gilt mit $\varepsilon=uvw$

$$\frac{\zeta v}{u}=\frac{\zeta u^2 v}{u^3}=\zeta u^2 v,\quad \frac{w}{\zeta u}=\frac{uvw}{\zeta u^2 v}=\frac{\varepsilon}{\zeta u^2 v}=\frac{\varepsilon\zeta^2 uv^2}{\zeta^3 u^3 v^3}=\varepsilon\zeta^2 uv^2,$$

was

$$x_1^3+\zeta u^2 vy_1^3=\varepsilon\zeta^2 uv^2\pi^{m-3}z_1^3$$

zeigt. Schreiben wir $\eta=\zeta u^2 v\in\{1,\zeta,\zeta^2\}$, so erhalten wir schließlich die gewünschte Darstellung

$$x_1^3+\eta y_1^3=\varepsilon\eta^2\pi^{m-3}z_1^3.$$

3. Ist nun $m\geq 5$, so folgt aus der letzten Gleichung

$$\eta\equiv-(\frac{x_1}{y_1})^3 \bmod \pi^2.$$

Wegen

$$\begin{aligned} -(\frac{x_1}{y_1})^3 &\equiv \pm 1 \bmod \pi^4, \\ 1 &\equiv 1 \bmod \pi^2, \\ \zeta &\equiv 1-\pi \bmod \pi^2, \\ \zeta^2 &\equiv (1-\pi)^2 \equiv 1-2\pi \equiv 1+\pi \bmod \pi^2 \end{aligned}$$

ist nur $\eta = 1$ möglich, was die Behauptung beweist.

4. Im Fall $m = 4$ erhalten wir die Gleichung

$$x_1^3 + \eta y_1^3 = \varepsilon \eta^2 \pi z_1^3$$

mit $\varepsilon, \eta \in \{1, \zeta, \zeta^2\}$. Modulo π gilt wegen $\zeta \equiv \zeta^2 \equiv 1 \bmod \pi$ die Kongruenz $(x_1+y_1)^3 \equiv x_1^3+\eta y_1^3 \equiv 0 \bmod pi$, was $y_1 \equiv -x_1 \bmod \pi$ liefert. Nach eventueller Multiplikation mit -1 können wir o.E. $x_1 \equiv 1 \bmod \pi$ und $y_1 \equiv -1 \bmod \pi$ annehmen. Modulo π^4 erhalten wir

$$1-\eta \equiv \varepsilon\eta^2\pi(\pm 1) \bmod \pi^4 \quad \text{bzw.} \quad \varepsilon\pi \equiv \pm(\eta-\eta^2) \bmod \pi^4.$$

Wir betrachten $\eta = 1, \zeta, \zeta^2$:

$$\begin{aligned} 1-1^2 &= 0, \\ \zeta-\zeta^2 &= \zeta(1-\zeta) = (1-\pi)\pi \equiv \pi-\pi^2 \bmod \pi^4, \\ \zeta^2-\zeta^4 &= \zeta^2-\zeta = -(\zeta-\zeta^2) \equiv -\pi+\pi^2 \bmod \pi^4. \end{aligned}$$

Die einzige Möglichkeit ist also

$$\varepsilon\pi \equiv \pm(\pi-\pi^2) \bmod \pi^4, \quad \text{d.h.} \quad \varepsilon \equiv \pm(1-\pi) \bmod \pi^3.$$

Wegen $\zeta^2 \equiv 1+\pi+\pi^2 \bmod \pi^3$, $1 \equiv 1 \bmod \pi^3$, $\zeta \equiv 1-\pi \bmod \pi^3$ bleibt $\varepsilon = \zeta$ übrig. ■

FOLGERUNG. *Ist $m \equiv 0 \bmod 3$ oder $m \equiv 2 \bmod 3$ und $\varepsilon \in \{1, \zeta, \zeta^2\}$, so gibt es keine $x, y, z \in \mathbf{Z}_K \setminus \{0\}$ mit*

$$x^3 + y^3 = \varepsilon\pi^m z^3 \quad \textit{und} \quad v_\pi(x) = v_\pi(y) = v_\pi(z) = 0.$$

Beweis: Wir betrachten zunächst den Fall $m \equiv 2 \bmod 3$. Wir nehmen an, es gäbe eine Lösung. Dann folgt $m \geq 5$. Mit dem letzten Lemma erhält man dann sukzessiv Lösungen, wobei der Exponent bei π jeweils um 3 kleiner wird t d.h. man erhält auch Lösungen mit $m = \ldots, 11, 8, 5$. Anwendung des Lemmas für $m = 5$ führt auf den Exponenten $m = 2$, was der Abschätzung $m \geq 4$ widerspricht.
Im Fall $m \equiv 0 \bmod 3$ wurde $m = 0$ bereits abgehandelt. Sei daher $m > 0$ und $m \equiv 0 \bmod 3$ vorausgesetzt. Wegen $m \geq 4$ erhält man $m \geq 6$. Wie zuvor bekommt man Lösungen der Gleichung mit Exponenten $m = \ldots, 12, 9, 6$. Nochmalige Reduktion liefert den Widerspruch $m = 3$. ■

Bemerkung: Im Fall $m \equiv 1 \bmod 3$ kann man keinen Widerspruch erhalten, da tatsächlich eine Lösung existiert: Wegen $3 = -\zeta^2\pi^2$, $9 = \zeta\pi^4$ gilt

$$1^3 + 2^3 = 9 \cdot 1^3 = \zeta\pi^4 \cdot 1^3,$$

d.h. im Fall $m = 4$ und $\varepsilon = \zeta$ gibt es tatsächlich eine Lösung. Wegen

$$1^3 + \zeta \cdot (-1)^3 = 1-\zeta = \pi = \zeta \cdot \zeta^2 \cdot \pi^2 \cdot 1^3$$

sieht man auch, dass die Gleichung $x_1^3 + \eta y_1^3 = \varepsilon\eta^2 z_1^3$ im Fall $\eta = \zeta$, $\varepsilon = \zeta$ eine Lösung besitzt.

Bemerkung: Wir wollen nochmals die Formeln des vorangegangenen Lemmas weiterverfolgen. Wir betrachten den Fall $\eta = 1$. Aus $\eta = \zeta u^2 v$ folgt dann $v = \zeta^{-1}u^{-2} = \zeta^2 u$. Wir hatten

$$x^3 + y^3 = \varepsilon\pi^m z^3 \quad \text{und} \quad x_1^3 + y_1^3 = \varepsilon\pi^{m-3} z_1^3.$$

Für x, y, z bestanden die Beziehungen:

$$\begin{aligned} x &= -\zeta u x_1^3 + v y_1^3 = -\zeta u x_1^3 + \zeta^2 u y_1^3 = u(-\zeta x_1^3 + \zeta^2 y_1^3), \\ y &= u x_1^3 - v y_1^3 = u x_1^3 - \zeta^2 u y_1^3 = u(x_1^3 - \zeta^2 y_1^3), \\ z &= -x_1 y_1 z_1. \end{aligned}$$

Dies wird im folgenden Lemma benutzt:

LEMMA. *Seien $x,y,z,\alpha\in\mathbf{Z}_K\setminus\{0\}$ und $m\geq 0$ mit*

$$x^3+y^3=\alpha\pi^m z^3,\quad \text{und}\quad v_\pi(x)=v_\pi(y)=v_\pi(z)=0.$$

Seien $\widetilde{x},\widetilde{y},\widetilde{z}$ definiert durch

$$\widetilde{x}=-\zeta x^3+\zeta^2y^3,\quad \widetilde{y}=x^3-\zeta^2y^3,\quad \widetilde{z}=-xyz,$$

dann gilt $\widetilde{x},\widetilde{y},\widetilde{z}\in\mathbf{Z}_K\setminus\{0\}$ und

$$\widetilde{x}^3+\widetilde{y}^3=\alpha\pi^{m+3}\widetilde{z}^3\quad \text{mit}\quad v_\pi(\widetilde{x})=v_\pi(\widetilde{y})=v_\pi(\widetilde{z})=0.$$

Beweis: Wir haben

$$\begin{aligned}
\widetilde{x} &= -\zeta x^3+\zeta^2y^3,\\
\widetilde{y} &= x^3-\zeta^2y^3,\\
\widetilde{x}+\widetilde{y} &= (1-\zeta)x^3=\pi x^3,\\
\widetilde{x}+\zeta\widetilde{y} &= -\zeta x^3+\zeta^2y^3+\zeta x^3-y^3)=-(1-\zeta^2)y^3=-(1-\zeta)(1+\zeta)y^3=\\
&= \zeta^2\pi y^3,\\
\widetilde{x}+\zeta^2\widetilde{y} &= (-\zeta x^3+\zeta^2y^3+\zeta^2x^3-\zeta y^3)=(\zeta^2-\zeta)(x^3+y^3)=-\zeta(1-\zeta)(x^3+y^3)=\\
&= -\zeta\pi(x^3+y^3)=-\zeta\pi\cdot\alpha\pi^mz^3,\\
\widetilde{x}^3+\widetilde{y}^3 &= (\widetilde{x}+\widetilde{y})(\widetilde{x}+\zeta\widetilde{y})(\widetilde{x}+\zeta^2\widetilde{y})=\pi x^3\cdot\zeta^2\pi y^3\cdot(-\zeta\pi^{m+1}\alpha z^3)=\\
&= -\alpha\pi^{m+3}x^3y^3z^3=\alpha\pi^{m+3}(-xyz)^3=\alpha\pi^{m+3}\widetilde{z}^3.
\end{aligned}$$

Wir wollen nun zeigen, dass $v_\pi(\widetilde{x})=0$ gilt. Angenommen, es würde $\pi|\widetilde{x}$ gelten. Dann folgte $0\equiv\widetilde{x}\equiv-\zeta x^3+\zeta^2y^3\equiv-x^3+y^3\equiv(y-x)^3 \bmod\pi$, also $x\equiv y \bmod\pi$. Wegen $v_\pi(x)=v_\pi(y)=0$ können wir nach eventuellem Vorzeichenwechsel $x\equiv y\equiv 1 \bmod\pi$ annehmen. Es würde folgen $x^3\equiv y^3\equiv 1 \bmod\pi^4$ und damit

$$2\equiv x^3+y^3\equiv\alpha\pi^mz^3\equiv 0 \bmod\pi,$$

ein Widerspruch. Daher muss $v_\pi(\widetilde{x})=0$ gelten. Auf die gleiche Weise folgt aus $\widetilde{y}\equiv x^3-\zeta^2y^3\equiv(x-y)^3 \bmod\pi$ dann $v_\pi(\widetilde{y})=0$. Die Aussage $v_\pi(\widetilde{z})=v_\pi(-xyz)=0$ ist klar nach Voraussetzung. Damit ist alles bewiesen. ■

FOLGERUNG. *Ist $m\equiv 1 \bmod 3$, so gibt es $x,y,z\in\mathbf{Z}_K\setminus\{0\}$ mit*

$$x^3+y^3=\zeta\pi^mz^3.$$

Beweis: Die Gleichung

$$1^3+2^3=9=\zeta\pi^4\cdot 1^3=\zeta\pi\cdot\pi^3$$

beweist die Behauptung in den Fällen $m=1$ und $m=4$. Mit dem vorangegangenen Lemma konstruiert man sich aus der Lösung für $m=4$ nacheinander Lösungen für $m=7,10,13,\ldots$, was die Behauptung beweist. ■

Wir können nun den eingangs aufgestellten Hauptsatz beweisen:

Beweis des Hauptsatzes: Wir wollen also zeigen, dass genau dann $x,y,z\in\mathbf{Z}_K\setminus\{0\}$ mit $x^3+y^3=\varepsilon\pi^mz^3$ gibt, wenn $\varepsilon=\zeta$ und $m\equiv 1 \bmod 3$ gilt.

$\Longleftarrow$ Die Existenz einer Lösung im Fall $\varepsilon=\zeta$ und $m\equiv 1 \bmod 3$ wurde eben gezeigt.

$\Longrightarrow$ Wir nehmen an, wir haben $x,y,z\in\mathbf{Z}_K\setminus\{0\}$ mit $x^3+y^3=\varepsilon\pi^mz^3$. Wir versuchen, dies auf bereits behandelte Fälle zu reduzieren.

- Nach eventueller Division von x,y,z durch $\mathrm{ggT}(x,y,z)$ können wir immer $\mathrm{ggT}(x,y,z)=1$ voraussetzen.

- Wir betrachten den Fall $\pi|x$, $\pi \nmid y$. Wir schreiben $x = \pi^k x_1$ mit $k \geq 1$, $v_\pi(x_1) = 0$ und $z = \pi^n z_1$ mit $n \geq 0$, $v_\pi(z_1) = 0$. Dann ist
$$\pi^{3k} x_1^3 + y^3 = \varepsilon \pi^{m+3n} z_1^3.$$
Wäre $m \geq 1$ oder $n \geq 1$, so würde der Widerspruch $\pi|y$ folgen. Daher ist $m = n = 0$ und
$$\pi^{3k} x_1^3 + y^3 = \varepsilon z^3 \quad \text{mit} \quad v_\pi(y) = v_\pi(z) = 0.$$
Modulo π^3 folgt $\varepsilon \equiv (\frac{y}{z})^3 \equiv \pm 1 \bmod \pi^3$. Beachtet man $\zeta \equiv 1 - \pi \bmod \pi^4$, $\zeta^2 \equiv 1 + \pi + \pi^2 + \pi^3 \bmod \pi^4$, so bleibt nur die Möglichkeit $\varepsilon = \pm 1$. Dann ist
$$y^3 + (-\varepsilon z)^3 = y^3 - \varepsilon z^3 = -\pi^{3k} x_1^3 = \pi^{3k}(-x_1)^3$$
mit
$$v_\pi(y) = v_\pi(-\varepsilon z) = v_\pi(x_1) = 0.$$
Der Exponent bei π ist $3k \equiv 0 \bmod 3$. Wir haben bereits gezeigt, dass es in diesem Fall keine Lösung gibt. Also ist der Fall $\pi|x$, $\pi \nmid y$ nicht möglich.
- Genau wie eben zeigt man, dass der Fall $\pi \nmid x$, $\pi|y$ nicht vorkommt.
- Wir betrachten den Fall $\pi|x$, $\pi|y$ und schreiben $x = \pi^k x_1$, $y = \pi^l y_1$ mit $k, l \geq 1$. Wegen $\mathrm{ggT}(x, y, z) = 1$ folgt $\pi \nmid z$. O.E. können wir $l \leq k$ voraussetzen. Aus
$$\pi^{3k} x_1^3 + \pi^{3l} y_1^3 = \varepsilon \pi^m z^3$$
folgt dann $3l \leq m$ und damit
$$(\pi^{k-l} x_1)^3 + y_1^3 = \varepsilon \pi^{m-3l} z^3.$$
Wir haben bereits gesehen, dass dann $k = l$ gelten muss. Somit gilt
$$x_1^3 + y_1^3 = \varepsilon \pi^{m-3l} z^3 \quad \text{mit} \quad v_\pi(x_1) = v_\pi(y_1) = v_\pi(z) = 0.$$
Wir haben bereits gezeigt, dass $m - 3l \equiv 0 \bmod 3$ oder $m - 3l \equiv 2 \bmod 3$ nicht möglich ist. Also bleibt nur die Möglichkeit $m \equiv 1 \bmod 3$. Durch sukzessive Anwendung des Lemmas finden wir schließlich $x_2, y_2, z_2 \in \mathbf{Z}_K \setminus \{0\}$ mit $v_\pi(x_2) = v_\pi(y_2) = v_\pi(z_2) = 0$ und
$$x_2^3 + y_2^3 = \varepsilon \pi^4 z_2^3.$$
Das Lemma liefert nun $\varepsilon = \zeta$, womit schließlich unsere Behauptung folgt. ■

ANHANG A

Maple-Funktionen

```
# az_ma
# Programme fuer Maple 6 zur Vorlesung ueber Algebraische Zahlentheorie
# im Wintersemester 2002/2003
# 13.3.2003

#########################################################################
# Rechnen im Zahlkoerper:
#   nf, pow, mulvek, rat_dar, cha_pol, Sp, N, sigma, dualbasis
# Faktorisierung von Polynomen ueber Zahlkoerpern:
#   ggT, factor_K
# Moduln in Zahlkoerpern:
#   modul2matrix, hnf_matrix, hnf_modul, modul_durchschnitt,
#   modul_quo, modul_index, disc
# Ordnungen:
#   ord_test, R_alpha, At_p, R_pmax_2, IpR, R_pmax, m2d, ord_max_2,
#   ord_max
# Ideale:
#   hnf_ideal, ideal_mult, v_p
# Gitter:
#   phi_modul, lll_modul, v_mult, v_add, v_smult, tausch, einh, lll
# Einheiten:
#   Einh_Absch, log_abb, ell_1
# Bestimmung von Klassengruppe und Einheiten:
#   MS, GRH_S, hnf_vp, rel_erzeugung, hR, restanteil, cl_einh_1,
#   cl_einh_2
# Reine kubische Zahlkoerper Q(d^(1/3)):
#   pur_cub, typ_pur_cub
#########################################################################

# Ein Zahlkoerper K wird durch ein Paar [f,a] angegeben, wobei f ein
# Polynom in a ist und im Zahlkoerper K die Beziehung f(a)=0 und K=Q(a)
# gilt.

#########################################################################
# Rechnen im Zahlkoerper ################################################
#########################################################################

# Normalform fuer Zahlkoerperelemente (21.11.2002 - 18.2.2003)
# nf(g,K) mit K=[f,a]
nf:=proc()
  local g, K, f, a, g_z, g_n, g_ni, ff;
  g:=normal(args[1]); K:=args[2]; f:=K[1]; a:=K[2];
  g_z:=numer(g); g_n:=denom(g);
```

Version vom 13.3.2003

```
  # g_n*g_ni + f*ff = 1, also g_n*g_ni = 1 (mod f) und
  # g= g_z/g_n = g_z*g_ni (mod f)
  if gcdex(g_n,f,a,'g_ni','ff')<>1 then error "gcdex<>1"; fi;
  rem(g_z*g_ni,f,a);
end;

# Potenzierung g^n fuer n aus Z im Zahlkoerper (21.11.2002)
# pow(g,n,[f,x]);
pow:=proc()
local g, n, zk, f, x, yy, nn, zz;
  g:=args[1]; n:=args[2];
  zk:=args[3]; f:=zk[1]; x:=zk[2];
  yy:=1; if n<0 then nn:=-n; zz:=nf(1/g,zk); else nn:=n; zz:=g; fi;
  while nn>0 do
    if nn mod 2=1 then yy:=rem(yy*zz,f,x); fi;
    nn:=trunc(nn/2); zz:=rem(zz*zz,f,x);
  od;
  yy;
end;

# Multiplikation g1^e1*...gr^er mod f (19.12.2002)
mulvek:=proc()
  local g, e, K, f, x, yy, i;
  g:=args[1]; e:=args[2]; K:=args[3]; f:=K[1]; x:=K[2];
  yy:=1;
  for i from 1 to nops(g) do yy:=nf(yy*pow(g[i],e[i],K),K); od;
  yy;
end:

# Rationale Darstellung von b aus K=[f,a]
# bzgl. Basis a^(n-1),...,a,1, falls rat_dar(b,K) eingegeben wird,
# bzgl. Basis R, falls rat_dar(b,R,K) eingegeben wird.
# (21.11.2002)
rat_dar:=proc()
  local b, K, f, a, n, A, i, c, j, R, M_R, A_b;
  if nargs=2 then
    b:=args[1]; K:=args[2]; f:=K[1]; a:=K[2]; n:=degree(f,a);
    b:=nf(b,K);
    A:=linalg[matrix](n,n);
    for i from 1 to n do
      c:=rem(b*a^(n-i),f,a);
      for j from 1 to n do
        A[i,j]:=coeff(c,a,n-j);
      od;
    od;
    return evalm(A);
  fi;
  if nargs=3 then
    b:=args[1]; R:=args[2]; K:=args[3];
    M_R:=modul2matrix(R,K);
    A_b:=rat_dar(b,K);
    return evalm(M_R&*A_b&*M_R^(-1));
  fi;
end;
```

```
# Charakteristisches Polynom (in t) von b aus K=[f,a] (21.11.2002)
# cha_pol(b,K,t)
cha_pol:=proc()
  local b, K, t;
  b:=args[1]; K:=args[2]; t:=args[3];
  linalg[charpoly](rat_dar(b,K),t);
end;

# Spur von b in K (21.11.2002)
# Sp(b,K)
Sp:=proc()
  local b, K, f, a, n, s, i;
  b:=args[1]; K:=args[2]; f:=K[1]; a:=K[2]; n:=degree(f,a);
  s:=0;
  for i from 0 to n-1 do
    s:=s+coeff(rem(b*a^i,f,a),a,i);
  od;
  s;
end;

# Norm von b in K (21.11.2002)
# N(b,[f,a])
N:=proc()
  linalg[det](rat_dar(args[1],args[2]));
end;

# Komplexe Einbettungen (9.1.2003)
sigma:=proc()
  local K, f, a, n, a_i, a_i_reell, a_i_komplex, i;
  Digits:=100;
  K:=args[1]; f:=K[1]; a:=K[2]; n:=degree(f,a);
  a_i:=[fsolve(f,a,complex,fulldigits)];
  a_i_reell:=[]; a_i_komplex:=[];
  for i from 1 to n do
    if Im(a_i[i])=0 then
      a_i_reell:=[op(a_i_reell),a_i[i]];
    elif Im(a_i[i])>0 then
      a_i_komplex:=[op(a_i_komplex),a_i[i]];
    fi;
  od;
  [a_i_reell,a_i_komplex];
end;

# Dualbasis (20.12.2002)
# dualbasis(alpha,K)
dualbasis:=proc()
  local alpha, K, f, a, n, S, i, j;
  alpha:=args[1]; K:=args[2]; f:=K[1]; a:=K[2]; n:=degree(f,a);
  S:=array(1..n,1..n);
  for i from 1 to n do
    for j from 1 to n do
      S[i,j]:=Sp(alpha[i]*alpha[j],K);
    od;
```

```
  od;
  convert(evalm(S^(-1)&*alpha),list);
end;

#########################################################################
# Faktorisierung von Polynomen ueber Zahlkoerpern #######################
#########################################################################

# ggT von Polynomen ueber Zahlkoerpern: ggT(f1,f2,K)
# Die verwendete Variable wird bestimmt. Der ggT wird normiert.
# 22.12.2002
ggT:=proc()
  local f1, f2, K, a, x, f3, m;
  f1:=args[1]; f2:=args[2]; K:=args[3]; a:=K[2];
  x:=op((indets(f1) union indets(f2)) minus {a});
  while f2<>0 do
    f3:=nf(rem(f1,f2,x),K);
    f1:=f2; f2:=f3;
  od;
  m:=degree(f1,x);
  f1:=nf(f1/coeff(f1,x,m),K);
end;

factor_K:=proc()
  local F, K, a, x, d, c, G, k, Ffactors, g_k, pp, i, p_i, P_i, e_i;
  F:=args[1]; K:=args[2]; a:=K[2];
  x:=op(indets(F) minus {a});
  d:=degree(F,x); c:=coeff(F,x,d);
  G:=F/c/ggT(F,diff(F,x),K); #printf("G=%a\n",G);
  k:=0; Ffactors:=[];
  do
    g_k:=N(subs(x=x-k*a,G),K); #printf("k=%d g_k=%a\n",k,g_k);
    #printf("ggT(g_k,g_k')=%a\n",gcd(g_k,diff(g_k,x)));
    if gcd(g_k,diff(g_k,x))=1 then
      pp:=factors(g_k)[2];
      #printf("pp=%a\n",pp);
      for i from 1 to nops(pp) do
        p_i:=pp[i][1]; #printf("i=%d p_i=%a\n",i,p_i);
        P_i:=ggT(G,subs(x=x+k*a,p_i),K);e_i:=0; #printf("P_i=%a\n",P_i);
        while nf(rem(F,P_i,x),K)=0 do
          F:=nf(quo(F,P_i,x),K); e_i:=e_i+1;
        od;
        Ffactors:=[op(Ffactors),[P_i,e_i]];
      od;
      return [c,Ffactors];
    fi;
    k:=k+1;
  od;
end;

#########################################################################
# Moduln in Zahlkoerpern ################################################
#########################################################################
```

```
# modul2matrix(U,K) oder modul2matrix(U,V,K) - Uebergangsmatrizen
# 18.12.2002 - 19.12.2002
modul2matrix:=proc()
  local U, V, K, f, a, n, M, i, M_i, j, matU, matV;
  if nargs=2 then
    U:=args[1]; K:=args[2]; f:=K[1]; a:=K[2]; n:=degree(f,a);
      M:=[];
      for i from 1 to nops(U) do
      M_i:=[];
      for j from n-1 to 0 by -1 do
        M_i:=[op(M_i),coeff(nf(U[i],K),a,j)];
      od;
      M:=[op(M),M_i];
    od;
    return M;
  fi;
  U:=args[1]; V:=args[2]; K:=args[3]; f:=K[1]; a:=K[2]; n:=degree(f,a);
  matU:=modul2matrix(U,K);
  matV:=modul2matrix(V,K);
  convert(evalm(matU&*matV^(-1)),listlist);
end;

# Hermitesche Normalform einer Matrix mit rationalen Zahlen
# (18.12.2002)
hnf_matrix:=proc()
  local M, n, M_nenner, d, dM, dMh, nz;
  M:=args[1]; n:=nops(M[1]);
  M_nenner:=denom(M); # Matrix mit Nennern
  d:=ilcm(op(map(x->ilcm(op(x)),M_nenner)));
  dM:=map(x->d*x,M);
  dMh:=convert(linalg[ihermite](dM),listlist);
  nz:=[seq(0,i=1..n)];
  while dMh[nops(dMh)]=nz do dMh:=subsop(nops(dMh)=NULL,dMh); od;
  [d,dMh];
end;

# Hermitesche Normalform bzgl. einer Basis: hnf_modul(U,basis,K)
# oder bzgl. der # Standardbasis a^(n-1),...,a,1: hnf_modul(U,K)
# (18.12.2002)
hnf_modul:=proc()
  local erzeuger, K, f, a, n, M, ddMh, d, dMh, basis;
  erzeuger:=args[1]; K:=args[nargs]; f:=K[1]; a:=K[2]; n:=degree(f,a);
  if nargs=2 then basis:=[seq(a^(n-i),i=1..n)]; fi;
  if nargs=3 then basis:=args[2]; fi;
  M:=modul2matrix(erzeuger,basis,K);
  ddMh:=hnf_matrix(M); d:=ddMh[1]; dMh:=ddMh[2];
  basis:=convert(evalm(dMh&*basis/d),list);
end;

# modul_durchschnitt(aa,bb,K) - Durchschnitt von Moduln
modul_durchschnitt:=proc()
 local aa, bb, K, f, a, n, A, B, AB, d, dAB, U21;
 aa:=args[1]; bb:=args[2]; K:=args[3];
 f:=K[1]; a:=K[2]; n:=degree(f,a);
```

```
 A:=modul2matrix(aa,K); B:=modul2matrix(bb,K);
 AB:=[op(A),op(B)];
 d:=ilcm(op(map(x->ilcm(op(x)),denom(AB))));
 dAB:=map(x->d*x,AB);
 linalg[ihermite](dAB,U); U21:=linalg[submatrix](U,n+1..2*n,1..n);
 hnf_modul(convert(evalm(U21&*aa),list),K);
end;

# modul_quo(aa,bb,K) - (aa:bb) Quotient von Moduln
modul_quo:=proc()
 local aa, bb, cc, K, f, a, n, i, aa_b_i;
 aa:=args[1]; bb:=args[2]; K:=args[3];
 f:=K[1]; a:=K[2]; n:=degree(f,a);
 cc:=map(x->nf(x/bb[1],K),aa);
 for i from 2 to n do
   aa_b_i:=map(x->nf(x/bb[i],K),aa);
   cc:=modul_durchschnitt(cc,aa_b_i,K);
 od;
 cc;
end;

# modul_index(U,V,K) - Indexberechnung [U:V] im Zahlkoerper K
modul_index:=proc()
  local U, V, K;
  U:=args[1]; V:=args[2]; K:=args[3];
  abs(linalg[det](modul2matrix(V,U,K)));
end;

# Diskriminante eines Moduls U wird hier berechnet mit
# der Formel disc(U)=[Z[a]:U]^2*disc(f), wobei U durch eine Z-Basis
# gegeben sein muss.
# disc(U,K)
# 20.12.2002
disc:=proc()
  local U, K, f, a;
  U:=args[1]; K:=args[2]; f:=K[1]; a:=K[2];
  linalg[det](modul2matrix(U,K))^2*discrim(f,a);
end;

#########################################################################
# Ordnungen #############################################################
#########################################################################

# ord_test(R,K) - Ist R eine Ordnung?
ord_test:=proc()
  local R, K, f, a, n, S, v, i, j, beta;
  R:=args[1]; K:=args[2]; f:=K[1]; a:=K[2]; n:=degree(f,a);
  S:={};
  v:=modul2matrix([1],R,K)[1];
  if max(op(denom(v)))>1 then S:=S union {[1,v]}; fi;
  for i from 1 to n do
    for j from i to n do
      beta:=nf(R[i]*R[j],K);
      v:=modul2matrix([beta],R,K)[1];
```

```
      if max(op(denom(v)))>1 then S:=S union {[[i,j],v]}; fi;
    od;
  od;
  S;
end;

# Konstruktion der Ordnung R[alpha]
R_alpha:=proc()
  local R, alpha, K, f, a, n, Ra, i, j;
  R:=args[1]; alpha:=args[2]; K:=args[3];
  f:=K[1]; a:=K[2]; n:=degree(f,a);
  Ra:=R;
  for i from 1 to n-1 do
    for j from 1 to n do
      Ra:=[op(Ra),nf(alpha^i*R[j],K)];
    od;
  od;
  Ra:=hnf_modul(Ra,K);
end;

# At_p(R,p,K) - es werden (p^n-1)/(p-1) normierte Elemente von
# (1/p*R)/R nach ganzen Elementen durchsucht und eventuell das zuerst
# gefundene ausgegeben. Wurde nichts gefunden, wird 0 zurueckgegeben.
At_p:=proc()
  local R, p, K, f, a, n, i, b1, b, beta, j, g, x, Nenner;
  R:=args[1]; p:=args[2]; K:=args[3];
  f:=K[1]; a:=K[2]; n:=degree(f,a);
  for i from 1 to n do
    for b1 from 0 to p^(n-i)-1 do
      b:=b1;
      beta:=R[i];
      for j from i+1 to n do
        beta:=beta+(b mod p)*R[j];
        b:=iquo(b,p);
      od;
      beta:=beta/p;
      g:=cha_pol(beta,K,x);
      Nenner:=denom(g);
      if Nenner=1 then return beta; fi;
    od;
  od;
  0;
end;

# zum 2. Verfahren im Kapitel ueber Ordnungen
R_pmax_2:=proc()
  local R, p, K, alpha, R1;
  R:=args[1]; p:=args[2]; K:=args[3];
  do
    alpha:=At_p(R,p,K);
    if alpha=0 then return R; fi;
    R1:=R_alpha(R,alpha,K);
    printf("Index=%d\n",modul_index(R1,R,K));
    R:=R1;
```

```
  od;
end;

# IpR(R,p,K)
IpR:=proc()
  local S, T, R, p, K, f, a, n, pp, nz, Fp, Ip, i;
  R:=args[1]; p:=args[2]; K:=args[3]; f:=K[1]; a:=K[2]; n:=degree(f,a);
  pp:=p; while pp<n do pp:=pp*p; od; # pp=p^k mit p^(k-1)<n<=p^k
  nz:=[seq(0,i=1..n)];
  Fp:=modul2matrix(map(x->pow(x,pp,K),R),R,K) mod p;
  linalg[ismith](Fp,S,T);
  S:=convert(S,listlist);
  Ip:=map(x->x*p,R);
  for i from 1 to n do
    if convert(evalm(S[i]&*Fp),list) mod p=nz then
      Ip:=[op(Ip),evalm(S[i]&*R)];
    fi;
  od;
  hnf_modul(Ip,K);
end;

R_pmax:=proc()
  local R, p, K, Ip, R1;
  R:=args[1]; p:=args[2]; K:=args[3];
  R:=hnf_modul(R,K);
  do
    Ip:=IpR(R,p,K);
    R1:=modul_quo(Ip,Ip,K);
    if R1=R then return R; fi;
    printf("Index=%d\n",modul_index(R1,R,K));
    R:=R1;
  od;
end;

# Zerlegung einer ganzen Zahl in die Gestalt m^2*d mit d quadratfrei
# P_m enthaelt die Primteiler von m
m2d:=proc()
  local n, nn, m, d, i, p, e, P_m;
  n:=args[1];
  nn:=ifactors(n);
  m:=1; d:=nn[1]; nn:=nn[2]; P_m:=[];
  for i from 1 to nops(nn) do
    p:=nn[i][1]; e:=nn[i][2];
    if e mod 2=1 then d:=d*p; e:=e-1; fi;
    if e>0 then m:=m*p^(e/2); P_m:=[op(P_m),p]; fi;
  od;
  if m^2*d<>n then error "Fehler!"; fi;
  [m,d,P_m];
end;

# Bestimmung der Maximalordnung zum 2. Verfahren im Kapitel ueber
# Ordnungen
ord_max_2:=proc()
  local R, K, d_R, d_R1, m, d, P, i;
```

```
  R:=args[1]; K:=args[2];
  d_R:=disc(R,K); d_R1:=m2d(d_R); m:=d_R1[1]; d:=d_R1[2]; P:=d_R1[3];
  printf("disc(R)=%d*%d^2 P=%a\n",d,m,P);
  for i from 1 to nops(P) do
    R:=R_pmax_2(R,P[i],K);
  od;
  printf("disc(R)=%d\n",disc(R,K));
  R;
end;

# Bestimmung der Maximalordnung
ord_max:=proc()
  local R, K, d_R, d_R1, m, d, P, i;
  R:=args[1]; K:=args[2];
  d_R:=disc(R,K); d_R1:=m2d(d_R); m:=d_R1[1]; d:=d_R1[2]; P:=d_R1[3];
  printf("disc(R)=%d*%d^2 P=%a\n",d,m,P);
  for i from 1 to nops(P) do
    printf("p=%d\n",P[i]);
    R:=R_pmax(R,P[i],K);
    printf("R=%a\n",R);
  od;
  printf("disc(R)=%d\n",disc(R,K));
  R;
end;

#############################################################################
# Ideale ####################################################################
#############################################################################

# Hermitesche Normalform eines Ideals
hnf_ideal:=proc()
  local aa, R, K, Raa, i, j;
  aa:=args[1]; R:=args[2]; K:=args[3];
  Raa:=[];
  for i from 1 to nops(aa) do
    for j from 1 to nops(R) do
      Raa:=[op(Raa),nf(aa[i]*R[j],K)];
    od;
  od;
  hnf_modul(Raa,K);
end;

# Multiplikation von Idealen (22.11.2002)
# ideal_mult(aa,bb,zk)
ideal_mult:=proc()
  local aa, bb, K, cc, i, j;
  aa:=args[1]; bb:=args[2]; K:=args[3];
  cc:=[];
  for i from 1 to nops(aa) do
    for j from 1 to nops(bb) do
      cc:=[op(cc),nf(aa[i]*bb[j],K)];
    od;
  od;
  cc;
```

```
end;

# Bewertung v_p(a,lambda_p,oo,zk)
# 19.12.2002
v_p:=proc()
  local v, a, lambda_p, oo, zk, nenner, aa;
  v:=0; a:=args[1]; lambda_p:=args[2]; oo:=args[3]; zk:=args[4];
  nenner:={1};
  while nenner={1} do
    a:=nf(lambda_p*a,zk);
    aa:=op(modul2matrix([a],oo,zk)); # Koeffizienten von a bzgl. oo
    nenner:=convert(denom(aa),set);
    if nenner={1} then v:=v+1; fi;
  od;
  v;
end;

#########################################################################
# Gitter ################################################################
#########################################################################

# 9.1.2003
# phi(aa) eines Moduls aa von K
phi_modul:=proc()
  local aa, K, a, sigma_a, phi_aa, i, phi_aa_i, j, b;
  Digits:=1000;
  aa:=args[1]; K:=args[2]; a:=K[2];
  sigma_a:=sigma(K);
  phi_aa:=[];
  for i from 1 to nops(aa) do
    phi_aa_i:=[];
    for j from 1 to nops(sigma_a[1]) do
      b:=subs(a=sigma_a[1][j],aa[i]);
      phi_aa_i:=[op(phi_aa_i),b];
    od;
    for j from 1 to nops(sigma_a[2]) do
      b:=subs(a=sigma_a[2][j],aa[i]);
      phi_aa_i:=[op(phi_aa_i),Re(b),Im(b)];
    od;
    phi_aa:=[op(phi_aa),phi_aa_i];
  od;
  phi_aa;
end;

lll_modul:=proc()
  local aa, K, b, T, aa_neu;
  Digits:=1000;
  aa:=args[1]; K:=args[2];
  b:=phi_modul(aa,K);
  T:=lll(b);
  #printf("T=%a\n",convert(T,listlist));
  aa_neu:=convert(evalm(T&*aa),list);
end;
```

```
# Skalarprodukt zweier Vektoren
v_mult:=proc()
  local a, b, s, i;
  a:=args[1]; b:=args[2];
  s:=0;
  for i from 1 to nops(a) do
    s:=s+a[i]*b[i];
  od;
  s;
end;

# Addition zweier Vektoren
v_add:=proc()
  local a, b, c, i;
  a:=args[1]; b:=args[2]; c:=[];
  for i from 1 to nops(a) do
    c:=[op(c),a[i]+b[i]];
  od;
  c;
end;

# Multiplikation eines Skalars mit einem Vektor
v_smult:=proc()
  local k, a, b, i;
  k:=args[1]; a:=args[2];
  b:=[];
  for i from 1 to nops(a) do
    b:=[op(b),k*a[i]];
  od;
  b;
end;

# Vertauschen von Basisvektoren
tausch:=proc()
  local i1, i2, b, bi1, bi2;
  i1:=args[1]; i2:=args[2]; b:=args[3];
  bi1:=b[i1]; bi2:=b[i2];
  subsop(i1=bi2,i2=bi1,b);
end;

# n x n - Einheitsmatrix
einh:=proc()
  local n, b0, b, i;
  n:=args[1];
  b0:=[seq(0,i=1..n)]; b:=[];
  for i from 1 to n do
    b:=[op(b),subsop(i=1,b0)];
  od;
  b;
end;

# LLL-Reduktion bei gegebener Gitterbasis
lll:=proc()
  local b_anfang, T, T_i, az, b_ende,
```

```
      b, m, n, i, j, b_stern, b_stern_i, c, b_i, mu_ij, k,
      mu_ii1, c_ii1, az_tausch;
Digits:=1000;
b:=args[1]; # b=[b_1,...,b_m]
b_anfang:=b;
#printf("Anfang: b=%a\n",b);
#detb:=linalg[det](b);
#printf("detb=%f\n",detb);
if nargs<2 then c:=3/4; else c:=args[2]; fi;
m:=nops(b); n:=nops(b[1]);
T:=einh(m); # Transformationsmatrix
az_tausch:=0;
i:=1;
while i<=m do
  if i=1 then
    b_stern:=[b[1]];
    i:=2;
    #printf("i=1\ni=2\n");
  fi;
  b_i:=b[i]; T_i:=T[i];
  b_stern_i:=[seq(0,i=1..n)];
  for j from i-1 to 1 by -1 do
    mu_ij:=v_mult(b_i,b_stern[j])/v_mult(b_stern[j],b_stern[j]);
    #printf("  mu_%d%d=%f\n",i,j,mu_ij);
    k:=floor(mu_ij+1/2);
    if type(k,integer)=false then
      printf("**************************************************\n");
      printf("mu_ij=%a\n",mu_ij);
      printf("k=%a\n",k);
      printf("**************************************************\n");
    fi;
    if k<>0 then
      b_i:=v_add(b_i,v_smult(-k,b[j]));
      T_i:=v_add(T_i,v_smult(-k,T[j]));
      mu_ij:=mu_ij-k;
      #printf("  Ersetze b_%d durch b_%d-(%d)b_%d ",i,i,k,j);
      #printf("(neues mu_%d%d=%f)\n",i,j,mu_ij);
    fi;
    b_stern_i:=v_add(b_stern_i,v_smult(-mu_ij,b_stern[j]));
    if j=i-1 then mu_ii1:=mu_ij; fi;
  od;
  b:=subsop(i=b_i,b); T:=subsop(i=T_i,T);
  b_stern_i:=v_add(b_i,b_stern_i);
  b_stern:=[op(b_stern),b_stern_i];
  c_ii1:=v_mult(b_stern[i],b_stern[i])/v_mult(b_stern[i-1],b_stern[i-1])
      +mu_ii1^2;
  #printf("c_%d%d=%f\n",i,i-1,c_ii1);
  if c_ii1<c then
    #printf("Vertausche b_%d und b_%d\n",i,i-1);
    az[i-1]:=az[i-1]+1;
    b:=tausch(i,i-1,b);
    T:=tausch(i,i-1,T);
    az_tausch:=az_tausch+1;
    b_stern:=subsop(i=NULL,b_stern); b_stern:=subsop(i-1=NULL,b_stern);
```

```
      #printf("Ersetze i=%d durch i=%d\n",i,i-1);
      i:=i-1;
    else
      #printf("Ersetze i=%d durch i=%d\n",i,i+1);
      i:=i+1;
    fi;
  od;
  b;
  b_ende:=b;
  #printf("b_ende=%a\n",b);
  #printf("az_tausch=%d\n",az_tausch);
  #printf("%a\n",convert(evalm(b_ende-T&*b_anfang),listlist));
  T;
end;

#############################################################################
# Einheiten #################################################################
#############################################################################

# Einh_Absch - Abschaetzung fuer zusaetzliche Einheiten (8.1.2003)
# Einh_Absch(epsilon,R,K)
Einh_Absch:=proc()
  local epsilon, R, K, f, a, n, R_dual, r, a_i, c, j, k, sj_ek, x_i, i;
  epsilon:=args[1]; R:=args[2]; K:=args[3];
  f:=K[1]; a:=K[2]; n:=degree(f,a);
  R_dual:=dualbasis(R,K);
  r:=nops(epsilon);
  Digits:=50;
  a_i:=fsolve(f,a,complex,fulldigits);
  c:=array(1..n);
  for j from 1 to n do
    c[j]:=1;
    for k from 1 to r do
      sj_ek:=sqrt(abs(subs(a=a_i[j],epsilon[k])));
      c[j]:=c[j]*max(sj_ek,1/sj_ek);
    od;
  od;
  x_i:=array(1..n);
  for i from 1 to n do
    x_i[i]:=0;
    for j from 1 to n do
      x_i[i]:=x_i[i]+abs(subs(a=a_i[j],R_dual[i]))*c[j];
    od;
  od;
  convert(x_i,list);
end;

# Logarithmische Abbildung (8.1.2003)
# log_abb(aa,K)
log_abb:=proc()
  local aa, K, f, x, xxx, xx, u, i, log_aa, log_aa_i, j;
  aa:=args[1]; K:=args[2]; f:=K[1]; x:=K[2];
  Digits:=50;
  xxx:=[fsolve(f,x,complex)];
```

```
  xx:=[]; u:=[];
  for i from 1 to nops(xxx) do
    if Im(xxx[i])=0 then xx:=[op(xx),xxx[i]]; u:=[op(u),1];
    elif Im(xxx[i])>0 then xx:=[op(xx),xxx[i]]; u:=[op(u),2];
    fi;
  od;
  log_aa:=[];
  for i from 1 to nops(aa) do
    log_aa_i:=[];
    for j from 1 to nops(xx) do
      log_aa_i:=[op(log_aa_i),u[j]*ln(abs(subs(x=xx[j],aa[i])))];
    od;
    log_aa:=[op(log_aa),log_aa_i];
  od;
  log_aa;
end;

ell_1:=proc()
  local epsilon, K, f, a, a_i_alle, a_i, v_i, i, ell;
  epsilon:=args[1]; K:=args[2]; f:=K[1]; a:=K[2];
  Digits:=100;
  a_i_alle:=[fsolve(f,a,complex,fulldigits)];
  a_i:=[]; v_i:=[];
  # zuerst kommen die reellen Stellen
  for i from 1 to nops(a_i_alle) do
    if Im(a_i_alle[i])=0 then
      a_i:=[op(a_i),a_i_alle[i]]; v_i:=[op(v_i),1];
    fi;
  od;
  # dann die komplexen Stellen
  for i from 1 to nops(a_i_alle) do
    if Im(a_i_alle[i])>0 then
      a_i:=[op(a_i),a_i_alle[i]]; v_i:=[op(v_i),2];
    fi;
  od;
  a_i:=subsop(nops(a_i)=NULL,a_i); v_i:=subsop(nops(v_i)=NULL,v_i);
  ell:=[];
  for i from 1 to nops(a_i) do
    ell:=[op(ell),v_i[i]*ln(abs(subs(a=a_i[i],epsilon)))];
  end;
  ell;
end;

#########################################################################
# Bestimmung von Klassengruppe und Einheiten ############################
#########################################################################

# Minkowski-Schranke
# MS(R,K)
# 20.12.2002
MS:=proc()
  local R, K, f, x, n, disc_R, r1, r2;
  R:=args[1]; K:=args[2]; f:=K[1]; x:=K[2]; n:=degree(f,x);
  disc_R:=disc(R,K);
```

```
  r1:=nops([fsolve(f,x)]);
  r2:=(n-r1)/2;
  printf("r1=%d r2=%d\n",r1,r2);
  evalf((4/Pi)^r2*n!/n^n*sqrt(abs(disc_R)));
end;

# GRH-Schranke 12*ln^2|D|
GRH_S:=proc()
  local Z_K, K;
  Z_K:=args[1]; K:=args[2];
  evalf(12*ln(abs(disc(Z_K,K)))^2);
end;

# Normalisierung der Relationenmatrix mit den v_p's
# hnf_vp(A_neu,VP,A,Einh,lambda_p,Z_K,K)
hnf_vp:=proc()
  local A_neu, VP, A, Einh, lambda_p, Z_K, K, i, a, v_pa, j, T, TA,
        nzeile, VPh;
  A_neu:=args[1]; VP:=args[2]; A:=args[3]; Einh:=args[4];
  lambda_p:=args[5]; Z_K:=args[6]; K:=args[7];
  # Aufnahme neuer Relationen in die Matrix (VP,A)
  for i from 1 to nops(A_neu) do
    a:=A_neu[i];
    v_pa:=[];
    for j from 1 to nops(lambda_p) do
      v_pa:=[op(v_pa),v_p(a,lambda_p[j][2],Z_K,K)];
    od;
    VP:=[op(VP),v_pa]; A:=[op(A),a];
  od;
  printf("VP=%a\nA=%a\n",VP,A);
  # Normalisierung
  VPh:=linalg[ihermite](VP,'T');
  VP:=convert(VPh,listlist); T:=convert(T,listlist);
  TA:=[];
  for j from 1 to nops(A) do
    TA:=[op(TA),mulvek(A,T[j],K)];
  od;
  A:=TA;
  nzeile:=[seq(0,j=1..nops(VP[1]))];
  # Entfernung der letzten Zeilen
  while VP[nops(VP)]=nzeile do
    Einh:=[op(Einh),A[nops(VP)]];
    A:=subsop(nops(VP)=NULL,A);
    VP:=subsop(nops(VP)=NULL,VP);
  od;
  [VP,A,Einh];
end;

# Erzeugung von Relationen
# rel_erzeugung(az,h,Hp,Z_K,K)
rel_erzeugung:=proc()
  local az, h, Hp, Z_K, K, f, x, n, zz, pp, p, A, za, i, a, Na;
  az:=args[1]; h:=args[2]; Hp:=args[3]; Z_K:=args[4]; K:=args[5];
  f:=K[1]; x:=K[2]; n:=degree(f,x);
```

```
  zz:=rand(-h..h);
  pp:=1; p:=2;
  while p<=Hp do
    pp:=pp*p;
    p:=nextprime(p);
  od;
  printf("pp=%d\n",pp);
  A:=[];
  while az>0 do
    za:=[];
    for i from 1 to n do
      za:=[op(za),zz()];
    od;
    if igcd(op(za))=1 then
      a:=evalm(za&*Z_K);
      Na:=abs(N(a,K));
      while igcd(Na,pp)>1 do
        Na:=Na/igcd(Na,pp);
      od;
      if Na=1 and a<>1 and a<>-1 then
        A:=[op(A),a];
        az:=az-1;
      fi;
    fi;
  od;
  A;
end;

# 13.1.2003
# hR approximativ - bisher nur ein Fall behandelt.
# Nur R=Z[a] wird behandelt, ausserdem sollte nur 1 und -1
# Einheitswurzeln in R sein. Ist a_K der Ausgabewert, so gilt
# 2^(-1/2)<hR/a_K<2^(1/2) (unter der Annahme von GRH).
hR:=proc()
  local R, K, f, x, n, w, r1, r2, p_max, hR, p, i, a_p, F, j;
  R:=args[1]; K:=args[2]; f:=K[1]; x:=K[2]; n:=degree(f,x);
  if disc(R,K)<>discrim(f,x) then
    error "Der Fall R<>Z[a] wird nicht behandelt!";
  fi;
  w:=2;
  r1:=nops([fsolve(f,x)]); r2:=(n-r1)/2;
  p_max:=floor(12*ln(abs(discrim(f,x)))^2);
  printf("p_max=%d\n",p_max);
  hR:=w*sqrt(abs(discrim(f,x)))/2^r1/(2*Pi)^r2;
  p:=2; i:=1;
  while p<=p_max do
    a_p:=1-1/p:
    F:=(Factors(f) mod p)[2]:
    for j from 1 to nops(F) do
      a_p:=a_p/(1-1/p^degree(F[j][1],x)):
    od:
    hR:=hR*a_p:
    if i mod 100=0 then
      printf("$p\\le %d$ & %f \\\\ \\hline\n",p,evalf(hR)):
```

```
    fi:
    p:=nextprime(p); i:=i+1;
  od;
  evalf(hR);
end;

restanteil:=proc()
  local x, M;
  x:=abs(args[1]); M:=args[2];
  while igcd(x,M)>1 do x:=x/igcd(x,M); od;
  x;
end;

# Einhabe: K=[f(a),a], wobei Z_K=Z[a] gelten muss.
# Zurueckgegeben wird [hh_K,E], wobei h_K ein Teiler von hh_K ist und
# E aus nichttrivialen Einheiten besteht.
# (Bis zur Minkowski-Schranke werden alle Primideale betrachtet.)
cl_einh_1:=proc()
  local K, f, a, n, R, MS_RK, p_liste, p, prod_p_liste, streichen, F,
        i, grad_pp, pp, pp_ell, pp_lll, v, p_i, pp_i, la_i, la, j,
        p_i_set, prod_p_i, S, x, V, A, E, beta, v_beta, Vh, T, TA,
        nzeile, E1, e, hh_K;
  K:=args[1];
  f:=K[1]; a:=K[2]; n:=degree(f,a);
  R:=[seq(a^(n-i),i=1..n)];
  MS_RK:=MS(R,K); # Minkowski-Schranke
  printf("Minkowski-Schranke=%f\n",MS_RK);
  p_liste:=[]; prod_p_liste:=1;
  p:=2;
  while p<=MS_RK do
    if Irreduc(f) mod p=false then
      p_liste:=[op(p_liste),p];
      prod_p_liste:=prod_p_liste*p;
    fi;
    p:=nextprime(p);
  od;

  streichen:=1;
  while streichen=1 and nops(p_liste)>0 do
    p:=p_liste[nops(p_liste)];
    prod_p_liste:=prod_p_liste/p;
    F:=(Factors(f) mod p)[2];
    for i from 1 to nops(F) do
      grad_pp:=degree(F[i][1],a);
      pp:=hnf_ideal([p,F[i][1]],R,K);
      pp_lll:=lll_modul(pp,K);
      v:=map(x->restanteil(N(x,K)/p^grad_pp,prod_p_liste),pp_lll);
      streichen:=max(streichen,min(op(v)));
    od:
    if streichen=1 then p_liste:=subsop(nops(p_liste)=NULL,p_liste); fi;
  od;

  if p_liste=[] then printf("Klassenzahl 1\n"); return [[],[],[]]; fi;
```

```
p_i:=[]; pp_i:=[]; la_i:=[];
while nops(p_liste)>0 do
  p:=p_liste[nops(p_liste)];
  F:=(Factors(f) mod p)[2];
  for i from 1 to nops(F) do
    pp:=hnf_ideal([p,F[i][1]],R,K);
    pp:=lll_modul(pp,K);
    la:=1/p;
    for j from 1 to nops(F) do
      if j<>i then
        la:=expand(la*F[j][1]^F[j][2]);
      else
        la:=expand(la*F[j][1]^(F[j][2]-1));
      fi;
    od;
    p_i:=[op(p_i),p];
    pp_i:=[op(pp_i),pp];
    la_i:=[op(la_i),la];
  od;
  p_liste:=subsop(nops(p_liste)=NULL,p_liste);
od;

p_i_set:=convert(convert(p_i,set),list);
prod_p_i:=1;
for i from 1 to nops(p_i_set) do
  prod_p_i:=prod_p_i*p_i_set[i];
od;

S:=p_i_set;
for i from 1 to nops(pp_i) do
  pp:=pp_i[i];
  for j from 1 to nops(pp) do
    x:=pp[j];
    if igcd(op(op(modul2matrix([x],R,K))))=1 and
       restanteil(N(x,K),prod_p_i)=1 then
      S:=[op(S),x];
    fi;
  od;
od;

V:=[]; A:=[]; E:=[];
for i from 1 to nops(S) do
  beta:=S[i];
  v_beta:=map(x->v_p(beta,x,R,K),la_i);
  V:=[op(V),v_beta]; A:=[op(A),beta];
od;

Vh:=linalg[ihermite](V,'T'):
V:=convert(Vh,listlist): T:=convert(T,listlist):
TA:=[]:
for j from 1 to nops(A) do
 TA:=[op(TA),mulvek(A,T[j],K)]:
od:
A:=TA:
```

```
  nzeile:=[seq(0,j=1..nops(V[1]))]:
  while V[nops(V)]=nzeile do
    E:=[op(E),A[nops(V)]]:
    A:=subsop(nops(V)=NULL,A):
    V:=subsop(nops(V)=NULL,V):
  od:

  E1:=[];
  for i from 1 to nops(E) do
    e:=E[i];
    if abs(N(e,K))<>1 then printf("Fehler!\n"); fi;
    if e<>1 and e<>-1 then
      if coeff(e,a,degree(e,a))<0 then e:=-e; fi;
      E1:=[op(E1),e];
    fi;
  od;
  E1:=convert(E1,set); E:=convert(E1,list);

  hh_K:=0;
  if nops(V)=nops(V[1]) then hh_K:=linalg[det](V); fi;
  [hh_K,E];
end;

# Einhabe: K=[f(a),a], wobei Z_K=Z[a] gelten muss.
# Zurueckgegeben wird [hh_K,E], wobei h_K (sehr wahrscheinlich) ein
# Teiler von hh_K ist und E aus nichttrivialen Einheiten besteht.
# (Es wird nach Relationen zwischen den 20 ersten nichttraegen
# Primidealen gesucht, wobei sich die Relationen sich aus
# LLL-reduzierten Basiselementen der Primideale ergeben.)
cl_einh_2:=proc()
  local K, f, a, n, R, p_i, pp_i, la_i, p, F, i, pp, la, j, prod_p_i,
        A, beta, V, E, v_beta, Vh, T, TA, nzeile, E1, e, hh_K;
  K:=args[1];
  f:=K[1]; a:=K[2]; n:=degree(f,a);
  R:=[seq(a^(n-i),i=1..n)];

  p_i:=[]; pp_i:=[]; la_i:=[];

  p:=1;
  while nops(pp_i)<20 do
    printf("nops(pp_i)=%a\n",nops(pp_i));
    p:=nextprime(p);
    if Irreduc(f) mod p=false then
      F:=(Factors(f) mod p)[2];
      for i from 1 to nops(F) do
        pp:=hnf_ideal([p,F[i][1]],R,K);
        pp:=lll_modul(pp,K);
        la:=1/p;
        for j from 1 to nops(F) do
          if j<>i then
            la:=expand(la*F[j][1]^F[j][2]);
          else
            la:=expand(la*F[j][1]^(F[j][2]-1));
          fi;
```

```
      od;
      p_i:=[op(p_i),p];
      pp_i:=[op(pp_i),pp];
      la_i:=[op(la_i),la];
    od;
  fi;
od;

prod_p_i:=1;
for i from 1 to nops(p_i) do
  prod_p_i:=ilcm(prod_p_i,p_i[i]);
od;

A:=convert(convert(p_i,set),list);
printf("A=%a\n",A);
for i from 1 to nops(pp_i) do
  pp:=pp_i[i];
  for j from 1 to nops(pp) do
    beta:=pp[j];
    if restanteil(N(beta,K),prod_p_i)=1 then
      A:=[op(A),beta];
    fi;
    printf("A=%a\n",A);
  od;
od;

V:=[]; E:=[];

for i from 1 to nops(A) do
  beta:=A[i];
  v_beta:=map(x->v_p(beta,x,R,K),la_i);
  V:=[op(V),v_beta];
od;

Vh:=linalg[ihermite](V,'T'):
V:=convert(Vh,listlist): T:=convert(T,listlist):
TA:=[]:
for j from 1 to nops(A) do
 TA:=[op(TA),mulvek(A,T[j],K)]:
od:
A:=TA:
nzeile:=[seq(0,j=1..nops(V[1]))]:
while V[nops(V)]=nzeile do
  E:=[op(E),A[nops(V)]]:
  A:=subsop(nops(V)=NULL,A):
  V:=subsop(nops(V)=NULL,V):
od:

E1:=[];
for i from 1 to nops(E) do
  e:=E[i];
  if abs(N(e,K))<>1 then printf("Fehler!\n"); fi;
  if e<>1 and e<>-1 then
    if coeff(e,a,degree(e,a))<0 then e:=-e; fi;
```

```
      E1:=[op(E1),e];
    fi;
  od;
  E1:=convert(E1,set); E:=convert(E1,list);

  hh_K:=0;
  if nops(V)=nops(V[1]) then hh_K:=linalg[det](V); fi;
  [hh_K,E];
end;

#########################################################################
# Reine kubische Zahlkoerper Q(d^(1/3)) #################################
#########################################################################

# Ausgabe: K, R, pp, la bzw. K, R, pp1, pp2, la1, la2
pur_cub:=proc()
  local d, x, K, p, a, b, R, pp, uvw, u, v, w, la, M, pp1, pp2, la1,
        la2;
  d:=args[1]; x:=args[2];
  K:=[x^3-d,x];
  p:=2; a:=1; b:=1;
  while p<=d do
    if d mod p^2=0 then b:=b*p; fi;
    if d mod p^3=0 then
      printf("d=%d nicht kubikfrei!\n",d); return [];
    fi;
    p:=nextprime(p);
  od;
  a:=d/b^2;
  if (a^2-b^2) mod 9>0 then
    R:=[x^2/b,x,1];
    if d mod 3>0 then
      pp:=[x^2/b-b,x-a,3];
    else
      pp:=[x^2/b,x,3];
    fi;
    for uvw from 1 to 26 do
      u:=iquo(uvw,9) mod 3;
      v:=iquo(uvw,3) mod 3;
      w:=uvw mod 3;
      la:=(u*R[1]+v*R[2]+w*R[3])/3;
      M:=denom(modul2matrix(map(t->nf(la*t,K),pp),R,K));
      if M=[[1,1,1],[1,1,1],[1,1,1]] then break; fi;
    od;
    return [K,R,pp,la];
  else
    R:=[(x^2+d*x+b^2)/(3*b),x,1];
    pp1:=[R[1]-b*(a^2+2)/3,R[2]-a,3];
    pp2:=[R[1]-b*(a^2-1)/3,R[2]-a,3];
    for uvw from 1 to 26 do
      u:=iquo(uvw,9) mod 3;
      v:=iquo(uvw,3) mod 3;
      w:=uvw mod 3;
      la1:=(u*R[1]+v*R[2]+w*R[3])/3;
```

```
      M:=denom(modul2matrix(map(t->nf(la1*t,K),pp1),R,K));
      if M=[[1,1,1],[1,1,1],[1,1,1]] then break; fi;
    od;
    for uvw from 1 to 26 do
      u:=iquo(uvw,9) mod 3;
      v:=iquo(uvw,3) mod 3;
      w:=uvw mod 3;
      la2:=(u*R[1]+v*R[2]+w*R[3])/3;
      M:=denom(modul2matrix(map(t->nf(la2*t,K),pp2),R,K));
      if M=[[1,1,1],[1,1,1],[1,1,1]] then break; fi;
    od;
    return [K,R,pp1,pp2,la1,la2];
  fi;
end;

# Typ eines reinen kubischen Zahlkoerpers:
# a^2<>b^2 mod 9 oder a^2=b^2 mod 9
# ist d 3-te Potenz oder nicht kubikfrei, wird 0 zurueckgegeben
typ_pur_cub:=proc()
  local d, p, a, b;
  d:=args[1];
  if d=1 then return 0; fi:
  p:=2; a:=1; b:=1;
  while p<=d do
    if d mod p^2=0 then b:=b*p; fi;
    if d mod p^3=0 then return 0; fi;
    p:=nextprime(p);
  od;
  a:=d/b^2;
  if (a^2-b^2) mod 9>0 then return 1; else return 2; fi;
end;

#############################################################################
```

ANHANG B

Übungsaufgaben

Aufgabe 1: Zeige, dass $\pi = 3.141592\ldots$ irrational ist.

(Anleitung: Wir nehmen an, es gilt $\pi = \frac{a}{b}$ mit natürlichen Zahlen a und b. Wir definieren

$$f(x) = \frac{x^n(a-bx)^n}{n!} \quad \text{und} \quad F(x) = f(x) - f^{(2)}(x) + f^{(4)}(x) - \cdots + (-1)^n f^{(2n)}(x).$$

Zeige zunächst, dass $f^{(i)}(0), f^{(i)}(\pi) \in \mathbf{Z}$ für alle i und damit $F(0), F(\pi) \in \mathbf{Z}$ gilt. Folgere mit

$$\frac{d}{dx}(F'(x)\sin x - F(x)\cos x) = (F''(x) + F(x))\sin x = f(x)\sin x$$

die Beziehung

$$\int_0^\pi f(x)\sin x dx = F(\pi) + F(0) \in \mathbf{Z}.$$

Zeige für $0 < x < \pi$ und hinreichend großes n

$$0 < f(x)\sin x < \frac{\pi^n a^n}{n!} < \frac{1}{\pi}$$

und folgere den Widerspruch

$$0 < \int_0^\pi f(x)\sin x dx < 1.)$$

Aufgabe 2: Zeige, dass die Menge der algebraischen Zahlen (in $\mathbf{C}$) abzählbar ist.

Aufgabe 3: Zeige, dass $\ln 2 = 0.6931\ldots$ transzendent ist.

Aufgabe 4: Zeige, dass $e^\pi = i^{-2i}$ gilt, und folgere mit dem Satz von Gelfond-Schneider die Transzendenz von e^π.

Aufgabe 5: Zeige mit dem Satz von Liouville, dass die Zahl $\sum_{k=1}^{\infty} \frac{1}{2^{k!}}$ transzendent ist.

Aufgabe 6: Zeige (mit dem Satz von Roth), dass die diophantische Gleichung

$$ax^3 + by^3 = c$$

bei vorgegebenen $a, b, c \in \mathbf{N}$ nur endlich viele Lösungen $x, y \in \mathbf{Z}$ hat.

Version vom 13.3.2003

Aufgabe 7: Zeige, dass mindestens eine der beiden Zahlen $e+\pi$ oder $e\pi$ irrational ist.

Aufgabe 8: Sei K der Zahlkörper $\mathbf{Q}(\alpha)$, wobei $f(\alpha)=0$ gilt mit $f=2x^4+3x^3+5x^2+7x+11$. Für die Elemente

$$\beta=\frac{13+17\alpha}{19+23\alpha} \quad \text{und} \quad \gamma=\alpha^{2002}$$

bestimme man die Darstellung als Linearkombination von $1,\alpha,\alpha^2,\alpha^3$ und das Minimalpolynom.

Aufgabe 9: (Erweiterter euklidischer Algorithmus für Polynome) Durch folgendes Verfahren erhält man zu zwei Polynomen $A,B\in\mathbf{Q}[x]$ eine Darstellung

$$AU+BV=D \quad \text{mit} \quad U,V,D\in\mathbf{Q}[x] \quad \text{und} \quad D=\mathrm{ggT}(A,B).$$

1. Setze $U:=1$, $D:=A$, $V_1:=0$, $V_3:=B$.
2. Ist $V_3=0$, berechne $V:=(D-AU)/B$ und gib U,V,D als Lösung aus.
3. Teile D durch V_3 mittels Polynomdivision: $D=QV_3+R$, setze $T:=U-V_1Q$, $U:=V_1$, $D:=V_3$, $V_1:=T$, $V_3:=R$ und gehe zurück zu 2.

Warum funktioniert das Verfahren?

Aufgabe 10: Ist K ein quadratischer Zahlkörper, so gilt für die Quadrate:

$$K^{*2}\cap\mathbf{Q}^*=\mathbf{Q}^{*2}\cup\mathbf{Q}^{*2}d,$$

wo d eine quadratfreie ganze Zahl ist. Zeige so, daß die quadratischen Zahlkörper in Bijektion zu den quadratfreien ganzen Zahlen $\neq 0,1$ stehen.

Aufgabe 11: Sind $K\subseteq L$ Zahlkörper, so ist L ein K-Vektorraum, jedes $\alpha\in L$ liefert also durch Multiplikation einen K-Vektorraum-Endomorphismus f_α von L. Man definiert dann Spur und Norm durch

$$\mathrm{Sp}_{L|K}(\alpha)=\mathrm{Sp}(f_\alpha) \quad \text{und} \quad \mathrm{N}_{L|K}(\alpha)=\det(f_\alpha).$$

Zeige, dass für drei Zahlkörper $K\subseteq L\subseteq M$ und $\alpha\in M$ gilt:

$$\mathrm{Sp}_{M|K}(\alpha)=\mathrm{Sp}_{L|K}(\mathrm{Sp}_{M|L}(\alpha)) \quad \text{und} \quad \mathrm{N}_{M|K}(\alpha)=\mathrm{N}_{L|K}(\mathrm{N}_{M|L}(\alpha)).$$

Aufgabe 12: Ist K ein Zahlkörper und $\alpha\in K$, so ist das charakteristische Polynom von α eine Potenz des Minimalpolynoms von α.

Aufgabe 13: Ist der Zahlkörper K über $\mathbf{Q}$ galoissch, so sind die Einbettungen $\sigma_i:K\to\mathbf{C}$ entweder alle reell oder es ist keine davon reell.

Aufgabe 14: Für einen kubischen Zahlkörper gilt $(r_1,r_2)\in\{(3,0),(1,1)\}$. Gib Beispiele für beide Möglichkeiten an.

Aufgabe 15: $K = \mathbf{Q}(\alpha)$ mit $f(\alpha) = 0$ und $f = x^3 - 3x + 1$.

1. Das Polynom f hat drei Nullstellen in K. Bestimme sie.
2. Diagonalisiere die rationale Darstellung von α.

Aufgabe 16: Sei K ein Zahlkörper vom Grad n und $n = r_1 + 2r_2$. Ist $\alpha_1, \ldots, \alpha_n$ eine $\mathbf{Q}$-Basis von K, so gilt für das Vorzeichen der Diskiminante

$$\operatorname{sgn}(\operatorname{disc}(\alpha_1, \ldots, \alpha_n)) = (-1)^{r_2}.$$

Aufgabe 17: Ist K ein Zahlkörper vom Grad n, so gibt es eine $\mathbf{Q}$-Basis $\alpha_1, \ldots, \alpha_n$ von K, so daß $(\operatorname{Sp}(\alpha_i\alpha_j))$ eine Diagonalmatrix ist.

Aufgabe 18: Sei K ein Zahlkörper vom Grad n, seien $\sigma_1, \ldots, \sigma_{r_1}$ die reellen, $\tau_1, \overline{\tau_1}, \ldots, \tau_{r_2}, \overline{\tau_{r_2}}$ die komplexen Einbettungen von K in $\mathbf{C}$. Wir betrachten $\mathbf{R}^n$ mit den Koordinaten

$$x_1, \ldots, x_{r_1}, y_1, z_1, \ldots, y_{r_2}, z_{r_2}$$

und definieren eine symmetrische Bilinearform auf $\mathbf{R}^n$ durch

$$Q((x_1, \ldots, x_{r_1}, y_1, z_1, \ldots, y_{r_2}, z_{r_2}), (\widetilde{x}_1, \ldots, \widetilde{x}_{r_1}, \widetilde{y}_1, \widetilde{z}_1, \ldots, \widetilde{y}_{r_2}, \widetilde{z}_{r_2})) = \sum_{i=1}^{r_1} x_i\widetilde{x}_i + 2\sum_{j=1}^{r_2}(y_j\widetilde{y}_j - z_j\widetilde{z}_j).$$

Definiert man $\psi : K \to \mathbf{R}^n$ durch

$$\psi(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_{r_1}(\alpha), \operatorname{Re}(\tau_1(\alpha)), \operatorname{Im}(\tau_1(\alpha)), \ldots, \operatorname{Re}(\tau_{r_2}(\alpha)), \operatorname{Im}(\tau_{r_2}(\alpha))),$$

so gilt:

1. $\alpha_1, \ldots, \alpha_n \in K$ sind genau dann eine $\mathbf{Q}$-Basis von K, wenn $\psi(\alpha_1), \ldots, \psi(\alpha_n)$ eine $\mathbf{R}$-Basis von $\mathbf{R}^n$ bilden.
2. Für $\alpha, \beta \in K$ gilt
$$\operatorname{Sp}(\alpha\beta) = Q(\psi(\alpha), \psi(\beta)).$$
3. Ist $\alpha_1, \ldots, \alpha_n \in K$ eine Orthogonalbasis bzgl. der Spurform von K, d.h. gilt $\operatorname{Sp}(\alpha_i\alpha_j) = 0$ für $i \neq j$, so sind von den n Zahlen $\operatorname{Sp}(\alpha_i\alpha_i)$ genau $r_1 + r_2$ Zahlen positiv und r_2 negativ. (Hinweis: Sylvesterscher Trägheitssatz)

Aufgabe 19: Man definiere Zahlkörper $K = \mathbf{Q}(\alpha)$ und $L = \mathbf{Q}(\beta)$ durch $f(\alpha) = 0$ und $g(\beta) = 0$, wobei

$$f = x^3 - 86x^2 - 51x - 8 \quad \text{und} \quad g = x^3 - 38x^2 + 234x - 431$$

gilt. Sind K und L isomorph?

Aufgabe 20: Sei $K = \mathbf{Q}(\alpha)$ mit $\alpha^3 = 2$ und U der von

$$\frac{1}{\alpha + 1}, \quad \frac{1}{\alpha + 2}, \quad \frac{1}{\alpha + 3}$$

erzeugte Untermodul von K. Bestimme die Hermitesche Normalform von U bzgl. der $\mathbf{Q}$-Basis $1, \alpha, \alpha^2$ und $\operatorname{disc}(U)$.

Aufgabe 21: Wieviele Untermoduln vom Index p hat $\mathbf{Z}^2$, wenn p eine Primzahl ist?

Aufgabe 22: Zeige, daß sich jedes Element α eines Zahlkörpers schreiben läßt als $\alpha = \frac{1}{d}\beta$, wo d eine natürliche Zahl ist und β ganz algebraisch ist.

Aufgabe 23: Sei K ein Zahlkörper vom Grad $n \geq 2$ und

$$R = \mathbf{Z} + \mathbf{Z}\omega_2 + \cdots + \mathbf{Z}\omega_n$$

eine Ordnung. Für $d \in \mathbf{N}$ ist dann

$$R_d = \mathbf{Z} + \mathbf{Z} \cdot d\omega_2 + \cdots + \mathbf{Z} \cdot d\omega_n$$

eine Ordnung mit $[R : R_d] = d^{n-1}$.

Aufgabe 24: Sei $K = \mathbf{Q}(\alpha)$ mit $\alpha^3 = 2$. Zeige:

1. $\mathbf{Z}[\alpha] = \mathbf{Z}[\alpha + \alpha^2]$, aber $\mathbf{Z}[2\alpha] \neq \mathbf{Z}[2\alpha + 2\alpha^2]$.
2. $\mathbf{Z}[\alpha - \alpha^2] = \mathbf{Z}[5\alpha + 4\alpha^2]$.

Aufgabe 25: Zeige, daß folgende Gleichungen keine Lösungen $x, y \in \mathbf{Z}$ besitzen:

$$x^3 - 2y^3 = 4, \quad x^3 - 2y^3 = 5, \quad x^3 - 2y^3 = 9.$$

Aufgabe 26: Sei $d \in \mathbf{Z} \setminus \{0, 1\}$ quadratfrei. Die Ordnungen des Zahlkörpers $\mathbf{Q}(\sqrt{d})$ sind dann

$$R_f = \begin{cases} \mathbf{Z} + \mathbf{Z}f\frac{1+\sqrt{d}}{2} & \text{für } d \equiv 1 \bmod 4, \\ \mathbf{Z} + \mathbf{Z}f\sqrt{d} & \text{für } d \equiv 2, 3 \bmod 4 \end{cases} \quad \text{mit} \quad f \in \mathbf{N}.$$

Zeige für $f, g \in \mathbf{N}$

$$R_g \subseteq R_f \quad \Longleftrightarrow \quad f | g$$

und

$$R_f R_g = R_{\mathrm{ggT}(f,g)}.$$

Aufgabe 27: Sei $f = a_3x^3 + a_2x^2 + a_1x + a_0 \in \mathbf{Z}[x]$ ein über $\mathbf{Q}$ irreduzibles Polynom, $K = \mathbf{Q}(\alpha)$ mit $f(\alpha) = 0$, und $\beta = a_3\alpha, \gamma = a_3\alpha^2 + a_2\alpha \in K$. Zeige, dass

$$R = \mathbf{Z} + \mathbf{Z}\beta + \mathbf{Z}\gamma$$

eine Ordnung in K ist, und dass $\mathrm{disc}\,(R) = \mathrm{disc}\,(f)$ gilt.

Aufgabe 28: Bestimme für jedes $d \in \{-23, -31, -44\}$ einen kubischen Zahlkörper K mit Diskriminante $\mathrm{disc}\,(K) = d$.

Aufgabe 29: Bestimme eine Ganzheitsbasis für $K = \mathbf{Q}(\alpha)$ mit $\alpha^3 = 10$.

Aufgabe 30: Sei $K = \mathbf{Q}(\alpha)$ mit $\alpha^2 = -5$ und $R = \mathbf{Z}[\alpha]$. Es gilt

$$6 = 2 \cdot 3 = (1+\alpha)(1-\alpha).$$

Bestimme Ideale $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \mathfrak{a}_4 \subseteq R$ (und ihre hermitesche Normalform bzgl. der Basis $\alpha, 1$), sodass

$$(2) = \mathfrak{a}_1\mathfrak{a}_2, \quad (3) = \mathfrak{a}_3\mathfrak{a}_4, \quad (1+\alpha) = \mathfrak{a}_1\mathfrak{a}_3, \quad (1-\alpha) = \mathfrak{a}_2\mathfrak{a}_4$$

gilt, und erkläre damit obige Faktorisierung auf Idealebene.

Aufgabe 31: Sei $K = \mathbf{Q}(\alpha)$ mit $\alpha^3 - \alpha - 1 = 0$.

1. Zeige, dass $\mathbf{Z}[\alpha]$ die Maximalordnung von K ist.
2. Bestimme die hermitesche Normalform aller Ideale von $\mathbf{Z}[\alpha]$ mit Norm 59 bzgl. der $\mathbf{Z}$-Basis $\alpha^2, \alpha, 1$.

Aufgabe 32: Zeige, dass für teilerfremde Ideale $\mathfrak{a}$ und $\mathfrak{b}$ einer Ordnung R gilt:

$$\mathrm{N}(\mathfrak{a}\mathfrak{b}) = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b}).$$

Aufgabe 33: Sei $\mathfrak{a}$ ein Ideal einer Ordnung R, seien a_1, a_2 teilerfremde natürliche Zahlen mit $a_1 a_2 \in \mathfrak{a}$. Zeige: $\mathfrak{a}_1 = \mathfrak{a} + Ra_1$ und $\mathfrak{a}_2 = \mathfrak{a} + Ra_2$ sind teilerfremde Ideale und es gilt

$$\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2, \quad \mathrm{N}(\mathfrak{a}) = \mathrm{N}(\mathfrak{a}_1)\mathrm{N}(\mathfrak{a}_2), \quad \mathrm{ggT}(\mathrm{N}(\mathfrak{a}_1), \mathrm{N}(\mathfrak{a}_2)) = 1.$$

Aufgabe 34: Sei $K = \mathbf{Q}(\alpha)$ mit $\alpha^2 = 17$. Bestimme die Primideale der Ordnungen $R = \mathbf{Z}[\alpha]$ und $S = \mathbf{Z}[\frac{1+\alpha}{2}]$, die das Element 2 enthalten, und vergleiche sie.

Aufgabe 35: In der Maximalordnung $R = \mathbf{Z}[\frac{1+\sqrt{-3}}{2}]$ des Zahlkörpers $K = \mathbf{Q}(\sqrt{-3})$ gibt es für $p \equiv 1 \bmod 3$ genau zwei Primideale, die p enthalten, sonst genau eines. (Hinweis: $R = \mathbf{Z}[\zeta_3]$ mit der dritten Einheitswurzel $\zeta_3 = \frac{-1+\sqrt{-3}}{2}$.)

Aufgabe 36: Die drei Polynome

$$f_1 = x^3 - 18x - 6, \quad f_2 = x^3 - 36x - 78, \quad f_3 = x^3 - 54x - 150$$

sind irreduzibel über $\mathbf{Q}$ und haben die gleiche Diskriminante $\mathrm{disc}\, f_i = 22356 = 2^2 \cdot 3^5 \cdot 23$. Man definiert

$$K_i = \mathbf{Q}(\alpha_i) \quad \text{mit} \quad f_i(\alpha_i) = 0.$$

1. Zeige, dass $\mathbf{Z}_{K_i} = \mathbf{Z}[\alpha_i]$ gilt. (Insbesondere haben dann alle drei Zahlkörper die gleiche Diskriminante 22356.)
2. Bestimme jeweils die $p = 5$ und $p = 11$ enthaltenden Primideale von $\mathbf{Z}_{K_i}$.
3. Folgere, dass alle drei Zahlkörper K_i paarweise nicht isomorph sind.

Aufgabe 37: Sei $K = \mathbf{Q}(\xi)$ mit $f(\xi) = 0$ und $f = x^3 + x^2 - 2x + 8$. Dann ist

$$\mathbf{Z}_K = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2 + \mathbf{Z}\omega_3 \quad \text{mit} \quad \omega_1 = \frac{\xi^2 + \xi}{2}, \quad \omega_2 = \xi, \quad \omega_3 = 1.$$

Die Primideale von $\mathbf{Z}_K$, die 2 enthalten, sind

$$\mathfrak{p}_1 = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2 + \mathbf{Z}2, \quad \mathfrak{p}_2 = \mathbf{Z}(\omega_1+1) + \mathbf{Z}\omega_2 + \mathbf{Z}2, \quad \mathfrak{p}_3 = \mathbf{Z}(\omega_1+1) + \mathbf{Z}(\omega_2+1) + \mathbf{Z}2.$$

1. Zeige, dass es für jedes $i = 1,2,3$ eine Ordnung $R_i = \mathbf{Z}[\alpha_i]$ und ein Primideal $\mathfrak{q}_i \subseteq R_i$ gibt mit $\mathbf{Z}_K\mathfrak{q}_i = \mathfrak{p}_i$.
2. Zeige, dass in jedem Fall $R_1 \neq R_2$, $R_1 \neq R_3$, $R_2 \neq R_3$ gelten muss.

Aufgabe 38: Für $K = \mathbf{Q}(\sqrt{2},\sqrt{3})$ ist $\mathbf{Z}_K = \mathbf{Z}[\alpha]$ mit $\alpha = \frac{1}{2}(\sqrt{2}+\sqrt{6})$, wobei α das Minimalpolynom $f = x^4 - 4x^2 + 1$ hat.

1. Bestimme für jede Primzahl $p \leq 30$ alle Primideale $\mathfrak{p} \subseteq \mathbf{Z}_K$, die p enthalten.
2. Zeige, dass es kein Primideal $\mathfrak{p} \subseteq \mathbf{Z}_K$ gibt mit

$$\mathrm{N}(\mathfrak{p}) = p^3 \quad \text{oder} \quad \mathrm{N}(\mathfrak{p}) = p^4,$$

wenn p die in $\mathfrak{p}$ enthaltende Primzahl ist.

Aufgabe 39: Sei $\mathfrak{a}$ ein von 0 verschiedenes Ideal der Ordnung R eines Zahlkörpers K vom Grad n. Dann gibt es eine natürliche Zahl $\ell(\mathfrak{a}) \in \mathbf{N}$ mit $\mathfrak{a} \cap \mathbf{Z} = \mathbf{Z}\ell(\mathfrak{a})$. Zeige die Teilbarkeitsbeziehungen

$$\ell(\mathfrak{a}) | \mathrm{N}(\mathfrak{a}) \quad \text{und} \quad \mathrm{N}(\mathfrak{a}) | \ell(\mathfrak{a})^n.$$

Aufgabe 40: Sei R Ordnung eines Zahlkörpers und m eine natürliche Zahl ($\neq 0$). Zeige, dass es nur endlich viele R-Ideale gibt mit $\mathfrak{a} \cap \mathbf{Z} = \mathbf{Z} \cdot m$.

Aufgabe 41: Sei $K = \mathbf{Q}(\alpha)$ mit $\alpha^3 - \alpha - 1 = 0$ und $R = \mathbf{Z}[\alpha]$. Bestimme für das R-Ideal $\mathfrak{a} = (5, \alpha^2+2\alpha+3)$ eine $\mathbf{Z}$-Basis des gebrochenen R-Ideals $\widetilde{\mathfrak{a}} = \{\lambda \in K : \lambda\mathfrak{a} \subseteq R\}$.

Aufgabe 42: Sei R eine Ordnung eines Zahlkörpers K und $\mathfrak{b} \subseteq \mathfrak{c}$ Ideale in R. Man definiert

$$(\mathfrak{b} : \mathfrak{c}) = \{\lambda \in K : \lambda\mathfrak{c} \subseteq \mathfrak{b}\}.$$

Zeige:

1. $(\mathfrak{b} : \mathfrak{c})$ ist ein gebrochenes R-Ideal.
2. Ist $\mathfrak{c}$ invertierbar, so gilt $(\mathfrak{b} : \mathfrak{c}) = \mathfrak{b}\mathfrak{c}^{-1}$ und $(\mathfrak{b} : \mathfrak{c}) \subseteq R$.
3. Für $R = \mathbf{Z}[\sqrt{5}]$ und $\mathfrak{b} = \mathfrak{c} = \mathbf{Z} \cdot (1+\sqrt{5}) + \mathbf{Z} \cdot 2$ ist $(\mathfrak{b} : \mathfrak{c}) \supsetneq R$.

Aufgabe 43: Sei $K = \mathbf{Q}(\alpha)$ mit $\alpha^2 = -11$ und $R = \mathbf{Z}[\alpha]$. Bestimme für die R-Ideale

$$\mathfrak{a}_2 = (2, \alpha+1) \quad \text{und} \quad \mathfrak{a}_8 = 2\mathfrak{a}_2$$

das gebrochene R-Ideal $(\mathfrak{a}_8 : \mathfrak{a}_2)$ und zeige, dass

$$R/(\mathfrak{a}_8 : \mathfrak{a}_2) \not\cong \mathfrak{a}_2/\mathfrak{a}_8$$

gilt.

Aufgabe 44: Seien $R \subseteq S$ Ordnungen eines Zahlkörpers K. Zeige:

1. Ist das R-Ideal $\mathfrak{a} \subseteq R$ invertierbar, so auch das S-Ideal $S\mathfrak{a} \subseteq S$.
2. Ist das S-Ideal $\mathfrak{A} \subseteq S$ invertierbar und gilt $\mathrm{ggT}(\mathrm{N}\mathfrak{A}, [S : R]) = 1$, so ist auch das R-Ideal $\mathfrak{A} \cap R \subseteq R$ invertierbar.

Aufgabe 45: Im Zahlkörper $K = \mathbf{Q}(\alpha)$ mit $\alpha^4 - 4\alpha^2 + 1 = 0$ ist $\mathbf{Z}_K = \mathbf{Z}[\alpha]$. Bestimme die Primidealzerlegung von $\alpha^3 + 50$.

Aufgabe 46: Sei $\mathbf{Z}_K = \mathbf{Z}[\alpha]$ und $m \in \mathbf{Z}$. Ist dann

$$(\alpha - m) = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_r^{e_r}$$

die Primidealzerlegung von $\alpha - m$ in $\mathbf{Z}_K$ und

$$\mathrm{N}\mathfrak{p}_i = p_i^{f_i},$$

so gilt $f_i = 1$ und $p_i \neq p_j$ für $i \neq j$.

Aufgabe 47: Sei $\mathfrak{p}$ ein die Primzahl p enthaltendes Primideal der Maximalordnung $\mathbf{Z}_K$ eines Zahlkörpers K. Dann gibt es für alle $m \in \mathbf{N}$ eine Zahl $u(m) \in \mathbf{N}$ mit

$$\mathfrak{p}^m \cap \mathbf{Z} = \mathbf{Z}p^{u(m)}.$$

Bestimme $u(m)$.

Aufgabe 48: Sei $\mathfrak{p} = (p, \alpha)$ ein Primideal in der Maximalordnung eines Zahlkörpers, p eine Primzahl und $e = v_{\mathfrak{p}}(p)$. Zeige, daß für alle $m \in \mathbf{N}$

$$(p, \alpha^m) = \mathfrak{p}^{\min(e,m)}$$

gilt.

Aufgabe 49: Bestimme die ganzzahligen Lösungen der Gleichung

$$x^3 - y^3 = 728.$$

Aufgabe 50: Das Polynom $f = x^4 - 5x^3 + 15x^2 - 5x + 55$ kann modulo p in verschiedener Weise zerfallen, z.B. in 4 Linearfaktoren, in 2 irreduzible quadratische Faktoren, etc. Untersuche experimentell, welche Möglichkeiten auftreten. Kann man der Primzahl p das Zerfallsverhalten von $f \bmod p$ ansehen?

Aufgabe 51: Seien $\alpha_1, \ldots, \alpha_r$ Elemente der Maximalordnung eines Zahlkörpers. Dann gilt für alle natürlichen Zahlen m die Idealgleichung

$$(\alpha_1, \ldots, \alpha_r)^m = (\alpha_1^m, \ldots, \alpha_r^m).$$

Aufgabe 52: Sei $K = \mathbf{Q}(\alpha)$ mit $\alpha^3 - \alpha - 8 = 0$.

1. Bestimme eine Ganzheitsbasis von $\mathbf{Z}_K$.
2. In $\mathbf{Z}_K$ gilt eine Primidealzerlegung $(2) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$. Bestimme α_i mit $\mathfrak{p}_i = (2, \alpha_i)$.

Aufgabe 53: Bestimme für $K = \mathbf{Q}(\alpha)$ mit $\alpha^3 - \alpha - 8 = 0$ das Führerideal $\mathfrak{f}$ der Ordnung $\mathbf{Z}[\alpha]$ in $\mathbf{Z}_K$ sowie seine Primidealzerlegung in $\mathbf{Z}_K$.

Aufgabe 54: Bestimme alle ganzzahligen Lösungen der Gleichung

$$y^2 = x^3 - 11.$$

(Hinweis: Man faktorisiere $x^3 = (y+\sqrt{-11})(y-\sqrt{-11})$ und rechne in der Maximalordnung von $\mathbf{Q}(\sqrt{-11})$.)

Aufgabe 55: Ein Integritätsring R heißt euklidisch bzgl. einer Funktion $\lambda : R \to \mathbf{N}_0$, wenn zu $a, b \in R$ mit $b \neq 0$ stets $q, r \in R$ mit $a = qb + r$ und $\lambda(r) < \lambda(b)$ existieren. Sei $\{\lambda(a) : a \in R\} = \{n_0, n_1, n_2, \dots\}$ mit $n_0 < n_1 < n_2 < \dots$ und $\widetilde{\lambda} : R \to \mathbf{N}_0$ mit $\widetilde{\lambda}(a) = \min\{\lambda(ua) : u \in R^*\}$. Zeige:

1. R ist auch euklidisch bzgl. der Funktion $\widetilde{\lambda}$. (Elemente, die sich nur um eine Einheit unterscheiden haben dann den gleichen $\widetilde{\lambda}$-Wert.)
2. $\lambda(a) = n_0 \iff a = 0$.
3. $\widetilde{\lambda}(a) = n_1 \iff a \in R^*$.
4. Für $a, b \in R \setminus \{0\}$ mit $Rb \subsetneq Ra$ gilt $\widetilde{\lambda}(a) < \widetilde{\lambda}(b)$.
5. Ist $\widetilde{\lambda}(a) = n_2$, so gilt für $x \in R$ die Kongruenz $x \equiv 0 \bmod a$ oder $x \equiv u \bmod a$ mit einer Einheit $u \in R^*$. (Insbesondere folgt $\#R/Ra \leq 1 + \#R^*$.)

Aufgabe 56: Sei $R = \mathbf{Z}_K$ mit $K = \mathbf{Q}(\sqrt{-d})$, $d \geq 1$ quadratfrei und $d \neq 1, 2, 3, 7, 11$. Dann gilt:

1. $R^* = \{\pm 1\}$.
2. Für $\alpha \in R$, $\alpha \neq 0, \pm 1$ gilt $N\alpha \geq 4$.
3. Folgere (mit Aufgabe 55.5), dass R kein euklidischer Ring sein kann.

(Die einzigen imaginärquadratischen Ordnungen $\mathbf{Z}_{\mathbf{Q}(\sqrt{-d})}$, die euklidisch sind, treten also für $d = 1, 2, 3, 7, 11$ auf und sind bereits euklidisch bzgl. der Norm.)

Aufgabe 57: Zeige, dass die Ringe $\mathbf{Z}[\sqrt{2}]$ und $\mathbf{Z}[\sqrt{3}]$ euklidisch bzgl. der Normfunktion $\alpha \mapsto |\mathrm{N}\alpha|$ sind.

Aufgabe 58: Mit dieser Aufgabe soll gezeigt werden, dass die Ringe

$$\mathbf{Z}[\sqrt{2}], \quad \mathbf{Z}[\sqrt{3}], \quad \mathbf{Z}[\sqrt{6}], \quad \mathbf{Z}[\sqrt{7}]$$

euklidisch bzgl. der Normabbildung $\alpha \mapsto |\mathrm{N}(\alpha)|$ sind.

1. Sei $d \geq 2$ eine quadratfreie natürliche Zahl und seien r, s rationale Zahlen, sodass

$$|(r - x)^2 - d(s - y)^2| \geq 1 \quad \text{für alle } x, y \in \mathbf{Z}$$

gilt.

   (a) Zeige, dass man o.E. $0 \leq r, s \leq \frac{1}{2}$ annehmen kann. (Sei von hier an $0 \leq r, s \leq \frac{1}{2}$.)

(b) Zeige, dass $|(1-r)^2 - ds^2| \geq 1$ und

$$ds^2 \geq 1 + (1-r)^2$$

gilt.

(c) Zeige, dass $|(1+r)^2 - ds^2| \geq 1$ gilt.

(d) Gilt $(1+r)^2 - ds^2 \geq 1$, so folgt $r = s = \frac{1}{2}$ und $d = 5$.

(e) Gilt $ds^2 - (1+r)^2 \geq 1$, so folgt $d \geq 8$.

(f) Folgere $d \notin \{2, 3, 6, 7\}$.

2. Zeige, dass der Ring $\mathbf{Z}[\sqrt{d}]$ für $d \in \{2, 3, 6, 7\}$ euklidisch bzgl. der Norm ist.

(Bemerkung: Für reellquadratische Zahlkörper $K = \mathbf{Q}(\sqrt{d})$, $d \geq 2$ quadratfrei, ist $\mathbf{Z}_K$ genau dann euklidisch bzgl. der Norm $\alpha \mapsto |\mathrm{N}\alpha|$, wenn

$$d \in \{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}$$

gilt.)

Aufgabe 59: Zeige, dass $\mathbf{Z}[\sqrt{10}]$ nicht euklidisch bzgl. der Norm $\alpha \mapsto |\mathrm{N}(\alpha)|$ ist. (Hinweis: Versuche, $\sqrt{10}$ durch 2 mit Rest zu dividieren.)

Aufgabe 60: Die Aufgabe soll zeigen, dass $\mathbf{Z}[\sqrt{23}]$ ein Hauptidealring, aber kein (bzgl. der Norm) euklidischer Ring ist.

1. Zeige, dass die Gleichungen $23x^2 - (11 - 23y)^2 = 17$ und $23x^2 - (11 - 23y)^2 = -6$ keine ganzzahligen Lösungen besitzen.
2. Zeige, dass es keine $q, r \in \mathbf{Z}[\sqrt{23}]$ gibt mit

$$11\sqrt{23} = q \cdot 23 + r \quad \text{und} \quad |\mathrm{N}(r)| < |\mathrm{N}(23)|.$$

Also ist $\mathbf{Z}[\sqrt{23}]$ nicht euklidisch bzgl. der Normfunktion.

3. Beweise, dass $\mathbf{Z}[\sqrt{23}]$ ein Hauptidealring ist.

Aufgabe 61: Sei $d \geq 2$ eine quadratfreie natürliche Zahl mit $d \equiv 2, 3 \bmod 4$. Es wird ein hinreichendes Kriterium hergeleitet um zu zeigen, dass der Ring $\mathbf{Z}[\sqrt{d}]$ nicht euklidisch bzgl. der Normfunktion ist.

1. Es existiere eine natürliche Zahl m mit

$$m \equiv 1 \bmod 2 \quad \text{und} \quad \begin{cases} \sqrt{2d} < m < \sqrt{3d} & \text{für } d \equiv 2 \bmod 4, \\ \sqrt{5d} < m < \sqrt{6d} & \text{für } d \equiv 3 \bmod 4. \end{cases}$$

(a) Für alle $x, y \in \mathbf{Z}$ gilt

$$\begin{aligned} x^2 - dy^2 + 2my &\not\equiv 2 \bmod 8 \quad \text{für } d \equiv 2 \bmod 4, \\ x^2 - dy^2 + 2my &\not\equiv 3 \bmod 8 \quad \text{für } d \equiv 2 \bmod 4, \\ x^2 - dy^2 + 2my &\not\equiv 5 \bmod 8 \quad \text{für } d \equiv 3 \bmod 4, \\ x^2 - dy^2 + 2my &\not\equiv 6 \bmod 8 \quad \text{für } d \equiv 3 \bmod 4. \end{aligned}$$

(b) Für alle $x, y \in \mathbf{Z}$ gilt

$$|x^2 - (\frac{m}{d} - y)^2 d| \geq 1.$$

(c) Schreibt man $m\sqrt{d} = q \cdot d + r$ mit $q, r \in \mathbf{Z}[\sqrt{d}]$, so folgt $|\mathrm{N}(r)| \geq |\mathrm{N}(d)|$. Insbesondere ist dann $\mathbf{Z}[\sqrt{d}]$ nicht euklidisch bzgl. der Normabbildung $\alpha \mapsto |\mathrm{N}\alpha|$.

2. Bestimme alle d's, die die Voraussetzung in 1. erfüllen, für die demnach $\mathbf{Z}[\sqrt{d}]$ nicht euklidisch bzgl. der Normabbildung $\alpha \mapsto |\mathrm{N}\alpha|$ ist.

Aufgabe 62: Beweise folgende Version des Minkowskischen Gitterpunktsatzes: Ist $\Gamma \subseteq \mathbf{R}^n$ ein Gitter vom Rang n und $X \subseteq \mathbf{R}^n$ kompakt, symmetrisch, konvex mit

$$\mathrm{vol}\,(X) \geq 2^n \mathrm{vol}\,(\Gamma),$$

so enthält der Durchschnitt $X \cap \Gamma$ einen von 0 verschiedenen Punkt.

Aufgabe 63: Beweise mit Hilfe des Minkowskischen Gitterpunktsatzes den Minkowskischen Linearformensatz: Ist $(a_{ij}) \in GL_n(\mathbf{R})$ und sind $c_1, \ldots, c_n$ positive reelle Zahlen mit $c_1 \ldots c_n > |\det(a_{ij})|$, so gibt es ganze Zahlen $m_1, \ldots, m_n \in \mathbf{Z}$, $(m_1, \ldots, m_n) \neq (0, \ldots, 0)$, mit

$$|\sum_{j=1}^{n} a_{ij} m_j| < c_i \quad \text{für} \quad i = 1, \ldots, n.$$

Aufgabe 64: Zeige, dass folgende Ringe faktoriell sind:

$$\mathbf{Z}[\sqrt{-1}], \quad \mathbf{Z}[\sqrt{-2}], \quad \mathbf{Z}[\frac{1+\sqrt{-3}}{2}], \quad \mathbf{Z}[\frac{1+\sqrt{-7}}{2}], \quad \mathbf{Z}[\frac{1+\sqrt{-11}}{2}], \quad \mathbf{Z}[\frac{1+\sqrt{-19}}{2}],$$
$$\mathbf{Z}[\frac{1+\sqrt{-43}}{2}], \quad \mathbf{Z}[\frac{1+\sqrt{-67}}{2}], \quad \mathbf{Z}[\frac{1+\sqrt{-163}}{2}].$$

Aufgabe 65: Berechne in $K = \mathbf{Q}(\alpha)$ mit $\alpha^2 = -7$ die Klassengruppen $C\ell(R)$ für die Ordnungen

$$R = \mathbf{Z}[\alpha] \quad \text{und} \quad R = \mathbf{Z}[\frac{1+3\alpha}{2}].$$

Aufgabe 66: Bestimme die Klassengruppen für $\mathbf{Z}[\sqrt{-17}]$ und $\mathbf{Z}[\sqrt{-21}]$.

Aufgabe 67: Ist d eine natürliche Zahl mit $d = 3m$ und $m \equiv 2, 3, 4, 5, 6, 7 \bmod 9$, so hat die diophantische Gleichung

$$x^3 + dy^3 = 3z^3$$

nur die triviale Lösung $x = y = z = 0$ in ganzen Zahlen.

Aufgabe 68:

1. Ist d eine kubenfreie natürliche Zahl und p ein Primteiler von d, sodass die Kongruenz $x^3 \equiv 3 \bmod p$ keine Lösung besitzt, so hat die diophantische Gleichung
$$x^3 + dy^3 = 3z^3$$
nur die Lösung $x = y = z = 0$ in ganzen Zahlen.
2. Für welche $d \leq 100$ kann man das Kriterium in 1. anwenden?

Aufgabe 69: Für $K = \mathbf{Q}(\alpha)$ mit $2 + 3\alpha + 5\alpha^2 + 7\alpha^3 + \alpha^4 = 0$ ist $\mathbf{Z}_K = \mathbf{Z}[\alpha]$ ein Hauptidealring. Es gibt genau ein Primideal $\mathfrak{p}$ mit Norm $p = 2^{128} - 159$. Bestimme ein $\pi \in \mathbf{Z}_K$ mit $\mathfrak{p} = (\pi)$.

Aufgabe 70: Welche Einheitswurzeln kann ein Zahlkörper vom Grad 2, 4, 6, 8 oder 10 enthalten?

Aufgabe 71: Beweise folgenden Zusammenhang zwischen Regulator und Gittervolumen für die Einheiten einer Ordnung R

$$\mathrm{vol}\,(\ell(R^*)) = \sqrt{r_1 + r_2} \cdot \mathrm{Reg}\,(R).$$

Aufgabe 72: Bestimme für $K = \mathbf{Q}(\alpha)$ mit $\alpha^3 + 7\alpha + 20 = 0$ eine Grundeinheit des Ringes $\mathbf{Z}_K$.

Aufgabe 73: Bestimme eine Grundeinheit des Ringes $\mathbf{Z}_K$ für $K = \mathbf{Q}(i, \sqrt{2})$.

Aufgabe 74: Bestimme alle ganzzahligen Lösungen der diophantischen Gleichungen

$$3x^2 - 4y^2 = 11.$$

Aufgabe 75: Sei $K = \mathbf{Q}(\alpha)$ mit $\alpha^6 + 3 = 0$.

1. Bestimme eine $\mathbf{Z}$-Basis von $\mathbf{Z}_K$.
2. Bestimme die Primidealzerlegungen von 2 und 3 in $\mathbf{Z}_K$.
3. Bestimme $\mathbf{Z}_K^*$.

Aufgabe 76: Sei $K = \mathbf{Q}(\sqrt{61})$.

1. Zeige, dass
$$\varepsilon = \frac{39}{2} - \frac{5}{2}\sqrt{61}$$
eine Grundeinheit von $\mathbf{Z}_K = \mathbf{Z}[\frac{1+\sqrt{61}}{2}]$ ist.
2. Sind $x, y \in \mathbf{Z}$ mit $x^2 - 61y^2 = 1$, so ist $x + y\sqrt{61}$ eine Einheit von $\mathbf{Z}_K$, also gibt es ein $n \in \mathbf{Z}$ mit
$$x + y\sqrt{61} = \pm\varepsilon^n.$$
Welche n's kommen vor?

Aufgabe 77: Bestimme das kleinste $x \in \mathbf{N} \setminus \{1\}$, sodass ein $y \in \mathbf{Z}$ existiert mit

$$x^2 - 109y^2 = 1.$$

(Hinweis: Bestimme zunächst eine Grundeinheit von $\mathbf{Z}_{\mathbf{Q}(\sqrt{109})}$.)

Aufgabe 78: Die Schlacht von Hastings (14.10.1066): Harolds Mannen standen nach alter Gewohnheit dichtgedrängt in 13 gleichgroßen Quadraten aufgestellt, und wehe dem Normannen, der es wagte, in eine solche Phalanx einbrechen zu wollen ... Als aber Harold selbst auf dem Schlachtfeld erschien, formten die Sachsen ein einziges gewaltiges Quadrat mit ihrem König an der Spitze und stürmten mit den Schlachtrufen 'Ut!', 'Olicrosse!', 'Godemite!' vorwärts ... (vgl. Carmen de Hastingae Proelio von Guy, Bischof

von Amiens).
Frage: Wie groß soll die Armee Harolds II. gewesen sein?
(Aus: J. Neukirch, Algebraische Zahlentheorie, nach einer Mitteilung von W.-D. Geyer.)

Aufgabe 79: Bestimme die Klassenzahl von $\mathbf{Q}(\sqrt[3]{170})$.

Aufgabe 80: Bestimme die Klassenzahl von $\mathbf{Q}(\sqrt[3]{239})$.

Aufgabe 81: Sei p eine Primzahl. Zeige:

1. Es gibt ein $c \in \mathbf{Z}$, sodass das Polynom $x^2 + x + c$ irreduzibel modulo p ist.
2. Sei $\ell \geq 1$ und setze mit einem c wie in 1.
$$f = x^2 + p^\ell x + cp^{2\ell}.$$
Dann ist
$$f(0) \equiv 0 \bmod p^{2\ell} \quad \text{und} \quad v_p(f'(0)) = \ell,$$
aber es gibt kein $w \in \mathbf{Z}$ mit $f(w) \equiv 0 \bmod p^{2\ell+1}$.

Aufgabe 82: Sei $a \in \mathbf{Z}$ mit $a \equiv 1 \bmod 2$. Charakterisiere, wann das Polynom $f(x) = x^2 - a$ für alle $n \geq 1$ eine Nullstelle modulo 2^n hat.

Aufgabe 83: Sei
$$f(x, y, z) = 3y^2z + 3x^2y - 6y^2x - 21xzy + z^3 + y^3 + x^3 - 6yz^2 + 3xz^2 - 6x^2z.$$
Zeige, dass $f(x, y, z) \equiv 0 \bmod p$ genau dann eine nichttriviale Lösung modulo p besitzt, wenn $p \equiv 1, 3, 8 \bmod 9$ gilt.

Aufgabe 84: Seien p und q ungerade Primzahlen, die den Ungleichungen
$$p < q < p + 2\sqrt{2p} + 2$$
genügen. Zeige, dass dann
$$\frac{p+q}{2} = \lceil \sqrt{N} \rceil$$
gilt, und folgere, dass das Fermatsche Faktorisierungsverfahren gleich im ersten Schritt Erfolg hat.

Aufgabe 85: Zeige anhand nachfolgender Teilaufgaben, dass für eine Primzahl p
$$(p-1)! \equiv -1 \bmod p$$
gilt. Diese Aussage wird auch als Satz von Wilson bezeichnet. Im Folgenden kann man o.E. $p \geq 5$ annehmen.

1. Zu jedem $a \in S = \{1, 2, \ldots, p-2, p-1\}$ gibt es genau ein $i(a) \in S$ mit $a \cdot i(a) \equiv 1 \bmod p$. Insbesondere folgt $i(i(a)) = a$.
2. Genau dann gilt $i(a) = a$, wenn $a = 1$ oder $a = p - 1$ ist.

3. Es gibt $a_1, \ldots, a_{(p-3)/2} \in S$ mit
$$S = \{a_1, i(a_1), a_2, i(a_2), \ldots, a_{(p-3)/2}, i(a_{(p-3)/2}), 1, p-1\}.$$
Folgere daraus $\prod_{a \in S} a \equiv -1 \bmod p$ und damit die Behauptung.
4. Berechne für eine multiplikativ geschriebene endliche zyklische Gruppe G das Produkt $\prod_{g \in G} g$ und gib damit einen anderen Beweis für obige Behauptung.

Aufgabe 86: Definiere für natürliche Zahlen k und N
$$F(k, N) = \mathrm{ggT}(k! \bmod N, N).$$
1. Zeige, dass $F(k, N) = \mathrm{ggT}(k!, N)$ gilt.
2. Zeige, dass in der Primfaktorzerlegung von $F(k, N)$ genau die Primteiler von N vorkommen, die $\leq k$ sind, d.h.
$$p | \mathrm{ggT}(k! \bmod N, N) \quad \Longleftrightarrow \quad p \leq k \quad \text{und} \quad p | N.$$
3. Konstruiere unter der Annahme, dass $k! \bmod N$ schnell berechnet werden kann, einen schnellen Faktorisierungsalgorithmus.

Aufgabe 87: Seien $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $\ldots$, p_r die ersten r Primzahlen und $P = p_1 p_2 p_3 \ldots p_r$.
1. Definiere für $L \in \mathbf{N}$
$$\begin{aligned} S_L &= \{L, L+1, L+2, \ldots, L+(P-1)\}, \\ S_L^* &= \{N \in S : N \text{ hat einen Primteiler } \leq p_r\} = \{N \in S : \mathrm{ggT}(N, P) > 1\}, \end{aligned}$$
beweise, dass
$$\#S_L^* = P - \varphi(P)$$
gilt, und folgere
$$\frac{\#S_L^*}{\#S} = 1 - \prod_{i=1}^{r} (1 - \frac{1}{p_i}).$$
2. Zeige, dass für $T \in \mathbf{N}$ der Grenzwert
$$a(T) = \lim_{M \to \infty} \frac{1}{M} \#\{1 \leq N \leq M : N \text{ hat einen Primteiler } \leq T\}$$
existiert, und berechne seinen Wert.

Aufgabe 88: Bestimme die kleinste zusammengesetzte Zahl $N > 10^{10}$, für die $2^{N-1} \equiv 1 \bmod N$ gilt. (N ist dann eine Fermatsche Pseudoprimzahl zur Basis 2.)

Aufgabe 89: Sei p eine ungerade Primzahl und $N = p^2$.
1. Es gibt $p - 1$ Elemente a in $\{0, 1, 2, \ldots, N-1\}$, für die $a^{N-1} \equiv 1 \bmod N$ gilt. (N ist dann Fermatsche Pseudoprimzahl zur Basis a.)
2. Bestimme die kleinste Primzahl p mit
$$2^{N-1} \equiv 1 \bmod N.$$

Aufgabe 90: Sind für eine natürliche Zahl $u \geq 1$ die drei Zahlen

$$p_1 = 6u + 1, \quad p_2 = 12u + 1, \quad p_3 = 18u + 1$$

prim, so ist

$$N = p_1 p_2 p_3 = (6u + 1)(12u + 1)(18u + 1)$$

eine Carmichael-Zahl. (Hinweis: Zeige zunächst $p_i - 1 | n - 1$.)

Aufgabe 91: Zeige, dass es keine Carmichael-Zahl mit nur zwei Primteilern gibt.

Aufgabe 92: Beweise mit der $(p-1)$-Methode, dass $p = 2^{128} - 159$ eine Primzahl ist.

Aufgabe 93: Bestimme mindestens 17 Lösungen der Gleichung

$$x^3 - 3y^3 = 2^u \cdot 3^v \cdot 5^w$$

mit $x, y, u, v, w \in \mathbf{Z}$, $u, v, w \geq 0$ und $\mathrm{ggT}(x, y) = 1$.

Aufgabe 94: Sei $\Gamma \subseteq \mathbf{R}^2$ ein Gitter vom Rang 2. Zeige, dass ein $(\alpha_1, \alpha_2) \in \Gamma \setminus \{0\}$ existiert mit

$$|\alpha_1 \alpha_2| \leq \frac{1}{\sqrt{5}} \det \Gamma.$$

Aufgabe 95: Welche kubischen Zahlkörper K lassen sich schreiben als $K = \mathbf{Q}(\alpha)$ mit $a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0 = 0$, $a_i \in \mathbf{Z}$ und $|a_i| \leq 1$? Wieviele solcher Zahlkörper gibt es?

Literaturverzeichnis

[Beukers] F. Beukers, Lattice Reduction, in A. M. Cohen, H. Cuypers, H. Sterk (Eds.), Some Tapas of Computer Algebra, Springer 1999.

[BorewiczSafarevic] S. I. Borewicz, I. R. Šafarevič, Zahlentheorie, Birkhäuser 1966.

[CasselsFroehlich] J. W. S. Cassels, A. Fröhlich, Algebraic Number Theory, Academic Press 1967.

[Cohen] H. Cohen, A Course in Computational Algebraic Number Theory, Graduate Texts in Mathematics 138, Springer 1993.

[CohenCCFT] H. Cohen, Computational Class Field Theory.

[Cohn] H. Cohn, A Classical Invitation to Algebraic Numbers and Class Fields, Springer 1978.

[FroehlichTaylor] A. Fröhlich, M. J. Taylor, Algebraic number theory, Cambridge Studies in Advanced Mathematics 27, Cambridge University Press 1991.

[Hasse] H. Hasse, Number Theory, Springer 1980.

[KANT] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, K. Wildanger, KANT V4, J. Symbolic Comp. **24** (1997), 267–283.

[Koch] H. Koch, Algebraic Number Fields, Encyclopaedia of Mathematical Sciences, Volume 62, Springer 1992.

[LenstraLenstra] A. K. Lenstra, H. W. Lenstra, Jr. (Eds.), The development of the number field sieve, Lecture Notes in Mathematics 1554, Springer 1993.

[LangAlgebra] S. Lang, Algebra, 1993 (3. Auflage).

[Lang] S. Lang, Algebraic Number Theory, 1994 (2. Auflage).

[LangDA] S. Lang, Introduction to Diophantine Approximations, Addison-Wesley 1966.

[Marcus] D. A. Marcus, Number Fields, Springer 1977.

[Narkiewicz] Narkiewicz, W., Elementary and Analytic Theory of Algebraic Numbers, Springer-Verlag, PWN-Polish Scientific Publishers, Warszawa, 1990 (2. Auflage).

[Neukirch] J. Neukirch, Algebraische Zahlentheorie, Springer 1992.

[Pohst] M. E. Pohst, Computational Algebraic Number Theory, DMV Seminar, Band 21, Birkhäuser 1993.

[Serre] J.-P. Serre, Local Fields, Springer 1979.

Version vom 13.3.2003