Algebra und Zahlentheorie

Wolf P. Barth

Wintersemester 01/02, Sommersemester 02

Version vom 8. Juli 2002
Mathematisches Institut der Universität
Bismarckstr. 1 1/2, D - 91054 Erlangen

Inhaltsverzeichnis

0 Einführung

Unter 'Algebra' verstand man ursprünglich die Theorie des Auflösens von Polynomgleichungen in einer Unbekannten x. Lineare und quadratische Gleichungen

$$p \cdot x + q = 0, \quad x^2 + p \cdot x + q = 0,$$

waren schon den Ägyptern und Babyloniern bekannt. Mit kubischen Gleichungen

$$x^3 + p \cdot x^2 + q \cdot x + r = 0$$

beschäftigte man sich schon im antiken Griechenland. Die griechische Mathematik beeinflusste die indischen und arabischen Mathematiker, und diese schließlich die italienischen Mathematiker der Renaissance. Um 1550 fanden sie Lösungsformeln für Gleichungen dritten und vierten Grades. Seitdem war der Versuch, solche Formeln auch für Gleichungen vom Grad ≥ 5 anzugeben, eines der ganz großen offenen Probleme in der Mathematik. Die Lösung dieses Problems viel allerdings unerwartet negativ aus: Ruffini (1799) und Abel (1826) bewiesen, dass es i.a. unmöglch ist, eine Gleichung fünften oder höheren Grades durch (iteriertes) Wurzelziehen aufzulösen.

Die Argumente von Ruffini und Abel waren wohl nicht ganz vollständig. Ein wirkliches Verständnis für die Gründe der Nicht-Auflösbarkeit algebraischer Gleichungen hatte zuerst Galois ($\sim$ 1830). Der Grund besteht in Symmetrien zwischen den Lösungen. Der einfachste Fall ist die Formel

$$x_{1,2} = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}$$

für die beiden Lösungen einer quadratischen Gleichung. Die Symmetrie steckt hier in den beiden Vorzeichen der Wurzel. Vor allem wegen seines frühen tragischen Todes wurden die Argumente von Galois der mathematischen Öffentlichkeit erst um 1850 bekannt. Dann aber hatten sie gewaltige Konsequenzen: Die Untersuchung von Symmetrien führte zum Begriff der Gruppe (Cauchy 1844, Cayley 1854). Dieser Begriff führte zu radikaler Umgestaltung vieler mathematischer Gebiete. Vor allem Emmy Noether ($\sim$ 1920) veränderte die Algebra, die ursprünglich Gleichungen als Objekte hatte, zu einer Strukturtheorie. Mathematische Strukturen gewannen dann auch in vielen anderen Gebieten zentrale Bedeutung.

Die Strukturen der Algebra sind Gruppen, Ringe und Körper. Und in dieser Reihenfolge wollen wir sie in dieser Vorlesung auch behandeln. Diese Strukturen sind aus Inhalten entstanden und dienen dem Verständnis dieser Inhalte. Es handelt sich

bei	um die Struktur hinter der
Gruppen	Symmetrie
Ringen	Teilbarkeit
Körpern	Auflösbarkeit von Gleichungen

Bei der Ausarbeitung dieser Vorlesung habe ich aus den folgenden Büchern, z.T. hemmungslos, abgeschrieben:

- M. Artin: Algebra. Birkhäuser 1993

- N. Jacobson: Basic Algebra I. Freeman u. Co. 1985
- B.L v.d. Waerden: Algebra I. Springer 1960

Vor etwa zehn Jahren habe ich diese Vorlesung schon einmal (zum ersten Mal) gehalten. Weil ich kein strukturierter Algebraiker bin, ging das damals böse ins Auge. (Die Schwester eines Studenten aus dieser Vorlesung, die später bei mir ihre Diplomarbeit schrieb, meinte allerdings, ganz so schlimm sei es doch nicht empfunden worden.) Damals habe ich das Buch

- F. Lorenz: Einführung in die Algebra I. BI 1992

benutzt. Nochmal würde ich das nicht tun. Bei Studenten ziemlich beliebt ist das Buch

- K. Meyberg: Algebra, Teile 1 und 2. Hanser 1975/76

Diesmal halte ich diese Vorlesung, um Lehramts-Studenten optimal auf die schriftliche Algebra-Prüfung im Hauptexamen vorzubereiten. Deswegen sind die Aufgaben auch vor allem früheren Staatsexamen entnommen. Ich selbst habe auch mal - vor langer, langer Zeit - das bayerische Staatsexamen abglegt. Damals war der Algebra-Stoff fest umrissen: Van der Waerden bis Seite 200. Heutzutage ist das anscheinend nicht mehr so. Deswegen ist es schwierig den Stoff so zu strukturieren, dass alle wesentlichen Inhalte des Staatsexamens abgedeckt werden. Ich werde es versuchen.

Natürlich ist es auch Diplomern nicht verboten, diese Vorlesung zu hören.

1 Gruppen

1.1 Definitionen

Was eine Gruppe ist, muss man schon in der Anfängervorlesung 'Lineare Algebra' lernen, weil man ohne diesen Begriff einfach nicht auskommt.

Definition 1.1 *Eine* Gruppe *ist eine Menge G zusammen mit einer Verknüpfung*

$$G \times G \ni (g,h) \mapsto gh \in G.$$

Für diese Verknüpfung gelten folgende Eigenschaften:
Assoziativität: $(gh)k = g(hk)$.
Existenz der Eins: Es gibt ein Element $e \in G$ mit $eg = ge = g$ für alle $g \in G$.
Existenz des Inversen: Zu jedem $g \in G$ gibt es ein $g^{-1} \in G$ mit $gg^{-1} = g^{-1}g = e$.

Beispiel 1.1 *Die folgenden Mengen mit den angegebenen Verknüpfungen sind Gruppen: $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{Q}^*,\cdot)$, $(\mathbb{R}^*,\cdot)$. Diese Beispiele sind ebenso fundamental wie trivial. Nicht ganz so trivial sind folgende Beispiele:*

Die Permutationsgruppe S_n: Sie besteht aus allen bijektiven Abbildungen der Menge $\{1,...,n\}$ auf sich. Die Verknüpfung ist die Hintereinanderausführung:

$$(\sigma\tau)(k) = \sigma(\tau(k)), \quad k = 1,...,n.$$

Die Matrizengruppe $GL(n,\mathbb{R})$: Sie besteht aus allen invertierbaren $n \times n$-Matrizen mit reellen Einträgen. Die Gruppe $GL(n,\mathbb{R})$ hat viele interessante Untergruppen, wie etwa

$SL(n,\mathbb{R})$	*Matrizen mit der Determinante 1,*
$O(n)$	*orthogonale $n \times n$-Matrizen,*
$\Delta(n)$	*invertierbare obere Dreiecksmatrizen.*

Es gibt auch Gruppen ganzzahliger Matrizen: Die Gruppe $SL(n,\mathbb{Z})$ besteht aus allen $n \times n$-Matrizen, deren Einträge ganze Zahlen sind, und deren Determinante $= 1$ ist. Dazu gehört die Einheitsmatrix, und mit je zwei Matrizen gehört auch deren Matrizenprodukt dazu. Nicht-trivial ist, dass für jede dieser Matrizen auch die inverse Matrix ganzzahlig ist. Das folgt aus der Formel

$$A^{-1} = \frac{1}{det(A)} \cdot \Big((-1)^{i+j} det(A_{j,i})\Big)_{i,j}.$$

Dabei ist $A_{i,j}$ die (i,j)-Streichungsmatrix von A, und deren Determinante ist wieder ganzzahlig.

Hat man zwei Gruppen G und H, so ist deren kartesisches Produkt

$$G \times H = \{(g,h) : g \in G, h \in H\}$$

wieder eine Gruppe. Man definiert die Verknüpfung komponentenweise

$$(g_1,h_1)(g_2,h_2) = (g_1g_2, h_1h_2).$$

Dann ist (e_G, e_H) das Eins-Element in $G \times H$ und das Inverse zu (g,h) ist $(g,h)^{-1} = (g^{-1},h^{-1})$. Man nennt die so definierte Gruppe $G \times H$ das direkte Produkt *oder auch* direkte Summe *der Gruppen G und H.*

Eine sehr häufig vorkommende Gruppe wird $\mathbb{Z}_n$ sein, die Gruppe der ganzen Zahlen modulo n. Dabei ist $n > 1$ eine natürliche Zahl. Die Elemente von $\mathbb{Z}_n$ sind die natürlichen Zahlen $0, 1, 2, ..., n-1$. Und die Verknüpfung ist Addition modulo n:

$$0 \leq k, l < n: \quad k + l \bmod n := \begin{cases} k + l & \text{falls } k + l < n \\ k + l - n & \text{falls } k + l \geq n. \end{cases}$$

Das Eins-Element ist natürlich $e = 0$ und das Inverse zu k ist $n - k$.

Beispiel 1.2 *Die* Kleinsche Vierergruppe *V_4 ist das direkte Produkt $\mathbb{Z}_2 \times \mathbb{Z}_2$. Wenn wir die beiden Elemente in $\mathbb{Z}_2$ mit 0 und 1 bezeichnen, so besteht die Gruppe V_4 also aus den Elementen*

$$(0,0),\ (0,1),\ (1,0),\ (1,1).$$

Satz 1.1 *a) In einer Gruppe G gibt es nur ein einziges Eins-Element.*

b) Zu einem Gruppenelement g gibt es nur ein einziges Inverses g^{-1}.

c) (Kürzungsregel) Sind $g, g_1, g_2 \in G$ Gruppenelemente mit $gg_1 = gg_2$, so folgt $g_1 = g_2$. Ebenso folgt $g_1 = g_2$ aus $g_1 g = g_2 g$.

Beweis. a) Es seien e und $e' \in G$ zwei Eins-Elemente. Dann folgt

$$\begin{aligned} e &= ee' \quad (e' \text{ Eins-Element}) \\ &= e' \quad (e \text{ Eins-Element}). \end{aligned}$$

b) Aus $gg_1 = e = g_1 g$ und $gg_2 = e = g_2 g$ folgt

$$g_1 = (g_1 g)g_1 = (g_2 g)g_1 = g_2(gg_1) = g_2.$$

c) Aus der Gleichung $gg_1 = gg_2$ folgt durch Links-Multiplikation mit g^{-1} dass $g_1 = g_2$ ist. Analog folgt $g_1 = g_2$ aus der Gleichung $g_1 g = g_2 g$ durch Rechts-Multiplikation mit g^{-1}. □

Oben haben wir vorausgegriffen und den Begriff der Untergruppe benutzt:

Definition 1.2 *Eine Teilmenge $H \subset G$ der Gruppe G heißt Untergruppe, wenn sie mit der Verknüpfung aus G selbst eine Gruppe ist. Das bedeutet:*

$e_G \in H$,

$h_1, h_2 \in H \quad \Rightarrow \quad h_1 h_2 \in H$,

$h \in H \quad \Rightarrow \quad h^{-1} \in H$.

In manchen, aber nur in den allerwenigsten Gruppen gilt

$$gh = hg \text{ für alle } g, h \in G.$$

Dann nennt man die Gruppe *kommutativ* oder *abelsch*. Die Permutationsgruppen S_n, $n \geq 3$, und die meisten Matrizengruppen sind nicht abelsch.

Beispiel 1.3 *Die* Quaternionengruppe H *besteht aus acht Elementen, die man*

$$\pm 1,\ \pm i, \pm j,\ \pm k$$

schreibt. Das neutrale Element ist $+1$*. Das Element* -1 *multipliziert jedes Element aus* $h \in H$ *auf* $-h$*. Die Gruppenstruktur auf* H *wird festgelegt durch*

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j.$$

Die Gruppe heißt Quaternionengruppe, weil sie mit den Hamiltonschen Quaternionen zu tun hat. Sie ist nicht abelsch.

Viele Gruppen, vor allem die abelschen, sind langweilig. Von Interesse sind sie oft nur wegen zusätzlicher Strukturen. (Das gilt in besonderem Maß für die Vektorräume aus der linearen Algebra.) Interessant sind Gruppen, die *Symmetrien* darstellen. Das machen wir jetzt exakt:

Definition 1.3 *Es sei* G *eine Gruppe und* M *eine Menge. Eine* Operation *von* G *auf* M *ist eine Abbildung*

$$G \times M \ni (g, m) \mapsto g(m) \in M$$

mit den Eigenschaften

$$e(m) = m \text{ für das Eins-Element } e \in G \text{ und alle } m \in M,$$

sowie

$$(gh)(m) = g(h(m)) \text{ für alle } g, h \in G \text{ und } m \in M.$$

Beispiel 1.4 *Die Permutationsgruppe* S_n *operiert auf der Menge* $\{1, 2, ..., n\}$*. Die Matrizengruppe* $GL(n, \mathbb{R})$ *operiert auf dem Vektorraum* $\mathbb{R}^n$*. Jede Gruppe operiert auf sich selbst durch* Links-Multiplikation:

$$g(m) := gm \text{ für } g \in G,\ m \in G.$$

Die Bedingung

$$(gh)(m) = g(h(m))$$

ist gerade die Assoziativität in der Gruppe. Es gibt aber auch eine Rechts-Multiplikation *von* G *auf sich: Das ist*

$$g(m) := mg.$$

In diesem Fall ist aber i.a.

$$(gh)(m) = mgh \neq mhg = g(h(m)).$$

Aus der Rechts-Multiplikation kann man allerdings eine Gruppenoperation machen, wenn man definiert:

$$g(m) := mg^{-1}.$$

Dann gilt nämlich

$$(gh)(m) = m(gh)^{-1} = mh^{-1}g^{-1} = g(h(m)).$$

Operiert die Gruppe G auf der Menge M, so definiert jedes Element $m \in M$ eine Untergruppe $G_m \subset G$:

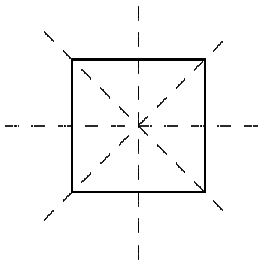
$$G_m := \{g \in G : g(m) = m\}.$$

Dies ist tatsächlich eine Untergruppe: $e \in G_m$ wegen $e(m) = m$, $g, h \in G_m \Rightarrow g(m) = h(m) = m \Rightarrow (gh)(m) = g(h(m)) = g(m) = m \Rightarrow gh \in G_m$ und $g \in G_m \Rightarrow g^{-1}(m) = g^{-1}(g(m)) = (g^{-1}g)(m) = e(m) = m$. Die soeben definierte Untergruppe G_m heißt die *Standgruppe* oder *Isotropie-Gruppe* oder *Stabilisator* des Elementes m.

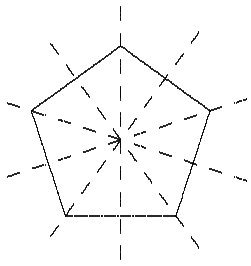
Beispiel 1.5 *Die Standgruppe der Zahl n unter der Operation von S_n auf der Menge $\{1, ..., n\}$ ist die Menge der Permutationen $\sigma \in S_n$, die die Zahl n fest lassen. Diese Permutationen permutieren nur die Zahlen $1, ..., n-1$ und bilden eine Untergruppe $S_{n-1} \subset S_n$.*

Interessante Gruppen-Operationen verkörpern Symmetrien geometrischer Objekte. Betrachten wir etwa ein reguläres n-Eck. Da gibt es n Drehungen um das Zentrum des n-Ecks, welche diese Figur in sich überführen. Das sind aber noch nicht alle Symmetrien des regulären n-Ecks: Jede Ecke liegt auf einer Geraden durch das Zentrum, und die Spiegelung an dieser Geraden ist auch eine Symmetrie der Figur. Aber schon wird das Leben kompliziert: Nur wenn n ungerade ist, erhalten wir so die volle Symmetriegruppe. Sie besteht aus n Drehungen und n Spiegelungen, insgesamt aus $2n$ Symmetrien. Wenn n jedoch gerade ist, liegen immer zwei Ecken gegenüber auf der Spiegelungs-Gerade. Wir bekommen so nur $n/2$ Spiegelungen. Nocheinmal $n/2$ Spiegelungen bekommen wir, wenn wir Spiegel-Geraden nehmen, die die Mittelpunkte gegenüber liegender Seiten verbinden. So kommen wir dann auch hier auf eine Gruppe aus n Drehungen und n Spiegelungen. Diese Symmetrie-Gruppe des regulären n-Ecks heißt *Dieder-Gruppe* D_n.

Spiegelungsachsen des regulären



Vierecks



Fünfecks

Definition 1.4 *Eine Operation der Gruppe G auf der Menge M heißt* transitiv, *falls zu je zwei Elementen $m_1, m_2 \in M$ ein Gruppenelement $g \in G$ existiert mit $g(m_1) = m_2$. Ist die Operation nicht transitiv, so heißt sie* intransitiv.

Beispiel 1.6 *Die Operation der symmetrischen Gruppe S_n auf der Menge $\{1, ..., n\}$ ist transitiv: Zu je zwei Zahlen n_1, n_2 gibt es die Transposition $(n_1, n_2) \in S_n$, welche diese beiden Zahlen vertauscht. Die oben angegebene Untergruppe $S_{n-1} \subset S_n$, die Standgruppe der Zahl n operiert allerdings nicht transitiv auf der Menge $\{1, ..., n\}$, denn es gibt kein Element in S_{n-1}, welches die Zahl n auf irgend eine andere Zahl abbildet.*

Ist die Operation nicht transitiv, dann bildet G jedes Element $m \in M$ nur auf Elemente einer echten Teilmenge von M ab. Solche Teilmengen $G \cdot m = \{g(m) : g \in G\}$ heißen *Bahnen* von G auf M. Diese Bahnen bilden eine disjunkte Zerlegung von $M = \cup M_i$ in Teilmengen M_i, auf denen G transitiv operiert.

Definition 1.5 *Enthält die Gruppe G nur endlich viele Elemente, so heißt die Anzahl dieser Elemente die* Ordnung $|G|$ *der Gruppe G.*

Satz 1.2 (Bahnensatz) *Die endliche Gruppe G operiere transitiv auf der Menge M. Dann gilt für die Ordnung der Gruppe G, die Ordnung $|G_m|$ einer jeden Standgruppe $G_m \subset G$, und die Anzahl der $|M|$ Elemente von M:*

$$|G| = |G_m| \cdot |M|.$$

Beweis. Wir fixieren ein Element $m_0 \in M$ und betrachten die Abbildung

$$G \to M, \quad g \mapsto g(m_0).$$

Diese Abbildung ist surjektiv wegen der Transitivität der Operation. Insbesondere ist deswegen $|M|$ auch endlich. Zu jedem Element $m \in M$ gibt es die Teilmenge

$$U_m := \{g \in G : g(m_0) = m\}.$$

Wegen der Transitivität der Operation ist U_m, $m \in M$, nie leer. Für $m_1 \neq m_2 \in M$ gilt $U_{m_1} \cap U_{m_2} = \emptyset$. Jedes Element in $U_{m_1} \cap U_{m_2}$ würde nämlich m sowohl auf m_1 als auch auf $m_2 \neq m_1$ abbilden, das geht nicht. So erhalten wir eine Zerlegung

$$G = \bigcup_{m \in M} U_m$$

in disjunkte Teilmengen U_m. Für die Anzahlen $|U_m|$ von Elementen in den Teilmengen U_m folgt daraus

$$\sum_{m \in M} |U_m| = |G|.$$

Die Behauptung ergibt sich, wenn wir zeigen:

$$|U_m| = |G_{m_0}| \text{ für alle } m \in M.$$

Sei ein $m \in M$ fest gehalten und $g \in U_m$ ein Gruppenelement mit $g(m_0) = m$. Für alle $h \in G_{m_0}$ gilt dann auch

$$(gh)(m_0) = g(h(m_0)) = g(m_0) = m.$$

Die Menge

$$g \cdot G_{m_0} = \{gh : h \in G_{m_0}\}$$

ist also eine Teilmenge von U_m. Wenn h die Elemente von G_{m_0} durchläuft, erhalten wir so lauter verschiedene Elemente von U_m. Deren Anzahl ist aber $= |G_{m_0}|$. Die Behauptung folgt, wenn wir zeigen: $U_m = g \cdot G_{m_0}$. Sei dazu $u \in U_m$, also $u(m_0) = m = g(m_0)$. Wegen

$$(g^{-1}u)(m_0) = g^{-1}(u(m_0)) = g^{-1}(m) = m_0$$

ist $h := g^{-1}u \in G_{m_0}$, also $u = g \cdot h \in g \cdot G_{m_0}$. □

Satz 1.3 (von Lagrange) *Es sei $H \subset G$ eine Untergruppe der endlichen Gruppe G. Dann teilt die Ordnung $|H|$ von H die Ordnung $|G|$ der Gruppe G.*

Beweis. Zu jedem Gruppen-Element $g \in G$ betrachten wir die Links-Nebenklasse

$$g \cdot H = \{g \cdot h : h \in H\}.$$

Wenn sich zwei solche Nebenklassen, etwa g_1H und g_2H schneiden, dann gilt $g_1h_1 = g_2h_2$ mit $h_1, h_2 \in H$. Es folgt $g_2 = g_1h_1h_2^{-1} \in g_1H$ und $g_2H = g_1H$. Weil jedes Element $g = ge \in gH$ in seiner eigenen Nebenklasse liegt, ist die Vereinigung der Nebenklassen die ganze Gruppe. Und wie wir eben sahen, ist diese Vereinignung eine disjunkte Vereinigung.

Die Anzahl $|gH|$ der Elemente in einer Nebenklasse gH ist immer gleich der Gruppenordnung $|H|$. Ist k die Anzahl der Nebenklassen, so ist also $|G| = k \cdot |H|$. □

Definition 1.6 (Index) *Es sei H eine Untergruppe der endlichen Gruppe G. Dann heißt die (nach Lagrange ganze) Zahl*

$$[G : H] := |G|/|H|$$

der Index von H in G.

Aufgabe 1.1 *Es sei $(i_1, ..., i_k) \in S_n$ ein Zyklus. Zeigen Sie für alle $\sigma \in S_n$:*

$$\sigma(i_1, ..., i_k)\sigma^{-1} = (\sigma(i_1), ..., \sigma(i_k)).$$

Aufgabe 1.2 (H 98, T 3, Aufg 1) *a) Geben Sie eine Untergruppe der Ordnung 20 in der symmetrischen Gruppe S_5 an.*

b) Gibt es Untergruppen der Ordnung 20 in A_5?

Aufgabe 1.3 (F 94, T1, A1a)) *Es sei $\xi \in S_n$ ein Zykel der Länge n. Bestimmen Sie alle $\pi \in S_n$, die mit ξ vertauschbar sind.*

Aufgabe 1.4 (H 93, T1, Teil von A3) *Sei $(G, +)$ eine endliche abelsche Gruppe mit neutralem Element 0 und $G_2 = \{x \in G : 2x = 0\}$. Man setzt*

$$\sigma(G) := \sum_{x \in G} x.$$

Zeigen Sie:

i) G_2 ist eine Untergruppe von G, und es ist $\sigma(G) = \sigma(G_2)$. Hinweis: Betrachten Sie auf G die Äquivalenzrelation $x \sim y \Leftrightarrow x = y$ oder $x = -y$, $(x, y \in G)$.

ii) Ist $\#G_2 \neq 2$, so ist $\sigma(G) = 0$; ist $\#G_2 = 2$, so ist $\sigma(G)$ das von 0 verschiedene Element aus G_2.

Aufgabe 1.5 (F 92, T1, A1) *Eine Gruppe der Ordnung 55 operiere auf einer Menge M mit 18 Elementen. Zeigen Sie, dass die Gruppe auf M mindestens 2 Fixpunkte hat.*

1.2 Homomorphismen und Normalteiler

Definition 1.7 *G und H seien Gruppen, $\varphi : G \to H$ eine Abbildung. Die Abbildung φ heißt* (Gruppen)-Homomorphismus*, oder einfach Morphismus, falls für alle $g_1, g_2 \in G$ gilt*

$$\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2).$$

Beispiel 1.7 *Ist $G \subset H$ eine Untergruppe, so ist die Inklusion $G \to H$, bei der jedes Element aus G auf dieses gleiche Element, aufgefasst als in H liegend, abgebildet wird, ein Morphismus.*

Die Determinante $det : GL(n, \mathbb{R}) \to \mathbb{R}^*$ ist ein Morphismus von Gruppen. Dabei verstehen wir unter $\mathbb{R}^*$ die Gruppe der reellen Zahlen $\neq 0$ mit der Multiplikation als Verknüpfung. Dass diese Abbildung $A \mapsto det(A)$ ein Homomorphismus ist, das ist gerade die Aussage des Determinanten-Multiplikations-Satzes.

Die Exponentialfunktion $exp : (\mathbb{R}, +) \to (\mathbb{R}^*, \cdot)$ ist auch ein Morphismus wegen der Funktionalgleichung $exp(r + s) = exp(r) \cdot exp(s)$.

Auch die Signum-Funktion $sign : S_n \to \{\pm 1\}$ ist ein Homomorphismus. Dabei muss man die Menge $\{\pm 1\}$ mit der Multiplikation zu einer Gruppe machen.

Wie üblich nennt man einen Morphismus *Monomorphismus*, wenn er injektiv ist, und *Epimorphismus*, wenn er surjektiv ist. Ein bijektiver Morphismus heißt *Isomorphismus*. Hierzu ein Beispiel:

Satz 1.4 (von Cayley) *Jede endliche Gruppe ist isomorph zu einer Untergruppe einer symmetrischen Gruppe S_n für ein geeignetes $n \in \mathbb{N}$.*

Beweis. Es sei $n = |G|$ die Ordnung der Gruppe G. Wir ordnen die Elemente von G irgenwie an, etwa $G = \{g_1, ..., g_n\}$. Die Links-Translation von G auf sich selbst

$$G \ni g : h \mapsto g \cdot h, \text{ bzw } g_\nu \mapsto g \cdot g_\nu = g_{\nu'}$$

bewirkt eine Abbildung $\sigma_g : \nu \mapsto \nu'$ der Indexmenge $\{1, ..., n\}$ auf sich selbst. Jedem Gruppenelement $g \in G$ wird so eine Permutation σ_g der Zahlen $1, ..., n$ zugeordnet und wir erhalten so eine Abbildung $G \to S_n$.

Aus der Assoziativität $(gg')h = g(g'h)$ folgt $\sigma_{gg'} = \sigma_g \sigma_{g'}$, d.h., die Abbildung $G \to S_n$, $g \mapsto \sigma_g$, ist ein Gruppenhomomorphismus. Dieser ist injektiv. Denn aus $\sigma_g = \sigma_{g'}$ folgt insbesondere $g \cdot e = g' \cdot e$ und $g = g'$. Also ist dieser Homomorphismus ein Isomorphismus von G auf eine Untergruppe der symmetrischen Gruppe S_n □

Dieser sogenannte Satz von Cayley ist relativ banal, vom modernen Standpunkt aus geradezu trivial. Das sagt aber nichts darüber, wie wichtig Cayley für die Entwicklung der Gruppentheorie war: Vor Cayley betrachtete man nur Untergruppen der symmetrischen Gruppe S_n. Cayley war der erste, der Gruppen ganz losgelöst von Permutationen untersuchte.

Satz 1.5 (Homomorphismen) *Für jeden Gruppen-Homomorphismus $\varphi : G \to H$ gilt:*

a) $\varphi(e_G) = e_H$;

b) $\varphi(g^{-1}) = \varphi(g)^{-1}$;

c) Die Menge

$$Kern(\varphi) := \{g \in G : \varphi(g) = e_H\} \subset G$$

ist eine Untergruppe von G. Der Morphismus φ ist genau dann injektiv, wenn $Kern(\varphi) = \{e_G\}$.

d) Die Menge

$$Bild(\varphi) := \{h \in H : h = \varphi(g) \text{ für ein } g \in G\} \subset H$$

ist eine Untergruppe von H. Der Morphismus φ ist genau dann surjektiv, wenn $Bild(\varphi) = H$.

e) Ist $U \subset H$ eine Untergruppe von H, so ist

$$\varphi^{-1}(U) := \{g \in G : \varphi(g) \in U\}$$

eine Untergruppe von G, das Urbild *der Untergruppe U*

Hier bezeichnt e_G das Eins-Element in G und e_H das Eins-Element der Gruppe H.

Beweis. a) Für jedes $g \in G$ ist

$$\varphi(g) = \varphi(e_G g) = \varphi(e_G)\varphi(g).$$

Multipliziert man diese Gleichung von rechts mit $\varphi(g)^{-1}$, so folgt

$$e_H = \varphi(g)\varphi(g)^{-1} = \varphi(e_G)\varphi(g)\varphi(g)^{-1} = \varphi(e_G).$$

b) Für jedes $g \in G$ ist

$$\varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(e_G) = e_H.$$

Also ist $\varphi(g^{-1}) = \varphi(g)^{-1}$.

c) Wegen $\varphi(e_G) = e_H$ ist e_G ein Element im Kern. Für $g_1, g_2 \in Kern(\varphi)$ gilt $\varphi(g_1) = \varphi(g_2) = e_H$ und deswegen $\varphi(g_1)\varphi(g_2) = e_H$, also gehört auch $g_1 g_2$ zum Kern. Falls $g \in Kern(\varphi)$, so ist

$$\varphi(g^{-1}) = \varphi(g)^{-1} = e_H^{-1} = e_H,$$

also gehört auch g^{-1} zu $Kern(\varphi)$.

Wenn φ injektiv ist, dann kann außer e_G kein anderes Element $g \in G$ auf e_H abgebildet werden. Es folgt $Kern(\varphi) = \{e_G\}$. Sei umgekehrt $Kern(\varphi) = \{e_G\}$ vorausgesetzt. Falls für zwei Elemente $g_1, g_2 \in G$ gilt, dass $\varphi(g_1) = \varphi(g_2)$ ist, dann folgt

$$\varphi(g_1 g_2^{-1}) = \varphi(g_1)\varphi(g_2)^{-1} = e_H$$

und $g_1 g_2^{-1}$ gehört zu $Kern(\varphi)$. Also ist $g_1 g_2^{-1} = e_G$ und $g_1 = g_2$. Damit ist φ injektiv.

d) Wegen $e_H = \varphi(e_G)$ gehört e_H zu $Bild(\varphi)$. Mit $h_1 = \varphi(g_1)$ und $h_2 = \varphi(g_2) \in Bild(\varphi)$ gehört auch $h_1 h_2 = \varphi(g_1 g_2)$ zu $Bild(\varphi)$. Mit $h = \varphi(g) \in Bild(\varphi)$ gehört auch $h^{-1} = \varphi(g^{-1})$ zu $Bild(\varphi)$.

e) Wegen $\varphi(e_G) = e_H \in U$ gehört e_G zu $\varphi^{-1}(U)$. Sind $g_1, g_2 \in \varphi^{-1}(U)$, so gilt $\varphi(g_1) \in U$ und $\varphi(g_2) \in U$, also $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) \in U$. Es folgt $g_1 g_2 \in \varphi^{-1}(U)$. Schließlich gehört mit $g \in \varphi^{-1}(U)$ auch immer g^{-1} zu $\varphi^{-1}(U)$, denn $\varphi(g^{-1}) = \varphi(g)^{-1} \in U$. □

Zu einem Morphismus $\varphi : G \to H$ gehören also zwei Untergruppen: $Kern(\varphi) \subset G$ und $Bild(\varphi) \subset H$. Es ist klar, dass jede Untergruppe $U \subset H$ als Bild eines Morphismus auftritt, mämlich z.B. als Bild der Inklusion $U \subset H$. Aber als Kern eines Morphismus kann keineswegs jede Untergruppe von G auftreten. Ein Kern hat folgende besondere Eigenschaft:

Satz 1.6 *Ist $u \in G$ eine Element im Kern des Morphismus $\varphi : G \to H$, so ist für jedes $g \in G$ auch*

$$g \cdot u \cdot g^{-1}$$

wieder ein Element in $Kern(\varphi)$.

Beweis. $\varphi(gug^{-1}) = \varphi(g)\varphi(u)\varphi(g^{-1}) = \varphi(g)e_H\,\varphi(g)^{-1} = e_H$. □

Die soeben notierte Eigenschaft ist so wichtig, dass Untergruppen mit dieser Eigenschaft einen eigenen Namen bekommen:

Definition 1.8 *Eine Untergruppe $U \subset G$ heißt* Normalteiler *oder* normale Untergruppe *von G, wenn für alle $u \in U$ und $g \in G$ gilt: $g \cdot u \cdot g^{-1} \in U$.*

Beispiel 1.8 *Falls G abelsch ist, dann ist jede Untergruppe $U \subset G$ ein Normalteiler, denn dann gilt $gug^{-1} = gg^{-1}u = u \in U$.*

Sei etwa D_3 die Dieder-Gruppe der Ordnung 6, realisiert als Permutationsgruppe S_3 mit den beiden Dreierzyklen $(1,2,3), (1,3,2)$ (Rotationen) und den drei Zweierzyklen $(1,2), (1,3), (2,3)$ (Spiegelungen). Dann ist die Untergruppe

$$A_3 = \{id, (1,2,3), (1,3,2)\}$$

ein Normalteiler, denn sie ist der Kern des signum-Morphismus. Aber die Untergruppe

$$U := \{id, (1,2)\}$$

der Ordnung zwei ist kein Normalteiler:

$$(1,2,3)(1,2)(1,2,3)^{-1} = (1,2,3)(1,2)(1,3,2) = (1,2,3)(1,3) = (2,3) \notin U.$$

Wir wollen Normalteiler noch etwas formaler betrachten:

Definition 1.9 *Es sei G eine Gruppe und ein Element $g \in G$ werde festgehalten. Dann ist die Abbildung*

$$G \ni h \mapsto ghg^{-1} \in G$$

ein Gruppen-Isomorphismus $G \to G$. Er heißt die Konjugation *unter g.*

Dass die Konjugation ein Morphismus ist, das folgt aus

$$g \cdot (h_1h_2) \cdot g^{-1} = (gh_1g^{-1}) \cdot (gh_2g^{-1}).$$

Die Konjugation mit g^{-1}, $h \mapsto g^{-1}hg$, ist die Umkehr-Abbildung, denn

$$g^{-1} \cdot (ghg^{-1}) \cdot g = h.$$

also ist die Konjugationsabbildung bijektiv.

Definition 1.10 *Jeden Gruppen-Isomorphismus $G \to G$ nennt man einen* Automorphismus *von G. Die Konjugations-Automorphismen nennt man* innere *Automorphismen von G.*

Die Normalteiler-Eigenschaft der Untergruppe $U \subset G$ kann man so formulieren: Für jedes $g \in G$ ist

$$g \cdot U \cdot g^{-1} := \{gug^{-1}, u \in U\}$$

in U enthalten: $gUg^{-1} \subset U$. Weil aber auch

$$U = g \cdot (g^{-1}Ug) \cdot g^{-1} \subset g \cdot U \cdot g^{-1}$$

ist, folgt daraus sogar: $gUg^{-1} = U$.

Die Normalteiler-Eigenschaft hat Konsequenzen für Nebenklassen:

Definition 1.11 (Nebenklassen) *Sei $U \subset G$ eine Untergruppe und $g \in G$. Dann heißt die Menge*

$$gU := \{gu : u \in U\}$$

eine Links-Nebenklasse zu U und

$$Ug := \{ug : u \in U\}$$

eine Rechts-Nebenklasse zu U.

Im Allgemeinen sind Links- und Rechts-Nebenklassen verschieden: Sei etwa $U \subset S_3$ die Untergruppe $\{id, (1,2)\}$ und $g := (1,2,3)$. Dann ist

$$gU = \{(1,2,3), (1,2,3)(1,2)\} = \{(1,2,3), (1,3)\}$$

und

$$Ug = \{(1,2,3), (1,2)(1,2,3)\} = \{(1,2,3), (2,3)\},$$

die Nebenklassen sind voneinander verschieden.

Satz 1.7 *Eine Untergruppe $U \subset G$ ist genau dann ein Normalteiler, wenn für alle $g \in G$ gilt*

$$gU = Ug.$$

Links- und Rechts-Nebenklassen stimmen überein.

Beweis. Die Untergruppe U ist genau dann Normalteiler, wenn für alle $g \in G$

$$U = gUg^{-1} = \{gug^{-1}, u \in U\}.$$

Multipliziert man diese Mengen-Gleichung von rechts mit g, so findet man

$$Ug = (gUg^{-1})g = gU.$$

□

Ist $U \subset G$ eine Untergruppe, so bezeichnet man mit $G/U = \{gU : g \in G\}$ die Menge der Links-Nebenklassen und mit $U \setminus G = \{Ug : g \in G\}$ die Menge der Rechts-Nebenklassen.

Bei Vektorräumen kann man Nebenklassen zu einem Untervektorraum addieren und damit den Quotienten-Vektorrraum definieren. Bei Gruppen funktioniert diese Konstruktion nur bei Normalteilern. Das wollen wir jetzt durchführen. Sei also $U \subset G$ ein Normalteiler in der Gruppe G.

Seien $g_1, g_2 \in G$ zwei Gruppenelemente mit ihren Nebenklassen g_1U und g_2U. Wir bezeichnen mit $g_1U \cdot g_2U$ die Menge der Produkte aus Elementen beider Nebenklassen:

$$g_1U \cdot g_2U = \{g_1u_1 \cdot g_2u_2 : \ u_1, u_2 \in U\}.$$

Dann gilt aber wegen der Normalteiler-Eigenschaft:

$$g_1U \cdot g_2U = g_1 \cdot g_2Ug_2^{-1} \cdot g_2U = g_1g_2U \cdot U = g_1g_2U.$$

Das soeben definierte Produkt der Nebenklassen zu g_1 und g_2 ist wieder eine Nebenklasse, und zwar die Nebenklasse zum Produkt g_1g_2. Damit definieren wir auf der Nebenklassen-Menge $G/U = U \setminus G$ eine Verknüpfung:

Sind g_1U und $g_2U \in G/U$ Nebenklassen, so heißt

$$g_1U \cdot g_2U = (g_1g_2)U$$

ihr Produkt.

Satz 1.8 (Faktorgruppe) *Es sei $U \subset G$ ein Normalteiler.*

a) Das Produkt $g_1U \cdot g_2U$ ist wohldefiniert. D.h., das Produkt hängt nur von den Nebenklassen, und nicht von den gewählten Repräsentanten g_1 und g_2 ab.

b) Das so definierte Produkt ist assoziativ.

c) Die Menge G/U, versehen mit diesem Produkt ist wieder eine Gruppe. Ihr neutrales Element ist die Nebenklasse $eU = U$. Das Inverse der Nebenklasse gU ist die Nebenklasse $g^{-1}U$.

d) Die Abbildung

$$G \to G/U, \quad g \mapsto gU$$

ist ein surjektiver Gruppen-Homorphismus mit Kern U.

Beweis. Seien $g_1U = h_1U$ und $g_2U = h_2U$. Dann bedeutet das $h_1 = g_1u_1$ und $h_2 = g_2u_2$ mit $u_1, u_2 \in U$. Daraus folgt

$$h_1U \cdot h_2U = g_1u_1U \cdot g_2u_2U = g_1U \cdot g_2U.$$

Die Eigenschaften b) und c) folgen aus den entsprechenden Eigenschaften der Gruppe G und $g_1U \cdot g_2U = g_1g_2 \cdot U$. Aus dieser Gleichung folgt auch, dass die Nebenklassen-Abbildung $g \mapsto gU$ ein Gruppen-Homomorphismus $G \to G/U$ ist. Wegen $uU = U$ für alle $u \in U$ ist der Normalteiler im Kern dieses Morphismus enthalten. Ist umgekehrt g ein Element im Kern, dann bedeutet das $gU = U$ und $g \in U$. Also stimmt der Kern mit dem Normalteiler überein.

Definition 1.12 (Nebenklassengruppe, Faktorgruppe) *Die soeben definierte Gruppe G/U zum Normalteiler $U \subset G$ heißt* Nebenklassengruppe *zu U oder* Quotienten-, *bzw.* Faktorgruppe *nach U.*

Beispiel 1.9 *Für jedes $1 < n \in \mathbb{Z}$ ist*

$$\mathbb{Z} \cdot n := \{k \cdot n : k \in \mathbb{Z}\}$$

eine Untergruppe von $\mathbb{Z}$. Weil $\mathbb{Z}$ abelsch ist, ist diese Untergruppe ein Normalteiler und die Restklassengruppe $\mathbb{Z}/\mathbb{Z} \cdot n$ ist nach Satz 1.8 wohldefiniert. Die Abbildung

$$\mathbb{Z}/\mathbb{Z} \cdot n \to \mathbb{Z}_n, \quad k \mapsto m \text{ falls } k = q \cdot n + m,\ k \in \mathbb{Z}, 0 \leq m < n,$$

Ist ein Gruppen-Isomorphismus. Anstatt der Restklassen-Notation $k + \mathbb{Z} \cdot n$ für Elemente aus $\mathbb{Z}/\mathbb{Z} \cdot n = \mathbb{Z}_n$ werden wir die Notation $k \bmod n$ verwenden.

Satz 1.9 (Erster Homomorphiesatz) *Es sei $\varphi : G \to H$ ein Gruppen-Homomorphismus mit Kern $K \subset G$ und Bild $B \subset H$. Dann gibt es einen Gruppen-Isomorphismus $\psi : B \to G/K$ derart, dass das Diagramm*

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & B \\ & \searrow & \downarrow \psi \\ & & G/K \end{array}$$

kommutiert. Dabei ist $G \to G/K$ der Restklassen-Homomorphismus.

Beweis. Es sei $b = \varphi(g) \in B$ ein Element im Bild. Wir definieren $\psi(b) := gK \in G/K$. Zuerst müssen wir zeigen, dass diese Abbildung $B \to G/K$ wohldefiniert ist: Wenn $b = \varphi(g_1) = \varphi(g_2)$ ist, dann ist $\varphi(g_1 g_2^{-1}) = bb^{-1} = e_H$ und $g_1 g_2^{-1} \in K$. Es folgt

$$g_1 K \cdot g_2^{-1} K = g_1 g_2^{-1} K = K = e_{G/K}$$

und $g_1 K = g_2 K$.

Als nächstes zeigen wir, dass ψ ein Homomorphismus ist. Seien dazu $b_1 = \varphi(g_1)$ und $b_2 = \varphi(g_2)$ Elemente in B. Dann gilt $b_1 b_2 = \varphi(g_1 g_2)$ (weil φ ein Homomorphismus ist) und

$$\psi(b_1 b_2) = g_1 g_2 K = g_1 K \cdot g_2 K = \psi(b_1)\psi(b_2).$$

Aus der Definition von ψ folgt

$$\psi(\varphi(g)) = gK$$

für alle $g \in G$. Das ist die Kommutativität des Diagramms. Es bleibt noch die Bijektivität von ψ nachzuweisen.

Surjektivität: Jede Restklasse $gK = \psi(\varphi(g)) \in G/K$ gehört zum Bild von ψ.

Injektivität: Sei $\psi(b) = e_{G/K}$ für $b = \varphi(g) \in B$. Das bedeutet $gK = e_{G/K} = K$, also $g \in K$ und $b = \varphi(g) = e_H$. □

Satz 1.10 (Zweiter Homomorphiesatz) *Es sei N ein Normalteiler in der Gruppe G und $H \subset G$ eine Untergruppe. Dann ist*

$$H \cdot N := \{h \cdot n : h \in H, n \in N\}$$

eine Untergruppe von G. Weiter ist $H \cap N$ ein Normalteiler in H und es gilt

$$(H \cdot N)/N \simeq H/(H \cap N).$$

Beweis. Wegen $e \in N$ und $e \in H$ ist $e = e \cdot e \in H \cdot N$. Es seien $h_1, h_2 \in H$ und $n_1, n_2 \in N$. Dann ist

$$h_1 n_1 \cdot h_2 n_2 = h_1 h_2 \cdot (h_2^{-1} n_1 h_2) n_2.$$

Weil N normal ist, gehört $h_2^{-1} n_1 h_2$ wieder zu N. Also ist $h_2^{-1} n_1 h_2 n_2 \in N$ und wegen $h_1 h_2 \in H$ gehört das ganze Produkt zu $H \cdot N$. Das Inverse eines Elements $hn \in N \cdot N$ ist

$$(hn)^{-1} = n^{-1} h^{-1} = h^{-1}(hn^{-1}h^{-1}) \in H \cdot N.$$

Wir haben gezeigt: $H \cdot N$ ist eine Untergruppe von G.

Als nächstes zeigen wir: $H \cap N \subset H$ ist ein Normalteiler in H. Dazu sei $n \in H \cap N$. Für jedes $h \in H$ ist $hnh^{-1} \in N$, weil N Normalteiler in G ist. Und wegen $n \in H$ ist auch $hnh^{-1} \in H$. Also ist $hnh^{-1} \in H \cap N$ für alle $n \in H \cap N$ und $h \in H$.

Wir definieren eine Abbildung

$$(H \cdot N)/N \to H/(H \cap N)$$

durch

$$(hn) \cdot N \mapsto h \cdot (H \cap N).$$

Diese Abbildung ist wohldefiniert: Wenn $h_1 n_1 \cdot N = h_2 n_2 \cdot N$ gilt, dann ist

$$\begin{aligned} h_2 n_2 &= h_1 n_1 \cdot n, \quad n \in N, \\ h_2 &= h_1 \cdot n_1 n n_2^{-1}, \\ n_1 n n_2^{-1} &= h_1^{-1} h_2 \in H \cap N, \end{aligned}$$

also $h_2 \cdot (H \cap N) = h_1 \cdot (H \cap N)$.

Wegen der Nomalteiler-Eigenschaft von N ist ist $h_1 N \cdot h_2 N = (h_1 h_2) \cdot N$, und die oben definierte Abbildung $hN \mapsto h \cdot (H \cap N)$ ist ein Gruppen-Homomorphismus.

Injektivität: hn liegt im Kern, falls $h \in H \cap N$, also $hN = N \in HN/N$.

Surjektivität: Jedes $h \cdot (H \cap N)$ ist das Bild von $h \cdot N \in H \cdot N/N$. □

Nicht jede Gruppe besitzt nichttriviale Normalteiler. Die Untergruppen $\{1\}$ und G sind trivialerweise Normalteiler, aber eben triviale Normalteiler. Ist etwa p eine Primzahl, so besitzt die Gruppe $\mathbb{Z}/\mathbb{Z} \cdot p$ keine nicht-trivialen Normalteiler: diese Gruppe hat ja außer den trivialen Normalteilern überhaupt keine anderen Untergruppen (Satz von Lagrange).

Definition 1.13 *Die Gruppe G heißt* einfach *wenn sie keine nicht-trivialen Normalteiler besitzt.*

Eine typisch mathematische Definition: Die einfachen nicht-abelschen Gruppen sind so ziemlich das Kompliziertes, was es gibt.

Aus zwei Gruppen G_1 und G_2 kann man nicht nur das direkte Produkt $G_1 \times G_2$, sondern auch semi-direkte Produkte bilden. Um sie besser zu unterscheiden, nenne ich die beiden Gruppen jetzt N und G. Man braucht eine Operation von G auf N durch Automorphismen von N, d.h., einen Gruppen-Homomorphismus $\rho : G \to Aut(N)$. Als Menge definiert man das semi-direkte

Produkt durch $N \times_\rho G$, wie das direkte Produkt. Aber die Gruppen-Struktur definiert man anders:

$$(n_1, g_1)(n_2, g_2) = (n_1 \rho(g_1) n_2, g_1 g_2).$$

Das ist auch eine Gruppe:

Assoziativität: Es ist

$$\begin{aligned}
((n_1, g_1)(n_2, g_2))(n_3, g_3) &= (n_1 \rho(g_1)(n_2), g_1 g_2)(n_3, g_3) \\
&= (n_1 \rho(g_1) n_2 \rho(g_1 g_2) n_3, g_1 g_2 g_3) \\
&= (n_1 \rho(g_1)(n_2 \rho(g_2 n_3)), g_1 g_2 g_3, \\
(n_1, g_1)((n_2, g_2)(n_3, g_3)) &= (n_1, g_1)(n_2 \rho(g_2) n_3, g_2 g_3) \\
&= (n_1 \rho(g_1)(n_2 \rho(g_2) n_3)), g_1, g_2, g_3).
\end{aligned}$$

Eins-Element: Wegen $\rho(e_G) = id_N$ ist $(e_N, e_G)(n, g) = (n, g)$. Und weil $\rho(g)(e_N) = e_N$ ist, gilt $(n, g)(e_N, e_G)$. Also ist (e_N, e_G) das Eins-Element in der neuen Gruppe.

Inverses: Zu gegebenem (n, g) ist dies $(\rho(g^{-1})n^{-1}, g^{-1})$.

Beide Gruppen, N und G kann man als Untergruppen $N \times e_G$ und $e_N \times G$ im semi-direkten Produkt auffassen. Dabei ist allerdings N ein Normalteiler und G i.a. nicht. Die Operation ρ von G auf N ist genau die Konjugation in $N \times_\rho G$:

$$(1, g)(n, 1)(1, g^{-1}) = (\rho(g)n, g)(1, g^{-1}) = (\rho(g)n, 1).$$

Der Quotient des semi-direkten Produkts nach N ist isomorph zur Gruppe G.

Semi-direkte Produkte kommen häufig vor. So ist z.B. die affine Gruppe des $\mathbb{R}^n$ ein solches Produkt. Man setzt $N = \mathbb{R}^n$, $G = GL(n, \mathbb{R})$ und lässt die $GL(n, \mathbb{R})$ wie üblich auf dem $\mathbb{R}^n$ operieren. Ein Element (t, g) bewirkt die affine Abbildung

$$\mathbb{R}^n \to \mathbb{R}^n, \quad x \mapsto t + gx.$$

Dann ist die Zusammensetzung zweier affiner Abbildungen

$$(t_1 g_1)(t_2, g_2)(x) = (t_1, g_1)(t_2 + g_2 x) = t_1 + g_1 t_2 + g_1 g_2 x$$

dasselbe wie die Anwendung von

$$(t_1, g_1)(t_2, g_2) = (t_1 + g_1 t_2, g_1 g_2),$$

dem soeben definierten Produkt.

Die symmetrische Gruppe S_3 enthält den Normalteiler $A_3 \simeq \mathbb{Z}_3$ der Ordnung 3 und die Faktorgruppe ist $\mathbb{Z}_2$. Diese Faktorgruppe ist das Bild der Untergruppe $\{id, (1, 2)\} \simeq \mathbb{Z}_2$. Diese Gruppe operiert auf dem Normalteiler A_3 durch

$$\rho(1, 2) : (1, 2, 3) \leftrightarrow (1, 3, 2).$$

Und vermöge dieser Operation ist S_3 das semi-direkte Produkt $\mathbb{Z}_3 \times_\rho \mathbb{Z}_2$. Allgemeiner ist die Dieder-Gruppe D_n ein semi-direktes Produkt $\mathbb{Z}_n \times_\rho \mathbb{Z}_2$.

Aufgabe 1.6 *Zeigen Sie, dass jede Untergruppe H einer endlichen Gruppe G vom Index $[G : H] = 2$ normal in G ist.*

Aufgabe 1.7 *Zeigen Sie: Jede Gruppe der Ordnung 4 ist abelsch. Es gibt genau zwei nichtisomorphe Gruppen der Ordnung 4.*

Aufgabe 1.8 *a) Zeigen Sie: In der symmetrischen Gruppe S_n sind je zwei Zyklen gleicher Länge konjugiert.*

b) Gilt dies auch in der alternierenden Gruppe A_n?

Aufgabe 1.9 (F 97, T2, A1) *a) Zeigen Sie, dass die Symmetriegruppe (= Gruppe der Isometrien) eines regulären Oktaeders im euklidischen $\mathbb{R}^3$ isomorph zur Symmetriegruppe des Würfels ist.*

b) Welche Ordnung hat die Gruppe?

c) Wieviele Elemente der Ordnung 3 besitzt sie?

Aufgabe 1.10 (H 96, T3, A1) *Sei G eine Gruppe, N ein Normalteiler in G und $\nu : G \to G/N$ der natürliche Epimorphismus auf die Faktorgruppe G/N. Man zeige:*

a) ν induziert eine Bijektion von der Menge aller Normalteiler H von G mit $N \subset H$ in die Menge aller Normalteiler von G/N.

b) Gibt es einen Normalteiler vom Index 4 in G, dann auch einen Normalteiler vom Index 2.

Aufgabe 1.11 (F 95, T1, Teil von A1+2) *Seien E, G Gruppen und $\pi : E \to G$ ein Epimorphismus. π heißt zerfallend, falls ein Homomorphismus $\rho : G \to E$ mit $\pi\rho = id_G$ existiert. Zeigen Sie:*

a) Ist π zerfallender Epimorphismus mit Kern K, so ist $K \times G \to E$, $(k, g) \mapsto k\rho(g)$ für alle $k \in K$ und $g \in G$, Isomorphismus, falls $K \times G$ mit der Gruppenstruktur des semidirekten Produkts bezügliche einer passenden Operation von G auf K versehen wird.

b) Der kanonische Epimorphismus $\mathbb{Z}/(9) \to \mathbb{Z}/(3)$ ist nicht zerfallend.

Aufgabe 1.12 (H 91, T1, A1) *Man beweise, dass es bis auf Isomorphie genau zwei Gruppen der Ordnung 6 gibt.*

Aufgabe 1.13 (H 91, T2, A1) *Man gebe eine nichtabelsche Gruppe der Ordnung 24 an, die nicht zur symmetrischen Gruppe S_4 isomorph ist.*

Aufgabe 1.14 (F 91, T1, A1) *Sei $\alpha : G \to H$ ein Gruppenhomomorphismus, wobei H abelsch sei. Man zeige: α ist genau dann surjektiv, wenn für je zwei Gruppenhomomorphismen $\beta, \gamma : H \to K$ mit $\beta \circ \alpha = \gamma \circ \alpha$ gilt: $\beta = \gamma$.*

1.3 Zyklische Gruppen

Es sei G eine Gruppe und $g \neq e \in G$ eines ihrer Elemente. Dann gibt es in G die Folge aller Potenzen von g:

$$g^0 = e,\ g^1 = g,\ g^2 = gg,\ g^3 = ggg,\ ...$$

Es kann sein, dass dies unendlich viele verschiedene Gruppen-Elemente sind. Dann sagt man, das Element g hat *unendliche Ordnung*. Es kann aber auch sein, dass irgendwann einmal zwei dieser Elemente übereinstimmen: $g^k = g^l$ für $0 < k < l$. Dann folgt $g^{l-k} = g^l(g^k)^{-1} = e$. Es gibt also eine natürliche Zahl $n > 0$, z.B. $n = l - k$ mit $g^n = e$.

Definition 1.14 (Ordnung) *Es sei $g \in G$. Die kleinste natürliche Zahl $0 < n \in \mathbb{N}$ mit $g^n = e$ heißt die* Ordnung *des Gruppenelementes g. Falls es eine solche Zahl nicht gibt, hat g unendliche Ordnung.*

Satz 1.11 *a) Hat $g \in G$ unendliche Ordnung, so wird durch*

$$\mathbb{Z} \ni k \mapsto g^k$$

ein injektiver Gruppen-Homomorphismus $\mathbb{Z} \to G$ definiert.

b) Hat g die Ordnung n, so wird durch

$$\mathbb{Z}_n \ni k \, mod \, n \mapsto g^k$$

Ein injektiver Gruppen-Homomorphismus definiert.

Beweis. a) Für $k \in \mathbb{N}$ identifiziert man g^{-k} mit $(g^k)^{-1} = (g^{-1})^k$. Damit ist die Abbildung

$$\mathbb{Z} \mapsto G, \quad k \mapsto g^k,$$

wohldefiniert und ein Gruppen-Homomorphismus. Zu zeigen bleibt die Injektivität: Seien also $k < l \in \mathbb{Z}$ mit $g^k = g^l$. Dann wäre $g^{l-k} = e$ und g hätte endliche Ordnung.

b) Jetzt habe g die endliche Ordnung n. Das heißt also $g^n = e$, $g^k \neq e$ für alle $0 < k < n$. Für zwei ganze Zahlen $k_1 = k_2 \, mod \, n$ ist $k_1 - k_2 = q \cdot n$ ein Vielfaches von n und deswegen

$$g^{k_1}(g^{k_2})^{-1} = g^{k_1 - k_2} = (g^n)^q = e, \quad g^{k_1} = g^{k_2}.$$

Die Abbildung

$$\mathbb{Z}_n \ni k \, mod \, n \mapsto g^k \in G$$

ist also wohldefiniert und auch wieder ein Gruppen-Homomorphismus. Weil n die kleinste natürliche Zahl mit $g^n = 1$ ist, ist dieser Morphismus injektiv. □

Definition 1.15 *Die Untergruppe $< g >= \{g^k, k \in \mathbb{Z}\} \subset G$, endlich oder unendlich, heißt die* von g erzeugte Untergruppe *von G. Wenn G selbst von der Form $G =< g >$ ist, heißt G* zyklisch. *Dann ist der Homomorphismus aus Satz 1.11 auch surjektiv und G ist isomorph zu $\mathbb{Z}$ oder $\mathbb{Z}_n$.*

Satz 1.12 *Jede Untergruppe und jede Quotientengruppe einer zyklischen Gruppe ist wieder zyklisch.*

Beweis. Die Gruppe G sei zyklisch. D.h., es gebe einen surjektiven Gruppen-Homomorphismus $\mathbb{Z} \to G$. Für jeden surjektiven Homomorphismus $G \to H$ ist auch $\mathbb{Z} \to G \to H$ surjektiv, also ist H zyklisch.

Sei jetzt $H \subset G$ eine Untergruppe und $\varphi : \mathbb{Z} \to G$ surjektiv. Nach Satz 1.5 e) ist dann $U := \varphi^{-1}(H)$ eine Untergruppe von $\mathbb{Z}$. Wegen $\varphi(\varphi^{-1}(H)) = H$ genügt es also zu zeigen: jede Untergruppe $U \subset \mathbb{Z}$ von $\mathbb{Z}$ ist zyklisch. Die triviale Untergruppe $\{0\} \subset \mathbb{Z}$ ist auf triviale Weise zyklisch. Nehmen wir also an, U enthalte ein Element $k \neq 0$. Nachdem wir eventuell k durch $-k$ ersetzen, können wir annehmen, $k > 0$. Sei $m \in U$ die kleinste Zahl > 0. Wir zeigen

$$U = \mathbb{Z} \cdot m = \{n \cdot m : \ n \in \mathbb{Z}\}.$$

Dann ist U also das Bild des surjektiven Gruppen-Homomorphismus $\mathbb{Z} \ni n \mapsto n \cdot m$ und damit zyklisch.

Sei dazu $0 < k \in U$ beliebig. Wir dividieren k durch m mit Rest:

$$k = q \cdot m + r, \quad q, r \in \mathbb{N},\ 0 \leq r < m.$$

Wir schreiben diese Formel um

$$r = k - q \cdot m$$

und finden $r \in U$. Wegen $r < k$ muss $r = 0$ gelten. Also ist jedes positive (und dann auch jedes negative) $k \in U$ durch m teilbar. □

Satz 1.13 *Wir betrachten eine endliche zyklische Grupppe $\mathbb{Z}_n$.*
a) Die Ordnung eines jeden Elementes $k \,mod\, n$ in $\mathbb{Z}_n$ ist ein Teiler von n.
b) Die Multiplikation mit $q \in \mathbb{N}$

$$\mathbb{Z}_n \to \mathbb{Z}_n, \quad k \,mod\, n \mapsto q \cdot k \,mod\, n$$

ist genau dann ein Gruppen-Isomorphismus, wenn q und n teilerfremd sind .

Beweis. a) Ist l die Ordnung von $k \,mod\, n$, so erzeugt $k \,mod\, n$ in $\mathbb{Z}_n$ eine zyklische Untergruppe der Ordnung l. Diese Ordnung l teilt die Gruppenordnung n nach dem Satz von Lagrange (Satz 1.3).

b) Es ist klar, dass die Abbildung $k \,mod\, n \mapsto q \cdot k \,mod\, n$ ein Homomorphismus ist. Dieser Homomorphismus ist genau dann ein Isomorphismus, wenn er injektiv ist. Eine Restklasse $k \,mod\, n$ liegt genau dann im Kern, wenn $q \cdot k = 0 \,mod\, n$, d.h., wenn n das Produkt $q \cdot k$ teilt.

Wenn n und q teilerfremd sind, muss n die Zahl k teilen. Es ist $k \,mod\, n = 0 \,mod\, n$, und der Kern besteht nur aus der Null. Der Homomorphismus ist injektiv.

Wenn n und q nicht teilerfremd sind, gibt es eine Primzahl p, welche n und q teilt. Sei etwa $n = p \cdot n_1$ und $q = p \cdot q_1$. Dann ist $n_1 \,mod\, n$ ein nicht-triviales Element in $\mathbb{Z}_n$ mit

$$q \cdot n_1 \,mod\, n = q_1 \cdot (pn_1) \,mod\, n = q_1 \cdot 0 \,mod\, n = 0 \,mod\, n.$$

Der Kern ist nicht-trivial, und die Abbildung ist kein Isomorphismus. □

Beispiel 1.10 *Wir betrachten $n = 5$ und $q = 3$ und iterieren diese Multiplikation:*

	0	1	2	3	4
3	0	3	1	4	2
$3^2 = 4$	0	4	3	2	1
$3^3 = 2$	0	2	4	1	3

Definition 1.16 *Die Restklassen $q \bmod n \in \mathbb{Z}_n$, wo q teilerfremd zu n ist, heißen* prime *Restklassen modulo n.*

Unter der Multiplikation mit q wird das erzeugende Element $1 \in \mathbb{Z}_n$ auf $q \bmod n$ abgebildet. Ist q zu n teilerfremd, so ist nach Satz 1.13 also auch $q \bmod n$ ein erzeugendes Element der zyklischen Gruppe $\mathbb{Z}_n$. Insbesondere hat $q \bmod n$ auch die Ordnung n in $\mathbb{Z}_n$. Und umgekehrt: Die Restklasse $q \bmod n \in \mathbb{Z}_n$ habe die Ordnung n. Dann ist also auch $\mathbb{Z}_n =< q \bmod n >$ und die Multiplikation mit q ist ein Isomorphismus $\mathbb{Z}_n \to \mathbb{Z}_n$, weil sie $1 \bmod n$ auf das Erzeugende $q \bmod n$ abbildet.

Satz 1.14 *Die primitiven Restklassen modulo n bilden eine Gruppe $\mathbb{Z}_n^*$ bezüglich der* Multiplikation. *Jede prime Restklasse $q \bmod n$ definiert durch Multiplikation*

$$\mathbb{Z}_n \ni k \bmod n \quad \mapsto \quad q \cdot k \bmod n \in \mathbb{Z}_n$$

einen Gruppen-Automorphismus der zyklischen Gruppe $\mathbb{Z}_n$. Vermöge dieser Zuordnung ist die Gruppe der primen Restklassen modulo n isomorph zur Automorphismengruppe der zyklischen Gruppe $\mathbb{Z}_n$.

Beweis. Sind q_1 und $q_2 \in \mathbb{N}$ relativ prim zu n, so ist dies auch ihr Produkt $q_1 \cdot q_2$. Das Produkt von zwei primen Restklassen modulo n ist also wieder eine prime Restklasse modulo n. Dieses Produkt definiert den Automorphismus von $\mathbb{Z}_n$, der die Hintereinanderschaltung der Automorphismen zu q_1 und zu q_2 ist. Die angegebene Abbildung $\mathbb{Z}_n^* \to$ Automorphismengruppe von $\mathbb{Z}_n$ ist also multiplikativ. Als nächstes zeigen wir, dass sie auch bijektiv ist.

Injektivität: Stimmen für zwei primitive Restklassen q_1, q_2 modulo n die Multiplikationsabbildungen $k \bmod n \mapsto q_i \cdot k \bmod n$ überein, dann ist insbesondere $(k = 1 \bmod n)$

$$q_1 = q_1 \cdot 1 = q_2 \cdot 1 = q_2 \text{ modulo } n.$$

Surjektivität: Jeder Automorphismus $\alpha : \mathbb{Z}_n \to \mathbb{Z}_n$ ist festgelegt durch das Bild $\alpha(1)$ der Restklasse $1 \bmod n$. Denn dann ist

$$\alpha(k) = \alpha(\underbrace{1 + ... + 1}_{k}) = \underbrace{\alpha(1) + ... + \alpha(1)}_{k} = k \cdot \alpha(1) \text{ modulo } n.$$

Ist $\alpha : \mathbb{Z}_n \to \mathbb{Z}_n$ ein Automorphismus so erzeugt auch $q := \alpha(1)$ die zyklische Gruppe $\mathbb{Z}_n$. Deswegen ist q eine prime Restklasse modulo n und α ist die Multiplikation mit dieser Restklasse.

Wir haben jetzt eine bijektive Abbildung von $\mathbb{Z}_n^*$ auf die Automorphismengruppe von $\mathbb{Z}_n$ definiert, die das Produkt erhält. Dann muss $\mathbb{Z}_n^*$ mit diesem Produkt eine Gruppe sein, und die angegebene Abbildung ein Gruppen-Isomorphismus. □

Die Automorphismengruppe von $\mathbb{Z}_n$ ist nach Satz 1.14 insbesondere abelsch. Aber sie braucht nicht zyklisch zu sein.

Beispiel 1.11 *Die primen Restklassen modulo 8 sind*

$$1,\ 3,\ 5,\ 7\, mod\, 8.$$

Die Automorphismengruppe hat also die Ordnung vier. Für die nichttrivialen primen Restklassen gilt

$$\begin{array}{rcrcl} 3^2 & = & 9 & = & 1\, mod\, 8 \\ 5^2 & = & 25 & = & 1\, mod\, 8 \\ 7^2 & = & 49 & = & 1\, mod\, 8 \end{array}$$

Jedes Element hat die Ordnung zwei. Die Automorphismengruppe ist die Kleinsche Vierergruppe $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Definition 1.17 *Für* $n \in \mathbb{N}$ *bezeichnet man mit* $\varphi(n)$ *die Anzahl der primen Restklassen modulo* n. *Das ist also die Anzahl der natürlichen Zahlen* $< n$, *die zu* n *teilerfremd sind. Die Abbildung* $n \mapsto \varphi(n)$ *heißt* Eulersche φ-Funktion.

Beispiel 1.12 *Für eine Primzahl* p *ist* $\varphi(p)$ *die Anzahl aller Restklassen modulo* p, *die* $\neq 0$ *sind. Also ist* $\varphi(p) = p - 1$. *Für eine Primzahl-Potenz* p^k *ist* q *genau dann teilerfremd zu* p^k, *wenn* q *nicht durch* p *teilbar ist. Die durch* p *teilbaren Zahlen zwischen* 0 *und* $p^k - 1$ *sind*

$$0,\ p,\ 2 \cdot p,\ \ldots,\ (p^{k-1} - 1) \cdot p.$$

Deren Anzahl ist p^{k-1}. *Also gilt*

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1).$$

Die direkte Summe zyklischer Gruppen ist i.a. nicht wieder zyklisch. Als Beispiel betrachten wir die Gruppe $\mathbb{Z}_n \times \mathbb{Z}_n$. Sie enthält n^2 Elemente. Wenn sie zyklisch wäre, wäre sie also isomorph zur Gruppe $\mathbb{Z}_{n^2}$ und ihr Erzeuger hätte die Ordnung n^2. Nun gilt aber für jedes Element $(k_1\, mod\, n, k_2\, mod\, n) \in \mathbb{Z}_n \times \mathbb{Z}_n$:

$$(k_1\, mod\, n, k_2\, mod\, n)^n = (nk_1\, mod\, n, nk_2\, mod\, n) = (0,0).$$

Jedes Element in $\mathbb{Z}_n \times \mathbb{Z}_n$ hat die Ordnung n. Also können die beiden Gruppen $\mathbb{Z}_n \times \mathbb{Z}_n$ und $\mathbb{Z}_{n^2}$ nicht isomorph sein.

Satz 1.15 *Es seien* $m, n > 1$ *natürliche Zahlen. Dann sind äquivalent:*
a) Die Gruppen $\mathbb{Z}_m \times \mathbb{Z}_n$ *und* $\mathbb{Z}_{m \cdot n}$ *sind isomorph;*
b) Die Zahlen m *und* n *sind teilerfremd.*

Beweis. a) $\Rightarrow$ b): Es sei $p > 1$ ein Teiler von m und von n, etwa $m = p \cdot m'$ und $n = p \cdot n'$. Der Homomorphismus

$$\mathbb{Z} \to \mathbb{Z}_m \to \mathbb{Z}_{m'}, \quad k \mapsto k\, mod\, m \mapsto k\, mod\, m'$$

ist surjektiv. Also enthält $\mathbb{Z}_m$ eine Untergruppe isomorph zu $\mathbb{Z}_p$. Ebenso enthält $\mathbb{Z}_n$ eine Untergruppe isomorph zu $\mathbb{Z}_p$. Die Gruppe $\mathbb{Z}_m \times \mathbb{Z}_n$ enthält also eine Untergruppe isomorph zu

$\mathbb{Z}_p \times \mathbb{Z}_p$. Das eben angegebene Beispiel zeigt, dass diese Untergruppe nicht zyklisch ist. Wegen Satz 1.12 kann dann auch $\mathbb{Z}_m \times \mathbb{Z}_n$ nicht zyklisch sein.

b) $\Rightarrow$ a): Wir betrachten den Homomorphismus

$$\mathbb{Z} \to \mathbb{Z}_m \times \mathbb{Z}_n, \quad k \mapsto (k \bmod m, k \bmod n).$$

Sein Kern ist die Untergruppe von $\mathbb{Z}$ bestehend aus den Zahlen k, welche sowohl durch m als auch durch n teilbar sind. Weil m und n teilerfremd sind, heißt dieses: k ist durch $m \cdot n$ teilbar. Dieser Kern ist also die Untergruppe $\mathbb{Z} \cdot (m \cdot n) \subset \mathbb{Z}$. Nach dem Homomorphie-Satz 1.9 ist das Bild des Homomorphismus in $\mathbb{Z}_m \times \mathbb{Z}_n$ isomorph zur Quotientengruppe $\mathbb{Z}/\mathbb{Z} \cdot (m \cdot n) = \mathbb{Z}_{m \cdot n}$. Dieses Bild hat die Ordnung $m \cdot n$, ebenso wie die ganze Gruppe $\mathbb{Z}_m \times \mathbb{Z}_n$. Das Bild $\mathbb{Z}_{m \cdot n}$ muss also mit der ganzen Gruppe $\mathbb{Z}_m \times \mathbb{Z}_n$ übereinstimmen. □

Satz 1.16 (Korollar: Chinesischer Restsatz) *Sind die Zahlen m und n teilerfremd, so gibt es zu jedem Paar von Restklassen*

$$a \bmod m \text{ und } b \bmod n$$

genau eine Zahl k, $0 \leq k < m \cdot n$ mit

$$k \bmod m = a \bmod m, \quad k \bmod n = b \bmod n.$$

Die Zahlen m und $n \in \mathbb{N}$ seien teilerfremd. Wenn ein Paar $(q \bmod m, r \bmod n) \in \mathbb{Z}_m \times \mathbb{Z}_n$ diese Gruppe erzeugt, dann muss q teilerfremd zu m und r teilerfremd zu n sein. Und umgekehrt: Es sei q teilerfremd zu m und r zu n. Falls $k(q, r) = (0, 0)$ ist, muss $k \cdot q$ durch m teilbar sein. Kein Teiler von m teilt q. Also muss m die Zahl k teilen. Ebenso sieht man, dass n die Zahl k teilt. Weil m und n teilerfremd sind, ist k durch $m \cdot n$ teilbar. D.h., das Element $(q, r) \in \mathbb{Z}_m \times \mathbb{Z}_n$ hat die Ordnung $m \cdot n$. Daraus folgt:

Satz 1.17 *Für zwei teilerfremde Zahlen m und $n \in \mathbb{N}$ ist*

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n).$$

Damit kann man eine allgemeine Formel für die Eulersche φ-Funktion angeben: Die Zahl $n \in \mathbb{N}$ habe die Primfaktor-Zerlegung

$$n = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}, \quad k_1, \ldots, k_r \geq 1,$$

wo $p_1, \ldots, p_r$ verschiedene Primzahlen sind. Dann ist

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{k_1}) \cdot \ldots \cdot \varphi(p_r^{k_r}) \\ &= p_1^{k_1 - 1}(p_1 - 1) \cdot \ldots \cdot p_r^{k_r - 1}(p_r - 1) \\ &= p_1^{k_1}(1 - \frac{1}{p_1}) \cdot \ldots \cdot p_r^{k_r}(1 - \frac{1}{p_r}) \\ &= n \cdot (1 - \frac{1}{p_1}) \cdot \ldots \cdot (1 - \frac{1}{p_r}). \end{aligned}$$

Beispiel 1.13 *Es ist*

$$\varphi(100) = \varphi(2^2 \cdot 5^2) = 100 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{5}) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40.$$

Beispiel 1.14 (F 00, T3, A1) *: Bestimmen Sie den Isomorphietyp der primen Restklassengruppe modulo 360, und geben sie hierin explizit ein Element $n + 360\mathbb{Z}$ maximaler Ordnung an.*

Lösung: Wir zerlegen

$$360 = 2^3 \cdot 3^2 \cdot 5$$

in Primzahlpotenzen. Nach dem Beweis von Satz 1.17 ist also die prime Restklassengruppe

$$\mathbb{Z}_{360}^* = \mathbb{Z}_8^* \times \mathbb{Z}_9^* \times \mathbb{Z}_5^*.$$

Aus den schon diskutierten Beispielen wissen wir: $\mathbb{Z}_8^*$ ist die Kleinsche Vierergruppe $\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_5^* =< 2 >$ ist die zyklische Gruppe $\mathbb{Z}_4$. Wir müssen noch die prime Restklassengruppe $\mathbb{Z}_9^*$ bestimmen.

Die primen Restklassen modulo 9 sind $1, 2, 4, 5, 7, 8$. Nun ist modulo 9

$$2^2 = 4, \quad 2^3 = 8, \quad 2^4 = 7, \quad 2^5 = 5, \quad 2^6 = 1.$$

Also ist $\mathbb{Z}_9^* =< 2 >$ zyklisch von der Ordnung 6. Damit ist die prime Restklassengruppe modulo 360

$$\mathbb{Z}_{360}^* = (\mathbb{Z}_2 \times \mathbb{Z}_2) \times \mathbb{Z}_6 \times \mathbb{Z}_4 \simeq (\mathbb{Z}_2)^3 \times \mathbb{Z}_3 \times \mathbb{Z}_4$$

identifiziert. Die maximale Ordnung eines Elementes in dieser Gruppe ist 12. Und $n \, mod \, 360$ hat diese Ordnung 12, wenn etwa

$$n \equiv 2 \, mod \, 9, \quad n \equiv 2 \, mod \, 5$$

ist. Eine solche Zahl ist etwa $n = 47$.

Probe: Wir berechnen die Potenzen von 47 modulo 360:

$$\begin{array}{rcrcrcrcr} & & 47^2 & = & 2209 & = & 6 \cdot 360 + 49 & = & 49, \\ 47^4 & = & 49^2 & = & 2401 & = & 6 \cdot 360 + 241 & = & 241, \\ 47^8 & = & 241^2 & = & 58081 & = & 161 \cdot 360 + 121 & = & 121, \\ 47^{12} & = & 241 \cdot 121 & = & 29161 & = & 81 \cdot 360 + 1 & = & 1. \end{array}$$

Es stimmt.

Satz 1.18 *Die Gruppe G sei abelsch. Dann bilden die Elemente endlicher Ordnung (zusammen mit dem neutralen Element $e \in G$) eine Untergruppe $T \subset G$. Kein Element der Faktorgruppe G/T hat endliche Ordnung.*

Beweis. Nach Definition gehört das neutrale Element zu T. Wenn $g_1, g_2 \in G$ endliche Ordnung haben, etwa $g_1^{k_1} = g_2^{k_2} = e$, dann ist

$$(g_1 g_2)^{k_1 k_2} = (g_1^{k_1})^{k_2} (g_2^{k_1})^{k_1} = e^{k_2} e^{k_1} = e$$

und $g_1 g_2$ hat wieder endliche Ordnung. Schließlich hat auch g^{-1} die endliche Ordnung k, wenn g die Ordnung k hat.

Sei jetzt $gT \in G/T$ eine Nebenklasse endlicher Ordnung, etwa $(gT)^k = T$. Daraus folgt $g^k T = T$ und $g^k \in T$. Deswegen hat g^k endliche Ordnung, etwa die Ordnung l. Daraus folgt $g^{kl} = e$ und $g \in T$. Es war $gT = e_{G/T}$. □

Definition 1.18 *Die Untergruppe $T \subset G$ aus Satz 1.18 heißt* Torsions-Untergruppe. *Ihre Elemente heißen die* Torsions-Elemente *von G. Die abelsche Gruppe G heißt* torsionsfrei *oder kurz* frei *wenn ihre Torsionsuntergruppe $T = 0$ trivial ist.*

Aufgabe 1.15 *Zeigen Sie: Jede endliche Gruppe, deren Ordnung eine Primzahl ist, ist zyklisch.*

Aufgabe 1.16 *Bestimmen Sie für $n = 2, ..., 10$ die Werte der Eulerschen φ-Funktion $\varphi(n)$ und geben Sie die primen Restklassen modulo n explizit an.*

Aufgabe 1.17 (H 01, T2, A1) *Für $3 \leq n$ sei D_n die Diedergruppe der Ordnung $2n$, es sei H die Quaternionengruppe der Ordnung 8, und S_3 die symmetrische Gruppe auf 3 Elementen.*

a) Zeigen Sie: Die drei Gruppen D_8, $D_4 \times \mathbb{Z}_2$ und $H \times \mathbb{Z}_2$ sind paarweise nicht isomorph.

b) Bestimmen Sie für jede der drei Gruppen aus a) die Anzahl der zyklischen Untergruppen der Ordnung 4 und geben Sie jeweils die Menge dieser Untergruppen an.

c) Zeigen Sie: Die Gruppen D_6 und $S_3 \times \mathbb{Z}_2$ sind isomorph.

Aufgabe 1.18 (F 99, T1, A1) *a) Sei C_8 die zyklische Gruppe der Ordnung 8. Man zeige, dass die Automorphismengruppe $Aut(C_8)$ isomorph zur Kleinschen Vierergruppe V ist.*

b) Man zeige, dass die Automorphismengruppe $Aut(V)$ der Kleinschen Vierergruppe isomorph zur symmetrischen Gruppe S_3 ist.

Aufgabe 1.19 (H 97, T3, A1) *Sei $G = S_4$ die Gruppe der Permutationen von $\{1, 2, 3, 4\}$.*

a) Geben Sie eine nicht zyklische Untergruppe H der Ordnung 4 von G an, die auf $\{1, 2, 3, 4\}$ transitiv ist.

b) Zeigen Sie, dass H normal ist.

c) Zeigen Sie, dass durch $f(g)(h) := ghg^{-1}$ für $g \in G$ und $h \in H$ ein Homomorphismus $f : G \to Aut(H)$ definiert wird, der surjektiv ist und den Kern H hat.

Aufgabe 1.20 (H 98, T1, A1) *Sei p eine Primzahl und G die additive Gruppe $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.*

a) Wieviele Untergruppen der Ordnung p besitzt G?

b) Seien $x, y \in G$ mit $x \neq y$ gegeben. Man zeige, dass es genau eine Untergruppe $H \subset G$ der Ordnung p gibt, für die $x + H = y + H$ gilt.

c) Zu einer sechstägigen Konferenz treffen sich 25 Teilnehmer. Die sechs gemeinsamen Mittagessen nehmen sie an 5 Tischen mit je 5 Plätzen ein. Ist es möglich, täglich wechselnde Sitzordnungen derart festzulegen, dass jeder Teilnehmer mit jedem anderen genau einmal am gleichen Tisch sitzt?

Aufgabe 1.21 (H 95, T1, A1) *Eine Gruppe G heißt lokal-zyklisch, falls jede endlich-erzeugte Untergruppe von G zyklisch ist. Nan zeige:*

a) Jede lokal-zyklische Gruppe ist abelsch.

b) Unter- und Faktorgruppen einer lokal-zyklischen Gruppe sind lokal-zyklisch.

c) Die additiven Gruppen $\mathbb{Q}$ und $\mathbb{Q}/\mathbb{Z}$ sind lokal-zyklisch.

Aufgabe 1.22 (F 94, T1, A2) *Es sei n eine ungerade natürliche Zahl. Zeigen Sie: Wenn es bis auf Isomorphie nur eine einzige Gruppe der Ordnung n gibt, dann gilt $(\varphi(n), n) = 1$.*

Aufgabe 1.23 (H 92, T3, A1) *Es seien $m_1, m_2, ..., m_r$ durch 3 teilbare natürliche Zahlen, und G die abelsche Gruppe*

$$G = \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times ... \times \mathbb{Z}/m_r\mathbb{Z}.$$

a) Man bestimme die Anzahl der Elemente von G der Ordnung 3.

b) Man bestimme die Anzahl der Untergruppen von G der Ordnung 3.

Aufgabe 1.24 (H 91, T1, A1) *Man beweise, dass es bis auf Isomorphie genau zwei Gruppen der Ordnung 6 gibt.*

1.4 Endlich erzeugte Gruppen

Definition 1.19 *Es sei G eine (abelsche oder nicht-abelsche) Gruppe und $M \subset G$ eine Teilmenge. Die* von M erzeugte Untergruppe $< M > \subset G$ *ist die kleinste Untergruppe von G, welche die Menge M enthält, d.h., der Durchschnitt aller Untergruppen von G, welche M enthalten.*

Diese Definition ist ziemlich formal. Man kann die Elemente von $< M >$ aber auch explizit angeben, zumindest im Prinzip:

Definition 1.20 *Sei $M \subset G$ wie in Definition 1.19. Ein* Wort *über M ist ein Gruppenelement*

$$g_1 \cdot g_2 \cdot ... \cdot g_r,$$

wo

- *entweder $g_i = e \in G$ (dann kann man den Faktor e natürlich weglassen, außer im kurzen Wort e),*

- *oder* $g_i \in M$,
- *oder* $g_i^{-1} \in M$.

Es ist klar, dass jede Untergruppe $H \subset G$, welche die Menge M enthält, auch jedes Wort über M enthält. Wir zeigen, dass die Menge all dieser Wörter eine Untergruppe von G ist. Dann muss $< M >$ die Menge aller dieser Wörter über M sein.

In der Tat: Das Eins-Element e ist eines der Wörter über M. Und das Produkt

$$(g_1 g_2 ... g_r) \cdot (h_1 h_2 ... h_s) = g_1 g_2 ... g_r h_1 h_2 ... h_s$$

zweier Wörter über M ist stets auch wieder ein solches Wort. Schließlich ist das Inverse

$$(g_1 g_2 ... g_r)^{-1} = g_r^{-1} ... g_2^{-1} g_1^{-1}$$

eines Wortes über M auch wieder ein solches Wort.

Die von einem Gruppenelement $g \in G$ erzeugte, zyklische, Untergruppe $< g >$ ist ziemlich einfach zu verstehen. Bei nicht-abelschen Gruppen kann aber schon die von zwei Elementen erzeugte Gruppe $< g, h >$ ziemliche Überraschungen bergen. Dazu ein Beispiel:

Satz 1.19 *In der symmetrischen Gruppe S_n seien die beiden Elemente*

$$g := (1, 2, ..., n) \text{ und } h = (1, 2)$$

festgehalten. Dann ist die von diesen erzeugte Gruppe

$$< g, h >= S_n.$$

Beweis. Man berechnet

$$\begin{aligned} (1,2,...,n)(1,2)(1,2,...,n)^{-1} &= (1,2,...,n)(1,2)(n,...,2,1) \\ &= (1,3,...,n)(n,...,2,1) \\ &= (2,3), \end{aligned}$$

und ebenso

$$(1, 2, ..., n)^k (1, 2)(1, 2, ..., n)^{-k} = (k + 1, k + 2)$$

für $k = 1, ..., n - 2$. Also gehören alle Transpositionen

$$(1, 2), (2, 3), ..., (n - 1, n)$$

zu $< g, h >$. Für $1 \leq i < j \leq n$ ist

$$(i, i + 1)(i + 1, i + 2)...(j - 1, j)(j - 2, j - 1)...(i + 1, i + 2)(i, i + 1) = (i, j),$$

also gehört jede beliebige Transposition (i, j) zur erzeugten Gruppe $< g, h >$. Aus

$$(i_1, ..., i_k)(i_k, i_{k+1}) = (i_1, ..., i_k, i_{k+1})$$

folgt mit Induktion nach k, dass jeder Zyklus zu $< g, h >$ gehört. Und weil jede Permutation ein Produkt von Zyklen ist, erhält man daraus die Behauptung. □

Bei abelschen Gruppen ist die Situation allerdings wesentlich einfacher. Dies illustriert folgender Satz:

Satz 1.20 *Es sei A eine abelsche Gruppe mit den Untergruppen A_1 und A_2.*

a) Die Abbildung

$$A_1 \times A_2 \to A, \quad (a_1, a_2) \mapsto a_1 a_2$$

ist ein Gruppen-Homomorphismus, dessen Bild die von A_1 und A_2 erzeugte Untergruppe $< A_1 \cup A_2 >$ ist.

b) Der Homomorphismus $A_1 \times A_2 \to A$ aus a) ist genau dann ein Isomorphismus, wenn
i) $< A_1 \cup A_2 >= A$ und
ii) $A_1 \cap A_2 = \{e\}$.

Beweis. a) Die Elemente in $< A_1 \cup A_2 >$ sind die Worte $g_1^{\pm 1} g_2^{\pm 1} \cdot ...$ mit $g_1, g_2, ... \in A_1$ oder $\in A_2$. Weil A abelsch ist, kann man die Reihenfolge dieser Elemente vertauschen. Insbesondere kann man die Elemente in A_1 zu einem einzigen solchen Element $a_1 \in A_1$ und die Elemente in A_2 zu einem Element $a_2 \in A_2$ zusammenfassen. Die von A_1 und A_2 erzeugte Untergruppe besteht also genau aus den Produkten $a_1 a_2$ mit $a_1 \in A_1$ und $a_2 \in A_2$. Deswegen ist diese Untergruppe $< A_1 \cup A_2 >$ das Bild des angegebenen Homomorphismus.

b) Der angegebene Homomorphismus ist genau dann surjektiv, wenn $< A_1 \cup A_2 >= A$ ist. Wenn er nicht injektiv ist, gibt es $a_i \in A_i$, nicht $a_1 = a_2 = e$ mit $a_1 a_2 = e$. Dann ist aber $a_1 = a_2^{-1}$ ein nicht-triviales Element in $A_1 \cap A_2$. □

Definition 1.21 *Eine Gruppe G heißt* endlich erzeugt, *wenn es endlich viele Elemente $g_1, ..., g_k \in G$ gibt, die G erzeugen:*

$$G =< g_1, ..., g_k >$$

Satz 1.21 *a) Jedes Bild einer endlich erzeugten Gruppe unter einem surjektiven Gruppen-Homomorphismus ist wieder endlich erzeugt.*

b) Es sei $\varphi : G \to H$ ein Gruppen-Homomorphismus, dessen Kern K und Bild B endlich erzeugt sind. Dann ist auch G endlich erzeugt.

Beweis. a) Es sei $\varphi : G \to B$ surjektiv. Es gelte $G =< g_1, ..., g_k >$. Dann ist also jedes Element in $g \in G$ ein Wort über der Menge $\{g_1, ..., g_k\}$. Und jedes Element $b = \varphi(g) \in B$ ist dann ein Wort über der Menge $\{\varphi(g_1), ..., \varphi(g_k)\}$.

b) Es sei $K =< g_1, ..., g_k >$ und $B =< b_1, ..., b_l >$. Wir wählen $h_1, ..., h_l \in G$ mit $\varphi(h_1) = b_1, ..., \varphi(h_l) = b_l$. Für jedes $g \in G$ ist $\varphi(g) = b_{l_1}^{\pm 1} b_{l_2}^{\pm 1} ...$ ein Wort über der Menge $\{b_1, ..., b_l\}$. Wir bezeichnen mit $h \in G$ das entsprechende Wort $h_{l_1}^{\pm 1} h_{l_2}^{\pm 1} ...$ über der Menge $\{h_1, ..., h_l\}$. Dann ist $\varphi(g) = \varphi(h)$ und $g' := gh^{-1} \in K$. Also ist $g' = g_{k_1}^{\pm 1} g_{k_2}^{\pm 1} ...$ ein Wort über der Menge $\{g_1, ..., g_k\}$. Daraus folgt:

$$g = g'h = g_{k_1}^{\pm 1} g_{k_2}^{\pm 1} ... h_{l_1}^{\pm 1} h_{l_2}^{\pm 1} ...$$

ist ein Wort über der endlichen Menge $\{g_1, ..., g_k, h_1, ..., h_l\}$. □

Satz 1.22 *Für eine* abelsche *Gruppe G sind äquivalent:*

a) G ist endlich erzeugt;

b) es gibt ein k und einen surjektiven Gruppen-Homomorphismus

$$\mathbb{Z}^k \to G.$$

(Dabei bedeutet $\mathbb{Z}^k$ die k-fache direkte Summe $\mathbb{Z} \times \mathbb{Z} \times ... \times \mathbb{Z}$.)

Beweis. a) $\Rightarrow$ b): Es seien $g_1, ..., g_k \in G$ Elemente, welche G erzeugen. Dann besteht G also aus allen Worten, die man mit $g_1, ..., g_k$ zusammensetzen kann. Weil G abelsch vorausgesetzt ist, kann man die Buchstaben in diesen Worten vertauschen, und deswegen jedes dieser Worte als

$$g_1^{r_1} \cdot g_2^{r_2} \cdot ... \cdot g_k^{r_k}, \quad r_1, r_2, ..., r_k \in \mathbb{Z}$$

schreiben. Jetzt betrachten wir die Abbildung

$$\mathbb{Z}^k \to G, \quad (r_1, r_2, ..., r_k) \mapsto g_1^{r_1} \cdot g_2^{r_2} \cdot ... \cdot g_k^{r_k}.$$

Nach dem eben Bewiesenen ist diese Abbildung surjektiv. Und weil G abelsch ist, folgt auch sehr schnell, dass die Abbildung ein Homomorphismus ist.

b) $\Rightarrow$ a): Die Gruppe $\mathbb{Z}^k$ ist von den k Elementen

$$(1, 0, ..., 0), (0, 1, 0, ...0), ..., (0, 0, ..., 0, 1)$$

erzeugt. Und das Bild einer endlich erzeugten Gruppe unter einem surjektiven Gruppen-Homomorphismus ist immer wieder endlich erzeugt. (Satz 1.21 a) □

Für den Rest dieses Abschnitts betrachten wir nur noch endlich erzeugte abelsche Gruppen A.

Satz 1.23 *Jede Untergruppe einer endlich erzeugten* abelschen *Gruppe ist selbst wieder endlich erzeugt.*

Wegen Satz und Satz 1.21 a) folgt dies aus

Satz 1.24 *Jede Untergruppe der Gruppe $\mathbb{Z}^k$ ist endlich erzeugt, und zwar durch $\leq k$ Elemente.*

Beweis (Induktion nach k). Der Induktions Anfang ($k = 1$) ist Satz 1.12. Sei also jetzt $k > 1$ und die Behauptung für die Gruppe $\mathbb{Z}^{k-1}$ die Induktions-Annahme. Wir fassen $\mathbb{Z}^{k-1} \subset \mathbb{Z}^k$ als die Untergruppe aller Vektoren $(0, z_2, ..., z_k)$ mit dem ersten Eintrag $= 0$ auf.

Sei jetzt $G \subset \mathbb{Z}^k$ eine Untergruppe. Wir betrachten den Gruppen-Homomorphismus

$$G \to \mathbb{Z}, \quad (z_1, z_2, ..., z_k) \mapsto z_1.$$

Sein Kern ist die Untergruppe $G \cap \mathbb{Z}^{k-1}$ und durch $\leq k - 1$ Elemente erzeugt nach Induktions-Annahme. Das Bild des Homomorphismus ist eine Untergruppe von $\mathbb{Z}$ und nach Satz 1.12 durch höchstens ein Element erzeugt. Aus Satz 1.21 b) folgt die Behauptung. □

Insbesondere ist die Torsions-Untergruppe $T \subset A$ endlich erzeugt. Seien etwa $t_1, ..., t_k \in T$ Erzeugende dieser Gruppe mit den Ordnungen $n_1, ..., n_k$. Dann ist der Homomorphismus

$$\mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_k} \to T, \quad (t_1^{l_1}, ..., t_k^{l_k}) \mapsto t_1^{l_1} \cdot ... \cdot t_k^{l_k}$$

surjektiv. Somit ist die Torsionsgruppe T selbst sogar endlich (nicht nur endlich erzeugt).

Satz 1.25 (Hauptsatz über endlich erzeugte abelsche Gruppen) *Jede endlich erzeugte abelsche Gruppe A ist isomorph zu einer direkten Summe*

$$\mathbb{Z} \times \mathbb{Z} \times ... \times \mathbb{Z} \times \mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \times ... \times \mathbb{Z}_{k_t}$$

zyklischer Gruppen.

Beweis. Nach Satz 1.22 gibt es einen Epimorphismus

$$\mathbb{Z}^k \to A.$$

Sein Kern $K \subset \mathbb{Z}^k$ ist nach Satz 1.24 auch wieder endlich erzeugt. Erzeugende seien etwa $v_1, ..., v_r \in \mathbb{Z}^k$.

Elemente $v \in \mathbb{Z}^k$ schreiben wir jetzt als Zeilenvektoren

$$v = (v_1, ..., v_k) \in \mathbb{Z}^k, \quad v_i \in \mathbb{Z}.$$

Die Vektoren $v_1, ..., v_r$ ordnen wir zu einer $r \times k$-Matrix

$$\begin{pmatrix} v_{1,1} & ... & v_{1,k} \\ v_{2,1} & ... & v_{2,k} \\ \vdots & & \vdots \\ v_{r,1} & ... & v_{r,k} \end{pmatrix}$$

an. Auf diese Matrix werden wir elementare Zeilenumformungen anwenden, und zwar:

- *Multiplikation einer Zeile mit* -1. Dabei wird ein erzeugendes Element v_i durch $-v_i$ ersetzt. Die Gruppe $K =< v_1, ..., v_r >$ bleibt unverändert.
- *Vertauschen zweier Zeilen.* Dabei ändert sich die Reihenfolge der Erzeugenden $v_1, ..., v_r$, aber nicht die erzeugte Gruppe K.
- *Ersetzen einer Zeile v_i durch $v_i + nv_j$, $n \in \mathbb{Z}$ und $i \neq j$.* Wegen $v_i = (v_i + nv_j) - nv_j$ erzeugen v_i und v_j dieselbe Gruppe wie $v_i + nv_j$ und v_j.

Aber wir werden auch elementare Spaltenumformungen vornehmen. Dabei ändert sich natürlich die Untergruppe $K \subset \mathbb{Z}^k$. Durch geeignetes Verändern der Erzeugenden

$$e_1 = (1, 0, ..., 0), ..., e_k = (0, ..., 0, 1) \in \mathbb{Z}^k$$

bleibt die Gruppe $A = \mathbb{Z}^k / K$ aber doch dieselbe:

- *Multiplikation einer Spalte mit* -1. Ersetzen wir gleichzeitig den zugehörigen Vektor e_i durch $-e_i$, dann bleibt K und damit auch A ungeändert.
- Vertauschen zweier Spalten. Vertauschen wir hier auch die zugehörigen Basisvektoren e_i, so bleibt K wieder ungeändert.

- *Addition eines ganzzahligen Vielfachen der i-ten Spalte zur j-ten Spalte, $j \neq i$.* Der Vektor

$$v = (v_1, ..., v_i, ..., v_j, ..., v_k)$$

wird ersetzt durch

$$(v_1, ..., v_i, ..., v_j + nv_i, ..., v_k) = v_1e_1 + ... + v_ie_i + ... + (v_j + nv_i)e_j + ... + v_ke_k.$$

Aber auch die Vektoren $e_1, ..., e_i + ne_j, ..., e_j, ..., e_k \in \mathbb{Z}^k$ erzeugen die ganze Gruppe $\mathbb{Z}^k$. Und in diesen Erzeugenden hat der neue Vektor wieder die Koeffizienten des alten Vektors v. Mit diesen Erzeugenden haben wir dann dieselbe Gruppe K und denselben Quotienten A.

Wir beginnen mit der ersten Spalte. Falls hier alle Einträge $v_{i,1} = 0$ sind, vertauschen wir sie mit einer Spalte $\neq 0$ und wenden uns sogleich der neuen ersten Spalte zu. Andernfalls sei etwa v_i ein Zeilenvektor mit minimalem $|v_{i,1}| \neq 0$. Nachdem wir eventuell v_i mit -1 multiplizieren, können wir $v_{i,1} > 0$ annehmen. Dann dividieren wir für alle $j \neq i$ mit Rest

$$v_{j,1} = q_jv_{i,1} + r_j, \quad q_j, r_j \in \mathbb{Z}, |r_j| < q_{i,1}.$$

Nachdem wir v_j durch $v_j - q_jv_i$ ersetzen, haben wir $|v_{j,1}| = |r_j| < v_{i,1}$. Wir suchen einen neuen Vektor v_i mit minimalem $|v_{i,1}| \neq 0$ und wiederholen das Verfahren. Weil die Einträge in der ersten Spalte immer echt kleiner werden, muss das Verfahren irgend wann abbrechen. Das kann nur so aussehen, dass alle Einträge $v_{i,1}$ bis auf einen $= 0$ sind. Diesen einen Zeilenvektor vertauschen wir mit v_1 und haben danach $v_{i,1} = 0$ für $i > 1$.

Jetzt führen wir dasselbe Verfahren in der ersten Zeile durch. Falls wir dabei die erste Spalte verändern müssen, gehen uns natürlich die schönen Nullen in dieser Spalte verloren. Aber dann ist danach $|v_{1,1}|$ echt kleiner geworden. Dann müssen wir halt nochmal die erste Spalte behandeln, usw. Irgend wann ist Schluss. Und dann ist $v_{i,1} = v_{1,j} = 0$ für $i, j \neq 1$.

Wir streichen dann die erste Spalte und die erste Zeile und wenden uns der übrig bleibenden $(r-1) \times (k-1)$-Matrix zu. Auf diese Weise fabrizieren wir eine Matrix

$$\begin{pmatrix} v_1 \\ \vdots \\ v_r \end{pmatrix} = \begin{pmatrix} d_1 & 0 & 0 & ... \\ 0 & d_2 & 0 & ... \\ 0 & 0 & d_3 & ... \\ \vdots & \vdots & \vdots & \end{pmatrix}$$

mit $v_{i,j} = 0$ für $i \neq j$. Dann ist endlich

$$A = \mathbb{Z}^k / < d_1e_1, d_2e_2, ... >= \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times ...$$

ein Produkt zyklischer Gruppen geworden. □

Spezialfälle dieses Hauptsatzes sind:

Satz 1.26 *Die endlich erzeugte abelsche Gruppe F sei frei. Dann ist $F \simeq \mathbb{Z}^r = \mathbb{Z} \times ... \times \mathbb{Z}$ (r Faktoren) eine direkte Summe unendlicher zyklischer Gruppen.*

Satz 1.27 *Jede endliche abelsche Gruppe ist eine direkte Summe endlicher zyklischer Gruppen.*

Der oben bewiesene Hauptsatz ist eine reine Existenzaussage. Es gibt aber auch Eindeutigkeitsaussagen:

Satz 1.28 *Für die abelsche Gruppe G gelte*

$$G = T_1 \times \mathbb{Z}^{r_1} \text{ und } G = T_2 \times \mathbb{Z}^{r_2}$$

mit endlichen Gruppen $T_1, T_2 \subset G$. Dann ist $r_1 = r_2$.

Beweis. Beweis $r_1 = r_2$ ist die kleinste Anzahl von Erzeugenden für die freie Gruppe A/T. □

Die Zerlegung der Torsions-Untergruppe T in endliche zyklische Gruppen ist wegen Satz 1.15 allerdings nicht eindeutig.

Beispiel 1.15 (F 01, T2, A1) *: Es sei $N \subset \mathbb{Z}^4$ die von*

$$n_1 = (4, 3, 2, 1),\ n_2 = (1, 2, 3, 4),\ n_3 = (-1, -1, -2, 2)$$

erzeugte Untergruppe. Man schreibe $\mathbb{Z}^4/N$ als Produkt zyklischer Gruppen.

Lösung: Wir fassen die Erzeugenden von N zu einer 3×4-Matrix zusammen:

$$\begin{pmatrix} 4 & 3 & 2 & 1 \\ 1 & 2 & 3 & 4 \\ -1 & -1 & -2 & 2 \end{pmatrix}.$$

Ohne die Untergruppe N zu ändern, können wir an dieser Matrix elementare Zeilenumformungen vornehmen. Wir ziehen n_2 viermal von n_1 ab und addieren n_2 zu n_3:

$$\begin{pmatrix} 0 & -5 & -10 & -15 \\ 1 & 2 & 3 & 4 \\ 0 & 1 & 1 & 6 \end{pmatrix}.$$

Wir addieren die dritte Zeile fünf mal zur ersten und ziehen sie zwei mal von der zweiten ab:

$$\begin{pmatrix} 0 & 0 & -5 & 15 \\ 1 & 0 & 1 & -8 \\ 0 & 1 & 1 & 6 \end{pmatrix}.$$

Durch Vertauschen können wir noch Zeilen-Stufen-Form erreichen

$$\begin{pmatrix} 1 & 0 & 1 & -8 \\ 0 & 1 & 1 & 6 \\ 0 & 0 & -5 & 15 \end{pmatrix}.$$

Jetzt ist die Matrix so schön geworden, wie man es sich nach Zeilen-Umformungen nur wünschen kann.

Nun wenden wir elementare Spalten-Umformungen an. Auch das ist erlaubt. So können wir alle Zeilen reinigen und die Matrix in die Form

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -5 & 0 \end{pmatrix}$$

bringen. Jetzt sehen wir

$$\mathbb{Z}^4/N = (\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z})/(\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \cdot 5 \times 0) = \mathbb{Z}_5 \times \mathbb{Z}.$$

Aufgabe 1.25 *Es sei $(i_1, i_2, ..., i_5) \in S_5$ ein Fünferzyklus und $(j_1, j_2) \in S_5$ eine Transposition. Zeigen Sie, dass beide Permutationen zusammen die ganze symmetrische Gruppe S_5 erzeugen.*

Aufgabe 1.26 *Bestimmen Sie alle abelschen Gruppen der Ordnung 72.*

Aufgabe 1.27 (F 99, T3, A1) *Seien U und V Untergruppen der endlichen Gruppe G mit $U \cap V = \{1\}$. Es bezeichne $< U \cup V >$ die von $U \cup V$ erzeugte Untergruppe von G. Man zeige:*

a) $|U||V| \leq | < U \cup V > |$.

b) In a) gilt Gleichheit, wenn U Normalteiler von G ist.

c) Man gebe eine Gruppe G mit zwei Untergruppen U und V mit $U \cap V = \{1\}$ an, so dass in a) nicht Gleichheit besteht.

Aufgabe 1.28 (H 95, T3, A2) *a) Zeigen Sie, dass jede abelsche Gruppe der Ordnung 1995 zyklisch ist.*

b) Geben Sie eine nichtabelsche Gruppe der Ordnung 1995 an.

Aufgabe 1.29 (F 93, T1, A1) *Geben Sie alle Isomorphieklassen von abelschen Gruppen der Ordnung 240 an.*

Aufgabe 1.30 (F 93, T2, A1) *Es seien N eine natürliche Zahl, G eine abelsche Gruppe der Ordnung 2^N und A die Anzahl der Elemente der Ordnung 2 in G.*

a) Ist die Anzahl s der Faktoren in der Zerlegung von G in ein direktes Produkt zyklischer Gruppen eindeutig durch A bestimmt?

b) Ist der Isomorphietyp von G eindeutig durch A bestimmt?

1.5 Sylow-Untergruppen

Jede endliche abelsche Gruppe A ist ein Produkt zyklischer Gruppen (Satz 1.27)

$$A = A_1 \times ... \times A_k, \quad A_l \simeq \mathbb{Z}_{n_l}.$$

Wegen Satz 1.15 können wir diese zyklischen Faktoren wieder als Produkte von zyklischen Gruppen schreiben, deren Ordnungen eine Primzahlpotenz p^k sind. Fassen wir dann alle zyklischen Gruppen zusammen, deren Ordnungen Potenzen der gleichen Primzahl sind, so finden wir

$$A = A_1 \times ... \times A_k, \quad |A_l| = p_l^{q_l}, \quad p_i \neq p_j \text{ falls } i \neq j.$$

Dabei ist die Ordnung $|A|$ von A das Produkt $p_1^{q_1} \cdot ... \cdot p_k^{q_k}$.

Insbesondere gibt es zu jeder Primzahl p_l, welche die Ordnung $|A|$ teilt, eine Untergruppe $A_l \subset A$ der Ordnung $p_l^{q_l}$. Diese Untergruppe muss natürlich nicht unbedingt zyklisch sein.

Definition 1.22 *Eine endliche Gruppe heißt p-Gruppe zur Primzahl p, wenn ihre Ordnung eine Potenz p^q ist.*

Satz 1.29 *Jede* abelsche *p-Gruppe A enthält Untergruppen der Ordnung p^l, jeder Potenz von p, welche die Gruppenordnung p^k teilt.*

Beweis. Weil A ein Produkt zyklischer Gruppen ist, brauchen wir die Aussage nur für eine zyklische Gruppe $A \simeq \mathbb{Z}_{p^k}$ zu zeigen. Sei etwa p^l eine Primzahlpotenz mit $1 \leq l \leq q$. Wir betrachten den Homomorphismus

$$\mathbb{Z}_{p^k} \to \mathbb{Z}_{p^{k-l}}, \quad a \mapsto p^l \cdot a.$$

sein Kern hat die Ordnung p^l. □

Diese Aussagen zeigen wir jetzt auch für nicht-abelsche endliche Gruppen.

Wir brauchen einige Voraussetzungen über die Konjugations-Abbildung $G \to G$, $g \mapsto hgh^{-1}$.

Definition 1.23 *Zwei Elemente $g_1, g_2 \in G$ heißen* konjugiert, *wenn es ein $h \in G$ gibt mit $g_2 = hg_1h^{-1}$.*

Diese Konjugiertheit ist eine Äquivalenz-Relation auf G:
Reflexivität: $g = ege^{-1}$.
Symmetrie: $g_2 = hgh^{-1} \Rightarrow g_1 = h^{-1}g_2h$.
Transitivität: $g_2 = h_1g_1h_1^{-1}$ und $g_3 = h_2g_2h_2^{-1} \Rightarrow g_3 = h_2h_1g_1h_1^{-1}h_2^{-1} = h_2h_1g_1(h_2h_1)^{-1}$.
Die Gruppe G zerfällt also in Äquivalenzklassen unter dieser Relation. Diese Klassen heißen *Konjugations-Klassen* oder einfach *Klassen*. Die Konjugations-Klasse eines Elementes $g \in G$ besteht also aus allen Elementen hgh^{-1}, wo h alle Gruppen-Elemente in G durchläuft. Diese Klasse bezeichnen wir mit C_g.

Beispiel 1.16 *Die Konjugations-Klasse des neutralen Elements besteht wegen $heh^{-1} = e$ nur aus diesem neutralen Element.*

Sei G die symmetrische Gruppe S_3. Außer der Klasse des neutralen Elements gibt es noch die beiden Klassen

$$\{(1,2),(1,3),(2,3)\}, \quad \{(1,2,3),(1,3,2)\}.$$

Definition 1.24 *Ein Gruppen-Element $z \in G$ heißt* zentral, *wenn es mit allen Gruppen-Elementen kommutiert:*

$$hz = zh \text{ für alle } h \in G.$$

die Menge $Z \subset G$ aller zentralen Elemente heißt das Zentrum *von G.*

Dass $z \in G$ zentral ist, das ist äquivalent zu $hzh^{-1} = z$ für alle $h \in G$. D.h.: Die Klasse von z besteht nur aus diesem einen Element z.

Das Zentrum $Z \subset G$ ist eine Untergruppe von G. Sie ist abelsch und bildet einen Normalteiler in G.

Beweis: $e \in Z$ ist klar. Falls $z_1, z_2 \in Z$, dann ist für alle $h \in G$:

$$h(z_1 z_2)h^{-1} = (hz_1h^{-1})(hz_2h^{-1}) = h_1h_2.$$

Wenn $z \in Z$, dann gilt für alle $h \in G$ dass $hzh^{-1} = z$ und, invers dazu, $z^{-1} = hz^{-1}h^{-1}$. □

Die Gruppe G operiert durch Konjugation

$$G \ni k : \; hgh^{-1} \mapsto khgh^{-1}k^{-1}$$

auf jeder Klasse. Diese Operation ist sogar transitiv. Wir wollen Satz 1.2 auf diese Operation anwenden. Dazu brauchen wir die Standgruppe

$$Z_g = \{h \in G : \; hgh^{-1} = g\}$$

des Elementes $g \in G$. Sie enthält die Gruppen-Elemente, welche mit g kommutieren. Man sieht sofort: $Z_g \subset G$ ist eine Unter-Gruppe.

Definition 1.25 *Die Untergruppe $Z_g \subset G$ heißt der* Zentralisator *des Elements g.*

Jetzt können wir Satz 1.2 anwenden. Falls G endlich ist, folgt

$$|G| = |C_g| \cdot |Z_g|,$$

oder

$$|C_g| = [G : Z_g].$$

Weil G die disjunkte Vereinigung der Konjugations-Klassen ist, ist die Gruppen-Ordnung die Summe aller Zahlen $|C_g|$, wobei g Repräsentanten aller verschiedenen Klassen durchläuft. Daraus folgt

Satz 1.30 (Klassen-Gleichung) *Für jede endliche Gruppe G mit Zentrum Z ist*

$$|G| = |Z| + \sum_g |C_g| = |Z| + \sum_g [G : Z_g].$$

Dabei durchläuft g in der Summe Repräsentanten aller verschiedenen Klassen, die mehr als ein Element enthalten.

Beipiel: $|S_3| = 6 = 1 + 2 + 3$, wo 1 die Ordnung des Zentrums $\{id\}$, zwei die Länge der Klasse $\{(1,2,3),(1,3,2)\}$ und 3 die Länge der Klasse $\{(1,2),(1,3),(2,3)\}$.

Eine typische Anwendung dieser Klassengleichung ist

Satz 1.31 *a) Jede endliche, nicht notwendig abelsche, p-Gruppe hat ein nicht-triviales Zentrum*
b) Jede Gruppe, deren Ordnung ein Quadrat p^2 einer Primzahl ist, ist abelsch.

Beweis. a) Die Gruppe G operiert vermöge Konjugation transitiv auf jeder Klasse C_g. Die Anzahl $|C_g|$ der Elemente in dieser Klasse ist ein Quotient von $|G| = p^k$ und damit wieder eine Potenz der Primzahl p. Entweder ist also $C_g = g$ oder $|C_g|$ ist durch p teilbar. Aus der Klassengleichung folgt, dass $|Z|$ durch p teilbar sein muss. Es gibt also mindestens p Elemente im Zentrum.

b) Nach a) hat die Gruppe ein nicht-triviales Zentrum Z. Dessen Ordnung $|Z|$ ist ein Teiler von p^2. Wenn $|Z| = p^2 = |G|$ ist, dann muss $G = Z$ abelsch sein. Wir können also annehmen $|Z| = p$. Der Quotient G/Z ist zyklisch und hat die Ordnung p, ist also isomorph zur zyklischen Gruppe $\mathbb{Z}_p$. Wir wählen ein erzeugendes Element $g' \in G/Z$ und davon ein Urbild $g \in G$. Dieses Element kann nicht die Ordnung p^2 haben, denn sonst wäre $G =< g >$ zyklisch. Also hat g die Ordnung p und erzeugt eine Untergruppe $H \subset G$ der Ordnung p. Wir betrachten die Abbildung des direkten Produkts

$$Z \times H \to G, \quad (z,h) \mapsto z \cdot h.$$

Wegen

$$(z_1 h_1)(z_2 h_2) = z_1 z_2 \cdot h_1 h_2$$

ist diese Abbildung ein Gruppenhomomorphismus. Weil sein Bild Z und das Element g enthält, ist er surjektiv. Weil $Z \times H$ und G beide die Ordnung p^2 haben, ist er auch injektiv und damit ein Isomorphismus. $G \simeq \mathbb{Z}_p \times \mathbb{Z}_p$ war eben doch abelsch. □

Satz 1.32 (Sylow I) *Teilt eine Primzahl-Potenz p^k die Ordnung $|G|$ der endlichen Gruppe G, so enthält G eine Untergruppe dieser Ordnung p^k.*

Beweis (Induktion nach $|G|$). Man unterscheidet zwei Fälle. Der einfachere Fall ist, dass p die Ordnung des Zentrums Z teilt. Dann enthält die abelsche Gruppe Z eine zyklische Untergruppe $\mathbb{Z}_p$. Alle ihre Elemente kommutieren mit allen Elementen $g \in G$. Deswegen ist $Z_p \subset G$ ein Normalteiler. Wir betrachten die Restklassen-Abbildung

$$G \to G/\mathbb{Z}_p.$$

Die Ordnung von $G/\mathbb{Z}_p$ ist $|G|/p$, kleiner als die Ordnung von G. Die Primzahl-Potenz p^{k-1} teilt die Ordnung $|G/\mathbb{Z}_p|$. Nach Induktions-Annahme enthält $G/\mathbb{Z}_p$ eine Untergruppe der Ordnung p^{k-1}. Ihr Urbild in G ist eine Untergruppe der Ordnung $p \cdot p^{k-1} = p^k$.

Der kompliziertere Fall liegt vor, wenn p die Ordnung $|Z|$ des Zentrums nicht teilt. Wir betrachten die Klassen-Gleichung. Die Ordnung $|G|$ ist teilbar durch p, die Ordnung $|Z|$ nicht.

Dann können nicht alle Längen $[G : C_g]$ durch p teilbar sein. Es gibt also mindestens ein $g \in G, g \notin Z$, derart, dass $[G : C_g]$ nicht durch p teilbar ist. Weil p die Gruppenordnung

$$|G| = |Z_g| \cdot |C_g|$$

teilt, muss die Ordnung $|Z_g|$ des Zentralisators Z_g durch p^k teilbar sein. Wegen $g \notin Z$ ist Z_g eine echte Untergruppe von G und hat kleinere Ordnung. Nach Induktion folgt: Es gibt eine Untergruppe der Ordnung p^k in $Z_g \subset G$. □

Definition 1.26 *Es sei G eine endliche Gruppe und p^k eine maximale Primzahl-Potenz, die die Gruppen-Ordnung teilt. Das heißt also $|G| = p^k \cdot m$, wo p die Zahl m nicht teilt. Nach Satz 1.32 gibt es eine Untergruppe der Ordnung p^k von G. Jede solche Gruppe heißt* Sylow-p-Untergruppe *von G.*

Jedes $g \in G$ definiert die Konjugations-Abbildung

$$G \to G, \quad h \mapsto ghg^{-1}.$$

Dies ist ein Automorphismus von G. Jede Sylow-p-Untergruppe S wird deswegen wieder auf eine solche Sylow-p-Untergruppe $gSg^{-1} \subset G$ abgebildet.

Satz 1.33 (Sylow II) *Es sei G eine endliche Gruppe, $H \subset G$ eine Untergruppe, deren Ordnung durch p teilbar ist, und $S \subset G$ eine Sylow-p-Untergruppe. Dann gibt es ein g aus G so, dass $H \cap gSg^{-1}$ eine Sylow-p-Untergruppe von H ist.*

Beweis. Wir betrachten die Menge M der Links-Nebenklassen zu S:

$$M = \{gS : g \in G\}.$$

Auf dieser Menge M operiert G durch Links-Translation:

$$h \in G,\, gS \in M \quad \mapsto \quad hgS \in M.$$

Diese Operation ist transitiv, weil die Links-Translation von G auf sich selbst transitiv ist. Wir bestimmen die Stabilisator-Gruppe G_m des Elements $m := eS = S \in M$. Es ist $gS = S$ genau dann wenn $g \in S$. Also ist $G_m = S$. Aus dem Bahnensatz (Satz 1.2) folgt

$$|M| = |G|/|S| = |G|/p^k$$

ist nicht durch p teilbar.

Jetzt betrachten wir die Operation von $H \subset G$ auf M. Dabei zerfällt M in H-Bahnen, auf denen H transitiv operiert. Weil $|M|$ nicht durch p teilbar ist, können nicht alle diese H-Bahnen eine durch p teilbare Länge haben. Sei etwa die Länge der H-Bahn von $m_1 = g_1 S$ nicht durch p teilbar. Die Stabilisator-Untergruppe in G von m_1 ist $g_1 S g_1^{-1}$ und in H die Untergruppe $g_1 S g_1^{-1} \cap H$. Der Bahnensatz für die transitive Operation von H auf der Bahn von $g_1 S$ zeigt:

$$[H : H \cap g_1 S g_1^{-1}] = |H - \text{Bahn von } m_1|$$

ist nicht durch p teilbar.

Nun ist $g_1 S g_1^{-1}$ ebenso wie S eine Gruppe der Ordnung p^k. Die Ordnung der Untergruppe $H \cap g_1 S g_1^{-1}$ ist ein Teiler p^l von p^k. Weil der Index $[H : h \cap g_1 S g_1^{-1}]$ nicht durch p teilbar ist, ist die Untergruppe $H \cap g_1 S g_1^{-1} \subset H$ maximal mit der Eigenschaft, dass ihre Ordnung eine p-Potenz ist. Nach Voraussetzung ist die Ordnung $|H|$ durch p teilbar. Also ist $l \geq 1$ und $H \cap g_1 S g_1^{-1}$ eine Sylow-p-Untergruppe von H. □

Satz 1.34 (Korollar) *Die Gruppe G sei endlich.*

a) Je zwei Sylow-p-Untergruppen von G sind konjugiert.

b) Jedes Element $g \in G$, dessen Ordnung eine Potenz p^l, $l > 0$, ist, ist in einer Sylow-p-Untergruppe enthalten.

Beweis. a) Es seien $S_1, S_2 \subset G$ zwei Sylow-p-Untergruppen. Wir setzen in Satz 1.33 $S := S_1$ und $H := S_2$. Dann ist H eine Sylow-p-Untergruppe von sich selbst, sogar die einzige. Es gibt ein $g \in G$ mit $g S_1 g^{-1} \cap H = H = S_2$. Weil die Gruppen $g S_1 g^{-1}$ ind S_2 die gleiche Ordnung haben, folgt $S_2 = g S_1 g^{-1}$.

b) Die von g in G erzeugte Untergruppe $< g >$ hat die Ordnung p^l. Es sei $S \subset G$ eine Sylow-p-Untergruppe. Wir setzen $H :=< g >$. Wieder ist H die einzige Sylow-p-Untergruppe von sich selbst, und nach Satz 1.33 gibt es ein $g \in G$ mit $g \in H \subset g S g^{-1}$. □

Definition 1.27 *Es sei $H \subset G$ eine Untergruppe. Dann heißt*

$$N(H) = N_G(H) := \{g \in g : g H g^{-1} = H\}$$

der Normalisator *von H in G.*

Satz 1.35 (Normalisator) *Der Normalisator $N_G(H)$ ist eine Untergruppe von G. Diese Untergruppe enthält H als Normalteiler. (Deswegen der Name Normalisator).*

Beweis: Falls $g_1, g_2 \in N(H)$, dann ist $g_1 H g_1^{-1} = g_2 H g_2^{-1} = H$ und

$$g_1 g_2 H (g_1 g_2)^{-1} = g_1 \cdot g_2 H g_2^{-1} \cdot g_1^{-1} = g_1 \cdot H \cdot g_1^{-1} = H,$$

also $g_1 g_2 \in N_G$. Für alle $g \in N_G$ ist

$$g^{-1} \cdot H \cdot g = g^{-1} \cdot g H g^{-1} \cdot g = H,$$

also auch $g^{-1} \in N_G$.

Wenn $h \in H$ liegt, ist $hHh^{-1} = Hh^{-1} = H$, also ist $H \subset N_H$ eine Untergruppe. Diese Untergruppe ist normal in N_H nach der Definition von N_H. □

Satz 1.36 (Sylow III) *Es sei G eine endliche Gruppe der Ordnung $|G| = p^k \cdot m$ so, dass p die Zahl m nicht teilt. Für die Anzahl s der Sylow-p-Untergruppen gilt dann:*

i) s teilt m: $s|m$.

ii) p teilt $s - 1$: $s \equiv 1 \, mod \, p$.

Beweis. i) Es sei $S \subset G$ eine Sylow-p-Untergruppe. Alle Sylow-p-Untergruppen sind nach Sylow II konjugiert. Deswegen operiert G durch Konjugation auf der Menge dieser Sylow-Gruppen transitiv. Der Stabilisator von S unter dieser Operation ist gerade der Normalisator $N_G(S)$. Aus dem Bahnensatz 1.2 folgt

$$s = |G|/|N_G(S)|.$$

Wegen $S \subset N_G(S)$ teilt p^k die Ordnung von $N_G(S)$ und s muss ein Teiler von m sein.

ii) Jetzt betrachten wir die Operation von S auf der Menge $M = \{S = S_1, S_2, ...\}$ aller Sylow-p-Untergruppen durch Konjugation

$$s : S_i \mapsto sS_is^{-1}.$$

M zerfällt dabei in Bahnen. Wegen $sSs^{-1} = s$ für alle $s \in S$ ist die ein-elementige Menge $\{S\}$ eine dieser Bahnen. Sie ist aber auch die einzige Bahn, die nur aus einem Element besteht: Wenn $sS_is^{-1} = S_i$ für alle $s \in S$, dann gehört S, ebenso wie S_i zum Normalisator $N_G(S_i)$. Sowohl S als auch S_i sind Sylow-p-Untergruppen von $N_G(S_i)$ und nach Sylow II in $N_G(S_i)$ konjugiert. Weil aber S_i normal in $N_G(S_i)$ ist, muss $S = S_i$ sein.

Alle anderen Bahnen, außer $\{S\}$ bestehen also aus mehr als einem Element. Weil die Länge einer Bahn immer ein Teiler von $|S| = p^k$ ist, teilt p die Länge jeder dieser Bahnen. Es folgt $s \equiv 1 \, mod \, p$. □

Beispiel 1.17 (F 01, T2, A 2i) *: Es sei G eine Gruppe der Ordnung 63. Man zeige, dass G einen nicht-trivialen Normalteiler hat.*

Die Primzahl-Potenz-Zerlegung der Gruppen-Ordnung ist

$$63 = 7 \cdot 3^2.$$

Die Gruppe enthält also Sylow-Untergruppen der Ordnungen 7 und 9. Für deren Anzahl sagt Sylow III

Ordnung	*Anzahl s*
7	$s \mid 9 \quad s \equiv 1 \, mod \, 7$
9	$s \mid 7 \quad s \equiv 1 \, mod \, 3$

Es gibt also genau eine Sylow-7-Untergruppe und entweder eine oder sieben Sylow-3-Untergruppen. Alle Konjugierten der Sylow-7-Untergruppe stimmen mit dieser Untergruppe überein. Sie ist ein Normalteiler.

Aufgabe 1.31 *Zeigen Sie, dass die symmetrische Gruppe S_4 eine Untergruppe der Ordnung 6 besitzt, die alternierende Gruppe A_4 jedoch nicht.*

Aufgabe 1.32 *Es sei $G \subset S_4$ eine Untergruppe, die auf der Menge $\{1, 2, 3, 4\}$ transitiv operiert. Zeigen Sie, dass G in S_4 konjugiert zu einer der folgenden fünf Gruppen ist:*

i) Kleinsche Vierergruppe $V_4 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$;

ii) zyklische Gruppe $< (1,2,3,4) > \simeq \mathbb{Z}_4$*;*

iii) 2*-Sylow-Untergruppe* $\simeq D_4$*;*

iv) alternierende Gruppe A_4*;*

v) symmetrische Gruppe S_4*.*

Aufgabe 1.33 (F 01, T3, A2) *Zeigen Sie* $N_G(N_G(P)) = N_G(P)$ *für eine* p*-Sylowuntergruppe* P *der endlichen Gruppe* G*.*

Aufgabe 1.34 (H 00, T1, A1) *Sei* G *eine Gruppe mit 2001 Elementen. Zeigen Sie:*
a) Die p*-Sylowgruppen von* G *sind für* $p = 23$ *und* $p = 29$ *normal.*
b) Auch die 3*-Sylowgruppe von* G *ist normal.*
c) Die Gruppe G *ist zyklisch.*

Aufgabe 1.35 (F 00, T2, A1) *Man entscheide, für welche* $n = 2, 3, 4$ *die symmetrische Gruppe* S_n *eine nichttriviale normale Sylowuntergruppe besitzt.*

Aufgabe 1.36 (F 00, T3, A2) *Zeigen Sie, dass eine endliche Gruppe mit einem Normalteiler, dessen Ordnung gleich dem kleinsten Primteiler ihrer Ordnung ist, ein nichttriviales Zentrum hat. (Hinweis: Man betrachte die Operation der Gruppe auf dem Normalteiler durch Konjugation.)*

Aufgabe 1.37 (H 99, T1, A1) *Sei* p *eine Primzahl. Wie viele* p*-Sylow-Untergruppen besitzt die symmetrische Gruppe* S_p*?*

Aufgabe 1.38 (H 99, T2, A1) *a) Sei* $p \in \mathbb{N}$ *eine Primzahl und* G *eine nichttriviale endliche* p*-Gruppe. Man beweise, dass das Zentrum von* G *nichttrivial ist.*
b) Man konstruiere eine nicht-abelsche Gruppe G *der Ordnung 27, in der jedes Element* $x \in G \setminus 1$ *die Ordnung 3 hat.*

Aufgabe 1.39 (H 98, T2, A1) *Sei* G *eine endliche Gruppe, seien* P *eine* p*-Sylowuntergruppe und* U *eine weitere Untergruppe von* G*. Zeigen Sie:*
a) Ist U *oder* P *normal, so ist* $P \cap U$ *eine* p*-Sylowuntergruppe von* U*.*
b) Ist P *nicht normal, so gibt es eine Untergruppe* U*, so dass* $P \cap U$ *keine* p*-Sylowuntergruppe von* U *ist.*

Aufgabe 1.40 (F 95, T1, A2b)) *Sei* G *eine Gruppe der Ordnung 196. Dann besitzt* G *eine normale* 7*-Sylowuntergruppe* P*, und der kanonische Epimorphismus* $G \to G/P$ *ist zerfallend. (Vgl. Aufgabe 1.10)*

Aufgabe 1.41 (F 95, T2, A2) *a) Sei* G *eine einfache Gruppe der Ordnung 60. Man zeige, dass* G *genau sechs 5-Sylowuntergruppen und 24 Elemente der Ordnung 5 hat.*
b) Man zeige, dass es in jeder Gruppe der Ordnung 56 nichttriviale Normalteiler gibt.

Aufgabe 1.42 (F 95, T3, A1) *Sei G eine Gruppe der Ordnung 300. Zeigen Sie, dass G nicht einfach ist. (Hinweis: Lassen Sie die Gruppe G auf der Menge ihrer 5-Sylowgruppen operieren.)*

Aufgabe 1.43 (F 94, T1, A1b)) *Es sei n ungerade und $n > 1$. Zeigen Sie: Die Menge der Zyklen der Länge n von A_n zerfällt in genau zwei Konjugiertenklassen, von denen jede $\frac{1}{2}(n-1)!$ Elemente enthält.*

Aufgabe 1.44 (H 93, T1, Teil von A3) *Zur Notation vgl. Aufgabe 1.4. Zeigen Sie: Genau dann ist $\#G_2 = 2$, wenn die 2-Sylowgruppe von G zyklisch und $\neq 0$ ist.*

Aufgabe 1.45 (F 93, T3, A2) *a) Es sei p eine Primzahl. Bekanntlich ist jede Gruppe der Ordnung p^2 abelsch. Man gebe die Isomorphietypen aller Gruppen der Ordnung p^2 an.*

b) Für jede Gruppe der Ordnung p^2 bestimme man die Automorphismengruppe und ihre Ordnung.

c) Es seien p und q Primzahlen mit $2 < p < q$ und p kein Teiler von $q^2 - 1$. Es sei G eine gruppe der Ordnung p^2q^2. Man beweise, dass G genau eine p-Sylowgruppe besitzt.

d) Man beweise, dass die Gruppe G aus c) abelsch ist.

Aufgabe 1.46 (H 92, T2, A3) *Es sei G eine endliche Gruppe mit $|G| = k$, und es sei P die Menge aller Produkte $g_1g_2...g_k$ aller Elemente von G. Zeigen Sie:*

a) P ist eine Vereinigung von Konjugiertenklassen von G.

b) Ist G kommutativ und k ungerade, so ist $P = \{1\}$.

c) Ist G die symmetrische Gruppe S_3, so ist P die Menge der Transpositionen.

Aufgabe 1.47 (H 92, T3, A2) *Man bestimme die Isomorphieklassen von Gruppen der Ordnung 1225.*

Aufgabe 1.48 (H 90, T3, A1) *a) Man bestimme die Struktur und die Anzahl der 2-Sylowgruppen der symmetrischen Gruppe S_5.*

b) Man bestimme die Anzahl der 5-Sylowgruppen von S_5.

c) Besitzt S_5 eine Untergruppe der Ordnung 15?

d) Besitzt S_5 zwei zueinander nicht isomorphe Untergruppen der Ordnung 6?

Aufgabe 1.49 (F 90, T2, A1) *G sei eine endliche Gruppe, in der Elemente teilerfremder Ordnung stets miteinander vertauschbar sind. Zeigen Sie: G ist das direkte Produkt von Sylow-Gruppen.*

1.6 Auflösbare Gruppen

Auflösbare Gruppen sind an sich sehr langweilig. Aber sie sind wichtig, weil die Auflösbarkeit einer Polynom-Gleichung zur Auflösbarkeit einer Gruppe äquivalent ist.

Definition 1.28 *Es seien G eine Gruppe und $g, h \in G$ zwei Elemente. Das Produkt*

$$g^{-1}h^{-1}gh \in G$$

heißt ein Kommutator.

Beispiel 1.18 *Der Kommutator der Permutationen $(1,2)$ und $(1,3) \in S_3$ ist*

$$(1,2)(1,3)(1,2)(1,3) = (1,3,2)(1,3,2) = (1,2,3).$$

Falls g und h kommutieren, d.h., $gh = hg$, dann ist auch $h^{-1}g = gh^{-1}, g^{-1}h^{-1} = h^{-1}g^{-1}$, und ihr Kommutator ist

$$g^{-1}h^{-1}gh = g^{-1}gh^{-1}h = e.$$

Davon gilt auch die Umkehrung: Aus $g^{-1}h^{-1}gh = e$ folgt $gh = hg$. Der Kommutator von g und h ist also das Hindernis dagegen, dass g und h kommutieren. Eine Gruppe ist abelsch, genau dann, wenn alle Kommutatoren mit dem Eins-Element übereinstimmen.

Ist $\varphi : G \to H$ ein Homomorphismus, so ist das Bild des Kommutators

$$\varphi(g^{-1}h^{-1}gh) = \varphi(g)^{-1}\varphi(h)^{-1}\varphi(g)\varphi(h)$$

der Kommutator der Bilder. Jeder Kommutator in einer abelschen Gruppe ist das Eins-Element e. Daraus folgt:

Satz 1.37 *Ist $\varphi : G \to A$ ein Homomorphismus der Gruppe G in die* abelsche *Gruppe A, so liegt jeder Kommutator von G im Kern von φ.*

Definition 1.29 *Es sei G eine Gruppe. Die* abgeleitete Gruppe *oder* Kommutatorgruppe *G' von G ist die Untergruppe von G, welche von allen Kommutatoren in G erzeugt wird.*

Beispiel 1.19 *Die symmetrische Gruppe S_n lässt den signum-Homomorphismus in die abelsche Gruppe $\mathbb{Z}_2$ zu. Die abgeleitete Gruppe von S_n ist also im Kern dieses Homomorphismus, der alternierenden Gruppe A_n enthalten.*

Insbesondere liegt die abgeleitete Gruppe von S_3 in der alternierenden Gruppe $A_3 = <(1,2,3)>$. Oben haben wir ausgerechnet, dass $(1,2,3)$ ein Kommutator in S_3 ist. Also stimmt die abgeleitete Gruppe von S_3 mit der Untergruppe A_3 überein.

Satz 1.38 *a) Die abgleitete Gruppe G' einer Gruppe G ist ein Normalteiler in G, und der Quotient G/G' ist abelsch.*

b) Ist $\varphi : G \to A$ ein Morphismus von G in eine abelsche Gruppe A, so gibt es einen Morphismus $\psi : G/G' \to A$ so, dass das Diagramm

$$\begin{array}{ccc} & & G/G' \\ & \overset{\psi}{\nearrow} & \downarrow \\ G & \xrightarrow{\varphi} & A \end{array}$$

kommutiert.

Beweis. a) Bei der Konjugation $G \to G$, $g \mapsto aga^{-1}$ geht jeder Kommutator $g^{-1}h^{-1}gh$ in den Kommutator

$$a(g^{-1}h^{-1}gh)a^{-1} = (ag^{-1}a^{-1})(ah^{-1}a^{-1})(aga^{-1})(aha^{-1}) = (aga^{-1})^{-1}(aha^{-1})^{-1}(aga^{-1})(aha^{-1})$$

über. Die Menge aller Kommutatoren wird also auf sich abgebildet, ebenso die von diesen Kommutatoren erzeugte Untergruppe G'.

b) Weil G' im Kern von φ liegt, folgt die Behauptung aus dem Homomorphiesatz 1.9. □

Definition 1.30 *Für $1 \leq k \in \mathbb{N}$ wird die k-te Kommutatorgruppe G^k induktiv wie folgt definiert: G^1 ist die abgeleitete Gruppe G' und G^k ist die abgeleitete Gruppe $(G^{k-1})'$ der $k-1$-ten Kommutatorgruppe G^{k-1}.*

Einer Gruppe G wird so eine ganze Reihe von Gruppen

$$G \supset G^1 \supset G^2 \supset ...$$

zugeordnet. Jede Gruppe in dieser Reihe ist Normalteiler in der vorhergehenden Gruppe und die sukzessiven Quotienten sind immer abelsch. Die so definierte Reihe von Gruppen heißt *Kommutator-Reihe* der Gruppe G.

Definition 1.31 *Eine* Normalreihe *der Gruppe G ist eine Reihe*

$$G \supset G_1 \supset G_2 \supset ...$$

von Untergruppen so, dass jede Gruppe G_k normal in der vorhergehenden Gruppe G_{k-1} ist.

Die Kommutator-Reihe einer endlichen Gruppe bricht nach endlich vielen Schritten ab. Es muss ein k_0 geben, so, dass $G^{k_0+1} = G^{k_0}$ ist. Dann ist $G^{k_0+l} = G^{k_0}$ für alle $l > 0$. Es kann sein, dass dies mit der trivialen Untergruppe geschieht: $G^k = \{1\}$ für ein $k > 0$, oder auch nicht.

Definition 1.32 *Eine Gruppe G heißt* auflösbar *wenn es ein $k \in \mathbb{N}$ gibt derart, dass die k-te abgeleitete Gruppe $G^k = \{1\}$ trivial ist.*

Satz 1.39 (Endliche auflösbare Gruppen) *Für eine endliche Gruppe G sind äquivalent:*

a) Die Gruppe G ist auflösbar.

b) Es gibt eine Normalreihe so, dass alle sukzessiven Faktorgruppen G_{l-1}/G_l abelsch sind, die mit $G_k = \{1\}$ abbricht.

c) Es gibt eine Normalreihe so, dass alle sukzessiven Faktorgruppen G_{l-1}/G_l zyklisch von Primzahl-Ordnung sind, die mit $G_k = \{1\}$ abbricht.

Beweis. a) $\Rightarrow$ b): Die Kommutator-Reihe einer auflösbaren Gruppe bricht mit $G^k = \{1\}$ und alle sukzessiven Quotienten sind abelsch.

b) $\Rightarrow$ c): Es genügt zu zeigen: Ist $G_l \subset G_{l-1}$ eine normale Untergruppe so, dass G_{l-1}/G_l endlich und abelsch ist, dann gibt es eine Reihe

$$G_{l-1} \supset H_1 \supset H_2 \supset ... \supset H_m = G_l,$$

so, dass jeder Quotient $H_{\mu-1}/H_\mu$ zyklisch von Primzahlordnung ist. Dies beweisen wir durch Induktion nach dem Index $[G_{l-1} : G_l]$.

Der Quotient $A := G_{l-1}/G_l$ ist nach Satz 1.27 eine direkte Summe zyklischer Gruppen. Jede zyklische Gruppe hat eine zyklische Faktor-Gruppe von Primzahl-Ordnung. Deswegen hat A eine zyklische Faktorgruppe, etwa $C := A/B$ von Primzahl-Ordnung. Es sei $H_1 \subset G_{l-1}$ das Urbild von B unter dem Morphismus $G_{l-1} \to G_{l-1}/G_l = A$. H ist normal in G_{l-1}. Nach dem Homomorphie-Satz 1.9 ist $G_{l-1}/H_1 = A/B = C$ zyklisch von Primzahlordnung. Wir haben eine Normal-Reihe

$$G_{l-1} \supset H_1 \supset G_l$$

gefunden, so, dass G_{l-1}/H_1 zyklisch von Primzahl-Ordnung ist, und $[H_1 : G_l] < [G_{l-1} : G_l]$. Nach Induktionsannahme gibt es eine Normal-Reihe

$$H_1 \supset H_2 \supset ... \supset H_m = G_l,$$

deren sukzessive Quotienten zyklisch von Primzahl-Ordnung sind. Setzen wir die beiden Reihen zusammen, so folgt die Behauptung.

c) $\Rightarrow$ a): Nach Voraussetzung gibt es eine Normal-Reihe

$$G \supset G_1 \supset G_2 \supset ... \supset G_k = \{1\},$$

deren sukzessive Quotienten abelsch sind. Weil G/G_1 abelsch ist, muss die abgeleitete Gruppe G^1 in G_1 enthalten sein. Die zweite abgeleitete Gruppe $G^2 = (G^1)'$ muss in G_1' enthalten sein, und weil G_1/G_2 abelsch ist, in G_2, usw. Die l-te abgeleitete Gruppe G^l ist Untergruppe von G_l. Insbesondere ist $G^k = G_k = \{1\}$. □

Beispiel 1.20 *Die symmetrische Gruppe $S_2 \simeq \mathbb{Z}_2$ ist abelsch, und damit auflösbar.*

Die symmetrische Gruppe S_3 besitzt den abelschen Normalteiler $A_3 \simeq \mathbb{Z}_3$ vom Index 2. Der Quotient S_3/A_3 ist deswegen abelsch, und S_3 ist auflösbar.

Die symmetrische Gruppe S_4 besitzt die Normalreihe

$$S_4 \subset A_4 \subset V_4$$

mit den sukzessiven Quotienten $\mathbb{Z}_2$ und $\mathbb{Z}_3$. Deswegen ist auch S_4 auflösbar.

Satz 1.40 *Ist die Gruppe G auflösbar, so ist dies auch jede Untergruppe und jede Faktorgruppe von G.*

Beweis. Es sei $H \subset G$ eine Untergruppe. Dann ist die k-te abgeleitete Gruppe H^k eine Untergruppe von G^k. Es gibt also ein k derart, dass $H^k = \{1\}$ trivial ist.

Es sei $H = G/N$ eine Faktorgruppe und $\varphi : G \to H$ der Restklassenhomomorphismus. Jeder Kommutator

$$h_1 h_2 h_1^{-1} h_2^{-1} = \varphi(g_1)\varphi(g_2)\varphi(g_1)^{-1}\varphi(g_2)^{-1} = \varphi(g_1 g_2 g_1^{-1} g_2^{-1}), \quad h_1 = \varphi(g_1), h_2 = \varphi(g_2)$$

ist Bild eines Kommutators aus G. Deswegen ist die abgeleitete Gruppe H' das Bild der abgeleiteten Gruppe G'. Es ist also H' eine Faktorgruppe $G'/(G' \cap N)$ von G'. Induktiv folgt, dass die k-te abgeleitete Gruppe H^k eine Faktorgruppe von G^k ist. Es gibt also ein k derart, dass $H^k = \{1\}$ trivial ist. □

Eine einfache, nicht-abelsche Gruppe G kann nie auflösbar sein: Der Normalteiler G' kann nicht die triviale Untergruppe $\{1\}$ sein, denn dann wäre G abelsch. Also ist $G' = G$, und dann auch $G^k = G$ für alle k.

Satz 1.41 (Galois) *Für $n \geq 5$ ist die alternierende Gruppe A_n einfach.*

Beweis. Wir müssen zeigen, jeder Normalteiler $N \subset A_n$, $N \neq \{1\}$, stimmt mit der ganzen Gruppe A_n überein. Mit jedem Element $\sigma \in N$ enthält der Normalteiler N auch jedes konjugierte Element $g\sigma g^{-1}$, $g \in A_n$.

Als erstes zeigen wir, dass N einen Dreier-Zyklus (i, j, k) enthält. Dazu nehmen wir ein Element $\sigma \in N$, $\sigma \neq id$ her, schreiben es in Zyklenschreibweise

$$\sigma = \sigma_1 \sigma_2 ...$$

und unterscheiden eine ganze Anzahl von Fällen:

1) Der erste Zyklus σ_1 hat eine Länge ≥ 5, etwa $\sigma_1 = (i_1, i_2, i_3, i_4, i_5, ...)$. Dann gehört zu N auch die Permutation

$$\tau := (i_2, i_3, i_4)\sigma_1\sigma_2...(i_2, i_4, i_3) = (i_1, i_3, i_4, i_2, i_5, ...)\sigma_2...,$$

sowie

$$\tau^{-1}\sigma = (..., i_5, i_2, i_4, i_3, i_1)(i_1, i_2, i_3, i_4, i_5, ...) = (i_1, i_4, i_2),$$

ein Dreier-Zyklus.

2) σ_1 ist ein Vierer-Zyklus, etwa $\sigma_1 = (i_1, i_2, i_3, i_4)$. Jetzt betrachten wir

$$\tau := (i_1, i_2, i_3)\sigma_1\sigma_2...(i_1, i_3, i_2) = (i_1, i_4, i_2, i_3)\sigma_2....$$

Zu N gehört dann auch

$$\tau^{-1}\sigma = (i_1, i_3, i_2, i_4)(i_1, i_2, i_3, i_4) = (i_1, i_4, i_3),$$

ein Dreier-Zyklus.

3) $\sigma_1 = (i_1, i_2), \sigma_2 = (i_3, i_4)$. Jetzt ist

$$\tau := (i_1, i_2, i_3)\sigma_1\sigma_2...(i_3, i_2, i_1) = (i_1, i_4)(i_2, i_3)... \in N.$$

Und

$$\tau^{-1}\sigma = (i_1, i_3)(i_2, i_4).$$

Der Normalteiler N enthält das Paar von Zweier-Zyklen $(i_1, i_3)(i_2, i_4)$. Wir wählen eine fünfte Zahl i_5 und berechnen

$$\rho := (i_3, i_4, i_5)\tau^{-1}\sigma(i_3, i_5, i_4) = (i_1, i_4)(i_2, i_5).$$

Dann enthält N den Fünfer-Zyklus

$$\rho\tau^{-1}\sigma = (i_1, i_4)(i_2, i_5)(i_1, i_3)(i_2, i_4) = (i_1, i_3, i_4, i_5, i_2).$$

Aus Fall 1) folgt, dass auch jetzt N einen Dreier-Zyklus enthält.

In allen behandelten Fällen enthält N einen Dreier-Zyklus. Nicht behandelt haben wir den Fall, dass der erste Zyklus σ_1 ein Dreier-Zyklus ist. Wenn $\sigma = \sigma_1$ ist, sind wir fertig. Andernfalls können wir durch Umordnen der Zyklen einen der Fälle 1)-3) herbeiführen, außer wenn σ nur aus Dreier-Zyklen aufgebaut ist, etwa

$$\sigma = (i_1, i_2, i_3)(i_4, i_5, i_6)\sigma_3....$$

Wir berechnen

$$\tau := (i_2, i_3, i_4)\sigma(i_2, i_4, i_3) = (i_1, i_3, i_4)(i_2, i_5, i_6)\sigma_3...$$

und

$$\tau^{-1}\sigma = (i_1, i_4, i_3)(i_2, i_6, i_5)(i_1, i_2, i_3)(i_4, i_5, i_6) = (i_1, i_6, i_3, i_4, i_2).$$

wir sind in Fall 1) gelandet.

Wir wissen also jetzt: N enthält einen Dreier-Zyklus, etwa (i_1, i_2, i_3). Den konjugieren wir mit

$$g = \begin{pmatrix} i_1 & i_2 & i_3 & i_4 & i_5 & ... \\ i & j & k & l & m & ... \end{pmatrix} \in S_n.$$

Falls g nicht zu A_n gehören sollte, ersetzen wir g durch

$$(l, m)g = \begin{pmatrix} i_1 & i_2 & i_3 & i_4 & i_5 & ... \\ i & j & k & m & l & ... \end{pmatrix} \in A_n,$$

und können o.B.d.A. $g \in A_n$ annehmen. Wir berechnen

$$g(i_1, i_2, i_3)g^{-1} = (i, j, k).$$

Deswegen enthält N jeden Dreier-Zyklus $(i, j, k) \in A_n$. Aus

$$(i, k, j)(i, j, k, l, ..., u) = (k, l, ..., u)$$

folgt durch Induktion nach der (ungeraden) Länge eines Zykels in A_n, dass jeder dieser Zyklen zu N gehört, und dass dann $N = A_n$ gilt. □

Aufgabe 1.50 *Zeigen Sie, dass die alternierende Gruppe A_5 einfach ist in folgenden Schritten:*

a) Bestimmen Sie alle Konjugationsklassen in A_5 und die Anzahlen der Elemente in diesen Klassen.

b) Zeigen Sie: Für jeden Normalteiler $N \subset A_5$ gibt es natürliche Zahlen $x, y, z \in \mathbb{N}$ mit

$$|N| = 1 + 12 \cdot x + 15 \cdot y + 20 \cdot z.$$

c) Bestimmen Sie mit b) alle Normalteiler von A_5.

Aufgabe 1.51 (H 00, T3, A1b)) *Sei G eine Gruppe der Ordnung 100. Zeigen Sie:*

i) G ist auflösbar.

ii) Hat G einen Normalteiler der Ordnung 4, so ist G abelsch.

(Es darf verwendet werden, dass Gruppen der Ordnung p^2 abelsch sind, wenn p eine Primzahl ist.)

Aufgabe 1.52 (H 99, T3, A1) *Seien p und q verschiedene Primzahlen. Man beweise, dass jede Gruppe der Ordnung pq^2 auflösbar ist.*

Aufgabe 1.53 (F 96, T2, A2) *a) Wieviele Isomorphieklassen von abelschen Gruppen der Ordnung 64 gibt es?*

b) Bestimmen Sie die kleinste natürliche Zahl n, so dass es genau 6 Isomorphieklassen von abelschen Gruppen der Ordnung n gibt.

Aufgabe 1.54 (H 94, T2, A1) *a) Sei N eine normale Untergruppe einer Gruppe G. Zeigen Sie: Sind die Faktorgruppe G/N und N auflösbar, so ist auch G auflösbar.*

b) Sei G eine nicht-triviale endliche p-Gruppe. Zeigen Sie: G besitzt ein nicht-triviales Zentrum und G ist auflösbar.

Aufgabe 1.55 (H 94, T3, A1) *Beweisen Sie: Jede Gruppe der Ordnung 297 ist auflösbar.*

Aufgabe 1.56 (F 02, T1, A3) *Es sei a ein Element der Ordnung $d > 1$ in der multiplikativen Gruppe des Körpers $\mathbb{Z}/p\mathbb{Z}$ und G die von den Abbildungen $\mu : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}\,(xmapstoax)$ und $\alpha : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}\,(x \mapsto x + 1)$ erzeugte Untergruppe der Permutationsgruppe von $\mathbb{Z}/p\mathbb{Z}$. Zeigen Sie:*

a) G ist nicht abelsch.

b) Jedes $g \in G$ besitzt eine eindeutige Darstellung $g = \mu^r \alpha^s$ $(0 \leq r < d, 0 \leq s < p)$.

c) G ist auflösbar.

d) Es gibt eine nicht abelsche Gruppe der Ordnung 555.

2 Ringe

2.1 Definitionen

Definition 2.1 *Ein* Ring *ist eine Menge R mit zwei Rechenstrukturen:*

1) der Struktur einer abelschen Gruppe. Die Verknüpfung bezeichnet man üblicherweise mit $+$, das neutrale Element mit 0.

2) einer zweiten Verknüpfung, die man üblicherweise als Multiplikation bezeichnet und $r, s \mapsto rs$ oder $r \cdot s$ schreibt.

Diese beiden Verknüpfungen sollen durch das Distributivgesetz

$$r(s+t) = rs + rt, \quad (s+t)r = sr + tr$$

verknüpft sein.

Aus dem Distributivgesetz folgt

$$0r = r0 = 0 \text{ für alle } r \in R.$$

Beweis. Es ist $0 = 0 - 0$ und deswegen

$$r0 = r(0-0) = r0 - r0 = 0, \quad 0r = (0-0)r = 0r - 0r = 0.$$

Hier beginnen sich schon die Geister zu scheiden: Die Kommutativität der Multiplikation, d.h. $rs = sr$ wird nicht immer vorausgesetzt. (Deswegen habe ich auch das Distributivgesetz in zwei Versionen hingeschrieben.) Wenn $rs = sr$ gilt für alle $r, s \in R$, dann nennt man den Ring *kommutativ*.

Noch schlimmer ist, dass man manchmal nicht einmal die Assoziativität der Multiplikation

$$(rs)t = r(st)$$

voraussetzt. Ich kann dieser Perversion allerdings nichts Positives abgewinnen. In dieser Vorlesungen wird also die Multiplikation in einem Ring stets assoziativ sein.

Der Ring kann ein neutrales Element für die Multiplikation enthalten, muss es aber nicht. So ein neutrales Element nennt man Eins-Element und schreibt es 1. Es erfüllt

$$1 \cdot r = r \cdot 1 = r \text{ für alle } r \in R.$$

Wenn es sowas gibt, nennt man den Ring einen Ring mit Eins.

Beispiel 2.1 *Die Mutter aller Ringe ist der Ring $\mathbb{Z}$ der ganzen Zahlen. Er ist ein kommutativer Ring mit Eins. Er zeigt schon die wesentliche Eigenschaft der Ringe: Inverse bezüglich der Multiplikation braucht es nicht zu geben! In $\mathbb{Z}$ haben nur die Zahlen ± 1 ein solches Inverses.*

Man kann modulo n addieren und multiplizieren. Die Menge $\mathbb{Z}_n = \{0, 1, ..., n-1\}$ mit dieser Addition und Multiplikation bildet auch einen Ring (kommutativ mit Eins).

Die Menge $M(n \times n, \mathbb{R})$ aller reellen $n \times n$-Matrizen ist ein Ring mit der üblichen Addition und Multiplikation von Matrizen. Für $n \geq 2$ ist dieser Ring nicht kommutativ, aber er hat ein Eins-Element: die Einheitsmatrix. Invertierbar in diesem Ring sind nur die invertierbaren Matrizen.

Die wichtigsten Beispiele für uns sind *Polynomringe*. Dazu sei R ein Ring und X eine Unbestimmte. (Was ist denn das?) Der Polynomring $R[X]$ besteht aus allen Polynomen

$$r_0 + r_1X + r_2X^2 + ... + r_nX^n, \quad n \in N, r_0, ..., r_n \in R.$$

Die größte Zahl n mit $r_n \neq 0$ heißt der *Grad* des Polynoms. (Formal kann man so ein Polynom mit der Folge $r_0, r_1, ..., r_n$ identifizieren. Aber man rechnet mit diesen Objekten eben wie mit Polynomen.) Die Summe zweier Polynome ist

$$(r_0 + r_1X + ...) + (s_0 + s_1X + ...) = r_0 + s_0 + (r_1 + s_1)X + ...$$

und das Produkt

$$(r_0 + r_1X + ...)(s_0 + s_1X + ...) = r_0s_0 + (r_0s_1 + r_1s_0)X + ...$$

Der Polynomring $R[X]$ ist kommutativ, wenn R das ist. Er hat eine Eins, wenn R eine hat. Nur Polynome vom Grad 0, d.h. also die Ringelemente, können invertierbar sein.

Polynome sind a priori endlich. Aber auch Potenzreihen können Ringe bilden. Man nennt

$$R[[X]] := \{\sum_{k=0}^{\infty} r_kX^k : \ r_k \in \mathbb{R}\}$$

den Ring der formalen Potenzreihen. Addition und Multiplikation ist wie bei normalen Potenzreihen definiert. Konvergenz spielt hier keine Rolle.

In ein Polynom $f \in R[X]$ kann man Ring-Elemente einsetzen:

$$f = r_0 + r_1X + ... + r_nX^n, \ a \in R \ \Rightarrow f(a) = r_0 + r_1a + ... + r_na^n \in R.$$

$a \in R$ heißt *Nullstelle* des Polynoms $f \in R[X]$, wenn das Resultat $f(a) = 0$ ist.

Satz 2.1 (Vieta) *Der Ring R sei kommutativ. Ist $a \in R$ eine Nullstelle des Polynoms $f \in R[X]$, so gibt es eine Faktorisierung*

$$f = (X - a) \cdot g \ \textit{mit} \ g \in R[X], \quad Grad(g) = Grad(f) - 1.$$

Beweis. Weil R kommutativ vorausgesetzt ist, gilt für jedes $k \in \mathbb{N}$

$$X^k - a^k = (X - a) \cdot (X^{k-1} + X^{k-2}a + ... + Xa^{k-2} + a^{k-1}) =: (X - a) \cdot q_{k-1}.$$

Aus $f(a) = 0$ folgt dann

$$\begin{aligned} f(X) &= f(X) - f(a) \\ &= \sum_{\nu=0}^{n} r_\nu X^\nu - \sum_{\nu=0}^{n} r_\nu a^\nu \\ &= \sum_{\nu=0}^{n} r_\nu \cdot (X^\nu - a^\nu) \\ &= \sum_{\nu=1}^{n} r_\nu (X - a) \cdot q_{\nu-1} \\ &= (X - a) \cdot \underbrace{\sum_{\nu=0}^{n-1} r_{\nu+1} q_\nu}_{g}. \end{aligned}$$

□

Nachdem wir nun die Rechenstruktur erklärt haben, müssen wir wie üblich Unter- und Quotientenstrukturen erklären.

Definition 2.2 *Eine Teilmenge $S \subset R$ eines Rings R heißt* Unterring, *wenn S mit der Addition und Multiplikation aus R einen Ring bildet. D.h.:*

$$0 \in S, \quad r, s \in S \Rightarrow r + s \in S,\, rs \in S.$$

Beispiel 2.2 *Die Teilmenge $2\mathbb{Z} \subset \mathbb{Z}$ aller geraden Zahlen ist ein Unterring von $\mathbb{Z}$. Allerdings hat dieser Unterring leider keine Eins.*

Im Polynomring $R[X]$ ist der Ring R selbst als Teilmenge $\{rX^0 : r \in R\}$ enthalten und bildet einen Unterring.

Der Ring $R[[X]]$ der formalen Potenzreihen enthält den Polynomring $R[X]$ als Unterring.

Definition 2.3 *Sind R und S zwei Ringe, so heißt eine Abbildung $f : R \to S$ ein Ring-Homomorphismus, wenn sie die beiden Rechenstrukturen erhält:*

$$f(r_1 + r_2) = f(r_1) + f(r_2), \quad f(r_1 r_2) = f(r_1) f(r_2) \quad \textit{für alle } r_1, r_2 \in R.$$

Weil f ein Gruppen-Homomorphismus bezüglich der Addition ist, gilt $f(0_R) = 0_S$. Aber $f(1_R) = 1_S$ braucht nicht zu gelten. Hierzu ein Beispiel: Seien R_1, R_2 beliebige Ringe mit Eins. Die direkte Summe $R_1 \oplus R_2$ ist als Menge das kartesische Produkt. Die Operationen sind komponentenweise erklärt:

$$(r_1, r_2) + (r_1', r_2') = (r_1 + r_1', r_2 + r_2'), \quad (r_1, r_2)(r_1', r_2') = (r_1 r_1', r_2 r_2,) \quad (r_1, r_1' \in R_1, r_2, r_2' \in R_2).$$

Falls R_1 und R_2 Eins-Elemente haben, ist $(1_{R_1}, 1_{R_2})$ ein Eins-Element in der direkten Summe. Die Abbildung

$$R_1 \to R_1 \oplus R_2, \quad r \mapsto (r, 0)$$

ist ein Ring-Homomorphismus. Aber das Bild $(1_{R_1}, 0)$ des Eins-Elementes aus R_1 ist nicht das Eins-Element in $R_1 \oplus R_2$.

Satz 2.2 *Ist $f : R \to S$ ein Ring-Homomorphismus, so ist*

$$Bild(f) = \{f(r) \in S : r \in R\}$$

ein Unterring von S und

$$Kern(f) = \{r \in R : f(r) = 0\}$$

ein Unterring von R.

Der Beweis ist offensichtlich.

Beispiel 2.3 (F 97, T3, A1) *: a) Beweisen Sie, dass die Abbildung*

$$\phi : \begin{cases} \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \to Z\ 45\mathbb{Z} \\ (a \bmod 9,\ b \bmod 5) \mapsto 10a - 9b \bmod 45 \end{cases}$$

wohldefiniert und ein Ringisomorphismus ist.

b) Bestimmen Sie den zu ϕ inversen Isomorphismus.

c) Bestimmen Sie alle nilpotenten Elemente von $\mathbb{Z}/45\mathbb{Z}$.

a) Wenn $a_1 \bmod 9 = a_2 \bmod 9$ ist, dann ist $a_1 - a_2 = k \cdot 9$ mit $k \in \mathbb{Z}$. Es folgt $10a_1 - 10a_2 = 2 \cdot 5 \cdot (a_1 - a_2) = 2k \cdot 45$. Also ist $10a_1 = 10a_2 \bmod 45$. Ebenso sieht man $9b_1 = 9b_2 \bmod 45$, wenn $b_1 = b_2 \bmod 5$. Damit ist die Abbildung wohldefiniert.

Die Abbildung ϕ ist ein Gruppen-Homomorphismus, weil sie aus zwei Multiplikationsabbildungen zusammengesetzt ist. Es ist noch die Multiplikativität zu zeigen. Das machen wir wieder komponentenweise: Es seien $a_1 \bmod 9$ und $a_2 \bmod 9$ zwei Restklassen in $\mathbb{Z}/9\mathbb{Z}$. Das Bild von $a_1 \cdot a_2 \bmod 9$ ist $10a_1a_2 \bmod 45$. Das Produkt der Bilder ist

$$\phi(a_1)\phi(a_2) = 10a_1 \cdot 10a_2 \bmod 45 = 100a_1a_2 \bmod 45 = 10a_1a_2 \bmod 45.$$

Der Beweis für die zweite Komponente läuft auf die Rechnung

$$(-9b_1)(-9b_2) = 81b_1b_2 = -9b_1b_2 \bmod 45$$

hinaus.

Bleibt noch die Bijektivität von ϕ zu zeigen. Weil beide Ringe endlich mit gleich vielen Elementen sind, genügt es, die Injektivität von ϕ zu zeigen. Sei also $(a \bmod 9,\ b \bmod 5)$ ein Element im Kern. Das heißt

$$10a - 9b = 0 \bmod 45.$$

Daraus folgt, dass a durch 9 und b durch 5 teilbar ist.

b) Wir setzen an

$$\phi^{-1}(x) = (\alpha x \bmod 9,\ \beta x \bmod 5).$$

Hier müssen $\alpha, \beta \in \mathbb{Z}$ so bestimmt werden, dass

$$\phi(\phi^{-1}(x)) = (10\alpha - 9\beta)x = x \bmod 45$$

ist. Es genügt, $\alpha = \beta = 1$ zu setzen. Damit ist also

$$\phi^{-1}(x \bmod 45) = (x \bmod 9,\ x \bmod 5).$$

c) Ein Ringelement c ist nilpotent, wenn eine Potenz c^n, $n \in \mathbb{N}$, die Null wird. Wegen des Ring-Isomorphismus können wir auch im Produkt $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ rechnen, und hier komponentenweise. Sei etwa $a \in \mathbb{Z}/9\mathbb{Z}$ mit $a^n = 0 \bmod 9$, $n \geq 1$. Dann muss auf jeden Fall a durch 3 teilbar sein. In diesem Fall ist aber auch schon $a^2 = 0 \bmod 9$. Die nilpotenten Elemente im Ring $\mathbb{Z}/9\mathbb{Z}$ sind die Restklassen von $0, 3$ und 6. Sei jetzt $b \bmod 5$ nilpotent. Dann ist eine Potenz b^n durch 5 teilbar. Weil 5 eine Primzahl ist, muss b selbst durch 5 teilbar sein und es ist $b = 0 \bmod 5$. Die nilpotenten Elemente im Produkt sind

$$(0,0),\ (3,0),\ (6,0),$$

und in $\mathbb{Z}/45\mathbb{Z}$ *sind es ihre Bilder unter* ϕ*:*

$$0,\ 30,\ 60 = 15\, mod\, 45.$$

Der Kern eines Ringhomomorphismus f ist aber kein Unterring wie jeder andere. Er hat noch folgende merkwürdige Eigenschaft:

$$a \in Kern(f),\ r \in R \Rightarrow\ ra \in Kern(f),\ ar \in Kern(f).$$

Beweis. $f(ra) = f(r)f(a) = f(r)0 = 0, \quad f(ar) = f(a)f(r) = 0r = 0.$ □

Definition 2.4 *Eine Teilmenge* $I \subset R$ *des Rings* R *heißt* Ideal*, wenn*

1) $I \subset R$ *eine Untergruppe bezüglich der Addition ist,*

2) für alle $a \in I$ *und* $r \in R$ *gilt:*

$$ra \in I, \quad ar \in I.$$

Wenn R kommutativ ist, gilt $ra = ar$ und die beiden Bedingungen in Teil 2) der Definition sind äquivalent. Wenn R nicht kommutativ ist, muss man sie aber leider auseinander halten. Manche Haarspalter definieren sogar: $I \subset R$ heißt *Links-Ideal*, wenn für alle $a \in I$, $r \in R$ gilt $ra \in I$, und *Rechts-Ideal*, wenn stets $ar \in I$.

Beispiel 2.4 *In jedem Ring* R *gibt es das Null-Ideal* $\{0\}$ *und das allumfassende Ideal* R*. Ist* $a \in R$ *ein beliebiges Element, so ist*

$$Ra = \{ra :\ r \in R\}$$

ein Links-Ideal und

$$aR = \{ar :\ r \in r\}$$

ein Rechts-Ideal. Falls R *kommutativ ist, stimmen beide Ideale überein. Dann nennt man*

$$(a) := Ra$$

das Haupt-Ideal *erzeugt von* a*. Das Null-Ideal* (0) *ist das Haupt-Ideal erzeugt von* $0 \in R$ *und* R *ist das Haupt-Ideal* (1)*.*

Ein Haupt-Ideal $(a) \subset \mathbb{Z}$ *im Ring* $\mathbb{Z}$ *besteht aus allen ganzzahligen Vielfachen der Zahl* $a \in \mathbb{Z}$*, also aus allen ganzen Zahlen, die durch* a *teilbar sind.*

Satz 2.3 *Jedes Ideal* $I \subset \mathbb{Z}$ *im Ring der ganzen Zahlen ist ein Haupt-Ideal.*

Beweis. Das Ideal $I \subset \mathbb{Z}$ ist insbesondere eine Untergruppe. Und in Satz 1.12 haben wir gesehen, dass jede Untergruppe von $\mathbb{Z}$ die Form $Z \cdot a$, $a \in \mathbb{Z}$, hat. Also ist jedes Ideal ein solches Haupt-Ideal (a). □

Was Normalteiler für Gruppen waren, das sind Ideale für Ringe: Man kann nach ihnen austeilen. Um nicht zu viele Fälle unterscheiden zu müssen, werden wir von jetzt an voraussetzen: *Alle vorkommenden Ringe seien kommutativ.*

Sei also jetzt R ein Ring und $I \subset R$ ein Ideal. Da I insbesondere eine Untergruppe der abelschen Gruppe $(R,+)$ ist, ist die Faktorgruppe $(R/I,+)$ wohldefiniert. Wir zeigen, dass die Ring-Struktur auf R ein Multiplikation auf R/I induziert:

Es seien r_1+I und r_2+I zwei Restklassen in R/I. Dann hängt die Restklasse

$$(r_1+I)\cdot(r_2+I) := (r_1\cdot r_2)+I$$

nur von den beiden Restklassen r_1+I und r_2+I ab, und nicht von den gewählten Repräsentanten.

Beweis. Sei $r_i+I = s_i+I$, $i=1,2$, d.h. $s_i = r_i+d_i$ mit $d_1,d_2 \in I$. Dann ist

$$s_1s_2 = (r_1+d_1)(r_2+d_2) = r_1r_2 + \underbrace{d_1r_2+d_2r_1+d_1d_2}_{\in I}$$

wegen der Ideal-Eigenschaft von I. □

Für die so definierte Multiplikation auf der Menge R/I beweist man Assoziativität, Kommutativität und das Distributivgesetz sofort mit den entsprechenden Eigenschaften von R.

Definition 2.5 *Der soeben definierte Ring R/I heißt* Faktor- *oder* Restklassenring *von R nach dem Ideal I.*

Beispiel 2.5 *Für jede natürliche Zahl $n>1$ ist $\mathbb{Z}_n$ der Faktorring des Ringes $\mathbb{Z}$ nach dem Ideal (n).*

Beispiel 2.6 *Sei*

$$P := X^n + c_{n-1}X^{n-1} + ... + c_1X + c_0,\ c_i \in R,$$

ein normiertes Polynom im Polynomring $R[X]$. Im Faktorring $R[X]/(P)$ ist $P=0$. Oder anders geschrieben

$$X^n = Q := -c_{n-1}X^{n-1} - ... - c_1X - c_0 \quad \in R[X]/(P).$$

Jede Restklasse in $R[X]/(P)$ wird repräsentiert von einem Polynom $F = a_mX^m + ...$ Ersetzt man hier

$$\begin{array}{lll} X^n & \textit{durch} & Q, \\ X^{n+1} & \textit{durch} & X\cdot Q \\ & & = -c_{n-1}X^n - c_{n-2}X^{n-1} - ... \\ & & = -c_{n-1}Q - c_{n-2}X^{n-1} - ... \end{array}$$

usw., so findet man: jede Restklasse in $R[X]/(P)$ wird repräsentiert durch ein Polynom vom Grad $\leq n-1$.

Nehmen wir als konkretes Beispiel $R=\mathbb{Z}$ und $P=X^2+1 \in \mathbb{Z}[X]$, so sehen wir: Jede Restklasse in $\mathbb{Z}[X]/(X^2+1)$ wird repräsentiert durch ein Polynom $aX+b$, $a,b\in\mathbb{Z}$, vom Grad ≤ 1. Addition solcher Restklassen geschieht wie üblich durch Addition der Koeffizienten. Bei der Multiplikation zweier Polynome passiert folgendes:

$$(a_1X+b_1)(a_2X+b_2) = a_1a_2X^2 + (a_1b_2+b_1a_2)X + b_1b_2 = (b_1b_2-a_1a_2) + (a_1b_2+b_1a_2)X.$$

Man rechnet wie üblich mit den linearen Polynomen, nur ist $X^2=-1$. Der Ring ist isomorph zu

$$\mathbb{Z}[i] := \{b+ai \in \mathbb{C} :\ b,a\in\mathbb{Z}\}.$$

Wie bei Gruppen gilt auch hier

Satz 2.4 (Homomorphiesatz) *Es sei $f : R \to S$ ein Homomorphismus von Ringen. Dann gibt es einen Ring-Isomorphismus $g : R/Kern(f) \to Bild(f) \subset S$ so, dass das Diagramm*

$$\begin{array}{ccc} R & \to & R/Kern(f) \\ f & \searrow & \downarrow g \\ & & S \end{array}$$

kommutiert.

Der Beweis ist auch ganz genau derselbe, wie für Satz 1.9, und wir lassen ihn weg.

Beispiel 2.7 (H 98, T1, A2) *: Wieviele Lösungen besitzt die Kongruenz*

$$x^2 \equiv 9 \, mod \, 1386$$

im Bereich $\{0, ..., 1385\}$?
Der Ring $\mathbb{Z} \, mod \, 1386$ ist uns zu groß. Wir zerlegen ihn, indem wir

$$1386 = 2 \cdot 693 = 2 \cdot 9 \cdot 77 = 2 \cdot 9 \cdot 7 \cdot 11$$

in Primzahlpotenzen zerlegen. Nach Satz 1.15 (iteriert) ist dann

$$f : \mathbb{Z}_{1386} \to \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_7 \times \mathbb{Z}_{11}, \quad x \, mod \, 1386 \mapsto (x \, mod \, 2, \; x \, mod \, 9, \; x \, mod \, 7, \; x \, mod \, 11)$$

ein Gruppen-Isomorphismus. Weil er offensichtlich multiplikativ ist, ist er auch ein Ring-Isomorphismus. Gesucht ist die Anzahl der Zahlen x mit

$$x^2 \, mod \, 1386 = (x \, mod \, 1386)^2 = 9 \, mod \, 1386.$$

Ist (x_1, x_2, x_3, x_4) das Bild von x unter unserem Ring-Homomorphismus, so bedeutet dies

$$x_1^2 = 9 \, mod \, 2 = 1 \, mod \, 2, \quad x_1 = 1 \, mod \, 2;$$

$$x_2^2 = 9 \, mod \, 9 = 0 \, mod \, 9, \quad x_2 = 0, \, 3 \; oder \, 6 \, mod \, 9;$$

$$x_3^2 = 9 \, mod \, 7 = 2 \, mod \, 7, \quad x_3 = 3 \; oder \, 4 \, mod \, 7;$$

$$x_4^2 = 9 \, mod \, 11, \quad x_4 = 3 \; oder \, 8 \, mod \, 11.$$

Die gesuchte Anzahl ist

$$3 \cdot 2 \cdot 2 = 12.$$

Sind $I_1, I_2 \subset R$ zwei Ideale, so ist $I_1 \cap I_2$ wieder ein Ideal. Als Beispiel betrachten wir $I_1 := (2)$ und $I_2 := (3) \subset \mathbb{Z}$. Das erste Ideal besteht aus allen ganzen Zahlen, die durch 2 teilbar sind,

das zweite aus den Zahlen, die durch 3 teilbar sind. Deswegen besteht $I_1 \cap I_2$ aus allen ganzen Zahlen die durch 2 und durch 3, d.h., durch 6 teilbar sind:

$$(2) \cap (3) = (6).$$

Der Durchschnitt $I_1 \cap I_2$ der beiden angegebenen Ideale ist also dasselbe wie das *Produkt*

$$I_1 \cdot I_2 := \{r \cdot s : \, r \in I_1, s \in I_2\}$$

beider Ideale. Aber Vorsicht:

$$(2) \cdot (2) = \{r \cdot s : \, r, s \text{ gerade}\} = \{n \in \mathbb{Z} : \, n \text{ durch } 4 \text{ teilbar}\} = (4) \neq (2) = (2) \cap (2).$$

Die Vereinigung zweier Ideale ist i.a. nicht wieder ein Ideal, weil diese Vereinigung nicht einmal eine Untergruppe zu sein braucht. Statt dessen definiert man (wie bei Untervektorräumen):

$$I_1 + I_2 := \{r + s, \, r \in I_1, s \in I_1\}.$$

Man sieht sofort:

Satz 2.5 *Sind I_1, I_2 Ideale im Ring R, so ist $I_1 + I_2 \subset R$ ein Ideal, das beide Ideale I_1 und I_2 enthält. Es ist das kleinste derartige Ideal: Ist $J \subset R$ ein Ideal mit $I_1, I_2 \subset J$, so gilt $I_1 + I_2 \subset J$.*

Das Ideal $I_1 + I_2$ heißt die *Summe* der beiden Ideale I_1 und I_2 oder das von I_1 und I_2 *erzeugte* Ideal. Diese Konstruktion kann man iterieren. Insbesondere definiert man: Sind $r_1, ..., r_k \in R$ Ring-Elemente, so heißt

$$(r_1, ..., r_k) := (r_1) + ... + (r_k) \subset R$$

das von diesen Elementen erzeugte Ideal. Seine Elemente sind

$$s_1 r_1 + ... + s_k r_k, \, s_1, ..., s_k \in R.$$

Es sei $n \neq 0, 1$ eine ganze Zahl. Dann gibt es die Wurzel $\sqrt{n} \in \mathbb{C}$. Man definiert $\mathbb{Z}[\sqrt{n}]$ als die Menge

$$\{a + b\sqrt{n} \in \mathbb{C} : \, a, b \in \mathbb{Z}\}.$$

Dies ist ein Teilring von $\mathbb{C}$: Es ist klar dass $\mathbb{Z}[\sqrt{n}] \subset \mathbb{C}$ eine Untergruppe bezüglich der Addition ist. Aber $\mathbb{Z}[\sqrt{n}]$ ist auch abgeschlossen unter der Multiplikation:

$$(a_1 + b_1\sqrt{n})(a_2 + b_2\sqrt{n}) = a_1 a_2 + b_1 b_2 n + (a_1 b_2 + b_1 a_2)\sqrt{n}.$$

Der wichtigste Spezialfall ist $\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i]$, der Ring der *ganzen Gaußschen Zahlen.* Falls $\sqrt{n}$ selbst ganz ist, d.h., wenn $n = d^2$ ein Quadrat einer ganzen Zahl ist, erhält man nichts neues: $\mathbb{Z}[\sqrt{d^2}] = \mathbb{Z}[d] = \mathbb{Z}$. Deswegen interessieren wir uns nur für den Fall, dass n kein Quadrat ist.

Es gibt eine Abbildung

$$\mathbb{Z}[X] \to \mathbb{Z}[\sqrt{n}], \quad X \mapsto \sqrt{n},$$

des Polynomrings $\mathbb{Z}[X]$ auf den Ring $\mathbb{Z}[\sqrt{n}]$. Man bildet ab

$$c_0 + c_1 X + ... + c_k X^k \mapsto c_0 + c_1\sqrt{n} + ... + c_k \sqrt{n}^k$$

und führt den rechten Ausdruck mit der Multiplikation in $\mathbb{Z}[\sqrt{n}]$ über in einen Ausdruck $a + b\sqrt{n}$, $a, b, \in \mathbb{Z}$. Es ist klar, dass diese Abbildung ein surjektiver Ring-Homomorphismus ist. Was ist sein Kern? Offensichtlich liegt $X^2 - n$ in diesem Kern, und damit auch das Ideal $(X^2 - n)$. Die Restklassen im Faktorring $\mathbb{Z}[X]/(X^2 - n)$ werden genau durch die Polynome $a + bX$ vom Grad ≤ 1 repräsentiert. Damit ist dieser Faktorring eine freie abelsche Gruppe vom Rang zwei mit den Erzeugenden 1 und X. Weil auch $\mathbb{Z}[\sqrt{n}]$ eine freie abelsche Gruppe mit den Erzeugenden 1 und $\sqrt{n}$ ist, muss der Epimorphismus

$$\mathbb{Z}[X]/(X^2 - n) \to \mathbb{Z}[\sqrt{n}]$$

ein Isomorphismus sein.

Leider kommen in den Staatsexamensaufgaben Begriffe vor, die ich in einer Algebra-Vorlesung eigentlich nicht behandeln würde. Nur aus diesem Grund sollen noch die beiden folgenden Definitionen angegeben werden.

Definition 2.6 *Ein kommutativer Ring R heißt* noethersch, *wenn jede aufsteigende Kette von Idealen in R*

$$I_1 \subset I_2 \subset ... \subset R$$

irgend wann stationär wird. Das bedeutet, es gibt in dieser Kette ein Ideal I_n mit $I_j = I_n$ für alle $j \geq n$.

Der Ring R heißt artinsch, *wenn jede absteigende Kette von Idealen*

$$R \supset I_1 \supset I_2 \supset ...$$

irgend wann stationär wird.

Satz 2.6 *Der kommutative Ring R ist genau dann noethersch, wenn jedes Ideal $I \subset R$ endlich erzeugt ist.*

Beweis. Sei R noethersch und $I \subset R$ ein Ideal. Wenn $I = (0)$ das Null-Ideal ist, dann ist es endlich erzeugt. Andernfalls gibt es ein Element $r_1 \in I$, $r_1 \neq 0$. Wenn $I = (r_1)$ ist, sind wir fertig. Andernfalls gibt es ein Element $r_2 \in I$ mit $r_2 \notin (r_1)$. Wenn $I = (r_1, r_2)$ ist, sind wir fertig. Andernfalls gibt es ein $r_3 \in I$ mit $r_3 \notin (r_1, r_2)$. Und so weiter. Entweder ist nach endlich vielen solchen Schritten $I = (r_1, r_2, ..., r_n)$, oder wir finden eine echt aufsteigende Kette von Idealen, die nie stationär wird. Aber wegen der Eigenschaft noethersch kann letzteres nicht der Fall sein.

Sei jetzt vorausgesetzt, dass jedes Ideal $I \subset R$ endlich-erzeugt ist. Wir betrachten eine echt aufsteigende Kette $I_1 \subset I_2 \subset ...$ von Idealen in R. Dann ist auch $I := \bigcup I_k$ ein Ideal in R und nach Voraussetzung endlich erzeugt, etwa $I = (r_1, ..., r_n)$. Jedes Element r_ν gehört zu einem Ideal I_{k_ν} in unserer Kette. Ist $n = max\{k_\nu\}$, so gehören also alle r_ν zu I_n. Es folgt $I = I_n$ und $I_j = I_n$ für $j \geq n$. □

Aufgabe 2.1 *a) Es seien $m, n \in \mathbb{N}$ teilerfremde natürliche Zahlen. Zeigen Sie, dass der Gruppen-Isomorphismus $\mathbb{Z}_{m \cdot n} \to Z_m \times \mathbb{Z}_n$ von Satz 1.15 auch ein Ring-Isomorphismus ist.*

b) Bestimmen Sie ein $a \in \mathbb{N}$ mit $a = 0$ modulo $3, 5, 7, 11$, aber $a = 1$ modulo 13.

Aufgabe 2.2 (F 02, T1, A4) *Sei $I \subset \mathbb{Z}[X]$ das von den Polynomen $X^4 + 33X^3 + X$ und $X^5 - 9X^3 + X^2 - 3X + 3$ erzeugte Ideal.*

a) Zeigen Sie, dass $3 \in I$ ist.

b) Bestimmen Sie die Anzahl der Elemente von $R := \mathbb{Z}[X]/I$.

c) Zeigen Sie, dass R eine zu $(\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/3\mathbb{Z})^2$ isomorphe Einheitengruppe hat.

Aufgabe 2.3 (F 02, T3, A4b) *Ist $x^2 + x + 11 = 0\,(mod 370368)$ lösbar?*

Aufgabe 2.4 (F 94, T2, A2) *Man bestimme alle Lösungen der Kongruenz*

$$3x^2 - 2x + 9 \equiv 0\,(mod\,35).$$

Aufgabe 2.5 (F 01, T3, A4) *Sei k eine positive Zahl und sei $R := M_k(\mathbb{Z})$ der Ring der ganzzahligen $k \times k$-Matrizen. Zeigen Sie:*

a) Für jede natürliche Zahl $n \geq 0$ ist nR ein zweiseitiges Ideal in R.

b) Jedes zweiseitge Ideal in R ist von der in a) genannten Art.

Aufgabe 2.6 (H 00, T2, A2) *Wie viele Elemente x mit der Eigenschaft $x^2 = x$ hat der Ring $\mathbb{Z}/15015\mathbb{Z}$? Geben Sie vier solche Elemente explizit an.*

Aufgabe 2.7 (F 95, T2, A1) *Auf der reellen Zahlengeraden $\mathbb{R}$ definiere man die Verknüpfung*

$$\circ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}, \quad x \circ y := x + y + x^2 y.$$

Man zeige:

a) Es gibt genau ein Einselement $e \in \mathbb{R}$ bezüglich $\circ$.

b) Zu jedem $x \in \mathbb{R}$ gibt es genau ein Rechtsinverses (d.h. es gibt ein $y \in \mathbb{R}$ mit $x \circ y = e$).

c) Für welche $x \in \mathbb{R}$ gibt es ein Linksinverses?

Aufgabe 2.8 (F 94, T3, A3) *Sei R ein noetherscher kommutativer Ring mit Eins, und sei $f : R \to R$ ein Ringendomorphismus. Zeigen Sie: f surjektiv $\Rightarrow$ f injektiv. (Hinweis: Betrachten Sie die Folge $f, f^2, f^3, ...$)*

Aufgabe 2.9 (F 93, T3, A1) *Es seien p, q zwei verschiedene Primzahlen und R ein Ring mit Einselement mit pq Elementen. Man beweise, dass*

$$R \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$

ist.

Aufgabe 2.10 (F 91, T1 A1) *Sei $\mathbb{Q}$ die Menge der rationalen Zahlen. Sei M eine Teilmenge der natürlichen Zahlen, die 1 enthält. Sei*

$$\mathbb{Q}_M := \{a/b \in \mathbb{Q} : a \in \mathbb{Z},\ b \in M \text{ teilerfremd}\}.$$

Zeigen Sie:

1) $\mathbb{Q}_M$ ist genau dann eine Gruppe unter Addition, eine sog. rationale Gruppe, wenn M alle Teiler und alle kleinsten gemeinsamen Vielfachen seiner Elemente enthält.

2) Eine solche rationale Gruppe Q_M ist genau dann ein Teilring von $\mathbb{Q}$, wenn M multiplikativ abgeschlossen ist.

Aufgabe 2.11 (F 90, T3, A1) *Seien p und q aus $\mathbb{N}$ teilerfremd. Wir wollen einsehen, dass die Ringe*

$$R = \mathbb{Z}[U,V]/(U^p - 1, V^q - 1) = \mathbb{Z}[u,v] \text{ und } S = \mathbb{Z}[W]/(W^{pq} - 1) = \mathbb{Z}[w]$$

isomorph sind. Hierbei bezeichnen u, v und w die Restklassen von U, V und W. Dazu betrachten wir den Einsetzungshomomorphismus

$$\Phi : \mathbb{Z}[U,V] \to \mathbb{Z}[W], \quad U \mapsto W^q, V \mapsto W^p.$$

Zeigen Sie:

a) Φ induziert einen Homomorphismus $\varphi : R \to S$ mit $\varphi(u) = w^q$ und $\varphi(v) = w^p$.

b) Die additive Gruppe $(S, +)$ von S ist frei vom Rang pq und $(R, +)$ wird von pq Elementen erzeugt.

c) $w \in Bild(\varphi)$.

d) φ ist ein Isomorphismus.

2.2 Körper

Das Produkt zweier Ring-Elemente kann $= 0$ sein, ohne dass einer der beiden Faktoren $= 0$ ist. Beispiel: In $\mathbb{Z}_6$ gilt

$$2 \cdot 3 = (2 + \mathbb{Z} \cdot 6) \cdot (3 + \mathbb{Z} \cdot 6) = 6 + \mathbb{Z} \cdot 6 = 0.$$

Definition 2.7 *Ein* Nullteiler *im Ring R ist ein Ring-Element $r \neq 0$, zu dem es ein Ring-Element $s \neq 0$ gibt mit $r \cdot s = 0$. (In nicht-kommutativen Ringen muss man fein säuberlich zwischen Rechts- und Links-Nullteilern unterscheiden.) Ein Ring, in dem es keine Nullteiler gibt heißt* nullteilerfrei *oder* Integritätsring

Beispiel 2.8 *Sei etwa $R = \mathbb{Z}/(n)$ der Faktorring auch einem Hauptideal $(n) \subset \mathbb{Z}$, $2 \leq n \in \mathbb{Z}$. Besitzt n echte Teiler, etwa $n = n_1 n_2$ mit $n_1, n_2 \neq \pm 1, \pm n$, so sind die Restklassen von n_1 und n_2 modulo n von Null verschieden, ihr Produkt $n_1 n_2$ modulo n aber ist $= 0$. Wir sehen: Der Faktorring $\mathbb{Z}/(n)$ ist genau dann nullteilerfrei, wenn n eine Primzahl ist.*

In Integritätsringen gilt die Kürzungsregel:

$$r \cdot t = s \cdot t \text{ mit } t \neq 0 \quad \Rightarrow \quad r = s.$$

Beweis: Nach Voraussetzung ist $(r - s) \cdot t = 0$ mit $t \neq 0$. Weil $t \in R$ kein Nullteiler ist, folgt daraus $r - s = 0$, also $r = s$. □

Definition 2.8 *Ein* Körper *ist ein kommutativer Ring K mit Eins, in dem jedes Element $\neq 0$ ein Inverses unter der Multiplikation hat. Äquivalent dazu ist: Die Menge*

$$K^* := \{a \in K : a \neq 0\}$$

bildet unter der Multiplikation eine Gruppe.

Ein Körper ist ein Integritätsring: Sei etwa $a \cdot b = 0$ für $a, b \in K$. Falls $a \neq 0$ ist, gilt

$$b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0.$$

Beispiele für Körper sind die wohlbekannten Körper $\mathbb{R}$ und $\mathbb{C}$ aus der Analysis. Außerdem bilden die rationalen Zahlen einen Körper $\mathbb{Q}$. Ist K ein Körper, so bezeichnet man mit $K(X)$ den Körper der rationalen Funktionen in einer Unbestimmten X mit Koeffizienten aus K. Die Elemente aus K sind also (rein formale) Quotienten

$$\frac{p(X)}{q(X)}, \quad p(X), q(X) \in K[X], q(X) \neq 0,$$

von Polynomen mit Koeffizienten aus K. Ein etwas anderer Körper ist

$$\mathbb{Q}(i) := \{a + bi \in \mathbb{C} : a, b \in \mathbb{Q}\}.$$

Eine Abbildung $f : K \to L$ des Körpers K in den Körper L heißt Körper-Homomorphismus, wenn sie ein Ring-Homomorphismus ist. Falls f nicht der Null-Homomorphismus ist (dem man normalerweise das Recht abspricht, ein Homomorphismus von Körpern zu sein), dann induziert f einen Homomorphismus $(K^*, \cdot) \to (L^*, \cdot)$ Es folgt $f(1_K) = 1_L$. Für $a \neq 0$, $a \in K$, ist $f(a) \cdot f(a^{-1}) = f(a \cdot a^{-1}) = f(1_K) = 1_L$. Also muss auch $f(a) \neq 0$ sein. Es folgt: f ist injektiv, und $K \simeq f(K)$ ist ein Unterkörper von L.

Den nullteilerfreien Ring $\mathbb{Z}$ kann man als Unterring in den Körper $\mathbb{Q}$ einbetten. Diese Konstruktion kann man wie folgt verallgemeinern:

Satz 2.7 *a) Es sei R ein Integritätsring. Dann gibt es einen Körper Q und einen injektiven Ring-Homomorphismus $R \to Q$ derart, dass gilt: Ist $f : R \to L$ ein injektiver Ring-Homomorphismus in einen Körper L, so gibt es einen eindeutig bestimmten Körper-Homomorphismus $Q \to L$, der f fortsetzt.*

b) Das Paar $R \subset Q$ ist bis auf Isomorphie eindeutig bestimmt.

Beweis. a) Wir kopieren die Konstruktion der rationalen Zahlen aus den ganzen Zahlen. Dazu betrachten wir alle Paare $(z,n) \in R \times R$ mit $n \neq 0$. (Nur für den Zweck dieses Beweises schreiben wir so ein Paar als Paar. Später werden wir immer z/n dafür schreiben.) Auf der Menge dieser Paare definieren wir eine Relation durch

$$(z_1,n_1) \sim (z_2,n_2) \Leftrightarrow z_1n_2 = z_2n_1.$$

Diese Relation ist offensichtlich reflexiv ($(z,n) \sim (z,n)$) und symmetrisch ($(z_1,n_1) \sim (z_2,n_2) \Rightarrow (z_2,n_2) \sim (z_1,n_1)$). Aber sie ist auch transitiv:

$$\begin{aligned}(z_1,n_1) \sim (z_2,n_2) \text{ und } (z_2,n_2) \sim (z_3,n_3) &\Rightarrow z_1n_2 = z_2n_1 \text{ und } z_2n_3 = z_3n_2\\ &\Rightarrow z_1n_2n_3 = z_3n_1n_2\\ &\Rightarrow z_1n_3 = z_3n_1 \quad \text{(Kürzungsregel).}\end{aligned}$$

Die Relation $\sim$ ist also eine Äquivalenzrelation. Wir setzen $Q := (R \times R)/\sim$ und haben einiges zu zeigen:

Es gibt eine injektive Abbildung $R \to Q$: Ein Element $r \in R$ bilden wir auf das Paar (rs,s) ab. Dabei ist $0 \neq s \in R$ beliebig. Die Äquivalenzklasse (rs,s) ist unabhängig von der Wahl von s.

Die folgenden Eigenschaften rechnen wir jetzt nicht mehr alle nach:

Die Addition auf R setzt sich fort zu einer Addition auf Q: Wir definieren

$$(z_1,n_1) + (z_2,n_2) := (z_1n_2 + z_2n_1, n_1n_2).$$

Die Multiplikation auf R setzt sich fort zu einer Multiplikation auf Q: Wir definieren

$$(z_1n_1)(z_2,n_2) := (z_1z_2, n_1n_2).$$

Die so definierte Addition und Multiplikation auf Q sind kommutativ und assoziativ. Es gilt das Distributivgesetz. $(Q,+)$ ist eine abelsche Gruppe mit neutralem Element $(0,n)$. (Dieses Element hängt nicht ab von der Wahl von n.)

$(Q^*,\cdot)$ ist eine abelsche Gruppe: Das Einselement ist (n,n). Ist $(z,n) \neq 0$, so ist $z \neq 0$ und (n,z) ist das Inverse zu (z,n).

Sei jetzt $f : R \to L$ ein injektiver Ring-Homomorphismus in den Körper L. Durch $(z,n) \mapsto f(z)/f(n) \in L$ wird er fortgesetzt zu einem Homomorphismus $Q \to L$. Diese Fortsetzung kann auch gar nicht anders definiert werden.

b) Seien jetzt Q und Q' zwei Körper mit den Eigenschaften aus a). Dann gibt es also Homomorphismen $f : Q \to Q'$ und $g : Q' \to Q$, die auf der Teilmenge $R \subset Q$ und $R \subset Q'$ die identische Abbildung sind. Deswegen ist $g \circ f|R = id_R$. Daraus folgt $g \circ f = id_Q$ und ebenso $f \circ g = id_{Q'}$. Wir können Q und Q' mit Hilfe von g identifizieren. □

Definition 2.9 *Der bis auf Isomorphie eindeutig bestimmte Körper Q aus Satz 2.7 heißt der* Quotientenkörper *des Integritätsrings R.*

Beispiel 2.9 *Der Quotientenkörper des Rings $\mathbb{Z}$ der ganzen Zahlen ist der Körper $\mathbb{Q}$ der rationalen Zahlen. Das Paar (z,n) aus dem Beweis von Satz 2.7 stellt den Bruch z/n dar. Und die Äquivalenzrelation $\sim$ im Beweis bedeutet*

$$\frac{z_1}{n_1} = \frac{z_2}{n_2} \Leftrightarrow \frac{z_1 n_2 - z_2 n_1}{n_1 n_2} = 0.$$

Beispiel 2.10 *Ist $R = K[X]$ der Polynomring über einem Körper K, so ist sein Quotientenkörper der Körper aller Quotienten Z/N von Polynomen, d.h., der Körper $K(X)$ der rationalen Funktionen über K.*

Jeder Körper K ist auch ein Ring. Deswegen ist auch definiert, was ein Ideal $I \subset K$ ist. In K gibt es aber nur zwei Ideale: Eines ist das Null-Ideal (0). Ist $I \subset K$ ein Ideal $\neq (0)$, so enthält I ein Element $a \in K$, $a \neq 0$. Dann gehört auch $1 = a^{-1}a$ zu I und damit jedes Körperelement. Es ist $I = (1) = K$. Davon gilt auch die Umkehrung:

Satz 2.8 *Es sei R ein kommutativer Ring mit Eins, der nur zwei verschiedene Ideale enthält. Dann ist R ein Körper.*

Beweis. Die beiden Ideale in K sind notwendigerweise das Null-Ideal (0) und das Eins-Ideal $(1) = R$. Jedes Ring-Element $0 \neq r \in R$ erzeugt ein Hauptideal $(r) \neq (0)$. Es folgt $(r) = (1)$, also $1 \in (r)$ und damit ist r invertierbar. □

Satz 2.9 *Es sei R ein kommutativer Ring mit Eins und $I \subset R$, $I \neq R$, ein Ideal. Dann sind äquivalent:*
1) R/I ist ein Körper;
2) ist $J \subset R$ ein Ideal mit $I \subset J$, dann gilt entweder $J = I$ oder $J = R$.

Beweis. R/I ist genau dann ein Körper, wenn es in R/I nur zwei Ideale gibt. Jedes Ideal $J \subset R$ mit $I \subset J$ definiert aber ein Ideal J/I in R/I. Ist J/I das Null-Ideal, dann ist $J = I$, und ist $J/I = R/I$, dann ist $J = R$. □

Definition 2.10 *Ein Ideal $I \neq R$ im Ring R heißt* maximal, *wenn es kein Ideal $J \subset R$ mit $I \subset J$ und $J \neq I, R$ gibt.*

Beispiel 2.11 *Nach Satz 2.3 ist jedes Ideal $I \subset \mathbb{Z}$ ein Hauptideal $I = (n)$, $n \geq 1$. Besitzt n einen echten Teiler p, so ist das Hauptideal (n) im Hauptideal (p) echt enthalten. Das Ideal (n) ist also genau dann maximal, wenn die Zahl n keine Teiler ($\neq \pm 1, \pm n$) besitzt. Solche Zahlen heißen* Primzahlen. *Ist $p \in \mathbb{N}$ eine Primzahl, so ist das Ideal (p) also maximal und*

$$\mathbb{F}_p := \mathbb{Z}/(p)$$

ist ein Körper. Seine Elemente sind die Restklassen von $0, 1, ..., p-1$ modulo p. Addition und Multiplikation sind genau die Addition und Multiplikation ganzer Zahlen modulo p.

Jeder Körper enthält eine Eins = 1. Dann enthält er auch eine Minus-Eins = -1 und eine Zwei $2 = 1 + 1$. Durch

$$\mathbb{Z} \ni n \mapsto n \cdot 1 \in K$$

wird ein Ring-Homomorphismus $\mathbb{Z} \to K$ definiert. Da kann (und muss) man jetzt zwei Fälle unterscheiden:

1) Der Ring-Homomorphismus $\mathbb{Z} \to K$ ist injektiv. Dann enthält K wegen Satz 2.7 einen Unterkörper isomorph zu $\mathbb{Q} = Q(\mathbb{Z})$.

2) Der Ring-Homomorphismus $\mathbb{Z} \to K$ hat einen Kern. Dieser Kern ist ein Haupt-Ideal (n), $0 < n \in \mathbb{N}$. Wegen $1 \mapsto 1$ kann nicht $n = 1$ sein. Weil der Faktor-Ring $\mathbb{Z}/(n) \subset K$ nullteilerfrei ist, muss $n = p$ eine Primzahl sein. Dann ist $\mathbb{Z}/(p) = \mathbb{F}_p$ ein Unterkörper von K. Wir haben bewiesen:

Satz 2.10 *Jeder Körper K enthält einen kleinsten Unterkörper. Dieser Unterkörper ist entweder isomorph zum Körper $\mathbb{Q}$ der rationalen Zahlen, oder zu einem Körper $\mathbb{F}_p$.*

Definition 2.11 *Der Unterkörper von K aus Satz 2.10 heißt der* Primkörper *von K. Ist der Primkörper isomorph zu $\mathbb{Q}$, so sagt man, K hat die Charakteristik 0. Ist der Primkörper isomorph zu $\mathbb{F}_p$, so sagt man, K hat die Charakteristik p.*

Die Einheiten eines Körpers K, d.h., die Körper-Elemente $\neq 0$ bilden eine Gruppe K^* bezüglich der Multiplikation. Besonders interessant sind die Einheitengruppen endlicher Körper. Betrachten wir etwa $\mathbb{F}_5$. Hier ist

$$2^2 = 4,\ 2^3 = 3,\ 2^4 = 1.$$

Die Einheitengruppe von $\mathbb{F}_5$ ist also die zyklische Gruppe

$$\{2, 4, 3, 1\} \simeq \mathbb{Z}_4$$

der Ordnung 4. Die Einheitengruppen aller endlichen Körper sind zyklisch. Das ist ein Spezialfall des folgenden Satzes:

Satz 2.11 *Jede endliche Untergruppe $G \subset K^*$ der Einheitengruppe eines Körpers K ist zyklisch.*

Beweis. Weil K^* abelsch ist, ist die Gruppe G auch abelsch. Weil sie endlich ist, ist sie nach Satz 1.27 ein Produkt

$$G = \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_r}$$

endlicher zyklischer Gruppen. Wenn alle diese Zahlen $n_1, ..., n_r$ teilerfremd sind, dann ist nach Satz 1.15 die Gruppe G selbst zyklisch.

Andernfalls gibt es zwei verschiedene Untergruppen

$$G_1 \simeq \mathbb{Z}_n,\ G_2 \simeq \mathbb{Z}_n,\ G_1 \neq G_2 \subset G.$$

Sei g_1 ein Erzeugendes von G_1. Dann ist

$$G_1 = < g_1 > = \{1, g_1, g_1^2, ..., g_1^{n-1}\}.$$

Dies sind n verschiedene Körper-Elemente $g \in K^*$ mit $g^n = 1$. Alle sind sie Nullstellen des Polynoms $X^n - 1 \in K[X]$. Durch wiederholte Anwendung des Satzes von Vieta (Satz 2.1) folgt

$$X^n - 1 = (X-1)(X-g_1)(X-g_1^2) \cdot ... \cdot (X-g_1^{n-1}).$$

Jedes Element $g \in G_2$ erfüllt aber auch $g^n = 1$. Daraus folgt

$$(g-1)(g-g_1)(g-g_1^2) \cdot ... \cdot (g-g_1^{n-1}) = g^n - 1 = 0.$$

Also muss einer der Faktoren $g - g_1^k = 0$ sein. Das bedeutet $g = g_1^k \in G_1$. wir haben $G_2 \subset G_1$ gezeigt, im Widerspruch zu $G_2 \neq G_1$. □

Aufgabe 2.12 (F 01, T1, A3) *Für ein Element r eines assoziativen Ringes R mit 1, das ein Rechtsinverses s in R besitzt, sind äquivalent:*

(1) r hat mindestens zwei verschiedene Rechtsinverse in R;

(2) r ist ein Linksnullteiler in R;

(3) r hat kein Linksinverses in R.

Aufgabe 2.13 (H 99, T1, A3) *Seien a und b Elemente eines assoziativen kommutativen Integritätsrings R. Es bezeichne α die Restklasse von a in $R/(b)$ und β die von b in $R/(a)$. Zeigen Sie: Ist α kein Nullteiler von $R/(b)$, so ist β keiner von $R/(a)$.*

Aufgabe 2.14 (H 99, T3, A3) *Es bezeichne $M_4(\mathbb{Q})$ den Ring aller rationalen 4×4-Matrizen und R die Menge aller $A \in M_4(\mathbb{Q})$ der Form $A = \begin{pmatrix} a & d & c & b \\ b & a & d & c \\ c & b & a & d \\ d & c & b & a \end{pmatrix}$. Es sei $E \in M_4(\mathbb{Q})$ die Einheitsmatrix und $P = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$.*

a) Zeigen Sie, dass $P^4 = E$ ist, und dass jedes $A \in R$ in der Form

$$A = a_0 E + a_1 P + a_2 P^2 + a_3 P^3$$

mit rationalen a_k dargestellt werden kann ($k = 0, ..., 3$).

b) Zeigen Sie, dass R ein kommutativer Teilring von $M_4(\mathbb{Q})$ ist.

c) Zeigen Sie, dass R isomorph ist zu einem Produkt von drei Körpern, und bestimmen Sie diese Körper.

Aufgabe 2.15 (F 99, T2, A2) *Seien $Mat(2 \times 2, \mathbb{R})$ der Ring aller reellen 2×2-Matrizen, $A \in Mat(2 \times 2, \mathbb{R})$ eine Matrix, und $\mathbb{R}[A] \subset Mat(2 \times 2, \mathbb{R})$ der von A und $\mathbb{R}$ erzeugte Teilring. Man zeige, dass dann (in Abhängigkeit von A) genau einer der folgenden $\mathbb{R}$-linearen Ringisomorphismen existiert:*

$$i)\, \mathbb{R}[A] \simeq \mathbb{R}, \quad ii)\, \mathbb{R}[A] \simeq \mathbb{R} \times \mathbb{R}, \quad iii) \mathbb{R}[A] \simeq R[X]/(X^2), \quad \mathbb{R}[A] \simeq \mathbb{C}.$$

Aufgabe 2.16 (F 99, T3, A2) *Man beweise oder widerlege die Behauptung*

$$x^{200} \equiv x^8 \, mod \, 221 \text{ für alle } x \in \mathbb{Z}.$$

Aufgabe 2.17 (H 98, T2, A2) *Im Ring $M_3(\mathbb{Q})$ der dreireihigen Matrizen über $\mathbb{Q}$ sei R der von der Einheitsmatrix E und von der Matrix*

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 3 & -6 & 18 \\ 1 & -2 & 6 \end{pmatrix}$$

erzeugte Unterring. Ist R isomorph zu einem direkten Produkt von Körpern? Geben Sie alle $X \in R$ mit $X^2 = X$ und alle $Y \in R$ mit $Y^2 = 0$ an. (Hinweis: Fassen Sie R als Faktorring eines Polynomrings auf.)

Aufgabe 2.18 (F 97, T1, A4) *Sei R ein kommutativer Ring mit Einselement. Ein Ideal $I \subset R$ heißt* Primideal, *falls der Restklassenring R/I nullteilerfrei ist. Es heißt ein* Primärideal, *falls für jeden Nullteiler $\bar{a}$ in R/I eine Potenz $\bar{a}^m = 0$ in R/I ist. Das Radikal $\sqrt{I}$ des Ideals I besteht aus allen $a \in R$, für die es eine natürliche Zahl k mit $a^k \in I$ gibt.*

Sei $R = \mathbb{Z}$ und $I = (n)$ das von der natürlichen Zahl $n \geq 0$ erzeugte Hauptideal in $\mathbb{Z}$. Geben Sie notwendige und hinreichende Bedingungen dafür an, dass

a) I ein Primideal ist;

b) I ein Primärideal ist;

c) $\sqrt{I} = I$ gilt.

Aufgabe 2.19 (H 95, T3, A1) *Es sei K ein Körper und R die Menge aller 2×2-Matrizen, die mit $\begin{pmatrix} 0 & -2 \\ 1 & 1 \end{pmatrix}$ vertauschbar sind. Zeigen Sie:*

a) R ist Unterring von $M(2 \times 2, K)$ und R ist kommutativ.

b) Es existiert ein $f \in K[X]$ mit $R \simeq K[X]/(f)$.

c) Für $K = \mathbb{Q}$ und $K = \mathbb{Z}/3\mathbb{Z}$ ist R ein Körper. Für $K = \mathbb{Z}/11\mathbb{Z}$ ist R kein Körper.

Aufgabe 2.20 (H 95, T3, A2c)) *Wieviele maximale Ideale hat der Restklassenring $\mathbb{Z}/1995\mathbb{Z}$?*

Aufgabe 2.21 (H 93, T2, A2) *a) Zeigen Sie: Jeder Ring R mit Einselement ist vermöge*

$$R \to End \, R^+, \quad a \mapsto (L_a : x \mapsto ax)$$

isomorph zum einem Unterring des Isomorphismenrings seiner additiven Gruppe R^+.

b) Zu einem beliebigen Ring Q seien auf der Menge $S_Q := \{(m, a) | \, m \in \mathbb{Z}, a \in Q\}$ die Verknüpfungen

$$(m, a) + (n, b) := (m + n, a + b), \quad (m, a) \cdot (n, b) := (mn, ab + mb + na)$$

definiert. Zeigen Sie: Dadurch erhält S_Q die Struktur eines Ringes mit Einselement. Der Ring S_Q ist kein Integritätsbereich, falls Q ein Einselement besitzt.

c) Kann ein beliebiger Ring Q als Unterring eines Endomorphismenringes aufgefasst werden?

Aufgabe 2.22 (F 93, T1, A2) *Zeigen Sie, dass der Ring der Gaußschen Zahlen*

$$\mathbb{Z}[i] = \{a + bi |\, a, b \in \mathbb{Z}\}, \quad i = \sqrt{-1},$$

aus genau denjenigen Elementen des Körpers $\mathbb{Q}(i)$ besteht, die einer normierten Gleichung

$$X^2 + cX + d = 0$$

mit ganzen Koeffizienten $c, d \in \mathbb{Z}$ genügen.

Aufgabe 2.23 (F 91, T2, A2) *Sei R ein Integritätsring. Man beweise: R ist ein Körper, wenn jeder von einem Element erzeugte Unterring von R nur endlich viele Elemente enthält.*

Aufgabe 2.24 (F 90, T1, A3) *Sei K ein Körper und $m \in K$. Man betrachte folgende Menge des Matrizenrings $M(2 \times 2, K)$:*

$$L_m := \left\{ \begin{pmatrix} a & b \\ mb & a \end{pmatrix} : \, a, b \in K \right\}.$$

a) Man zeige: L_m ist bezüglich der Matrizen-Addition und -Multiplikation ein kommutativer Ring.

b) Man beweise: Genau dann ist L_m ein Körper, wenn m kein Quadrat in K ist.

c) Sei speziell $K = \mathbb{F}_p$ mit einer ungeraden Primzahl p. Man zeige, dass es stets ein $m \in \mathbb{F}_p$ gibt, das der Bedingung in b) genügt. Welcher Körper entsteht dabei?

Aufgabe 2.25 (F 90, T2, A3) *$R = C[a, b]$ ist der Ring der auf $[a, b]$ stetigen reellwertigen Funktionen. Beweisen Sie: Eine Funktion f ist genau dann Nullteiler von R, wenn*

$$N_f := \{x |\, x \in [a, b],\, f(x) = 0\}$$

ein offenes Intervall enthält.

2.3 Teilbarkeit

In diesem Abschnitt bedeutet 'Ring' stets 'kommutativer, nullteilerfreier Ring mit Eins'. Wir wollen den Begriff der Teilbarkeit vom Ring $\mathbb{Z}$ auf einen solchen Ring R verallgemeinern. Unser eigentliches Ziel ist das Lösen von Polynom-Gleichungen. Aber Teilbarkeit von Polynomen ist eine allgemeinere Fragestellung im folgenden Sinn:

Satz 2.12 *Es seien R ein Ring, p ein Polynom im Ring $R[X]$ und $a \in R$. Dann sind äquivalent:*

a) $p(a) = 0$;

b) das Polynom p spaltet den Linearfaktor $X - a$ ab, d.h., es gibt ein Polynom $q \in R[X]$ mit $p = q \cdot (X - a)$.

Beweis. Die Richtung b) $\Rightarrow$ a) ist offensichtlich. Die Richtung a) $\Rightarrow$ b) ist Satz 2.1 (Vieta) $\square$

Die natürliche Zahl $n \in \mathbb{N}$ heißt durch $m \in \mathbb{N}$ teilbar, wenn ein $q \in \mathbb{N}$ existiert mit $n = q \cdot m$. Man schreibt dafür $m|n$. Genau dieselbe Definition funktioniert für alle ganzen, nicht notwendig positiven Zahlen $m, n \in \mathbb{Z}$. Weil das aber nur eine Sache des Vorzeichens ist, kümmert man sich meist nicht um Teilbarkeit bei negativen Zahlen. Auf die beiden Zahlen $\pm 1 \in \mathbb{Z}$ kommt es nicht so furchtbar an. Bei Ringen ist das i.A. anders:

Definition 2.12 *Ein Element e des Rings R heißt* Einheit *, wenn e in R invertierbar (bezüglich der Multiplikation) ist, d.h., wenn es ein $e^{-1} \in R$ gibt mit $e \cdot e^{-1} = 1$.*

Sind e_1, e_2 Einheiten in einem Ring R, so auch $e_1 e_2$ und e_1^{-1}. Die Einheiten eines Rings R bilden also eine Gruppe unter der Multiplikation.

Definition 2.13 *Die Gruppe $R^* \subset R$ der Einheiten eines Rings R heißt seine Einheitengruppe.*

Beispiel 2.12 *Einheiten im Ring $\mathbb{Z}$ sind genau die beiden Zahlen ± 1.*
Einheit in einem Körper ist jedes Element $e \neq 0$.
Einheiten des Polynomrings $R[X]$ über einem Ring R sind genau die Einheiten von R.

Beispiel 2.13 *Sei $R = \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \subset \mathbb{C}$ der Ring der ganzen Gaußschen Zahlen. Die Zahl $e = a + bi$ ist eine Einheit in diesem Ring, wenn es $e' = a' + b'i \in R$ gibt mit*

$$ee' = (a + bi)(a' + b'i) = aa' - bb' + (ab' + ba')i = 1.$$

Für jede Gaußsche Zahl $e = a + bi$ ist $|e|^2 = a^2 + b^2 \in \mathbb{Z}$. Aus $|ee'| = |e||e'|$ folgt $|e|^2 \cdot |e'|^2 = |1|^2 = 1$. Also ist $|e|^2 = 1$ und entweder $a = \pm 1$, $b = 0$ oder $a = 0$, $b = \pm 1$. Die Einheiten in $\mathbb{Z}[i]$ sind also genau die vier Zahlen $\pm 1, \pm i$.

Beispiel 2.14 *Etwas komplizierter wird es schon, wenn wir die Einheiten im Ring $\mathbb{Z}[\sqrt{2}]$ bestimmen wollen. Eine Zahl*

$$a + b\sqrt{2},\ a, b \in \mathbb{Z},$$

ist genau dann eine Einheit in diesem Ring, wenn $c, d \in \mathbb{Z}$ existieren mit

$$1 = (a + b\sqrt{2})(c + d\sqrt{2}) = ac + 2bd + (ad + bc)\sqrt{2}.$$

Dies ist äquivalent zu

$$ac + 2bd = 1, \quad ad + bc = 0.$$

Dann gilt aber auch

$$(a - b\sqrt{2})(c - d\sqrt{2}) = ac + 2bd - (ad + bc)\sqrt{2} = 1.$$

Auch $a - b\sqrt{2}$ ist eine Einheit, und damit auch das Produkt

$$(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2 \in \mathbb{Z}.$$

Eine Zahl $c \in \mathbb{Z}$ kann nur dann Einheit in $\mathbb{Z}[\sqrt{2}]$ sein, wenn sie es in $\mathbb{Z}$ ist, also, wenn $c = \pm 1$. Für die Einheit $a + b\sqrt{2}$ muss also notwendigerweise $a^2 - 2b^2 = \pm 1$ gelten. Davon gilt aber auch die Umkehrung: Wenn $a^2 - 2b^2 = \pm 1$, dann ist $(a+b\sqrt{2})(a-b\sqrt{2}) = a^2 - 2b^2 = \pm 1$ und $a + b\sqrt{2}$ ist eine Einheit. Das ist die erste, allerdings sehr implizite Charakterisierung der Einheiten im Ring $\mathbb{Z}[\sqrt{2}]$:

Die Zahl $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, $a, b \in \mathbb{Z}$, ist genau dann eine Einheit in diesem Ring, wenn $a^2 - 2b^2 = \pm 1$.

Damit ist allerdings die Struktur der Einheitengruppe noch nicht aufgeklärt. Dazu überlegen wir uns zunächst:

Die Abbildung $N : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}$, $a + b\sqrt{2} \mapsto a^2 - 2b^2$ ist multiplikativ, d.h., $N(cc') = N(c)N(c')$. *Das folgt aber sofort aus $N(a + b\sqrt{2}) = (a + b\sqrt{2})(a - b\sqrt{2})$. Insbesondere ist die Abbildung*

$$N : (\mathbb{Z}[\sqrt{2}])^* \to \{\pm 1\}$$

ein Gruppen-Homomorphismus. Wegen $N(1) = 1$ und $N(1 + \sqrt{2}) = -1$ ist dieser surjektiv. Wir kümmern uns jetzt um den Kern dieses Homomorphismusses:

Die Zahl $a+b\sqrt{2}$, $a, b \geq 0$, mit $a^2 - 2b^2 = 1$ ist genau dann eine Einheit, wenn sie eine Potenz von

$$3 + 2\sqrt{2} = (1 + \sqrt{2})^2$$

ist.

Beweis. Falls $b = 0$ ist $a = 1 = (1 + \sqrt{2})^0$. Andernfalls ist $b \geq 1$ und wegen $a^2 = 1 + 2b^2$ sogar $b \geq 2$. Dann berechnen wir

$$(a + b\sqrt{2})(3 + 2\sqrt{2})^{-1} = (a + b\sqrt{2})(3 - 2\sqrt{2}) = 3a - 4b + (-2a + 3b)\sqrt{2}.$$

Aus $a = \sqrt{2b^2 + 1}$ und $a, b \geq 0$ folgt

$$(3a)^2 = 18b^2 + 9 > 4b^2, \quad 3a - 2b \geq 0.$$

Aus $b \geq 2$ folgt

$$(3b)^2 - (2a)^2 = 9b^2 - (8b^2 + 4) \geq 0, \quad 3b \geq 2a.$$

Auch der Koeffizient $-2a + 3b$ ist ≥ 0. Und außerdem ist wegen $3a - 4b < a \Leftrightarrow 4b > 2a$ nach Multiplikation mit der Einheit $3 - 2\sqrt{2}$ der Koeffizient a echt kleiner geworden, solange nur $b > 0$. Weil das nicht ewig so weiter gehen kann, kommen wir dabei irgend wann auf den Fall $b = 0$ und $a = 1$. Wir haben

$$(a + b\sqrt{2})(3 - 2\sqrt{2})^k = 1$$

für ein geeignetes $k \geq 0$ bewiesen, bzw. $a + b\sqrt{2} = (3 + 2\sqrt{2})^k$.

Es folgt für $a^2 - 2b^2 = 1$, $a, b \geq 0$, dass auch $a - b\sqrt{2} = (3 - 2\sqrt{2})^k$. Es sind also alle Einheiten $a + b\sqrt{2}$ mit $a^2 - 2b^2 = 1$, $a \geq 0$, ganzzahlige Potenzen von $3 + 2\sqrt{2}$. Alle Einheiten mit $a \geq 0$ sind dann ganzzahlige Potenzen von $1 + \sqrt{2}$. Und alle beliebigen Einheiten in $(\mathbb{Z}[\sqrt{2}])^*$ sind von der Form

$$\pm(1 + \sqrt{2})^k, \quad k \in \mathbb{Z}.$$

Die Einheitengruppe ist eine direkte Summe der zyklischen Gruppe $\{\pm 1\}$ und der freien zyklischen Gruppe erzeugt von $1 + \sqrt{2}$.

Definition 2.14 *Zwei Ring-Elemente $r, s \in R$ heißen* assoziiert, *wenn es eine Einheit $e \in R$ gibt mit $s = er$.*

Weil die Einheiten eine Gruppe bezüglich der Multiplikation bilden, ist klar, dass diese Assoziiertheit von Ring-Elementen eine Äquivalenzrelation ist.

Satz 2.13 *Zwei Ring-Elemente r und s erzeugen genau dann dasselbe Haupt-Ideal $(r) = (s)$, wenn sie assoziiert sind.*

Beweis. Seien r und s assoziiert, also $s = er$ mit einer Einheit e. Dann gilt $s \in (r)$ und deswegen $(s) \subset (r)$. Aus $r = e^{-1}s$ folgt ebenso $(r) \subset (s)$.

Sei $(r) = (s)$, also $r = as$ und $s = br$. Es folgt $r = (ab)r$ und $(1 - ab)r = 0$. Wenn $r = 0$ ist, folgt aus $(r) = (s)$, dass auch $s = 0$ ist. $ab = 1$. Also sind a und b Einheiten, r und s sind assoziiert. □

Definition 2.15 *Es seien r und s zwei Elemente des Rings R. Man sagt, r teilt s, in Zeichen $r|s$, wenn es ein $q \in R$ gibt mit $r \cdot q = s$. (Weil R nullteilerfrei vorausgesetzt ist, ist q durch r und s eindeutig bestimmt.)*

Beispiel 2.15 *Die Teiler der Eins $1 \in R$ sind genau die Einheiten.*

Die Teilbarkeit $r|s$ ist äquivalent zur Inklusion $(s) \subset (r)$ der Hauptideale.
Diese Teilbarkeitsrelation hat folgende triviale Eigenschaften:

- $a|a, \quad 1|a, \quad a|0$;
- $a|b$ und $b|c \Rightarrow a|c$;
- $a|b$ und $c|d \Rightarrow ac|bd$;
- $a|b$ und $a|c \Rightarrow a|(b + c)$;
- $ac|bc$ und $c \neq 0 \Rightarrow a|b$.

Mit diesem Teilbarkeits-Begriff kann man wie in der Schule größte gemeinsame Teiler und kleinste gemeinsame Vielfache definieren:

Definition 2.16 *Es seien $s_1, ..., s_k \in R$.*

$r \in R$ heißt ein $ggT(s_1, ..., s_k)$ wenn gilt: r teilt $s_1, ..., s_k$, und teilt auch $r' \in R$ die Elemente $s_1, ..., s_k$, so gilt $r'|r$. Die Ringelemente $s_1, ..., s_k$ heißen teilerfremd, *wenn $ggT(s_1, ..., s_k) = 1$.*

$r \in R$ heißt ein $kgV(s_1, ..., s_k)$ wenn gilt: $s_1, ..., s_k$ teilen r, und teilen $s_1, ..., s_k$ auch r', so gilt $r|r'$.

Bemerkung: Wenn $ggT(s_1, ..., s_k) = r$ und $ggT(s_1, ..., s_k) = r'$, dann sind die Ringelemente r und r' assoziiert. Ebenso folgt aus $r = kgV(s_1, ..., s_k)$ und $r' = kgV(s_1, ..., s_k)$, dass r und r' assoziiert sind.

Wir haben ggT und kgV wohl definiert, über deren Existenz aber überhaupt nichts bewiesen. Dazu brauchen wir eine neue Eigenschaft des Rings R:

Definition 2.17 *Der Ring R heißt* Hauptideal-Ring, *wenn jedes Ideal $I \subset R$ ein Hauptideal ist.*

Beispiel 2.16 *Der Ring $\mathbb{Z}$ ist ein Hauptideal-Ring nach Satz 2.3.*

Das Verfahren, mit dem wir gezeigt haben, dass jedes Ideal in $\mathbb{Z}$ ein Hauptideal ist, kann man wie folgt formalisieren.

Definition 2.18 *Der Ring R heißt* euklidisch, *wenn es eine Abbildung*

$$R \to \mathbb{N}, \quad r \mapsto |r|$$

gibt mit

- $|r| = 0$ *genau dann, wenn* $r = 0$*;*
- *Division mit Rest: Zu je zwei Ring-Elementen $a, b \in R$, $a \neq 0$, gibt es Ring-Elemente $q, r \in R$ so, dass*
$$b = q \cdot a + r \text{ und } |r| < |a|.$$

Beispiel 2.17 *Der Ring $\mathbb{Z}$ ist euklidisch. Dabei ist $|r|$ der übliche Absolutbetrag.*

Beispiel 2.18 *Auch der Polynomring $K[X]$ über einem Körper ist euklidisch, wenn man setzt:*

$$|p(X)| := \begin{cases} 1 + Grad(p) \text{ falls } p \neq 0, \\ 0 \text{ falls } p = 0. \end{cases}$$

Im Polynomring $K[X]$ gibt es ja die Division mit Rest

$$b = qa + r,\ Grad(r) < Grad(a), \quad \text{also} \quad |r| < |a|.$$

Satz 2.14 *Jeder euklidische Ring ist ein Hauptideal-Ring.*

Beweis. Sei R ein euklidischer Ring und $I \subset R$ ein Ideal. Weil das Null-Ideal (0) ein Hauptideal ist können wir annehmen, dass I Elemente $a \neq 0$ enthält. Sei $a \in I$ ein Element $\neq 0$ und so, dass $|a|$ minimal unter allen Elementen $\neq 0$ aus I ist. Wir behaupten $I = (a)$.

Sei also $b \in I$ und

$$b = qa + r,\ |r| < |a|$$

die Division durch a mit Rest r. Wegen $b \in I$ und $qa \in I$ ist auch $r \in I$. Weil $|a| \neq 0$ minimal war, muss $|r| = 0$ gelten, d.h., $r = 0$. Es folgt $b = qa \in (a)$. □

Satz 2.15 *In einem Hauptideal-Ring existieren $t = ggT(s_1, ..., s_k)$ und $v = kgV(s_1, ..., s_k)$. Es ist*

$$(t) = (s_1, ..., s_k) \quad \text{und} \quad v = (s_1) \cap ... \cap (s_k).$$

Beweis. Nach Voraussetzung sind $(s_1, ..., s_k) =: (t)$ und $(s_1) \cap ... \cap (s_k) =: (v)$ Hauptideale.

Wegen $s_i \in (t)$ ist t ein Teiler von s_i für $i = 1, ..., k$. Ist t' ein weiterer Teiler von $s_1, ..., s_k$, so gilt

$$(t) = (s_1, ..., s_k) \in (t')$$

und $t'|t$.

Wegen $v \in (s_i)$ gilt $s_i|v$ für $i = 1, ..., k$. Ist v' ein weiteres Ring-Element mit dieser Eigenschaft, so gilt

$$v' \in (s_1) \cap ... \cap (s_k) = (v)$$

und $v|v'$. □

Man kann die iterierte Division mit Rest auch benützen, um den ggT konkret auszurechnen. Dieses Verfahren heißt *euklidischer Algorithmus*. Ich möchte hier kein abstraktes Rezept formulieren, sondern an einem Beispiel zeigen, wie das funktioniert:

Gesucht sei im Ring $\mathbb{Z}$ der ggT von 701391 und 70851. Wir iterieren die Division mit Rest:

$$\begin{aligned} 701391 &= 9 \cdot 70851 + 63732 \\ 70851 &= 63732 + 7119 \\ 63732 &= 8 \cdot 7119 + 6780 \\ 7119 &= 6780 + 339 \\ 6780 &= 20 \cdot 339. \end{aligned}$$

Jeder gemeinsame Teiler von 701391 und 70851 teilt auch 63732, sowie 7119, 6780 und schließlich 339. Umgekehrt teilt 339 die Zahl 6780, sowie 7119, 63732, 70851 und 701391. Es folgt

$$339 = ggT(701391, 70851).$$

(Eigentlich wollte ich hier noch ein Beispiel im Ring $\mathbb{Q}[X]$ rechnen, aber meine MAPLE-Version schafft das irgendwie nicht.)

Satz 2.16 (Korollar zu Satz 2.15) *In einem Hauptideal-Ring R ist $r = ggT(s_1, ..., s_k)$ eine Linearkombination*

$$r = x_1 s_1 + ... + x_k s_k, \quad x_1, ..., x_k \in R.$$

Beweis. $r \in (s_1, ..., s_k) = \{(x_1 s_1 + ... + x_k s_k : x_1, ..., x_k \in R\}$. □

In unserem obigen Beispiel etwa ist

$$\begin{aligned} 339 &= 7119 - 6780 \\ &= 7119 - (63732 - 8 \cdot 7119) \\ &= -63732 + 9 \cdot 7119 \\ &= -63732 + 9 \cdot (70851 - 63732) \\ &= 9 \cdot 70851 - 10 \cdot 63732 \\ &= 9 \cdot 70851 - 10 \cdot (701391 - 9 \cdot 70851) \\ &= -10 \cdot 701391 + 99 \cdot 70851. \end{aligned}$$

Definition 2.19 *Ein Ring-Element $r \in R$ heißt* irreduzibel, *wenn es selbst keine Einheit in R^* ist, und wenn gilt*

$$r = ab,\ a, b \in R \quad \Rightarrow \quad a \in R^* \text{ oder } b \in R^*.$$

Das Ring-Element $r \notin R^*$ heißt prim, *wenn gilt*

$$r|a \cdot b,\ a, b \in R \quad \Rightarrow \quad r|a \text{ oder } r|b.$$

Beispiel 2.19 *Eine Zahl $0 \neq n \in \mathbb{Z}$ ist irreduzibel, genau dann wenn $n = \pm p$ mit einer Primzahl p ist. Genau dann ist n auch prim.*

Beispiel 2.20 *Weil man nach dem Fundamentalsatz der Algebra jedes Polynom $p \in \mathbb{C}[X]$ in komplexe Linearfaktoren zerlegen kann, ist p irreduzibel genau dann wenn $p = aX + b$ den Grad eins hat. Ein reelles Polynom $p \in \mathbb{R}[X]$ ist irreduzibel genau dann, wenn p den Grad eins hat oder $p = aX^2 + bX + c$ den Grad zwei und eine Diskriminante $b^2 - 4ac < 0$ hat. In diesen Fällen ist p auch immer prim.*

Allgemein gilt: *Ist $0 \neq r \in R$ prim, so ist r auch irreduzibel.*

Beweis. Sei $r \in R$ prim und $r = ab$ mit $a, b \in R$. Wegen $r|r = ab$ folgt daraus $r|a$ oder $r|b$, etwa o.B.d.A. $r|a$. Dann ist also $a = \alpha r$ und $r = ab = \alpha br$. Aus $r(1 - \alpha b) = 0$ und $r \neq 0$ folgt, weil R nullteilerfrei vorausgesetzt ist, dass $\alpha b = 1$, also $b \in R^*$. □

Die Umkehrung 'r irreduzibel $\Rightarrow$ r prim' gilt i.a. nicht. Das Standard-Beispiel dafür ist allerdings schon recht anspruchsvoll:

Beispiel 2.21 *Es sei R der Ring*

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\} \subset \mathbb{C}.$$

In diesem Ring betrachten wir die Konjugationsabbildung

$$R \to R, \quad x = a + b\sqrt{-5} \mapsto \bar{x} = a - b\sqrt{-5}.$$

Diese Abbildung ist ein Ring-Homomorphismus. Additivität ist klar. Wir weisen die Multiplikativität nach. Seien dazu

$$x = a + b\sqrt{-5} \text{ und } y = c + d\sqrt{-5} \quad \in R.$$

Wir berechnen

$$\overline{xy} = \overline{(a + b\sqrt{-5})(c + d\sqrt{-5})} = \overline{ac - 5bd + (ad + bc)\sqrt{-5}} = ac - 5bd - (ad + bc)\sqrt{-5},$$

$$\bar{x}\bar{y} = (a - b\sqrt{-5})(c - d\sqrt{-5}) = ac - 5bd - (ad + bc)\sqrt{-5}.$$

Behauptung 1: Die Zahl $2 \in R$ ist irreduzibel. *Sei etwa $2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$ mit $a, b, c, d \in \mathbb{Z}$. Daraus folgt*

$$4 = 2 \cdot \bar{2} = (a^2 + 5b^2)(c^2 + 5d^2)$$

und

- *entweder* $a^2 + 5b^2 = 1$, *also* $b = 0$ *und* $a = \pm 1$; *die Zahl* $a + b\sqrt{-5} = \pm 1$ *ist eine Einheit in* R;
- *oder* $a^2 + 5b^2 = 2$, *das geht nicht;*
- *oder* $a^2 + 5b^2 = 4$, *also* $b = 0$ *und* $a = \pm 2$; *jetzt ist* $c + d\sqrt{-5} = \pm 1$ *eine Einheit.*

Behauptung 2: Die Zahl $2 \in R$ ist nicht prim. *Das folgt aus*

$$2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

wegen $2|6$ *aber* $2 \nmid (1 + \sqrt{-5})$ *und* $2 \nmid (1 - \sqrt{-5})$.*a*

Definition 2.20 *Ein Ringelement* $a \in R$ besitzt eine Zerlegung in irreduzible Faktoren, *wenn* $a = er_1 ... r_k$ *mit* $e \in R^*$ *und* $r_1, ..., r_k \in R$ *irreduzibel.*

Das Ringelement $a \in R$ *besitzt eine* eindeutige *Zerlegung in irreduzible Faktoren, falls zusätzlich gilt: Ist*

$$a = er_1 \cdot ... \cdot r_k = e' r'_1 \cdot ... \cdot r'_{k'}, \quad e, e' \in R^*, \, r_1, ..., r'_{k'} \in R \text{ irreduzibel,}$$

dann ist $k = k'$ *und nach eventueller Umordnung* r_1 *assoziiert zu* r'_1,...,r_k *assoziiert zu* r'_k.

Ein Ring R *(kommutativ mit Eins, nullteilerfrei) heißt* faktoriell, *wenn jedes* $0 \neq a \in R$ *eine eindeutige Zerlegung in irreduzible Faktoren besitzt.*

Satz 2.17 *Im Ring* R *besitze jedes* $0 \neq a \in R$ *eine Zerlegung in irreduzible Faktoren. Dann sind äquivalent:*

1) R *ist faktoriell (d.h. die Zerlegung ist eindeutig);*

2) $r \in R$ *irreduzibel* $\Rightarrow$ r *ist prim.*

Beweis. 1) $\Rightarrow$ 2): Sei $r \in R$ irreduzibel und es gelte $r|ab$ mit $a, b \in R$. O.B.d.A. können wir $a \neq 0 \neq b$ annehmen. Dann zerlegen wir in irreduzible Faktoren

$$a = ea_1 \cdot ... \cdot a_k, \quad b = e' b_1 \cdot ... \cdot b_l, \quad ab = ee' a_1 \cdot ... \cdot a_k b_1 \cdot ... \cdot b_l$$

mit $e, e' \in R^*$ und $a_1, ..., b_l$ irreduzibel. Weil das irreduzible Ringelement r das Produkt ab teilt, gibt es eine Zerlegung $ab = r \cdot ...$ in irreduzible Faktoren. Wegen der Eindeutigkeit dieser Zerlegung muss r zu einem der irreduziblen Elemente $a_1, ..., b_l$ assoziiert sein. Es folgt $r|a$ oder $r|b$.

2) $\Rightarrow$ 1): Es werde $r \in R$ auf zwei Weisen

$$r = ea_1 \cdot ... \cdot a_k = e' b_1 \cdot ... \cdot b_l$$

in irreduzible Faktoren zerlegt. Das irreduzible a_1 teilt also das Produkt $e' b_1 \cdot ... b_l$. Wegen 2) ist a_1 prim und teilt einen der Faktoren $b_1, ..., b_l$. Nach Umordnung können wir $a_1 | b_1$ annehmen. Weil b_1 irreduzibel ist, gibt es eine Einheit $e'' \in R^*$ mit $b_1 = e'' a_1$. In der obigen Gleichung können wir a_1 kürzen und erhalten

$$ea_2 \cdot ... \cdot a_k = e' e'' b_2 \cdot ... \cdot b_l.$$

Die Behauptung ergibt sich durch Induktion nach k. □

Satz 2.18 *Der Ring R (kommutativ mit Eins, nullteilerfrei) ist genau dann faktoriell, wenn er die beiden folgenden Eigenschaften hat:*

i) Jede aufsteigende Kette

$$(r_1) \subset (r_2) \subset ... \subset (r_n) \subset (r_{n+1}) \subset ...$$

von Hauptidealen in R wird stationär, d.h., es gibt ein n mit $(r_j) = (r_n)$ für $j \geq n$.

ii) $r \in R$ irreduzibel $\Rightarrow$ r ist prim.

Beweis. Sei R faktoriell. Wegen Satz 2.17 ist dann jedes irreduzible Ringelement auch prim. Sei nun $(r_1) \subset (r_2) \subset ... \subset R$ eine aufsteigende Kette von Hauptidealen. Wenn alle $r_j = 0$ sind, ist nichts zu zeigen. Auch wenn es ein r_j mit $(r_j) = R$ gibt, ist nichts zu zeigen. Sei also o.B.d.a. $r_1 \neq 0$ und $r_1 = ea_1 \cdot ... \cdot a_k$ seine Zerlegung in irreduzible Faktoren. Sei weiter $(s) = (r_j)$ eines der Hauptideale in der Kette. Es folgt $s | ea_1 \cdot ... \cdot a_k$. Wegen der Eindeutigkeit der Faktorzerlegung von r_1 hat s eine Zerlegung, die aus einigen der irreduziblen Faktoren $a_1, ..., a_k$ von r_1 besteht. Und wenn $(r_1) \neq (s)$ ist, müssen dies weniger als k sein. Iteriert man dieses Argument, so folgt die Abbruch-Bedingung i).

Seien jetzt i) und ii) vorausgesetzt. Wegen Satz 2.17 müssen wir zeigen: jedes $0 \neq r \in R$ besitzt eine Zerlegung in irreduzible Faktoren. Sei M die Menge der Hauptideale $(r) \subset R$, wo r keine solche Zerlegung besitzt. Wenn $M \neq \emptyset$ ist, gibt es eine echt aufsteigende Kette $(r_1) \subset (r_2) \subset ...$ von Hauptidealen $(r_i) \in M$, die wegen Eigenschaft i) abbricht. Es gibt also ein maximales Element $(r) \in M$. Weil r keine Zerlegung in irreduzible Faktoren zulässt, ist r keine Einheit und auch nicht irreduzibel. Es ist also $r = ab$, wo weder a noch b zu r assoziiert sind. Das heißt

$$(r) \subset (a),\ (r) \subset (b), \quad (r) \neq (a),\ (r) \neq (b).$$

Weil $(r) \in M$ maximal war, gehört weder (a) noch (b) zu M. Beide Elemente a und b besitzen also eine Zerlegung in irreduzible Faktoren. Dann besitzt auch ihr Produkt $r = ab$ eine solche Zerlegung. Widerspruch! □

Satz 2.19 *Jeder Hauptidealring (kommutativ mit Eins, nullteilerfrei) ist faktoriell.*

Beweis. Wir weisen die Eigenschaften i) und ii) aus Satz 2.18 nach.

i) Sei $(r_1) \subset (r_2) \subset ... \subset R$ eine Kette von Hauptidealen. Auch deren Vereinigung

$$I := \bigcup_j (r_j) \subset R$$

ist ein Ideal, und damit ein Hauptideal (r). Das Ringelement r gehört zu einem der Ideale in der Kette, etwa $r \in (r_n)$. Für alle $j \geq n$ ist dann

$$(r_j) \subset I = (r) \subset (r_n) \subset (r_j),$$

also $(r_j) = (r_n)$.

ii) Sei $r \in R$ irreduzibel und $r | ab$ mit $a, b \in R$. Weil R ein Hauptidealring ist, gibt es $t = ggT(r, a)$. Wenn r das Element a nicht teilt, kann r nicht assoziiert zu t sein. Weil r

irreduzibel ist, muss deswegen $t \in R^*$ eine Einheit sein. Dann ist $(r, a) = (1)$ und es gibt $x, y \in R$ mit $1 = xr + ya$. Daraus folgt

$$b = xbr + yab, \quad r|b.$$

Also ist r prim. □

Bemerkung: Die Umkehrung von Satz 2.19, dass nämlich Hauptidealring aus der Eigenschaft faktoriell folgt, das gilt nicht!

Satz 2.20 *Der Ring $R[X]$ ist genau dann ein Hauptidealring, wenn R ein Körper ist.*

Beweis. Wenn R ein Körper ist, dann ist $R[X]$ euklidisch, und $R[X]$ ein Hauptidealring, vgl. Beispiel 2.18.

Es sei $0 \neq r \in R$. Wir betrachten das Ideal (r, X). Wäre es ein Hauptideal, gäbe es ein Polynom $p(X) \in R[X]$ mit $(r, X) = p$. Es folgt $p(X)|r$ und $p \in R$. Aus $p|X$ folgt $p \in R$ ist eine Einheit, also $(r, X) = (1) = R[X]$. Insbesondere ist $1 = a \cdot r + b \cdot X$ mit $a, b \in R[X]$. Auf diese Gleichung wenden wir den Ring-Homomorphismus

$$\varphi : R[X] \to R, \quad \varphi : g(X) \mapsto g(0),$$

an. Aus $\varphi(1) = 1$ und $\varphi(r) = r$ folgt

$$1 = \varphi(a)r + \varphi(b)\varphi(X) = \varphi(a)r.$$

Also ist r eine Einheit. Der Ring R enthält außer (0) und (1) keine anderen Ideale und ist nach Satz 2.8 ein Körper. □

Beispiel 2.22 *Insbesondere ein Polynomring $K[X]$ ist nie ein Körper, weil X kein Inverses hat. Deswegen ist der Polynomring in zwei Unbestimmten $K[X, Y] = K[X][Y]$ kein Hauptidealring. Natürlich ist auch ein Polynomring $K[X_1, ..., X_n]$ in $n \geq 2$ Unbestimmten kein Hauptidealring.*

Ist $r \in R$ prim, so ist der Faktorring $R/(r)$ nullteilerfrei.

Beweis. Seien $a + (r)$, $b + (r) \in R/(r)$ Restklassen mit Produkt

$$(a + (r)) \cdot (b + (r)) = ab + (r) = 0 \in R/(r).$$

Das bedeutet $ab \in (r)$ und $r|ab$. Weil r prim ist, teilt r entweder a, dann ist $a + (r) = 0 \in R/(r)$ oder b, und dann ist $b + (r) = 0 \in R/(r)$. □

Definition 2.21 *Das Ideal $I \subset R$ heißt* Primideal*, wenn der Faktorring nullteilerfrei ist.*

Anders ausgedrückt: I ist Primideal, wenn aus $ab \in I$ folgt, dass entweder $a \in I$ oder $b \in I$. Ein Hauptideal (r) ist genau dann ein Primideal, wenn das Element $r \in R$ prim ist.

Satz 2.21 *Jedes maximale Ideal $I \subset R$ ist ein Primideal.*

Beweis. Nach Satz 2.9 ist der Faktorring R/I ein Körper und damit nullteilerfrei. □

Noch so eine Definition, die ich nicht bringen würde, wenn sie nicht in (einigen wenigen) Staatsexamensaufgaben vorkäme.

Definition 2.22 *Ein* R-Modul *ist eine Menge* M*, zu der sich der Ring* R *verhält, wie ein Körper* K *zu einem* K*-Vektorraum. D.h. also, es gibt eine Abbildung*

$$R \times M \to M$$

mit allen möglichen Eigenschaften, die ich hier nicht aufschreiben möchte. Schauen Sie sich die Eigenschaften in der Definition des K*-Vektorraums an!*

Beispiel 2.23 *Ist* R *ein Unterring des Rings* S*, so ist* S *ein* R*-Modul. Jedes Ideal* $I \subset R$ *ist ein* R*-Modul und jeder Faktorring* R/I *auch.*

Aufgabe 2.26 (F 99, T1, A3) *Sei* R *ein kommutativer Ring mit Einselement und* $S \supset R$ *ein kommutativer Oberring von* R*, das Einselement von* R *sei auch das Einselement von* S*.*

a) Man zeige: Ist $I \subset S$ *ein Ideal von* S*, so ist* $I \cap R$ *ein Ideal von* R*.*

b) Sei $I \subset S$ *ein Ideal. Man untersuche, welche der folgenden Implikationen wahr sind:*

i) I *Primideal in* $S \Longrightarrow I \cap R$ *Primideal in* R*.*

ii) $I \cap R$ *Primideal in* $R \Longrightarrow I$ *Primideal in* S*.*

(Beweis oder Gegenbeispiel!)

Aufgabe 2.27 (F 99, T3, A3) *Gegeben sei der Teilring* $R = \mathbb{Z} + \mathbb{Z}\sqrt{5}$ *von* $\mathbb{C}$*.*

a) Man zeige, dass in R *jedes von* (0) *verschiedene Primideal maximal ist.*

b) R^* *bezeichne seine Einheitengruppe. Man zeige:*

Für alle $\epsilon = x + y\sqrt{5} \in R^*$ *gilt* $x^2 - y^2 5 = \pm 1$*.*

Aufgabe 2.28 (H 99, T1, A2) *a) Sei* p *eine ungerade Primzahl und* $\nu \in \mathbb{Z}, \nu > 0$*. Zeigen Sie, dass die Gleichung* $X^2 = 1$ *im Ring* $\mathbb{Z}/(p^\nu)$ *genau 2 Lösungen besitzt.*

b) Sei $n = p_1^{\nu_1} \cdot ... \cdot p_s^{\nu_s}$ *mit paarweise verschiedenen ungeraden Primzahlen* p_i *und positiven ganzen Zahlen* $\nu_i (i = 1, ..., s)$*. Ferner sei* a *eine Einheit des Rings* $\mathbb{Z}/(n)$*. Zeigen Sie, dass die Gleichung* $X^2 = a$ *in* $\mathbb{Z}/(n)$ *eintweder keine oder genau* 2^s *verschiedene Lösungen besitzt.*

Aufgabe 2.29 (H 99, T2, A2) *Sei* $R = \mathbb{R}[[X]]$ *der Ring der formalen Potenzreihen mit reellen Koeffizienten. Man zeige:*

a) Jede Potenzreihe $a = a_0 + a_1 X + a_2 X^2 + ...$ *mit* $a_0 \neq 0$ *ist eine Einheit in* R*.*

b) R *ist Hauptidealring.*

c) Es gibt genau ein maximales Ideal in R*.*

d) Es gibt genau zwei Primideale in R*.*

e) Der Quotientenkörper Q *von* R *besitzt als* R*-Modul ein abzählbares Erzeugendensystem.*

Aufgabe 2.30 (H 99, T2, A3) *a) Seien R ein Integritätsring und $a \in R$. Man zeige: Das Polynom $X^2 + a$ ist genau dann reduzibel in $R[X]$, wenn $-a$ ein Quadrat in R ist.*

b) Sei K ein Körper, der nicht die Charakteristik 2 besitzt. Man zeige: Für alle $n \in \mathbb{N}, n \geq 3$, ist das Polynom $X_1^2 + X_2^2 + ... + X_n^2$ im Polynomring $K[X_1, ..., X_n]$ irreduzibel.

Aufgabe 2.31 (H 97, T3, A2) *Sei $R = \{f \in \mathbb{R}[X];\ f(0) \in \mathbb{Q}\}$ der Ring aller Polynome mit reellen Koeffizienten, deren konstantes Glied rational ist. Zeigen Sie:*

a) Das Element X ist im Ring R unzerlegbar, aber kein Primelement.

b) Jede aufsteigende Folge $I_1 \subseteq I_2 \subseteq ... \subseteq I_n \subseteq ...$ von Hauptidealen wird stationär.

c) Das Ideal $I = \{f \in R : f(0) = 0\}$ von R ist nicht endlich erzeugt.

Aufgabe 2.32 (F 97, T1, A1a)) *Zu welchem direkten Produkt zyklischer Gruppen ist die Einheitengruppe des Rings $\mathbb{Z}/255\mathbb{Z}$ isomorph?*

Aufgabe 2.33 (F 97, T2, A3b)) *Ist $1997^{1997} - 4$ durch 7 teilbar?*

Aufgabe 2.34 (H 96, T2, A3) *Zeigen Sie, dass der Ring $Z[\sqrt{-31}] = \{a + b\sqrt{-31} | a, b$ ganze Zahlen $\}$ nicht faktoriell ist, d.h. keine Primfaktorzerlegung hat. Verwenden Sie etwa, dass $32 = (1 + \sqrt{-31})(1 - \sqrt{-31})$.*

Aufgabe 2.35 (H 96, T3, A2) *Man definiere für einen kommutatvien Ring die Begriffe ,,irreduzibles Element", ,,Primelement" und ,,Primideal" und zeige, dass in einem Integritätsring A mit 1 für ein Element $p \in A$ gilt:*

a) p Primelement $\Rightarrow$ p irreduzibel

b) p Primelement $\Leftrightarrow$ (p) Primideal $\neq 0$

c) p irreduzibel $\Leftrightarrow$ Es gilt $0 \neq (p) \subset A, (p) \neq A$, und es existiert kein $a \in A$ mit $(p) \subset (a) \subset A, (p) \neq (a) \neq A$.

Aufgabe 2.36 (F 96, T2, A1) *Es sei a eine zu 10 teilerfremde natürliche Zahl. Man zeige, dass unendlich viele Zahlen 1, 11, 111, 1111, ... durch a teilbar sind.*

Aufgabe 2.37 (F 96, T2, A3) *Es sei I die Menge aller Polynome $f \in \mathbb{Q}[X]$ mit $f(0) = f'(0) = 0$.*

a) Man zeige, dass I ein Ideal von $\mathbb{Q}[X]$ ist.

b) Geben Sie ein erzeugendes Element für das Ideal I an.

c) Ist I ein Primideal?

Aufgabe 2.38 (F96, T3, A2) *Im Ring $R := \mathbb{Z}[\sqrt{-3}]$ sei die Norm eines Elementes $x = a + b\sqrt{-3}$ definiert durch:*

$$N(a + b\sqrt{-3}) := (a + b\sqrt{-3})(a - b\sqrt{-3}) = a^2 + 3b^2.$$

Zeigen Sie:

a) $x \in R$ ist eine Einheit in R genau dann, wenn $N(x) = 1$ gilt, und dies gilt genau dann, wenn $x = \pm 1$.

b) 2 ist ein irreduzibles Element in R, das heißt, es gibt keine Zerlegung $2 = xy$, *wobei* $x, y \in R$ *beide keine Einheiten in R sind.*

c) Das von 2 und $1 + \sqrt{-3}$ *in R erzeugte Ideal ist kein Hauptideal.*

d) 2 ist kein Primelement in R.

Aufgabe 2.39 (F 95, T2, A3) *Sei R der Integritätsbereich*

$$R := \mathbb{Z}[\sqrt{-5}].$$

Man zeige:

a) Für Elemente $x := x_1 + x_2\sqrt{-5} \neq 0$ *und* $y := y_1 + y_2\sqrt{-5}$ *von R gilt:*
$x|y \iff x_1^2 + 5x_2^2$ *ist gemeinsamer Teiler von* $x_1y_1 + 5x_2y_2$ *und* $y_2x_1 - y_1x_2$ *in* $\mathbb{Z}$.

b) Die Einheitengruppe von R ist $R^* = \{\pm 1\}$.

c) Jede Nichteinheit $\neq 0$ *aus R ist Produkt von irreduziblen Elementen.*

d) R ist nicht faktoriell.

Aufgabe 2.40 (H 94, T1, A3) *Gegeben sei der Teilring* $R = \mathbb{Z} + \mathbb{Z}\sqrt{2}$ *von* $\mathbb{C}$. R^* *bezeichne seine Einheitengruppe. Man zeige:*

a) Für alle $\epsilon = x + y\sqrt{2} \in R^*$ *gilt* $x^2 - y^2 2 = \pm 1$.

b) Für alle $\epsilon = x + y\sqrt{2} \in R^*$ *gilt:* $(\epsilon > 1 \Rightarrow x, y > 0)$,

c) $\mathrm{Min}\{\epsilon \in R^* | \epsilon > 1\} = 1 + \sqrt{2}$,

d) $R^* = \{\pm(1 \pm \sqrt{2})^n | n \in \mathbb{N}\}$.

Aufgabe 2.41 (H 94, T1, A5) *Sei x ein Geldbetrag (in Mark und Pfennig) unter 100 Mark mit folgender Eigenschaft: Vertauscht man Mark- und Pfennigbeträge miteinander und zieht* 5 *Pfennig ab, so erhält man das Doppelte von x. Wie groß ist x?*

Aufgabe 2.42 (F 94, T1, A3) *Es sei R ein kommutativer Ring,* $R \neq 0$. *Zeigen Sie: In der Menge der Primideale von R gibt es ein minimales Element (bezüglich der Inklusion).*

Aufgabe 2.43 (F 94, T3, A5) *Sei p eine Primzahl. Dazu werde die Menge*

$$\mathbb{Z}_{(p)} := \left\{ \frac{a}{b} | b \in \mathbb{N}, a \in \mathbb{Z}; ggt(a,b) = 1, ggt(b,p) = 1 \right\}$$

betrachtet. Zeigen Sie:

1) $\mathbb{Z}_{(p)}$ *ist ein Unterring mit Eins von* $\mathbb{Q}$.

2) $m_p := \{\frac{a}{b} | p$ *teilt* $a\}$ *ist das einzige maximale Ideal in* $\mathbb{Z}_{(p)}$.

3) $\mathbb{Z}_{(p)}/m_p$ *ist isomorph zu* $\mathbb{F}_p$, *dem Körper mit p Elementen. Geben Sie den Isomorphismus an.*

Aufgabe 2.44 (H 93, T1, A2) *Sei* $R := \mathbb{Z}/100000\mathbb{Z}$ *der Ring der ganzen Zahlen modulo 100 000.*

(i) Bestimmen Sie alle nilpotenten und alle idempotenten Elemente von R sowie die Anzahl der Nullteiler von R.

(ii) Geben Sie alle Primideale und alle maximalen Ideale von R an.

(iii) Bestimmen Sie die Struktur der Einheitengruppe von R durch Angabe ihrer invarianten Faktoren.

Aufgabe 2.45 (H 92, T3, A3) *Es sei R der folgende Teilring des Körpers der rationalen Zahlen*

$$R = \{\frac{a}{b} | a, b \in \mathbb{Z}, ggt(b, 10) = 1\}.$$

a) Man bestimme die Einheitengruppe von R.

b) Man bestimme alle Ideale von R und zeige, dass R ein Hauptidealring ist.

c) Man bestimme alle irreduziblen Elemente von R bis auf Assoziierte.

Aufgabe 2.46 (F 92, T1, A2) *Seien R ein kommutativer Ring, S eine multiplikative Teilmenge (d.h. $S \neq 0$ und $S \cdot S \subset S$) und I ein Ideal mit $I \cap S = \emptyset$. Zeigen Sie mit Hilfe des Zornschen Lemmas, dass es ein Primideal P von R gibt mit $I \subset P$ und $P \cap S = \emptyset$.*

Aufgabe 2.47 (F92, T3, A3) *a) Wie ist das Produkt zweier Ideale in einem kommutativen Ring definiert?*

Es sei $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} | a, b \in \mathbb{Z}\}$. Es sei P das von 3 und $1 + \sqrt{-5}$ erzeugte Ideal und Q das von 3 und $1 - \sqrt{-5}$ erzeugte Ideal in R.

b) Berechnen Sie PQ, und bestimmen Sie die Anzahl der Elemente sowie die Anzahl der Einheiten des Restklassenringes R/PQ.

Aufgabe 2.48 (H 91, T1, A2) *Es sei R ein kommutativer Ring mit 1. Die folgenden Behauptungen sind zu beweisen oder durch ein Gegenbeispiel zu widerlegen:*

a) Ist M ein maximales Ideal von$R$, so ist M auch ein Primideal von R.

b) Ist P ein Primideal von R, so ist P auch ein maximales Ideal von R.

c) R hat stets ein maximales Ideal.

d) R hat höchstens ein maximales Ideal.

e) Es seien P, Q Primideale von R. Dann gilt:

i) $P \cap Q$ ist ein Primideal von R.

ii) $P \cap Q$ ist ein Ideal von R.

iii) $P \cup Q$ ist ein Ideal von R.

iv) $P \cup Q$ ist ein Primideal von R.

Aufgabe 2.49 (H91, T2, A2) *a) Es sei n eine natürliche Zahl in ihrer Dezimaldarstellung*

$$n = \sum_{k=\geq 0} a_k 10^k, \; 0 \leq a_k \leq 9.$$

Man beweise die Kongruenz

$$n \equiv \sum_{k \geq 0} (-1)^k a_k \pmod{11}$$

und leite daraus ein Kriterium für die Teilbarkeit durch 11 her.

b) Man zerlege 1991 in Primfaktoren.

c) Man bestimme alle Gruppen (bis auf Isomorphie) der Ordnung 1991.

d) Es sei R der Restklassenring $\mathbb{Z}/1991\mathbb{Z}$ und R^* seine Einheitengruppe. Man stelle R^* als direktes Produkt von zylischen Gruppen von Primzahlpotenz-Ordnung dar.

Aufgabe 2.50 (F 91, T1, A2) *Zeigen Sie:*

1) In einem Hauptidealring werden alle aufsteigenden Ketten von Idealen stationär.

2) Sei P eine (beliebige) Menge von Primzahlen. Ganze Zahlen $\neq 0$, deren Primteiler sämtlich aus P sind, heißen P-Zahlen. Dann ist die Menge der rationalen Zahlen

$$\varphi(P) := \{a/b | a \in \mathbb{Z}, b \ \ P\text{-Zahl } \}$$

ein Hauptidealring.

Aufgabe 2.51 (F 91, T3, A3) *Sei $R = \mathbb{R}[x,y]/(x^2+y^2-1)$.*

a) Zeigen Sie, dass jedes Element von R durch genau ein $f \in R[x,y]$ der Form

$$f = a + by, a, b \in \mathbb{R}[x],$$

repräsentiert wird.

b) Zeigen Sie, dass R ein Integritätsbereich ist.

c) Bestimmen Sie die Einheiten von R.

Aufgabe 2.52 (H 90, T1, A3) *Zerlegen Sie 2, 3 und 5 im Ring $\mathbb{Z}[i]$ der Gaußschen ganzen Zahlen in Primfaktoren.*

Aufgabe 2.53 (F 90, T1, A1) *Sei $P = \{2,3,5,7,...\}$ die Menge aller Primzahlen. Für eine natürliche Zahl $n > 2$ sei*

$$P_n = \{p \in P : p < n\}.$$

Man betrachte die Ringe $R_n := \Pi_{p \in P_n} F_p$ und $R := \Pi_{p \in P} F_p$; dabei ist $F_p = \mathbb{Z}/p\mathbb{Z}$ der Primkörper der Charakteristik p. Die kanonische Abbildung $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ induziert Abbildungen

$$\varphi_n : \mathbb{Z} \to R_n,\ x \to (x \bmod p)_{p \in P_n},$$

$$\varphi : \mathbb{Z} \to R,\ x \to (x \bmod p)_{p \in P}.$$

Man zeige: φ_n ist surjektiv, aber nicht injektiv; und φ ist injektiv, aber nicht surjektiv.

Aufgabe 2.54 (F 90, T1, A2) *Mit den Bezeichnungen von Aufgabe 2.47 sei $I \subset R$ die Menge aller Folgen $(a_p)_{p \in P} \in R$ mit folgender Eigenschaft: Es gibt ein $n \in N$, so dass $a_p = 0$ für alle $p > n$.*

a) Man zeige, dass I ein Ideal von R ist.

b) Sei $\overline{R} = R/I$ der Restklassenring und $\overline{\varphi} : \mathbb{Z} \to \overline{R}$ die Komposition der Abbildung $\varphi : \mathbb{Z} \to R$ und der kanonischen Abbildung $R \to \overline{R}$. Man zeige, dass $\overline{\varphi}$ injektiv, aber nicht surjektiv ist.

2.4 Quadratische Reste

Ein Rest im Sinn der Überschrift ist eine Restklasse $a \bmod n$ in einem der Faktorringe $\mathbb{Z}_n$.

Definition 2.23 *Eine Restklasse $a \bmod n$ in $\mathbb{Z}_n$ heißt* quadratischer Rest, *wenn es ein $c \bmod n \in \mathbb{Z}_n$ gibt mit $c^2 = a$.*

Beispiel 2.24 *Die Restklassen $0 = 0^2$ und $1 = 1^2 \bmod n$ sind immer quadratische Reste.*

Beispiel 2.25 *$n = 3$. Wegen $1^2 = 1$ und $2^2 = 1 \bmod 3$ ist nur $1 \bmod 3$ ein quadratischer Rest modulo 3, und $2 \bmod 3$ ist keiner.*

Beispiel 2.26 *$n = 4$. Jetzt ist $2^2 = 0$, $3^2 = 1 \bmod 4$. Wieder ist nur $1 \bmod 4$ ein quadratischer Rest $\neq 0$.*

Beispiel 2.27 *$n = 5$. Hier ist $2^2 = 4$, $3^2 = 4$, $4^2 = 1 \bmod 5$. Deswegen sind 1 und 4 quadratische Reste modulo 5, die Restklassen 2 und $3 \bmod 5$ sind keine.*

Satz 2.22 *Es sei $n = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}$ die Zerlegung der Zahl $1 < n \in \mathbb{N}$ in Primzahlpotenzen. Dann ist $a \bmod n$ quadratischer Rest genau dann, wenn $a \bmod p_1^{k_1}, \ldots, a \bmod p_r^{k_r}$ quadratische Reste sind.*

Beweis. Die Abbildung

$$a \bmod n \mapsto (a \bmod p_1^{k_1}, \ldots, a \bmod p_r^{k_r})$$

ist ein Ring-Isomorphismus

$$\mathbb{Z}_n \to \mathbb{Z}_{p_1^{k_1}} \times \ldots \times \mathbb{Z}_{p_r^{k_r}}.$$

Quadrate in $\mathbb{Z}_n$ gehen dabei auf r-tupel von Quadraten in den einzelnen Faktoren des direkten Produkts. □

Das Problem, die quadratischen Reste modulo n zu bestimmen, ist damit zurückgeführt auf das Problem, quadratische Reste modulo einer Primzahlpotenz p^k zu bestimmen. Man muss unterscheiden zwischen primen Restklassen modulo p^k und den Restklassen $p \cdot m \bmod p^k$, die nicht prim sind.

Satz 2.23 *Es sei $n = p^k$ Potenz einer Primzahl $p > 2$.*

a) Eine prime Restklasse $a \bmod p^k$ ist genau dann quadratischer Rest modulo p^k, wenn $a \bmod p$ ein quadratischer Rest ist.

b) Eine nicht-prime Restklasse $a = p^l \cdot m$, $ggT(m, p) = 1$, ist genau dann quadratischer Rest modulo p^k, wenn l gerade, und die prime Restklasse $m \bmod p$ ein quadratischer Rest ist.

Beweis. a) Die multiplikative Gruppe $\mathbb{Z}_{p^k}^*$ der primitiven Restklassen modulo p^k ist abelsch von der Ordnung $\varphi(p^k) = p^{k-1} \cdot (p-1)$. Die Restklasse $a \bmod p^k \in \mathbb{Z}_{p^k}^*$ ist genau dann quadratischer Rest, wenn sie ein Quadrat in dieser Gruppe ist. Nach Beispiel 1.12 ist $\mathbb{Z}_{p^k}^*$ ein direktes

Produkt $A \times B$, wo A eine p-Gruppe der Ordnung p^{k-1} und B eine Gruppe der Ordnung $p-1$ ist.

Weil 2 relativ prim zu p vorausgesetzt ist, ist die Abbildung

$$(A,+) \to (A,+),\ a \mapsto 2a, \quad \text{bzw.} \quad (A,\cdot) \to (A,\cdot),\ a \mapsto a^2 \in A \subset \mathbb{Z}_{p^k}^*$$

ein Isomorphismus. Mit anderen Worten: Jedes Element $a \in A$ ist ein Quadrat.

Der Ring-Homomorphismus

$$\mathbb{Z}_{p^k} \to \mathbb{Z}_p, \quad a \, mod \, p^k \mapsto a \, mod \, p,$$

bildet Quadrate auf Quadrate ab. Wenn also $a \, mod \, p^k$ ein quadratischer Rest ist, dann auch $a \, mod \, p$. Ist umgekehrt $a = c^2 \, mod \, p$ ein quadratischer Rest, dann ist $a = c^2 \cdot \alpha$, $\alpha \in A$. Weil $\alpha = \gamma^2$ ein Quadrat in A ist, ist auch $a = (c \cdot \gamma)^2$ ein Quadrat in $A \times B$ und damit in $\mathbb{Z}_{p^k}^*$.

b) $\Rightarrow$: Es sei $a = p^l \cdot m$ ein Quadrat $c^2 = (p^\lambda \cdot \mu)^2$ mit $ggT(\mu, p) = 1$. Mit $m = \mu^2$ ist dann auch $ggT(m,p) = 1$. Es folgt $a = c^2 = p^{2\lambda}\mu^2 = p^l m$. Also ist $l = 2\lambda$ gerade und $m = \mu^2$ ist ein quadratischer Rest modulo p^k. Nach a) ist letzteres genau dann der Fall, wenn $m \, mod \, p$ ein quadratischer Rest ist.

$\Leftarrow$: Es sei $a = p^{2\lambda} \cdot m$ und m quadratischer Rest modulo p. Nach a) ist dann $m = \mu^2 \, mod \, p^k$ auch quadratischer Rest modulo p^k, ebenso wie $a = (p^\lambda \cdot \mu)^2$. □

Beispiel 2.28 *n=9. Die primen Restklassen modulo* 9 *sind* $1,2,4,5,7,8$ *und ihre Quadrate sind* $1,4,7,7,4,1 \, mod \, 9$. *Das sind genau die Restklassen, die auch modulo* 3 *ein Quadrat sind. Die nicht-primen Restklassen sind* $0,3,6$ *mit den Quadraten* $0,0,0$. *Wie bewiesen sind* $3 = 3^1$ *und* $6 = 3^1 \cdot 2$ *keine quadratischen Reste modulo* 9.

Beispiel 2.29 *n=27: Die nicht-primen Restklassen sind*

$$0,\ 3,\ 6 = 3 \cdot 2,\ 9 = 3^2,\ 12 = 3 \cdot 4,\ 15 = 3 \cdot 5,\ 18 = 3^2 \cdot 2,\ 21 = 3 \cdot 7, 24 = 3 \cdot 8$$

mit den Quadraten

$$0,9,9,0,9,9,0,9,9.$$

Nur 0 *und* $9 = 3^2$ *sind nicht-primitive quadratische Reste modulo* 27.

Satz 2.24 *Die Restklasse* $a \, mod \, 2^k$ *mit* $2 \not| a$, *ist genau dann quadratischer Rest modulo* 2^k *wenn*

$$\begin{array}{lll} k = 1 & und & a = 1 \, mod \, 2, \\ k = 2 & und & a = 1 \, mod \, 4, \\ k \geq 3 & und & a = 1 \, mod \, 8. \end{array}$$

Beweis. Nur die Restklasse $1 \, mod \, 2$ ist quadratischer primer Rest modulo 2. Die primen quadratischen Reste modulo 4 sind $1^2 = 1$ und $3^2 = 1$. Die primen quadratischen Reste modulo 8 sind

$$1^2 = 1, \quad 3^2 = 1, \quad 5^2 = 1, \quad 7^2 = 1,$$

wieder nur $1 \, mod \, 8$.

Sei nun $n = 2^k$ mit $k > 3$. Wenn a quadratischer Rest modulo 2^k ist, dann auch modulo 8 und es folgt $a = 1 \, mod \, 8$. Sei umgekehrt $a = 1 \, mod \, 8$. Wir beweisen, dass a quadratischer Rest modulo 2^k ist durch Induktion nach $k \geq 3$. Sei also $a = c^2 \, mod \, 2^k$ angenommen. Weil c ungerade ist, gibt es ein $\gamma \in \mathbb{Z}$ mit

$$\frac{c^2 - a}{2^k} + \gamma \cdot c = 0 \, mod \, 2.$$

Daraus folgt

$$(c + \gamma \cdot 2^{k-1})^2 = c^2 + \gamma c \cdot 2^k + \gamma^2 \cdot 2^{2k-2} = a \, mod \, 2^{k+1}.$$

(Wegen $k \geq 3$ ist 2^{2k-2} durch 2^{k+1} teilbar.) Also ist a auch quadratischer Rest modulo 2^{k+1}. □

Um eine bessere Übersicht über die quadratischen Reste modulo p zu bekommen, formalisiert man den Umgang mit ihnen wie folgt:

Definition 2.24 *Es sei p eine Primzahl > 2 und $a \in \mathbb{Z}$ nicht durch p teilbar. Dann heißt*

$$\left(\frac{a}{p}\right) := \begin{cases} +1 & \text{wenn } a \, mod \, p \text{ quadratischer Rest ist,} \\ -1 & \text{wenn } a \, mod \, p \text{ kein quadratischer Rest ist,} \end{cases}$$

das Legendre-Symbol.

Eine gewisse Rechtfertigung bekommt diese Definition durch die folgende Produktformel.

Satz 2.25 *Es seien $p > 2$ eine Primzahl und $a, b \in \mathbb{Z}$ nicht durch p teilbar. Dann gilt*

$$\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right).$$

Beweis. Wenn a und $b \, mod \, p$ quadratische Reste modulo p sind, dann gilt dies auch für $a \cdot b \, mod \, p$. Wenn $a \, mod \, p$ quadratischer Rest und $b \, mod \, p$ keiner ist, dann kann auch $a \cdot b \, mod \, p$ kein Quadrat sein, ebenso wenn $b \, mod \, p$ quadratischer Rest ist und $a \, mod \, p$ keiner. Der einzige nicht ganz triviale Fall ist, dass beide, a und $b \, mod \, p$ keine quadratischen Reste sind.

Wir erinnern uns daran, dass die Gruppe $\mathbb{Z}_p^* = \mathbb{F}_p^*$ zyklisch ist (Satz 2.11). Sei c ein Erzeugendes dieser Gruppe. Weil die Ordnung $p - 1$ der Gruppe gerade ist, sind genau die geradzahligen Potenzen $c^{2k} \, mod \, p$ quadratische Reste. Und das Produkt zweier ungeradzahligen Potenzen von c ist eben eine geradzahlige Potenz. □

Satz 2.26 (Kriterium von Euler) *Sei $p > 2$ eine Primzahl und $a \in \mathbb{Z}$ nicht durch p teilbar. Dann ist*

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \, mod \, p.$$

Beweis. Wieder betrachten wir die zyklische Gruppe $\mathbb{Z}_p^* =< c >$. Ihre Elemente schreiben wir multiplikativ $c, c^2, ..., c^{p-2}, c^{p-1} = 1$. Die Abbildung

$$\mathbb{Z}_p^* \to \mathbb{Z}_2 = \{1 = c^{p-1}, c^{\frac{p-1}{2}} = -1 \, mod \, p\} \quad c^k \mapsto (c^k)^{\frac{p-1}{2}}$$

ist ein Gruppen-Epimorphismus. Die Hälfte der Potenzen $a = c^k$ geht dabei auf $+1$, die andere auf -1. Weil alle geradzahligen Potenzen von c auf $+1$ gehen, sind dies genau die Elemente mit Bild $= +1$. Genau die Quadrate $a = c^{2k}$ haben die Eigenschaft $a^{\frac{p-1}{2}} = 1 \, mod \, p$. □

Beispiel 2.30 *$-1 = p-1 \, mod \, p$ ist genau dann ein quadratischer Rest, wenn*

$$(-1)^{\frac{p-1}{2}} = 1$$

ist. Das ist genau dann der Fall, wenn die gerade Zahl $p-1$ sogar durch vier teilbar ist. Primzahlen > 2 sind immer ungerade, also $p \equiv 1$ oder 3 modulo 4. Wir finden:

$$\begin{array}{rcl} p \equiv 1 \, mod \, 4 & \Leftrightarrow & p-1 \text{ quadratischer Rest,} \\ p \equiv 3 \, mod \, 4 & \Leftrightarrow & p-1 \text{ kein quadratischer Rest.} \end{array}$$

Beispielsweise ist $12 = 5^2 \, mod \, 13$ quadratischer Rest, aber $10 \, mod \, 11$ keiner.

Im folgenden setzen wir immer voraus: $p > 2$ ist eine Primzahl und $a \in \mathbb{Z}$ ist nicht durch p teilbar. Nur für die noch kommenden Beweise benötigen wir folgende Definition:

Definition 2.25 *Ein* Halbsystem *modulo p ist eine Menge $a_1, ..., a_{(p-1)/2}$ von genau $(p-1)/2$ verschiedenen Restklassen $\neq 0$ modulo p, die zusammen mit den komplementären Restklassen $-a_1, ..., -a_{(p-1)/2} \, mod \, p$ die ganze Menge $\{1, ..., p-1 \, mod \, p\}$ ergeben.*

Beispiel 2.31 *Die Restklassen $1, ..., (p-1)/2 \, mod \, p$ bilden so ein Halbsystem, ebenso wie die komplementären Restklassen $(p+1)/2, ..., p-1$.*

Satz 2.27 (Lemma von Gauß) *Es sei $a_1, ..., a_{(p-1)/2}$ ein Halbsystem. Dann sind die $(p-1)/2$ Produkte $a \cdot a_1, ..., a \cdot a_{(p-1)/2}$ modp alle voneinander verschieden. Sei h die Anzahl solcher Produkte, welche nicht wieder dem gewählten, sondern seinem komplementären Halbsystem angehören. Dann ist*

$$\left(\frac{a}{p}\right) = (-1)^h.$$

Beweis. Die Restklassen $-a_1, ..., -a_{(p-1)/2} \, mod \, p$ bilden das komplementäre Halbsystem. Für $i = 1, ..., (p-1)/2$ ist

$$a \cdot a_i = \pm a_{\sigma(i)},$$

je nachdem, ob das Produkt $a \cdot a_i$ wieder zum ausgewählten Halbsystem, oder zu seinem Komplement gehört. Der entscheidende Punkt ist, dass die Zahlen $\sigma(i)$, $i = 1, ..., (p-1)/2$, eine Permutation der Zahlen $1, ..., (p-1)/2$ bilden. Denn für $1 \leq i \neq j \leq (p-1)/2$ folgt aus $\sigma(i) = \sigma(j)$, dass $a \cdot a_i = \pm a \cdot a_j$. Weil p eine Primzahl ist, können wir kürzen und finden $a_i = \pm a_j$. Das geht aber nicht nach Definition eines Halbsystems. Also sind alle Zahlen $\sigma(i)$ voneinander verschieden und bilden eine Permutation der Zahlen $1, ..., (p-1)/2$.

Jetzt multiplizieren wir alle Produkte $a \cdot a_i$ modulo p:

$$\begin{array}{rcl} a^{(p-1)/2} \cdot a_1 \cdot ... \cdot a_{(p-1)/2} & = & (a \cdot a_1) \cdot ... \cdot (a \cdot a_{(p-1)/2}) \\ & = & (\pm a_{\sigma(1)}) \cdot ... \cdot (\pm \cdot a_{\sigma((p-1)/2)}) \\ & = & (-1)^h a_1 \cdot ... \cdot a_{(p-1)/2}, \\ a^{(p-1)/2} & = & (-1)^h. \end{array}$$

Die Behauptung ergibt sich aus dem Eulerschen Kriterium (Satz 2.26). □

Beispiel 2.32 *Wir wollen*

$$\left(\frac{2}{p}\right)$$

berechnen für eine ungerade Primzahl p. Dazu verwenden wir das Halbsystem $1, 2, ..., (p-1)/2 \, mod \, p$. Wenn wir seine Zahlen mit $a = 2$ multiplizieren, erhalten wir die Zahlen

$$2, 4, ..., p-1.$$

Es kommt darauf an, wieviele von denen $\leq p/2$ sind, und wieviele nicht. Das Legendre-Symbol ist ja

$$\left(\frac{2}{p}\right) = (-1)^s,$$

wo s die Anzahl der Zahlen $2, 4, ..., p-1$ ist, welche $> (p-1)/2$ sind. Das ist natürlich die Anzahl der Zahlen $1, 2, ..., (p-1)/2$, welche $> (p-1)/4$ sind. Wenn $(p-1)/4$ selbst ganz ist, dann haben wir

$$s = \frac{p-1}{2} - \frac{p-1}{4} = \frac{p-1}{4}.$$

Aber, wenn $(p-1)/4$ keine ganze Zahl ist, dann ist $(p-3)/4$ ganz, und

$$s = \frac{p-1}{2} - \frac{p-3}{4} = \frac{p+1}{4}.$$

Nun ist

$$\frac{p-1}{4} = k \text{ ganz} \quad \Leftrightarrow \quad p = 4 \cdot k + 1 \quad \Leftrightarrow \quad p = 1 \, mod \, 4.$$

Wir haben also bewiesen

$$\left(\frac{2}{p}\right) = \begin{cases} (-1)^{\frac{p-1}{4}} & \text{für} \quad p = 1 \, mod \, 4, \\ (-1)^{\frac{p+1}{4}} & \text{für} \quad p = 3 \, mod \, 4. \end{cases}$$

Das kann man noch etwas vereinheitlichen:

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

In der Tat, es ist

$$\frac{p^2-1}{8} = \frac{p-1}{4} \cdot \frac{p+1}{2} = \frac{p+1}{4} \cdot \frac{p-1}{2}.$$

Der Fall $p = 1 \, mod \, 4$: Hier ist $p = 4k+1$, $k \in \mathbb{N}$, und $(p+1)/2 = (4k+2)/2 = 2k+1$ ungerade. Also ist $(p^2-1)/8$ gerade oder ungerade, jenachdem ob $(p-1)/4$ dies ist.

Der Fall $p = 3 \, mod \, 4$: Jetzt ist $p = 4k+3$, $k \in \mathbb{N}$, und $(p-1)/2 = (4k+2)/2$ ungerade. Die Zahl $(p^2-1)/8$ ist gerade oder ungerade, jenachdem ob $(p+1)/4$ dies ist.

Betrachten wir die ersten sieben ungeraden Primzahlen:

p	$mod\,4$	$(p-1)/4$	$(p+1)/4$	p^2-1	$\left(\frac{2}{p}\right)$
3	3		1	8	-1
5	1	1		24	-1
7	3		2	48	1
11	3		3	120	-1
13	1	3		168	-1
19	3		5	360	-1
23	3		6	528	1

Das ist ja interessant!

Auf Grund der Sätze 2.22 , 2.23 und 2.24 ist die Frage, ob $a\,mod\,p$ ein quadratischer Rest ist, zurückgeführt auf die Berechnung von Legendre-Symbolen $\left(\frac{p}{q}\right)$, wo p und $q > 2$ Primzahlen sind. Den Fall $p = 2$ haben wir im letzten Beispiel erledigt. Bleibt der Fall, dass beide Zahlen, p und q ungerade Primzahlen sind. Da greift ein absolut unglaubliches Hilfsmittel:

Satz 2.28 (Quadratisches Rezprozitätsgesetz) *Sind p und q zwei verschiedene ungerade Primzahlen, so gilt*

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Das heißt also, das Produkt der beiden Legendre-Symbole ist $= +1$, beide Symbole sind gleich, außer wenn $p = q = 3\,mod\,4$ sind. Dann sind beide Symbole verschieden. Ein Beispiel dafür, wie man das anwendet:

Beispiel 2.33 (H 97, T1, A2c) *Untersuchen Sie, ob die Kongruenz $X^2 = 593\,mod\,1997$ eine Lösung in $\mathbb{Z}/1997\mathbb{Z}$ besitzt.*

Es gilt also, zu entscheiden, ob 593 ein quadratischer Rest modulo 1997 ist. Zunächst müssen wir versuchen, die beiden Zahlen 593 und 1997 in Primfaktoren zu zerlegen. Dabei wird sich herausstellen: Beides sind Primzahlen! Ihre Restklassen modulo 4 sind

$$593 = 600 - 8 + 1 = 1\,mod\,4, \quad 1997 = 2000 - 4 + 1 = 1\,mod\,4.$$

Also sagt das quadratische Reziprozitätsgesetz

$$\left(\frac{593}{1997}\right) = \left(\frac{1997}{593}\right).$$

Wozu nützt diese Information? Es ist

$$3\cdot 593 = 1779, \quad 1997 = 3\cdot 593 + 218 = 218 = 6^3\,mod\,593.$$

Somit ist

$$\left(\frac{1997}{593}\right) = \left(\frac{2^3}{593}\right)\cdot\left(\frac{3^3}{593}\right).$$

Nun ist $593 = 1 \, mod \, 4$*, also (Beispiel 2.32)*

$$\left(\frac{2}{593}\right) = (-1)^{\frac{592}{4}} = (-1)^{148} = +1.$$

Und $3^3 = 3^2 \cdot 3$ *ist genau dann quadratischer Rest modulo* 593*, wenn* 3 *dies ist. Wegen* $593 = 1 \, mod \, 4$ *ist*

$$\left(\frac{3}{593}\right) = \left(\frac{593}{3}\right).$$

Wegen $593 = 600 - 9 + 2 = 2 \, mod \, 3$ *ist* 593 *kein quadratischer Rest modulo* 3*. Deswegen ist auch* 3^3 *kein quadratischer Rest modulo 593 und die ursprüngliche Kongruenz ist nicht lösbar.*

Beweis von Satz 2.28 (Absolut genial! Abgeschreiben aus dem Buch 'Zahlentheorie' von S.I. Borevicz und I.R. Safarevic, Birkhäuser 1966). Zur Beschreibung von $\left(\frac{p}{q}\right)$ verwenden wir das Halbsystem $1, 2, ..., (q-1)/2$. Nach Satz 2.27 ist

$$\left(\frac{p}{q}\right) = (-1)^s,$$

wo s die Anzahl der Zahlen $k = 1, ..., (q-1)/2$ ist, für die $p \cdot k \, mod \, q$ zum Halbsystem $(q+1)/2, ..., q-1$ gehört. Dazu äquivalent ist

$$(m - \frac{1}{2}) \cdot q < p \cdot k < m \cdot q$$

für ein $m \in \mathbb{N}$. (Es kann nicht $p \cdot k = (m - \frac{1}{2}) \cdot q$ sein, weil $q/2$ nicht ganz ist. Und auch $p \cdot k = m \cdot q$ kann nicht gelten, weil dann q die Zahl $k < q/2$ teilen müsste.) Wenn m obige Ungleichung erfüllt, dann ist auch

$$q \cdot m < p \cdot k + \frac{q}{2} < p \cdot \frac{q}{2} + \frac{q}{2} = \frac{p+1}{2} \cdot q,$$

also muss $m \in \mathbb{N}$ sogar die Bedingung

$$1 \leq m \leq \frac{p-1}{2}$$

erfüllen. Damit ist s die Anzahl aller Paare (k, m) ganzer Zahlen, welche folgende Bedingungen erfüllen:

$$k = 1, 2, ..., \frac{q-1}{2},$$

$$m = 1, 2, ..., \frac{p-1}{2},$$

$$-\frac{q}{2} < k \cdot p - m \cdot q < 0.$$

Vertauschen wir die Rollen von p und q, so finden wir

$$\left(\frac{q}{p}\right) = (-1)^t,$$

wo t die Anzahl der Paare (l,n) ganzer Zahlen ist, welche

$$l = 1, 2, ..., \frac{p-1}{2},$$

$$n = 1, 2, ..., \frac{q-1}{2},$$

$$-\frac{p}{2} < l \cdot q - n \cdot p < 0,$$

erfüllen. Ändern wir in der letzten Ungleichung das Vorzeichen, so finden wir, dass t die Anzahl aller Paare $(n,l) = (k,m)$ ganzer Zahlen ist, welche folgende Bedingungen erfüllen:

$$k = 1, 2, ..., \frac{q-1}{2},$$

$$m = 1, 2, ..., \frac{p-1}{2},$$

$$0 < k \cdot p - m \cdot q < \frac{p}{2}.$$

Nun ist das Produkt

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{s+t},$$

wo $s+t$ die Anzahl aller Paare (k,m) von ganzen Zahlen ist, welche eine der beiden Bedingungstripel erfüllen. Dabei kann nie $k \cdot p = m \cdot q$ sein, denn dann müsste p die Zahl m teilen und q die Zahl k. Wegen $m < p$ und $k < q$ geht dies nicht. Also ist $s+t$ die Anzahl aller Paare (k,m) von ganzen Zahlen, welche die Bedingungen

$$k = 1, 2, ..., \frac{q-1}{2},$$

$$m = 1, 2, ..., \frac{p-1}{2},$$

$$-\frac{q}{2} < k \cdot p - m \cdot q < \frac{p}{2}$$

erfüllen.

Jetzt kommt der Trick: Wir spiegeln k an $(q+1)/4$ und m an $(p+1)/4$ und gehen über zu

$$k' := \frac{q+1}{2} - k, \quad m' := \frac{p+1}{2} - m.$$

Auch diese Zahlen sind im Bereich

$$k' = 1, 2, ..., \frac{q-1}{2}, \quad m' = 1, 2, ..., \frac{p-1}{2}.$$

Und es ist

$$\begin{aligned} k' \cdot p - m' \cdot q &= (\frac{q+1}{2} - k) \cdot p - (\frac{p+1}{2} - m) \cdot q \\ &= \frac{q+1}{2} \cdot p - \frac{p+1}{2} \cdot q - (k \cdot p - m \cdot q) \\ &= \frac{p}{2} - \frac{q}{2} - (k \cdot p - m \cdot q). \end{aligned}$$

Wegen $k \cdot p - m \cdot q > -q/2$ ist

$$k' \cdot p - m' \cdot q < \left(\frac{p}{2} - \frac{q}{2}\right) + \frac{q}{2} = \frac{p}{2},$$

und wegen $k \cdot p - m \cdot q < p/2$ ist

$$k' \cdot p - m' \cdot q > \left(\frac{p}{2} - \frac{q}{2}\right) - \frac{p}{2} = -\frac{q}{2}.$$

Das Zahlenpaar (k', m') erfüllt genau dieselben Bedingungen wie das Paar (k, m).

Die Zahlenpaare (k, m) kommen also in Paaren. Damit ist ihre Gesamtzahl $s + t$ gerade, außer, wenn es ein Paar mit

$$k = k', \quad m = m'$$

gibt, in diesem Fall ist $s + t$ ungerade. Wann ist das der Fall? Da muss also

$$k = \frac{q+1}{2} - k, \quad \frac{q+1}{2} = 2k, \quad q = 4k - 1$$

und

$$l = \frac{p+1}{2} - l, \quad \frac{p+1}{2} = 2l, \quad q = 4l - 1$$

sein, d.h., $p = q = 3 \, mod \, 4$. Genau dann ist das Produkt

$$\frac{p-1}{2} \cdot \frac{q-1}{2}$$

ungerade. □

Aufgabe 2.55 (F 93, T2, A3) *Welche der folgenden Aussagen ist für alle Primzahlen p gültig?*

a) Das Polynom $X^2 - 17$ ist genau dann irreduzibel in $\mathbb{F}_p[X]$, wenn $X^2 - p$ irreduzibel in $\mathbb{F}_{17}[X]$ ist.

b) Das Polynom $X^2 - 3$ ist genau dann irreduzibel in $\mathbb{F}_p[X]$, wenn $X^2 - p$ irreduzibel in $\mathbb{F}_3[X]$ ist.

Aufgabe 2.56 (F 92, T3, A2) *Kennzeichnen Sie durch Kongruenzbedingungen diejenigen ungeraden Primzahlen p, für die das Polynom $X^2 - 5$ irreduzibel in $\mathbb{F}_p[X]$ ist.*

2.5 Polynomringe

In diesem Abschnitt sei wieder R ein nullteilerfreier kommutativer Ring mit Eins. Wir interessieren uns für die Teilbarkeit im Polynomring $R[X]$. Auch $R[X]$ ist nullteilerfrei, kommutativ mit Eins. Alle Begriffe des vorletzten Abschnittes sind also in $R[X]$ definiert.

In dieser Situation ist das am häufigsten angewendete Kriterium für Irreduzibilität das *Eisenstein-Kriterium.*

Satz 2.29 (Eisenstein) *Es sei*

$$f = a_0 + a_1 X + ... + a_n X^n \in R[X], \quad a_n \neq 0,$$

ein Polynom. Wenn es ein Primelement $p \in R$ gibt mit

$$p \not| a_n, \quad p | a_i \text{ für alle } i < n, \quad p^2 \not| a_0,$$

dann ist $f \in R[X]$ irreduzibel.

Beweis. Wir nehmen an $f = g \cdot h$ mit

$$g = \sum_0^r b_\nu X^\nu, \; h = \sum_0^s c_\nu X^\nu \; \in R[X],$$

mit $r > 0$, $s > 0$, und $r + s = n$. Es folgt

$$p | a_0 = b_0 c_0.$$

Weil p prim ist, teilt es einen der beiden Faktoren, etwa $p | b_0$. Dann kann p aber c_0 nicht teilen, weil $p^2 \not| a_0$ vorausgesetzt ist.

Nicht alle Koeffizienten von g können durch p teilbar sein. Denn dann wären dies auch alle Koeffizienten von f, aber der Koeffizient a_n von f ist dies nicht. Sei also b_i der erste Koeffizient von g, der nicht durch p teilbar ist, $0 < i \leq r < n$. Nach Voraussetzung gilt

$$p | a_i = b_i c_0 + b_{i-1} c_1 + ... + b_0 c_i.$$

Weil p die Zahlen a_i, sowie $b_0, ..., b_{i-1}$ teilt, teilt es auch $b_i c_0$. Weil p prim ist, teilt es entweder c_0 oder b_i. Wir sahen, c_0 kann es nicht teilen, also gilt $p | b_i$, Widerspruch! □

Beispiel 2.34 *Sei $p \in \mathbb{Z}$ eine Primzahl. Dann erfüllt $X^n - p \in \mathbb{Z}[X]$, $n \geq 1$ das Eisenstein-Kriterium und ist in $\mathbb{Z}[X]$ irreduzibel.*

Beispiel 2.35 *Das* Kreisteilungs-Polynom *zur Primzahl p*

$$\frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + ... + X + 1 \in \mathbb{Z}[X]$$

ist auch irreduzibel. Auf f kann man das Eisenstein-Kriterium nicht direkt anwenden. Aber wenn f reduzibel wäre, so wäre dies auch

$$\begin{aligned} f(X+1) &= \frac{(X+1)^p - 1}{X} \\ &= \frac{X^p + \binom{p}{1} X^{p-1} + ... + \binom{p}{p-1} X}{X} \\ &= X^{p-1} + \binom{p}{1} X^{p-2} + ... + \binom{p}{p-1}. \end{aligned}$$

Für $i \geq 1$ sind hier alle Koeffizienten

$$\binom{p}{i} = \frac{p(p-1)\cdot ... \cdot (p-i+1)}{i!}$$

durch p teilbar, denn der Zähler ist durch p teilbar, der Nenner aber nicht. Der Konstante Koeffizient $= p$ schließlich ist nicht durch p^2 teilbar.

Beispiel 2.36 *Es gibt auch ein* reziprokes Eisensteinkriterium*: Im Polynom*

$$f(X) = a_0 + a_1 X + ... + a_n X^n$$

sei a_0 nicht durch p teilbar, die Koeffizienten $a_1, ..., a_n$ seien durch p teilbar, aber a_n nicht durch p^2. Eisenstein ist nicht direkt anwendbar. Aber wir betrachten das Polynom

$$g(X) := X^n \cdot f(\frac{1}{X}) = a_0 X^n + a_1 X^{n-1} + ... + a_{n-1} X + a_n.$$

Dieses ist irreduzibel nach Eisenstein. Daraus folgt, dass f selbst irreduzibel ist. Denn falls $f = f_1 \cdot f_2$ mit $deg(f_i) = n_i$, dann wären $g_i := X^{n_i} f_i(1/X)$ Polynome mit $g = g_1 \cdot g_2$.

Ein weiteres häufig angewendetes Verfahren um Irreduzibilität von Polynomen $f \in \mathbb{Z}[X]$ zu beweisen, ist Reduktion modulo $n \in N$. Wäre nämlich $f = g \cdot h \in \mathbb{Z}[X]$, so wäre

$$f \bmod n = (g \bmod n) \cdot (h \bmod n)$$

im Ring $\mathbb{Z}_n[X]$. In diesem Ring gibt es nur endlich viele Polynome gegebenen Grades, und Teilbarkeit ist nach endlich vielen Schritten entscheidbar.

Beispiel 2.37 *Wir untersuchen*

$$f(X) = X^5 - X^2 + 1 \in \mathbb{Z}[X].$$

Wäre f reduzibel, so hätte einer der Faktoren einen Grad ≤ 2. Wir reduzieren modulo 2: In $\mathbb{F}_2[X]$ gibt es nur die zwei linearen Polynome

$$X \text{ und } X+1$$

und ein einziges irreduzibles quadratisches Polynom

$$X^2 + X + 1.$$

Nun ist über $\mathbb{F}_2$

$$X^5 + X^2 + 1 = X^2(X^3+1) + 1 = X^2(X+1)(X^2+X+1) + 1$$

durch keines dieser drei Polynome teilbar. Also ist $f \bmod 2$ irreduzibel, und damit auch f selbst.

Beispiel 2.38 *Wir betrachten*

$$f(X) = X^4 + 3X^3 + 3X^2 - 5 \in \mathbb{Z}[X].$$

Es ist

$$f \, mod \, 2 = X^4 + X^3 + X^2 + 1 = (X+1)(X^3 + X + 1).$$

Modulo 2 ist $X^3 + X + 1$ *irreduzibel. Wenn* $f \in \mathbb{Z}[X]$ *reduzibel wäre, so müsste es einen Linearfaktor abspalten. Jetzt rechnen wir modulo 3: Die einzigen linearen Polynome in* $\mathbb{F}_3[X]$ *sind* X, $X+1$ *und* $X-1$. *Sie gehen nicht in*

$$f \, mod \, 3 = X^4 + 1$$

auf. Also ist $f \in \mathbb{Z}[X]$ *irreduzibel.*

Wir vergleichen jetzt den Ring R und seinen Polynomring $R[X]$ in Bezug auf verschiedene Eigenschaften.

1) *Die Einheiten in* $R[X]$ *sind genau die Einheiten in* R*:* Sind $a, b \in R[X]$ Polynome mit $ab = 1$, so können sie keinen Grad > 0 haben.

2) *Ist* $r \in R$ *irreduzibel, dann auch in* $R[X]$*:* Sei $r = ab$ mit $a, b \in R[X]$. Wenn a oder b einen Grad ≥ 1 hätte, dann auch ab. Es folgt $a, b \in R$. Weil r in R irreduzibel ist, muss a oder b eine Einheit in R und dann auch in $R[X]$ sein.

3) *Ist* $r \in R$ *prim, dann auch in* $R[X]$*:* $r \in R$ teilt ein Polynom $g(X) \in R[X]$, wenn r alle Koeffizienten von g teilt. Seien jetzt

$$g(X) = \sum_0^k a_\nu X^\nu, \; h(X) = \sum_0^l b_\nu X^\nu \in R[X]$$

Polynome mit $r | gh$. Wenn r weder g noch h teilt, gibt es ein kleinstes i mit $r \not| \, a_i$ und ein kleinstes j mit $r \not| \, b_j$. Der Koeffizient in fg von X^{i+j} ist

$$\underbrace{a_0 b_{i+j} + ... + a_{i-1} b_{j+1}}_{\text{teilbar durch } r} + a_i b_j + \underbrace{a_{i+1} b_{j-1} + ... + a_{i+j} b_0}_{\text{teilbar durch } r}.$$

Also ist auch $a_i b_j$ durch p teilbar. Weil p prim ist, muss entweder a_i oder b_j durch r teilbar sein. Widerspruch!

4) *Ist* $R[X]$ *faktoriell, dann ist dies auch* R*:* Jedes $a \in R$ lässt eine Zerlegung $a = e r_1 \cdot ... r_k$ mit einer Einheit $e \in R[X]$ und irreduziblen Polynomen $r_i \in R[X]$ zu. Nach 1) ist e eine Einheit in R. Aus Grad-Gründen sind alle Polynome $r_1, ..., r_k$ in Wirklichkeit Elemente aus R. Weil sie in $R[X]$ irreduzibel sind, sind sie dies auch in R. Damit besitzt jedes $0 \neq a \in R$ eine Zerlegung in irreduzible Faktoren.

Wir wollen Satz 2.17 anwenden, und müssen noch zeigen: Jedes in R irreduzible Element r ist in R prim. Nach 2) ist r in $R[X]$ irreduzibel. Weil $R[X]$ faktoriell ist, ist r dort dann auch prim. Deswegen ist r auch prim in R.

Von nun an sei R *als faktoriell vorausgesetzt.*

Definition 2.26 *Es sei*

$$f(X) = a_0 + a_1X + ... + a_nX^n \in R[X]$$

ein Polynom. Dann heißt

$$c(f) := ggT(a_0, a_1, ..., a_n)$$

der Inhalt *(='content') des Polynoms f.*

Beispiel 2.39 *Jedes* normierte *Polynom*

$$f = X^n + a_{n-1}X^{n-1} + ...$$

hat den Inhalt 1.

Satz 2.30 *Es seien $f, g \in R[X]$ Polynome. Dann ist*

$$c(f \cdot g) = c(f) \cdot c(g).$$

Beweis. Weil R faktoriell ist, gibt es eine eindeutige Zerlegung

$$c(f \cdot g) = e \cdot r_1 \cdot ... \cdot r_k$$

von $c(f \cdot g)$ in irreduzible Faktoren r_i. Wir beweisen die Aussage durch Induktion nach k. Weil $r_1 \in R$ prim ist, teilt r_1 nach Eigenschaft 3) entweder f oder g. Entsprechend ersetzen wir f oder g durch f/r_1 oder g/r_1 und haben in $c(f \cdot g)$ einen irreduziblen Faktor weniger. □

Erinnern Sie sich jetzt: $Q(R)$ bedeutet den Quotientenkörper des Ringes R.

Satz 2.31 (Lemma von Gauß) *Das Polynom $f \in R[X]$ sei in $Q(R)[X]$ zerlegbar, etwa*

$$f = F_1 \cdot F_2, \quad F_i \in Q(R)[X].$$

Dann ist f schon in $R[X]$ zerlegbar:

$$f = f_1 \cdot f_2, \quad f_i \in R[X], \quad f_i = c_iF_i, c_i \in Q(R).$$

Beweis. Es genügt, die Aussage für Polynome f mit dem Inhalt $c(f) = 1$ zu beweisen.

Die Koeffizienten des Polynoms F_i, $i = 1, 2$, sind (gekürzte) Brüche $z/n \in Q(R)$ mit $z, n \in R$. Wenn wir das kgV aller Nenner vorausnehmen, können wir schreiben

$$F_i = \frac{1}{n_i} \cdot g_i, \quad g_i \in R[X].$$

Es sei z_i der Inhalt $c(g_i)$, also $g_i = z_if_i$ mit $f_i \in R[X]$, $c(f_i) = 1$. Es folgt

$$n_1n_2 \cdot f = z_1z_2 \cdot f_1 \cdot f_2,$$

und bis auf Faktoren, die Einheiten in R sind,

$$n_1n_2 = c(n_1n_2 \cdot f) = c(z_1f_1 \cdot z_2f_2) = z_1z_2 \cdot c(f_1) \cdot c(f_2) = z_1z_2.$$

Also gilt $f = f_1f_2$ bis auf Faktoren, die Einheiten in R sind. □

Satz 2.32 (Korollar) *a) Hat ein normiertes Polynom $f \in \mathbb{Z}[X]$ eine Nullstelle $x_0 \in \mathbb{Q}$, so ist x_0 in Wirklichkeit eine ganze Zahl.*

b) Ist $f \in \mathbb{Z}[X]$ irreduzibel über $\mathbb{Z}$, so auch über $\mathbb{Q}$.

Beweis. a) Nach Vieta ist $f = g_1 \cdot (X - x_0)$ mit $g_1 \in \mathbb{Q}[X]$. Nach Satz 2.31 gibt es $c_1, c_2 \in \mathbb{Q}$ so, dass $f_1 := c_1 g_1$ und $c_2(X - x_0)$ ganzzahlig sind, und $f = f_1 \cdot c_2(X - x_0)$ erfüllen. Insbesondere ist $c_2 \in \mathbb{Z}$. Der höchste Koeffizient von $f = f_1 \cdot c_2(X - x_0)$ ist $= 1$. Daraus folgt $c_2 = \pm 1$ und $c_2 x_0 = \pm x_0 \in \mathbb{Z}$.

b) Wenn $f = F_1 F_2$ mit $F_1, F_2 \in \mathbb{Q}[X]$, dann ist nach Satz 2.31 $f = f_1 f_2$ mit $f_i = c_i F_i \in \mathbb{Z}[X]$. Weil f über $\mathbb{Z}$ irreduzibel ist, muss für $i = 1$ oder $= 2$ gelten $Grad(f_i) = Grad(F_i) = 0$. □

Satz 2.33 (von Gauß) *Der Ring $R[X]$ ist genau dann faktoriell, wenn R dies ist.*

Beweis. Wenn $R[X]$ faktoriell ist, dann ist R faktoriell nach Eigenschaft 4) von oben. Sei also jetzt R faktoriell vorausgesetzt. Jedes $f \in R[X]$ ist auch ein Polynom $\in Q(R)[X]$ über $Q(R)$.

Weil $Q(R)[X]$ faktoriell ist (Sätze 2.19 und 2.20), gibt es eine Zerlegung

$$f = F_1 \cdot ... \cdot F_k, \quad F_k \in Q(R)[X],$$

mit irreduziblen Polynomen F_i, $i = 1, ..., k$. Wir schreiben

$$F_i = c_i f_i, \quad c_i \in Q(R),\ f_i \in R[X],\ c(f_i) = 1.$$

Mit $c_1 \cdot ... \cdot c_k = z/n$, $z, n \in R$, ist also

$$nf = z \cdot f_1 \cdot ... \cdot f_k$$

und $nc(f) = ez$ mit einer Einheit $e \in R$. Also können wir z in R durch n teilen:

$$f = q \cdot f_1 \cdot ... \cdot f_k,\ q \in R,$$

mit $f_i \in R[X]$, $c(f_i) = 1$, irreduzibel in $Q(R)[X]$. Weil dann auch f_i irreduzibel in $R[X]$ ist, folgt die Existenz der Zerlegung von f in irreduzible Faktoren.

Zu zeigen bleibt die Eindeutigkeit dieser Zerlegung. Sei etwa

$$f = q \cdot f_1 \cdot ... \cdot f_k = q' \cdot f_1' \cdot ... \cdot f_l' \text{ mit } q, q' \in R,\ f_1, ..., f_l' \in R[X] \text{ irreduzibel.}$$

Weil $f_1, ..., f_l'$ in $R[X]$ irreduzibel sind, folgt $e(f_1) = ... = e(f_l') = 1$. Nach dem Lemma von Gauß sind $f_1, ..., f_l'$ auch in $Q(R)[X]$ irreduzibel. Weil $Q(R)[X]$ faktoriell ist, gilt $k = l$ und man kann die Faktoren so umordnen, dass $f_i = c_i f_i'$ mit $c_i \in Q(R)$. Aus $c(f_i) = c(f_i') = 1$ folgt aber $c_i = 1$. Wir haben also

$$f = q \cdot f_1 \cdot ... \cdot f_k = q' \cdot f_1 \cdot ... \cdot f_k.$$

Weil $R[X]$ ein Integritätsring ist, folgt $q = q'$. Die Eindeutigkeit der Zerlegungvon q in irreduzible Faktoren zeigt nun die Eindeutigkeit der Zerlegung von f. □

Beispiel 2.40 *Wenn das Polynom X^3-2 über $\mathbb{Q}$ reduzibel wäre, würde es einen Linear-Faktor $X-x_0$ abspalten. Weil X^3-2 ganzzahlig ist, müsste nach dem Lemma von Gauß $x_0 \in \mathbb{Z}$ sein. Aus der Monotonie der Funktion $x \mapsto x^3$ folgt in diesem Fall $1 < x_0 < 2$. Es gibt aber keine solche ganze Zahl x_0. Deswegen ist X^3-2 irreduzibel über $\mathbb{Q}$. Insbesondere ist die Zahl $\sqrt[3]{2}$ irrational.*

Aufgabe 2.57 *a) Zeigen Sie, dass die Polynome*

$$f := X^4 + X + 1, \quad g := X^4 - X^2 + 1 \in \mathbb{Q}[X]$$

irreduzibel sind.

b) Ist g irreduzibel in $\mathbb{Q}(i)[X]$?

Aufgabe 2.58 (F 02, T2, A1) *Sei $f(X) = a_4X^4 + a_3X^3 + a_2X^2 + a_1X + a_0$ ein Polynom mit ganzzahligen Koeffizienten. Seien alle a_i ungerade. Man zeige, dass f irreduzibel über $\mathbb{Q}$ ist.*

Aufgabe 2.59 (H 00, T1, A2) *Seien a, b, c positive natürliche Zahlen. Man zeige:*

a) Das Polynom $X^a + Y^b$ ist im Polynomring $\mathbb{C}[X, Y]$ durch kein Quadrat eines Primpolynoms teilbar.

b) Das Polynom $X^a + Y^b + Z^c$ ist irreduzibel in $\mathbb{C}[X, Y, Z]$.

Aufgabe 2.60 (H 00, T3, A2) *Sei P der Polynomring über $\mathbb{Q}$ in den Unbestimmten X, Y und Z und $f = X^a + Y^b \cdot Z^c \in P$ mit positiven, teilerfremden, ganzen Zahlen a, b, c. Zeigen Sie:*

a) Es gibt ganze Zahlen α, β und γ, so dass

$$2^{\alpha a} \cdot f(2^{-\alpha} \cdot X, 2^{\beta} \cdot Y, 2^{\gamma} \cdot Z) = X^a + 2Y^b \cdot Z^c$$

b) f ist in P irreduzibel.

Aufgabe 2.61 (H 98, T1, A3) *Ist das Polynom*

$$3X^3 - 6X^2 + \frac{3}{2}X - \frac{3}{5}$$

in $\mathbb{Q}[X]$ irreduzibel?

Aufgabe 2.62 (H 98, T2, A3) *Sei p eine Primzahl.*

a) Zeigen Sie, dass das Polynom $f = X^p - X - 1$ irreduzibel über dem endlichen Körper $\mathbb{F}_p$ ist.

b) Ist f auch irreduzibel über $\mathbb{Z}$?

Aufgabe 2.63 (F 97, T3, A2) *Bestimmen Sie alle ganzen Zahlen a, für die das Polynom $f_a(X) = 4X^2 + 4X + a$ in $\mathbb{Z}[X]$ bzw. in $\mathbb{Q}[X]$ irreduzibel ist.*

Aufgabe 2.64 (F 95, T3, A2) *Sei A kommutativer nullteilerfreier Ring mit Eins, und sei $A[X]$ der Polynomring in einer Variablen über A.*

a) Seien $a, b \in A$, und a sei eine Einheit. Zeigen Sie, dass der A-Algebra Endomorphismus ϕ von $A[X]$ mit $\phi(X) = aX + b$ ein Automorphismus von $A[X]$ ist.

b) Zeigen Sie, dass jeder A-Algebra Automorphismus von $A[X]$ von der in a) beschriebenen Form ist.

Aufgabe 2.65 (H 94, T3, A2) *Sind folgende Polynome reduzibel oder irreduzibel in $\mathbb{Q}[X]$?*

(a) $x^3 - 5x^2 + 2x + 1$

(b) $x^4 - 4x^3 + 6x^2 - 4x + 4$

Aufgabe 2.66 (F 93, T2, A2) *Es sei R ein Polynomring in zwei Unbestimmten X und Y über einem Körper K. Es sei P das von $X - Y$ erzeugte Ideal in R, und es sei M das von $X - Y$ und X erzeugte Ideal in R. Zeigen Sie:*

a) P ist Primideal.

b) M ist ein maximales Ideal.

(Sie dürfen verwenden, dass R faktoriell ist.)

Aufgabe 2.67 (H 92, T2, A1) *Es sei p ein Primelement eines faktoriellen Ringes R. Für $q \in R$ mit $q \neq 0$ sei $S := R[X]/(X^2 - pq^2)$, und es bezeichne ξ die Restklasse von X in S. Zeigen Sie:*

a) S ist ein Integritätsring.

b) $S = R \oplus R\xi$.

c) $I := \{aq + b\xi | a, b \in R\}$ ist ein Ideal von S.

d) Es ist $S/I \simeq R/(q)$, und I ist genau dann ein Primideal von S, wenn q ein Primelement von R ist.

Aufgabe 2.68 (F92, T2, A2) *Sei K ein Körper, und es bezeichne a_b mit $b \in L$ den Kern des Homomorphismus $\varphi_b : K[X] \to K$, der durch $f(X) \to f(b)$ gegeben ist. Man zeige*

a) Für $b_1, b_2 \in K, b_1 \neq b_2$, sind a_{b_1}, a_{b_2} teilerfremde Ideale in $K[X]$.

b) Zu $a_1, ..., a_n \in K$ und paarweise verschiedenen $b_1, ..., b_n \in K$ gibt es ein $g(X) \in K[X]$ mit $g(b_i) = a_i, i = 1, ..., n$.

Aufgabe 2.69 (H 90, T1, A4) *Beweisen Sie, dass folgende Polynome über $\mathbb{Q}$ irreduzibel sind:*
$f = x^4 - 4x^3 + 2$
$g = x^2 + 4x + 7$
$h = x^3 - 38x^2 - 5x + 719$.

2.6 Polynomrechnen

Wir wollen hier einige sehr konkrete Formeln für Polynome herleiten. Ich lehne mich dabei ziemlich an das Buch von van der Waerden an.

2.6.1 Elementarsymmetrische Polynome

Ein Polynom

$$f(X) = X^n + a_{n-1}X^{n-1} + ... + a_1X + a_0 \in R[X]$$

zerfalle über R vollständig in Linearfaktoren. Das bedeutet

$$f(X) = (X - x_1) \cdot (X - x_2) \cdot ... \cdot (X - x_n), \quad x_1, ..., x_n \in R.$$

Wenn man hier ausmultipliziert und nach Potenzen von X sortiert, findet man für die Koeffizienten a_ν

$$\begin{array}{lcll} a_{n-1} & = & -\sum_\nu x_\nu & = & -(x_1 + ... + x_n), \\ a_{n-2} & = & \sum_{\mu<\nu} x_\mu x_\nu & = & x_1x_2 + ... + x_{n-1}x_n, \\ a_{n-3} & = & -\sum_{\lambda<\mu<\nu} x_\lambda x_\mu x_\nu & = & -(x_1x_2x_3 + ... + x_{n-2}x_{n-1}x_n), \\ & \vdots & & \vdots & \\ a_0 & = & & = & (-1)^n x_1x_2 \cdot ... \cdot x_n \end{array}$$

Diese Ausdrücke sind symmetrisch in den Wurzeln $x_1, ..., x_n$. Permutiert man die Wurzeln, dann ändert sich das Polynom f nicht, und auch seine Koeffizienten bleiben unverändert.

Definition 2.27 *Es seien $x_1, ..., x_n$ Unbestimmte. Ein Polynom $\sigma \in R[x_1, ..., x_n]$ heißt* symmetrisch*, wenn für jede Permutation $\pi \in S_n$ gilt*

$$\sigma(x_1, ..., x_n) = \sigma(x_{\pi(1)}, ..., x_{\pi(n)}).$$

Die elementarsymmetrischen Polynome *in $x_1, ..., x_n$ sind*

$$\begin{array}{rcl} \sigma_1 & = & x_1 + ... + x_2, \\ \sigma_2 & = & x_1x_2 + ... + x_{n-1}x_n, \\ & \vdots & \\ \sigma_{n-1} & = & x_1x_2 \cdot ... \cdot x_{n-1} + ... + x_2x_3 \cdot ... \cdot x_n, \\ \sigma_n & = & x_1x_2 \cdot ... \cdot x_{n-1}x_n. \end{array}$$

Bis auf das Vorzeichen sind das genau die Koeffizienten im obigen Polynom f. Das Hauptproblem dieser Vorlesung, nämlich das Problem, die Wurzeln $x_1, ..., x_n$ eines Polynoms zu finden, kann man dann so formulieren:

- Gegeben die Werte der elementarsymmetrischen Polynome in $x_1, ..., x_n$,
- gesucht die Werte $x_1, ..., x_n$ selbst.

Satz 2.34 (Hauptsatz über symmetrische Polynome) *Jedes symmetrische Polynom $f \in R[x_1, ..., x_n]$ lässt sich eindeutig als ein Polynom $\varphi(\sigma_1, ..., \sigma_n)$ darstellen.*

Beispiel 2.41 *Für jedes $r \geq 1$ ist die Potenz-Summe*

$$s_r = x_1^r + ... + x_n^r$$

ein symmetrisches Polynom vom Grad r. Seine Darstellung als Polynom in den elementarsymmetrischen Polynomen ist z.B. für $n \geq 2$

$$\begin{aligned} s_2 &= x_1^2 + x_2^2 + ... + x_n^2 \\ &= (x_1 + ... + x_n)^2 - 2(x_1x_2 + ... + x_{n-1}x_n) \\ &= \sigma_1^2 - 2\sigma_2, \end{aligned}$$

und für $n \geq 3$

$$\begin{aligned} s_3 &= x_1^3 + x_2^3 + ... + x_n^3 \\ &= (x_1 + ... + x_n)^3 - 3(x_1^2x_2 + ... + x_{n-1}x_n^2) - 6(x_1x_2x_3 + ... + x_{n-2}x_{n-1}x_n) \\ &= \sigma_1^3 - 3(s_1s_2 - s_3) - 6\sigma_3 \\ &= 3s_3 + \sigma_1^3 - 3\sigma_1(\sigma_1^2 - 2\sigma_2) - 6\sigma_3 \\ &= 3s_3 - 2\sigma_1^3 + 6\sigma_1\sigma_2 - 6\sigma_3, \\ s_3 &= \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3. \end{aligned}$$

Definition 2.28 *Ein Polynom*

$$f = \sum_{k_1,...,k_n} a_{k_1,...,k_n} x_1^{k_1} \cdot ... \cdot x_n^{k_n}$$

heißt homogen *vom Grad d, wenn $a_{k_1,...,k_n} = 0$, falls $k_1 + ... + k_n \neq d$.*

Jedes Polynom $f \in R[X]$ ist Summe von (eindeutig bestimmten) homogenen Polynomen. Das elementarsymmetrische Polynom σ_d ist homogen vom Grad d. Ein Monom in den elementarsymmetrischen Polynomen

$$\varphi(\sigma_1, ..., \sigma_n) = \sigma_1^{\mu_1} \cdot ... \cdot \sigma_n^{\mu_n}$$

ist als Polynom in $x_1, ..., x_n$ homogen vom Grad

$$g = \mu_1 + 2\mu_2 + ... + n\mu_n.$$

Man nennt diese Zahl g das Gewicht des Monoms φ.

Um Satz 2.34 zu zeigen, genügt es folgende Hilfsaussage zu beweisen.

Satz 2.35 *Jedes symmetrische Polynom $f \in R[X]$, homogen vom Grad d, lässt sich auf genau eine Weise schreiben als Summe von Monomen des Gewichts d in den elementarsymmetrischen Polynomen.*

Beweis. Existenz: Wir ordnen f lexikographisch. D.h., ein Monom $a_{k_1,...,k_n}x^{k_1}\cdot ...\cdot x^{k_n}$ kommt vor $a_{l_1,...,l_n}x^{l_1}\cdot ...\cdot x_n^{l_n}$, wenn die erste Differenz $k_i - l_i \neq 0$ positiv ist. Konkret sieht das so aus:

$$f = a_{d,0,...,0}x_1^d + a_{d-1,1,0,...,0}x_1^{d-1}x_2 + ...$$

Natürlich braucht f nicht mit dem Monom x_1^d anzufangen. Sei etwa

$$f = a_{k_1,...,k_n}x_1^{k_1}\cdot ...\cdot x_n^{k_n} + (\text{ lexikographisch höhere Summanden }).$$

Wegen der lexikographischen Anordung ist hier $k_1 \geq k_2 \geq ... \geq k_n$.

Der erste Summand von f ist auch der lexikographisch erste Summand im Monom

$$\varphi_1 := a_{k_1,...,k_n}\sigma_1^{k_1-k_2}\sigma_2^{k_2-k_3}\cdot ...\cdot \sigma_n^{k_n}$$

aus elementarsymmetrischen Polynomen. In der Differenz $f - \varphi_1$ kürzt sich der lexikographisch erste Summand weg. So kann man weitermachen und findet nach endlich vielen Schritten

$$f - \varphi_1 - ... - \varphi_s = 0.$$

Eindeutigkeit: Es sei

$$f = \varphi_1(\sigma_1, ..., \sigma_n) + \varphi_2(\sigma_1, ..., \sigma_n) + ...$$

mit Monomen φ_1, $\varphi_2, ...$. Das Monom vom Gewicht d zum lexikographisch ersten Summanden von f ist durch f eindeutig bestimmt. Das subtrahieren wir von f und beweisen die Aussage durch Induktion nach der Anzahl der vorkommenden Monome $\varphi_1, ..., \varphi_s$. □

Satz 2.36 (Formeln von Newton) *Die Potenz-Summen s_r und die elementarsymmetrischen Polynome $\sigma_\nu \in R[x_1, ..., x_n]$ sind durch die folgenden Formeln verknüpft:*

Für $r > n$ ist

$$s_r - s_{r-1}\sigma_1 + s_{r-2}\sigma_2 \pm ... + (-1)^{n-1}s_{r-n+1}\sigma_{n-1} + (-1)^n s_{r-n}\sigma_n = 0.$$

Für $r \leq n$ gilt

$$s_r - s_{r-1}\sigma_1 + s_{r-2}\sigma_2 \pm ... + (-1)^{r-1}s_1\sigma_{r-1} + (-1)^r r\cdot\sigma_r = 0.$$

Beweis. Im Ring $R[x_1, ..., x_n][x]$ betrachten wir das Polynom

$$(x - x_1)\cdot(x - x_2)\cdot ...\cdot(x - x_n) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} \pm ... + (-1)^n\sigma_n.$$

Setzen wir hierin $x = x_i$, so folgt

$$x_i^n - \sigma_1 x_i^{n-1} + \sigma_2 x_i^{n-2} \pm ... + (-1)^n\sigma_n = 0, \quad i = 1, ..., n.$$

Das ist unsere Ausgangsformel.

Addieren wir in dieser Ausgangsformel über $i = 1, ..., n$, so bekommen wir

$$s_n - \sigma_1 s_{n-1} + \sigma_2 s_{n-1} \pm ... + (-1)^{n-1}\sigma_{n-1}s_1 + (-1)^n n\cdot\sigma_n = 0.$$

Das ist die Behauptung für $r = n$. Für $r > n$ multiplizieren wir die Ausgangsformel mit x_i^{r-n}

$$x_i^r - \sigma_1 x_i^{r-1} + \sigma_2 x_i^{r-2} \pm ... + (-1)^n x_i^{r-n} \sigma_n = 0$$

und addieren wieder über $i = 1, ..., n$ um die behauptete Formel zu erhalten. Wenn $r < n$ ist, betrachten wir das symmetrische Polynom

$$f(x_1, ..., x_n) := s_r - s_{r-1}\sigma_1 + s_{r-2}\sigma_2 \pm ... + (-1)^{r-1}\sigma_{r-1} + (-1)^r r \cdot \sigma_r = 0$$

vom Grad $r < n$. Hier ist $f(x_1, ..., x_r, 0, ..., 0) = 0$, weil $s_k(x_1, ..., x_r, 0, ..., 0)$ und $\sigma_k(x_1, ..., x_r, 0, ..., 0)$ die entsprechenden Polynome über dem Ring $R[x_1, ..., x_r]$ sind, und weil hier die Formel vom Grad r schon bewiesen ist. Jedes Monom in $f(x_1, ..., x_n)$ enthält höchstens r verschiedene Unbestimmte x_i. Bis auf Permutationen der x_i ist es ein Monom in $f(x_1, ..., x_r, 0, ..., 0)$ und hat somit den Koeffizienten 0. □

Aufgabe 2.70 *Bestimmen Sie mit den Formeln von Newton die Darstellung der Potenzsummen*

$$s_2,\ s_3,\ s_4,\ s_5$$

als Polynome in den elementarsymmetrischen Polynomen.

2.6.2 Resultante

Jetzt sei K ein Körper. Der Ring $K[X]$ ist faktoriell, und wir behandeln die Frage: Wann haben zwei Polynome

$$f = a_m X^m + a_{m-1} X^{m-1} + a_0,\ g = b_n X^n + b_{n-1} X^{n-1} + ... + b_0 \ \in K[X], \quad a_m, b_n \neq 0,$$

einen gemeinsamen irreduziblen Faktor (notwendig ein Polynom vom Grad ≥ 1 in $K[X]$)?

Satz 2.37 *Die Polynome f und g haben genau dann einen gemeinsamen irreduziblen Faktor, wenn es Polyme $\varphi, \psi \in K[X]$ gibt mit*

$$\varphi \cdot f + \psi \cdot g = 0, \quad Grad(\varphi) < n = Grad(g),\ Grad(\psi) < m = Grad(f).$$

Beweis. $\Rightarrow$: Voraussetzung ist $f = f_1 \cdot h$ und $g = g_1 \cdot h$ mit $Grad(h) > 0$. Dann hat also g_1 einen kleineren Grad als g, und f_1 einen kleineren Grad als f. Wir setzen $\varphi := g_1$ und $\psi := -f_1$, und finden

$$\varphi \cdot f + \psi \cdot g = (g_1 \cdot f_1 - f_1 \cdot g_1) \cdot h = 0.$$

$\Leftarrow$: Wir zerlegen $f = f_1 \cdot ... \cdot f_k$ in ein Produkt irreduzibler Faktoren f_i. Wegen $Grad(\psi) < Grad(f)$ können nicht alle diese Faktoren in ψ vorkommen. Mindestens einer muss in g vorkommen und ist eine gemeinsamer irreduzibler Faktor von f und g. □

Um die Bedingung aus Satz 2.37 auszuwerten, schreiben wir sie um als ein lineares Gleichungssystem für die unbekannten Koeffizienten von φ und ψ. Wir setzen an

$$\varphi = c_{n-1}X^{n-1} + c_{n-2}X^{n-2} + ... + c_0, \quad \psi = d_{m-1}X^{m-1} + d_{m-2}X^{m-2} + ... + d_0.$$

Dann wird die Gleichung $\varphi f + \psi g = 0$ äquivalent zu den $m+n$ linearen Gleichugen

$$\begin{array}{llllllll}
a_0c_0 & & & & +b_0d_0 & & & = 0 \\
a_1c_0 & +a_0c_1 & & & +b_1d_0 & +b_0d_1 & & = 0 \\
... & ... & ... & & ... & ... & ... & \vdots \\
 & & a_mc_{n-2} & +a_{m-1}c_{n-1} & & & b_nd_{m-2} & +b_{n-1}d_{m-1} = 0 \\
 & & & a_mc_{n-1} & & & & +b_nd_{m-1} = 0
\end{array}$$

für die $m+n$ unbekannten Koeffizienten $c_0, ..., d_{m-1}$. Es gibt genau dann nicht-triviale Lösungen, wenn die Determinante der $(m+n) \times (m+n)$-Koeffizientenmatrix $= 0$ ist. Die Determinante der transponierten Matrix

$$Res(f,g) := det \begin{pmatrix}
a_0 & a_1 & ... & ... & a_m & & & \\
 & a_0 & a_1 & ... & a_{m-1} & a_m & & \\
 & & \ddots & \ddots & & \ddots & \ddots & \\
 & & & & & & a_{m-1} & a_m \\
b_0 & b_1 & ... & ... & b_n & & & \\
 & b_0 & b_1 & ... & b_{n-1} & b_n & & \\
 & & \ddots & \ddots & & \ddots & \ddots & \\
 & & & & & & b_{n-1} & b_n
\end{pmatrix} \begin{matrix} \} n \\ \\ \\ \\ \} m \\ \\ \\ \end{matrix}$$

heißt *Resultante* der Polynome f und g. Da es verschiedene andere Formeln für diese Resultante gibt, nennt man diese Determinante auch die *Sylvestersche* Form der Resultante.

Satz 2.37' *Zwei Polynome f und $g \in K[x]$ haben genau dann einen gemeinsamen irreduziblen Faktor, wenn $Res(f,g) = 0$.*

Die Resultante $R(f,g)$ der beiden Polynome ist nicht ganz unabhängig von der Reihenfolge dieser Polynome: Vertauscht man f mit g, so vertauscht man in der $(m+n) \times (m+n)$-Matrix die ersten n mit den letzten m Zeilen. Die Determinante ändert dabei ihr Vorzeichen $m \cdot n$ mal:

Satz 2.38 *Für zwei Polynome f, bzw. g vom Grad m, bzw. n ist*

$$Res(f,g) = (-1)^{m \cdot n} Res(g,f).$$

Für konkrete Rechnungen ist diese Resultante ziemlich unhandlich. Dazu das einfachste, nicht ganz triviale

Beispiel 2.42 *Die Resultante zweier quadratischer Polynome*

$$f(X) = a_1X^2 + b_1X + c_1 \quad und \quad g(X) = a_2X^2 + b_2X + c_2$$

ist die Determinante der 4×4-Matrix

$$\begin{pmatrix} c_1 & b_1 & a_1 & 0 \\ 0 & c_1 & b_1 & a_1 \\ c_2 & b_2 & a_2 & 0 \\ 0 & c_2 & b_2 & a_2 \end{pmatrix}.$$

Damit diese Polynome wirklich den Grad zwei haben, nehmen wir $a_1 \neq 0 \neq a_2$ an. Wir multiplizieren die zweite Zeile mit $-a_2/a_1$ und ziehen sie dann von der vierten Zeile ab:

$$\begin{pmatrix} c_1 & b_1 & a_1 & 0 \\ 0 & c_1 & b_1 & a_1 \\ c_2 & b_2 & a_2 & 0 \\ 0 & c_2 - \frac{a_2}{a_1}c_1 & b_2 - \frac{a_2}{a_1}b_1 & 0 \end{pmatrix}$$

Hier entwickeln wir nach der letzten Spalte und finden für die Determinante

$$a_1 \cdot det \begin{pmatrix} c_1 & b_1 & a_1 \\ c_2 & b_2 & a_2 \\ 0 & c_2 - \frac{a_2}{a_1}c_1 & b_2 - \frac{a_2}{a_1}b_1 \end{pmatrix} = \begin{pmatrix} c_1 & b_1 & a_1 \\ c_2 & b_2 & a_2 \\ 0 & a_1c_2 - a_2c_1 & a_1b_2 - a_2b_1 \end{pmatrix}.$$

Entwicklung nach der letzten Zeile liefert

$$\begin{aligned} Res(f,g) &= (a_2c_1 - a_1c_2)(c_1a_2 - a_1c_2) + (a_1b_2 - a_2b_1)(c_1b_2 - b_1c_2) \\ &= (a_1c_2 - c_1a_2)^2 + (a_1b_2 - b_1a_2)(c_1b_2 - b_1c_2). \end{aligned}$$

Beispiel 2.43 *Für jedes Polynom*

$$f(X) = a_0 + a_1X + ... + a_{m-1}X^{m-1} + a_mX^m$$

ist $Res(f, X - c)$ die Determinante der $(m+1) \times (m+1)$ Matrix

$$\begin{pmatrix} a_0 & a_1 & ... & a_{m-1} & a_m \\ -c & 1 & & & \\ & -c & \ddots & & \\ & & \ddots & 1 & \\ & & & -c & 1 \end{pmatrix}.$$

Wir beseitigen die Einträge $= -c$ unterhalb der Diagonale, indem wir rechts beginnend jede Spalte c-mal zur vorhergehenden addieren. Dabei ändern sich die Einträge der ersten Zeile wie folgt:

$$\begin{aligned} a_{m-1} \quad & wird \quad a_{m-1} + ca_m, \\ a_{m-2} \quad & wird \quad a_{m-2} + ca_{m-1} + c^2a_m, \\ & \vdots \\ a_0 \quad & wird \quad a_0 + a_1c + ... + a_{m-1}c^{m-1} + a_mc^m = f(c). \end{aligned}$$

Also ist

$$Res(f, X-c) = det \begin{pmatrix} f(c) & * & \dots & * \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} = f(c).$$

Dies ist der Spezialfall $n = 1$ der folgenden wichtigen Form der Resultante:

Satz 2.39 *Die Polynome f und g seien normiert und mögen in Linearfaktoren zerfallen:*

$$f(X) = (X-\alpha_1) \cdot \dots \cdot (X-\alpha_m), \quad g(X) = (X-\beta_1) \cdot \dots \cdot (X-\beta_n).$$

Dann ist

$$Res(f,g) = \prod_{i,j} (\beta_i - \alpha_j) = \prod_i f(\beta_i),$$

wo $i = 1, \dots, n$ und $j = 1, \dots, m$ unabhängig voneinander laufen.

Das Produkt in Satz 2.39 bleibt offensichtlich beim Vertauschen der Nullstellen a_j von f ungeändert. Es ist eine symmetrische Funktion dieser Nullstellen. Nach dem Hauptsatz über symmetrische Polynome ist es also ein Polynom in den elementarsymmetrischen Funktionen der a_j, d.h., in den Koeffizienten des Polynoms f. Ebenso ist das Produkt symmetrisch in den b_i und deswegen ein Ausdruck in den Koeffizienten des Polynoms g. Die Sylvestersche Form der Resultante gibt genau diesen Ausdruck.

Dem Beweis von Satz 2.39 schicken wir eine Hilfsaussage voraus:

Satz 2.40 (Hilfssatz) *Für je zwei Polynome f und g gilt*

$$Res(f, (X-c) \cdot g) = f(c) \cdot Res(f,g).$$

Beweis. Es sei wieder

$$f(X) = a_0 + a_1 X + \dots + a_m X^m, \quad g(X) = b_0 + b_1 X + \dots + b_n X^n.$$

Dann ist

$$(X-c) \cdot g(X) = -cb_0 + (-cb_1 + b_0)X + \dots + (-cb_m + b_{m-1})X^m + b_m X^{m+1},$$

und die Resultante $Res(f, (X-c) \cdot g)$ ist die Determinante der Matrix

$$\left.\begin{pmatrix} a_0 & \dots & \dots & a_m & & & \\ & \ddots & & & \ddots & & \\ & & \ddots & \dots & \dots & \ddots & \\ & & & a_0 & & & a_m \\ -cb_0 & -cb_1+b_0 & \dots & -cb_m+b_{m-1} & b_m & & \\ & \ddots & \ddots & & \ddots & \ddots & \\ & & -cb_0 & -cb_1+b_0 & \dots & -cb_m+b_{m-1} & b_m \end{pmatrix}\right\} \begin{matrix} n+1 \\ \\ \\ \\ \\ \\ m \end{matrix}$$

Ohne diese Determinante zu ändern addieren wir, rechts beginnend, jede Spalte c-mal zur vorhergehenden. Dabei ändern sich die Einträge in jeder Zeile wie folgt:

$$\begin{array}{ll} b_m & \text{wird } b_m \\ -cb_m + b_{m-1} & \text{wird } b_{m-1}, \\ & \vdots \\ -cb_1 + b_0 & \text{wird } b_0, \\ -cb_0 & \text{wird } 0. \end{array}$$

Die Änderung der Matrix in ihrer oberen Hälfte ist etwas schwerer zu verfolgen. Dafür kürzen wir ab:

$$f^{(k)}(X) := \sum_{\mu=k}^{m} a_\mu X^{\mu-k}, \quad 0 \le k \le m.$$

Dann ist also

$$f^{(0)}(X) = f(X), \quad f^{(k)}(X) = a_k + X \cdot f^{(k+1)}(X), \quad f^{(m)}(X) = a_m.$$

Die Einträge in der i-ten Zeile, $1 \le i \le n+1$, ändern sich wie folgt:

$$\begin{array}{ll} 0 & \text{wird } 0, \\ & \vdots \\ a_m & \text{wird } a_m, \\ a_{m-1} & \text{wird } a_{m-1} + c \cdot a_m = f^{(m-1)}(c), \\ & \vdots \\ a_k & \text{wird } a_k + c \cdot f^{(k+1)}(c) = f^{(k)}(c), \\ & \vdots \\ a_0 & \text{wird } a_0 + c \cdot f^{(1)}(c) = f(c), \\ 0 & \text{wird } c \cdot f(c), \\ & \vdots \\ 0 & \text{wird } c^{i-1} \cdot f(c). \end{array}$$

Danach sieht unsere Matrix also folgendermaßen aus:

$$\begin{pmatrix} f(c) & f^{(1)}(c) & \dots & f^{(m-1)}(c) & a_m & & & \\ c \cdot f(c) & f(c) & f^{(1)}(c) & \dots & f^{(m-1)}(c) & a_m & & \\ \vdots & \ddots & \ddots & \ddots & & \ddots & \ddots & \\ c^n \cdot f(c) & \dots & c \cdot f(c) & f(c) & f^{(1)}(c) & \dots & f^{(m-1)}(c) & a_m \\ 0 & b_0 & b_1 & \dots & b_n & & & \\ & 0 & b_0 & b_1 & \dots & b_n & & \\ & & \ddots & \ddots & \ddots & & \ddots & \\ & & & 0 & b_0 & b_1 & \dots & b_n \end{pmatrix}$$

Jetzt ändern wir die Matrix in ihrem oberen Teil, indem wir, mit der n-ten Zeile beginnend, jede Zeile c-mal von der nachfolgenden abziehen. Wegen $f^{(k)}(c) - c \cdot f^{(k+1)}(c) = a_k$ bekommen wir danach die Matrix

$$\begin{pmatrix} f(c) & * & * & * & * & * & * \\ 0 & a_0 & a_1 & & a_m & & \\ \vdots & \ddots & \ddots & \ddots & & \ddots & \\ 0 & ... & 0 & a_0 & a_1 & & a_m \\ 0 & b_0 & b_1 & ... & b_n & & \\ \vdots & \ddots & \ddots & \ddots & & \ddots & \\ 0 & ... & 0 & b_0 & b_1 & ... & b_n \end{pmatrix}$$

Deren Determinante, immer noch die ursprüngliche Resultante, ist in der Tat $= f(c) \cdot Res(f, g)$. □

Satz 2.41 (Folgerung) *Für jedes Polynom f und jedes normierte, in Linearfaktoren zerfallende Polynom*

$$g(X) = (X - \beta_1) \cdot ... \cdot (X - \beta_n)$$

gilt

$$Res(f, g) = f(\beta_1) \cdot ... \cdot f(\beta_n).$$

Diese Aussage folgt aus Satz 2.40 durch Induktion nach n.

Dieser Beweis von Satz 2.41 ist sehr rechnerisch. Einen rein begrifflichen Beweis findet man z.B. im Buch von van der Waerden.

2.6.3 Diskriminante

Das normierte Polynom

$$F(X) = a_0 + a_1 X + ... + a_{n-1} X^{n-1} + X^n = (X - \alpha_1) \cdot ... \cdot (X - \alpha_n) \in K[X]$$

zerfalle in Linearfaktoren zu den Nullstellen $\alpha_i \in K$. Das Produkt aller Differenzen von Nullstellen

$$\prod_{i<j} (\alpha_i - \alpha_j) \in K$$

ist bis auf das Vorzeichen unabhängig von der Reihenfolge dieser Nullstellen. Es verschwindet genau dann, wenn f eine mehrfache Nullstelle besitzt.

Definition 2.29 (Diskriminante) *Das Produkt aller Differenzen-Quadrate*

$$D = D(f) := \prod_{i<j} (\alpha_i - \alpha_j)^2 \in K$$

heißt die Diskriminante des Polynoms f.

Vertauscht man die Reihenfolge der Nullstellen, so ändern sich diese Differenzen-Quadrate nicht. Die Diskriminante ist unabhängig von der Reihenfolge der Nullstellen! Damit ist sie eine symmetrische Funktion in den Nullstellen $\alpha_1, ..., \alpha_n$. Nach Satz 2.34 ist sie ein Polynomausdruck in den symmetrischen Funktionen dieser Nullstellen, d.h., in den Koeffizienten des Polynoms f. Wir geben jetzt einen solchen Ausdruck für D an. Damit kann man feststellen, ob ein Polynom mehrfache Nullstellen hat, ohne diese Nullstellen selbst zu kennen.

Beispiel 2.44 *Für ein quadratisches Polynom*

$$f(X) = X^2 + bX + c = (X - \alpha_1)(X - \alpha_2) \in \mathbb{C}[X]$$

ist

$$\alpha_1 = -\frac{b}{2} + \sqrt{(\frac{b}{2})^2 - c}, \quad \alpha_2 = -\frac{b}{2} - \sqrt{(\frac{b}{2})^2 - c},$$

und

$$\alpha_1 - \alpha_2 = 2\sqrt{(\frac{p}{2})^2 - c} = \sqrt{b^2 - 4c}.$$

Es folgt

$$D(f) = (\alpha_1 - \alpha_2)^2 = b^2 - 4c.$$

Für jedes Polynom $f(X) = a_0 + a_1X + ... + a_mX^m \in K[X]$ ist durch

$$f'(X) := a_1 + 2a_2X + ... + ma_mX^{m-1}$$

rein formal die Ableitung $f'(X) \in K[X]$ definiert. Mit Grenzwerten hat das jetzt nichts mehr zu tun. Die Ableitung $f \mapsto f'$ ist eine rein algebraische Operation auf Polynomen. Alle für die Ableitung von Polynomen gültigen algebraischen Formeln gelten auch für diese Ableitung. Insbesondere haben wir

$$c \in K \Rightarrow (cf)' = cf', \quad (f + g)' = f' + g', \quad (fg)' = f'g + fg'.$$

Wir betrachten jetzt die Resultante

$$R(f, f')$$

eines Polynoms f und seiner Ableitung.

Beispiel 2.45 *Für quadratisches Polynom $f(X) = aX^2 + bX + c$ ist*

$$Res(f, f') = \begin{pmatrix} c & b & a \\ b & 2a & 0 \\ 0 & b & 2a \end{pmatrix} = 4a^2c + ab^2 - 2ab^2 = -a(b^2 - 4ac) = -aD(f).$$

Satz 2.42 *Es sei*

$$f(X) = (X - \alpha_1) \cdot ... \cdot (X - \alpha_m)$$

ein normiertes Polynom, das in Linearfaktoren zerfällt. Dann ist

$$Res(f, f') = \pm \prod_{i<j} (\alpha_i - \alpha_j)^2 = \pm D(f).$$

Beweis. Nach der Produktformel ist

$$f'(X) = \sum_{k=1}^{m} (X - \alpha_1) \cdot ... \cdot \underbrace{(X - \alpha_k)}_{\text{weglassen}} \cdot ... \cdot (X - \alpha_m)$$

und

$$f'(\alpha_i) = (\alpha_i - \alpha_1) \cdot ... \cdot (\alpha_i - \alpha_{i-1}) \cdot (\alpha_i - \alpha_{i+1}) \cdot ... \cdot (\alpha_i - \alpha_m).$$

Aus den Sätzen 2.38 und 2.41 folgt dann

$$Res(f, f') = Res(f', f) = f'(\alpha_1) \cdot ... \cdot f'(\alpha_m) = \prod_{i \neq j} (\alpha_i - \alpha_j) = (-1)^{m \cdot (m-1)/2} \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

□

Die Diskriminante ist auch deswegen wichtig, weil sie nicht nur mehrfache Nullstellen, sondern auch mehrfache Faktoren in der Zerlegung von f in irreduzible Faktoren entdeckt:

Satz 2.43 *Für ein Polynom $f \in K[X]$, dessen Ableitung $f' \in K[X]$ nicht das Nullpolynom ist, sind äquivalent:*

i) In der Zerlegung von f in irreduzible Faktoren gibt es einen Faktor, der mehrfach vorkommt.

ii) Die Diskriminante $D(f)$ ist $= 0$.

Beweis. i) $\Rightarrow$ ii): Ist $f = g^2 \cdot h$, so berechnet man wie üblich mit der Produktregel

$$f' = 2gg' \cdot h + g^2 \cdot h' = g \cdot (2g'h + gh').$$

Die Polynome f und f' haben einen gemeinsamen Faktor, und nach Satz 2.37' ist ihre Resultante $R(f, f') = D(f) = 0$.

ii) $\Rightarrow$ i): Ist $D(f) = Res(f, f') = 0$, so gibt es einen irreduziblen Faktor $g \in K[x]$, der beide Polynome f und f' teilt. Sei etwa $f = g \cdot h$. Dann teilt g das Polynom

$$f' = g' \cdot h + g \cdot h',$$

also auch das Produkt $g' \cdot h$. Weil g irreduzibel ist, teilt es einen der beiden Faktoren g' oder h. Wenn g seine Ableitung g' teilen würde, kann das wegen $Grad(g') < Grad(g)$ nur passieren, wenn g' das Nullpolynom ist. Dann wäre aber $f' = 0$, im Widerspruch zur Voraussetzung. Wenn g das Polynom h teilt, ist g ein mehrfacher Faktor in f. □

Beispiel 2.46 *Die Diskriminante* $-(b^2 - 4c)$ *des quadratischen Polynoms* $X^2 + bX + c$ *verschwindet genau dann, wenn* $b^2 = 4c$. *Dann ist* $c = b^2/4$ *und*

$$X^2 + bX + \left(\frac{b}{2}\right)^2 = (X + \frac{b}{2})^2$$

ist ein Quadrat. Hier haben wir allerdings stillschweigend $0 \neq 2 \in K$ *vorausgesetzt. Wäre* $2 = 0$, *dann würde aus* $b^2 - 4c = 0$ *folgen* $b = 0$. *Die Ableitung des quadratischen Polynoms wäre das Nullpolynom* $2X$, *und das Kriterium aus Satz 2.42 wäre nicht anwendbar.*

Aufgabe 2.71 *Zeigen Sie:*

für das Polynom	*ist die Diskriminante* $D(f)$
$X^3 + aX^2 + bX + c$	$a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc$
$aX^4 + bX^2 + c$	$2^4a^2c(4ac - b^2)^2$

3 Körpererweiterungen

Eine Körpererweiterung des Körpers K ist ein Körper L, in dem K als Unterkörper enthalten ist. (Als ich diese Vorlesung hörte, hat man das Wort 'Unterkörper' in diesem Zusammenhang vermieden und ausschließlich 'Teilkörper' benutzt.) Der Inhalt dieses und des nächsten Kapitels ist die Theorie der Auflösbarkeit von Polynom-Gleichungen durch Radikale (= iteriertes Wurzel-Ziehen). (Wieder so ein Wort, das manche Kollegen vermeiden.) Dass diese Auflösbarkeit mit Körper-Erweiterungen zusammenhängt, das soll in diesen Kapiteln deutlich werden.

3.1 Definitionen

Definition 3.1 *Ist der Körper K ein Unterkörper eines Körpers L, so nennt man L eine (Körper-) Erweiterung von K.*

Das bedeutet also, $K \subset L$ ist abgeschlossen unter Addition, Subtraktion, Multiplikation und Division.

Beispiel 3.1 *Das Standard-Beispiel ist $\mathbb{R} \subset \mathbb{C}$. Aber auch $\mathbb{Q} \subset \mathbb{R}$ ist eine Körpererweiterung.*

Beispiel 3.2 *Sei K ein Körper und $p(X) \in K[X]$ ein* irreduzibles *Polynom. Weil $K[X]$ ein Hauptideal-Ring ist, ist das Ideal $(p) \subset K[X]$ maximal. Der Faktorring $L := K[X]/(p)$ ist dann nach Satz 2.9 ein Körper. Er ist eine Körpererweiterung von K.*

Ein Spezialfall dieser Konstruktion ist die Körpererweiterung $\mathbb{R} \subset \mathbb{C}$. Das Polynom $p(X) := X^2 + 1$ ist irreduzibel über $\mathbb{R}$. (Wäre es reduzibel würde es in Linearfaktoren zerfallen, die zu reellen Lösungen der Gleichung $X^2 = -1$ gehörten. Solche gibt es nicht.) Also ist $\mathbb{R}[X]/(X^2+1)$ ein Körper. Der Ring-Epimorphismus

$$\mathbb{R}[X] \to \mathbb{C}, \quad X \mapsto i,$$

hat als Kern ein Ideal $I \subset \mathbb{R}[X]$, welches das Ideal (X^2+1) enthält. Weil X^2+1 irreduzibel ist, muss $I = (X^2+1)$ sein. Folglich ist die Körpererweiterung $\mathbb{R} \subset \mathbb{C}$ isomorph zur Erweiterung $\mathbb{R} \subset \mathbb{R}[X]/(X^2+1)$.

Beispiel 3.3 *Die einzigen linearen Polynome in $\mathbb{F}_2[X]$ sind X und $X+1$. Das Polynom $p(X) := X^2 + X + 1 \in \mathbb{F}_2[X]$ spaltet keines von beiden ab und ist deswegen irreduzibel. Also ist*

$$\mathbb{F}_2 \subset L := \mathbb{F}_2[X]/(p)$$

eine Körpererweiterung. Die Elemente $0, 1 \in \mathbb{F}_2$, sowie die Restklassen von X und $X+1$ sind vier verschiedene Elemente in L. Weil $X^2 = X + 1 \, modulo \, (p)$, gibt es in L keine anderen Elemente. Für die Multiplikation in L gilt

$$X^2 = X + 1, \quad X(X+1) = 1, \quad (X+1)^2 = X^2 + 1 = X.$$

Ist $K \subset L$ eine Körpererweiterung, so ist L ein K-Vektorraum. Man kann ja die Elemente von L mit Elementen aus K multiplizieren. Die Eigenschaften des Vektorraums folgen aus den Körpereigenschaften von L.

Definition 3.2 *Ist $K \subset L$ eine Körpererweiterung, so heißt*

$$[L : K] := dim_K(L)$$

der Grad der Erweiterung. Die Erweiterung $K \subset L$ heißt endlich, wenn ihr Grad $[L : K]$ endlich ist.

Die oben angegebenen Körpererweiterungen $\mathbb{R} \subset \mathbb{C}$ und $\mathbb{F}_2 \subset \mathbb{F}_2[X]/(X^2 + X + 1)$ sind endliche Körpererweiterungen vom Grad zwei. Die Körpererweiterung $K \subset K(X)$ (rationale Funktionen) hat keinen endlichen Grad.

Satz 3.1 (Grad-Formel) *Sind*

$$K \subset L \subset M$$

endliche Körpererweiterungen, so gilt

$$[M : K] = [M : L] \cdot [L : K].$$

Beweis. Wir wählen eine K-Basis $l_1, ..., l_a \in L$ und eine L-Basis $m_1, ..., m_b \in M$. Die Behauptung ist bewiesen, wenn wir zeigen: Die $a \cdot b$ Produkte

$$l_1 \cdot m_1,\ l_1 \cdot m_2,\ ...,\ l_a \cdot m_b$$

bilden eine K-Basis von M. Wie in der Linearen Algebra müssen wir dazu zwei Dinge nachweisen:

1) Die angegebenen Produkte erzeugen den K-Vektorraum M: Jedes $m \in M$ ist eine Linearkombination

$$m = c_1 m_1 + ... + c_b m_b, \quad c_1, ..., c_b \in L.$$

Und jedes $c_i \in L$ ist eine Linearkombination

$$c_i = d_{1,i} l_1 + ... + d_{a,i} l_a, \quad d_{1,i}, ..., d_{a,i} \in K.$$

Daraus folgt

$$m = (d_{1,1} l_1 + ... + d_{a,1} l_a) \cdot m_1 + ... + (d_{1,b} l_1 + ... + d_{a,b} l_a) \cdot m_a = \sum_{i,j} d_{i,j} \cdot l_i m_j.$$

2) Die Produkte $l_i m_j \in M$ sind linear unabhängig über K: Sei etwa

$$\sum_{i=1,j=1}^{a,b} d_{i,j} \cdot l_i m_j = 0, \quad d_{i,j} \in K.$$

Dann gilt

$$\sum_{j=1}^{b} (\sum_{i=1}^{a} d_{i,j} l_i) m_j = 0.$$

Weil $m_1, ..., m_b \in M$ linear unabhängig über L sind, folgt

$$\sum_{i=1}^{a} d_{i,j} l_i = 0 \text{ für } j = 1, ..., b.$$

Und weil die $l_1, ..., l_a$ linear unabhängig über K sind, folgt $d_{i,j} = 0$, $i = 1, ..., a, j = 1, ..., b$. □

Definition 3.3 *Es sei $K \subset L$ eine Körpererweiterung und $a \in L$ ein Element, nicht $a \in K$. Dann bezeichnet man mit*

$$K(a) \subset L$$

den kleinsten Unterkörper von L, der a enthält. (D.h. also, den Durchschnitt aller Unterkörper von L, die a enthalten.) Der Körper $K(a)$ heißt der von a über K erzeugte Unterkörper von L.

Der Unterkörper $K(a) \subset L$ enthält alle Elemente $l \in L$, die sich als rationale Funktionen in a der Form

$$l = \frac{c_0 + c_1 a + ... + c_r a^r}{d_0 + d_1 a + ... + d_s a^s}, \quad c_0, ..., d_s \in K,$$

mit Nenner $\neq 0$ ausdrücken lassen. Weil diese Elemente offensichtlich einen Unterkörper von L bilden, stimmt $K(a)$ mit der Menge dieser Elemente überein.

Beispiel 3.4 *Wir betrachten in der Körpererweiterung $\mathbb{Q} \subset \mathbb{C}$ das Element $a := i$. Wegen $i^2 = -1$ ist jedes Polynom in i*

$$c_0 + c_1 i + ... + c_r i^r \in \mathbb{C},\ c_0, ..., c_r \in \mathbb{Q},$$

in Wirklichkeit ein Polynom $c_0 + c_1 i$ vom Grad ≤ 1 in i. Wenn $c_0 + c_1 i \neq 0$, ist sein Kehrwert

$$\frac{1}{c_0 + c_1 i} = \frac{1}{c_0^2 + c_1^2}(c_0 - c_1 i)$$

wieder ein solches Polynom in i vom Grad ≤ 1. Der Körper $\mathbb{Q}(i) \subset \mathbb{C}$ ist genau der in 2.2 definierte Körper $\mathbb{Q}(i)$.

Für so ein Element $a \in L \supset K$, $a \notin K$, gibt es zwei Möglichkeiten: Entweder gibt es ein Polynom $p(X) \in K[X]$, nicht das Null-Polynom, mit $p(a) = 0$, oder es gibt kein solches Polynom. Für das Element $i \in \mathbb{C} \supset \mathbb{Q}$ tut es das Polynom $p(X) = X^2 + 1$, für $\sqrt{2} \in \mathbb{R} \supset \mathbb{Q}$ das Polynom $p(X) = X^2 - 2$. In der Körpererweiterung $\mathbb{Q} \subset \mathbb{Q}(X)$ gibt es für die Unbestimmte X kein Polynom mit $p(X) = 0$.

Definition 3.4 *Es sei $K \subset L$ eine Körpererweiterung und $a \in L$. Das Körperelement $a \in L$ heißt* algebraisch über K, *wenn es ein Polynom $p(X) \in K[X]$ gibt derart, dass $p(a) = 0 \in L$ ist. Andernfalls heißt a* transzendent über K. *Die Körpererweiterung $K \subset L$ heißt* algebraisch, *wenn jedes Element $a \in L$ algebraisch über K ist.*

Das Element $a \in L \supset K$ ist genau dann algebraisch über K, wenn der Ring-Homomorphismus

$$K[X] \to L, \quad q(X) \mapsto q(a)$$

nicht injektiv ist. Weil $K[X]$ ein Hauptidealring ist, ist der Kern dieses Homomorphismusses ein Hauptideal $(p) \subset K[X]$. Jedes Polynom $q \in K[X]$ mit $q(a) = 0 \in L$ ist durch p teilbar. Von allen Polynomen q, die a annullieren, hat p den kleinsten Grad. Wenn wir p durch seinen höchsten Koeffizienten $\neq 0$ austeilen, können wir p normiert annehmen.

Definition 3.5 *Das Element $a \in L \supset K$ sei algebraisch über K. Das normierte Polynom kleinsten Grades, welches $a \in L$ annulliert, heißt das* Minimalpolynom *von $a \in L$ über K.*

Das Minimalpolynom eines algebraischen Elementes ist immer irreduzibel in $K[X]$. Wäre nämlich $p = p_1 \cdot p_2$, $p_1, p_2 \in K[X]$, mit $Grad(p_i) > 0$, so würde aus $p_1(a) \cdot p_2(a) = 0$ folgen, dass entweder $p_1(a) = 0$ oder $p_2(a) = 0$ wäre. Das Polynom p wäre nicht minimal gewesen.

Satz 3.2 *Das Element $a \in L \supset K$ ist genau dann algebraisch über K, wenn die Körpererweiterung $K \subset K(a)$ endlich ist.*

Beweis. $\Rightarrow$: Sei $a \in L$ algebraisch über K mit Minimalpolynom p. Dann gilt in L also

$$p(a) = c_0 + c_1 a + ... + c_{n-1} a^{n-1} + a^n = 0, \quad c_1, ..., c_n \in K,\ c_n \neq 0,$$

bzw.

$$a^n = -c_0 - c_1 a - ... - c_{n-1} a^{n-1}$$

Jeder Polynomausdruck $p(a) \in L$ ist also in Wirklichkeit ein Polynomausdruck vom Grad $\leq n-1$. Sei nun $q(X) \in K[X]$ ein Polynom mit $q(a) \neq 0$. Dann ist q nicht durch p teilbar und, weil p irreduzibel ist, gilt $ggT(p, q) = 1$. Nach Satz 2.16 gibt es Polynome $p_1, q_1 \in K[X]$ mit $p_1 p + q_1 q = 1$. Daraus folgt

$$q_1(a)q(a) = q_1(a)q(a) + p_1(a)p(a) = 1$$

und

$$\frac{1}{q(a)} = q_1(a) \in L.$$

Jeder rationale Ausdruck in a, jedes Element von $K(a)$ ist also ein Polynom in a vom Grad $\leq n-1$. Der Körper $K(a)$ wird als K-Vektorraum von den Potenzen $1 = a^0, a, a^2, ..., a^{n-1}$ erzeugt und ist eine endliche Erweiterung von K.

$\Leftarrow$: Sei umgekehrt die Körpererweiterung $K \subset K(a)$ endlich. Wir betrachten die Folge $a^0, a, a^2, ...$ der Potenzen von a. Weil $[K(a) : K]$ endlich ist, können diese Potenzen nicht alle linear unabhängig über K sein. Es gibt Potenzen $a^0, a, ..., a^n$ und Elemente $c_0, c_1, ..., c_n \in K$, $c_n \neq 0$, mit

$$c_0 + c_1 a + ... + c_n a^n = 0 \in L.$$

Das Element $a \in L$ ist algebraisch über K. $\square$

Satz 3.3 (Folgerung 1) *Es sei $a \in L \supset K$ algebraisch über K mit Minimalpolynom p. Dann hat $p \in K[X]$ den Grad $[K(a) : K]$. Der Ringhomomorphismus*

$$K[X] \to K(a), \quad X \mapsto a$$

induziert einen Körperisomorphismus $K[X]/(p) \to K(a)$.

Beweis. Der Grad des Minimalpolynoms p sei n. Im Beweis von Satz 3.2 haben wir gezeigt, dass die n Potenzen $a^0 = 1, a, ..., a^{n-1}$ von a den K-Vektorraum $K(a)$ aufspannen. Wegen der Minimalität von p sind diese Potenzen aber auch linear unabhängig über K und bilden eine Körperbasis von $K(a)$ über K. □

Satz 3.4 (Folgerung 2) *Jede endliche Körpererweiterung $K \subset L$ ist algebraisch.*

Beweis. Für alle $a \in L$ ist die Körpererweiterung $K \subset K(a)$ endlich, weil $K(a)$ ein K-Untervektorraum des endlich-dimensionalen K-Vektorraums L ist. □

Von diesem Satz gilt aber nicht die Umkehrung, denn es gibt auch unendliche algebraische Körpererweiterungen. Dazu betrachten wir $K = \mathbb{Q}$ und bezeichnen mit $L \subset \mathbb{C}$ die Menge aller algebraischen Zahlen. Dabei heißt eine Zahl $a \in \mathbb{C}$ *algebraisch*, wenn a algebraisch über $\mathbb{Q}$ ist. Algebraische Zahlen sind z.B. die unendlich vielen n-ten Wurzeln $\sqrt[n]{2}$ aus 2. Jede dieser Wurzeln wird von einem Polynom $X^n - 2$ annulliert. Nach Eisenstein (mit der Primzahl 2) ist dieses Polynom irreduzibel über $\mathbb{Z}$ und nach Gauß dann auch über $\mathbb{Q}$. Also ist $X^n - 2$ das Minimalpolynom von $\sqrt[n]{2}$ über $\mathbb{Q}$ und die Körpererweiterung $\mathbb{Q} \subset \mathbb{Q}(\sqrt[n]{2})$ hat den Grad n. Die Menge $L \subset \mathbb{C}$ aller algebraischen Zahlen enthält also Körpererweiterungen von beliebig großem Grad über $\mathbb{Q}$. Wenn wir jetzt noch zeigen, dass L ein Körper ist, dann ist $\mathbb{Q} \subset L$ eine unendliche, aber algebraische Erweiterung von $\mathbb{Q}$. Dazu verallgemeinern wir Definition 3.3.

Definition 3.6 *Es seien $K \subset L$ eine Körpererweiterung und $a_1, a_2, ... \in L$ Elemente im Erweiterungskörper. Dann ist $K(a_1, a_2, ...) \subset L$ der kleinste Unterkörper von L, der alle Elemente $a_1, a_2, ...$ enthält.*

Der Körper $K(a_1, a_2, ...)$ ist also der Durchschnitt aller Unterkörper von L, welch alle Elemente $a_1, a_2, ...$ enthalten. Seine Elemente sind die rationalen Ausdrücke $p(a_1, a_2, ...)/q(a_1, a_2, ...)$, wo p und q Polynome in endlich vielen der Elemente $a_1, a_2, ...$ mit $q(a_1, a_2, ...) \neq 0 \in L$ sind.

Satz 3.5 *Die Elemente a_1 und $a_2 \in L$ seien algebraisch über K. Dann ist auch der Körper $K(a_1, a_2) \subset L$ eine endliche Erweiterung von K.*

Beweis. Wegen Satz 3.2 brauchen wir nur zu zeigen, dass die Erweiterung $K(a_1) \subset K(a_1, a_2)$ endlich ist. Aber weil a_2 algebraisch über K ist, ist es erst recht algebraisch über $K(a_1)$ und die Körpererweiterung $K(a_1) \subset K(a_1, a_2)$ damit endlich. □

Satz 3.6 (Folgerung) *Die (über $\mathbb{Q}$) algebraischen, komplexen Zahlen bilden einen Unterkörper von $\mathbb{C}$.*

Beweis. Sind a_1 und a_2 zwei solche algebraische Zahlen, so ist die Körpererweiterung $\mathbb{Q} \subset \mathbb{Q}(a_1, a_2)$ nach Satz 3.5 algebraisch über $\mathbb{Q}$. Sie enthält Summe, Differenz, Produkt und (falls Nenner $\neq 0$) Quotienten von a_1 und a_2. Alle diese Zahlen sind deswegen algebraisch über $\mathbb{Q}$. $\square$

Aufgabe 3.1 (F 02, T3, A4d)) *Sei $f(X) = X^{19} + 19X + 57 \in \mathbb{Q}[X]$. Ist die Restklasse von $X^{18} + 2$ in $\mathbb{Q}[X]/(f)$ invertierbar?*

Aufgabe 3.2 *Es seien $K \subset L$ eine Körpererweiterung und $f, g \in K[X]$ Polynome. Die größten gemeinsamen Teiler von f und g in $K[X]$, bzw. $L[X]$ seien*

$$t_K = ggT(f, g) \in K[X], \quad bzw. \quad t_L = ggT(f, g) \in L[X].$$

Zeigen Sie: t_K und t_L sind in $L[X]$ assoziiert, d.h., unterscheiden sich höchstens um einen konstanten Faktor aus L.

Aufgabe 3.3 (H 99, T2, A4a)) *Sei K ein Erweiterungskörper von $\mathbb{Q}$ mit $[K : \mathbb{Q}] = 2$. Zeigen Sie, dass es genau eine quadratfreie Zahl $m \in \mathbb{Z}$ gibt, so dass $K \simeq \mathbb{Q}(\sqrt{m})$ ist. ($m \in \mathbb{Z}$ heißt quadratfrei, wenn $m \notin \{0, 1\}$ und wenn m nicht durch das Quadrat einer Primzahl teilbar ist.)*

Aufgabe 3.4 (H 98, T3, A4) *Sei $K|k$ eine algebraische Körpererweiterung. Seien $\alpha_1, ..., \alpha_n$ Elemente aus K und $f_1(X), ..., f_n(X)$ die zugehörigen Minimalpolynome über k. Beweisen Sie:*

$$[k(\alpha_1, ..., \alpha_n) : k] \leq \prod_{i=1}^{n} grad\, f_i.$$

Aufgabe 3.5 (H 97, T2, A1) *Sei $K \subset L$ eine endliche Körpererweiterung und $f \in K[X]$ ein irreduzibles nichtlineares Polynom mit*

$$ggT(grad\, f,\, [L : K]) = 1.$$

Zeigen Sie, dass f keine Nullstelle in L hat.

Aufgabe 3.6 (F 96, T1, A2) *Man betrachte das Polynom $f = X^7 + X - Y$ im Polynomring $\mathbb{Q}[X, Y]$.*

a) Zeigen Sie: Der Ring $R := \mathbb{Q}[X, Y]/(f)$ ist ein Integritätsring.

b) Zeigen Sie: Durch $\varphi(X) := X + (f)$ ist ein injektiver $\mathbb{Q}$-Homomorphismus $\varphi : \mathbb{Q}[X] \to R$ gegeben.

c) Ist der Quotientenkörper $Quot(R)$ von R eine algebraische Erweiterung von $\mathbb{Q}$?

Aufgabe 3.7 (F 96, T2, A4) *a) Zeigen Sie, dass $f := X^3 - X + 1 \in \mathbb{Q}[X]$ keine Nullstelle in $\mathbb{Q}$ hat.*

b) Sei $z \in \mathbb{C}$ eine Nullstelle von f. Stellen Sie z^{-1} als Linearkombination von $1, z, z^2$ mit rationalen Koeffizienten dar.

c) Bestimmen Sie das Minimalpolynom von z^2 über $\mathbb{Q}$.

Aufgabe 3.8 (F 95, T2, A5) *Sei x transzendent über einem Körper k.*

a) Man zeige: $k(x)$ ist eine algebraische Erweiterung von $k(\frac{x^3}{x+1})$.

b) Man bestimme das Minimalpolynom von x über $k(\frac{x^3}{x+1})$.

Aufgabe 3.9 (F 95, T3, A3) *Sei $f(X) = X^3 + 2X + 2 \in \mathbb{Q}[X]$, und sei α eine komplexe Nullstelle von f.*

a) Zeigen Sie, dass $1, \alpha, \alpha^2$ eine Basis des $\mathbb{Q}$-Vektorraums $\mathbb{Q}(\alpha)$ ist.

b) Schreiben Sie $(1+\alpha)^{-1}$ als Linearkombination mit rationalen Koeffizienten bezüglich dieser Basis.

Aufgabe 3.10 (H 94, T1, A2) *a) Sei $k(a)/k$ eine endliche Körpererweiterung. Für einen Teilkörper L, $k(a) \supset L \supset k$, sei $m_{a,L}(X)$ das Minimalpolynom von a über L. Man zeige:*

$$m_{a,L}(X) \mid m_{a,k}(X).$$

b) Man bestimme den Grad und alle Zwischenkörper von $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$.

Aufgabe 3.11 (H 94, T2, A3) *Gegeben Seien $a, b \in \mathbb{Q}^*$. Zeigen Sie: Wenn es einen Körperisomorphismus $\varphi : \mathbb{Q}(\sqrt{a}) \to \mathbb{Q}(\sqrt{b})$ gibt, dann gilt $\frac{a}{b} \in (\mathbb{Q}^*)^2$.*

Aufgabe 3.12 (H 94, T3, A3) *Sei L/K eine endliche Körpererweiterung und $\alpha \in L$. Multiplikation mit α definiert eine K-lineare Abbildung $\varphi_\alpha : L \to L$. Sei χ_α das charakteristische Polynom dieses K-Vektorraumhomomorphismus. Zeigen Sie: χ_α ist eine Potenz des Minimalpolynoms P_α von α.*

Aufgabe 3.13 (H 92, T1, A4) *Zeigen Sie durch Gradbetrachtung einer geeigneten Erweiterung von $\mathbb{Q}$, dass der Grad des Minimalpolynoms der komplexen Zahl*

$$z := \frac{\sqrt{2} + \sqrt{3} + i\sqrt{3}}{\sqrt{5} + \sqrt{7} + i\sqrt{7}}$$

über $\mathbb{Q}$ ein Teiler von 32 ist.

Aufgabe 3.14 (H 91, T1, A3) *$K(z)$ sei eine einfache transzendente Erweiterung des Körpers K. Man beweise die beiden folgenden Aussagen:*

a) $K(z^2)$ ist eine transzendente Erweiterung von K.

b) Es gibt unendlich viele Zwischenkörper zwischen K und $K(z)$.

3.2 Konstruktionen mit Zirkel und Lineal

Aus der Antike stammen die folgenden drei Konstruktionsprobleme:

- *Würfel-Verdopplung (Delisches Problem):* Gegeben ist eine Strecke a, zu konstruieren ist eine Strecke b mit
$$b^3 = 2 \cdot a^3.$$
- *Winkeldreiteilung:* Gegeben ist ein Winkel α, zu konstruieren ist der Winkel $\alpha/3$.
- *Reguläres n-Eck:* Zu $n \in \mathbb{N}$ ist der Winkel $2\pi/n$ zu konstruieren.

Aus irgend einem Grund haben dabei die alten Griechen unter 'Konstruktion' eine geometrische Konstruktion verstanden, die ausschließlich Zirkel und Lineal benutzt. Das kann keine Frage der Präzision gewesen sein, denn so ganz genau kann man nie eine Strecke durch zwei Punkte mit dem Lineal zeichnen. Ein ganz klein wenig verrutscht das Lineal immer. Und auch ein Zirkel ist ein ziemlich eigenwilliges Gerät, und macht nicht immer das, was man von ihm will. Außerdem haben die Griechen sich durchaus für Konstruktionen interessiert, die sehr viel kompliziertere Hilfsmittel benutzten, wie z.B. die Vorgabe recht komplizierter algebraischer Kurven. Es geht bei diesen drei Problemen also 'nur' um das Prinzip. Es sind rein intellektuelle Fragen.

Wir werden als Zeichenebene für diese Konstruktionen jetzt die komplexe Zahlenebene $\mathbb{C}$ zugrunde legen. Vorgegebene Größen werden wir uns als komplexe Zahlen vorstellen. Beim Delischen Problem etwa die Zahl $a \in \mathbb{R}$ und bei der Winkeldrittelung die Zahlen 1 und $e^{i\cdot\alpha/2\pi}$. Ist so eine Menge $M \subset \mathbb{C}$ von Zahlen vorgegeben, so nennen wir eine Zahl $z \in \mathbb{C}$ *aus M konstruierbar*, wenn der Punkt z nach endlich vielen Schritten mit Zirkel und Lineal aus Punkten von M konstruierbar ist. Mit Zirkel und Lineal ist es insbesondere möglich, zu einer gegebenen Geraden durch einen gegebenen Punkt eine Parallele zu konstruieren, und auf dieser Parallelen eine Strecke gegebener Länge abzutragen.

Der Schlüssel ist folgende Bemerkung:

Satz 3.7 *Die Menge $M \subset \mathbb{C}$ enthalte die Zahlen 0 und 1. Dann bilden alle aus M kostruierbaren Zahlen einen Unterkörper $C(M) \subset \mathbb{C}$. Er hat insbesondere die Eigenschaften:*

1) $i \in C(M)$;

2) $z \in C(M) \Rightarrow Re(z), Im(z) \in C(M)$;

3) $z \in C(M) \Rightarrow \bar{z} \in C(M)$;

Beweis. 1) Wir schlagen den Kreis um 0 durch die Zahl 1. Der zweite Schnittpunkt dieses Kreises mit der Geraden durch 0 und 1 (der reellen Achse) ist die Zahl $-1 \in C(M)$. Wir errichten mit Zirkel und Lineal die Mittelsenkrechte auf der Strecke $-1, 1$. Diese schneidet den ersten Kreis in den Punkten $\pm i \in C(M)$.

2) Wir fällen mit Zirkel und Lineal das Lot von z auf die Gerade durch 0 und 1. Der Lotfußpunkt ist die Zahl $Re(z)$. Ebenso ist der Lotfußpunkt von z auf die Gerade durch 0 und

i die Zahl $Im(z) \cdot i$. Der Kreis mit Zentrum 0 durch diese Zahl schneidet die reelle Achse in $\pm Im(z)$.

3) Der Kreis durch z um $Re(z)$ schneidet die Gerade durch z und $Re(z)$ außer in z noch in $\bar{z}$.

Jetzt müssen wir für $C(M) \subset \mathbb{C}$ noch die Körper-Eigenschaften nachweisen, also

4) $z \in C(M) \to -z \in C(M)$;

5) $z_1, z_2 \in C(M) \Rightarrow z_1 + z_2 \in C(M)$;

6) $z_1, z_2 \in C(M) \Rightarrow z_1 \cdot z_2 \in C(M)$;

7) $0 \neq z \in C(M) \Rightarrow z^{-1} \in C(M)$;

4) $-z$ ist der zweite Schnittpunkt des Kreises um 0 durch z mit der Geraden durch 0 und z.

5) Wir verschieben die Gerade durch 0 und z_1 parallel durch z_2 und tragen dann auf ihr von z_2 aus die Strecke $|z_1|$ in der richtigen Richtung ab. Dies ist die übliche Parallelogramm-Konstruktion für die Summe zweier Vektoren in der Ebene.

6) Wegen

$$z_1 = a_1 + ib_1,\ z_2 = a_2 + ib_2 \quad \Rightarrow \quad z_1 z_2 = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)i,$$

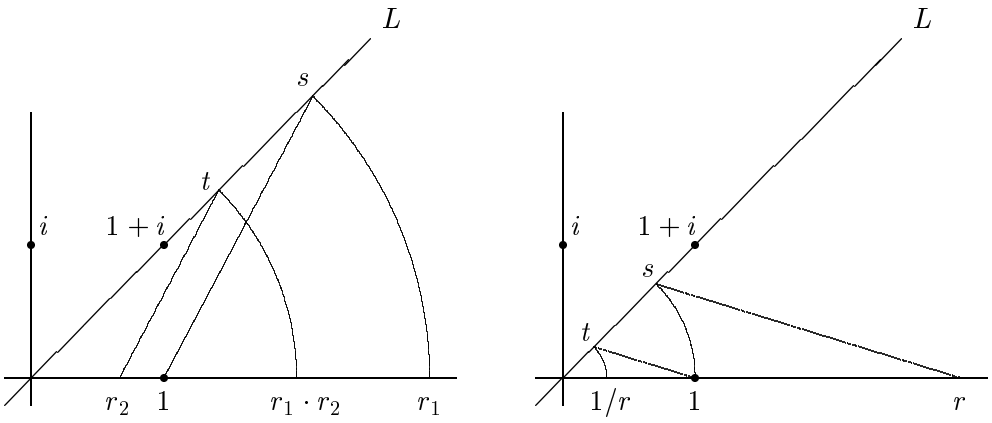
sowie 1),4) und 5) genügt es, die Behauptung für $0 < z_1 = r_1, z_2 = r_2 \in \mathbb{R}$ zu zeigen. Weiter können wir natürlich $r_2 \neq 1$ annehmen.

Wir schlagen den Kreis um 0 durch r_2 und schneiden ihn mit einer Geraden L durch 0 und $1 + i$. Einen der Schnittpunkte wählen wir und nennen ihn s. Die Gerade durch 1 und s verschieben wir parallel durch r_1 (das geht mit Zirkel und Lineal). Den Schnittpunkt dieser Parallelen mit L nennen wir t. Dann sind $0, 1, s$ und $0, r_1, t$ zwei ähnliche Dreiecke, und aus dem Strahlensatz folgt

$$\frac{t}{s} = \frac{r_1}{1} = r_1.$$

Der Kreis um 0 durch t trifft die positive reelle Achse in

$$|t| = r_1 |s| = r_1 r_2.$$



7) Wegen

$$\frac{1}{z} = \frac{\bar{z}}{z\bar{z}} = \frac{1}{Re(z)^2 + Im(z)^2}\bar{z},$$

sowie 2),3) und 6) genügt es, die Behauptung für $0 < z = r \in \mathbb{R}$ zu zeigen.

Wir schneiden den Kreis um 0 durch 1 mit der Geraden L durch 0 und $1+i$. Einen Schnittpunkt s verbinden wir mit r. Die Verbindungsgerade verschieben wir parallel durch 1. Der Schnittpunkt dieser Parallelen mit L sei t. Aus dem Strahlensatz folgt wieder

$$\frac{1}{|t|} = \frac{|s|}{|t|} = \frac{r}{1} = r.$$

Der Kreis um 0 durch t schneidet die positive reelle Achse im Punkt $1/r$. □

Der Körper $C(M)$ aus Satz 3.7 enthält insbesondere den Körper $\mathbb{Q}(M, \bar{M}) \subset \mathbb{C}$, der aus $\mathbb{Q}$ durch Adjunktion aller Zahlen aus M und ihrer komplex-konjugierten Zahlen entsteht.

Satz 3.8 *Eine Zahl $z \in \mathbb{C}$ gehört genau dann zu $C(M)$ (d.h., ist aus $0, 1$ und den Punkten von M konstruierbar), wenn es eine endliche Folge*

$$\mathbb{Q}(M, \bar{M}) = K_0 \subset K_1 \subset ... \subset K_n \subset \mathbb{C}$$

von quadratischen Körpererweiterungen $K_{\nu-1} \subset K_\nu$ gibt mit $z \in K_n$. Insbesondere ist

$$[\mathbb{Q}(M, \bar{M})(z) : \mathbb{Q}(M, \bar{M})] = 2^m,\ m \leq n,$$

eine Zweier-Potenz.

Beweis $\Rightarrow$: Eine Zahl $z \in C(M)$ entsteht aus bereits konstruierten Zahlen z_i durch eine von drei Konstruktionen:

1) Schneiden der Gerade durch z_1 und z_2 mit der Gerade durch z_3 und z_4;

2) Schneiden der Gerade durch z_1 und z_2 mit dem Kreis um z_3 durch z_4;

3) Schneiden des Kreises um z_1 durch z_2 mit dem Kreis um z_3 durch z_4.

Wir betrachten nacheinander diese drei Konstruktionen. Dabei nehmen wir an, die Zahlen z_1, z_2, z_3, z_4 seien bereits konstruiert. Da dies in endlich vielen Schritten passiert ist, können wir voraussetzen, die $z_k = a_k + ib_k$ liegen in einem Körper K_m, der aus $\mathbb{Q}(M, \bar{M})$ durch sukzessive quadratische Erweiterungen entstanden ist. Wir nehmen außerdem an, dass wir mit jeder Zahl auch die konjugiert-komplexe Zahl konstruiert haben (auch höchstens quadratische Erweiterungen). Mit jeder Zahl z_k liegt also auch $\bar{z}_k$ in K_m, damit auch $a_k = (z_k + \bar{z}_k)/2$ und $ib_k = z_k - a_k$.

1) Auf der Gerade durch z_1 und z_2 liegen alle Punkte $z_1 + s \cdot (z_2 - z_1)$, $s \in \mathbb{R}$, und auf der Gerade durch z_3 und z_4 die Punkte $z_3 + t \cdot (z_4 - z_3)$, $t \in \mathbb{R}$. Diese Parameter s und t für den Schnittpunkt erfüllen

$$\begin{aligned} z_1 + s \cdot (z_2 - z_1) &= z_3 + t \cdot (z_4 - z_3), \\ s \cdot (z_2 - z_1) + t \cdot (z_3 - z_4) &= z_3 - z_1. \end{aligned}$$

Wenn wir die letzte Gleichung als zwei Gleichungen für Real- und Imaginärteil schreiben, erhalten wir das lineare Gleichungssystem

$$\begin{aligned}(a_2-a_1)\cdot s+(a_4-a_3)\cdot t &= a_3-a_1,\\ i(b_2-b_1)\cdot s+i(b_4-b_3)\cdot t &= i(b_3-b_1),\end{aligned}$$

mit Koeffizienten in K_m. Auch dessen Lösungen s,t gehören zu K_m, und damit der Schnittpunkt.

2) Ein Punkt $z=a+ib$ aus der Gerade $z_1+s\cdot(z_2-z_1)$, $s\in\mathbb{R}$, liegt auf dem Kreis um z_3 durch z_4, wenn

$$\begin{aligned}|z-z_3|^2 &= |z_4-z_3|^2=:r^2\in K_m,\\ |z_1-z_3+s\cdot(z_2-z_1)|^2 &= r^2,\\ s^2\cdot|z_2-z_1|^2+2s\cdot Re((z_1-z_3)\cdot(\overline{z_2-z_1})) &= r^2-|z_1-z_3|^2.\end{aligned}$$

Dies ist eine quadratische Gleichung für s mit Koeffizienten in K_m. Die Lösungen $s_{1,2}$ liegen in einer quadratischen Erweiterung K_{m+1} von K_m. Zu dieser quadratischen Erweiterung gehören dann auch die beiden Schnittpunkte.

3) Ein Schnittpunkt z der beiden Kreise erfüllt die beiden Gleichungen

$$|z-z_1|^2=|z_2-z_1|^2,\quad |z-z_3|^2=|z_4-z_3|^2,$$

beziehungsweise

$$\begin{aligned}|z|^2+2\cdot Re(z\cdot\bar{z}_1) &= |z_2-z_1|^2-|z_1|^2,\\ |z|^2+2\cdot Re(z\cdot\bar{z}_3) &= |z_4-z_3|^2-|z_3|^2.\end{aligned}$$

Dann erfüllt z auch die Differenz beider Gleichungen

$$2\cdot Re(z\cdot(\overline{z_1-z_3}))=|z_2-z_1|^2-|z_1|^2-|z_4-z_3|^2+|z_3|^2=:c\in K_m.$$

Für $z=a+ib$ und $z_1-z_3=u+iv$ bedeutet dies

$$\begin{aligned}(a+ib)\cdot(u-iv)+(a-ib)\cdot(u+iv) &= c,\\ a\cdot u-(ib)\cdot(iv)&=c/2.\end{aligned}$$

Dies ist eine lineare Gleichung für die beiden Unbekannten a und ib. Die Koeffizienten der Gleichung gehören zum Körper K_m. Sie definiert eine Gerade in der Ebene $K_m\times K_m$. Diese wird aufgespannt von zwei Punkten (a_1,ib_1) und $(a_2,ib_2)\in K_m\times K_m$. Die Gleichung beschreibt in $\mathbb{C}$ die relle Gerade $a\cdot u+b\cdot v=c/2$. Auf ihr liegen die beiden Punkte $y_1:=a_1+ib_1$ und $y_2:=a_2+ib_2\in K_m$. Damit ist die Berechnung der Schnittpunkte beider Kreise zurückgeführt auf die Berechnung der Schnittpunkte eines der beiden Kreise mit der Gerade durch die Punkte y_1 und y_2. Dies war Rechnung 2).

$\Leftarrow$: Es genügt die Aussage für eine einzige quadratische Körpererweiterung $K_0\subset K_1$ zu zeigen: Jede Zahl in $c\in K_1$ ist aus Zahlen von K_0 mit Zirkel und Lineal konstruierbar. Wenn c nicht zu K_0 gehört, hat sein Minimalpolynom über K_0 den Grad zwei. Es sei etwa

$$X^2+p\cdot X+q,\quad p,q\in K_0.$$

Beide Nullstellen

$$c_{1,2} = -\frac{p}{2} \pm \sqrt{\left(\frac{p}{2}\right)^2 - q}$$

sind aus Zahlen von K_0 mit Zirkel und Lineal konstruierbar, wenn für jedes $z \in K_0$ die Quadratwurzel $\sqrt{z}$ so konstruierbar ist. Sei etwa

$$z = r \cdot e^{i\varphi}, \quad 0 < r \in \mathbb{R},\ \varphi \in \mathbb{R},$$

dann ist

$$\sqrt{z} = \sqrt{r} \cdot e^{i\varphi/2}.$$

Die komplexe Zahl $e^{i\varphi/2}$ ist durch Konstruktion der Winkelhalbierenden zu finden. Deswegen genügt es, die Behauptung für $z = r$, $0 < r \in \mathbb{R}$ zu zeigen.

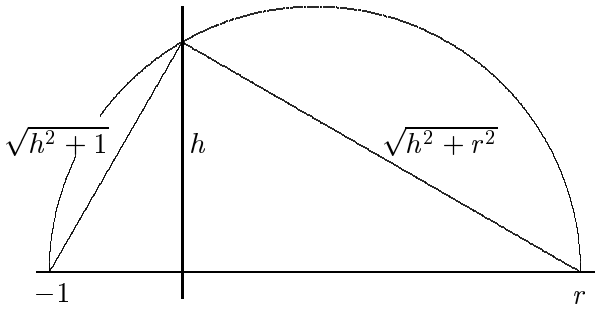
Wir konstruieren den Thaleskreis über dem Intervall $[-1, r]$. Er schneidet die imaginäre Achse in den Punkten $\pm i \cdot h$, $0 < h \in \mathbb{R}$. Das Dreieck mit den Ecken $-1, r$ und $i \cdot h$ hat bei $i \cdot h$ einen rechten Winkel. Die Kathetenlängen des Dreiecks sind

$$\sqrt{h^2+1} \quad \text{und} \quad \sqrt{h^2+r^2}.$$

Mit Pythagoras folgt

$$\begin{aligned} (h^2+1) + (h^2+r^2) &= (r+1)^2, \\ 2h^2 &= 2r, \\ h &= \sqrt{r}. \end{aligned}$$

Die gesuchte Wurzel ist also h und deswegen durch den Schnitt des Thaleskreises mit der imaginären Achse zu konstruieren. □



Wir wenden Satz 3.8 an auf die drei eingangs beschriebenen klassischen Probleme.

Delisches Problem: Es ist $a \in \mathbb{R}$ gegeben und $b \in \mathbb{R}$ mit $b = \sqrt[3]{2}a$ zu konstruieren. Wenn das mit Zirkel und Lineal ginge, dann ginge es auch für $a = 1$. Wir setzen hier $M = \emptyset$ und haben $\mathfrak{Q}(M, \bar{M}) = \mathbb{Q}$. Jeder Punkt, der mit Zirkel und Lineal konstruierbar ist, liegt in einem Erweiterungskörper K von $\mathbb{Q}$, für den $[K : \mathbb{Q}] = 2^n$ eine Zweierpotenz ist. Nun ist $b := \sqrt[3]{2}$ Nullstelle des über $\mathbb{Q}$ irreduziblen Polynoms $X^3 - 2$ und $[\mathbb{Q}(b) : \mathbb{Q}] = 3$. Wäre b in einem solchen Körper K enthalten, widerspräche dies der Gradformel (Satz 3.1). Das Delische Problem ist unlösbar.

Winkel-Dreiteilung: Jetzt sei $M = \{e^{i\alpha}\}$. Die Frage ist, ob $e^{i\alpha/3}$ zu einer Körpererweiterung von $\mathbb{Q}(e^{i\alpha})$ gehört, deren Grad eine Zweier-Potenz ist. Für manche α kann dies der Fall sein. Wenn z.B. $\alpha = \pi/2 = 90^0$ ist, dann ist $\alpha/3 = 30^0$ und $e^{i\alpha/3}$ eine Quadratwurzel von

$$e^{i\pi/3} = \frac{1}{2} + \frac{1}{2}\sqrt{-3}.$$

Die Zahl

$$e^{i\alpha/3} = \frac{i}{2} + \frac{1}{2}\sqrt{3}$$

liegt in dem Erweiterungskörper von $\mathbb{Q}(i, \sqrt{3})$ vom Grad 4.

Aber i.A. ist diese Eigenschaft eben nicht erfüllt. Dazu überlegen wir uns, dass es unendlich viele Zahlen $z = e^{i\alpha}$ gibt, die transzendent über $\mathbb{Q}$ sind. In der Tat: Der Einheitskreis $|z| = 1 \subset \mathbb{C}$ ist eine überabzählbare Menge. Und die über $\mathbb{Q}$ algebraischen Zahlen in $\mathbb{C}$ sind Nullstellen einer abzählbaren Menge von Polynomen, und bilden deswegen eine abzählbare Menge.

Wir wählen nun $z = e^{i\alpha}$ transzendent. Dann ist also $Q(z)$ der Körper der rationalen Funktionen in einer Unbestimmten z. Wir zeigen, dass $\sqrt[3]{z}$ nicht zu $\mathbb{Q}(z)$ gehört. Dann hat das Polynom $X^3 - z$ keine Nullstelle in $\mathbb{Q}(z)$ und ist irreduzibel. Es folgt

$$[Q(z, \sqrt[3]{z}) : \mathbb{Q}(z)] = 3,$$

und wegen der Gradformel kann $\mathbb{Q}(z, \sqrt[3]{z})$ in keiner Körpererweiterung von $\mathbb{Q}(z)$ liegen, deren Grad eine Zweier-Potenz ist.

In der Tat, sei etwa

$$\sqrt[3]{z} = \frac{p}{q}, \quad p, q \in \mathbb{Q}[z] \text{ teilerfremd.}$$

Weil dann auch p^3 und q^3 teilerfremd sind, würde aus

$$(\frac{p}{q})^3 = \frac{p^3}{q^3} = z, \quad p^3 = z \cdot q^3$$

folgen

$$3 \cdot Grad(p) = 1 + 3 \cdot Grad(q).$$

Das geht nicht. □

Reguläres n-Eck: Wenn man das reguläre n-Eck mit Zirkel und Lineal konstruieren kann, dann kann man die n-te Einheitswurzel $e^{2\pi i/n}$ mit Zirkel und Lineal aus 0 und 1 konstruieren, sie muss in einem Erweiterungskörper $K \supset \mathbb{Q}$ liegen, dessen Grad über $\mathbb{Q}$ eine Zweier-Potenz ist. Für manche n geht das:

$n = 3$: Die dritte Einheits-Wurzel

$$e^{2\pi i/3} = -\frac{1}{2} + \frac{i}{2}\sqrt{3}$$

ist Nullstelle des quadratischen Kreisteilungs-Polynoms

$$X^2 + X + 1 \in \mathbb{Q}[X].$$

$n = 4$: Die vierte Einheitswurzel i ist Nullstelle des quadratischen Polynoms $X^2 + 1 \in \mathbb{Q}[X]$.

$n = 5$: Die fünfte Einheits-Wurzel $\epsilon := e^{2\pi i/5}$ ist Nullstelle des nach Abschnitt 2.5 irreduziblen Kreisteilungs-Polynoms

$$X^4 + X^3 + X^2 + X + 1 \in \mathbb{Q}[X]$$

vom Grad vier. A priori bedeutet dies noch nicht, dass man die Körpererweiterung $Q(\epsilon) \supset \mathbb{Q}$ durch zwei quadratische Erweiterung bekommt. Aber in diesem Fall geht es: Man setzt

$$\eta := \epsilon + \epsilon^4 \in \mathbb{Q}(\epsilon).$$

Dann gilt

$$\eta^2 = \epsilon^2 + 2 + \epsilon^3 = 1 - (\epsilon + \epsilon^4) = 1 - \eta.$$

Also ist η eine Nullstelle des quadratischen Polynoms $X^2 + X - 1 \in \mathbb{Q}[X]$. Dieses Polynom hat die reellen Nullstellen

$$\eta_{1,2} = \frac{1}{2}(-1 \pm \sqrt{5}) \notin \mathbb{Q}.$$

Also ist $X^2 + X - 1$ über $\mathbb{Q}$ irreduzibel und $[\mathbb{Q}(\eta) : \mathbb{Q}] = 2$. Aus der Gradformel (Satz 2.1) folgt dann auch $[\mathbb{Q}(\epsilon) : \mathbb{Q}(\eta)] = 2$.

Auch das reguläre Fünfeck ist mit Zirkel und Lineal konstruierbar.

$n = p$ eine Primzahl: Die n-te Einheitswurzel $w := e^{2\pi i/n}$ ist Nullstelle des nach Abschnitt 2.5 irreduziblen Kreisteilungs-Polynoms

$$X^{p-1} + X^{p-2} + ... + X + 1 \in \mathbb{Q}[X].$$

Der Körpergrad $[\mathbb{Q}(w) : Q]$ ist deswegen $= p - 1$. Das reguläre p-Eck ist höchstens dann mit Zirkel und Lineal konstruierbar, wenn $p-1$ eine Zweier-Potenz ist. Für die 'meisten' Primzahlen, etwa $p = 7, 11, 13, 19$ ist dies nicht der Fall. Aber es gilt z.B. für $p = 17$. Und tatsächlich: Gauß gab mit 18 Jahren eine Konstruktion des regulären 17-Ecks mit Zirkel und Lineal.

Aufgabe 3.15 *Bestimmen Sie die kleinste Primzahl $p > 17$ mit der Eigenschaft, dass $p - 1$ eine Zweierpotenz ist.*

Aufgabe 3.16 *Die Zahl $x \in [0, 1]$ teilt das Intervall $[0, 1]$ im Verhältnis des* goldenen Schnittes, *wenn*

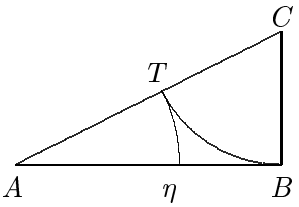
$$\frac{1}{x} = \frac{x}{1 - x}.$$

Daraus folgt

$$x = \eta = \frac{1}{2}(-1 + \sqrt{5}).$$

Zeigen Sie, dass dieser goldene Schnitt folgendermaßen konstruierbar ist: Man betrachte ein rechtwinkliges Dreieck ABC mit rechtem Winkel bei B und den Seiten $AB = 1$, $BC = 1/2$. Um

die Ecke C werde der Kreis vom Radius $1/2$ geschlagen. Dieser Kreis treffe die Hypotenuse AC im Punkt T. Dann ist $AT = \eta$.



Verwenden Sie dies, um das reguläre Fünfeck mit Zirkel und Lineal zu konstruieren.

Aufgabe 3.17 (H 96, T2, A1) *Zeigen Sie, dass die Fermatzahlen $F_n = 2^{2^n} + 1$ paarweise teilerfremd sind, z.B. mittels einer Zerlegung von $F_{n+k} - 2$, und folgern Sie daraus den Satz von Euklid, dass es unendlich viele Primzahlen gibt.*

3.3 Normale Körpererweiterungen

In 3.1 haben wir den Körper $K(a)$ definiert in der Situation, wo $K \subset L$ und $a \in L$ war. Man sagt, dieser Körper $K(a)$ entsteht aus K durch *Adjunktion* des Elementes $a \in L$. Man kann aber auch Elemente a an einen Körper K adjungieren, völlig losgelöst von einem eventuellen Erweiterungskörper L.

Dazu sei jetzt K ein Körper. Wir wollen die Nullstelle a eines irreduziblen Polynoms $p(X) \in K[X]$ adjungieren. Wir setzen ganz einfach

$$K(a) := K[X]/(p).$$

Weil das Polynom $p(X) \in K[X]$ irreduzibel ist, ist das Ideal $(p) \subset K[X]$ maximal, und der Ring $K[X]/(p)$ ist ein Körper. Insbesondere ist $X = (X \, mod \, (p)) \in K[X]/(p)$ ein Körperelement in der Erweiterung mit der Eigenschaft $p(X) = 0$. Der Körpergrad $[K[X]/(p) : K]$ stimmt mit dem Grad des Polynoms p überein. Das Polynom p, nachdem man es normiert hat, ist das Minimalpolynom des Elements X über K.

Definition 3.7 *Man sagt, der Körper $K[X]/(p)$ ist aus K entstanden durch symbolische Adjunktion einer Nullstelle des irreduziblen Polynoms p. Meist gibt man der Nullstelle einen anderen Namen als X, etwa c, nennt den Erweiterungskörper $K(c)$ und sagt dann: $K(c)$ ist aus K entstanden durch symbolische Adjunktion einer Wurzel des irreduziblen Polynoms p. Natürlich kann man diesen Prozess wiederholen und nacheinander Wurzeln $c_1, ..., c_k$ adjungieren um einen Körper $K(c_1, ..., c_k)$ zu erhalten. Die Körper $K(c)$, welche man durch Adjunktion einer einzigen Wurzel c erhält, heißen* einfache Körpererweiterungen

Beispiel 3.5 *Es sei K ein Körper und $c \in K$. Wir betrachten das Polynom $p(X) = X^2 - c$. Ist p reduzibel in $K[X]$, so spaltet es einen Linearfaktor $X - w, w \in K$, ab. Dann ist w eine Nullstelle von $X^2 - c$, d.h., es gilt $w^2 = c$. Somit ist c ein Quadrat in K. Das Polynom $p = X^2 - c$ ist also genau dann irreduzibel in $K[X]$, wenn $c \in K$ kein Quadrat ist.*

Sei nun $c \in K$ kein Quadrat (wie etwa $2 \in \mathbb{Q}$). Dann ist $X^2 - c$ irreduzibel und $K[X]/(X^2 - c)$ ist ein Körper. Er enthält die Nullstelle $X \bmod (X^2 - c)$ des Polynoms $X^2 - c$. Man setzt $X \bmod (X^2 - c) = \sqrt{c}$, nennt den Erweiterungskörper $K(\sqrt{c})$, und sagt, er ist aus K entstanden durch die Adjunktion der Wurzel aus c. Erweiterungskörper, die durch Adjunktion der Wurzel eines Körperelements entstehen, nennt man quadratische Erweiterungen.

Wir bezeichnen jetzt den Erweiterungskörper $K[X]/(X^2 - c)$ mit $K(\sqrt{c})$. Dann ist also $\sqrt{c}$ ein Element des Erweiterungskörpers, das die Gleichung $(\sqrt{c})^2 = c$ erfüllt. Es folgt

$$p(X) = X^2 - c = X^2 - (\sqrt{c})^2 = (X - \sqrt{c})(X + \sqrt{c}) \in K(\sqrt{c})[X].$$

Das Polynom $p(X) = X^2 - c$ zerfällt über $K(\sqrt{c})$ in zwei Linearfaktoren.

Beispiel 3.6 *Man braucht nicht unbedingt so ein reines quadratisches Polynom wie $X^2 - c$ zu betrachten sondern z.B. das Polynom*

$$p(X) = X^2 + b \cdot X + c, \quad b, c \in K.$$

Wenn p eine Nullstelle in K hat, zerfällt es in Linearfaktoren über K. Äquivalent dazu ist (Lösungsformel für die quadratische Gleichung), dass die Wurzel

$$\sqrt{D} \text{ aus der Diskriminante } D = b^2 - 4c$$

zu K gehört. Wir setzen also voraus, dies sei nicht der Fall, Das Polynom p sei irreduzibel über K.

Wir adjungieren eine Wurzel x_1 der Gleichung $p(X) = 0$, etwa die Restklasse von X in $K[X]/(X^2 + bX + c) = K(x_1)$. Sie erfüllt

$$x_1^2 + bx_1 + c = (x_1 + \frac{b}{2})^2 + c - \frac{b^2}{4} = 0.$$

Deswegen ist $2x_1 + b$ eine Wurzel aus der Diskriminante $D = b^2 - 4c \in K$. Der Körper $K(x_1)$ enthält den Körper $K(\sqrt{D})$, und wegen

$$[K(x_1) : K] = [K(\sqrt{D}) : K] = 2$$

ist $K(x_1) = K(\sqrt{D})$. Der Körper $K(x_1)$ ist also eine quadratische Erweiterung von K, wo man die Wurzel aus D adjungiert (falls nicht zufällig D ein Quadrat in K ist). Jetzt zerlegen wir $p(X)$ in Linearfaktoren über $K(x_1)$ durch gewöhnliche Polynomdivision

$$p(X) = X^2 + bX + c = (X - x_1)(X + b + x_1) = (X - x_1)(X - (-b - x_1)).$$

Der quadratische Erweiterungskörper $K(x_1) = K(\sqrt{D})$ enthält nicht nur die Wurzel

$$x_1 = \frac{-b + \sqrt{D}}{2},$$

sondern auch die zweite Wurzel

$$x_2 = -b - x_1 = \frac{-b - \sqrt{D}}{2}$$

des Polynoms $p(X)$.

Ein Polynom zweiten Grades zerfällt, wie diese Beispiele zeigen, nach der symbolischen Adjunktion einer Wurzel immer in Linearfaktoren. Bei Polynomen von höherem Grad ist dies leider meist nicht der Fall.

Beispiel 3.7 *Wir betrachten das Polynom dritten Grades*

$$p(X) = X^3 - 2 \in \mathbb{Q}[X].$$

Wir adjungieren formal eine Nullstelle $a = \sqrt[3]{2}$ *dieses Polynoms. In* $\mathbb{Q}(a)$ *dividieren wir*

$$X^3 - 2 = X^3 - a^3 = (X - a)(X^2 + aX + a^2).$$

Der quadratische Faktor hat die Diskriminante

$$D = a^2 - 4a^2 = -3a^2.$$

Falls $\mathbb{Q}(a)$ *die Wurzel der Diskriminante*

$$\sqrt{D} = a\sqrt{-3}$$

enthielte, würde die Körpererweiterung $\mathbb{Q}(a) : \mathbb{Q}$ *vom Grad drei die quadratische Erweiterung* $\mathbb{Q}(\sqrt{-3}) : \mathbb{Q}$ *enthalten. Nach der Gradformel (Satz 2.1) ist das aber nicht möglich.*

Diese symbolische Adjunktion einer Wurzel des irreduziblen Polynoms $p \in K[X]$, wo man zum Körper $K[X]/(p)$ übergeht, ist etwas anderes als die Adjunktion $K(a)$ einer Wurzel a des Polynoms p, die in einem Erweiterungskörper $L \supset K$ liegt (Abschnitt 3.1). Etwas ganz völlig anderes ist es aber doch nicht:

Satz 3.9 *Es sei* $K \subset L$ *eine Körpererweiterung, die eine Wurzel* $a \in L$ *des in* $K[X]$ *irreduziblen Polynoms* $p(X)$ *enthält. Weiter sei* $K(x_1) = K[X]/(p)$ *der Erweiterungskörper, der aus* K *durch symbolische Adjunktion einer Wurzel* x_1 *von* p *entsteht. Dann induziert* $x_1 \mapsto a$ *einen Körper-Isomorphismus*

$$K(x_1) \to K(a).$$

Beweis. Wir betrachten die beiden Ring-Homomorphismen

$$K[X] \to K(x_1),\ X \mapsto x_1, \quad K[X] \to K(a),\ X \mapsto a.$$

Nach Definition ist der erste dieser beiden surjektiv mit dem Hauptideal (p) als Kern.

Aber nach Satz 3.3 ist auch der zweite dieser Homomorphismen surjektiv und hat den Kern (p). Deswegen sind beide Körper als Ringe isomorph zum Ring $K[X]/(p)$. Damit sind sie als Ringe, und dann auch als Körper isomorph. □

Diese Situation gibt Anlass zu folgender Definition.

Definition 3.8 *Es seien $K \subset L_1$ und $K \subset L_2$ zwei Körpererweiterungen von K. Ein Körper-Isomorphismus $\varphi : L_1 \to L_2$ heißt K-Isomorphismus, wenn $\varphi(k) = k$ für alle $k \in K$. $\varphi : L_1 \to L_2$ heißt K-Homomorphismus, wenn er kein Körper-Isomorphismus sondern bloß ein Homomorphismus $L_1 \to L_2$ ist.*

Beispiel 3.8 *Es sei $c \in K$ kein Quadrat und $K(x_1)$ die Körpererweiterung von K entstanden durch symbolische Adjunktion von $\sqrt{c}$. Auch $-x_1 \in K(x_1)$ ist eine Wurzel von c. (Wenn K nicht die Charakteristik 2 hat, ist $-x_1 \neq x_1$.) Nach Satz 3.9 wird durch $x_1 \mapsto -x_1$ ein K-Isomorphismus $K(x_1) \mapsto K(x_1)$, also ein K-Automorphismus von $K(x_1)$ definiert. Man kann dies auch explizit, ohne Satz 3.9, nachrechnen:*

Die Elemente von $K(x_1)$ sind Ausdrücke $a + bx_1$, $a, b \in K$. Die Abbildung ist $a + bx_1 \mapsto a - bx_1$. Dass dies ein K-Isomorphismus ist, rechnet man sofort nach: Additivität ist klar. Zur Multiplikativität:

$$a + bx_1 \mapsto a - bx_1, \quad a' + b'x_1 \mapsto a' - b'x_1,$$

$$\begin{aligned} (a + bx_1)(a' + b'x_1) &= aa' + bb'c + (ab' + ba')x_1 \\ &\mapsto aa' + bb'c - (ab' + ba')x_1, \\ (a - bx_1)(a' - b'x_1) &= aa' + bb'c - (ab' + ba')x_1. \end{aligned}$$

Für den Fall $K = \mathbb{R}$ und $c = -1$ ist $K(\sqrt{-1}) = \mathbb{C}$ und der K-Automorphismus ist genau die komplexe Konjugation.

Beispiel 3.9 *Das Polynom $p(X) = X^3 - 2$ hat in $\mathbb{C}$ die drei Nullstellen*

$$a_1 := \sqrt[3]{2}, \quad a_2 := \frac{1}{2}(-1 + i\sqrt{3})a_1, \quad a_3 = \frac{1}{2}(-1 - i\sqrt{3})a_1.$$

Die Körper $\mathbb{R}(a_1)$ und $\mathbb{R}(a_2)$ sind als Teilkörper von $\mathbb{C}$ verschieden, aber als Erweiterungen von $\mathbb{R}$ isomorph.

Beispiel 3.10 (H 97, T3, A4) *Sei $f = X^3 - 9X + 3 \in \mathbb{Q}[X]$.*

a) Zeigen Sie, dass $K = \mathbb{Q}[X]/(f)$ ein Körper ist.

b) Bestimmen Sie die Anzahl der Körperhomomorphismen $K \to \mathbb{R}$ von K in die reellen Zahlen.

Um zu zeigen, dass K ein Körper ist, müssen wir nachweisen, dass f über $\mathbb{Q}$ irreduzibel ist. Wegen des Lemmas von Gauß (Satz 2.31) genügt es zu zeigen: $f \in \mathbb{Z}[X]$ ist irreduzibel. Das erledigt aber Eisenstein für uns mit der Primzahl 3.

Der Körper K ensteht also aus $\mathbb{Q}$ durch symbolische Adjunktion einer Nullstelle a des Polynoms f. Ist $a_1 \in \mathbb{R}$ eine reelle Nullstelle von f, so wird durch $a \mapsto a_1$ ein $\mathbb{Q}$-Isomorphismus $\mathbb{Q}(a) \to \mathbb{Q}(a_1)$ definiert, und damit ein Körper-Homomorphismus $K \to \mathbb{R}$. Jeder solcher Körperhomomorphismus wird durch $a \mapsto a_1$ induziert, wo a_1 eine reelle Nullstelle von f ist. Es kommt also darauf an, zu entscheiden, wieviele reelle Nullstellen das Polynom f hat: eine oder drei.

Dazu benützen wir Analysis. In einer Algebra-Vorlesung ist das natürlich stilwidrig und deswegen ehrenrührig. Aber: Wie ist der Körper $\mathbb{R}$ definiert? Wenn Sie die Vorlesung 'Aufbau des

Zahlsystems' hinter sich gebracht haben, dann wissen Sie, dass das analytisch geht: $\mathbb{R}$ *ist die Menge aller Grenzwerte von Cauchy-Folgen in* $\mathbb{Q}$*. Das ist analytisch. Also kann man mit* $\mathbb{R}$ *kaum anders zu Rande kommen als mit analytischen Methoden.*

Die stetige Funktion $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto f(x)$, *wächst von* $-\infty$ *nach* ∞ *und hat nach dem Zwischenwertsatz immer mindestens eine reelle Nullstelle. Sie hat zwei weitere Nullstellen, wenn sie zwei lokale Extrema besitzt, von denen das erste positiv und das zweite negativ ist. Die Ableitung*

$$f' = 3X^2 - 9$$

hat die beiden reellen Nullstellen $x_{1,2} = \pm\sqrt{3}$ *mit*

$$f(x_1) = -3\sqrt{3} + 9\sqrt{3} + 3 = 6\sqrt{3} + 3 > 0$$

und

$$f(x_2) = 3\sqrt{3} - 9\sqrt{3} + 3 = 3 - 6\sqrt{3} < 0.$$

Zwischen den beiden Extrema liegt eine reelle Nullstelle von f *und deswegen hat* f *drei verschiedene reelle Nullstellen. Deswegen gibt es drei Körperhomomorphismen* $K \to \mathbb{R}$*.*

Definition 3.9 *Es sei* $K \subset L$ *eine Körpererweiterung. Zwei über* K *algebraische Elemente* $a_1, a_2 \in L$ *heißen* über K konjugiert*, wenn es einen* K*-Isomorphismus* $K(a_1) \mapsto K(a_2)$ *gibt, der* a_1 *auf* a_2 *abbildet.*

Satz 3.10 *Die Elemente* a_1 *und* $a_2 \in L \supset K$ *sind genau dann konjugiert über* K*, wenn sie über* K *dasselbe Minimalpolynom besitzen.*

Beweis $\Rightarrow$: Es sei $p \in K[X]$ das Minimalpolynom von a_1. Weil p seine Koeffizienten in K hat, bleibt es bei dem K-Isomorphismus $K(a_1) \mapsto K(a_2)$ unverändert. Auch $p(a_1) = 0$ ändert sich nicht. Andererseits geht $p(a_1)$ in $p(a_2)$ über. Also ist auch a_2 eine Nullstelle von p. Weil p irreduzibel und normiert ist, muss es das Minimalpolynom von a_2 sein.

$\Leftarrow$: Es sei $p \in K[X]$ irreduzibel mit $p(a_1) = p(a_2) = 0$. Der Körper $K(a) = K[X]/(p)$ entstehe aus K durch symbolische Adjunktion einer Wurzel von p. Nach Satz 3.9 gibt es dann K-Isomorphismen $K(a_1) \to K(a) \to K(a_2)$. □

Ist also $f \in K[X]$ ein irreduzibles Polynom vom Grad n, so gibt es eine Körpererweiterung $K(a) = K[X]/(f)$, in der f eine Nullstelle a hat. Und alle derartigen Körpererweiterungen sind K-isomorph. Außer, wenn $n = 2$ ist, braucht f in $K(a)$ keine weiteren Nullstellen zu haben. Aber nach Vieta können wir über $K(a)$ den Linearfaktor $X - a$ aus f abdividieren:

$$f = (X - a) \cdot g, \quad g \in K(a)[X], \quad Grad(g) = n - 1.$$

Das Polynom $g \in K(a)[X]$ ist möglicherweise nicht irreduzibel:

$$g = g_1^{r_1} \cdot \ldots \cdot g_k^{r_k}, \quad g_1, \ldots, g_k \in K(a)[X] \text{ irreduzibel.}$$

Die Faktoren g_i vom Grad eins interessieren uns nicht, ihre Nullstellen liegen in $K(a)$. Aber falls g über $K(a)$ nicht in Linearfaktoren zerfällt, sei etwa $Grad(g_1) > 1$. Dann können wir eine

Nullstelle von g_1 adjungieren, und immer so weitermachen. Nach spätestens $n-1$ symbolischen Adjunktionen von Nullstellen des Polynoms f zerfällt f in dem erhaltenenen Erweiterungskörper in n Linearfaktoren.

Falls das ursprüngliche Polynom $f \in K[X]$ nicht irreduzibel gewesen sein sollte, können wir es in irreduzible Faktoren $f_i \in K[X]$ zerlegen, und das beschriebene Verfahren für jeden dieser Faktoren durchführen. Damit haben wir bewiesen:

Satz 3.11 *Sei K ein Körper und $f \in K[X]$ ein Polynom. Dann gibt es einen Erweiterungskörper $L = K(a_1, ..., a_k)$, der aus K durch symbolische Adjunktion von Wurzeln a_i des Polynoms f entsteht und in dem f vollständig in Linearfaktoren zerfällt.*

Definition 3.10 (Zerfällungskörper) *Es sei K ein Körper und $L \supset K$ eine Körpererweiterung. Dann heißt L ein Zerfällungskörper des Polynoms f, wenn*

1) f über L vollständig in Linearfaktoren zerfällt;

2) L aus K durch Adjunktion von Wurzeln des Polynoms f entsteht.

Das Polynom f kann hier durchaus über K reduzibel sein und in mehrere irreduzible Faktoren zerfallen: $f = f_1 \cdot ... \cdot f_k$, $f_i \in K[X]$. Kommt einer dieser Faktoren in f mehrfach vor, so ändert sich der Zerfällungskörper nicht, wenn wir den mehrfachen Faktor $f_i^{r_i}$ in f durch den einfachen Faktor f_i ersetzen.

Satz 3.11 sagt aus, dass ein Zerfällungskörper stets existiert. Es gibt aber auch eine Eindeutigkeitsaussage:

Satz 3.12 *Es seien $K \subset L_1$ und $K \subset L_2$ zwei Zerfällungskörper des Polynoms $f \in K[X]$. Dann gibt es einen K-Isomorphismus $L_1 \to L_2$.*

Beweis. Wenn f Nullstellen in K hat, spalten wir die zugehörigen Linearfaktoren von f ab, und beweisen die Aussage für den dadurch entstehenden Quotienten von f. Wir können also o.B.d.a. annehmen $f = f_1 \cdot ... \cdot f_k$ mit irreduziblen Polynomen $f_i \in K[X]$ vom Grad ≥ 2.

Wir adjungieren formal eine Nullstelle a von f_1 und erhalten einen Erweiterungskörper $K(a)$. Nach Voraussetzung zerfällt f und damit auch f_1 in L_1, ebenso wie in L_2 vollständig in Linearfaktoren. Es gibt also Nullstellen $a_1 \in L_1$ und $a_2 \in L_2$ von f_1. Nach Satz 3.9 induziert $a_1 \mapsto a \mapsto a_2$ einen K-Isomorphismus

$$L_1 \supset K(a_1) \simeq K(a) \simeq K(a_2) \subset L_2.$$

Vermöge dieses Isomorphismus identifizieren wir $K(a_1) = K(a_2)$. Weil f seine Koeffizienten in K hat, geht bei dieser Identifikation $f \in K(a_1)[X]$ in $f \in K(a_2)[X]$ über. Wegen $a_1 \mapsto a_2$ geht der Linearfaktor $X - a_1 \in K(a_1)[X]$ in den Linearfaktor $X - a_2 \in K(a_2)[X]$ über. Dann wird auch der Quotient

$$g_1 := f/(X - a_1) \in K(a_1)[X] \quad \text{mit} \quad g_2 := f/(X - a_2) \in K(a_2)[X]$$

identifiziert.

Wir brauchen die Behauptung jetzt nur noch für die Zerfällungskörper L_1 und L_2 des Polynoms $g = g_1 = g_2$ mit Koeffizienten in $K(a_1) = K(a_2)$ zu beweisen. Aber g hat einen kleineren Grad als f, und die Behauptung folgt durch Induktion nach diesem Grad. □

Häufig werden wir Satz 3.12 in einer Version verwenden, die nur scheinbar allgemeiner ist:

Satz 3.13 *Es seien $K_1 \subset L_1$ Zerfällungskörper des Polynoms $f_1 \in K_1[X]$ und $K_2 \subset L_2$ Zerfällungskörper des Polynoms $f_2 \in K_2[X]$. Jeder Körper-Isomorphismus $\varphi : K_1 \to K_2$, der f_1 in f_2 überführt, lässt sich fortsetzen zu einem Körper-Isomorphismus $\Phi : L_1 \to L_2$.*

Der Beweis verläuft ganz genauso wie der von Satz 3.12. Nur muss man immer Isomorphismen

$$K_1(a_1) \simeq K(a) \simeq K_2(a_2)$$

verwenden, und nicht identifizieren.

Satz 3.14 *Es sei $K \subset L$. Weiter seien L_1 und $L_2 \subset L$ zwei Zerfällungskörper desselben Polynoms $f \in K[X]$. Dann sind L_1 und L_2 nicht nur isomorph als Erweiterungskörper von K, sondern sogar gleich als Teilmengen von L.*

Beweis. Beide Körper, L_1 sowie L_2 entstehen aus K durch Adjunktion aller Nullstellen in L desselben Polynoms. □

Beispiel 3.11 *Wir betrachten $f = X^3 - 2 \in \mathbb{Q}[X]$. Adjungieren wir an $\mathbb{Q}$ die relle Zahl $\sqrt[3]{2}$, so ist $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ eine Körpererweiterung von $\mathbb{Q}$ vom Grad drei. Über diesem Körper spaltet f einen Linearfaktor ab:*

$$X^3 - 2 = (X - \sqrt[3]{2})(X^2 + \sqrt[3]{2}X + \sqrt[3]{2}^2).$$

Der quadratische Faktor hat die Diskriminante

$$D = -3 \cdot \sqrt[3]{2}^2.$$

Er zerfällt erst in der Erweiterung

$$\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}) \subset \mathbb{C}$$

vom Grad sechs. Diese Erweiterung ist der Zerfällungskörper von f. Auch wenn wir zuerst nicht $\sqrt[3]{2}$, sondern eine der beiden anderen dritten Wurzeln aus 2 adjungiert hätten, hätten wir nach dem zweiten Schritt denselben Teilkörper von $\mathbb{C}$ erhalten.

Definition 3.11 *Eine Körpererweiterung $K \subset L$ heißt* normal, *wenn sie folgende Eigenschaft besitzt: Ist $a \in L$ Nullstelle eines irreduziblen Polynoms $p \in K[X]$, so zerfällt p über L vollständig in Linearfaktoren.*

Satz 3.15 *Eine endliche Körpererweiterung $K \subset L$ ist genau dann normal, wenn L Zerfällungskörper eines Polynoms $f \in K[X]$ ist.*

Beweis $\Rightarrow$: Sei $a_1 \in L$ ein Element, das nicht zu K gehört. Nach Satz 3.2 ist a_1 algebraisch über K. Es gibt also ein irreduzibles Polynom $f_1 \in K[X]$ mit $f_1(a_1) = 0$. Nach Voraussetzung zerfällt f_1 über L in Linearfaktoren. Es gibt also einen Zwischenkörper $K \subset K_1 \subset L$, der Zerfällungskörper von f_1 ist. Wenn $K_1 = L$ ist, sind wir fertig.

Andernfalls sei $a_2 \in L$ ein Element, das nicht zu K_1 gehört. Wieder gibt es ein irreduzibles Polynom $f_2 \in K[X]$ mit Nullstelle a_2. Und wieder enthält L einen Zerfällungskörper K_2 für f_2. Er entsteht aus K durch Adjunktion endlich vieler Elemente von L. Wenn wir alle Nullstellen aus L von f_1 und vonf_2 an K adjungieren, erhalten wir einen Teilkörper von L, der Zerfällungskörper des Polynoms $f_1 \cdot f_2 \in K[X]$ ist. Diesen Schritt können wir, wenn nötig wiederholen. Bei jedem dieser Schritte wird der Körpergrad von L über dem jeweiligen Zerfällungskörper echt kleiner. Weil $[K : L]$ endlich vorausgesetzt ist, muss nach endlich vielen dieser Schritte, L mit dem erhaltenen Zerfällungskörper übereinstimmen.

$\Leftarrow$: Sei $K \subset L$ Zerfällungskörper eines Polynoms $f \in K[X]$. Dann ist $L = K(a_1, ..., a_n)$, wo $a_1, ..., a_n \in L$ die Nullstellen von f sind.

Sei nun $c \in L$ Nullstelle eines irreduziblen Polynoms $p \in K[X]$. Dieses Polynom p spaltet über L den Linearfaktor $X - c$ ab. Falls p über L in Linearfaktoren zerfällt, sind wir fertig. Andernfalls enthält p einen irreduziblen Faktor $p_1 \in L[X]$ vom Grad ≥ 2. Der Erweiterungskörper $L(c_1)$ entstehe aus L durch symbolische Adjunktion einer Nullstelle von p_1.

Sowohl c als auch $c_1 \in L(c_1)$ sind Nullstellen des irreduziblen Polynoms $p \in K[X]$. Nach Satz 3.9 sind die Körper $K(c)$ und $K(c_1)$ K-isomorph (nicht gleich als Teilmengen von $L(c_1)$). Bei diesem K-Isomorphismus geht das Polynom $f \in K[X]$ in sich selbst über.

Der Körper L entsteht aus K, und dann auch aus $K(c)$, durch Adjunktion aller Nullstellen des Polynoms $f \in K[X] \subset K(c)[X]$. Er ist ein Zerfällungskörper von f über $K(c)$.

Wegen

$$L(c_1) = K(a_1, ..., a_n, c_1) = K(c_1)(a_1, ..., a_n)$$

entsteht auch $L(c_1)$ aus $K(c_1)$ durch Adjunktion aller Nullstellen von $f \in K(c_1)[X]$. Er ist ein Zerfällungskörper von f über $K(c_1)$.

Weil der K-Isomorphismus $K(c) \to K(c_1)$ das Polynom f in sich überführt, lässt er sich fortsetzen zu einem K-Isomorphismus der Zerfällungskörper (Satz 3.13). Insbesondere folgt daraus

$$[L(c_1) : K] = [L : K].$$

Wegen $L \subset L(c_1)$ folgt daraus $L = L(c_1)$. Die Wurzel c_1 von p_1 muss schon in L gelegen sein.

So sieht man, dass alle Nullstellen von p schon in L liegen. □

Satz 3.16 (Normale Körpererweiterungen) *a) Es seien $K \subset L \subset N$ endliche Körpererweiterungen. Wenn N normal über K ist, dann auch über L.*

b) Es sei $K \subset L$ eine endliche Körpererweiterung. Dann gibt es eine endliche Körpererweiterung $L \subset N$ derart, dass N über K normal ist.

c) Unter allen Körpererweiterungen $L \subset N$ wie in b) gibt es eine kleinste $L \subset N_0$. D.h.: Zu jeder Erweiterung $L \subset N$ wie in b) gibt es einen L-Isomorphismus von N_0 auf einen Teilkörper von N. Insbesondere ist N_0 selbst bis auf L-Isomorphie eindeutig bestimmt.

Beweis. a) Es sei $c \in N$ algebraisch über L und $p \in L[X]$ sein Minimalpolynom über L. Weil N auch über K endlich ist, ist c auch über K algebraisch und hat über K ein Minimalpolynom $f \in K[X]$. Dieses Polynom f zerfällt über L in irreduzible Faktoren: $f = p_1^{r_1} \cdot ... \cdot p_k^{r_k}$, $p_i \in L[X]$. Wegen $f(c) = 0$ gilt $p_i(c) = 0$ für ein $i = 1, ..., k$. Wir können o.B.d.A. das Polynom p_i normiert annehmen. Weil es irreduzibel mit $p_i(c) = 0$ ist, stimmt es mit p überein. Nun zerfällt f nach Voraussetzung über N in Linearfaktoren. Aus der Eindeutigkeit der Zerlegung in irreduzible Faktoren (Satz 2.33) folgt, dass auch $p_1 = p$ über N in Linearfaktoren zerfällt.

b) Weil L über K endlich ist, gibt es endlich viele Elemente $a_1, ..., a_n \in L$ mit $L = K(a_1, ..., a_n)$. Die Minimalpolynome von $a_1, ..., a_n$ über K seien $f_1, ..., f_n \in K[X]$. Wir definieren $N \supset L$ als Zerfällungskörper von $f := f_1 \cdot ... \cdot f_n$ über L. Weil $f \in K[X]$ über N in Linearfaktoren zerfällt, enthält N einen Zerfällungskörper N' von f über K. Dieser Zerfällungskörper enthält die Nullstellen $a_1, ..., a_n \in N$ von f. Dann enthält er auch $L = K(a_1, ..., a_n)$. Und dann ist N' auch Zerfällungskörper über L. Aus Satz 3.14 folgt $N' = N$. Deswegen ist N normal über K und wir sind fertig.

c) Es sei $L \subset N_0$ die in b) konstruierte Körpererweiterung. Sie ist aus L entstanden durch symbolische Adjunktion aller Nullstellen $b_1, ..., b_m$ von endlich vielen irreduziblen Polynome $f_1, ..., f_n \in K[X]$, die in L eine Nullstelle haben, also $N_0 = L(b_1, ..., b_m)$.

Sei nun $L \subset N$ eine Körpererweiterung, die über K normal ist. Weil jedes Polynom f_i eine Nullstelle in $L \subset N$ hat, zerfällt es über N in Linearfaktoren. Deswegen enthält N einen Teilkörper $L(b'_1, ..., b'_m) \subset N$, der aus L entsteht durch Adjunktion der Nullstellen derselben Polynome, wie bei der Konstruktion von N_0. Es folgt

$$N_0 = L(b_1, ..., b_m) \simeq L(b'_1, ..., b'_m) \subset N.$$

□

Definition 3.12 *Die in Satz 3.16c) konstruierte, über K normale Körpererweiterung $K \subset L \subset N_0$ heißt* normale Hülle *von L über K.*

Aufgabe 3.18 *Es seien K ein Körper, $p_1, p_2 \in K[X]$ irreduzible Polynome, nicht zueinander assoziiert, und $f = p_1 \cdot p_2$. Zeigen sie: Der Faktorring $K[X]/(f)$ ist isomorph zum Produkt der Körper $K[X]/(p_1)$ und $K[X]/(p_2)$.*

Aufgabe 3.19 (H 97, T1, A3) *Sei $f = X^4 + aX + 2 \in \mathbb{Z}[X]$. Beweisen Sie: Der Restklassenring $\mathbb{Q}[X]/(f)$ ist, abhängig von a, entweder ein Körper oder isomorph zu einem direkten Produkt $K_1 \times K_2$ von zwei Körpern, die die Grade 1 bzw. 3 über $\mathbb{Q}$ haben. Für welche a treten die jeweiligen Fälle ein?*

Aufgabe 3.20 (H 93, T3, A3a)b)) *Im Polynomring $\mathbb{Q}[X]$ sei f das Polynom*

$$f(X) := X^4 + 3.$$

a) Man zeige: f ist irreduzibel.

b) Man bestimme den Zerfällungskörper K von f als Unterkörper des Körpers der komplexen Zahlen $\mathbb{C}$, bestimme seinen Grad und gebe eine Basis von K über $\mathbb{Q}$ an.

3.4 Separable Körpererweiterungen

Definition 3.13 *Es sei $K \subset L$ eine Körpererweiterung. Ein K-Automorphismus von L ist ein K-Isomorphismus $L \to L$. Es ist klar, dass die K-Automorphismen $L \to L$ eine Gruppe bilden. Wir nennen sie $G(L:K)$.*

Wir interessieren uns hier für K-Automorphismen, die wie folgt entstehen: Es sei $f \in K[X]$ ein Polynom und $K \subset L$ ein Zerfällungskörper von f. Es sei $c \in L, c \notin K$, eine der Nullstellen von f. Es gibt also einen über K irreduziblen Faktor f_1 von f vom Grad > 1 mit $f_1(c) = 0$. Er zerfällt über L in Linearfaktoren und hat noch eine Nullstelle $c' \neq c$. Die Teilkörper $K(c)$ und $K(c')$ sind K-isomorph (Satz 3.9). Es gibt einen K-Isomorphismus $\varphi : K(c) \to K(c')$ mit $\varphi(c) = c'$. Bei diesem Isomorphismus wird

$$f \mapsto f, \quad g := \frac{f}{X-c} \mapsto \frac{f}{X-c'} =: g'$$

abgebildet. Weil L ein Zerfällungskörper von f über K ist, ist L auch ein Zerfällungskörper von g über $K(c)$. Ebenso ist L ein Zerfällungskörper von g' über $K(c')$. Nach Satz 3.13 gibt es einen Körper-Isomorphismus $\Phi : L \to L$, der φ fortsetzt. Dies ist ein K-Automorphismus $L \to L$ mit $\Phi(c) = c'$.

Beispiel 3.12 *Es sei $K = \mathbb{Q}$ und $L = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ der schon oft bemühte Zerfällungskörper des Polynoms $X^3 - 2$ über $\mathbb{Q}$. Zur Abkürzung bezeichnen wir die nicht-trivialen dritten Einheitswurzeln in L mit*

$$\omega := \frac{1}{2}(-1 + i\sqrt{3}), \quad \omega^2 = \frac{1}{2}(-1 - i\sqrt{3}).$$

Die drei Wurzeln in L des über $\mathbb{Q}$ irreduziblen Polynoms $X^3 - 2$ sind dann

$$\sqrt[3]{2}, \quad \omega \cdot \sqrt[3]{2}, \quad \omega^2 \cdot \sqrt[3]{2}.$$

Jeder $\mathbb{Q}$-Automorphismus $\varphi : L \to L$ permutiert diese drei Wurzeln. Umgekehrt ist φ durch diese Permutation der drei Wurzeln festgelegt. Eine Körperbasis von L über $\mathbb{Q}$ bilden nämlich die sechs Zahlen

$$1,\ \sqrt[3]{2},\ \sqrt[3]{4},\ \omega,\ \omega\sqrt[3]{2},\ \omega\sqrt[3]{4}.$$

Natürlich ist $\varphi(1) = 1$. Die Permutation der drei Wurzeln von $X^3 - 2$ legt dann die Bilder $\varphi(\sqrt[3]{2})$ und $\varphi(\omega \cdot \sqrt[3]{2})$ fest. Dadurch ist auch

$$\varphi(\sqrt[3]{4}) = \varphi(\sqrt[3]{2})^2$$

bestimmt, sowie

$$\varphi(\omega) = \varphi\left(\frac{\omega \cdot \sqrt[3]{2}}{\sqrt[3]{2}}\right),$$

und dadurch schließlich $\varphi(\omega \cdot \sqrt[3]{4})$.

Die Gruppe $G(L:\mathbb{Q})$ ist also eine Untergruppe der symmetrischen Gruppe S_3, welche die drei Wurzeln von X^3-2 permutiert. Nach Satz 3.10 und Satz 3.13 operiert $G(L:\mathbb{Q})$ transitiv auf diesen drei Wurzeln. Die Gruppe hat also mindestens die Ordnung 3. Nun enthält $G(L:\mathbb{Q})$ aber auch die Konjugation $\sqrt{-3} \mapsto -\sqrt{-3}$ der quadratischen Erweiterung $\mathbb{Q}(\sqrt[3]{2})(\sqrt{-3}) \supset \mathbb{Q}(\sqrt[3]{2})$. Also hat $G(L:\mathbb{Q})$ die Ordnung sechs und stimmt mit der vollen Permutationsgruppe der drei Wurzeln von X^3-2 überein.

Satz 3.17 *Es sei $K \subset L$ Zerfällungskörper eines Polynoms $f \in K[X]$. Wir nehmen an, dass f keinen mehrfachen irreduziblen Faktor enthält. Dann hat die Gruppe $G(L:K)$ der K-Automorphismen von L eine Ordnung*

$$|G(L:K)| \leq [L:K].$$

Genau dann ist $|G(L:K)| = [L:K]$, wenn f in L keine mehrfachen Nullstellen besitzt.

Der Beweis geht über Induktion nach $[L:K]$. Dabei brauchen wir allerdings eine allgemeinere Aussage.

Satz 3.18 *Es sei $f \in K[X]$ ein Polynom ohne mehrfachen irreduziblen Faktor. Weiter sei $\varphi : K \to K'$ ein Körper-Isomorphismus, bei dem $f \in K[X]$ in $f' \in K'[X]$ übergeht. Außerdem seien $K \subset L$ und $K' \subset L'$ Zerfällungskörper von f, bzw. f'. Nach Satz 3.13 gibt es Körperisomorphismen $\Phi : L \to L'$, die φ fortsetzen. Deren Anzahl ist immer $\leq [L:K] = [L':K']$. Die Anzahl ist genau dann gleich diesem Körpergrad, wenn f in L (und dann auch f' in L') keine mehrfachen Nullstellen besitzt.*

Beweis (Induktion nach $[L:K]$). Es sei $c \in L$ Nullstelle eines irreduziblen Faktors $f_1 \in K[X]$ von f. Das Bild von f_1 unter $\varphi : K \to K'$ sei $f_1' \in K'[X]$. Ist $c' \in L'$ eine Nullstelle von f_1', so gibt es nach Satz 3.9 einen K-Isomorphismus $\varphi_1 : K(c) \to K'(c') \subset L'$ mit $\varphi_1(c) = c'$. Jeder Köperhomomorphismus $\varphi_1 : K(c) \to L'$, der φ fortsetzt, bildet c auf eine Nullstelle von f_1' ab und ist durch diese Nullstelle eindeutig bestimmt. Die Anzahl der Nullstellen von f_1' in L', und damit die Anzahl der Homomorphismen $\varphi_1 : K(c) \to L'$, die φ fortsetzen, ist

$$\leq [K(c'):K] = Grad(f_1') = Grad(f_1) = [K(c):K].$$

Und sie ist genau dann gleich diesem Körpergrad, wenn f_1' in L' lauter verschiedene Nullstellen besitzt.

Nach Induktionsannahme gibt es zu jedem $\varphi_1 : K(c) \to L'$ Fortsetzungen $\Phi_1 : L \to L'$. Deren Anzahl ist $\leq [L':K(c')] = [L:K(c)]$. Und sie ist nach Induktionsannahme genau dann gleich diesem Körpergrad, wenn $g := f/(X-c) \in K(c)[X]$ und dann auch $g' = f'/(X-c') \in K'(c')[X]$ keine mehrfachen Nullstellen hat. Die Anzahl aller Fortsetzungen Φ von φ ist

$$\#\Phi = (\#\varphi_1) \cdot (\#\Phi_1) \leq [K(c):K] \cdot [L:K(c)] = [L:K].$$

Und genau dann ist ihre Anzahl $= [L:K]$, wenn f_1 und $f/(X-c)$ in L keine mehrfachen Nullstellen haben. Das ist aber äquivalent dazu, dass f in L keine mehrfachen Nullstellen besitzt. □

Nun ist es für ein irreduzibles Polynom $f \in K[X]$ ziemlich schwer, in einer Erweiterung von K mehrfache Nullstellen zu haben. Seien etwa f_1 und f_2 zwei verschiedene irreduzible Faktoren von f. (D.h., f_1 und f_2 sollen sich nicht nur um einen Faktor aus K^* unterscheiden.) Sei $K \subset L$ eine Erweiterung, in der f einen mehrfachen Linearfaktor $X - c$ abspaltet, weil sowohl f_1 als auch f_2 ihn abspalten. Die Polynome f_1 und f_2 haben einen gemeinsamen Faktor über L. Ihre Resultante $Res(f_1, f_2) = 0$ verschwindet, wenn man sie über dem Körper L ausrechnet. Die Sylvestersche Formel für die Resultante in 2.6.2 zeigt aber, dass dies genau dieselbe Resultante ist, wie wenn man sie über K ausrechnet. Die Polynome f_1 und f_2 haben einen gemeinsamen Faktor in $K[X]$. Dann können sie nicht irreduzibel und verschieden gewesen sein.

Das Polynom $f \in K[X]$ kann also nur dann mehrfache Nullstellen in einer Erweiterung $L \supset K$ haben, wenn entweder f selbst mehrfache Faktoren aus $K[X]$ besitzt, oder wenn ein irreduzibler Faktor von f in L mehrfache Nullstellen hat. Untersuchen wir diesen Fall weiter.

Es sei $f \in K[X]$ irreduzibel und habe in einer Erweiterung $L \supset K$ einen mehrfachen Linearfaktor $X - c$. Über L ist dann

$$f(X) = (X - c)^2 \cdot g(X), \quad g \in L[X].$$

Für die Ableitung $f' \in K[X]$ folgt daraus

$$f'(x) = 2(X - c) \cdot g(X) + (X - c)^2 \cdot g'(x) = (X - c) \cdot h(X), \quad h \in L[X].$$

Die Polynome f und f' haben in $L[X]$ einen nichtkonstanten gemeinsamen Faktor. Es ist $Res(f, f') = 0$ über L, und was dasselbe ist, über K. Also haben f und f' einen gemeinsamen Faktor in $K[X]$. Weil f irreduzibel ist, muss dieser Faktor $= f$ sein. Und wegen $Grad(f') < Grad(f)$ geht das nur, wenn f' das Null-Polynom ist.

Nun sei etwa $f(X) = a_n X^n + ...$ mit $n \geq 1$ und $a_n \neq 0$. Dann ist

$$f'(X) = n a_n X^{n-1} + ... \neq 0,$$

falls $n a_n \neq 0$. Wenn f' das Null-Polynom sein sollte, muss also $n = 0$ in K sein. In Charakteristik 0 geht das nicht. Aber wenn die Charakteristik von K eine Primzahl p ist, dann geht das leider schon, nämlich, wenn n durch p teilbar ist.

Definition 3.14 *Es sei $K \subset L$ eine Körpererweiterung. Ein über K algebraisches Element $c \in L$ heißt* separabel, *wenn es eine einfache Nullstelle seines Minimalpolynoms $p \in K[X]$ ist. Ein Polynom $p \in K[X]$ heißt* separabel, *wenn es in seinem Zerfällungskörper keine mehrfachen Nullstellen hat. Eine algebraische Körpererweiterung $K \subset L$ heißt* separabel, *wenn jedes Element $c \in L$ über K separabel ist.*

Wir müssen uns natürlich um Strukturaussagen über separable Körpererweiterungen kümmern. Das wollen wir aber erst tun, nachdem ich die Standardbeispiele separabler und inseparabler Körpererweiterungen besprochen habe.

Eben haben wir bewiesen:

Satz 3.19 *Es sei K ein Körper der Charakteristik 0. Dann ist jedes irreduzible Polynom $p \in K[X]$, und damit auch jede algebraische Körpererweiterung von K separabel.*

Schauen wir uns also jetzt den Fall an, wo der Körper K eine Charakteristik $p > 0$ hat. Wie kann es passieren, dass ein irreduzibles Polynom

$$f = a_n X^n + a_{n-1} X^{n-1} + ... + a_1 X + a_0 \ \in K[X]$$

nicht separabel ist? Dann muss also seine Ableitung

$$f' = n a_n X^{n-1} + (n-1) a_{n-1} X^{n-2} + ... + a_1$$

das Nullpolynom sein. Falls der Koeffizient a_k von f nicht $= 0$ war, muss also $k \cdot a_k = 0$ sein. Das heißt, der Exponent k ist dann durch p teilbar. Das Polynom f muss so aussehen:

$$f = b_m (X^p)^m + b_{m-1} (X^p)^{m-1} + ... + b_1 X^p + b_0.$$

Alle Potenzen von X, die wirklich vorkommen, sind Potenzen von X^p.

In Charakteristik p gibt es aber einen ganz komischen Effekt:

Satz 3.20 *Es sei K ein Körper der Charakteristik $p > 1$. Dann ist die Abbildung*

$$F : K \to K, \quad c \mapsto c^p,$$

ein Körperhomomorphismus.

Beweis. Wegen $(c_1 c_2)^p = c_1^p \cdot c_2^p$ ist die Abbildung F multiplikativ. Aber sie ist auch addititv: Aus der binomischen Formel

$$(c_1 + c_2)^p = c_1^p + p c_1^{p-1} c_2 + \binom{p}{2} c_1^{p-2} c_2^2 + ... + \binom{p}{p-2} c_1^2 c_2^{p-2} + p c_1 c_2^{p-1} + c_2^p$$

folgt wegen

$$p \Big| \binom{p}{\nu} \text{ für } \nu = 1, ..., p-1 \quad \text{(s. Abschnitt 2.5)}$$

dass

$$F(c_1 + c_2) = (c_1 + c_2)^p = c_1^p + c_2^p = F(c_1) + F(c_2)$$

ist. □

Definition 3.15 *Es sei K ein Körper der Charakteristik p. Der Körper-Homomorphismus*

$$F : K \to K, \quad F(c) = c^p,$$

heißt Frobenius-Homomorphismus.

Der Frobenius-Homomorphismus F ist immer injektiv: Aus $c^p = 0$ folgt $c = 0$. Wenn der Körper K endlich ist, ist F also auch immer surjektiv und deswegen ein Isomorphismus. Die Surjektivität von F kann man auch so formulieren:

Satz 3.21 *Es sei K ein endlicher Körper der Charakteristik $p > 1$. Dann gibt es zu jedem Körperelement $c \in K$ genau eine p-te Wurzel, d.h., ein Element $a \in K$ mit $a^p = c$.*

Schauen wir uns in diesem Fall das Polynom

$$f = b_m(X^p)^m + b_{m-1}(X^p)^{m-1} + ... + b_1X^p + b_0$$

mit $f' = 0$ noch einmal an. Für $\mu = 0, ..., m$ ist $b_\mu = a_\mu^p$, und daraus folgt

$$\begin{aligned} f &= (a_mX^m)^p + (a_{m-1}X^{m-1})^p + ... + (a_1X)^p + a_0^p \\ &= (a_mX^m + a_{m-1}X^{m-1} + ... + a_1X + a_0)^p. \end{aligned}$$

Das Polynom f war also nicht irreduzibel, sondern hochgradig reduzibel. Wir haben bewiesen:

Satz 3.22 *Es sei K ein endlicher Körper. Dann ist jedes irreduzible Polynom $f \in K[X]$, und damit auch jede algebraische Körpererweiterung von K separabel.*

Eine inseparable Körpererweiterung muss also eine Körpererweiterung eines unendlichen Körpers der Charakteristik $p > 0$ sein. Solche gibt es eben leider doch:

Beispiel 3.13 *Es sei $\mathbb{F}_p$ der Primkörper der Charakteristik p und K der Körper $\mathbb{F}_p(X)$ der rationalen Funktionen in einer Unbestimmten über $\mathbb{F}_p$. Das ist ein unendlicher Körper der Charakteristik p. Die einfachsten inseparablen Polynome in*

$$K[Z] = \mathbb{F}_p(X)[Z]$$

sind von der Form

$$Z^p - f, \quad f \in \mathbb{F}_p(X).$$

Satz 3.23 *Es sei K ein Körper der Charakteristik $p > 1$ und $f \in K$. Das Polynom*

$$Z^p - f \in K[Z]$$

$$\textit{ist} \quad \begin{array}{ll} \textit{irreduzibel,} & \textit{wenn } f \in K \textit{ keine } p\textit{-te Potenz} \\ \textit{reduzibel} = (Z-g)^p, & \textit{wenn } f = g^p \in K \textit{ eine } p\textit{-te Potenz} \end{array} \quad \textit{ist.}$$

Beweis. Es sei $Z^p - f$ reduzibel in $K[Z]$. Dann gibt es also Polynome $P(Z), Q(Z) \in K[Z]$ mit $P(Z) \cdot Q(Z) = Z^p - f$. Wir betrachten einen Zerfällungskörper $K \subset L$ für das Polynom $Z^p - f$. Dort gibt es eine Nullstelle dieses Polynoms, also ein Element $g \in L$ mit $g^p = f$. Über L gilt

$$Z^p - f = Z^p - g^p = (Z - g)^p.$$

Aber über L gilt genauso wie über K

$$Z^p - f = P(Z) \cdot Q(Z).$$

Weil $K[Z]$ ein faktorieller Ring ist, folgt daraus

$$P(Z) = (Z-g)^k, \quad Q(Z) = (Z-g)^l, \quad k + l = p.$$

Insbesondere gehört $P(0) = g^k$ zu K.

Weil p eine Primzahl ist, ist $ggT(p,k) = 1$ und nach Satz 2.16 gibt es ganze Zahlen π und κ mit

$$p \cdot \pi + k \cdot \kappa = 1.$$

Daraus folgt

$$g = g^{p\cdot\pi+k\cdot\kappa} = (g^p)^\pi \cdot (g^k)^\kappa = f^\pi \cdot (g^k)^\kappa \in K.$$

Also ist $f = g^p$ mit $g \in K$. □

Jetzt sei wieder $K = \mathbb{F}_p(X)$. Das Element $X \in \mathbb{F}_p(X)$ kann keine p-te Potenz f^p, $f \in \mathbb{F}_p(X)$, sein. Denn, wenn

$$f(X) = \frac{a_0 + a_1X + ...}{b_0 + b_1X + ...},$$

dann ist

$$f^p(X) = \frac{(a_0 + a_1X + ...)^p}{(b_0 + b_1X + ...)^p} = \frac{a_0^p + a_1^pX^p + ...}{b_0^p + b_1^pX^p + ...} \in \mathbb{F}_p(X^p),$$

und X gehört nicht zum Körper $\mathbb{F}_p(X^p)$. Das inseparable Polynom

$$Z^p - X \in K[Z] = \mathbb{F}_p(X)[Z]$$

ist nach Satz 3.23 irreduzibel über K. Dann ist also

$$K(\sqrt[p]{X}) = \mathbb{F}_p(X)[Z]/(Z^p - X)$$

eine inseparable Erweiterung von K. In dieser Erweiterung hat

$$Z^p - X = (Z - \sqrt[p]{X})^p$$

nur eine einzige Nullstelle $\sqrt[p]{X}$. Diese Körpererweiterung ist das Standardbeispiel für eine inseparable Körpererweiterung.

Jetzt kommen die Strukturaussagen über separable Körpererweiterungen.

Satz 3.24 (Separable Körperelemente) *Es sei $K \subset L$ eine Körpererweiterung und $c \in L$ algebraisch über K. Dann sind äquivalent:*

a) c ist separabel über K;

b) jedes Konjugierte c' in einem über K normalen Erweiterungskörper von L ist separabel über K;

c) das Minimalpolynom $p \in K[X]$ von c über K ist separabel;

d) Ist $L \subset N$ eine über K normale Erweiterung von L, so ist die Anzahl der K-Homomorphismen $K(c) \to N$ gleich dem Körpergrad $[K(c) : K]$.

Beweis. a) ⇒ b): Nach Satz 3.9 gibt es einen K-Isomorphismus $K(c) \to K(c')$, $c \mapsto c'$. Ist c separabel über K, so spaltet das Minimalpolynom $p \in K[X]$ von c über K den Linearfaktor $X - c$ nur einfach ab. p ist auch das Minimalpolynom von c' über K. Weil bei dem K-Isomorphismus $K(c) \to K(c')$ die Polynome $p \mapsto p$, $X - c \mapsto X - c'$ abgebildet werden, spaltet p über $K(c')$ den Linearfaktor $X - c'$ nur einmal ab.

b) $\Rightarrow$ c): Jede Nullstelle c' von p in seinem Zerfällungskörper ist nach b) eine einfache Nullstelle. Deswegen zerfällt p über seinem Zerfällungskörper nur in einfache Linearfaktoren.

c) $\Rightarrow$ d): Das Minimalpolynom p von c über K zerfällt über N in Linearfaktoren. Diese sind nach c) alle einfach. Ihre Anzahl ist deswegen $= Grad(p) = [K(c) : K]$. Soviele verschiedene Nullstellen c' hat dann auch p in N. Jeder K-Homomorphismus $K(c) \to N$ ist durch eine Abbildung $c \mapsto c'$ auf eine dieser Nullstellen definiert. Die Anzahl der K-Homomorphismen $K(c) \to N$ ist deswegen gleich der Anzahl dieser Nullstellen, und damit $= [K(c) : K]$.

d) $\Rightarrow$ a): Ist die Anzahl der K-Homomorphismen $K(c) \to N$ gleich dem Körpergrad $[K(c) : K]$, so hat das Minimalpolynom p von c über K soviele Nullstellen, wie sein Grad angibt. Alle diese Nullstellen, und damit auch die Nullstelle c müssen einfach sein. $\square$

Satz 3.25 (Separable Körpererweiterungen) *a) Es seien $K \subset L \subset M$ Körpererweiterungen. Ist M separabel über K, dann auch über L.*

b) Es seien $K \subset L \subset N$ Körpererweiterungen, wobei L über K endlich und N über K normal ist. Dann sind äquivalent:

i) L ist separabel über K;

ii) die Anzahl der K-Homomorphismen $L \to N$ ist gleich dem Körpergrad $[L : K]$;

iii) die Anzahl der K-Homomorphismen $L \to N$ ist $\geq$ dem Körpergrad $[L : K]$.

Beweis. a) Es sei $c \in M$ mit Minimalpolynom $f \in K[X]$ über K. Weil c über K separabel ist, spaltet f über einer über K normalen Erweiterung N von L in lauter verschiedene Linearfaktoren. Das Minimalpolynom p von c über L ist ein irreduzibler Faktor von f. Wegen der Eindeutigkeit der Zerlegung von $f \in N[X]$ in irreduzible Faktoren zerfällt auch $p \in N[X]$ in lauter verschiedene Linearfaktoren.

b) i) $\Rightarrow$ ii) Nach Voraussetzung ist $L = K(c_1, ..., c_n)$, wo alle c_i über K algebraisch sind. Wir beweisen die Aussage durch Induktion nach n. Der Induktionsanfang ($n = 1$) ist gerade Satz 3.24, Aussage d). Sei also jetzt $K(c_1, ..., c_n, c_{n+1})$ separabel über K und N eine über K normale Erweiterung von $K(c_1, ..., c_{n+1})$. Dann ist auch $K(c_1, ..., c_n)$ separabel über K und nach Induktionsannahme ist die Anzahl der K-Homomorphismen $\varphi : K(c_1, ..., c_n) \to N$ gleich dem Körpergrad $[K(c_1, ..., c_n) : K]$.

Jeder K-Homomorphismus $\Phi : K(c_1, ..., c_n, c_{n+1}) \to N$ definiert einen K-Homomorphismus $\varphi : K(c_1, ..., c_n) \to K(c'_1, ..., c'_n) \subset N$. Dabei ist Φ durch φ und das Bild $\Phi(c_{n+1})$ festgelegt. Es sei $p \in K(c_1, ..., c_n)[X]$ das Minimalpolynom von c_{n+1} und p' das Bild von p unter φ. Das Bild $\Phi(c_{n+1})$ ist eine Nullstelle von p' und umgekehrt: zu jeder Nullstelle $c'_{n+1} \in N$ von p' gibt es eine Fortsetzung Φ von φ mit $\Phi(c_{n+1}) = c'_{n+1}$. Die Behauptung folgt aus der Gradformel, wenn wir zeigen, dass p' über N in lauter verschiedene Linearfaktoren zerfällt. Denn dann ist die Anzahl der Nullstellen von p' der Grad

$$Grad(p') = Grad(p) = [K(c_1, ..., c_n)(c_{n+1}) : K(c_1, ..., c_n)],$$

und die Anzahl der K-Homomorphismen Φ ist

$$\#\Phi = (\#\varphi) \cdot Grad(p') = [K(c_1, ..., c_n) : K] \cdot [K(c_1, ..., c_{n+1}) : K(c_1, ..., c_n)] = [K(c_1, ..., c_{n+1}) : K].$$

Sei nun $f \in K[X]$ das Minimalpolynom von c_{n+1} über K. Weil c_{n+1} separabel über K ist, zerfällt f über N in lauter einfache Linearfaktoren. Weil $f \in K[X]$ unter φ in sich übergeht,

ist auch c'_{n+1} eine Nullstelle von f. Das Minimalpolynom p' von c'_{n+1} über $K(c'_1, ..., c'_n)$ ist über diesem Körper ein irreduzibler Faktor von f. Dann zerfällt auch p' über N in lauter einfache Linearfaktoren.

Die Aussage ii) $\rightarrow$ iii) ist trivial.

iii) $\Rightarrow$ i): Jetzt ist $K \subset L$ eine Körpererweiterung, bei der die Anzahl der K-Homomorphismen $\Phi : L \rightarrow N$ mindestens gleich dem Körpergrad $[L : K]$ ist. Wir beweisen, dass L über K separabel ist durch Induktion nach diesem Körpergrad. Sei dazu $c \in L$ algebraisch über K. Jeder K-Homomorphismus $\Phi : L \rightarrow N$ definiert einen K-Homomorphismus $\varphi : K(c) \rightarrow K(c') \subset N$ mit $\varphi(c) = c'$. Die Anzahl dieser K-Homomorphismen φ ist gleich der Anzahl der Konjugierten $c' \in N$ von c. Damit ist sie $\leq$ dem Körpergrad $[K(c) : K]$, und wenn sie gleich diesem Körpergrad ist, dann ist c über K separabel.

Weil L auch über $K(c)$ endlich ist, ist $L = K(c)(c_1, ..., c_n)$ eine Folge einfacher algebraischer Körpererweiterungen von $K(c)$. Nach Satz 3.13 kann man φ sukzessive auf jede dieser Erweiterungen fortsetzen zu einem K-Homomorphismus

$$\Phi : L = K(c)(c_1, ..., c_n) \rightarrow K(c')(c'_1, ..., c'_n) =: L' \subset N.$$

Die Anzahl dieser Forsetzungen ist gleich der Anzahl der $K(c')$-Homomorphismen $L' \rightarrow N$. Ist diese Anzahl $\geq$ dem Körpergrad $[L' : K(c')] = [L : K(c)]$, so ist L' über $K(c')$ nach Induktionsannahme separabel, und wegen der schon bewiesenen Richtung i) $\Rightarrow$ ii) ist die Anzahl dann genau gleich diesem Körpergrad. Damit ist die Anzahl der K-Homomorphismen $\Phi : L \rightarrow N$

$$= (\#\varphi) \cdot (\#\text{ Fortsetzungen}) \leq [K(c) : K] \cdot [L : K(c)] = [L : K].$$

Weil diese Zahl aber nach Voraussetzung

$$\geq [L : K] = [K(c) : K] \cdot [L : K(c)]$$

ist, muss die Anzahl der K-Homomorphismen $\varphi : K(c) \rightarrow N$ gerade gleich dem Körpergrad $[K(c) : K]$ sein, und c war separabel über K. □

Aus Satz 3.25 b) ergeben sich eine Reihe von Folgerungen:

Satz 3.26 *a) Es sei $L = K(c_1, ..., c_n)$ eine endliche Körpererweiterung, so dass für $i = 1, ..., n$ das Element c_i separabel über $K(c_1, ..., c_{i-1})$ ist. Dann ist L separabel über K.*

b) (Transitivität) Es seien $K \subset L \subset M$ Körpererweiterungen, M algebraisch über K. Sind L über K und M über L separabel, dann ist auch M über K separabel.

c) Ist $f \in K[X]$ separabel, dann ist auch der Zerfällungskörper von f über K separabel.

d) Ist die endliche Körpererweiterung $K \subset L$ separabel, dann ist auch die normale Hülle N von L über K separabel.

e) Ist $K \subset L$ eine Körpererweiterung, so bilden alle über K separablen Elemente aus L einen Zwischenkörper $K \subset L_s \subset L$.

Beweis. a) (Induktion nach n): Der Induktionsanfang ($n = 1$) folgt aus den Sätzen 3.24 und 3.25. Sei also jetzt $L = K(c_1, ..., c_n)$ separabel über K und $L' = L(c_{n+1})$ separabel über L. Es sei N eine über K normale Erweiterung von L'. Nach Satz 3.25 b) ist die Anzahl der

K-Homomorphismen $L \to N$ gleich dem Körpergrad $[L : K]$. Weil L' über L separabel ist, ist die Anzahl der L-Homomorphismen $L' \to N$ gleich dem Körpergrad $[L' : L]$. Daraus folgt, dass die Anzahl der K-Homomorphismen $L' \to N$

$$= [L : K] \cdot [L' : L] = [L' : K]$$

ist. Nach Satz 3.25 b) ist L separabel über K.

b) Es sei $c \in M$ und $p \in L[X]$ sein Minimalpolynom. Es sei $L' \subset L$ der Unterkörper, der aus K durch Adjunktion der endlich vielen, über K algebraischen Koeffizienten von p entsteht. Dann ist L' eine endliche Körpererweiterung, $L' = K(c_1, ..., c_n)$, von K so, dass jedes c_i über K und dann auch über $K(c_1, ..., c_{i-1})$ separabel ist. Das Element c ist separabel über $L' = K(c_1, ..., c_n)$. Nach a) ist $K(c_1, ..., c_n, c)$ separabel über K. Also ist $c \in M$ separabel über K.

c) Der Zerfällungskörper von f entsteht aus K durch Adjunktion endlich vieler Nullstellen $c_1, ..., c_n$. Weil f separabel über K ist, ist jede dieser Nullstellen einfach. Damit sind $c_1, ..., c_n$ separabel über K. Nach Satz 3.25 a) ist c_i separabel über $K(c_1, ..., c_{i-1})$. Nach a) ist dann $K(c_1, ..., c_i)$ separabel über K für $i = 1, ..., n$.

d) Die normale Hülle von L über K entsteht aus L durch Adjunktion endlich vieler Nullstellen $c_1, ..., c_n$ von irreduziblen Polynomen aus $K[X]$, die in L eine Nullstelle besitzen. Weil L über K separabel ist, sind die Nullstellen in L separabel über K und damit auch ihre Konjugierten $c_1, ..., c_n$. Die Behauptung folgt aus a).

e) Es seien c_1 und $c_2 \in L$ algebraisch und separabel über K. Nach a) ist der Körper $K(c_1, c_2) \subset L$ separabel über K. Er enthält die Elemente $c_1 \pm c_2$, $c_1 \cdot c_2$ sowie c_1/c_2, falls $c_2 \neq 0$. Die Menge $L_s \subset L$ aller über K algebraischen Elemente aus L bildet also einen Unterkörper von L. □

Definition 3.16 *Der Unterkörper L_s aus Satz 3.26 e) heißt* separabler Abschluss *von K in L.*

Kein Element aus L, das nicht in L_s liegt, ist separabel über L_s, denn nach Satz 3.26 b) wäre es auch separabel über K.

Satz 3.27 (vom primitiven Element) *Der Körper K enthalte unendlich viele Elemente. Dann ist jede endliche separable Körpererweiterung $K \subset L$ einfach, d.h., es gibt ein $c \in L$ mit $L = K(c)$.*

Beweis. Weil L endlich über K ist entsteht dieser Körper $L = K(a_1, ..., a_n)$ aus K durch Adjunktion endlich vieler algebraischer Elemente $(a_1, ..., a_n)$. Wir beweisen die Aussage durch Induktion nach n. Für $n = 1$ ist nichts zu zeigen. Induktionsannahme ist die Behauptung im Fall $n - 1$. Dann ist also $K(a_1, ..., a_{n-1}) = K(c)$ eine einfache Erweiterung von K. Zu zeigen ist, dass dann auch $K(c, a_n)$ einfach über K ist. Mit anderen Worten: Es genügt, die Aussage für $n = 2$ zu beweisen.

Wir nennen die beiden algebraischen Elemente lieber a_1 und b_1, und nicht a_1 und a_2. Es seien $f, g \in K[X]$ die Minimalpolynome für a_1, bzw, b_1. Weiter sei $N \supset L$ eine normale Hülle von L. Dann zerfallen

$$f(X) = (X - a_1) \cdot ... \cdot (X - a_k), \quad g(X) = (X - b_1) \cdot ... \cdot (X - b_l), \quad a_1, ..., b_l \in N,$$

über N vollständig in Linearfaktoren. Weil b_1 separabel ist, sind die Nullstellen $b_1, ..., b_l$ von g paarweise voneinander verschieden. Damit hat jede Gleichung

$$a_i + xb_j = a_1 + xb_1, \quad i = 1, ..., k,\ j = 2, ..., l,$$

höchstens eine Nullstelle $x \in K$. Weil K unendlich ist, gibt es ein $u \in K$, das mit keiner dieser endlich vielen Lösungen übereinstimmt. Es ist also

$$a_i + ub_j \neq a_1 + ub_1 \text{ für } i = 1, ..., k,\ j = 2, ..., l.$$

Wir zeigen, dass $c := a_1 + ub_1 \in L$ ein primitives Element für L über K ist:

Das Element b_1 genügt den Gleichungen

$$g(b_1) = 0, \quad f(c - ub_1) = f(a_1) = 0.$$

Die Koeffizienten der Polynome $g(X)$ und $f(c - uX)$ liegen in $K(c)$. Für alle anderen Nullstellen b_j, $j \geq 2$, von g ist

$$c - ub_j = a_1 + u(b_1 - b_j) \neq a_i,\ i = 1, ..., k,$$

nach Wahl von u. Damit haben die Polynome $g(X)$ und $f(c - uX)$ nur die eine gemeinsame Nullstelle b_1. Weil alle Nullstellen von g verschieden sind, ist $X - b_1$ der $ggT(f(c - uX), g)$ über dem Körper N. Weil beide Polynome ihre Koeffizienten in $K(c)$ haben, gehört nach Aufgabe 3.1 dieser ggT schon zu $K(c)[X]$. Damit ist bewiesen: $b_1 \in K(c)$. Dann ist auch $a_1 = c - ub_1 \in K(c)$. Es folgt $L = K(a_1, b_1) \subset K(c)$. Wegen $c \in L$ gilt die Gleichheit $L = K(c)$. □

Beispiel 3.14 (F 00, T2, A3a) *Man bestimme ein primitives Element für die Körpererweiterung* $\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5})/\mathbb{Q}$.

Lösung: Wir könnten uns am Beweis von Satz 3.27 orientieren, und eine geeignete Linearkombination von $\sqrt[3]{2}$ *und* $\sqrt[4]{5}$ *suchen (wahrscheinlich wird es schon* $\sqrt[3]{2} + \sqrt[4]{5}$ *tun). Aber das ist mir zu arbeitsaufwendig. Sehen wir uns erst mal an, welchen Grad die Körpererweiterung* $\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5})$ *über* $\mathbb{Q}$ *besitzt, denn diesen Grad über* $\mathbb{Q}$ *müsste auch ein primitives Element haben. Die Erweiterung hat den Teilkörper* $\mathbb{Q}(\sqrt[3]{2})$. *Weil* $X^3 - 2 \in \mathbb{Q}[X]$ *irreduzibel ist (Eisenstein mit* $p = 2$*), hat diese Erweiterung den Grad drei. Außerdem gibt es den Zwischenkörper* $\mathbb{Q}(\sqrt[4]{5})$. *Auch* $X^4 - 5 \in \mathbb{Q}[X]$ *ist irreduzibel (Eisenstein mit* $p = 5$*), also ist dies eine Erweiterung vom Grad vier. Nach der Gradformel (Satz 3.1) hat also* $\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5})/Q$ *mindestens den Grad* $3 \cdot 4 = 12$. *Andererseits hat* $\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5})$ *über* $\mathbb{Q}(\sqrt[3]{2})$ *höchstens den Grad vier. Aus der Gradformel folgt, dass die Erweiterung* $\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5})$ *über* $\mathbb{Q}$ *genau den Grad 12 hat.*

Wir suchen also ein Element c, das über $\mathbb{Q}$ *den Grad 12 besitzt. Ein solches ist z.B.*

$$c = \sqrt[3]{2} \cdot \sqrt[4]{5}.$$

Es genügt über $\mathbb{Q}$ *der Gleichung*

$$X^{12} = (\sqrt[3]{2})^{12} \cdot (\sqrt[4]{5})^{12} = 2^4 \cdot 5^3 = 2000.$$

Nur wissen wir leider nicht, ob $X^{12} - 2000$ *über* $\mathbb{Q}$ *irreduzibel ist. Eisenstein greift hier nicht. Schauen wir uns mal den Zwischenkörper* $\mathbb{Q}(c) \subset \mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5})$ *an. Er enthält z.B. das Element*

$$c^4 = (\sqrt[3]{2})^4 \cdot 5 = 10 \cdot \sqrt[3]{2}.$$

Damit enthält $Q(c)$ das Element

$$\sqrt[3]{2} = \frac{1}{10}c^4,$$

und dann auch

$$\sqrt[4]{5} = \frac{c}{\sqrt[3]{2}}.$$

Also ist $\mathbb{Q}(c)$ der ganze Körper $\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5})$ und c ist ein primitives Element.

Weil wir schon wissen, dass die Erweiterung $\mathbb{Q}(c)$ über $\mathbb{Q}$ den Grad 12 hat, muss das Minimalpolynom von c über $\mathbb{Q}$ auch den Grad 12 besitzen. Nun ist c eine Nullstelle von $X^{12} - 2000$. Es folgt, dass $X^{12} - 2000$ dieses Minimalpolynom, und insbesondere irreduzibel über $\mathbb{Q}$ ist. So kann man die Irreduzibilität von Polynomen auch beweisen!

Beispiel 3.15 (F 00, T2, A3b) *Seien x und y Unbestimmte über dem Körper $\mathbb{F}_p$ von p Elementen. Man zeige: Die Körpererweiterung $\mathbb{F}_p(x,y)/\mathbb{F}_p(x^p, y^p)$ besitzt kein primitives Element.*

Lösung: Die Körpererweiterung $\mathbb{F}_p(x,y^p)/\mathbb{F}_p(x^p,y^p)$ entsteht durch Adjunktion des Elements x mit Minimalpolynom $X^p - x^p$ und hat deswegen den Grad p. Sie enthält das Element y nicht. Das Minimalpolynom von y über $\mathbb{F}_p(x,y^p)$ ist $Y^p - y^p$ und hat auch den Grad p. Die angegebene Körpererweiterung $\mathbb{F}_p(x,y)/\mathbb{F}_p(x^p,y^p)$ hat also den Grad p^2. Ein primitives Element für diese Körpererweiterung wäre ein Polynom

$$c(x,y) = \sum_{\mu,\nu=0}^{p-1} a_{\mu,\nu} x^\mu y^\nu, \quad a_{\mu,\nu} = a_{\mu,\nu}(x^p, y^p) \in \mathbb{F}_p(x^p, y^p),$$

dessen Minimalpolynom über $\mathbb{F}_p(x^p,y^p)$ den Grad p^2 hat. Wegen der komischen Eigenschaften des Frobenius ist

$$c(x,y)^p = \sum_{\mu,\nu} a_{\mu,\nu}^p (x^p)^\mu (y^p)^\nu$$

ein Element aus dem Grundkörper $\mathbb{F}_p(x^p,y^p)$. Das Minimalpolynom von c über diesem Grundkörper teilt

$$X^p - c(x,y)^p \in \mathbb{F}_p(x^p,y^p)[X]$$

und hat einen Grad $\leq p$. Es gibt kein Element vom Grad p^2 über dem Grundkörper, und deswegen auch kein primitives Element.

Aufgabe 3.21 (H 99, T1, A5) *a) Gibt es ein irreduzibles Polynom aus $\mathbb{Q}[X]$, das in $\mathbb{C}$ eine doppelte Nullstelle besitzt?*

b) Gibt es ein irreduzibles Polynom aus $K[X]$, das in einem Erweiterungskörper von K eine doppelte Nullstelle besitzt, wenn K ein endlicher Körper ist?

Aufgabe 3.22 (F 91, T3, A2) *Sei $K(\alpha)|K$ eine separable Körpererweiterung, und das Minimalpolynom g von α über K habe den Grad $n > 1$. Zeigen Sie:*

a) Die Gleichung $x^3 = \alpha$ besitzt genau dann eine Lösung in $K(\alpha)$, wenn das Polynom $f(x) = g(x^3) \in K[x]$ vom Grad $3n$ reduzibel ist.

b) Die Grade der irreduziblen Faktoren von f sind Vielfache von n.

c) f besitzt genau dann eine mehrfache Nullstelle in einem Erweiterungskörper von K, wenn $\mathrm{char}K = 3$ *ist.*

3.5 Galoissche Körpererweiterungen

Es sei $K \subset L$ eine Körpererweiterung und $G(L:K)$ die Gruppe der K-Automorphismen von L.

Definition 3.17 *Es sei $H \subset G(L:K)$ eine Untergruppe. Die Menge der unter H invarianten Körperelemente*

$$L^H := \{x \in L : g(x) = x \text{ für alle } g \in H\}$$

aus L heißt Fix-Körper *der Gruppe H.*

Die Teilmenge $L^H \subset L$ ist tatsächlich ein Körper. Dies folgt daraus, dass für jeden Körper-Automorphismus $g : L \to L$ gilt

$$g(x_1) = x_1, g(x_2) = x_2 \quad \Rightarrow g(x_1+x_2) = g(x_1)+g(x_2) = x_1+x_2,\ g(x_1 \cdot x_2) = g(x_1)\cdot g(x_2) = x_1 \cdot x_2.$$

Und wenn g ein K-Automorphismus von L ist, dann gilt $g(x) = x$ für alle $x \in K$. Also ist L^H ein Zwischenkörper

$$K \subset L^H \subset L.$$

Beispiel 3.16 *Es sei $L = K(\sqrt{c})$, wo $c \in K$ kein Quadrat ist, eine quadratische Erweiterung von K. Alle Elemente aus L haben die Form $a + b\sqrt{c}$, und die Konjugation*

$$g : a + b\sqrt{c} \mapsto a - b\sqrt{c}$$

erzeugt eine Untergruppe $< g > \subset G(L:K)$ der Ordnung zwei. Weil es zu $\sqrt{c} \in L$ nur das einzige andere konjugierte Element $-\sqrt{c} \in L$ gibt, stimmt jeder nicht-triviale K-Automorphismus von L mit g überein. Es ist $G(L:K) =< g >$. Der Fix-Körper $L^{<g>}$ besteht aus allen Elementen $a+b\sqrt{c} \in L$ mit $b = -b$. Falls K eine Charakteristik $\neq 2$ hat, bedeutet dies $b = 0$. Der Fixkörper von $G(K:L)$ ist der Grundkörper K.

Beispiel 3.17 *Es sei $K = \mathbb{Q}$ und*

$$L = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$$

der Zerfällungskörper von $f = X^3 - 2$ über $\mathbb{Q}$. Dieser Körper enthält die drei konjugierten Nullstellen

$$\sqrt[3]{2},\ \omega\sqrt[3]{2},\ \omega^2\sqrt[3]{2}, \quad \omega = e^{2\pi i/3}$$

von f. Am Anfang von Abschnitt 3.4 haben wir gesehen: Die Gruppe $G(K:\mathbb{Q})$ stimmt überein mit der Permutationsgruppe S_3 dieser drei Wurzeln. Diese Gruppe enthält vier echte Untergruppen: Die Gruppe $\mathbb{Z}_3$ der zyklischen Permutationen dieser drei Wurzeln, und drei Gruppen $\simeq \mathbb{Z}_2$, welche zwei Wurzeln vertauschen, und die dritte festlassen.

Ist $H \simeq \mathbb{Z}_2$ eine der Untergruppen der Ordnung 2, so sei etwa $\sqrt[3]{2}$ die fest gelassene Wurzel. Sie erzeugt einen Unterkörper $\mathbb{Q}(\sqrt[3]{2}) \subset K$ vom Grad 3. Nach der Gradformel (Satz 3.1) gibt es zwischen diesem und K keinen echten Unterkörper. Weil K^H nicht ganz L sein kann (H vertauscht ja zwei Wurzeln), ist also K^H dieser Unterkörper vom Grad 3.

Ist $H \simeq \mathbb{Z}_3$ die zyklische Gruppe der Ordnung 3, so sei etwa

$$h : \sqrt[3]{2} \mapsto \omega \cdot \sqrt[3]{2} \mapsto \omega^2 \cdot \sqrt[3]{2} \mapsto \sqrt[3]{2}$$

ein Erzeugendes. Wegen

$$\omega = \frac{\omega \cdot \sqrt[3]{2}}{\sqrt[3]{2}}$$

ist

$$h(\omega) = \frac{h(\omega \cdot \sqrt[3]{2})}{h(\sqrt[3]{2})} = \frac{\omega^2 \cdot \sqrt[3]{2}}{\omega \cdot \sqrt[3]{2}} = \omega.$$

Die quadratische Erweiterung $\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$ gehört also zu K^H. Wieder folgt aus der Gradformel (Satz 3.1), dass K^H dieser quadratische Zwischenkörper ist.

Definition 3.18 *Eine endliche Körpererweiterung $K \subset L$ heißt* galoissch, *wenn sie*

1) normal und

2) sparabel ist.

Die Gruppe $G(L:K)$ der K-Automorphismen $L \to L$ heißt dann Galoisgruppe *dieser Körpererweiterung.*

Diese Definition charakterisiert galoissche Körpererweiterungen rein körpertheoretisch. Es gibt aber auch eine gruppentheoretische Charakterisierung.

Satz 3.28 (Galoissche Körpererweiterungen) *Es sei $K \subset L$ eine endliche Körpererweiterung und $G = G(L:K)$ die Gruppe der K-Automorphismen von L. Dann sind äquivalent:*
i) die Erweiterung $K \subset L$ ist galoissch;
ii) es ist $L^G = K$.
Das heißt also: Nur die Elemente aus K bleiben unter allen Automorphismen $g \in G$ fest.

Beweis. i) $\Rightarrow$ ii): Weil jeder K-Automorphismus alle Elemente aus K in sich überführt ist $K \subset L^G$ offensichtlich. Nicht trival ist die Eigenschaft $L^G \subset K$.

Sei also $c \in L$ und $c \notin K$. Das Minimalpolynom $p \in K[X]$ von c hat dann einen Grad ≥ 2. Weil L über K normal ist, zerfällt p über L in Linearfaktoren. Weil L über K separabel ist, sind diese alle verschieden. Es gibt also mindestens eine weitere Nullstelle $c' \neq c$ von p in L. Die Unterkörper $K(c)$ und $K(c') \subset L$ sind K-isomorph. Durch $c \mapsto c'$ wird ein K-Isomorphismus

$K(c) \to K(c')$ definiert. Weil L über K normal ist, lässt sich dieser nach Satz 3.13 zu einem K-Isomorphismus $g : L \to L$ fortsetzen. Für dieses $g \in G$ gilt $g(c) = c' \neq c$. Also kann c nicht zum Fix-Körper L^G gehören. Der Fixkörper L^G kann nur Elemente aus K enthalten.

ii) $\Rightarrow$ i): Es sei $c \in L$ und $c \notin K$. Jetzt ist $L^G = K$ vorausgesetzt. Es gibt also Transformationen $g \in G$ mit $g(c) \neq c$. Nach Satz 3.17 ist $G = \{g_1, ..., g_n\}$ endlich. Es seien $c_1 = g_1(c), ..., c_n = g_n(c)$ die Transformierten von c. Diese brauchen nicht alle verschieden zu sein. Es seien $c = c_1, ..., c_m$, $m \leq n$, die paarweise Verschiedenen. Wir betrachten das Polynom

$$f(X) := \prod_1^m (X - c_\mu) \in L[X].$$

Alle $g \in G$ führen f in sich selbst über. Also sind alle Koeffizienten von f invariant unter allen $g \in G$ und gehören zu $L^G = K$. In Wirklichkeit ist $f \in K[X]$.

Nun sei $p \in K[X]$ das Minimalpolynom von c über K. Es hat in L die m verschiedenen Nullstellen $c = c_1, ..., c_m$. Also ist $Grad(p) \geq m$. Andererseits teilt p das Polynom f vom Grad m. Es folgt $Grad(p) = Grad(f)$ und $p = f$. Nun zerfällt p über L in soviele verschiedene Linearfaktoren, wie sein Grad angibt. Daraus folgt: L ist über K normal und separabel. □

Von nun an sei für den Rest dieses Paragraphen $K \subset L$ eine galoissche Erweiterung mit Galois-Gruppe $G = G(L : K)$.

In Definition 3.9 haben wir definiert, was über K konjugierte Elemente c_1 und $c_2 \in G$ sind. Sie sind Nullstellen desselben Minimalpolynoms $p \in K[X]$ und die Körper $K(c_1)$, bzw. $K(c_2)$ sind K-isomorph. Dieser K-Isomorphismus mit $c_1 \mapsto c_2$ kann nach Satz 3.13 zu einem K-Isomorphismus $g : L \to L$ des Zerfällungskörpers L fortgesetzt werden. Es gibt also ein $g \in G$ mit $g(c_1) = c_2$. Wenn es umgekehrt ein solches $g \in G$ gibt, dann sind die Unterkörper $K(c_1)$ und $K(c_2) \subset L$ isomorph, und die beiden Elemente c_1 und c_2 sind konjugiert. Wir sehen: Zwei Elemente aus L sind genau dann konjugiert über K, wenn es ein $g \in G$ gibt, das eines in das andere überführt. Wir verallgemeinern diese Eigenschaft jetzt auf Zwischenkörper $K \subset Z \subset L$.

Definition 3.19 *Zwei Zwischenkörper $K \subset Z_1 \subset L$ und $K \subset Z_2 \subset L$ heißen über K* konjugiert, *wenn es ein $g \in G$ gibt mit $g(K_1) = K_2$. Wegen Satz 3.13 ist dies genau dann der Fall, wenn die Zwischenkörper Z_1 und Z_2 K-isomorph sind.*

Satz 3.29 *Ist $K \subset Z \subset L$ ein Zwischenkörper, so ist die Erweiterung $L \supset Z$ wieder galoissch. (Die Erweiterung $Z \supset K$ ist i.a. nicht galoissch, weil sie i.a. nicht normal ist.) Die Galois-Gruppe $G(L : Z)$ ist eine Untergruppe U der Galoisgruppe $G = G(L : K)$. Der Zwischenkörper Z ist der Unterkörper L^U und damit durch U eindeutig bestimmt.*

Beweis. Weil L normal über K ist, ist L nach 3.16 a) auch normal über Z. Weil L separabel über K ist, ist L nach Satz 3.25 a) auch separabel über Z.

Die Galoisgruppe $G(L : Z)$ besteht aus allen Z-Isomorphismen $L \to L$. Wegen $K \subset Z$ sind diese auch K-Isomorphismen.

Weil L über Z galoissch ist, ist Z nach Satz 3.28 der Fixkörper L^U seiner Galoisgruppe $U = G(L : Z)$. □

Satz 3.30 (Hauptsatz der Galoistheorie) *Die Zuordnung*

$$\textit{Zwischenkörper } K \subset Z \subset L \quad \mapsto \quad \textit{Untergruppe } U = G(L:Z) \subset G(L:K)$$

definiert eine bijektive Abbildung der Mengen

$$\{\textit{Zwischenkörper } K \subset Z \subset L\} \mapsto \{\textit{Untergruppen } U \subset G(L:K)\}.$$

Ihre Umkehrabbildung ist

$$\textit{Untergruppe } U \subset G(L:K) \quad \mapsto \quad \textit{Zwischenkörper } Z = L^U.$$

Beweis. In Satz 3.29 heben wir gesehen: Der Zwischenkörper Z ist durch die Untergruppe $U = G(L:Z)$ eindeutig bestimmt als $Z = L^U$. Deswegen ist die angegebene Abbildung injektiv.

Ist $U \subset G(L:K)$ eine Untergruppe, so gehört dazu ein Zwischenkörper $Z = L^U$. Nach Satz 3.28 ist U die Galoisgruppe $G(L:Z)$. Deswegen ist die angegebene Abbildung auch bijektiv. □

Wegen $|G(L:Z)| = [L:Z]$ ist der folgende Zusatz offensichtlich.

Satz 3.31 (Zusatz) *In der Situation von Satz 3.30 gilt*

$$|U| = |G(L:Z)| = [L:Z], \quad [G:U] = [Z:K].$$

Beispiel 3.18 *Es sei $L = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ der Zerfällungskörper des Polynoms $X^3 - 2$ über $\mathbb{Q}$. Am Anfang von Abschnitt 3.4 haben wir die Galoisgruppe $G(L:\mathbb{Q})$ mit der symmetrischen Gruppe S_3 identifiziert. Diese Gruppe besitzt drei Untergruppen der Ordnung zwei und eine Untergruppe der Ordnung drei. Die Zwischenkörper sind*

$$\mathbb{Q}(\sqrt[3]{2}), \quad \mathbb{Q}(\omega\sqrt[3]{2}), \quad \mathbb{Q}(\omega^2\sqrt[3]{2})$$

vom Grad drei über $\mathbb{Q}$ und

$$\mathbb{Q}(\sqrt{-3})$$

vom Grad zwei über $\mathbb{Q}$.

Zu jeder Untergruppe $U \subset G$ gibt es die *konjugierten* Untergruppen

$$gUg^{-1} = \{gug^{-1} : u \in U\}, \quad g \in G.$$

Genau dann wenn $U \subset G$ ein Normalteiler ist, stimmen alle diese Gruppen mit U überein.

Satz 3.32 *Es sei $U \subset G$ eine Untergruppe mit zugehörigem Fixkörper $Z = L^U$. Zur konjugierten Untergruppe gUg^{-1} gehört dann der konjugierte Zwischenkörper gZ. Insbesondere ist $U \subset G$ genau dann ein Normalteiler, wenn die Körpererweiterung $K \subset Z$ normal ist. Dann ist auch $Z \supset K$ galoissch mit Galoisgruppe $G(Z:K) = G/U$.*

Beweis. Für $u \in U$, $g \in G$ und $c \in L$ ist

$$gug^{-1}(c) = c \quad \Leftrightarrow \quad u(g^{-1}c) = g^{-1}c.$$

Also gehört c genau dann zum Fixkörper $L^{gUg^{-1}}$ der konjugierten Gruppe, wenn $g^{-1}c$ zum Fixkörper L^U gehört. Dies zeigt $L^{gUg^{-1}} = g\,L^U$.

Ist $U \subset L$ ein Normalteiler mit Fixkörper $Z = L^U$, so ist also $gZ = Z$ für alle $g \in G$. Alle zu Z konjugierten Zwischenkörper stimmen mit Z überein. Mit $c \in Z$ gehören auch alle Konjugierten von c zu Z. Die Körpererweiterung $K \subset Z$ ist also normal.

Ist umgekehrt $K \subset Z$ eine normale Körpererweiterung, so ist $gZ = Z$ für alle $g \in G$. Die Galoisgruppe gUg^{-1} von gZ stimmt also mit U überein und $U \subset L$ ist ein Normalteiler.

Ist schließlich $K \subset Z \subset L$ ein über K normaler Zwischenkörper, so wird durch

$$G(L:K) \ni g \mapsto g|Z \in G(Z:K)$$

ein Gruppenhomomorphismus definiert. Sein Kern besteht aus allen K-Isomorphismen $g : L \to L$, deren Einschränkung auf Z die Identität ist. Das sind genau die Z-Isomorphismen von L. Aus dem Homomorphiesatz 1.9 folgt, dass die angegebene Vorschrift einen injektiven Gruppen-Homomorphismus $G(L:K)/G(L:Z) \to G(Z:K)$ definiert. Nach Satz 3.13 kann man aber auch jeden K-Homomorphismus $Z \to Z$ auf L fortsetzen. Deswegen ist diese Abbildung bijektiv. □

Satz 3.33 *Zu einer galoisschen Erweiterung $K \subset L$ gibt es nur endlich viele Zwischenkörper $K \subset Z \subset L$.*

Beweis. Die Galois-Korrespondenz zwischen Zwischenkörpern Z und Untergruppen $U \subset G$ ist bijektiv. Weil G endlich ist, hat diese Gruppe nur endlich viele Untergruppen. □

Beispiel 3.19 (F 00, T1, A3) *Beweisen Sie folgende Aussagen:*

i) Die Körper $\mathbb{Q}(\sqrt{d})$, wobei d die quadratfreien ganzen Zahlen ungleich 1 durchlaufe, sind genau alle quadratischen Erweiterungskörper von $\mathbb{Q}$.

ii) Sind $d_1, ..., d_n$ paarweise teilerfremde quadratfreie ganzen Zahlen ungleich 1, so ist $\mathbb{Q}(\sqrt{d_1}, ..., \sqrt{d_n})$ eine über $\mathbb{Q}$ galoissche Körpererweiterung mit Galoisgruppe $(\mathbb{Z}/2\mathbb{Z})^n$.

ii) Die Quadratwurzeln von endlich vielen paarweise verschiedenen Primzahlen sind linear unabhängig über $\mathbb{Q}$.

Lösung: *i) Eine quadratische Erweiterung $K \supset \mathbb{Q}$ entsteht durch Adjunktion der Wurzel eines über $\mathbb{Q}$ irreduziblen quadratischen Polynoms, das wir normiert annehmen können:*

$$f(X) = X^2 + pX + q.$$

Dann ist $K = \mathbb{Q}(x_1)$ mit

$$x_1 = \frac{p}{2} + \sqrt{\frac{p^2}{4} - q},$$

bzw.

$$K = \mathbb{Q}\left(\sqrt{p^2 - 4q}\right).$$

Seien etwa

$$p = \frac{p_1}{p_2}, \quad q = \frac{q_1}{q_2}, \quad p_1, p_2, q_1, q_2 \in \mathbb{Z}.$$

Dann ist

$$K = \mathbb{Q}\left(\sqrt{(\frac{p_1}{p_2})^2 - 4\frac{q_1}{q_2}}\right) = \mathbb{Q}\left(\frac{1}{p_2 q_2}\sqrt{p_1 p_2 q_2^2 - 4 q_1 q_2 p_2^2}\right) = \mathbb{Q}(\sqrt{d})$$

mit $d = p_1 p_2 q_2^2 - 4 q_1 q_2 p_2^2 \in \mathbb{Z}$. *Enthält* $d = c^2 d_1, c \in \mathbb{Z}$, *einen quadratischen Faktor, so ist* $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d_1})$. *Deswegen können wir d quadratrei annehmen.*

ii) Beweis durch Induktion nach n: Wir beweisen, dass $\mathbb{Q}(\sqrt{d_1}, ..., \sqrt{d_n})$ *eine galoissche Erweiterung von* $\mathbb{Q}$ *mit Galoisgruppe* $(\mathbb{Z}/2\mathbb{Z})^n$ *ist, die durch*

$$(\mathbb{Z}/2\mathbb{Z})^n \ni (z_1, ..., z_n) : (\sqrt{d_1}, ..., \sqrt{d_n}) \mapsto ((-1)^{z_1}\sqrt{d_1}), ..., (-1)^{z_n}\sqrt{d_n})$$

operiert (eine etwas genauere Aussage). Als Induktionsannahme werde dies für $n-1$ *vorausgesetzt.*

Jede Untergruppe $U \subset (\mathbb{Z}/2\mathbb{Z})^{n-1}$ *vom Index zwei in der Galoisgruppe der Erweiterung* $\mathbb{Q}(\sqrt{d_1}, ..., \sqrt{d_{n-1}})$ *ist Kern eines Homomorphismus*

$$(\mathbb{Z}/2\mathbb{Z})^{n-1} \to \mathbb{Z}/2\mathbb{Z}, \quad (z_1, ..., z_{n-1}) \mapsto a_1 z_1 + ... + a_{n-1} z_{n-1}, \quad \text{nicht } a_1 = ... = a_{n-1} = 0.$$

Seien hier etwa $a_{i_1} = ... = a_{i_k} = 1 \, mod 2$ *die Koeffizienten* $\neq 0$. *Dann gehören also genau die Vektoren* $(z_1, ..., z_n)$ *zur Untergruppe, für die* $z_{i_1} + ... + z_{i_k} = 0$. *Es gibt daher insgesamt*

$$\#\{i_1, ..., i_k\} = \sum_{k=1}^{n-1} \binom{n-1}{k} = 2^{n-1} - 1$$

derartige Untergruppen. Zu jeder gehört eine quadratische Erweiterung von $\mathbb{Q}$ *in* $\mathbb{Q}(\sqrt{d_1}, ..., \sqrt{d_{n-1}})$.

Nun gibt es in $\mathbb{Q}(\sqrt{d_1}, ..., \sqrt{d_{n-1}})$ *die* $2^{n-1}-1$ *quadratischen Erweiterungen* $\mathbb{Q}(\sqrt{d_{i_1}} \cdot .... \cdot \sqrt{d_{i_k}})$. *Genau das Element* $\sqrt{d_{i_1}} \cdot ... \cdot \sqrt{d_{i_k}}$ *wird von der obigen Untergruppe U fest gelassen. Deswegen ist dieser Zwischenkörper der Fixkörper der Untergruppe U. Es folgt, dass die angegebenen Erweiterungen grade alle quadratischen Zwischenkörper in* $\mathbb{Q}(\sqrt{d_1}, ..., \sqrt{d_{n-1}})$ *sind.*

Wir adjungieren $\sqrt{d_n}$ *an den Körper* $\mathbb{Q}(\sqrt{d_1}, ..., \sqrt{d_n})$. *Der entstehende Körper ist der Zerfällungskörper des Polynoms*

$$(X^2 - d_1) \cdot ... \cdot (X^2 - d_n) \in \mathbb{Q}[X].$$

Damit ist er galoissch über $\mathbb{Q}$. *Falls er nicht den Grad* 2^n *über* $\mathbb{Q}$ *hätte, müsste* $\sqrt{d_n}$ *schon in* $\mathbb{Q}(\sqrt{d_1}, ..., \sqrt{d_{n-1}})$ *liegen.* $\mathbb{Q}(\sqrt{d_n})$ *wäre einer der genannten quadratischen Zwischenkörper, und wir hätten*

$$\sqrt{d_n} = a + b\sqrt{d_{i_1} \cdot ... \cdot d_{i_k}}, \quad a, b \in \mathbb{Q}.$$

Daraus würde folgen

$$d_n = a^2 + b^2 \cdot d_{i_1} \cdot .. \cdot d_{i_k} + 2ab\sqrt{d_{i_1} \cdot ... \cdot d_{i_k}} \in \mathbb{Q}.$$

Das geht nur, wenn $ab = 0$.

Seien etwa $a = a_1/a_2$, $b = b_1/b_2$, $a_1, a_2, b_1, b_2 \in \mathbb{Z}$, *gekürzte Brüche. Dann würde* $a = 0$ *bedeuten, dass*

$$d_n \cdot b_2^2 = b_1^2 \cdot d_{i_1} \cdot ... \cdot d_{i_k}$$

gilt. Alle Primteiler von b_1 würden quadratisch in d_n aufgehen. Weil d_n quadratfrei vorausgesetzt ist, folgt $b_1^2 = 1$. Weil die Zahlen $d_{i_1}, ...d_{i_k}$ teilerfremd sind, würde jeder Primteiler von b_2 quadratisch in einer dieser Zahlen aufgehen. Die Zahlen d_i sind aber quadratfrei vorausgesetzt, also ist auch $b_2^2 = 1$. Damit wären alle $d_{i_1}, ..., d_{i_k}$ Teiler von d_n, im Widerspruch zur Angabe.

Und $b = 0$ würde auf $d_n = a^2$ führen. d_n wäre dann nicht quadratfrei.

Also gehört $\sqrt{d_n}$ nicht zum Körper $\mathbb{Q}(\sqrt{d_1}, ..., \sqrt{d_{n-1}})$, und der Körper $\mathbb{Q}(\sqrt{d_1}, ..., \sqrt{d_n})$ hat tatsächlich den Grad 2^n über $\mathbb{Q}$. Dann hat auch die Galoisgruppe dieses Körpers die Ordnung 2^n über Q. Jeder Galoisautomorphismus wird festgelegt durch eine Transformation

$$\sqrt{d_1}, ..., \sqrt{d_n} \mapsto \pm\sqrt{d_1}, ..., \pm\sqrt{d_n},$$

und hat deswegen die Ordnung zwei. Die Galoisgruppe enthält also kein Element der Ordnung vier, und muss $\simeq (\mathbb{Z}/2\mathbb{Z})^k$ sein. Um auf die Zahl von 2^n Gruppenelementen zu kommen, müssen in obiger Vorschrift die Vorzeichen unabhängig voneinander gewählt werden können. Damit ist die Induktionsbehauptung bewiesen.

iii) Es seien $d_1, ..., d_n \in \mathbb{N}$ paarweise verschiedene Primzahlen. Wenn die Wurzeln daraus über $\mathbb{Q}$ linear abhängig wären, gäbe es eine Gleichung

$$c_1\sqrt{d_1} + ... + c_n\sqrt{d_n} = 0, \quad c_1, ..., c_n \in \mathbb{Q},$$

wo wir o.B.d.A. $c_n \neq 0$ annehmen können. Dann würde aber $\sqrt{d_n}$ zum Körper $\mathbb{Q}(\sqrt{d_1}, ..., \sqrt{d_n})$ gehören, im Widerspruch zu ii).

Wenn $c \in L$ ein primitives Element für die galoissche Erweiterung $K \subset L$ ist, dann muss das Minimalpolynom $p \in K[X]$ von c über K den Grad $n := [L : K]$ haben. (Sonst wäre c ja in einem Unterkörper von L enthalten, der über K einen kleineren Grad als n hat.) Weil p separabel ist, sind die n Konjugierten von c in L über K alle voneinander verschieden.

Satz 3.34 (Folgerung aus Satz 3.27) *Die Körpererweiterung $K \subset L$ sei galoissch über dem unendlichen Körper L. Dann sind die Elemente der Galois-Gruppe $G(L : K)$ linear unabhängig über L.*

Ich will nicht sagen, in welchem Vektorraum diese lineare Unabhängigkeit gemeint ist. Deswegen eine explizitere Formulierung: Es seien $g_1, ..., g_n \in G(L : K)$, $n = [L : K]$, die Elemente dieser Galoisgruppe. Sind dann $a_1, ..., a_n \in L$ so gewählt, dass

$$a_1g_1 + ... + a_ng_n : L \to L$$

die Nullabbildung ist, dann gilt $a_1 = ... = a_n = 0$.

Oder noch expliziter: Sind $a_1, ..., a_n \in L$, nicht $a_1 = ... = a_n = 0$, dann gibt es ein $x \in L$ mit

$$a_1g_1(x) + ... + a_ng_n(x) \neq 0.$$

Beweis. Nach Satz 3.27 existiert ein primitives Element $c \in L$ für die Erweiterung $L \supset K$. Seien nun $a_1, ..., a_n \in L$ mit $a_1g_1(x) + ... + a_ng_n(x) = 0$ für alle $x \in L$. Insbesondere ist

$$\sum_1^n a_\nu g_\nu(1) = \sum_{\nu=1}^n a_\nu g_\nu(c) = \sum_{\nu=1}^n a_\nu g_\nu(c^2) = ... = \sum_{\nu=1}^n g_\nu(c^{n-1}) = 0.$$

Wegen $g_\nu(c^k) = (g_\nu(c))^k$ ist der Vektor $(a_1, ..., a_n)^t$ eine Lösung des linearen Gleichungssystems mit der $n \times n$-Koeffizientenmatrix

$$\begin{pmatrix} 1 & 1 & ... & 1 \\ g_1(c) & g_2(c) & ... & g_n(c) \\ g_1(c)^2 & g_2(c)^2 & ... & g_n(c)^2 \\ \vdots & \vdots & & \vdots \\ g_1(c)^{n-1} & g_2(c)^{n-1} & ... & g_n(c)^{n-1} \end{pmatrix}.$$

Diese Matrix ist die bekannte Vandermonde-Matrix zu den n Zahlen

$$g_1(c),\ g_2(c),\ ...,\ g_n(c) \in L.$$

Und ihre Determinante ist die bekannte Vandermonde-Determinante

$$\prod_{i<j}(g_j(c) - g_i(c)).$$

Weil c ein primitives Element ist, sind die n Konjugierten $g_i(c) \in L$ von c alle paarweise voneinander verschieden. Deswegen ist die Vandermonde-Determinante $\neq 0$ und der Lösungsvektor $(a_1, ..., a_n)^t$ muss der Nullvektor gewesen sein. □

Definition 3.20 *Es sei $f \in K[X]$ ein separables Polynom und $L \supset K$ sein Zerfällungskörper. L ist normal und separabel, also galoissch über K. Die Galoisgruppe von $G(L : K)$ heißt die* Galoisgruppe des Polynoms *f.*

Die Galoisgruppe bildet die Nullstellen von f wieder auf solche Nullstellen ab. Jedes $g \in G(L : K)$ permutiert die Nullstellen von f. Ist n die Anzahl dieser Nullstellen so erhalten wir daraus einen Homomorphismus von $G(L : K)$ in die symmetrische Gruppe S_n. Weil L aus K durch Adjunktion dieser Nullstellen entsteht, ist jedes $g \in G(L : K)$ durch seine Permutation der Nullstellen von f eindeutig festgelegt. Der Homomorphismus $G(L : K) \to S_n$ ist injektiv. Man kann also die Galoisgruppe eines Polynoms auffassen als eine Untergruppe der Permutationsgruppe dieser Nullstellen.

Zerfällt f über K in verschiedene irreduzible Faktoren, so gehen unter $g \in G(L : K)$ Nullstellen eines dieser Faktoren immer wieder in Nullstellen desselben Faktors über. Die Operation der Galoisgruppe auf den Nullstellen von f ist intransitiv.

Ist dagegen f irreduzibel über K, so sind alle Nullstellen von f konjugiert über K. die Operation der Galoisgruppe von f auf den Nullstellen dieses Polynoms ist transitiv.

Die Galoisgruppe G eines irreduziblen Polynoms $f \in K[X]$ ist eine Untergruppe der symmetrischen Gruppe S_n. Diese enthält die alternierende Gruppe A_n als Normalteiler vom Index zwei. Natürlich kann G in A_n enthalten sein. Dann lässt G die Wurzel aus der Diskriminante

$$\sqrt{D} = \prod_{i<j}(a_i - a_j)$$

invariant, wo $a_1, ..., a_n$ die Nullstellen von f in seinem Zerfällungskörper sind. Diese $\sqrt{D}$ liegt dann also schon im Grundkörper. Und umgekehrt:

Satz 3.35 *Die Galoisgruppe eines irreduziblen Polynoms $f \in K[X]$ ist genau dann eine Untergruppe der alternierenden Gruppe $A_n \subset S_n$, wenn $\sqrt{D}$ zu K gehört.*

Im Allgemeinen braucht das nicht der Fall zu sein. Dann enthält die Galoisgruppe den Normalteiler $G \cap A_n$ vom Index zwei. Dazu gehört im Zerfällungskörper von f der quadratische Zwischenkörper $K(\sqrt{D})$.

Aufgabe 3.23 *Es seien $a, b \in \mathbb{Q}$ und $K = \mathbb{Q}(\sqrt{a+ib})$ eine Körpererweiterung vom Grad 4 über $\mathbb{Q}$. Zeigen Sie:*

a) Die vier Zahlen $\pm\sqrt{a \pm ib}$ sind konjugiert über $\mathbb{Q}$.

b) Es gibt keine galoissche Körpererweiterung K von $\mathbb{Q}$, die $Q(i)$ enthält, und deren Galoisgruppe zyklisch von der Ordnung 4 ist.

Aufgabe 3.24 *Es sei p eine Primzahl und $f \in \mathbb{Q}[X]$ irreduzibel vom Grad p. Weiter sei α eine Nullstelle von f in seinem Zerfällungskörper und $\beta \neq \alpha$, $\beta \in \mathbb{Q}(\alpha)$, eine weitere Nullstelle von f. Zeigen Sie:*

a) Es gibt einen nichttrivialen Körperautomorphismus g von $\mathbb{Q}(\alpha)$ über $\mathbb{Q}$.

b) Die Erweiterung $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ ist galoissch mit zyklischer Galoisgruppe der Ordnung p.

Aufgabe 3.25 *Es seien $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ und $c = \sqrt{2} + \sqrt{3} \in K$.*

a) Bestimmen Sie das Minimalpolynom von c über $\mathbb{Q}$.

b) Zeigen Sie, dass c ein primitives Element für die Körpererweiterung $\mathbb{Q} \subset K$ ist.

c) Drücken Sie $\sqrt{2}$ und $\sqrt{3}$ als Polynom in c aus.

Aufgabe 3.26 *Was ist die Automorphismengruppe $G(K(x) : K)$?*

Aufgabe 3.27 (F 02, T2, A5) *Bestimmen Sie die Galoisgruppe über $\mathbb{Q}$ des Zerfällungskörpers von $\varphi(X) = X^4 + 6X^2 + 2 \in \mathbb{Z}[X]$.*

Aufgabe 3.28 (F 02, T3, A3) *Bestimmen Sie die Primfaktorzerlegung von*

$$f(x) = x^5 + x^4 + 14x^3 + 14x^2 + 28x + 28$$

in den Polynomringen $\mathbb{F}_2[x]$, $F_3[X]$ und $\mathbb{Q}[X]$. Bestimmen Sie in diesen drei Fällen jeweils die Ordnung der Galoisgruppe von f.

Aufgabe 3.29 (H 00, T2, A4) *Sei $\alpha \in \mathbb{C}$ eine Lösung der Gleichung*

$$\alpha^4 + 2\alpha^3 + 5\alpha^2 + 4\alpha + 1 = 0.$$

a) Seien $\beta := 2\alpha^3 + 3\alpha^2 + 9\alpha + 4$ und $\gamma := \alpha - \beta$. Zeigen Sie, dass β das Minimalpolynom $X^2 + 1$ und γ das Minimalpolynom $X^2 + X + 1$ über $\mathbb{Q}$ hat.

b) Zeigen Sie, dass $\mathbb{Q}(\alpha)$ über $\mathbb{Q}$ galoissch ist, und bestimmen Sie die Galoisgruppe.

Aufgabe 3.30 (H 99, T2, A4b)) *Sei $\alpha := \sqrt{7} + \sqrt{6}$. Man berechne das Minimalpolynom von α über $\mathbb{Q}$, den zugehörigen Zerfällungskörper und seine Galoisgruppe.*

Aufgabe 3.31 (F 99, T1, A4) *Der Körper $\mathbb{Q}(t)$ der rationalen Funktionen über $\mathbb{Q}$ hat zwei Automorphismen σ, τ mit $\sigma(t) = \frac{1}{t}$ und $\tau(t) = 1 - t$. Es sei G die von diesen beiden Autormorphismen erzeugte Untergruppe von $\mathrm{Aut}\mathbb{Q}(t)$ und F der Fixkörper von G.*

a) Bestimmen Sie die Ordnung und die Struktur von G.

b) Wie viele Zwischenkörper hat die Erweiterung $\mathbb{Q}(t)|F$ und was sind deren Grade über F? (Begründung!)

Aufgabe 3.32 (F 99, T2, A4) *Sei $f(X) = 1 - \frac{X^2}{2!} + \frac{X^4}{4!} \in \mathbb{Q}[X]$. Sei K der Zerfällungskörper von f über $\mathbb{Q}$.*

a) Man beweise, dass der Erweiterungsgrad $[K : \mathbb{Q}] = 8$ ist.

b) Man bestimme die Struktur der Galoisgruppe $\mathrm{Gal}(K|\mathbb{Q})$.

Aufgabe 3.33 (F 99, T3, A4) *Welche der folgenden Körpererweiterungen sind galoissch?*

a) $\mathbb{Q}(\sqrt[6]{-3})/\mathbb{Q}$,

b) $\mathbb{Q}(X)/\mathbb{Q}(X^3), X$ über $\mathbb{Q}$ transzendent.

c) $\mathbb{F}_2(X)/\mathbb{F}_2(X^2), X$ über $\mathbb{F}_2$ transzendent.

Aufgabe 3.34 (F 99, T3, A5) *Sei $K/\mathbb{Q}$eine galoissche Erweiterung vom Grade 55 mit einer Galoisgruppe G, die nicht abelsch ist. Man zeige, dass es genau einen echten Zwischenkörper L von $K/\mathbb{Q}$ gibt, der über $\mathbb{Q}$ galoissch ist und bestimme seinen Grad über $\mathbb{Q}$.*

Aufgabe 3.35 (H 97, T2, A2) *Sei $L|K$ eine galoissche Körpererweiterung vom Grad 40. Beweisen Sie, dass es Zwischenkörper vom Grad 2, 4 und 8 über K gibt, die galoissch über K sind.*

Aufgabe 3.36 (H 96, T1, A4) *Sei K ein Körper, G eine Gruppe von Automorphismen von K und $k = K^G$ der Fixkörper. Man beweise: Ein Element $\alpha \in K$ ist algebraisch über k genau dann, wenn die Menge $\{\sigma(\alpha)|\sigma \in G\}$ endlich ist.*

Aufgabe 3.37 (F 95, T1, A 4) *Sei $M := \mathbb{Q}(\sqrt{2}, \sqrt{6}, i)$ (wobei $i^2 = -1$).*

a) Berechnen Sie den Körpergrad $[M : \mathbb{Q}]$.

b) Zeigen Sie, dass $\mathbb{Q} \subset M$ Galoiserweiterung ist und berechnen Sie $\mathrm{Aut}(M/\mathbb{Q})$.

Aufgabe 3.38 (F 95, T2, A4) *Sei $\alpha = \sqrt{5 + 2\sqrt{5}}$.*

a) Man bestimme das Minimalpolynom von α über $\mathbb{Q}$.

b) Zeigen Sie: $\mathbb{Q}(\alpha)/\mathbb{Q}$ ist galoissch.

c) Bestimmen Sie die Galoisgruppe von $\mathbb{Q}(\alpha)/\mathbb{Q}$.

Aufgabe 3.39 (H 94, T1, A4) *Welche der folgenden Körpererweiterungen sind galoissch? Man begründe das Ergebnis.*

a) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$,

b) $\mathbb{Q}(\sqrt[6]{2})/\mathbb{Q}$,

c) $\mathbb{Q}(t)/\mathbb{Q}(t^2)$, t über $\mathbb{Q}$ transzendent,

d) $\mathbb{Z}_p(t)/\mathbb{Z}_p(t^p)$, p eine Primzahl, t über $\mathbb{Z}_p$ transzendent, $\mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z}$.

Aufgabe 3.40 (H 94, T3, A4) *Bestimmen Sie den Zerfällungskörper K und die Galoisgruppe G von*

$$x^4 - 4x^2 + 1$$

über $\mathbb{Q}$. Welche Unterkörper hat K?

Aufgabe 3.41 (F 94, T3, A2) *Sei k ein Körper und $f(t) \in k[t]$ ein irreduzibles, separables Polynom über k mit abelscher Galoisgruppe G. Zeigen Sie, dass die Ordnung von G gleich dem Grad von f ist.*

Aufgabe 3.42 (H 93, T1, A5) *Bestimmen Sie alle Unterkörper von $L := \mathbb{Q}(\sqrt{3}, \sqrt{5}, \sqrt{7})$, und geben Sie deren Körpergrad über $\mathbb{Q}$ an.*

Aufgabe 3.43 (H 93, T3, A3) *Im Polynomring $\mathbb{Q}[X]$ sei f das Polynom*

$$f(X) := X^4 + 3.$$

(vergleiche Aufgabe 3.19)

c) Man skizziere die Wurzeln $\zeta_1, \zeta_2, \zeta_3, \zeta_4 \in \mathbb{C}$ des Polynoms f in der komplexen Ebene und zeige: Die Galoisgruppe $\mathrm{Gal}(K/\mathbb{Q})$ induziert genau diejenigen Permutationen σ von $\{\zeta_1, ..., \zeta_4\}$, für die

$$|\sigma(\zeta_\nu) - \sigma(\zeta_\mu)| = |\zeta_\nu - \zeta_\mu|$$

für alle $\nu, \mu \in \{1, 2, 3, 4\}$.

d) Man bestimme eine Kompositionsreihe von $\mathrm{Gal}(K/\mathbb{Q})$ und die zugehörige Folge von Unterkörpern von K.

Aufgabe 3.44 (F 93, T1, A3) *Sei $K|\mathbb{Q}$ die Körpererweiterung, die aus $\mathbb{Q}$ durch Adjunktion aller Nullstellen in $\mathbb{C}$ aller Polynome $X^2 + aX + b \quad (a, b \in \mathbb{Q})$ hervorgeht. Ferner sei M die Menge der Quadratwurzeln $\sqrt{p}$, wobei $p = -1$ oder p eine Primzahl ist. Zeigen Sie:*

a) $K = \mathbb{Q}(M)$.

b) Für jeden Zwischenkörper Z von $K|\mathbb{Q}$ mit $[Z : \mathbb{Q}] < \infty$ gibt es Elemente $\sqrt{p_1}, ..., \sqrt{p_n} \in M$ mit $Z \subset \mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n})$.

c) Jede solche Erweiterung $Z|\mathbb{Q}$ ist galoissch und ihre Galoisgruppe $G(Z|\mathbb{Q})$ ist isomorph zu einem Produkt $\mathbb{Z}/2\mathbb{Z} \times 2\mathbb{Z} \times ... \times \mathbb{Z}/2\mathbb{Z}$.

Aufgabe 3.45 (F 93, T2, A4) *Es seien p eine Primzahl, α eine Nullstelle von $f(x) = x^3 + p^2$ und E der Zerfällungskörper von f in $\mathbb{C}$.*

a) Begründen Sie, warum $E \neq \mathbb{Q}(\alpha)$ ist.

b) Welchen Grad und welche Galoisgruppe hat E über $\mathbb{Q}$?

c) Geben Sie für jeden Körper $L \neq E$ mit $L \subset E$ ein primitives Element an!

Aufgabe 3.46 (H 92, T1, A3) *Es sei $f = a_n X^n + a_{n-1} X^{n-1} + ... + a_1 X + a_0 \in K[X]$ ein nichtkonstantes, separables Polynom mit $a_0 a_n \neq 0$. Sei $g = a_0 X^n + a_1 X^{n-1} + ... + a_{n-1} X + a_n$ das sogenannte ,,reziproke" Polynom zu f. Zeigen Sie: f und g haben dieselbe Galoisgruppe über K.*

Aufgabe 3.47 (F 92, T1, A4) *a) Sei $f \in \mathbb{Q}[X]$ ei irreduzibles Polynom ungeraden Grades $n > 1$, das höchstens $n-1$ reelle Nullstellen besitzt. Zeigen Sie, dass die Ordnung der Galoisgruppe von f über $\mathbb{Q}$ durch $2n$ teilbar ist.*

b) Zeigen Sie, dass $X^5 + 2X + 2$ über $\mathbb{Q}$ irreduzibel ist und dass $\mathbb{Q}[X]/(X^5 + 2X + 2)$ keine galoissche Erweiterung von $\mathbb{Q}$ ist.

Aufgabe 3.48 (F 92, T3, A5) *Es sei E der Zerfällungskörper des Polynoms $X^4 - 3$ über $\mathbb{Q}$. Zeigen Sie: Der Grad von E über $\mathbb{Q}$ ist 8 . Die Galoisgruppe von E über $\mathbb{Q}$ ist nicht abelsch.*

Aufgabe 3.49 (H 91, T3, A1) *Es sei K/k eine endliche galoissche Körpererweiterung, deren Galoisgruppe isomorph zur symmetrischen Gruppe $S_n (n \geq 2)$ ist. Man beweise, dass K einen und nur einen über k quadratischen Teilkörper enthält.*

Aufgabe 3.50 (F 91, T2, A4) *a) Man zeige, dass $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3})$ und $\mathbb{Q}(\sqrt{6})$ die einzigen echten Unterkörper von $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sind.*

b) Man berechne das Minimalpolynom von $\sqrt{2} + \sqrt{3}$ über $\mathbb{Q}$ und $\mathbb{Q}(\sqrt{2})$.

Aufgabe 3.51 (H 90, T2, A2) *Sei $\mathbb{Q}[X, Y]$ der Polynomring in Unbestimmten X, Y mit von $X^3 - 2$ und $X^2 + XY + Y^2$ erzeugtem Ideal I.*

a) Zeigen Sie, dass $\mathbb{Q}[X, Y]/I =: K$ ein Zerfällungskörper von $X^3 - 2$ über $\mathbb{Q}$ ist, und geben Sie die Galoisgruppe von K über $\mathbb{Q}$ an.

b) Zeigen Sie, dass man einen Isomorphismus $\mathbb{Q}[Z]/(Z^6 + 108) \xrightarrow{\sim} K$ durch $Z \mapsto X + 2Y$ hat.

4 Beispiele

4.1 Kreisteilungskörper

Wir definieren formal einen Begriff, den wir schon mehrmals informell benutzten.

Definition 4.1 *Es sei K ein Körper und $1 \leq n \in N$. Eine Zahl $w \in K$ heißt n-te* Einheitswurzel, *wenn sie $w^n = 1$ erfüllt. Sie heißt* primitive n-te Einheitswurzel, *wen sie keine m-te Einheitswurzel für ein $m < n$ ist.*

Beispiel 4.1 *Es gibt immer eine erste Einheitswurzel $w = 1$, und - in Charakteristik $\neq 2$ - zwei zweite Einheitswurzeln ± 1. Im Körper $\mathbb{C}$ gibt es drei dritte Einheitswurzeln*

$$1, \quad \omega = \frac{1}{2}(-1 + i\sqrt{3}) \quad und \quad \omega^2.$$

Davon sind ω und ω^2 primitiv. In $\mathbb{C}$ gibt es vier vierte Einheitswurzeln

$$\pm 1, \quad \pm i.$$

Davon sind $\pm i$ primitiv.

Häufig benutzte Gleichungen für n-te Einheitswurzeln sind:

Satz 4.1 *a) Ist w eine n-te Einheitswurzel, so gilt*

$$1 + w + w^2 + ... + w^{n-1} = \begin{cases} n & (w = 1), \\ 0 & (w \neq 1). \end{cases}$$

b) Ist w sogar eine primitive n-te Einheitswurzel, so haben wir

$$w \cdot w^2 \cdot ... \cdot w^{n-1} = (-1)^{n-1},$$

$$(1 - w) \cdot (1 - w^2) \cdot ... \cdot (1 - w^{n-1}) = n.$$

Beweis. a) Die Summe werde mit s abgekürzt. Dann ist

$$w \cdot s = w + w^2 + ... + w^n = s.$$

Also ist $s \cdot (w - 1) = 0$.

b) Nach Vieta ist

$$\frac{X^n - 1}{X - 1} = X^{n-1} + ... + X + 1 = \prod_{i=1}^{n-1} (X - w^i).$$

Setzen wir hier $X = 0$, so finden wir

$$1 = (-1)^{n-1} \cdot w \cdot w^2 \cdot ... \cdot w^{n-1},$$

und mit $X = 1$

$$n = \prod_{i=1}^{n-1} (1 - w^i).$$

□

Im folgenden werde immer $n > 1$ vorausgesetzt. n-te Einheitswurzeln sind Nullstellen des Polynoms

$$X^n - 1 = (X - 1) \cdot (X^{n-1} + ... + X + 1).$$

Satz 4.2 *Das Polynom $X^n - 1$ ist genau dann separabel über K, wenn entweder K die Charakteristik 0 hat, oder eine Charakteristik $p > 0$, und n nicht durch p teilbar ist.*

Beweis. Die Ableitung des Polynoms $X^n - 1$ ist

$$(X^n - 1)' = nX^{n-1}.$$

Wenn $n \neq 0$ ist, hat die Ableitung nur den einzigen irreduziblen Faktor X, und der teilt das Polynom $X^n - 1$ nicht. Dann ist also $X^n - 1$ separabel.

Der Fall $n = 0$ tritt nur dann ein, wenn K eine Charakteristik $p > 1$ hat, und n durch p teilbar ist. Sei dann etwa $n = p^r \cdot m$, wo p die Zahl m nicht mehr teilt. Dann ist

$$X^n - 1 = (X^m)^{p^r} - 1 = (X^m - 1)^{p^r},$$

und $X^n - 1$ ist inseparabel. Es hat dieselben Nullstellen wie $X^m - 1$. □

Wir setzen also jetzt voraus: Der Körper K hat entweder die Charakteristik 0, oder n ist nicht durch die Charakteristik p von K teilbar. Dann ist das Polynom $X^n - 1$ separabel und hat in seinem Zerfällungskörper L genau n verschiedene Nullstellen. In L gibt es genau n verschiedene n-te Einheitswurzeln.

Das Produkt zweier n-ter Einheitswurzeln ist wieder eine n-te Einheitswurzel. Deswegen bilden die n-ten Einheitswurzeln eine Untergruppe der Ordnung n in der multiplikativen Gruppe L^* des Körpers L. Nach Satz 2.11 ist diese Gruppe zyklisch $\simeq \mathbb{Z}_n$. Unter diesem Isomorphismus werden prime Restklassen modulo n auf primitive n-te Einheitswurzeln abgebildet. Insbesondere ist die Anzahl der primitiven n-ten Einheitswurzeln $= \varphi(n)$, wo φ die Eulersche φ-Funktion ist. Ist w eine primitive n-te Einheitswurzel, so ist

$$k \, mod \, n \mapsto w^k$$

ein Isomorphismus der additiven Gruppe $\mathbb{Z}_n$ auf die multiplikative Gruppe der n-ten Einheitswurzeln.

Beispiel 4.2 *Ist $K = \mathbb{C}$, so ist $e^{2\pi i/n}$ ein primitive n-te Einheitswurzel, und die Zahlen $e^{2\pi i \cdot k/n}$, $0 \leq k \leq n - 1$, sind alle n-ten Einheitswurzeln.*

Jede Restklasse $k \, mod \, n$ hat eine Ordnung d, welche die Zahl n teilt. Sie erzeugt die eindeutig bestimmte Untergruppe $\mathbb{Z}_d \subset \mathbb{Z}_n$. In dieser Untergruppe ist sie eine primitive Restklasse modulo d. Daraus folgt

$$n = \sum_{d|n} \varphi(d).$$

Hat $k \bmod n$ die Ordnung d, so gilt für die zugehörige Einheitswurzel w^k, dass $(w^k)^d = 1$ ist, aber $(w^k)^{d'} \neq 1$, falls $1 \leq d' < d$. Die Einheitswurzel w^k ist eine primitive d-te Einheitswurzel.

Definition 4.2 *Es seien $w_1, ..., w_{\varphi(n)}$ die primitiven n-ten Einheitswurzeln in L. Dann heißt*

$$\Phi_n(X) := (X - w_1) \cdot ... \cdot (X - w_{\varphi(n)}) \in L[X]$$

das n-te Kreisteilungspolynom.

Satz 4.3 *a) Für die Kreisteilungspolynome Φ_n gilt*

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

b) Hat L die Charakteristik 0, so ist $\Phi_n \in \mathbb{Z}[X]$ ein ganzzahliges Polynom unabhängig von L.

c) Hat L eine Charakteristik $p > 1$, so ist das n-te Kreisteilungspolynom über L die Reduktion modulo p des Polynoms Φ_n aus der Charakteristik 0. Seine Koeffizienten liegen alle im Primkörper $\mathbb{F}_p \subset L$.

Beweis. a) Das Produkt aller linearen Polynome $X - w$, wo w alle n-ten Einheitswurzeln durchläuft, stimmt mit $X^n - 1$ überein. Jede n-te Einheitswurzel ist eine primitive d-te Einheitswurzel für genau einen Teiler d von n. Also ist

$$X^n - 1 = \prod_w (X - w) = \prod_{d|n} \Phi_d(X).$$

b) (Induktion nach n): Es ist $\Phi_1(X) = X - 1$. Ist die Behauptung für alle $d < n$ bewiesen so ist nach a)

$$X^n - 1 = \underbrace{\prod_{d|n, d<n} \Phi_d(X)}_{\in \mathbb{Z}[X]} \cdot \Phi_n(X).$$

Φ_n ist der Quotient des ganzzahligen Polynoms $X^n - 1$ durch einen ganzzahligen, normierten Teiler dieses Polynoms. Das Polynom Φ_n ergibt sich, indem man $X^n - 1$ nach dem Polynomdivisionsalgorithmus durch diesen normierten, ganzzahligen Teiler dividiert. Dabei entstehen im Quotienten stets nur ganze Koeffizienten.

c) Man muss den Beweis für b) modulo p reduzieren. □

Beispiel 4.3 *Ist p eine Primzahl, so gibt es $p-1$ primitive Einheitswurzeln. Das p-te Kreisteilungspolynom ist*

$$\Phi_p(x) = \frac{X^p - 1}{X - 1} = X^{p-1} + ... + X + 1.$$

(Dieses Polynom haben wir schon in Abschnitt 2.5 Kreisteilungspolynom genannt.)

Die ersten zwölf Kreisteilungspolynome sind

$$\begin{aligned}
\Phi_1(X) &= X-1,\\
\Phi_2(X) &= X+1,\\
\Phi_3(X) &= X^2+X+1,\\
\Phi_4(X) &= (X^4-1)/(\Phi_1(X)\cdot\Phi_2(X))\\
&= (X^4-1)/(X^2-1)\\
&= X^2+1,\\
\Phi_5(X) &= X^4+X^3+X^2+X+1,\\
\Phi_6(X) &= (X^6-1)/(\Phi_1(X)\cdot\Phi_2(X)\cdot\Phi_3(X))\\
&= (X^6-1)/(X^4+X^3-X-1)\\
&= X^2-X+1,\\
\Phi_7(X) &= X^6+X^5+X^4+X^3+X^2+X+1,\\
\Phi_8(X) &= (X^8-1)/(\Phi_1(X)\cdot\Phi_2(X)\cdot\Phi_4(X))\\
&= (X^8-1)/(X^4-1)\\
&= X^4+1,\\
\Phi_9(X) &= (X^9-1)/(\Phi_1(X)\cdot\Phi_3(X))\\
&= (X^9-1)/(X^3-1)\\
&= X^6+X^3+1,\\
\Phi_{10}(X) &= (X^{10}-1)/(\Phi_1(X)\cdot\Phi_2(X)\cdot\Phi_5(X))\\
&= (X^{10}-1)/((X^5-1)\cdot(X+1))\\
&= (X^5+1)/(X+1)\\
&= X^4-X^3+X^2-X+1,\\
\Phi_{11}(X) &= X^{10}+X^9+X^8+X^7+X^6+X^5+X^4+X^3+X^2+X+1,\\
\Phi_{12}(X) &= (X^{12}-1)/(\Phi_1(X)\cdot\Phi_2(X)\cdot\Phi_3(X)\cdot\Phi_4(X)\cdot\Phi_6(X))\\
&= (X^{12}-1)/((X^6-1)\cdot(X^2+1))\\
&= (X^6-1)/(X^2+1)\\
&= X^4-X^2+1.
\end{aligned}$$

Ist w eine primitive n-te Einheitswurzel, so wird durch

$$k \bmod n \mapsto w^k$$

ein Isomorphismus der additiven zyklischen Gruppe $\mathbb{Z}_n$ auf die multiplikative Gruppe der n-ten Einheitswurzeln definiert. Dabei werden genau die primen Restklassen modulo n auf primitive n-te Einheitswurzeln abgebildet. Daraus folgt, dass die primitiven n-ten Einheitswurzeln genau die Potenzen w^k sind, für welche die Zahlen k und n teilerfremd sind.

Satz 4.4 *Jedes Kreisteilungspolynom $\Phi_n \in \mathbb{Q}[X]$ ist irreduzibel über $\mathbb{Q}$.*

Beweis. Es seien $w \in \mathbb{C}$ eine primitive n-te Einheitswurzel und $p \in \mathbb{Q}[X]$ das Minimalpolynom von w. Dann teilt p das Kreisteilungspolynom Φ_n und ist nach Satz 2.31 selbst auch ganzzahlig. Wir müssen zeigen: $\Phi_n = p$.

Dazu zeigen wir die

Hilfsausage: Für jede Primzahl $q \not| n$ ist auch w^q eine Nullstelle von p.

Jede andere primitive n-te Einheitswurzel ist eine Potenz w^k, wo $1 < k < n$ und k teilerfremd zu n ist. Es sei $k = q_1^{r_1} \cdot \ldots \cdot q_m^{r_m}$ die Primfaktorzerlegung von k. Dann ist also q_1 kein Teiler von n und nach der Hilfsaussage ist auch w^{q_1} eine Nullstelle von p. Ebenso ist

$$w^{q_1^2} = (w^{q_1})^{q_1}$$

eine Nullstelle von p (Hilfsaussage mit der Einheitswurzel w^{q_1}). So macht man weiter und findet schließlich, dass w^k eine Nullstelle von p ist. Damit hat das irreduzible, normierte Polynom p denselben Grad $\varphi(n)$ wie das Kreisteilungspolynom Φ_n. Weil p dieses Polynom teilt, folgt $\Phi_n = p$ ist irreduzibel.

Beweis der Hilfsaussage. Das Minimalpolynom von w^q sei $r \in \mathbb{Q}[X]$. Auch r teilt $X^n - 1$ und ist deswegen ganzzahlig. Wenn $p \neq r$ wäre, dann wäre $X^n - 1$ durch das Produkt $p \cdot r$ teilbar:

$$X^n - 1 = p(X) \cdot r(X) \cdot f(X), \quad p, r, f \in \mathbb{Z}[X].$$

Das Polynom $r(X^q)$ hat die Nullstelle w, ist also durch das Minimalpolynom p von w teilbar:

$$r(X^q) = p(X) \cdot p_1(X).$$

Wir betrachten nun die beiden letzten Gleichungen modulo der Primzahl q (alle Polynome sind ganzzahlig). Weil die Frobenius-Abbildung $F : \mathbb{F}_q \to \mathbb{F}_q$, $c \mapsto c^q$, ein Körper-Isomorphismus ist (Satz 3.20), folgt

$$r(X^q) = (r(X))^q = p(X) \cdot p_1(X) \quad \text{modulo } q.$$

Weil der Ring $\mathbb{F}_q[X]$ faktoriell ist (Satz 2.33), kommt jeder irreduzible Faktor $p_0 \in \mathbb{F}_q[X]$ von p modulo q auch in r^q modulo q und deswegen in r modulo q vor. Deswegen teilt p_0^2 das Polynom

$$X^n - 1 = p(X) \cdot r(X) \cdot f(X) \quad \text{modulo } q.$$

Das Polynom $X^n - 1$ *modulo* q hat einen mehrfachen Faktor, ist also nicht separabel über $\mathbb{F}_q$. Das ist ein Widerspruch zu Satz 4.2. □

Definition 4.3 *Der n-te Kreisteilungskörper $\mathbb{Q}(\sqrt[n]{1})$, ist der Körper, der aus $\mathbb{Q}$ durch Adjunktion aller n-ten Einheitswurzeln entsteht.*

Weil alle n-ten Einheitswurzeln Potenzen einer einzigen primitiven Einheitswurzel w sind, ist $\mathbb{Q}(\sqrt[n]{1})$ schon die einfache Erweiterung $\mathbb{Q}(w)$. Nach Satz 4.4 hat die Körpererweiterung $\mathbb{Q} \subset \mathbb{Q}(w)$ den Grad $\varphi(n)$.

Der Körper $\mathbb{Q}(w)$ ist normal und separabel, also galoissch über $\mathbb{Q}$. Wir wollen seine Galoisgruppe identifizieren.

Jeder Galois-Automorphismus permutiert die n-ten Einheitswurzeln, wobei Produkte zweier Einheitswurzeln auf die Produkte der Bilder beider Einheitswurzeln übergehen. Unter dem Gruppen-Isomorphismus

$$(\mathbb{Z}_n, +) \to \{n\text{-te Einheitswurzeln}, \cdot\), \quad k \, mod \, n \mapsto w^k,$$

induziert er einen Gruppen-Automorphismus der zyklischen Gruppe $\alpha : \mathbb{Z}_n \to \mathbb{Z}_n$. Nach Satz 1.13 ist die Automorphismengruppe von $\mathbb{Z}_n$ isomorph zur multiplikativen Gruppe $\mathbb{Z}_n^*$ der primen Restklassen modulo n. Jeder Automorphismus ist von der Form $k \, mod \, n \mapsto r \cdot k \, mod \, n$, wo r eine prime Restklasse modulo n ist.

Was entspricht dem Automorphismus $\alpha : k \mapsto r \cdot k \, mod \, n$ unter dem Isomorphismus von $\mathbb{Z}_n$ auf die multiplikative Gruppe der n-ten Einheitswurzeln? Bei diesem Isomorphismus geht $1 \in \mathbb{Z}_n$ auf eine primitive Einheitswurzel w und

$$k \mapsto w^k, \quad k \cdot r \mapsto w^{k \cdot r} = (w^k)^r$$

über. Jede n-te Einheitswurzel w^k wird auf ihre r-te Potenz abgebildet. Insbesondere wird die primitive n-te Einheitswurzel w auf die primitive Einheitswurzel w^r abgebildet. Nach Satz 4.4 sind aber alle primitiven n-ten Einheitswurzeln konjugiert über $\mathbb{Q}$. Es gibt also einen Galois-Automorphismus $g : L \to L$ mit $g(w) = w^r$. Für diesen gilt dann auch

$$g(w^k) = (w^r)^k = (w^k)^r.$$

Der Galois-Automorphismus g operiert auf den n-ten Einheitswurzeln genau wie α auf der Gruppe $\mathbb{Z}_n$. Wir haben bewiesen:

Satz 4.5 *Die Galoisgruppe des n-ten Kreisteilungskörpers über $\mathbb{Q}$ ist isomorph zur primen Restklassengruppe modulo n. Ist w eine primitive n-te Einheitswurzel, so wird jeder Galois-Automorphismus durch*

$$w \mapsto w^r$$

induziert, wo r die primen Restklassen modulo n durchläuft.

Insbesondere ist die Galoisgruppe des Kreisteilungskörpers stets abelsch. Aber sie braucht nicht zyklisch zu sein. In 1.3 haben wir gesehen: Die prime Restklassengruppe modulo 8 ist isomorph zur Kleinschen Vierergruppe.

Die Kenntnis der Galoisgruppe erlaubt, die Anzahl der Zwischenkörper und deren Grad über $\mathbb{Q}$ anzugeben.

Beispiel 4.4 *Die Galoisgruppe des Kreisteilungskörpers $\mathbb{Q}(\sqrt[8]{1})$ vom Grad $\varphi(8) = 4$ über $\mathbb{Q}$ ist die Kleinsche Vierergruppe. Sie hat drei Untergruppen der Ordnung zwei. Also gibt es genau drei Zwischenkörper, alle vom Grad zwei.*

Eine primitive achte Einheitswurzel ist

$$\tau := \frac{1}{2}\sqrt{2}(1 + i).$$

Wegen $\tau^2 = i$ ist einer der Zwischenkörper $\mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$. Aber es muss noch zwei andere quadratische Zwischenkörper geben. In der Tat: $\mathbb{Q}(\sqrt[8]{1})$ enthält

$$\tau + \tau^7 = \frac{1}{2}\sqrt{2}[(1+i) + (1-i)] = \sqrt{2}$$

sowie

$$\tau + \tau^3 = \frac{1}{2}\sqrt{2}[(1+i) + (-1+i)] = i\sqrt{2}.$$

Die beiden anderen Zwischenkörper sind $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\sqrt{-2})$.

Ist $n = p$ eine Primzahl, so ist $\varphi(p) = p - 1$. Die Galoisgruppe des Körpers $\mathbb{Q}(\sqrt[p]{1})$ über $\mathbb{Q}$ hat die Ordnung $p - 1$. Die prime Restklassengruppe modulo p ist die Einheitengruppe des Primkörpers $\mathbb{F}_p$ und nach Satz 2.11 zyklisch. Also ist die Galoisgruppe von $\mathbb{Q}(\sqrt[p]{1})$ über $\mathbb{Q}$ zyklisch von der Ordnung $p - 1$. Auch der Körpergrad $[\mathbb{Q}(\sqrt[p]{1}) : \mathbb{Q}]$ ist $p - 1$.

Satz 4.6 *Ist $w \neq 1$ eine p-te Einheitswurzel, so bilden die Potenzen*

$$w,\ w^2,\ ...,\ w^{p-1}$$

eine $\mathbb{Q}$-Basis von $\mathbb{Q}(\sqrt[p]{1})$.

Beweis. Weil der Körpergrad $= p - 1$ ist, genügt es zu zeigen, dass diese $p - 1$ Potenzen über $\mathbb{Q}$ linear unabhängig sind. Andernfalls gäbe es eine lineare Relation

$$c_1 w + c_2 w^2 + ... + c_{p-1} w^{p-1} = 0, \quad c_1, ..., c_{p-1} \in \mathbb{Q}.$$

Hier kann man w kürzen und erhält eine Gleichung vom Grad $p - 2$

$$c_1 + c_2 w + ... + c_{p-1} w^{p-2} = 0$$

für w mit Koeffizienten in $\mathbb{Q}$. Deren linke Seite muss ein Vielfaches des Minimalpolynoms Φ_p sein. Weil Φ_p den Grad $p - 1$ hat, geht das nur, wenn $c_1 = ... = c_{p-1} = 0$. □

Ist $q \in (\mathbb{Z}_p)^*$ ein erzeugendes Element dieser Gruppe, so sind alle primen Restklassen modulo p gerade $q, q^2, ..., q^{p-1} = 1 \, mod \, p$. Das zu q gehörende Erzeugende der Galoisgruppe operiert durch

$$w \mapsto w^q \mapsto w^{q^2} \mapsto ... \mapsto w^{q^{p-1}} = w.$$

Mit dieser Information kann man die Zwischenkörper zwischen $\mathbb{Q}$ und $\mathbb{Q}(\sqrt[p]{1})$ sehr explizit durch Angabe einer $\mathbb{Q}$-Basis beschreiben. Jede Untergruppe der Galoisgruppe $\mathbb{Z}_{p-1}$ ist zyklisch von einer Ordnung m die $p - 1$ teilt. Und zu jeder Ordnung m gibt es genau eine solche Untergruppe. Ist $p - 1 = m \cdot r$, so ist diese Untergruppe

$$U_m = \{0,\ r,\ 2r,\ ...,\ (m-1)r \, mod \, (p-1)\}.$$

Ein Erzeugendes g dieser Gruppe U_m operiert auf der Körperbasis w, w^2, ..., w^{p-1} durch $g : w \mapsto w^{q^r}$. Die folgenden r Körperelemente sind deswegen invariant unter allen Transformationen der Gruppe U_m, und gehören zu deren Fixkörper:

$$\begin{array}{ccccccccc} w & + & w^{(q^r)} & + & w^{(q^{2r})} & + & ... & + & w^{(q^{(m-1)r})}, \\ w^q & + & w^{(q^{r+1})} & + & w^{(q^{2r+1})} & + & ... & + & w^{(q^{(m-1)r+1})}, \\ \vdots & & & & & & & & \\ w^{(q^{r-1})} & + & w^{(q^{2r-1})} & + & w^{(q^{3r-1})} & + & ... & + & w^{(q^{mr})}. \end{array}$$

Diese r Elemente des Kreisteilungskörpers heißen nach Gauß *m-gliedrige Perioden.* In den r Linearkombinationen kommt jede Potenz $w^1, ..., w^{p-1}$ genau einmal vor. Also sind sie linear unabhängig über $\mathbb{Q}$. Weil der Fixkörper von U_m den Körpergrad r über $\mathbb{Q}$ hat, bilden sie eine $\mathbb{Q}$-Basis dieses Fixkörpers. Keines der Elemente ist invariant unter einer Untergruppe der Galoisgruppe, die U_m echt enthält. Also liegt keines in einem echt kleineren Unterkörper, und jedes dieser Elemente erzeugt den Fixkörper von U_m.

Beispiel 4.5 *p=5. Die Galoisgruppe ist zyklisch von der Ordnung vier. Sie hat genau eine echte Untergruppe, und diese hat die Ordnung zwei. Wählen wir $q = 2$ als Erzeugendes der primen Restklassengruppe modulo 2, so wird die Untergruppe der Ordnung 2 erzeugt von $2q = 4$. Im Kreisteilungskörper $\mathbb{Q}(\sqrt[5]{1})$ vom Körpergrad vier über $\mathbb{Q}$ gibt es deswegen genau einen echten Zwischenkörper, und dieser hat den Körpergrad zwei über $\mathbb{Q}$. Ist ϵ eine primitive fünfte Einheitswurzel, so sind*

$$\epsilon,\ \epsilon^2,\ \epsilon^4, \epsilon^8 = \epsilon^3$$

alle primitiven fünften Einheitswurzeln. Die zweigliedrigen Perioden

$$\eta := \epsilon + \epsilon^4, \quad \eta' := \epsilon^2 + \epsilon^3$$

erzeugen jede für sich den eindeutig bestimmten quadratischen Teilkörper. Wegen

$$\eta^2 = 2 + \eta' = 1 - \eta, \quad \eta^2 + \eta - 1 = 0$$

ist $\eta = (-1 \pm \sqrt{5})/2$, und dieser Teilkörper ist $\mathbb{Q}(\sqrt{5})$.

Beispiel 4.6 (H 00, T3, A4) *Sei $n > 2$ eine ganze Zahl und φ die Eulersche φ-Funktion.*

a) Zeigen Sie, dass $\mathbb{Q}(cos\frac{2\pi}{n})/\mathbb{Q}$ eine Galoiserweiterung vom Grad $\frac{\varphi(n)}{2}$ ist.

b) Bestimmen Sie das neunte Kreisteilungspolynom über $\mathbb{Q}$.

c) Bestimmen sie das Minimalpolynom von $cos\frac{2\pi}{9}$ über $\mathbb{Q}$.

Lösung: *a) Es sei*

$$w = e^{2\pi i/n} = cos\frac{2\pi}{n} + i \cdot sin\frac{2\pi}{n} \in \mathbb{C}$$

die erste primitive n-te Einheitswurzel. Dann ist

$$cos\frac{2\pi}{n} = \frac{1}{2}(w + \bar{w}) = \frac{1}{2}(w + w^{-1}).$$

Deswegen genügt w über $\mathbb{Q}(cos\frac{2\pi}{n})$ der quadratischen Gleichung

$$w^2 - 2cos\frac{2\pi}{n} \cdot w + 1 = 0.$$

Weil $\mathbb{Q}(cos\frac{2\pi}{n})$ in $\mathbb{R}$ enthalten ist, kann dieser Körper nicht mit dem Kreisteilungskörper $\mathbb{Q}(\sqrt[n]{1})$ übereinstimmen. Also ist $\mathbb{Q}(\sqrt[n]{1})$ eine quadratische Erweiterung von $\mathbb{Q}(cos\frac{2\pi}{n})$. Daraus folgt

$$[\mathbb{Q}\left(cos\frac{2\pi}{n}\right) : \mathbb{Q}] = \frac{1}{2}[\mathbb{Q}(\sqrt[n]{1}) : \mathbb{Q}] = \frac{1}{2}\varphi(n).$$

Die Galoisgruppe $G(\mathbb{Q}(\sqrt[n]{1}) : \mathbb{Q})$ ist abelsch von der Ordnung $\varphi(n)$. Die Gruppe $G(\mathbb{Q}(\sqrt[n]{1}) : \mathbb{Q}(cos\frac{2\pi}{n}))$ ist Normalteiler (vom Index 2) in $G(\mathbb{Q}(\sqrt[n]{1}) : \mathbb{Q})$, weil diese Gruppe abelsch ist. Also ist der Körper $\mathbb{Q}(cos\frac{2\pi}{n})$ normal über $\mathbb{Q}$ und damit galoissch.

b) Das neunte Kreisteilungspolynom haben wir schon bestimmt. Es ist

$$\Phi_9(X) = X^6 + X^3 + 1.$$

c) Wegen

$$[\mathbb{Q}(cos\frac{2\pi}{9}) : \mathbb{Q}] = \frac{1}{2}\varphi(9) = \frac{1}{2} \cdot 6 = 3,$$

hat das Minimalpolynom von $cos\frac{2\pi}{9}$ über $\mathbb{Q}$ den Grad 3. Es sei $w = e^{2\pi i/9}$ die erste primitive 9-te Eineitswurzel. Ausgehend von

$$cos\frac{2\pi}{9} = \frac{1}{2} \cdot (w + w^8)$$

berechnen wir die Potenzen

$$\left(cos\frac{2\pi}{9}\right)^2 = \frac{1}{4} \cdot (w^2 + 2 + w^7) \quad \textit{leider nutzlos,}$$

$$\left(cos\frac{2\pi}{9}\right)^3 = \frac{1}{8} \cdot (w^3 + 3w + 3w^8 + w^6) = \frac{1}{8} \cdot (-1 + 6\,cos\frac{2\pi}{9}).$$

Also erfüllt $cos\frac{2\pi}{9}$ die Polynomgleichung

$$X^3 = \frac{3}{4}X - \frac{1}{8}, \quad \textit{bzw.} \quad X^3 - \frac{3}{4}X + \frac{1}{8} = 0.$$

Deswegen ist

$$X^3 - \frac{3}{4}X + \frac{1}{8}$$

das gesuchte Minimalpolynom.

Beispiel 4.7 *p=17. Die Galoisgruppe ist zyklisch von der Ordnung 16. Eine prime Restklasse modulo 16 ist $q = 3$. Ihre Potenzen modulo 17 sind*

$$\begin{array}{llll} q = 3, & q^2 = 9, & q^3 = 10, & q^4 = 13, \\ q^5 = 5, & q^6 = 15, & q^7 = 11, & q^8 = 16, \\ q^9 = 14, & q^{10} = 8, & q^{11} = 7, & q^{12} = 4, \\ q^{13} = 12, & q^{14} = 2, & q^{15} = 6, & q^{16} = 1. \end{array}$$

In der Galoisgruppe gibt es je eine Untergruppe der Ordnung 2, 4 und 8. Entsprechend gibt es Zwischenkörper vom Grad 2, 4 und 8.

Ist w eine primitive 17-te Einheitswurzel, so wird der Zwischenkörper vom Grad zwei erzeugt von jeder der acht-gliedrigen Perioden

$$\eta_0 := w + w^9 + w^{13} + w^{15} + w^{16} + w^8 + w^4 + w^2,$$

$$\eta_1 := w^3 + w^{10} + w^5 + w^{11} + w^{14} + w^7 + w^{12} + w^6.$$

Weil der Körper quadratisch über $\mathbb{Q}$ ist, müssen beide einer quadratischen Gleichung mit ganzen Koeffizienten genügen. Wir berechnen etwa

$$\begin{aligned} \eta_0^2 &= w^2 + w + w^9 + w^{13} + w^{15} + w^{16} + w^8 + w^4 + \\ &\quad 2 \cdot (w^{10} + w^{14} + w^{16} + 1 + w^9 + w^5 + w^3 + \\ &\quad\quad w^5 + w^7 + w^8 + 1 + w^{13} + w^{11} + \\ &\quad\quad w^{11} + w^{12} + w^4 + 1 + w^{15} + \\ &\quad\quad w^{14} + w^6 + w^2 + 1 + \\ &\quad\quad w^7 + w^3 + w + w^{12} + w^{10} + w^6) \\ &= \eta_0 + 2 \cdot (4 + \eta_0 + 2\eta_1) \\ &= \eta_0 + 2 \cdot (2 - \eta_0) \\ &= -\eta_0 + 4. \end{aligned}$$

Die Zahl η_0 ist damit eine Wurzel der quadratischen Gleichung

$$X^2 + X - 4 = 0$$

mit den beiden Lösungen

$$\eta_{0,1} = \frac{1}{2}(-1 \pm \sqrt{17}).$$

Die viergliedrigen Perioden sind

$$\xi_0 := w + w^{13} + w^{16} + w^4, \quad \xi_1 := w^3 + w^5 + w^{14} + w^{12},$$

$$\xi_2 := w^9 + w^{15} + w^8 + w^2, \quad \xi_3 := w^{10} + w^{11} + w^7 + w^6.$$

Für ξ_0 berechnen wir

$$\begin{aligned}\xi_0\eta_0 &= \xi_0^2+\xi_2\eta_0\\ &= \xi_0^2+\\ &\quad w^{10}+w^{16}+w^9+w^3+w^5+w^{11}+w^4+w^{15}+\\ &\quad w^8+w^{14}+w^7+w+w^{13}+w^2+w^{12}+w^6\\ &= \xi_0^2-1.\end{aligned}$$

Die Zahl ξ_0 genügt also über dem Körper $\mathbb{Q}(\eta_0)$ der quadratischen Gleichung

$$X^2-\eta_0X-1=0.$$

Die erste zweigliedrige Periode

$$\theta_0:=w+w^{16}$$

erfüllt

$$\begin{aligned}\theta_0^2 &= w^2+2+w^{15},\\ \theta_0\xi_0 &= w^2+w^{14}+1+w^5+1+w^{12}+w^{15}+w^3\\ &= \theta_0^2+\xi_1.\end{aligned}$$

Sie genügt also über $\mathbb{Q}(\xi_0)=\mathbb{Q}(\xi_1)$ der quadratischen Gleichung

$$X^2-\xi_0X+\xi_1=0.$$

Schließlich erfüllt w selbst die quadratische Gleichung

$$w+w^{-1}=\theta_0,\quad w^2-w\theta_0+1=0.$$

Die Rechnung für $p=17$ expliziter Spezialfall der allgemeinen Aussage:

Satz 4.7 *Ist p eine Primzahl derart, dass $p-1$ eine Zweierpotenz ist, so entsteht $\mathbb{Q}(\sqrt[p]{1})$ aus $\mathbb{Q}$ durch eine Folge quadratischer Körpererweiterungen. Insbesondere ist das reguläre p-Eck mit Zirkel und Lineal konstruierbar.*

Beweis. Die Galoisgruppe G von $\mathbb{Q}(\sqrt[p]{1})$ ist zyklisch von der Ordnung $p-1=2^m$. Die Gruppe $G\simeq\mathbb{Z}_{2^m}$ hat also eine Kette von Untergruppen

$$G\supset\mathbb{Z}_{2^{m-1}}\supset\mathbb{Z}_{2^{m-2}}\supset\ldots\supset\mathbb{Z}_4\supset\mathbb{Z}_2.$$

Zu ihnen gehört eine aufsteigende Kette von Körpererweiterungen

$$\mathbb{Q}\subset K_2\subset K_4\subset\ldots\subset K_{2^{m-2}}\subset K_{2^{m-1}}\subset\mathbb{Q}(\sqrt[2^m]{1})$$

der Körpergrade $2,4,\ldots,2^{m-2},2^{m-1},2^m$ über $\mathbb{Q}$. Jeder dieser Körper ist eine quadratische Erweiterung des vorhergehenden. □

Aufgabe 4.1 *Sind die primitiven 6-ten, bzw. 9-ten Einheitswurzeln in* $\mathbb{Q}(\sqrt[6]{1})$*, bzw. in* $\mathbb{Q}(\sqrt[9]{1})$ *linear unabhängig über* $\mathbb{Q}$*?*

Aufgabe 4.2 (F 02, T2, A3) *Sei* $\xi \in \mathbb{C}$ *eine primitive* 7*-te Einheitswurzel.*

i) Man bestimme α*, bzw.* β *in* $\mathbb{Q}(\xi)$ *so, dass* $[Q(\alpha) : \mathbb{Q}] = 2$ *und* $\mathbb{Q}(\beta) : \mathbb{Q}] = 3$ *ist.*

ii) Man bestimme jeweils das Minimalpolynom von α *und von* β*.*

Aufgabe 4.3 (F 00, T3, A3) *Sei* $\xi = e^{\frac{2\pi i}{5}}$*.*

a) Zeigen Sie, dass $\alpha = \xi + \xi^{-1}$ *einer normierten quadratischen Gleichung mit Koeffizienten aus* $\mathbb{Z}$ *genügt.*

b) Stellen Sie α^{-1} *als Polynom in* α *dar und zeigen Sie* $0 < \alpha < 1$*.*

Aufgabe 4.4 (F 00, T3, A4) *Sei* p *prim und* $f(x) = x^p - a \in \mathbb{Q}[x]$ *irreduzibel. Zeigen Sie, dass die Galoisgruppe von* $f(x)$ *über* $\mathbb{Q}$ *isomorph ist zu der Gruppe der Transformationen des Primkörpers* $\mathbb{F}_p$ *von der Form* $y \mapsto ky + l$ *mit* $k, l \in \mathbb{F}_p, k \neq 0$*.*

Aufgabe 4.5 (F 99, T2, A1) *Sei* $\zeta \in \mathbb{C}$ *eine primitive* 7*-te Einheitswurzel. Man bestimme das Minimalpolynom von* $\zeta + \zeta^2 + \zeta^4$ *über* $\mathbb{Q}$*.*

Aufgabe 4.6 (H 97, T1, A4) *Sei* $n > 1$ *eine natürliche Zahl, sei* K *ein Körper der Charakteristik Null, der eine primitive* n*-te Einheitswurzel* ζ *enthält, und sei* $K(X)$ *der Körper der rationalen Funktionen in der Unbestimmten* X *über* K*. Ferner seien* α *bzw.* β *die* K*-Automorphismen von* $K(X)$*, die durch*

$$\alpha(X) = \zeta X \text{ bzw. } \beta(X) = \frac{1}{X}$$

bestimmt sind. Sei G *die von* α, β *erzeugte Gruppe und* $G \subset K(X)$ *der Fixkörper von* G*, Zeigen Sie:*

a) G *ist die Diedergruppe der Ordnung* $2n$*.*

b) $K(X)$ *ist eine Galoiserweiterung vom Grad* $2n$ *über* F*.*

c) Das Minimalpolynom von X *über* F *ist* $T^{2n} - (X^n + X^{-n})T^n + 1$*.*

d) Es ist $F = K(X^n + X^{-n})$*.*

Aufgabe 4.7 (H 96, T1, A3) *Man bestimme (bis auf Isomorphie) die Galoisgruppe des Polynoms*

$$X^4 + X^3 + X^2 + X + 1$$

über $\mathbb{Q}$*.*

Aufgabe 4.8 (F 96, T1, A3) *Sei* p *eine Primzahl.* $\zeta = \zeta_0$ *eine primitive* p*-te Einheitswurzel über* $\mathbb{Q}$*. Sei* $\varphi : \zeta \mapsto \zeta^s$ *(wobei* $1 \leq s \leq p-1$ *und* $\overline{s}$ *erzeugt* $(\mathbb{Z}/p\mathbb{Z})^*$*) ein erzeugendes Element der Galoisgruppe* $G(\mathbb{Q}(\zeta)/\mathbb{Q})$ *des* p*-ten Kreisteilungskörpers* $\mathbb{Q}(\zeta)/\mathbb{Q}$*. Zeigen Sie: Zu jedem Teiler* d *von* $p-1$ *gibt es genau einen Zwischenkörper* M *von* $\mathbb{Q}(\zeta)/\mathbb{Q}$ *mit* $[M : \mathbb{Q}] = m$*, wobei* $p-1 = d \cdot m$ *und es gilt* $M = \mathbb{Q}(\nu_i)$ *mit* $\nu_i := \sum_{k=0}^{d-1} \zeta_{i+km} (0 =\leq i \leq m-1)$*, wobei* $\zeta_j := \varphi^j(\zeta) = \zeta^{s^j}$ *für* $j \geq 1$ *und* $\zeta_0 = \zeta$ *(i.e. jedes der Elemente* ν_i *hat die Eigenschaft, den Zwischenkörper* M *zu erzeugen).*

Aufgabe 4.9 (F 96, T3, A3) *Sei n eine natürliche Zahl und ζ_n eine primitive n-te Einheitswurzel. Bestimmen Sie alle Einheitswurzeln im Körper $\mathbb{Q}(\zeta_n)$.*

Aufgabe 4.10 (F 96, T3, A4) *Sei ζ_7 eine primitive 7. Einheitswurzel und $E := \mathbb{Q}(\zeta_7)$. Zeigen Sie:*

a) Es gibt genau eine über $\mathbb{Q}$ quadratische Teilerweiterung L in E.

b) Zeigen Sie: $L = \mathbb{Q}(\sqrt{-7})$.

Aufgabe 4.11 (H 95, T2, A1) *Sei K ein Körper, $n \geq 2$ eine natürliche Zahl und ζ eine n-te Einheitswurzel über K. Man beweise:*

a)

$$\sum_{k=0}^{n-1} \zeta^k = \begin{cases} n & \text{falls } \zeta = 1 \\ 0 & \text{sonst} \end{cases}$$

b) ζ ist genau dann primitive n-te Einheitswurzel über K, wenn gilt:

$$\forall_{i \in \{1,\ldots,n-1\}} \quad \sum_{k=0}^{n-1} \zeta^{ik} = 0$$

c) Ist $n = 2^r$ mit einer natürlichen Zahl r, so gilt für alle $a \in K$:

$$\sum_{k=0}^{n-1} a^k = \prod_{k=0}^{r-1} (1 + a^{2^k})$$

d) Sei nun p eine Fermatsche Primzahl und $K = \mathbb{Z}_p$. Seinen r, s natürliche Zahlen mit $2^{2^{r+s-1}} = p - 1$. Sei $n = 2^r$ und $\zeta = \overline{2^{2^s}} \in K$. Dann ist ζ eine primitive n-te Einheitswurzel.

e) Man bestimme eine primitive 16-te Einheitswurzel in $\mathbb{Z}_{65537}$.

Aufgabe 4.12 (F 95, T1, A3) *Sei ζ_{23} primitive 23-te Einheitswurzel in $\mathbb{C}$. Bestimmen Sie die Anzahl aller Zwischenkörper K mit $\mathbb{Q} \subset K \subset \mathbb{Q}(\zeta_{23})$, $\mathbb{Q} \neq K \neq \mathbb{Q}(\zeta_{23})$.*

4.2 Endliche Körper

Jeder endliche Körper L enthält seinen eindeutig bestimmten Primkörper K. Dieser hat eine Primzahlcharakteristik $p > 1$. Weil L endlich ist, ist insbesondere seine Dimension als K-Vektorraum endlich. Diese Dimension sei $n = [L : K]$. Eine K-Basis von L besteht dann aus n Elementen $c_1, ..., c_n \in L$. Jedes Element $c \in L$ ist eine Linearkombination $\gamma_1 c_1 + ... + \gamma_n c_n$ mit durch c eindeutig bestimmten Koeffizienten $\gamma_1, ..., \gamma_n \in K$. Durchlaufen diese n Koeffizienten unabhängig voneinander all die p Zahlen in K, so erhält man p^n verschiedene Zahlen in L. Es folgt

Satz 4.8 *Die Anzahl der Elemente eines endlichen Körpers ist eine Potenz $q = p^n$ seiner Charakteristik p.*

Die Einheitengruppe L^* hat $q-1$ Elemente. Für alle Elemente $0 \neq c \in L$ folgt daraus

$$c^{q-1} = 1.$$

Multiplizieren wir diese Gleichung mit c, so finden wir $c^q = c$. Das Element c ist Wurzel der Gleichung

$$X^q - X = 0.$$

Weil auch $c = 0$ eine Wurzel dieser Gleichung ist, genügen ihr alle q Elemente von L. Nach Vieta wird $X^q - X$ vom Polynom

$$\prod_{c \in L} (X - c)$$

geteilt. Beide Polynome sind normiert vom gleichen Grad. Also ist

$$X^q - X = \prod_{c \in L} (X - c).$$

Daraus folgt:

Satz 4.9 *Je zwei endliche Körper mit gleicher Anzahl von Elementen sind isomorph.*

Beweis. Wenn $q_1 = p_1^{n_1}$ und $q_2 = p_2^{n_2}$ die Anzahlen der Elemente in diesen beiden Körpern sind, so folgt aus $p_1^{n_1} = p_2^{n_2}$ dass $p_1 = p_2$ und $n_1 = n_2$ ist. Beide Körper entstehen also aus demselben Primkörper $\mathbb{F}_p$ durch Adjunktion aller Wurzeln des Polynoms $X^q - X$ und sind nach Satz 3.12 $\mathbb{F}_p$-isomorph. □

Das war die Eindeutigkeitsaussage. Es gilt aber auch die entsprechende Existenxaussage:

Satz 4.10 *Zu jeder Primzahlpotenz $q = p^n$ gibt es einen Körper mit q Elementen.*

Beweis. Es sei Z der Zerfällungskörper des Poynoms $X^q - X$ über $\mathbb{F}_p$. In Z liegt die Menge L aller Nullstellen dieses Polynoms. Zwei Elemente $c_1, c_2 \in Z$ gehören genau dann zu L, wenn $c_1^q = c_1$ und $c_2^q = c_2$ gilt. Daraus folgt

$$(c_1 \cdot c_2)^q = c_1^q \cdot c_2^q = c_1 \cdot c_2,$$

und für $c_2 \neq 0$

$$\left(\frac{c_1}{c_2}\right)^q = \frac{c_1^q}{c_2^q} = \frac{c_1}{c_2}.$$

Also liegen Produkte und Quotienten von Elementen aus L wieder in L. Durch wiederholte Anwendung des Frobenius-Homomorphismus findet man aber auch

$$(c_1 + c_2)^q = (c_1 + c_2)^{p^n} = c_1^{p^n} + c_2^{p^n} = c_1 + c_2.$$

Also liegen auch Summen von Elementen aus L wieder in L. Wegen $-1 \in \mathbb{F}_p \subset L$ gehören dann auch die Differenzen solcher Elemente wieder zu L. Damit ist L ein Unterkörper von Z.

Die Ableitung des Polynoms $X^q - X$ ist

$$qX^{q-1} - 1 = p^n X^{q-1} - 1 = -1 \neq 0.$$

Das Polynom $X^q - X$ ist also separabel über $\mathbb{F}_p$ und hat genau q verschiedene Nullstellen in Z. Damit hat L genau q Elemente. □

Definition 4.4 *Man nennt den nach Satz 4.10 und Satz 4.9 existierenden und bis auf $\mathbb{F}_p$-Isomorphie eindeutig bestimmten endlichen Körper der Ordnung p^n den* Galois-Körper *oder das* Galois-Feld *der Ordnung p^n und bezeichnet ihn (es) mit $GF(p^n)$.*

Die Einheitengruppe L^* des Körpers L mit $q = p^n$ Elementen ist nach Satz 2.11 zyklisch von der Ordnung $q - 1$. Ist $c \in F^*$ ein Erzeugendes dieser Gruppe, so sind alle Körperelemente $\neq 0$ in L Potenzen von c. Es folgt

Satz 4.11 (vom primitiven Element in Char p) *Jede endliche Erweiterung eines endlichen Körpers ist einfach.*

Weil der Satz vom primitiven Element jetzt auch für Galois-Erweiterungen eines endlichen Körpers richtig ist, gilt auch die Folgerung Satz 3.34 jetzt auch für Galois-Erweiterungen eines endlichen Körpers.

Im Beweis von Satz 4.10 haben wir auch gesehen, dass die Körpererweiterung $\mathbb{F}_p \subset L$ vom Grad n normal und separabel ist. Sie ist also galoissch und die Galoisgruppe hat die Ordnung $[L : \mathbb{F}_p] = n$. Wegen

$$c^p = c \text{ für alle } c \in \mathbb{F}_p$$

ist der Frobenius-Homomorphismus

$$F : L \ni c \mapsto c^p \in L$$

ein K-Automorphismus von L.

Satz 4.12 *Die Galoisgruppe $G(L : \mathbb{F}_p)$ ist zyklisch von der Ordnung n. Sie wird erzeugt vom Frobenius-Homomorphismus.*

Beweis. Die Iterierten von F sind die Homomorphismen

$$F^k : c \mapsto c^{p^k},\ k = 1, 2, ...$$

Solange $k < n$ ist, gilt für ein primitives Element $c \in L$, dass $F^k(c) \neq c$ ist. Denn andernfalls wären alle p^n Körperelemente $c \in L$ Wurzeln der Gleichung $X^{p^k} = X$. Nach Vieta geht das nicht für $k < n$. Damit haben wir $n - 1$ verschiedene, nicht-triviale $\mathbb{F}_p$-Homomorphismen F^k von L. Weil die Ordnung der Galoisgruppe n ist, besteht sie aus diesen $n - 1$ Homomorphismen und der Identität. □

Zu jedem Teiler m von n gibt es genau eine zyklische Untergruppe der Ordnung m in der Galoisgruppe. Ist $r = n/m$, so wird diese von F^r erzeugt. Diese Untergruppen bestimmen nach Satz 3.30 die Zwischenkörper zwischen $\mathbb{F}_p$ und L, also die Unterkörper von L. Daraus folgt

Satz 4.13 *Zu jedem Teiler m von n gibt es genau einen Unterkörper der Ordnung p^m. Er ist der Fixkörper des iterierten Frobenius F^m. Er besteht also aus allen $c \in L$ mit $c^{p^m} = c$. Ein Element $0 \neq c \in L$ gehört genau dann zu diesem Körper, wenn $c^{p^m-1} = 1$ ist, also wenn seine Ordnung in der Einheitengruppe $= p^m - 1$ ist.*

Alle Elemente $0 \neq c \in L = GF(p^n)$ genügen der Gleichung

$$c^{p^n-1} = 1,$$

sind also $(p^n - 1)$-te Einheitswurzeln über $\mathbb{F}_p$. Weil deren Anzahl $= p^n - 1$ ist, ist $GF(p^n)$ der $(p^n - 1)$-te Kreisteilungskörper über $\mathbb{F}_p$.

Aufgabe 4.13 *a) (Kleiner Fermat) Für jede Primzahl p und jede natürliche Zahl $n \neq 0 \, mod \, p$ ist $n^{p-1} = 1 \, mod \, p$.*

b) (Satz von Wilson) Für jede Primzahl p ist

$$(p-1)! = -1 \, mod \, p.$$

Aufgabe 4.14 *Es sei $K = \mathbb{F}_3(\sqrt{2})$. Zeigen Sie, dass*

$$\sqrt{2} \mapsto -\sqrt{2}$$

den Frobenius-Automorphismus auf K induziert.

Aufgabe 4.15 *Zeigen Sie, dass es in $\mathbb{F}_3[X]$ zwölf irreduzible Polynome vom Grad 3 gibt, und bestimmen Sie diese.*

Aufgabe 4.16 (F 01, T2, A4) *Sei $\mathbb{F}_q$ ein Körper mit q Elementen und sei $n \in \mathbb{N}$ teilerfremd zu q. Sei K ein Zerfällungskörper von $x^n - 1$ über $\mathbb{F}_q$. Man zeige $[K : \mathbb{F}_q] = \min\{k \in \mathbb{N} | n \text{ teilt } q^k - 1\}$.*

Aufgabe 4.17 (H 00, T1, A3) *Sei $K = \mathbb{F}_{2^{2000}}$ der Körper mit 2^{2000} Elementen.*

a) Wie viele Teilkörper besitzt K?

b) Wie viele erzeugende Elemente hat die Erweiterung $K|\mathbb{F}_2$? (Hinweis: Die bei der Berechnung auftretenden Potenzen von 2 müssen nicht „ausgerechnet" werden.)

Aufgabe 4.18 (H 00, T2, A1) *Seien K ein Körper mit 15625 Elementen und G seine Automorphismengruppe. Wie viele und wie große Bahnen hat G in K?*

Aufgabe 4.19 (H 00, T2, A3) *a) Sei $p \neq 2$ eine Primzahl. Zeigen Sie, dass der Körper $\mathbb{F}_{p^2}$ mit p^2 Elementen eine primitive 8-te Einheitswurzel enthält.*

b) Zeigen Sie, dass das Polynom $X^4 + 1$ über $\mathbb{Q}$ irreduzibel und über jedem endlichen Körper reduzibel ist.

Aufgabe 4.20 (H 00, T3, A3) *Sei k ein endlicher Körper und K/k eine algebraische Körpererweiterung. f und g seien irreduzible Polynome in $K[X]$ vom gleichen Grad. Zeigen Sie,dass die Körper $K[X]/(f)$ und $K[X]/(g)$ isomorph sind. (Anleitung: Nehmen Sie zunächst an, dass K ebenfalls endlich ist, und führen Sie den allgemeinen Fall darauf zurück.)*

Aufgabe 4.21 (F 00, T1, A1) *Weisen Sie für eine Primzahl p die Äquivalenz folgender Aussagen nach:*

i) $f(X) = X^2 + 2X + 2$ ist irreduzibel über dem Körper mit p^3 Elementen.

ii) $p \equiv 3 \, mod \, 4$.

Aufgabe 4.22 (F 99, T1, A2) *Bekanntlich kann man den Körper der komplexen Zahlen aus dem Körper $K := \mathbb{R}$ der reellen Zahlen wie folgt gewinnen: Man führe auf der Menge $C(K) := K \times K$ aller Paare von Elementen von K folgende Addition und Multiplikation ein:*

$$\begin{array}{lcl} (x,y) + (x',y') & := & (x+x', y+y'), \\ (x,y) \cdot (x',y') & := & (xx' - yy', xy' + yx'). \end{array}$$

Für einen beliebigen Körper K ist $C(K)$ mit den obigen Verknüpfungen nicht notwendig ein Körper, jedoch stets ein kommutativer Ring mit Einselement (dies braucht nicht bewiesen zu werden).

a) Für welche Primzahlen p ist $C(\mathbb{F}_p)$ ein Körper? (Dabei ist $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ der Körper mit p Elementen.)

b) Man zeige: Ist p eine ungerade Primzahl und $C(\mathbb{F}_p)$ kein Körper, so gibt es einen Ring-Isomorphismus

$$C(\mathbb{F}_p) \cong \mathbb{F}_p \times \mathbb{F}_p,$$

wobei die Ringstruktur auf $\mathbb{F}_p \times \mathbb{F}_p$ durch komponentenweise Addition und Multiplikation gegeben ist.

c) Ist folgende Aussage richtig: Für eine ungerade Primzahl p ist $C(\mathbb{F}_p)$ genau dann ein Körper, wenn die multiplikative Gruppe $C(\mathbb{F}_p)^*$ der Einheiten von $C(\mathbb{F}_p)$ zyklisch ist?

Aufgabe 4.23 (H 97, T1, A1) *Gegeben seien eine Primzahl p, eine natürliche Zahl n mit $q = p^n > 2$ und ein Primteiler r von $q-1$. Wie üblich bezeichne $\mathbb{F}_q$ den Körper mit q Elementen.*

a) Zeigen Sie, dass die multiplikative Gruppe $\mathbb{F}_q^\times = \mathbb{F}_q \setminus \{0\}$ ein Element γ der Ordnung r enthält und dass die Menge

$$G = \left\{ \begin{pmatrix} 1 & \alpha \\ 0 & \beta \end{pmatrix} \in GL(2, \mathbb{F}_q); \alpha \in \mathbb{F}_q, \beta \in \langle \gamma \rangle \right\}$$

eine Untergruppe der Ordnung qr von $GL(2, \mathbb{F}_q)$ ist. Dabei ist $\langle \gamma \rangle$ die von γ erzeugte Untergruppe von $\mathbb{F}_q^\times$.

b) Bestimmen Sie die Ordnungen der Elemente von G.

c) Geben Sie die Anzahl der p- und der r-Sylowgruppen von G an.

Aufgabe 4.24 (H 97, T2, A3) *Sei $K = \mathbb{F}_q$ der Körper mit $q = 2^{10}$ Elementen und $k = \mathbb{F}_2$ der Primkörper von K. Bestimmen Sie*

a) die Anzahl der erzeugenden Elemente der multiplikativen Gruppe $K^\times = K \setminus \{0\}$,
b) alle Unterkörper von K,
c) die Anzahl der primitiven Elemente von $K|k$.

Aufgabe 4.25 (H 97, T3, A3) *Sei* $L|K$ *eine endliche galoissche Erweiterung mit Galoisgruppe* G. *Sei* H *eine Untergruppe von* G. *Zeigen Sie, dass es ein* $\ell \in L$ *gibt mit* $H = \{g \in G; g(\ell) = \ell\}$.

Aufgabe 4.26 (F 97, T1, A1c)) *Welche Teilkörper besitzt der Körper mit 128 Elementen?*

Aufgabe 4.27 (H 96, T3, A3) *Sei* $p \in \mathbb{N}$ *eine Primzahl, seien* $n, m \geq 1$ *natürliche Zahlen und* K *ein Körper mit* p^n *Elementen. Man zeige:*
a) $p^m - 1$ *teilt genau dann* $p^n - 1$ *wenn* m *Teiler von* n *ist.*
b) K *enthält genau dann einen Unterkörper mit* p^m *Elementen, wenn* m *Teiler von* n *ist.*
c) In wie viele irreduzible Faktoren zerfällt das Kreisteilungspolynom Φ_{31} *über* $\mathbb{Z}/2\mathbb{Z}$?

Aufgabe 4.28 (H 95, T1, A2) *Man bestimme alle unitären Ringhomomorphismen des Ringes* $\mathbb{Z}[X]/(X^4 - 1)$ *in die Ringe* $\mathbb{Z}/(16), \mathbb{Z}/(60)$ *sowie in den Körper* $\mathbb{F}_{64}$ *mit 64 Elementen.*

Aufgabe 4.29 (H 95, T2, A3) *Sei* K *ein Körper der Charakteristik* $p > 0$ *und* $f \in K[X]$ *ein nicht-konstantes irreduzibles Polynom. Man beweise:*
a) f *ist genau dann separabel, wenn die Ableitung* $Df \neq 0$ *ist.*
b) Ist f *nicht separabel, so gibt es ein Polynom* $g \in K[X]$ *mit* $f(X) = g(X^p)$.
c) Jede endliche Körpererweiterung von K *ist separabel* $\Longleftrightarrow$ *Der Frobenius-Homomorphismus von* K *ist ein Automorphismus.*

Aufgabe 4.30 (F 94, T2, A5) *Es sei* $f(X) = X^6 + 3$, $\mathbb{F}$ *der Körper mit 7 Elementen und* L *der Zerfällungskörper von* $f(X)$ *über* $\mathbb{F}$. *Man berechne* $[L : \mathbb{F}]$.

Aufgabe 4.31 (H 93, T2, A3) *Sei* $f \in K[X]$ *ein normiertes irreduzibles Polynom über dem Körper* K, *sei* α *eine Nullstelle von* f *in einem Erweiterungskörper von* K *und es gelte* $f(\alpha+1) = 0$. *Man zeige:*
a) Der Körper K *hat positive Charakteristik.*
Ist $\mathrm{char}(K) = p$ *eine Primzahl und gilt zudem* $\alpha^p - \alpha \in K$, *so zeige man:*
b) f *stimmt mit dem Polynom* $X^p - X - \alpha^p + \alpha$ *überein.*
c) Die Erweiterung $K(\alpha)/K$ *hat eine zyklische Galoisgruppe der Ordnung* p.

Aufgabe 4.32 (H 91, T1, A4) *Es sei* K *ein endlicher Körper mit* p^n *Elementen* ($n, p \in \mathbb{N}, p$ *eine Primzahl). Man beweise:*
i) $\sigma : K \to K, a \to a^p$ *ist ein Automophimus von* K.
ii) Die Automorphismengruppe G *von* K *ist zyklisch von der Ordnung* n. *(Hinweis:* G *wird von* σ *erzeugt.)*

Aufgabe 4.33 (F 91, T1, A3) *Sei* $f = x^6 + x^4 + x^2 + 1$ *ein Polynom.*
1) Bestimmen Sie einen Zerfällungskörper von f *über den rationalen Zahlen* $\mathbb{Q}$.
2) Bestimmen Sie die Galoisgruppe von f *über* $\mathbb{Q}$.
3) Bestimmen Sie die Galoisgruppe von f *über dem Primkörper* $\mathbb{Z}_5$ *mit 5 Elementen.*

Aufgabe 4.34 (H 90, T2, A1) *Sei $\mathbb{F}_4$ der Körper mit 4 Elementen und sei*

$$R := \mathbb{F}_4[X]/(X^5 - X^2).$$

a) Wie viele Elemente besitzt R?
b) Wie viele Primideale gibt es in R?
c) Wie viele Einheiten besitzt R?
d) Wie viele Nullteiler besitzt R?

Aufgabe 4.35 (F 90, T2, A5) *K sei ein Körper der Charakteristik 2, die Polynome $f_1 = x^2 - a_1$ und $f_2 = x^2 - x - a_2$ mit $a_1, a_2 \in K$, seien über K irreduzibel, L_1 bzw. L_2 seien Zerfällungskörper von f_1 bzw. f_2. Kann es einen K-Isomorphismus von L_1 auf L_2 geben?*

4.3 Zyklische Körper

In diesem Paragraphen setzen wir zunächst voraus: Es sei K ein Körper, der alle n-ten Einheitswurzeln enthält. Dabei nehmen wir an, dass entweder K die Charakteristik 0 hat, oder dass K eine Charakteristik $p > 1$ hat und n nicht durch p teilbar ist. Dann gibt es in K also n verschiedene n-te Einheitswurzeln. Wir bezeichnen sie mit

$$w, w^2, ..., w^{n-1}, w^n = 1.$$

Wir betrachten hier die *reine Gleichung*

$$X^n - a = 0, \quad 0 \neq a \in K.$$

Ist $L \supset K$ eine Körpererweiterung, die eine Nullstelle c dieser Gleichung enthält, so enthält sie auch die insgesamt n verschiedenen Nullstellen

$$c,\ wc,\ w^2c,\ ...,\ w^{n-1}c.$$

Das Polynom $X^n - c$ ist also separabel über K. Es zerfällt über $K(c)$ in Linearfaktoren. Der Körper $K(c)$ ist damit galoisch über K.

Satz 4.14 *a) Die Galoisgruppe des Polynoms $X^n - a$ über K ist zyklisch.*
b) Ist das Polynom $X^n - a$ irreduzibel über K, dann ist die Galoisgruppe zyklisch von der Ordnung n.

Beweis. a) Jede Galois-Transformation $g \in G(K(c) : K)$ wird durch eine Transformation

$$c \mapsto w^k \cdot c, \quad k \in \mathbb{Z}_n,$$

definiert. Die Hintereinanderschaltung zweier Transformationen $c \mapsto w^k \cdot c$ und $c \mapsto w^l \cdot c$ gehört dabei zur Transformation $w^{k+l} \cdot c$. Damit wird die Galois-Gruppe eine Untergruppe der Gruppe der n-ten Einheitswurzeln. Nach Satz 2.11 ist diese Gruppe zyklisch, und die Galoisgruppe als Untergruppe einer zyklischen Gruppe ist auch wieder zyklisch.

b) Ist $X^n - a$ irreduzibel über K, so sind alle Wurzeln dieses Polynoms konjugiert über K. Die Galoisgruppe operiert transitiv auf diesen Wurzeln, und hat damit mindestens die Ordnung n. □

Von Satz 4.14 b) gilt auch die Umkehrung:

Satz 4.15 *Es sei $K \subset L$ eine galoissche Körpererweiterung mit zyklischer Galoisgruppe der Ordnung n. Dann entsteht L aus K durch Adjunktion einer n-ten Wurzel aus einem Element $a \in K$.*

Beweis. Es sei $g \in G(L:K) \simeq \mathbb{Z}_n$ ein Erzeugendes dieser Gruppe.

Für ein Element $c \in L$ bilden wir die sogenannte *Lagrangesche Resolvente*

$$(w,c) := c + wg(c) + w^2 g^2(c) + ... + w^{n-1} g^{n-1}(c).$$

Wäre diese Lagrangesche Resolvente $(w,c) = 0$, so wäre c eine Nullstelle der Abbildung

$$L \to L, \quad x \mapsto x + wg(x) + w^2 g^2(x) + ... + w^{n-1} g_{n-1}(x).$$

Setzen wir $a_\nu = w^\nu$ in Satz 3.34, so sehen wir dass diese Abbildung nicht die Nullabbildung ist. Es muss also ein $c \in L$ mit $(w,c) \neq 0$ geben. Ein solches c wählen wir.

Das Bild der Lagrangeschen Resolvente unter g ist

$$g(w,c) = g(c) + wg^2(c) + w^2 g^3(c) + ... + w^{n-1} c = (w,c)/w.$$

Die n-te Potenz $a := (w,c)^n$ bleibt also unter g, und dann unter der ganzen Galoisgruppe invariant. Deswegen liegt a in K.

Die n Konjugierten von (w,c) unter der Galoisgruppe

$$(w,c),\ (w,c)/w,\ (w,c)/w^2,\ ...,\ (w,c)/w^{n-1}$$

sind alle voneinander verschieden (weil $(w,c) \neq 0$ ist). Deswegen muss das Minimalpolynom von (w,c) über K den Grad n haben. Weil (w,c) eine Nullstelle des Polynoms $X^n - a$ ist, muss dies das Minimalpolynom von (w,c) sein. L entsteht also aus K durch Adjunktion einer (und dann auch aller) Nullstelle(n) $\sqrt[n]{a}$ von $X^n - a$. □

Beispiel 4.8 *Es sei $K = \mathbb{Q}(\sqrt{-3})$ der dritte Kreisteilungskörper über $\mathbb{Q}$. Das Polynom $f(X) = X^3 - 2$ ist irreduzibel über $\mathbb{Q}$ vom Grad drei. Deswegen kann es in K keine Nullstelle haben, und ist irreduzibel über K. Der Zerfällungskörper $L := K(\sqrt{-3}, \sqrt[3]{2})$ von f über $\mathbb{Q}$ ist zyklisch vom Grad drei über K. Die drei Konjugierten von $\sqrt[3]{2}$ über K sind*

$$\sqrt[3]{2},\ g(\sqrt[3]{2}) = \omega \cdot \sqrt[3]{2},\ g^2(\sqrt[3]{2}) = \omega^2 \cdot \sqrt[3]{2},$$

wo $\omega \in \mathbb{C}$ eine der beiden primitiven dritten Einheitswurzeln ist. Wegen

$$\sqrt[3]{2} + \omega \cdot g(\sqrt[3]{2}) + \omega^2 \cdot g^2(\sqrt[3]{2}) = (1 + \omega^2 + \omega) \cdot \sqrt[3]{2} = 0$$

ist die Lagrangesche Resolvente $(\omega, \sqrt[3]{2}) = 0$. Aber für $c = \sqrt[3]{4} = (\sqrt[3]{2})^2$ ist

$$g(c) = \omega^2 \cdot \sqrt[3]{4},\ g^2(c) = \omega \sqrt[3]{4},$$

und die Lagrangesche Resolvente ist

$$(\omega, c) = \sqrt[3]{4} + \omega \cdot \omega^2 \sqrt[3]{4} + \omega^2 \cdot \omega \sqrt[3]{4} = 3 \cdot \sqrt[3]{4} \neq 0.$$

Die dritte Potenz dieser Lagrangeschen Resolvente ist

$$a := (\omega, c)^3 = 108 \in K.$$

Und L entsteht aus K durch Adjunktion der dritten Wurzel

$$\sqrt[3]{a} = 3 \sqrt[3]{4}.$$

Wir wenden uns jetzt der Frage zu, wann die reine Gleichung $X^n - a$ über K irreduzibel ist, und zwar für den Fall, dass $n = p \neq char(K)$ eine Primzahl ist.

Satz 4.16 *Das Polynom $X^p - a \in K[X]$ ist irreduzibel über K, oder es zerfällt schon über K in Linearfaktoren.*

Beweis. Nach Satz 4.14a) ist für $L = K(\sqrt[p]{a})$ die Galoisgruppe $G(L : K)$ isomorph zu einer Untergruppe der Gruppe der p-ten Einheitswurzeln in K. Weil diese zyklisch von Primzahlordnung ist die Galoisgruppe entweder trivial, oder zyklisch von der Ordnung p.

Wenn die Galoisgruppe trivial ist, gilt $L = K$. Es gibt eine Wurzel $\sqrt[p]{a}$ in K, und weil alle p-ten Einheitswurzeln in K liegen sollten, liegen alle p-ten Wurzeln aus a schon in K. Das Polynom $X^p - a$ zerfällt über K in Linearfaktoren.

Wenn die Galoisgruppe zyklisch von der Ordnung p ist, ist jede Galoistransformation $g \in G(L : K)$ festgelegt durch das Bild $g(\sqrt[p]{a}) \in L$. Das Element $\sqrt[p]{a}$ besitzt also p verschiedene Konjugierte in L. Sein Minimalpolynom muss den Grad p haben und mit $X^p - a$ übereinstimmen. Deswegen ist dieses Polynom irreduzibel. □

Was bleibt von diesen schönen Sätzen, wenn K nicht alle n-ten Einheitswurzeln enthält?

Satz 4.17 *a) Es sei $X^n - a$ über K separabel und $L \supset K$ der Zerfällungskörper dieses Polynoms. Dann enthält L alle n-ten Einheitswurzeln und ist zyklisch über dem Zwischenkörper $K(\sqrt[n]{1})$.*

b) Es sei $L \supset K$ eine zyklische, galoissche Körpererweiterung vom Grad n. Dann ist L enthalten in einer Erweiterung, die aus $K(\sqrt[n]{1})$ durch Adjunktion aller Wurzeln einer reinen Gleichung entsteht.

Beweis. a) Das Polynom $X^n - a$ hat über L insgesamt n verschiedene Wurzeln. Ist c_1 eine dieser Wurzeln, so sind die anderen Wurzeln von der Form $w \cdot c_1$, wo w alle n-ten Einheitswurzeln durchläuft. Der Körper L enthält also den n-ten Kreisteilungskörper $K(\sqrt[n]{1})$ über K. Der Körper L entsteht aus diesem Kreisteilungskörper durch Adjunktion aller Wurzeln des Polynoms $X^n - a$ und ist nach Satz 4.14a) zyklisch über $K(\sqrt[n]{1})$.

b) Der Körper L' entstehe aus L durch Adjunktion aller n-ten Einheitswurzeln. Er enthält also den Kreisteilungs-Körper $K' := K(\sqrt[n]{1})$. Es sei $c \in L$ ein primitives Element für die Körpererweiterung $K \subset L$. Dann ist $L' = K'(c)$. Jedes $g' \in G(L' : K')$ wird definiert durch $g(c) = c'$, wo $c' \in L'$ konjugiert zu c über K' ist. Dann ist c' auch konjugiert zu c über K und liegt in L. Der Galois-Automorphismus g' induziert damit einen Galois-Automorphismus $g \in G(L : K)$. Die Abbildung $g' \mapsto g$ ist ein injektiver Gruppen-Homomorphismus $G(L' : K') \to G(L : K)$. Damit ist auch $G(L' : K')$ als Untergruppe der zyklischen Gruppe $G(L : K)$ selbst wieder zyklisch. □

Satz 4.18 *Es sei $p \neq char(K)$ eine Primzahl. Entweder ist das Polynom $X^p - a \in K[X]$ irreduzibel, oder $a = b^p, b \in K$, ist eine p-te Potenz, und*

$$X^p - b^p = (X - b) \cdot (X^{p-1} + bX^{p-2} + ... + b^{p-2}X + b^{p-1})$$

spaltet über K den Linearfaktor $X - b$ ab.

Beweis. Entweder ist $X^p - a$ irreduzibel über K oder es gibt eine Zerlegung

$$X^p - a = f(X) \cdot g(X), \quad f, g \in K[X].$$

In seinem Zerfällungskörper zerfällt $X^p - a$ in Linearfaktoren

$$X^p - a = \prod_{\nu=0}^{p-1} (X - w^\nu \alpha),$$

wo α eine p-te Wurzel von a und w eine primitive p-te Einheitswurzel ist. Auch f zerfällt hier in ein Produkt aus Linearfaktoren $X - w^\nu \alpha$. Hat f den Grad m, so ist der konstante Summand $b = f(0)$ von f von der Form

$$b = w^k \cdot \alpha^m.$$

Es folgt

$$b^p = \alpha^{p^m} = a^m.$$

Wegen $0 < m = Grad(f) < p$ ist $ggT(m, p) = 1$ und es gibt ganze Zahlen μ, π mit $\mu m + \pi p = 1$. Daraus folgt, dass

$$a = a^{\mu m} \cdot a^{\pi p} = b^{\mu p} \cdot a^{\pi p} = (b^\mu \cdot a^\pi)^p$$

eine p-te Potenz ist. □

Beispiel 4.9 (H 00, T1, A4) *a) Man zeige, dass das Polynom $f = X^{1999} - 2000$ irreduzibel über $\mathbb{Q}$ ist.*

b) Man bestimme die Ordnung der Galoisgruppe von f über $\mathbb{Q}$.

a) Die Zahl 1999 ist eine Primzahl. Ich habe das natürlich mit dem Befehl 'ifactor' von MAPLE gecheckt. MAPLE darf man in die Staatsexamensklausur nicht mitnehmen. Man muss also die Zahl 1999 durch alle Primzahlen

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 < \sqrt{1999} = 44, ...$$

teilen, und sehen, dass diese Division nie aufgeht. Mit dem Taschenrechner geht das in etwa zwei bis drei Minuten. Mit der Hand braucht man etwa eine Viertelstunde. Man ist sich da aber nie sicher. Also: In die Klausur unbedingt einen Taschenrechner mitnehmen!

Wir können deswegen Satz 4.18 anwenden. Damit ist f irreduzibel, falls nicht 2000 eine 1999-te Potenz in $\mathbb{Q}$ ist. In diesem Fall hätte $f \in \mathbb{Q}[X]$ eine Wurzel $c \in \mathbb{Q}$ und nach Satz 2.32a) wäre c sogar ein ganze Zahl. Weil c nicht $= 1$ sein kann, wäre $c \geq 2$ und

$$2000 = c^{1999} \geq (1+1)^{1999} > 1 + 1999 + \binom{1999}{2} > 2000.$$

Das geht nicht! Also ist f irreduzibel über $\mathbb{Q}$.

b) Die Galoisgruppe von f über $\mathbb{Q}$ ist die Galoisgruppe des Zerfällungskörpers L von f über $\mathbb{Q}$. Dieser Körper enthält den Kreisteilungskörper $\mathbb{Q}(\sqrt[1999]{1})$ vom Grad 1998 über $\mathbb{Q}$. Es gibt eine (eindeutig bestimmte) reelle Zahl c mit $c^{1999} = 2000$. Der Unterkörper $\mathbb{Q}(c) \subset L$ hat den Grad 1999 über $\mathbb{Q}$, weil f über $\mathbb{Q}$ irreduzibel ist. Also liegt c nicht im Kreisteilungskörper K. Nach Satz 4.18 ist das Polynom f dann auch irreduzibel über K, und $L = K(c)$ hat über K den Grad 1999. Die Galoisgruppe hat die Ordnung

$$[L : \mathbb{Q}] = [L : K] \cdot [K : \mathbb{Q}] = 1999 \cdot 1998.$$

Beispiel 4.10 *Jetzt sei*

$$f = X^{1991} - 2000 \in \mathbb{Q}[X].$$

Was kann man da sagen? Weil $1991 = 11 \cdot 181$ keine Primzahl ist, greift keiner unserer schönen Sätze. Wenn $f = g \cdot h$ über $\mathbb{Q}$ reduzibel wäre, dann wären die Polynome g und h nach Satz 2.31 schon ganzzahlig. Und der konstante Koeffizient $g_0 := g(0)$ wäre ein ganzzahliger Teiler von 2000. Weil $2000 = 2^4 \cdot 5^3$ ist, gibt es davon eine ganze Menge, nämlich die 40 Zahlen

$$\pm 2^k \cdot 5^l, \quad k = 0, ..., 4,\ l = 0, ..., 3.$$

Jetzt hilft nur noch absolute Brutalität: Es sei c die (eindeutig bestimmte) reelle Zahl mit $c^{1991} = 2000$ und $w \in \mathbb{C}$ ein primitive 1991-te Einheitswurzel. Über $\mathbb{C}$ zerfällt

$$f(X) = \prod_{m=0}^{1990} (X - w^m c)$$

in Linearfaktoren. Ist $d := Grad(g)$, so ist g_0 ein Produkt von d verschiedenen Zahlen $w^m c$ und

$$2^k \cdot 5^l = |g_0| = c^d = (\sqrt[1991]{2000})^d.$$

Daraus folgt

$$2^{1991 \cdot k} \cdot 5^{1991 \cdot l} = 2000^d = 2^{4 \cdot d} \cdot 5^{3 \cdot d},$$

$$1991 \cdot k = 4 \cdot d, \quad 1991 \cdot l = 3 \cdot d,$$
$$\frac{k}{l} = \frac{4}{3}.$$

Mit den zur Verfügung stehenden Zahlen $k = 0, ..., 4$ und $l = 0, ..., 3$ ist dies nur für $k = 4$, $l = 3$ und $d = 1991$ möglich. Es folgt

$$Grad(g) = 1991 = Grad(f),$$

und f ist irreduzibel über $\mathbb{Q}$.

Was ist jetzt die Galois-Gruppe von f über $\mathbb{Q}$? Wieder haben wir Körpererweiterungen

$$\mathbb{Q} \subset K = \mathbb{Q}(\sqrt[1991]{1}) \subset L = K(c),$$

wo L der Zerfällungskörper von f ist. Weil f irreduzibel über $\mathbb{Q}$ ist, hat $\mathbb{Q}(c)$ den Grad 1991 über $\mathbb{Q}$. Der Grad des Kreisteilungskörpers K über $\mathbb{Q}$ ist

$$\varphi(1991) = \varphi(11) \cdot \varphi(181) = 10 \cdot 180 = 1800.$$

Also liegt c nicht in K. Nach Satz 4.14 a) ist die Galoisgruppe $G(L : K)$ zyklisch von der Ordnung 1991. Der Kreisteilungskörper K ist normal in L. Deswegen ist $G(L : K) \simeq \mathbb{Z}_{1991} \subset G(L : \mathbb{Q})$ ein Normalteiler. Der Quotient $G(L : \mathbb{Q})/G(L : K)$ ist die Galoisgruppe $G(K : \mathbb{Q})$. Dies ist die prime Restklassengruppe $\mathbb{Z}^*_{1991}$. Die Galoisgruppe $G(L : \mathbb{Q})$ hat also die Ordnung

$$1991 \cdot \varphi(1991) = 1991 \cdot 1800.$$

Aufgabe 4.36 *Es sei p eine Primzahl. Zeigen Sie: Ist $a \in \mathbb{Q}$ eine p-te Potenz in $\mathbb{Q}(\sqrt[p]{1})$, dann ist a schon in $\mathbb{Q}$ eine p-te Potenz.*

Aufgabe 4.37 *Welche der folgenden Polynome sind irreduzibel in $\mathbb{Q}[X]$:*

$$X^{12} - 1, \quad X^{12} - 3, \quad X^{12} - 4, \quad X^{12} + 4,$$
$$X^{12} - 6, \quad X^{12} - 8, \quad X^{12} - 9, \quad X^{12} - 12.$$

Aufgabe 4.38 (H 98, T2, A4) *Sei n eine natürliche Zahl und w eine primitive n-te Einheitswurzel.*

a) Zeigen Sie, dass für jeden Teilkörper $K \subseteq \mathbb{C}$ der Körpergrad $[K(w) : K]$ ein Teiler von $\varphi(n)$ ist.

b) Sei d ein positiver Teiler von $\varphi(n)$. Zeigen Sie, dass es einen Körper $K \subseteq \mathbb{C}$ gibt, für den $[K(w) : K] = d$ ist.

c) Sei speziell $n = 5$. Geben Sie für jeden positiven Teiler d von $\varphi(5)$ einen Körper $K \subseteq \mathbb{C}$ an, für den $[K(w) : K] = d$ ist.

Aufgabe 4.39 (F 97, T1, A3) *Sei $G = C_q$ eine zyklische Gruppe, deren Ordnung q eine Primzahlpotenz sei. Es sei p eine Primzahl mit $p \equiv 1 \bmod q$, und $K_p = \mathbb{Q}(e^{2\pi i/p})$ sei der p-te Kreisteilungskörper.*

a) Konstruieren Sie einen surjektiven Gruppenhomomorphismus $\phi : H \to G$, wobei $H = C_{p-1}$ die zyklische Gruppe der Ordnung $p-1$ sei.

b) Begründen Sie kurz, warum H zur Galoisgruppe von K_p über $\mathbb{Q}$ isomorph ist.

c) Warum gibt es einen Teilkörper von K_p, dessen Galoisgruppe über $\mathbb{Q}$ isomorph zu G ist?

d) Nennen Sie eine normale Erweiterung von $\mathbb{Q}$ mit der Galoisgruppe C_3 über $\mathbb{Q}$.

Aufgabe 4.40 (F 97, T2, A3a)) *Zeigen Sie: Für jede Primzahl p ist die Menge der primitiven p-ten Einheitswurzeln aus $\mathbb{C}$ linear unabhängig über $\mathbb{Q}$.*

Aufgabe 4.41 (F 97, T2, A5) *Sei p eine ungerade Primzahl und q eine weitere Primzahl. Setze $f := X^p - q$.*

a) Zeigen Sie: Ist $x \in \mathbb{C}$ eine Nullstelle von f, so enthält der Körper $\mathbb{Q}(x)$ keine weitere Nullstelle von f.

b) Welche Ordnung besitzt die Galoisgruppe von f über $\mathbb{Q}$?

Aufgabe 4.42 (F 97, T3, A4) *a) Es sei ζ eine primitive fünfte Einheitswurzel und $\eta = \zeta + \zeta^{-1}$. Leiten Sie aus der Minimalgleichung von ζ über $\mathbb{Q}$ eine quadratische Gleichung von η über $\mathbb{Q}$ her. Beweisen Sie, dass $\sqrt{5}$ in $\mathbb{Q}(\zeta)$ enthalten ist.*

b) Zeigen Sie, dass $X^5 - 2$ über $\mathbb{Q}(\sqrt{5})$ irreduzibel ist.

c) Es sei E der Zerfällungskörper von $X^5 - 2$ über $\mathbb{Q}(\sqrt{5})$. Bestimmen Sie den Grad $[E : \mathbb{Q}(\sqrt{5})]$.

d) Bestimmen Sie die Galoisgruppe G von E über $\mathbb{Q}(\sqrt{5})$ und alle Zwischenkörper.

e) Ist E über $\mathbb{Q}$ normal?

Aufgabe 4.43 (F 96, T2, A5) *Seien k, ℓ, n natürliche Zahlen mit $n = k\ell$. Sei K ein Körper der Charakteristik 0, der eine primitive n-te Einheitswurzel enthält. Sei $f = X^n - a$ ein irreduzibles Polynom aus $K[X]$ und L sein Zerfällungskörper über K. Sei $z \in L$ eine Nullstelle von f. Man zeige, dass $L = K(z)$ ist. Man zeige, dass es genau einen Zwischenkörper Z von $L|K$ gibt mit $[Z : K] = k$. Man zeige, dass $Z = K(z^\ell)$ ist.*

Aufgabe 4.44 (H 95, T1, A5) *Sei $K = \mathbb{Q}(\omega)$ mit $\omega := e^{2\pi i/5}$ und F ein Zwischenkörper mit $\mathbb{Q} \subset F \subset K$, $\mathbb{Q} \neq F \neq K$.*

a) Man ermittle das Minimalpoynom von ω über $\mathbb{Q}$ und gebe eine Vektorraum-Basis von K über $\mathbb{Q}$ an.

b) Warum ist $K \supset \mathbb{Q}$ galoissch? Man berechne $\mathrm{Gal}(K/\mathbb{Q})$.

c) Man berechne das Minimalpolynom von ω über F.

Aufgabe 4.45 (H 95, T3, A4) *a) Zeigen Sie, dass $f = X^8 - 2$ über $\mathbb{Q}(i)$ irreduzibel ist.*

b) Bestimmen Sie den Zerfällungskörper L von f über $\mathbb{Q}(i)$ und berechnen Sie den Grad $[L : \mathbb{Q}(i)]$.

c) Beweisen Sie, dass die Galoisgruppe von $L/\mathbb{Q}(i)$ zyklisch ist.

d) Bestimmen Sie den Grad des Zerfällungskörpers von f über dem Grundkörper $\mathbb{Z}/17\mathbb{Z}$.

Aufgabe 4.46 (H 94, T2, A4) *Sei K ein Körper. Zeigen Sie: Ist n eine positive ganze Zahl, die kein Vielfaches der Charakteristik von K ist, und enthält K die n-ten Einheitswurzeln, so ist jede Körpererweiterung L der Form $K(\sqrt[n]{a})$, $a \in K$, von K eine Galoiserweiterung mit zyklischer Galoisgruppe* $\mathrm{Gal}(L/K)$. *Die Ordnung von* $\mathrm{Gal}(L/K)$ *ist ein Teiler von n.*

Aufgabe 4.47 (H 94, T3, A5) *Sei $k \in \mathbb{N}, k \geq 1, n = 3 \cdot 2^k$ und $\xi = e^{\frac{2\pi i}{n}} \in \mathbb{C}$. Bestimmen Sie das Minimalpolynom von ξ über $\mathbb{Q}$ explizit.*

Aufgabe 4.48 (F 94, T1, A5) *Es sei K ein Körper, der eine primitive n-te Einheitswurzel enthält. Außerdem sei $charK = p, p \neq 0$, und p sei kein Teiler von n. Es sei L ein Zerfällungskörper des Polynoms $f = (x^n - a_1)(x^n - a_2) \in K[x]$. Zeigen Sie:*

(i) $L : K$ ist eine Galois-Erweiterung.

(ii) Die Galoisgruppe $G = G(L : K)$ ist abelsch.

(iii) Die Ordnung jedes Elements von G teilt n.

Aufgabe 4.49 (F 94, T2, A4) *Man bestimme den Zerfällungskörper L des Polynoms $f(X) = X^6+3$ über $\mathbb{Q}$. Man bestimme den Grad $[L : \mathbb{Q}]$ und die Struktur der Galoisgruppe $G = \mathrm{Gal}(L|\mathbb{Q})$.*

Aufgabe 4.50 (H 93, T1, A1) *Sei K ein Körper, $n \in \mathbb{N}$ mit $\mathrm{char}K \not| n$ und L ein Zerfällungskörper des Polynoms $X^n - a \in K[X]$. Zeigen Sie: Die Galoisgruppe von $L|K$ ist isomorph zu einer Untergruppe der Gruppe der Matrizen $\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix}$ mit $x \in (\mathbb{Z}/n\mathbb{Z})^*$ und $y \in \mathbb{Z}/n\mathbb{Z}$.*

Aufgabe 4.51 (H 93, T2, A4) *Sei $\zeta = e^{\frac{2\pi i}{12}}$ eine primitive 12-te Einheitswurzel. Die relativen Automorphismen des Kreisteilungskörpers $\mathbb{Q}(\zeta)$ über $\mathbb{Q}$ sind durch die Zuordnungen*

$$\delta_k : \zeta \mapsto \zeta^k \qquad [k] \text{ prime Restklasse modulo 12 i.e. } [k] \in (\mathbb{Z}/12\mathbb{Z})^*$$

vollständig beschrieben, und die Zuordnung $j : \delta_k \mapsto k \bmod 12$ liefert einen Isomorphismus der Galoisgruppe G der Erweiterung $\mathbb{Q}(\zeta)/\mathbb{Q}$ auf $(\mathbb{Z}/12\mathbb{Z})^*$.

a) Zeigen Sie: Die Galoisgruppe von $\mathbb{Q}(\zeta)/\mathbb{Q}$ wird durch die Automorphismen $\delta_1, \delta_5, \delta_7$ und δ_{11} gebildet und ist isomorph zur Kleinschen Vierergruppe.

b) Man bestimme sämtliche Unterkörper der Erweiterung $\mathbb{Q}(\zeta)/\mathbb{Q}$ und schreibe sie als einfache Erweiterungen von $\mathbb{Q}$.

Aufgabe 4.52 (F 93, T1, A4) *Es gibt keine galoissche Erweiterung $K|\mathbb{Q}$ mit zyklischer Galoisgruppe der Odnung 4, welche $i = \sqrt{-1}$ enthält. Hinweis: Fassen Sie K als Teilkörper von $\mathbb{C}$ auf!*

Aufgabe 4.53 (F 93, T3, A3) *a) Man beweise, dass $\zeta = \frac{1+i}{\sqrt{2}}$ eine primitive achte Einheitswurzel ist.*

b) Man beweise, dass $\mathbb{Q}(\zeta) = \mathbb{Q}(\sqrt{2}, i)$ ist, und man bestimme den Grad dieses Körpers über $\mathbb{Q}$.

c) Man bestimme die Galoisgruppe $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ und alle quadratischen Teilkörper von $\mathbb{Q}(\zeta)$.

d) Es sei $\alpha = \sqrt[8]{2}$. Man berechne den Grad von $\mathbb{Q}(\alpha)$ über $\mathbb{Q}$.

e) Man beweise, dass $\mathbb{Q}(\alpha, i)$ der Zerfällungskörper des Polynoms $x^8 - 2$ über $\mathbb{Q}$ ist, und man berechne seinen Grad über $\mathbb{Q}$.

f) Man bestimme die Struktur der Galoisgruppe von $\mathbb{Q}(\alpha, i)$ über $\mathbb{Q}$ durch Angabe von Erzeugenden und definierenden Relationen.

Aufgabe 4.54 (H 92, T3, A4) *Es sei a eine primitive siebente Einheitswurzel. Dann ist ihr Minimalpolynom über $\mathbb{Q}$ bekanntlich gleich dem siebenten Kreisteilungspolynom*

$$f(X) = \sum_{j=0}^{6} X^j.$$

Ferner ist $\mathbb{Q}(a)|\mathbb{Q}$ eine galoissche Erweiterung. Mit G sei die zugehörige Galoisgruppe bezeichnet.

a) Man beweise, dass ein $\sigma \in G$ existiert mit $\sigma(a) = a^3$. Man berechne die Ordnung von σ.

b) Man beweise, dass G von σ erzeugt wird.

c) Man beweise, dass $\sigma^3(z) = \overline{z}$ ist für alle $z \in \mathbb{Q}(a)$.

d) Man bestimme die Minimalpolynome von $b := a + a^6$ und von $c := a + a^2 + a^4$ über $\mathbb{Q}$.

e) Man beweise, dass $\mathbb{Q}(b)$ und $\mathbb{Q}(c)$ die einzigen echten Zwischenkörper der Erweiterung $\mathbb{Q}(a)|\mathbb{Q}$ sind.

Aufgabe 4.55 (F 92, T2, A4) *a) Sei K ein Körper, a ein Element von K, und seien m und n zwei natürliche Zahlen $\neq 0$, die relativ prim zueinander sind. Zeigen Sie, dass das Polynom $X^{mn} - a$ genau dann irreduzibel über K ist, wenn die Polynome $g_m(X) = X^m - a$ und $g_n(X) = X^n - a$ irreduzibel über K sind.*

b) Sei p eine Primzahl, und sei a ein Element in K, das in K keine p-te Wurzel besitzt. Zeigen Sie, dass $X^p - a = g_p(X)$ irreduzibel über K ist.

Aufgabe 4.56 (H 91, T2, A3) *Für jede natürliche Zahl n sei $\mathbb{Q}_n$ der Körper, der aus $\mathbb{Q}$ durch Adjunktion aller n-ten Einheitswurzeln entsteht.*

a) Man beweise, dass für ungeraden natürlichen Zahlen n gilt: $\mathbb{Q}_n = \mathbb{Q}_{2n}$.

b) Man bestimmme alle natürlichen Zahlen n, für welche die Erweiterung $\mathbb{Q}_n|\mathbb{Q}$ den Grad 6 hat.

c) Für jede Erweiterung $\mathbb{Q}_n|\mathbb{Q}$ vom Grad 6 bestimme man den Zwischenkörper, der über $\mathbb{Q}$ den Grad 2 hat.

Aufgabe 4.57 (F 91, T2, A5) *Sei L der Zerfällungskörper des Polynoms $X^5 - 2$ über $\mathbb{Q}$. Man berechne $[L : \mathbb{Q}]$.*

Aufgabe 4.58 (F 91, T2, A6) *Sei $m > 1$ eine ungerade natürliche Zahl. Man zeige:*

a) $a \in \mathbb{C}$ ist genau dann eine primitive m-te Einheitswurzel (über $\mathbb{Q}$), wenn $-a$ eine primitive $2m$-te Einheitswurzel ist.

b) Kreisteilungspolynome erfüllen die Indentität:

$$\Phi_{2m}(X) = \Phi_m(-X).$$

Aufgabe 4.59 (F 91, T3, A1) *Sei $\zeta \in \mathbb{C}$eine primitive siebente Einheitswurzel.*

a) Zeigen Sie, dass $\sqrt{-7}$ in $\mathbb{Q}(\zeta)$ liegt.

b) Berechnen Sie das Minimalpolynom von ζ über $K = \mathbb{Q}(\sqrt{-7})$.

c) Bestimmen Sie ein Polynom $f \in K[x]$ mit $f(\zeta) = \zeta^{-1}$.

Aufgabe 4.60 (H 90, T1, A5) *Bestimmen Sie die Galois-Gruppen des Polynoms $x^4 - 5$ über den Körpern $\mathbb{Q}, \mathbb{Q}(\sqrt{5})$ und $\mathbb{Q}(i)$.*

Aufgabe 4.61 (H 90, T3, A3) *In dieser Aufgabe ist der Grundkörper $K = \mathbb{Q}(i)$. Es sei $f(X) = X^8 - 2$, α eine Nullstelle von $f(X)$ und $L := K(\alpha)$. Man beweise die folgenden Aussagen a) bis e) .*

a)$f(X)$ ist über K irreduzibel .

b) L enthält die achten Einhietswurzeln.

c) L ist Zerfällungskörper von $f(X)$ über K .

d) Es gibt genau einen Automorphismus σ von $L|K$ mit $\sigma(\alpha) = (1+i)\alpha^{-3}$.

e) Die Galoisgruppe von $L|K$ ist zyklisch und wird von dem Autormorphismus σ in Teil d) der Aufgabe erzeugt.

f) Man bestimme alle Zwischenkörper von $L|K$.

Aufgabe 4.62 (F 90, T1, A4) *a) Man gebe eine komplexe Zahl z an, so dass $\mathbb{Q}(z)/\mathbb{Q}$ eine galoissche Körpererweiterung mit einer zyklischen Galoisgruppe der Ordnung 22 ist.*

b) Man löse die gleiche Aufgabe für die zyklische Gruppe der Ordnung 11. (Insbesondere soll wie in a) ein primitives Element angegeben werden.)

Aufgabe 4.63 (F 90, T2, A4) *Es sei α eine primitive $(2n+1)$-te Einheitswurzel über $\mathbb{Q}$. Zeigen Sie:*

$$\beta = -\alpha^2$$

ist eine primitive $(4n+2)$-te Einheitswurzel. Folgern Sie daraus, dass $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$ ist.

4.4 Auflösbare Körper

Die Generalvoraussetzung für diesen Paragraphen ist:

Der Körper K habe entweder die Charakteristik 0 oder, wenn er eine Charakteristik $p > 1$ hat, dann sei er endlich.

Jedes Polynom $f \in K[X]$ ist dann separabel, und jeder Zerfällungskörper über K galoissch. Wenn das nicht der Fall ist, dann kann man die Aussagen dieses Paragraphen immer noch in modifizierter Form beweisen. Man muss dann aber so viele Ausnahmen machen, dass ich dabei einfach nicht den Überblick behalte.

Definition 4.5 *Eine galoissche Körperweiterung $K \subset L$ heiße* auflösbar, *wenn die Galoisgruppe $G(L:K)$ auflösbar ist.*

Dies ist keine Standardbezeichnung. Ich benutze sie hier, weil sie so schön in mein System passt. Ich glaube, die Standardbezeichnung ist *metazyklischer* Körper.

Wir erinnern uns: Eine Gruppe G heißt auflösbar, wenn es eine endliche Kette

$$G = G_0 \supset G_1 \supset G_2 \supset ... \supset G_{k-1} \supset G_k = \{1\}$$

von Untergruppen $G_i \subset G$ gibt derart, dass G_{i+1} Normalteiler in G_i ist, und die Faktorgruppe G_i/G_{i+1} zyklisch von Primzahlordnung ist.

Satz 4.19 *Eine galoissche Körpererweiterung $K \subset L$ ist genau dann auflösbar, wenn es eine Kette*

$$K = K_0 \subset K_1 \subset ... \subset K_{k-1} \subset K_k = L$$

von Zwischenkörpern K_i gibt derart, dass K_{i+1} normal über K_i und die Galoisgruppe $G(K_{i+1}:K_i)$ zyklisch von Primzahlordnung ist.

Bemerkung: Ist $K \subset L = K_k$ galoissch und $K_{k-1} \subset L$ normal, so ist auch $K \subset K_{k-1}$ galoissch (Satz 3.32) und damit die Erweiterung $K_{k-2} \subset K_{k-1}$ (Satz 3.29). Iteriert man dieses Argument, so sieht man, dass jede der Erweiterungen $K_i \subset K_{i+1}$ galoissch ist.

Beweis des Satzes (Induktion nach k) $\Rightarrow$: Es sei $G_1 \subset G$ ein Normalteiler und G/G_1 zyklisch von Primzahlordnung p. Zu G_1 gehört ein Zwischenkörper K_1 mit $K \subset K_1 \subset L$, der normal über K ist. Er ist dann auch galoissch über K und seine Galoisgruppe

$$G(K_1:K) = G(L:K)/G(L:K_1) = G/G_1$$

ist zyklisch von der Ordnung p. Die Galoisgruppe $G(L:K_1) = G_1 \subset G$ ist auflösbar, und die Anzahl der zur Auflösung nötigen Normalteiler ist $k-1$. Die Behauptung für $K_1 \subset L$ ist die Induktionsannahme, und daraus folgt die Behauptung für $K \subset L$.

$\Leftarrow$: Wenn der Zwischenkörper $K_1 \subset L$ normal über K ist, dann ist die zugehörige Untergruppe $G_1 := G(L:K_1)$ ein Normalteiler in G. Ist $K \subset K_1$ zyklisch von Primzahlgrad, so ist auch die Faktorgruppe $G/G_1 = G(K_1:K)$ zyklisch von Primzahlordnung. Nach Induktionsannahme für $K_1 \subset L$ gibt es eine Kette von Normalteilern

$$G_1 \supset G_2 \supset ... \supset G_{k-1} \supset G_k = \{1\},$$

in der alle sukzessiven Quotienten zyklisch von Primzahlordnung sind. Die Kette

$$G \supset G_1 \supset ... \supset G_{k-1} \supset G_k = \{1\}$$

liefert die Behauptung für G. □

Satz 4.20 *a) Die Iteration auflösbarer Körpererweiterungen ist wieder auflösbar. Genauer: Sind $K \subset L$ und $L \subset M$ auflösbare Körpererweiterungen, und ist M normal über K, so ist M auch auflösbar über K.*

b) Ist K_1 normaler Zwischenkörper einer auflösbaren Körpererweiterung $K \subset L$, so ist auch die Erweiterung $K \subset K_1$ auflösbar.

c) Der Zerfällungskörper einer reinen Gleichung $X^n - a = 0$, $a \in K$, ist auflösbar über K.

Beweis. a) Die Galoisgruppe $G(M:K)$ enthält den auflösbaren Normalteiler $G(M:L)$, und auch die Faktorgruppe $G(L:K) = G(M:K)/G(M:L)$ ist auflösbar. Nach Satz 1.39 ist damit $G(M:K)$ selbst auflösbar.

b) Die Galoisgruppe $G(K_1:K)$ ist Faktorgruppe der auflösbaren Galoisgruppe $G(L:K)$ und nach Satz 1.40 selbst auflösbar.

c) Der Zerfällungskörper Z der reinen Gleichung $X^n - a = 0$ enthält den n-ten Kreisteilungskörper $K(\sqrt[n]{1})$ als normalen Zwischenkörper. Nach Satz 4.5 ist die Galoisgruppe $G(K(\sqrt[n]{1}):K)$ abelsch, und damit auflösbar. Nach Satz 4.14 a) ist die Galoisgruppe von Z über $K(\sqrt[n]{1})$ zyklisch, und somit auflösbar. Die Behauptung folgt aus a). □

Definition 4.6 *Es sei $f \in K[X]$ ein Polynom mit Koeffizienten im Körper K. Die Gleichung*

$$f(X) = 0$$

heißt (durch Radikale) auflösbar, *wenn man alle ihre Lösungen (im Zerfällungskörper von f) durch iteriertes Wurzelziehen, beginnend mit Elementen aus K, hinschreiben kann.*

Was das heißt, ist intuitiv ziemlich klar. Es exakt zu beschreiben ist etwas umständlich: alle Nullstellen von f in seinem Zerfällungskörper liegen in einer Körpererweiterung von K, die man wie folgt erhält:

1) Man zieht aus einem Element $a \in K$ eine Wurzel $\sqrt[n]{a}$ irgend eines endlichen Grades. Die erhaltene Körpererweiterung sei K_1.

2) Man iteriert das Verfahren aus 1) endlich oft über dem jeweiligen Erweiterungskörper.

Adjungiert man an K eine n-te Wurzel $\sqrt[n]{a}$ wo $n = n_1 \cdot n_2$ keine Primzahl ist, so ist

$$\sqrt[n]{a} = \sqrt[n_1]{\sqrt[n_2]{a}}$$

zu adjungieren, indem man Adjungieren von Wurzeln von Primzahlgrad iteriert. Man kann sich deswegen beim Wurzelziehen auf Wurzeln von Primzahlgrad beschränken. Hat K eine Charakteristik $p > 1$, so liegen alle p-ten Wurzeln von Elementen aus K schon in K. Man kann deswegen weiter annehmen, dass der Primzahlgrad der zu ziehenden Wurzeln $\neq p$ ist.

Der folgende Satz ist der krönende Höhepunkt dieser Vorlesung.

Satz 4.21 (Galois) *Für ein irreduzibles Polynom $f \in K[X]$ sind äquivalent:*

i) Es gibt eine Wurzel von f, die man durch iteriertes Wurzelziehen hinschreiben kann;

ii) der Zerfällungskörper Z von f ist Zwischenkörper $K \subset Z \subset L$ einer auflösbaren Erweiterung $K \subset L$;

iii) der Zerfällungskörper Z ist selbst eine auflösbare Körpererweiterung von K;

iv) die Polynomgleichung $f(X) = 0$ ist auflösbar.

Beweis i) $\Rightarrow$ ii): Die genannte Wurzel von f liegt in einem Körper K_m, der aus K durch endlich viele Körpererweiterungen

$$K \subset K_1 \subset K_2 \subset ... \subset K_{m-1} \subset K_m$$

entsteht, wobei jede dieser Körperereiterungen $K_\mu \subset K_{\mu+1}$ Adjunktion einer $\sqrt[n_\mu]{a_\mu}$, $a_\mu \in K_\mu$, ist. Wir ersetzen nun K_1 durch den Zerfällungskörper $L_1 \supset K_1$ der reinen Gleichung $X_0^n - a_0$. Dieser Körper ist normal über K und nach Satz 4.20c) auch auflösbar über K. Als nächstes ersetzen wir K_2 durch den Zerfällungskörper L_2 des Polynoms

$$(X^{n_1} - a_1^{(1)}) \cdot (X^{n_1} - a_1^{(2)}) \cdot ... \cdot (X^{n_1} - a_1^{(i_1)}) \in K[X]$$

über K_1, wo $a_1^{(1)} = a_1, a_1^{(2)}, ..., a_1^{(i_1)} \in K_1$ die Konjugierten von $a_1 \in K_1$ über K sind. Dann ist L_2 normal über K. Der Körper L_2 entsteht aus K_1 durch sukzessive Adjunktion aller Wurzeln einer reinen Gleichung über K_1. Nach Satz 4.20c) entsteht bei jeder dieser Adjunktionen ein über dem vorhergehenden Körper auflösbarer und über K_1 normaler Zwischenkörper. Der ist nach Satz 4.20b) auch über K_1 auflösbar. Schließlich ist dann L_2 über K_1 auflösbar und über K normal. Dann ist L_2 nach Satz 4.20a) auch über K auflösbar. L_2 enthält den Körper $K_2 = K_1(\sqrt[n_1]{a_1})$ und damit das Element a_2.

Dieses Verfahren iterieren wir. Im $\mu+1$-ten Schritt ersetzen wir also den Körper $K_{\mu+1}$ durch den Zerfällungskörper über L_μ des Polynoms

$$(X^{n_\mu} - a_\mu^{(1)}) \cdot (X^{n_\mu} - a_\mu^{(2)}) \cdot ... \cdot (X^{n_\mu} - a_\mu^{(i_\mu)}),$$

wo $a_\mu^{(1)} = a_\mu, a_\mu^{(2)}, ..., a_\mu^{(i_\mu)} \in L_\mu$ die Konjugierten von a_μ über K sind. Dann enthält $L_{\mu+1}$ den Körper $K_{\mu+1}$ und damit $a_{\mu+1}$. Der Körper $L_{\mu+1}$ ist wieder auflösbar über K.

Am Schluss entsteht ein über K auflösbarer Körper $L = L_m$, der eine Nullstelle von f, und damit den Zerfällungskörper Z von f über K enthält.

ii) $\Rightarrow$ iii): Der Zerfällungskörper Z ist ein über K normaler Zwischenkörper in dem über K auflösbaren Körper L aus ii). Dann ist auch Z selbst nach Satz 4.20b) auflösbar über K.

iii) $\Rightarrow$ iv): Alle Nullstellen von f liegen in Z. Weil Z auflösbar über K ist, werden alle Elemente dieses Körpers, und damit auch alle Nullstellen von f durch iteriertes Wurzelziehen erhalten.

iv $\Rightarrow$ i) ist offensichtlich. □

Satz 4.22 (Anwendung) *Jede Gleichung zweiten, dritten oder vierten Grades ist auflösbar.*

Beweis. Die Galoisgruppe der Gleichung ist eine Untergruppe der symmetrischen Gruppe S_2, S_3, bzw. S_4. Diese Gruppen sind auflösbar (Beispiel 1.20), und damit ist es auch jede ihrer Untergruppen. □

Aufgabe 4.64 (F 95, T3, A5) *Sei F/K eine nichttriviale endliche Galoiserweiterung mit auflösbarer Galoisgruppe. Zeigen Sie, dass es einen Zwischenkörper $K \subset E \subseteq F$ gibt, so dass E/K galoissch mit abelscher Galoisgruppe ist.*

4.4.1 Gleichungen vom Grad drei

Die symmetrische Gruppe S_3 hat eine Normalreihe

$$S_3 \supset A_3 \supset \{1\}.$$

Der Zerfällungskörper Z eines Polynoms f vom Grad 3 hat entsprechend den Zwischenkörper

$$K \subset K(\sqrt{D}) \subset Z.$$

Im Allgemeinen (z.B für $f(X) = X^3 - 2$ über $K = \mathbb{Q}$) ist die Galoisgruppe G die ganze symmetrische Gruppe. Die Galoisgruppe eines irreduziblen Polynoms vom Grad drei operiert transitiv auf den drei Wurzeln. Deswegen ist die Ordnung der Galoisgruppe durch 3 teilbar. Für ein irreduzibles Polynom vom Grad drei gibt es deswegen nur die Möglichkeiten A_3 oder S_3. Wegen Satz 3.35 unterscheiden sich beide durch die Diskriminante D:

$$\begin{array}{rcl} G = A_3 & \Leftrightarrow & D \text{ ist ein Quadrat in } K, \\ G = S_3 & \Leftrightarrow & D \text{ ist kein Quadrat in } K. \end{array}$$

Beispiel 4.11 (F 01, T3, A5) *Welches sind die Galoisgruppen der Polynome* x^3-3x+3, x^3-1, x^3-3x+1 *über* $\mathbb{Q}$*?*

Lösung: *Das Polynom* x^3-3x+3 *ist irreduzibel über* $\mathbb{Q}$ *(Eisenstein zur Primzahl* 3*),* $x^3-1 = (x-1)(x^2+x+1)$ *ist reduzibel, seine Galoisgruppe ist die Galoisgruppe* $\mathbb{Z}_2$ *des dritten Kreisteilungspolynoms, und das Polynom* x^3-3x+1 *ist wieder irreduzibel. Wäre es nämlich reduzibel über* $\mathbb{Q}$*, würde es einen ganzzahligen Linearfaktor* $x-a$, $a \in \mathbb{Z}$, *abspalten. Als Teiler des konstanten Koeffizienten* 1*, kann* a *nur* $= \pm 1$ *sein. Beide Zahlen sind aber keine Nullstelle des Polynoms.*

Um die Frage bei den beiden irreduziblen Polynomen zu entscheiden, muss man für ein quadratfreies Polynom dritten Grades x^3+px+q *die Formel*

$$D = -4p^3 - 27q^2$$

für die Diskriminante kennen (s. Aufgabe 2.71). Beim ersten Polynom ist

$$D = -4 \cdot (-3)^3 - 27 \cdot 3^2 = 4 \cdot 27 - 27 \cdot 9 = -5 \cdot 27$$

kein Quadrat in $\mathbb{Q}$*. Die Galoisgruppe ist die symmetrische Gruppe* S_3*. Beim zweiten Polynom ist*

$$D = -4 \cdot (-3)^3 - 27 = 4 \cdot 27 - 27 = 3 \cdot 27 = 81 = 9^2$$

ein Quadrat in $\mathbb{Q}$*. Die Galoisgruppe ist die alternierende Gruppe* A_3*.*

Nehmen wir jetzt an, wir haben den Allgemeinfall $G = S_3$. Um zum Zerfällungskörper Z eines Polynoms

$$f(X) = X^3 + a_1X^2 + a_2X + a_3$$

zu gelangen, muss man zunächst die Wurzel der Diskriminante adjungieren. Man vereinfacht sich das Leben, wenn man zuerst durch eine Substitution $Y = X + a_1/3$ das quadratische Glied entfernt, und das Polynom auf eine quadratfreie Form

$$X^3 + pX + q$$

bringt. Nach Aufgabe 2.71 ist in diesem Fall

$$D = -4p^3 - 27q^2.$$

Über dem Zwischenkörper $K(\sqrt{D})$ hat Z die zyklische Galoisgruppe $A_3 \simeq \mathbb{Z}_3$. Der Zerfällungskörper enthält auf jeden Fall die dritten Einheitswurzeln

$$\omega = \frac{1}{2}(-1 + \sqrt{-3}) \quad \text{und} \quad \omega^2 = \frac{1}{2}(-1 - \sqrt{-3}).$$

Über $K(\sqrt{D}, \omega)$ erhält man Z durch Adjunktion einer Lagrangeschen Resolvente (ω, x).

Sind $x_1, x_2, x_3 \in Z$ die Nullstellen von f, so ist z.B.

$$(1, x_1) = x_1 + x_2 + x_3 = 0, \quad (\omega, x_1) = x_1 + \omega x_2 + \omega^2 x_3, \quad (\omega^2, x_1) = x_1 + \omega^2 x_2 + \omega x_3.$$

Nach dem Beweis von Satz 4.15 enthält $K(\sqrt{D}, \omega)$ die dritte Potenz

$$\begin{aligned}(\omega, x_1)^3 &= x_1^3 + x_2^3 + x_3^3 \\ &\quad +3\omega(x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1) + 3\omega^2(x_1 x_2^2 + x_2 x_3^2 + x_3 x_1^2) \\ &\quad +6x_1 x_2 x_3.\end{aligned}$$

Unser Ziel ist es, diese Zahl durch die elementarsymmetrischen Funktionen der Wurzeln

$$\begin{aligned}\sigma_1 &= x_1 + x_2 + x_3 = 0, \\ \sigma_2 &= x_1 x_2 + x_1 x_3 + x_2 x_3 = p, \\ \sigma_3 &= x_1 x_2 x_3 = -q\end{aligned}$$

und

$$\sqrt{D} = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3) = x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1 - (x_1 x_2^2 + x_2 x_3^2 + x_3 x_1^2)$$

auszudrücken. Mit der Newtonschen Formel (Satz 2.36) für $r = n = 3$ finden wir (wegen $s_1 = \sigma_1 = 0$)

$$\begin{aligned}s_3 &= s_2\sigma_1 - s_1\sigma_2 + 3\sigma_3 \\ &= 3\sigma_3, \\ x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1 + x_1 x_2^2 + x_2 x_3^2 + x_3 x_1^2 &= (x_1^2 + x_2^2 + x_3^2)(x_1 + x_2 + x_3) - s_3 \\ &= -3\sigma_3, \\ x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1 &= \frac{1}{2}(-3\sigma_3 + \sqrt{D}), \\ x_1 x_2^2 + x_2 x_3^2 + x_3 x_1^2 &= \frac{1}{2}(-3\sigma_3 - \sqrt{D}).\end{aligned}$$

Somit ist

$$\begin{aligned}(\omega, x_1)^3 &= 3\sigma_3 + \frac{3\omega}{2}(-3\sigma_3 + \sqrt{D}) + \frac{3\omega^2}{2}(-3\sigma_3 - \sqrt{D}) + 6\sigma_3 \\ &= \frac{27}{2}\sigma_3 + \frac{3}{2}\sqrt{-3}\sqrt{D} \\ &= -\frac{27}{2}q + \frac{3}{2}\sqrt{-3}\sqrt{D}.\end{aligned}$$

Die Zahl (ω^2, x_1) erhält man aus (ω, x_1), indem man ω und ω^2 vertauscht. Das ändert das Vorzeichen vor $\sqrt{D}$. Also ist

$$(\omega^2, x_1)^3 = -\frac{27}{2}q - \frac{3}{2}\sqrt{-3}\sqrt{D}.$$

Die dritten Wurzeln (ω, x_1) und (ω^2, x_1) sind jeweils dreier Werte fähig. Wegen

$$\begin{aligned}(\omega, x_1)(\omega^2, x_1) &= (x_1 + \omega x_2 + \omega^2 x_3)(x_1 + \omega^2 x_2 + \omega x_3) \\ &= x_1^2 + x_2^2 + x_3^2 + (\omega + \omega^2)(x_1x_2 + x_1x_3 + x_2x_3) \\ &= \sigma_1^2 - 3\sigma_2 \\ &= -3\sigma_2 \\ &= -3p\end{aligned}$$

sind sie aber nicht unabhängig, sondern so zu wählen dass

$$(\omega, x_1)(\omega^2, x_1) = -3p$$

ist. Die Wurzeln x_i selbst erhält man dann aus

$$\begin{aligned}3x_1 &= (1, x_1) + (\omega, x_1) + (\omega^2, x_1) \\ &= (\omega, x_1) + (\omega^2, x_1), \\ 3x_2 &= (1, x_1) + \omega^2(\omega, x_1) + \omega(\omega^2, x_1) \\ &= \omega^2(\omega, x_1) + \omega(\omega^2, x_1), \\ 3x_2 &= (1, x_1) + \omega(\omega, x_1) + \omega^2(\omega^2, x_1) \\ &= \omega(\omega, x_1) + \omega^2(\omega^2, x_1).\end{aligned}$$

Beispiel 4.12 *Eine kubische Gleichung mit den Nullstellen* $1, 2$ *und* -3 *ist*

$$f(X) = X^3 - 7X + 6 = 0.$$

Hier ist also

$$p = -7, \quad q = 6, \quad D = -4 \cdot (-7)^3 - 27 \cdot 6^2 = 400.$$

Damit wird

$$(\omega, x_1)^3 = -81 + 30\sqrt{-3}, \quad (\omega^2, x_1)^3 = -81 - 30\sqrt{-3}.$$

Wählen wir für (ω, x_1) eine dritte Wurzel

$$\sqrt[3]{-81+30\sqrt{-3}},$$

so ist

$$(\omega^2, x_1) = \frac{21}{\sqrt[3]{-81+30\sqrt{-3}}}.$$

Und eine Lösung der Gleichung ist

$$\frac{1}{3}((\omega, x_1)+(\omega^2, x_1)) = \frac{1}{3}\left(\sqrt[3]{-81+30\sqrt{-3}} + \frac{21}{\sqrt[3]{-81+30\sqrt{-3}}}\right).$$

Das soll eine der Wurzeln $1, 2$ oder 3 sein? So habe ich mir das Auflösen einer kubischen Gleichung aber nicht vorgestellt!

Man kommt der Sache etwas näher, wenn man den Computer ausrechnen lässt, was die dritte Wurzel numerisch ist. MAPLE liefert mit ziemlicher Präzision

$$(\omega, x_1) = 3+2\sqrt{3}i, \quad \frac{21}{(\omega, x_1)} = 3-2\sqrt{3}i.$$

Und in der Tat:

$$(3+2\sqrt{3}i)^3 = 27+54\sqrt{3}i-108-24\sqrt{3}i = -81+30\sqrt{3}i,$$

$$(3+2\sqrt{3}i)(3-2\sqrt{3}i) = 9+12 = 21.$$

Die MAPLE-Näherung ist tatsächlich exakt. Damit erhält man die Lösungen

$$x_1 = \frac{1}{3}(3+2\sqrt{3}i+3-2\sqrt{3}i) = 2,$$

$$x_2 = \frac{1}{3}(3\omega^2+2\omega^2\sqrt{3}i+3\omega-2\omega\sqrt{3}i) = \frac{1}{3}(-3+6) = 1,$$

$$x_3 = \frac{1}{3}(3\omega+2\omega\sqrt{3}i+3\omega^2-2\omega^2\sqrt{3}i) = \frac{1}{3}(-3-6) = -3.$$

Aufgabe 4.65 *Bestimmen Sie alle Nullstellen des Polynoms*

$$f(X) = X^3-7X+6$$

a) durch Probieren;
b) mit der Cardanoschen Formel (Hinweis:

$$\left(\frac{1}{6}(3-5i\sqrt{3})\right)^3 = -\frac{1}{\sqrt{3}^3}(9\sqrt{3}-10i). \quad)$$

Aufgabe 4.66 *Bestimmen Sie die Galoisgruppe der Polynome*

$$X^3 - 15X + 10 \quad \textit{und} \quad X^3 - 10X + 15$$

über $\mathbb{Q}(\sqrt[3]{1})$.

Aufgabe 4.67 (F 01, T1, A4) *Bestimmen Sie alle Teilkörper eines Zerfällungskörpers E des Polynoms $(x^3 - 3x + 1)(x^2 + 2)$ über $\mathbb{Q}$ und ein primitives Element von $E/\mathbb{Q}$.*

Aufgabe 4.68 (F 01, T2, A5) *Seien S_2 respektive S_3 die Gruppen der Permutationen von $\{1, 2\}$ resp. $\{1, 2, 3\}$. Man zeige, dass es eine Galoissche Erweiterung $K/\mathbb{Q}$ gibt mit Galoisgruppe* $\mathrm{Gal}(K/\mathbb{Q}) \simeq S_2 \times S_3$.

Aufgabe 4.69 (H 98, T1, A4) *Man gebe eine komplexe Zahl α an, für die $\mathbb{Q}(\alpha)|\mathbb{Q}$ eine Galoiserweiterung von Grad 3 ist.*

4.4.2 Gleichungen vom Grad vier

Die allgemeine Polynomgleichung vom Grad vier

$$X^4 + a_3X^3 + a_2X^2 + a_1X + a_0 = 0$$

kann wieder durch die Transformation $Y = X + a_3/4$ auf eine Form

$$X^4 + pX^2 + qX + r = 0$$

ohne einen Anteil dritten Grades gebracht werden. Diese Form legen wir jetzt zu Grunde. Wieder setzen wir voraus, dass die Gleichung die volle Gloisgruppe S_4 hat.

Die symmetrische Gruppe S_4 ist auflösbar mit einer Normalreihe

$$S_4 \supset A_4 \supset \mathbb{Z}_2 \times \mathbb{Z}_2 \supset \mathbb{Z}_2 \supset \{1\}.$$

Dazu gehören Zwischenkörper zwischen dem Grundkörper K und dem Zerfällungskörper Z der Gleichung:

$$K \subset K(\sqrt{D}) \subset K_1 \subset K_2 \subset Z.$$

Die (unbekannten) Wurzeln der Gleichung nennen wir $x_1, x_2, x_3, x_4 \in Z$. Die elementarsymmetrischen Funktionen in $x_1, ..., x_4$ sind dann

$$\begin{aligned} \sigma_1 &= 0, \\ \sigma_2 &= p, \\ \sigma_3 &= -q, \\ \sigma_4 &= r. \end{aligned}$$

K_1 ist der Fixkörper der Kleinschen Vierergruppe $\mathbb{Z}_2 \times \mathbb{Z}_2 \subset S_3$. Zu ihm gehören die drei Elemente

$$\begin{aligned}\theta_1 &:= (x_1+x_2)(x_3+x_4),\\ \theta_2 &:= (x_1+x_3)(x_2+x_4),\\ \theta_3 &:= (x_1+x_4)(x_2+x_3),\end{aligned}$$

Keines dieser drei Elemente ist invariant unter dem Dreierzyklus $(1,2,3) \in A_4$. Also gehört keines dieser Elemente zu $K(\sqrt{D})$, dem Fixkörper von A_4. Jedes für sich erzeugt den Körper K_1 über $K(\sqrt{D})$.

Unter S_4 werden die drei Elemente $\theta_1, \theta_2, \theta_3$ permutiert. Sie sind also über K untereinander konjugiert (und auch ihre einzigen Konjugierten). Deswegen genügen sie einer Polynomgleichung vom Grad drei

$$X^3 + b_2X^2 + b_1X + b_0 = 0$$

über K. Die Koeffizienten sind (bis auf das Vorzeichen) die elementarsymmetrischen Funktionen der θ_i:

$$\begin{aligned}b_2 &= -(\theta_1+\theta_2+\theta_3)\\ &= -2\sigma_2,\\ b_1 &= \theta_1\theta_2+\theta_1\theta_3+\theta_2\theta_3\\ &= (x_1+x_2)(x_3+x_4)(x_1+x_3)(x_2+x_4)+\\ &\quad (x_1+x_2)(x_3+x_4)(x_1+x_4)(x_2+x_3)+\\ &\quad (x_1+x_3)(x_2+x_4)(x_1+x_4)(x_2+x_3)\\ &= \alpha\sigma_2^2+\beta\sigma_4,\\ b_0 &= -\theta_1\theta_2\theta_3\\ &= -(x_1+x_2)(x_1+x_3)(x_1+x_4)(x_2+x_3)(x_2+x_4)(x_3+x_4)\\ &= \gamma\sigma_2^3+\delta\sigma_2\sigma_4+\epsilon\sigma_3^2.\end{aligned}$$

Die unbekannten Koeffizienten $\alpha, ..., \epsilon$ sind dabei universell, völlig unabhängig von K und der Gleichung. Sie sind am einfachsten zu bestimmen, indem wir für $x_1, ..., x_4$ spezielle Werte einsetzen:

(x_1,x_2,x_3,x_4)	θ_1	θ_2	θ_3	b_1	b_0	σ_2	σ_3	σ_4
$(1,-1,0,0)$	0	-1	-1	1	0	-1	0	0
$(1,-1,1,-1)$	0	-4	0	0	0	-2	0	1
$(1,1,-2,0)$	-4	-1	-1	$-$	4	-3	-2	0

Für α und β folgen daraus die Gleichungen

$$\alpha = 1, \quad 4\alpha+\beta = 0 \quad \Rightarrow \quad \beta = -4,$$

und für γ, δ, ϵ

$$\gamma = 0, \quad -2\delta = 0, \quad 4\epsilon = -4 \quad \Rightarrow \quad \epsilon = 1.$$

Wir haben also gefunden

$$b_1 = \sigma_2^2 - 4\sigma_4 = p^2 - 4r, \quad b_0 = \sigma_3^2 = q^2.$$

Das Minimalpolynom der θ_i hat damit die Form

$$X^3 - 2pX^2 + (p^2 - 4r)X + q^2 = 0.$$

Diese Gleichung heißt die *kubische Resolvente* der ursprünglichen Gleichung vom Grad vier.

Diese kubische Resolvente kann man, wie im letzten Abschnitt erläutert, auflösen, und erhält Formeln für θ_1, θ_2 und θ_3. Damit ist der Körper K_1 gefunden. Der Körper K_2 entsteht daraus durch Adjunktion von $x_1 + x_2$, weil dieses Element nicht unter der ganzen Kleinschen Vierergruppe invariant ist, sondern nur unter der Untergruppe $< (1,2)(3,4) > \simeq \mathbb{Z}_2$. Wegen

$$(x_1 + x_2)(x_3 + x_4) = \theta_1, \quad (x_1 + x_2) + (x_3 + x_4) = 0,$$

findet man

$$x_1 + x_2 = -(x_3 + x_4) = \sqrt{-\theta_1}$$

und ebenso

$$x_1 + x_3 = -(x_2 + x_4) = \sqrt{-\theta_2}, \quad x_1 + x_4 = -(x_2 + x_3) = \sqrt{-\theta_3}.$$

Die Vorzeichen dieser Quadratwurzeln sind aber nicht unabhängig voneinander, denn

$$\begin{aligned}
\sqrt{-\theta_1}\sqrt{-\theta_2}\sqrt{-\theta_3} &= (x_1 + x_2)(x_1 + x_3)(x_1 + x_4) \\
&= x_1^3 + x_1^2(x_2 + x_3 + x_4) + x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 \\
&= \sigma_3 \\
&= -q.
\end{aligned}$$

Aus diesen Quadratwurzeln findet man die Lösungen vermöge

$$\begin{aligned}
2x_1 &= \sqrt{-\theta_1} + \sqrt{-\theta_2} + \sqrt{-\theta_3}, \\
2x_2 &= \sqrt{-\theta_1} - \sqrt{-\theta_2} - \sqrt{-\theta_3}, \\
2x_3 &= -\sqrt{-\theta_1} + \sqrt{-\theta_2} - \sqrt{-\theta_3}, \\
2x_4 &= -\sqrt{-\theta_1} - \sqrt{-\theta_2} + \sqrt{-\theta_3}.
\end{aligned}$$

Eine Untergruppe $G \subset S_4$ kann nur dann als Galoisgruppe eines irreduziblen Polynoms über K vorkommen, wenn G transitiv auf den vier Wurzeln $x_1, ..., x_4$ operiert. Nach Aufgabe 1.32 ist dann G konjugiert zu einer der folgenden fünf Untergruppen:

- Kleinsche Vierergruppe $V = \{id, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$,
- zyklische Gruppe $< (1,2,3,4) >$,
- 2-Sylow-Untergruppe $\simeq D_4 =< V, (1,2,3,4) >$,

- alternierende Gruppe A_4,
- ganze zyklische Gruppe S_4.

Wann G eine Untergruppe von A_4 ist, wird dadurch entschieden, ob $\sqrt{D}$ im Grundkörper K liegt oder nicht. Aus obiger Liste sind nur die Untergruppen V oder A_4 Untergruppen der alternierenden Gruppe A_4. Wir sehen: Genau dann ist $G = V$ oder A_4, wenn $\sqrt{D} \in K$. Weitere Unterscheidungen erlaubt die Kenntnis der kubischen Resolvente. Auf ihren drei Wurzeln $\theta_1, \theta_2, \theta_3$ operiert die symmetrische Gruppe S_4 transitiv. Diese drei Wurzeln sind auch alle voneinander verschieden: Es ist z.B.

$$\begin{aligned}
\theta_1 - \theta_2 &= (x_1 + x_2)(x_3 + x_4) - (x_1 + x_3)(x_2 + x_4) \\
&= x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 - (x_1x_2 + x_1x_4 + x_2x_3 + x_3x_4) \\
&= x_1(x_3 - x_2) + x_4(x_2 - x_3) \\
&= (x_1 - x_4)(x_3 - x_2) \\
&\neq 0,
\end{aligned}$$

weil das Polynom vierten Grades irreduzibel vorausgesetzt ist, und seine Wurzeln deswegen alle voneinander verschieden sind.

Die Stabilisatoruntergruppe einer jeden dieser drei Wurzeln hat also den Index 3 in G, deswegen die Ordnung 8 und ist konjugiert zu einer der drei 2-Sylowgruppen $\simeq D_4$. Die Galoisgruppe G ist genau dann in einer dieser drei Gruppen enthalten, wenn sie eine Wurzel θ_i der kubischen Resolvente fest lässt. Das ist genau dann der Fall, wenn diese Wurzel im Grundkörper K liegt, und die kubische Resolvente über K reduzibel ist.

Damit kommen wir zur folgenden (beinahe vollständigen) Fallunterscheidung:

Satz 4.23 *Das Polynom vierten Grades $f \in K[X]$ sei irreduzibel. Dann gilt*

Diskriminante	*kubische Resolvente*	*Galoisgruppe*
$\sqrt{D} \notin K$	*irreduzibel*	S_4
$\sqrt{D} \notin K$	*reduzibel*	D_4 *oder* $\mathbb{Z}_4$
$\sqrt{D} \in K$	*irreduzibel*	A_4
$\sqrt{D} \in K$	*reduzibel*	V

Aufgabe 4.70 *Zeigen Sie für die Nullstellen θ_i der kubischen Resolvente*

$$\begin{aligned}
\theta_1 - \theta_2 &= (x_1 - x_4)(x_3 - x_2), \\
\theta_1 - \theta_3 &= (x_1 - x_3)(x_4 - x_2), \\
\theta_2 - \theta_3 &= (x_1 - x_2)(x_4 - x_3),
\end{aligned}$$

und folgern Sie daraus, dass die kubische Resolvente die gleiche Diskriminante hat, wie die ursprüngliche Gleichung vierten Grades.

Aufgabe 4.71 *Gegeben sei das Polynom*

$$f(X) = X^4 - 15X^2 + 10X + 24.$$

a) Bestimmen Sie seine kubische Resolvente.
b) Bestimmen Sie die Nullstellen dieser kubischen Resolvente, notfalls durch Probieren.
c) Lösen Sie die Gleichung $f(X) = 0$.

Aufgabe 4.72 *Es seien K ein Körper der Charakteristik 0 und $n \in \mathbb{N}$. Zeigen Sie, dass die Galoisgruppe des Polynoms*

$$X^{4n} + aX^{3n} + bX^{2n} + cX^n + d, \quad a, b, c, d \in K,$$

auflösbar ist.

Aufgabe 4.73 *Es sei $f(X) = X^4 - a \in \mathbb{Q}[X]$. Zeigen Sie:*
a) f ist irreduzibel genau dann, wenn a kein Quadrat und $-4a$ keine vierte Potenz in $\mathbb{Q}$ ist.
b) Wenn f irreduzibel ist, dann ist seine Galoisgruppe entweder die zyklische Gruppe $\mathbb{Z}_4$ oder die Diedergruppe D_4.

Aufgabe 4.74 (H 96, T2, A4) *Bestimmen Sie den Isomorphietyp der Galoisgruppe des Polynoms $x^4 - 13x^2 + 1$ über dem Körper der rationalen Zahlen.*

Aufgabe 4.75 (H 96, T3, A4) *Man zeige für das Polynom $f = X^4 - X + 1 \in \mathbb{Z}[X]$:*
a) f hat keine reelle Nullstelle.
b) f ist irreduzibel über $\mathbb{Q}$. (Hinweis: Reduktion modulo 2)
c) Ist $u + iv$ (mit $u, v \in \mathbb{R}$) eine Nullstelle von f in $\mathbb{C}$, so ist $g = X^3 - 4X - 1$ das Minimalpolynom von $4u^2$ über $\mathbb{Q}$.
d) Die Galoisgruppe von f über $\mathbb{Q}$ besitzt ein Element der Ordnung 3.
e) Keine Nullstelle $a \in \mathbb{C}$ von f ist, als Punkt der Zahlenebene, aus den Punkten 0 und 1 mit Zirkel und Lineal konstruierbar.

4.4.3 Gleichungen vom Grad ≥ 5

In diesem Abschnitt sei K stets ein Körper der Charakteristik $= 0$.

In Abschnitt 1.6 haben wir bewiesen: Die alternierende Gruppe A_n ist für $n \geq 5$ einfach. Sie ist offensichtlich nicht abelsch. Deswegen ist sie nicht auflösbar. Damit ist auch die Gruppe S_n, welche A_n als Untergruppe enthält, für $n \geq 5$ nicht auflösbar wegen Satz 1.40. Ob eine Gleichung vom Grad $n \geq 5$ auflösbar ist oder nicht, hängt also von der Galoisgruppe dieser Gleichung ab. Ist diese Galoisgruppe die volle symmetrische Gruppe S_n, oder die alternierende Gruppe A_n, dann kann die Gleichung nicht durch iteriertes Wurzelziehen aufgelöst werden. Es ist zu erwarten, dass dies der 'Allgemeinfall' sein wird. Aber es ist nicht ganz einfach, das präzise zu machen. Eine mögliche Form dafür ist die folgende Aussage:

Satz 4.24 (Abel) *Die allgemeine Gleichung vom Grad $n \geq 5$ über K hat die Galoisgruppe S_n.*

Hier versteht man unter der 'allgemeinen Gleichung' die Gleichung

$$X^n + u_1 X^{n-1} + ... + u_{n-1} X + u_n = 0,$$

wo $u_1, ..., u_n$ Unbestimmte über K sind. Das ist also eine Gleichung über dem Körper $K(u_1, ..., u_n)$ der rationalen Funktionen in n Unbestimmten $u_1, ..., u_n$. (Den Index an den u_i habe ich nur der Bequemlichkeit halber verändert, anders als bei der bisherigen Schreibweise von Polynomen.)

Beweis des Satzes. Wir nehmen eine neue Kollektion $x_1, ..., x_n$ von n Unbestimmten und bilden damit den Körper $K(x_1, ..., x_n)$ der rationalen Funktionen in $x_1, ..., x_n$. Auf diesem Körper operiert die symmetrische Gruppe S_n durch Permutation der x_i.

Die elementarsymmetrischen Funktionen der $x_1, ..., x_n$

$$\sigma_\nu(x_1, ..., x_n) \in K(x_1, ..., x_n)$$

erzeugen einen Teilkörper

$$K(\sigma_1, ..., \sigma_n) \subset K(x_1, ..., x_n).$$

Dieser Teilkörper ist der Quotientenkörper des Rings $K[\sigma_1, ..., \sigma_n]$ der symmetrischen Polynome in $x_1, ..., x_n$. Jedes Element des Teilkörpers ist ein Bruch p/q, wo p und q symmetrische Funktionen in den $x_1, ..., x_n$ sind. Deswegen gehört der Teilkörper zum Fixkörper der Gruppe S_n:

$$K(\sigma_1, ..., \sigma_n) \subset K(x_1, ..., x_n)^{S_n}.$$

Nun sind alle x_i Nullstellen des Polynoms

$$f(X) := X^n - \sigma_1 X^{n-1} \pm ... + (-1)^{n-1} \sigma_{n-1} X + (-1)^n \sigma_n \in K(\sigma_1, ..., \sigma_n)[X].$$

Damit ist $K(x_1, ..., x_n)$ ein Zerfällungskörper dieses Polynoms f über $K(\sigma_1, ..., \sigma_n)$ und insbesondere galoissch über diesem Teilkörper. Die Galoisgruppe

$$G = G(K(x_1, ..., x_n) : K(\sigma_1, ..., \sigma_n))$$

ist eine Untergruppe der Permutationsgruppe S_n der Wurzeln x_i von f. Wir wissen aber schon, dass die volle symmetrische Gruppe S_n auf dieser Körpererweiterung operiert. Es folgt $G = S_n$. Die Körpererweiterung $K(x_1, ..., x_n)$ ist also galoissch über dem Unterkörper $K(\sigma_1, ..., \sigma_n)$ mit Galoisgruppe S_n.

Der Körper $K(\sigma_1, ..., \sigma_n)$ ist K-isomorph zum Körper der rationalen Funktionen in den $\sigma_1, ..., \sigma_n$, und insbesondere isomorph zum Körper $K(u_1, ..., u_n)$. Auch

$$K(u_1, ..., u_n) \ni u_i \mapsto (-1)^i \sigma_i \in K(\sigma_1, ..., \sigma_n)$$

ist ein K-Isomorphismus. Unter diesem geht die oben beschriebene allgemeine Gleichung über in die Gleichung $f = 0$. Deren Galoisgruppe haben wir als die volle symmetrische Gruppe S_n identifiziert. Diese Gruppe ist dann auch die Galoisgruppe der allgemeinen Gleichung. □

Praktisch ist dieser Satz 4.24 allerdings von beschränktem Wert. Wir könnten ihn über $K = \mathbb{Q}$ anwenden, wenn wir Zahlen $u_1, ..., u_n \in \mathbb{C}$ finden könnten derart, dass

u_1 transzendet über $\mathbb{Q}$ ist (das ist kein großes Problem),

u_2 transzendent über $Q(u_1)$ ist (das ist schon ein ziemlich tiefliegendes Problem),
u_3 transzendent über $Q(u_1, u_2)$,
usw. ...
Es ist nicht-trivial, auf diese Weise ein Beispiel einer konkreten Gleichung mit Galoisgruppe S_n zu konstruieren.

Um ein konkretes Beispiel einer irreduziblen Gleichung vom Grad fünf mit Galoisgruppe S_5 zu konstruieren, geht man anders vor:

Ist $f = X^5 + ... \in \mathbb{Q}[X]$ ein irreduzibles Polynom mit Galoisgruppe G, so operiert G transitiv auf der Menge $\{x_1, ..., x_5\}$ seiner Wurzeln. Weil f separabel ist, sind diese alle voneinander verschieden. Nach dem Bahnensatz 1.2 muss G eine Permutation der Ordnung 5 enthalten. Die einzigen Permutationen der Ordnung 5 in S_n sind aber Fünferzyklen $(i_1, ..., i_5)$. Fabrizieren wir das Polynom so, dass G noch eine Transposition (j_1, j_2) enthält, so ist nach Aufgabe 1.25

$$< (i_1, ..., i_5), (j_1, j_2) >= S_5$$

die volle symmetrische Gruppe. Damit muss $G = S_5$ sein.

Die Idee besteht darin, ein irreduzibles Polynom f mit genau drei rellen Nullstellen x_1, x_2, x_3 anzugeben. Dann ist $K = \mathbb{Q}(x_1, x_2, x_3)$ ein Zwischenkörper zwischen $\mathbb{Q}$ und dem Zerfällungskörper Z, der die beiden Nullstellen x_4 und x_5 nicht enthält. Wegen

$$\begin{aligned} x_4 + x_5 &= \sigma_1(x_1, ..., x_5) - (x_1 + x_2 + x_3) \in K, \\ x_4 \cdot x_5 &= \sigma_2(x_1, ..., x_5) - (x_4 + x_5) \cdot (x_1 + x_2 + x_3) \in K \end{aligned}$$

sind x_4 und x_5 die beiden Nullstellen einer quadratischen Gleichung über K. Die Untergruppe $G(Z : K) \subset G$ vertauscht die beiden Wurzeln.

Beispiel 4.13 *Das Polynom*

$$f(X) = X^5 - 16X + 2$$

ist nach Eisenstein irreduzibel über $\mathbb{Q}$. Um die Anzahl seiner reellen Nullstellen zu finden, suchen wir die reellen Nullstellen seiner Ableitung

$$f'(x) = 5X^4 - 16.$$

Die Nullstellen von f' erfüllen

$$X^2 = \pm\frac{4}{\sqrt{5}}, \quad X = \pm 2\sqrt{\frac{\pm 1}{\sqrt{5}}}.$$

Es gibt nur die beiden reellen Nullstellen

$$y_{1,2} = \pm\frac{2}{\sqrt[4]{5}}.$$

Nun ist

$$\begin{aligned} f(y_1) &= \frac{2^5}{(\sqrt[4]{5})^5} - \frac{32}{\sqrt[4]{5}} + 2 \\ &= \frac{1}{(\sqrt[4]{5})^5} \cdot (32 - 32\sqrt[4]{5}^4 + 2(\sqrt[4]{5})^5) \\ &< \frac{1}{(\sqrt[4]{5})^5} \cdot (52 - 160) \\ &< 0, \end{aligned}$$

wegen $5 \cdot \sqrt[4]{5} < 10$, *und*

$$\begin{aligned} f(y_2) &= -\frac{2^5}{(\sqrt[4]{5})^5} + \frac{32}{\sqrt[4]{5}} + 2 \\ &= \frac{1}{(\sqrt[4]{5})^5} \cdot (-32 + 32\sqrt[4]{5}^4 + 2(\sqrt[4]{5})^5) \\ &> \frac{1}{(\sqrt[4]{5})^5} \cdot (160 - 32) \\ &> 0. \end{aligned}$$

In der negativen Nullstelle x_2 *der Ableitung ist der Funktionswert* $f(x_2)$ *positiv und in der positiven Nullstelle* x_1 *der Ableitung ist der Funktionswert* $f(x_1)$ *negativ. Nach dem Zwischenwertsatz hat* f *mindestens drei reelle Nullstellen. Nach dem Satz von Rolle liegt zwischen zwei Nullstellen auch immer mindestens eine Nullstelle der Ableitung. Also hat* f *genau drei reelle Nullstellen. Seine Galoisgruppe ist* S_5.

Aufgabe 4.76 (H 97, T2, A4) *Es sei* $f(X) = X^5 - 5X - 1 \in \mathbb{Q}[X]$.

a) Beweisen Sie, dass f *über* $\mathbb{Q}$ *irreduzibel ist.*

b) Bestimmen Sie die Anzahl der reellen Nullstellen von f.

c) Bestimmen Sie die Galoisgruppe von f *über* $\mathbb{Q}$.

5 Miszellen

Miszellen ist ein schönes Wort. Ich wollte es auch mal benutzen. Dieses Wort bezeichnet eine Anzahl verschiedener Dinge, die man noch behandeln könnte oder sollte. Es geht hier also um einige diverse Punkte, die in einigen wenigen Staatsexamensaufgaben vorkommen, die ich aber in meinen Aufbau der Algebra nicht zwanglos einordnen konnte.

5.1 Algebraischer Abschluss

Definition 5.1 *Ein Körper K heißt* algebraisch abgeschlossen, *wenn jedes Polynom $f \in K[X]$ schon über K in Linearfaktoren zerfällt.*

Äquivalente Bedingungen sind offensichtlich:
i) Jedes Polynom $f \in K[X]$ vom Grad > 0 hat eine Nullstelle in K;
ii) es gibt keine echten endlichen Körpererweiterungen von K.

Beispiel 5.1 *Der Fundamentalsatz der Algebra besagt, dass der Körper $\mathbb{C}$ algebraisch abgeschlossen ist. Die Körper $\mathbb{Q}$ und $\mathbb{R}$ sind nicht algebraisch abgeschlossen, weil das Polynom X^2+1 in diesen Körpern keine Nullstelle hat. Kein endlicher Körper ist algebraisch abgeschlossen, weil er immer echte endliche Köpererweiterungen zulässt.*

Definition 5.2 *Eine Körpererweiterung $\bar{K}$ des Körpers K heißt* algebraischer Abschluss *von K, wenn $\bar{K}$ algebraisch abgeschlossen ist, und jedes Element aus $\bar{K}$ algebraisch über K ist.*

Beispiel 5.2 *Der Körper $\mathbb{C}$ ist ein algebraischer Abschluss des Körpers $\mathbb{R}$.*

Beispiel 5.3 *Es sei $\bar{\mathbb{Q}} \subset \mathbb{C}$ die Menge aller komplexen Zahlen, welche über $\mathbb{Q}$ algebraisch sind. Nach Satz 3.6 bilden sie einen Unterkörper von $\mathbb{C}$. Dieser Körper $\bar{\mathbb{Q}}$ ist ein algebraischer Abschluss von $\mathbb{Q}$. Dazu ist zu zeigen, dass $\bar{\mathbb{Q}}$ algebraisch abgeschlossen ist: Sei etwa*

$$f(X) = a_n X^n + ... + a_1 X + a_0 \in \bar{\mathbb{Q}}[X]$$

ein Polynom. Die Körpererweiterung $\mathbb{Q} \subset \mathbb{Q}(a_0, ..., a_n)$ ist eine Folge endlicher Körpererweiterungen, und damit endlich über $\mathbb{Q}$. Weil $\mathbb{C}$ algebraisch abgeschlossen ist, besitzt f eine Nullstelle $c \in \mathbb{C}$. Diese Nullstelle ist algebraisch über $\mathbb{Q}(a_0, ..., a_n)$, damit ist $\mathbb{Q}(a_0, ..., a_n, c)$ eine endliche Körpererweiterung von $\mathbb{Q}$. Jedes Element in dieser Körpererweiterung, insbesondere das Element c, ist algebraisch über $\mathbb{Q}$. Damit gehört c zu $\bar{\mathbb{Q}}$. Also hat $f \in \bar{\mathbb{Q}}[X]$ eine Nullstelle in $\bar{\mathbb{Q}}$, und wir haben gezeigt, dass $\bar{\mathbb{Q}}$ algebraisch abgeschlossen ist.

Satz 5.1 *a) Jeder Körper K besitzt einen algebraischen Abschluss $\bar{K}$.*
b) Dieser algebraische Abschluss ist bis auf K-Isomorphie eindeutig bestimmt.

Diesen sehr allgemeinen Satz möchte ich hier in voller Allgemeinheit nicht beweisen. Der Beweis strapaziert die mathematische Logik so sehr, dass ich mich dabei etwas unwohl fühle. (S. etwa das Buch von Lorenz, der aber den Beweis praktisch wörtlich aus dem französischen Buch 'Algebre' von N. Bourbaki abgeschrieben hat.) Falls K allerdings ein Unterkörper von $\mathbb{C}$ ist, dann ist $\bar{K}$ die Menge aller über K algebraischen Zahlen $c \in \mathbb{C}$. Nach Satz 3.6 bilden sie einen Unterkörper von $\mathbb{C}$, und dass dieser algebraisch abgeschlossen ist, das sieht man ganz genau so wie wir es eben für $\bar{\mathbb{Q}}$ eingesehen haben. Das zeigt in diesem Fall die Existenz von $\bar{K}$. Der Beweis dafür, dass $\bar{K}$ bis auf K-Isomorphie eindeutig bestimmt ist, der macht allerdings wieder exzessiven Gebrauch von mir unheimlichen logischen Methoden.

Den algebraischen Abschluss eines Körpers K braucht man eigentlich auch nie. Solange man es mit einem konkreten Problem zu tun hat, geht es immer um endliche Körpererweiterungen. Und die haben immer eine normale Hülle. Und für alle praktischen Zwecke ist die genau so gut wie der algebraische Abschluss von K. Man braucht den algebraischen Abschluss $\bar{K}$ nur, wenn man überperfekte Aussagen formulieren will. Hierfür ein Beispiel:

Satz 5.2 *Es sei K ein Körper und $\bar{K}$ ein algebraischer Abschluss dieses Körpers. Eine endliche Körpererweiterung $K \subset L$ ist genau dann normal, wenn es nur einen einzigen Zwischenkörper $K \subset L' \subset \bar{K}$ gibt, der K-isomorph zu L ist.*

Beweis. $\Rightarrow$: Sei also $L = K(a_1, ..., a_n)$ normal über K. Das Minimalpolynom $p_1 \in K[X]$ von a_1 hat eine Nullstelle $a_1' \in \bar{K}$. Durch $a_1 \mapsto a_1'$ wird ein K-Isomorphismus $K(a_1) \to K(a_1') \subset \bar{K}$ definiert. Durch Induktion nach n folgt, dass es einen K-Isomorphismus $L \to L' \subset \bar{K}$ gibt.

Sei nun $K \subset L'' \subset \bar{K}$ ein anderer Zwischenkörper, der K-isomorph zu L ist. Jedes Element $c'' \in L''$ ist Bild eines Elementes $c \in L$ unter dem K-Isomorphismus $L \to L''$. Sei $c' \in L'$ das Bild von c unter $L \to L'$. Dann haben c'', c und c' dasselbe Minimalpolynom $p \in K[X]$ über K. Mit L ist auch L' normal über K. Das irreduzible Polynom p hat die Nullstelle $c' \in L'$. Über dem normalen Körper $L' \subset \bar{K}$ zerfällt p in Linearfaktoren. Nach Vieta (über dem Körper $\bar{K}$) ist c'' Nullstelle eines dieser Linearfaktoren, und gehört damit zu L'. Also gilt $L'' \subset L'$. Wegen der K-Isomorphie $L' \to L''$ gilt $[L'' : K] = [L' : K]$. Daraus folgt $L'' = L'$.

$\Leftarrow$: Es sei $K \subset L$ eine endliche Körpererweiterung, und es gebe einen einzigen Zwischenkörper $K \subset L' \subset \bar{K}$, der K-isomorph zu L ist. Zu zeigen ist, dass L, bzw. L' normal über K ist. Sei dazu $c' \in L'$ mit Minimalpolynom $p(X) \in K[X]$ über K und $c'' \in \bar{K}$ eine weitere Nullstelle von p. Dann wird also durch $c' \mapsto c''$ ein K-Isomorphismus $K(c') \to K(c'')$ definiert.

Der Körper L' entsteht aus $K(c')$ durch Adjunktion endlich vieler algebraischer Elemente $c_1', ..., c_n' \in \bar{K}$, also $L' = K(c', c_1', ..., c_n')$. Das Minimalpolynom von c_1' über $K(c')$ sei p_1'. Unter dem Isomorphismus $K(c') \to K(c'')$ geht es über in ein Polynom $p_1'' \in K(c'')[X]$. Ist $c_1'' \in \bar{K}$ eine Nullstelle von p_1'', so wird durch $c' \mapsto c''$, $c_1' \mapsto c_1''$ ein K-Isomorphismus

$$K(c', c_1') \to K(c'', c_1'') \subset \bar{K}$$

definiert. So hangelt man sich hoch, und findet schließlich einen K-Isomorphismus

$$L' = K(c', c_1', ..., c_n') \to K(c'', c_1'', ..., c_n'') \subset \bar{K}.$$

Damit ist $K(c'', c_1'', ..., c_n'')$ ein zu L' K-isomorpher Unterkörper von $\bar{K}$. Nach Voraussetzung gibt es davon nur einen einzigen, nämlich L'. Es folgt $c'' \in L'$. $\square$

Die folgenden beiden Aufgaben illustrieren eigentlich nur, dass man sehr gut ohne den Begriff des algebraischen Abschlusses auskommen kann.

Aufgabe 5.1 (H 95, T3, A3) *Es sei F ein endlicher Körper und $\bar{F}$ sein algebraischer Abschluss. Bekanntlich gibt es für jede natürliche Zahl n genau einen Zwischenkörper von $\bar{F}/F$, der über F den Grad n hat. Es sei n eine natürliche Zahl und $f \in F[X]$ irreduzibel vom Grad n. Zeigen Sie, dass der Zerfällungskörper von f über F den Grad n über F hat.*

Aufgabe 5.2 (F 90, T3, A4) *Sei p eine Primzahl und $f_p = X^p - X - 1$ ein Polynom. K sei ein algebraischer Abschluss des Körpers $\mathbb{F}_p$ mit p Elementen und $a \in K$ eine Nullstelle von f_p. Zeigen Sie:*

a) Es ist $a \notin \mathbb{F}_p$ und $f_p(a+1) = 0$.

b) $\mathbb{Z}/p\mathbb{Z}$ ist die Galoisgruppe von f_p über $\mathbb{F}_p$.

c) Als Polynom in $\mathbb{Q}[X]$ ist f_p irreduzibel.

Aufgabe 5.3 (F 02, T1, A2) *Sei Ω der algebrische Abschluss des Körpers $\mathbb{Z}/p\mathbb{Z}$, und seien K und L endliche Teilkörper von Ω mit p^r beziehungsweise p^s Elementen. α sei ein primitives element von K über $\mathbb{Z}/p\mathbb{Z}$. Zeigen sie die Äquivalenz der folgenden Aussagen:*

a) r und s sind teilerfremd.

b) Das Minimalpolynom von α über $\mathbb{Z}/p\mathbb{Z}$ ist in $L[X]$ irreduzibel.

c) $K \cap L = \mathbb{Z}/p\mathbb{Z}$.

5.2 Ganze algebraische Zahlen

Eine Zahl $c \in \mathbb{C}$ heißt algebraisch, wenn sie einer Polynomgleichung $f(c) = 0$, $f \in \mathbb{Q}[X]$, genügt. Wenn man will, kann man f normieren und auch irreduzibel annehmen. Wenn man will, kann man aber f auch mit den Nennern aller seiner Koeffizienten durchmultiplizieren und $f \in \mathbb{Z}[X]$ annehmen. Beides gleichzeitig - f normiert und ganzzahlig - kann man aber i.A. nicht erreichen.

Definition 5.3 *Eine Zahl $c \in \mathbb{C}$ heißt* ganz algebraisch, *wenn sie Nullstelle eines normierten Polynoms $\in \mathbb{Z}[X]$ ist.*

Satz 5.3 *Für $c \in C$ sind äquivalent:*

i) c ist ganz algebraisch;

ii) c ist algebraisch über $\mathbb{Q}$ und das Minimalpolynom von c über $\mathbb{Q}$ ist ganzzahlig.

Beweis. i) $\Rightarrow$ ii): Nach Voraussetzung gibt es ein normiertes Polynom $f \in \mathbb{Z}[X]$ mit $f(c) = 0$. Wenn f über $\mathbb{Q}$ reduzibel ist, gilt nach Satz 2.31 $f = g \cdot h$, wo die Polynome g und h ganzzahlig sind. Dann müssen sie aber auch beide die höchsten Koeffizienten $+1$ oder -1 haben. Ist letzteres der Fall, multiplizieren wir beide Polynome mit -1 und können also g und h normiert annehmen.

Aus $f(c) = 0$ folgt $g(c) = 0$ oder $h(c) = 0$. Wenn wir so weitermachen kommen wir nach endlich vielen Schritten zu einem über $\mathbb{Q}$ irreduziblen, normierten und ganzzahligen Polynom $p \in \mathbb{Z}[X]$ mit $p(c) = 0$. Dieses p ist dann das Minimalpolynom von c über $\mathbb{Q}$.

Die Richtung ii) $\Rightarrow$ i) ist offensichtlich. $\square$

Beispiel 5.4 *Es sei $c \in \mathbb{Q}$ eine ganze algebraische Zahl. Das Minimalpolynom von c über $\mathbb{Q}$ ist dann $X - c$. Wenn dieses Polynom ganzzahlig ist, muss $c \in \mathbb{Z}$ gelten. Die ganzen algebraischen Zahlen in $\mathbb{Q}$ sind also genau die ganzen Zahlen.*

Beispiel 5.5 *Wann ist eine Zahl $c = r + s \cdot i \in \mathbb{Q}(i)$, $r, s \in \mathbb{Q}$, ganz algebraisch? Wenn $s = 0$ ist, muss sie nach dem vorhergehenden Beispiel selbst ganz sein. Nehmen wir also $s \neq 0$ an. Aus*

$$c^2 = r^2 - s^2 + 2rs \cdot i = r^2 - s^2 + 2rs \cdot \frac{c - r}{s} = r^2 - s^2 - 2r^2 + 2r \cdot c$$

folgt, dass c Nullstelle des quadratischen Polynoms

$$p(X) = X^2 - 2r \cdot X + r^2 + s^2 \in \mathbb{Q}[X]$$

ist. Dieses Polynom p ist dann auch das Minimalpolynom von c über $\mathbb{Q}$. Wenn es ganzzahlig ist, muss $2r \in \mathbb{Z}$ gelten. Dann gibt es zwei Möglichkeiten:

Entweder ist $r \in \mathbb{Z}$. Weil auch $r^2 + s^2$ ganz ist, folgt daraus $s^2 = (r^2 + s^2) - r^2 \in \mathbb{Z}$. Dann muss auch $s \in \mathbb{Z}$ ganz sein.

Oder es ist $r = a/2$ mit $a \in \mathbb{Z}$. Daraus folgt

$$(2s)^2 = 4(r^2 + s^2) - a^2 \in \mathbb{Z},$$

und $b = 2s \in \mathbb{Z}$. Dann ist aber

$$r^2 + s^2 = \frac{1}{4}(a^2 + b^2) \in \mathbb{Z},$$

d.h.,

$$a^2 + b^2 \equiv 0 \, mod \, 4.$$

Die quadratischen Reste modulo 4 sind aber nur 0 und 1. Dann kann diese letzte Bedingung nur erfüllt sein, wenn a^2 und b^2 beide durch 4 teilbar sind. In Wirklichkeit waren also auch hier r und s ganz.

Die ganzen algebraischen Zahlen in $\mathbb{Q}(i)$ sind also genau die Zahlen $r + s \cdot i$, wo beide Zahlen r und s ganz sind, d.h. also, genau die ganzen Gaußschen Zahlen.

Beispiel 5.6 *Jede Einheitswurzel $w \in \mathbb{C}$ mit $w^n = 1$ ist ganz-algebraisch. Sie ist ja Nullstelle des normierten ganzzahligen Polynoms $X^n - 1$.*

Beispiel 5.7 *Noch ein Beispiel für Zahlen, die nicht ganz-algebraisch sind: Dazu sei $p > 2$ eine Primzahl, $w \neq 1$ eine p-te Einheitswurzel und $n \in \mathbb{Z}$ nicht durch p teilbar. Ich behaupte:*

$$b := \frac{n}{1 - w}$$

ist nicht ganz-algebraisch. Es ist nämlich

$$w = 1 - \frac{n}{b}$$

und

$$(1 - \frac{n}{b})^p = 1, \quad (b - n)^p = b^p.$$

Deswegen ist b Nullstelle des Polynoms

$$f(X) := (X - n)^p - X^p = -npX^{p-1} + n^2 \binom{p}{2} X^{p-2} \pm ... + (-n)^{p-1} pX + (-n)^p \in \mathbb{Z}[X].$$

Alle Koeffizienten bis auf den letzten sind duch p teilbar und der erste ist nicht durch p^2 teilbar. Nach dem reziproken Eisenstein (Beispiel 2.36) ist f irreduzibel. Deswegen ist

$$\frac{1}{-np} f(X) = ... + \frac{(-n)^{p-1}}{p}$$

das Minimalpolynom von b. Weil n nicht durch p teilbar ist, hat dieses Polynom einen nicht-ganzen konstanten Koeffizienten. Das Minimalpolynom von b ist nicht ganzzahlig, und b ist nicht ganz-algebraisch.

Satz 5.4 *Für eine Zahl $c \in \mathbb{C}$ sind äquivalent:*
i) c ist ganz algebraisch;
ii) es gibt eine endlich erzeugte additive Untergruppe U von $(\mathbb{C}, +)$ mit:
a) $\mathbb{Z} \subset U$,
b) U wird durch c in sich selbst multipliziert, d.h., es ist $c \cdot u \in U$ für alle $u \in U$.

Beweis. i) $\Rightarrow$ ii): Es sei

$$p(X) = X^n + a_{n-1}X^{n-1} + ... + a_1 X + a_0, \quad a_\nu \in \mathbb{Z},$$

das Minimalpolynom von c. Dann gehört also

$$c^n = -(a_0 + a_1 c + ... + a_{n-1} c^{n-1})$$

zur Untergruppe

$$U := \mathbb{Z} + \mathbb{Z} \cdot c + ... + \mathbb{Z} \cdot c^{n-1} \subset \mathbb{C}.$$

Jedes Element $u \in U$ hat die Form

$$u = m_0 + m_1 c + ... + m_{n-1} c^{n-1}, \quad m_0, ..., m_{n-1} \in \mathbb{Z}.$$

Und wegen $c^n \in U$ gehört auch

$$c \cdot u = m_0 c + m_1 c^2 + ... + m_{n-1} c^n$$

wieder zu U.

ii) $\Rightarrow$ i): Es sei

$$U = \mathbb{Z}u_1 + ... + \mathbb{Z}u_n \subset \mathbb{C}$$

eine endlich-erzeugte Untergruppe mit $\mathbb{Z} \subset U$ und $c \cdot U \subset U$. Dann ist also für $i = 1, ..., n$

$$c \cdot u_i = a_{i,1}u_1 + ... + a_{i,n}u_n, \quad a_{i,\nu} \in \mathbb{Z}.$$

Das lineare Gleichungssystem

$$\begin{array}{ccccccccc} (a_{1,1}-c)x_1 & + & a_{1,2}x_2 & + & ... & + & a_{1,n}x_n & = & 0 \\ a_{2,1}x_1 & + & (a_{2,2}-c)x_2 & + & ... & + & a_{2,n}x_n & = & 0 \\ & & & & & & & \vdots & \\ a_{n,1}x_1 & + & a_{n,2}x_2 & + & & + & (a_{n,n}-c)x_n & = & 0 \end{array}$$

hat also die Lösung $(x_1, ..., x_n) = (u_1, ..., u_n)$. Wegen $1 \in U$ können nicht alle $u_1 = ... = u_n = 0$ sein. Die Lösung ist also nicht-trivial und die Determinante

$$det(a_{i,j} - c\delta_{i,j})$$

verschwindet. Also ist c ein Eigenwert der ganzzahligen Matrix $(a_{i,j})$ und damit Nullstelle von deren charakteristischem Polynom $det(a_{i,j} - X \cdot \delta_{i,j})$. Dieses Polynom ist ganzzahlig und (bis eventuell auf das Vorzeichen) normiert, deswegen ist c ganz algebraisch. □

Satz 5.5 *Es sei $K \subset \mathbb{C}$ ein Teilkörper. Dann bilden die ganzen algebraischen Zahlen in K einen Unterring von K.*

Beweis. Es genügt, die Aussage für $K = \mathbb{C}$ zu beweisen. Denn wenn die ganzen algebraischen Zahlen einen Unterring von $\mathbb{C}$ bilden, dann ist der Durchschnitt dieses Unterrings mit K ein Unterring von K.

Nun seien c_1 und $c_2 \in \mathbb{C}$ ganz algebraisch. Wir müssen zeigen: Auch $c_1 + c_2$ und $c_1 \cdot c_2$ sind dies. Dazu seien U_1 und $U_2 \subset \mathbb{C}$ endlich erzeugte Untergruppen mit $\mathbb{Z} \subset U_i$ und $c_i \cdot U_i \subset U_i$.

Wir betrachten die Menge

$$U_1 \cdot U_2 =< \{u_1 \cdot u_2 : \ u_i \in U_i\} >\subset \mathbb{C}.$$

Sie ist eine Untergruppe von $\mathbb{C}$, die $\mathbb{Z}$ enthält. Sind

$$u_{1,1}, ..., u_{1,m} \in U_1, \quad u_{2,1}, ..., u_{2,n} \in U_2$$

Erzeugendensysteme dieser Gruppen, so ist

$$\{u_{1,i} \cdot u_{2,j}, \ i = 1, ..., m, \ j = 1, ..., n\}$$

ein endliches Erzeugendensystem von $U_1 \cdot U_2$. Wegen $c_1 \cdot u_{1,i} \in U_1$ und $c_2 \cdot u_{2,j} \in U_2$ gilt

$$c_1 \cdot (U_1 \cdot U_2) \subset U_1 \cdot U_2 \text{ und } c_2 \cdot (U_1 \cdot U_2) \subset U_1 \cdot U_2.$$

Daraus folgt dann auch

$$(c_1 + c_2) \cdot (U_1 \cdot U_2) \subset U_1 \cdot U_2 \text{ und } (c_1c_2) \cdot (U_1 \cdot U_2) \subset U_1 \cdot U_2.$$

□

Aufgabe 5.4 (F 92, T1, A3a)) *Zeigen Sie: Ist $z \in \mathbb{C}$ algebraisch über $\mathbb{Q}$, dann gibt es ein $q \in \mathbb{Z}$ mit $q \neq 0$ und $q \cdot z$ ganz algebraisch über $\mathbb{Q}$.*

5.3 Norm und Spur

Es sei $K \subset L$ eine endliche Körpererweiterung und $c \in L$. Die Multiplikation mit c

$$m_c : L \ni x \mapsto c \cdot x \in L$$

ist eine Abbildung $L \to L$. Wegen

$$m_c(x+y) = m_c(x) + m_c(y), \quad m_c(k \cdot x) = k \cdot m_c(x) \text{ für } k \in K$$

ist m_c sogar eine K-lineare Abbildung des K-Vektorraums L in sich.

Definition 5.4 *Die* Norm $N_{L/K}(c)$ *des Elementes $c \in L$ über K ist die Determinante der Abbildung $m_c : L \to L$, die* Spur $Tr_{L/K}(c)$ *des Elementes $c \in L$ über K ist die Spur dieser Abbildung.*

Zur Erinnerung: Jede lineare Abbildung eines n-dimensionalen K-Vektorraums in sich kann nach Wahl einer Basis durch eine darstellende $n \times n$-Matrix beschrieben werden. Deren Determinante und Spur sind unabhängig von der gewählten Basis und heißen die Determinante, bzw. Spur der linearen Abbildung.

Satz 5.6 *Für $0 \neq c \in L$ ist stets*

$$N_{L/K}(c) \neq 0.$$

Beweis. Die Multiplikation m_c ist eine invertierbare lineare Abbildung mit der Inversen $m_{c^{-1}}$. □

Beispiel 5.8 *Ist $c \in K \subset L$ eine Körpererweiterung vom Grad n, so wird m_c durch eine Diagonalmatrix mit dem einzigen Eintrag c beschrieben. Es folgt*

$$N_{L/K}(c) = c^n, \quad Tr_{L/K}(c) = n \cdot c,$$

wo $n = [L : K]$.

Satz 5.7 *Es sei $K \subset L$ eine endliche Körpererweiterung und c schon in einem Zwischenkörper Z, $K \subset Z \subset L$, enthalten. Dann ist*

$$N_{L/K}(c) = (N_{Z/K}(c))^{[L:Z]}, \quad Tr_{L/K}(c) = [L : Z] \cdot Tr_{Z/K}(c).$$

Beweis. Es sei $z_1, ..., z_m$ eine Körperbasis von Z über K und $C = (c_{i,j})_{i,j=1,...,m}$ eine darstellende Matrix von $m_c : Z \to Z$. Das heißt also

$$c \cdot z_j = \sum_{i=1}^{m} c_{i,j} z_i.$$

Weiter sei $l_1, ..., l_n \in L$, $n = [L : Z]$, eine Körperbasis von L über Z. Nach dem Beweis von Satz 3.1 ist dann

$$z_1 l_1, z_2 l_2, ..., z_m l_1, z_1 l_2, ..., z_m l_n \in L$$

eine Körperbasis von L über K. Wegen

$$c \cdot z_j l_\nu = (\sum_{i=1}^{m} c_{i,j}) z_i l_\nu = \sum_{i=1}^{m} c_{i,j}(z_i x_\nu)$$

bildet $m_c : L \to L$ jedes Element $z_j l_\nu$ auf eine Linearkombination der $z_1 l_\nu, ..., z_m l_\nu$ ab. Die darstellende Matrix von $m_c : L \to L$ ist eine direkte Matrizensumme

$$D = \left(\begin{array}{cccc} C & 0 & ... & 0 \\ 0 & C & & \\ \vdots & & \ddots & \\ 0 & & & C \end{array} \right) \left. \begin{array}{c} \\ \\ \\ \\ \end{array} \right\} n$$

aus n Kopien der Matrix C. Es folgt

$$N_{L/K}(c) = det(D) = det(c)^n, \quad Tr_{L/k}(c) = n \cdot Tr(c) = n \cdot Tr_{K/L}(c).$$

□

Satz 5.8 *Es seien $c_1, c_2 \in L$ zwei Elemente des endlichen Erweiterungskörpers L von K. Dann gilt*

$$N_{L/K}(c_1 \cdot c_2) = N_{L/K}(c_1) \cdot N_{L/K}(c_2), \quad Tr_{L/K}(c_1 + c_2) = Tr_{L/K}(c_1) + Tr_{L/K}(c_2).$$

Beweis. Sind C_1, bzw. C_2 darstellende Matrizen von m_{c_1}, bzw. m_{c_2} bezüglich einer K-Basis von L, so ist $C_1 \cdot C_2$ die darstellende Matrix von $m_{c_1 \cdot c_2} = m_{c_1} \circ m_{c_2}$ und $C_1 + C_2$ die darstellende Matrix von $m_{c_1 + c_2} = m_{c_1} + m_{c_2}$. Es ist $det(C_1 \cdot C_2) = det(C_1) \cdot det(C_2)$ und $Tr(C_1 + C_2) = Tr(C_1) + Tr(C_2)$. □

Satz 5.9 *Es sei $L = K(c)$ der Erweiterungskörper, der aus K durch Adjunktion des algebraischen Elementes c mit Minimalpolynom*

$$p(X) = X^n + a_{n-1} X^{n-1} + ... + a_1 X + a_0$$

entsteht. Dann ist

$$N_{L/K}(c) = (-1)^n a_0 \quad \textit{und} \quad Tr_{L/K}(c) = -a_{n-1}.$$

Beweis. Der Körpergrad $[L:K]$ ist $Grad(p) = n$. Das charakteristische Polynom von $m_c : L \to L$ ist deswegen ein Polynom

$$\chi(X) = det(m_c - X \cdot \mathbb{1}) = (-1)^n X^n + b_{n-1}X^{n-1} + ... + b_1 X + b_0, \quad b_0, b_1, ..., b_{n-1} \in K,$$

vom Grad n. Hier ist

$$b_0 = \chi(0) = det(m_c) = N_{L/K}(c)$$

und

$$(-1)^{n-1} b_{n-1} = Tr(m_c) = Tr_{L/K}(c).$$

Nach Cayley-Hamilton gilt

$$\chi(m_c) = m_c^n + b_{n-1}m_c^{n-1} + ... + b_1 m_c + b_0 = 0.$$

Wendet man diese lineare Abbildung auf $1 \in K$ an, so folgt

$$0 = \chi(m_c)(1) = c^n + b_{n-1}c^{n-1} + ... + b_1 c + b_0.$$

Es folgt, dass das Minimalpolynom $p(X)$ das charakteristische Polynom $\chi(X)$ teilen muss. Weil beide vom gleichen Grad sind, gilt $\chi(X) = (-1)^n p(X)$. Also ist $(-1)^n a_0 = b_0 = N_{L/K}(c)$ und $-a_{n-1} = (-1)^n(-1)^{n-1} b_{n-1} = Tr_{L/K}(c)$. □

Beispiel 5.9 *Es sei $a \in K$ kein Quadrat und L die quadratische Erweiterung $K(\sqrt{a})$. Alle Elemente aus L schreiben sich $c = u + v\sqrt{a}$ mit $u, v \in K$. Wir betrachten hier nur den Fall $v \neq 0$. Dann ist also $c \notin K$ und $L = K(c)$. Norm und Spur von c berechnen sich also aus dem Minimalpolynom von c über K.*

Nun ist

$$c^2 = u^2 + av^2 + 2uv\sqrt{a}, \quad v\sqrt{a} = c - u,$$

und deswegen

$$c^2 - 2u(c-u) - (u^2 + av^2) = c^2 - 2uc + u^2 - av^2 = 0.$$

Das Minimalpolynom von c ist

$$p(X) = X^2 - 2uX + u^2 - av^2.$$

Aus Satz 5.8 folgt

$$N_{L/K}(c) = u^2 - av^2, \quad Tr_{L/K}(c) = 2u.$$

Satz 5.10 *Es sei $p \in K[X]$ ein normiertes, irreduzibles, separables Polynom über K, und $L = K(c)$ entstehe aus K durch Adjunktion einer Wurzel c von p. Die Konjugierten von c (in einer normalen Hülle von L über K) seien $c = c_1, c_2, ..., c_n$. Dann ist*

$$N_{L/K}(c) = c_1 \cdot c_2 \cdot ... \cdot c_n, \quad Tr_{L/K}(c) = c_1 + c_2 + ... + c_n.$$

Beweis. Über der normalen Hülle zerfällt das Minimalpolynom $p \in K[X]$ von c in Linearfaktoren

$$p(X) = (X - c_1) \cdot (X - c_2) \cdot ... \cdot (X - c_n).$$

Also hat p die Koeffizienten

$$p(X) = X^n - (c_1 + ... + c_n)X + ... + (-1)^n \cdot c_1 \cdot c_2 \cdot ... \cdot c_n.$$

Aus Satz 5.8 folgt

$$N_{L/K}(c) = c_1 \cdot ... \cdot c_n$$

und

$$Tr_{L/K} = -(-c_1 - ... - c_n) = c_1 + ... + c_n.$$

□

Beispiel 5.10 *Die Konjugierten von $c = u + v\sqrt{a}$ in der quadratischen Erweiterung $K(\sqrt{a}) = K(c)$, $v \neq 0$, sind $c = c_1$ und $c_2 = u - v\sqrt{a}$. Aus Satz 5.9 ergibt sich*

$$N_{L/K}(c) = (u + v\sqrt{a})(u - v\sqrt{a}) = u^2 - av^2, \quad Tr_{L/K}(c) = (u + v\sqrt{a}) + (u - v\sqrt{a}) = 2u$$

in Einklang mit Beispiel 5.9.

Satz 5.11 *Es sei $K \subset L$ eine galoissche Körpererweiterung mit Galoisgruppe G. Für jedes $c \in L$ gilt dann*

$$N_{L/K}(c) = \prod_{g \in G} g(c), \quad Tr_{L/K}(c) = \sum_{g \in G} g(c).$$

Beweis. Es seien $c_1, ..., c_k \in L$ die Konjugierten von c. Nach Satz 5.9 ist

$$N_{K(c)/K}(c) = c_1 \cdot ... \cdot c_k, \quad Tr_{K(c)/K}(c) = c_1 + ... + c_k.$$

Mit Satz 5.6 folgt daraus

$$N_{L/K}(c) = (c_1 \cdot ... \cdot c_k)^n, \quad Tr_{L/K}(c) = n \cdot (c_1 + ... + c_k),$$

wo n der Körpergrad $[L : K(c)]$ ist.

Der Körpergrad $[K(c) : K]$ ist der Grad des Minimalpolynoms von c, und weil c separabel ist, die Anzahl k der verschiedenen Konjugierten von c. Für die Ordnung der Galoisgruppe von L über K folgt daraus

$$|G| = k \cdot n.$$

Der Bahnensatz 1.2 zeigt für die Standgruppe $G_c \subset G$ des Elements c

$$|G_c| = \frac{1}{k} \cdot (g \cdot n) = n.$$

Also ist

$$\prod_{g \in G} g(c) = (c_1 \cdot ... \cdot c_k)^n, \quad \sum_{g \in G} g(c) = n \cdot (c_1 + ... + c_n).$$

□

Satz 5.12 (Transitivität) *Es seien $K \subset L \subset M$ separable Körpererweiterungen und $c \in M$. Dann gilt*

$$N_{M/K}(c) = N_{L/K}(N_{M/L}(c)), \quad Tr_{M/K}(c) = Tr_{L/K}(Tr_{M/L}(c)).$$

Beweis. Es sei $M \subset M'$ ein normaler Abschluss von M über K. Ist $m = [M' : M]$ der Körpergrad, so folgt aus Satz 5.6

$$N_{M'/L}(c) = (N_{M/L}(c))^m,\ N_{M'/K}(c) = (N_{M/K}(c))^m,$$

$$Tr_{M'/L}(c) = m \cdot Tr_{M/L}(c),\ Tr_{M'/K}(c) = m \cdot Tr_{M/K}(c)^m.$$

Wegen der Multiplikativität von $N_{L/K}$ und der Additivität von $Tr_{L/K}$ (Satz 5.7) genügt es, die Behauptungen für die galoissche Körpererweiterung M' zu beweisen. Wir nehmen also o.B.d.a. an, dass galoissch über K und dann auch über L ist.

Sei $H \subset G$ die Galoisgruppe $G(M : L)$. Ihre Ordnung ist $n := |H| = [M : L]$ und für $l \in L$

$$N_{M/K}(l) = (N_{L/K}(l))^n, \quad Tr_{M/K}(l) = n \cdot Tr_{L/K}(l).$$

Mit Satz 5.10 finden wir

$$\begin{aligned}
N_{M/K}(c) &= \prod_{g \in G} g(c), \\
N_{M/L}(c) &= \prod_{g \in H} g(c), \\
N_{L/K}(N_{M/L}(c)) &= N_{L/K} \prod_{h \in H} h(c) \\
&= \sqrt[n]{N_{M/K} \prod_{h \in H} h(c)} \\
&= \sqrt[n]{\prod_{g \in G} g \left(\prod_{h \in H} h(c) \right)} \\
&= \sqrt[n]{\prod_{g \in G, h \in H} gh(c)} \\
&= \sqrt[n]{\left(\prod_{g \in G} g(c) \right)^n} \\
&= \prod_{g \in G} g(c) \\
&= N_{M/K}(c), \\
Tr_{M/K}(c) &= \sum_{g \in G} g(c), \\
Tr_{M/L}(c) &= \sum_{h \in G} h(c),
\end{aligned}$$

$$\begin{aligned}
Tr_{L/K}(Tr_{M/L}(c)) &= Tr_{L/K}\left(\sum_{h\in H} h(c)\right) \\
&= \frac{1}{n}\cdot Tr_{M/K}\left(\sum_{h\in H} h(c)\right) \\
&= \frac{1}{n}\cdot \sum_{g\in G} g\left(\sum_{h\in H} h(c)\right) \\
&= \frac{1}{n}\cdot \sum_{g\in G, h\in H} gh(c) \\
&= \frac{1}{n}\cdot n\sum_{g\in G} g(c) \\
&= \sum_{g\in G} g(c) \\
&= Tr_{M/K}(c),
\end{aligned}$$

denn wenn $g \in G$ und $h \in H$ unabhängig voneinander laufen, dann durchläuft das Produkt $g \cdot h$ alle Elemente von G, aber jedes davon tritt n-mal auf. □

Aufgabe 5.5 (H 91, T3, A2) *Für eine endliche Körpererweiterung K/k bezeichne $tr_{K/k} : K \to k$ die Spurabbildung. Man beweise (mit den Mitteln der linearen Algebra): Ist K/k eine endliche zyklische Erweiterung und σ ein erzeugendes Element der Galoisgruppe G von K/k, so sind für ein Element $\alpha \in K$ die folgenden Bedingungen äquivalent:*

i) $tr_{K/k}(\alpha) = 0$

ii) $\alpha = \sigma(\beta) - \beta$ mit einem $\beta \in K$.

6 Algebraische Zahlkörper

Als ich dieses Skriptum produzierte, hatte ich beabsichtigt, im ersten Semester die ersten vier Kapitel zu behandeln, und dann, je nach dem, ob noch Zeit bliebe, die Miszellen (Kapitel 5). Das wäre dann fast der ganze Stoff für das Staatsexamen gewesen. Es wäre ganz im Einklang mit meiner Staats-Examens-Philosophie gewesen: Eine Einzel-Prüfung im Hauptexamen soll den Stoff einer einsemestrigen Vorlesung abprüfen. Soweit ist es allerdings nicht gekommen. Einerseits ist das schade, weil dies meine Staats-Examens-Philosophie ruiniert hat. (Ganz im Einklang mit den üblichen Analysis-Klausuren wäre sie ja ehe nicht gewesen.) Andererseits ist es aber auch gut so, weil wir jetzt genügend Zeit hatten, in Kapitel 4 die abstrakten Begriffe aus Kapitel 3 noch einmal an Beispielen durchzugehen, und Aufgaben zu rechnen. Der häufigste Vorwurf, der mir auf den Evaluierungsbögen gemacht wurde, war ja auch, dass ich zu schnell vorgegangen bin, und dass die Aufgaben zu schwer waren. Es ist also gut so, wenn wir jetzt eine Art von zweitem Anlauf in die Algebra unternehmen.

In diesem sechsten Kapitel möchte ich einen Einblick in die algebraische Zahlentheorie geben. Zum Teil überschneidet sich das mit Kapitel 5, wo ich das allernotwendigste zusammenstellte, was noch fehlte. Aber es ist vielleicht ganz förderlich für das Verständnis, wenn erst eine konzentrierte Zusammenschau gebracht wird, auf die jetzt eine ausführliche Diskussion folgt. Als zusätzliche Literatur habe ich die folgenden Bücher benutzt:

- H. Cohn: A Classical Invitation to Algebraic Numbers and Class Fields, Springer 1978,
- K. Ireland, M. Rosen: A Classical Introduction to Modern Number Theory, Springer 1972,
- H. Pollard: The Theory of Algebraic Numbers, J. Wiley 1950.

Ein algebraischer Zahlkörper K ist eine endliche Körpererweiterung von $\mathbb{Q}$. Nach Satz 3.27 ist er eine einfache Erweiterung $K = \mathbb{Q}(c)$. Dabei ist das primitive Element c Nullstelle eines irreduziblen Polynoms $p \in \mathbb{Q}[X]$. Nach dem Fundamentalsatz der Algebra besitzt p eine Nullstelle $c_0 \in \mathbb{C}$. Nach Satz 3.9 wird durch $c \mapsto c_0$ ein Isomorphismus

$$K = \mathbb{Q}(c) \to \mathbb{Q}(c_0) \subset \mathbb{C}$$

induziert. Es ist deswegen keine Beschränkung der Allgemeinheit, wenn wir gleich $c = c_0 \in \mathbb{C}$ und auch $K \subset \mathbb{C}$ voraussetzen. Im Folgenden sei stets $K \subset \mathbb{C}$ eine solche endliche Körpererweiterung.

6.1 Der Ring der ganz-algebraischen Zahlen

In 5.2 haben wir definiert, wann eine Zahl $a \in K$ ganz-algebraisch heißt: wenn ihr (normiertes) Minimalpolynom über $\mathbb{Q}$ ganze Koeffizienten hat. Nach Satz 5.5 bilden die ganz-algebraischen Zahlen in K einen Unterring $O(K) \subset K$.

Beispiel 6.1 (Quadratische Zahlkörper) *Nach Beispiel 3.6 ist jede quadratische Erweiterung K von $\mathbb{Q}$ von der Form $\mathbb{Q}(\sqrt{D})$, wo $D \neq 0, 1$ eine quadratfreie ganze Zahl ist. Z.B. sind die quadratfreien ganzen Zahlen vom Betrag ≤ 10 die 13 Zahlen*

$$-10,\ -7,\ -6,\ -5,\ -3,\ -2,\ -1,\ 2,\ 3,\ 5,\ 6,\ 7,\ 10.$$

Jede Zahl $c \in \mathbb{Q}(\sqrt{D})$ ist eine Linearkombination $c = a + b\sqrt{D}$ mit $a, b \in \mathbb{Q}$. Sie hat die Konjugierte $c' = a - b\sqrt{D}$ und das Minimalpolynom

$$X^2 - Tr_{K/\mathbb{Q}}(c) \cdot X + N_{K/\mathbb{Q}}(c) = X^2 - 2aX + a^2 - Db^2.$$

Somit ist c genau dann ganz-algebraisch, wenn

$$Tr(c) = 2a \in \mathbb{Z} \quad und \quad N(c) = a^2 - D \cdot b^2 \in \mathbb{Z}.$$

Es ist also $a = a_0/2$ mit $a_0 \in \mathbb{Z}$. Sei nun $b = b_0/b_1$ mit $b_0, b_1 \in \mathbb{Z}$ als gekürzter Bruch. Dann muss $4D \cdot b_0^2/b_1^2$ ganzzahlig sein. Jeder Primteiler $p \neq 2$ von b_1 müsste quadratisch in D aufgehen. Weil D quadratfrei ist, folgt $p = 1$. Damit kann nur $b_1 = 1$ oder $b_1 = 2$ vorliegen. Wir haben bewiesen: Jede ganz-algebraische Zahl in $\mathbb{Q}(\sqrt{D})$ ist von der Form

$$c = \frac{a_0}{2} + \frac{b_0}{2}\sqrt{D}, \quad a_0, b_0 \in \mathbb{Z}.$$

Wann ist ein solches c nun wirklich ganz-algebraisch? Wegen $Tr(c) = a_0 \in \mathbb{Z}$ ist die notwendige und hinreichende Bedingung dafür

$$N(c) = \frac{a_0^2}{4} - D\frac{b_0^2}{4} \in \mathbb{Z} \quad bzw. \quad a_0^2 - Db_0^2 = 0 \, mod \, 4.$$

Als Quadrate sind a_0^2 und $b_0^2 = 0$ oder $= 1 \, mod \, 4$ und weil D quadratfrei ist, gilt $D = 1, 2$ oder $3 \, mod \, 4$. Es gibt nur die Möglichkeiten

$$\begin{aligned} a_0^2 = b_0^2 = 0 \, mod \, 4, &\quad D \ beliebig, \\ a_0^2 = b_0^2 = 1 \, mod \, 4, &\quad D = 1 \, mod \, 4. \end{aligned}$$

Wir haben bewiesen:

Satz 6.1 *Es sei $K = \mathbb{Q}(\sqrt{D})$, $D \in \mathbb{Z}$ quadratfrei, ein quadratischer Zahlkörper. Dann sind die ganz-algebraischen Zahlen in K*

	für	*von der Form*
i)	$D = 2, 3 \, mod \, 4$	$a + b \cdot \sqrt{D}$,
ii)	$D = 1 \, mod \, 4$	*zusätzlich* $(a + b \cdot \sqrt{D})/2$, *a und b ungerade*,

mit $a, b \in \mathbb{Z}$.

Z.B. für die Zahlen D mit $|D| \leq 10$ gilt

-10	-7	-6	-5	-3	-2	-1	2	3	5	6	7	10
i)	*ii)*	*i)*	*i)*	*ii)*	*i)*	*i)*	*i)*	*i)*	*ii)*	*i)*	*i)*	*i)*

Satz 6.2 (Transisitivität) *Die Zahl $c \in \mathbb{C}$ sei Nullstelle eines normierten Polynoms*

$$f(X) = X^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$$

mit ganz-algebraischen Koeffizienten $a_{n-1}, ..., a_0$. Dann ist auch c ganz-algebraisch.

Beweis. Ein Polynom $f_i(X) \in \mathbb{C}[X]$ heiße konjugiert zu f, wenn es einen $\mathbb{Q}$-Homomorphismus $\mathbb{Q}(a_{m-1}, ..., a_0) \to \mathbb{C}$ gibt, der f auf f_i abbildet. Weil es nur endlich viele solche $\mathbb{Q}$-Homomorphismen gibt, gibt es nur endlich viele verschiedene zu $f(X)$ konjugierte Polynome $f(X), f_2(X), ..., f_n(X)$. Das Polynom

$$F(X) := f(X) \cdot f_2(X) \cdot ... \cdot f_n(X)$$

ist dann invariant unter allen Galois-Automorphismen einer normalen Hülle von $\mathbb{Q}(a_{n-1}, ..., a_0)$ über $\mathbb{Q}$. Deswegen sind alle seine Koeffizienten ganz, und $F(X) \in \mathbb{Z}(X)$. Die Zahl c ist eine Nullstelle des normierten Polynoms $F(X)$ und damit ganz. □

Jede rationale Zahl $a \in \mathbb{Q}$ ist Quotient zweier ganzer Zahlen. Ebenso ist jede Zahl $a \in K$ Quotient zweier ganz-algebraischer Zahlen in K. Genauer gilt

Satz 6.3 (Aufgabe 5.3) *Zu jedem $a \in K$ gibt es ein $b \in \mathbb{N}$ derart, dass $b \cdot a \in K$ ganz-algebraisch ist.*

Beweis. Die Zahl a ist Nullstelle ihres Minimalpolynoms

$$p(X) = X^n + c_{n-1}X^{n-1} + ... + c_1X + c_0 \in \mathbb{Q}[X], \quad c_{n-1}, ..., c_1, c_0 \in \mathbb{Q}.$$

Wenn wir darauf verzichten, p als normiert anzunehmen, können wir mit dem Hauptnenner aller Koeffizienten durchmultiplizieren, und sehen, dass a Nullstelle eines Polynoms

$$q(X) = b_nX^n + b_{n-1}X^{n-1} + ... + b_1X + b_0, \quad b_n, ..., b_0 \in \mathbb{Z},$$

mit ganzen Koeffizienten ist. Hier ist natürlich $b_n \neq 0$, und nach eventueller Vorzeichenänderung beim Polynom q können wir sogar $b_n \in \mathbb{N}$ annehmen. Dann ist

$$\begin{aligned} b_n^{n-1}q(a) &= b_n^n a^n + b_{n-1} \cdot b_n^{n-1}a^{n-1} + b_{n-2}b_n \cdot b_n^{n-2}a^{n-2} + ... + b_1b_n^{n-2} \cdot b_n a + b_0 b_n^{n-1} \\ &= (b_n a)^n + b_{n-1} \cdot (b_n a)^{n-1} + b_{n-2}b_n \cdot (b_n a)^{n-2} + ... + b_1b_n^{n-2} \cdot (b_n a) + b_0 b_n^{n-1} \\ &= 0. \end{aligned}$$

Die Zahl $b_n a$ ist ganz-algebraisch. □

Wir können also, wenn wir wollen, annehmen, dass $K = \mathbb{Q}(a)$, wo a ganz-algebraisch ist. Die Potenzen $1, a, a^2, ..., a^{n-1} \in K$ sind ganz-algebraisch, weil die ganz-algebraischen Zahlen einen Ring bilden. Und sie sind linear unabhängig über $\mathbb{Q}$, denn sonst wäre a Nullstelle eines Polynoms vom Grad $\leq n-1$. Also bilden diese ganz-algebraischen Zahlen eine Körperbasis von K über $\mathbb{Q}$.

Die Zahl a ist Nullstelle ihres Minimalpolynoms $p \in \mathbb{Q}[X]$, eines irreduziblen Polynoms vom Grad $n = [K : \mathbb{Q}]$. Weil p separabel ist (Charakteristik = 0), hat p in $\mathbb{C}$ lauter verschiedene einfache Nullstellen $a = a_1, a_2, ..., a_n \in \mathbb{C}$, die Konjugierten von a über $\mathbb{Q}$. Durch $g_i : a \mapsto a_i, i = 1, ..., n$, werden $\mathbb{Q}$-Isomorphismen $g_i : K \to K_i \subset \mathbb{C}$ definiert. Dies sind genau die Bilder von K unter allen Galois-Automorphismen einer normalen Hülle N von K über $\mathbb{Q}$.

Definition 6.1 *Es sei $a_1, ..., a_n \in K$ eine $\mathbb{Q}$-Basis von K. Dann heißt das Quadrat der Determinante*

$$\Delta := det \begin{pmatrix} g_1(a_1) & ... & g_1(a_n) \\ \vdots & & \vdots \\ g_n(a_1) & ... & g_n(a_n) \end{pmatrix}^2$$

die Diskriminante $\Delta(a_1, ..., a_n)$ dieser Basis.

Bei Übergang zu einer anderen Basis

$$\begin{aligned} a_1' &= c_{1,1}a_1 + ... + c_{1,n}a_n \\ &\vdots \\ a_n' &= c_{n,1}a_1 + ... + c_{n,n}a_n \end{aligned}$$

mit $c_{i,j} \in \mathbb{Q}$ ist

$$g_k(a_i') = c_{i,1}g_k(a_1) + ... + c_{i,n}g_k(a_n),$$

und es folgt

$$det \begin{pmatrix} g_1(a_1') & ... & g_1(a_n') \\ \vdots & & \vdots \\ g_n(a_1') & ... & g_n(a_n') \end{pmatrix} = det \begin{pmatrix} g_1(a_1) & ... & g_1(a_n) \\ \vdots & & \vdots \\ g_n(a_1) & ... & g_n(a_n) \end{pmatrix} \cdot det \begin{pmatrix} c_{1,1} & ... & c_{n,1} \\ \vdots & & \vdots \\ c_{1,n} & ... & c_{n,n} \end{pmatrix}.$$

Die Diskriminante multipliziert sich bei diesem Basiswechsel also mit $det(c_{i,j})^2$.

Satz 6.4 *i) Die Diskriminante $\Delta(a_1, ..., a_n)$ ist stets eine Zahl aus $\mathbb{Q}$.*
ii) Sind $a_1, ..., a_n$ ganz-algebraisch, so gilt sogar $\Delta(a_1, ..., a_n) \in \mathbb{Z}$.

Beweis. i) Die Konjugierten von Δ über $\mathbb{Q}$ sind die Bilder

$$g_k(\Delta) = det \begin{pmatrix} g_k g_1(a_1) & ... & g_k g_1(a_n) \\ \vdots & & \vdots \\ g_k g_n(a_1) & ... & g_k g_n(a_n) \end{pmatrix}^2$$

unter den Galois-Automorphismen g_k, $k = 1, ..., n$. Die Produkte $g_k g_1, ..., g_k g_n$ durchlaufen auch alle Galois-Automorphismen. Deswegen ändert sich in unserer $n \times n$-Matrix nur die Reihenfolge der Zeilen. Die Determinante ändert höchstens ihr Vorzeichen, und Δ selbst ist unter allen Galois-Automorphismen invariant. Nach Satz 3.28 gehört Δ zum Grundkörper $\mathbb{Q}$.

ii) Wenn die a_i ganz-algebraisch sind, dann sind dies auch ihre Konjugierten $g_k(a_i)$, und damit ist auch $\Delta \in \mathbb{Q}$ ganz algebraisch. Nach Beispiel 5.4 folgt $\Delta \in \mathbb{Z}$. □

Beispiel 6.2 (Kreisteilungskörper) *Es sei $3 \leq p \in \mathbb{N}$ eine Primzahl und $K = \mathbb{Q}(\sqrt[p]{1})$ der p-te Kreisteilungskörper. Ist $w \in K$ eine primitive p-te Einheitswurzel, so ist*

$$w,\ w^2,\ ...,\ w^{p-1}$$

nach Satz 4.6 eine $\mathbb{Q}$-Basis von K. Aber natürlich ist auch

$$1,\ w,\ ...,\ w^{p-2}$$

eine solche $\mathbb{Q}$-Basis. Wir wollen deren Diskriminante berechnen.

Die Galois-Automorphismen g_k werden induziert durch $w \mapsto w^k$, $k = 1, ..., p-1$, und es ist

$$g_k(w^i) = (w^k)^i.$$

Deswegen ist

$$det \begin{pmatrix} 1 & w & w^2 & ... & w^{p-2} \\ 1 & g_2(w) & g_2(w^2) & ... & g_2(w^{p-2}) \\ \vdots & \vdots & \vdots & ... & \vdots \\ 1 & g_{p-1}(w) & g_{p-1}(w^2) & ... & g_{p-1}(w^{p-2}) \end{pmatrix} = det \begin{pmatrix} 1 & w & w^2 & ... & w^{p-2} \\ 1 & w^2 & (w^2)^2 & ... & (w^{p-2})^2 \\ \vdots & \vdots & \vdots & ... & \vdots \\ 1 & w^{p-1} & (w^2)^{p-1} & ... & (w^{p-2})^{p-1} \end{pmatrix}$$

die Vandermonde-Determinante

$$\prod_{i<j}(w^i - w^j),$$

und die Diskriminante ist

$$\Delta(1, ..., w^{p-2}) = \prod_{i<j}(w^i - w^j)^2.$$

Nach Vieta ist das p-te Kreisteilungspolynom

$$\frac{X^p - 1}{X - 1} = X^{p-1} + ... + 1 = \prod_{i=1}^{p-1}(X - w^i).$$

Wir differenzieren das Kreisteilungspolynom nach X:

$$\frac{d}{dX}(L.S.) = \frac{d}{dX}\frac{X^p - 1}{X - 1} = \frac{pX^{p-1}(X-1) - (X^p - 1)}{(X-1)^2} = \frac{(p-1)X^p - pX^{p-1} + 1}{(X-1)^2},$$

$$\frac{d}{dX}(R.S.) = \frac{d}{dX}\prod_{i=1}^{p-1}(X - w^i) = \sum_{j=1}^{p-1}\prod_{i\neq j}(X - w^i).$$

Hier setzen wir $X = w^j$ ein und erhalten wegen $w^p = 1$ für die linke Seite

$$\frac{p - p(w^j)^{p-1}}{(w^j - 1)^2} = p\frac{1 - w^{-j}}{(w^j - 1)^2} = p\frac{w^{-j}(w^j - 1)}{(w^j - 1)^2} = p\frac{w^{-j}}{w^j - 1},$$

während von der rechten Seite dies nur der Summand

$$\prod_{i\neq j}(w^j - w^i)$$

überlebt. Wir haben also bewiesen

$$p\frac{w^{-j}}{w^j - 1} = \prod_{i\neq j}(w^j - w^i).$$

Diese Gleichungen für $j = 1, ..., p-1$ multiplizieren wir alle miteinander. Mit Satz 4.1 b) wird das Produkt auf der linken Seite

$$p^{p-1}\frac{w \cdot w^2 \cdot ... \cdot w^{p-1}}{(w-1)\cdot(w^2-1)\cdot ... \cdot (w^{p-1}-1)} = p^{p-1}\frac{1}{p} = p^{p-2}.$$

Das Produkt auf der rechten Seite ist

$$\prod_{j\neq i}(w^j - w^i) = (-1)^{\frac{(p-1)(p-2)}{2}} \prod_{i<j}(w^i - w^j)^2 = (-1)^{\frac{p-1}{2}}\Delta(1, w, w^2, ..., w^{p-2}).$$

Das Endergebnis ist

$$\Delta(1, w, w^2, ..., w^{p-2}) = (-1)^{\frac{p-1}{2}}p^{p-2}.$$

Definition 6.2 *Eine Körperbasis $a_1, ..., a_n$ von K über $\mathbb{Q}$ heißt* Ganzheitsbasis, *wenn*

1) alle $a_1, ..., a_n$ ganz-algebraisch sind, und

2) jede ganz-algebraische Zahl $b \in K$ eine Linearkombination

$$b = b_1a_1 + ... + b_na_n \quad mit \quad b_1, ..., b_n \in \mathbb{Z}$$

ist.

Beispiel 6.3 (Quadratische Zahlkörper) *Satz 6.1 besagt, dass für den quadratischen Zahlkörper $\mathbb{Q}(\sqrt{D})$*

im Fall	*die Zahlen*
$D = 2, 3 \, mod \, 4$	$1, \sqrt{D}$
$D = 1 \, mod \, 4$	$\frac{1+\sqrt{D}}{2}, \frac{1-\sqrt{D}}{2}$

eine Ganzheitsbasis bilden.

Satz 6.5 *Jeder algebraische Zahlkörper $K \subset \mathbb{C}$ besitzt eine Ganzheitsbasis.*

Beweis. Wie wir oben sahen, gibt es Körperbasen $a_1, ..., a_n \in K$ aus ganz-algebraischen Zahlen. (Z.B. die Zahlen $1, a, a^2, ..., a^{n-1}$ wo $K = \mathbb{Q}(a)$ und a ganz-algebraisch ist.) Für alle diese Basen ist $\Delta(a_1, ..., a_n) \neq 0$ eine ganze Zahl. Es gibt deswegen eine solche Basis, deren Diskriminante minimal unter allen Diskriminanten von Körperbasen aus ganz-algebraischen Zahlen ist. Genauer: $|\Delta(a_1, ..., a_n)| \in \mathbb{N}$ soll minimal sein. Wir fixieren eine solche Basis, und zeigen, dass sie eine Ganzheitsbasis ist.

Wären nicht alle ganz-algebraischen Zahlen $b \in K$ ganzzahlige Linearkombinationen, so gäbe es ein ganz-algebraisches $b \in K$ mit

$$b = b_1a_1 + ... + b_na_n, \quad \text{nicht alle} \quad b_1, ..., b_n \in \mathbb{Z}.$$

O.B.d.A. können wir $b_1 \notin \mathbb{Z}$ annehmen. Dann ist

$$b_1 = b_0 + r, \quad b_0 \in \mathbb{Z}, \, r \in \mathbb{Q}, \, 0 < r < 1.$$

Wir setzen

$$a_1' := b - b_0 a_1 = (b_1 - b_0)a_1 + b_2 a_2 + ... + b_n a_n \in O(K)$$

und betrachten die Zahlen $a_1', a_2, ..., a_n \in K$. Dazu gehört die Übergangsmatrix

$$(c_{i,j}) = \begin{pmatrix} b_1 - b_0 & 0 & ... & 0 \\ b_2 & 1 & & 0 \\ \vdots & & \ddots & \vdots \\ b_n & & & 1 \end{pmatrix}$$

mit der Determinante $b_1 - b_0 = r < 1$. Die ganz-algebraischen Zahlen $a_1', a_2, ..., a_n$ bilden also auch eine Körperbasis von K, aber mit dem Absolutbetrag der Diskriminante

$$|\Delta(a_1', ..., a_n)| = r^2 |\Delta(a_1, ..., a_n)| < |\Delta(a_1, ..., a_n)|.$$

Dies ist ein Widerspruch zur Minimalität von $\Delta(a_1, ..., a_n)$. □

Beispiel 6.4 (Kreisteilungskörper) *Wieder sei p eine ungerade Primzahl und $K = K(\sqrt[p]{1})$ der p-te Kreisteilungskörper. Es sei $w \in K$ eine primitive p-te Einheitswurzel. Wir setzen*

$$v := 1 - w$$

und behaupten, die Zahlen

$$1, v, v^2, ..., v^{p-2}$$

sind eine Ganzheitsbasis von K. Wegen

$$\begin{aligned} v &= 1 - w \\ v^2 &= 1 - 2w + w^2 \\ v^3 &= 1 - 3w + 3w^2 - w^3 \\ &\vdots \end{aligned}$$

ist

$$\Delta(1, v, ..., v^{p-2}) = det(a_{i,j})^2 \cdot \Delta(1, w, ..., w^{p-2})$$

mit ganzen Zahlen $a_{i,j}$. Genauso folgt aus $w = 1 - v$

$$\Delta(1, w, ..., w^{p-2}) = det(a_{i,j})^2 \cdot \Delta(1, v, ..., v^{p-2}).$$

Es muss also $det(a_{i,j})^4 = 1$ und

$$\Delta(1, v, ..., v^{p-2}) = \Delta(1, w, ..., w^{p-2}) = (-1)^{\frac{p-1}{2}} p^{p-2}$$

sein. Wir kennen damit die Diskriminante unserer Basis $1, v, ..., v^{p-2}$.

Wir wählen nun eine beliebige Ganzheitsbasis $a_1, ..., a_{p-1}$ und schreiben

$$v^j = \sum_{i=1}^{p-1} c_{j,i} a_i, \quad j = 0, ..., p-2.$$

Hier gilt für die Determinante

$$det(c_{i,j})^2 \cdot \Delta(a_1, ..., a_{p-1}) = \Delta(1, v, ..., v^{p-2}).$$

Deswegen ist $det(c_{i,j})$ bis auf das Vorzeichen eine Potenz von p. Lösen wir jetzt das Gleichungssystem nach den a_i auf (etwa mit der Kramerschen Regel), so wird jedes a_i ein Quotient

$$a_i = \frac{1}{p^{m_i}}(n_{i,1} + n_{i,2}v + ...n_{i,p-2}v^{p-2})$$

mit ganzen Zahlen $n_{i,j}$. Weil die a_i eine Ganzheitsbasis sind, lässt sich jede ganz-algebraische Zahl $c \in K$ als ein derartiger Quotient ausdrücken, in dessen Nenner nur eine p-Potenz steht.

Wenn $1, v, ..., v^{p-1}$ keine Ganzheitsbasis wären, dann gäbe es eine ganz-algebraische Zahl

$$c = \frac{1}{p} \cdot (n_0 + n_1 v + ... + n_{p-2}v^{p-2}), \quad n_0, ..., n_{p-2} \in \mathbb{Z},$$

derart, dass nicht alle Zahlen n_k durch p teilbar sind. Sei n_m die erste davon. Dann ist

$$\frac{1}{p} \cdot (n_m v^m + ... + n_{p-2}v^{p-2})$$

ganz-algebraisch. Aus Satz 4.1 b) wissen wir

$$p = (1 - w)(1 - w^2) \cdot ... \cdot (1 - w^{p-1}).$$

Jeder dieser Faktoren ist durch $v = 1 - w$ teilbar. Dann ist also $p = v^{p-1} \cdot k$ und $p = v^{m+1} \cdot k'$ mit ganz-algebraischen Zahlen k und k'. Deswegen ist dann auch

$$\frac{1}{v^{m+1}} \cdot (n_m v^m + ... + n_{p-2}v^{p-2})$$

sowie

$$\frac{n_m v^m}{v^{m+1}} = \frac{n_m}{v} = \frac{n_m}{1 - w} =: b$$

ganz-algebraisch. Weil n_m nicht durch p teilbar ist, wäre dies ein Widerspruch zu Beispiel 5.7. Unsere Basis war eben doch eine Ganzheitsbasis.

Sind $a_1, ..., a_n$ und $a'_1, ..., a'_n$ zwei Ganzheitsbasen, so ist die Übergangsmatrix $(c_{i,j})$ ebenso wie deren inverse Matrix ganzzahlig. Daraus folgt $det(c_{i,j}) = \pm 1$. Beide Ganzheitsbasen haben dieselbe Diskriminante.

Definition 6.3 *Die Diskrimininante einer Ganzheitsbasis (und damit aller Ganzheitsbasen) von K heißt die* Diskriminante *$d(K)$ des Zahlkörpers K.*

Beispiel 6.5 (Quadratische Zahlkörper) *Es sei $K = \mathbb{Q}(\sqrt{D})$ mit $D \in \mathbb{Z}$ quadratfrei. Im Fall $D = 2, 3 \, mod \, 4$ bilden die Zahlen 1 und $\sqrt{D}$ eine Ganzheitsbasis. Die Diskriminante ist*

$$d(K) = det \begin{pmatrix} 1 & \sqrt{D} \\ 1 & -\sqrt{D} \end{pmatrix}^2 = (-2\sqrt{D})^2 = 4D.$$

Im Fall $D = 1 \, mod \, 4$ *bilden* $(1+\sqrt{D})/2$ *und* $(1-\sqrt{D})/2$ *eine Ganzheitsbasis und die Diskriminante ist*

$$d(K) = det \begin{pmatrix} \frac{1}{2}(1+\sqrt{D}) & \frac{1}{2}(1-\sqrt{D}) \\ \frac{1}{2}(1-\sqrt{D}) & \frac{1}{2}(1+\sqrt{D}) \end{pmatrix}^2 = \left(\frac{1}{4}(1+\sqrt{D})^2 - \frac{1}{4}(1-\sqrt{D})^2\right)^2 = D.$$

Beispiel 6.6 (Kreisteilungskörper) *Unsere Berechnung der Ganzheitsbasis zeigt*

$$\Delta(\mathbb{Q}(\sqrt[p]{1})) = \Delta(1, w, ..., w^{p-2}) = (-1)^{\frac{p-1}{2}} \cdot p^{p-2}.$$

Konkret haben wir etwa für

p	3	5	7	11
Δ	-3	5^3	-7^5	-11^9

Aufgabe 6.1 *Es sei* K *ein reell-quadratischer Zahlkörper. Zeigen Sie: In* K *gibt es ganz-algebraische Zahlen* $c \neq 1$ *mit beliebig kleinem Abstand* $|c-1| > 0$.

Aufgabe 6.2 *Bestimmen Sie das Minimalpolynom über* $\mathbb{Q}$ *für*

$$a = \sqrt{2} + \sqrt{3}, \quad b = \sqrt{2} + \sqrt{5}, \quad c = \sqrt{3} + \sqrt{7}.$$

Aufgabe 6.3 *Es sei* $a_1, ..., a_n \in K$ *eine Körperbasis von* K *über* $\mathbb{Q}$ *derart, dass alle* a_i *ganz sind und die Diskriminante* $\Delta(a_1, ..., a_n) \in \mathbb{Z}$ *quadratfrei ist. Zeigen Sie, dass die* a_i *eine Ganzheitsbasis von* K *bilden.*

Aufgabe 6.4 *Es seien* D_1 *und* $D_2 \in \mathbb{Z}$ *quadratfreie, teilerfremde Zahlen. Zeigen Sie, dass*

$$\frac{1}{2}(\sqrt{D_2} + \sqrt{D_1 D_2}$$

ganz-algebraisch ist in den folgenden Fällen:

a) $D_1 = 1$, $D_2 = 3 \, mod \, 4$;
b) $D_1 = 1$, $D_2 = 2 \, mod \, 4$;
c) $D_1 = 3$, $D_2 = 2 \, mod \, 4$.

Aufgabe 6.5 *Es sei* K *der bi-quadratische Körper* $\mathbb{Q}(i, \sqrt{2})$. *Eine Zahl* $z \in K$ *hat also eine Darstellung*

$$a + bi + c\sqrt{2} + di\sqrt{2}, \quad a, b, c, d \in \mathbb{Q}.$$

a) Zeigen Sie für ganz-algebraisches z: $a = \frac{\alpha}{2}$, $b = \frac{\beta}{2}, c = \frac{\gamma}{2}$, $d = \frac{\delta}{2}$, $\quad \alpha, \beta, \gamma, \delta \in \mathbb{Z}$.
b) Zeigen Sie (mit MAPLE) Das Minimalpolynom von z *ist*

$$X^4 - 4aX^3 + (6a^2 + 2c^2 + 4(d^2 - b^2))X^2 - 4(a^3 + ac^2 + 2a(b^2 - d^2) - 4bcd)X$$
$$+(a^2 + c^2)^2 + 4(c^2 - a^2)(b^2 - d^2) - 16abcd + 4(b^2 + d^2)^2.$$

c) Zeigen Sie für ganz-algebraisches z:

$$a = c \, mod \, 2, \; b = d \, mod \, 2, a, c \in \mathbb{Z}.$$

d) Bestimmen Sie eine Ganzheitsbasis und die Diskriminante von K.

6.2 Einheiten

Die ganz-algebraischen Zahlen in einem algebraischen Zahlkörper K bilden einen nullteiler-freien, kommutativen Ring $O(K)$ mit 1. Deswegen sind alle Begriffe aus Abschnitt 2.3 (Teilbarkeit) hier anwendbar. Um die Ideale in $O(K)$ kümmern wir uns später. Hier wollen wir erst die Einheiten in $O(K)$, sozusagen die neutralen Elemente bezüglich Teilbarkeit, untersuchen. Sie bilden den Einheitenring $O^*(K)$ des Zahlkörpers K.

Satz 6.6 *Die ganz-algebraische Zahl $c \in K$ ist genau dann eine Einheit in $O(K)$, wenn ihre Norm $N_{K/\mathbb{Q}}(c) = \pm 1$ ist.*

Beweis. „$\Rightarrow$“: Ist $c \in O(K)$ eine Einheit, dann gibt es ein $c' \in O(K)$ mit $c \cdot c' = 1$. Weil die Norm multiplikativ ist (Satz 5.7), folgt daraus

$$N(c) \cdot N(c') = 1.$$

Nach Satz 5.9 sind $N(c)$ und $N(c') \in \mathbb{Q}$ ganze Zahlen. Deswegen ist $N(c) \in \mathbb{Z}$ eine Einheit, d.h. $N(c) = \pm 1$.

„$\Leftarrow$“: Jetzt ist $N(c) = \pm 1$ vorausgesetzt. Nach Satz 5.9 ist

$$N_{K/\mathbb{Q}}(c) = (c \cdot c_2 \cdot ... \cdot c_k)^{[K:\mathbb{Q}(c)]},$$

wo $c_2, ..., c_k \neq c$ die Konjugierten von c über $\mathbb{Q}$ sind. Als Nullstellen desselben Minimalpolynoms sind diese alle ganz-algebraisch. Also ist auch $c' := c_2 \cdot ... \cdot c_k$ ganz-algebraisch. Aus $c \cdot c' = \pm 1$ folgt zunächst $c' \in K$, dann $c' \in O(K)$, und damit, dass $c \in O(K)$ eine Einheit ist. □

Beispiel 6.7 (Quadratische Zahlkörper) *Für $c = a + b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$ ist $N(c) = a^2 - D \cdot b^2$. Die Frage ist, wann für ganz-algebraisches c diese Norm $= \pm 1$ ist. Die Antwort fällt ganz verschieden aus, abhängig vom Vorzeichen der Zahl D.*

a) $\mathbb{Q}(\sqrt{D})$ *heißt* imaginär-quadratischer Zahlkörper*, wenn $D < 0$ ist. Für eine Einheit c gilt dann also*

$$N(c) = a^2 + |D|b^2 = \pm 1.$$

Trivialerweise kommt -1 hier nicht in Frage. Aber auch die Bedingung $a^2 + |D|b^2 = 1$ ist ziemlich restriktiv.

Betrachten wir zunächst den Fall $D = 2, 3 \bmod 4$, wo a und b ganz sind. Wenn $|D| \geq 2$ ist, gibt es nur den Fall $a = \pm 1$ und $b = 0$. Einheiten sind nur die beiden Zahlen ± 1. Aber für $D = -1$ gibt es noch die Möglichkeiten $a = 0$, $b = \pm 1$. Einheiten in $\mathbb{Q}(i)$ sind die vier Zahlen ± 1 und $\pm i$.

Wenn $D = 1 \bmod 4$ ist, gibt es noch $a = a_0/2$ und $b = b_0/2$ mit $a_0, b_0 \in \mathbb{Z}$ ungerade. Die Bedingung lautet dann

$$a_0^2 + |D|b_0^2 = 4.$$

Für $D \leq -5$ haben wir wieder nur $a = \pm 1$ und $b = 0$. Aber für $D = -3$ gibt es noch die Möglichkeit $a_0^2 = b_0^2 = 1$. Einheiten im Körper $\mathbb{Q}(\sqrt{-3})$ sind also die sechs Zahlen

$$\pm 1, \quad \frac{1}{2}(\pm 1 \pm \sqrt{-3}).$$

Der Körper $\mathbb{Q}(\sqrt{-3})$ ist übrigens der Kreisteilungskörper $\mathbb{Q}(\sqrt[3]{1})$ und seine sechs Einheiten sind genau die sechs 6-ten Einheitswurzeln.

b) $\mathbb{Q}(\sqrt{D})$ *heißt* reell-quadratischer Zahlkörper, *wenn $D > 0$ ist. Einheiten $c \in O^*(\mathbb{Q}(\sqrt{D}))$ sind dann durch*

$$N(c) = a^2 - D \cdot b^2 = \pm 1$$

charakterisiert. Wegen des Minus-Zeichens vor dem D gibt es hier viel mehr Möglichkeiten. Entsprechend schwieriger ist es jetzt auch, diese Einheiten explizit zu bestimmen. Das Resultat ist ganz analog zum Fall $\mathbb{Q}(\sqrt{2})$. In 2.3 haben wir gesehen: Einheiten in $O(\mathbb{Q}(\sqrt{2}))$ sind genau die unendlich vielen Zahlen $\pm(1+\sqrt{2})^n$, $n \in \mathbb{Z}$. Aber im Allgemeinfall ist der Beweis nicht-trivial und, vor allem, nicht konstruktiv. Die Bestimmung der Einheiten in einem gegebenen reell-quadratischen Zahlkörper ist deswegen in jedem Einzelfall ein aufregendes Unterfangen.

Beispiel 6.8 (Einheitswurzeln) *Jede n-te Einheitswurzel w ist in $\mathbb{Q}(\sqrt[n]{1})$ ganz-algebraisch, denn die Kreisteilungspolynome haben ganze Koeffizienten. Auch w^{-1} ist ganz-algebraisch mit $w \cdot w^{-1} = 1$. Einheitswurzeln in K sind also stets Einheiten. In einem reell-quadratischen Zahlkörper gibt es nur die beiden Einheitswurzeln ± 1. In einem imaginär-quadratischen Zahlkörper K kann es noch mehr n-te Einheitswurzeln geben, und zwar genau dann, wenn $\varphi(n) = [K : \mathbb{Q}] = 2$ ist. Das ist genau dann der Fall, wenn $n = 3$ oder $= 4$ ist. In Beispiel 6.7 a) haben wir also gezeigt: In einem imaginär-quadratischen Zahlkörper sind genau die in diesem Körper enthaltenen Einheitswurzeln Einheiten.*

Beispiel 6.9 *Es sei p eine Primzahl und $w \in K := \mathbb{Q}(\sqrt[p]{1})$ eine primitive p-te Einheitswurzel. Für jedes $k = 2, ..., p-1$ ist*

$$1 - w^k = (1-w) \cdot (1 + w + ... + w^{k-1}).$$

Die Zahl $1+w+...+w^{k-1}$ ist ganz-algebraisch. Also teilt $1-w$ die Zahl $1-w^k$ in K. Umgekehrt ist auch w^k eine primitive p-te Einheitswurzel und $w = (w^k)^l$ mit $2 \le l \le p-1$. Also teilt umgekehrt auch $1-w^k$ die Zahl $1-w$ in $O(K)$. Es folgt: In $\mathbb{Q}(\sqrt[p]{1})$ sind die $p-1$ Zahlen

$$1 - w, \quad 1 - w^2, \quad ..., \quad 1 - w^{p-1}$$

assoziiert. Und Einheiten sind z.B. alle Zahlen

$$1 + w + ... + w^m = \frac{1 - w^{m+1}}{1 - w}, \quad 0 \le m \le p-2.$$

Für den Rest dieses Abschnittes sei $D > 0$, quadratfrei, und $K = \mathbb{Q}(\sqrt{D})$ vorausgesetzt. Eine Zahl $e = a + b\sqrt{D}\, a, b \in \mathbb{Z}$, ist eine Einheit in K, genau dann, wenn

$$N(e) = a^2 - D \cdot b^2 = \pm 1$$

ist. Diese diophantische Gleichung heißt *Pellsche Gleichung.* Die Bezeichnung ist ein schönes Beispiel dafür, wie der Name eines Mathematikers völlig unverdient unsterblich werden kann. Soweit ich weiß hat Pell mit der Gleichung nichts zu tun. Sie heißt so, weil Euler den Namen Pell irrtümlich mit der Gleichung in Zusammenhang brachte.

Im Fall $D = 2, 3 \, mod \, 4$ kommt es darauf an, alle ganzzahligen Lösungen (a, b) der Pellschen Gleichung zu finden. Im Fall $D = 1 \, mod \, 4$ sind auch halbganzzahlige Lösungen gefragt. Triviale Lösungen der Pellschen Gleichung sind $(a, b) = (\pm 1, 0)$. Aber die sind eben trivial. Nicht-trivial ist, dass es nicht-triviale Lösungen der Pellschen Gleichung gibt. Und das wollen wir jetzt als erstes beweisen. Dazu Vorbereitungen:

Satz 6.7 *Es sei $q \in \mathbb{R}$ irrational, d.h., $q \notin \mathbb{Q}$. Dann gibt es zu jedem $n \in \mathbb{N}$ teilerfremde Zahlen $x, y \in \mathbb{Z}$ mit*

$$|x - yq| < \frac{1}{n} \quad und \quad \left|\frac{x}{y} - q\right| < \frac{1}{y^2}.$$

Beweis. Das halboffene Intervall $[0, 1)$ ist disjunkte Summe

$$[0, 1) = [0, \frac{1}{n}) \cup [\frac{1}{n}, \frac{2}{n}) \cup ... \cup [\frac{n-1}{n}, 1)$$

von n Teilintervallen der Länge $1/n$. Für jede reelle Zahl bezeichen wir wie üblich mit $[r]$ die größte ganze Zahl $\leq r$. Dann ist also

$$0 \leq r - [r] < 1,$$

und $r - [r]$ gehört zu genau einem Intervall in der obigen Zerlegung.

Wegen $q \neq 0$, sind die $n + 1$ Zahlen $0, q, 2q, ..., nq$ alle voneinander verschieden, und es gibt zwei dieser Zahlen iq und jq mit $0 \leq i < j \leq n$, $i, j \in \mathbb{N}$, für die $iq - [iq]$ und $jq - [jq]$ im gleichen Intervall liegen. Das heißt also

$$|iq - [iq] - (jq - [jq])| < \frac{1}{n}.$$

Wir setzen

$$x := [jq] - [iq] \in \mathbb{Z}, \quad y := j - i \in \mathbb{N}.$$

Dann ist also

$$|x - yq| = |[jq] - jq - ([iq] - iq)| < \frac{1}{n}$$

und

$$\left|\frac{x}{y} - q\right| < \frac{1}{yn} \leq \frac{1}{y^2}.$$

Falls x und y einen gemeinsamen Teiler besitzen, können wir durch den austeilen, ohne eine der beiden Bedingungen zu verändern. Wir können also $ggT(x, y) = 1$ annehmen. □

Wenn wir hier n immer größer wählen, erhalten wir

Satz 6.8 (Folgerung) *Zu $q \in \mathbb{R} \setminus \mathbb{Q}$ gibt es unendlich viele verschiedene Paare (x, y) teilerfremder Zahlen $x, y \in \mathbb{Z}$ mit*

$$\left|\frac{x}{y} - q\right| < \frac{1}{y^2}.$$

Satz 6.9 *Ist* $1 < D \in \mathbb{N}$ *quadratfrei, so gibt es eine Konstante* $M \in \mathbb{R}$ *und unendlich viele verschiedene Paare* (x, y) *teilerfremder ganzer Zahlen* x, y *mit*

$$|x^2 - D \cdot y^2| < M.$$

Beweis. Es ist

$$x^2 - D \cdot y^2 = (x + \sqrt{D}y)(x - \sqrt{D}y)$$

mit $q := \sqrt{D}$ irrational. Nach Satz 6.6 gibt es unendlich viele Paare (x, y) von teilerfremden ganzen Zahlen x, y mit $y > 0$ und

$$|x - \sqrt{D}y| < \frac{1}{y}.$$

Aus der Dreiecksungleichung folgt

$$|x + \sqrt{D}y| \leq |x - \sqrt{D}y| + |2\sqrt{D}y| < \frac{1}{y} + 2\sqrt{D}y$$

und

$$|x^2 - D \cdot y^2| < \frac{1}{y} \cdot (\frac{1}{y} + 2\sqrt{D}y) = 2\sqrt{D} + \frac{1}{y^2} \leq 2\sqrt{D} + 1.$$

Mit $M := 2\sqrt{D} + 1$ ergibt sich die Behauptung. □

Satz 6.10 *Es sei* $1 < D \in \mathbb{N}$ *quadratfrei. Dann gibt es unendlich viele verschiedene Paare* (x, y) *ganzer Zahlen, welche die Pellsche* $+1$*-Gleichung*

$$x^2 - D^2y^2 = 1$$

lösen.

Beweis. Nach Satz 6.8 gibt es ein $M \in \mathbb{R}$ und unendlich viele verschiedene Paare (x, y), $y > 0$, ganzer Zahlen mit $|x^2 - Dy^2| < M$. Dann gibt es auch eine ganze Zahl m mit $|m| < M$ und unendliche viele Lösungen (x, y), $y > 0$, der Gleichung $x^2 - Dy^2 = m$. Wir können hier sogar $x > 0$ annehmen, und dass alle x-Werte voneinander verschieden sind. Weil es nur endlich viele Restklassen modulo $|m|$ gibt, folgt daraus die Existenz zweier solcher Paare (x_1, y_1) und (x_2, y_2) mit $x_1 \neq x_2$ und

$$x_1 = x_2 \, mod \, |m|, \quad y_1 = y_2 \, mod \, |m|.$$

Wir setzen

$$c_1 := x_1 - y_1\sqrt{D} \quad \text{und} \quad c_2 := x_2 + y_2\sqrt{D}.$$

Mit $x_2 = x_1 + \xi m$, $y_2 = y_1 + \eta m$, $\xi, \eta \in \mathbb{Z}$, folgt daraus

$$\begin{aligned} c_1c_2 &= x_1x_2 - D \cdot y_1y_2 + (x_1y_2 - y_1x_2)\sqrt{D} \\ &= x_1^2 + x_1\xi m - Dy_1^2 - Dy_1\eta m + (x_1y_1 + x_1\eta m - y_1x_1 - y_1\xi m)\sqrt{D} \\ &= x_1^2 - Dy_1^2 + m(x_1\xi - Dy_1\eta + (x_1\eta - y_1\xi)\sqrt{D}) \\ &= m \cdot \left[1 + x_1\xi - Dy_1\eta + (x_1\eta - y_1\xi)\sqrt{D}\right] \\ &= m(u + v\sqrt{D}) \end{aligned}$$

mit ganzen Zahlen u und v. Wegen

$$N(c_1) = x_1^2 - Dy_1^2 = m = x_2^2 - Dy_2^2 = N(c_2)$$

folgt daraus

$$m^2 = N(c_1 c_2) = m^2 \cdot (u^2 - Dv^2).$$

Also ist

$$u^2 - Dv^2 = 1,$$

und (u, v) ist eine Lösung der Pellschen Gleichung.

Wir zeigen als nächstes, dass diese Lösung nicht-trivial ist, d.h. $v \neq 0$. Aber $v = 0$ würde $u = \pm 1$ und $c_1 c_2 = \pm m$ implizieren. Wir multiplizieren diese Gleichung mit der Konjugierten $c_2' := x_2 - y_2\sqrt{D}$:

$$\begin{aligned} c_1 \cdot c_2 c_2' &= \pm m c_2', \\ c_1 \cdot N(c_2) &= \pm m c_2', \\ m c_1 &= \pm m c_2', \\ c_1 &= \pm c_2', \\ x_1 &= \pm x_2. \end{aligned}$$

Wegen $x_i > 0$ und $y_i > 0$ würde daraus $x_1 = x_2$, $y_1 = y_2$ und der Widerspruch $c_1 = c_2$ folgen.

Wir haben also eine Lösung (u, v) der Pellschen Gleichung $u^2 - Dv^2 = 1$ mit $v > 0$ gefunden. Weil $\sqrt{D}$ irrational ist, kann dann nicht $u + \sqrt{D}v = \pm 1$ gelten. Also sind die unendlich vielen Zahlen $(u + \sqrt{D}v)^n$, $n \in \mathbb{Z}$ alle voneinander verschieden. Wegen

$$N((u + \sqrt{D}v)^n) = (N(u + \sqrt{D}v))^n = 1^n = 1$$

gehören sie alle zu (unendlich vielen, voneinander verschiedenen) Lösungen der Pellschen Gleichung. □

Jetzt wissen wir, dass es im reell-quadratischen Zahlkörper $\mathbb{Q}(\sqrt{D})$ unendlich viele Einheiten gibt. Aber die Struktur der Einheitengruppe $O^*(\mathbb{Q}(\sqrt{D}))$ kennen wir noch nicht. Dazu beweisen wir zunächst eine Hilfsaussage:

Satz 6.11 *Es sei $K = \mathbb{Q}(\sqrt{D})$ ein reell-quadratischer Zahlkörper und $0 < M \in \mathbb{R}$ eine feste Schranke. Dann gibt es nur endlich viele ganz-algebraische Zahlen $c \in K$ mit $|c| < M$ und $|c'| < M$. (Hier ist $c' \in K$ die Konjugierte von c.)*

Beweis. Falls $D = 2, 3 \, mod \, 4$, sind die ganzen Zahlen c von der Form $a + b\sqrt{D}$ mit $a, b \in \mathbb{Z}$. Aus $|c| < M$ und $|c'| < M$ folgt

$$\begin{aligned} |c|^2 &= a^2 + Db^2 + 2ab\sqrt{D} &< M^2, \\ |c'|^2 &= a^2 + Db^2 - 2ab\sqrt{D} &< M^2, \\ & \qquad a^2 + Db^2 &< M^2. \end{aligned}$$

Wegen $D \neq 0$ gibt es nur endlich viele Paare (a, b) ganzer Zahlen, welche diese Ungleichung erfüllen.

Bei $D = 1 \, mod \, 4$ gibt es noch die Möglichkeit $c = (a + \sqrt{D}b)/2$, aber der Beweis (mit M ersetzt durch $2M$) verläuft ganz analog. □

Definition 6.4 *Eine* Fundamental-Einheit *im reell-quadratischen Zahlkörper K ist eine Einheit $c_0 \in O^*(K)$, derart, dass alle Einheiten $c \in O^*(K)$ von der Form*

$$\pm c_0^n,\ n \in \mathbb{Z}$$

sind.

Beispiel 6.10 *In Beispiel 2.14 haben wir bewiesen, dass $1+\sqrt{2}$ eine Fundamentaleinheit im Zahlkörper $\mathbb{Q}(\sqrt{2})$ ist.*

Satz 6.12 *Jeder reell-quadratische Zahlkörper K besitzt eine Fundamentaleinheit.*

Beweis. Nach Satz 6.10 gibt es nicht-triviale Lösungen $1 < x, y \in \mathbb{N}$ der Pellschen Gleichung $x^2 - Dy^2 = 1$, $D > 0$. Dazu gehören Einheiten $c = x + \sqrt{D}y$ in $K = \mathbb{Q}(\sqrt{D})$ mit $c > 1$. Wir wählen eine solche Einheit $c \in O^*(K)$ und eine reelle Schranke $M > c + 1$.

Aus $N(c) = cc' = 1$ folgt für die Konjugierte c' von c

$$0 < c' < 1 < M.$$

Nach Satz 6.11 gibt es nur endlich viele Einheiten $c \in O^*(K)$ mit $0 < c, c' < M$ und deswegen auch nur endlich viele Einheiten $c \in O^*(K)$ mit $1 < c < M$. Die kleinste davon wählen wir und nennen sie c_0. Ich behaupte: c_0 ist eine Fundamentaleinheit.

Zu zeigen ist: Jede positive Einheit $0 < e \in O^*(K)$ ist eine Potenz von c_0. Der Beweis dazu verläuft wie üblich. Die Intervalle $[c_0^n, c_0^{n+1}), n \in \mathbb{Z}$, bilden eine disjunkte Überdeckung der positiven reellen Halbachse. In einem dieser Intervalle muss e liegen. Es gibt also eine ganze Zahl n mit $c_0^n \le e < c_0^{n+1}$. Auch e/c_0^n ist eine Einheit. Für sie gilt

$$1 \le \frac{e}{c_0^n} < \frac{c_0^{n+1}}{c_0^n} = c_0.$$

Weil c_0 die kleinste Einheit > 1 ist, muss $e/c_0^n = 1$, d.h. $e = c_0^n$ gelten. □

Satz 6.13 (Korollar) *Die Einheitengruppe $O^*(K)$ eines reell-quadratischen Zahlkörpers K ist isomorph zum Produkt $\mathbb{Z}_2 \times \mathbb{Z}$.*

Beweis. Die zyklische Gruppe $\mathbb{Z}_2 \in O^*(K)$ wird erzeugt von -1, und eine unendliche zyklische Gruppe $\simeq \mathbb{Z}$ wird erzeugt von einer Fundamentaleinheit $c_0 > 1$. Und dann ist $O^*(K)$ das direkte Produkt beider Untergruppen. □

Die Fundamental-Einheit $c_0 = a + b\sqrt{D} \in O^*(K)$ ist nicht eindeutig bestimmt. Denn mit c sind auch die vier Zahlen

$$\pm a \pm b\sqrt{D}$$

Fundamental-Einheiten. Jede davon liegt in genau einem der vier offenenen Intervalle

$$(-\infty, -1), \quad (-1, 0), \quad (0, 1), \quad (1, \infty).$$

Die Fundamentaleinheit $c_0 \in (1, \infty)$ mit $a, b > 0$ ist allerdings eindeutig bestimmt. Für sie ist a minimal unter allen Einheiten $c > 1$.

Beispiel 6.11 *In $K = \mathbb{Q}(\sqrt{3})$ ist $c := 2 + \sqrt{3}$ eine Einheit, weil $N(c) = 4 - 3 = 1$. Wenn c keine Fundamental-Einheit wäre, gäbe es eine Einheit $c' = 1 + b\sqrt{3}$, $1 \leq b \in \mathbb{N}$. Wegen*

$$N(c') = 1 - 3b^2 \leq -2$$

kann ein solches c' aber keine Einheit sein. Also ist c eine Fundamental-Einheit in $\mathbb{Q}(\sqrt{3})$.

In $K = \mathbb{Q}(\sqrt{5})$ ist

$$c := \frac{1}{2}(1 + \sqrt{5})$$

eine Einheit, denn $N(c) = -1$. Weil es in K keine ganz-algebraische Zahl $a + b\sqrt{5}$ mit $0 < a < 1/2$ gibt, ist c eine Fundamentaleinheit.

In $K = \mathbb{Q}(\sqrt{13})$ ist $c = (3 + \sqrt{13})/2$ eine Einheit wegen $N(c) = -1$. Wäre c keine Fundamental-Einheit, gäbe es in K Einheiten

$$c_1 = 1 + b\sqrt{13} \quad \textit{oder} \quad c_2 = (1 + b\sqrt{13})/2, \quad 0 < b \in \mathbb{N}.$$

Wegen $N(c_1) = 1 - 13b^2 \leq -12$ und $N(c_2) = (1 - 13b^2)/4 \leq -3$ ist dies aber unmöglich. Also ist c eine Fundamental-Einheit.

In $K = \mathbb{Q}(\sqrt{10})$ ist $c := 3 + \sqrt{10}$ eine Einheit mit $N(c) = -1$. Wäre sie keine Fundamental-Einheit, gäbe es in K Einheiten

$$c_1 = 2 + b\sqrt{10} \quad \textit{oder} \quad c_2 = 1 + b\sqrt{10}, \quad 0 < b \in \mathbb{N}.$$

Wegen $N(c_1) = 4 - 10b^2 \leq -6$ und $N(c_2) = 1 - 10b^2 \leq -9$ ist dies aber nicht möglich. Also ist $c \in \mathbb{Q}(\sqrt{10})$ eine Fundamental-Einheit.

Eine Fundamental-Einheit in $\mathbb{Q}(\sqrt{94})$ ist die schöne große Zahl

$$2143295 + 221064\sqrt{94}.$$

Das möchte ich jetzt aber nicht mehr nachprüfen.

Aufgabe 6.6 *Finden Sie Fundamental-Einheiten für $\mathbb{Q}(\sqrt{15})$ und $\mathbb{Q}(\sqrt{39})$.*

Aufgabe 6.7 *Zeigen Sie: Für jedes k, $1 \leq k \leq p - 1$, ist*

$$\frac{sin(\frac{k\pi}{p})}{sin(\frac{\pi}{p})}$$

eine Einheit in $\mathbb{Q}(\sqrt[p]{1})$.

Aufgabe 6.8 *Es sei K ein reell-quadratischer Zahlkörper. Zeigen Sie: In K gibt es Einheiten $e \neq 1$ mit beliebig kleinem Abstand $|e - 1| > 0$.*

Aufgabe 6.9 *Es sei $D = 1 \, mod \, 8$ eine quadratfreie ganze Zahl. Zeigen Sie:*

a) Ist $e := (x + y\sqrt{D})/4$, $x, y \in \mathbb{Z}$ eine Einheit in $\mathbb{Q}(\sqrt{D})$, so sind x und y gerade.

b) Ist e eine Einheit, so ist $e^3 = u + v\sqrt{D}$ mit $u, v \in \mathbb{Z}$.

6.3 Irreduzible ganz-algebraische Zahlen

Wieder sei $K \subset \mathbb{C}$ ein algebraischer Zahlkörper mit seinem Ring $O(K)$ der ganz-algebraischen Zahlen und der Gruppe $O^*(K)$ der Einheiten. Nach Definition 2.19 heißt $c \in O(K)$, $c \neq 0$, keine Einheit, *irreduzibel*, wenn c die folgende Eigenschaft hat: Ist $c = a \cdot b$ mit a und $b \in O(K)$, dann ist entweder a oder b eine Einheit $\in O^*(K)$.

Satz 6.14 *Wenn die Zahl $|N_{K/\mathbb{Q}}(c)| \in \mathbb{N}$ eine Primzahl ist, dann ist $c \in O(K)$ irreduzibel.*

Beweis. Es sei $c = a \cdot b$ mit a und $b \in O(K)$. Wegen der Multiplikativität der Norm (Satz 5.8) ist

$$|N(c)| = |N(a)| \cdot |N(b)|, \quad |N(a)|, |N(b)| \in \mathbb{N},$$

eine Primzahl. Daraus folgt entweder $N(a) = \pm 1$ oder $N(b) = \pm 1$. Nach Satz 6.6 ist also entweder a oder b eine Einheit in $O(K)$. □

Beispiel 6.12 *Die irreduziblen Zahlen in $O(\mathbb{Q}) = \mathbb{Z}$ sind genau die Zahlen $\pm p$, wo $p \in \mathbb{N}$ eine Primzahl ist. Das ist vertrauensbildend. Dumm ist allerdings, dass Primzahlen $p \in \mathbb{N}$ in algebraischen Erweiterungen K von $\mathbb{Q}$ reduzibel sein können. So gilt etwa in $K = \mathbb{Q}(i)$*

$$5 = (2 + i) \cdot (2 - i), \quad 2 \pm i \in O(K).$$

Wegen

$$N_{K/\mathbb{Q}}(2 + i) = N_{K/\mathbb{Q}}(2 - i) = 5$$

sind beide Faktoren $2 \pm i$ keine Einheit in K. Deswegen ist die Primzahl 5 nicht irreduzibel in $\mathbb{Q}(i)$. Satz 6.14 greift hier nicht, denn nach Satz 5.7 ist

$$N_{\mathbb{Q}(i)/\mathbb{Q}}(5) = 5^2$$

keine Primzahl.

Zwei Zahlen c_1 und $c_2 \in O(K)$ sind assoziiert, wenn es eine Einheit $e \in O^*(K)$ gibt mit $c_2 = e \cdot c_1$. Ist $c \in O(K)$ irreduzibel, so sind auch alle zu c assoziierten Zahlen in $O(K)$ irreduzibel.

Satz 6.15 *Jede ganz-algebraische Zahl $c \in O(K)$, keine Einheit, besitzt eine Produkt-Zerlegung*

$$c = c_1 \cdot \ldots \cdot c_k$$

mit irreduziblen ganz-algebraischen Zahlen $c_1, \ldots, c_k \in O(K)$.

Beweis. Ist c selbst irreduzibel, so ist nichts zu zeigen. Andernfalls gilt $c = c_1 \cdot c_2$, wo $c_1, c_2 \in O(K)$ keine Einheiten sind. Also ist für $j = 1, 2$

$$|N_{K/\mathbb{Q}}(c_j)| > 1,$$

und die Behauptung folgt durch Induktion nach $|N_{K/\mathbb{Q}}(c)|$. □

Satz 6.16 (Euklid) *In jedem algebraischen Zahlkörper $K \subset \mathbb{C}$ gibt es unendlich viele, nicht assoziierte irreduzible ganz-algebraische Zahlen.*

Beweis. Wegen $2 \in \mathbb{Z} \subset O(K)$ ist $2 = c_1 \cdot ... \cdot c_k$ nach Satz 6.15 ein Produkt irreduzibler ganz-algebraischer Zahlen $c_j \in O(K)$. Es gibt also mindestens eine irreduzible Zahl $c_1 \in O(K)$. Wir zeigen durch Induktion nach $n \in \mathbb{N}$, dass es mehr als n solcher Zahlen gibt:

Seien etwa $c_1, ..., c_n \in O(K)$ irreduzible ganz-algebraische Zahlen, und $c := 1 + |N_{K/\mathbb{Q}}(c_1 \cdot ... \cdot c_n)| = 1 + |N(c_1)| \cdot ... \cdot |N(c_n)| \in \mathbb{Z} \subset O(K)$. Keine der Zahlen $c_1, ..., c_n$ kann c in $O(K)$ teilen, denn wegen $c_\nu | \pm N(c_\nu)$ würde sie auch 1 teilen und wäre eine Einheit. Das ist aber ausgeschlossen.

Weiter kann c auch keine Einheit $\in O(K)$ sein, denn wegen $|N(c_\nu)| > 1$ ist $c > 1$. Mit Satz 5.7 folgt daraus

$$N_{K/\mathbb{Q}}(c) = c^{[K:\mathbb{Q}]} > 1,$$

und $N_{K/\mathbb{Q}}(c) \neq \pm 1$.

Nach Satz 6.15 besitzt c eine Zerlegung in irreduzible Faktoren. Keiner dieser Faktoren kann mit $c_1, c_2, ...,$ oder c_n übereinstimmen. Also gibt es noch mindestens eine weitere irreduzible Zahl $c_{n+1} \in O(K)$. □

Dies waren die guten Nachrichten. Aber leider gibt es mehr schlechte Nachrichten: Zunächst einmal brauchen die uns geläufigen klassischen Primzahlen $p = 2, 3, 5, ... \in \mathbb{N}$ nicht irreduzibel in einer algebraischen Erweiterung K von $\mathbb{Q}$ zu sein.

Definition 6.5 *Die Primzahl $p \in \mathbb{N}$* zerfällt *in dem Zahlkörper K , wenn sie eine Produktzerlegung $p = c_1 \cdot c_2$ in ganz-algebraische Zahlen $c_1, c_2 \in K$ zulässt, von denen keine eine Einheit ist.*

Sowas ist schnell passiert:

Beispiel 6.13 *Es sei $K = \mathbb{Q}(i)$. In K zerfallen z.B. die Primzahlen*

$$2 = (1+i) \cdot (1-i) \quad \textit{oder} \quad 5 = (2+i) \cdot (2-i).$$

Weil die Faktoren hier nicht die Norm 1 haben, sind sie keine Einheiten.

Im fünften Kreisteilungskörper $K = \mathbb{Q}(\sqrt[5]{1})$ mit der primitiven Einheitswurzel $\epsilon = e^{2\pi i/5}$ sind die vier Zahlen $2 + \epsilon^k$, $k = 1, 2, 3, 4$, ganz-algebraisch und haben das Produkt

$$\begin{aligned}
(2+\epsilon)(2+\epsilon^2)(2+\epsilon^3)(2+\epsilon^4) &= (2+\epsilon)(2+\epsilon^4) \cdot (2+\epsilon^2)(2+\epsilon^3) \\
&= (4 + 2(\epsilon+\epsilon^4) + 1) \cdot (4 + 2(\epsilon^2+\epsilon^3) + 1) \\
&= (5 + 2(\epsilon+\epsilon^4)) \cdot (5 + 2(\epsilon^2+\epsilon^3)) \\
&= 25 + 10(\epsilon+\epsilon^2+\epsilon^3+\epsilon^4) + 4(\epsilon+\epsilon^2+\epsilon^3+\epsilon^4) \\
&= 25 - 10 - 4 \\
&= 11.
\end{aligned}$$

Die Primzahl 11 zerfällt hier also.

Satz 6.17 *a) Es sei K ein Zahlkörper über $\mathbb{Q}$. Jede Primzahl $p \in \mathbb{N}$, die (bis auf das Vorzeichen) Norm $\pm N_{K/\mathbb{Q}}(c)$ einer ganz-algebraischen Zahl $c \in K$ ist, zerfällt in K.*

b) Ist $K = \mathbb{Q}(\sqrt{D})$ ein quadratischer Zahlkörper, so gilt auch die Umkehrung: p zerfällt genau dann in K, wenn $p = \pm N(c)$ (bis auf das Vorzeichen) die Norm einer ganz-algebraischen Zahl $c \in K$ ist.

Beweis. a) Wenn $p = \pm N(c)$ mit einer ganz-algebraischen Zahl $c \in K$ ist, so ist nach Satz 5.7

$$p = ((\pm c) \cdot c_2 \cdot ... \cdot c_n)^{[K:\mathbb{Q}(c)]},$$

wo $c_2, ..., c_n \in K$ die Konjugierten von c sind. Offensichtlich muss $[K : \mathbb{Q}(c)] = 1$ sein. Wegen $N(c_i) = N(c) = \pm p \neq 1$ ist keine der Zahlen $c, c_2, ..., c_n$ eine Einheit. Dann ist auch $c' = c_2 \cdot ... \cdot c_n$ keine Einheit und $p = (\pm c) \cdot c'$ zerfällt in K.

b) Die Primzahl p zerfalle in $K = \mathbb{Q}(\sqrt{D})$, also etwa $p = c \cdot c'$ mit $N(c)$ und $N(c') \neq \pm 1$. Nach Satz 5.7 folgt

$$N(c) \cdot N(c') = N_{K/\mathbb{Q}}(p) = p^2$$

und $N(c) = N(c') = \pm p$. □

Satz 6.18 *a) Wenn die Primzahl p im quadratischen Zahlkörper $\mathbb{Q}(\sqrt{D})$ zerfällt, dann ist D ein quadratischer Rest modulo p.*

b) Wenn der Ring $O(\mathbb{Q}(\sqrt{D}))$ faktoriell ist, dann gilt auch eine teilweise Umkehrung von a): Es sei $p > 2$ eine Primzahl. Wenn D quadratischer Rest modulo p ist, dann zerfällt p in $\mathbb{Q}(\sqrt{D})$.

Beweis. a) Für $D = 2$ oder 3 modulo 4 sind die ganzen Zahlen in $K = \mathbb{Q}(\sqrt{D})$ von der Form $a + b\sqrt{D}$, $a, b \in \mathbb{Z}$. Nach Satz 6.17 b) zerfällt p genau dann, wenn

$$\pm p = N(a + b\sqrt{D}) = a^2 - D \cdot b^2, \quad a, b \in \mathbb{Z},$$

ist. Hier kann b nicht durch p teilbar sein, denn dann wäre dies auch a, und p^2 würde p teilen, das geht nicht. Also ist $b \, mod \, p$ eine prime Restklasse modulo p. Es gibt eine ganze Zahl b' mit $bb' = 1 \, mod \, p$. Daraus folgt

$$0 = a^2(b')^2 - Db^2(b')^2 = (ab')^2 - D \quad mod \quad p,$$

d.h., D ist ein quadratischer Rest modulo p.

Für $D = 1 \, mod \, 4$ gibt es noch den Fall

$$\pm p = N(\frac{a}{2} + \frac{b}{2}\sqrt{D}) = \frac{1}{4}(a^2 - b^2 D),$$

oder

$$a^2 - Db^2 = \pm 4p.$$

Wieder kann b nicht durch p teilbar sein, denn daraus würde folgen

$$p|a, \quad p^2|(a^2 - Db^2) = 4p, \quad p|4, \quad p = 2,$$

im Widerspruch zu $p = 1 \, mod \, 4$. Es gibt also ein $b' \in \mathbb{Z}$ mit $bb' = 1 \, mod \, p$ und

$$(a^2 - Db^2)(b')^2 = (ab')^2 - D = \pm 4p(d')^2 = 0 \quad mod \quad p.$$

Auch jetzt ist D ein quadratischer Rest modulo p.

b) Wenn D quadratischer Rest modulo p ist, dann gibt es ganze Zahlen m und $q \in \mathbb{Z}$ mit

$$D = m^2 + p \cdot q, \quad \text{bzw.} \quad p \cdot q = D - m^2 = -(m - \sqrt{D}) \cdot (m + \sqrt{D}).$$

Nach Voraussetzung besitzt $p \cdot q$ eine eindeutige Zerlegung in irreduzible Faktoren aus $O(\mathbb{Q}(\sqrt{D}))$. Einer dieser Faktoren, etwa c, muss dann p teilen und auch entweder $m + \sqrt{D}$ oder $m - \sqrt{D}$. Der Faktor c kann nicht assoziiert zu p sein, denn dann wäre $(m \pm \sqrt{D})/p$ ganz-algebraisch in $\mathbb{Q}(\sqrt{D})$. Weil $p > 2$ vorausgesetzt ist, geht das nicht. Also ist c ein echter Teiler von p, und die Primzahl p zerfällt. □

Es kommt noch schlimmer: Die irreduziblen ganz-algebraischen Zahlen brauchen im Ring $O(K)$ nicht prim im Sinn von Definition 2.19 zu sein. Dann ist nach Satz 2.17 die Zerlegung in irreduzible Faktoren in $O(K)$ nicht eindeutig, und $O(K)$ ist nicht faktoriell. Hierzu das Standard-Beispiel:

Beispiel 6.14 *In* $K = \mathbb{Q}(\sqrt{-5})$ *ist*

$$21 = 3 \cdot 7 = (4 + \sqrt{-5}) \cdot (4 - \sqrt{-5}).$$

Alle beteiligten Faktoren sind sind irreduzibel. Das ist allerdings nicht ganz offensichtlich:

Wäre 3 *nicht irreduzibel in* K*, so würde aus Satz 6.17 b)*

$$3 = N(a + b\sqrt{-5}) = a^2 + 5b^2, \quad a, b \in \mathbb{Z},$$

folgen. Offensichtlich geht das nicht.

Wäre 7 *nicht irreduzibel, so hätten wir ebenso*

$$7 = N(a + b\sqrt{-5}) = a^2 + 5b^2, \quad a, b \in \mathbb{Z}.$$

Es würde $b^2 = 0$ *oder* $= 1$ *folgen, und das geht auch nicht.*

Nehmen wir nun an

$$4 + \sqrt{-5} = c \cdot c', \quad c, c' \in O(K), N(c), N(c') > 1,$$

wäre nicht irreduzibel. Wegen $N(4 + \sqrt{-5}) = 21$ *hätten wir o.B.d.A.* $N(c) = 3$, $N(c') = 7$. *Wie wir gerade gesehen haben geht das aber nicht. Weil* $4 - \sqrt{-5}$ *konjugiert zu* $4 + \sqrt{-5}$ *ist, muss auch dieser Faktor irreduzibel sein.*

Sehr verwirrend ist hier auch der übliche Sprachgebrauch: In der Zahlentheorie nennt man die irreduziblen ganz-algebraischen Element eines Zahlkörpers seine Prim-Elemente oder Prim-Zahlen, obwohl sie eben i.A. nicht prim im Sinn der Ring-Theorie sind.

Weil in einem quadratischen Zahlkörper K i.A. die irreduziblen ganzen Zahlen nicht prim sind, ist die Zerlegung in irreduzible Faktoren i.A. nicht eindeutig. I.A. ist also der Ring $O(K)$ nicht faktoriell. (Satz 2.17) Es ist merkwürdig, dass es aber doch ein paar solche Körper gibt, wo der Ring $O(K)$ faktoriell, und sogar euklidisch ist. Das ist der eigentliche Grund für die Wichtigkeit des euklidischen Algorithmus. Als euklidische Gradfunktion nehmen wir dabei $|N(c)|$. Wir erinnern uns an Satz 5.6: Es ist $N(c) = 0$ nur dann, wenn $c = 0$.

Definition 6.6 *Der quadratische Zahlkörper heißt* Norm-euklidisch, *wenn der Ring $O(K)$ mit dieser Norm ein euklidischer Ring ist.*

Wir erinnern uns mühsam, was das bedeutet: Zu je zwei ganz-algebraischen Zahlen $a, b \in O(K)$ mit $b \neq 0$ gibt es ganz-algebraische Zahlen $q, r \in O(K)$ derart, dass

$$a = b \cdot q + r, \quad |N(r)| < |N(b)|.$$

Wenn wir diese Zeile durch b austeilen, und benutzen, dass die Norm multiplikativ ist, wird sie äquivalent zu

$$\frac{a}{b} = q + \frac{r}{b}, \quad |N(\frac{r}{b})| < 1.$$

Das ist nun wieder äquivalent zu folgender Eigenschaft: Zu jeder Zahl $c \in K, (c = a/b)$, gibt es eine ganz-algebraische Zahl $q \in O(K)$ mit

$$|N(c - q)| < 1.$$

Beispiel 6.15 *Die Zahlen in $\mathbb{Q}(i)$ sind von der Form $u+v\cdot i$, $u, v \in \mathbb{Q}$, und die ganz-algebraischen (die ganzen Gaußschen Zahlen) sind diejenigen, wo $u = m$ und $v = n$ ganzzahlig ist. Nun liegt jede komplexe Zahl $c = u + v \cdot i$ in genau einem Quadrat der Seitenlänge 1 mit ganzzahligen Ecken $m + n \cdot i$, $m + 1 + n \cdot i$, $m + (n + 1) \cdot i$, $m + 1 + (n + 1) \cdot i$. Es gibt eine dieser Ecken, $= q$, von der c einen Abstand*

$$|c - q| \leq \sqrt{(\frac{1}{2})^2 + (\frac{1}{2})^2} = \sqrt{\frac{1}{2}}$$

besitzt. In $Q(i)$ ist aber $N(c) = |c^2|$ und es folgt

$$N(c - q) = |c - q|^2 \leq \frac{1}{2} < 1.$$

Wir haben gezeigt: Die ganzen Zahlen in $\mathbb{Q}(i)$ bilden einen norm-euklidischen Ring! Es gibt noch vier andere derartige imaginär-quadratische Körper:

Satz 6.19 *Die ganz-algebraischen Zahlen des imaginär-quadratischen Körpers $K = \mathbb{Q}(\sqrt{D})$, $D < 0$ quadratfrei, bilden einen norm-euklidischen Ring genau dann, wenn*

$$D \quad = \quad -1, \quad -2, \quad -3, \quad -7, \quad -11.$$

Beweis. Die ganzen Zahlen in K sind $q = m + n\sqrt{D}, m, n \in \mathbb{Z}$, und jede Zahl $c \in K$ liegt in genau einem Rechteck mit den Ecken q, $q+1$, $q+\sqrt{D}$, $q+1+\sqrt{D}$. Verschieben wir c um $-q$, so sehen wir: es genügt zu zeigen, dass zu jeder Zahl $c \in K$ im Rechteck mit den Ecken 0, 1, $\sqrt{D}$, $1+\sqrt{D}$ eine ganze Zahl $q \in O(K)$ existiert mit

$$N(c-q) < 1.$$

Dieses Rechteck nennen wir das Fundamental-Rechteck.

Nun ist für $x + y\sqrt{D}$

$$N(x+y\sqrt{D}) = x^2 + |D|y^2 = \left|x + i\sqrt{|D|}y\right|^2$$

das Quadrat der üblichen komplexen Norm. Die Menge $N(c-q) < 1$ ist deswegen das Innere des normalen Kreises um q vom Radius 1 in der komplexen Ebene.

Wir müssen die Fälle $d = 2,\ 3\, mod\, 4$ und $d = 1\, mod\, 4$ unterscheiden:

$D = 2,\ 3\, mod\, 4$: Hier ist die Frage, ob die vier Kreise vom Radius 1 um die Ecken des Fundamentalrechtecks das ganze Rechteck überdecken. Das ist offenbar genau dann der Fall, wenn der Mittelpunkt

$$m = \frac{1}{2}(1+\sqrt{D})$$

einen Abstand < 1 vom Nullpunkt besitzt. Das bedeutet

$$\begin{aligned} \frac{1}{4}(1+|D|) &< 1, \\ 1+|D| &< 4 \\ |D| &< 3. \end{aligned}$$

Wir erhalten die beiden Fälle $D = -1$ und $D = -2$.

$D = 1\, mod\, 4$. Da gibt es im Fundamentalrechteck noch die ganz-algebraische Zahl

$$m = \frac{1}{2} + \frac{1}{2}\sqrt{D},$$

den Mittelpunkt. Jetzt stellt sich die Frage, ob die fünf Einheitskreise (um die vier Ecken und um m) das ganze Rechteck überdecken. Der Kreis um $q = 0$ trifft die Gerade $x = 1/2$ in den Punkten $1/2 + iy$ mit $y^2 < 3/4$. Die Frage ist also: Wann liegt der Punkt $(1+i\sqrt{3})/2$ im Inneren des Einheitskreises um m? Die Bedingung ist

$$\begin{aligned} \frac{1}{2}\sqrt{3}+1 &> \frac{1}{2}\sqrt{|D|}, \\ 2+\sqrt{3} &> \sqrt{|D|}, \\ 7+4\sqrt{3} &> |D|. \end{aligned}$$

Wegen $7 + 4\sqrt{3} > 11$ ist dies für $|D| = 3, 7$ oder 11 noch der Fall, wegen $7 + 4\sqrt{3} < 15$ für $|D| \geq 15$ aber nicht mehr. □

Schwieriger ist der reell-quadratische Fall $K = \mathbb{Q}(\sqrt{D})$ mit $D > 0$. Die Norm von $a+b\sqrt{D}$ ist jetzt a^2-Db^2 und $|N(c)| < 1$ beschreibt die Punkte $(x, y) = (a, b\sqrt{D})$ der Ebene mit $|x^2-y^2| < 1$. Tröstlich daran ist eigentlich nur, dass das Quadrat $|x| < 1$, $|y| < 1$ mit Seitenlänge 2 zu diesem Bereich gehört.

Satz 6.20 *Die ganz-algebraischen Zahlen im reell-quadratischen Zahlkörper $K = \mathbb{Q}(\sqrt{D})$, $D > 0$ quadratfrei, bilden jedenfalls dann einen norm-euklidischen Ring, wenn*

$$D \quad = \quad 2, \quad 3, \quad 5, \quad 13.$$

Beweis. Wieder haben wir in der Ebene ein Fundamentalrechteck mit den Ecken

$$(0,0), \quad (1,0), \quad (0,\sqrt{D}), \quad (1,\sqrt{D}).$$

Wenn seine Höhe $\sqrt{D} < 2$ ist, wird es durch die vier Quadrate der Seitenlänge 2, zentriert in den vier Ecken, überdeckt. Dies liefert die Aussage für $D < 4$, $D = 2, 3$.

Für $D = 1 \, mod \, 4$ gehört auch noch der Mittelpunkt

$$m = (\frac{1}{2}, \frac{\sqrt{D}}{2})$$

zu einer ganz-algebraischen Zahl. Das in ihm zentrierte Quadrat der Seitenlänge 2 schneidet aus der linken und rechten Seite des Fundamentalrechtecks die Strecken

$$(0,t) \text{ und } (1,t) \quad \text{mit} \quad \frac{\sqrt{D}}{2} - 1 < t < \frac{\sqrt{D}}{2} + 1$$

aus. Zusammen mit den in den Ecken zentrierten Quadraten überdeckt es das ganze Fundamentalrechteck genau dann, wenn

$$\frac{\sqrt{D}}{2} - 1 < 1, \quad \sqrt{D} < 4, \quad D < 16.$$

Dies liefert die Fälle $D = 5$ und 13. □

Der eben bewiesene Satz 6.20 ist nicht scharf, weil das Gebiet $|x^2 - y^2| < 1$ einfach durch ein darin gelegenes Quadrat ersetzt wurde. Tut man das nicht, so kann man die Eigenschaft „norm-euklidisch“ noch für $D = 6$ und 7 beweisen. (S. das in 6.1 zitierte Buch von Cohn. Den Beweis konnte ich allerdings nicht nachvollziehen, auch enthält das Buch entstellende Druckfehler.) Das ist alles auch nicht so wichtig, denn es kommt vor allem auf die Folgerungen aus dieser Eigenschaft an: Wenn der Ring $O(K)$ euklidisch ist, dann ist er auch ein Hauptidealring und nach Satz 2.19 faktoriell. Irreduzible Zahlen sind prim und die Zerlegung in irreduzible Faktoren ist eindeutig.

Es ist eine berühmte Vermutung von Gauß, die erst in der zweiten Hälfte des 19. Jahrhunderts von H. Stark bewiesen wurde, dass der Ring der ganzen Zahlen in einem imaginär-quadratischen Zahlkörper $Q(\sqrt{D})$ genau für die neun Zahlen

$$D \quad = \quad -1, \quad -2, \quad -3, \quad -7, \quad -11, \quad -19, \quad -43, \quad -67, \quad -163$$

faktoriell ist. Es ist eine offene Vermutung, dass dies für unendlich viele reell-quadratische Zahlkörper der Fall ist.

Die Faktorialität des Rings der ganzen Zahlen in $\mathbb{Q}(\sqrt{D})$ hat sehr bemerkenswerte zahlentheoretische Konsequenzen. Schauen wir uns das mal in den einfachsten Fällen an.

Beispiel 6.16 (D=-1) *Ein Primzahl p zerfällt in $\mathbb{Q}(\sqrt{-1})$ genau dann, wenn $\pm p = N(c) = a^2 + b^2$ ist, wo $c = a + b \cdot i$. Natürlich kommt $-p$ hier nicht in Frage. Also zerfällt p genau dann, wenn man es als Summe zweier Quadrate schreiben kann. Wegen $2 = 1 + 1$ gilt das für $p = 2$ trivialerweise. Und für $p > 2$ sagt Satz 6.18 a): $p = a^2 + b^2$ ist Summe zweier Quadrate genau dann, wenn -1 quadratischer Rest modulo p ist. Nach Beispiel 2.30 ist dies genau dann der Fall, wenn $p = 1 \, mod \, 4$ ist. Das ist ein klassisches Resultat von Euler.*

Beispiel 6.17 (D=-2) *Die Primzahl p zerfällt in $\mathbb{Q}(\sqrt{-2})$ genau dann, wenn man sie als $a^2 + 2b^2$ mit ganzen Zahlen a und b schreiben kann. Wieder geht das für $p = 2 = 0 + 2 \cdot 1^2$ auf triviale Weise. Und für $p > 2$ ist dies nach Satz 6.18 a) genau dann der Fall, wenn -2 quadratischer Rest modulo p ist. Wir betrachten die Fälle*

$p = 1 \, mod \, 4$: Jetzt ist -1 quadratischer Rest modulo p und die Bedingung ist genau dann erfüllt, wenn auch 2 quadratischer Rest modulo p ist. Nach Beispiel 2.32 ist dies genau dann der Fall, wenn $(p-1)/4$ gerade, also $p = 1 \, mod \, 8$ ist.

$p = 3 \, mod \, 4$: Jetzt ist -1 kein quadratischer Rest modulo p, und die Bedingung ist genau dann erfüllt, wenn 2 auch keiner ist. Nach Beispiel 2.32 ist letzteres genau dann der Fall, wenn $(p+1)/4$ ungerade ist. Und das bedeutet $p = 3 \, mod \, 8$.

Wir haben gezeigt: Eine Primzahl $p > 2$ lässt sich genau dann als $a^2 + 2b^2$, $a, b \in \mathbb{Z}$, schreiben, wenn $p = 1$ oder $= 3 \, mod \, 8$ ist.

Beispiel 6.18 (D=-3) *Eine Primzahl p zerfällt genau dann, wenn $p = a^2 + 3b^2$, $a, b \in \mathbb{Z}$ ist. Für $p = 2$ geht das nicht (2 ist kein quadratischer Rest modulo 3), und für $p = 3$ geht es auf triviale Weise. Die Bedingung aus Satz 6.18 b) lautet jetzt: -3 ist quadratischer Rest modulo p. wieder unterscheiden wir:*

$p = 1 \, mod \, 4$, es ist -1 quadratischer Rest modulo p, und die Frage ist: Wann ist 3 quadratischer Rest modulo p? Nach dem quadratischen Reziprozitätsgesetz ist dies genau dann erfüllt, wenn p quadratischer Rest modulo 3 ist, d.h., $p = 1 \, mod \, 3$.

$p = 3 \, mod \, 4$, nun ist -1 kein quadratischer Rest modulo p, und wir müssen entscheiden: Wann ist auch 3 kein quadratischer Rest modulo p? Nach dem quadratischen Reziprozitätsgesetz gilt dies genau dann, wenn p quadratischer Rest, also $p = 1 \, mod \, 3$ ist.

Wir haben gefunden: Eine Primzahl $p > 3$ lässt sich genau dann in der Form $a^2 + 3b^2$, $a, b \in \mathbb{Z}$, schreiben, wenn $p = 1 \, mod \, 3$ ist.

Beispiel 6.19 (D=2) *Eine Primzahl p zerfällt, wenn p oder $-p$ eine Norm $N(c) = a^2 - 2b^2$, $a, b \in \mathbb{Z}$ ist. Für $p > 2$ ist die Bedingung (Satz 6.18 b), Beispiel 2.32)*

$$(-1)^{(p^2-1)/8} = \left(\frac{2}{p}\right) = 1.$$

Es muss also $(p^2 - 1)/8$ gerade sein, und $p = \pm 1 \, mod \, 8$.

Beispiel 6.20 (D=3) *Die Primzahl p zerfällt, genau dann, wenn $\pm p = a^2 - 3b^2$, $a, b \in \mathbb{Z}$, ist. Für $p = 2$ und für $p = 3$ geht das auf triviale Weise. Für $p > 3$ lautet die Bedingung: 3 ist quadratischer Rest modulo p. Das quadratische Reziprozitätsgesetz liefert für $p = 1 \, mod \, 4$*

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = 1$$

genau dann, wenn $p = 1 \, mod \, 3$. Mit $p = 1 \, mod \, 4$ ist dies äquivalent zu $p = 1 \, mod \, 12$. Für $p = 3 \, mod \, 4$ lautet das quadratische Reziprozitätsgesetz

$$\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = 1$$

genau dann, wenn $p = 2 \, mod \, 3$. Zusammen mit $p = 3 \, mod \, 4$ ist dies äquivalent zu $p = -1 \, mod \, 12$.

Wir stellen die Resultate zusammen:

$p = a^2 + b^2$	$p = 2$, oder $p = 1 \, mod \, 4$;
$p = a^2 + 2b^2$	$p = 2$, oder $p = 1$ oder $3 \, mod \, 8$;
$p = a^2 + 3b^2$	$p = 3$, oder $p = 1 \, mod \, 3$;
$\pm p = a^2 - 2b^2$	$p = 2$, oder $p = \pm 1 \, mod \, 8$;
$\pm p = a^2 - 3b^2$	$p = 2, 3$, oder $p = \pm 1 \, mod \, 12$.

Weil das so lustig ist, sehen wir uns die einfachsten Beispiele an:

$p = 1 \, mod \, 4$	5	13	17	29	37	41
$a^2 + b^2$	$1 + 2^2$	$2^2 + 3^2$	$1 + 4^2$	$2^2 + 5^2$	$1 + 6^2$	$4^2 + 5^2$

$p = 1 \, bzw. \, 3 \, mod \, 8$	3	11	17	19	41	43
$a^2 + 2 \cdot b^2$	$1 + 2 \cdot 1$	$3^2 + 2 \cdot 1$	$3^2 + 2 \cdot 2^2$	$1 + 2 \cdot 3^2$	$3^2 + 2 \cdot 4^2$	$5^2 + 2 \cdot 3^2$

$p = 1 \, mod \, 3$	7	13	19	31	37	43
$a^2 + 3 \cdot b^2$	$2^2 + 3 \cdot 1$	$1 + 3 \cdot 2^2$	$4^2 + 3 \cdot 1$	$2^2 + 3 \cdot 3^2$	$5^2 + 3 \cdot 2^2$	$4^2 + 3 \cdot 3^2$

$p = \pm 1 \, mod \, 8$	7	17	23	31	41	47
$a^2 - 2 \cdot b^2$	$3^2 - 2 \cdot 1$	$5^2 - 2 \cdot 2^2$	$5^2 - 2 \cdot 1$	$7^2 - 2 \cdot 3^2$	$7^2 - 2 \cdot 2^2$	$7^2 - 2 \cdot 1$

$p = \pm 1 \, mod \, 12$	11	13	23	37	47	61
$\pm(a^2 - 3 \cdot b^2)$	$3 \cdot 3^2 - 4^2$	$4^2 - 3 \cdot 1$	$3 \cdot 4^2 - 5^2$	$7^2 - 3 \cdot 2^2$	$3 \cdot 4^2 - 1$	$8^2 - 3 \cdot 1$

Aufgabe 6.10 *Zeigen Sie, dass die folgenden Zahlen in $\mathbb{Q}(\sqrt{-5})$ irreduzibel sind:*

$$1 + 2\sqrt{-5}, \quad 2 + \sqrt{-5}, \quad 3 + \sqrt{-5}.$$

Aufgabe 6.11 *Untersuchen Sie, ob die Primzahlen*

$$2,\ 3,\ 5,\ 7,\ 11,\ 13$$

in $\mathbb{Q}(\sqrt{6})$ *zerfallen.*

Aufgabe 6.12 *Zeigen Sie: In* $\mathbb{Q}(\sqrt[8]{1})$ *zerfällt jede Primzahl* $p \in \mathbb{Z}$.

Aufgabe 6.13 *Es sei* $p > 2$ *eine Primzahl und* $w \neq 1$ *eine* p*-te Einheitswurzel. Zeigen Sie:* $1 - w$ *ist irreduzibel in* $\mathbb{Q}(\sqrt[p]{1})$.

Aufgabe 6.14 *Zerlegen Sie die Zahl 100 in irreduzible Faktoren im Ring* $\mathbb{Z}[i]$ *der ganzen gaußschen Zahlen.*

6.4 Die Fermatsche Vermutung

Die berühmte Vermutung von Fermat lautet: Für $n \in \mathbb{N}$, $n > 2$, gibt es keine ganzzahligen Lösungen x, y, z der diophantischen Gleichung

$$x^n + y^n = z^n,$$

außer den trivialen Lösungen, wo $x = 0$, $y = 0$, oder $z = 0$. Ausgangspunkt ist natürlich die pythagoräische Gleichung

$$x^2 + y^2 = z^2, \quad x, y, z \in \mathbb{Z}.$$

Deren Lösungen überblickt man vollständig. Wir wollen sie explizit beschreiben.

Wenn x, y und z einen gemeinsamen Faktor besitzen, kann man durch ihren größten gemeinsamen Faktor austeilen, und kann deswegen o.B.d.A.

$$ggT(x, y, z) = 1$$

annehmen. Außerdem kann man (nach eventueller Vorzeichenänderung) $x, y, z > 0$ annehmen.

Satz 6.21 *Sind* x, y, z *natürliche Zahlen ohne gemeinsamen Teiler, welche* $x^2 + y^2 = z^2$ *erfüllen, dann gibt es teilerfremde natürliche Zahlen* $r > s$*, nicht beide ungerade, derart, dass (nach eventuellem Vertauschen von* x *und* y*)*

$$z = r^2 + s^2, \quad y = r^2 - s^2, \quad x = 2 \cdot rs.$$

Umgekehrt genügen solche Zahlen x, y, z *immer der pythagoräischen Gleichung.*

Beweis. Jeder gemeinsame Teiler von Zweien der Zahlen x, y, z teilt auch die dritte. Deswegen sind je zwei dieser Zahlen teilerfremd. Insbesondere sind keine zwei dieser Zahlen gerade. Sie können aber auch nicht alle drei ungerade sein, denn dies würde auf den Widerspruch

$$x^2 + y^2 = 2 \, mod \, 4, \quad z^2 = 1 \, mod \, 4$$

führen. Zwei davon sind also ungerade, und eine gerade. Die gerade Zahl kann nicht z sein, denn dann hätten wir $x^2 + y^2 = 2 \, mod \, 4$ und $z^2 = 0 \, mod \, 4$. Also ist z ungerade, und nach eventuellem Vertauschen von x mit y können wir x gerade und y ungerade annehmen.

Wir schreiben die pythagoräische Gleichung um:

$$x^2 = z^2 - y^2 = (z + y) \cdot (z - y).$$

Jeder gemeinsame Teiler von $z + y$ und $z - y$ teilt auch

$$ggT((z + y) + (z - y), (z + y) - (z - y)) = ggT(2z, 2y) = 2.$$

Weil $z + y$ und $z - y$ gerade sind, ist also $ggT(z + y, z - y) = 2$. Wir schreiben

$$x = 2x_0, \quad z + y = 2a, \quad z - y = 2b \quad \text{mit} \quad (a, b) = 1$$

und finden

$$x_0^2 = a \cdot b.$$

Weil a und b teilerfremd sind, geht jeder Primteiler von x_0 quadratisch in a oder b auf. Beide Zahlen $a = r^2$ und $b = s^2$ sind Quadrate. (Dies ist der Fundamentaltrick auf diesem Gebiet der Zahlentheorie.) Wir haben also

$$\begin{aligned} z + y &= 2r^2, & z - y &= 2s^2, \\ 2z &= 2r^2 + 2s^2, & 2y &= 2r^2 - 2s^2, \\ z &= r^2 + s^2, & y &= r^2 - s^2 \end{aligned}$$

mit natürlichen Zahlen r und s. Wegen $y > 0$ ist $s < r$. Jeder gemeinsame Teiler von r und s wäre auch ein Teiler von y und z, also gilt $(r, s) = 1$. Insbesondere sind nicht r und y beide gerade. Aber auch, wenn sie beide ungerade wären, kämen wir auf gerade Zahlen z und y, und das haben wir ausgeschlossen.

Schließlich führt $x_0^2 = a \cdot b = r^2 \cdot s^2$ auf $x_0 = r \cdot s$ und $x = 2 \cdot rs$.

Dass diese Zahlen x, y, z die pythagoräische Gleichung erfüllen ist offensichtlich. □

Die Lösungen x, y, z der pythagoräischen Gleichung heißen *pythagoräische Zahlentripel*. Wir wollen die ersten, teilerfremden, dieser Zahlentripel zusammenstellen:

	$r = 2$	$r = 3$	$r = 4$	$r = 5$	$r = 6$	$r = 7$	$r = 8$
$s = 1$	$4, 3, 5$		$8, 15, 17$		$12, 35, 37$		$16, 63, 65$
$s = 2$		$12, 5, 13$		$20, 21, 29$		$28, 45, 53$	
$s = 3$			$24, 7, 25$		$36, 27, 45$		$48, 55, 73$
$s = 4$				$40, 9, 41$		$56, 33, 65$	
$s = 5$					$60, 11, 61$		$80, 39, 89$
$s = 6$						$84, 13, 85$	
$s = 7$							$112, 15, 113$

Fällt Ihnen hier etwas auf?

Fermat hat also offenbar versucht die pythagoräische Gleichung auf höhere Potenzen als 2 zu verallgemeinern. Das gelang ihm nicht, und da hat er 1637 die Vermutung formuliert, dass dies unmöglich sei. (Genauer: Er hat behauptet, er hätte einen Beweis dafür, aber der Buchrand, auf den er dies schrieb, sei zu schmal für die Wiedergabe des Beweises.) Bewiesen wurde sie erst im letzten Jahrzehnt des 20. Jahrhunderts von A. Wiles. In den 350 Jahren dazwischen haben sich wohl alle berühmten Mathematiker damit beschäftigt, und sie nicht beweisen können. Deswegen ist diese Vermutung so berühmt. Zur Formulierung der Vermutung braucht man nichts anderes, als die vom Gymnasium her bekannte Potenzfunktion x^n. Deswegen haben sich auch viele mathematische Laien mit der Vermutung beschäftigt, und dadurch ist sie so populär geworden.

Eine besondere mathematische Bedeutung hat die Vermutung nicht. Ihre Bedeutung für die Entwicklung der Zahlentheorie ist allerdings enorm. Denn die Beschäftigung mit der Vermutung hat zur Entwicklung vieler Methoden der algebraischen Zahlentheorie geführt. Dem wollen wir hier ein wenig nachgehen.

Satz 6.22 *Die Fermatsche Vermutung gilt für alle natürlichen Zahlen $n > 2$, wenn sie richtig ist für $n = 4$ und für alle Primzahlen $n = p > 2$.*

Beweis. Jede Zahl n ist von der Form $n = p \cdot m$, wo p eine Primzahl ist. Somit ist

$$x^n + y^n = z^n \quad \Leftrightarrow \quad (x^m)^p + (y^m)^p = (z^m)^p.$$

Sie gilt also, für n, wenn wir sie für die Primzahl p beweisen können. Für die Primzahl $p = 2$ ist das natürlich illusorisch. Aber wenn $n = 2^k$, $k \geq 2$, eine Zweierpotenz ist, schreiben wir $n = 4 \cdot 2^{k-2}$ und sehen, dass wir sie nur für $n = 4$ zu beweisen brauchen. □

Der Fall $n = 4$ wurde von Euler erledigt:

Satz 6.23 (Euler) *Die Gleichung*

$$x^4 + y^4 = z^4$$

besitzt keine ganzzahligen Lösungen x, y, z mit $x \cdot y \cdot z \neq 0$.

Beweis. Wie bei der Analyse der pythagoräischen Gleichung können wir annehmen: die drei Zahlen x, y, z sind > 0, paarweise teilerfremd, und x ist gerade, während y und z ungerade sind. Wenn wir noch z durch z^2 ersetzen, sehen wir: Es genügt zu zeigen, dass die Gleichung

$$x^4 + y^4 = z^2$$

keine ganzzahligen Lösungen hat.

Wir schreiben die Gleichung

$$y^4 = (z + x^2) \cdot (z - x^2).$$

Wegen

$$ggT(z + x^2, z - x^2) \,|2z, 2x^2,$$

kann der größte gemeinsame Teiler von $z + x^2$ und $z - x^2$ höchstens 2 sein. Beide Zahlen sind aber ungerade, und somit teilerfremd. Mit dem Fundamentaltrick sehen wir

$$z + x^2 = u^4,\ z - x^2 = v^4, \quad u, v \in \mathbb{N} \text{ ungerade.}$$

Es folgt

$$2x^2 = u^4 - v^4 = (u^2 + v^2) \cdot (u^2 - v^2).$$

Hier sind u und v teilerfremd. Daraus folgt wie üblich, dass $u^2 + v^2$ und $u^2 - v^2$ den größten gemeinsamen Teiler 2 besitzen. Dann muss eine der beiden Zahlen $u^2 + v^2$, $u^2 - v^2$ ein Quadrat a^2 sein, während die andere von der Form $2b^2$ ist, $a, b \in \mathbb{N}$. Weil u und v beide ungerade sind, ist $u^2 + v^2 = 2\, mod\, 4$ kein Quadrat. Wir haben also

$$u^2 - v^2 = a^2, \quad u^2 + v^2 = 2b^2.$$

Die erste Gleichung ist die pythagoräische Gleichung

$$a^2 + v^2 = u^2, \quad u, v \text{ ungerade.}$$

Nach Satz 6.21 schreiben sich ihre Lösungen

$$u = r^2 + s^2, \quad v = r^2 - s^2, \quad a = 2 \cdot rs.$$

Daraus folgt

$$2b^2 = u^2 + v^2 = 2(r^4 + s^4).$$

Wir sind bei der Gleichung

$$r^4 + s^4 = b^2$$

angekommen. Das ist unsere Ausgangangsgleichung, nur mit r, s, b statt x, y, z. Das kann nicht genau dieselbe Gleichung sein: $u = v = 1$ würde nämlich auf eine triviale Lösung mit $x = 0$ für die erste Gleichung führen. Also ist $u^4 + v^4 > u^2 + v^2$ und daraus folgt

$$z = \frac{u^4 + v^4}{2} > \frac{u^2 + v^2}{2} = b^2 \geq b.$$

Obwohl sich die Gleichung reproduziert hat, ist die Zahl z auf der rechten Seite echt kleiner geworden. Wenn es also eine Lösung x, y, z der Gleichung $x^4 + y^4 = z^2$ gibt, dann gibt es auch eine weitere Lösung mit einem echt kleineren $z > 0$.

Wenn wir am Anfang $z > 0$ minimal gewählt haben, kann das nicht sein. Es kann überhaupt kein Lösungen geben. □

Die im Beweis von 6.23 verwendete Methode heißt die Methode des unendlichen Abstiegs.

Es genügt also, die Vermutung für Primzahlen $n = p > 2$ zu betrachten. Wenn wir z durch $-z$ ersetzen, wird aus der Gleichung $x^p + y^p = (-z)^p = -z^p$. Es genügt also zu zeigen, dass

$$x^p + y^p + z^p$$

keine nicht-trivialen ganzzahligen Lösungen hat. Üblicherweise teilt man das Problem in zwei Fälle ein:

Fall 1: p teilt keine der drei Zahlen x, y, z;
Fall 2: p teilt eine der drei Zahlen x, y, z, aber keine zwei.

(Wenn p zwei dieser Zahlen teilen würde, dann auch die dritte, und wir könnten die Gleichung durch p^p dividieren.)

Im Rest dieses Paragraphen werden wir uns um den ersten Fall kümmern. Zunächst ein weiteres elementares Resultat:

Satz 6.24 (Fermat) *Die Gleichung*

$$x^3 + y^3 = z^3$$

besitzt keine ganzzahligen Lösungen $x, y, z \in \mathbb{Z}$ mit $x \cdot y \cdot z \neq 0$.

Beweis. Nachdem wir eventuell y durch $-z$ und z durch $-y$ ersetzen, können wir annehmen, dass beide Zahlen, x und y nicht durch 3 teilbar sind.

Nach dem kleinen Fermat für die Primzahl $p = 3$ gilt $n^3 = n \, mod 3$ für jede ganze Zahl $n \in \mathbb{Z}$. Wenn $x^3 + y^3 = z^3$ wäre, dann hätten wir also

$$x + y = x^3 + y^3 = z^3 = z \, mod 3,$$

und $z = x + y + 3u$, $u \in \mathbb{Z}$. Daraus folgt

$$x^3 + y^3 = (x + y + 3u)^3 = x^3 + y^3 + 3x^2y + 3xy^2 \, mod 9,$$

$$0 = x^2y + xy^2 = xy \cdot (x + y) = xyz \, mod 3.$$

Weil x und y nicht durch 3 teilbar sind, ist $z = x + y = 0 \, mod 3$. D.h., z ist durch 3 teilbar. Wir sind bei Fall 2 der Fermatschen Vermutung gelandet.

Sei nun 3^k, $k \in \mathbb{N}$, die höchste Potenz von 3, welche in z aufgeht. Die Fermatsche Gleichung ist dann

$$x^3 + y^3 = z^3 = (3^k \cdot v)^3, \quad v \in \mathbb{Z}.$$

Wegen $x + y = z \, mod 3$ ist $x + y$ durch 3 teilbar. Wir faktorisieren im Ring O der ganzen Zahlen des dritten Kreisteilungskörpers $\mathbb{Q}(\omega)$

$$3^{3k}v^3 = z^3 = x^3 + y^3 = (x + y) \cdot (x + \omega y) \cdot (x + \omega^2 y).$$

Nach Satz 6.19 ist O ein faktorieller Ring. Wegen der Eindeutigkeit der Zerlegung von z^3 in irreduzible Faktoren muss jeder Faktor von z^3 in einem der drei Faktoren der rechten Seite aufgehen. Nun kann aber $x + \omega y$ nicht durch 3 teilbar sein:

$$x + y = x + \omega y = 0 \, mod 3 \quad \Rightarrow \quad (1 - \omega)y = 0 \, mod 3,$$

und weil y nicht durch 3 teilbar ist, wäre

$$\frac{1}{3}(1 - \omega) = \frac{1}{2} + \frac{1}{6}\sqrt{-3}$$

eine ganz-algebraische Zahl im Widerspruch zu Satz 6.1.

Ebenso sieht man natürlich, dass $x+\omega^2 y$ nicht durch 3 teilbar ist. Die Potenz 3^{3k} muss also ganz in $x+y$ aufgehen. Und 3^{9k} geht in

$$(x+y)^3 = x^3+y^3+3\cdot xy\cdot(x+y) = z^3+3\cdot xy\cdot(x+y)$$

auf. Wegen $3^{9k} > 3^{3k+1}$ muss z^3 durch den Faktor 3^{3k+1} von $3\cdot(x+y)$ teilbar sein. Dann kann 3^k nicht die höchste Potenz von 3 gewesen sein, welche in z aufgeht. Widerspruch! □

Auch der eben geführte Beweis ist eine Variante der Methode des unendlichen Abstiegs.

Die Fermatsche Gleichung hängt folgendermaßen mit p-ten Einheitswurzeln zusammen: Ist w eine primitive p-te Einheitswurzel, so haben wir die bekannte Produkt-Zerlegung nach Vieta

$$X^p-1 = (X-1)(X-w)\cdot\ldots\cdot(x-w^{p-1}).$$

Daraus folgt

$$\begin{aligned} X^p+1 &= -((-X)^p-1) \\ &= -(-X-1)(-X-w)\cdot\ldots\cdot(-X-w^{p-1}) \\ &= (X+1)(X+w)\cdot\ldots\cdot(X+w^{p-1}). \end{aligned}$$

Hier setzen wir $X=x/y$, multiplizieren mit y^p durch, und erhalten

$$x^p+y^p = (x+y)(x+wy)\cdot\ldots\cdot(x+w^{p-1}y).$$

Das ist die linke Seite der Fermatschen Gleichung.

Wir setzen jetzt $K=\mathbb{Q}(\sqrt[p]{1})$ und brauchen einige Eigenschaften dieses Körpers.

Satz 6.25 *In K sind genau die $2p$-ten Einheitswurzeln $\pm w^j$ enthalten, und keine anderen. (Z.B. gehört $i=\sqrt{-1}$ nicht zu K.)*

Beweis. Die Einheitswurzeln in K bilden eine Gruppe unter der Multiplikation. Wir überlegen uns zunächst, dass diese Gruppe endlich ist. Andernfalls gäbe es in dieser Gruppe Elemente unendlich hoher Ordnung m, d.h. primitive m-te Einheitswurzeln beliebig hoher Ordnung m. Wenn $m=p_1^{r_1}\cdot\ldots\cdot p_k^{r_k}$ die Primfaktorzerlegung von m, ist, so kann nur dann $m\to\infty$ gehen, wenn entweder die Anzahl k der Primfaktoren $\to\infty$ geht, oder ein Exponent r_j. In beiden Fällen geht $\varphi(m)$ auch $\to\infty$. Nun ist $\varphi(m)$ der Körpergrad über $\mathbb{Q}$ von $\mathbb{Q}(\sqrt[m]{1})\subset\mathbb{Q}(\sqrt[p]{1})$. Dieser Grad ist durch $\varphi(p)$ beschränkt.

Die Gruppe der Einheitswurzeln in K ist also zyklisch, erzeugt von einem Element einer endlichen Ordnung m. Weil $\mathbb{Q}(\sqrt[p]{1})$ alle p-ten Einheitswurzeln enthält, ist p ein Teiler von m und wir können zerlegen

$$m = p^k\cdot m_0$$

mit $(p,m_0)=1$. Aus $\mathbb{Q}(\sqrt[p]{1})=\mathbb{Q}(\sqrt[m]{1})$ folgt

$$p-1=\varphi(p)=\varphi(m)=p^{k-1}\cdot(p-1)\cdot\varphi(m_0).$$

Also ist $p^{k-1}\cdot\varphi(m_0)=1$. Das bedeutet $k=1$, $m_0=2$ und $m=2p$, wenn nicht $m=p$. □

Satz 6.26 *Die Zahl $a \in \mathbb{C}$ sei ganz-algebraisch über $\mathbb{Q}$. Wenn alle Konjugierten $a, a_2, ..., a_k \in \mathbb{C}$ von a den Betrag $|a_i| = 1$ haben, dann ist a eine Einheitswurzel.*

Beweis. Für alle $n \in \mathbb{N}$ bilden wir

$$\begin{aligned} P_n(X) &:= (X - a^n) \cdot (X - a_2^n) \cdot ... \cdot (X - a_k^n) \\ &= X^k + c_{n,k-1}X^{k-1} + ... + c_{n,1}X + c_{n,0}. \end{aligned}$$

Hier sind die Koeffizienten die symmetrischen Polynome in den a_i^n. Deswegen sind sie invariant unter der Galoisgruppe $G(\mathbb{Q}(a) : \mathbb{Q})$ und gehören zu $\mathbb{Q}$. Weil sie ganz-algebraisch sind, gilt sogar $c_{n,i} \in \mathbb{Z}$. Aus $|a_i|^n = 1$ folgt

$$|c_{n,i}| \leq \binom{k}{i}.$$

Es gibt aber nur endlich viele verschiedene Polynome $P_n(X)$ mit solchen Koeffizienten. Es gibt also unendlich viele Zahlen $n \in \mathbb{N}$ mit demselben Polynom P_n. Die Nullstellen a_i^n dieser Polynome unterscheiden sich also nur um eine Permutation. Weil es nur $k!$ Permutationen gibt, muss es zwei Zahlen $n_1 < n_2$ geben mit $a_i^{n_1} = a_i^{n_2}$ für ein i. Aus $a_i^{n_2-n_1} = 1$ folgt, dass a_i eine Einheitswurzel ist. Dann ist auch die Konjugierte a von a_i eine Einheitswurzel. □

Satz 6.27 (Lemma von Kummer) *Jede Einheit $e \in O(K)$ ist von der Form*

$$w^j \cdot r$$

mit einer Einheit $r \in \mathbb{R}$.

Beweis. Mit der Ganzheitsbasis $1, w, ..., w^{p-2}$ schreiben wir

$$e = a_0 + a_1 w + ... + a_{p-2}w^{p-2}, \quad a_0, ..., a_{p-2} \in \mathbb{Z}.$$

Wir kürzen ab

$$P(X) := a_0 + a_1 X + ... + a_{p-2}X^{p-2} \in \mathbb{Z}[X].$$

Dann ist also $e = P(w)$. Die komplex-konjugierte Zahl

$$\bar{e} = P(\bar{w}) = P(w^{-1}) = P(w^{p-1})$$

ist auch eine Einheit in K, ebenso wie die Zahl $q := e/\bar{e}$ vom Betrag 1. Die Konjugierten von q unter den Galois-Automorphismen von K

$$q_j := \frac{P(w^j)}{P(w^{-j})}$$

haben auch alle den Betrag 1. Nach Satz 6.26 ist q eine Einheitswurzel in K und wegen Satz 6.25 von der Form $\pm w^k$.

Wir schreiben $k = 2s \, mod \, p$ und haben

$$e = \pm w^{2s}\bar{e}, \quad \frac{e}{w^s} = \pm w^s \cdot \bar{e} = \pm\overline{\frac{e}{w^s}}.$$

Hier kann nicht das Minus-Zeichen gelten, denn dann wäre $e/w^s = t \cdot i, t \in \mathbb{R}$. Alle Konjugierten von $t \cdot i$ wären Einheiten und hätten dann eine Norm vom Absolutbetrag 1. Mit Satz 5.7 folgt $t = \pm 1$ und $i = \pm e/w^s \in K$, im Widerspruch zu Satz 6.25. Also ist $e/w^s = r \in \mathbb{R}$ und $e = r \cdot w^s$. □

Beispiel 6.21 *Die Einheiten im dritten Kreisteilungskörper* $\mathbb{Q}(\sqrt[3]{1})$ *sind genau die Zahlen*

$$\pm 1, \pm\omega, \pm\omega^2,$$

wo ω *eine primitive dritte Einheitswurzel ist. Hier ist also stets* $r = \pm 1$.

Beispiel 6.22 *Einheiten im fünften Kreisteilungskörper* $\mathbb{Q}(\sqrt[5]{1})$ *sind genau die Zahlen* $\epsilon^j \cdot r$, *wo* ϵ *eine primitive* 5*-te Einheitswurzel und* r *eine reelle Einheit in* $\mathbb{Q}(\sqrt[5]{1})$ *ist. Das ist dasselbe, wie eine Einheit im Teilkörper* $\mathbb{Q}(\sqrt[5]{1}) \cap \mathbb{R}$. *Dieser Teilkörper kann nicht der ganze Körper sein* ($\epsilon \notin \mathbb{R}$), *enthält andererseits den reell-quadratischen Zahlkörper* $\mathbb{Q}(\sqrt{5})$, *s. Beispiel 4.5. Also stimmt dieser Teilkörper mit* $\mathbb{Q}(\sqrt{5})$ *überein. Eine Fundamental-Einheit in diesem Körper ist* $(1+\sqrt{5})/2$ *(Beispiel 6.11). Deswegen sind die Einheiten in* $\mathbb{Q}(\sqrt[5]{1})$ *genau die Zahlen*

$$\pm\epsilon^j \cdot \left(\frac{1+\sqrt{5}}{2}\right)^k, \quad j = 0, ..., 4,\ k \in \mathbb{Z}.$$

Satz 6.28 *Die ganzen Zahlen* $x, y \in \mathbb{Z}$ *seien teilerfremd, und* $x + y$ *sei nicht durch* p *teilbar. Dann gibt es für* $w^j \neq w^k$ *Zahlen* u *und* $v \in O(K)$ *mit*

$$u \cdot (x + w^j y) + v \cdot (x + w^k y) = 1.$$

(Das Ideal $(x + w^j y, x + w^k y) \subset O(K)$ *ist das Einheitsideal (1).)*

Beweis. Wir nehmen $j < k$ an. Dann ist

$$x + w^k y - (x + w^j y) = w^k(1 - w^{j-k})y = w^k(1 - w) \cdot e_{j-k} y$$

mit einer Einheit e_{j-k} (Beispiel 6.9). Ebenso ist

$$(x + w^k y)w^j - (x + w^j y)w^k = -w^k(1 - w^{j-k})x = -w^k(1 - w) \cdot e_{j-k} x.$$

Da $w^k e_{j-k}$ eine Einheit ist, gehören die Zahlen $(1-w)x$ und $(1-w)y$ zum Ideal $(x+w^k y, x+w^j y)$.

Weil x und y teilerfremd vorausgesetzt sind, gibt es Zahlen $a, b \in \mathbb{Z}$ mit $ax + by = 1$. Daraus folgt

$$1 - w = (1 - w)xa + (1 - w)yb \in (x + w^k y, x + w^j y).$$

Weil $1 - w$ ein Teiler von p ist (Satz 4.1 b), gilt dann auch $p \in (x + w^k y, x + w^j y)$. Weiter ist

$$x + y = x + w^k y + (1 - w^k)y = x + w^k y + (1 - w) \cdot e_k y$$

mit einer Einheit e_k. Also gehört auch $x + y$ zu dem Ideal. Weil $x + y$ nicht durch p teilbar ist, ist 1 der größte gemeinsame Teiler von p und $x + y$ in $\mathbb{Z}$. Also gehört auch 1 zum Ideal und das Ideal ist tatsächlich das Einheitsideal (1). □

Nach diesen Vorbereitungen wenden wir uns jetzt direkt der Fermatschen Vermutung zu. Wir werden einen speziellen Fall von Fall 1 dieser Vermutung beweisen. Speziell daran ist folgendes: Für die Primzahl $p > 2$ sei $K := \mathbb{Q}(\sqrt[p]{1})$ der p-te Kreisteilungskörper. Mit O werde der Ring $O(K)$ der ganz-algebraischen Zahlen in K bezeichnet. Wir werden voraussetzen, dass dieser Ring faktoriell ist. Das ist ziemlich gewagt, denn wir haben keinerlei Information darüber, wann dies der Fall ist. Nur für $p = 3$, wo $\mathbb{Q}(\sqrt[3]{1}) = \mathbb{Q}(\sqrt{-3})$ ist, wissen wir, dass dieser Ring faktoriell ist (Satz 6.20). Aber für $p = 3$ haben wir den ersten Fall der Fermatschen Vermutung ja direkt und elementar bewiesen (Satz 6.24). Trotzdem möchte ich den folgenden Beweis vorstellen, einfach um zu zeigen, welche Rolle die Teilbarkeitseigenschaften des Ringes O für die Fermatsche Vermutung spielen.

Satz 6.29 *Es sei p eine Primzahl > 2. Von den drei ganzen Zahlen $x, y, z \in \mathbb{Z}$ sei keine durch p teilbar. Außerdem sei der Ring O der ganz-algebraischen Zahlen in $K = \mathbb{Q}(\sqrt[p]{1})$ faktoriell. Dann ist*

$$x^p + y^p \neq z^p.$$

Beweis. Die Technik des Beweises besteht darin, modulo p zu rechnen. Eine ganze Zahl $m \in \mathbb{Z}$ ist $= 0 \, mod \, p$, wenn $m = q \cdot p$ mit einer ganzen Zahl $q \in \mathbb{Z}$ ist. Das ist aber genau dasselbe, wie wenn $m = 0 \, mod \, p$ in O ist. Denn letzteres bedeutet $m = q \cdot p$ mit $q \in O$. Natürlich ist hier $q = m/p \in \mathbb{Q}$ eine rationale Zahl. Und wenn sie ganz-algebraisch ist, muss sie selbst ganz, d.h. $\in \mathbb{Z}$ sein (Beispiel 5.4)

Wir nehmen also an, die Gleichung $x^p + y^p = z^p$ würde gelten. Ausgangspunkt dafür, dies zum Widerspruch zu führen, ist, wie im Spezialfall $p = 3$, der kleine Fermat in der Form

$$x + y = x^p + y^p = z^p = z \neq 0 \, mod \, p.$$

Dann schreiben wir die Fermatsche Gleichung in der Form

$$z^p = x^p + y^p = (x + y) \cdot (x + wy) \cdot (x + w^2 y) \cdot \ldots \cdot (x + w^{p-1} y).$$

Jetzt kommt die entscheidende Stelle: Weil O faktoriell vorausgesetzt ist hat sowohl z^p wie auch das lange Produkt auf der rechten Seite eine eindeutige Zerlegung in irreduzible Faktoren aus O. Nach Satz 6.28 haben keine zwei der Zahlen $x + w^k y$ einen gemeinsamen irreduziblen Faktor in O. Jeder irreduzible Faktor von z muss p-mal in einem einzigen Faktor $x + w^k y$ der rechten Seite aufgehen (Fundamentaltrick). Also ist jeder dieser Faktoren, bis auf eine Einheit in O, eine p-te Potenz. Insbesondere haben wir

$$x + wy = e \cdot a^p, \quad e \in O \text{ Einheit}, \, a \in O.$$

Genauso folgt aus

$$(-y)^p = x^p + (-z)^p = (x - z) \cdot (x - wz) \cdot (x - w^2 z) \cdot \ldots \cdot (x - w^{p-1} z),$$

dass

$$x - wz = e' \cdot b^p, \quad e' \in O \text{ Einheit}, \, b \in O.$$

Mit der Ganzheitsbasis $1, w, ..., w^{p-2}$ (s. Beispiel 6.4) schreiben wir

$$a = a_0 + a_1 w + ... + a_{p-2} w^{p-2}, \quad a_0, ..., a_{p-2} \in \mathbb{Z}.$$

Wegen der p-Teilbarkeit der Binomialkoeffizienten und $w^p = 1$ folgt daraus wie üblich

$$a^p = a_0^p + a_1^p + ... + a_{p-2}^p =: m \, mod \, p.$$

Nach dem Lemma von Kummer (Satz 6.27) ist $e = w^s \cdot r$ mit einer Einheit $r \in O \cap \mathbb{R}$. Es folgt

$$x + wy = w^s rm = w^s \cdot r' \, mod \, p, \quad r' \in O \cap \mathbb{R}.$$

Wir schreiben diese Gleichung um:

$$w^{-s}(x + wy) = r' \, mod \, p.$$

Dann gilt auch die komplex-konjugierte Gleichung

$$w^s(x + w^{-1}y) = r' \, mod \, p.$$

Beide Gleichungen zusammen zeigen

$$xw^s + yw^{s-1} - xw^{-s} - yw^{1-s} = 0 \, mod \, p.$$

Falls die Zahlen $s, s-1, -s, 1-s \, mod \, p$ paarweise voneinander und von $p-1$ verschieden sind, sind die Zahlen w^s, w^{s-1}, w^{-s} und w^{1-s} vier verschiedene Zahlen aus der Ganzheitsbasis $1, w, ..., w^{p-2}$. Wegen der Eindeutigkeit der Darstellung einer Zahl $b = b_0 + b_1 w + ... + b_{p-2} w^{p-2} \in O$ folgt: Wenn b durch p teilbar ist, dann sind dies alle Koeffizienten $b_0, ..., b_{p-2}$. In unserem Fall wären also x und y durch p teilbar im Widerspruch zur Voraussetzung. Wir hätten fertig.

Es bleiben zwei Fälle zu analysieren:

Entweder ist eine der vier Zahlen $s, s-1, -s, 1-s = p-1 \, mod \, p$. Das führt auf die Möglichkeiten

s	$s-1$	$-s$	$1-s$
$p-1$	$p-2$	1	2
0	$p-1$	0	1
1	0	$p-1$	0
2	1	$p-2$	$p-1$

modulo p. In jedem dieser vier Fälle ist genau ein Exponent $= p-1 \, mod \, p$. Wenn wir in der Gleichung

$$xw^s + yw^{s-1} - xw^{-s} - yw^{1-s} = 0 \, mod \, p$$

w^{p-1} durch

$$-1 - w - ... - w^{p-2}$$

ersetzen, erhalten wir eine neue Linearkombination unserer Ganzheitsbasis, die $= 0 \, mod \, p$ ist. Wenn $p \geq 5$ ist, ist mindestens einer der Koeffizienten $= \pm x$ oder $\pm y$ modulo p. Wieder ein Widerspruch zur Voraussetzung, fertig. Aber den Fall $p = 3$ haben wir ja schon elementar erledigt (Satz 6.24).

Oder es stimmen zwei der Zahlen $s, s-1, -s, 1-s$ modulo p überein. Hier kann $s = s-1 \, mod p$ oder $-s = 1 - s \, mod \, p$ nicht vorliegen. Sonst könnte noch Folgendes passieren:

- $s = -s \, mod p$: Dann wäre $2s = 0 \, mod p$ und $s = 0 \, mod p$. Wir hätten $s - 1 = p - 1 \, mod p$.
- $s = 1 - s \, mod p$: In diesem Fall wäre $2s = 1 \, mod p$ und $s = (p+1)/2 \, mod p$. Wir hätten $s = 1 - s = 1 - (p+1)/2 = (-p+1)/2 = (p+1)/2 \, mod p$ und $s - 1 = -s = (p-1)/2 \, mod p$. Unsere Gleichung wäre

$$\begin{aligned} xw^s + yw^{s-1} - xw^{-s} - yw^{1-s} &= (x-y)w^{(p+1)/2} + (y-x)w^{(p-1)/2} \\ &= 0 \, mod p. \end{aligned}$$

  Aus der Eindeutigkeit der Darstellung in der Ganzheitsbasis würde $x = y \, mod p$ folgen. Hier können wir aber y durch $-z$ ersetzen und finden $x = -x - y = -2x = -z \, mod p$. Wegen $x + y = z \, mod p$ bekämen wir damit

$$2x = -x, \quad 3x = 0 \, mod p, \quad p = 3.$$

  Das ist Pech. Aber den Fall $p = 3$ haben wir schon elementar erledigt (Satz 6.24) und können ihn deswegen hier ausschließen.
- $s - 1 = -s \, mod p$: Das ist dasselbe, wie $s = 1 - s \, mod p$, erledigt.
- $s - 1 = 1 - s \, mod p$: Jetzt folgt $2s = 2 \, mod p$ oder $s = 1 \, mod p$. In diesem Fall wäre $-s = p - 1 \, mod p$.

Keiner dieser Fälle kann eintreten, oder er führt auf die Situation, wo eine der vier Zahlen $s, s-1, -s, 1-s = p-1 \, mod p$ ist, und das ist schon erledigt. □

Aufgabe 6.15 *Beweisen Sie elementar den ersten Fall der Fermatschen Vermutung für $p = 5$.*

6.5 Idealtheorie

Das Leben wäre viel einfacher, wenn der Ring der ganzen Zahlen in jedem algebraischen Zahlkörper faktoriell wäre. Aber das Beispiel

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5}) \cdot (1 - 2\sqrt{-5}) \quad \in \mathbb{Q}(\sqrt{-5})$$

zeigt, dass das leider nicht so ist. Wir wollen analysieren, woran das liegt. Der Zahlkörper $\mathbb{Q}(\sqrt{-5})$ enthält die ganz-algebraischen Zahlen

$$a := 2 + \sqrt{-5} \quad \text{und} \quad b := 2 + 3\sqrt{-5}.$$

Für sie und ihre Konjugierten $a' = 2 - \sqrt{5}, b' = 2 - 3\sqrt{5}$ gilt

$$a \cdot a' = 9, \quad b \cdot b' = 49.$$

Es gibt also Wurzeln $\sqrt{a}, \sqrt{a'}, \sqrt{b}, \sqrt{b'} \in \mathbb{C}$ dieser Zahlen mit

$$\sqrt{a} \cdot \sqrt{a'} = 3, \quad \sqrt{b} \cdot \sqrt{b'} = 7.$$

Nun ist

$$a \cdot (-b') = -(2 + \sqrt{-5}) \cdot (2 - 3\sqrt{-5}) = -19 + 4\sqrt{-5} = (1 + 2\sqrt{-5})^2,$$
$$a' \cdot (-b) = -(2 - \sqrt{-5}) \cdot (2 + 3\sqrt{-5}) = -19 - 4\sqrt{5} = (1 - 2\sqrt{-5})^2.$$

Bis auf ein eventuelles Vorzeichen ist also

$$\sqrt{a} \cdot \sqrt{-b'} = 1 + 2\sqrt{-5}, \quad \sqrt{a'} \cdot \sqrt{-b} = 1 - 2\sqrt{-5}.$$

Beide Faktorisierungen der Zahl 21 lassen sich weiter in

$$21 = \sqrt{a} \cdot \sqrt{a'} \cdot \sqrt{-b} \cdot \sqrt{-b'}$$

faktorisieren. Damit wäre die Nicht-Eindeutigkeit der Faktorisierung von 21 beseitigt.

Aber leider gehören die Wurzeln aus $a, a', -b, -b'$ nicht zum Ring der ganzen Zahlen im Zahlkörper $\mathbb{Q}(\sqrt{-5})$. Sie hätten ja die Norm 3, bzw. 7, und das geht nicht (Beispiel 6.14). Um die Faktorisierung zu retten, hätten die Zahlentheoretiker des 19. Jahrhunderts diese Zahlen aber sehr gerne gehabt. Sie verfielen auf den Ausweg, sie als *ideale Zahlen* in $\mathbb{Q}(\sqrt{-5})$ anzusehen. Im Körper $K = \mathbb{Q}(\sqrt{-5})$ sieht man von diesen Zahlen nur die Menge ihrer Vielfachen, wie z.B.

$$\{c \in K : \, c = x \cdot \sqrt{a}, x \text{ ganz-algebraisch}\}.$$

Solche Mengen nannten sie zuerst *ideale Zahlen*, und später einfach *Ideale*. Die Menge ist ja ein Ideal im heutigen Sinn. Und daher kommt der Name Ideal.

Für diesen ganzen Paragraphen machen wir die Voraussetzungen: K mit $\mathbb{Q} \subset K \subset \mathbb{C}$ ist eine endliche, galoissche Körpererweiterung. Der Ring $O(K)$ der ganz-algebraischen Zahlen in K werde einfach mit O bezeichnet. Das Ideal in O, das von Zahlen $c_1, ..., c_k \in O$ erzeugt wir, werden wir mit

$$(c_1, ..., c_k)$$

bezeichnen.

Satz 6.30 *Jedes Ideal $(0) \neq I \subset O$ enthält eine ganze Zahl $0 \neq q \in \mathbb{Z}$.*

Beweis. Wegen $I \neq (0)$ gibt es ein $0 \neq c \in I$. Es seien $c_2, ..., c_k \in \mathbb{C}$ die Konjugierten von c. Dann ist

$$N_{\mathbb{Q}(c)/\mathbb{Q}}(c) = c \cdot c_2 \cdot ... \cdot c_k \in \mathbb{Z}$$

eine ganze Zahl $q \neq 0$. Daraus folgt $c' := c_2 \cdot ... \cdot c_k \in K$. Aber c' ist auch ganz-algebraisch, also $c' \in O$. Deswegen ist $q = c \cdot c' \in I \cap \mathbb{Z}$. □

Definition 6.7 *Es sei $I \subset O$ ein Ideal. Zahlen $c_1, ..., c_k \in I$ heißen eine* Idealbasis *von I, wenn*

1. *$c_1, ..., c_k$ linear unabhängig über $\mathbb{Q}$ sind und*

2. *$I = \mathbb{Z}c_1 + ... + \mathbb{Z}c_k$ ist, d.h., jede Zahl $c \in I$ schreibt sich (eindeutig) als Linearkombination der $c_1, ..., c_k$ mit Koeffizienten aus $\mathbb{Z}$.*

Die Zahl k heißt Länge *der Idealbasis.*

Satz 6.31 *Jedes Ideal $(0) \neq I \subset O$ hat eine Idealbasis. Alle Idealbasen von I haben dieselbe Länge $= [K : \mathbb{Q}]$.*

Beweis. Wegen $I \neq (0)$ gibt es ein $0 \neq c \in I$. Wir wählen eine Ganzheitsbasis $a_1, ..., a_n$ von K über $\mathbb{Q}$ nach Satz 6.5. Dann sind $ca_1, ..., ca_n \in I$ linear unabhängig über $\mathbb{Q}$. Also gibt es auch über $\mathbb{Q}$ linear unabhängige Zahlen $c_1, ..., c_n \in I$ mit minimaler Diskriminante $\Delta(c_1, ..., c_n)$. Dass diese eine Idealbasis bilden, folgt ganz genau wie im Beweis von Satz 6.5.

Ist $b_1, ..., b_m \in I$ eine Idealbasis, so gibt es eine ganzzahlige $n \times m$-Matrix $(\gamma_{i,j})$ mit

$$c_i = \sum_{j=1}^{m} \gamma_{i,j} b_j, \quad i = 1, ..., n.$$

Die n über $\mathbb{Q}$ linear unabhängigen Zahlen $c_1, ..., c_n$ sind also in dem $\mathbb{Q}$-Vektorraum enthalten, der von $b_1, ..., b_m$ aufgespannt wird. Daraus folgt $m \geq n$. Die andere Ungleichung $m \leq n$ folgt aus

$$dim_{\mathbb{Q}}(K) = n.$$

□

Eine Idealbasis von I ist nicht dasselbe, wie ein Erzeugendensystem:

Definition 6.8 *Es sei $I \subset O$ ein Ideal. Zahlen $a_1, ..., a_k \in I$ heißen ein* Erzeugendensystem, *wenn*

$$I = O \cdot a_1 + ... + O \cdot a_k = \{\sum_{l=1}^{k} c_l a_l, \quad c_l \in O\} = (a_1, ..., a_k).$$

Ein Ideal I heißt wie üblich Hauptideal, *wenn es ein Erzeugendensystem besitzt, das nur aus einem einzigen Element besteht.*

Beispiel 6.23 *Es sei $K := \mathbb{Q}(i)$ und $I := (2) \subset O$. Ein Erzeugendensystem des Hauptideals I ist also die einzelne Zahl 2. Eine Idealbasis kann sie aber nicht bilden, denn eine Idealbasis müsste aus $[K : \mathbb{Q}] = 2$ Zahlen bestehen. Zwei über $\mathbb{Q}$ linear unabhängige Zahlen sind z.B. 2 und $2i \in I$. Bilden sie eine Idealbasis? Die ganz-algebraischen Zahlen in K sind genau die ganzen Gaußschen Zahlen $c = a + bi$, $a, b \in \mathbb{Z}$. Eine solche Zahl liegt in I genau dann, wenn sie in O durch 2 teilbar ist, d.h., wenn*

$$\frac{a}{2} + \frac{b}{2} i \in O$$

wieder ganz ist. Das heißt, die Zahlen $a = 2\alpha$ und $b = 2\beta$ müssen gerade sein, es gilt $\alpha, \beta \in \mathbb{Z}$. Daraus folgt $c = \alpha \cdot 2 + \beta \cdot 2i$. Die Zahlen 2 und $2i$ bilden tatsächlich eine Idealbasis des Hauptideals (2).

Beispiel 6.24 (Hauptideal) *Es sei* $(0) \neq (c) \subset O$ *ein Hauptideal und* $a_1, ..., a_n \in O$ *eine Ganzheitsbasis. Die Zahlen in* I *sind also alle von der Form* $a \cdot c$ *mit* $a = k_1 a_1 + ... + k_n a_n$, $k_1, ..., k_n \in \mathbb{Z}$. *Deswegen ist jedes* $r \in I$ *eine ganzzahlige Linearkombination*

$$r = k_1 \cdot a_1 c + ... + k_n \cdot a_n c.$$

Weil die $a_1, ..., a_n$ *linear unabhängig über* $\mathbb{Q}$ *sind, sind es auch die Zahlen* $c_1 := a_1 c, ..., c_n := a_n c$. *Sie bilden also eine Idealbasis von* (c).

Beispiel 6.25 *Es sei* $K = \mathbb{Q}(\sqrt{-5})$ *und* $I = (3,\ 1+2\sqrt{-5})$ *das von den Zahlen* 3 *und* $1+2\sqrt{-5}$ *erzeugte Ideal. Nach Beispiel 6.14 ist* 3 *irreduzibel. Und* $N(1+2\sqrt{-5}) = 21$, *also ist auch diese Zahl irreduzibel (s. Beispiel 6.14). Beide Erzeugende des Ideals sind irreduzibel in* O. *Weil sie verschiedene Normen haben, sind sie auch nicht assoziiert. Eine Zahl* $a \in O$, *welche beide teilt, müsste also eine Einheit* $a \in O$ *sein. Wäre* $I = (a)$ *ein Hauptideal, so wäre* a *eine Einheit, und* I *das Eins-Ideal* $(1) = O$. *Weiter wissen wir, dass die ganz-algebraische Zahl* $l := \sqrt{2+\sqrt{-5}} \in \mathbb{C}$ *(im Ring aller ganz-algebraischen Zahlen aus* $\mathbb{C}$*) die beiden Erzeugenden teilt. Wäre* I *das Eins-Ideal, so wäre* l *auch eine Teiler der Eins und* $1/l \in \mathbb{C}$ *ganz-algebraisch. Dann wäre auch*

$$\frac{1}{l^2} = \frac{1}{2+\sqrt{-5}} = \frac{2-\sqrt{-5}}{9} \in K$$

ganz-algebraisch. Das ist diese Zahl aber nicht. Also ist I *kein Hauptideal.*

Satz 6.32 *Für jedes Ideal* $(0) \neq I \subset O$ *ist der Restklassenring* O/I *endlich.*

Beweis. Nach Satz 6.30 gibt es eine ganze Zahl $0 \neq q \in I \cap \mathbb{Z}$. Ist $c_1, ..., c_n \in K$ eine Ganzheitsbasis, so gehören also alle Zahlen $q \cdot c_1, ..., q \cdot c_n$ zu I. Es sei $J := (qc_1, ..., qc_n)$ das von diesen erzeugte Ideal in O. Dann ist $J \subset I$ und es gibt einen Ring-Epimorphismus

$$O/J \to O/I.$$

Es genügt also zu zeigen, dass O/J ein endlicher Ring ist.

Nun sind die Zahlen in O alle von der Form $c = k_1 c_1 + ... + k_n c_n$, $k_1, ..., k_n \in \mathbb{Z}$. Und eine solche Zahl gehört genau dann zu J, wenn alle Koeffizienten $k_1, ..., k_n$ durch q teilbar sind. Ein Repräsentantensystem von O/J sind deswegen die Zahlen c mit $0 \leq k_1, ..., k_n < q$. Das sind q^n Zahlen, und O/J enthält genau q^n Elemente. □

Ein Erzeugendensystem eines Ideals I ist also nicht unbedingt eine Idealbasis. Aber umgekehrt ist natürlich jede Idealbasis ein Erzeugendensystem. Daraus folgt:

Satz 6.33 *Jedes Ideal* $I \subset O$ *besitzt ein endliches Erzeugendensystem. Insbesondere ist* O *noethersch (Satz 2.6), d.h., jede echt aufsteigende Kette* $I_1 \subset I_2 \subset ... \subset O$ *bricht nach endlich vielen Schritten ab.*

Diese Eigenschaft „noethersch“ des Rings O werden wir jetzt noch etwas anlysieren. Dazu die folgende sophistische Definition.

Definition 6.9 *Das Ideal $J \subset O$ heißt* Teiler *des Ideals $I \subset O$, wenn $I \subset J$.*

Das Ideal $J \subset O$ heißt Faktor *des Ideals I, in Zeichen: $J|I$, wenn es ein Ideal $J' \subset O$ gibt mit*

$$J \cdot J' = I.$$

Dabei ist das Produkt $J \cdot J'$ zweier Ideale definiert als das Ideal, das von allen Produkten $x \cdot x'$, $x \in J, x' \in J'$, erzeugt wird.

Beispiel 6.26 *Es sei O ein Hauptidealring (z.B. $O = \mathbb{Z}$). Dann ist also $I = (c)$ und $J = (a)$. J ist genau dann ein Teiler von I, wenn $c \in (a)$, d.h., $a|c$ im Sinn von Definition 2.15.*

Und J ist ein Faktor von I genau dann, wenn es ein Ideal $J' = (b)$ gibt mit $J \cdot J' = (a \cdot b) = (c)$. Auch das ist äquivalent mit $a|c$. In einem Hauptidealring stimmen also beide Eigenschaften überein.

Satz 6.34 *a) Jeder Faktor J des Ideals I ist auch ein Teiler.*

b) Jeder echte Faktor J des Ideals I (d.h. $J \cdot J' = I$ mit $J' \neq O$) ist auch ein echter Teiler (d.h. $J \neq I$).

Beweis. a) Das Produkt-Ideal $J \cdot J'$ wird erzeugt von allen Produkten $a \cdot b$, $a \in J, b \in J'$. Alle diese Produkte gehören zu J. Deswegen ist $J \cdot J' \subset J$. Und wenn $I = J \cdot J'$, dann gilt $I \subset J$, und J ist ein Teiler von I.

b) Es seien $a_1, ..., a_n$ eine Idealbasis von J und $b_1, ..., b_n$ eine Idealbasis von J'. Dann ist $a_i b_j$, $i, j = 1, ..., n$, ein Erzeugendensystem von $I = J \cdot J'$. Wenn $I = J$ wäre, dann wären insbesondere alle $a_\nu \in J$ Linearkombinationen

$$a_\nu = \sum_{i,j=1}^{n} c_{\nu,i,j} a_i b_j = \sum_{i=1}^{n} \beta_{\nu,i} a_i, \quad \beta_{\nu,i} = \sum_j c_{\nu,i,j} b_j \in J'.$$

Wir bezeichnen mit $a \in K^n$ den Vektor $(a_1, ..., a_n)$ und mit B die Matrix $(\beta_{\nu,i})$ mit Einträgen aus J'. Die Gleichung

$$a = B \cdot a$$

zeigt, dass a Eigenvektor der Matrix B zum Eigenwert 1 ist. Also ist 1 eine Nullstelle des charakteristischen Polynoms

$$\chi_B(X) = \pm X^n + q_{n-1} X^{n-1} + ... + q_1 X + q_0.$$

Alle Koeffizienten $q_{n-1}, ..., q_1, q_0$ gehören zu J'. Und die Gleichung

$$0 = \chi_B(1) = \pm 1 + q_{n-1} + ... + q_1 + q_0$$

zeigt $1 \in J'$. Es wäre $1 \in J'$ und $J' = O$. □
□

Satz 6.35 *Jedes Ideal $(0) \neq I \subset O$ gehört nur zu endlich vielen Idealen $J \subset O$, hat also nur endlich viele Teiler.*

Beweis. Wir betrachten den Restklassen-Homomorphismus

$$\pi : O \to O/I.$$

Jedes Ideal R im Restklassen-Ring hat als Urbild $\pi^* R$ ein Ideal in O, welches I enthält. Und umgekehrt: Jedes Ideal J, das I enthält, ist von dieser Form $\pi^* R$. Weil der Restklassenring endlich ist (Satz 6.32), enthält er nur endlich viele Teilmengen, und dann auch nur endlich viele Ideale R. Dann gibt es also auch nur endlich viele Ideale $J \subset O$ mit $J \subset I$. □

Satz 6.36 (Korollar) *Jedes Ideal $(0) \neq I \subset O$ hat nur endlich viele Faktoren.*

Beweis. Satz 6.34

Wir erinnern uns an die Definition des maximalen Ideals: Ein Ideal $M \subset O$, $M \neq O$, heißt maximal, wenn es kein Ideal I mit $M \subset I \subset O$, $I \neq O, I \neq M$, gibt. Äquivalent dazu ist: Der Restklassenring O/M besitzt kein Ideal außer (0) und $(1) = O/M$, was bedeutet: er ist ein Körper.

Satz 6.37 *Jedes Ideal $I \subset O$, $I \neq O$, hat*
a) einen maximalen Teiler $J \supset I$;
b) nur endlich viele maximale Teiler;
c) nur endlich viele maximale Faktoren.

Beweis. a) Wenn I selbst maximal ist, sind wir fertig. Andernfalls gibt es ein Ideal $J_1 \subset O$ mit $I \subset J_1$, $J_1 \neq I$. Wenn J_1 maximal ist, sind wir fertig. Andernfalls machen wir weiter: $J_1 \subset J_2$, $J_2 \neq J_1$. So erhalten wir eine echt aufsteigende Kette $I \subset J_1 \subset J_2 \subset ...$ von echten Idealen $J_k \subset O$, $J_k \neq O$. Weil I nur in endlich-vielen Idealen J enthalten ist (Satz 6.35), bricht diese Kette irgend wann ab. Das letzte Ideal in der Kette ist maximal.

b) Jeder maximale Teiler von I enthält dieses Ideal I. Nach Satz 6.35 gibt es nur endlich viele solche Ideale.

c) Jeder maximale Faktor von I ist nach Satz 6.34 auch ein maximaler Teiler. □

Und noch eine Erinnerung: Das Ideal $(0) \neq I \subset O$ heißt Prim-Ideal, wenn der Restklassenring O/I nullteilerfrei ist. Äquivalent dazu: Sind $a, b \in O$ mit $a \cdot b \in I$, dann ist entweder $a \in I$ oder $b \in I$.

Satz 6.38 *Für Ideale $(0) \neq I \subset O$ sind die Eigenschaften „maximal“ und „prim“ äquivalent.*

Beweis. Maximale Ideale sind immer Prim-Ideale. Wir müssen also zeigen: Jedes Prim-Ideal $I \subset O$ ist maximal. Nun ist der Restklassenring O/I nullteilerfrei und nach Satz 6.32 endlich. Die Eigenschaft „nullteilerfrei“ bedeutet: Zu $0 \neq r \in O/I$ gibt es kein $0 \neq s \in O/I$ mit $r \cdot s = 0$. Die Multiplikationsabbildung

$$m_r : O/I \to O/I, \quad s \mapsto r \cdot s,$$

ist injektiv. Weil R/I endlich ist, muss diese Multiplikation dann auch surjektiv sein. Insbesondere gehört $1 = r \cdot s$ zum Bild dieser Abbildung. Das heißt: Jedes $r \neq 0$ besitzt ein Inverses. Der Restklassenring ist ein Körper, und I ist maximal. □

Satz 6.39 (Korollar) *Enthält ein maximales Ideal $M \subset O$ ein Produktideal $I \cdot J$, so gilt entweder $I \subset M$ oder $J \subset M$.*

Beweis. Wenn I nicht in M enthalten ist, dann gibt es ein $a \in I$ mit $a \notin M$. Für alle $b \in J$ gilt aber $a \cdot b \in I \cdot J \subset M$. Weil M ein Primideal ist, folgt daraus $b \in M$ für alle $b \in J$. Also ist $J \subset M$. □

Nun folgen zwei Hilfsaussagen:

Satz 6.40 *Es sei*

$$f(X) = a_m X^m + a_{m-1} X^{m-1} + ... + a_1 X + a_0 \in \mathbb{C}[X]$$

ein Polynom mit ganz-algebraischen Koeffizienten $a_m, ..., a_0$ und den Nullstellen $r_1, ..., r_m \in \mathbb{C}$. Dann gelten:

a) Das Polynom $f(X)/(X - r_1) \in \mathbb{C}[X]$ hat nur ganz-algebraische Koeffizienten.

b) Für jedes $k = 1, ..., m-1$ hat das Polynom

$$\frac{f(X)}{(X - r_{k+1}) \cdot ... \cdot (X - r_m)} = a_m \cdot (X - r_1) \cdot ... \cdot (X - r_k)$$

nur ganz-algebraische Koeffizienten.

c) Für jedes $k = 1, ..., m$ ist $a_m \cdot r_1 \cdot ... \cdot r_k$ eine ganz-algebraische Zahl.

Beweis. a) (Induktion nach m) Induktionsanfang $m = 1$: Jetzt hat $f(X) = a_1 X - a_0$ ganz-algebraische Koeffizienten a_1 und a_0. Seine Nullstelle ist $r_1 = a_0/a_1$ und

$$\frac{f(X)}{X - \frac{a_0}{a_1}} = a_1$$

ist ein konstantes Polynom mit dem ganz-algebraischen Wert a_1.

Induktionsschluss: Die Zahl $a_m \cdot r_1$ ist Nullstelle des normierten Polynoms

$$X^m + a_{m-1} X^{m-1} + a_m a_{m-2} X^{m-2} + ... + a_m^{m-1} a_0$$

mit ganz-algebraischen Koeffizienten. Wegen der Transitivität (Satz 6.2) ist $a_m \cdot r_1$ selbst ganz-algebraisch. Dann hat das Polynom

$$g(X) := f(X) - a_m X^{m-1} \cdot (X - r_1)$$

vom Grad $m - 1$ ganz-algebraische Koeffizienten und ebenso wie f die Nullstelle r_1. Nach Induktionsannahme hat dann

$$\frac{g(X)}{X - r_1} = \frac{f(X)}{X - r_1} - a_m X^{m-1}$$

ganz-algebraische Koeffizienten. Weil a_m ganz-algebraisch ist, hat auch $f(X)/(X - r_1)$ ganz-algebraische Koeffizienten.

b) Die Aussage folgt aus a) durch Induktion nach Anzahl der Nullstellen.

c) Die Zahl $a_m \cdot r_1 \cdot ... \cdot r_k$ ist bis auf das Vorzeichen der konstante Koeffizient des Polynoms aus b), und damit ganz-algebraisch. □

Satz 6.41 *Es seien*

$$f(X) = a_m X^m + ... + a_0, \quad g(X) = b_n X^n + ... + b_0 \quad \in \mathbb{C}[X]$$

Polynome mit ganz-algebraischen Koeffizienten und

$$h(X) = c_s X^s + ... + c_0 = f(X) \cdot g(X)$$

deren Produkt. Ist dann $d \in \mathbb{C}$ eine ganz-algebraische Zahl derart, dass alle Quotienten c_k/d, $k = 0, ..., s$ ganz-algebraisch sind, dann sind auch alle Zahlen $a_i b_j/d$, $i = 0, ..., m, j = 0, ..., n$, ganz-algebraisch.

Beweis. Wir schreiben nach Vieta

$$f(X) = a_m \cdot (X - u_1) \cdot ... \cdot (X - u_m), \quad g(X) = b_n \cdot (X - v_1) \cdot ... \cdot (X - v_n)$$

mit algebraischen Zahlen $u_1, ..., v_n \in \mathbb{C}$. Dann ist

$$\frac{h(X)}{d} = \frac{a_m \cdot b_n}{d} \cdot (X - u_1) \cdot ... \cdot (X - v_n)$$

nach Voraussetzung ein Polynom mit ganz-algebraischen Koeffizienten. Nach Satz 6.40 c) ist dann jedes Produkt

$$\frac{a_m \cdot b_n}{d} \cdot u_{i_1} \cdot ... \cdot u_{i_k} \cdot v_{j_1} \cdot ... \cdot v_{j_l}$$

ganz-algebraisch. Weil a_i/a_m und b_j/b_n elementar-symmetrische Funktionen der $u_1, ..., u_m$, bzw. $v_1, ..., v_n$ sind, ist damit auch

$$\frac{a_i \cdot b_j}{d} = \frac{a_m \cdot b_n}{d} \cdot \frac{a_i}{a_m} \cdot \frac{b_j}{b_n}$$

ganz-algebraisch. □

Die eben bewiesene Aussage ist eine Verallgemeinerung von Satz 2.30: Dort sind $f(X)$ und $g(X) \in \mathbb{Z}[X]$ ganzzahlige Polynome vom Inhalt $c(f)$ bzw $c(g)$. Hat ihr Produkt h den Inhalt c, so sind alle Zahlen $a_i b_j/c \in \mathbb{Q}$ ganz-algebraisch und nach Beispiel 5.4 selbst ganz. Jeder Teiler von c, der nicht in $c(f)$ aufgeht, muss also in allen b_j, und damit in $c(g)$ aufgehen. Es folgt: c teilt $c(f) \cdot c(g)$. Die Umkehrung ist offensichtlich.

Satz 6.42 *Zu jedem Ideal $(0) \neq I \subset O$ gibt es ein Ideal $J \subset O$ so, dass $I \cdot J$ ein Hauptideal (c) mit $c \in \mathbb{N}$ ist.*

Beweis. Es sei etwa $I = (a_1, ..., a_r)$. Wir betrachten das Polynom

$$g(X) := a_1 X + a_2 X^2 + ... + a_r X^r \in O[X]$$

und seine Konjugierten $g(X), g_2(X), ..., g_s(X)$ unter allen Galois-Automorphismen von K über $\mathbb{Q}$. Das Produkt-Polynom

$$f(X) := g(X) \cdot g_2(X) \cdot ... \cdot g_s(X) =: \sum_{\nu=1}^{n} c_\nu X^\nu$$

ist dann invariant unter allen Galois-Automorphismen von K über $\mathbb{Q}$. Es folgt $f(X) \in \mathbb{Q}[X]$, und weil alle Koeffizienten c_ν von $f(X)$ ganz-algebraisch sind, sogar $f(X) \in \mathbb{Z}[X]$. Der Quotient

$$h(X) = \frac{f(X}{g(X)} = g_2(X) \cdot ... \cdot g_s(X) =: \sum_{\mu=1}^{m} b_\mu X^\mu$$

hat alle seine Koeffizienten $b_\mu \in O$.

Es sei nun $c \in \mathbb{N}$ der ggT aller c_ν, so dass $f(X)/c \in \mathbb{Z}[X]$ den Inhalt $= 1$ hat. Weiter sei $J := (b_1, ..., b_m)$. Wir zeigen: das Produkt $I \cdot J$ der Ideale I und J ist das Hauptideal (c).

$I \cdot J \subset (c)$: Das Ideal $I \cdot J$ wird erzeugt von allen Produkten $a_i \cdot b_j$ der Koeffizienten von g und h. Nach Satz 6.41 teilt c alle diese Produkte in O.

$(c) \subset I \cdot J$: Weil $c = ggT(c_1, ..., c_n)$ ist, gibt es ganze Zahlen $x_1, ..., x_n \in \mathbb{Z}$ mit $c = x_1c_1 + ... + x_nc_n$. Jeder Koeffizient c_ν von f ist Summe von Produkten $a_i \cdot b_j \in I \cdot J$. Es folgt $c \in I \cdot J$. □

Satz 6.43 (Korollar) *a) Es seien $(0) \neq I \subset O$ ein Ideal und $J_1, J_2 \subset O$ zwei Ideale mit $I \cdot J_1 = I \cdot J_2$. Dann ist $J_1 = J_2$.*

b) Ist $J \subset O$ ein Teiler des Ideals $I \subset O$, dann ist J auch ein Faktor.

c) Ein Ideal $M \subset O$ ist maximal genau dann, wenn es irreduzibel ist, d.h., wenn es keine echten Teiler (=Faktoren) hat.

Beweis. a) Nach Satz Satz 6.42 gibt es ein Ideal J derart, dass $I \cdot J$ ein Hauptideal (c), $c \in \mathbb{N}$, ist. Aus $I \cdot J_1 = I \cdot J_2$ folgt damit

$$(c) \cdot J_1 = J \cdot I \cdot J_1 = J \cdot I \cdot J_2 = (c) \cdot J_2.$$

Das Ideal $(c) \cdot J_1$ besteht aber aus allen Produkten $c \cdot x$, $x \in J_1$, ebenso wie $(c) \cdot J_2$ aus allen Produkten $c \cdot y$, $y \in J_2$ besteht. Wir finden $J_1 = J_2$.

b) J ist ein Teiler von I, wenn $I \subset J$. Es gibt ein Ideal J' mit $J \cdot J' = (c)$, $c \in \mathbb{N}$. Das Ideal $I \cdot J'$ ist dann im Hauptideal (c) enthalten. Ist $I = (a_1, ..., a_r)$ und $J' = (b_1, ..., b_s)$, so sind alle Produkte $a_i \cdot b_j$ in O durch c teilbar, etwa $a_i \cdot b_j = c \cdot l_{i,j}$. Dann ist

$$I \cdot J' = (c \cdot l_{1,1}, ..., c \cdot l_{r,s}) = (c) \cdot (l_{1,1}, ..., l_{r,s}) = J \cdot J' \cdot (l_{1,1}, ..., l_{r,s}).$$

Mit a) folgt $I = J \cdot (l_{1,1}, ..., l_{r,s})$ und J ist auch ein Faktor von I.

c) Das Ideal $M \subset O$ ist maximal, genau dann wenn es keine echten Teiler I, $M \subset I \subset O$, $I \neq M, O$, besitzt. Weil Faktoren dasselbe wie Teiler von M sind, kann man M nicht in ein Produkt $I \cdot J$, $I, J \neq M, O$ zerlegen. Wegen $M \neq M^2$ (Satz 6.34 b) kann hier nicht $I = J = M$ gelten. Also ist entweder $I = O$ und dann $J = M$ oder umgekehrt. □

Wir kommen zum krönenden Abschluss dieses Paragraphen.

Satz 6.44 (Hauptsatz über Ideale in algebraischen Zahlkörpern) *Jedes Ideal $I \subset O$, $I \neq (0), (1)$, kann eindeutig (bis auf die Reihenfolge) faktorisiert werden als Produkt*

$$I = M_1 \cdot ... \cdot M_k$$

maximaler Ideale $M_\kappa \subset O$.

Beweis. Existenz: Wenn I selbst nicht maximal ist, dann ist es in einem maximalen Ideal $M_1 \subset O$ enthalten (Satz 6.37 a). Das Ideal M_1 ist ein Teiler von I und nach Satz 6.43 b) auch ein Faktor: Es gibt ein Ideal I_1 mit $I = M_1 \cdot I_1$, $I_1 \supset I, I_1 \neq I$. Wenn I_1 maximal ist, sind wir fertig. Andernfalls machen wir weiter: $I = M_1 \cdot M_2 \cdot I_2$ mit einem maximalen Ideal M_2 und einem Ideal $I_2 \supset I_1$, $I_2 \neq I_1$. Nichts hindert uns daran, immer so weiter zu machen, außer der Tatsache, dass eine echt aufsteigende Idealkette $I \subset I_1 \subset I_2 \subset ... \subset I_k$ irgendwann abbrechen muss (Eigenschaft noethersch, Definition 2.6). Dann ist also $I_k = M_k$ maximal und $I = M_1 \cdot ... \cdot M_k$.

Eindeutigkeit: Es sei

$$I = M_1 \cdot ... \cdot M_k = M_1' \cdot ... \cdot M_l'$$

mit maximalen Idealen $M_1, ..., M_l'$. Weil das maximale Ideal M_1' prim ist, ist es in einem der Ideale $M_1, ..., M_k$ enthalten. Nach Umordnung können wir annehmen $M_1' \subset M_1$. Weil beide Ideale maximal sind, folgt $M_1 = M_1'$ und aus Satz 6.43 a)

$$M_2 \cdot ... \cdot M_k = M_2' \cdot ... \cdot M_l'.$$

Die Behauptung folgt durch Induktion nach $max\{k, l\}$. □

Alles, was man multiplikativ mit ganzen Zahlen in $\mathbb{Z}$ machen kann, oder mit Elementen eines Hauptidealrings, kann man also jetzt mit Idealen in O machen. Insbesondere haben je zwei Ideale $I, J \subset O$ einen größten gemeinsamen Teiler. Das ist ein Ideal T mit $I, J \subset T$ und, falls $T' \subset O$ ein weiteres Ideal mit $I, J \subset T'$ ist, dann gilt $T \subset T'$. Natürlich gibt es die triviale Art, diesen ggT anzugeben: Wenn $I = (a_1, ..., a_k)$ und $J = (b_1, ..., b_l)$, dann ist $T = (a_1, ..., b_l)$. Man schreibt dann abkürzend (und konsequent) $ggT(I, J) = (I, J)$. Dieses Ideal (I, J) besteht aus allen Linearkombinationen

$$\alpha_1 \cdot a_1 + ... + \alpha_k \cdot a_k + \beta_1 \cdot b_1 + ... + \beta_l \cdot b_l, \quad \alpha_1, ..., \beta_l \in O,$$

d.h., aus allen Summen $a + b$ mit $a \in I$ und $b \in J$. Deswegen schreibt man auch

$$(I, J) = I + J.$$

Aber, wenn wir Produkt-Zerlegungen

$$I = M_1^{k_1} \cdot ... \cdot M_r^{k_r}, \quad J = M_1^{l_1} \cdot ... \cdot M_r^{l_r},$$

kennen, dann ist

$$(I, J) = M_1^{min\{k_1, l_1\}} \cdot ... \cdot M_r^{min\{k_r, l_r\}}.$$

Hier ist natürlich $M^0 = O$ zu setzen.

Definition 6.10 *Zwei Ideale I und $J \subset O$ heißen* teilerfremd, *in Zeichen $(I, J) = (1)$, wenn*

$$(I, J) = (1) = O$$

ist.

Satz 6.45 *Für zwei teilerfremde Ideale $I, J \subset O$ gilt:*

a) $I \cdot J = I \cap J$;

b)[Chinesischer Restsatz] Durch $c \bmod I \cdot J \mapsto (c \bmod I, c \bmod J)$ wird ein Ring-Isomorphismus

$$O/I \cdot J \to O/I \times O/J$$

definiert.

Beweis. a) Offensichtlich ist $I \cdot J \subset I \cap J$. Weil $I, J \supset I \cap J$ Teiler des Ideals $I \cdot J$ sind, ist nach Satz 6.43 b)

$$I \cap J = I \cdot I' = J \cdot J'.$$

Weil I und J teilerfremd sind, folgt daraus: Auch $I \cdot J$ ist ein Teiler von $I \cap J$, also $I \cap J \subset I \cdot J$.

b) Weil I und J teilerfremd sind, ist $O = I + J$, und es gibt Zahlen $a \in I$ und $b \in J$ mit $1 = a + b$. Das Element $(1 \bmod I, 0) \in (O/I \times O/J)$ ist dann das Bild von $b \bmod I \cdot J$, während $(0, 1 \bmod J)$ das Bild von $a \bmod I \cdot J$ ist. Der angegebene Ring-Homomorphismus ist also surjektiv.

Sein Kern besteht aus allen Restklassen $c \bmod I \cdot J$ mit $c \in I \cap J = I \cdot J$ (nach a). Deswegen besteht der Kern des Homomorphismus nur aus der Null-Klasse, und der angegebene Epimorphismus ist auch injektiv. □

Satz 6.46 *Es sei $M \subset O$ ein maximales Ideal. Dann gibt es für alle $n \in \mathbb{N}$ einen Isomorphismus von abelschen Gruppen*

$$O/M \to M^n/M^{n+1}.$$

Beweis. Wegen $M^{n+1} \neq M^n$ gibt es ein $a \in M^n$, $a \notin M^{n+1}$. Nach dem Hauptsatz besitzt das Hauptideal (a) eine Produkt-Zerlegung $(a) = M^n \cdot I$ mit einem zu M teilerfremden Ideal I. Die Multiplikation mit a induziert einen Gruppen-Isomorphismus

$$O/M \to O \cdot a/M \cdot a \simeq M^n I/M^{n+1} I.$$

Die Produkt-Zerlegung für das Ideal $(M^n I, M^{n+1})$ zeigt $(M^n I, M^{n+1}) = M^n$, während sie für $M^n I \cap M^{n+1}$ liefert $M^n I \cap M^{n+1} = M^{n+1} I$. Wir betrachten den Restklassen-Gruppen-Homomorhismus

$$M^n I \subset O \to O/M^{n+1}.$$

Sein Kern ist $M^n I \cap M^{n+1} = M^{n+1} I$ und sein Bild ist

$$(M^n I + M^{n+1})/M^{n+1} = M^n/M^{n+1}.$$

Also definiert er einen Gruppen-Isomorphismus $M^n I/M^{n+1} I \to M^n/M^{n+1}$ und wir sind fertig. □

Satz 6.47 *a) Das Ideal $I \subset O$ habe eine Faktorisierung $I = M_1^{r_1} \cdot \ldots \cdot M_k^{r_k}$ als Produkt maximaler Ideale. Dann ist die Anzahl der Elemente im Restklassenring O/I*

$$|O/M_1|^{r_1} \cdot \ldots \cdot |O/M_k|^{r_k}.$$

b) Für ein Produkt $I \cdot J$ ist die Anzahl der Elemente im Restklassenring $O/I \cdot J$

$$|O/I| \cdot |O/J|.$$

Beweis. a) Nach dem Chinesischen Restsatz gibt es einen Ring-Isomorphismus

$$O/I \to (O/M_1^{k_1}) \times ... \times (O/M_k^{r_k}).$$

Es genügt also, für jedes maximale Ideal $M \subset O$ zu zeigen:

$$|O/M^r| = |O/M|^r.$$

Wegen $M^{r+1} \subset M^r$ gibt es einen Ring-Epimorphismus

$$O/M^{r+1} \to O/M^r$$

mit Kern M^r/M^{r+1}. Die Behauptung folgt durch Induktion nach r mit Satz 6.46.

b) Wir faktorisieren $I = M_1^{r_1} \cdot ... \cdot M_k^{r_k}$ und $M_1^{s_1} \cdot M_k^{s_k}$. Dann ist

$$I \cdot J = M_1^{r_1+s_1} \cdot ... \cdot M_k^{r_k+s_k}.$$

□

Aufgabe 6.16 *Es sei O der Ring der ganz-algebraischen Zahlen im imaginär-quadratischen Körper $\mathbb{Q}(\sqrt{-5})$. Zeigen Sie:*

a) Das Ideal $(2+\sqrt{-5}, 2-\sqrt{-5})$ ist das Ideal (1).

b) Der Restklassenring $\mathbb{Z}(\sqrt{-5})/(2)$ ist isomorph zum Ring $\mathbb{F}_2[X]/(X^2)$.

Aufgabe 6.17 *Es sei O der Ring der ganz-algebraischen Zahlen im Zahlkörper $\mathbb{Q}(\sqrt{5})$.*

a) Zeigen Sie: $I := (3, 1+2\sqrt{5}) \subset O$ ist ein Ideal $\neq O$.

b) Ist I ein Prim-Ideal?

Aufgabe 6.18 *Es sei O der Ring der ganz-algebraischen Zahlen in einem algebraischen Zahlkörper K. Weiter seien $P, Q \subset O$ zwei verschiedene Primideale. Zeigen Sie für alle natürlichen Zahlen $m, n \geq 1$:*

$$(P^m, Q^n) = O.$$

6.6 Idealklassen

Für jedes Ideal $I \subset O$, $I \neq (0)$, ist der Restklassenring O/I endlich.

Definition 6.11 *Ist $I \neq (0)$ ein Ideal in O, so heißt die Anzahl der Elemente in O/I die* Norm *von I.*

Satz 6.48 *Es sei $c_1, ..., c_n$ eine Idealbasis von I. Dann gilt*

$$(N(I))^2 = \frac{1}{d} \cdot \Delta(c_1, ..., c_n).$$

Dabei ist d die Diskriminante des Körpers K.

Beweis. Es sei $a_1, ..., a_n \in O$ eine Ganzheitsbasis. Als abelsche Gruppe ist

$$O = \mathbb{Z} \cdot a_1 + ... + \mathbb{Z} \cdot a_n \simeq \mathbb{Z}^n.$$

$I \subset O$ ist eine Untergruppe mit endlichem Quotienten O/I. Nach dem Hauptsatz über endlich erzeugte abelsche Gruppen Satz 1.25 ist dieser Quotient ein Produkt $\mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_n}$ endlich vieler zyklischer Gruppen. Genauer (Beweis dieses Satzes) gibt es eine Ganzheitsbasis $a'_1, ..., a'_n$ derart, dass

$$c'_1 = m_1 a'_1, ..., c'_n = m_n a'_n$$

ein Erzeugendensystem für die Untergruppe I, also eine Idealbasis von I ist. Beim Übergang in die neuen Basen ändert sich weder $\Delta(a_1, ..., a_n) = d$, noch $\Delta(a_1, ..., a_n)$. Für alle Galois-Automorphismen g von K ist $g(c'_i) = m_i g(a'_i)$, $i = 1, ..., n$. Daraus folgt

$$det \begin{pmatrix} c'_1 & ... & c'_n \\ g_2(c'_1) & ... & g_2(c'_n) \\ \vdots & & \vdots \\ g_n(c'_1) & ... & g_n(c'_n) \end{pmatrix} = det \begin{pmatrix} a'_1 & ...a'_n & \\ g_2(a'_1) & ... & g_2(a'_n) \\ \vdots & & \vdots \\ g_n(a'_1) & ... & g_n(a'_n) \end{pmatrix} \cdot det \begin{pmatrix} m_1 & & \\ & \ddots & \\ & & m_n \end{pmatrix}$$

und

$$\Delta(c'_1, ..., c'_n) = \Delta(a'_1, ..., a'_n) \cdot m_1^2 \cdot ... \cdot m_n^2 = d \cdot |O/I|^2.$$

□

Satz 6.49 (Folgerung) *Für ein Hauptideal $(0) \neq (c) \subset O$ ist*

$$N((c)) = |N_{K/\mathbb{Q}}(c)|.$$

Beweis. Ist $a_1, ..., a_n \in O$ eine Ganzheitsbasis, so ist $a_1 \cdot c, ..., a_n \cdot c$ eine Idealbasis von I. Damit folgt

$$\Delta(a_1 c, ..., a_n c) = N_{K/\mathbb{Q}}(c)^2 \Delta(a_1, ..., a_n) = N_{K/\mathbb{Q}}(c)^2 \cdot d.$$

Mit Satz 6.48 finden wir

$$N((c))^2 = N_{K/\mathbb{Q}}(c)^2,$$

und wegen $N((c)) > 0$ die Behauptung. □

Satz 6.50 *a) Für je zwei Ideale $(0) \neq I, J \subset O$ gilt*

$$N(I \cdot J) = N(I) \cdot N(J).$$

b) Ist $N(I) \in \mathbb{N}$ eine Primzahl, so ist $I \subset O$ ein Primideal.
c) Die Zahl $N(I) \in \mathbb{N}$ gehört zum Ideal I.
d) Es gibt nur endlich viele Ideale $I \subset O$ vorgegebener Norm $N(I) = n \in \mathbb{N}$.

Beweis. a) Nach Satz 6.47 b) ist

$$N(I \cdot J) = |O/I \cdot J| = |O/I| \cdot |O/J| = N(I) \cdot N(J).$$

b) Zu jedem maximalen Ideal $M \supset I$ gibt es ein Ideal $J \subset O$ mit $I = M \cdot J$. Nach a) ist dann $N(I) = N(M) \cdot N(J)$. Wegen $M \neq O$ kann hier nicht $N(M) = 1$ sein. Ist $N(I)$ eine Primzahl, so muss $N(J) = |O/J| = 1$ gelten. Das heißt $J = O$ und $I = M$ ist maximal.

c) Es sei $c_1 = 0, c_2, ..., c_{N(I)}$ ein Repräsentantensystem für die Restklassen modulo I. Dann sind auch $c_1 + 1, c_2 + 1, ..., c_{N(I)} + 1$ paarweise modulo I voneinander verschieden, und bilden ebenso ein Repräsentantensytem für die Restklassen modulo I. Wir finden modulo I

$$\begin{aligned} c_1 + ... + c_{N(I)} &= (c_1 + 1) + ... + (c_{N(I)} + 1) \\ &= c_1 + ... + c_{N(I)} + N(I), \\ N(I) &= 0. \end{aligned}$$

Also liegt $N(I)$ im Ideal I.

d) Jedes Ideal I gegebener Norm $N(I) = n$ enthält nach c) die Zahl $n \in \mathbb{N}$. Nach Satz 6.35 gibt es in O nur endlich viele derartige Ideale. □

Satz 6.51 (Kleiner Fermat) *Es sei $P \subset O$ ein Prim-Ideal und $c \in O$, $c \notin P$. Dann ist*

$$c^{N(P)-1} \equiv 1 \, mod \, P.$$

Beweis. Es sei $c_1, ..., c_{N(P)} \in O$ ein Repräsentantensystem für die Restklassen modulo P. Weil P ein Prim-Ideal und $c \notin P$ ist, liegt keine der Differenzen $c \cdot c_i - c \cdot c_j$, $i \neq j$, in P. Auch die Zahlen $c \cdot c_1, ..., c \cdot c_{N(P)}$ repräsentieren alle Restklassen modulo P. Eine der Zahlen c_i, etwa c_1 gehört zu P. Dann gehört auch $c \cdot c_1$ zu P. Es folgt modulo P

$$\begin{aligned} c_2 \cdot ... \cdot c_{N(P)} &= (c \cdot c_2) \cdot ... \cdot (c \cdot c_{N(P)}) \\ &= c_2 \cdot ... \cdot c_{N(P)} \cdot c^{N(P)-1} \end{aligned}$$

und

$$c_2 \cdot ... \cdot c_{N(P)} \cdot (c^{N(P)-1} - 1) \in P.$$

Weil keine der Zahlen c_i, $i \geq 2$ zu P gehört, und weil P ein Primideal ist, folgt daraus $c^{N(P)-1} - 1 \in P$. □

Eine fundamentale Aussage über Ideale in algebraischen Zahlkörpern ist folgender

Satz 6.52 *Es sei K ein Zahlkörper $\neq \mathbb{Q}$ und $I \neq (0)$ ein Ideal in $O = O(K)$. Dann gibt es in I eine Zahl $c \neq 0$ mit*

$$|N_{K/\mathbb{Q}}(c)| \leq N(I)\sqrt{|d|}.$$

Hier ist d die Diskriminante des Zahlkörpers K.

Der Beweis benutzt Eigenschaften der sogenannten „Geometrie der Zahlen“ .

Satz 6.53 (Reelles Lemma von Minkowski) *Es sei $(a_{\mu,\nu})$ eine reelle $n \times n$-Matrix mit Determinante $a = det(a_{\mu,\nu}) \neq 0$. Sind $k_1, ..., k_n > 0$ reelle Zahlen mit $k_1 \cdot ... \cdot k_n > |a|$, so gibt es ganze Zahlen $z_1, ..., z_n \in \mathbb{Z}$, nicht alle $z_\nu = 0$, mit*

$$|\sum_{\nu=1}^{n} a_{\mu,\nu} z_\nu| \leq k_\mu \quad \textit{für} \quad \mu = 1, ..., n.$$

Vor dem Beweis veranschaulichen wir uns diese Aussage: Für jedes $\mu = 1, ..., n$ ist die Menge

$$\{(x_1, ..., x_n) \in \mathbb{R}^n : |\sum_{\nu=1}^{n} a_{\mu,\nu} x_\nu| = k_\mu\}$$

ein Paar paralleler Ebenen im $\mathbb{R}^n$. Alle n Paare solcher Ebenen begrenzen im $\mathbb{R}^n$ ein Parallelotop

$$P_0 := \{(x_1, ..., x_n) \in \mathbb{R}^n : |\sum_{\nu=1}^{n} a_{\mu,\nu} x_\nu| \leq k_\mu,\ \mu = 1, ..., n\}.$$

Wegen $det(a_{\mu,\nu}) \neq 0$ ist dieses Parallelotop nicht ausgeartet. Es ist das Urbild des n-dimensionalen Quaders

$$Q := \{(x_1, ..., x_n) \in \mathbb{R}^n : |x_i| \leq k_i\}$$

des Volumens $2^n \cdot k_1 \cdot ... \cdot k_n$ unter der linearen Abbildung mit der Matrix $(a_{\mu,\nu})$. Deswegen hat P_0 das Volumen

$$\frac{1}{|a|} \cdot k_1 \cdot ... \cdot k_n \cdot 2^n > 2^n.$$

Die Behauptung ist, dass P_0 einen ganzzahligen Vektor $z = (z_1, ..., z_n) \neq 0$ enthält.

Beweis des Satzes. Wir betrachten das geschrumpfte Parallelotop

$$P := \{(x_1, ..., x_n) \in \mathbb{R}^n : |\sum_{\nu=1}^{n} a_{\mu,\nu} x_\nu| \leq k_\mu/2,\ \mu = 1, ..., n\}$$

mit dem Volumen

$$|P| = \frac{k_1 \cdot ... \cdot k_n}{|a|} =: 1 + \epsilon.$$

Und für jeden ganzzahligen Vektor $z = (z_1, ..., z_n) \in \mathbb{Z}^n$ betrachten wir das verschobene Parallelotop

$$P + z := \{(x_1, ..., x_n) \in \mathbb{R}^n : |\sum_{\nu=1}^{n} a_{\mu,\nu}(x_\nu - z_\nu)| \leq k_\mu/2,\ \mu = 1, ..., n\}.$$

Wir zeigen, dass es zwei verschiedene verschobene Parallelotope $P + z$ und $P + z'$, $z \neq z'$, geben muss, die sich schneiden. Ist nämlich $x \in (P + z) \cap (P + z')$, so gilt für $\mu = 1, ..., n$

$$|\sum_{\nu=1}^{n} a_{\mu,\nu}(z_\nu - z'_\nu)| \leq |\sum_{\nu=1}^{n} a_{\mu,\nu}(z_\nu - x_\nu)| + |\sum_{\nu=1}^{n} a_{\mu,\nu}(z'_\nu - x_\nu)| \leq k_\mu,$$

und $z - z' \neq 0$ ist ein ganzzahliger Vektor, der die behaupteten Anforderungen erfüllt.

Wenn sich keine zwei verschobenen Parallelotope $P+z$ und $P+z'$, $z \neq z' \in \mathbb{Z}^n$, schneiden, dann sind sie alle disjunkt. Wir betrachten einen großen Würfel

$$W(N) := \{(x_1, ..., x_n) \in \mathbb{R}^n : |x_\nu| \leq N\}$$

mit $N \in \mathbb{N}$. Ist

$$c := max\{\| x \| : x \in P\},$$

so liegen alle 2^{2N+1} verschobenen Parallelotope

$$P + z, \quad z = (z_1, ..., z_n) \in \mathbb{Z}^n, \quad |z_\nu| \leq N,$$

in dem etwas größeren Würfel $W(N+c)$ der Kantenlänge $2(N+c)$. Er hat das Volumen $2^n(N+c)^n$ und enthält die $(2N+1)^n$ disjunkten verschobenen Parallelotope mit einem Volumen

$$|P| = 1 + \epsilon, \quad \epsilon > 0.$$

Es folgt für alle N

$$(2N+1)^n \cdot (1+\epsilon) \leq (2N+2c)^n,$$

bzw.

$$1 + \epsilon \leq \frac{(2N+2c)^n}{(2N+1)^n}.$$

Für $N \to \infty$ geht die rechte Seite gegen 1, Widerspruch! □

Satz 6.54 (Komplexes Lemma von Minkowski) *Nun sei die $n \times n$-Matrix $a_{\mu,\nu}$ komplex. Wir setzen allerdings voraus: Die ersten r Zeilen, $0 \leq r \leq n$, seien reell, und die anderen paarweise konjugiert-komplex, etwa $n = r + 2s$ und*

$$a_{r+s+\mu,\nu} = \bar{a}_{r+\mu,\nu}, \quad \mu = 1, ..., s, \ \nu = 1, ..., n.$$

Außerdem gelte $k_{r+s+\mu} = k_{r+\mu}$ für $\mu = 1, ..., s$. Dann gilt dieselbe Aussage: Ist $k_1 \cdot ... \cdot k_n > |a|$ mit $a = det(a_{\mu,\nu})$, so gibt es ganze Zahlen $z_1, ..., z_n$, nicht alle $= 0$, die

$$|\sum_{\nu=1}^{n} a_{\mu,\nu} z_\nu| \leq k_\mu \quad \text{für} \quad \mu = 1, ...n,$$

erfüllen.

Beweis. Wir ersetzen die $2s$ komplexen Ungleichungen durch die $2s$ reellen Ungleichungen

$$|\sum_{\nu=1}^{n} (a_{\mu,\nu} + \bar{a}_{\mu,\nu}) z_\nu| / \sqrt{2} \leq k_\mu, \quad |\sum_{\nu=1}^{n} \frac{1}{i} (a_{\mu,\nu} - \bar{a}_{\mu,\nu}) z_\nu| / \sqrt{2} \leq k_\mu.$$

Die neue reelle Koeffizientenmatrix ensteht aus der alten komplexen, indem man sie von links mit einer Matrix

$$\begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & \frac{1}{\sqrt{2}} & \cdots & \frac{1}{\sqrt{2}} & & \\ & & & \ddots & & \ddots & \\ & & \frac{1}{i\sqrt{2}} & & -\frac{1}{i\sqrt{2}} & & \\ & & & \ddots & & \ddots & \end{pmatrix}$$

multipliziert. Diese Matrix hat eine Determinante vom Betrag 1. Deswegen hat die neue Koeffizientenmatrix eine Determinante vom gleichen Betrag wie die alte Koeffizientenmatrix. Es gibt aslo einen ganzzahligen Vektor $0 \neq z \in \mathbb{Z}$, der die neuen Ungleichungen erfüllt:

$$\begin{aligned} |\sum_{\nu=1}^{n} Re(a_{\mu,\nu}) z_\nu| &\leq k_\mu/\sqrt{2}, \\ |\sum_{\nu=1}^{n} Im(a_{\mu,\nu}) z_\nu| &\leq k_\mu/\sqrt{2}, \\ |\sum_{\nu=1}^{n} a_{\mu,\nu} z_\nu|^2 &\leq k_\mu^2, \end{aligned}$$

und daraus folgt die Behauptung.

Beweis von Satz 6.52: Es sei $c_1, ..., c_n$ eine Idealbasis von I. Die Elemente von I sind dann die ganzzahligen Linearkombinationen $\sum_{\nu=1}^{n} c_\nu z_\nu$, $z_\nu \in \mathbb{Z}$. Ihre Konjugierten über $\mathbb{Q}$ sind die Zahlen

$$\sum_{\nu=1}^{n} g_\mu(c_\nu) \cdot z_\nu,$$

wo g_μ die Galois-Automorphismen von K über $\mathbb{Q}$ durchläuft. Die komplexe Matrix

$$(a_{\mu,\nu}) = (g_\mu(c_\nu))$$

hat nach Satz 6.48 eine Determinante vom Betrag $N(I) \cdot \sqrt{d}$. Ein Galois-Automorphismus ist die komplexe Konjugation. Wenn er trivial ist, sind alle $g_\mu(c_\nu)$ reell. Andernfalls ist $n = r + 2s$, und man kann die Galois-Automorphismen so ordnen, dass

$$\overline{g_{r+\mu}(c_\nu)} = g_{r+s+\mu}(c_\nu), \quad \mu = 1, ..., s, \nu = 1, ..., n.$$

Die komplexe Matrix $(a_{\mu,\nu})$ erfüllt also die Voraussetzungen von Satz 6.54.

Wir setzen in Satz 6.54

$$k_1 = ... = k_n = k := \sqrt[n]{N(I)\sqrt{|d|} + \epsilon}$$

und finden einen Vektor $0 \neq z \in \mathbb{Z}^n$ mit

$$|\sum_{\nu=1}^{n} g_\mu(c_\nu) z_\nu| \leq k.$$

Die Zahl

$$0 \neq c := \sum_{\nu=1}^{n} c_\nu z_\nu \in I$$

hat dann eine Norm

$$N_{K/\mathbb{Q}}(c) \leq k^n = N(I) \cdot \sqrt{|d|} + \epsilon.$$

Dieses tun wir für jedes $\epsilon > 0$. Nun ist $N_{K/\mathbb{Q}}(c) \in \mathbb{Z}$. Wenn $\sqrt{|d|}$ ganzzahlig ist, wählen wir $\epsilon < 1/2$ und finden $N_{K/\mathbb{Q}}(c) \leq N(I)\sqrt{|d|}$. Wenn $\sqrt{|d|}$ nicht ganzzahlig ist, dann ist diese Wurzel auch nicht rational. Es gibt also ein $n \in \mathbb{N}$ mit $n - 1 < N(I)\sqrt{|d|} < n$. Wir wählen $\epsilon < n - N(I)\sqrt{|d|}$ und finden jetzt sogar $N_{K/\mathbb{Q}}(c) \leq n - 1 < N(II)\sqrt{|d|}$. □

So, jetzt wird's echt klassisch:

Definition 6.12 *Zwei Ideale $I, J \subset O$ heißen äquivalent, in Zeichen $I \sim J$, wenn es Hauptideale $(a), (b) \neq (0)$ mit*

$$(a) \cdot I = (b) \cdot J$$

gibt.

Satz 6.55 *Die soeben definierte Relation zwischen Idealen in O ist eine Äquivalenzrelation.*

Beweis. Reflexivität: Es ist $(1) \cdot I = I = (1) \cdot I$.

Symmetrie: Wenn $(a) \cdot I = (b) \cdot J$ gilt, dann ist $(b) \cdot J = (a) \cdot I$.

Transitivität: Es sei $I_1 \sim I_2$ und $I_2 \sim I_3$, d.h. $(a_1) \cdot I_1 = (b_1)I_2$ und $(a_2) \cdot I_2 = (b_2)I_3$ mit $a_1, a_2, b_1, b_2 \neq 0$. Dann ist

$$(a_1 a_2)I_1 = (b_1 a_2)I_2 = (b_1 b_2)I_3$$

mit $a_1 a_2, b_1 b_2 \neq 0$. □

Definition 6.13 *Eine Idealklasse in O ist eine Äquivalenzklasse von Idealen in O bezüglich der Äquivalenzrelation aus Definition 6.12.*

Satz 6.56 *a) Alle Hauptideale $\neq (0)$ in O sind äquivalent und gehören zur gleichen Klasse wie (1).*

b) Ist ein Ideal $I \sim (1)$, so ist I selbst ein Hauptideal. Alle Hauptideale in O bilden also eine Idealklasse.

c) Aus $I_1 \sim I_2$ folgt $I_1 \cdot J \sim I_2 \cdot J$ für jedes Ideal $J \subset O$.

d)[Kürzungsregel] Ist $I_1 \cdot J \sim I_2 \cdot J$ für ein Ideal $J \neq (0)$, so ist $I_1 \sim I_2$.

e) Die Anzahl der Idealklassen in O ist endlich.

Beweis. a) Für ein Hauptideal (a), $a \neq 0$, ist

$$(1) \cdot (a) = (a) \cdot (1),$$

also $(a) \sim (1)$.

b) Die Äquivalenz $I \sim (1)$ bedeutet $(a) \cdot I = (b) \cdot (1) = (b)$ mit $a, b \neq 0$. Insbesondere gehört b zum Ideal (a) und $b = b' \cdot a$, $b' \in O$. Es gilt also $(a) \cdot I = (a) \cdot (b')$, und aus Satz 6.43 a) folgt $I = (b')$.

c) aus $I_1 \sim I_2$ folgt $(a) \cdot I_1 = (b) \cdot I_2$ und $(a) \cdot I_1 J = (b) \cdot I_2 J$ mit $a, b \neq 0$.

d) Nach Satz 6.42 gibt es ein Ideal J' derart, dass $J \cdot J' = (b)$ ein Hauptideal $\neq (0)$ ist. Aus $I_1 \cdot J \sim I_2 \cdot J$ folgt also $I_1 \cdot (b) \sim I_2 \cdot (b)$ und $(a_1 b) \cdot I_1 = (a_2 b) \cdot I_2$.

e) Es genügt zu zeigen, dass es in jeder Idealklasse ein Ideal I mit $N(I) \leq \sqrt{|d|}$ gibt, denn die Anzahl der Ideale gegebener Norm ist endlich nach Satz 6.50 d). Sei also J ein Ideal, das eine Idealklasse repräsentiert. Nach Satz 6.42 gibt es ein Ideal $J' \neq (0)$ derart, dass JJ' ein Hauptideal ist. Es ist also $JJ' \sim (1)$. Nach Satz 6.52 enthält J' ein Element $a \neq 0$ mit $|N(a)| \leq N(J')\sqrt{|d|}$. Wegen $(a) \subset J'$ ist J' ein Teiler des Hauptideals (a) und nach Satz 6.43 b) gibt es ein Ideal I mit $(a) = J' \cdot I$. Mit Satz 6.50 a) folgt

$$N(J') \cdot N(I) = N((a)) = |N(a)| \leq N(J') \cdot \sqrt{|d|},$$

also $N(I) \leq \sqrt{|d|}$. Weiter ist

$$J \cdot J' \sim (1) \sim I \cdot J',$$

und aus der Kürzungsregel folgt $J \sim I$. In der Idealklasse von J liegt also das Ideal I mit $N(I) \leq \sqrt{|d|}$. □

Definition 6.14 *Die Anzahl h der Idealklassen in O heißt* Klassenzahl *des Zahlkörpers K.*

Die Klasssenzahl h ist also genau dann $= 1$, wenn alle Ideale in O Hauptideale sind, d.h., wenn O ein Hauptidealring ist.

Satz 6.57 *Die Multiplikation von Idealen definiert auf der Menge der Idealklassen $\not\sim (0)$ die Struktur einer (endlichen) abelschen Gruppe.*

Beweis. Die Multiplikation von Idealen ist kommutativ und assoziativ. Deswegen ist auch die Multiplikation von Idealklassen kommutativ und assoziativ. Die Klasse (1) der Hauptideale ist ein neutrales Element bezüglich dieser Multiplikation. Und nach Satz 6.42 gibt es zu jedem Ideal $I \neq (0)$ ein Ideal J derart dass $I \cdot J$ ein Hauptideal $\neq (0)$, also $I \cdot J \sim (1)$ ist. Die Klasse von J ist das Inverse der Klasse von I bezüglich der Multiplikation von Idealklassen. □

Definition 6.15 *Die Gruppe $C(K)$ aus Satz 6.57 heißt die* Idealklassengruppe *des Körpers K.*
.

Satz 6.58 *In jeder Idealklasse des Zahlkörpers K liegt ein Ideal $I \subset O$ mit Norm*

$$N(I) \leq \sqrt{|d|}.$$

Dies wurde im Beweis von Satz 6.56 e) gezeigt.

Beispiel 6.27 *Nach Satz 6.19 haben die imaginär-quadratischen Zahlkörper* $\mathbb{Q}(\sqrt{-p})$ *die Klassenzahl* 1 *für* $p = 1, 2, 3$. *Der erste imaginär-quadratische Zahlkörper mit Klassenzahl* > 1 *ist* $K = \mathbb{Q}(\sqrt{-5})$, *weil hier die Zerlegung in irreduzible Faktoren nicht eindeutig ist. Wir wollen seine Klassenzahl berechnen.*

Die Norm von K *ist* $d = -20$, *und nach Satz 6.58 liegt in jeder Idealklasse ein Ideal* I *mit Norm* $\leq \sqrt{20}$, *also* $N(I) \leq 4$. *Wir untersuchen alle Ideale* $I \subset O(K) = \mathbb{Z}(\sqrt{-5})$ *der Norm* $2, 3$ *oder* 4. *Dabei gehen wir davon aus, dass* $N(I)$ *zu* I *gehört (Satz 6.50 c)*

Norm 2: *Sei* $N(I) = 2$. *Mit* 2 *gehört auch das Hauptideal* (2) *zu* I. *Die Restklassen modulo* (2) *sind*

$$0, \quad 1, \quad , \sqrt{-5}, \quad 1 + \sqrt{-5}.$$

Wenn 1 *zu* I *gehört, dann ist* $I = (1)$. *Wegen*

$$\sqrt{-5}^2 = -5 = -1 \, mod \, (2)$$

kann auch -5 *nicht zu* I *gehören. Die einzige Möglichkeit ist* $1 + \sqrt{-5} \in I$ *und dann auch* $1 - \sqrt{-5} \in I$. *Nun bilden die Zahlen* $1 + \sqrt{-5}$ *und* $1 - \sqrt{-5}$ *eine Idealbasis des Ideals* $I_2 := (1 + \sqrt{-5}, 1 - \sqrt{-5})$. *Das ist nicht ganz offensichtlich - es folgt aus* $(2) \subset I_2$ *und*

$$(1 + \sqrt{-5}) \cdot \sqrt{-5} = -5 + \sqrt{-5} = -(1 - \sqrt{-5}) \in I_2,$$

$$(1 - \sqrt{-5}) \cdot \sqrt{-5} = 5 + \sqrt{-5} = 1 + \sqrt{-5} \in I_2$$

modulo 2. *Für die Norm von* I_2 *finden wir nach Satz 6.48*

$$N(I_2)^2 = \frac{1}{d} \cdot det \begin{pmatrix} 1 + \sqrt{-5} & 1 - \sqrt{-5} \\ 1 - \sqrt{-5} & 1 + \sqrt{-5} \end{pmatrix}^2 = \frac{-80}{-20} = 4,$$

also $N(I_2) = 2$. *Das einzige Ideal* $I \subset O$ *der Norm* 2 *ist* $I_2 := (1 + \sqrt{-5}, 1 - \sqrt{-5})$.

Norm 3: *Jetzt ist* $(3) \subset I$. *Ein Restklassensystem modulo* (3) *ist*

$$\begin{array}{lll} 0, & 1, & 2, \\ \sqrt{-5}, & 1 + \sqrt{-5}, & 2 + \sqrt{-5}, \\ 2\sqrt{-5}, & 1 + 2\sqrt{-5}, & 2 + 2\sqrt{-5}. \end{array}$$

Die Zahlen $1, 2, \sqrt{-5}$ *und* $2\sqrt{-5}$ *sind Einheiten modulo* (3) *und dürfen nicht zu* I *gehören. Modulo dieser Einheiten gibt es noch die beiden folgenden Repräsentanten:*

$$1 + \sqrt{-5}, \quad 1 + 2\sqrt{-5} = 1 - \sqrt{5}.$$

Wegen

$$(1 + \sqrt{-5}) \cdot \sqrt{-5} = -5 + \sqrt{-5} = 1 + \sqrt{-5}$$

modulo 3 *ist* $1 + \sqrt{-5}$ *und* 3 *eine Idealbasis des Ideals* $I_3 := (1 + \sqrt{-5}, 3)$. *Mit Satz 6.48 ist*

$$N(I_3)^2 = \frac{1}{d} det \begin{pmatrix} 1 + \sqrt{-5} & 3 \\ 1 - \sqrt{-5} & 3 \end{pmatrix}^2 = \frac{-180}{-20} = 9,$$

also $N(I_3) = 3$. *Genauso findet man für*

$$I_3' := (1 - \sqrt{-5}, 3)$$

$N(I_3') = 3$. *Die einzigen Ideale der Norm* 3 *in* O *sind* I_3 *und* I_3'.

Norm 4: *Die Restklassen modulo* (4) *in* O *werden repräsentiert von*

$$\begin{array}{llll} 0, & 1, & 2, & 3, \\ \sqrt{-5}, & 1+\sqrt{-5}, & 2+\sqrt{-5}, & 3+\sqrt{-5}, \\ 2\sqrt{-5}, & 1+2\sqrt{-5}, & 2+2\sqrt{-5}, & 3+2\sqrt{-5}, \\ 3\sqrt{-5}, & 1+3\sqrt{-5}, & 2+3\sqrt{-5}, & 3+3\sqrt{-5}. \end{array}$$

Hiervon sind die Zahlen $1, 3, \sqrt{-5}, 3\sqrt{-5}$ *Einheiten in* $I/(4)$ *und können nicht in* I *legen. Wenn die Zahl* 2 *zu* I *gehört, dann ist* $(2) \subset I$, *und aus* $N((2)) = 4$ *folgt* $I = (2)$. *Es wird sich herausstellen, dass dies die einzige Möglichkeit ist:*

Aus $2\sqrt{-5} \in I$ *folgt* $2 \in I$ *und* $I = (2)$.

Wenn $1 + \sqrt{-5}$ *zu* I *gehört, dann auch*

$$(1 + \sqrt{-5}) \cdot \sqrt{-5} = -5 + \sqrt{-5} = -1 + \sqrt{-5} \, mod \, 4.$$

also würde auch in diesem Fall $2 \in I$ *und* $I = (2)$ *gelten.*

Die Assoziierten von $1 + \sqrt{-5} \, mod \, (4)$ *im Ring* $O/(4)$ *haben die Repräsentanten* $3 + 3\sqrt{-5}$, $(1 + \sqrt{-5}) \cdot \sqrt{-5} = 3 + \sqrt{-5} \, mod \, 4$ *und* $3 \cdot (3 + \sqrt{-5}) = 1 + 3\sqrt{-5} \, mod \, 4$. *Auch wenn eine dieser Zahlen in* I *liegt, gilt* $I = (2)$.

Wenn $1 + 2\sqrt{-5}$ *in* I *liegt, dann auch*

$$(1 + 2\sqrt{-5}) \cdot \sqrt{-5} = -10 + \sqrt{-5} = 2 + \sqrt{-5} \, mod \, 4.$$

Es würde folgen $3 + 3\sqrt{-5} \in I$ *und* $I = (2)$.

Die Assoziierten von $1 + 2\sqrt{-5}$ *in* $O/(4)$ *sind* $3 + 2\sqrt{-5}$, $2 + 3\sqrt{-5}$ *und* $2 + 3\sqrt{-5}$. *Enthielte* I *eine dieser Zahlen, so hätten wir wieder* $I = (2)$.

Damit sind wir alle Repräsentanten modulo (4) *durchgegangen und haben gefunden: Das einzige Ideal* $I \subset O$ *der Norm* 4 *ist das Hauptideal* (2).

Durch 'Checking Cases' haben wir gesehen: Die einzigen nicht-trivialen Idealklassen in $C(K)$ *werden repräsentiert durch* I_2, I_3 *oder* I_3'. *Nun gilt*

$$I_2 \cdot (1 + \sqrt{-5}) = (1 + \sqrt{-5}, 1 - \sqrt{-5}) \cdot (1 + \sqrt{-5}) = (-4 + 2\sqrt{-5}, 6) = (2 + 2\sqrt{-5}, 6),$$

$$I_3 \cdot (2) = (1 + \sqrt{-5}, 3) \cdot (2) = (2 + 2\sqrt{-5}, 6).$$

also repräsentieren I_2 *und* I_3 *dieselbe Idealklasse in* $C(K)$. *Ganz analog sieht man* $I_2 \sim I_3'$. *Es gibt also höchstens eine nicht-triviale Idealklasse. Wegen* $C(K) \neq \{1\}$ *folgt endlich* $C(K) \simeq \mathbb{Z}_2$.

Satz 6.59 *Es sei* $I \subset O$ *ein Ideal in* K *und* h *die Klassenzahl von* K. *Dann ist* I^h *ein Hauptideal.*

Beweis. Für $I = (0)$ ist die Aussage trivial. Sei also $I \neq (0)$.

Die Idealklassengruppe $C(K)$ hat die Ordnung h. Für jedes Element $c \in C(K)$ ist also $c^h = 1$. Insbesondere gilt auch für I, dass $I^h \sim (1)$ ist. NachSatz 6.56 b) ist dann I^h ein Hauptideal. □

Satz 6.60 *Es sei $p \in \mathbb{N}$ eine Primzahl, welche die Klassenzahl h des Körpers K nicht teilt. Ist dann $I^p \sim J^p$ für Ideale $I, J \subset K$, so gilt $I \sim J$.*

Beweis. Die Voraussetzung ist $(a) \cdot I^p = (b) \cdot J^p$ mit $0 \neq a, b \in O$. Weil p und h relativ prim sind, gibt es ganze Zahlen $r, s \in \mathbb{Z}$ mit $pr - hs = 1$. Dann ist

$$\begin{aligned} (a)^r I^{pr} &= (b)^r J^{pr}, \\ (a)^r I I^{hs} &= (b)^r J J^{hs} \end{aligned}$$

mit Hauptidealen $I^{hs} = (I^h)^s$ und $J^{hs} = (J^h)^s$. Aus Definition 6.12 folgt die Behauptung. □

Definition 6.16 *Eine Primzahl $p \in \mathbb{N}$ heißt* regulär, *wenn p die Klassenzahl h des p-ten Kreisteilungskörpers $\mathbb{Q}(\sqrt[p]{1})$ nicht teilt. Andernfalls heißt p* irreguläre *Primzahl.*

Die erste irreguläre Primzahl ist die Brieskorn-Zahl 37. Es gibt unendlich viele irreguläre Primzahlen. Das ist nicht-trivial, und wir können es hier nicht beweisen. Das ist aber auch sehr schade, denn es gilt der von Kummer bewiesene:

Satz 6.61 (Fermat für reguläre Primzahlen, Fall 1) *Es sei $p \in \mathbb{N}$ eine reguläre Primzahl. Dann gibt es keine Lösungen $x, y, z \in \mathbb{Z}$ der Gleichung*

$$x^p + y^p = z^p$$

mit $p \not| x, y, z$.

Beweis. Wie im Beweis von Satz 6.29 können wir x, y, z paarweise relativ prim annehmen. Dort haben wir benutzt

$$z^p = (x + y) \cdot (x + wy) \cdot \ldots \cdot (x + w^{p-1} y)$$

mit einer primitiven p-ten Einheitswurzel w. Nach Satz 6.28 sind alle Faktoren $x + w^k y$ auf der rechten Seite teilerfremd. Der wesentliche Punkt im Beweis von Satz 6.29 war, zu schließen dass jeder Faktor $x + w^k y$ und insbesondere

$$x + wy = e \cdot a^p$$

bis auf eine Einheit e eine p-te Potenz $a^p \in O$ ist. Das stimmt, wenn O ein Hauptidealring, und deswegen faktoriell ist. Aber es stimmt auch allgemeiner, wenn p die Klassenzahl h von $\mathbb{Q}(\sqrt[p]{1})$ nicht teilt:

Aus der Eindeutigkeit der Primfaktorzerlegung für Ideale (Satz 6.44) folgt $(x + wy) = I^p$ mit einem Ideal $I \subset O$. Das Ideal I^p ist also ein Hauptideal $I^p \sim (1) = (1)^p$. Mit Satz 6.60 folgt jetzt, dass auch $I \sim (1)$, und I selbst ein Hauptideal $I = (a)$ ist. Es ist also

$$(x + wy) = (a)^p = (a^p).$$

Daraus folgt auch jetzt wieder $x + wy = e \cdot a^p$ mit einer Einheit $e \in O$. Der Rest des Beweises ist wörtlich derselbe. □

Ganz am Schluss wollen wir noch einmal auf den Begriff des Ideals als ideale Zahl zurück kommen.

Satz 6.62 *Es sei I ein Ideal im Ring $O(K)$ des algebraischen Zahlkörpers K. Dann gibt es eine ganz-algebraische Zahl a (i.A. nicht in K) derart, dass I aus allen Produkten $a \cdot b$ besteht, die in K liegen, und wo b eine ganz-algebraische Zahl ist.*

Beweis. Ist h die Klassenzahl von K, so ist $I^h = (u)$, $u \in O(K)$, ein Hauptideal. Nach Satz 6.2 ist $a := \sqrt[h]{u}$ ganz-algebraisch. Wir betrachten die Körper-Erweiterung $L := K(a)$ und in $O(L)$ die Ideale

$$I_L := O(L) \cdot I, \quad (u)_L := O(L) \cdot u.$$

Auch in L gilt

$$I_L^h = O(L) \cdot I^h = O(L) \cdot (u) = (u)_L.$$

Insbesondere ist

$$I_L^h = (u)_L = (a)^h.$$

Aus der Eindeutigkeit der Faktor-Zerlegung für Ideale (Satz 6.44) folgt $I_L = (a)$. Dann ist jede Zahl $c \in I \subset I_L = (a)$ von der Form $c = a \cdot b$ mit einer ganz-algebraischen Zahl $b \in O(L)$.

Wir müssen noch umgekehrt zeigen: Jedes Produkt $c = a \cdot b \in K$, wo b eine ganz-algebraische Zahl ist, gehört zu I. Wegen $c \in K \subset L$ und $a \in L$ ist hier notwendig $b \in O(L)$, also $c \in (a)_L$. Sei nun k der Körpergrad $[L : K]$ und seien $a_1, ..., a_k$ die Konjugierten von a über K, sowie $b_1, ..., b_k$ die Konjugierten von b. Weil $c \in K$ ist, stimmt c mit all seinen Konjugierten über K überein, und wir haben

$$c = a_i b_i, \quad i = 1, ..., k.$$

Ebenso folgt aus $a^h = u$, dass $a_i^h = u$ ist für alle i. Mit $v := b_1 \cdot ... \cdot b_k \in K$ finden wir

$$c^k = (a_1 \cdot ... \cdot a_k) \cdot (b_1 \cdot ... \cdot b_k) = (a_1 \cdot ... \cdot a_k) \cdot v$$

und

$$c^{hk} = (a_1^h \cdot ... \cdot a_k^h) \cdot v^h = u^k \cdot v^h.$$

Dies ist eine Gleichung für Zahlen in K. Für die entsprechenden Hauptideale in $O(K)$ folgt daraus

$$(c)^{hk} = (u)^k \cdot (v)^h = I^{hk} \cdot v^h.$$

Wieder benutzen wir die Eindeutigkeit der Primfaktorzerlegung bei Idealen um

$$(c)^k = I^k \cdot (v)$$

zu schließen. Als Faktor des Ideals $(c)^k$ ist I^k auch ein Teiler. Noch eine Anwendung der Eindeutigkeit der Faktorzerlegung zeigt dass I ein Teiler des Hauptideals (c) ist. Dies hat nun endlich $c \in I$ zur Folge. □

Aufgabe 6.19 *a) Bestimmen Sie die Normen der Ideale* $(1+i)$ *und* (2) *im Zahlkörper* $\mathbb{Q}(i)$.
b) Welches dieser Ideale ist ein Primideal?
c) Zeigen Sie, dass der Restklassenring $\mathbb{Z}[i]/(2)$ *isomorph zum Ring* $\mathbb{F}_2[X]/(X^2)$ *ist.*

Aufgabe 6.20 *Bestimmen Sie die Norm des Ideals* $(1+2i)$ *im Zahlkörper* $\mathbb{Q}(i)$ *und ein Repräsentantensystem für die Restklassen modulo* $(1+2i)$.

Aufgabe 6.21 *Es sei* $D = 2$ *oder* $3 \bmod 4$ *eine ganze Zahl und* $I \subset O(\mathbb{Q}(\sqrt{D}))$ *ein Ideal mit der Idealbasis*

$$a + b\sqrt{D},\ b + c\sqrt{D}, \quad a, b, c, d \in \mathbb{Z}.$$

Zeigen Sie: $N(I) = |ad - bc|$.

Aufgabe 6.22 *a) Bestimmen Sie die Norm des Ideals*

$$I = (7 + \sqrt{-5},)3 + 3\sqrt{-5})$$

im Körper $\mathbb{Q}(\sqrt{-5})$.
b) Schreiben Sie I *als Produkt von Primidealen in* $O(\mathbb{Q}(\sqrt{-5}))$.

Uijuiuijui-uijui! Uff! Ende der Fahnenstange! Die Fabrikation dieses Skriptums hat mich sehr viel Energie und Grips, und die letzten Monate so ziemlich meine ganze freie Zeit gekostet. Hoffentlich reicht dieses Skriptum bis zum Ende des Semesters. Mir reicht es jedenfalls!

Index