Algebra I

Eine beispielorientierte Einführung in die Algebra und Zahlentheorie

Wintersemester 2019/20

M. Schütt (basierend auf dem Skript von W. Ebeling
mit Ergänzungen von K. Hulek)

Institut für Algebraische Geometrie
Leibniz Universität Hannover
Welfengarten 1
30167 Hannover
E-mail: schuett@math.uni-hannover.de

Kapitel 1

Arithmetik der ganzen Zahlen

1.1 Elementare Zahlentheorie

Wir wollen Eigenschaften der ganzen Zahlen untersuchen. Die Menge $\mathbb{N}$ der natürlichen Zahlen ist die Menge

$$\mathbb{N} = \{1, 2, 3, \ldots\}.$$

Die Menge $\mathbb{Z}$ der ganzen Zahlen ist die Menge

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

Definition Es seien a, b ganze Zahlen. Wir sagen, dass die Zahl a die Zahl b *teilt*, in Zeichen $a|b$, falls es eine ganze Zahl q gibt mit

$$b = q \cdot a.$$

Bemerkung (a) Für jede ganze Zahl a gilt $a|a$.
(b) Für jede ganze Zahl a gilt $a|0$.
(c) Aus $a|b$ folgt $a|bc$ für jede ganze Zahl c.
(d) Was sind die Teiler von 1?

Lemma 1.1 *Es seien a, b, b' ganze Zahlen. Dann gilt:*

$$a|b \text{ und } a|b' \Rightarrow a|(b + b') \text{ und } a|(b - b').$$

Beweis.

$$\begin{aligned} a|b \text{ und } a|b' &\Rightarrow \exists q, q' \in \mathbb{Z} : b = q \cdot a \text{ und } b' = q' \cdot a \\ &\Rightarrow b + b' = q \cdot a + q' \cdot a = (q + q') \cdot a \\ &\Rightarrow a|(b + b') \end{aligned}$$

Analog zeigt man $a|(b - b')$. □

Definition Es sei a eine ganze Zahl. Der *Absolutbetrag* von a, in Zeichen $|a|$, ist wie folgt definiert:

$$|a| := \begin{cases} a & \text{falls } a \geq 0, \\ -a & \text{falls } a < 0. \end{cases}$$

Lemma 1.2 *Es seien a, b ganze Zahlen mit $b \neq 0$. Dann gilt:*

$$a|b \Rightarrow |a| \leq |b|.$$

Beweis. Zunächst seien $a > 0$ und $b > 0$. Aus $a|b$ folgt, dass es eine ganze Zahl q gibt mit $b = q \cdot a$. Wegen $a > 0$ und $b > 0$ folgt auch $q > 0$. Also gilt

$$a = \frac{b}{q} \leq b.$$

Der allgemeine Fall ergibt sich aus:

$$a|b \Rightarrow |a||b|.$$

□

Lemma 1.3 *Es seien a, b ganze Zahlen mit $a > 0$, $-(a-1) \leq b \leq a-1$ und $a|b$. Dann ist $b = 0$.*

Beweis. Angenommen, $b \neq 0$. Dann folgt aus Lemma 1.2 $a \leq |b|$. Aus $-(a-1) \leq b \leq a-1$ folgt aber $|b| \leq a-1$, ein Widerspruch. Also ist $b = 0$. □

Satz 1.4 (Division mit Rest) *Es seien a, b ganze Zahlen mit $a \neq 0$. Dann gibt es eindeutig bestimmte ganze Zahlen q ("*Quotient*") und r ("*Rest*") mit*

$$b = qa + r \text{ und } 0 \leq r < |a|.$$

Beweis. (a) Wir zeigen zunächst die *Eindeutigkeit*: Angenommen, es gibt ganze Zahlen q, r und q', r' mit

$$b = qa + r = q'a + r' \text{ und } 0 \leq r, r' < |a|.$$

Dann folgt

$$(q - q')a = r' - r \text{ und } -(|a| - 1) \leq r - r' \leq |a| - 1.$$

Aus Lemma 1.3 folgt dann $r - r' = 0$, also $r = r'$. Aus

$$(q - q')a = 0$$

folgt dann wegen $a \neq 0$ auch $q = q'$.

(b) Nun zeigen wir die *Existenz* von q, r. Wir zeigen dies zunächst für $b \geq 0$ und dann für $b < 0$.

Es sei zunächst $b \geq 0$. Wir beweisen die Behauptung durch Induktion nach b.

Induktionsanfang: Es sei $b < |a|$. Dann setzen wir $q := 0$ und $r := b$. Dann gilt

$$b = 0 \cdot a + b = q \cdot a + r.$$

Induktionsschritt: Es sei $b \geq |a|$ und die Behauptung sei richtig für alle Zahlen $\widetilde{b}$ mit $\widetilde{b} < b$. Setze

$$\widetilde{b} := b - |a|.$$

Dann gilt $\widetilde{b} < b$. Nach Induktionsannahme gibt es ganze Zahlen $\widetilde{q}$ und r mit

$$b - |a| = \widetilde{q} \cdot a + r \text{ und } 0 \leq r < |a|.$$

Dann folgt

$$b = q \cdot a + r \text{ und } 0 \leq r < |a|$$

mit $q := \widetilde{q} + 1$, falls $a > 0$, und $q := \widetilde{q} - 1$, falls $a < 0$.

Wenn $b < 0$ ist, dann ist $-b > 0$. Wir haben gerade gezeigt, dass es ganze Zahlen q' und r' gibt mit

$$-b = q' \cdot a + r' \text{ und } 0 \leq r' < |a|.$$

Dann folgt

$$b = q \cdot a + r \text{ und } 0 \leq r < |a|$$

mit

$$\begin{aligned} q := -q', r := r', &\quad \text{falls } r' = 0, \\ q := -q' - 1, r := |a| - r', &\quad \text{falls } r' \neq 0, a > 0, \\ q := -q' + 1, r := |a| - r', &\quad \text{falls } r' \neq 0, a < 0. \end{aligned}$$

□

Beispiel $37 = 3 \cdot 11 + 4$.

Der Rest r bei der Division mit Rest ist so wichtig, dass wir ihm einen eigenen Namen geben:

Definition Es seien a, b ganze Zahlen mit $a \neq 0$ und q und r die nach dem vorher gehenden Satz eindeutig bestimmten ganzen Zahlen mit

$$b = q \cdot a + r \text{ und } 0 \leq r < |a|.$$

Dann wird die Zahl r mit $b \bmod a$ (ausgesprochen b *modulo* a) bezeichnet:

$$b \bmod a := r.$$

Beispiel $37 \bmod 11 = 4$.

Definition Es seien a, b, b' ganze Zahlen mit $a \neq 0$. Wir sagen, b ist *kongruent* zu b', in Zeichen $b \equiv b' \mod a$, falls a die Differenz $b' - b$ teilt.

Übungsaufgabe $b \equiv b' \mod a \iff b \bmod a = b' \bmod a$.

Es seien a und b ganze Zahlen, die nicht beide gleich 0 sind. Es sei

$$M := \{t \in \mathbb{N} \mid t|a \text{ und } t|b\}.$$

Die Menge M ist nicht leer, da $1 \in M$. Außerdem ist die Menge M nach oben beschränkt: Für $t \in M$ gilt nach Lemma 1.2 $t \leq |a|$, falls $a \neq 0$, bzw. $t \leq |b|$, falls $b \neq 0$. Also ist die Menge M endlich und besitzt ein größtes Element. Dieses Element ist die größte natürliche Zahl t, die sowohl a als auch b teilt.

Definition Es seien a und b ganze Zahlen, die nicht beide gleich 0 sind. Die größte natürliche Zahl t, die sowohl a als auch b teilt, wird der *größte gemeinsame Teiler* von a und b genannt und mit $\mathrm{ggT}(a, b)$ (oder kurz mit (a, b)) bezeichnet.

Die Zahlen a und b heißen *teilerfremd*, falls ihr größter gemeinsamer Teiler 1 ist.

Beispiele (a) $(37, 11) = 1$.
(b) $(247, 266) = 19$.

Bemerkung (a) Für natürliche Zahlen a, b mit $a \neq 0$ und $a|b$ gilt $(a, b) = a$.
(b) Für eine natürliche Zahl $a \neq 0$ gilt $(a, 0) = a$.

Es seien a und b ganze Zahlen, die beide ungleich 0 sind. Es sei

$$N := \{v \in \mathbb{N} \mid a|v \text{ und } b|v\}.$$

Auch diese Menge ist nicht leer, da z.B. $|a| \cdot |b| \in N$, und nach unten beschränkt. Also besitzt die Menge N ein kleinstes Element. Dieses Element ist die kleinste natürliche Zahl, die sowohl Vielfaches von a als auch von b ist.

Definition Es seien a und b ganze Zahlen, die beide ungleich 0 sind. Die kleinste natürliche Zahl v, die sowohl Vielfaches von a als auch von b ist, wird das *kleinste gemeinsame Vielfache* von a und b genannt und mit $\mathrm{kgV}(a,b)$ (oder kurz mit $[a,b]$) bezeichnet. Ist a eine beliebige ganze Zahl, so setzen wir außerdem $[a,0] := 0$.

Reduktionsschritt zur Berechnung des ggT:

Satz 1.5 *Es seien a, b ganze Zahlen mit $a \neq 0$. Es seien q, r ganze Zahlen mit*

$$b = qa + r.$$

Dann gilt $(b,a) = (a,r)$.

Beweis. Es sei $M(a,b)$ die Menge der Teiler von a und b und $M(a,r)$ die Menge der Teiler von a und r. Wir zeigen: $M(a,b) = M(a,r)$. Daraus folgt die Behauptung, da dann auch die jeweils größten Elemente dieser Mengen übereinstimmen.

$M(a,b) \subset M(a,r)$: Es sei $t \in M(a,b)$. Dann teilt t sowohl a als auch b, aber auch qa und $b - qa = r$. Also ist $t \in M(a,r)$.

$M(a,b) \supset M(a,r)$: Es sei $d \in M(a,r)$. Dann teilt d die Zahl a und die Zahl r und damit auch qa und $b = qa + r$. Also ist $d \in M(a,b)$. □

Wir wollen nun den g.g.T. zweier ganzer Zahlen a und b mit $a > 0$ bestimmen. Dies geschieht mit dem *euklidischen Algorithmus*, den wir nun beschreiben. Wir setzen zunächst $a_1 := b$, $a_2 := a$. Nun dividieren wir a_1 durch a_2. Dann erhalten wir eine Darstellung $a_1 = q_1 a_2 + a_3$ mit $0 \leq a_3 < a_2$. Ist nun $a_3 > 0$, so können wir im nächsten Schritt a_2 durch a_3 mit einem Rest a_4 teilen, usw. Da $a_2 > a_3 > a_4 > \ldots$ gilt, kommt dieser Prozess nach endlich vielen Schritten zum Stillstand, nämlich dann, wenn der anfallende Rest Null wird. Wir erhalten also ein Schema wie folgt:

$$\begin{aligned}
a_1 &= q_1 a_2 + a_3, \quad a_2 > a_3,\\
a_2 &= q_2 a_3 + a_4, \quad a_3 > a_4,\\
&\vdots \quad \vdots \quad \vdots\\
a_{m-1} &= q_{m-1} a_m + a_{m+1}, \quad a_m > a_{m+1},\\
a_m &= q_m a_{m+1}
\end{aligned}$$

Hierbei gilt $a_i > 0$, $i = 1, \ldots, m+1$.

Satz 1.6 *Die Zahl a_{m+1} ist der g.g.T. von a_1 und a_2.*

Beweis. Nach Satz 1.5 folgt aus den einzelnen Zeilen

$$\begin{aligned}(a_1, a_2) &= (a_2, a_3),\\ (a_2, a_3) &= (a_3, a_4),\\ &\vdots \quad \vdots \quad \vdots\\ (a_{m-1}, a_m) &= (a_m, a_{m+1}),\\ (a_m, a_{m+1}) &= (a_{m+1}, 0) = a_{m+1}.\end{aligned}$$

□

Darüberhinaus kann man mit Hilfe dieses Algorithmus Elemente $r, s \in \mathbb{Z}$ finden, so dass

$$a_{m+1} = (a, b) = ra + sb$$

gilt. Dazu beginnt man mit der vorletzten Gleichung

$$a_{m+1} = a_{m-1} - q_{m-1}a_m$$

und setzt rückwirkend die vorherigen Gleichungen ein, wobei jedesmal a_i durch einen Ausdruck mit a_{i-1} und a_{i-2} ersetzt wird.

Damit haben wir bewiesen:

Satz 1.7 (Lemma von Bézout) *Es seien a und b ganze Zahlen, die nicht beide gleich 0 sind, und es sei $d = (a, b)$. Dann gibt es ganze Zahlen r und s mit*

$$d = ra + sb.$$

Insbesondere gilt: Wenn a und b teilerfremd sind, dann gibt es ganze Zahlen r und s mit $ra + sb = 1$.

Beispiel Es sei $a = 36$ und $b = 85$. Der euklidische Algorithmus sieht dann wie folgt aus:

$$\begin{aligned}85 &= 2 \cdot 36 + 13\\ 36 &= 2 \cdot 13 + 10\\ 13 &= 1 \cdot 10 + 3\\ 10 &= 3 \cdot 3 + 1\\ 3 &= 3 \cdot 1.\end{aligned}$$

Daraus folgt $(36, 85) = 1$. Nun wollen wir die Zahlen r, s aus Satz 1.7 berechnen. Es gilt zunächst

$$1 = 10 - 3 \cdot 3.$$

Die Zahlen 10 und 3 können wir nun durch die vorherigen Gleichungen ausdrücken:

$$1 = (36 - 2 \cdot 13) - 3 \cdot (13 - 1 \cdot 10) = 36 - 5 \cdot 13 + 3 \cdot 10.$$

Man beachte dabei, dass wir die rechte Seite nicht vollständig ausmultiplizieren, sondern nur die Klammern auflösen und nach den Resten 36, 13 und 10 ordnen. Nun drücken wir 10 und 13 wieder durch die vorherigen Reste aus:

$$1 = 36 - 5 \cdot (85 - 2 \cdot 36) + 3 \cdot (36 - 2 \cdot 13) = 14 \cdot 36 - 5 \cdot 85 - 6 \cdot 13.$$

Setzen wir noch $13 = 85 - 2 \cdot 36$ ein, so erhalten wir schließlich:

$$1 = 14 \cdot 36 - 5 \cdot 85 - 6 \cdot (85 - 2 \cdot 36) = 26 \cdot 36 + (-11) \cdot 85.$$

Korollar 1.8 *Es seien $a, b \in \mathbb{Z}$, nicht beide gleich 0, $c, t \in \mathbb{N}$, $c \neq 0$, t ein gemeinsamer Teiler von a und b, v ein gemeinsames Vielfaches von a und b. Dann gilt*

$$(ca, cb) = c(a, b), \quad t|(a, b), \quad (\frac{a}{t}, \frac{b}{t}) = \frac{(a, b)}{t}, \quad [a, b]|v \text{ und } [a, b] = \frac{|ab|}{(a, b)}.$$

Korollar 1.9 *Es seien t, a, b ganze Zahlen und $(t, a) = 1$. Dann gilt*

$$t|ab \Rightarrow t|b.$$

Beweis. Nach dem Lemma von Bézout gibt es ganze Zahlen r, s mit

$$rt + sa = 1.$$

Multiplikation dieser Gleichung mit b liefert

$$rtb + sab = b.$$

Nach Voraussetzung ist die linke Seite durch t teilbar, also auch b. □

Satz 1.10 *Es seien a und n teilerfremde positive ganze Zahlen mit $n \geq 2$. Dann gibt es genau eine ganze Zahl a' mit $1 \leq a' \leq n-1$ und $a \cdot a' \equiv 1 \bmod n$.*

Definition Die Zahl a' heißt das *modulare Inverse* von a modulo n.

Beweis. (a) *Existenz*: Da $(a, n) = 1$ ist, existieren nach Satz 1.7 ganze Zahlen r und s mit $1 = r \cdot a + s \cdot n$. Daraus ergibt sich

$$r \cdot a \equiv 1 \bmod n.$$

Ist k eine beliebige ganze Zahl, so gilt auch

$$(r + kn) \cdot a \equiv 1 \bmod n.$$

Daraus folgt, dass auch $a' := r \bmod n$ die Gleichung $a \cdot a' \equiv 1 \bmod n$ erfüllt.

(b) *Eindeutigkeit*: Es sei $a \cdot a' \equiv 1 \bmod n$ und $a \cdot a'' \equiv 1 \bmod n$. Dann folgt $a \cdot a' \equiv a \cdot a'' \bmod n$, also $n|a(a' - a'')$. Da n und a teilerfremd sind, folgt aus Korollar 1.9 $n|(a' - a'')$, also $a' \equiv a'' \bmod n$. Also ist a' mit der Bedingung $1 \leq a' \leq n - 1$ eindeutig bestimmt. □

Beispiel Es sei $n = 5$. Die zu 5 teilerfremden Zahlen, die kleiner gleich 5 sind, lauten: 1,2,3,4. Es gilt

$$\begin{aligned} 1 \cdot 1 &= 1, \\ 3 \cdot 2 &= 5 + 1, \\ 2 \cdot 3 &= 5 + 1, \\ 4 \cdot 4 &= 3 \cdot 5 + 1 \end{aligned}$$

Also erhalten wir die folgende Tabelle von modularen Inversen:

a	1	2	3	4
a'	1	3	2	4

1.2 Zahlendarstellung

Die Zahlen, mit denen wir täglich umgehen, sind im Dezimalsystem dargestellt. Die Zahl 2017 ist eine abkürzende Schreibweise für

$$2 \cdot 1000 + 0 \cdot 100 + 1 \cdot 10 + 7 \cdot 1 = 2 \cdot 10^3 + 0 \cdot 10^2 + 1 \cdot 10^1 + 7 \cdot 10^0.$$

Im Computer ist die binäre oder hexadezimale Zahlendarstellung gebräuchlich.

Es sei $b \geq 2$ eine natürliche Zahl. Wir wollen nun allgemein definieren, was wir unter der b-adischen Darstellung einer Zahl verstehen.

Satz 1.11 *Es sei $b \geq 2$ eine natürliche Zahl. Dann gibt es zu jeder natürlichen Zahl $n \neq 0$ eine natürliche Zahl k und Zahlen a_i, $0 \leq a_i \leq b - 1$, $i = 0, \ldots, k - 1$, $a_{k-1} \neq 0$, mit*

$$n = a_{k-1}b^{k-1} + a_{k-2}b^{k-2} + \cdots + a_1 b^1 + a_0 b^0.$$

Die Zahlen k und $a_{k-1}, a_{k-2}, \ldots, a_1, a_0$ sind eindeutig bestimmt.

Definition Man spricht von dem *Zahlensystem* zur *Basis* b. Die Zahlen $0, \ldots, b-1$ heißen die *Ziffern* des Zahlensystems. Die Darstellung der Zahl n in Satz 1.11 heißt auch die *b-adische Darstellung* der Zahl n oder die *Darstellung* der Zahl n *zur Basis* b. Die Zahl k heißt die *Stellenzahl* von n und die Zahlen $a_{k-1}, a_{k-2}, \ldots, a_1, a_0$ die *Ziffern* der Zahl n zur Basis b.

Beweis. (a) *Existenz*: Es sei k die kleinste natürliche Zahl, so dass $b^k > n$, d.h. $b^k > n$, aber $b^{k-1} \leq n$. Wir beweisen die Aussage durch Induktion nach k.

Induktionsanfang $k = 1$: Dann gilt $0 < n < b$. Wir setzen $a_0 := n$. Dann gilt

$$n = n \cdot 1 = a_0 b^0.$$

Induktionsschritt $k-1 \to k$: Es sei $k > 1$ und die Aussage sei richtig für Zahlen l mit $b^{k-1} > l$.

Zunächst teilen wir n durch b^{k-1} mit Rest:

$$n = a_{k-1} b^{k-1} + n' \text{ mit } 0 \leq n' < b^{k-1}.$$

Dann ist $a_{k-1} > 0$, denn sonst wäre $n = n' < b^{k-1}$, im Widerspruch zur Wahl von k. Außerdem ist $a_{k-1} < b$, denn sonst wäre $n \geq b \cdot b^{k-1} = b^k$, was erneut im Widerspruch zur Wahl von k steht.

Ist $n' = 0$, so sind wir fertig. Ansonsten können wir auf n' die Induktionsannahme anwenden. Danach gibt es Zahlen a_i, $0 \leq a_i \leq b-1$, $i = 0, \ldots, k-2$, mit

$$n' = a_{k-2} b^{k-2} + \cdots + a_1 b^1 + a_0 b^0.$$

Zusammen folgt

$$n = a_{k-1} b^{k-1} + a_{k-2} b^{k-2} + \cdots + a_1 b^1 + a_0 b^0.$$

(b) *Eindeutigkeit*: Angenommen,

$$\begin{aligned} n &= a_{k-1} b^{k-1} + a_{k-2} b^{k-2} + \cdots + a_1 b^1 + a_0 b^0 \\ &= c_{\ell-1} b^{\ell-1} + c_{\ell-2} b^{\ell-2} + \cdots + c_1 b^1 + c_0 b^0, \end{aligned}$$

wobei $a_{k-1} \neq 0$ und $c_{\ell-1} \neq 0$. Wir behaupten, dass

$$b^k > n \geq b^{k-1} \text{ und } b^\ell > n \geq b^{\ell-1}.$$

Daraus folgt $k = \ell$. Die Ungleichung $b^k > n$ folgt dabei aus der Abschätzung

$$a_{k-1} b^{k-1} + a_{k-2} b^{k-2} + \cdots + a_1 b^1 + a_0 b^0 \leq$$

$$(b-1) b^{k-1} + (b-1) b^{k-2} + \ldots + (b-1) b + b - 1 =$$

$$b^k - b^{k-1} + b^{k-1} - + \ldots - b + b - 1 = b^k - 1 < b^k.$$

Analog schließt man im zweiten Fall. Nun subtrahieren wir die beiden Darstellungen von n voneinander:

$$0 = (a_{k-1} - c_{k-1})b^{k-1} + (a_{k-2} - c_{k-2})b^{k-2} + \cdots + (a_1 - c_1)b^1 + (a_0 - c_0)b^0.$$

Mit einer analogen Abschätzung wie oben zeigt man

$$(a_{k-2} - c_{k-2})b^{k-2} + \cdots + (a_1 - c_1)b^1 + (a_0 - c_0)b^0 < b^{k-1}.$$

Daher muss $a_{k-1} - c_{k-1} = 0$, also $a_{k-1} = c_{k-1}$ gelten. Weiter schließt man entsprechend $a_{k-2} = c_{k-2}$, usw., bis man schließlich zu $a_0 = c_0$ gelangt. □

Wichtige Zahlensysteme sind

- $b = 10$: *Dezimalsystem*, *Dezimalzahl*
- $b = 2$: *Binärsystem*, *Binärzahl*
- $b = 16$: *Hexadezimalsystem*, *Hexadezimalzahl*

Beispiel Man hat die folgende Tabelle für die Zahlendarstellung im Dezimal-, Binär- und Hexadezimalsystem:

$b = 10$	1	2	3	4	5	6	7	8
$b = 16$	1	2	3	4	5	6	7	8
$b = 2$	1	10	11	100	101	110	111	1000

$b = 10$	9	10	11	12	13	14	15
$b = 16$	9	A	B	C	D	E	F
$b = 2$	1001	1010	1011	1100	1101	1110	1111

Der Beweis von Satz 1.11 liefert einen Algorithmus, wie man die b-adische Darstellung einer Zahl erhalten kann. In der Praxis ist aber ein anderer Algorithmus geeigneter:

$$\begin{aligned}
a_0 &:= n \bmod b, \quad n_1 := (n - a_0)/b, \\
a_1 &:= n_1 \bmod b, \quad n_2 := (n_1 - a_1)/b, \\
&\vdots \quad \vdots \quad \vdots \\
a_{k-2} &:= n_{k-2} \bmod b, \quad n_{k-1} := (n_{k-2} - a_{k-2})/b, \\
a_{k-1} &:= n_{k-1}.
\end{aligned}$$

Der Algorithmus bricht ab, wenn $n_{k-1} < b$ ist.

Die Umwandlung einer Hexadezimalzahl in eine Binärzahl oder umgekehrt geht sehr einfach (nämlich wie?).

Beispiel Wir wollen die binäre Darstellung der Zahl 29 bestimmen:

$$\begin{aligned} a_0 &:= 29 \bmod 2 = 1, \quad n_1 := (29-1)/2 = 14, \\ a_1 &:= 14 \bmod 2 = 0, \quad n_2 := (14-0)/2 = 7, \\ a_2 &:= 7 \bmod 2 = 1, \quad n_3 := (7-1)/2 = 3, \\ a_3 &:= 3 \bmod 2 = 1, \quad n_4 := (3-1)/2 = 1, \\ a_4 &:= 1 \end{aligned}$$

Also gilt

$$29 = 11101.$$

Daraus ergibt sich die hexadezimale Darstellung der Zahl 29:

$$29 = 1\mathrm{D}.$$

An einer Darstellung einer Zahl in einem Zahlensystem kann man einige einfache Teilbarkeitsbeziehungen ablesen. Das wollen wir nun betrachten.

Satz 1.12 (Endstellenregel) *Es sei n eine natürliche Zahl, die im System zur Basis b dargestellt ist:*

$$n = a_{k-1}b^{k-1} + a_{k-2}b^{k-2} + \cdots + a_1 b^1 + a_0 b^0.$$

Dann gilt für jeden Teiler t von b:

$$t|n \Leftrightarrow t|a_0.$$

Beispiel (a) $b = 10$: Eine Dezimalzahl ist genau dann durch 2 bzw. 5 teilbar, wenn ihre Endziffer durch 2 bzw. 5 teilbar ist. Eine Dezimalzahl ist genau dann durch 10 teilbar, wenn ihre Endziffer gleich 0 ist.

(b) $b = 2$. Eine Binärzahl ist genau dann gerade, wenn ihre Endziffer gleich 0 ist.

Beweis von Satz 1.12. Es gilt:

$$n - a_0 = a_{k-1}b^{k-1} + a_{k-2}b^{k-2} + \cdots + a_1 b^1.$$

Da t ein Teiler von b ist, teilt t auch $n - a_0$. Mit Lemma 1.1 folgt daraus die Behauptung. □

Definition Es sei n eine natürliche Zahl, die im System zur Basis b dargestellt ist:

$$n = a_{k-1}b^{k-1} + a_{k-2}b^{k-2} + \cdots + a_1 b^1 + a_0 b^0.$$

Die *Quersumme von n zur Basis b*, in Zeichen $Q(n)$, ist die Summe der Ziffern von n:

$$Q(n) = a_{k-1} + a_{k-2} + \cdots + a_1 + a_0.$$

Satz 1.13 (Quersummenregel) *Es sei n eine natürliche Zahl, die im System zur Basis b dargestellt ist. Dann gilt für jeden Teiler t von $b-1$:*

$$t|n \Leftrightarrow t|Q(n).$$

Beispiel (i) Eine Dezimalzahl ist genau dann durch 3 bzw. 9 teilbar, wenn ihre Quersumme durch 3 bzw. 9 teilbar ist.

(ii) Eine Zahl ist genau dann durch 11 teilbar, wenn ihre Quersumme zur Basis $b = 100$ durch 11 teilbar ist.

Beweis von Satz 1.13. Es gilt

$$\begin{aligned} b^2-1 &= (b-1)(b+1), \\ b^3-1 &= (b-1)(b^2+b+1), \\ &\vdots \quad \vdots \quad \vdots \\ b^{k-1}-1 &= (b-1)(b^{k-2}+\cdots+b+1). \end{aligned}$$

Da t die Zahl $b-1$ teilt, teilt t deswegen auch die Zahl

$$a_{k-1}(b^{k-1}-1)+a_{k-2}(b^{k-2}-1)+\cdots+a_1(b^1-1) = n-Q(n).$$

Daraus folgt mit Lemma 1.1 wieder die Behauptung. □

Definition Es sei n eine natürliche Zahl, die im System zur Basis b dargestellt ist:

$$n = a_{k-1}b^{k-1}+a_{k-2}b^{k-2}+\cdots+a_1b^1+a_0b^0.$$

Die *alternierende Quersumme von n zur Basis b*, in Zeichen $A(n)$, ist die alternierende Summe der Ziffern von n:

$$A(n) = (-1)^{k-1}a_{k-1}+(-1)^{k-2}a_{k-2}\pm\cdots-a_1+a_0.$$

Satz 1.14 (Alternierende Quersummenregel) *Es sei n eine natürliche Zahl, die im System zur Basis b dargestellt ist. Dann gilt für jeden Teiler t von $b+1$:*

$$t|n \Leftrightarrow t|A(n).$$

Beispiel Eine Dezimalzahl ist genau dann durch 11 teilbar, wenn ihre alternierende Quersumme durch 11 teilbar ist.

Beweis von Satz 1.14. Es gilt

$$\begin{aligned} b^3+1 &= (b+1)(b^2-b+1), \\ b^5+1 &= (b+1)(b^4-b^3+b^2-b+1). \\ \cdots &\quad \cdots \quad \cdots \end{aligned}$$

Ferner gilt

$$\begin{aligned} b^2-1 &= (b+1)(b-1), \\ b^4-1 &= (b^2-1)(b^2+1), \\ b^6-1 &= (b^2-1)(b^4+b^2+1), \\ &\dots \quad \dots \quad \dots \end{aligned}$$

Eine natürliche Zahl t, die $b+1$ teilt, teilt deshalb auch die Zahl

$$a_{k-1}(b^{k-1}-(-1)^{k-1})+a_{k-2}(b^{k-2}-(-1)^{k-2})+\cdots+a_1(b^1+1)=n-A(n).$$

Daraus folgt mit Lemma 1.1 wieder die Behauptung. □

1.3 Primzahlen

Eine wichtige Rolle spielen in der Mathematik die Primzahlen.

Definition Eine natürliche Zahl p heißt *Primzahl*, falls $p>1$ und 1 und p die einzigen natürlichen Zahlen sind, die p teilen. Wir bezeichnen mit $\mathbb{P}$ die Menge aller Primzahlen.

Warnung 1 ist keine Primzahl!

Beispiel Die einzige gerade Primzahl ist 2.

Es gibt einige Primzahlen besonderer Art.

Definition Die Primzahlen der Form $p=2^a-1$ heißen *Mersennesche Primzahlen.*

Bemerkung Man beachte, dass die binäre Darstellung der Zahl 2^a-1 aus a Ziffern 1 besteht.

Lemma 1.15 *Die Mersenneschen Primzahlen sind von der Form $p=2^a-1$, wobei a eine Primzahl ist.*

Beweis. Angenommen, $a=bc$ mit $b,c\in\mathbb{N}$, $b,c>1$. Dann ist

$$p=2^{bc}-1=(2^c-1)(2^{c(b-1)}+2^{c(b-2)}+\cdots+2^c+1),$$

also wäre p keine Primzahl. □

Beispiel Die ersten Mersenneschen Primzahlen sind

$$3(a=2), \quad 7(a=3), \quad 31(a=5), \quad 127(a=7), \quad 8191(a=13), \quad \ldots$$

Im Dezember 2018 (siehe www.wikipedia.org) waren 51 Mersennesche Primzahlen bekannt. Die größte ist $2^{82589933}-1$, sie hat 25 Mio. Stellen.

Definition Die Primzahlen der Form $p = 2^a + 1$ heißen *Fermatsche Primzahlen.*

Lemma 1.16 *Eine Fermatsche Primzahl ist tatsächlich von der Form* $p = 2^{2^e} + 1$.

Beweis. Angenommen, $a = bc$ mit einer ungeraden Zahl $b \in \mathbb{N}$, $b > 2$. Dann ist

$$p = 2^{bc} + 1 = (2^c + 1)(2^{c(b-1)} - 2^{c(b-2)} + \cdots - 2^c + 1),$$

also wäre p keine Primzahl. □

Beispiel Die einzigen Fermatschen Primzahlen, die man bis heute kennt (siehe auch www.wikipedia.org), sind

$$3(e=0), \quad 5(e=1), \quad 17(e=2), \quad 257(e=3), \quad 65537(e=4).$$

Schon Euler hat gezeigt, dass die nächste Zahl von dieser Form, wenn man also $e = 5$ wählt, keine Primzahl ist:

$$2^{2^5} + 1 = 2^{32} + 1 = 4.294.967.297 = 641 \cdot 6.700.417.$$

Wie findet man Primzahlen? Eine klassische Methode ist das *Sieb des Eratosthenes* (Eratosthenes von Kyrene, 284-200 v. Chr.).

Aufgabe: Man finde alle Primzahlen $\leq n$.

Dazu geht man wie folgt vor

1. Schreibe die Zahlen $2, 3, \ldots, n$ in eine Liste.
2. Setze $k := 2$.
3. Die Zahl k ist eine Primzahl. Streiche alle echten Vielfachen von k.
4. Setze $k_0 := k$. Gibt es keine Zahl $> k_0$ in der Liste, so sind wir fertig. Ansonsten setze k gleich der kleinsten Zahl $> k_0$ in der Liste und gehe zu 3.

Beispiel Bestimme alle Primzahlen ≤ 20:

$$2, 3, 5, 7, 11, 13, 17, 19.$$

Satz 1.17 (Euklid) *Es gibt unendlich viele Primzahlen.*

Für den Beweis dieses Satzes, der auf Euklid (ca. 300 v. Chr.) zurückgeht, brauchen wir einen Hilfssatz.

Lemma 1.18 *Es sei n eine natürliche Zahl > 1. Dann gibt es mindestens eine Primzahl, die n teilt.*

Beweis. (durch Induktion nach n)

Induktionsanfang $n = 2$: 2 ist eine Primzahl.

Induktionsannahme: Die Behauptung sei richtig für alle Zahlen n' mit $1 < n' < n$.

Induktionsschritt: Wir zeigen die Behauptung für $n > 2$. Wenn n eine Primzahl ist, sind wir fertig. Ansonsten hat n einen Teiler n' mit $1 < n' < n$. Nach Induktionsannahme gibt es eine Primzahl p, die n' teilt. Wegen $p|n'$ und $n'|n$ folgt auch $p|n$. □

Beweis von Satz 1.17. Wir führen einen Widerspruchsbeweis.

Angenommen, es gibt nur endlich viele Primzahlen $p_1, p_2, \ldots, p_s$. Dann betrachten wir die Zahl

$$n = p_1 \cdot p_2 \cdots p_s + 1.$$

Nach Lemma 1.18 gibt es eine Primzahl p, die n teilt. Da $p_1, p_2, \ldots, p_s$ nach unserer Annahme alle Primzahlen sind, muss $p = p_i$ für ein $i \in \{1, \ldots, s\}$ gelten. Die Zahl p_i teilt aber nach Konstruktion von n die Zahl $n - 1$. Also gilt

$$p_i|n \text{ und } p_i|(n-1) \Rightarrow p_i|n - (n-1) \Rightarrow p_i|1.$$

Das ist aber ein Widerspruch, da p_i eine Primzahl ist. □

Definition Für eine positive reelle Zahl x bezeichne $\pi(x)$ die Anzahl der Primzahlen, die kleiner oder gleich x sind, d.h.

$$\pi(x) := |\{p \,|\, p \text{ Primzahl}, p \leq x\}|.$$

Beispiel Es gilt $\pi(20) = 8$.

Ohne Beweis geben wir den folgenden Satz an, der von Gauß vermutet und unabhängig von J. Hadamard (1865-1963) und Ch. de la Vallée Poussin (1866-1962) bewiesen wurde.

Satz 1.19 (Primzahlsatz) *Die Funktion $\pi(x)$ wächst asymptotisch wie*

$$\pi(x) \approx \frac{x}{\ln x}.$$

Genauer gilt

$$\lim_{x\to\infty} \pi(x) \cdot \frac{\ln x}{x} = 1.$$

Das bedeutet: Die Anzahl der Primzahlen kleiner oder gleich x ist ungefähr $x/\ln x$.

Beispiel Es gilt $e^{10} \approx 22026$, $\ln(e^{10}) = 10$. Also gibt es ungefähr 2202 Primzahlen, die kleiner oder gleich 22026 sind. Das bedeutet, dass etwa jede zehnte Zahl zwischen 0 und 22026 eine Primzahl ist.

Nachgerechnet: $\pi(22026) = 2466$

Anwendung Der Primzahlsatz führt auf die Heuristik, dass es nur endlich viele Fermatsche Primzahlen geben dürfte, aber durchaus unendlich viele Mersennesche (kein Beweis!!).

Bemerkung Über die Verteilung der Primzahlen gibt es immer noch viele offene Fragen. Beispielsweise ist unbekannt, ob es unendlich viele *Primzahlzwillinge* wie $(3, 5)$, $(5, 7)$, $(11, 13)$ oder $(22037, 22039)$ gibt.

Eine Funktion, welche eng mit der Verteilung der Primzahlen zu tun hat, ist die *Riemannsche Zetafunktion*. Für reelle Zahlen $s > 1$ kann diese definiert werden durch

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p\in\mathbb{P}} \frac{1}{1-p^{-s}}.$$

Ein spezieller Wert der ζ-Funktion ist beispielsweise

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \cdots = \frac{\pi^2}{6}.$$

Man kann die ζ-Funktion zu einer (analytischen) Funktion

$$\zeta : \mathbb{C} \setminus \{1\} \to \mathbb{C}$$

erweitern. Diese Funktion hat so genannte *triviale* Nullstellen

$$\zeta(-2) = \zeta(-4) = \ldots = \zeta(-2n) = \ldots = 0.$$

Es ist bekannt, dass die Riemannsche Zetafunktion weitere Nullstellen in dem Bereich $\{0 < \mathrm{Re}(s) < 1\}$ hat. Die *Riemannsche Vermutung*, eines der großen ungelösten Probleme der Mathematik, besagt, dass alle nicht-trivialen Nullestellen auf der Gerade $\mathrm{Re}(s) = \frac{1}{2}$ liegen.

Wir wollen nun zeigen, dass sich jede natürliche Zahl $n > 1$ in Primfaktoren zerlegen lässt. Dazu dienen die folgenden Vorbereitungen.

Lemma 1.20 *Seien $a \in \mathbb{Z}, p \in \mathbb{P}$. Falls $p \nmid a$, so folgt $(a, p) = 1$.*

Beweis. Da p prim ist, also nur die Teiler $1, p$ in $\mathbb{N}$ hat, gilt

$$M(a, p) \subset \{1, p\}.$$

Da $p \nmid a$, folgt schon $M(a, p) \subset \{1\}$ und der besagte ggT. □

Anwendung Sind $p, p' \in \mathbb{P}$ mit $p \neq p'$, so gilt $(p, p') = 1$.

Lemma 1.21 *Es sei p eine Primzahl und a und b ganze Zahlen. Dann gilt*

$$p|ab \Rightarrow p|a \text{ oder } p|b.$$

Beweis. Dies folgt unmittelbar aus Korollar 1.9 und Lemma 1.20 mit $t = p$. □

Satz 1.22 (Zerlegung in Primfaktoren) *Es sei n eine natürliche Zahl mit $n > 1$. Dann kann n in Primfaktoren zerlegt werden, d.h. es gibt verschiedene Primzahlen $p_1, \ldots, p_s$ und positive ganze Zahlen $e_1, \ldots, e_s$, so dass gilt:*

$$n = p_1^{e_1} \cdots p_s^{e_s}.$$

Diese Zerlegung ist bis auf Reihenfolge der Faktoren eindeutig bestimmt.

Beweis.

(a) *Existenz*: Wir führen Induktion über n durch.

Induktionsanfang $n = 2$: $s = 1$, $p_1 = 2$, $e_1 = 1$.

Induktionssannahme: Die Aussage sei richtig für alle natürlichen Zahlen n' mit $1 < n' < n$.

Induktionsschritt: Wir beweisen die Aussage für $n > 2$. Nach Lemma 1.18 gibt es eine Primzahl p, die n teilt. Wenn $n = p$ ist, sind wir fertig. Andernfalls setzen wir $n' := n/p$. Dann gilt $1 < n' < n$. Nach Induktionssannahme ist n' ein Produkt von Primzahlpotenzen. Also ist auch $n = pn'$ ein Produkt von Primzahlpotenzen.

(b) *Eindeutigkeit*: Auch diese Behauptung beweisen wir durch Induktion über n.

Induktionsanfang: Die Zahl $n = 2$ kann nur auf eine Weise als Produkt von Primzahlen geschrieben werden.

Induktionsschritt: Angenommen, die Zahl $n > 2$ kann auf zwei Arten als Produkt von Primzahlpotenzen geschrieben werden. Indem wir nötigenfalls Exponenten gleich Null setzen, können wir annehmen:

$$n = p_1^{e_1} \cdots p_s^{e_s} = p_1^{e'_1} \cdots p_s^{e'_s}, \qquad e_i, e'_j \geq 0.$$

Es sei $i \in \{1, \ldots, s\}$ mit $e_i > 0$. Dann teilt p_i die Zahl n. Nach Lemma 1.21 gilt dann auch $e'_i > 0$. Nun betrachten wir die Zahl $n' = n/p_i$. Dann gilt

$$n' = p_1^{e_1} \cdots p_i^{e_i - 1} \cdots p_s^{e_s} = p_1^{e'_1} \cdots p_i^{e'_i - 1} \cdots p_s^{e'_s}.$$

Nach Induktionsannahme ist die Zerlegung der Zahl $n' < n$ in Primfaktoren eindeutig. Also folgt

$$e_j = e'_j$$

für jedes $j \in \{1, \ldots, s\}$. □

1.4 Kongruenzen

Wir kommen nun auf die in 1.1 eingeführte Kongruenz modulo n zurück. Wir werden zeigen, dass die Kongruenz modulo n eine Äquivalenzrelation liefert.

Wir erinnern an die Definition einer Äquivalenzrelation.

Eine *Relation* R auf einer Menge M ist eine Teilmenge von $M \times M$. Für $(a, b) \in R$ schreiben wir $a \sim b$.

Definition Eine Relation $\sim$ auf einer Menge M heißt *Äquivalenzrelation*, wenn die folgenden Bedingungen erfüllt sind:

(R) $a \sim a$ für alle $a \in M$ (*Reflexivität*).

(S) Für alle $a, b \in M$ gilt: Aus $a \sim b$ folgt $b \sim a$ (*Symmetrie*).

(T) Für alle $a, b, c \in M$ gilt: Aus $a \sim b$ und $b \sim c$ folgt $a \sim c$ (*Transitivität*).

Beispiel Es sei n eine feste positive ganze Zahl und a, b seien zwei ganze Zahlen. In 1.1 haben wir definiert:

$$a \equiv b \bmod n :\Leftrightarrow n|(a - b).$$

Dies definiert eine Äquivalenzrelation auf $\mathbb{Z}$.

Beweis. (i) Für alle $a \in \mathbb{Z}$ gilt $n|(a - a)$. Also gilt $a \equiv a \bmod n$.

(ii) Aus $a \equiv b \bmod n$ folgt $n|(a - b)$, also auch $n| - (a - b)$. Daher gilt $n|(b - a)$ und $b \equiv a \bmod n$.

(iii) Es gelte $a \equiv b \bmod n$ und $b \equiv c \bmod n$. Dann folgt $n|(a - b)$ und $n|(b - c)$, also $n|((a - b) + (b - c))$. Also gilt $n|(a - c)$ und $a \equiv c \bmod n$. □

Definition Ist $\sim$ eine Äquivalenzrelation auf M und $a \in M$, dann heißt

$$[a] := \{x \in M \mid x \sim a\}$$

die *Äquivalenzklasse* von a. Das Element a nennt man auch einen *Repräsentanten* der Äquivalenzklasse $[a]$.

Für die Äquivalenzrelation $\equiv \bmod n$ gilt für eine ganze Zahl a:

$$[a] = \{b \in \mathbb{Z} \mid b \equiv a \bmod n\} = \{b \in \mathbb{Z} \mid b \bmod n = a \bmod n\}.$$

Man bezeichnet diese Menge auch als die *Restklasse von a modulo n*. Die Zahl n heißt auch der *Modul*.

Explizit ausgeschrieben sieht die Restklasse modulo n einer ganzen Zahl a wie folgt aus:

$$[a] = \{\ldots, a-3n, a-2n, a-n, a, a+n, a+2n, a+3n, \ldots\}.$$

Satz 1.23 *Ist $\sim$ eine Äquivalenzrelation auf M, dann gilt:*

(i) *Aus $a \sim b$ folgt $[a] = [b]$.*

(ii) *Aus $[a] \cap [b] \neq \emptyset$ folgt $a \sim b$.*

(iii) *Die Äquivalenzklassen bilden eine* Partition *von M, d.h. M kann als die disjunkte Vereinigung der verschiedenen Äquivalenzklassen geschrieben werden.*

Beweis. (i) Es sei $a \sim b$ und $x \in [a]$. Dann gilt $x \sim a$ und aus der Transitivität folgt $x \sim b$. Also gilt $x \in [b]$. Daraus folgt $[a] \subset [b]$.

Aus der Symmetrie folgt $b \sim a$ und wir können in dem obigen Argument die Rollen von a und b vertauschen. Also folgt $[b] \subset [a]$ und damit $[a] = [b]$.

(ii) Es sei $x \in [a] \cap [b]$. Dann gilt $x \sim a$ und $x \sim b$. Aus der Symmetrie und Transitivität folgt dann $a \sim b$.

(iii) Aus (i) und (ii) folgt, dass zwei Äquivalenzklassen entweder gleich oder disjunkt sind. Aus der Reflexivität folgt, dass jedes Element $a \in M$ in der Äquivalenzklasse $[a]$ liegt. Also ist M die disjunkte Vereinigung aller Äquivalenzklassen. □

Beispiel Die Restklassen modulo 3 sind

$$\begin{aligned} [0] &= \{\ldots, -3, 0, 3, 6, 9, \ldots\}, \\ [1] &= \{\ldots, -2, 1, 4, 7, 10, \ldots\}, \\ [2] &= \{\ldots, -1, 2, 5, 8, 11, \ldots\}. \end{aligned}$$

Damit sind alle ganzen Zahlen erfasst.

Korollar 1.24 *Es gibt genau n verschiedene Restklassen modulo n. Dies sind die Restklassen* $[0], [1], \ldots, [n-1]$.

Beweis. Es sei $[a]$ eine beliebige Restklasse modulo n. Es sei $r := a \bmod n$. Dann ist $r \in \{0, 1, \ldots, n-1\}$. Nach Satz 1.23 gilt $[r] = [a]$, die Restklassen sind $[0], [1], \ldots, [n-1]$, und sie sind alle verschieden. □

Definition Die Menge aller Restklassen modulo n bezeichnen wir mit $\mathbb{Z}_n$, d.h.

$$\mathbb{Z}_n := \{[0], [1], \ldots, [n-1]\}.$$

Die Zahlen $0, 1, \ldots, n-1$ nennt man ein *vollständiges Restsystem* mod n. Sind allgemeiner $a_1, \ldots, a_n \in \mathbb{Z}$ mit $\mathbb{Z}_n = \{[a_1], \ldots, [a_n]\}$, so nennt man $a_1, \ldots, a_n$ ein *vollständiges Restsystem* mod n.

Bemerkung In der Literatur bezeichnet $\mathbb{Z}_p$ für eine Primzahl p auch oft die Menge der *p-adischen Zahlen*, während die Menge der Restklassen mit $\mathbb{Z}/p\mathbb{Z}$ bezeichnet wird.

Wir wollen nun mit den Elementen von $\mathbb{Z}_n$ rechnen. Genauer gesagt wollen wir eine Addition und eine Multiplikation auf $\mathbb{Z}_n$ definieren. Wie sollen wir die Summe und das Produkt von zwei Restklassen erklären? Eine naheliegende Definition ist die folgende:

Definition Für zwei Restklassen $[a], [b] \in \mathbb{Z}_n$ definieren wir:

$$\begin{aligned} [a] + [b] &:= [a + b], \\ [a] \cdot [b] &:= [a \cdot b]. \end{aligned}$$

Das Problem bei dieser Definition ist, dass die Summe und das Produkt durch Repräsentanten der Restklassen erklärt werden. Was passiert, wenn wir andere Repräsentanten $a' \in [a]$ und $b' \in [b]$ auswählen? Ist dann die Restklasse von $a' + b'$ dieselbe wie die von $a + b$? Wenn das der Fall ist, dann sagen wir, das die Addition der Restklassen *wohldefiniert* ist. Der folgende Hilfssatz zeigt, dass die oben definierte Addition von Restklassen tatsächlich wohldefiniert ist.

Lemma 1.25 *Es seien $[a], [b] \in \mathbb{Z}_n$ zwei Restklassen modulo n, $a' \in [a]$ und $b' \in [b]$ beliebig. Dann gilt $[a' + b'] = [a + b]$.*

Beweis. Aus $a' \in [a]$ und $b' \in [b]$ folgt , dass es ganze Zahlen s und t mit

$$a' = a + sn \text{ und } b' = b + tn$$

gibt. Also gilt

$$a' + b' = a + sn + b + tn = a + b + (s + t)n \equiv a + b \,(\mathrm{mod}\ n).$$

□

Beispiel Als Beispiel stellen wir die Additionstafel von $\mathbb{Z}_4$ auf:

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

Das Produkt von Restklassen ist ebenfalls wohldefiniert:

Lemma 1.26 *Es seien $[a], [b] \in \mathbb{Z}_n$ zwei Restklassen modulo n, $a' \in [a]$ und $b' \in [b]$ beliebig. Dann gilt $[a' \cdot b'] = [a \cdot b]$.*

Beweis. Aus $a' \in [a]$ und $b' \in [b]$ folgt, dass es ganze Zahlen s und t mit

$$a' = a + sn \text{ und } b' = b + tn$$

gibt. Also gilt

$$a' \cdot b' = (a + sn) \cdot (b + tn) = a \cdot b + (at + sb + stn)n \equiv a \cdot b \,(\mathrm{mod}\ n).$$

□

Beispiel Wir stellen nun die Multiplikationstafel von $\mathbb{Z}_4$ auf:

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	$[1]$

Der Einfachheit halber lassen wir bei dem Produkt in $\mathbb{Z}_n$ meistens den Malpunkt weg.

Satz 1.27 *In $\mathbb{Z}_n$ gelten die folgenden Rechenregeln für alle $[a], [b], [c] \in \mathbb{Z}_n$:*

$$\begin{aligned}
([a] + [b]) + [c] &= [a] + ([b] + [c]) && (1.1)\\
[a] + [0] &= [a] && (1.2)\\
\exists [x] \in \mathbb{Z}_n \text{ mit } [a] + [x] &= [0] && (1.3)\\
[a] + [b] &= [b] + [a] && (1.4)\\
([a][b])[c] &= [a]([b][c]) && (1.5)\\
([a] + [b])[c] &= ([a][c]) + ([b][c]) && (1.6)\\
[a]\,[1] &= [a] && (1.7)\\
[a]\,[b] &= [b][a] && (1.8)
\end{aligned}$$

Beweis. Der Beweis ist sehr einfach, da alles repräsentantenweise nachgerechnet werden kann:

(1.1) $([a]+[b])+[c] = [a+b]+[c] = [(a+b)+c] = [a+(b+c)] = [a]+[b+c] = [a] + ([b] + [c])$.

(1.2) $[a] + [0] = [a + 0] = [a]$.

(1.3) Man wählt

$$[x] := [-a] = [n - a]$$

und nennt diese Restklasse das *additive Inverse* von a, kurz geschrieben als $-[a]$. Es gilt

$$[a] + [-a] = [a + (-a)] = [0].$$

Den Rest lassen wir als Übung. □

Sehen wir uns die Multiplikationstafel von $\mathbb{Z}_4$ (siehe Beispiel) an, so fällt auf, dass gilt: $[2] \cdot [2] = [0]$. Wir sagen auch, dass [2] ein Nullteiler und $\mathbb{Z}_4$ nicht nullteilerfrei ist.

Lemma 1.28 *Es seien $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$ und a und n teilerfremd. Dann folgt aus $a \equiv b \bmod n$, dass auch b und n teilerfremd sind.*

Beweis. Aus Satz 1.7 folgt, dass es ganze Zahlen r und s gibt mit

$$ra + sn = 1.$$

Dann gilt für $b = a + kn$

$$1 = r(a + kn) + (s - kr)n = rb + (s - kr)n,$$

also sind auch b und n teilerfremd. □

Definition Sind a und n teilerfremd, so bezeichnet man die Restklasse $[a]$ mod n als *prime Restklasse* mod n. Alle primen Restklassen mod n werden zu der Menge

$$\mathbb{Z}_n^* \subset \mathbb{Z}_n$$

zusammengefasst, die auch prima Restklassengruppe genannt wird (Gruppe s.u.).

Beispiel Es gilt $\mathbb{Z}_4^* = \{[1], [3]\}$.

Satz 1.29 *Es sei $n \in \mathbb{N} \setminus \{0\}$.*

(i) *Es seien $[a], [b] \in \mathbb{Z}_n^*$. Dann ist auch das Produkt $[a][b] \in \mathbb{Z}_n^*$.*

(ii) *Für $[a] \in \mathbb{Z}_n^*$ ist die Gleichung $[a][x] = [1]$ in $\mathbb{Z}_n^*$ lösbar, d.h. es gibt ein $x \in \mathbb{Z}$ mit $(x, n) = 1$, so dass die Kongruenz $ax \equiv 1 \bmod n$ gilt. Die Lösung x ist sogar modulo n eindeutig bestimmt.*

Beweis. (i) Die Zahlen a und b sind nach Lemma 1.28 teilerfremd zu n. Dann ist auch das Produkt ab teilerfremd zu n. Denn ein gemeinsamer Primteiler von ab und n müsste auch a oder b teilen. Wieder nach Lemma 1.28 folgt $[a] \cdot [b] \in \mathbb{Z}_n^*$.

(ii) Dies ist genau die Aussage von Satz 1.10. Hier noch einmal das Argument im einzelnen: da a teilerfremd zu n ist, gibt es nach Satz 1.7 $x, s \in \mathbb{Z}$ mit

$$ax + sn = 1.$$

Diese Gleichung lässt sich auch als $ax \equiv 1 \bmod n$ lesen. Sie zeigt auch, dass x und n teilerfremd sind.

Zur Eindeutigkeit: Ist $y \in \mathbb{Z}$ eine weitere Lösung von $ay \equiv 1 \bmod n$, dann gilt nach Satz 1.27 und Korollar 1.9 wegen $(a, n) = 1$

$$a(x - y) \equiv 0 \bmod n \Rightarrow n | a(x - y) \Rightarrow n | (x - y) \Rightarrow x \equiv y \bmod n.$$

□

Korollar 1.30 *Es sei $n \in \mathbb{N} \setminus \{0\}$, $a, c \in \mathbb{Z}$.*

(i) *Gilt $(a, n) = 1$, so hat die Kongruenz $ax \equiv c \bmod n$ eine modulo n eindeutige Lösung $x \in \mathbb{Z}$.*

(ii) *Die Kongruenz $ax \equiv c \bmod n$ hat genau dann eine Lösung $x \in \mathbb{Z}$, wenn für $d := (a, n)$ gilt: $d | c$. In diesem Fall ist $x \bmod \frac{n}{d}$ eindeutig bestimmt, d.h. in $\mathbb{Z}_n$ hat die Gleichung $[a][x] = [c]$ genau d Lösungen, nämlich die Lösungen*

$$[x], \left[x + \frac{n}{d}\right], \ldots, \left[x + (d-1)\frac{n}{d}\right].$$

Beweis. (i) Die Existenz der Lösung folgt aus Satz 1.29 durch Multiplikation der Kongruenz mit c. Die Eindeutigkeit sieht man wie folgt: es seien $ax \equiv c \bmod n$ und $ay \equiv c \bmod n$. Dann folgt, dass $a(x-y) = kn$ für ein $k \in \mathbb{Z}$. Da $(a,n) = 1$ gilt $a|k$ und wir erhalten $x - y = \frac{k}{a}n$ also $x \equiv y \bmod n$.

(ii) Es gilt

$$ax \equiv c \bmod n \Leftrightarrow n|(ax - c) \Rightarrow d|c.$$

Gilt $d|c$, so gilt

$$ax \equiv c \bmod n \Leftrightarrow \frac{n}{d}\Big|\left(\frac{a}{d}x - \frac{c}{d}\right) \Leftrightarrow \frac{a}{d}x \equiv \frac{c}{d} \bmod \frac{n}{d}.$$

Nun gilt aber $(\frac{a}{d}, \frac{n}{d}) = 1$. Damit folgt die Behauptung aus (i). □

Wir betrachten nun simultane Kongruenzen.

Satz 1.31 (Chinesischer Restsatz) *Es seien $n_1, \ldots, n_m$ paarweise teilerfremde positive ganze Zahlen und $a_1, \ldots, a_m \in \mathbb{Z}$. Dann gibt es ein $x \in \mathbb{Z}$, das alle Kongruenzen*

$$x \equiv a_1 \bmod n_1, \quad \ldots \quad , x \equiv a_m \bmod n_m$$

erfüllt. Die Lösung x ist modulo $n_1 n_2 \cdots n_m$ eindeutig bestimmt, und mit x ist auch jeder andere Repräsentant in seiner Restklasse $\bmod n_1 n_2 \cdots n_m$ *eine Lösung.*

Beweis.

(a) *Eindeutigkeit*: Angenommen, $y \in \mathbb{Z}$ ist ebenfalls eine Lösung dieser Kongruenzen. Dann muss gelten:

$$n_i|(x-y) \text{ für alle } i = 1, \ldots, m.$$

Da die n_i paarweise teilerfremd sind, ist dies äquivalent zu

$$n_1 \cdots n_m|(x-y).$$

(b) *Existenz*: Wir führen den Beweis durch Induktion nach m.

Induktionsanfang $m = 2$: Wir führen den Induktionsanfang für $m = 2$ durch. Wir betrachten zunächst den Fall $a_1 = 1$, $a_2 = 0$. Nach Satz 1.29(ii) gibt es eine Lösung $y \in \mathbb{Z}$ der Kongruenz

$$yn_2 \equiv 1 \bmod n_1.$$

Setze $u := yn_2$. Dann gilt für u

$$u \equiv 1 \bmod n_1, \quad u \equiv 0 \bmod n_2.$$

Analog findet man eine Lösung $v \in \mathbb{Z}$ der Kongruenzen

$$v \equiv 0 \bmod n_1, \quad v \equiv 1 \bmod n_2.$$

Zurück zum allgemeinen Fall mit beliebigen a_1, a_2: Mit obigen u, v gilt für $x := ua_1 + va_2$

$$x \equiv a_1 \bmod n_1, \quad x \equiv a_2 \bmod n_2.$$

Also haben wir eine Lösung für den Fall $m = 2$ gefunden.

Induktionsschluss $m - 1 \to m$: Nach Induktionsannahme können wir annehmen, dass ein $y \in \mathbb{Z}$ existiert, das die Kongruenzen

$$y \equiv a_2 \bmod n_2, \quad \ldots \quad , y \equiv a_m \bmod n_m$$

löst. Dann ist wie im Induktionsanfang nur noch ein $x \in \mathbb{Z}$ zu finden, das die Kongruenzen

$$x \equiv a_1 \bmod n_1 \text{ und } x \equiv y \bmod n_2 \cdots n_m$$

löst. Dies ist genau die Situation wie im Induktionsanfang, wenn man beachtet, dass nach Voraussetzung auch n_1 und $n_2 \cdots n_m$ teilerfremd sind. □

Korollar 1.32 *Es seien $n_1, \ldots, n_m$ paarweise teilerfremde positive ganze Zahlen. Setze $n = n_1 \cdots n_m$. Die Abbildung*

$$\begin{array}{rcl} \mathbb{Z}_n & \to & \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_m} \\ [x] & \mapsto & ([x], \ldots, [x]) \end{array}$$

ist bijektiv (sogar ein Ringisomorphimus, wie wir später sehen werden).

Wir führen nun die Eulersche φ-Funktion ein.

Definition Für eine positive ganze Zahl n ist die *Eulersche φ-Funktion* $\varphi(n)$ definiert als die Anzahl der positiven ganzen Zahlen kleiner oder gleich n, die teilerfremd zu n sind:

$$\varphi(n) = \#\{t \in \mathbb{N};\ \ t \leq n,\ (t, n) = 1\}.$$

Es gilt $\varphi(1) = 1$ und für alle natürlichen Zahlen $n > 1$ ist $\varphi(n)$ gerade die Anzahl der Elemente von $\mathbb{Z}_n^*$:

$$\varphi(n) = \#\mathbb{Z}_n^*. \tag{1.9}$$

Lemma 1.33 *Für eine Primzahl p und eine positive ganze Zahl a gilt*

$$\varphi(p^a) = p^a \left(1 - \frac{1}{p}\right).$$

Beweis. Es gibt p^a positive ganze Zahlen, die kleiner oder gleich p^a sind. Die Zahlen, die nicht teilerfremd zu p^a sind, sind aber gerade Vielfache von p. Unter den Zahlen, die kleiner oder gleich p^a sind, gibt es davon gerade p^{a-1}. Also gilt

$$\varphi(p^a) = p^a - p^{a-1} = p^a \left(1 - \frac{1}{p}\right).$$

□

Satz 1.34 *Die Eulersche φ-Funktion ist* multiplikativ*, d.h. für alle teilerfremden $m, n \in \mathbb{N} \setminus \{0\}$ gilt*

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

Beweis. Aus Korollar 1.9 folgt, dass x genau dann teilerfremd zu mn ist, wenn x teilerfremd zu m und zu n ist. In der Tat lässt sich analog zu Korollar 1.32 die folgende Aussage herleiten, die Satz 1.34 angesichts von (1.9) impliziert. □

Korollar 1.35 *Es seien $n_1, \ldots, n_m$ paarweise teilerfremde positive ganze Zahlen. Setze $n = n_1 \cdots n_m$. Die Abbildung*

$$\begin{array}{ccc} \mathbb{Z}_n^* & \to & \mathbb{Z}_{n_1}^* \times \ldots \times \mathbb{Z}_{n_m}^* \\ [x] & \mapsto & ([x], \ldots, [x]) \end{array}$$

ist bijektiv (sogar ein Gruppenisomorphimus, wie wir später sehen werden).

Korollar 1.36 *Für beliebige $n \in \mathbb{N} \setminus \{0\}$ gilt*

$$\varphi(n) = n \prod_{p \in \mathbb{P}, p|n} \left(1 - \frac{1}{p}\right).$$

Beweis. Dies folgt unmittelbar aus Lemma 1.33, der eindeutigen Primfaktorzerlegung von n und Satz 1.34. □

Kapitel 2

Gruppen

2.1 Symmetriegruppen

Wir erinnern zunächst an die Definition einer Gruppe, die wir schon in Lineare Algebra I hatten.

Definition Eine *Verknüpfung* auf einer Menge G ist eine Abbildung

$$* : G \times G \to G.$$

Wir schreiben oft

$$a * b := *(a, b).$$

Definition Eine Menge G zusammen mit einer Verknüpfung $*$ heißt *Gruppe* genau dann, wenn folgende Axiome erfüllt sind:

(A) $(a * b) * c = a * (b * c)$ für alle $a, b, c \in G$ (*Assoziativgesetz*).

(N) Es gibt ein $e \in G$ mit $a * e = a$ für alle $a \in G$ (*Neutrales Element*).

(I) Zu jedem $a \in G$ gibt es ein $a' \in G$ mit $a * a' = e$ (*Inverses Element*).

Die Gruppe heißt *abelsch* (oder *kommutativ*), falls zusätzlich folgendes Axiom erfüllt ist:

(K) $a * b = b * a$ für alle $a, b \in G$ (*Kommutativgesetz*).

Beispiel Als Beispiele für Gruppen hatten wir bereits betrachtet: $(\mathbb{R}, +)$ und $(\mathbb{R}^*, \cdot)$ sind abelsche Gruppen. $(\mathrm{GL}(n, K), *)$ mit der Verknüpfung $A * B := AB$ für $A, B \in \mathrm{GL}(n, K)$ ist eine Gruppe.

Wir hatten bereits den folgenden Satz bewiesen:

Satz 2.1 *Ist G eine Gruppe, so gilt:*

(a) *Das neutrale Element $e \in G$ ist eindeutig bestimmt und hat auch die Eigenschaft $e * a = a$ für alle $a \in G$.*

(b) *Das inverse Element a' zu einem Element $a \in G$ ist eindeutig bestimmt und hat auch die Eigenschaft $a' * a = e$. Wir bezeichnen es mit a^{-1}.*

(c) $(a^{-1})^{-1} = a$ *für alle* $a \in G$.

(d) $(a * b)^{-1} = b^{-1} * a^{-1}$ *für alle* $a, b \in G$.

(e) *Es gelten die folgenden Kürzungsregeln:*

$$a * x = a * \tilde{x} \Rightarrow x = \tilde{x} \text{ und } y * a = \tilde{y} * a \Rightarrow y = \tilde{y}.$$

Definition Die Anzahl der Elemente einer Gruppe G wird mit $|G|$ oder $\#G$ bezeichnet und die *Ordnung der Gruppe* genannt. Die Gruppe G heißt *endliche Gruppe*, wenn $|G|$ endlich ist, andernfalls heißt G *unendliche Gruppe*.

Wir wollen nun weitere Beispiele für Gruppen betrachten.

Beispiel $(\mathbb{Z}, +)$ und $(\mathbb{Q}, +)$ sind unendliche abelsche Gruppen, $(\mathbb{N}, +)$ ist keine Gruppe, da z.B. 2 kein inverses Element in $\mathbb{N}$ besitzt.

Beispiel In 1.4 haben wir für eine natürliche Zahl $n \geq 1$ die Menge $\mathbb{Z}_n$ der Restklassen mod n definiert. Auf dieser Menge wurde eine Addition definiert. Nach Satz 1.27 (1.1)–(1.4) ist $\mathbb{Z}_n$ mit dieser Addition eine abelsche Gruppe. Die Ordnung dieser Gruppe ist nach Korollar 1.24 die Zahl n.

Beispiel In 1.4 wurde außerdem die Menge $\mathbb{Z}_n^*$ aller primen Restklassen mod n eingeführt. Nach Satz 1.29 ist $\mathbb{Z}_n^*$ mit der Multiplikation als Verknüpfung eine Gruppe. Nach Satz 1.27 (1.8) ist diese Gruppe abelsch. Diese Gruppe heißt die *prime Restklassengruppe* mod n. Die Ordnung dieser Gruppe ist $\varphi(n)$.

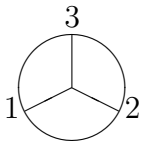
Beispiel In Lineare Algebra I haben wir Permutationen der Menge $\{1, 2, \ldots, n\}$ betrachtet und gezeigt, dass die Menge der Permutationen mit der Hintereinanderschaltung als Verknüpfung eine Gruppe bildet. Diese Gruppe heißt die *symmetrische Gruppe von n Elementen* und wird mit S_n bezeichnet. Sie ist nur für $n \leq 2$ abelsch. Die Ordnung der Gruppe S_n ist $n!$, wie wir in Lineare Algebra I gesehen haben.

Eine weitere Klasse von Beispielen sind Symmetriegruppen von geometrischen Figuren.

Definition Es sei F eine geometrische Figur in der Ebene oder im Raum. Eine *Symmetrie der Figur* F ist eine bijektive Abbildung $f : F \to F$, die Abstände erhält, d.h. für alle Punkte $p, q \in F$ ist der Abstand von $f(p)$ zu $f(q)$ gleich dem Abstand von p zu q.

Die Menge aller Symmetrien einer geometrischen Figur bildet mit der Hintereinanderausführung als Verknüpfung eine Gruppe, da die Hintereinanderausführung von zwei abstandserhaltenden Abbildungen wieder abstandserhaltend ist und das Inverse einer abstandserhaltenden Abbildung ebenfalls abstandserhaltend ist. Man nennt diese Gruppe die *Symmetriegruppe der Figur*.

Beispiel Wir betrachten die folgende Figur.



(Die Zahlen sind nur zur Hilfe angegeben.) Wie sehen die Symmetrien dieser Figur aus? Drehen der Figur liefert

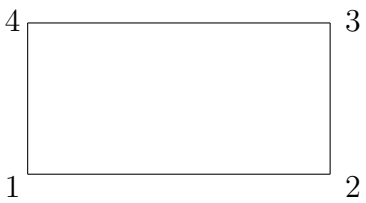
$$(1,2,3) \mapsto (1,2,3), \quad (1,2,3) \mapsto (2,3,1), \quad (1,2,3) \mapsto (3,1,2).$$

Darüber hinaus können wir Spiegelungen betrachten:

$$(1,2,3) \mapsto (1,3,2), \quad (1,2,3) \mapsto (3,2,1), \quad (1,2,3) \mapsto (2,1,3).$$

Die angebene Beschreibung zeigt, dass wir diese Gruppe mit der Gruppe aller Permutationen der Zahlen $1, 2, 3$ identifizieren können, die wir bereits in Lineare Algebra I betrachtet haben.

Beispiel Als weiteres Beispiel betrachten wir die Symmetriegruppe eines Rechtecks mit ungleichen Seiten:



Wir haben die folgenden Symmetrien, die die Abstände erhalten: die Spiegelung a an einer horizontalen Achse durch den Mittelpunkt, d.h.

$$a : (1, 2, 3, 4) \mapsto (4, 3, 2, 1),$$

die entsprechende Spiegelung b an einer vertikalen Achse durch den Mittelpunkt, d.h.

$$b : (1, 2, 3, 4) \mapsto (2, 1, 4, 3),$$

und die Drehung c um 180° um den Mittelpunkt, d.h.

$$c : (1, 2, 3, 4) \mapsto (3, 4, 1, 2).$$

Schließlich ist die identische Abbildung e eine Symmetrie. Die Gruppentafel sieht nun wie folgt aus

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Diese Gruppe nennt man auch die *Kleinsche Vierergruppe* nach dem Mathematiker Felix Klein (1849–1925).

Notation Wir lassen im Folgenden das Verknüpfungszeichen $*$ weg, d.h. $a * b$ wird einfach als ab geschrieben.

Definition Eine Teilmenge H einer Gruppe G heißt *Untergruppe* von G genau dann, wenn die folgenden Bedingungen erfüllt sind:

(UG0) $H \neq \emptyset$.

(UG1) Für alle $a, b \in H$ gilt $ab \in H$.

(UG2) Für alle $a \in H$ gilt $a^{-1} \in H$.

Satz 2.2 *Eine Untergruppe H einer Gruppe G ist mit der induzierten Verknüpfung eine Gruppe.*

Beweis. Wir müssen zeigen, dass die Gruppenaxiome in H erfüllt sind. Nach (UG1) induziert die Verknüpfung auf G eine Verknüpfung auf H. Das Assoziativgesetz gilt in H, da es in G gilt. Da H nicht leer ist, enthält H mindestens ein Element $h \in H$. Nach (UG2) ist auch $h^{-1} \in H$. Damit ist auch $e = hh^{-1} \in H$. Nach (UG2) liegt zu jedem Element $a \in H$ das inverse Element a^{-1} in H. Also erfüllt H die Gruppenaxiome. □

Bemerkung Die Bedingungen (UG1) und (UG2) sind zu der folgenden einzigen Bedingung äquivalent

(UG) Für alle $a, b \in H$ gilt $ab^{-1} \in H$.

Beispiel Die Gruppe $\mathbb{Z}$ ist eine Untergruppe von $\mathbb{Q}$, $\mathbb{Q}$ ist eine Untergruppe von $\mathbb{R}$ und $\mathbb{R}$ ist eine Untergruppe von $\mathbb{C}$.

Beispiel Es sei A_n die Menge aller geraden Permutationen. Da die Hintereinanderschaltung von zwei geraden Permutationen wieder gerade ist und auch das Inverse einer geraden Permutation gerade ist, ist A_n eine Untergruppe von S_n. Sie wird die *alternierende Gruppe von n Elementen* genannt.

2.2 Zyklische Gruppen

Eine wichtige Klasse von Gruppen sind die zyklischen Gruppen.

Definition Eine Gruppe G heißt *zyklisch* genau dann, wenn ein Element $g \in G$ existiert, so dass $G = \{g^n \mid n \in \mathbb{Z}\}$. In diesem Fall sagt man, dass g die zyklische Gruppe G *erzeugt*.

Notation: $\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$.

Bemerkung Eine zyklische Gruppe G ist abelsch, da

$$g^n g^m = g^{n+m} = g^m g^n.$$

Beispiel (a) Die Gruppe $\mathbb{Z}$ ist eine unendliche zyklische Gruppe, die von dem Element 1 (oder -1) erzeugt wird.

(b) Die Gruppe $\mathbb{Z}_n$ ist eine endliche zyklische Gruppe, sie wird von dem Element [1] erzeugt.

Definition Die *Ordnung eines Elements* g in einer Gruppe G, in Zeichen $\operatorname{ord} g$, ist die kleinste positive ganze Zahl r, so dass $g^r = e$ ist. Wenn keine solche Zahl r existiert, so sagt man, dass die Ordnung des Elements g *unendlich* ist.

Satz 2.3 *Wenn g ein Element der Ordnung k der Gruppe G ist, dann ist $H = \{g^n \mid n \in \mathbb{Z}\}$ eine Untergruppe von G der Ordnung k.*

Definition In diesem Fall nennt man H *die von g erzeugte zyklische Untergruppe* von G.

Beweis. Wir zeigen zunächst, dass H eine Untergruppe von G ist. Das Axiom (UG1) ist erfüllt, da $g^m g^n = g^{m+n} \in H$, (UG2), da $(g^m)^{-1} = g^{-m} \in H$ für alle $m, n \in \mathbb{Z}$ ist.

Nun zeigen wir, dass H die Ordnung k hat.

Es sei zunächst $k = \infty$. Dann zeigen wir, dass alle Elemente g^n verschieden sind. Denn angenommen, $g^n = g^m$, wobei $m < n$. Dann gilt $n - m > 0$ und $g^{n-m} = e$. Das ist aber ein Widerspruch dazu, dass g unendliche Ordnung hat. Also ist die Ordnung von H unendlich.

Es sei nun $k < \infty$. Dann zeigen wir:

Behauptung $H = \{g^0 = e, g^1, g^2, \ldots, g^{k-1}\}$.

Beweis. Zunächst zeigen wir, dass die Elemente g^n, $n = 0, 1, \ldots, k-1$, alle verschieden sind. Angenommen, $g^n = g^m$, wobei $0 \leq m < n \leq k-1$. Dann folgt $g^{n-m} = e$ mit $0 < n - m < k$. Dies widerspricht der Minimalität von k, der Ordnung von g. Also sind die Elemente g^0, g^1, …, g^{k-1} alle verschieden. Für ein beliebiges anderes Element g^m können wir $m = qk + r$ mit $0 \leq r < k$ schreiben. Dann gilt

$$g^m = g^{qk+r} = \left(g^k\right)^q (g^r) = (e^q)(g^r) = g^r.$$

Also liegt g^m in H. Damit ist die Behauptung bewiesen. □

Aus der Behauptung folgt nun, dass $|H| = k$. □

Merke: $\operatorname{ord}(g) = k < \infty, g^r = e \Longrightarrow k \mid r$.

Beispiel Die von der Zahl 2 in $\mathbb{Z}$ erzeugte zyklische Untergruppe von $\mathbb{Z}$ enthält alle geraden Zahlen und wir bezeichnen diese Untergruppe mit $2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$.

Satz 2.4 *Ist G eine endliche Gruppe der Ordnung n und besitzt G ein Element g der Ordnung n, so ist G eine zyklische Gruppe, die von g erzeugt ist.*

Beweis. Es sei H die von g erzeugte zyklische Untergruppe von G. Nach dem vorhergehenden Satz hat H die Ordnung n. Aus $H \subset G$ und $|H| = |G| = n < \infty$ folgt aber $H = G$. Also ist G die von g erzeugte zyklische Gruppe. □

Beispiel Es sei C_n die Gruppe der Drehungen eines regulären n-Ecks in der Ebene. Dann ist C_n eine zyklische Gruppe der Ordnung n, die von einer Drehung um den Winkel $\frac{2\pi}{n}$ erzeugt wird. Denn C_n hat die Ordnung n: Wenn wir die Ecken des n-Ecks mit $1, 2, \ldots n$ bezeichnen, so werden bei einer

Drehung die Eckennummern zyklisch vertauscht. Bezeichnet g die Drehung des n-Ecks um den Winkel $\frac{2\pi}{n}$, so hat g die Ordnung n. Nach Satz 2.4 ist C_n zyklisch von der Ordnung n und wird von g erzeugt.

Beispiel Die Kleinsche Vierergruppe ist nicht zyklisch, da sie die Ordnung 4 hat, aber kein Element der Ordnung 4 besitzt.

Wir erinnern nun an die Definition eines Gruppenhomomorphismus (siehe Lineare Algebra I).

Definition Es seien $(G, *)$ und $(H, \cdot)$ zwei Gruppen. Eine Abbildung $f : G \to H$ heißt *Gruppenhomomorphismus* genau dann, wenn gilt

$$f(a * b) = f(a) \cdot f(b).$$

Ein Gruppenhomomorphismus $f : G \to H$ ist ein *Isomorphismus* falls es einen Gruppenhomomorphismus $g : H \to G$ gibt mit $g \circ f = \mathrm{id}_G$ und $f \circ g = \mathrm{id}_H$. In diesem Fall sagen wir, dass die Gruppen G und H *isomorph* sind und schreiben $G \cong H$.

Ein injektiver Gruppenhomomorphismus heißt ein *Monomorphismus* und ein surjektiver Gruppenhomomorphismus heißt ein *Epimorphismus*.

Bemerkung Ist $f : G \to H$ is bijektiver Gruppenhomomorphismus, dann ist $f^{-1} : H \to G$ ebenfalls ein Gruppenhomomorphismus und f ist ein Gruppenisomorphismus.

Beispiel (1) Es seien G und H Gruppen und e das neutrale Element von H. Die Abbildung $f : G \to H$ mit $f(a) = e$ für alle $a \in G$ ist ein Gruppenhomomorphismus.

(2) Ist H eine Untergruppe von G, so ist die Inklusionsabbildung $i : H \to G$ ein Gruppenhomomorphismus.

(3) Es sei $f : \mathbb{Z} \to \{1, -1\}$ definiert durch $f(n) = 1$, falls n gerade, und $f(n) = -1$, falls n ungerade. Dann ist f ein Gruppenhomomorphismus von $(\mathbb{Z}, +)$ nach $(\{1, -1\}, \cdot)$

(4) Die Exponentionalabbildung $\exp : (\mathbb{R}, +) \to (\mathbb{R}^*, \cdot), e \mapsto e^x$ ist ein Gruppenhomomomorphismus, da

$$e^{x+y} = e^x \cdot e^y.$$

(5) Die Abbildung

$$\mathrm{sign} : S_n \to \{\pm 1\}, \sigma \mapsto \mathrm{sign}(\sigma)$$

ist ein Gruppenhomomorphismus.

(6) Die Abbildung

$$\det : \mathrm{GL}(n; K) \to K^*, A \mapsto \det(A)$$

ist ein Gruppenhomomorphismus, da

$$\det(AB) = \det(A)\det(B)$$

gilt.

(7) Die Abbildung

$$\frac{d}{dx} : C^1[a, b] \to C[a, b], f \mapsto f'$$

welche einer stetig differenzierbaren Funktion f auf einem Intervall $[a, b]$ ihre Abbildung $f' = \frac{df}{dx}$ zuordnet, ist ein Gruppenhomomorphismus, da

$$(f + g)' = f' + g'.$$

In Lineare Algebra I haben wir bereits bewiesen:

Satz 2.5 *Es sei $f : G \to H$ ein Gruppenhomomorphismus. Dann gilt:*

(i) *$f(e_G) = e_H$, wobei e_G bzw. e_H das neutrale Element von G bzw. H ist.*

(ii) *$f(a^{-1}) = f(a)^{-1}$ für alle $a \in G$.*

Satz 2.6 *Zyklische Gruppen der gleichen Ordnung sind isomorph.*

Beweis. Es seien G und H zyklische Gruppen, die von g bzw. h erzeugt werden. Wenn G und H unendliche Ordnung haben, so definieren wir $f : G \to H$ durch $f(g^r) = h^r$ für alle $r \in \mathbb{Z}$. Dann ist f bijektiv. Es gilt

$$f(g^r g^s) = f(g^{r+s}) = h^{r+s} = h^r h^s = f(g^r) f(g^s).$$

Also ist f ein Isomorphismus.

Wenn G und H die Ordnung n haben, so definieren wir $f : G \to H$ durch $f(g^r) = h^r$ für $r = 0, 1, \ldots, n-1$. Dann ist f bijektiv. Für $0 \leq r, s \leq n-1$ sei $r + s = kn + l$, wobei $0 \leq l \leq n-1$. Dann gilt

$$f(g^r g^s) = f(g^{r+s}) = f(g^{kn+l}) = f((g^n)^k g^l) = f(e^k g^l) = f(g^l) = h^l$$

und

$$f(g^r) f(g^s) = h^r h^s = h^{r+s} = h^{kn+l} = (h^n)^k h^l = e^k h^l = h^l.$$

Also ist f ein Isomorphismus. □

Korollar 2.7 *Jede zyklische Gruppe ist entweder isomorph zu $\mathbb{Z}$ oder zu $\mathbb{Z}_n$ für ein gewisses $n \in \mathbb{N}$.*

Für eine zyklische Gruppe der Ordnung n schreibt man oft auch C_n.

Ausblick: Ähnliche Struturresultate gelten für alle endlich erzeugten abelschen Gruppen.

Bemerkung Ein Gruppenhomomorphismus $f : G \to H$ von einer *zyklischen* Gruppe G auf eine beliebige Gruppe H ist schon durch das Bild eines erzeugenden Element $g \in G$ bestimmt. Denn gilt $f(g) = h$, so folgt aus der Definition des Gruppenhomomorphismus, dass $f(g^r) = f(g)^r = h^r$ für alle $r \in \mathbb{Z}$ gilt.

Satz 2.8 *Ist $f : G \to H$ ein Monomorphismus und gilt $f(g) = h$, so haben g und h die gleiche Ordnung.*

Beweis. Angenommen, g hat die Ordnung m und h hat die Ordnung n. Ist $m < \infty$, so gilt

$$h^m = f(g)^m = f(g^m) = f(e) = e.$$

Daraus folgt, dass auch n endlich ist und $n \leq m$ gilt.

Ist n endlich, so gilt

$$f(g^n) = f(g)^n = h^n = e = f(e).$$

Da f injektiv ist, folgt daraus $g^n = e$. Also ist auch m endlich und es gilt $n \leq m$.

Also sind entweder m und n beide endlich und es gilt $m = n$, oder $m = n = \infty$. □

2.3 Quotientengruppen

Eine wichtige Konstruktionsmethode für Gruppen ist die Quotientenkonstruktion, die wir nun betrachten wollen.

In 1.4 haben wir die Gruppe $\mathbb{Z}_n$ definiert. Diese Gruppe war mit Hilfe der Kongruenzrelation modulo n auf $\mathbb{Z}$ erklärt. Wir können diese Relation auch so definieren:

$$a \equiv b \bmod n \Leftrightarrow a - b \in n\mathbb{Z},$$

wobei $n\mathbb{Z}$ die Untergruppe von $\mathbb{Z}$ ist, die aus allen Vielfachen von n besteht. Wir wollen nun diese Kongruenzrelation auf beliebige Untergruppen von Gruppen erweitern.

Definition Es sei G eine Gruppe, H eine Untergruppe von G und $a, b \in G$. Dann sagen wir, *a ist kongruent zu b modulo H*, in Zeichen $a \equiv b \bmod H$, genau dann, wenn $ab^{-1} \in H$ gilt.

Satz 2.9 *Die Relation $a \equiv b \bmod H$ ist eine Äquivalenzrelation auf G. Die Äquivalenzklasse von a ist von der Form $Ha := \{ha \mid h \in H\}$.*

Definition Die Menge $Ha := \{ha \mid h \in H\}$ wird eine *Rechtsnebenklasse* von H in G genannt. Das Element a heißt ein *Repräsentant* der Rechtsnebenklasse Ha.

Beweis. (i) Die Relation ist reflexiv, da für alle $a \in G$ gilt $aa^{-1} = e \in H$.

(ii) Aus $a \equiv b \bmod H$ folgt $ab^{-1} \in H$. Da H eine Untergruppe ist, ist auch $(ab^{-1})^{-1} = ba^{-1} \in H$. Also folgt $b \equiv a \bmod H$. Die Relation ist daher symmetrisch.

(iii) Aus $a \equiv b \bmod H$ und $b \equiv c \bmod H$ folgt $ab^{-1} \in H$ und $bc^{-1} \in H$. Da H eine Untergruppe ist, gilt $ab^{-1}bc^{-1} = ac^{-1} \in H$, also $a \equiv c \bmod H$. Daher ist die Relation auch transitiv.

Wir zeigen nun: $[a] = Ha$. Es sei zunächst $x \in [a]$. Dann gilt $x \equiv a \bmod H$. Also ist $h := xa^{-1} \in H$. Nun gilt aber $x = ha$. Also ist $x \in Ha$. Damit gilt $[a] \subset Ha$. Sei umgekehrt $x \in Ha$. Dann gibt es ein $h \in H$ mit $x = ha$. Daraus folgt aber $xa^{-1} = h \in H$, also $x \equiv a \bmod H$ und damit $x \in [a]$. Daraus folgt $Ha \subset [a]$ und damit $[a] = Ha$. □

Beispiel Die Rechtsnebenklassen von A_3 in S_3 sind (in Zykelschreibweise)

$$\begin{aligned} [(1)] &= \{(1), (123), (132)\} = A_3(1) \\ [(12)] &= \{(12), (13), (23)\} = A_3(12) \end{aligned}$$

Lemma 2.10 *Zwischen je zwei Rechtsnebenklassen von H in G gibt es eine bijektive Abbildung.*

Beweis. Es sei Ha eine Rechtsnebenklasse von H in G. Um die Behauptung zu zeigen, genügt es, eine bijektive Abbildung von $H = He$ nach Ha zu konstruieren.

Wir definieren $\psi_a : H \to Ha$ durch $\psi_a(h) = ha$. Nach Definition der Menge Ha ist ψ_a surjektiv. Die Abbildung ψ ist auch injektiv: Dazu nehmen wir $\psi_a(h_1) = \psi_a(h_2)$ an. Daraus folgt $h_1 a = h_2 a$. Indem wir beide Seiten dieser Gleichung von rechts mit a^{-1} multiplizieren, erhalten wir $h_1 = h_2$. Also ist ψ_a bijektiv.

Die Bijektivität von H_a und H_b folgt nun mittels $\psi_b \circ \psi_a^{-1}$. □

Korollar 2.11 *Jede Rechtsnebenklasse von H in G enthält dieselbe Anzahl an Elementen:*

$$\forall a, b \in G : \#(Ha) = \#(Hb).$$

Bemerkung Anstelle der Relation $a \equiv b \bmod H :\Leftrightarrow ab^{-1} \in H$ hätte man auch definieren können

$$a \equiv' b \bmod H :\Leftrightarrow b^{-1}a \in H.$$

Die Äquivalenzklassen dieser Relation sind von der Form $aH := \{ah \mid h \in H\}$ und werden *Linksnebenklassen* von H in G genannt. Auch zwischen je zwei Linksnebenklassen von H in G gibt es eine bijektive Abbildung.

Für abelsche Gruppen stimmen Rechts- und Linksnebenklassen natürlich überein. Im Allgemeinen sind die Rechts- und Linksnebenklassen einer Untergruppe H von G verschieden, wie das nächste Beispiel zeigt. Allerdings ist ihre Gesamtanzahl gleich, denn die Abbildung

$$Ha \mapsto (Ha)^{-1} := \{(ha)^{-1} \mid h \in H\} = a^{-1}H$$

ist eine Bijektion zwischen der Menge der Rechts- und der Menge der Linksnebenklassen.

Beispiel (i) Es sei $G = S_3$ und $H = \{(1), (12)\}$ (Zykelschreibweise). Dann sind die Rechtsnebenklassen von H in G

$$H(1) = \{(1), (12)\},\ H(13) = \{(13), (132)\},\ H(23) = \{(23), (123)\}.$$

und die Linksnebenklassen

$$(1)H = \{(1), (12)\},\ (13)H = \{(13), (123)\},\ (23)H = \{(23), (132)\}$$

(ii) Dagegen gilt für $G = S_3 \supset H' = A_3$ nach dem vorherigen Beispiel:

$$H'g = gH' \quad \forall g \in G.$$

Satz 2.12 (Satz von Lagrange) *Ist G eine endliche Gruppe und H eine Untergruppe von G, so teilt die Ordnung von H die Ordnung von G.*

Beweis. Die Rechtsnebenklassen von H in G bilden eine Partition von G. Also kann G als die disjunkte Vereinigung

$$G = Ha_1 \cup Ha_2 \cup \ldots \cup Ha_k$$

für gewisse endlich viele Elemente $a_1, a_2, \ldots, a_k \in G$ geschrieben werden. Nach Korollar 2.11 ist die Anzahl der Elemente in jeder Rechtsnebenklasse gleich, nämlich $|H|$. Da die obige Vereinigung disjunkt ist, folgt $|G| = k|H|$. Also teilt $|H|$ die Ordnung $|G|$ von G. □

Definition Es sei H eine Untergruppe von G. Die Anzahl der verschiedenen Rechtsnebenklassen von H in G heißt der *Index* von H in G und wird mit $[G : H]$ bezeichnet.

Beispiel Im letzten Beispiel gilt $[S_3 : H] = 3,\ [S_3 : A_3] = 2$.

Korollar 2.13 *Ist G eine endliche Gruppe und H eine Untergruppe von G, so gilt*

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

Korollar 2.14 *Ist G eine endliche Gruppe und a ein Element von G, so teilt die Ordnung von a die Ordnung von G.*

Beweis. Es sei $H := \{a^r \mid r \in \mathbb{Z}\}$ die von a erzeugte zyklische Untergruppe von G. Nach Satz 2.3 ist die Gruppenordnung von H gleich der Ordnung von a. Also teilt die Ordnung von a nach dem Satz von Lagrange die Ordnung von G. □

Korollar 2.15 *Ist die Ordnung der Gruppe G eine Primzahl, so ist G zyklisch.*

Beweis. Es sei $|G| = p$, wobei p eine Primzahl ist. Nach Korollar 2.14 hat jedes Element die Ordnung 1 oder p. Ordnung 1 hat aber nur das neutrale Element. Da $|G| \geq 2$ gilt, gibt es also mindestens ein Element a der Ordnung p. Nach Satz 2.4 ist G zyklisch. □

Eine weitere Folgerung ist der Satz von Euler:

Satz 2.16 (Euler) *Ist G eine endliche Gruppe und a ein Element von G, dann gilt*

$$a^{|G|} = e.$$

Beweis. Es sei m die Ordnung von a. Nach Korollar 2.14 gilt $|G| = mk$ für ein $k \in \mathbb{N}$. Also gilt

$$a^{|G|} = a^{mk} = (a^m)^k = e^k = e.$$

□

Den Satz von Euler können wir auf prime Restklassengruppen anwenden. Daraus ergeben sich zahlentheoretische Konsequenzen:

Korollar 2.17 *Es sei $n \in \mathbb{N}$, $n \geq 1$, $a \in \mathbb{Z}$, $(a, n) = 1$. Dann ist*

$$a^{\varphi(n)} \equiv 1 \bmod n.$$

Beweis. Rechne in $G = \mathbb{Z}_n^*$ und wende Satz 2.16 mit $\#G = \varphi(n)$ an. □

Korollar 2.18 (Kleiner Satz von Fermat) *Es sei p eine Primzahl und $a \in \mathbb{Z}$ eine Zahl, die von p nicht geteilt wird. Dann gilt*

$$a^{p-1} \equiv 1 \bmod p.$$

Für alle $a \in \mathbb{Z}$ ist

$$a^p \equiv a \bmod p.$$

Anwendung: Primzahltest Ist $n \in \mathbb{N}, n > 1$, so können wir einen einfachen Primzahltest wie folgt aufsetzen:

1. Wähle $a \in \mathbb{Z}, a \neq 0, \pm 1$.

2. Berechne (a, n); ist $(a, n) > 1$, so gilt entweder $n \mid a$ (und wir beginnen wieder bei 1.) oder wir erhalten einen nicht-trivialen Faktor von n.

3. Ist $(a, n) = 1$, so berechne $a^{n-1} \mod n$. Liefert dies nicht 1, so ist n nicht prim. Andernfalls wiederhole beginnend mit 1.

Bemerkung Leider gibt es Nicht-Primzahlen, die bei diesem Test nie entlarvt werden (die sogenannten Carmichael-Zahlen). Es gibt jedoch Verfeinerungen (basierend auf der Gruppenstruktur von $\mathbb{Z}_n^*$), denen keine Nicht-Primzahl entkommt (s. Kryptographie).

Wir wollen nun auf der Quotientenmenge G/H eine Gruppenstruktur definieren. Dies ist allerdings nicht immer möglich, sondern nur in dem Fall, dass H ein Normalteiler ist.

Definition Eine Untergruppe H einer Gruppe G heißt *Normalteiler* von G, falls für alle $g \in G$ und $h \in H$ gilt: $g^{-1}hg \in H$. Wir führen für Normalteiler die Notation

$$H \lhd G \quad \text{(bzw. meist } \; N \lhd G)$$

ein.

Bemerkung Wir können dies auch in der Form

$$gH = Hg$$

schreiben. Das heißt wir fordern, daß die Rechtsnebenklassen mit den Linksnebenklassen übereinstimmen.

Satz 2.19 *Jede Untergruppe einer abelschen Gruppe ist ein Normalteiler.*

Beweis. Es sei H eine Untergruppe der abelschen Gruppe G. Dann gilt für alle $g \in G$ und $h \in H$

$$g^{-1}hg = hg^{-1}g = h \in H.$$

Also ist H ein Normalteiler. □

Beispiel (1) Die alternierende Gruppe A_n ist ein Normalteiler von S_n.
(2) Die Untergruppe $H = \{(1), (12)\}$ der Gruppe S_3 ist kein Normalteiler (s. vorheriges Beispiel).

Satz 2.20 *Es sei N ein Normalteiler einer Gruppe G. Dann bildet die Menge der Rechtsnebenklassen $G/N = \{Ng \mid g \in G\}$ zusammen mit der Verknüpfung*

$$(Ng_1) \cdot (Ng_2) := N(g_1g_2)$$

eine Gruppe.

Definition Diese Gruppe heißt die *Quotientengruppe* oder *Faktorgruppe* von G nach N.

Beweis. Die Verknüpfung auf G/N ist mit Hilfe von Repräsentanten g_1 und g_2 der Rechtsnebenklassen definiert. Wir müssen zunächst zeigen, dass diese Verknüpfung *wohldefiniert* ist, d.h. nicht von der Auswahl der Repräsentanten abhängt. Das bedeutet, dass wir zeigen müssen, dass, wenn wir andere Elemente $h_1 \in Ng_1$ und $h_2 \in Ng_2$ in den gleichen Rechtsnebenklassen wählen, die Rechtsnebenklassen $N(h_1h_2)$ und $N(g_1g_2)$ übereinstimmen.

Aus $h_1 \in Ng_1$ folgt $h_1g_1^{-1} = n_1 \in N$ und aus $h_2 \in Ng_2$ folgt $h_2g_2^{-1} = n_2 \in N$. Zu zeigen ist $Nh_1h_2 = Ng_1g_2$ oder $h_1h_2(g_1g_2)^{-1} \in N$. Nun gilt aber

$$h_1h_2(g_1g_2)^{-1} = h_1h_2g_2^{-1}g_1^{-1} = h_1n_2g_1^{-1} = h_1g_1^{-1}g_1n_2g_1^{-1} = n_1g_1n_2g_1^{-1}.$$

Da N ein Normalteiler ist, ist $g_1n_2g_1^{-1} = n_3 \in N$. Daraus folgt aber $n_1g_1n_2g_1^{-1} = n_1n_3 \in N$. Also folgt $h_1h_2(g_1g_2)^{-1} \in N$, was zu zeigen war. Deshalb ist die Verknüpfung wohldefiniert.

Nun müssen wir die Gruppenaxiome nachweisen.
Assoziativgesetz:

$$\begin{aligned} (Na \cdot Nb) \cdot Nc &= N(ab) \cdot Nc = N((ab)c) \\ Na \cdot (Nb \cdot Nc) &= Na \cdot N(bc) = N(a(bc)) = N((ab)c) \end{aligned}$$

Neutrales Element ist $Ne = N$ denn es gilt

$$Na \cdot Ne = N(ae) = Na.$$

Inverses Element: Das Inverse zu Na ist Na^{-1}, denn es gilt

$$Na \cdot Na^{-1} = N(aa^{-1}) = Ne.$$

Also ist G/N eine Gruppe. □

Bemerkung Ist G eine endliche Gruppe, so gilt für die Ordnung der Gruppe G/N:

$$|G/N| = [G : N] = |G|/|N|.$$

In Lineare Algebra I wurde bereits definiert:

Definition Es sei $f : G \to H$ ein Gruppenhomomorphismus. Dann definieren wir

$$\begin{aligned} \operatorname{Ker} f &:= \{g \in G \mid f(g) = e_H\}, \\ \operatorname{Im} f &:= \{f(g) \mid g \in G\}. \end{aligned}$$

Satz 2.21 *Es sei $f : G \to H$ ein Gruppenhomomorphismus. Dann gilt*

(i) *$\operatorname{Ker} f$ ist ein Normalteiler von G.*

(ii) *f ist genau dann injektiv, wenn $\operatorname{Ker} f = \{e_G\}$ gilt.*

(iii) *$\operatorname{Im} f$ ist eine Untergruppe von H (nicht notwendig ein Normalteiler).*

Beweis. (i) Nach Lineare Algebra I ist $\operatorname{Ker} f$ eine Untergruppe von G.
Es sei nun $a \in \operatorname{Ker} f$ und $g \in G$. Dann gilt

$$f(g^{-1}ag) = f(g^{-1})f(a)f(g) = f(g)^{-1}e_H f(g) = f(g)^{-1}f(g) = e_H.$$

Daher ist $g^{-1}ag \in \operatorname{Ker} f$. Also ist $\operatorname{Ker} f$ ein Normalteiler.
(ii) und (iii) haben wir ebenfalls bereits in der Linearen Algebra I gesehen. □

Beispiel Dies liefert einen direkten Weg, um zu schließen, dass $A_3 \lhd S_3$, ja sogar $A_n \lhd S_n$ für jedes $n \in \mathbb{N}$.

Bemerkung Wir haben eine natürliche Abbildung

$$\pi : G \to G/N, g \mapsto Ng.$$

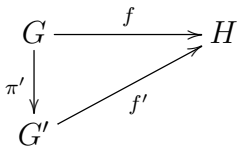
Dies ist ein Gruppenhomomorphismus mit $\operatorname{Ker} \pi = N$. Man nennt π die *kanonische Projektion.*

Bemerkung Wir haben im obigen Satz gesehen, dass der Kern eines Gruppenhomomorphismus stets ein Normalteiler ist. Davon gilt auch die Umkehrung. Ist nämlich $N \lhd G$, dann ist $N = \operatorname{Ker} \pi$ wobei

$$\pi : G \to G/N$$

die kanonische Projektion ist.

Bemerkung Wir können die Quotientengruppe auch über eine universelle Eigenschaft definieren. Dazu sei $N \lhd G$. Gesucht ist eine Gruppe G', zusammen mit einem Homomorphismus $\pi' : G \to G'$, so dass folgendes gilt: ist $f : G \to H$ ein Gruppenhomorphismus mit $N \subset \operatorname{Ker} f$ dann gibt es genau einen Homomorphismus $f' : G' \to H$ mit $f = f' \circ \pi'$. In anderen Worten, wir fordern, dass das Diagramm



kommutiert. Man sagt dazu auch, dass f über G' faktorisiert.

Man kann dann zeigen, dass es eine solches Paar $(G', \pi' : G \to G')$ stets gibt, und dass $G' \cong N/G$ ist, wobei unter dieser Identifikation die Abbildung π' mit der kanonischen Projektion π identifiziert wird.

Beispiel Die Gruppe $\mathbb{Z}_n$ ist die Quotientengruppe von $\mathbb{Z}$ nach der Untergruppe $n\mathbb{Z} := \{nk \mid k \in \mathbb{Z}\}$.

Beweis. Da $\mathbb{Z}$ abelsch ist, ist jede Untergruppe ein Normalteiler. Es gilt

$$a \equiv b \bmod n\mathbb{Z} \Leftrightarrow a - b \in n\mathbb{Z} \Leftrightarrow n|(a-b) \Leftrightarrow a \equiv b \bmod n.$$

Also gilt $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ und die Verknüpfung auf $\mathbb{Z}_n$ ist definiert durch $[a]+[b] = [a+b]$. □

Die Gruppe $\mathbb{Z}_n$ ist eine zyklische Gruppe, die von $[1]$ erzeugt wird. Nach Satz 2.6 ist $\mathbb{Z}_n$ isomorph zu C_n. Wenn es nicht zur Verwirrung führt, bezeichnen wir die Elemente von $\mathbb{Z}_n$ auch durch $0, 1, 2, \ldots, n-1$ anstelle von $[0], [1], [2], \ldots, [n-1]$ oder auch $\overline{0}, \overline{1}, \ldots, \overline{n-1}$.

Satz 2.22 (Homomorphiesatz) *Es sei $f : G \to H$ ein Gruppenhomomorphismus. Dann gilt*

$$G/\operatorname{Ker} f \cong \operatorname{Im} f.$$

Beweis. Es sei $K = \operatorname{Ker} f$. Wir definieren eine Abbildung $\psi : G/K \to \operatorname{Im} f$ durch $\psi(Kg) = f(g)$. Wir müssen zeigen:

(a) ψ ist wohldefiniert.

(b) ψ ist ein Gruppenhomomorphismus.

(c) ψ ist injektiv.

(d) ψ ist surjektiv.

Zu (a): Hierzu ist zu zeigen: Aus $Kg = Kg'$ folgt $f(g) = f(g')$. Es sei $Kg = Kg'$ für ein $g' \in G$. Dann gilt $g'g^{-1} = k \in K$. Daraus folgt

$$f(g') = f(kg) = f(k)f(g) = e_H f(g) = f(g).$$

Also ist ψ wohldefiniert.

Zu (b):

$$\psi(Kg_1Kg_2) = \psi(K(g_1g_2)) = f(g_1g_2) = f(g_1)f(g_2) = \psi(Kg_1)\psi(Kg_2).$$

Zu (c):

$$\psi(Kg) = e_H \Leftrightarrow f(g) = e_H \Leftrightarrow g \in K \Leftrightarrow Kg = K = Ke.$$

Also besteht der Kern von ψ nur aus der Rechtsnebenklasse K, die das neutrale Element von G/K ist. Daher ist ψ injektiv.

Zu (d): Nach Definition von ψ gilt $\operatorname{Im}\psi = \operatorname{Im} f$. Also ist ψ surjektiv. □

Beispiel Für den Quotienten der symmetrischen Gruppe nach der alternierenden Gruppe gilt:

$$S_n/A_n \cong \{\pm 1\} \cong \mathbb{Z}_2.$$

Der Isomorphismus wird durch die Funktion sign induziert.

Produkte

Wenn man zwei Mengen M und N gegeben hat, dann kann man ihr kartesisches Produkt $M \times N := \{(x, y) \mid x \in M, y \in N\}$ bilden. Wir wollen nun zeigen, dass man auf dem kartesischen Produkt zweier Gruppen in natürlicher Weise eine Gruppenstruktur definieren kann.

Definition Es seien G und H zwei Gruppen. Dann definieren wir auf $G \times H$ eine Verknüpfung $*$ wie folgt

$$(g_1, h_1) * (g_2, h_2) = (g_1 g_2, h_1 h_2).$$

Man kann leicht zeigen, dass $G \times H$ mit dieser Verknüpfung eine Gruppe bildet. Das neutrale Element ist (e_G, e_H) und das inverse Element zu (g, h) ist (g^{-1}, h^{-1}). Die Gruppe $G \times H$ heißt das *direkte Produkt* der Gruppen G und H.

Beispiel Wir betrachten die Gruppe $\mathbb{Z}_2 \times \mathbb{Z}_2$. Die Gruppentafel sieht wie folgt aus

$*$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

Daraus folgt, dass die Gruppe $\mathbb{Z}_2 \times \mathbb{Z}_2$ isomorph zur Kleinschen Vierergruppe ist. (Insbesondere sind beide Gruppen abelsch.)

Wir haben bereits gesehen, dass die Kleinsche Vierergruppe keine zyklische Gruppe ist. Daraus folgt $\mathbb{Z}_2 \times \mathbb{Z}_2 \ncong \mathbb{Z}_4$. Es gilt aber:

Satz 2.23 *Es seien m und n teilerfremde positive ganze Zahlen. Dann gilt*

(i) $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$,

(ii) $\mathbb{Z}_{mn}^* \cong \mathbb{Z}_m^* \times \mathbb{Z}_n^*$.

Beweis. Die Bijektion der Mengen haben wir schon in Korollar 1.32 und Korollar 1.35 gesehen. Wir geben trotzdem noch einmal das vollständige Argument, nun mit Gruppenstruktur:

Wir definieren $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ durch $f([r]) = ([r], [r])$. Diese Abbildung ist wohldefiniert, denn aus $r \equiv r' \bmod mn$ folgt $r \equiv r' \bmod m$ und $r \equiv r' \bmod n$.

Aus dem chinesischen Restsatz 1.31 folgt, dass diese Abbildung Bijektionen

$$\begin{aligned} \mathbb{Z}_{mn} &\xrightarrow{\cong} \mathbb{Z}_m \times \mathbb{Z}_n \text{ und} \\ \mathbb{Z}_{mn}^* &\xrightarrow{\cong} \mathbb{Z}_m^* \times \mathbb{Z}_n^* \end{aligned}$$

induziert.

Aus

$$f([r]+[s]) = f([r+s]) = ([r+s],[r+s]) = ([r],[r])+([s],[s]) = f([r])+f([s])$$

für $[r],[s] \in \mathbb{Z}_{mn}$ folgt, dass f ein Gruppenhomomorphismus und damit ein Isomorphismus ist. Dies beweist Teil (i).

Weiterhin gilt

$$f([r][s]) = f([rs]) = ([rs],[rs]) = ([r],[r]) \cdot ([s],[s]) = f([r]) \cdot f([s])$$

für $[r],[s] \in \mathbb{Z}_{mn}^*$. Daraus folgt, dass f einen Gruppenhomomorphismus $\mathbb{Z}_{mn}^* \to \mathbb{Z}_m^* \times \mathbb{Z}_n^*$ induziert. Das beweist (ii). □

Wie beenden diesen Abschnitt mit dem *Struktursatz für endlich erzeugte abelsche Gruppen*, den wir hier nur zitieren.

Definition Eine Gruppe G heißt *endlich erzeugt*, wenn es eine endliche Teilmenge $A \subset G$ gibt, so dass jedes Element g in G als endliches Produkt von Elementen in A geschrieben werden kann.

Beispiel Beispiele sind die Gruppe $\mathbb{Z}$ und alle endlichen Gruppen, sowie Produkte endlich erzeugter Gruppen, aber/also auch $\mathbb{Z}[i]$ mit der Addition (Erzeuger etwa $1, i$).

Theorem 2.24 *Jede endlich erzeugte abelsche Gruppe G ist von der Form*

$$G \cong \mathbb{Z}^r \times \mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \ldots \times \mathbb{Z}_{p_k^{n_k}}$$

wobei $r \geq 0$, $p_1 \leq p_2 \leq \ldots \leq p_k$ eindeutig bestimmte Primzahlen sind und $n_1, \ldots, n_k \in \mathbb{N}$.

Bemerkung Man nennt r den *Rang* der Gruppe G. Eine Gruppe G mit $G \cong \mathbb{Z}^r$ heißt *freie abelsche Gruppe* vom *Rang* r. Ferner definiert man den *Torsionsanteil* der Gruppe G durch

$$\mathrm{Tors}(G) = G_{\mathrm{tor}} = \{g \in G \mid g \text{ hat endliche Ordnung}\}.$$

Dies ist eine Untergruppe von G und $G_{\mathrm{tor}} \cong \mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \ldots \times \mathbb{Z}_{p_k^{n_k}}$. Es gibt dagegen im allgemeinen keine kanonische Untergruppe von G, welche isomorph zu der Gruppe $\mathbb{Z}^r$ ist.

Speziell die Berechnung des Ranges einer endlich erzeugten abelschen Gruppe kann in konkreten Fällen nicht-trivial sein. Man kann hier an elliptische Kurven mit ihren Anwendungen in der Kryptographie denken, aber auch an den einfachsten Fall des Dirichletschen Einheitensatzes:

Ausblick Algebraische Zahlentheorie Sei $d \in \mathbb{Z}$ quadratfrei, $d \neq 0, 1$. Analog zu $\mathbb{Z}[i]$ betrachten wir den Ring $\mathbb{Z}[\sqrt{d}]$ mit Addition und Multiplikation wie in $\mathbb{R}$ oder $\mathbb{C}$ (s. nächster Abschnitt). Die Einheitengruppe $\mathbb{Z}[\sqrt{d}]^\times$ ist abelsch und endlich erzeugt von Rang $r = 0$, falls $d < 0$, bzw. $r = 1$, falls $d > 0$.

2.4 Gruppenoperationen

Es sei G eine Gruppe, die wir wie immer multiplikativ schreiben. Wir betrachten nun eine Operation der Gruppe G auf einer beliebigen Menge M.

Definition Man sagt, die Gruppe G *operiert* auf der Menge M, wenn eine Abbildung

$$G \times M \to M, \quad (g, x) \mapsto gx$$

definiert ist, die folgende Eigenschaften besitzt:

(O1) $(gh)x = g(hx)$ für alle $g, h \in G$ und $x \in M$.

(O2) $ex = x$ für alle $x \in M$.

Die Menge M wird dann auch eine G-Menge genannt.

Notation $G \curvearrowright X$.

Bemerkung Jedes $g \in G$ definiert eine Abbildung (*Translation*) $T_g : M \to M$, $x \mapsto gx$. Diese Abbildung ist bijektiv, denn die Umkehrabbildung wird durch $T_{g^{-1}}$ gegeben: Es gilt

$$g^{-1}(gx) \overset{(O1)}{=} (g^{-1}g)x = ex \overset{(O2)}{=} x.$$

Diese Abbildungen haben die folgenden Eigenschaften:

$$T_e = \mathrm{id}, \quad T_{gh} = T_g T_h, \quad T_{g^{-1}} = (T_g)^{-1}.$$

Mit anderen Worten: Die Abbildung $g \mapsto T_g$ definiert einen Gruppenhomomorphismus von G in die Gruppe $\mathrm{Bij}(M, M)$ der bijektiven Abbildungen von M auf sich.

Definition Für alle $x \in M$ heißt

$$Gx := \{gx \in M \mid g \in G\} \subset M$$

die *Bahn* oder der *Orbit* von x (bezüglich G). Ist $Gx = \{x\}$, so nennt man x auch einen *Fixpunkt* von G.

Man zeigt leicht:

Lemma 2.25 *Für alle $x \in M$ ist*

$$G_x := \{g \in G \,|\, gx = x\} \subset G$$

eine Untergruppe von G.

Definition Die Untergruppe G_x heißt die *Isotropiegruppe*, *Fixgruppe* oder der *Stabilisator* von $x \in M$.

Definition Man sagt, G operiert *transitiv* auf M, wenn es ein $x \in M$ gibt mit $Gx = M$.

Definition Man sagt, G operiert *frei* auf M, wenn stets $G_x = \{e\}$ für alle $x \in M$.

Wir betrachten nun Beispiele von Gruppenoperationen.

Beispiel Die Gruppe $\mathrm{GL}(n, K)$ operiert auf K^n durch Matrizenmultiplikation:

$$\mathrm{GL}(n, K) \times K^n \to K^n, \quad (A, x) \mapsto Ax.$$

Ist diese Operation transitiv oder frei? Was ist die Isotropiegruppe von 0?

Man kann natürlich auch die analoge Wirkung von $\mathrm{GL}(n+1, K)$ auf $\mathbb{P}^n(K)$ untersuchen...

Beispiel Die Gruppe S_n operiert auf $M = \{1, \ldots, n\}$ durch Permutationen der Zahlen $1, \ldots, n$. Wir betrachten speziell $n = 3$. Was ist die Isotropiegruppe von 1?

Beispiel Jede Gruppe G operiert auf sich selbst durch Translationen:

$$G \times G \to G, \quad (g, h) \mapsto gh.$$

Wie sehen die Isotropiegruppen aus?

Definition Jede Gruppe G operiert auf sich selbst durch *Konjugation*

$$G \times G \to G, \quad (g, h) \mapsto ghg^{-1}.$$

Die Bahnen dieser Operation bezeichnet man auch als *Konjugationsklassen*.

Die Fixgruppe eines Elements $h \in G$ ist gerade der Zentralisator von h:

Definition Für ein $h \in G$ ist der *Zentralisator* $C_G(h)$ definiert durch

$$C_G(h) := \{g \in G \,|\, gh = hg\}.$$

Das *Zentrum* Z der Gruppe G ist die Untergruppe

$$Z := Z(G) := \{g \in G \,|\, gh = hg \text{ für alle } h \in G\} = \bigcap_{h \in G} C_G(h).$$

Beispiel Das Zentrum der allgemeinen linearen Gruppe $\mathrm{GL}(n, \mathbb{R})$ ist

$$Z(\mathrm{GL}(n; \mathbb{R})) = \{M \mid M = cE_n,\ c \in \mathbb{R}^*\}.$$

In dem folgenden Hilfssatz stellen wir einige offensichtliche Eigenschaften von Gruppenoperationen zusammen.

Lemma 2.26 *Die Gruppe G operiere auf der Menge M. Dann gilt:*

(i) *Eine Bahn ist eine Äquivalenzklasse bezüglich der Äquivalenzrelation*

$$x \sim y :\Leftrightarrow \exists g \in G : y = gx.$$

(ii) *Für alle $g, h \in G$ und $x \in M$ gilt*

$$gx = hx \Leftrightarrow g \text{ und } h \text{ liegen in der gleichen Linksnebenklasse von } G_x.$$

(iii) *Die Anzahl $|Gx|$ der Elemente der Bahn Gx ist der Index $[G : G_x]$.*

(iv) *Für alle $x, y \in M$ und $g \in G$ mit $gx = y$ gilt*

$$G_y = gG_xg^{-1}.$$

(v) *Die Isotropiegruppe G_x ist genau dann ein Normalteiler in G, wenn $G_y = G_x$ für alle $y \in Gx$ gilt.*

Beweis. (i) ist klar.

(ii) Es gilt:

$$gx = hx \Leftrightarrow h^{-1}gx = x \Leftrightarrow h^{-1}g \in G_x \Leftrightarrow g \in hG_x.$$

(iii) Aus (ii) folgt, dass wir eine Bijektion zwischen den Linksnebenklassen von G_x und den Elementen der Bahn Gx haben.

(iv) Es gilt:

$$h \in G_y \Leftrightarrow h \in G_{gx} \Leftrightarrow hgx = gx \Leftrightarrow g^{-1}hgx = x \Leftrightarrow h \in gG_xg^{-1}.$$

(v) folgt sofort aus (iv). □

Satz 2.27 (Klassenformel) *Es sei R ein Repräsentantensystem der Bahnen für die Operation der Gruppe G auf der Menge M. Dann gilt*

$$|M| = \sum_{x \in R} [G : G_x].$$

Für die Operation durch Konjugation ergibt sich:

Korollar 2.28 *Es sei R ein Repräsentantensystem der Konjugationsklassen der Gruppe G. Dann gilt*

$$|G| = \sum_{h \in R} [G : C_G(h)].$$

Eine Konjugationsklasse besteht genau dann nur aus einem Element g, wenn $g \in Z$.

Beispiel Es sei K ein Körper und der Polynomring $K[x_1, \ldots, x_n]$ gegeben. Betrachte

$$M := \left\{ \prod_{1 \le i < j \le n} (x_j - x_i), - \prod_{1 \le i < j \le n} (x_j - x_i) \right\}.$$

Diese Menge besteht aus zwei Polynomen. Die symmetrische Gruppe S_n operiert auf dieser Menge durch Permutation der Indizes. Ein $\sigma \in S_n$ operiert wie folgt:

$$\pm \prod_{1 \le i < j \le n} (x_j - x_i) \mapsto \pm \prod_{1 \le i < j \le n} (x_{\sigma(j)} - x_{\sigma(i)}).$$

Diese Operation ist transitiv, denn die Transposition (12) bewirkt eine Vorzeichenänderung in genau einem Faktor. Es gibt also nur eine Bahn M. Die Isotropiegruppe jedes Elements von M ist die alternierende Gruppe A_n. Nach Lemma 2.26 (v) ist A_n ein Normalteiler in S_n und aus Satz 2.27 erhalten wir wieder $[S_n : A_n] = 2$.

Beispiel Hier sei noch einmal auf einen Zusammenhang mit Linearer Algebra 2 hingewiesen. Die Gruppe $\mathrm{GL}(n; \mathbb{C})$ operiert auf dem Raum $Mat(n; \mathbb{C})$ der $(n \times n)$-Matrizen ebenfalls duch Konjugation

$$(A, M) \mapsto AMA^{-1}.$$

Die Frage nach der Klassifikation der Bahnen unter dieser Operation ist genau die Frage nach der *Jordanschen Normalform*. Hierdurch werden für jede Bahn explizite Repräsentanten bestimmt.

2.5 Endliche einfache Gruppen

Die elementaren Bausteine von Gruppen sind die sogenannten einfachen Gruppen.

Definition Eine Gruppe G heißt *einfach* wenn sie nicht trivial ist und die einzigen Normalteiler von G die Gruppe $\{e\}$ und G selbst sind.

Beispiel Die folgenden Gruppen sind einfach:

(1) Die zyklischen Gruppen $\mathbb{Z}_p$ von Primzahlordnung-

(2) Die alternierenden Gruppen A_n für $n \geq 5$.

Bemerkung Zur Begründung der Terminologie 'Bausteine': Ist G eine endliche Gruppe mit Normalteiler $N \neq \{e\}, G$, so können wir versuchen, G anhand der Untergruppe N und der Faktorgruppe G/N zu verstehen (oder 'zusammenzubauen'). Üblicherweise geschieht dies mittels der exakten Sequenz

$$1 \to N \to G \to G/N \to 1.$$

In der Folge kann man dann untersuchen, ob N oder G/N einfach sind (da wir mit endlichen Gruppen arbeiten, führen endliche viele Schritte auf einfache Gruppen).

Man kann nun fragen, ob es möglich ist, alle einfachen endlichen Gruppen zu klassifizieren. In der Tat gibt es heute eine vollständige Klassifikation dieser Gruppen. Diese setzt sich aus einer Vielzahl von Einzelarbeiten zusammen.

Theorem 2.29 *Es gibt genau die folgenden endlichen einfachen Gruppen:*

(i) *Zykliche Gruppen von Primzahlordnung.*

(ii) *Die alternierenden Gruppen $A_n, n \geq 5$.*

(iii) *Gruppen vom Lietyp (16 Familien).*

(iv) *26 sporadische Gruppen.*

Beispiel Ein Beispiel für eine Gruppe vom Lietyp sind die Gruppen $\mathrm{PSL}(n, \mathbb{Z}_p), n \geq 2, p \in \mathbb{P}$ mit den Ausnahmen $n = 2, p = 2, 3$.

Beispiel Die größte einfache sporadische Gruppe ist das von Fischer und Griess 1973 gefundene Monster. Die Ordnung dieser Gruppe beträgt $2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$.

Kapitel 3

Ringe

3.1 Ringaxiome

Definition Eine Menge R zusammen mit zwei Verknüpfungen $+$ und $\cdot$ heißt *Ring mit* 1 genau dann, wenn die folgenden Eigenschaften erfüllt sind:

(AG) R bildet zusammen mit der Verknüpfung $+$ eine abelsche Gruppe.

(MA) Für alle $a, b, c \in R$ gilt

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

(*Assoziativgesetz der Multiplikation*).

(D) Für alle $a, b, c \in R$ gilt

$$a \cdot (b + c) = a \cdot b + a \cdot c \text{ und } (b + c) \cdot a = b \cdot a + c \cdot a$$

(*Distributivgesetz*).

(MN) Es existiert ein Element $1 \in R$, so dass für alle $a \in R$ gilt

$$1 \cdot a = a \cdot 1 = a$$

(*Existenz der 1*).

Ein Ring mit 1 R heißt *kommutativ* genau dann, wenn gilt:

(MK) Für alle $a, b \in R$ gilt

$$a \cdot b = b \cdot a$$

(*Kommutativgesetz der Multiplikation*).

Beispiel $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sind kommutative Ringe mit 1.

Beispiel $\mathrm{Mat}(n,n)$ ist ein Ring mit 1, der für $n > 1$ nicht kommutativ ist.

Beispiel $\mathbb{Z}_n$ ist ein kommutativer Ring mit 1, wobei die Addition und Multiplikation durch $[x]+[y]=[x+y]$ und $[x]\cdot[y]=[x\cdot y]$ für $x,y\in\mathbb{Z}$ definiert sind.

Beweis. Wir wissen bereits, dass $\mathbb{Z}_n$ mit der Addition eine abelsche Gruppe bildet.

Nach Lemma 1.26 ist die Multiplikation wohldefiniert und nach Satz 1.27 (1.5) – (1.8) ist $\mathbb{Z}_n$ ein kommutativer Ring mit 1. □

Verknüpfungstafeln für $\mathbb{Z}_4$:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Beispiel Es sei $\mathbb{Q}(\sqrt{2}) := \{a+b\sqrt{2} \mid a,b\in\mathbb{Q}\} \subset \mathbb{R}$. Dann ist $\mathbb{Q}(\sqrt{2})$ ein kommutativer Ring mit 1.

Beweis. Zunächst müssen wir zeigen, dass $+$ und $\cdot$ Verknüpfungen auf $\mathbb{Q}(\sqrt{2})$ definieren. Es seien $a,b,c,d\in\mathbb{Q}$. Dann gilt

$$(a+b\sqrt{2})+(c+d\sqrt{2}) = (a+c)+(b+d)\sqrt{2} \in \mathbb{Q}(\sqrt{2}),$$

da $(a+b),(c+d)\in\mathbb{Q}$. Ebenso

$$(a+b\sqrt{2})\cdot(c+d\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2} \in \mathbb{Q}(\sqrt{2}).$$

Nun müssen wir zeigen, dass die Axiome eines kommutativen Ringes mit 1 erfüllt sind. Das neutrale Element der Addition ist $0 = 0+0\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. Das additive Inverse eines Elements $a+b\sqrt{2}$ ist $(-a)+(-b)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. Die 1 ist $1 = 1+0\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. Die restlichen Axiome gelten in $\mathbb{Q}(\sqrt{2})$, da sie in $\mathbb{R}$ gelten. □

Aus den Ringaxiomen leitet man die folgenden Eigenschaften eines Ringes ab.

Satz 3.1 (Vorzeichenregeln) *Es sei R ein Ring mit 1. Dann gilt für alle $a,b\in R$:*

(i) $a \cdot 0 = 0 \cdot a = 0$.

(ii) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$.

(iii) $(-a) \cdot (-b) = a \cdot b$.

(iv) $(-1) \cdot a = -a$.

(v) $(-1) \cdot (-1) = 1$.

Beweis. (i) $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$. Addition von $-(a \cdot 0)$ auf beiden Seiten ergibt $0 = a \cdot 0$. Analog zeigt man $0 \cdot a = 0$.

(ii) $a \cdot (-b) + a \cdot b = a \cdot (-b + b) = a \cdot 0 \overset{\text{(i)}}{=} 0 \Rightarrow a \cdot (-b) = -(a \cdot b)$.
Analog $(-a) \cdot b = -(a \cdot b)$.

(iii) $(-a) \cdot (-b) \overset{\text{(ii)}}{=} -(a \cdot (-b)) \overset{\text{(ii)}}{=} -(-(a \cdot b)) = a \cdot b$.

(iv) $(-1) \cdot a \overset{\text{(ii)}}{=} -(1 \cdot a) = -a$.

(v) $(-1) \cdot (-1) \overset{\text{(iii)}}{=} 1 \cdot 1 = 1$. □

Bemerkung Ist $1 = 0$, so gilt $R = \{0\}$. Denn für $a \in R$ gilt $a = a \cdot 1 = a \cdot 0 = 0$. Der Ring $R = \{0\}$ heißt der *triviale Ring*. Alle anderen Ringe heißen *nichttrivial*.

3.2 Integritätsbereiche und Körper

Gilt in einem Ring mit 1

$$a \cdot b = 0 \Rightarrow a = 0 \text{ oder } b = 0?$$

Beim Beispiel $\mathbb{Z}_4$ haben wir gesehen $[2] \cdot [2] = [0]$.

Definition Es sei R ein kommutativer Ring mit 1. Ein Element $a \in R$, $a \neq 0$, heißt *Nullteiler*, falls es ein $b \in R$, $b \neq 0$, gibt mit $a \cdot b = 0$.

Beispiel $R = \mathbb{Z}_4$, $[2]$ ist ein Nullteiler, denn $[2] \cdot [2] = [0]$.

Definition Ein nichttrivialer kommutativer Ring R mit 1 heißt *Integritätsbereich*, falls R keine Nullteiler hat.

Beispiel (1) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sind Integritätsbereiche.
(2) $\mathbb{Z}_4$ ist kein Integritätsbereich, da $[2]$ ein Nullteiler von $\mathbb{Z}_4$ ist.
(3) Allgemeiner ist $\mathbb{Z}_n$ kein Integritätsbereich, wenn n keine Primzahl ist.

Anwendung Seien R, R' kommutative Ringe mit 1, wobei R' Integritätsbereich sei. Existiert ein Ringmonomorphismus

$$R \hookrightarrow R'$$

(s.u.), so ist auch R Integritätsbereich.

Satz 3.2 (Kürzungsregel) *Ist R ein Integritätsbereich und $a \in R$, $a \neq 0$, dann gilt für alle $b, c \in R$:*

$$a \cdot b = a \cdot c \Rightarrow b = c.$$

Anwendung In einem Integritätsbereich R gilt

$$x^2 = y^2 \implies x = \pm y.$$

Beweis. Aus $a \cdot b = a \cdot c$ folgt $a \cdot (b - c) = a \cdot b - a \cdot c = 0$. Da $a \neq 0$ kein Nullteiler ist, folgt $b - c = 0$, also $b = c$. □

Definition Ein *Körper* ist ein Ring R mit 1, bei dem $(R \setminus \{0\}, \cdot)$ eine abelsche Gruppe bildet, d.h. R ist ein nichttrivialer kommutativer Ring mit 1 mit der Eigenschaft

(MI) Für alle $a \in R$ mit $a \neq 0$ gibt es ein $a^{-1} \in R$ mit

$$a \cdot a^{-1} = 1$$

(*Existenz des multiplikativen Inversen*).

Beispiel (1) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sind Körper.

(2) $\mathbb{Z}$ und $\mathbb{Z}_4$ sind keine Körper.

(3) $\mathbb{Q}(\sqrt{2})$ ist ein Körper. Ist $a + b\sqrt{2} \neq 0$, so ist auch $a - b\sqrt{2} \neq 0$ und es gilt

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a}{a^2 - 2b^2} + \left(-\frac{b}{a^2 - 2b^2}\right)\sqrt{2} \in \mathbb{Q}(\sqrt{2}).$$

Formal sollten wir hier noch prüfen, dass der Nenner nicht 0 werden kann (etwa weil $\mathbb{Q}(\sqrt{2})$ ein Integritätsbereich ist). Dies folgt direkt aus dem folgenden Lemma 3.3.

(4) Ist d quadratfrei, dann ist $\mathbb{Q}(\sqrt{d})$ ein Körper. Dies folgt mit derselben Argumentation zusammen mit der Feststellung, dass $a^2 - db^2 \neq 0$ ist falls a und b nicht beide Null sind. Man nennt dann $\mathbb{Q}(\sqrt{d})$ einen *reell-quadratischen Zahlkörper*.

Lemma 3.3 $\sqrt{2} \notin \mathbb{Q}$.

Beweis. Nehmen wir an, dass

$$\sqrt{2} = \frac{a}{b} \in \mathbb{Q}, \quad \text{d.h.} \quad a^2 = 2b^2 \tag{3.1}$$

wobei o.B.d.A. $b \in \mathbb{N}$. Betrachte die Primfaktorzerlegungen

$$a = \prod_{p \in \mathbb{P}} p^{e_p}, \quad b = \prod_{p \in \mathbb{P}} p^{e'_p}$$

wobei natürlich fast alle $e_p, e'_p \in \mathbb{N}_0$ verschwinden. Auf (3.1) angewandt erhalten wir

$$\prod_{p \in \mathbb{P}} p^{2e_p} = 2 \prod_{p \in \mathbb{P}} p^{2e'_p}.$$

Der Vergleich der Potenzen von 2 liefert mit

$$2e_2 = 1 + 2e'_2$$

eine Gleichung, die sich nicht in $\mathbb{Z}$ lösen läßt, Widerspruch. □

Bemerkung Das selbe Beweisprinzip lässt sich auf $\sqrt{d}$ für jedes $d \in \mathbb{N}$ ($d > 1$) übertragen, welches quadratfrei ist, d.h. es gibt einen Primteiler p mit ungerader Vielfachheit ($2 \nmid e_p$).

Satz 3.4 *Ein Körper ist ein Integritätsbereich.*

Beweis. Es sei K ein Körper und $a, b \in K$ mit $a \cdot b = 0$. Ist $a \neq 0$, so existiert ein inverses Element $a^{-1} \in K$. Also

$$b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0.$$

□

Anwendung Lässt sich ein Ring R in einen Körper einbetten, so ist R ein Integritätsbereich.

Satz 3.5 *Ein endlicher Integritätsbereich ist ein Körper.*

Beweis. Es sei R ein endlicher Integritätsbereich. Wir müssen zeigen, dass jedes Element $a \neq 0$ ein multiplikatives Inverses besitzt. Dazu betrachten wir die Abbildung

$$\begin{array}{rccc} l_a : & R & \longrightarrow & R \\ & x & \longmapsto & a \cdot x \end{array}.$$

Diese Abbildung ist injektiv:

$$l_a(x) = l_a(y) \Leftrightarrow a \cdot x = a \cdot y \overset{\text{Satz } 3.2}{\Rightarrow} x = y.$$

Da R endlich ist, ist l_a auch surjektiv. Also gibt es ein $b \in R$ mit $l_a(b) = a \cdot b = 1$. □

Satz 3.6 *$\mathbb{Z}_n$ ist genau dann ein Körper, wenn n eine Primzahl ist.*

Beweis. Es sei zunächst n eine Primzahl. Nach dem vorherigen Satz reicht es zu zeigen, dass $\mathbb{Z}_n$ ein Integritätsbereich ist. Es sei $[a] \cdot [b] = [0]$ in $\mathbb{Z}_n$. Dann folgt $n|ab$. Da n eine Primzahl ist, gilt $n|a$ oder $n|b$. Also gilt $[a] = [0]$ oder $[b] = [0]$. Also besitzt $\mathbb{Z}_n$ keine Nullteiler.

Es sei nun n keine Primzahl. Dann können wir $n = rs$ schreiben, wobei r und s ganze Zahlen mit $1 < r < n$ und $1 < s < n$ sind. Dann gilt $[r] \neq [0]$ und $[s] \neq [0]$, aber $[r] \cdot [s] = [rs] = [0]$. Also besitzt $\mathbb{Z}_n$ Nullteiler und ist kein Körper. □

Definition Es sei R ein kommutativer Ring mit 1. Ein Element $a \in R$ heißt *Einheit*, falls es ein Element $b \in R$ mit $ab = 1$ gibt. Die Menge aller Einheiten in einem kommutativen Ring R wird mit R^* bezeichnet.

Beispiel (a) In einem Körper K sind alle von Null verschiedenen Elemente Einheiten und es gilt $K^* = K \setminus \{0\}$.

Umgekehrt ist ein Ring $R \neq \{0\}$ genau dann ein Körper, wenn $R^\times = R \setminus \{0\}$.

(b) Die Einheiten in $\mathbb{Z}$ sind ± 1.

Interpretation der Primfaktorzerlegung: Faktoren sind Primzahlen und Einheiten.

(c) Die Einheiten von $\mathbb{Z}_n$ sind gerade die primen Restklassen mod n, also ist für $R = \mathbb{Z}_n$ die Menge der Einheiten $R^* = \mathbb{Z}_n^*$.

Prüfe: jedes $0 \neq x \in \mathbb{Z}_n$ ist entweder Einheit oder Nullteiler.

Satz 3.7 *In einem kommutativen Ring R mit 1 bildet die Menge R^* der Einheiten mit der Multiplikation als Verknüpfung eine abelsche Gruppe.*

Beweis. Es seien $a_1, a_2 \in R^*$ und $b_1, b_2 \in R$ mit $a_1 b_1 = a_2 b_2 = 1$. Dann gilt $(a_1 a_2)(b_1 b_2) = 1$. Also ist $a_1 a_2$ eine Einheit in R. Die Gruppenaxiome folgen sofort. □

3.3 Polynomringe

Definition Es sei R ein kommutativer Ring mit 1. Ein *Polynom* über dem Ring R ist ein Ausdruck

$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n,$$

wobei $a_0, a_1, a_2, \ldots, a_n \in R$ und $n \in \mathbb{N}$. Hier ist x eine Unbestimmte. Das Element a_i heißt der *Koeffizient* von x^i in $p(x)$. Einen Term $0x^i$ lassen wir weg und für $1x^i$ schrieben wir einfach x^i. Zwei Polynome sind gleich, wenn alle ihre Koeffizienten gleich sind. Die größte Zahl n mit $a_n \neq 0$ heißt der *Grad* des Polynoms $p(x)$, in Zeichen $n = \operatorname{grad} p(x)$ oder $n = \deg p$. Sind alle Koeffizienten von $p(x)$ gleich Null, so heißt $p(x)$ das *Nullpolynom*. Den Grad des Nullpolynoms definieren wir als $-\infty$.

Definition Die Menge aller Polynome in x über dem kommutativen Ring R mit 1 wird mit $R[x]$ bezeichnet. Also

$$R[x] := \{a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \mid n \in \mathbb{N},\ a_i \in R,\ i = 0, \ldots, n\}.$$

Wir definieren eine Addition und Multiplikation von Polynomen

$$p(x) = \sum_{i=0}^{n} a_i x^i \quad \text{und} \quad q(x) = \sum_{i=0}^{m} b_i x^i$$

durch

$$p(x) + q(x) = \sum_{i=0}^{\max(m,n)} (a_i + b_i) x^i,$$

$$p(x) \cdot q(x) = \sum_{k=0}^{m+n} c_k x^k, \quad \text{wobei} \quad c_k = \sum_{i=0}^{k} a_i b_{k-i}.$$

Die Menge $R[x]$ zusammen mit dieser Addition und Multiplikation bildet einen kommutativen Ring mit 1, der der *Polynomring mit Koeffizienten aus* R heißt. Die Null ist das Nullpolynom und die 1 das konstante Polynom 1.

Etwas formaler kann als die Menge aller Polynome mit dem Raum der Abbildungen

$$\operatorname{Abb}[\mathbb{N}_0, R] = \{f : \mathbb{N}_0 \to R \mid f(i) \neq 0 \,\text{für nur endlich viele}\, i\}$$

definieren. Ist n die maximale Zahl mit $f(n) \neq 0$, dann setzt man $a_i = f(i)$ für $i = 0, \ldots n$ und schreibt

$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n.$$

Ein Polynom $p \in R[x]$ definiert eine *Polynomfunktion*

$$p : R \to R, r \mapsto p(r).$$

Es kann passieren, dass zwar $p(x) \neq 0$ als Polynomfunktion gilt, jedoch die zugehörige Polynumfunktion die Nullfunktion ist. Ein Beispiel erhält an für endliche Ringe R, indem man

$$p(x) = \prod_{a \in R} (x - a)$$

setzt. Wenn R ein unendlicher Integritätsbereich ist, dann kann man Polynome mit Polynomfunktionen identifizieren (vgl. LAII, wo wir das für Körper hergeleitet haben).

Satz 3.8 (Gradformel) *Wenn R ein Integritätsbereich ist und $p(x)$ und $q(x)$ Polynome in $R[x]$ sind, so gilt*

$$\operatorname{grad}(p(x) \cdot q(x)) = \operatorname{grad} p(x) + \operatorname{grad} q(x).$$

Beweis. Ist eins der beiden Polynome das Nullpolynom, so ist auch $p(x) \cdot q(x)$ das Nullpolynom. In diesem Fall ist die Behauptung richtig, da das Nullpolynom den Grad $-\infty$ hat.

Andernfalls sei $\operatorname{grad} p(x) = n$, $\operatorname{grad} q(x) = m$ und $p(x) = a_0 + \cdots + a_n x^n$, $q(x) = b_0 + \cdot + b_m x^m$, wobei $a_n \neq 0$, $b_m \neq 0$. Dann ist der Koeffizient der größten Potenz von x in $p(x) \cdot q(x)$ gleich $a_n b_m$. Es gilt aber $a_n b_m \neq 0$, da R keine Nullteiler besitzt. Also gilt $\operatorname{grad}(p(x) \cdot q(x)) = m + n$. □

Korollar 3.9 *Es sei R ein kommutativer Ring mit 1. Der Polynomring $R[x]$ ist genau dann ein Integritätsbereich, wenn R ein Integritätsbereich ist.*

Beweis. Indem wir jedem $a \in R$ das konstante Polynom $a \in R[x]$ zuordnen, sehen wir, dass $R \subset R[x]$. Wenn also $R[x]$ keine Nullteiler enthält, dann enthält erst recht R keine Nullteiler. Es sei umgekehrt R ein Integritätsbereich. Sind nun $p(x)$ und $q(x)$ Polynome aus $R[x]$, die verschieden vom Nullpolynom sind, so ist nach der Gradformel auch $p(x) \cdot q(x)$ von Null verschieden. Also enthält $R[x]$ keine Nullteiler. □

Korollar 3.10 *In einem Integritätsbereich R gilt $R[x]^\times = R^\times$.*

Wenn a und b ganze Zahlen mit $b \neq 0$ sind, so gibt es eindeutig bestimmte ganze Zahlen q und r, so dass gilt

$$a = qb + r \quad \text{und} \quad 0 \leq r < |b|.$$

Die Zahl q heißt der *Quotient* bei Division von a durch b und r heißt der *Rest*. Wir betrachten nun Ringe, in denen eine solche *Division mit Rest* möglich ist.

Definition Ein Integritätsbereich R heißt ein *euklidischer Ring*, wenn es eine Abbildung $d : R \setminus \{0\} \to \mathbb{N}$ in die Menge der natürlichen Zahlen gibt, so dass gilt:

(DmR) Für alle $a, b \in R$ mit $b \neq 0$ gibt es Elemente $q, r \in R$ mit

$$a = qb + r, \quad \text{wobei entweder } r = 0 \text{ oder } d(r) < d(b).$$

Beispiel $\mathbb{Z}$ ist ein euklidischer Ring, wenn wir $d(a) := |a|$ für $a \in \mathbb{Z}$, $a \neq 0$, setzen. Ein Körper K ist trivialerweise ein euklidischer Ring, wenn wir $d(a) = 1$ für alle $a \in K \setminus \{0\}$ setzen.

Satz 3.11 *Es sei K ein Körper. Dann ist der Polynomring $K[x]$ mit der Abbildung $d = \operatorname{grad}$ ein euklidischer Ring.*

Achtung: Dies gilt i.a. nicht für Polynomringe über Ringen.

Beweis. Dies folgt aus dem *Divisionsalgorithmus für Polynome*:

Behauptung Es seien $f(x), g(x) \in K[x]$ und $g(x)$ sei nicht das Nullpolynom. Dann gibt es eindeutig bestimmte Polynome $q(x), r(x) \in K[x]$, so dass

$$f(x) = q(x) \cdot g(x) + r(x),$$

wobei $\operatorname{grad} r(x) < \operatorname{grad} g(x)$.

Beweis. (a) Wir zeigen zunächst die Existenz der Polynome $q(x)$ und $r(x)$.

Ist $f(x)$ das Nullpolynom oder $\operatorname{grad} f(x) < \operatorname{grad} g(x)$, dann können wir $f(x) = 0 \cdot g(x) + f(x)$ schreiben. Es sei also $f(x) \neq 0$ und $n := \operatorname{grad} f(x) \geq \operatorname{grad} g(x)$. Wir beweisen die Behauptung durch Induktion nach n.

Induktionsanfang: Es sei $n = 0$. Dann gilt $\operatorname{grad} f(x) = \operatorname{grad} g(x) = 0$, also $f(x) = a_0$, $g(x) = b_0$. Dann ist $f(x) = (a_0 b_0^{-1}) g(x)$.

Es sei nun $g(x)$ fest. Wir nehmen an, dass die Behauptung für alle Polynome $f(x)$ mit $\operatorname{grad} f(x) < n$ gilt. Es sei $f(x) = a_0 + \cdots + a_n x^n$, $g(x) = b_0 + \cdots + b_m x^m$ mit $a_n \neq 0$, $b_m \neq 0$, $n \geq m$. Dann setze

$$\tilde{f}(x) := f(x) - a_n b_m^{-1} x^{n-m} g(x).$$

Dann gilt $\operatorname{grad} \tilde{f}(x) < n$. Nach Induktionsannahme gibt es $\tilde{q}(x)$, $r(x)$ mit

$$\tilde{f}(x) = \tilde{q}(x) \cdot g(x) + r(x), \quad \text{wobei} \quad \operatorname{grad} r(x) < \operatorname{grad} g(x).$$

Also gilt

$$f(x) = a_n b_m^{-1} x^{n-m} g(x) + \tilde{f}(x) = (a_n b_m^{-1} x^{n-m} g(x) + \tilde{q}(x)) \cdot g(x) + r(x).$$

Dies ist eine Darstellung der gewünschten Form.

(b) Wir zeigen nun die Eindeutigkeit von $q(x)$ und $r(x)$. Es sei $f(x) = q_1(x) \cdot g(x) + r_1(x) = q_2(x) \cdot g(x) + r_2(x)$ mit $\operatorname{grad} r_2(x) \leq \operatorname{grad} r_1(x) < \operatorname{grad} g(x)$. Dann gilt

$$(q_2(x) - q_1(x)) \cdot g(x) = r_1(x) - r_2(x).$$

Ist $q_2(x) - q_1(x)$ nicht das Nullpolynom, so folgt aus der Gradformel

$$\operatorname{grad}(r_1(x) - r_2(x)) = \operatorname{grad}((q_2(x) - q_1(x)) \cdot g(x)) \geq \operatorname{grad} g(x),$$

im Widerspruch zu $\operatorname{grad}(r_1(x) - r_2(x)) < \operatorname{grad} g(x)$. Also gilt $q_1(x) = q_2(x)$ und damit auch $r_1(x) = r_2(x)$. □

□

Beispiel In $\mathbb{Z}_3[x]$ gilt

$$\begin{array}{rcrcrcl|l}
x^3 & + & 2x^2 & + & & & 1 & : \; x^2 + 2 = x + 2 \\
\cline{1-7}
x^3 & + & & & 2x & & & \\
\cline{1-5}
 & & 2x^2 & + & x & + & 1 & \\
 & & 2x^2 & + & & & 1 & \\
\cline{3-5}
 & & & & x & & &
\end{array}$$

Es ist also $x^3 + 2x^2 + 1 = (x + 2)(x^2 + 2) + x$.

Korollar 3.12 *Teilt man das Polynom $f(x) \in K[x]$ durch $(x - \alpha)$, dann ergibt sich als Rest $f(\alpha)$.*

Beweis. Nach dem Divisionsalgorithmus existieren $q(x), r(x) \in K[x]$ mit $f(x) = q(x)(x - \alpha) + r(x)$, wobei $\operatorname{grad} r(x) < 1$. Also ist $r(x) = r_0 \in K$ und $f(x) = q(x)(x - \alpha) + r_0$. Setzen wir hier $x = \alpha$ ein, so erhalten wir $f(\alpha) = r_0$. □

Korollar 3.13 *Das Polynom $f(x) \in K[x]$ ist genau dann durch $(x - \alpha)$ teilbar, wenn $f(\alpha) = 0$.*

Beweis. Nach dem vorherigen Korollar gilt $f(x) = q(x)(x - \alpha) + f(\alpha)$. Also gilt $f(x) = q(x)(x - \alpha)$ genau dann, wenn $f(\alpha) = 0$. □

Definition Es sei $f(x) \in K[x]$. Ein Element $\alpha \in K$ mit $f(\alpha) = 0$ heißt *Nullstelle* oder *Wurzel* des Polynoms $f(x)$.

Satz 3.14 *Ein Polynom vom Grad $n \geq 0$ über einem Körper K hat höchstens n Wurzeln in K.*

Achtung: Dies gilt i.a. nicht für Polynome in $R[x]$, d.h. über Ringen. Prüfen Sie, was im nullteilerfreien Fall gilt!

Beweis. Wir beweisen den Satz durch Induktion nach n. Ein Polynom vom Grad 0 ist von der Form $f(x) = a_0$ mit $a_0 \neq 0$. Ein solches Polynom hat keine Nullstellen.

Wir nehmen nun an, dass der Satz für Polynome vom Grad $n-1$ gilt. Es sei $f(x) \in K[x]$ ein Polynom vom Grad n. Hat $f(x)$ keine Nullstellen, so ist der Satz richtig. Andernfalls sei α eine Nullstelle von $f(x)$. Nach dem vorhergehenden Korollar können wir dann schreiben:

$$f(x) = (x - \alpha)g(x).$$

Nach der Gradformel gilt $\operatorname{grad} g(x) = n-1$. Da K als Körper keine Nullteiler besitzt, gilt $f(\beta) = 0$ genau dann, wenn $(\beta - \alpha) = 0$ oder $g(\beta) = 0$. Also ist eine Nullstelle von $f(x)$ entweder gleich α oder eine Nullstelle von $g(x)$. Nach Induktionsannahme hat $g(x)$ höchstens $n-1$ Wurzeln in K. Also hat $f(x)$ höchstens n Wurzeln in K. □

Beispiel Der Ring $\mathbb{Z}[i] := \{a + ib \,|\, a, b \in \mathbb{Z}\}$ (der Ring der *Gaußschen ganzen Zahlen*) ist ein euklidischer Ring mit $d(a + ib) = a^2 + b^2$.

Wegen $\mathbb{Z}[i] \subset \mathbb{C}$ sieht man leicht, dass $\mathbb{Z}[i]$ ein Integritätsbereich ist.

Es seien $z, w \in \mathbb{Z}[i]$ mit $w \neq 0$. Dann gilt

$$\frac{z}{w} = c + id \quad \text{mit } c, d \in \mathbb{Q},$$

Es seien $a, b \in \mathbb{Z}$ mit $|c - a| \leq \frac{1}{2}$ und $|d - b| \leq \frac{1}{2}$. Dann gilt

$$\frac{z}{w} = a + ib + ((c - a) + i(d - b)).$$

Daraus folgt

$$z = (a + ib)w + ((c - a) + i(d - b))w$$

mit

$$\begin{aligned} d(((c - a) + i(d - b))w) &= d(((c - a) + i(d - b)))d(w) \\ &= ((c - a)^2 + (d - b)^2)d(w) \\ &\leq \left(\frac{1}{4} + \frac{1}{4}\right) d(w) < d(w). \end{aligned}$$

Also ist in $\mathbb{Z}[i]$ Division mit Rest möglich.

3.4 Der euklidische Algorithmus

Der Name "euklidischer Ring" rührt daher, dass in einem solchen Ring der euklidische Algorithmus funktioniert.

Definition Es sei R ein Ring mit 1, $a, b \in R$. Wir sagen a *teilt* b oder a ist ein *Teiler* von b, in Zeichen $a|b$, falls es ein $q \in R$ gibt mit $b = qa$.

Definition Es sei R ein Integritätsbereich und $a, b \in R$. Ein Element $g \in R$ heißt ein *größter gemeinsamer Teiler* von a und b, in Zeichen $g = \mathrm{ggT}(a, b)$, falls

(i) $g|a$ und $g|b$,

(ii) Für alle $c \in R$ gilt: Aus $c|a$ und $c|b$ folgt $c|g$.

Ein Element $k \in R$ heißt *kleinstes gemeinsames Vielfaches* von a und b, in Zeichen $k = \mathrm{kgV}(a, b)$, falls

(i) $a|k$ und $b|k$,

(ii) Für alle $c \in R$ gilt: Aus $a|c$ und $b|c$ folgt $k|c$.

Bemerkung ggT und kgV existieren i.a. nicht unbedingt (Beispiel?!). Falls sie existieren, so sind sie bis auf Einheiten eindeutig bestimmt (prüfen!).

Es sei R ein euklidischer Ring. Wir wollen einen g.g.T. zweier von Null verschiedener Elemente $a, b \in R$ bestimmen. Dies geschieht mit dem *euklidischen Algorithmus*, den wir nun beschreiben. Wir setzen zunächst $a_1 := a$, $a_2 := b$. Nun dividieren wir a_1 durch a_2. Dann erhalten wir eine Darstellung $a_1 = q_1 a_2 + a_3$ mit $d(a_3) < d(a_2)$. Ist nun $a_3 \neq 0$, so können wir im nächsten Schritt a_2 durch a_3 mit einem Rest a_4 teilen, usw. Da $d(a_2) > d(a_3) > d(a_4) > \ldots$ gilt (und $d : R \setminus \{0\} \to \mathbb{N}_0$), kommt dieser Prozeß nach endlich vielen Schritten zum Stillstand, nämlich dann, wenn der anfallende Rest Null wird. Wir erhalten also ein Schema wie folgt:

$$\begin{aligned}
a_1 &= q_1 a_2 + a_3, \quad d(a_2) > d(a_3), \\
a_2 &= q_2 a_3 + a_4, \quad d(a_3) > d(a_4), \\
&\vdots \quad \vdots \quad \vdots \\
a_{m-1} &= q_{m-1} a_m + a_{m+1}, \quad d(a_m) > d(a_{m+1}), \\
a_m &= q_m a_{m+1}
\end{aligned}$$

Hierbei gilt $a_i \neq 0$, $i = 1, \ldots, m+1$.

Behauptung a_{m+1} ist ein g.g.T. von a_1 und a_2.

Beweis. (i) Aus der letzten Zeile folgt $a_{m+1}|a_m$, aus der vorletzten $a_{m+1}|a_{m-1}$, usw. Aus der zweiten und ersten Zeile folgt schließlich $a_{m+1}|a_2$ und $a_{m+1}|a_1$. Also ist a_{m+1} ein Teiler von a und b.

(ii) Es sei c ein Teiler von a und b. Aus der ersten Zeile folgt, dass $c|a_3$, aus der zweiten $c|a_4$ usw. Aus der vorletzten Zeile folgt schließlich $c|a_{m+1}$. Also ist a_{m+1} ein größter gemeinsamer Teiler von a und b. □

Darüberhinaus kann man mit Hilfe dieses Algorithmus Elemente $s, t \in R$ finden, so dass

$$a_{m+1} = \mathrm{ggT}(a, b) = sa + tb$$

gilt. Dazu beginnt man mit der vorletzten Gleichung

$$a_{m+1} = a_{m-1} - q_{m-1}a_m$$

und setzt rückwirkend die vorherigen Gleichungen ein, wobei jedesmal a_i durch einen Ausdruck mit a_{i-1} und a_{i-2} ersetzt wird.

Damit haben wir bewiesen

Satz 3.15 *Es sei R ein euklidischer Ring. Dann haben je zwei Elemente a und b in R einen größten gemeinsamen Teiler g. Ferner gibt es $s, t \in R$, so dass*

$$g = sa + tb.$$

Beispiel Wir bestimmen einen größten gemeinsamen Teiler von x^3+2x^2+1 und x^2+2 in $\mathbb{Z}_3[x]$. Nach Beispiel gilt

$$\begin{aligned} x^3 + 2x^2 + 1 &= (x+2)(x^2+2) + x \\ x^2 + 2 &= x \cdot x + 2 \\ x &= 2x \cdot 2 \end{aligned}$$

Daraus folgt $\mathrm{ggT}(x^3 + 2x^2 + 1, x^2 + 2) = 2$ und

$$\begin{aligned} 2 &= (x^2+2) - x \cdot x \\ &= (x^2+2) - (x^3 + 2x^2 + 1 - (x+2)(x^2+2))x \\ &= 2x(x^3 + 2x^2 + 1) + (x^2 + 2x + 1)(x^2 + 2) \end{aligned}$$

Der euklidische Algorithmus liefert eine praktische Methode, um die Zahlen s und t aus dem Beweis des vorherigen Satzes zu bestimmen.

3.5 Ideale

Wir betrachten nun Teilmengen von Ringen mit 1, die unter den Ringoperationen abgeschlossen sind.

Definition Es sei R ein Ring mit Einselement 1. Eine Teilmenge $S \subset R$ heißt *Unterring* von R, wenn gilt:

(UR1) Für alle $a, b \in S$ gilt $a + b \in S$.

(UR2) Für alle $a \in S$ gilt $-a \in S$.

(UR3) Für alle $a, b \in S$ gilt $a \cdot b \in S$.

(UR4) $1 \in S$.

Satz 3.16 *Ein Unterring S eines Rings R mit 1 ist ebenfalls ein Ring mit 1.*

Beweis. Wegen (UR4) gilt $S \neq \emptyset$. Aus (UR1) und (UR2) folgt damit, dass S bezüglich der Addition eine Untergruppe von R ist. Aus Satz 2.2 folgt, dass $(S, +)$ eine abelsche Gruppe ist. Die Bedingungen (UR3) und (UR4) zeigen, dass S abgeschlossen bezüglich der Multiplikation ist und $1 \in S$ gilt. Die übrigen Axiome gelten in S, da sie in R gelten. □

Beispiel $\mathbb{Z}$ ist ein Unterring von $\mathbb{Q}$, $\mathbb{Q}$ ist ein Unterring von $\mathbb{R}$ und $\mathbb{R}$ ist ein Unterring von $\mathbb{C}$, aber $n\mathbb{Z}$ ist für $n > 1$ kein Unterring.

Es stellt sich heraus, dass wichtiger als Unterringe eine andere Art von Untergruppen sind, nämlich die Ideale, die den Normalteilern von Gruppen entsprechen.

Definition Es sei R ein Ring mit 1. Eine Teilmenge $I \subset R$ heißt *Ideal* von R, wenn gilt:

(I0) $I \neq \emptyset$.

(I1) Für alle $x, y \in I$ gilt $x - y \in I$.

(I2) Für alle $x \in I$ und $r \in R$ gilt $r \cdot x \in I$ und $x \cdot r \in I$.

Aus (I0) und (I1) folgt, dass $(I, +)$ eine Untergruppe von $(R, +)$ ist.

Bemerkung (1) Oft wird (I1) auch in der folgenden Form formuliert: für alle $x, y \in I$ gilt $x + y \in I$. Zusammen mit (I2) ist dies zu (I1) äquivalent.

(2) Man schreibt (I2) auch oft in der Form $RI \subset I$ und $IR \subset I$ und spricht von einem *beidseitigen Ideal*. Fordert man nur $RI \subset I$ oder $IR \subset I$, so spricht man von einem *linksseitigen* oder *rechtsseitigen* Ideal. In einem kommutativen Ring fallen diese Begriffe zusammen.

Beispiel Es sei R ein Ring mit 1. Dann sind R und $\{0\}$ Ideale in R.

Satz 3.17 *Es sei R ein Ring mit 1 und I ein Ideal in R. Enthält I eine Einheit von R, so ist I der ganze Ring R.*

Beweis. Es sei $e \in I$ eine Einheit von R. Dann gibt es ein $u \in R$ mit $eu = 1$. Da I ein Ideal ist, ist dann auch $1 \in I$. Ist nun $r \in R$, so ist auch $r \cdot 1 = r \in I$, also $I = R$. □

Aufgabe: Bestimmen Sie alle Ideale in einem Körper.

Satz 3.18 *Es sei R ein kommutativer Ring mit 1, $a \in R$. Die Menge $\{ra \,|\, r \in R\}$ ist ein Ideal in R.*

Definition Die Menge $\{ra \,|\, r \in R\}$ bezeichnen wir mit $(a), aR$ oder Ra und nennen sie das von a erzeugte *Hauptideal*.

Beweis. Es ist $I \neq \emptyset$, da $a \in (a)$. Es sei $ra, sa \in (a)$ und $t \in R$. Dann gilt

$$\begin{aligned} ra - sa &= (r - s)a \in (a), \\ t(ra) &= (tr)a \in (a). \end{aligned}$$

Also ist (a) ein Ideal von R. □

Beispiel (0) $\{0\} = (0)$.

(1) $(n) = n\mathbb{Z}$ ist das von n erzeugte Hauptideal in $\mathbb{Z}$.

(2) Die Menge aller Polynome in $\mathbb{Z}_2[x]$, die $x+1$ als Faktor haben ist das Hauptideal

$$(x + 1) = \{p(x)(x + 1) \,|\, p(x) \in \mathbb{Z}_2[x]\}$$

in $\mathbb{Z}_2[x]$, das von $x + 1$ erzeugt wird. Es enthält alle Polynome, die 1 als Nullstelle haben.

(3) Die Menge aller Polynome in zwei Variablen x und y mit reellen Koeffizienten bezeichnen wir mit $\mathbb{R}[x, y]$. Die Menge aller solchen Polynome mit konstanten Glied $a_0 = 0$ ist ein Ideal von $\mathbb{R}[x, y]$. Dieses Ideal ist aber kein Hauptideal.

(4) Sei K ein Körper, $n \in \mathbb{N}$ und $R_0 = \mathrm{Mat}(n, K)$ ein Ring sowie $0 \neq A \in R_0$. Dann ist $R = K[A]$ ein (kommutativer!) Unterring und $(A) \subset R$ ein Ideal. Frage: wann gilt $(A) = R$ bzw. $A \neq R$?

Definition Ein kommutativer Ring R mit 1 heißt *Hauptidealring*, wenn jedes Ideal von R ein Hauptideal ist.

Satz 3.19 *Ein euklidischer Ring ist ein Hauptidealring.*

Beweis. Es sei R ein euklidischer Ring und I ein Ideal von R. Ist $I = \{0\}$, so ist $I = (0)$, das von 0 erzeugte Hauptideal von R. Andernfalls enthält I mindestens ein von 0 verschiedenes Element. Es sei $b \in I$, $b \neq 0$, mit $d(b)$ minimal. Ist nun $a \in I$, so gibt es $q, r \in R$ mit

$$a = qb + r \quad \text{wobei } r = 0 \text{ oder } d(r) < d(b).$$

Nun ist $r = a - qb \in I$. Da b ein Element aus I mit $d(b)$ minimal ist, muss $r = 0$ und $a = qb$ gelten. Also gilt $a \in (b)$ und $I \subset (b)$.

Umgekehrt ist jedes Element von (b) von der Form qb für ein $q \in R$. Dann ist aber $qb \in I$, da I ein Ideal ist. Also folgt $(b) \subset I$ und $I = (b)$. Also ist R ein Hauptidealring. □

Korollar 3.20 *Der Ring der ganzen Zahlen $\mathbb{Z}$ ist ein Hauptidealring, ebenso die Gaußschen Zahlen $\mathbb{Z}[i]$. Ist K ein Körper, so ist $K[x]$ ein Hauptidealring.*

Beweis. $\mathbb{Z}, \mathbb{Z}[i]$ und $K[x]$ sind euklidische Ringe. □

Problem: Sei $d \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei und betrachte den Ring $R = \mathbb{Z}[\sqrt{d}]$. Es ist ein klassisches Problem der algebraischen Zahlentheorie, wann R ein Hauptidealring ist ($\rightarrow$ Klassenzahlproblem).

Für $d < 0$ ist die Antwort bekannt, nämlich genau für $d = -1, -2$. Für $d = -3, -7$ ist R ebenfalls fast ein Hauptidealring in dem Sinne, dass es lediglich ein Primideal (nämlich $(2, \sqrt{d})$) gibt, das nicht Hauptideal ist (s.u.).

Für $d > 0$ ist jedoch noch nicht einmal erwiesen, ob es unendlich viele d gibt, für die R ein Hauptidealring ist.

3.6 Restklassenringe

Es sei R ein Ring mit 1 und I ein Ideal in R. Dann ist I insbesondere ein Normalteiler von der Gruppe $(R, +)$. Wir erinnern an die Kongruenzrelation modulo I

$$r_1 \equiv r_2 \bmod I \Leftrightarrow r_1 - r_2 \in I.$$

Die Äquivalenzklasse, die $r \in R$ enthält, also die Rechtsnebenklasse von I in R, die r enthält, bezeichnen wir mit $I + r$ (oder auch $r + I$). Also

$$I + r := \{x + r \,|\, x \in I\}.$$

Die Menge der Rechtsnebenklassen

$$R/I = \{I + r \,|\, r \in R\}$$

mit der Verknüpfung

$$(I + r_1) + (I + r_2) := I + (r_1 + r_2)$$

bildet eine abelsche Gruppe nach Satz 2.20.

Satz 3.21 *Es sei I ein Ideal im Ring R mit 1. Dann bildet die Menge der Rechtsnebenklassen R/I zusammen mit den Verknüpfungen*

$$(I + r_1) + (I + r_2) := I + (r_1 + r_2) \text{ und } (I + r_1) \cdot (I + r_2) := I + (r_1 r_2)$$

einen Ring mit Einselement $I + 1$.

Definition Dieser Ring heißt der *Restklassenring* oder der *Faktorring* von R nach I.

Beweis. Wir müssen nur noch die Axiome der Multiplikation nachweisen.

Zunächst zeigen wir, dass die Multiplikation wohl definiert ist. Es sei $r_1' \in I + r_1$ und $r_2' \in I + r_2$. Dann ist $r_1' - r_1 = x_1 \in I$ und $r_2' - r_2 = x_2 \in I$. Dann gilt

$$r_1' r_2' = (x_1 + r_1)(x_2 + r_2) = x_1 x_2 + r_1 x_2 + x_1 r_2 + r_1 r_2.$$

Da I ein Ideal ist, gilt $x_1 x_2, r_1 x_2, x_1 r_2 \in I$. Also gilt $r_1' r_2' - r_1 r_2 \in I$, also

$$I + r_1' r_2' = I + r_1 r_2.$$

Daraus folgt, dass die Multiplikation auf R/I wohl definiert ist.

Die Axiome können nun leicht bewiesen werden. □

Beispiel

$$\mathbb{Z}/(n) = \mathbb{Z}_n.$$

Es sei nun K ein Körper und $p(x) \in K[x]$ ein Polynom. Wir betrachten den Restklassenring $K[x]/(p(x))$.

Beachte: Mit $K[x]$ ist auch I ein K-Vektorraum und folglich auch $K[x]/I$. In folgenden wird es instruktiv sein, die Strukturen von $K[x]/I$ als Vektorraum (z.B. Dimension) und als (kommutativer) Ring mit 1 (z.B. Einheiten) zusammenzudenken.

Lemma 3.22 *Es sei* $f(x), g(x) \in K[x]$, $f(x) = q(x)p(x) + r(x)$, $g(x) = s(x)p(x) + t(x)$, $\operatorname{grad} r(x) < \operatorname{grad} p(x)$, $\operatorname{grad} t(x) < \operatorname{grad} p(x)$. *Dann gilt*

$$f(x) \equiv g(x) \bmod (p(x)) \Leftrightarrow r(x) = t(x).$$

Beweis.

$$\begin{aligned} & f(x) \equiv g(x) \bmod (p(x)) \\ \Leftrightarrow\ & f(x) - g(x) \in (p(x)) \\ \Leftrightarrow\ & p(x) | (f(x) - g(x)) \\ \Leftrightarrow\ & p(x) | [(q(x) - s(x))p(x) + (r(x) - t(x))] \\ \Leftrightarrow\ & p(x) | (r(x) - t(x)) \\ \Leftrightarrow\ & r(x) = t(x). \end{aligned}$$

Die letzte Äquivalenz folgt dabei direkt aus der Gradformel. □

Satz 3.23 *Es sei* $I = (p(x))$, *wobei* $p(x)$ *ein Polynom vom Grad* $n > 0$ *ist. Dann gilt*

$$K[x]/(p(x)) = \{I + a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \mid a_0, \ldots, a_{n-1} \in K\}.$$

Beweis. Es sei $I + f(x) \in K[x]/(p(x))$. Schreibe $f(x) = q(x)p(x) + r(x)$ mit $\operatorname{grad} r(x) < n$. Dann gilt $I + f(x) = I + r(x)$.

Angenommen, $I + r(x) = I + t(x)$ wobei $\operatorname{grad} r(x), \operatorname{grad} t(x) < n$. Dann gilt $r(x) \equiv t(x) \bmod I$. Nach dem vorhergehenden Lemma gilt $r(x) = t(x)$. □

Notation Wir schreiben oft die Repräsentanten $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ anstelle von $I + a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$. Also

$$K[x]/(p(x)) = \{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \mid a_0, \ldots, a_{n-1} \in K\}.$$

Korollar 3.24 *Für* $p \in K[x]$ *mit* $n = \deg p > 0$ *ist der Faktorring* $K[x]/(p)$ *ist ein endlich-dimensionaler* K*-Vektorraum mit Basis* $1, x, \ldots, x^{n-1}$.

Beispiel Wir betrachten $K[x]/(x^2 + x + 1)$. Es gilt

$$K[x]/(x^2 + x + 1) \cong K^2$$

mit Basis $1, x$ als Vektorraum. Rechnen wir in diesem Ring: Was ist z.B. $(x + 1)(x + 1)$ in $K[x]/(x^2 + x + 1)$? Es gilt

$$(x + 1)(x + 1) = x^2 + 2x + 1 = (x^2 + x + 1) + x.$$

Also gilt $(x+1)(x+1) = x$ in $K/(x^2+x+1)$. Es folgt, dass $x, x+1$ Einheiten sind – können Sie die Ordnung berechnen?

Auf diese Weise erhalten wir die komplette Multiplikationstafel über endlichen Körpern K – z.B. die folgende über $\mathbb{Z}_2$:

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

3.7 Ringhomomorphismen

Analog zu Gruppenhomomorphismen betrachten wir nun Abbildungen zwischen Ringen, die die Addition und Multiplikation erhalten.

Definition Es seien R und S zwei Ringe mit 1. Eine Abbildung $f : R \to S$ heißt *Ringhomomorphismus*, wenn für alle $a, b \in R$ gilt:

(i) $f(a+b) = f(a) + f(b)$,

(ii) $f(a \cdot b) = f(a) \cdot f(b)$,

(iii) $f(1) = 1$.

Ein *Ringisomorphismus* ist ein Ringisomorphismus,wenn es einen Ringhomomorphismus $g : S \to R$ gibt mit $g \circ f = \mathrm{id}_R$ und $f \circ g = \mathrm{id}_S$. Dies ist genau dann der Fall wenn f bijektiv ist. Wenn es einen Ringisomorphismus zwischen den Ringen mit Einselement R und S gibt, dann sagen wir, R und S sind *isomorph* und wir schreiben $R \cong S$.

Ein Ringhomomorphismus $f : R \to S$ ist insbesondere ein Gruppenhomomorphismus von $(R, +)$ nach $(S, +)$. Deswegen gilt nach Satz 2.5 $f(0) = 0$ und $f(-a) = -f(a)$ für alle $a \in R$.

Beispiel (a) $\mathbb{Z}$ besitzt einen eindeutigen Ringhomomorphismus in jeden Ring mit 1.

(b) Die Abbildung $f : \mathbb{Z} \to \mathbb{Z}_n$ mit $f(x) = [x]$ ist ein Ringhomomorphismus.

(c) Die natürlichen Abbildungen

$$\mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$$

sind allesamt injektive Ringhomomorphismen (sogenannte Einbettungen)

Analog zu Satz 2.21 gilt:

Satz 3.25 *Ist $f : R \to S$ ein Ringhomomorphismus, so ist* $\operatorname{Ker} f$ *ein Ideal von R.*

Beweis. Ist $x \in \operatorname{Ker} f$ und $r \in R$, so gilt

$$f(xr) = f(x)f(r) = 0 \cdot f(r) = 0,$$

also $xr \in \operatorname{Ker} f$. Analog $rx \in \operatorname{Ker} f$.Analog zeigt man $xr \in \operatorname{Ker} f$. Der Rest folgt aus Satz 2.21. □

Das Bild $\operatorname{Im} f$ eines Ringhomomorphismus $f : R \to S$ ist ein Unterring von S.

Analog zu Satz 2.22 gilt:

Satz 3.26 (Homomorphiesatz für Ringe) *Für einen Ringhomomorphismus $f : R \to S$ gilt:*

$$R/\operatorname{Ker} f \cong \operatorname{Im} f.$$

Beweis. Es sei $K = \operatorname{Ker} f$. Im Beweis des Homomorphiesatzes für Gruppen (Satz 2.22) hatten wir gesehen, dass $\psi : R/K \to \operatorname{Im} f$ mit $\psi(K + r) = f(r)$ ein Gruppenisomorphismus ist. Wir müssen also nur noch zeigen, dass ψ ein Ringhomomorphismus ist. Es gilt

$$\psi((K + r)(K + s)) = \psi(K + rs) = f(rs) = f(r)f(s) = \psi(K + r)\psi(K + s).$$

□

Beispiel Ein weiteres Beispiel für Ringhomomorphismen sind *Auswertungsabbildungen*. Darunter versteht man das Folgende: Es sei $K[x]$ der Polynomring über dem Körper K und $K' \supset K$ ein Körper, der K als Unterkörper enthält (z.B. $K = \mathbb{Q} \subset \mathbb{C} = K'$, aber auch Ringe $R \supset K$ wie z.B. $K[A]$ für eine Matrix $A \in \operatorname{Mat}(n, K)$ gehen, vgl. LAII). Für ein $\alpha \in K'$ betrachten wir die Abbildung

$$\begin{array}{rccc} \operatorname{Ev}_\alpha : & K[x] & \longrightarrow & K[\alpha] \subset K' \\ & p(x) & \longmapsto & p(\alpha) \end{array}.$$

Diese Abbildung ist ein Ringhomomorphismus von $K[x]$ in den Unterring

$$K[\alpha] := \{p(\alpha) \,|\, p(x) \in K[x]\} \subset K'.$$

Problem: berechnen Sie das Ideal $\ker \operatorname{Ev}_\alpha$.

Wir diskutieren 3 beispielhafte Fälle:
1. für $\alpha \in K$ gilt $\ker \mathrm{Ev}_\alpha = (x - \alpha)$.
2. für $\alpha = \pi \in \mathbb{R}$ und $K = \mathbb{Q}$ gilt $\ker \mathrm{Ev}_\alpha = (0)$ (Transzendenz von π).
3. für $d \in \mathbb{Z}\backslash\{0, 1\}$ quadratfrei und $\alpha = \sqrt{d}$ gilt $\ker \mathrm{Ev}_\alpha = (x^2 - d)$. (Beweis?!)

In diesem Zusammenhang erwähnen wir noch das folgende Resultat:

Satz 3.27 *Es sei $d \in \mathbb{Z}$, $d \neq 0, 1$, und d sei* quadratfrei*, d.h. in der Primfaktorzerlegung von d tritt jeder Primfaktor höchstens mit der Potenz 1 auf. Setze*

$$\alpha := \begin{cases} \sqrt{d} & \text{für } d \equiv 2, 3 \bmod 4, \\ \frac{1+\sqrt{d}}{2} & \text{für } d \equiv 1 \bmod 4. \end{cases}$$

Dann ist $\mathbb{Q}[\alpha] := \{r + s\alpha \mid r, s \in \mathbb{Q}\}$ ein Körper und $\mathbb{Z}[\alpha] := \{k + m\alpha \mid k, m \in \mathbb{Z}\}$ ein Ring.

Definition Unter den Voraussetzungen von Satz 3.27 nennt man $\mathbb{Q}[\alpha]$ einen *quadratischen Zahlkörper* und $\mathbb{Z}[\alpha]$ den *Ring der ganzen Zahlen* $\mathcal{O}_d$ dieses Körpers.

Beweis. Um zu zeigen, dass $\mathbb{Q}[\sqrt{d}]$ ein Körper ist, muss man zeigen, dass jedes von 0 verschiedene Element ein multiplikatives Inverses besitzt. Nun gilt:

$$(r + s\sqrt{d})^{-1} = \frac{r - s\sqrt{d}}{r^2 - s^2 d}.$$

Da d quadratfrei ist, ist der Nenner ungleich 0.

Im Fall $d \equiv 1 \bmod 4$ kann man analog argumentieren:

$$\frac{1}{r + s\alpha} = \frac{2}{(2r + s) + \sqrt{d}} = \frac{2(2r + s - \sqrt{d})}{(2r + s)^2 - d}.$$

Um zu sehen, dass $\mathcal{O}_d$ ein Unterring ist, muss man zeigen, dass $\alpha^2 \in \mathcal{O}_d$. Hierbei ist nur der Fall $d \equiv 1 \bmod 4$ zu überprüfen. Es gilt

$$\alpha^2 = \frac{1 + d + 2\sqrt{d}}{4}.$$

Da $d \equiv 1 \bmod 4$ ist $d = 1 + 4k$ für eine ganze Zahl k. Also gilt

$$\alpha^2 = \frac{2 + 4k + 2\sqrt{d}}{4} = k + \frac{1 + \sqrt{d}}{2} = k + \alpha \in \mathcal{O}_d$$

wie verlangt. □

Bemerkung Der Ring der ganzen Zahlen $\mathcal{O}_d$ lässt sich kanonisch definieren als der größte Ring in $\mathbb{Q}(\sqrt{d})$, welcher endlich erzeugt als abelsche Gruppe bezüglich + ist.

Zum Abschluss dieses Abschnitts betrachten wir das **kartesische Produkt** von zwei Ringen R und S

$$R \times S := \{(r, s) \mid r \in R, s \in S\}.$$

Wir hatten schon in §2.3 gesehen, dass die komponentenweise Addition eine Gruppenstruktur auf $R \times S$ definiert. Entsprechend definieren wir nun eine Multiplikation auf $R \times S$:

$$(r_1, s_1)(r_2, s_2) := (r_1 r_2, s_1 s_2).$$

Damit wird auch $R \times S$ zu einem Ring. Sind R und S Ringe mit 1, so ist auch $R \times S$ ein Ring mit dem Einselement $(1, 1)$. Man beachte aber, dass das direkte Produkt von zwei nicht trivialen Integritätsbereichen nicht wieder ein Integritätsbereich ist (warum?).

Es gilt der folgende Satz, der als eine Version des chinesischen Restsatzes angesehen werden kann.

Satz 3.28 *Es seien m und n teilerfremde positive ganze Zahlen. Dann gilt*

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n \quad \textit{(als Ringe).}$$

Ist $m = p_1^{e_1} \cdots p_r^{e_r}$ die Primfaktorzerlegung von m, so gilt

$$\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_r^{e_r}}.$$

Kontrolle: $\mathbb{Z}_m$ ist genau dann ein Integritätsbereich, wenn $r = e_1 = 1$.

3.8 Zerlegung in irreduzible Faktoren

Eine wichtige Eigenschaft der ganzen Zahlen ist die Tatsache, dass sich jede ganze Zahl > 1 in Primfaktoren zerlegen lässt. Wir wollen nun Ringe betrachten, in denen eine ähnliche Zerlegung möglich ist.

Lemma 3.29 *Es sei R ein Integritätsbereich. Dann gilt $a|b$ und $b|a$ genau dann, wenn $a = eb$ ist, wobei e eine Einheit in R ist. (a und b heißen dann* assoziiert.*)*

Beweis. "⇒": Aus $a|b$ folgt $b = ac$ für ein $c \in R$ und aus $b|a$ folgt $a = bd$ für ein $d \in R$. Dann gilt $a = bd = acd$, also $a(cd - 1) = 0$. Daraus folgt $a = 0$ oder $cd = 1$. Ist $a = 0$, so ist auch $b = 0$. Im anderen Fall ist d eine Einheit (und ebenso c).

"⇐": Aus $a = eb$ folgt $b|a$. Ist $c \in R$ mit $ce = 1$, so folgt $b = ca$, also $a|b$. □

Definition Es sei R ein Integritätsbereich. Ein Element $p \in R$ heißt *irreduzibel*, wenn p weder das Nullelement noch eine Einheit ist und wenn gilt: Aus $p = ab$ mit $a, b \in R$ folgt: a ist eine Einheit oder b ist eine Einheit.

Ein Element $p \in R$ heißt *Primelement*, wenn p weder das Nullelement noch eine Einheit ist und wenn gilt: Aus $p|ab$ für $a, b \in R$ folgt $p|a$ oder $p|b$.

Satz 3.30 *Jedes Primelement ist irreduzibel.*

Beweis. Es sei p ein Primelement in einem Integritätsbereich R. Wir betrachten eine Zerlegung $p = ab$ mit $a, b \in R$. Dann folgt $a|p$ und $b|p$. Da p ein Primelement ist, folgt $p|a$ oder $p|b$. Angenommen, $p|a$. Nach dem vorherigen Lemma gilt dann $a = ep$, wobei $e \in R$ eine Einheit ist. Daraus folgt $p = ebp$. Da $p \neq 0$ folgt daraus $eb = 1$. Also ist b eine Einheit. □

Die Umkehrung gilt im Allgemeinen nicht:

Beispiel In $\mathbb{Z}[\sqrt{-3}] := \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$ gilt

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

Die Elemente $2, 1+\sqrt{-3}, 1-\sqrt{-3}$ sind irreduzibel und es gilt $(1+\sqrt{-3})|2\cdot 2$, aber $1 + \sqrt{-3}$ teilt nicht 2. Die Aussage, dass etwa $1 + \sqrt{-3}$ irreduzibel ist, sieht man wie folgt. Für $z = a + b\sqrt{-3}$ ist der Absolutbetrag $|z|^2 = a^2 + 3b^2$. Für eine Darstellung $1 + \sqrt{-3} = rs$ würde also gelten $|r|^2|s|^2 = 1 + 3 = 4$. Nun ist $|r| = 1$ genau wenn $r = \pm 1$. Anderseits ist $|r|^2 = 4$ genau dann wenn $r = \pm 2$ oder $r = \pm(1 + \sqrt{-3})$. Da ± 2 kein Teiler von $1 + \sqrt{-3}$ ist, folgt die Irreduzibilität.

Wir betrachten nun den Zusammenhang mit Idealen.

Definition Es sei R ein kommutativer Ring mit 1. Ein Ideal $I \neq R$ von R heißt *Primideal*, wenn für alle $a, b \in R$ gilt: Aus $ab \in I$ folgt $a \in I$ oder $b \in I$.

Beispiel Das Ideal (0) ist genau dann Primideal, wenn R Integritätsbereich ist (während 0 als Primelement nicht zulässig ist).

Satz 3.31 *Es sei R ein Integritätsbereich, $a \in R$. Dann ist (a) genau dann ein vom Nullideal verschiedenes Primideal, wenn a ein Primelement ist.*

Beweis. "$\Rightarrow$": Es sei (a) ein Primideal. Da $(a) \neq R$, ist a keine Einheit. Wegen $(a) \neq (0)$ gilt $a \neq 0$. Es seien $x, y \in R$ und es gelte $a|xy$. Dann folgt $xy \in (a)$. Da (a) ein Primideal ist, folgt $x \in (a)$ oder $y \in (a)$. Also gilt $a|x$ oder $a|y$.

"$\Leftarrow$": Es sei a ein Primelement. Da $a \neq 0$ und a keine Einheit ist, gilt $(a) \neq (0), R$. Es sei $xy \in (a)$ für $x, y \in R$. Dann folgt $a|xy$. Da a ein Primelement ist, folgt $a|x$ oder $a|y$, also $x \in (a)$ oder $y \in (a)$. □

Satz 3.32 *Es sei I ein Ideal des Integritätsbereichs R. Dann ist I genau dann ein Primideal, wenn R/I ein Integritätsbereich ist.*

Beweis. "$\Rightarrow$": Es sei I ein Primideal. Angenommen

$$(a + I)(b + I) = (ab + I) = 0.$$

Dann gilt $ab \in I$ und da I Primideal ist folgt $a \in I$ oder $b \in I$, also $a + I = 0$ oder $b + I = 0$.

"$\Leftarrow$": Es sei R/I ein Integritätsbereich. Ferner sei $ab \in I$. Dann folgt

$$0 = (ab + I) = (a + I)(b + I).$$

Da R/I ein Integritätsbereich ist, folgt $a + I = 0$ oder $b + I = 0$, also $a \in I$ oder $b \in I$. □

Vergleiche das letzte kleine Beispiel:
(0) ist Primideal $\Leftrightarrow$ R ist Integritätsbereich $\Leftrightarrow$ $R/(0)$ ist Integritätsbereich.

Definition Es sei R ein kommutativer Ring mit 1. Ein Ideal I von R heißt *maximales Ideal* in R, wenn $I \neq R$ und für alle Ideale J von R mit $I \subset J \subset R$ gilt: $J = I$ oder $J = R$.

Satz 3.33 *Es sei R ein Integritätsbereich, $a \in R$, $a \neq 0$. Ist (a) ein maximales Ideal von R, so ist a irreduzibel.*

Beweis. Es sei (a) ein maximales Ideal. Angenommen, $a = st$ für $s, t \in R$. Wegen $a \neq 0$ ist $s, t \neq 0$. Dann gilt $(a) \subset (s)$. Da (a) ein maximales Ideal ist, folgt $(a) = (s)$ oder $(s) = R$. Gilt $(s) = R$, dann ist $1 \in (s)$, also ist s eine Einheit. Wenn $(a) = (s)$ gilt, dann gibt es ein $b \in R$ mit $s = ab$, also $a = st = abt$. Da R Integritätsbereich ist, folgt $bt = 1$, also ist t eine Einheit. □

Ist R zusätzlich ein Hauptidealring, so gilt auch die Umkehrung:

Satz 3.34 *Es sei R ein nullteilerfreier Hauptidealring, $a \in R$, $a \neq 0$. Dann ist (a) genau dann ein maximales Ideal von R, wenn a irreduzibel ist.*

Beweis. "$\Rightarrow$" ist Satz 3.33.

"$\Leftarrow$": Es sei a irreduzibel. Es sei $J \subset R$ ein Ideal mit $(a) \subset J \subset R$. Da R ein Hauptidealring ist, gibt es ein $b \in R$ mit $J = (b)$. Aus $(a) \subset (b)$ folgt, dass es ein $c \in R$ gibt mit $a = bc$. Da a irreduzibel ist, folgt, dass b oder c eine Einheit ist. Ist b eine Einheit, so folgt $(b) = R$, ist c eine Einheit, so gilt $(a) = (b)$. Also ist das Ideal (a) maximal. □

Satz 3.35 *Ein nichttrivialer kommutativer Ring R mit 1 ist genau dann ein Körper, wenn (0) und R die einzigen Ideale sind.*

Beweis. "$\Rightarrow$": Es sei R ein Körper und $I \subset R$ ein Ideal mit $I \neq (0)$. Dann gibt es ein $a \in I$ mit $a \neq 0$. Dann ist aber auch $aa^{-1} = 1 \in I$, also $I = R$ nach Satz 3.17.

"$\Leftarrow$": Es seien (0) und R die einzigen Ideale von R. Es sei $a \in R$, $a \neq 0$. Wir betrachten das Ideal (a). Es gilt $(a) \neq (0)$, da $1 \cdot a \in (a)$. Also folgt $(a) = R$. Dann gilt aber $1 \in (a)$ und es gibt ein $b \in R$ mit $ab = 1$. Also besitzt a ein inverses Element b und R ist ein Körper. □

Satz 3.36 *Es sei R ein Ring mit 1, I ein Ideal in R. Ist J ein Ideal von R mit $I \subset J$, so ist J/I ein Ideal von R/I. Ist umgekehrt U ein Ideal von R/I, so gibt es ein Ideal J von R mit $I \subset J$ und $U = J/I$.*

Beweis. Es sei $r+I \in R/I$, $a+I \in J/I$. Dann gilt $(r+I)(a+I) = ra+I \in J/I$, da $ra \in J$. Analog zeigt man $ar \in J$, also $(a+I)(r+I) \in J/I$, und die erste Behauptung ist gezeigt.

Für die zweite Behauptung betrachten wir die kanonischen Projektionen

$$R \xrightarrow{f} R/I, \quad R \xrightarrow{g} R/J.$$

Die Universelle Eigenschaft des Faktorrings (oder der Faktorgruppe) liefert einen Ringhomomorphismus

$$R/I \xrightarrow{\tilde{g}} R/J,$$

die in das folgende kommutative Diagramm passt:

$$\begin{array}{ccc} R & \xrightarrow{f} & R/I \\ g\downarrow & \swarrow \tilde{g} & \\ R/J & & \end{array}$$

Insbesondere ist $J/I = \ker \tilde{g}$ ein Ideal in R/I (wie schon gesehen).

Sein nun umgekehrt U ein Ideal von R/I. Setze

$$J := \{r \in R \,|\, r + I \in U\} = f^{-1}(U).$$

Dann ist J ein Ideal mit $I \subset J$ und $U = J/I = f(f^{-1}(U))$ (da f nach Konstruktion surjektiv ist). □

Bemerkung Man kann dies auch so ausdrücken: die kanonische Projektion $f : R \to R/I$ induziert durch $J \mapsto f(J)$, bzw. $\overline{J} \mapsto f^{-1}(\overline{J})$ eine Bijektion zwischen Idealen in R, welche I umfassen, und Idealen in R/I.

Satz 3.37 *Es sei I ein Ideal des kommutativen Rings R mit 1. Dann ist I genau dann ein maximales Ideal von R, wenn R/I ein Körper ist.*

Beweis. "⇒": Es sei I ein maximales Ideal. Es sei $U \subset R/I$ ein Ideal mit $U \neq (0)$. Dann gibt es nach Satz 3.36 ein Ideal $J \subset R$ mit $I \subset J$ und $J/I = U$. Da $U \neq (0)$, gilt $I \neq J$. Da I ein maximales Ideal ist, folgt $J = R$, also $U = R/I$. Nach Satz 3.35 ist R/I ein Körper.

"⇐": Es sei R/I ein Körper. Es sei $J \subset R$ ein Ideal in R mit $I \subset J$, aber $I \neq J$. Dann ist J/I ein Ideal von R/I mit $J/I \neq (0)$. Da R/I ein Körper ist, gilt nach Satz 3.35 $J/I = R/I$. Daraus folgt $J = R$, denn für jedes $r \in R$ existiert ein $j \in J$, so dass $r + I = j + I$. Andererseits gilt $j + I \subset J$ (da $J \supset I$ Ideal) und insbesondere $r \in J$. Folglich ist I ein maximales Ideal von R. □

Korollar 3.38 *In einem Integritätsbereich ist jedes maximale Ideal auch ein Primideal.*

Beweis. Ist I ein maximales Ideal, dann ist R/I ein Körper und damit insbesondere ein Integritätsbereich. Also ist I ein Primideal. □

In nullteilerfreien Hauptidealringen gilt auch die Umkehrung.

Korollar 3.39 *Es sei R ein nullteilerfreier Hauptidealring, $a \in R$. Dann ist $R/(a)$ genau dann ein Körper, wenn a irreduzibel in R ist.*

Beweis. Dies folgt nun aus Satz 3.34. □

Korollar 3.40 *In einem nullteilerfreien Hauptidealring ist jedes irreduzible Element ein Primelement.*

Beweis. Wenn a irreduzibel ist, dann ist folgt aus Korollar 3.39, dass $R/(a)$ ein Körper ist, insbesondere also ein Integritätsbereich und damit ist (a) ein Primideal. Nach Satz 3.31 ist a dann ein Primelement. □

Definition Ein Integritätsbereich R heißt *faktoriell* oder ein *ZPE-Ring*, wenn sich jede von Null verschiedene Nichteinheit aus R als Produkt von Primelementen schreiben lässt.

Beispiel Jeder Körper ist faktoriell.

Satz 3.41 *In einem faktoriellen Ring R ist die Zerlegung in Primfaktoren eindeutig, d.h. jede von Null verschiedene Nichteinheit aus R lässt sich als Produkt von Primelementen schreiben, wobei die Faktoren dieses Produktes bis auf Einheiten und Reihenfolge eindeutig bestimmt sind.*

Beweis. Es sei $a \in R$ eine von Null verschiedene Nichteinheit. Angenommen,

$$a = p_1 \cdots p_n = q_1 \cdots q_m,$$

wobei jedes p_i und jedes q_j ein Primelement ist. Dann gilt $p_1 | a$ und damit $p_1 | q_1 \cdots q_m$. Da p_1 ein Primelement ist, muss p_1 eins der q_j teilen. Nach eventueller Umnummerierung können wir annehmen, dass $p_1 | q_1$. Das bedeutet, $q_1 = u_1 p_1$ für ein $u_1 \in R$. Da p_1 und q_1 auch irreduzibel sind, folgt, dass u_1 eine Einheit ist. Also gilt

$$a = p_1 p_2 \cdots p_n = u_1 p_1 q_2 \cdots q_m$$

und daraus folgt $p_2 \cdots p_n = u_1 q_2 \cdots q_m$. Durch Induktion folgt $q_i = u_i p_i$ für $i = 1, \ldots, \min(m, n)$, wobei u_i eine Einheit ist.

Ist nun $m < n$, so folgt

$$p_{m+1} \cdots p_n = u_1 \cdots u_m.$$

Dies ist aber unmöglich, da irreduzible Elemente keine Einheit teilen können. Ist $m > n$, so folgt

$$1 = u_1 \cdots u_n q_{n+1} \cdots q_m.$$

Daraus folgt, dass q_m eine Einheit ist, ein erneuter Widerspruch. Also ist $m = n$ und die Primelemente $p_1, \ldots, p_n$ sind die gleichen wie die Primelemente $q_1, \ldots, q_m$ bis auf ihre Reihenfolge und die Multiplikation mit Einheiten. □

Lemma 3.42 *Die Ringe $\mathbb{Z}$ und $K[x]$ (K ein Körper) sind faktoriell.*

Beweis. Es sei $R = \mathbb{Z}$ oder $R = K[x]$. Dann ist R ein nullteilerfreier Hauptidealring. Nach Korollar 3.40 ist jedes irreduzible Element ein Primelement. Also reicht es zu zeigen, dass sich jede von Null verschiedene Nichteinheit $a \in R$ als Produkt von irreduziblen Elementen schreiben lässt. Ist a schon selbst irreduzibel, so ist nichts zu zeigen. Andernfalls zerlege man a in das Produkt $a = bc$ zweier Nichteinheiten in R. Diese Konstruktion kann man dann für b und c wiederholen, usw. Dieses Verfahren bricht nach endlich vielen Schritten ab: Für $R = \mathbb{Z}$ gilt $|b|, |c| < |a|$, für $R = K[x]$ hat man $\operatorname{grad} b, \operatorname{grad} c < \operatorname{grad} a$. Bei jeder neuen Zerlegung nimmt daher der Betrag bzw. der Grad ab, so dass das Verfahren nach endlich vielen Schritten abbrechen muss. □

Wir wollen nun allgemeiner zeigen, dass jeder nullteilerfreie Hauptidealring faktoriell ist.

Definition Ein kommutativer Ring R mit 1 heißt *noethersch*, wenn jede aufsteigende Kette von Idealen $I_0 \subset I_1 \subset \ldots$ stationär wird, d.h. es gibt ein $n \in \mathbb{N}$ gibt mit $I_j = I_n$ für alle $j \geq n$.

Übungsaufgabe: R ist genau dann noethersch, wenn jedes Ideal endlich erzeugt ist.

Bemerkung (1) Die Bezeichnung noethersch erinnert an die Mathematikerin Emmy Noether.

(2) Man sagt auch, dass der Ring R asc (ascending chain condition) erfüllt.

Wir benötigen das folgende Lemma:

Lemma 3.43 *Jeder Hauptidealring R ist* noethersch.

Beweis. Wir bilden die Menge

$$I := \bigcup_{j \geq 0} I_j.$$

Man kann leicht zeigen, dass I ein Ideal ist (Übungsaufgabe). Da R ein Hauptidealring ist, ist I ein Hauptideal, also $I = (a)$ für ein $a \in I$. Aus $a \in I$ folgt $a \in I_n$ für ein $n \in \mathbb{N}$. Dann gilt

$$(a) \subset I_n \subset I = (a).$$

Daraus folgt, dass die Idealkette $I_0 \subset I_1 \subset \ldots$ bei I_n stationär wird. □

Satz 3.44 *Jeder nullteilerfreie Hauptidealring R ist faktoriell.*

Beweis. Wir gehen wie in Lemma 3.42 vor. Nach Korollar 3.40 ist jedes irreduzible Element ein Primelement. Also reicht es zu zeigen, dass sich jede von Null verschiedene Nichteinheit $a \in R$ als Produkt von irreduziblen Elementen schreiben lässt. Ist a nicht schon selbst irreduzibel, so zerlegen wir a in das Produkt $a = bc$ zweier Nichteinheiten. Dann gilt:

$$(a) \subsetneq (b), \quad (a) \subsetneq (c).$$

(Beachte: $(a) = (b) \iff a \sim b$.) Diese Konstruktion kann man dann für b und c wiederholen, usw. Bricht dieses Verfahren nicht nach endlich vielen Schritten ab, so erhalten wir eine aufsteigende Kette von Hauptidealen in R, die nicht stationär wird. Das steht im Widerspruch zu Lemma 3.43. □

Satz 3.45 *In einem faktoriellen Ring ist jedes irreduzible Element ein Primelement.*

Beweis. Es sei R ein faktorieller Ring, $a \in R$ ein irreduzibles Element. Da a keine Einheit ist, lässt sich a als Produkt von Primelementen

$$a = p_1 \cdots p_n, \quad p_1, \ldots, p_n \in R,$$

schreiben. Da a irreduzibel ist, muss hierbei $n = 1$ sein. Also ist a ein Primelement. □

Beispiel $\mathbb{Z}[\sqrt{-3}]$ ist kein faktorieller Ring, da $1 + \sqrt{-3}$ irreduzibel, aber kein Primelement ist.

Satz 3.46 *Ein Integritätsbereich R ist genau dann faktoriell, wenn sich jede von Null verschiedene Nichteinheit als Produkt von irreduziblen Elementen schreiben lässt, wobei die Faktoren dieses Produktes bis auf Einheiten und Reihenfolge eindeutig bestimmt sind.*

Beweis. "⇒": Es sei R faktoriell. Dann lässt sich jede von Null verschiedene Nichteinheit aus R als Produkt von Primelementen schreiben. Nach Satz 3.41 sind die Faktoren dieses Produktes bis auf Einheiten und Reihenfolge eindeutig bestimmt. Nach Satz 3.30 ist jedes Primelement irreduzibel.

"⇐": Hier reicht es zu zeigen, dass jedes irreduzible Element von R ein Primelement ist. Es sei also $u \in R$ ein irreduzibles Element. Angenommen, $u|ab$ mit $a, b \in R$. Dann gilt $ab = cu$ mit einem $c \in R$. Die Elemente a, b und c zerlegen wir jedes für sich in ein Produkt irreduzibler Elemente und setzen die Produkte in $ab = cu$ ein. Nach Voraussetzung sind die Faktoren

der Produkte auf beiden Seiten der Gleichung die Gleichen bis auf Einheiten und Reihenfolge. Also muss u zu einem Teiler von a oder b assoziiert sein und somit selbst ein Teiler von a oder b sein. □

Beispiel Ist $K[x, y]$ oder $\mathbb{Z}[x]$ faktoriell? Integritätsbereich ist jeweils klar, die Zerlegung in irreduzible Faktoren sollte sich mittels Grad und Teilbarkeitsrelationen zwischen Koeffizienten leicht herleiten lassen, aber die verlangte Eindeutigkeit?!

3.9 Die Vermutung von Fermat

Wir betrachten eine Gleichung der Form

$$x^n + y^n = z^n \tag{3.2}$$

für eine natürliche Zahl $n \geq 2$. Gesucht sind die ganzzahligen Lösungen x, y, z dieser Gleichung. Für $n = 2$ sind Lösungen bekannt, z.B. das Tripel $(3, 4, 5)$. Die Lösungen dieser Gleichung für $n = 2$ sind die *Pythagoräischen Zahlentripel*. Da mit jedem Tripel von Lösungen auch alle Vielfachen Lösungstripel sind, kann man o.B.d.A. annehmen, dass x, y, z teilerfremd sind (äquivalent: paarweise teilerfremd (!)).

Lemma 3.47 *Für eine ganze Zahl $x \in \mathbb{Z}$ gilt*

$$x^2 \equiv 0 \bmod 4 \text{ oder } x^2 \equiv 1 \bmod 4.$$

Beweis. Für x gerade, $x = 2m$, gilt $x^2 = 4m^2 \equiv 0 \bmod 4$. Für x ungerade, $x = 2m + 1$, gilt $x^2 = (2m + 1)^2 = 4m^2 + 4m + 1 \equiv 1 \bmod 4$. □

Anwendung: betrachte 3.2 modulo 4. Mit dem Lemma folgt, dass entweder $x, y, z \equiv 0 \mod 2$ (und somit nicht teilerfremd) oder z und genau eine weitere Koordinate, sagen wir y, ungerade ist, während x demnach gerade ist.

Satz 3.48 (Pythagoräische Zahlentripel) *Die positiven teilerfremden Lösungen der Gleichung*

$$x^2 + y^2 = z^2$$

mit geradem x sind genau von der Form

$$x = 2ab, \quad y = a^2 - b^2, \quad z = a^2 + b^2, \quad a > b > 0, (a, b) = 1, a \not\equiv b \bmod 2.$$

Beweis. Wegen

$$4a^2b^2 + (a^2 - b^2)^2 = a^4 + 2a^2b^2 + b^4 = (a^2 + b^2)^2$$

führt jedes Paar (a, b) zu einer Lösung der Gleichung (3.2) für $n = 2$, die, wie man leicht prüft, teilerfremd ist.

Umgekehrt können wir nach den Vorbemerkungen zu Satz 3.48 annehmen, dass y und z beide ungerade sind und $(x, y) = (y, z) = 1$ gilt. Daraus folgt

$$\frac{z+y}{2}, \frac{z-y}{2} \in \mathbb{Z}, \quad \left(\frac{z+y}{2}, \frac{z-y}{2}\right) = 1.$$

Nun gilt aber

$$\begin{aligned} x^2 + y^2 = z^2 &\Leftrightarrow x^2 = z^2 - y^2 \\ &\Leftrightarrow x^2 = (z+y)(z-y) \\ &\Leftrightarrow \left(\frac{x}{2}\right)^2 = \left(\frac{z+y}{2}\right)\left(\frac{z-y}{2}\right). \end{aligned}$$

Wegen der Eindeutigkeit der Primfaktorzerlegung muss es natürliche Zahlen a, b geben mit

$$\frac{z+y}{2} = a^2, \quad \frac{z-y}{2} = b^2, \quad a > b > 0, (a, b) = 1, a \not\equiv b \bmod 2.$$

Hierbei gilt letztere Ungleichung, da sonst $z = a^2 + b^2$ und $y = a^2 - b^2$ beide gerade wären (und genau nicht teilerfremd). □

P. de Fermat hat nun um 1640 an den Rand eines Buches geschrieben, dass er einen Beweis hat, dass die Gleichung (3.2) für $n \geq 3$ keine Lösungen in den positiven ganzen Zahlen hat. 350 Jahre lang hat man vergeblich versucht, diesen Beweis zu rekonstruieren bzw. diesen Satz zu beweisen. Das Problem ist eigentlich uninteressant: Seine Lösung hat keine wichtigen Konsequenzen für die übrige Mathematik. Andererseits war dieses Problem für die Entwicklung der Mathematik sehr wichtig. Die Beschäftigung mit diesem Problem hat entscheidende Impulse für die Mathematik bis hin zur Entwicklung neuer mathematischer Theorien gegeben.

Zum Beispiel hat die Beschäftigung mit dem Fermatschen Problem wichtige Impulse für die algebraische Zahlentheorie geliefert. Z. B. kann man für $n = 3$ die Gleichung mit $\zeta = \frac{-1+\sqrt{-3}}{2} = e^{\frac{2\pi i}{3}}$ umschreiben in

$$x^3 + y^3 = (x + \zeta y)(x + \zeta^2 y)(x + y) = z^3.$$

Damit wird man auf ein zahlentheoretisches Problem im euklidischen Ring $\mathcal{O}_{-3}$ geführt. Wegen der eindeutigen Primfaktorzerlegung müssen nun die

einzelnen Faktoren entweder gemeinsame Primteiler haben oder aber jeder selbst assoziiert zu einer reinen dritten Potenz sein (wie mit den Quadraten im Fall $n = 2$ über $\mathbb{Z}$), was sich sodann auf einen Widerspruch führen lässt.

Dieser Ansatz überträgt sich auf den Fall $n = p \in \mathbb{P}$ mit $\zeta = e^{2\pi i/p}$ einer nicht-trivialen Nullstelle von $x^p - 1$. Jedoch stellt sich heraus, dass der resultierende Ring $\mathbb{Z}[\zeta]$ für $p > 19$ kein Hauptidealring ist – dies kann als einer der Startpunkte der algebraischen Zahlentheorie angesehen werden, der auf Idealklassentheorie führt, reguläre Primzahlen (nach Kummer) etc., jedoch nicht auf einen einigermaßen elementaren Beweis der Vermutung von Fermat.

Im Jahre 1993 konnte dann A. Wiles einen Beweis der Vermutung von Fermat mit Hilfe modernster Methoden wie Modulformen und Galoisdarstellungen liefern, der zunächst noch eine Lücke enthielt. Diese Lücke konnte dann von Wiles und R. Taylor im Oktober 1994 geschlossen werden[1].

[1]Weitere Einzelheiten findet man in dem populärwissenschaftlichen Buch S. Singh: Fermats letzter Satz. Die abenteuerliche Geschichte eines mathematischen Rätsels. dtv, das sehr zu empfehlen ist.

Kapitel 4

Arithmetik modulo n

4.1 Multiplikative zahlentheoretische Funktionen

Wir hatten gesehen, dass die Eulersche φ-Funktion multiplikativ ist. Es sei dran erinnert, dass $\mathbb{N} = \{1, 2, \ldots\}$.

Definition Eine Funktion $f : \mathbb{N} \to \mathbb{C}$ heißt *multiplikative zahlentheoretische Funktion*, wenn

$$f(1) = 1 \text{ und } f(mn) = f(m)f(n) \text{ für alle } m, n \in \mathbb{N}, (m, n) = 1.$$

Beispiel Die folgenden Funktionen sind multiplikative (zahlentheoretische) Funktionen:

(1) Die ε-Funktion

$$\begin{array}{rccl} \varepsilon: & \mathbb{N} & \longrightarrow & \mathbb{C} \\ & n & \longmapsto & \begin{cases} 1 & \text{für } n = 1, \\ 0 & \text{für } n \geq 2. \end{cases} \end{array}$$

(2) Die Identität $I : \mathbb{N} \to \mathbb{C}$, $I(n) = n$.

(3) Die Einsfunktion $1 : \mathbb{N} \to \mathbb{C}$, $n \mapsto 1$.

(4) Die Eulersche Phi-Funktion φ.

Nutzen: Oft lassen sich Eigenschaften von multiplikativer Funktionen auf den Fall von Primzahlpotenzen p^ℓ reduzieren.

Beispiel Die *Möbiussche μ-Funktion* ist wie folgt definiert:

$$\mu(n) := \begin{cases} 1 & \text{für } n = 1, \\ (-1)^r & \text{für } n = p_1 \cdots p_r, p_i \in \mathbb{P}, p_i \neq p_j, \\ 0 & \text{für } n \text{ nicht quadratfrei.} \end{cases}$$

Für eine Primzahl p gilt $\mu(p) = -1$, $\mu(p^\ell) = 0$ für $\ell > 1$. Man sieht leicht, dass die Möbiussche μ-Funktion eine multiplikative zahlentheoretische Funktion ist.

Definition Es seien f und g multiplikative zahlentheoretische Funktionen. Dann ist die *Faltung* von f und g, in Zeichen $f * g$, definiert durch

$$(f * g)(n) := \sum_{d|n} f(d)g(\frac{n}{d}).$$

(Die Summation wird hier und im Folgenden nur über die positiven Teiler von n durchgeführt.)

Für den folgenden Satz brauchen wir einen Hilfssatz, dessen einfachen Beweis wir als Übungsaufgabe überlassen.

Lemma 4.1 *Es seien m und n teilerfremde positive ganze Zahlen. Dann besitzt jeder Teiler d von mn eine eindeutige Zerlegung $d = d_1 d_2$ mit $d_1|m$, $d_2|n$.*

Satz 4.2 *Die multiplikativen zahlentheoretischen Funktionen bilden bezüglich der Faltung als Verknüpfung eine abelsche Gruppe (mit ε als neutralem Element).*

Beweis. (a) Wir müssen zunächst zeigen, dass mit f und g auch $f * g$ multiplikativ ist. Dazu seien m und n teilerfremd. Nach Lemma 4.1 hat jeder Teiler d von mn eine eindeutige Zerlegung $d = d_1 d_2$ mit

$$d_1|m, \quad d_2|n, \quad (d_1, d_2) = 1, \quad (\frac{m}{d_1}, \frac{n}{d_2}) = 1.$$

Also gilt

$$\begin{aligned}
(f * g)(mn) &= \sum_{d|mn} f(d)g(\frac{mn}{d}) = \sum_{d_1|m}\sum_{d_2|n} f(d_1 d_2)g(\frac{m}{d_1}\cdot\frac{n}{d_2}) \\
&= \sum_{d_1|m}\sum_{d_2|n} f(d_1)f(d_2)g(\frac{m}{d_1})g(\frac{n}{d_2}) \quad (\text{da } f, g \text{ multiplikativ}) \\
&= \left(\sum_{d_1|m} f(d_1)g(\frac{m}{d_1})\right)\left(\sum_{d_2|n} f(d_2)g(\frac{n}{d_2})\right) \\
&= (f * g)(m)\cdot(f * g)(n).
\end{aligned}$$

(b) Zum Beweis der Kommutativität und Assoziativität beachte man, dass man die Faltung auch wie folgt definieren kann:

$$(f * g)(n) = \sum_{\substack{d_1,d_2 \\ d_1 d_2 = n}} f(d_1)g(d_2).$$

Dies zeigt schon die Kommutativität; zudem folgt

$$(f * g * h)(n) = \sum_{\substack{d_1,d_2,d_3 \\ d_1 d_2 d_3 = n}} f(d_1)g(d_2)h(d_3),$$

also die Assoziativität.

(c) Das neutrale Element ist die Funktion ε.

(d) Das inverse Element $\check{f}$ zu einer multiplikativen zahlentheoretischen Funktion definieren wir induktiv:

$$\begin{aligned} \check{f}(1) &:= 1, \\ \check{f}(n) &:= -\sum_{\substack{d|n \\ d>1}} f(d)\check{f}(\frac{n}{d}) \text{ für } n > 1. \end{aligned}$$

Dann gilt

$$(f * \check{f})(n) = \sum_{d|n} f(d)\check{f}(\frac{n}{d}) = f(1)\check{f}(n) + \sum_{\substack{d|n \\ d>1}} f(d)\check{f}(\frac{n}{d}) = \varepsilon(n),$$

wegen $f(1) = 1$. Also folgt $f * \check{f} = \varepsilon$. Noch zu zeigen ist, dass $\check{f}$ multiplikativ ist. Dies zeigen wir induktiv. Es seien m und n teilerfremde positive ganze Zahlen. Wir müssen zeigen:

$$\check{f}(mn) = \check{f}(m)\check{f}(n).$$

Induktionsanfang: Für $m = 1$ oder $n = 1$ ist die Behauptung trivial.

Induktionsannahme: Wir nehmen an, dass die Behauptung für alle Produkte aus Faktoren $< m$ und $\leq n$ bzw. $\leq m$ und $< n$ gilt.

Induktionsschritt: Nach Lemma 4.1 und der Induktionsannahme gilt

$$\begin{aligned}
&\check{f}(mn)\\
&= -\sum_{\substack{d_1|m,d_2|n\\ d_1d_2>1}} f(d_1)f(d_2)\check{f}(\frac{m}{d_1})\check{f}(\frac{n}{d_2})\\
&= -\left(\sum_{\substack{d_1|m\\ d_1>1}} f(d_1)\check{f}(\frac{m}{d_1})\right)\left(\sum_{\substack{d_2|n\\ d_2>1}} f(d_2)\check{f}(\frac{n}{d_2})\right)\\
&\quad -\check{f}(m)\left(\sum_{\substack{d_2|n\\ d_2>1}} f(d_2)\check{f}(\frac{n}{d_2})\right)-\check{f}(n)\left(\sum_{\substack{d_1|m\\ d_1>1}} f(d_1)\check{f}(\frac{m}{d_1})\right)\\
&= -\check{f}(m)\check{f}(n)+\check{f}(m)\check{f}(n)+\check{f}(n)\check{f}(m).
\end{aligned}$$

(Man prüfe, dass mit dem Induktionsanfang in der Tat schon genug vorhanden ist, um die Behauptung für alle teilerfremden Paare (m,n) abzuleiten!) □

Definition Die *summatorische Funktion* einer zahlentheoretischen Funktion f ist definiert als

$$F(n) := \sum_{d|n} f(d) = f * 1.$$

Bemerkung Ist f multiplikativ, so auch F!

Beispiel Für die summatorische Funktion der Möbiusschen μ-Funktion gilt

$$\sum_{d|n}\mu(d) = \begin{cases} 1 & \text{für } n=1,\\ 0 & \text{für } n>1,\end{cases}$$

also

$$\mu * 1 = \varepsilon \quad \text{oder } \breve{\mu} = 1 \quad \text{oder } \check{1} = \mu.$$

Dies folgt für $F = \mu * 1$ aus

$$F(p^\ell) = \sum_{d|p^\ell}\mu(d) = \sum_{0\le\nu\le\ell}\mu(p^\nu) = 1+(-1) = 0 \text{ für } \ell \ge 1.$$

Satz 4.3 (Möbiussche Umkehrformel) *Für die summatorische Funktion F einer multiplikativen zahlentheoretischen Funktion f gilt:*

$$f(n) = \sum_{d|n} F(d)\mu(\frac{n}{d}) \quad \textit{für alle } n\in\mathbb{N}, n>0.$$

Beweis. Aus $F = f * 1$ folgt $f = f * \varepsilon = f * 1 * \mu = F * \mu$. □

Korollar 4.4 *Für die Eulersche φ-Funktion gilt*

$$\sum_{d|n} \varphi(d) = n \quad \textit{für alle } n \in \mathbb{N}, n > 0.$$

Beweis. Es gilt für $\ell > 1$ nach Lemma 1.33

$$\varphi(p^\ell) = p^\ell - p^{\ell-1} = \sum_{0 \le \nu \le \ell} I(p^\nu)\mu(p^{\ell-\nu}) = \sum_{d|p^\ell} I(d)\mu(\frac{p^\ell}{d}).$$

Daraus folgt $\varphi = I * \mu$. Aus der Möbiusschen Umkehrformel folgt $\varphi * 1 = I$. □

4.2 Die Struktur der primen Restklassengruppe

Wir wollen nun noch einmal die prime Restklassengruppe studieren. Es sei m eine positive ganze Zahl und $m = p_1^{e_1} \cdots p_r^{e_r}$ die Primfaktorzerlegung von m. Nach Satz 2.23 und Satz 3.28 gilt

$$\mathbb{Z}_m^* \cong \mathbb{Z}_{p_1^{e_1}}^* \times \cdots \times \mathbb{Z}_{p_r^{e_r}}^*.$$

Um etwas über die Struktur der primen Restklassengruppe zu erfahren, reicht es daher, sich auf Primpotenzen $m = p^\ell$ zu beschränken. Zunächst betrachten wir den Fall $m = p \in \mathbb{P}$. Wir zeigen, dass für eine Primzahl p die prime Restklassengruppe $\mathbb{Z}_p^*$ zyklisch ist. Allgemeiner gilt:

Satz 4.5 *Die multiplikative Gruppe $\mathbb{F}^*$ eines endlichen Körpers $\mathbb{F}$ ist zyklisch. Insbesondere gilt dies für $\mathbb{Z}_p^*$, p eine Primzahl.*

Achtung: Es gibt andere Körper als $\mathbb{Z}_p$!

Definition Ein erzeugendes Element der multiplikativen Gruppe $\mathbb{F}^*$ wird *primitives Element* von $\mathbb{F}$ genannt, im Fall von $\mathbb{Z}_p^*$ auch *Primitivwurzel* mod p. Eine Primitivwurzel mod p ist also ein Element $a \in \mathbb{Z}_p^*$ der Ordnung $p-1$, d.h. es gilt

$$\mathbb{Z}_p^* = \{a, a^2, \ldots, a^{p-2}, a^{p-1} = 1\}.$$

Notation Die von einem Element $a \in G$ einer Gruppe G erzeugte zyklische Gruppe bezeichnen wir mit $\langle a \rangle$.

Beweis von Satz 4.5. Es sei $\mathbb{F}$ ein endlicher Körper und N die Ordnung der Gruppe $\mathbb{F}^*$. Nach Satz 2.4 reicht es zu zeigen, dass es in $\mathbb{F}^*$ ein Element der Ordnung N gibt. Nach Korollar 2.14 teilt die Ordnung d eines Elements von $\mathbb{F}^*$ die Gruppenordnung N. Nach Satz 3.14 hat die Gleichung

$$x^d - 1 = 0 \tag{4.1}$$

im Körper $\mathbb{F}$ höchstens d Lösungen. Gibt es nun ein Element $a \in \mathbb{F}^*$ mit $\operatorname{ord} a = d$, so hat die Gleichung d Lösungen, nämlich $a, a^2, \ldots, a^{d-1}, a^d = 1$. Es gilt für alle $1 \leq m \leq d$

$$\operatorname{ord} a^m = d \Leftrightarrow (m, d) = 1.$$

Nun gibt es genau $\varphi(d)$ positive ganze Zahlen m mit $1 \leq m \leq d$ und $(m, d) = 1$. Nach Satz 2.6 gilt $\langle a \rangle \cong \mathbb{Z}_d$. Wenn es daher eine Lösung der Gleichung (4.1) der Ordnung d gibt, so gibt es genau $\varphi(d)$ Lösungen dieser Gleichung mit Ordnung d.

Wir bezeichnen nun mit $\psi(d)$ die Anzahl der Elemente der Ordnung d in $\mathbb{F}^*$. Dann folgt aus den obigen Argumenten

$$\psi(d) = \begin{cases} 0 & \text{für } d \not| N, \\ 0 \text{ oder } \varphi(d) & \text{für } d | N. \end{cases}$$

Mit Korollar 4.4 folgt nun

$$N = \sum_{d|N} \psi(d) \leq \sum_{d|N} \varphi(d) = N,$$

also $\psi(d) = \varphi(d)$ für alle $d|N$. Daraus folgt insbesondere, dass es Elemente $a \in \mathbb{F}^*$ der Ordnung N geben muss. □

Bemerkung Der Beweis von Satz 4.5, den wir gegeben haben, ist nicht konstruktiv, er gibt keine Methode an, ein primitives Element von $\mathbb{F}$ zu finden.

Nun betrachten wir den Fall $m = p^\ell$. Dazu benötigen wir zunächst einen Hilfssatz. Dabei benutzen wir eine wichtige elementare Tatsache, die wir ebenfalls als Lemma formulieren.

Lemma 4.6 *Es sei p eine Primzahl. Dann sind die Binomialkoeffizienten $\binom{p}{j}$ für $1 \leq j \leq p-1$ durch die Primzahl p teilbar.*

Beweis. Der Binomialkoeffizient

$$\binom{p}{j} = \frac{p(p-1)\cdots(p-j+1)}{1\cdot 2\cdots j}, \quad 1 \le j \le p-1,$$

ist eine ganze Zahl ist und die Primzahl p kann nicht gegen einen Faktor des Nenners, also eine Zahl zwischen 1 und $p-1$, gekürzt werden. □

Lemma 4.7 *Es sei p eine Primzahl, ℓ eine positive ganze Zahl, $a, b \in \mathbb{Z}$. Dann gilt*

(i) $a \equiv b \bmod p^\ell \quad \Rightarrow \quad a^p \equiv b^p \bmod p^{\ell+1}$.

(ii) $\ell \ge 2, p \ne 2 \quad \Rightarrow \quad (1+ap)^{p^{\ell-2}} \equiv 1 + ap^{\ell-1} \bmod p^\ell$.

(iii) *Ist $p \ne 2$ und p kein Teiler von a, so ist die Ordnung von $1+ap$ in $\mathbb{Z}_{p^\ell}^*$ gleich $p^{\ell-1}$.*

(iv) $\ell > 2 \quad \Rightarrow \quad 5^{2^{\ell-3}} \equiv 1 + 2^{\ell-1} \bmod 2^\ell$.

(v) *Ist $\ell > 2$, so ist die Ordnung von 5 in $\mathbb{Z}_{2^\ell}^*$ gleich $2^{\ell-2}$.*

Beweis. (i) Es sei $a \equiv b \bmod p^\ell$. Dann gilt $a = b + kp^\ell$ für ein $k \in \mathbb{Z}$. Dann gilt

$$a^p = b^p + pb^{p-1}kp^\ell + \binom{p}{2} b^{p-2}k^2p^{2\ell} + \ldots + k^p p^{p\ell} = b^p + sp^{\ell+1}$$

für ein $s \in \mathbb{Z}$.

(ii) folgt aus (i) durch Induktion über ℓ.

Induktionsanfang $\ell = 2$ ist trivial.

Induktionsschritt $\ell \to \ell+1$: Nach Induktionsannahme gilt:

$$(1+ap)^{p^{\ell-2}} \equiv 1 + ap^{\ell-1} \bmod p^\ell.$$

Daraus folgt mit Hilfe von (i)

$$(1+ap)^{p^{\ell-1}} = (1+ap)^{p^{\ell-2}\cdot p} \equiv (1+ap^{\ell-1})^p \bmod p^{\ell+1}. \tag{4.2}$$

Nach der binomischen Formel und mit Lemma 4.6 gilt wieder

$$(1+ap^{\ell-1})^p = 1 + ap^\ell + \binom{p}{2} a^2 p^{2(\ell-1)} + \ldots + a^p p^{p(\ell-1)} = 1 + ap^\ell + s'p^{\ell+1}$$

für ein $s' \in \mathbb{Z}$.

(iii) Aus Gleichung (4.2) und (ii) folgt

$$(1+ap)^{p^{\ell-2}\cdot p} \equiv (1+ap^{\ell-1})^p \equiv 1 \bmod p^\ell.$$

Damit teilt die Ordnung von $1+ap$ in $\mathbb{Z}_{p^\ell}^*$ die Zahl $p^{\ell-1}$. Eine kleinere Ordnung kommt aber wegen $p \not| a$ und Behauptung (ii) nicht in Frage.

(iv) wird analog wie (ii) durch Induktion über ℓ bewiesen.

(v) folgt daraus wie (iii) aus (ii). □

Satz 4.8 *Es sei $p > 2$ eine Primzahl und ℓ eine positive ganze Zahl. Dann ist die prime Restklassengruppe $\mathbb{Z}_{p^\ell}^*$ zyklisch.*

Beweis. Wir wissen schon, dass $\mathbb{Z}_p^\times$ zyklisch ist und können daher $\ell > 1$ annehmen. Sei also $g \in \mathbb{Z}$ so gewählt, dass $\langle \bar{g} \rangle = \mathbb{Z}_p^\times$; also hat g Ordnung $p-1$ in $\mathbb{Z}_p^\times$. Wir wollen dies mit der Ordnung von g in $\mathbb{Z}_{p^\ell}^\times$ vergleichen:

$$d := \operatorname{ord}(\bar{g}; \mathbb{Z}_{p^\ell}^\times);$$

Behauptung: $(p-1) \mid d$.

Begründung: Aus $g^d \equiv 1 \mod p^\ell$ folgt natürlich $g^d \equiv 1 \mod p$, also $(p-1) \mid d$ wie behauptet.

Sei also $g = r(p-1)$ mit $r \in \mathbb{N}$. Nach Definition hat g^r Ordnung $p-1$ in $\mathbb{Z}_{p^\ell}^\times$. Insbesondere enthält die prime Restklassengruppe $\mathbb{Z}_{p^\ell}^\times$ eine zyklische Untergruppe C_{p-1} der Ordnung $p-1$. Andererseits gilt nach Lemma 4.7 (iii), dass

$$\mathbb{Z}_{p^\ell}^\times \supset \langle 1+p \rangle \cong C_{p^{\ell-1}}.$$

Mit dem folgenden allgemeinen Hilfslemma können wir schon schließen, dass $\mathbb{Z}_{p^\ell}$ eine zyklische Gruppe der Ordnung $p^{\ell-1}(p-1)$ enthält. Da dies genau der Ordnung von $\mathbb{Z}_{p^\ell}$ entspricht, sind die beiden Gruppen gleich; insbesondere ist die prime Restklassengruppe zyklisch. □

Lemma 4.9 *Sei G eine abelsche Gruppe, welche zyklische Untergruppen C_m, C_n mit teilerfremder Ordnung besitze. Dann gilt $C_{mn} \hookrightarrow G$.*

Beweis. Sei $C_m = \langle g \rangle$, $C_n = \langle h \rangle$. Wir behaupten, dass $\langle gh \rangle \cong C_{mn}$.

Betrachten wir also

$$d = \operatorname{ord}(gh).$$

Es genügt zu zeigen, dass $d = mn$. Da $(gh)^{mn} = (g^m)^n (h^n)^m = 1$, gilt $d \mid mn$. Andererseits wissen wir, dass

$$1 = (hg)^d = g^d h^d, \quad \text{also} \quad g^{-d} = h^d.$$

Folglich $\operatorname{ord}(g^d) = \operatorname{ord}(g^{-d}) = \operatorname{ord}(h^d)$. Dies können wir aber umschreiben als

$$\frac{m}{(m,d)} = \operatorname{ord}(g^d) = \operatorname{ord}(h^d) = \frac{n}{(n,d)}.$$

Da m und n teilerfremd sind, ist dies nur möglich, wenn alle Terme 1 sind. Dies impliziert $m \mid d$ und $n \mid d$, was sich dank der Teilerfremdheit in $mn \mid d$ übersetzt. Dies beweist die Behauptung und somit das Lemma. □

Satz 4.10 *Die prime Restklassengruppe $\mathbb{Z}_{2^\ell}^*$ ist nur für $\ell = 1$ und $\ell = 2$ zyklisch, für $\ell > 2$ gilt*

$$\mathbb{Z}_{2^\ell}^* \cong \langle -1 \rangle \times \langle 5 \rangle.$$

Beweis. Für $\ell = 1$ ist die Behauptung klar. Für $\ell = 2$ gilt

$$\mathbb{Z}_4^* = \{3, 3^2 = 1\}, \quad |\mathbb{Z}_4^*| = 2.$$

Also ist auch in diesem Fall $\mathbb{Z}_{2\ell}^*$ zyklisch und wird von 3 erzeugt.

Für $\ell > 2$ gilt nach Lemma 4.7, dass 5 ein Element von $\mathbb{Z}_{2^\ell}^*$ der Ordnung $2^{\ell-2}$ ist. Die von 5 erzeugte zyklische Untergruppe von $\mathbb{Z}_{2^\ell}^*$ ist

$$\langle 5 \rangle = \{5^j \mid j = 1, 2, \ldots, 2^{\ell-2}\} = \{a \in \mathbb{Z}_{2^\ell}^* \mid a \equiv 1 \bmod 4\} = H,$$

denn: $\langle 5 \rangle \subset H$, da $5^j = (1+4)^j \equiv 1 \bmod 4$, und andererseits gilt

$$\#\langle 5 \rangle = \operatorname{ord}(5) = 2^{\ell-2} = \#H.$$

Letzteres folgt wiederum aus der kanonischen Abbildung

$$\mathbb{Z}_{2^\ell}^\times \to \mathbb{Z}_4^\times = \{\pm 1\},$$

deren Kern nach Definition genau H ist, weswegen $\#H = \#\mathbb{Z}_{2^\ell}^\times / 2$. Dies suggeriert schon den behaupteten Isomorphismus

$$\mathbb{Z}_{2^\ell}^\times \cong \langle -1 \rangle \times H,$$

der sich durch die zueinander inversen Homomorphismen

$$(a,b) \mapsto ab \quad \text{bzw.} \quad x \mapsto \begin{cases} (1,x), & \text{falls } x \equiv 1 \mod 4 \\ (-1,-x) & \text{falls } x \equiv -1 \mod 4 \end{cases}$$

realisieren lässt. Abschließend sieht man leicht, dass für jedes Element $g = (a,b) \in \langle -1 \rangle \times H$ gilt: $g^{2^{\ell-2}} = 1$ (s. Lemma 4.12). Folglich enthält $\mathbb{Z}_{2^\ell}^\times$ kein Element der Gruppenordnung $2^{\ell-1}$ und ist insbesondere nicht zyklisch. □

Damit haben wir eine Richtung des folgenden Satzes bewiesen (man beachte $\mathbb{Z}_{2p^\ell}^* \cong \mathbb{Z}_2^* \times \mathbb{Z}_{p^\ell}^* \cong \mathbb{Z}_{p^\ell}^*$):

Satz 4.11 *Die prime Restklassengruppe $\mathbb{Z}_m^*$ ist genau dann zyklisch, wenn*

$$m = 2, 4, p^\ell \text{ oder } 2p^\ell \text{ für eine Primzahl } p > 2.$$

Um zu zeigen, dass die prime Restklassengruppe nur in den angegebenen Fällen zyklisch ist, brauchen wir zwei Hilfssätze.

Lemma 4.12 *Es sei G das direkte Produkt der Gruppen $G_1, \ldots, G_r$ und*

$$a = (a_1, \ldots, a_r), \quad a_i \in G_i, \quad \operatorname{ord} a_i = n_i.$$

Dann gilt $\operatorname{ord} a = \operatorname{kgV}(n_1, \ldots, n_r)$.

Beweis. Übungsaufgabe. □

Lemma 4.13 *Es sei G das direkte Produkt der Gruppen $G_1, \ldots, G_r$. Dann ist G genau dann zyklisch, wenn alle G_i zyklisch sind mit paarweise teilerfremden Ordnungen.*

Beweis. Es sei a wie in Lemma 4.12. Dann erzeugt a die Gruppe G genau dann, wenn

$$\operatorname{ord} a = |G| = |G_1| \cdots |G_r|.$$

Nach Lemma 4.12 muss dann

$$\operatorname{ord} a_i = n_i = |G_i|, \quad i = 1, \ldots, r, \text{ und } \operatorname{kgV}(n_1, \ldots, n_r) = n_1 \cdots n_r$$

gelten, d.h. $n_1, \ldots, n_r$ sind paarweise teilerfremd (vgl. Korollar 1.8). □

Bemerkung Man vergleiche den Beweis von Lemma 4.9. Essentiell wurde die Eigenschaft, dass G abelsch ist, nur durch die Produktstruktur ersetzt.

Beweis von Satz 4.11. " $\Rightarrow$" Nach Satz 2.23 und Satz 3.28 gilt

$$\mathbb{Z}_m^* \cong \mathbb{Z}_{p_1^{e_1}}^* \times \cdots \times \mathbb{Z}_{p_r^{e_r}}^*,$$

wobei $m = p_1^{e_1} \cdots p_r^{e_r}$. Da die Ordnung von $\mathbb{Z}_{p^\ell}^*$ gerade ist, falls $p^\ell \neq 2$, sind die Ordnungen nicht teilerfremd mit Ausnahme der im Satz genannten Fälle. Damit folgt die Behauptung aus Lemma 4.13. □

Die Ergebnisse aus diesem Abschnitt kann man auf die Lösung von Kongruenzen anwenden:

$$x^n = b \mod m \tag{4.3}$$

für $m, n \in \mathbb{N}, m > 1$ und $b \in \mathbb{Z}$.

Lemma 4.14 *Sei $n \in \mathbb{N}, p \in \mathbb{P}$ und $b \in \mathbb{Z}$ mit $p \nmid b$. Dann hat die Kongruenz*

$$x^n \equiv b \bmod p \tag{4.4}$$

genau dann eine Lösung, wenn

$$b^{\frac{p-1}{(n,p-1)}} \equiv 1 \mod p.$$

Bezeichnung Wenn die Kongruenz 4.4 eine Lösung $x \in \mathbb{Z}$ hat, so nennt man b einen *n-ten Potenzrest* mod p.

Beweis. Wir wenden Satz 4.5 an. Es sei a eine Primitivwurzel mod p und $b \equiv a^z \bmod p$, $x \equiv a^y \bmod p$. Dann gilt

$$x^n \equiv b \bmod p \Leftrightarrow a^{ny} \equiv a^z \bmod p \Leftrightarrow ny \equiv z \bmod (p-1).$$

Nach Korollar 1.30 ist diese Kongruenz genau dann lösbar, wenn

$$d := (n, p-1) | z.$$

Nun gilt

$$d|z \Leftrightarrow (n, p-1)|(z, p-1) \Leftrightarrow \frac{p-1}{(z,p-1)} | \frac{p-1}{(n,p-1)}.$$

Nun ist $m = \frac{p-1}{(z,p-1)}$ die kleinste positive ganze Zahl mit der Eigenschaft $mz \equiv 0 \bmod (p-1)$. Daher gilt

$$d|z \Leftrightarrow b^{\frac{p-1}{(n,p-1)}} \equiv 1 \bmod p.$$

Also ist die Kongruenz (4.4) genau dann lösbar, wenn

$$b^{\frac{p-1}{(n,p-1)}} \equiv 1 \bmod p$$

wie behauptet. □

1. Spezialfall: $n = 2$: In diesem Fall nennt man einen n-ten Potenzrest mod p einen *quadratischen Rest* mod p. In diesem Fall ist b genau dann ein quadratischer Rest mod p, wenn

$$b^{\frac{p-1}{2}} \equiv 1 \bmod p.$$

Korollar 4.15 *Für $p \in \mathbb{P}, p \neq 2$ gibt es jeweils $\frac{p-1}{2}$ quadratische Reste und Nichtreste modulo p.*

2. Spezialfall: $b = -1$ und $n = 2$:

Korollar 4.16 *Die Restklasse* -1 *hat genau dann eine Quadratwurzel in* $\mathbb{Z}_p^*, p > 2$, *wenn* $p \equiv 1 \bmod 4$ *ist.*

(Vergleiche die Strukturen von $\mathbb{Z}[i]$, welche wir in den Übungen hergeleitet haben – etwa wann (p) prim ist!)

3. Spezialfall: $(n, p-1) = 1$

Korollar 4.17 *Die Lösung* x *existiert und ist eindeutig modulo* p.

Beweis. Dies rührt von einem allgemeinen gruppentheoretischen Resultat her. Schreibe

$$1 = (n, p-1) = rn + s(p-1), \quad r, s \in \mathbb{Z}.$$

Dann sind die folgenden Endomorphismen von $\mathbb{Z}_p^\times$ invers zueinander:

$$x \mapsto x^n \quad \text{und} \quad x \mapsto x^r.$$

□

4. Spezialfall: $(n, p-1) = 1, b \equiv 1 \mod p$.

In diesem Fall ist 1 die eindeutige Lösung modulo p (!).

Allgemeiner Fall:

1. Die Argumente von Lemma 4.14 lassen sich direkt auf Kongruenzen modulo $p^\ell (p \neq 2)$ übertragen, da essentiell nur die Eigenschaft genutzt wurde, dass $\mathbb{Z}_p^\times$ (ebenso wie $\mathbb{Z}_{p^\ell}^\times$) zyklisch ist.

2. Allgemeine Kongruenzen (4.3) lässt sich nun mit Hilfe des Chinesischen Restsatzes auf die obige Fälle reduzieren (mit zusätzlichem Augenmerk auf $p = 2$).

Kapitel 5

Körper

5.1 Konstruktionen mit Zirkel und Lineal

Die drei klassischen Probleme der Antike sind die folgenden Konstruktionsprobleme:

(a) **Delisches Problem der Würfelverdoppelung**

Zu einem gegebenen Würfel soll ein Würfel doppelten Volumens konstruiert werden.

Übungsaufgabe Man konstruiere mit Zirkel und Lineal zu einem gegebenen Quadrat ein Quadrat mit dem doppelten Flächeninhalt.

(b) **Dreiteilung des Winkels**

Zu einem Winkel φ soll der Winkel $\frac{\varphi}{3}$ konstruiert werden.

Übungsaufgabe Man konstruiere mit Zirkel und Lineal zu einem Winkel φ den Winkel $\frac{\varphi}{2}$.

(c) **Quadratur des Kreises**

Zu einem gegebenen Kreis soll ein flächengleiches Quadrat konstruiert werden.

Ein weiteres Problem ist die Konstruktion regelmäßiger n-Ecke mit Zirkel und Lineal.

(d) **Konstruktion des regulären n-Ecks**

Einem Kreis soll ein reguläres n-Eck eingeschrieben werden. Man interessiert sich dafür, für welche n ein solches n-Eck mit Zirkel und Lineal konstruiert werden kann.

Übungsaufgabe Man konstruiere mit Zirkel und Lineal ein Quadrat.

Wir wollen nun präzisieren, was wir unter "Konstruieren" (mit Zirkel und Lineal) verstehen wollen. Wir stellen uns die Ebene als komplexe Zahlenebene $\mathbb{C}$ vor. Vorgegeben sei eine nichtleere Menge $M \subset \mathbb{C}$ von Punkten.

Definition Die Menge $\mathcal{K}(M)$ der *aus M (mit Zirkel und Lineal) konstruierbaren Punkte* ist rekursiv wie folgt definiert:

($\mathcal{K}1$) $M \subset \mathcal{K}(M)$.

($\mathcal{K}2$) Sind g_1 und g_2 zwei nicht parallele Geraden durch Punkte $z_1, z_2 \in \mathcal{K}(M)$ bzw. $w_1, w_2 \in \mathcal{K}(M)$ und ist z der Schnittpunkt von g_1 und g_2, so ist $z \in \mathcal{K}(M)$.

($\mathcal{K}3$) Ist g eine Gerade durch die verschiedenen Punkte $z_1, z_2 \in \mathcal{K}(M)$ und k ein Kreis mit Mittelpunkt $w \in \mathcal{K}(M)$ und Radius $|w_2 - w_1|$, wobei $w_1, w_2 \in \mathcal{K}(M)$, und ist z ein Schnittpunkt von g und k, so ist $z \in \mathcal{K}(M)$.

($\mathcal{K}4$) Sind k_1 und k_2 zwei verschiedene Kreise mit Mittelpunkten $z_1, z_2 \in \mathcal{K}(M)$ und Radien $|w_2 - w_1|$ bzw. $|u_2 - u_1|$, wobei $w_1, w_2, u_1, u_2 \in \mathcal{K}(M)$, und ist z ein Schnittpunkt von k_1 und k_2, so ist $z \in \mathcal{K}(M)$.

Die Menge $\mathcal{K}(M)$ ist die Menge aller Punkte, die man durch endlichfache Anwendung der Regeln $\mathcal{K}1$–$\mathcal{K}4$ erhält.

Wir geben nun genaue Formulierungen der oben angeführten vier Probleme.

(a) **Delisches Problem der Würfelverdoppelung**

Die Menge M besteht hier aus den Punkten 0 und a, wobei a die Kantenlänge des Würfels ist. Die Frage lautet dann, ob der Punkt $\sqrt[3]{2} \cdot a$ zu $\mathcal{K}(M)$ gehört.

(b) **Dreiteilung des Winkels**

Die Menge M besteht aus den Punkten $0, 1, \cos\varphi + i \sin\varphi$. Das Problem besteht darin, zu entscheiden, ob der Punkt $\cos\frac{\varphi}{3} + i \sin\frac{\varphi}{3}$ zu $\mathcal{K}(M)$ gehört.

(c) **Quadratur des Kreises**

Hier besteht die Menge aus den Punkten 0 und r, wobei r der Radius des Kreises ist. Die Frage lautet dann, ob der Punkt $r\sqrt{\pi}$ zu $\mathcal{K}(M)$ gehört.

(d) **Konstruktion des regulären n-Ecks**

Die Menge M besteht aus den Punkten $0, 1$. Man hat zu entscheiden, für welche n der Punkt

$$\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

zu $\mathcal{K}(M)$ gehört.

Wir wollen nun voraussetzen, dass $\{0, 1\} \subset M$.

Satz 5.1 *Es sei M eine Menge von komplexen Zahlen mit $0 \in M$ und $1 \in M$. Dann ist die Menge $\mathcal{K}(M)$ der aus M mit Zirkel und Lineal konstruierbaren Punkte ein Unterkörper von $\mathbb{C}$.*

Beweis. Es sind die folgenden Aussagen zu zeigen:

(a) $z_1, z_2 \in \mathcal{K}(M) \Rightarrow z_1 + z_2 \in \mathcal{K}(M)$.

(b) $z \in \mathcal{K}(M) \Rightarrow -z \in \mathcal{K}(M)$.

(c) $z_1, z_2 \in \mathcal{K}(M) \Rightarrow z_1 z_2 \in \mathcal{K}(M)$.

(d) $z \in \mathcal{K}(M), z \neq 0 \Rightarrow \frac{1}{z} \in \mathcal{K}(M)$.

Zu (a): Der Vektor $z_1 + z_2$ ist die Diagonale des von z_1 und z_2 aufgespannten Parallelogramms, das sich aus z_1 und z_2 konstruieren lässt (wie?).

Zu (b): Der Kreis um 0 mit Radius z schneidet die Gerade durch 0 und z in z und $-z$.

Zu (c): Hierzu betrachten wir zunächst zwei positive reelle Zahlen r_1, r_2 und zeigen, dass mit $r_1, r_2 \in \mathcal{K}(M)$ auch $r_1 r_2 \in \mathcal{K}(M)$. Zunächst überlegt man sich, dass zu einer Geraden g und einem Punkt z auf g auch die Senkrechte zu g durch den Punkt z konstruierbar ist. Betrachtet man die Punkte 1 und r_2 auf der reellen Zahlengeraden, errichtet in diesen Punkten die Senkrechten, schlägt um den Punkt 1 einen Kreis vom Radius r_1, so schneidet die Gerade durch 0 und den Schnittpunkt $1 + ir_1$ die Senkrechte durch r_2 nach dem Strahlensatz in $r_2 + ir_1 r_2$ (Skizze!). Damit erhält man $r_1 r_2 \in \mathcal{K}(M)$.

Sind nun $z_1, z_2 \in \mathcal{K}(M)$ durch Polarkoordinaten

$$z_j = r_j(\cos\varphi_j + i\sin\varphi_j), \quad j = 1, 2,$$

gegeben, so ist

$$z_1 z_2 = r_1 r_2(\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2)).$$

Da man Winkel mit Zirkel und Lineal addieren kann, folgt, dass auch $z_1 z_2$ konstruierbar ist.

Zu (d): Es sei $z = r(\cos\varphi + i\sin\varphi) \in \mathcal{K}(M)$, $z \neq 0$. Dann gilt

$$\frac{1}{z} = \frac{1}{r}(\cos(-\varphi) + i\sin(-\varphi)).$$

Den Winkel $-\varphi$ erhält man durch Spiegelung an der reellen Achse, die mit Zirkel und Lineal durchführbar ist. Die Zahl $\frac{1}{r}$ erhält man nach dem Strahlensatz durch

$$\frac{\frac{1}{r}}{1} = \frac{1}{r}.$$

□

Bemerkung Jeder Unterkörper K von $\mathbb{C}$ enthält den Körper $\mathbb{Q}$ der rationalen Zahlen (warum?). Damit sind insbesondere alle rationalen Punkte konstruierbar.

Satz 5.2 *Mit $z \in \mathcal{K}(M)$ ist auch $\sqrt{z} \in \mathcal{K}(M)$. (Man sagt auch, $\mathcal{K}(M)$ ist* quadratisch abgeschlossen.*)*

Beweis. Für $z = r(\cos\varphi + i\sin\varphi)$ gilt

$$\sqrt{z} = \sqrt{r}(\cos\frac{\varphi}{2} + i\sin\frac{\varphi}{2}).$$

Da man die Winkelhalbierende mit Zirkel und Lineal konstruieren kann, genügt es zu zeigen, dass $\sqrt{r} \in \mathcal{K}(M)$. Dazu halbiere man die Strecke von $-r$ bis 1 auf der reellen Achse, schlage einen Kreis durch die Punkte $-r$ und 1 mit diesem Mittelpunkt und bestimme den Schnittpunkt mit der imaginären Achse. Nach dem Satz des Thales und dem Höhensatz von Euklid ist dieser Schnittpunkt $i\sqrt{r}$. □

Es stellt sich nun die Aufgabe, den Unterkörper $\mathcal{K}(M)$ der aus M konstruierbaren Punkte genauer zu charakterisieren. Das werden wir im Laufe der Vorlesung tun.

5.2 Körpererweiterungen

Definition Es sei R ein Ring mit 1. Die *Charakteristik* von R, in Zeichen $\operatorname{char} R$, ist die kleinste natürliche Zahl $q > 0$ (so eine existiert), so dass

$$\underbrace{1 + \cdots + 1}_{q} = 0$$

in R gilt. Wenn es kein solches q gibt, dann definieren wir die Charakteristik von R als 0.

Beispiel $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ haben die Charakteristik 0, $\mathbb{Z}_n$ hat die Charakteristik n.

Satz 5.3 *Die Charakteristik eines Integritätsbereichs ist* 0 *oder eine Primzahl.*

Beweis. Es sei R ein Ring mit 1. Wir betrachten den Ringhomomorphismus $f : \mathbb{Z} \to R$, der wie folgt definiert ist:

$$f(n) = \begin{cases} 1 + \cdots + 1 & (n \text{ mal}) & \text{falls } n > 0, \\ 0 & & \text{falls } n = 0, \\ -1 - \cdots - 1 & (|n| \text{ mal}) & \text{falls } n < 0. \end{cases}$$

Der Kern von f ist ein Ideal in dem Hauptidealring $\mathbb{Z}$, also gilt $\operatorname{Ker} f = (q)$ für ein $q \geq 0$. Diese Zahl q ist die Charakteristik von R. Nach dem Homomorphiesatz gilt

$$\operatorname{Im} f \cong \begin{cases} \mathbb{Z}_q & \text{falls } q \neq 0, \\ \mathbb{Z} & \text{falls } q = 0. \end{cases}$$

Es sei nun R ein Integritätsbereich. Dann ist auch $\operatorname{Im} f$ ein Integritätsbereich, da $\operatorname{Im} f$ ein Unterring von R ist. Nach Satz 3.32 ist $\operatorname{Im} f \cong \mathbb{Z}/(q)$ genau dann ein Integritätsbereich, wenn (q) ein Primideal in $\mathbb{Z}$ ist. Nach Satz 3.31 ist aber (q) genau dann ein Primideal in $\mathbb{Z}$, wenn q eine Primzahl ist oder $q = 0$ gilt. □

Beachte: Ist $R' \subset R$ ein Unterring (mit 1), so erhalten wir eine Einbettung $\operatorname{Im} f \hookrightarrow R'$, d.h. $\operatorname{Im} f$ ist allen Unterringen von R gemein.

Definition Eine Teilmenge k eines Körpers K heißt *Unterkörper* von K, wenn gilt:

(UK0) $0, 1 \in k$

(UK1) Für alle $a, b \in k$ liegt $a - b$ in k.

(UK2) Für alle $a, b \in k$ mit $b \neq 0$ liegt ab^{-1} in k.

Der Körper K heißt dann auch *Oberkörper* von k.

Bemerkung Ein Unterkörper k eines Körpers K ist zusammen mit den auf k induzierten Verknüpfungen $+$ und $\cdot$ ein Körper. Ein Unterkörper eines Körpers K ist ein Unterring k, der auch ein Körper ist.

Definition Ein Körper P heißt *Primkörper*, wenn es keinen Unterkörper Q von P mit $Q \neq P$ gibt.

Für jeden Körper K ist

$$P := \bigcap \{k \mid k \text{ Unterkörper von } K\}$$

ein in K enthaltener Primkörper. Man nennt ihn den (eindeutigen!) *Primkörper* von K.

Satz 5.4 *(a) Ist die Charakteristik eines Körpers K eine Primzahl p, so ist der Primkörper von K isomorph zu $\mathbb{Z}_p$.*

(b) Ist die Charakteristik eines Körpers K gleich Null, so ist der Primkörper isomorph zu $\mathbb{Q}$.

Beweis. (a) Der Körper K enthält den Unterring $\operatorname{Im} f$ (siehe den Beweis des vorhergehenden Satzes). Ist die Charakteristik von K eine Primzahl p, so ist dieser Unterkörper isomorph zu $\mathbb{Z}_p$ (denn $\mathbb{Z}_p \cong \operatorname{Im} f$ ist in jedem Unterkörper von K enthalten).

(b) Ist die Charakteristik des Körpers K gleich Null, so ist der Unterring $\operatorname{Im} f$ isomorph zu $\mathbb{Z}$. Der kleinste Unterkörper, der $\mathbb{Z}$ enthält, ist aber der Körper $\mathbb{Q}$. □

Korollar 5.5 *Die Charakteristik eines endlichen Körpers ist von Null verschieden.*

Korollar 5.6 *Ist K ein Körper mit $\#K = p \in \mathbb{P}$, so folgt $K \cong \mathbb{Z}_p$.*

Definition Ist K ein Unterkörper eines Körpers E, so nennt man E eine *Körpererweiterung* von K. Ein Körper L heißt *Zwischenkörper* der Körpererweiterung $K \subset E$, wenn K ein Unterkörper von L und L ein Unterkörper von E ist.

Notation Wir schreibe für eine Körpererweiterung $K \subset E$ auch E/K.

Satz 5.7 *Es sei K ein Körper und $f(x) \in K[x]$ irreduzibel. Dann ist $E = K[x]/(f(x))$ eine Körpererweiterung von K.*

Beweis. Mit f irreduzibel ist auch das Ideal (f) im Hauptidealring $K[x]$ maximal, also ist E ein Körper. Es sei

$$\widetilde{K} := \{(f(x)) + a_0 \mid a_0 \in K\} \subset E.$$

Dann ist $\widetilde{K}$ ein Unterkörper von E, der isomorph zu K ist. □

Satz 5.8 *Es sei E eine Körpererweiterung des Körpers K. Dann ist E ein Vektorraum über K.*

Beweis. Der Körper E ist eine abelsche Gruppe unter der Addition. Man kann Elemente von E mit Elementen von E multiplizieren, also insbesondere auch mit Elementen in K. Diese skalare Multiplikation genügt den Vektorraumaxiomen. □

Definition Der *Grad* der Körpererweiterung E über K ist die Dimension von E als Vektorraum über K, in Zeichen

$$[E : K] := \dim_K E.$$

Ist $[E : K] < \infty$, dann heißt E eine *endliche* Körpererweiterung von K.

Beispiel $[\mathbb{C} : \mathbb{R}] = 2$. Denn: $\mathbb{C} = \{a + ib \,|\, a, b \in \mathbb{R}\}$ und $\{1, i\}$ ist eine Basis von $\mathbb{C}$ über $\mathbb{R}$.

Satz 5.9 *Es sei K ein Körper, $f(x) \in K[x]$ ein irreduzibles Polynom vom Grad n und $E = K[x]/(f(x))$. Dann gilt $[E : K] = n$.*

Beweis. Dies haben wir schon in Korollar 3.24 bewiesen (ohne die Bedingung, dass E ein Körper ist). □

Erinnerung: Nach Satz 3.23 gilt

$$E = \{a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \,|\, a_0, \ldots, a_{n-1} \in K\}$$

und jedes Element von E kann auf eindeutige Weise so geschrieben werden. Also ist

$$\{1, x, x^2, \ldots, x^{n-1}\}$$

eine Basis von E über K.

Satz 5.10 *Es sei F eine Körpererweiterung von E und E eine Körpererweiterung von K. Dann ist F eine Körpererweiterung von K und*

$$[F : K] = [F : E][E : K].$$

Insbesondere ist die Körpererweiterung F von K genau dann endlich, wenn die Körpererweiterungen F von E und E von K endlich sind.

Beweis. a) Es gilt $K \subset E \subset F$. Ist $[F : E] = \infty$ oder $[E : K] = \infty$, dann gilt auch $[F : K] = \infty$.

b) Es sei $[F : E] = m$ und $\{u_1, \ldots, u_m\}$ eine Basis von F über E, $[E : K] = n$ und $\{v_1, \ldots, v_n\}$ eine Basis von E über K. Wir zeigen, dass

$$\mathcal{B} := \{v_j u_i \,|\, i = 1, \ldots, m,\ j = 1, \ldots, n\}$$

eine Basis von F über K ist.

Es sei $x \in F$. Dann ist $x = \sum_{i=1}^{m} \lambda_i u_i$ für $\lambda_i \in E$. Jedes λ_i kann nun als $\lambda_i = \sum_{j=1}^{n} \mu_{ij} v_j$ mit $\mu_{ij} \in K$ geschrieben werden. Also gilt

$$x = \sum_{i=1}^{m} \sum_{j=1}^{n} \mu_{ij} v_j u_i.$$

Also ist $\mathcal{B}$ ein Erzeugendensystem von F über K.

Es sei nun

$$\sum_{i=1}^{m} \sum_{j=1}^{n} \mu_{ij} v_j u_i = 0, \quad \mu_{ij} \in K.$$

Da $u_1, \ldots, u_m$ linear unabhängig über E sind, folgt, dass für jedes fest gewählte $i = 1, \ldots, m$ gilt: $\sum_{j=1}^{n} \mu_{ij} v_j = 0$. Da $v_1, \ldots, v_n$ linear unabhängig über K sind, folgt $\mu_{ij} = 0$ für jedes i und jedes j. Also ist $\mathcal{B}$ linear unabhängig. □

Definition Es sei E eine Körpererweiterung von K und $A \subset E$ eine Teilmenge. Dann heißt

$$K[A] := \bigcap \{R \,|\, R \text{ Unterring von } E \text{ und } K \cup A \subset R\}$$

der aus K durch *Adjunktion* von A enstandene Unterring von E und

$$K(A) := \bigcap \{F \,|\, F \text{ Unterkörper von } E \text{ und } K \cup A \subset F\}$$

der aus K durch *Adjunktion* von A enstandene Unterkörper von E. Im Falle $A = \{\alpha_1, \ldots, \alpha_n\}$ schreibt man meist $K[\alpha_1, \ldots, \alpha_n]$ und $K(\alpha_1, \ldots, \alpha_n)$.

Analog lässt sich $R_0[A]$ für einen Ring $R_0 \subset E$ definieren (z.B. für $R_0 = \mathbb{Z}$).

Beispiel (a) Es gilt $\mathbb{R}(i) = \mathbb{C}$, da jeder Unterkörper von $\mathbb{C}$, der $\mathbb{R}$ und i enthält, auch alle Elemente der Form $a + ib$, $a, b \in \mathbb{R}$, enthalten muss.

(b) Es gilt $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \,|\, a, b \in \mathbb{Q}\}$.

Um den Zusammenhang von $K[A]$ und $K(A)$ darzustellen, müssen wir zu einem Ring den Körper der Brüche einführen. Es sei R ein Integritätsbereich. Wie man die rationalen Zahlen als Brüche ganzer Zahlen konstruieren kann, so kann man zu R einen Körper, den *Körper der Brüche* $Q(R)$, konstruieren. Dazu betrachten wir

$$M := \{(a, b) \mid a \in R, b \in R \setminus \{0\}\}.$$

Definition Auf M betrachten wir die Relation

$$(a, b) \sim (a', b') \Leftrightarrow ab' = a'b.$$

Satz 5.11 *Die Relation $\sim$ ist eine Äquivalenzrelation auf M.*

Beweis. (R), (S) sind klar.

Zu (T): Es sei $(a, b) \sim (a', b')$, $(a', b') \sim (a'', b'')$. Dann gilt

$$\begin{aligned} (a, b) \sim (a', b') &\Rightarrow ab' = a'b \Rightarrow ab'b'' = a'bb'', \\ (a', b') \sim (a'', b'') &\Rightarrow a'b'' = a''b' \Rightarrow a'bb'' = a''bb'. \end{aligned}$$

Aus den jeweils letzten Gleichungen folgt

$$ab'b'' = a''bb'.$$

Da R ein Integritätsring ist, können wir diese Gleichung durch b' teilen und erhalten $ab'' = a''b$, also $(a, b) \sim (a'', b'')$. □

Die Menge der Äquivalenzklassen bezeichnen wir mit

$$Q(R) := M/\sim .$$

Notation Die zu $(a, b) \in M$ gehörige Äquivalenzklasse bezeichnen wir mit

$$\frac{a}{b} \in Q(R).$$

Damit gilt

$$\frac{a}{b} = \frac{a'}{b'} \Leftrightarrow ab' = a'b.$$

Insbesondere gilt

$$\frac{a}{b} = \frac{ac}{bc} \quad \text{für } \frac{a}{b} \in Q(R), c \in R \setminus \{0\},$$

d.h. man kann Brüche wie gewohnt erweitern und kürzen.

Wir definieren nun eine Addition und eine Multiplikation auf $Q(R)$, indem wir uns an den Bruchrechnungsregeln orientieren:

$$\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}, \quad \frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}.$$

Man rechnet leicht nach, dass die so erklärte Summe und das so erklärte Produkt nicht von der Bruchdarstellung abhängen und dass $Q(R)$ mit dieser Addition und Multiplikation ein Körper ist.

Definition Der Körper $Q(R)$ wird der *Körper der Brüche* (oder *Quotientenkörper*) zu R genannt.

Die Abbildung

$$R \to Q(R), \quad a \mapsto \frac{a}{1},$$

ist ein injektiver Ringhomomorphismus. Man kann daher R als Unterring von $Q(R)$ auffassen.

Beispiel (0) Ist R ein Körper, so gilt $Q(R) = R$.
(1) Für $R = \mathbb{Z}$ erhält man $Q(R) = \mathbb{Q}$, den Körper der rationalen Zahlen.
(2) Für $R = \mathbb{Z}[\sqrt{d}]$ erhält man $Q(R) = \mathbb{Q}(\sqrt{d})$.
(2) Es sei K ein Körper. Dann ist der Polynomring $K[x]$ ein Integritätsring. Seinen Körper der Brüche $Q(K[x])$ bezeichnet man meist mit $K(x)$ und nennt ihn den *Körper der rationalen Funktionen* in der Unbestimmten x mit Koeffizienten aus K.

Satz 5.12 *Es sei E eine Körpererweiterung von K. Dann gilt:*

(i) *Für $\alpha_1, \ldots, \alpha_n \in E$ ist*

$$K[\alpha_1, \ldots, \alpha_n] = \{f(\alpha_1, \ldots, \alpha_n) \mid f \in K[x_1, \ldots, x_n]\}.$$

(ii) *Für jede Teilmenge A von E ist $K(A)$ der Körper der Brüche von $K[A]$. Insbesondere ist also für $\alpha_1, \ldots, \alpha_n \in E$*

$$K(\alpha_1, \ldots, \alpha_n) = \left\{ \frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)} \;\middle|\; \begin{array}{l} f, g \in K[x_1, \ldots, x_n], \\ g(\alpha_1, \ldots, \alpha_n) \neq 0 \end{array} \right\}.$$

Beweis. Zu (i): Es sei

$$R := \{f(\alpha_1, \ldots, \alpha_n) \mid f \in K[x_1, \ldots, x_n]\}.$$

Dann ist R ein Unterring von E mit $K \cup \{\alpha_1, \ldots, \alpha_n\} \subset R$. Daher gilt $K[\alpha_1, \ldots, \alpha_n] \subset R$. Anderseits gilt für jeden Unterring S von E mit $K \cup \{\alpha_1, \ldots, \alpha_n\} \subset S$ auch $R \subset S$. Also folgt $K[\alpha_1, \ldots, \alpha_n] = R$.

Zu (ii): Es sei Q der Körper der Brüche von $K[A]$. Dann können wir Q als Unterkörper von E auffassen, und es gilt $K \cup A \subset Q$. Daher folgt $K(A) \subset Q$. Andererseits muss jeder Unterkörper von E, der $K \cup A$ enthält, auch Q enthalten. Also folgt $K(A) = Q$. □

Bemerkung Man kann damit $K[\alpha_1, \ldots, \alpha_n]$ auch als Bild der Auswertungsabbildung

$$\mathrm{Ev}_{(a_1,\ldots,a_n)} : K[x_1, \ldots, x_n] \to E, \quad f \mapsto f(a_1, \ldots, a_n)$$

beschreiben.

Definition Eine Körpererweiterung E von K heißt *einfach*, wenn es ein $\alpha \in E$ mit $E = K(\alpha)$ gibt. Das Element α heißt dann ein *primitives Element* der Körpererweiterung E von K.

Beispiel (1) Die Körpererweiterung $\mathbb{R} \subset \mathbb{C}$ ist wegen $\mathbb{C} = \mathbb{R}(i)$ einfach, und i ist ein primitives Element dieser Körpererweiterung.

(2) Sind x, y Variablen, so ist die Körpererweiterung $K(x, y)/K$ nicht einfach. (Definiere $K(x, y) = (K(x))(y)$.)

(3) Ist $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ einfach? (Übung!)

5.3 Irreduzible Polynome

Die Frage, ob ein Polynom irreduzibel ist oder nicht, wird im Folgenden sehr wichtig sein. Deswegen wollen wir nun Methoden betrachten, mit denen man diese Frage untersuchen kann. Dabei spielt es eine Rolle, über welchem Koeffizientenring wir das Polynom zerlegen wollen.

Wir erinnern daran, dass wir eine von Null verschiedene Nichteinheit $q \in R^*$ in einem Integritätsring R *irreduzibel* heißt, wenn für jede Darstellung $q = ab$ gilt, dass entweder a oder b eine Einheit ist. Für ein Polynom $f(x) \in R[x]$ bedeutet dies, dass $f(x)$ genau dann irreduzibel ist, wenn sich $f(x)$ nicht als Produkt von zwei Polynomen positiven Grades schreiben lässt und der ggT der Koeffizienten von $f(x)$ gleich 1 (eine Einheit) ist.

Bemerkung Man beachte, dass die Reduzibilität von R abhängt: Das Polynom $2x^2 + 2$ ist irreduzibel als ein Element von $\mathbb{R}[x]$ oder $\mathbb{Q}[x]$, aber reduzibel in $\mathbb{C}[x]$ oder $\mathbb{Z}[x]$.

Nun betrachten wir Polynome mit ganzzahligen Koeffizienten. Wir untersuchen, wann ein solches Polynom irreduzibel über $\mathbb{Q}$ ist.

Definition Ein Polynom $f(x) \in \mathbb{Z}[x]$ heißt *primitiv*, wenn alle seine Koeffizienten teilerfremd sind.

Eine Methode zur Untersuchung der Zerlegung eines Polynoms mit ganzzahligen Koeffizienten ist die Reduktion modulo einer Primzahl p.

Definition Es sei $f(x) \in \mathbb{Z}[x]$ und p eine Primzahl. Das *modulo p reduzierte Polynom* ist das Polynom $\overline{f(x)} \in \mathbb{Z}_p[x]$, das man erhält, wenn man alle Koeffizienten von $f(x)$ durch ihre Restklasse mod p ersetzt.

Bemerkung Die Reduktion mod p definiert einen Ringhomomorphismus

$$\mathbb{Z}[x] \to \mathbb{Z}_p[x], \sum a_n x^n \mapsto \overline{a}_n x^n$$

wobei $\overline{a}_n$ die Restklasse von a_n modulo p ist.

Lemma 5.13 *Sei $f \in \mathbb{Z}[x]$ primitiv. Existiert $p \in \mathbb{P}$ mit $\deg \bar{f} = \deg f$, so dass $\bar{f}$ irreduzibel über $\mathbb{Z}_p$ ist, so ist f irreduzibel über $\mathbb{Z}$.*

Beweis. Sei $f = g \cdot h$ in $\mathbb{Z}[x]$. Gilt $\deg g = 0$, so folgt aus der Primitivität von f schon $g = \pm 1$, und analog für h. Also können wir annehmen, dass $\deg g, \deg h > 0$. Wir haben

$$\bar{f} = \bar{g} \cdot \bar{h} \tag{5.1}$$

und nutzen, dass für jedes $F \in \mathbb{Z}[x]$ gilt:

$$\deg \bar{F} \leq \deg F,$$

wobei Gleichheit genau dann gilt, wenn p den Leitkoeffizienten von F nicht teilt. Auf unsere Situation gemünzt ergibt dies

$$\deg \bar{f} = \deg \bar{g} + \deg bar h \leq \deg g + \deg h = \deg f.$$

Da aber der erste und der letzte Term nach Annahmen gleich sind, folgt schon $\deg g = \deg \bar{g}, \deg h = \deg \bar{h}$, also liefert (5.1) einen Widerspruch zur Irreduzibilität von $\bar{f}$. □

Satz 5.14 (Lemma von Gauß) *Das Produkt zweier primitiver Polynome ist wieder primitiv.*

Beweis. Es seien $f(x), g(x) \in \mathbb{Z}[x]$ primitiv. Dann gilt $f(x)g(x) \in \mathbb{Z}[x]$ mit entsprechendem Grad.

$$\overline{f(x)g(x)} = \overline{f(x)} \cdot \overline{g(x)} = 0 \in \mathbb{Z}_p[x].$$

Da $\mathbb{Z}_p[x]$ ein Integritätsbereich ist, folgt dass $\overline{f(x)} = 0$ oder $\overline{g(x)} = 0$ in $\mathbb{Z}_p[x]$. Also ist $f(x)$ oder $g(x)$ nicht primitiv, ein Widerspruch. □

Korollar 5.15 *Es sei $f(x) \in \mathbb{Z}[x]$.*

(i) *Ist $f(x)$ irreduzibel über $\mathbb{Z}$ mit positivem Grad, so ist $f(x)$ auch irreduzibel über $\mathbb{Q}$.*

(ii) *In $\mathbb{Q}[x]$ gelte die Zerlegung $f(x) = g(x)h(x)$, wobei $g(x) \in \mathbb{Z}[x]$ und $f(x), g(x)$ primitiv sind und alle Polynome positiven Grad haben. Dann ist auch $h(x) \in \mathbb{Z}[x]$ und primitiv.*

Beweis. (i) Die Irreduzibilität (bei positivem Grad) impliziert, dass $f(x)$ primitiv ist. Angenommen, $f(x)$ ist in $\mathbb{Q}[x]$ reduzibel. Indem wir die Koeffizienten auf einen gemeinsamen Hauptnenner bringen und diesen Hauptnenner nach vorne ziehen, können wir annehmen

$$f(x) = \lambda g(x)h(x) \text{ mit } \lambda \in \mathbb{Q}, g(x), h(x) \in \mathbb{Z}[x] \text{ primitiv.}$$

Nach Satz 5.14 ist $g(x)h(x)$ primitiv. Also folgt $\lambda = \pm 1$ und $f(x) = \pm g(x)h(x)$ in $\mathbb{Z}[x]$, ein Widerspruch.

(ii) folgt analog zu (i). □

Satz 5.16 (Kriterium von Eisenstein) *Es sei $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$. Für eine Primzahl p gelte*

(i) *$p|a_0$, $p|a_1$, …, $p|a_{n-1}$,*

(ii) *$p \nmid a_n$ und*

(iii) *$p^2 \nmid a_0$.*

Dann ist $f(x)$ irreduzibel über $\mathbb{Q}$.

Beachte, dass das Eisenstein-Kriterium keine Aussage über die Irreduzibiltät über $\mathbb{Z}$ macht, denn f muss nicht primitiv sein.

Beweis. Angenommen, $f(x)$ ist reduzibel und in $\mathbb{Q}[x]$ gilt die Zerlegung $f(x) = g(x)h(x)$. Nach Korollar 5.15 (ii) können wir annehmen, dass $g(x), h(x) \in \mathbb{Z}[x]$. Reduktion mod p ergibt

$$\overline{g(x)h(x)} = \bar{a}_n x^n.$$

Also muss gelten

$$\overline{g(x)} = bx^k, \quad \overline{h(x)} = cx^{n-k} \text{ für } b, c \in \mathbb{Z}_p, k \in \mathbb{N} \text{ mit } 0 < k < n.$$

Das bedeutet aber, dass die konstanten Glieder von $g(x)$ und $h(x)$ durch p teilbar sind (wie alle Koeffizienten außer dem Leitkoeffizienten). Ihr Produkt ist aber gerade a_0, und das muss deshalb durch p^2 teilbar sein, ein Widerspruch zur Voraussetzung. □

Anwendung Es sei p eine Primzahl und

$$\Phi_p(x) = 1 + x + x^2 + \cdots + x^{p-1} = \frac{x^p - 1}{x - 1}.$$

Dieses Polynom heißt das *p-te Kreisteilungspolynom.*

Behauptung: Das Polynom Φ_p ist irreduzibel über $\mathbb{Q}$.

Beweis. Wir können das Kriterium von Eisenstein nicht direkt auf $\Phi_p(x)$ anwenden. Wir machen zuerst eine Variablentransformation $x = y+1$. Damit erhalten wir

$$\begin{aligned}
\Phi_p(y+1) &= \frac{(y+1)^p - 1}{y} \\
&= \sum_{i=1}^{p} \binom{p}{i} y^{i-1} \\
&= p + \binom{p}{2} y + \cdots + \binom{p}{p-2} y^{p-3} + p y^{p-2} + y^{p-1}.
\end{aligned}$$

Es gilt $p \mid \binom{p}{i}$ für $i = 1, \ldots, p-1$, $p \nmid \binom{p}{p}$, $p^2 \nmid \binom{p}{1}$, also ist $\Phi_p(y+1)$ nach dem Kriterium von Eisenstein irreduzibel. Da $\Phi_p(x)$ genau dann irreduzibel ist, wenn $\Phi_p(y+1)$ irreduzibel ist, ist auch $\Phi_p(x)$ irreduzibel. □

Korollar 5.17 *Für jedes $p \in \mathbb{P}$ ist $E_p = \mathbb{Q}[x]/(\Phi_p)$ eine primitive Körpererweiterung vom Grad $p = 1$ über $\mathbb{Q}$.*

Wir nennen E_p den p-ten Kreisteilungskörper (da E_p offensichtlich alle p-ten Einheitswurzeln aus $\mathbb{C}$ enthält). (Dieser ist implizit auch schon bei der Diskussion der Vermutung von Fermat in 3.9 aufgetaucht.)

Nun betrachten wir die Zerlegung von Polynomen über **endlichen Körpern**.

Um die Wurzeln eines Polynoms in $\mathbb{Z}_p[x]$ zu finden, kann man einfach alle p möglichen Werte für x ausprobieren.

Beispiel Wir betrachten das Polynom $x^2 + 1 \in \mathbb{Z}_3[x]$. Wir stellen eine Wertetabelle auf:

x	0	1	2
x^2	0	1	1
x^2+1	1	2	2

Aus dieser Tabelle ist ersichtlich, dass $x^2 + 1$ keine Wurzeln in $\mathbb{Z}_3$ hat, also irreduzibel in $\mathbb{Z}_3[x]$ ist.

Satz 5.18 *Ein Polynom in $\mathbb{Z}_2[x]$ hat genau dann einen Faktor $(x+1)$, wenn es eine gerade Anzahl von von Null verschiedenen Koeffizienten hat.*

Beweis. Es sei $p(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}_2[x]$. Nach Korollar 3.13 ist $(x + 1)$ genau dann ein Faktor von $p(x)$, wenn $p(1) = 0$. (Man beachte, dass in $\mathbb{Z}_2[x]$ gilt: $x - 1 = x + 1$.) Nun gilt

$$p(1) = a_0 + a_1 + \cdots + a_n.$$

Also ist $p(1) = 0$ genau dann, wenn $p(x)$ eine gerade Anzahl von Koeffizienten, die von Null verschieden sind, hat. □

Beispiel Wir bestimmen alle irreduziblen Polynome vom Grad ≤ 4 über $\mathbb{Z}_2$.

Jedes Polynom vom Grad 1 ist irreduzibel. Die Polynome vom Grad 1 in $\mathbb{Z}_2[x]$ sind x und $x + 1$.

Es sei $p(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}_2[x]$ mit $\text{grad}(p(x)) = n$. Dann gilt $a_n \neq 0$, also $a_n = 1$. Die möglichen Wurzeln sind 0 und 1. Das Element 0 ist genau dann eine Wurzel, wenn $a_0 = 0$ gilt, 1 ist genau dann eine Wurzel, wenn die Anzahl der a_i mit $a_i = 1$, $i = 0, \ldots, n$, gerade ist. Damit haben wir die folgende Liste von Polynomen vom Grad 2,3 und 4 in $\mathbb{Z}_2[x]$ ohne Linearfaktoren:

Grad 2 : $x^2 + x + 1$
Grad 3 : $x^3 + x + 1, x^3 + x^2 + 1$
Grad 4 : $x^4 + x + 1, x^4 + x^2 + 1, x^4 + x^3 + 1, x^4 + x^3 + x^2 + x + 1$

Wenn ein Polynom vom Grad 2 oder 3 reduzibel ist, so muss es einen Linearfaktor haben. Daher sind die obigen Polynome vom Grad 2 oder 3 irreduzibel. Wenn ein Polynom vom Grad 4 reduzibel ist, so hat es entweder einen Linearfaktor oder es ist das Produkt von zwei irreduziblen Polynomen vom Grad

2. Es gibt aber nur ein irreduzibles Polynom vom Grad 2 in $\mathbb{Z}_2[x]$, nämlich $x^2 + x + 1$, und es gilt

$$(x^2 + x + 1)^2 = x^4 + x^2 + 1.$$

Also sind die irreduziblen Polynome vom Grad ≤ 4 über $\mathbb{Z}_2$ die Polynome:

$$\begin{array}{ll} \text{Grad } 1: & x, x+1 \\ \text{Grad } 2: & x^2+x+1 \\ \text{Grad } 3: & x^3+x+1, x^3+x^2+1 \\ \text{Grad } 4: & x^4+x+1, x^4+x^3+1, x^4+x^3+x^2+x+1 \end{array}$$

Korollar 5.19 *Es gibt Körper mit 2, 4, 8 oder 16 Elementen.*

Bemerkung Wir werden später sehen, dass diese jeweils eindeutig sind.

5.4 Algebraische und transzendente Körpererweiterungen

Definition Es sei E eine Körpererweiterung von K. Ein Element $\alpha \in E$ heißt *algebraisch* über K, wenn es ein Polynom $0 \neq f(x) \in K[x]$ gibt mit $f(\alpha) = 0$. Anderenfalls heißt α *transzendent*.

Beispiel Ist $\alpha \in K$, so ist α algebraisch über K.

Bemerkung Ist α algebraisch, dann gibt es also $a_0, a_1, \ldots, a_n \in K$, so dass α die Gleichung

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$$

erfüllt.

Beispiel Die Zahlen $\sqrt{2}$ und i sind algebraisch über $\mathbb{Q}$. (Sie sind Wurzeln von $x^2 - 2$ und $x^2 + 1$.) F. v. Lindemann ($\star$ 1852 Hannover, † 1939) hat 1882 bewiesen, dass π transzendent ist.

Satz 5.20 *Es sei E eine Körpererweiterung von K und $\alpha \in E$ algebraisch über K. Dann gibt es ein eindeutig bestimmtes Polynom $\mu_\alpha(x) \in K[x]$ mit den folgenden Eigenschaften:*

(i) *$\mu_\alpha(x)$ ist ein vom Nullpolynom verschiedenes Polynom minimalen Grades mit α als Wurzel.*

(ii) *$\mu_\alpha(x)$ ist Teiler jedes Polynoms aus $K[x]$, das α als Wurzel besitzt.*

(iii) $\mu_\alpha(x)$ *ist* normiert*, d.h. der Leitkoeffizient von* $\mu_\alpha(x)$ *ist 1.*

Definition Das Polynom $\mu_\alpha(x)$ heißt das *Minimalpolynom* von α über K. Ist der Körper K nicht fest/klar, so schreiben wir auch $\mu_{\alpha/K}$.

Beweis. Wir betrachte die Evaluierungsabbildung

$$\mathrm{ev}_\alpha : K[x] \to E, f(x) \mapsto f(\alpha).$$

Der Kern ist ein Ideal $I \subset K[x]$ und da $K[x]$ ein Hauptidealring ist, gibt es genau ein normiertes Polynom $\mu_\alpha(x)$, welches dieses Ideal erzeugt. Da α algebraisch ist, existiert ein $0 \neq f \in K[x]$ mit $f(\alpha) = 0$, folglich $f \in I \neq (0)$ und $\mu_\alpha \neq 0$. Damit hat das Polynom $\mu_\alpha(x)$ die in dem Satz beschriebenen Eigenschaften. □

Bemerkung Der Beweis zeigt, dass wir nicht beide Bedingungen (i) und (ii) benötigen, sondern dass eine schon genügt.

Satz 5.21 *Es sei E eine Körpererweiterung von K und $\alpha \in E$ algebraisch über K. Ein Polynom $f(x) \in K[x]$ ist genau dann das Minimalpolynom von α über K, wenn $f(\alpha) = 0$ und $f(x)$ irreduzibel (über K) und normiert ist.*

Beweis. "⇒": Es sei $f(x)$ das Minimalpolynom von α über K. Angenommen, $f(x) = p(x)q(x)$. Aus $f(\alpha) = 0$ folgt dann $p(\alpha) = 0$ oder $q(\alpha) = 0$. Da der Grad von $f(x)$ minimal ist, folgt $\operatorname{grad} p(x) = \operatorname{grad} f(x)$ oder $\operatorname{grad} q(x) = \operatorname{grad} f(x)$. Das bedeutet aber, dass $q(x)$ oder $p(x)$ eine Einheit ist.

"⇐": Es sei $f(x)$ ein normiertes irreduzibles Polynom mit $f(\alpha) = 0$. Dann muss der Grad von $f(x)$ minimal unter den Polynomen aus $K[x]$ mit α als Wurzel sein. In dem Beweis des letzten Satzes haben wir gesehen, dass ein Polynom minimalen Grades mit α als Wurzel Teiler jedes Polynoms von $K[x]$, das α als Wurzel hat, ist (s. die folgende Bemerkung). Also ist $f(x)$ das Minimalpolynom von α. □

Satz 5.22 *Es sei E eine Körpererweiterung von K, $\alpha \in E$ algebraisch über K und $f(x)$ ein irreduzibles Polynom vom Grad n über K mit α als Wurzel. Dann gilt*

$$K(\alpha) \cong K[x]/(f(x))$$

und die Elemente von $K(\alpha)$ können in eindeutiger Weise in der folgenden Form geschrieben werden:

$$c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}, \quad c_i \in K.$$

Insbesondere gilt dann auch

$$K(\alpha) = K[\alpha] = \{g(\alpha) \mid g(x) \in K[x]\}.$$

Beweis. Wir definieren eine Abbildung $\varphi : K[x] \to K(\alpha)$ durch $q(x) \mapsto q(\alpha)$. Dann ist φ ein Ringhomomorphismus, also ist $\operatorname{Ker}\varphi$ ein Ideal von $K[x]$. Nach Korollar 3.20 sind alle Ideale in $K[x]$ Hauptideale. Daher gilt

$$\operatorname{Ker}\varphi = (r(x)), \quad r(x) \in K[x].$$

Da $f(\alpha) = 0$, gilt $f(x) \in \operatorname{Ker}\varphi$ und $r(x)|f(x)$. Da $f(x)$ irreduzibel ist, folgt $f(x) = kr(x)$ für ein $k \in K$ mit $k \neq 0$. Also gilt

$$\operatorname{Ker}\varphi = (f(x)).$$

Nach dem Homomorphiesatz für Ringe folgt

$$K[x]/(f(x)) \cong \operatorname{Im}\varphi \subset K(\alpha).$$

Nach Satz 3.39 ist $K[x]/(f(x))$ ein Körper. Daher ist $\operatorname{Im}\varphi$ ein Unterkörper von $K(\alpha)$, der K und α enthält. Da aber $K(\alpha)$ nach Definition der kleinste Körper ist, der K und α enthält, folgt

$$K[x]/(f(x)) \cong \operatorname{im}\varphi = K(\alpha).$$

Die Darstellung der Elemente von $K(\alpha)$ folgt aus diesem Isomorphismus und Satz 3.23. □

Korollar 5.23 *Ist n der Grad des Minimalpolynoms von α über K, so gilt:*

$$[K(\alpha) : K] = n.$$

Beweis. Aus den Sätzen 5.22 und 5.9 folgt:

$$[K(\alpha) : K] = [K[x]/(\mu_\alpha(x)) : K] = n.$$

□

Beispiel Es gilt $\mathbb{Q}(\sqrt[n]{2}) \cong \mathbb{Q}[x]/(x^n - 2)$ und $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$. (Wieso ist das Polynom irreduzibel über $\mathbb{Q}$?)

Definition Eine Körpererweiterung E von K heißt *algebraisch*, wenn jedes Element von E algebraisch über K ist. Sie heißt *transzendent*, wenn sie nicht algebraisch ist, d.h. wenn es ein über K transzendentes Element von E gibt.

Satz 5.24 *Es sei E eine Körpererweiterung von K. Dann gilt:*

(i) *Ist die Körpererweiterung endlich, so ist sie algebraisch und es gibt $\alpha_1, \ldots, \alpha_n \in E$ mit $E = K(\alpha_1, \ldots, \alpha_n)$.*

(ii) *Gibt es über K algebraische Elemente $\alpha_1, \ldots, \alpha_n \in E$ mit $E = K(\alpha_1, \ldots, \alpha_n)$, so ist die Körpererweiterung endlich und damit algebraisch.*

Achtung: Es gibt algebraische unendliche Körpererweiterungen.

Beweis. Zu (i): Ist $m := [E : K]$, so sind für jedes $\alpha \in E$ die Elemente

$$1, \alpha, \alpha^2, \ldots, \alpha^m$$

linear abhängig über K. Zu jedem $\alpha \in E$ gibt es daher ein vom Nullpolynom verschiedenes Polynom $f(x) \in K[x]$ mit $f(\alpha) = 0$. Also ist die Körpererweiterung E von K algebraisch. Ist $\{\alpha_1, \ldots, \alpha_m\} \subset E$ eine Basis des K-Vektorraums E, so gilt $E = K(\alpha_1, \ldots, \alpha_m)$.

Zu (ii): Beweis durch Induktion nach n: Ist $\alpha \in E$ algebraisch über K und gilt $E = K(\alpha)$, so gilt $[E : K] < \infty$ nach Korollar 5.23. Es sei nun $n > 0$ und die Behauptung sei richtig für alle Körpererweiterungen F von K, bei denen F durch Adjunktion von n über K algebraischen Elementen an K entstanden ist. Es sei nun $E = K(\alpha_1, \ldots, \alpha_{n+1})$ mit über K algebraischen Elementen $\alpha_1, \ldots, \alpha_{n+1} \in E$. Dann gilt

$$K(\alpha_1, \ldots, \alpha_{n+1}) = K(\alpha_1, \ldots, \alpha_n)(\alpha_{n+1})$$

und α_{n+1} ist auch algebraisch über $K(\alpha_1, \ldots, \alpha_n)$. Nach Satz 5.10, Korollar 5.23 und der Induktionsannahme gilt

$$\begin{aligned}&[K(\alpha_1, \ldots, \alpha_{n+1}) : K] \\ &\quad = \ [K(\alpha_1, \ldots, \alpha_{n+1}) : K(\alpha_1, \ldots, \alpha_n)][K(\alpha_1, \ldots, \alpha_n) : K] < \infty.\end{aligned}$$

□

Korollar 5.25 *Es sei E eine Körpererweiterung von K und F eine Körpererweiterung von E. Dann ist F genau dann algebraisch über K, wenn F algebraisch über E und E algebraisch über K ist.*

Beweis.

"$\Rightarrow$" ist klar.

"$\Leftarrow$": Es sei $\alpha \in F$. Da F algebraisch über E ist, gibt es $a_0, \ldots, a_n \in E$ mit

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0.$$

Dann ist α auch algebraisch über $K(a_0, \ldots, a_n)$. Da E algebraisch über K ist, sind $a_0, \ldots, a_n$ algebraisch über K und aus Satz 5.24 folgt

$$[K(\alpha) : K] \leq [K(a_0, \ldots, a_n)(\alpha) : K(a_0, \ldots, a_n)][K(a_0, \ldots, a_n) : K] < \infty.$$

Also ist α algebraisch über K. □

Korollar 5.26 *Es sei E eine Körpererweiterung von K und L die Menge aller über K algebraischen Elemente von E. Dann gilt:*

(i) *L ist ein Zwischenkörper von $K \subset E$.*

(ii) *Die Körpererweiterung L von K ist algebraisch.*

(iii) *Ist $\alpha \in E$ algebraisch über L, so gilt $\alpha \in L$.*

Bezeichnung: L heißt der algebraische Abschluss von K in E.

Beweis. Zu (i): Die Inklusion $K \subset L$ ist trivial. Wir müssen zeigen, dass L ein Unterkörper von E ist. Dazu seien $a, b \in L$. Nach Satz 5.24(ii) ist die Körpererweiterung $K(a, b)$ von K algebraisch. Nun gilt

$$a - b \in K(a, b) \text{ und } ab^{-1} \in K(a, b) \text{ (falls } b \neq 0).$$

Wegen $K(a, b) \subset L$ folgt damit auch $a - b \in L$ und $ab^{-1} \in L$.

(ii) ist klar.

Zu (iii): Es sei $\alpha \in E$ algebraisch über L. Dann ist nach Satz 5.24(ii) die Körpererweiterung $L(\alpha)$ von L algebraisch. Nach (ii) und Korollar 5.25 ist dann α algebraisch über K und liegt daher in L. □

Beispiel Die algebraischen Zahlen über $\mathbb{Q}$ definieren einen Zwischenkörper $\overline{\mathbb{Q}}$ mit

$$\mathbb{Q} \subset \overline{\mathbb{Q}} = \{\alpha \in \mathbb{C}; \alpha \text{ ist algebraisch über } \mathbb{Q}\} \subset \mathbb{C},$$

den algebraischen Abschluss von $\mathbb{Q}$ (in $\mathbb{C}$). Da jedes Element aus $\overline{\mathbb{Q}}$ Nullstelle eines Polynoms in $\mathbb{Q}[x]$ ist und letztere Menge abzählbar ist, folgt einfach, dass $\overline{\mathbb{Q}}$ abzählbar ist. Da $\mathbb{C}$ überabzählbar ist, ergibt dies sofort die *Existenz* von transzendenten Zahlen. Nachzuweisen, dass eine gegebene Zahl wie π transzendent ist, kann dagegen ein sehr schwieriges Problem sein.

5.5 Anwendung auf Konstruktionen mit Zirkel und Lineal

Wir wollen nun die bisherige Theorie auf die in §5.1 betrachteten Probleme der Konstruktion mit Zirkel und Lineal anwenden. Wir erinnern an die dortige Aufgabenstellung.

Gegeben ist eine nichtleere Teilmenge $M \subset \mathbb{C}$. Wir hatten definiert, was wir unter der Menge $\mathcal{K}(M)$ der aus M mit Zirkel und Lineal konstruierbaren Punkte verstehen wollen. Wir hatten außerdem vorausgesetzt, dass

$\{0,1\} \subset M$. Wir hatten dann gesehen, dass die Menge $\mathcal{K}(M)$ ein quadratisch abgeschlossener Unterkörper von $\mathbb{C}$ ist. Wir wollen nun diesen Unterkörper charakterisieren.

Mit $\overline{M} = \{\overline{z}; z \in M\}$ bezeichnen wir die Menge der konjugiert komplexen Zahlen $\overline{z}$ für $z \in M$. Da sie durch Spiegelung an der reellen Achse entstehen, sind sie konstruierbar, d.h. es gilt $\overline{M} \subset \mathcal{K}(M)$. Wir setzen nun

$$K_0 = \mathbb{Q}(M \cup \overline{M}).$$

Dann gilt $K_0 \subset \mathcal{K}(M)$.

Lemma 5.27 *Es gilt* $\overline{K_0} = K_0$.

Beweis. Die komplexe Konjugation $\bar{\cdot} : \mathbb{C} \to \mathbb{C}$, $z \mapsto \overline{z}$, ist ein Körperautomorphismus von $\mathbb{C}$. Daraus folgt, dass $\overline{K_0} = \{\overline{z} \,|\, z \in K_0\}$ ebenfalls ein Unterkörper von $\mathbb{C}$ ist. Aus $M, \overline{M} \subset K_0$ folgt $\overline{M}, M \subset \overline{K_0}$. Damit ergibt sich $K_0 \subset \overline{K_0}$. Die andere Inklusion $\overline{K_0} \subset K_0$ erhält man aus $\overline{K_0} \subset \overline{\overline{K_0}} = K_0$. □

Lemma 5.28 *Es sei L ein Unterkörper von $\mathbb{C}$ mit $L = \overline{L}$ und $i \in L$. Ist dann $z \in \mathbb{C}$ durch einen der elementaren Schritte (K2)–(K4) aus der Definition von $\mathcal{K}(M)$ aus L konstruierbar, so gibt es ein $w \in \mathbb{C}$ mit $w^2 \in L$ und $z \in L(w)$.*

Beweis. Zunächst bemerken wir, dass wegen der Voraussetzung $i \in L$ und $L = \overline{L}$ mit z auch Real- und Imaginärteil von z in L liegen, denn es gilt:

$$\mathrm{Re}(z) = \frac{1}{2}(z + \overline{z}), \quad \mathrm{Im}(z) = \frac{1}{2i}(z - \overline{z}).$$

Nun weisen wir die Behauptung für jeden einzelnen Konstruktionsschritt nach:

($\mathcal{K}2$): Es seien g_1 und g_2 zwei nicht parallele Geraden durch Punkte $z_1, z_2 \in L$ bzw. $w_1, w_2 \in L$ und z der Schnittpunkt von g_1 und g_2. Dann existieren $\lambda, \mu \in \mathbb{R}$ mit

$$z = z_1 + \lambda(z_2 - z_1) = w_1 + \mu(w_2 - w_1).$$

Zerlegen wir z_j und w_j in Real- und Imaginärteil $z_j = x_j + iy_j$, $w_j = x'_j + iy'_j$, $j = 1, 2$, so erhalten wir das folgende inhomogene Gleichungssystem für λ und μ:

$$\begin{aligned} x_1 + \lambda(x_2 - x_1) &= x'_1 + \mu(x'_2 - x'_1), \\ y_1 + \lambda(y_2 - y_1) &= y'_1 + \mu(y'_2 - y'_1). \end{aligned}$$

Hierbei gehören die Koeffizienten x_j, x'_j, y_j, y'_j zu $L \cap \mathbb{R}$ $(j = 1, 2)$. Damit gehören auch die Lösungen λ, μ zu $L \cap \mathbb{R}$. Also folgt $z \in L$.

($\mathcal{K}3$) Es sei nun g eine Gerade durch die verschiedenen Punkte $z_1, z_2 \in L$, k ein Kreis mit Mittelpunkt $w_1 \in L$ und Radius $|w_3 - w_2|$, wobei $w_2, w_3 \in L$ und z ein Schnittpunkt von g und k. Mit $\rho := |w_3 - w_2|$, $z_j = x_j + iy_j$, $j = 1, 2$, und $w_1 = a + ib$ folgt, dass es ein $\lambda \in \mathbb{R}$ gibt mit

$$(x_1 + \lambda(x_2 - x_1) - a)^2 + (y_1 + \lambda(y_2 - y_1) - b)^2 = \rho^2.$$

Diese quadratische Gleichung für λ. bringt man auf die Form

$$\lambda^2 + p\lambda + q = 0 \quad (p, q \in L)$$

mit den Lösungen

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

Setzen wir $w := \sqrt{\frac{p^2}{4} - q}$, so folgt $\lambda_{1,2} \in L(w)$ und damit auch $z \in L(w)$.

($\mathcal{K}4$) Es seien k_1 und k_2 zwei verschiedene Kreise mit verschiedenen Mittelpunkten $z_1, z_2 \in L$ und Radien $|w_2 - w_1|$ bzw. $|u_2 - u_1|$, wobei $w_1, w_2, u_1, u_2 \in L$, und z ein Schnittpunkt von k_1 und k_2. Mit $z = x + iy$, $z_j = x_j + iy_j$, $\rho_1 := |w_2 - w_1|$ und $\rho_2 := |u_2 - u_1|$ folgt

$$\begin{aligned} (x - x_1)^2 + (y - y_1)^2 &= \rho_1^2, \\ (x - x_2)^2 + (y - y_2)^2 &= \rho_2^2. \end{aligned}$$

Durch Subtraktion erhält man eine lineare Gleichung

$$(x_1 - x_2)x + (y_1 - y_2)y = c \quad (c \in L).$$

Da die Mittelpunkte der Kreise $z_1 = x_1 + iy_1$ und $z_2 = x_2 + iy_2$ verschieden sind, beschreibt diese Gleichung eine Gerade. Da z ein Schnittpunkt dieser Geraden mit k_1 ist, kann man wie im Fall ($\mathcal{K}3$) schließen. □

Satz 5.29 *Es sei M eine Teilmenge von $\mathbb{C}$ mit $\{0, 1\} \subset M$, $z \in \mathbb{C}$. Dann sind die folgenden Aussagen äquivalent:*

(i) $z \in \mathcal{K}(M)$.

(ii) *Es gibt eine Kette*

$$K_0 = \mathbb{Q}(M \cup \overline{M}) \subset K_1 \subset \ldots \subset K_m \subset \mathbb{C}$$

von Zwischenkörpern mit $z \in K_m$ und $K_j = K_{j-1}$ oder $[K_j : K_{j-1}] = 2$ für $j = 1, \ldots, m$.

Beweis.

(ii) $\Rightarrow$ (i): Wenn $[K_j : K_{j-1}] = 2$, so entsteht K_j aus K_{j-1} durch Adjunktion einer Quadratwurzel eines Elements von K_{j-1} (Übungsaufgabe). Nach Satz 5.2 folgt $K_m \subset \mathcal{K}(M)$.

(i) $\Rightarrow$ (ii): Es sei nun $z \in \mathcal{K}(M)$. Dann entsteht z durch endlichfache Anwendung eines der Konstruktionsschritte ($\mathcal{K}2$)–($\mathcal{K}4$) aus M. Nach Lemma 5.27 gilt $K_0 = \overline{K}_0$. Nun setzen wir $K_1 := K_0(i)$. Ist $i \in K_0$, so gilt $K_1 = K_0$, andernfalls gilt $[K_1 : K_0] = 2$ und in jedem Fall $K_1 = \overline{K}_1$. Ist nun z_1 der Punkt, der durch Anwendung eines der Konstruktionsschritte ($\mathcal{K}2$)–($\mathcal{K}4$) aus M entsteht, so gibt es nach Lemma 5.28 ein $w_1 \in \mathbb{C}$ mit $w_1^2 \in K_1$, so dass $z_1 \in K_1(w_1)$. Wir setzen $K_2 = K_1(w_1)$. Dann ist der Grad $[K_2 : K_1]$ gleich 1 oder 2. Da $K_1 = \overline{K}_1$ ist, ist mit $w_1^2 \in K_1$ auch $\overline{w}_1^2 \in K_1$. Setzen wir nun $K_3 = K_1(w_1, \overline{w}_1)$, so hat auch $[K_3 : K_2]$ den Grad ≤ 2. Ferner gilt $\overline{K}_3 = K_3$. Wir können nun dieses Verfahren fortsetzen und erhalten so eine Kette von Zwischenkörpern von $K_0 \subset \mathbb{C}$ mit den gewünschten Eigenschaften. □

Korollar 5.30 *Es sei M eine Teilmenge von $\mathbb{C}$ mit $\{0, 1\} \subset M$, $K_0 = \mathbb{Q}(M \cup \overline{M})$ und $z \in \mathcal{K}(M)$. Dann ist der Grad der Körpererweiterung $K_0 \subset K_0(z)$ eine Potenz von 2. Insbesondere ist z algebraisch über K_0.*

Wir sind nun in der Lage, die in §2 genannten klassischen Probleme zu behandeln.

(a) Delisches Problem der Würfelverdoppelung

Wir zeigen, dass das Delische Problem der Würfelverdopplung unlösbar ist. Die Menge M besteht hier aus den Punkten 0 und a, wobei a die Kantenlänge des Würfels ist. Es reicht, den Fall $a = 1$ zu behandeln. Es ist also zu entscheiden, ob der Punkt $b := \sqrt[3]{2}$ zu $\mathcal{K}(M)$ gehört. Die Zahl b ist Nullstelle des Polynoms

$$f(x) = x^3 - 2 \in \mathbb{Z}[x].$$

Nach dem Kriterium von Eisenstein ist $f(x)$ irreduzibel über $\mathbb{Z}$ und nach Korollar 5.15 irreduzibel über $\mathbb{Q}[x]$. Also ist $f(x) = \mu_b$ das Minimalpolynom von b über $\mathbb{Q}$ und es folgt

$$[\mathbb{Q}(b) : \mathbb{Q}] = 3.$$

Nach Korollar 5.30 liegt b nicht in $\mathcal{K}(M)$.

(b) **Dreiteilung des Winkels**

Wir zeigen, dass die Dreiteilung des Winkels im Allgemeinen unmöglich ist. Die Menge M besteht hier aus den Punkten $0, 1, \zeta$ mit $\zeta = \cos\varphi + i\sin\varphi$. Das Problem besteht darin, zu entscheiden, ob der Punkt $\cos\frac{\varphi}{3} + i\sin\frac{\varphi}{3}$ zu $\mathcal{K}(M)$ gehört. Wegen $\overline{\zeta} = \zeta^{-1}$ ist $\mathbb{Q}(M \cup \overline{M}) = \mathbb{Q}(\zeta)$. Nach Satz 5.29 kann φ genau dann nicht dreigeteilt werden, wenn das Polynom

$$x^3 - \zeta \in \mathbb{Q}(\zeta)[x]$$

irreduzibel ist. Es ist zu erwarten, dass dies von ζ abhängen wird. Wir geben nun ein konkretes Beispiel eines Winkels φ, der sich nicht dreiteilen lässt, an. Es sei $\alpha := \frac{\varphi}{3}$ und $c = \cos\varphi$. Dann reicht es zu zeigen, dass $\cos\alpha$ nicht aus $M' := \{0, 1, c\}$ konstruierbar ist. Nun gilt

$$\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha.$$

Damit ist $\cos\alpha$ Nullstelle des Polynoms

$$4x^3 - 3x - c \in \mathbb{Q}(c)[x].$$

Nun betrachten wir $\varphi = \frac{\pi}{3}$. Dann ist $c = \cos\varphi = \frac{1}{2}$ und es genügt zu zeigen, dass das Polynom

$$8x^3 - 6x - 1 \in \mathbb{Q}[x]$$

irreduzibel in $\mathbb{Q}[x]$ ist. Dies prüft man durch Substitution $y = 2x$ und Reduktion modulo 2 nach.

Betrachtet man dagegen den Winkel $\varphi = \pi$ so ergibt sich $\cos(\varphi) = -1$. Das Polynom

$$f(x) = 4x^3 - 3x + 1 \in \mathbb{Q}[x]$$

ist reduzibel, da $f(-1) = 0$. In der Tat ist der Winkel π mit Hilfe von Zirkel und Lineal durch 3 teilbar, da man mit Hilfe eines gleichseitigen Dreieicks einen 60°-Winkel konstruieren kann.

(c) **Quadratur des Kreises**

Die Quadratur des Kreises ist unmöglich. Es genügt, den Fall eines Kreises vom Radius 1 zu betrachten. Dann ist $M = \{0, 1\}$ und es ist zu entscheiden, ob $\sqrt{\pi}$ zu $\mathcal{K}(M)$ gehört. Wäre $\sqrt{\pi}$ aus M konstruierbar, so wäre auch π aus M konstruierbar und somit nach Korollar 5.30 algebraisch über $\mathbb{Q}$. Die Zahl π ist aber transzendent.

(d) **Konstruktion des regulären n-Ecks**

Die Menge M besteht aus den Punkten $0, 1$. Man hat zu entscheiden, für welche n der Punkt

$$\zeta_n := \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

zu $\mathcal{K}(M)$ gehört. Es sei p eine Primzahl. Dann ist nach Beispiel das Polynom

$$x^{p-1} + x^{p-2} + \cdots + x + 1$$

über $\mathbb{Q}$ irreduzibel. Daher gilt

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1.$$

Wir erhalten damit:

Satz 5.31 *Die Konstruktion des regulären p-Ecks mit Zirkel und Lineal ist sicher dann nicht möglich, wenn p eine Primzahl ist, für die $p-1$ keine Potenz von 2 ist.*

Primzahlen dieser Art sind z.B. 7, 11, 13, 19, 23. Um ein genaues Kriterium für die Konstruierbarkeit abzuleiten, braucht man die Galoistheorie (und auch für allgemeines $n \in \mathbb{N}$).

5.6 Zerfällungskörper

Definition Es sei K ein Körper und $f(x) \in K[x]$ ein nicht konstantes Polynom. Eine Körpererweiterung E von K heißt *Zerfällungskörper* von $f(x)$ über K, wenn gilt:

(a) Das Polynom $f(x)$ zerfällt über E in Linearfaktoren, d.h.

$$\text{es gibt } \alpha_1, \ldots, \alpha_n \in E \text{ und } b \in K \text{ mit } f(x) = b(x-\alpha_1)\cdots(x-\alpha_n).$$

(b) Der Körper E ist minimal mit dieser Eigenschaft, d.h. $f(x)$ zerfällt über keinem echten Zwischenkörper von $K \subset E$ in Linearfaktoren.

Beispiel Der Zerfällungskörper des Polynoms x^2+1 über $\mathbb{R}$ ist der Körper $\mathbb{C}$ der komplexen Zahlen.

Kriterium: Sei $f \in K[x]$ und eine Körpererweiterung E/K gegeben, über der f zerfällt. Zerfällt f nicht schon über K und gilt $[E : K] \in \mathbb{P}$, so ist E Zerfällungskörper von f über K.

Ziel dieses Abschnitts ist, die Existenz und Eindeutigkeit des Zerfällungskörper zu einem nicht konstanten Polynom zu zeigen. Dazu dienen die folgenden Vorbereitungen.

Lemma 5.32 *Es sei K ein Körper und $f(x) \in K[x]$ ein irreduzibles Polynom. Dann besitzt K eine endliche Körpererweiterung E, in der $f(x)$ eine Wurzel besitzt.*

Beweis. Es sei

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n, \quad I := (f(x)).$$

Betrachte $E := K[x]/I$. Nach Korollar 3.39 ist E ein Körper, der K enthält. Die Elemente von E sind Rechtsnebenklassen der Form $I+g(x)$. Das Element $I + x \in E$ ist eine Wurzel von $f(x)$, da

$$\begin{aligned} f(I+x) &= a_0 + a_1(I+x) + \cdots + a_n(I+x)^n \\ &= a_0 + (I + a_1 x) + \cdots + (I + a_n x^n) \\ &= I + (a_0 + a_1 x + \cdots + a_n x^n) \\ &= I + f(x) \\ &= I + 0 \end{aligned}$$

und $I + 0$ ist das Nullelement von E. □

Bemerkung Die Aussage gilt natürlich auch für nicht-irreduzible Polynome.

Satz 5.33 *Ist $f(x)$ ein nicht konstantes Polynom über dem Körper K, dann gibt es eine endliche Körpererweiterung E von K, in der $f(x)$ in Linearfaktoren zerfällt.*

Beweis. Der Beweis erfolgt durch Induktion über den Grad n von $f(x)$. Der Induktionsanfang: $n = 1$ ist klar.

Wir nehmen nun an, dass die Behauptung für Polynome vom Grad $n-1$ gelte. Es sei dann $f(x)$ ein Polynom vom Grad n. Dann gibt es eine Zerlegung

$$f(x) = p(x)q(x), \quad \text{wobei } p(x) \text{ irreduzibel ist}$$

(hier ist $f(x) = p(x)$ möglich). Nach Lemma 5.32 hat $p(x)$ eine Wurzel α in einem Erweiterungsköper E' von K. Also gilt über E':

$$f(x) = (x - \alpha)g(x), \quad \operatorname{grad} g(x) = n - 1.$$

Nach Induktionsannahme besitzt E' eine endliche Körpererweiterung E in der $g(x)$ in Linearfaktoren zerfällt. Also zerfällt auch $f(x)$ über E in Linearfaktoren. Nach Satz 5.10 ist E eine endliche Körpererweiterung von K. □

Bemerkung Der Beweis gibt eine sukzessive Methode zur Bestimmung einer Körpererweiterung, über der f zerfällt.

Beispiel Seien $p \neq q \in \mathbb{P}$ und $f = x^p - q \in \mathbb{Q}[x]$. Bestimme einen Körper, über dem f zerfällt.

Satz 5.34 (Existenz des Zerfällungskörpers) *Es sei K ein Körper und $f(x) \in K[x]$ ein nicht konstantes Polynom. Dann gibt es einen Zerfällungskörper von $f(x)$.*

Insbesondere gilt: ist E eine Körpererweiterung von K und zerfällt $f(x)$ über E in Linearfaktoren

$$f(x) = b(x - \alpha_1) \cdots (x - \alpha_n), \quad \alpha_1, \ldots, \alpha_n \in E, \quad b \in K,$$

so ist $K(\alpha_1, \ldots, \alpha_n)$ ein Zerfällungskörper von $f(x)$ über K.

Beweis. Aus Satz 5.33 folgt, dass es eine (endliche) Körpererweiterung E gibt, in der $f(x)$ in Linearfaktoren zerfällt:

$$f(x) = b(x - \alpha_1) \cdots (x - \alpha_n), \quad \alpha_1, \ldots, \alpha_n \in E, \quad b \in K,$$

Es ist dann klar, dass $f(x)$ über $K(\alpha_1, \ldots, \alpha_n)$ in Linearfaktoren zerfällt. Wir wollen zeigen, dass $K(\alpha_1, \ldots, \alpha_n)$ minimal mit dieser Eigenschaft ist. Angenommen, $f(x)$ zerfällt über einem Zwischenkörper L von $K \subset K(\alpha_1, \ldots, \alpha_n)$ in Linearfaktoren:

$$f(x) = c(x - \beta_1) \cdots (x - \beta_m), \quad \beta_1, \ldots, \beta_m \in L, \quad c \in K.$$

Da $K(\alpha_1, \ldots, \alpha_n)[x]$ ein faktorieller Ring ist, folgt $\{\beta_1, \ldots, \beta_m\} = \{\alpha_1, \ldots, \alpha_n\}$. Wegen

$$K(\beta_1, \ldots, \beta_m) \subset L \subset K(\alpha_1, \ldots, \alpha_n)$$

folgt dann aber $L = K(\alpha_1, \ldots, \alpha_n)$. □

Es bleibt nun, die Eindeutigkeit des Zerfällungskörpers (bis auf K-Isomorphismen) zu zeigen.

Lemma 5.35 *Es sei E eine Körpererweiterung des Körpers K und $\alpha, \alpha' \in E$ algebraisch über K. Stimmen die Minimalpolynome von α und α' über K überein, so gibt es genau einen Isomorphismus $\varphi : K(\alpha) \to K(\alpha')$ mit $\varphi|_K = \mathrm{id}_K$ und $\varphi(\alpha) = \alpha'$.*

Beweis. (a) Eindeutigkeit: Hat φ die gewünschten Eigenschaften, so gilt

$$\varphi(g(\alpha)) = g(\alpha') \text{ für jedes } g(x) \in K[x].$$

Nach Satz 5.12 gibt es höchstens ein derartiges φ.

(b) Existenz: Es sei $f(x)$ das Minimalpolynom von α und α' über K. Dann gilt für alle $g(x), h(x) \in K[x]$

$$g(\alpha) = h(\alpha) \Rightarrow (g-h)(\alpha) = 0 \Rightarrow g(x) - h(x) \in (f(x)) \Rightarrow g(\alpha') = h(\alpha').$$

Also können wir φ durch

$$\varphi(g(\alpha)) := g(\alpha') \text{ für jedes } g(x) \in K[x]$$

definieren. Für $a \in K \subset K[x]$ gilt dann

$$\varphi(a) = a,$$

also gilt $\varphi|_K = \mathrm{id}_K$. Ferner gilt

$$\varphi(\alpha) = \alpha'.$$

Man kann leicht zeigen, dass φ ein Körperhomomorphismus ist, Die Abbildung φ ist auch bijektiv, da man die Umkehrabbildung erhält, indem man in der Definition von φ die Rollen von α und α' vertauscht. Also ist φ ein Isomorphismus. □

Lemma 5.36 *Es seien K und K' Körper, $\varphi : K \to K'$ ein Isomorphismus, $\Phi : K[x] \to K'[x]$ der induzierte Isomorphismus der Polynomringe, $f(x) \in K[x]$ irreduzibel, α eine Nullstelle von $f(x)$ in einem Oberkörper von K und α' eine Nullstelle von $f'(x) := \Phi(f(x))$ in einem Oberkörper von K'.*

Dann gibt es genau einen Isomorphismus

$$\widehat{\varphi} : K(\alpha) \to K'(\alpha') \text{ mit } \widehat{\varphi}|_K = \varphi \text{ und } \widehat{\varphi}(\alpha) = \alpha'.$$

Beweis. (a) Eindeutigkeit: Hat $\widehat{\varphi}$ die gewünschten Eigenschaften, so gilt

$$\widehat{\varphi}(g(\alpha)) = \Phi(g(x))(\alpha') \text{ für jedes } g(x) \in K[x].$$

Nach Satz 5.12 gibt es höchstens ein derartiges $\widehat{\varphi}$.

(b) Existenz: Wie beim Beweis von Lemma 5.35 zeigt man, dass die Vorschrift in (a) einen Körperisomorphismus mit den gewünschten Eigenschaften definiert. □

Fazit: Nullstellen irreduzibler Polynome lassen sich permutieren.

Satz 5.37 *Es seien K und K' Körper, $\varphi : K \to K'$ ein Isomorphismus, $\Phi : K[x] \to K'[x]$ der zugehörige Isomorphismus, $f(x) \in K[x]$ nicht konstant. Es sei E ein Zerfällungskörper von $f(x)$ über K und E' ein Zerfällungskörper von $f'(x) = \Phi(f(x))$ über K'.*

Dann gibt es einen Isomorphismus $\psi : E \to E'$ mit den Eigenschaften

(i) $\psi|_K = \varphi$.

(ii) *ψ bildet die Menge der Nullstellen von $f(x)$ in E auf die Menge der Nullstellen von $f'(x)$ in E' ab.*

Ist $p(x)$ ein irreduzibler Faktor von $f(x)$, $\alpha \in E$ eine Nullstelle von $p(x)$ in E und $\alpha' \in E'$ eine Nullstelle von $p'(x) = \Phi(p(x))$ in E', so kann der Isomorphismus $\psi : E \to E'$ sogar so gewählt werden, dass $\psi(\alpha) = \alpha'$ gilt.

Beweis. Wir führen den Beweis durch Induktion über die Anzahl n der in $E \setminus K$ liegenden Nullstellen von $f(x)$.

Im Falle $n = 0$ gilt $E = K$. Es gibt also $\alpha_1, \ldots, \alpha_r, b \in K$ mit

$$f(x) = b(x - \alpha_1) \cdots (x - \alpha_r).$$

Dann gilt

$$f'(x) = \Phi(f(x)) = \varphi(b)(x - \varphi(\alpha_1)) \cdots (x - \varphi(\alpha_r)).$$

Also hat der Isomorphismus $\varphi : K \to K'$ die gewünschten Eigenschaften.

Es sei nun $n > 0$ und die Behauptung sei richtig für alle K, K', φ, $f(x)$,E, E', für die gilt, dass höchstens $n-1$ Nullstellen von $f(x)$ in $E \setminus K$ liegen. Es seien nun K, K', φ, $f(x)$,E, E' wie in der Voraussetzung des Satzes gegeben, so dass n Nullstellen $\alpha_1, \ldots, \alpha_n$ von $f(x)$ in $E \setminus K$ liegen. Es sei $p(x)$ das Minimalpolynom von α_1 über K. Dies ist ein Teiler von $f(x)$. Da $f'(x)$ über E' in Linearfaktoren zerfällt, gibt es eine Nullstelle α_1' von $p'(x) = \Phi(p(x))$ in E'. Nach Lemma 5.36 gibt es einen Isomorphismus $\widehat{\varphi} : K(\alpha_1) \to K'(\alpha_1')$ mit $\widehat{\varphi}|_K = \varphi$ und $\widehat{\varphi}(\alpha_1) = \alpha_1'$. Auf $K(\alpha_1)$, $K'(\alpha_1')$, $\widehat{\varphi}$, $f(x)$, E, E' können wir nun die Induktionsannahme anwenden. Damit folgt die Behauptung. □

Korollar 5.38 (Eindeutigkeit des Zerfällungskörpers) *Es sei K ein Körper und $f(x)$ ein nicht konstantes Polynom. Sind E und E' Zerfällungskörper von $f(x)$, so gibt es einen Isomorphismus $\varphi : E \to E'$ mit $\varphi|_K = \mathrm{id}_K$, der die Menge der Nullstellen von $f(x)$ in E auf die Menge der Nullstellen von $f(x)$ in E' abbildet. (Man kann daher von* dem *Zerfällungskörper eines nicht konstanten Polynoms sprechen.)*

Beweis. Dies folgt mit $K = K'$ und $\varphi = \mathrm{id}_K$ sofort aus Satz 5.37. □

Korollar 5.39 *Es sei K ein Körper und $f(x) \in K[x]$ ein nicht konstantes Polynom. Ist E eine Körpererweiterung von K und zerfällt $f(x)$ über E in Linearfaktoren*

$$f(x) = b(x-\alpha_1)\cdots(x-\alpha_n), \quad \alpha_1,\ldots,\alpha_n \in E, \quad b \in K,$$

so ist $K(\alpha_1,\ldots,\alpha_n)$ der Zerfällungskörper von $f(x)$ über K.

5.7 Kreisteilungskörper

Definition Es sei K ein Körper und $n \in \mathbb{N}\setminus\{0\}$. Ein Element $\alpha \in K$ heißt *n-te Einheitswurzel* in K, wenn $\alpha^n = 1$ gilt, d.h. wenn α Nullstelle des Polynoms $x^n - 1 \in K[x]$ ist. Es sei E der Zerfällungskörper dieses Polynoms. Die n-ten Einheitswurzeln in E bilden eine multiplikative Gruppe $\mu_n = \mu_n(K)$.

Beispiel Die Menge

$$\mu_n = \{e^{2\pi i\nu/n} \mid \nu = 0,\ldots,n-1\}$$

ist die Menge der n-ten Einheitswurzeln in $\mathbb{C}$.

Satz 5.40 *Die Gruppe μ_n der n-ten Einheitswurzeln ist zyklisch, und zwar von der Ordnung n, falls* $\operatorname{char} K$ *kein Teiler von n ist, und von der Ordnung m, falls* $\operatorname{char} K = p$ *und $n = p^\ell m$ mit $(p,m) = 1$.*

Wir machen zunächst nur einen kleinen Schritt in Richtung des Beweises des Satzes. Da μ_n durch die Nullstellen von $x^n - 1$ gegeben ist, haben wir natürlich

$$\#\mu_n \le n.$$

Falls $\operatorname{char} K = p$ und $n = p^\ell m$ mit $(p,m) = 1, \ell \in \mathbb{N}$, so können wir sogar mithilfe der Binomialkoeffizienten schreiben

$$x^n - 1 = (x^m - 1)^{p^\ell}. \tag{5.2}$$

Also folgt $\#\mu_n \le m$.

Um den Satz vollständig zu beweisen, brauchen wir noch einige Vorbereitungen.

Definition Ein irreduzibles Polynom $f(x) \in K[x]$ heißt *separabel*, wenn $f(x)$ keine mehrfachen Nullstellen in seinem Zerfällungskörper besitzt. Ein nicht konstantes Polynom $f(x) \in K[x]$ heißt *separabel*, wenn alle seine irreduziblen Faktoren es sind. Andernfalls heißt es *inseparabel*.

Wie erkennt man, ob ein Polynom mehrfache Nullstellen besitzt? In der Analysis bildet man dazu die Ableitung und untersucht, ob sie in einem Punkt verschwindet. Dies wollen wir nun formal imitieren. (Alternativ kann man algebraisch mit der Diskriminante argumentieren, s. Übungsblatt und Algebra II.)

Definition Es sei R ein kommutativer Ring mit 1. Für

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in R[x]$$

heißt

$$f'(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}$$

die *(formale) Ableitung* von $f(x)$.

Beispiel Es kann vorkommen, dass $\operatorname{grad} f(x) > 1$ ist, aber trotzdem $f'(x) = 0$ gilt: Es sei $f(x) = x^m$ und R habe die Charakteristik m. Dann gilt:

$$f'(x) = m x^{m-1} = 0.$$

Man beweist leicht die aus der Analysis bekannten Ableitungsregeln:

Satz 5.41 (Ableitungsregeln) *Es sei R ein kommutativer Ring mit 1, $\lambda, \mu \in R$, $f(x), g(x) \in R[x]$. Dann gilt:*

(i) *Ist* $\operatorname{grad} f(x) > 0$, *so ist* $\operatorname{grad} f'(x) < \operatorname{grad} f(x)$.

(ii) *Ist* $\operatorname{grad} f(x) = 0$, *so ist* $f'(x) = 0$.

(iii) Linearität*:* $(\lambda f(x) + \mu g(x))' = \lambda f'(x) + \mu g'(x)$.

(iv) Produktregel*:* $(f(x) \cdot g(x))' = f(x)g'(x) + f'(x)g(x)$.

Korollar 5.42 *Es sei $f(x) = (x-\alpha)^m g(x)$ mit $\alpha \in R$, $g(x) \in R[x]$. Dann ist*

$$f'(x) = (x-\alpha)^{m-1}(m g(x) + (x-\alpha) g'(x)).$$

Beweis. Dies folgt aus den Ableitungsregeln. □

Lemma 5.43 *Es sei K ein Körper und E der Zerfällungskörper eines nicht konstanten Polynoms $f(x) \in K[x]$. Dann ist $\alpha \in E$ genau dann eine mehrfache Nullstelle von $f(x)$ wenn $f(\alpha) = 0$ und $f'(\alpha) = 0$.*

Beweis. Es sei m die Vielfachheit der Nullstelle α. Dann gibt es ein $g(x) \in E[x]$ mit $f(x) = (x-\alpha)^m g(x)$ und $g(\alpha) \neq 0$. Damit folgt die Behauptung aus Korollar 5.42. □

Beispiel Es sei $\operatorname{char} K$ kein Teiler von $n \in \mathbb{N} \setminus \{0\}$. Dann ist das Polynom

$$f(x) = x^n - 1 \in K[x]$$

separabel. Denn nach Voraussetzung gilt

$$f'(x) = nx^{n-1} = 0 \Leftrightarrow n > 1 \text{ und } x = 0,$$

aber $f(0) = -1 \neq 0$.

Zu beachten ist allerdings, dass das Polynom $x^n - 1$ für $n > 1$ nicht irreduzibel ist (und man kann sogar zeigen, dass es immer separabel ist).

Beispiel Um ein Beispiel für ein irreduzibles inseparables Polynom zu bekommen betrachten wir den Körper der rationalen Funktionen in der Variablen t über dem endlichen Körper $\mathbb{Z}_p$, also $K = \mathbb{Z}_p(t)$. Dies ist der Quotientenkörper des Rings $\mathbb{Z}_p[t]$. Wir betrachten das Polynom

$$f(x) = x^p - t \in K[x] = (\mathbb{Z}_p(t))[x].$$

Aus dem Eisensteinkriterium, welches auch in dieser Situation gilt (vgl. die vormalige Bemerkung), angewandt auf das Primelement t, folgt, dass $f(x) \in (\mathbb{Z}_p[t])[x]$ irreduzibel ist. Wie beim Gaußkriterium folgt daraus, dass auch $f(x) = x^p - t \in K[x] = (\mathbb{Z}_p(t))[x]$ irreduzibel ist. Andererseits ist $f'(x) \equiv 0$, d.h. alle Nullstellen von $f(x)$ sind mehrfache Nullstellen.

Beweis von Satz 5.40.

(a) Wir betrachten zunächst den Fall, dass $\operatorname{char} K$ kein Teiler von n ist. Nach Beispiel ist dann das Polynom $x^n - 1$ separabel über K. Daraus folgt $|\mu_n| = n$. Der Rest des Beweises ist analog zum Beweis von Satz 4.5. Es sei $\psi(d)$ die Anzahl der Elemente von μ_n der Ordnung d. Dann gilt wie im Beweis von Satz 4.5:

$$\psi(d) = \begin{cases} 0 & \text{für } d \not| n, \\ 0 \text{ oder } \varphi(d) & \text{für } d | n. \end{cases}$$

Mit Korollar 4.4 folgt nun

$$n = \sum_{d|n} \psi(d) \leq \sum_{d|n} \varphi(d) = n,$$

also $\psi(d) = \varphi(d)$ für alle $d|n$. Daraus folgt insbesondere, dass es in μ_n Elemente der Ordnung n gibt. Also muss μ_n zyklisch sein.

(b) Nun betrachten wir den Fall $\operatorname{char} K = p \in \mathbb{P}$ und $p|n$. Dann gilt $n = p^\ell m$ für ein m mit $(p, m) = 1$ und mit (5.2):

$$x^{p^\ell m} - 1 = (x^m - 1)^{p^\ell}, \text{ also } \mu_{p^\ell m} = \mu_m.$$

Damit kann dieser Fall auf (a) zurückgeführt werden. □

Definition Ein erzeugendes Element von μ_n nennt man eine *primitive n-te Einheitswurzel*.

Bemerkung Ist $\operatorname{char} K$ kein Teiler von n, dann gibt es genau $\varphi(n)$ primitive Einheitswurzeln. Eine solche festgewählte Einheitswurzel wird mit ζ_n bezeichnet.

Beispiel Im Fall $K = \mathbb{C}$ ist $\zeta_n = e^{\frac{2\pi i}{n}}$ eine solche primitive Einheitswurzel. Es gilt dann

$$\mu_n = \{\zeta_n^k \mid k \in \mathbb{Z}\} = \{\zeta_n^k \mid k \in \mathbb{Z}_n\} :$$

Die primitiven Einheitswurzeln sind genau die Elemente ζ_n^k, $k \in \mathbb{Z}_n^*$.

Definition Es sei K ein Primkörper, also $K = \mathbb{Q}$ oder $K = \mathbb{Z}_p$, $n \in \mathbb{N} \setminus \{0\}$ mit $p \not| n$ und ζ_n eine primitive n-te Einheitswurzel. Dann heißt die Körpererweiterung $K(\zeta_n)$, also der Zerfällungskörper des Polynoms $x^n - 1 \in K[x]$, der *n-te Kreisteilungskörper*.

Unter der Voraussetzung $p \not| n$ ist das Polynom $x^n - 1$ separabel. Es ist nur für $n = 1$ irreduzibel, denn es wird von allen Polynomen $x^d - 1$ mit $d|n$ geteilt. Dividiert man $x^n - 1$ durch das kleinste gemeinsame Vielfache aller echten Teiler $x^d - 1$ so erhält man das folgende Polynom.

Definition Das Polynom

$$\Phi_n(x) := \prod_{k \in \mathbb{Z}_n^*} (x - \zeta_n^k) \in K[x]$$

heißt das *n-te Kreisteilungspolynom* von K. Es hat den Grad $\varphi(n)$.

Bemerkung Es gilt

(a) $x^n - 1 = \prod_{d|n} \Phi_d(x)$

(b) $K(\zeta_n)$ ist der Zerfällungskörper von $\Phi_n(x)$.

(c) $[K(\zeta_n) : K] \leq \varphi(n)$.

Wir wollen zeigen, dass $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$. Dazu müssen wir zeigen, dass die Kreisteilungspolynome $\Phi_n(x)$ irreduzibel in $\mathbb{Q}[x]$ sind.

Beispiel Es sei p eine Primzahl.

$$\begin{aligned}\Phi_p(x) &= \frac{x^p-1}{x-1} = x^{p-1}+\cdots+x+1,\\ \Phi_{p^\ell}(x) &= \frac{x^{p^\ell}-1}{x^{p^{\ell-1}}-1} = x^{(p-1)p^{\ell-1}}+\cdots+x^{p^{\ell-1}}+1,\\ \Phi_6(x) &= \frac{x^6-1}{(x-1)(x+1)(x^2+x+1)} = x^2-x+1.\end{aligned}$$

Lemma 5.44 *Das Kreisteilungspolynom $\Phi_n(x) \in \mathbb{Q}[x]$ liegt sogar in $\mathbb{Z}[x]$ und ist primitiv.*

Beweis. durch Induktion über n.

Induktionsanfang $n = 1$: Die Behauptung ist klar für $\Phi_1(x) = x - 1$.

Induktionsannahme: Es gelte $\Phi_d(x) \in \mathbb{Z}[x]$ und $\Phi_d(x)$ primitiv für alle $d|n$, $d < n$.

Induktionsschritt: Das Polynom $x^n - 1$ liegt in $\mathbb{Z}[x]$ und ist primitiv. Es gilt

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Nach Induktionsannahme und Korollar 5.15 (ii) liegt auch $\Phi_n(x)$ in $\mathbb{Z}[x]$ und ist primitiv. □

Lemma 5.45 *Es sei $f(x) \in \mathbb{Q}[x]$ das Minimalpolynom der primitiven Einheitswurzel $\zeta := \zeta_n$ und $p \nmid n$ prim. Dann ist auch $f(\zeta^p) = 0$.*

Beweis. Nach Voraussetzung teilt $f(x)$ das Polynom $\Phi_n(x)$. O.B.d.A. können wir annehmen, dass $f(x) \in \mathbb{Z}[x]$ und $f(x)$ primitiv ist. Nach Lemma 5.44 und Korollar 5.15 (ii) gilt also

$$\Phi_n(x) = f(x)h(x), \quad h(x) \in \mathbb{Z}[x] \text{ primitiv.}$$

Angenommen, $f(\zeta^p) \neq 0$. Da $\Phi_n(\zeta^p) = 0$, muss $h(\zeta^p) = 0$ gelten. Also gibt es ein Polynom $g(x) \in \mathbb{Z}[x]$ mit $g(x)|h(x)$ und $g(\zeta^p) = 0$, wobei o.B.d.A. $g(x)$ wieder primitiv und irreduzibel ist. Also gibt es eine andere Zerlegung

$$\Phi_n(x) = g(x)k(x), \quad k(x) \in \mathbb{Z}[x] \text{ primitiv.}$$

Auch $g(x^p)$ ist primitiv und verschwindet auf ζ. Damit gilt $f(x)|g(x^p)$. Nun betrachten wir die Reduktion aller dieser Polynome mod p. Wegen $p \nmid n$ ist $\overline{\Phi_n(x)}$ auch das n-te Kreisteilungspolynom in $\mathbb{Z}_p[x]$, hat also auch über $\mathbb{Z}_p$ keine mehrfachen Wurzeln und es gilt

$$\overline{\Phi_n(x)} = \overline{f(x)} \cdot \overline{h(x)} = \overline{g(x)} \cdot \overline{k(x)}.$$

Es sei

$$\overline{g(x)} = b_0 + b_1 x + \cdots + b_m x^m \text{ für } b_0, \ldots, b_m \in \mathbb{Z}_p.$$

Dann gilt analog zu (5.2) und dem kleinen Satz von Fermat

$$\begin{aligned}(\overline{g(x)})^p &= b_0^p + b_1^p x^p + \cdots + b_m^p x^{pm} \\ &= b_0 + b_1 x^p + \cdots + b_m x^{pm} = \overline{g(x^p)}\end{aligned}$$

Aus $f(x)|g(x^p)$ folgt auch $\overline{f(x)}|\overline{g(x^p)}$, also $\overline{f(x)}|(\overline{g(x)})^p$. Da weder $\overline{f(x)}$ noch $\overline{g(x)}$ mehrfache Wurzeln haben, folgt daraus $\overline{f(x)}|\overline{g(x)}$, also wegen $g(x)|h(x)$ auch $\overline{f(x)}|\overline{h(x)}$. Das ergibt aber einen Widerspruch, da daraus folgt, dass $\overline{\Phi_n(x)} = \overline{f(x)} \cdot \overline{h(x)}$ den Faktor $\overline{f(x)}$ zweimal enthält. □

Satz 5.46 *Das Kreisteilungspolynom $\Phi_n(x)$ ist irreduzibel über $\mathbb{Q}$ (und auch über $\mathbb{Z}$).*

Beweis. Es sei $f(x) \in \mathbb{Z}[x]$ ein primitiver irreduzibler Teiler von $\Phi_n(x)$, der auf $\zeta = \zeta_n$ verschwindet. Es sei $k \in \mathbb{Z}$ eine positive ganze Zahl mit $(k, n) = 1$ und

$$k = p_1^{e_1} \cdots p_r^{e_r}, \quad p_i \not| n, i = 1, \ldots, r,$$

die Primfaktorzerlegung von k. Mit Hilfe von Lemma 5.45 und Induktion über r kann man zeigen, dass gilt

$$f(\zeta^k) = 0 \text{ für alle } k \in \mathbb{Z}, k > 0, (k, n) = 1.$$

Daraus folgt $\Phi_n(x) = f(x)$. □

Korollar 5.47 *Es gilt*

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n) = \deg \Phi_n.$$

Wir geben nun Anwendungen dieses Resultats. Zunächst kommen wir zurück auf die Frage, für welche positiven ganzen Zahlen n ein reguläres n-Eck mit Zirkel und Lineal konstruierbar ist. Es gilt die folgende Aussage, die ein Teil eines Satzes von Gauss ist.

Satz 5.48 *Das reguläre n-Eck ist höchstens dann mit Zirkel und Lineal konstruierbar, wenn $\varphi(n)$ eine Potenz von 2 ist.*

Beweis. Nach §5.1 hat man das folgende Problem zu entscheiden: Es sei $M = \{0, 1\}$ und ζ_n eine primitive n-te Einheitswurzel. Für welche n ist $\zeta_n \in \mathcal{K}(\mathcal{M})$?

Nach Korollar 5.47 gilt $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$. Nach Korollar 5.30 folgt aus $\zeta_n \in \mathcal{K}(\mathcal{M})$, dass $\varphi(n)$ eine Zweierpotenz ist. □

Wir untersuchen nun, wann $\varphi(n)$ eine Zweierpotenz ist. Es sei $n = p_1^{e_1} \cdots p_r^{e_r}$ die Primfaktorzerlegung von n, wobei $p_1, \ldots, p_r$ paarweise verschiedene Primzahlen sind. Dann gilt nach Korollar 1.36

$$\varphi(n) = p_1^{e_1-1} \cdots p_r^{e_r-1}(p_1 - 1) \cdots (p_r - 1).$$

Also ist $\varphi(n)$ genau dann eine Potenz von 2, wenn für alle von 2 verschiedenen Primfaktoren p_j gilt:

$$e_j = 1 \text{ und } p_j - 1 \text{ ist ein Zweierpotenz.}$$

Eine Primzahl p, für die $p - 1$ eine Potenz von 2 ist, ist aber gerade eine Fermatsche Primzahl.

Damit können wir Satz 5.14 auch die folgende Fassung geben:

Satz 5.49 *Das reguläre n-Eck ist höchstens dann mit Zirkel und Lineal konstruierbar, wenn n die Darstellung*

$$n = 2^m p_1 \cdots p_r$$

besitzt, wobei $p_1, \ldots, p_r$ paarweise verschiedene Fermatsche Primzahlen sind.

Tatsächlich ist diese Bedingung auch eine hinreichende Bedingung für die Konstruierbarkeit. Dies können wir aber mit unseren bisherigen Mitteln noch nicht beweisen. Dazu braucht man die Galoistheorie (s. Satz 5.72). Zum Beispiel ist das reguläre n-Eck für $n = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20$ konstruierbar, während dies für $n = 7, 9, 11, 13, 14, 18, 19$ nicht möglich ist. Die Zahl $2^{2^4} + 1 = 65.537$ ist die grösste bekannte Fermatsche Primzahl. Die Konstruktion des regulären 65.537-Ecks wurde von Johann Gustav Hermes durchgeführt (1879). In Göttingen kann man einen Koffer, der die Anleitung für diese Konstruktion enthält, besichtigen.

Wir geben nun noch eine Anwendung auf die Zahlentheorie. Es gilt der Satz

Satz 5.50 (Dirichletscher Primzahlsatz) *Es sei n eine positive ganze Zahl. Dann liegen in jeder primen Restklasse mod n unendlich viele Primzahlen.*

Ein Beweis dieses Satzes geht über den Rahmen der Vorlesung hinaus. Wir wollen aber einen Spezialfall dieses Satzes beweisen. Dazu dient der folgende Hilfssatz.

Lemma 5.51 *Es sei $k \in \mathbb{Z}$. Jeder Primteiler p von $\Phi_n(k)$ erfüllt*

$$p|n \text{ oder } p \equiv 1 \bmod n.$$

Beweis. Angenommen, $p \nmid n$. Nach Bemerkung (a) gilt

$$k^n - 1 = \prod_{d|n} \Phi_d(k).$$

Da die Polynome $\Phi_d(x)$ für $d|n$ nach Lemma 5.44 in $\mathbb{Z}[x]$ liegen und primitiv sind, folgt

$$p|(k^n - 1), \quad \text{also } k^n \equiv 1 \bmod p.$$

Es sei m die Ordnung der Restklasse von k in der zyklischen Gruppe $\mathbb{Z}_p^*$. Also folgt $m|n$, $p|(k^m - 1)$ und damit

$$p|\Phi_m(k).$$

(Denn sonst müsste ein echter Teiler d von m existieren mit $p|\Phi_d(k)$. Dann hätte aber die Restklasse von k in $\mathbb{Z}_p^*$ höchstens die Ordnung d, im Widerspruch zur Definition von m.) Angenommen $n \neq m$. Dann folgt aus

$$p|\Phi_n(k) \text{ und } p|\Phi_m(k),$$

dass die Restklasse von k eine mehrfache Nullstelle des mod p reduzierten Polynoms $x^n - 1$ wäre. Das ist aber nicht möglich, da wegen $p \nmid n$ das mod p reduzierte Polynom $x^n - 1$ ebenfalls separabel über $\mathbb{Z}_p$ ist. Also folgt

$$n = m = \operatorname{ord}[k].$$

Nach dem Satz von Euler (Satz 2.16) folgt damit $n|(p-1)$, also $p \equiv 1 \bmod n$. □

Satz 5.52 *Es sei n eine positive ganze Zahl. Dann liegen in der Restklasse von 1 mod n unendliche viele Primzahlen.*

Beweis. Angenommen, es liegen in der Restklasse von 1 mod n nur endliche viele Primzahlen $p_1, \ldots, p_s$. Setze $m := np_1 \cdots p_s$. Das Kreisteilungspolynom $\Phi_m(x)$ ist nicht konstant. Daher ist die Folge $(|\Phi_m(km)|)_{k\in\mathbb{N}}$ nicht beschränkt. Es gibt also eine Primzahl p und ein $k \in \mathbb{N}$ mit

$$p|\Phi_m(km) \neq 0.$$

Wegen $p|((km)^m - 1)$ gilt $p \nmid m$. Aus Lemma 5.51 folgt daher $p \equiv 1 \bmod m$, also auch $p \equiv 1 \bmod n$. Also haben wir eine weitere Primzahl p in der Restklasse von 1 mod n gefunden, die m nicht teilt. Also muss sie verschieden von $p_1, \ldots, p_s$ sein, ein Widerspruch. □

5.8 Kreisteilungskörper und quadratische Zahlkörper

Wir wollen nun noch eine Beziehung zwischen quadratischen Zahlkörpern und Kreisteilungskörpern herleiten. Dazu erinnern wir an einige Resultate von §4.2.

In §4.2 wurde definiert:

Definition Es sei $p > 2$ eine Primzahl. Eine Zahl $b \in \mathbb{Z}$ heißt *quadratischer Rest* mod p, wenn die Kongruenz $x^2 \equiv b \bmod p$ eine Lösung in $\mathbb{Z}_p^*$ besitzt, andernfalls *quadratischer Nichtrest*.

Aus den Resultaten von §4.2 folgt:

Satz 5.53 *Es sei $p > 2$ eine Primzahl. Die quadratischen Reste $b \bmod p$ bilden eine Untergruppe vom Index 2 in $\mathbb{Z}_p^*$. Sie sind durch die Eigenschaft*

$$b^{\frac{p-1}{2}} \equiv 1 \bmod p$$

charakterisiert. Modulo p gibt es also jeweils $\frac{p-1}{2}$ quadratische Reste und Nichtreste.

Definition Für eine Primzahl $p > 2$ ist das *Legendresymbol* definiert durch

$$\left(\frac{b}{p}\right) := \begin{cases} 1, & \text{wenn } b \text{ quadratischer Rest mod } p, \\ -1, & \text{wenn } b \text{ quadratischer Nichtrest mod } p, \\ 0, & \text{wenn } b \equiv 0 \bmod p. \end{cases}$$

Aus Satz 5.53 folgt:

Satz 5.54 (i) *Das Legendresymbol definiert einen Gruppenhomomorphismus $\mathbb{Z}_p^* \to \{\pm 1\}$, dessen Kern genau aus der Untergruppe der quadratischen Reste mod p besteht.*

(ii) (Eulersches Kriterium) *Es gilt*

$$\left(\frac{b}{p}\right) \equiv b^{\frac{p-1}{2}} \bmod p.$$

(iii) (Erstes Ergänzungsgesetz) *Es gilt*

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \bmod p,$$

d.h. -1 ist quadratischer Rest mod p genau dann, wenn $p \equiv 1 \bmod 4$ ist.

Im Folgenden sei p stets eine Primzahl > 2 und $\zeta := \zeta_p := e^{\frac{2\pi i}{p}}$.

Lemma 5.55 *Für alle $a \in \mathbb{Z}$ gilt*

$$\sum_{t=0}^{p-1} \zeta^{at} = \begin{cases} p & \text{für } a \equiv 0 \bmod p, \\ 0 & \text{für } a \not\equiv 0 \bmod p. \end{cases}$$

Beweis. Für $a \equiv 0 \bmod p$ gilt

$$\sum_{t=0}^{p-1} \zeta^{at} = \sum_{t=0}^{p-1} 1 = p$$

und für $a \not\equiv 0 \bmod p$ gilt

$$\sum_{t=0}^{p-1} \zeta^{at} = \frac{\zeta^{ap} - 1}{\zeta^a - 1} = 0.$$

□

Aus diesem Lemma folgt:

Lemma 5.56 *Für alle $x, y \in \mathbb{Z}_p$ gilt*

$$\frac{1}{p} \sum_{t=0}^{p-1} \zeta^{t(x-y)} = \delta_{xy}.$$

Definition (quadratische Gaußsche Summe) Für $a \in \mathbb{Z}_p$ definiere

$$g_a := \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \zeta^{at}.$$

Insbesondere sei

$$g := g_1 = \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \zeta^t.$$

Satz 5.57 (i) $g_a = \left(\frac{a}{p}\right) g$.

(ii) $g = \sum_{t=0}^{p-1} \zeta^{t^2}$.

(iii) $g^2 = (-1)^{(p-1)/2} p$.

Beweis. (i) Wir betrachten zunächst den Fall $p|a$. Dann gilt $\left(\frac{a}{p}\right) = 0$. Auf der anderen Seite besagt Satz 5.53, dass es ebenso viele quadratische Reste wie Nichtreste gibt, also

$$g_a = \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) = 0.$$

Für $p \nmid a$ gilt

$$\left(\frac{a}{p}\right) g_a = \sum_{t=0}^{p-1} \left(\frac{at}{p}\right) \zeta^{at} = \sum_{x=0}^{p-1} \left(\frac{x}{p}\right) \zeta^{x} = g,$$

da die Abbildung $\mathbb{Z}_p \to \mathbb{Z}_p$, $t \mapsto x = at$, bijektiv ist. Die Behauptung folgt dann aus der Tatsache, dass

$$\left(\frac{a}{p}\right)\left(\frac{a}{p}\right) = \left(\frac{a^2}{p}\right) = 1.$$

(ii) Es sei Q die Untergruppe der quadratischen Reste in $\mathbb{Z}_p^*$ und $N := \mathbb{Z}_p^* \setminus Q$. Nach Lemma 5.55 gilt

$$1 + \sum_{t\in Q} \zeta^t + \sum_{t\in N} \zeta^t = \sum_{t=0}^{p-1} \zeta^t = 0.$$

Dann gilt

$$g = \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \zeta^t = \sum_{t\in Q} \zeta^t - \sum_{t\in N} \zeta^t = 1 + 2\sum_{t\in Q} \zeta^t = \sum_{s=0}^{p-1} \zeta^{s^2}.$$

(iii) Für $p \nmid a$ folgt aus (i) und Satz 5.54(iii)

$$g_a g_{-a} = \left(\frac{a}{p}\right)\left(\frac{-a}{p}\right) g^2 = \left(\frac{-a^2}{p}\right) g^2 = \left(\frac{-1}{p}\right) g^2 = (-1)^{\frac{p-1}{2}} g^2.$$

Daraus folgt

$$\sum_{a=0}^{p-1} g_a g_{-a} = (p-1)(-1)^{\frac{p-1}{2}} g^2.$$

Auf der anderen Seite gilt nach Definition

$$g_a g_{-a} = \sum_{x=0}^{p-1}\sum_{y=0}^{p-1} \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) \zeta^{a(x-y)}.$$

Aus Lemma 5.56 folgt

$$\sum_{a=0}^{p-1} g_a g_{-a} = \sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\left(\frac{xy}{p}\right)\sum_{a=0}^{p-1}\zeta^{a(x-y)} = p\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\left(\frac{xy}{p}\right)\delta_{xy} = p(p-1).$$

□

Wir erinnern daran, dass die quadratischen Zahlkörper genau die Körper $\mathbb{Q}(\sqrt{d})$ mit $d \in \mathbb{Z}$, $d \neq 0, 1$ quadratfrei, sind (vgl. Satz 3.27).

Satz 5.58 *Jeder quadratische Zahlkörper ist in einem Kreisteilungskörper enthalten.*

Beweis. (a) Es sei zunächst $p = 2$. Wir behaupten, dass $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\sqrt{-2})$ in $\mathbb{Q}(\zeta_8)$ enthalten ist. Hierzu bemerken wir, dass

$$x^8 - 1 = (x^4 - 1)(x^4 + 1).$$

Man rechnet leicht nach (vgl.Übungen), dass der Zerfällungskörper von x^4+1, der Körper $\mathbb{Q}(\sqrt{2}, i)$ ist. Da dieser $\sqrt{2}$ und $\sqrt{-2}$ enthält, folgt die Behauptung.

Nun sei p eine Primzahl > 2. Dann folgt aus Satz 5.57(iii), dass

$$\begin{aligned} \sqrt{p} &\in \mathbb{Q}(\zeta_p) \quad \text{für} \quad p \equiv 1 \bmod 4, \\ \sqrt{-p} &\in \mathbb{Q}(\zeta_p) \quad \text{für} \quad p \equiv 3 \bmod 4. \end{aligned}$$

Damit gilt

$$\begin{aligned} \mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta_p), \mathbb{Q}(\sqrt{-p}) \subset \mathbb{Q}(\zeta_{4p}) \quad &\text{für} \quad p \equiv 1 \bmod 4, \\ \mathbb{Q}(\sqrt{-p}) \subset \mathbb{Q}(\zeta_p), \mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta_{4p}) \quad &\text{für} \quad p \equiv 3 \bmod 4. \end{aligned}$$

Hier verwenden wir, dass $\mathbb{Q}(\zeta_p, \zeta_4) = \mathbb{Q}(4p)$ ist, da $(4, p) = 1$.

(b) Man zerlegt d in seine Primfaktoren und benutzt die auf dem Präsenzblatt 12.4 bewiesene Aussage, dass $\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_{mn})$ für $(m, n) = 1$ gilt. Dann folgt die Behauptung aus dem Obigen. □

5.9 Endliche Körper

Wir betrachten nun endliche Körper.

Satz 5.59 *Ist K ein endlicher Körper und P sein Primkörper, so gilt*

$$|K| = (\mathrm{char}(K))^{[K:P]}.$$

Ist $\mathrm{char}(K) = p$ *und* $[K : P] = n$*, so hat K also $q = p^n$ Elemente.*

Beweis. Da K endlich ist, gilt nach Satz 5.4 $P = \mathbb{Z}_p$ für eine Primzahl p. Außerdem ist der Grad der Körpererweiterung K von P endlich, also gilt $[K : P] = n$ für eine natürliche Zahl n. Der n-dimensionale P-Vektorraum K ist isomorph zu $\mathbb{Z}_p^n$. Daraus folgt

$$|K| = |\mathbb{Z}_p^n| = p^n.$$

□

Nach Satz 5.59 hat ein endlicher Körper p^n Elemente, wobei p eine Primzahl und $n \in \mathbb{N} \setminus \{0\}$ ist. Wir zeigen nun, dass es bis auf Isomorphie genau einen solchen Körper gibt.

Satz 5.60 *Es sei p eine Primzahl und $n \in \mathbb{N} \setminus \{0\}$. Dann gilt:*

(i) *Ist K der Zerfällungskörper des Polynoms*

$$x^{p^n} - x \in \mathbb{Z}_p[x],$$

so ist K ein Körper mit p^n Elementen.

(ii) *Ist K ein Körper mit p^n Elementen und P sein Primkörper, so ist K der Zerfällungskörper des Polynoms $x^{p^n} - x \in P[x]$.*

(iii) *Je zwei Körper mit p^n Elementen sind isomorph.*

Definition Der nach Satz 5.60 bis auf Isomorphie eindeutig bestimmte Körper mit p^n Elementen wird auch das *Galois-Feld* mit p^n Elementen genannt und mit $\mathrm{GF}(p^n)$ oder $\mathbb{F}_{p^n}$ bezeichnet.

Beweis.
(i): Wir zeigen zunächst, dass die Menge

$$L := \{\alpha \in K \mid \alpha \text{ Nullstelle von } f(x) := x^{p^n} - x\}$$

ein Zwischenkörper von $\mathbb{Z}_p \subset K$ ist. Dann folgt $L = K$.

Nach Satz 4.5 ist $\mathbb{Z}_p^*$ zyklisch von Ordnung $p-1$. Folglich hat jedes Element $a \in \mathbb{Z}_p^*$ als Ordnung einen Teiler von $p-1$ (vgl. auch den Satz von Lagrange, der sogar für den nicht-zyklischen Fall gilt). Damit gilt für jedes $a \in \mathbb{Z}_p^*$

$$a^{p-1} = 1 \Rightarrow a^p = a \Rightarrow a^{p^n} = a.$$

Also gilt $\mathbb{Z}_p \subset L$. Für $a, b \in L$ gilt nun

$$(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n} = a \pm b, \quad (ab)^{p^n} = a^{p^n} b^{p^n} = ab,$$

also $a \pm b \in L$ und $ab \in L$, und für $b \neq 0$

$$\left(\frac{a}{b}\right)^{p^n} = \frac{a^{p^n}}{b^{p^n}} = \frac{a}{b},$$

also $\frac{a}{b} \in L$. Damit ist L ein Zwischenkörper von $\mathbb{Z}_p \subset K$.

Wegen $f'(x) = -1$ haben $f(x)$ und $f'(x)$ keine gemeinsame Nullstelle. Aus Lemma 5.43 folgt, dass $f(x)$ separabel ist, also K genau p^n Elemente besitzt.

(ii): Da die Gruppe K^* die Ordnung $p^n - 1$ besitzt, gilt $a^{p^n} = a$ für alle $a \in K^*$ und natürlich auch für $a = 0$. Da das Polynom $x^{p^n} - x$ in einem Erweiterungskörper von $P = \mathbb{Z}_p$ höchstens p^n Nullstellen hat, ist

$$K = \{\alpha \in K \mid \alpha \text{ Nullstelle von } f(x) := x^{p^n} - x\}.$$

Nach (i) ist K der Zerfällungskörper von $f(x)$.

(iii): Sind K und K' Körper mit p^n Elementen, so gilt nach Satz 5.59 $\mathrm{char}(K) = \mathrm{char}(K') = p$. Nach Satz 5.4 ist der Primkörper P von K isomorph zum Primkörper P' von K'. Nach (ii) und Satz 5.37 sind K und K' isomorph. □

5.10 Galoistheorie

Die Grundfrage der Galoistheorie ist, ob ein Polynom

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n \in K[x]$$

durch die Grundrechenarten und sukzessives Wurzelziehen lösbar ist. Beispielsweise hat die Gleichung $f(x) = ax^2 + bx + c = 0$ mit $a \neq 0$ stets die Lösungen

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Auch Gleichungen der Form $x^n - a = 0$ sind durch n-faches Wurzelziehen lösbar. Ebenso gibt es explizite Lösungsformeln für Gleichungen dritten (Nicolo Tartaglia, 1499/1500 – 1557) und vierten Grades (Gerolamo Cardano, 1501 – 1576). Bis zu Beginn des 19. Jahrhunderts versuchte man (vergebens) entsprechende Formeln für Gleichungen fünften Grades zu finden. Mit Hilfe der Galoistheorie kann man beweisen, dass etwa die Gleichung $x^5 - x + 1 = 0$ nicht durch Wurzeln (Radikalerweiterungen) auflösbar ist. Die Galoistheorie übersetzt Fragen zur Lösbarkeit von Polynomgleichungen in gruppentheoretische Fragestellungen. Sie ist benannt zu Ehren des französischen Mathematikers Évariste Galois (1811 – 1832), der bei einem Duell ums Leben kam

und in der Nacht vor dem Duell seine Überlegungen zur Lösbarkeit von Polynomgleichungen in einem Brief niedergeschrieben hat.

Genauer geht es in der Galoistheorie um eine Beziehung zwischen Zwischenkörpern einer Körpererweiterung und Untergruppen der Gruppe der relativen Automorphismen einer Körpererweiterung.

Definition (a) Es sei K ein Körper. Mit $\mathrm{Aut}(K)$ bezeichnen wir die Menge der Automorphismen von K. Diese Menge bildet zusammen mit der Hintereinanderausführung als Verknüpfung eine Gruppe. Sie heißt die *Automorphismengruppe* von K.

(b) Es sei E eine Körpererweiterung von K. Die Menge

$$\mathrm{Aut}(E;K) := \{\varphi \in \mathrm{Aut}(E) \mid \varphi(a) = a \text{ für alle } a \in K\}$$

ist eine Untergruppe von $\mathrm{Aut}(E)$. Man nennt sie die *Gruppe der relativen Automorphismen* oder die *Galoisgruppe* von E über K.

(c) Es sei K ein Körper, $f(x) \in K[x]$ nicht konstant und E der Zerfällungskörper von $f(x)$. Dann heißt

$$\mathrm{Gal}(f(x);K) := \mathrm{Aut}(E;K)$$

die *Galoisgruppe* von $f(x)$ über K.

Satz 5.61 *Ist P der Primkörper eines Körpers K, so gilt* $\mathrm{Aut}(K;P) = \mathrm{Aut}(K)$.

Beweis. Es sei $\varphi \in \mathrm{Aut}(K)$. Dann gilt $\varphi(1) = 1$, also auch

$$\varphi(n \cdot 1) = \varphi(1 + \cdots + 1) = n \cdot \varphi(1) = n \cdot 1 \text{ für alle } n \in \mathbb{N} \setminus \{0\},$$

also auch $\varphi(n \cdot 1) = n \cdot 1$ für alle $n \in \mathbb{Z}$. Zu $a \in P$ gibt es aber $m, n \in \mathbb{Z}$ mit $n \cdot 1 \neq 0$ und $a = \frac{m \cdot 1}{n \cdot 1}$. Dann gilt

$$\varphi(a) = \varphi\left(\frac{m \cdot 1}{n \cdot 1}\right) = \frac{\varphi(m \cdot 1)}{\varphi(n \cdot 1)} = \frac{m \cdot 1}{n \cdot 1} = a.$$

□

Definition Es sei K ein Körper und G eine Untergruppe von $\mathrm{Aut}(K)$. Dann ist

$$\mathrm{Fix}(K;G) := \{a \in K \mid \varphi(a) = a \text{ für alle } \varphi \in G\}$$

ein Unterkörper von K. Man nennt ihn den *Fixkörper* von G in K.

Definition Eine Körpererweiterung E von K heißt *Galois-Erweiterung*, wenn es eine *endliche* Untergruppe G von $\mathrm{Aut}(E)$ gibt, so dass $K = \mathrm{Fix}(E; G)$ gilt.

In den nächsten Beispielen benutzen wir eine entscheidende Eigenschaft von $\mathrm{Aut}(L; K)$, welche für jede Körperweiterung L/K gilt:

Fakt: Jedes $\sigma \in \mathrm{Aut}(L; K)$ permutiert die Nullstellen in L eines jeden Polynoms in $K[x]$.

Angewandt auf irreduzible Polynome mit Nullstelle in L ergeben sich starke Einschränkungen für die möglichen Wirkungen von $\sigma \in \mathrm{Aut}(L; K)$.

Beispiel Sei K ein Körper und $f = x^2 - \alpha \in K[x]$ mit Zerfällungskörper E. Ist f reduzibel über K, so ist $E = K$ (und damit Galois über K). Andernfalls rechnet man direkt nach, dass $E = K[x]/(f)$ und dass dieser Körper genau dann Galois über K ist, wenn $\mathrm{char}(K) \neq 2$.

Beispiel Sei K ein Körper und $f = x^3 - \alpha \in K[x]$ mit Zerfällungskörper E. Ist f reduzibel über K, so prüft man direkt, dass E/K Galois ist. Wir nehmen also an, dass f irreduzibel über K ist, und setzen $L = K[x]/(f)$ vom Grad 3 über K – die folglich die Nullstelle $\beta = x \mod (f)$ von f enthält. Auf diesem Wege erhalten wir eine Kette an Körpererweiterungen

$$K \subsetneq L = K(\beta) \subseteq E.$$

Wir wollen klären, welche dieser Erweiterung Galois sind und wann $L = E$. Letztere Frage lässt sich relativ leicht anhand einer Wurzel ω des Polynoms $g = x^2 + x + 1 \in K[x]$ klären. Diese liegt folglich in K, wenn g reduzibel ist, oder in der quadratischen Körpererweiterung $K(\omega) = K[x]/(g)$ von K, wenn g irreduzibel über K ist.

Konkret zerfällt f über $K(\beta, \omega)$ wie folgt:

$$f = (x - \beta)(x - \omega\beta)(x - \omega^2\beta).$$

Ist $\omega \in K$, so ergibt sich $L = E$. Wir müssen nun noch unterscheiden, ob die Nullstellen unterschiedlich sind, d.h. ob f separabel ist. Dies ist natürlich genau in Charakteristik $\neq 3$ der Fall, so dass

$$\sigma \in \mathrm{Aut}(L; K) \quad \text{eindeutig durch} \quad \sigma(\beta) \in \{\beta, \omega\beta, \omega^2\beta\}$$

bestimmt ist (denn dies legt σ auf der K-Basis $\{1, \beta, \beta^2\}$ von L fest). Insbesondere gilt

$$\mathrm{Aut}(L; K) = \langle \beta \mapsto \omega\beta \rangle \cong C_3 \quad \text{und} \quad \mathrm{Fix}(L; C_3) = K.$$

Es folgt, dass L/K in diesem Fall Galois ist.

In Charakteristik 3 wiederum hat f nur die (dreifache) Nullstelle β in L, so dass jedes $\sigma \in \mathrm{Aut}(L;K)$ als Identität auf der obigen K-Basis von L operiert, also

$$\sigma = \mathrm{id}_E \quad \text{und} \quad \mathrm{Aut}(L;K) = \{\mathrm{id}_E\}$$

folgen und L/K **nicht** Galois ist.

Es bleibt der Fall $\omega \notin K$ zu untersuchen (der schon $\mathrm{char}(K) \neq 3$ impliziert!). In diesem Fall gilt auch $\omega \notin L$ (denn L/K hat Grad 3, während $K(\omega)/K$ Grad 2 hat). Also hat f in L nur eine Nullstelle, nämlich β. Wir schließen $L \neq E$ und, genau wie im obigen Fall von Charakteristik 3, dass $\sigma = \mathrm{id}_E$ für jedes $\sigma \in \mathrm{Aut}(L;K)$; also gilt auch $\mathrm{Aut}(L;K) = \{\mathrm{id}_E\}$, und L/K ist nicht Galois.

Für die Erweiterung E/K wiederum haben wir die K-Basis

$$\{1, \omega, \beta, \omega\beta, \beta^2, \omega\beta^2\}$$

(vgl. den Beweis von Satz 5.10). Man prüft direkt, dass $\sigma \in \mathrm{Aut}(E;K)$ durch die Bilder von β und ω festliegt, aber auch durch die Bilder von β und $\omega\beta$ (welche schon das Bild von $\omega^2\beta$ bestimmen). So verifiziert man direkt, dass

$$\mathrm{Aut}(E;K) \cong S_3 \quad \text{und} \quad \mathrm{Fix}(E;S_3) = K.$$

Insbesondere ist E/K Galois.

Natürlich ist auch E/L Galois nach dem vorherigen Beispiel (da g separable außerhalb Charakteristik 3 ist).

Es sei E eine Galois-Erweiterung des Körpers K, $\mathcal{K}$ die Menge der Zwischenkörper von $K \subset E$ und $\mathcal{G}$ die Menge der Untergruppen von $\mathrm{Aut}(E;K)$. Die Teilmengenbeziehung ist eine Halbordnung auf $\mathcal{K}$. Zu je zwei Elementen $L_1, L_2 \in \mathcal{K}$ existiert jeweils ein Supremum und ein Infimum:

$$\begin{aligned} L_1 \vee L_2 &:= \sup(L_1, L_2) = K(L_1 \cup L_2), \\ L_1 \wedge L_2 &:= \inf(L_1, L_2) = L_1 \cap L_2. \end{aligned}$$

Es gilt zudem, dass

$$L_1 \vee (L_1 \wedge L_2) = L_1 \,\text{und}\, L_1 \wedge (L_1 \vee L_2) = L_1.$$

Die Menge $\mathcal{K}$ bildet damit einen *Verband*. Es existiert sogar ein größtes Element, nämlich E, und ein kleinstes Element, nämlich K. Entsprechend bildet die Menge $\mathcal{G}$ einen Verband mit größtem Element $\mathrm{Aut}(E;K)$ und kleinstem

Element $\{\mathrm{id}\}$. Wir betrachten nun die folgenden Abbildungen zwischen diesen beiden Verbänden:

$$\begin{array}{rccc} \mathrm{Aut}(E;\cdot): & \mathcal{K} & \longrightarrow & \mathcal{G} \\ & L & \longmapsto & \mathrm{Aut}(E;L) \end{array}, \qquad \begin{array}{rccc} \mathrm{Fix}(E;\cdot): & \mathcal{G} & \longrightarrow & \mathcal{K} \\ & H & \longmapsto & \mathrm{Fix}(E;H) \end{array}.$$

Diese Abbildungen sind ordnungsumkehrend, d.h. für $L, L' \in \mathcal{K}$ und $H, H' \in \mathcal{G}$ gilt

$$\begin{aligned} L \subset L' &\Rightarrow \mathrm{Aut}(E;L') \subset \mathrm{Aut}(E;L), \\ H \subset H' &\Rightarrow \mathrm{Fix}(E;H') \subset \mathrm{Fix}(E;H). \end{aligned}$$

Der Hauptsatz der Galoistheorie besagt, dass diese Abbildungen bijektiv und zueinander invers sind.

Satz 5.62 (Hauptsatz der Galoistheorie) *Es sei E eine Galois-Erweiterung des Körpers K, $\mathcal{K}$ die Menge der Zwischenkörper von $K \subset E$ und $\mathcal{G}$ die Menge der Untergruppen von $\mathrm{Aut}(E;K)$. Dann sind die Abbildungen*

$$\begin{array}{rccc} \mathrm{Aut}(E;\cdot): & \mathcal{K} & \longrightarrow & \mathcal{G} \\ & L & \longmapsto & \mathrm{Aut}(E;L) \end{array} \quad \textit{und} \quad \begin{array}{rccc} \mathrm{Fix}(E;\cdot): & \mathcal{G} & \longrightarrow & \mathcal{K} \\ & H & \longmapsto & \mathrm{Fix}(E;H) \end{array}$$

bijektiv und zueinander invers, d.h. es gilt

$$\begin{aligned} \mathrm{Fix}(E;\mathrm{Aut}(E;L)) &= L \textit{ für alle } L \in \mathcal{K}, \\ \mathrm{Aut}(E;\mathrm{Fix}(E;H)) &= H \textit{ für alle } H \in \mathcal{G}. \end{aligned}$$

Beispiel Wir wollen den Hauptsatz der Galoistheorie anhand des Beispiels $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2},\sqrt{3})$ illustrieren. Man kann zeigen, dass die Körpererweiterung $\mathbb{Q}(\sqrt{2},\sqrt{3})$ von $\mathbb{Q}$ eine Galois-Erweiterung ist. Die Galoisgruppe G von $\mathbb{Q}(\sqrt{2},\sqrt{3})$ über $\mathbb{Q}$ ist die Gruppe

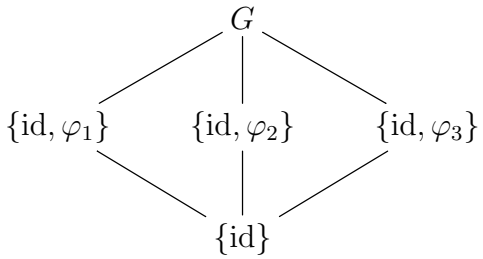
$$G = \{\mathrm{id}, \varphi_1, \varphi_2, \varphi_3\}$$

mit

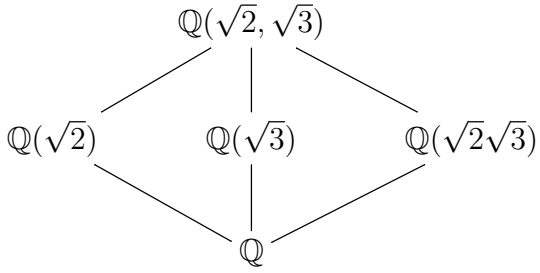
$$\begin{aligned} \varphi_1(\sqrt{2}) &= \sqrt{2}, \quad \varphi_1(\sqrt{3}) = -\sqrt{3}, \\ \varphi_2(\sqrt{2}) &= -\sqrt{2}, \quad \varphi_2(\sqrt{3}) = \sqrt{3}, \\ \varphi_3(\sqrt{2}) &= -\sqrt{2}, \quad \varphi_3(\sqrt{3}) = -\sqrt{3}. \end{aligned}$$

Sie ist isomorph zur Kleinschen Vierergruppe. Wir betrachten nun die Menge $\mathcal{G}$ der Untergruppen von G. Den Verband $\mathcal{G}$ der Untergruppen von G können

wir schematisch so darstellen:



Der Verband $\mathcal{K}$ der Zwischenkörper von $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ sieht in unserem Beispiel wie folgt aus:



Der Hauptsatz der Galoistheorie besagt nun, dass die Abbildungen $\mathrm{Fix}(E; \cdot)$ und $\mathrm{Aut}(E; \cdot)$ ordnungsumkehrende, bijektive und zueinander inverse Abbildungen zwischen diesen beiden Verbänden sind.

Beispiel Kehren wir zurück zum ausführlichen Beispiel mit Galoisgruppe S_3, so hat die S_3 vier nicht-triviale Untergruppen (erzeugt einmal durch eine Rotation und dreimal durch eine Spiegelung), die wir wie folgt identifizieren können:

$$\begin{aligned} \langle \beta \mapsto \omega\beta \mapsto \omega^2\beta \mapsto \beta \rangle &\cong C_3 \\ \langle \beta \mapsto \omega\beta \mapsto \beta \rangle &\cong C_2 = H_1 \\ \langle \beta \mapsto \omega^2\beta \mapsto \beta \rangle &\cong C_2 = H_2 \\ \langle \omega\beta \mapsto \omega^2\beta \mapsto \omega\beta \rangle &\cong C_2 = H_3 \end{aligned}$$

Als Fixkörper erhalten wir $\mathrm{Fix}(E; C_3) = K(\omega)$ sowie $\mathrm{Fix}(E; H_i) = K(\omega^{-i}\beta)$ mit ähnlichem Diagramm wie oben.

Den Beweis des Hauptsatzes der Galoistheorie zerlegen wir in einzelne kleine Schritte.

Definition Es sei G eine Gruppe, K ein Körper und $K^* = K \setminus \{0\}$. Ein Gruppenhomomorphismus

$$\chi : G \to K^*$$

heißt ein *Charakter* von G in K.

Lemma 5.63 *Es seien $\chi_1, \ldots, \chi_n$ paarweise verschiedene Charaktere einer Gruppe G in einen Körper K. Dann sind $\chi_1, \ldots, \chi_n$ im K-Vektorraum aller Abbildungen von G nach K linear unabhängig.*

Beweis. durch Induktion über n.

Induktionsanfang $n = 1$: Es sei $\chi : G \to K^*$ ein Charakter und e das neutrale Element von G. Es sei $\lambda\chi = 0$ für ein $\lambda \in K$. Dann folgt

$$\lambda = \lambda \cdot 1 = \lambda\chi(e) = 0.$$

Induktionsannahme: Die Behauptung sei richtig für je $n-1$ paarweise verschiedene Charaktere von G in K.

Induktionsschritt: Es seien $\chi_1, \ldots, \chi_n$ paarweise verschiedene Charaktere und $\lambda_1, \ldots, \lambda_n \in K$ mit

$$\lambda_1\chi_1 + \cdots + \lambda_n\chi_n = 0.$$

Wegen $\chi_1 \neq \chi_n$ gibt es ein $h \in G$ mit $\chi_1(h) \neq \chi_n(h)$. Es sei $g \in G$ beliebig. Die obige Gleichung ist eine Gleichung zwischen Abbildungen. Wir wenden diese Abbildungen einmal auf hg an, zum andern wenden wir sie auf g an und multiplizieren diese Gleichung mit $\chi_n(h)$:

$$\begin{aligned} \lambda_1\chi_1(h)\chi_1(g) + \cdots + \lambda_n\chi_n(h)\chi_n(g) &= 0, \\ \lambda_1\chi_n(h)\chi_1(g) + \cdots + \lambda_n\chi_n(h)\chi_n(g) &= 0. \end{aligned}$$

Subtraktion ergibt

$$\lambda_1(\chi_1(h) - \chi_n(h))\chi_1(g) + \cdots + \lambda_{n-1}(\chi_{n-1}(h) - \chi_n(h))\chi_{n-1}(g) = 0.$$

Da dies für alle $g \in G$ gelten muss, folgt aus der Induktionsannahme insbesondere

$$\lambda_1(\chi_1(h) - \chi_n(h)) = 0, \text{ also } \lambda_1 = 0.$$

Daraus folgt

$$\lambda_2\chi_2 + \cdots + \lambda_n\chi_n = 0.$$

Nach Induktionssannahme folgt hieraus $\lambda_2 = \ldots = \lambda_n = 0$. □

Wir erinnern zunächst daran, dass für Körperhomomorhismen $\varphi : K \to K'$ stets $\varphi(1) = 1$ gefordert wird. Daraus kann man sofort ableiten, dass Körperhomomorphismen stets injektiv, also Körpermonomorphismen sind.

Satz 5.64 *Es seien $\varphi_1, \ldots, \varphi_n$ paarweise verschiedene Homomorphismen eines Körpers K in einen Körper K'. Dann sind $\varphi_1, \ldots, \varphi_n$ im K'-Vektorraum aller Abbildungen von K nach K' linear unabhängig.*

Beweis. Für jeden Körperhomomorphismus $\varphi : K \to K'$ ist die Einschränkung auf K^* ein Homomorphismus $\varphi_{|K^*} : K^* \to (K')^*$, also ein Charakter in K'. Damit folgt die Behauptung aus Lemma 5.63. □

Lemma 5.65 *Es seien $\varphi_1, \ldots, \varphi_n$ paarweise verschiedene Homomorphismen eines Körpers K in einen Körper K' und es sei*

$$L := \{a \in K \mid \varphi_1(a) = \ldots = \varphi_n(a)\}.$$

Dann gilt

(i) *L ist ein Unterkörper von K.*

(ii) *$[K : L] \geq n$.*

Beweis. (i) rechnet man leicht nach.

Zu (ii): Angenommen, $r := [K : L] < n$. Dann sei $\{a_1, \ldots, a_r\}$ eine Basis des L-Vektorraums K. Dann betrachten wir das folgende homogene lineare Gleichungssystem über K':

$$\begin{array}{ccccc} \varphi_1(a_1)x_1 & +\cdots+ & \varphi_n(a_1)x_n & = & 0 \\ \vdots & & \vdots & & \vdots \\ \varphi_1(a_r)x_1 & +\cdots+ & \varphi_n(a_r)x_n & = & 0 \end{array}$$

Wegen $r < n$ hat dieses Gleichungssystem eine nicht triviale Lösung $(\lambda_1, \ldots, \lambda_n) \in (K')^n$. Zu jedem $a \in K$ gibt es $\mu_1, \ldots, \mu_r \in L$ mit

$$a = \mu_1 a_1 + \cdots + \mu_r a_r.$$

Wegen $\varphi_i(\mu_j) = \varphi_1(\mu_j)$ für alle $i = 1, \ldots, n$ und $j = 1, \ldots, r$ folgt

$$\begin{aligned} \sum_{i=1}^{n} \lambda_i \varphi_i(a) &= \sum_{i=1}^{n} \lambda_i \varphi_i(\sum_{j=1}^{r} \mu_j a_j) \\ &= \sum_{i=1}^{n} \lambda_i \sum_{j=1}^{r} \varphi_i(\mu_j)\varphi_i(a_j) \\ &= \sum_{j=1}^{r} \varphi_1(\mu_j) \sum_{i=1}^{n} \lambda_i \varphi_i(a_j) \\ &= 0 \end{aligned}$$

Da dies für alle $a \in K$ gilt, folgt daraus $\lambda_1\varphi_1 + \cdots \lambda_n\varphi_n = 0$ im Widerspruch zu Satz 5.64. □

Definition Es sei K ein Körper und H eine endliche Untergruppe von $\mathrm{Aut}(K)$. Dann heißt die Abbildung

$$\begin{array}{rccc} \mathrm{Spur}_H: & K & \longrightarrow & K \\ & a & \longmapsto & \sum_{\varphi\in H}\varphi(a) \end{array}$$

die *H-Spur* in K.

Beispiel Sei K von Charakteristik $\neq 2$ und $f = x^2 - \alpha \in K[x]$ irreduzibel wie zuvor. Dann gilt für $E = K[x]/(f)$

$$\mathrm{Aut}(E;K) = \{\mathrm{id}_E, \sigma\} \quad \text{mit} \quad \sigma(1) = 1,\ \sigma(x) = -x.$$

Sei $H = \mathrm{Aut}(E;K)$. Auf $a = b + cx \in E$ $(b, c \in K)$ wirkt die H-Spur dann durch $a \mapsto 2b$.

Lemma 5.66 *Ist K ein Körper und H eine endliche Untergruppe von $\mathrm{Aut}(K)$, so gilt*

$$\{0\} \neq \mathrm{Spur}_H(K) \subset \mathrm{Fix}(K;H).$$

Beweis. Für jedes $\psi \in H$ ist die Linkstranslation $\ell_\psi : H \to H$, $\varphi \mapsto \psi \circ \varphi$, eine bijektive Abbildung. Daraus folgt für jedes $a \in K$:

$$\psi(\sum_{\varphi\in H}\varphi(a)) = \sum_{\varphi\in H}\psi(\varphi(a)) = \sum_{\varphi\in H}\varphi(a).$$

Daraus folgt $\mathrm{Spur}_H(K) \subset \mathrm{Fix}(K;H)$.

Angenommen, $\mathrm{Spur}_H(K) = \{0\}$. Dann wäre $\sum_{\varphi\in H}\varphi$ die Nullabbildung. Damit wären die Elemente von $H \subset \mathrm{Aut}(K)$ linear abhängig im Widerspruch zu Satz 5.64. □

Korollar 5.67 *In der obigen Situation gilt* $\mathrm{Spur}_H(K) = \mathrm{Fix}(K;H)$.

Beweis. Sei $K_0 = \mathrm{Fix}(K;H)$. Nicht nur ist K ein K_0-Vektorraum, sondern auch Spur_H ein K_0-Vektorraum-Homomorphismus. Folglich ist auch das Bild von Spur_H ein K_0-Vektorraum – der nach Lemma 5.66 in K_0 enthalten ist, aber nicht der Nullraum ist, also K_0 gleicht. □

Lemma 5.68 *Ist K ein Körper und H eine endliche Untergruppe von $\mathrm{Aut}(K)$, so gilt*

$$[K : \mathrm{Fix}(K;H)] = |H|.$$

Beweis. Wegen Lemma 5.65 ist nur noch $[K : \mathrm{Fix}(K;H)] \leq |H|$ zu zeigen. Es sei $|H| = n$ und $H = \{\varphi_1, \ldots, \varphi_n\}$. Dann ist zu zeigen, dass für $m > n$ je m Elemente $a_1, \ldots, a_m \in K$ über $\mathrm{Fix}(K;H)$ linear abhängig sind. Dazu betrachten wir wieder ein homogenes lineares Gleichungssystem:

$$\begin{array}{ccccc} \varphi_1^{-1}(a_1)x_1 & +\cdots+ & \varphi_1^{-1}(a_m)x_m & = & 0 \\ \vdots & & \vdots & & \vdots \\ \varphi_n^{-1}(a_1)x_1 & +\cdots+ & \varphi_n^{-1}(a_m)x_m & = & 0 \end{array}$$

Wegen $n < m$ hat dieses Gleichungssystem eine nicht triviale Lösung $(\mu_1, \ldots \mu_m) \in K^m$. Es sei etwa $\mu_\ell \neq 0$. Dann wählen wir $b \in K$ mit $\mathrm{Spur}_H(b) \neq 0$ (möglich nach Lemma 5.66) und setzen

$$\lambda_i := b\mu_\ell^{-1}\mu_i, \quad i = 1, \ldots, m.$$

Dann ist $(\lambda_1, \ldots, \lambda_m)$ ebenfalls eine Lösung des obigen Gleichungssystems. Es gilt daher

$$\begin{array}{ccccc} a_1\varphi_1(\lambda_1) & +\cdots+ & a_m\varphi_1(\lambda_m) & = & 0 \\ \vdots & & \vdots & & \vdots \\ a_1\varphi_n(\lambda_1) & +\cdots+ & a_m\varphi_n(\lambda_m) & = & 0 \end{array}$$

Durch Aufsummieren erhält man

$$0 = \sum_{j=1}^{m} a_j \sum_{i=1}^{n} \varphi_i(\lambda_j) = \sum_{j=1}^{m} \mathrm{Spur}_H(\lambda_j)a_j.$$

Dies ist eine Linearkombination von $a_1, \ldots, a_m$, deren Koeffizienten nach Lemma 5.66 in $\mathrm{Fix}(K;H)$ liegen. Wegen $\mathrm{Spur}_H(\lambda_\ell) = \mathrm{Spur}_H(b) \neq 0$ ist diese Linearkombination nicht trivial. Also sind die Elemente $a_1, \ldots, a_m$ linear abhängig über $\mathrm{Fix}(K;H)$. □

Lemma 5.69 *Es sei K ein Körper und H eine endliche Untergruppe von* $\mathrm{Aut}(K)$*. Dann gilt*

$$\mathrm{Aut}(K; \mathrm{Fix}(K;H)) = H.$$

Beweis. "$\supset$" ist trivial.

"$\subset$": Es sei wieder $|H| = n$ und $H = \{\varphi_1, \ldots, \varphi_n\}$, wobei $\varphi_1 = \mathrm{id}_K$. Es sei $\varphi \in \mathrm{Aut}(K; \mathrm{Fix}(K;H))$. Angenommen, $\varphi \notin H$. Dann gilt

$$\begin{array}{rcl} \mathrm{Fix}(K;H) & = & \{a \in K \,|\, \varphi_1(a) = \varphi_2(a) = \ldots = \varphi_n(a)\} \\ & = & \{a \in K \,|\, a = \varphi_1(a) = \varphi_2(a) = \ldots = \varphi_n(a)\} \\ & = & \{a \in K \,|\, \varphi(a) = \varphi_1(a) = \varphi_2(a) = \ldots = \varphi_n(a)\}, \end{array}$$

da $\varphi(a) = a$ für alle $a \in \mathrm{Fix}(K; H)$. Aus Lemma 5.65 folgt $[K : \mathrm{Fix}(K; H)] \geq n + 1$. Dies steht aber im Widerspruch zu Lemma 5.68. □

Man beachte, dass alle bisherigen Aussagen für jeden Körper K richtig sind.

Beispiel Sei K_0 ein Körper und $K = K_0(t)$ der Funktionskörper in der Variablen t. Sei $n \in \mathbb{N}$ und $\zeta \in K_0$ eine primitive n-te Einheitswurzel. Dann wird durch $\varphi(t) = \zeta t$ eindeutig ein Körperhomomorphismus von K definiert, der K_0 invariant lässt. Man erhält

$$\mathrm{Fix}(K, \langle\varphi\rangle) = K_0(t^n).$$

Nun sind wir in der Lage, den Hauptsatz der Galoistheorie zu beweisen.

Beweis von Satz 5.62. Es sei E eine Galois-Erweiterung des Körpers K. Dann gibt es nach Definition eine endliche Untergruppe G von $\mathrm{Aut}(E)$ mit $K = \mathrm{Fix}(E; G)$. Nach Lemma 5.69 gilt $\mathrm{Aut}(E; K) = G$. Also ist G die Galoisgruppe $\mathrm{Aut}(E; K)$ und damit ist diese Gruppe insbesondere endlich. Es sei $\mathcal{K}$ die Menge der Zwischenkörper von $K \subset E$ und $\mathcal{G}$ die Menge der Untergruppen von $G = \mathrm{Aut}(E; K)$.

Wir müssen nun zeigen:

(1) $\mathrm{Aut}(E; \mathrm{Fix}(E; H)) = H$ für alle $H \in \mathcal{G}$.

(2) $\mathrm{Fix}(E; \mathrm{Aut}(E; L)) = L$ für alle $L \in \mathcal{K}$.

Aussage (1) folgt sofort aus Lemma 5.69.

Zu (2): Es sei L ein Zwischenkörper von $K \subset E$. Wir setzen $H := \mathrm{Aut}(E; L)$ und $L' := \mathrm{Fix}(E; H)$. Dann ist zu zeigen: $L' = L$.

Die Inklusion $L \subset L'$ ist klar.

Wir zeigen $L' \subset L$. Es sei $\{\varphi_1, \ldots, \varphi_r\} \subset G$ mit $\varphi_1 = \mathrm{id}_E$ ein Repräsentantensystem von G/H. Dann sind die Monomorphismen

$$\psi_i := \varphi_i|_L : L \to E, \quad i = 1, \ldots, r,$$

paarweise verschieden, denn

$$\psi_i = \psi_j \Rightarrow \varphi_i|_L = \varphi_j|_L \Rightarrow \varphi_j \circ \varphi_i^{-1} \in H \Rightarrow \varphi_j \in H \circ \varphi_i \Rightarrow i = j.$$

Wir zeigen nun

$$\{a \in L \mid \psi_1(a) = \ldots = \psi_r(a)\} = L \cap \mathrm{Fix}(E; G) = L \cap K = K.$$

Die Inklusion $L \cap \mathrm{Fix}(E;G) \subset \{a \in L \,|\, \psi_1(a) = \ldots = \psi_r(a)\}$ ist klar. Zum Beweis der umgekehrten Inklusion sei $a \in \{a \in L \,|\, \psi_1(a) = \ldots = \psi_r(a)\}$ und $\varphi \in G$. Dann müssen wir zeigen, dass $\varphi(a) = a$ gilt. Das Element φ liegt nun in einer Rechtsnebenklasse $H \circ \varphi_i$ für ein $i = 1, \ldots, r$, also $\varphi = \psi \circ \varphi_i$ für ein $\psi \in H$. Dann gilt

$$\varphi(a) = \psi(\varphi_i(a)) = \psi(\psi_i(a)) = \psi(\psi_1(a)) = \psi(a) = a.$$

Dabei folgt die letzte Gleichheit daraus, dass $\psi \in H$ ist, und die vorletzte Gleichheit daraus, dass $\psi_1 = \mathrm{id}_L$ ist. Damit ist die umgekehrte Inklusion bewiesen.

Aus Lemma 5.65 folgt dann $[L : K] \geq r$. Nach Lemma 5.68 und Satz 5.10 gilt

$$|G| = [E : K] = [E : L'][L' : L][L : K].$$

Auf der anderen Seite gilt

$$|G| = [G : H]|H| = r|H| = r[E : L'],$$

wobei wir im letzten Schritt wieder Lemma 5.68 angewendet haben. Wegen $[L : K] \geq r$ folgt daraus $[L' : L] = 1$, also $L = L'$ (und $[L : K] = r$). □

Anwendung/Ausblick: Ist H Normalteiler von G, so folgt aus der obigen Argumentation, dass $\mathrm{Fix}(E;H)$ eine Galoiserweiterung von K mit Galoisgruppe G/H ist.

Beispiel Angewandt auf die kubischen Erweiterungen von K mit Galoisgruppe S_3, die wir schon untersucht haben finden wir den Normalteiler C_3 mit Fixkörper $K(\omega)$ (Galois über K) und drei Untergruppen isomorph zu C_2, die jeweils nicht Normalteiler sind.

5.11 Galoisgruppen der Kreisteilungskörper und der endlichen Körper

Wir wollen nun die Galoisgruppe eines Kreisteilungskörpers bestimmen.

Satz 5.70 *Die prime Restklassengruppe $\mathbb{Z}_n^*$ ist isomorph zur Galoisgruppe $\mathrm{Aut}(\mathbb{Q}(\zeta_n);\mathbb{Q})$ des Kreisteilungskörpers $\mathbb{Q}(\zeta_n)$ vermöge des Isomorphismus*

$$\mathbb{Z}_n^* \to \mathrm{Aut}(\mathbb{Q}(\zeta_n);\mathbb{Q}), \quad k \mapsto \sigma_k,$$

wobei der Automorphismus σ_k eindeutig bestimmt ist durch $\sigma_k(\zeta_n) = \zeta_n^k$.

Beweis. Die oben angegebene Abbildung ist injektiv und ein Homomorphismus, denn

$$(\sigma_m \circ \sigma_k)(\zeta_n) = \sigma_m(\zeta_n^k) = \zeta_n^{mk} = \sigma_{mk}(\zeta_n).$$

Diese Abbildung ist auch surjektiv, denn jedes $\sigma \in \mathrm{Aut}(\mathbb{Q}(\zeta_n); \mathbb{Q})$ ist eindeutig durch seine Wirkung auf der primitiven Einheitswurzel ζ_n bestimmt, da diese ein erzeugendes Element der Körpererweiterung ist. Das Bild $\sigma(\zeta_n)$ muss also wieder eine primitive n-te Einheitswurzel sein, also muss gelten

$$\sigma(\zeta_n) = \zeta_n^k \text{ für ein } k \in \mathbb{Z} \text{ mit } (k, n) = 1.$$

. □

Korollar 5.71 *Die Galoisgruppe Aut*$(\mathbb{Q}(\zeta_n); \mathbb{Q})$ *ist abelsch von Ordnung* $\varphi(n)$.

Nun können wir zu unserem Ursprungsproblem der Konstruktion des regulären n-Ecks mit Zirkel und Lineal zurückkehren. Hierzu nutzen wir die folgende leicht beweisbare Tatsache für eine abelsche Gruppe G der Ordnung $n \in \mathbb{N}$:

für jeden Primteiler $p \mid n$ besitzt G eine Untergruppe H der Ordnung $\dfrac{n}{p}$.

Satz 5.72 *Sei* $n \in \mathbb{N}$. *Das reguläre* n*-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn es ein* $r \in \mathbb{N}$ *gibt, so dass* $\varphi(n) = 2^r$.

Beweis. Die eine Richtung haben wir bereits gesehen (Satz 5.48). Umgekehrt ist zu zeigen, dass sich unter der gegeben Bedingung an n der Kreisteilungskörper $\mathbb{Q}(\zeta_n)$ sukzessive durch Hinzufügen von Wuadratwurzeln aus $\mathbb{Q}$ gewinnen lässt. Sei $G = \mathrm{Aut}(\mathbb{Q}(\zeta_n); \mathbb{Q})$, betrachte eine Untergruppe $H \subset G$ der Ordnung 2^{r-1} (wie oben, d.h. $p = 2$) und setze $K_1 = \mathrm{Fix}(\mathbb{Q}(\zeta_n); H)$. Dann ist K_1 eine Galoiserweiterung von $\mathbb{Q}$ mit Galoisgruppe $G/H \cong C_2$, also ist K_1 quadratisch über $\mathbb{Q}$. Ferner gilt

$$\mathrm{Aut}(\mathbb{Q}(\zeta_n); K_1) = H.$$

Da H natürlich ebenfalls abelsch ist, können wir den obigen Ansatz interieren, um eine Kette an quadratischen Körpererweiterungen $\mathbb{Q}(\zeta_n) \supset K_{r-1} \supset \ldots \supset K_1 \supset \mathbb{Q}$ zu produzieren. □

Nun interessieren wir uns für die Galoisgruppen der endlichen Körper.

Satz 5.73 *Es sei* K *ein Körper der Charakteristik* $p > 0$. *Dann ist die Abbildung*

$$\begin{array}{rccc} \varphi: & K & \longrightarrow & K \\ & x & \longmapsto & x^p \end{array}$$

ein Monomorphismus. Ist K *endlich, so ist* φ *sogar ein Automorphismus.*

Definition Man nennt den Homomorphismus $\varphi : K \to K$, $x \mapsto x^p$, den *Frobenius-Homomorphismus* von K.

Beweis von Satz 5.73. Da nach Lemma 4.6

$$p|\binom{p}{i} \text{ für } i = 1, \ldots, p-1,$$

folgt aus der binomischen Formel

$$(x+y)^p = x^p + y^p.$$

Trivialerweise gilt $(xy)^p = x^p y^p$. Außerdem gilt $\varphi(1) = 1$. Also ist φ ein Körperhomomorphismus und damit auch injektiv. Ist K endlich, so ist φ als injektive Abbildung einer endlichen Menge auf sich selbst sogar surjektiv. □

Ist $K = \mathbb{Z}_p$, so gilt $x^p = x$ für alle $x \in \mathbb{Z}_p$, der Frobenius-Homomorphismus operiert also trivial auf $\mathbb{Z}_p$.

Satz 5.74 *Es sei p eine Primzahl und $n \in \mathbb{N} \setminus \{0\}$. Dann gilt für jeden Körper K mit p^n Elementen und seinen Primkörper P:*

(i) *Die Galoisgruppe $\mathrm{Aut}(K; P)$ ist eine zyklische Gruppe der Ordnung n, die von dem Frobenius-Homomorphismus φ von K erzeugt wird.*

(ii) *Die Unterkörper von K sind genau die Körper $\mathrm{Fix}(K; \langle\varphi^m\rangle)$, wobei $m \in \mathbb{N}$ und $m|n$ und $\langle\varphi^m\rangle$ die von φ^m erzeugte Untergruppe von $\mathrm{Aut}(K; P)$ bezeichnet.*

Beweis.

(i) Nach Satz 4.5 ist die Gruppe K^* zyklisch von Ordnung $p^n - 1$. Es sei a ein Erzeuger dieser Gruppe. Dann gilt für die Potenzen $\varphi^0, \varphi^1, \ldots, \varphi^{n-1}$ des Frobenius-Homomorphismus, dass

$$\varphi^i(a) = a^{p^i} \quad \text{für jedes } i \in \mathbb{N}.$$

Für $i = 0, 1, \ldots, n-1$ sind die Elemente a^{p^i} paarweise verschieden. Andererseits gilt $\varphi^n = \mathrm{id_K}$. Dait erzeugt der Frobenius-Homomorphismus eine zyklische Untergruppe H der Ordnung n von $\mathrm{Aut}(K; P)$ (wobei P der Primkörper ist). Nach Lemma 5.68 gilt

$$[K : \mathrm{Fix}(K; H)] = |H| = n = [K : P].$$

Also ist $P = \mathrm{Fix}(K; H)$ und $H = \mathrm{Aut}(K; P)$.

(ii) Nach (i) und dem Satz von Lagrange sind die Gruppen $\langle\varphi^m\rangle$ mit $m \in \mathbb{N}$ und $m|n$ die verschiedenen Untergruppen von $\mathrm{Aut}(K; P)$. Der Rest folgt aus dem Hauptsatz der Galoistheorie. □

Literaturverzeichnis

[1] M. Artin: Algebra. Birkhäuser Verlag, 1998. ISBN 3-7643-5938-2

[2] S. Bosch: Algebra. 4. überarb. Aufl., Springer-Verlag, 2001. ISBN 3-540-41852-0

[3] G. Fischer: Lehrbuch der Algebra. Vieweg, 2008. ISBN 978-3-8348-0226-2

[4] G. Fischer, R. Sacher: Einführung in die Algebra. B. G. Teubner Stuttgart, 1978. ISBN 3-519-12053-4

[5] J. C. Jantzen, J. Schwermer: Algebra. Springer-Verlag, 2006. ISBN 3-540-21380-5

[6] W. J. Gilbert: Modern Algebra with Applications. John Wiley and Sons, 1976. ISBN 0-471-29891-3

[7] M. Holz: Repetitorium der Algebra. 2. Auflage. Binomi Verlag, Springe, 2005. ISBN 3-923923-44-9

[8] E. Kunz: Algebra. Vieweg 1991. ISBN 3-528-07243-1

[9] H.-J. Reiffen, G. Scheja, U. Vetter: Algebra. B.I.-Wissenschaftsverlag, 1969. ISBN 3-411-00110-0

[10] J. Wolfart: Einführung in die Zahlentheorie und Algebra. Vieweg, 1996. ISBN 978-3-528-07286-5

[11] G. Wüstholz: Algebra. Vieweg, 2004. ISBN 978-3-528-07291-9

Inhaltsverzeichnis