

# Elementare Zahlentheorie

Dr. Stefan Kühnlein

Institut für Algebra und Geometrie, Universität Karlsruhe (TH), 2008

Dieses Skriptum unterliegt dem Urheberrecht. Vervielfältigungen jeder Art, auch nur auszugsweise, sind nur mit Erlaubnis des Autors gestattet.

Dieses Skriptum entstand im Sommersemester 2008 parallel zu meiner Vorlesung zur Elementaren Zahlentheorie. Ich habe mich bemüht, die Inhalte dieser Vorlesung recht getreu wiederzugeben. Insbesondere haftet auch diesem Skriptum der Makel (?) an, dass ich mir immer wieder den Luxus leiste, Sachverhalte erst für die ganzen Zahlen zu diskutieren und nachträglich noch auf ein abstrakteres Niveau hochzuheben. Dadurch werden manche Argumente doppelt vorgeführt, was aber hoffentlich die Lesbarkeit nicht erschwert. Manche Überlegungen tauchen vielleicht sogar noch häufiger auf. Die sind dann entweder sehr zentral, und können gar nicht oft genug vorgeführt werden, oder sie sind so dezentral, dass man sie schon wieder vergessen hat... eine Rechtfertigung mag es also jedes Mal geben.

Ich hoffe, dass die Querverweise ausreichend dokumentiert sind.

Auf Bilder habe ich im Skriptum verzichtet, die habe ich in der Vorlesung gezeigt. Ich empfehle natürlich allen, sich selbst immer wieder ein Bild von dem zu machen, wovon gerade die Rede ist. Ob das nun optischer oder beispielhafter Natur ist, ist der Situation und den persönlichen Vorlieben überlassen.

Ich hoffe, dass nach meiner relativ gründlichen Durchsicht keine ernsthaften inhaltlichen Fehler und auch nicht allzuvielen sonstige Fehler verblieben sind. Für Hinweise hierauf bedanke ich mich im Voraus.

Karlsruhe im Juli 2008

# Inhaltsverzeichnis

<b>1</b>	<b>Teilbarkeit und Primzahlen</b>	<b>5</b>
1.1	Aufbau des Zahlensystems - ein Abriss . . . . .	5
1.2	Teilbarkeit . . . . .	13
1.3	Primzahlen . . . . .	23
1.4	Zur Verteilung der Primzahlen . . . . .	31
1.5	Gleichungssysteme . . . . .	38
<b>2</b>	<b>Kongruenzrechnung</b>	<b>47</b>
2.1	Die Restklassenringe . . . . .	47
2.2	Endliche Körper . . . . .	57
2.3	Quadratische Reste . . . . .	64
<b>3</b>	<b>Quadratische Zahlkörper</b>	<b>71</b>
3.1	Der Ganzheitsring . . . . .	71
3.2	Geometrie der Zahlen . . . . .	80
3.3	Idealklassen . . . . .	86
3.4	Kettenbrüche . . . . .	90



# Kapitel 1

## Teilbarkeit und Primzahlen

### 1.1 Aufbau des Zahlensystems - ein Abriss

In diesem Abschnitt wollen wir kurz skizzieren, wie das Zahlensystem aufgebaut ist. Den allerunbequemsten Teil hierbei lasse ich aber weg: Ich zeige nicht, wie man sich nur unter Verwendung der Peano<sup>1</sup>-Axiome die Arithmetik und Anordnung auf den natürlichen Zahlen verschafft.

Ich setze die Kenntnis der Begriffe Gruppe und Ring voraus, also insbesondere auch, dass alle wissen, was Assoziativität, Kommutativität und das Distributivgesetz bedeuten.

#### Bemerkung 1.1.1 Natürliche Zahlen

Die natürlichen Zahlen  $\mathbb{N} := \{1, 2, 3, \dots\}$  werden als bekannt vorausgesetzt<sup>2</sup>, und natürlich auch, wie man sie addiert und multipliziert.

Addition und Multiplikation sind kommutativ und assoziativ, und sie erfüllen das Distributivgesetz.

Weiter gibt es eine Anordnung:

$$\forall m, n \in \mathbb{N} : m > n : \iff \exists k \in \mathbb{N} : k + n = m.$$

Beachten Sie, dass 0 hier keine natürliche Zahl ist – das ist für die elementare Zahlentheorie der richtige Standpunkt. In Mitteleuropa war ja bis in die frühe Neuzeit die Null überhaupt nicht als Zahl akzeptiert.

Es gilt für natürliche Zahlen  $m, n, s, t$ :

$$[m < n \text{ und } s < t] \Rightarrow [m \cdot s < n \cdot t \text{ und } m + s < n + t].$$

---

<sup>1</sup>Guiseppe Peano, 1858-1939

<sup>2</sup>Laut Leopold Kronecker (1823-1891) wurden sie vom lieben Gott gemacht, der Rest ist Menschenwerk.

Außerdem wissen wir schon, dass für  $a, b, c \in \mathbb{N}$  gilt:

$$[a + b = c + b \Rightarrow a = c] \quad \text{und} \quad [a \cdot b = c \cdot b \Rightarrow a = c].$$

Ärgerlicher Weise lässt sich nicht jede Subtraktion in  $\mathbb{N}$  durchführen, oder – was dasselbe ist – nicht jede Gleichung der Form

$$a + x = b$$

mit  $a, b \in \mathbb{N}$  durch ein  $x \in \mathbb{N}$  lösen.

Dazu müssen wir  $\mathbb{N}$  größer machen.

### Bemerkung 1.1.2 Endlich annulliert

Zunächst nehmen wir künstlich ein Element  $0$  zu  $\mathbb{N}$  dazu und definieren die Anordnung, Addition und Multiplikation auf  $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$  so, dass die alten Regeln für  $\mathbb{N}$  erhalten bleiben und

$$\forall n \in \mathbb{N}_0 : 0 \leq n, 0 + n = n + 0 = n, 0 \cdot n = n \cdot 0 = 0.$$

Dann gelten Kommutativität, Assoziativität und das Distributivgesetz immer noch für Addition und Multiplikation.

Wir hätten auch direkt zur Konstruktion von  $\mathbb{Z}$  schreiten und die  $0$  erst nachher darin entdecken können, aber so wird die Konstruktion etwas „natürlicher“.

### Bemerkung 1.1.3 Die Konstruktion der ganzen Zahlen

Wir brauchen ein Vehikel, um künstlich Differenzen  $a - b$  zu bilden. Dazu betrachten wir auf der Menge  $\mathbb{N}_0 \times \mathbb{N}_0$  die Relation

$$(a, b) \sim (c, d) : \iff a + d = c + b$$

Sie ist eine Äquivalenzrelation.

Denn:

- $(a, b) \sim (a, b)$  ist für alle  $(a, b) \in \mathbb{N}_0^2$  klar.
- Die Symmetrie ist auch offensichtlich.
- Die Transitivität gilt, da aus  $(a, b) \sim (c, d) \sim (e, f)$  folgt, dass

$$a + d = b + c \quad \text{und} \quad c + f = d + e, \quad \text{also} \quad a + d + c + f = b + c + d + e.$$

Hier kann man wegen 1.1.1 den Summanden  $d + c = c + d$  wegekürzen, und es verbleibt die Gleichheit  $a + f = b + e$ , also  $(a, b) \sim (e, f)$ .

Nun setzen wir  $\mathbb{Z} := \mathbb{N}_0^2 / \sim$ , die Menge aller Äquivalenzklassen von  $\sim$ :

$$\mathbb{Z} = \{[(a, b)] \mid a, b \in \mathbb{N}_0\}.$$

Wir sollten darauf eine Addition definieren wollen.

Dazu setzen wir  $(a, b) + (c, d) := (a + c, b + d)$  auf  $\mathbb{N}_0^2$ . Es folgt, dass

$$(a, b) + (c, d) = (c, d) + (a, b),$$

und falls  $(a, b) \sim (e, f)$ , so folgt

$$(a, b) + (c, d) \sim (e, f) + (c, d).$$

Beides impliziert gemeinsam, dass wir aus  $+$  eine Verknüpfung der Äquivalenzklassen machen können:

$$[(a, b)] + [(c, d)] := [(a, b) + (c, d)].$$

Diese Verknüpfung auf  $\mathbb{Z}$  ist wieder assoziativ und kommutativ.

Wir haben ein neutrales Element, nämlich  $[(0, 0)] = [(1, 1)]$ , und zu jedem  $[(a, b)] \in \mathbb{Z}$  gibt es ein bezüglich  $+$  inverses Element, nämlich  $[(b, a)]$ .

$$(a, b) + (b, a) = (a + b, b + a) \sim (0, 0).$$

Also ist  $\mathbb{Z}$  eine kommutative Gruppe. Die Abbildung

$$\Phi : \mathbb{N}_0 \ni n \mapsto [(n, 0)] \in \mathbb{Z}$$

ist injektiv und mit der Addition verträglich:

$$\Phi(m + n) = \Phi(m) + \Phi(n).$$

Außerdem ist für  $a \geq b$

$$[(a, b)] = [(a - b, 0)] \in \Phi(\mathbb{N}_0),$$

und es folgt sofort

$$\mathbb{Z} = \Phi(\mathbb{N}_0) \cup -\Phi(\mathbb{N}).$$

Nun macht man sich das Leben wieder leichter, vergisst  $\Phi$  und identifiziert wie folgt:

$$\mathbb{Z} = \mathbb{N}_0 \cup \{-k \mid k \in \mathbb{N}\}.$$

Hierbei ist  $-k$  das additiv inverse zu  $k$ .

**Bemerkung 1.1.4 Multiplikation der ganzen Zahlen**

Wir schreiben die Menge der ganzen Zahlen jetzt als  $\mathbb{Z} = \{a - b \mid a, b \in \mathbb{N}_0\}$ , wobei  $a - b = a + (-b)$  zu lesen ist:  $a - b = [(a, 0) + (0, b)] = [(a, b)]$ .

Dann definieren wir

$$(a - b) \cdot (c - d) := (ac + bd) - (ad + bc).$$

Wir müssen zeigen, dass dies wohldefiniert ist. Sei also  $a - b = e - f, c - d = g - h$ . Dann gilt

$$(a + f)c + (b + e)d = (b + e)c + (a + f)d,$$

also

$$(ac + bd) + (ed + fc) = (ec + fd) + (ad + bc),$$

und daher

$$(ac + bd) - (ad + bc) = (ec + fd) - (ed + fc).$$

Das zeigt, dass

$$(a - b) \cdot (c - d) \sim (e - f) \cdot (c - d),$$

und eine analoge Rechnung liefert

$$(e - f) \cdot (c - d) \sim (e - f) \cdot (g - h).$$

Also folgt, dass die Multiplikation wohldefiniert ist.

Man rechnet automatisch und ohne viel nachzudenken nach, dass die Multiplikation assoziativ und kommutativ ist und 1 als neutrales Element besitzt. Außerdem sind Addition und Multiplikation durch das Distributivgesetz verbunden.

Insgesamt wird  $(\mathbb{Z}, +, \cdot)$  ein kommutativer Ring, der sogar nullteilerfrei ist.

Wir haben immer noch eine Anordnung, die durch

$$a - b > c - d \iff a + d > b + c$$

auf die Anordnung der natürlichen Zahlen zurückgeführt werden kann.

Ärgerlicher Weise lässt sich in  $\mathbb{Z}$  nicht jede Division durchführen, oder – äquivalent –: Nicht jede Gleichung

$$a \cdot x = b, \quad a, b \in \mathbb{Z}, a \neq 0$$

ist lösbar. Dazu muss man  $\mathbb{Z}$  wieder etwas größer machen.

**Bemerkung 1.1.5 Die Ratio siegt**

Ähnlich wie bei der Konstruktion von  $\mathbb{Z}$  definieren wir die rationalen Zahlen als Menge von Äquivalenzklassen von Paaren ganzer Zahlen.

Konkreter betrachten wir  $S := \mathbb{Z} \times \mathbb{N}$  und führen darauf die Äquivalenzrelation

$$(z, n) \sim (w, m) \iff zm = wn$$

ein. Dabei sind  $z, w \in \mathbb{Z}$  und  $m, n \in \mathbb{N}$ . Man rechnet – unter Verwendung der Nullteilerfreiheit von  $\mathbb{Z}$  – leicht nach, dass dies eine Äquivalenzrelation ist. Die Paare stehen als Stellvertreter für Brüche,  $z$  soll der Zähler sein und  $n$  der Nenner.

$\mathbb{Q} := (\mathbb{Z} \times \mathbb{N}) / \sim$  sei die Menge der Äquivalenzklassen.

Nun müssen hier Addition und Multiplikation festgelegt werden. Dies funktioniert mit den Formeln

$$[(z, n)] \cdot [(w, m)] := [(zw, mn)], \quad [(z, n)] + [(w, m)] := [(zm + wn, mn)].$$

Wieder lässt sich leicht verifizieren, dass dies wohldefinierte Verknüpfungen auf  $\mathbb{Q}$  sind. Bei der Multiplikation geht das im Prinzip genauso, wie wir es eben für die Addition der ganzen Zahlen gemacht haben. Die Addition auf  $\mathbb{Q}$  ist auf die einzig mögliche Art gemacht, die das Distributivgesetz erfüllt und die Addition auf  $\mathbb{Z}$  nach  $\mathbb{Q}$  fortsetzt. Dabei muss man sagen, wie  $\mathbb{Z}$  in  $\mathbb{Q}$  liegt; das geht – ähnlich wie vorhin – so:

Die Abbildung  $\Psi : \mathbb{Z} \rightarrow \mathbb{Q}, z \mapsto [(z, 1)]$  ist eine injektive Abbildung, sie bildet 1 auf das neutrale Element der Multiplikation in  $\mathbb{Q}$  ab und verträgt sich mit Addition und Multiplikation:

$$\Psi(z + w) = [(z + w, 1)] = [(z, 1)] + [(w, 1)] = \Psi(z) + \Psi(w),$$

und analog für die Multiplikation.

Wir identifizieren  $\mathbb{Z}$  mit seinem Bild unter  $\Psi$ , sehen es also in Zukunft als eine Teilmenge von  $\mathbb{Q}$ .

Außerdem schreiben wir traditionsbewusst anstelle von  $[(z, n)]$  in Zukunft  $\frac{z}{n}$ .

Da jedes Element  $\frac{z}{n} \in \mathbb{Q}$ , das nicht 0 ist, bezüglich der Multiplikation invertiert werden kann, ist insgesamt  $\mathbb{Q}$  mit den gegebenen Verknüpfungen ein Körper im Sinne der Algebra.

Die Inverse zu  $\frac{z}{n} \neq \frac{0}{1}$  ist  $\frac{n}{z}$ , wenn  $z \in \mathbb{N}$ , sie ist  $\frac{-n}{-z}$ , wenn  $z \notin \mathbb{N}$ .

### Bemerkung 1.1.6 Etwas Geometrie und ein Problem

Nun wissen alle, dass es auch noch nicht rationale Zahlen gibt. Zum Beispiel ist der goldene Schnitt  $\tau$  nicht rational, auch wenn diese Zahl existieren muss, wenn man denn eine Diagonale in einem regelmäßigen Fünfeck haben will, denn  $\tau$  ist das Verhältnis der Diagonale zur Kantenlänge in solch einem Fünfeck.

Wenn das Verhältnis zweier Seitenlängen eine rationale Zahl ist, dann sagt man auch, die Seiten seien *kommensurabel*: Es gibt eine Längeneinheit, sodass beide Seiten bezüglich dieser Einheit ganzzahlige Längen haben.

Nehmen wir an, die Diagonale  $d$  und die Seite  $s$  im regelmäßigen Fünfeck seien beide ganzzahlig.

Elementar geometrische Überlegungen zeigen dann, dass  $s$  und  $d - s$  die Diagonale und Seite in einem kleineren regelmäßigen Fünfeck sind. Das heißt: Die Menge

$$\{d \in \mathbb{N} \mid \exists s \in \mathbb{N} : \frac{d}{s} = \tau\}$$

hat kein kleinstes Element. Das widerspricht der Wohlordnung der natürlichen Zahlen, und mithin sind Diagonale und Seite nicht kommensurabel.<sup>3</sup>

Es muss also noch mehr Zahlen geben als die rationalen. Man muss den Zahlenbereich noch einmal vergrößern.

Hierfür kann man entweder einen algebraischen Weg einschlagen und zum Beispiel zu  $\mathbb{Q}$  alle Lösungen von rationalen Polynomgleichungen dazunehmen, aber das überlassen wir der Algebra.

Wir sagen anstelle dessen, wie man die reellen Zahlen konstruiert.

### Bemerkung 1.1.7 Reelle Zahlen

Die rationalen Zahlen lassen sich mit einer Abstandsfunktion ausstatten. Dazu setzen wir für  $x \in \mathbb{Q}$

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

Der Abstand zweier rationaler Zahlen  $x, y$  ist dann definiert als

$$d(x, y) := |x - y|.$$

Eine Cauchy<sup>4</sup>-Folge in  $\mathbb{Q}$  ist dann eine Folge  $(x_n)_{n \in \mathbb{N}}$  von rationalen Zahlen, sodass es für jedes  $k \in \mathbb{N}$  ein  $N \in \mathbb{N}$  gibt, das die folgende Bedingung erfüllt:

$$\forall n, m > N : |x_n - x_m| < \frac{1}{k}.$$

Die Menge  $\mathcal{C}$  aller rationalen Cauchy-Folgen ist ein  $\mathbb{Q}$ -Vektorraum, und dieser enthält den Untervektorraum  $\mathcal{N}$  aller Nullfolgen.

<sup>3</sup>Hippasos von Metapont, ca. 450 v.Chr., wurde dafür, dass er dies an nicht Eingeweihte verraten hatte, von den Göttern bestraft: Er ertrank im Meer. Das zeigt, dass die Götter keine Mathematiker waren, die eben auch mit unbequemen Wahrheiten leben müssen.

<sup>4</sup>Augustin-Louis Cauchy, 1789-1857

Der Faktorraum  $\mathcal{C}/\mathcal{N}$  ist dann isomorph zur Menge der Grenzwerte aller rationalen Cauchy-Folgen. Das ist nach allgemeinem Verständnis die Menge der reellen Zahlen. Anders gesagt: Wenn wir schon die reellen Zahlen hätten, dann wäre

$$\Gamma : \mathcal{C} \longrightarrow \mathbb{R}, \quad (x_n) \mapsto \lim_{n \rightarrow \infty} x_n$$

eine  $\mathbb{Q}$ -lineare Abbildung und surjektiv, da  $\mathbb{Q}$  in  $\mathbb{R}$  dicht liegt. Ihr Kern wäre gerade  $\mathcal{N}$  nach Konstruktion. Der Homomorphiesatz für Vektorräume erlaubte uns also,  $\mathbb{R}$  mit  $\mathcal{C}/\mathcal{N}$  zu verwechseln.

Wenn es die reellen Zahlen noch nicht gibt, dann nimmt man diesen Faktorraum, um sie zu erschaffen.<sup>5</sup>

Die Vektorraumstruktur liefert insbesondere eine Addition auf  $\mathcal{C}/\mathcal{N}$ , und die Multiplikation von Cauchy-Folgen drückt sich wohldefiniert durch auf die Äquivalenzklassen (das lernt man eigentlich in Analysis I, auch wenn man dort reelle Cauchy-Folgen benutzt... die Multiplikation ist stetig!).

Die rationalen Zahlen liegen in  $\mathcal{C}/\mathcal{N}$  vermöge der injektiven Abbildung

$$\Phi : \mathbb{Q} \longrightarrow \mathcal{C}/\mathcal{N}, r \mapsto [(r, r, r, r, \dots)],$$

die Addition und Multiplikation erhält.  $\Phi(1)$  ist das neutrale Element für die Multiplikation, und für jede Cauchy-Folge  $(x_n) \notin \mathcal{N}$  gibt es ein  $M \in \mathbb{N}$ , sodass für alle  $m > M$  gilt, dass  $x_m \neq 0$ . Folglich ist die Folge  $(1/x_{M+n})_{n \in \mathbb{N}}$  wohldefiniert, und sie ist sogar eine Cauchy-Folge (siehe wieder Ana I). Ihre Klasse in  $\mathcal{C}/\mathcal{N}$  ist zu der von  $(x_n)$  bezüglich der Multiplikation invers, und da alles assoziativ, kommutativ, distributiv... ist, ist  $\mathcal{C}/\mathcal{N}$  ein Körper.

Die Metrik und die Anordnung lassen sich nach  $\mathbb{R}$  fortsetzen, und wir erhalten einen vollständigen und angeordneten Körper, der  $\mathbb{Q}$  als dichten Teilkörper enthält, und das archimedische Axiom erfüllt.

All dies müsste natürlich noch verifiziert werden, wir wollen hier darauf verzichten und es bei dieser Skizze belassen. Das einzige, was wir noch verfolgen wollen, ist die Vollständigkeit.

Dazu müssen wir erst einmal sagen, wann eine Folge in  $\mathbb{R}$  eine Cauchy-Folge ist. Oder: was der Abstand zweier reeller Zahlen ist.

Wir sagen,  $[(r_n)_{n \in \mathbb{N}}] \in \mathbb{R}$  sei positiv, wenn es ein  $K \in \mathbb{N}$  gibt, sodass für alle großen  $n \in \mathbb{N}$  die Bedingung

$$r_n > \frac{1}{K}$$

---

<sup>5</sup>Richard Dedekind, 1831-1916, hat einen alternativen Vorschlag für die Konstruktion von  $\mathbb{R}$  entworfen, die *Dedekindschen Schnitte*. Diese lassen sich nicht so gut verallgemeinern wie der hier vorgeführte Kompletierungsprozess, der sich in vielen Bereichen der Mathematik wiederfindet.

gilt.

Das ist unabhängig vom Repräsentanten und liefert durch  $x < y : \iff y - x > 0$  eine Anordnung auf  $\mathbb{R}$ . Außerdem ist jede Klasse in  $\mathbb{R}$  entweder positiv oder 0 oder negativ.

Wir definieren für  $x \in \mathbb{R}$  den Betrag durch

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

Dann ist  $d(x, y) := |x - y|$  eine Abstandsfunktion, und wir können wie in der Analysis üblich Cauchy-Folgen einführen.

### Hilfssatz 1.1.8 $\mathbb{R}$ ist vollständig

*Es sei  $(x_n)$  eine Cauchy-Folge in  $\mathbb{R}$ . Dann konvergiert  $(x_n)$  gegen ein Element von  $\mathbb{R}$ .*

*Beweis.* Wir müssen erst einmal präzisieren, was eine Cauchy-Folge  $(x_n)_{n \in \mathbb{N}}$  in  $\mathbb{R}$  ist. Jedes  $x_n$  wird durch eine rationale Cauchy-Folge  $(\xi_{n,l})_{l \in \mathbb{N}}$  repräsentiert. Cauchy-Folge zu sein heißt dann, dass für jedes  $K \in \mathbb{N}$  ein  $N \in \mathbb{N}$  existiert, sodass für alle natürlichen  $m, n \geq N$  ein  $L \in \mathbb{N}$  existiert mit

$$\forall l \geq L : |\xi_{m,l} - \xi_{n,l}| < \frac{1}{K}.$$

Um nun einen Kandidaten für den Limes von  $(x_n)_{n \in \mathbb{N}}$  zu konstruieren, wählen wir für jedes  $n \in \mathbb{N}$  eine rationale Zahl  $q_n$ , sodass für hinreichend großes  $l$  gilt:

$$|\xi_{n,l} - q_n| < \frac{1}{n}.$$

Dass dies geht folgt daraus, dass  $(\xi_{n,l})_l$  eine Cauchy-Folge ist.

Die Folge  $(q_n)_{n \in \mathbb{N}}$  ist eine Cauchy-Folge: Für alle  $K \in \mathbb{N}$  und  $m, n$  größer als das oben beschriebene  $L$  und größer als  $K$  gilt

$$|q_m - q_n| \leq |q_m - \xi_{m,l}| + |\xi_{m,l} - \xi_{n,l}| + |\xi_{n,l} - q_n| < \frac{3}{K},$$

wenn nur  $l$  groß genug ist. Da dies für jedes  $K$  geht, ist  $(q_n)$  eine Cauchy-Folge.

Schließlich gibt es für jedes  $K \in \mathbb{N}$  ein  $N \in \mathbb{N}$ , sodass

$$|\xi_{n,k} - q_k| < |\xi_{n,k} - q_n| + |q_n - q_k| < \frac{2}{K},$$

wenn nur  $n, k > N$ . Die Metrik in  $\mathbb{R}$  ist so gemacht, dass dies gerade heißt:  $x_n \rightarrow [(q_k)_{k \in \mathbb{N}}] \in \mathbb{R}$ .

Also ist  $\mathbb{R}$  vollständig. ○

**Ab jetzt geht es ernsthafter weiter, und wir fangen an, alles zu beweisen, was uns so interessiert.**

## 1.2 Teilbarkeit

### Definition 1.2.1 Teiler, ggT, kgV, Teilerfremdheit

Es sei  $n$  eine natürliche Zahl. Dann heißt  $d \in \mathbb{N}$  ein *Teiler* von  $n$ , falls ein  $t \in \mathbb{N}$  existiert mit  $d \cdot t = n$ . Wie schreiben dann  $d \mid n$ .

Die Zahl  $n$  heißt dann ein *Vielfaches* von  $d$ .

Die Menge aller Teiler von  $n$  ist endlich, denn alle Teiler von  $n$  sind  $\leq n$ .

Für zwei Zahlen  $n, m$  ist daher auch die Menge aller gemeinsamen Teiler endlich. Das größte Element dieser Menge heißt der *größte gemeinsame Teiler* von  $n$  und  $m$ . Er wird als  $\text{ggT}(m, n)$  notiert, oder manchmal auch einfach als  $(n, m)$ . Analog kann man den ggT einer endlichen Menge von natürlichen Zahlen definieren.

Die Menge aller gemeinsamen Vielfachen von  $m$  und  $n$  ist nicht leer, denn  $m \cdot n$  liegt darin. Also gibt es ein kleinstes Element dieser Teilmenge von  $\mathbb{N}$ . Es heißt das *kleinste gemeinsame Vielfache* von  $m$  und  $n$  und wird mit  $\text{kgV}(m, n)$  notiert.

Zwei natürliche Zahlen  $m, n$  heißen *teilerfremd*, wenn der einzige gemeinsame Teiler in den natürlichen Zahlen 1 ist.

### Hilfssatz 1.2.2 Euklidischer<sup>6</sup> Algorithmus

Es seien  $a, b \in \mathbb{N}$  gegeben. Dann gibt es  $c, d \in \mathbb{Z}$ , sodass

$$ac + bd = \text{ggT}(a, b).$$

*Beweis.* Es sei  $a \leq b \in \mathbb{N}$ . Man sieht schnell, dass der ggT von  $a$  und  $b$  dasselbe ist wie der ggT von  $a$  und  $b - a$ , denn jeder gemeinsame Teiler von  $a, b$  ist auch einer von  $a, b - a$  und umgekehrt.

Da im Fall  $a = b$  oder  $a = 1$  offensichtlich  $c = 1, d = 0$  eine gute Wahl ist, lässt sich also schön eine vollständige Induktion nach  $\max(a, b)$  machen.

Im Fall  $1 < a < b$  ist nämlich das Maximum von  $\{a, b - a\}$  kleiner als das von  $\{a, b\}$ , und es existieren  $\tilde{c}, \tilde{d} \in \mathbb{Z}$ , sodass

$$\tilde{c}a + \tilde{d}(b - a) = \text{ggT}(a, b - a) = \text{ggT}(a, b).$$

Also tun  $c := \tilde{c} - \tilde{d}$  und  $d := \tilde{d}$  was wir von ihnen wollen. ○

### Folgerung 1.2.3 Teiler des ggT

Für natürliche Zahlen  $a, b$  sind die Teiler von  $\text{ggT}(a, b)$  genau die gemeinsamen Teiler von  $a$  und  $b$ .

---

<sup>6</sup>Euklid, ca. 300 v. Chr.; im Prinzip wird das Vorgehen hier im siebten Buch der Elemente, §1 u. 2, beschrieben. Sehr wahrscheinlich hat Euklid das von pythagoräischen Quellen abgeschrieben.

Die bisher unklare Richtung wird nun geklärt, denn ein gemeinsamer Teiler von  $a$  und  $b$  teilt natürlich auch alle Zahlen der Form  $ca + db$ ,  $c, d \in \mathbb{Z}$ .

Insbesondere ist der ggT von  $a$  und  $b$  **der** gemeinsame Teiler, der ein Vielfaches aller gemeinsamen Teiler ist, also das kleinste gemeinsame Vielfache aller Teiler. Da gibt es nur eines – das ist das schöne an den natürlichen Zahlen.

### Bemerkung 1.2.4 Wieso Algorithmus?

Es seien wieder  $a, b$  natürliche Zahlen,  $a < b$ . Ein Verfahren, um den ggT von  $a$  und  $b$  zu bestimmen, geht so:

Setze  $a_0 := b, a_1 := a$ . Wähle  $k_1 \in \mathbb{N}$ , sodass

$$0 \leq a_2 := a_0 - k_1 a_1 < a_1.$$

Dadurch wird  $a_2$  festgelegt. Eine Wahl von  $k_1$  wie angegeben geht natürlich, denn nur endlich viele Zahlen  $k \cdot a_1$  sind kleiner als  $a_0$ , und wir setzen

$$k_1 := \max\{k \in \mathbb{N}_0 \mid k a_1 \leq a_0\}.$$

Dann gilt

$$k_1 a_1 \leq a_0 < (k_1 + 1) a_1,$$

und wir haben, was wir wollen.

Wenn hier  $a_2 = 0$  ist, dann ist  $a_1$  ein Teiler von  $a_0$ , also ist  $a$  der ggT von  $a$  und  $b$  und wir sind fertig.

Wenn  $a_2$  nicht 0 ist, so wähle eine natürliche Zahl  $k_2$ , sodass

$$0 \leq a_3 := a_1 - k_2 a_2 < a_2.$$

Mache sukzessive so weiter. Wenn  $a_i$  nicht 0 ist, so wähle  $k_i \in \mathbb{N}$  derart, dass

$$0 \leq a_{i+1} := a_{i-1} - k_i a_i < a_i.$$

Irgendwann wird das so definierte  $a_{i+1}$  Null sein, und dann brechen wir den Vorgang ab.

Dass  $a_{i+1} = 0$  gilt, heißt, dass  $a_i$  ein Teiler von  $a_{i-1}$  ist. Also ist  $a_i$  der ggT von  $a_i$  und  $a_{i-1}$ .

Wegen  $a_{i-2} = a_i + k_{i-1} a_{i-1}$  ist  $a_i$  dann auch ein Teiler von  $a_{i-2}$ , und jeder gemeinsame Teiler von  $a_{i-1}$  und  $a_{i-2}$  ist auch ein Teiler von  $a_i = a_{i-2} - k_{i-1} a_{i-1}$ . Also ist  $a_i$  der ggT von  $a_{i-1}$  und  $a_{i-2}$ . Sukzessive lässt sich das zurückverfolgen, und man sieht am Ende erstens, dass  $a_i$  der ggT von  $a_0 = b$  und  $a_1 = a$  ist, und zweitens, dass  $a_i$  sich als ganzzahlige Linearkombination von  $a$  und  $b$  schreiben lässt.

Anstatt das jetzt allgemein zurückzuverfolgen, machen wir das in einem Beispiel.

**Beispiel 1.2.5 Zwei Zahlen wohnen, ach, auf meinem Blatt**

Wir wollen den ggT der natürlichen Zahlen 117 und 265 finden und als ganzzahlige Linearkombination der beiden schreiben.

$$\begin{aligned}
 a_0 &= 265, & a_1 &= 117 \\
 k_1 &= 2, & a_2 &= 265 - 2 \cdot 117 = 265 - 234 = 31 \\
 k_2 &= 3, & a_3 &= 117 - 3 \cdot 31 = 117 - 93 = 24 \\
 k_3 &= 1, & a_4 &= 31 - 24 = 7 \\
 k_4 &= 3, & a_5 &= 24 - 3 \cdot 7 = 3 \\
 k_5 &= 2, & a_6 &= 7 - 2 \cdot 3 = 1 \\
 k_6 &= 3, & a_7 &= 3 - 3 \cdot 1 = 0 \quad - \text{ Bingo.}
 \end{aligned}$$

Der ggT ist also  $a_6 = 1$ , und die Zahlen waren demnach teilerfremd. Weiter gilt

$$\begin{aligned}
 1 &= 7 - 2 \cdot 3 = 7 - 2 \cdot (24 - 3 \cdot 7) \\
 &= 7 \cdot 7 - 2 \cdot 24 = 7 \cdot (31 - 24) - 2 \cdot 24 \\
 &= 7 \cdot 31 - 9 \cdot (117 - 3 \cdot 31) = 34 \cdot (265 - 2 \cdot 117) - 9 \cdot 117 \\
 &= 34 \cdot 265 - 77 \cdot 117,
 \end{aligned}$$

und wir können tatsächlich ganz stumpfsinnig den ggT als Linearkombination von 265 und 117 schreiben. Wir haben also konkrete Wahlen für die Zahlen  $c, d$  aus Hilfssatz 1.2.2 gefunden.

**Hilfssatz 1.2.6 Ein paar Folgerungen**

*Es seien  $a, b \in \mathbb{N}$  gegeben.*

- a) *Wenn  $g = \text{ggT}(a, b)$  gilt, dann sind die natürlichen Zahlen  $\frac{a}{g}$  und  $\frac{b}{g}$  teilerfremd.*
- b) *Wenn  $a, b$  teilerfremd sind und  $c \in \mathbb{N}$  eine Zahl ist, sodass  $a \mid bc$  gilt, dann teilt  $a$  schon  $c$ .*
- c) *Es gilt  $\text{kgV}(a, b) \cdot \text{ggT}(a, b) = a \cdot b$ .*

*Beweis.* a) Wir können  $g$  nach 1.2.2 schreiben als

$$g = ax + by, \quad x, y \in \mathbb{Z}.$$

Daher ist

$$1 = \frac{a}{g} \cdot x + \frac{b}{g} \cdot y,$$

und jeder gemeinsame natürliche Teiler von  $\frac{a}{g}$  und  $\frac{b}{g}$  teilt auch 1, muss also selbst 1 sein.

b) Es sei  $bc = ad$ ,  $d \in \mathbb{N}$ .

Jetzt ist ja 1 der ggT von  $a$  und  $b$ , wir können also 1 schreiben als

$$1 = ax + by, \quad x, y \in \mathbb{Z}.$$

Multiplikation mit  $c$  liefert

$$c = acx + bcy = a(cx + dy), \quad \text{also } a \mid c.$$

Ach so:  $(cx + dy)$  ist eine natürliche Zahl, denn sie ist ganz und  $a$  und  $c$  sind positiv, also ist auch  $(cx + dy)$  positiv.

c) Das ist eine nette Übung zum b)-Teil. Am besten fängt man mit teilerfremden  $a, b$  an... ○

### Folgerung 1.2.7 Gekürzte Brüche

Jede rationale Zahl  $q$  lässt sich auf genau eine Art als

$$q = \frac{z}{n}, \quad z \in \mathbb{Z}, \quad n \in \mathbb{N},$$

schreiben, wobei entweder  $z = 0$ ,  $n = 1$  gilt oder  $|z|$  und  $n$  teilerfremd sind.

NB: Nachher brauchen wir diese Fallunterscheidung nicht mehr, weil wir für alle Paare ganzer Zahlen einen ggT definieren werden.

*Beweis.* Wenn  $q = 0$  ist, so ist  $q = \frac{0}{1}$ . Das ist der eine Fall.

Sei also  $q \neq 0$ . Dann ist  $q = \frac{w}{m}$  für geeignete  $w \in \mathbb{Z}, m \in \mathbb{N}$ . Wenn  $g$  der größte gemeinsame Teiler von  $|w|$  und  $m$  ist, dann gilt für  $z = w/g$ ,  $n = m/g$ , dass

$$q = \frac{z}{n},$$

und  $|z|$  und  $n$  sind nach dem letzten Hilfssatz teilerfremd.

Ist  $q = \frac{s}{k}$  eine weitere Darstellung von  $q$  als Bruch teilerfremder Zahlen  $s \in \mathbb{Z}$ ,  $k \in \mathbb{N}$ , so gilt

$$\frac{s}{k} = \frac{z}{n}, \quad \text{also } |z| \cdot k = |s| \cdot n.$$

Da  $|z|, n$  und  $|s|, k$  jeweils teilerfremd sind, folgt aus dem letzten Hilfssatz, dass  $|z|$  ein Teiler von  $|s|$  ist und umgekehrt. Daher sind sie gleich. Genauso auch  $k$  und  $n$ . Die Vorzeichen von  $z$  und  $s$  sind durch das Vorzeichen von  $q$  festgelegt, also sind auch  $z$  und  $s$  gleich. ○

Nun wollen wir den Begriff der Teilbarkeit auf ein etwas abstrakteres Niveau heben. Zunächst sollte man von den natürlichen zu den ganzen Zahlen übergehen. Aber wieso nicht gleich zu kommutativen Ringen?

**Definition 1.2.8 Nochmals die Teilbarkeit**

Es sei  $R$  ein kommutativer Ring. Dann heißt  $a \in R$  ein *Teiler* von  $b \in R$ , falls ein  $c \in R$  existiert, sodass  $b = c \cdot a$ .

Für natürliche Zahlen ergibt das den alten Begriff, wenn wir  $\mathbb{Z}$  als  $\mathbb{N}$  enthaltenden Ring verwenden.

Für beliebiges  $R$  ist der zweite Faktor  $c$  jetzt nicht mehr eindeutig. In der Welt der natürlichen Zahlen war das so, und es bleibt so, wenn wir voraussetzen, dass  $R$  nullteilerfrei ist und  $a \neq 0$  gilt. Das ist für Teilbarkeitseigenschaften in Ringen oft eine gute Voraussetzung.

**Definition 1.2.9 Assoziiertheit**

Es sei  $R$  ein kommutativer Ring. Zwei Elemente  $a, b \in R$  heißen *assoziiert*, falls eine Einheit<sup>7</sup>  $e \in R^\times$  existiert, sodass  $b = a \cdot e$ .

Für  $R = \mathbb{Z}$  heißt das einfach, dass die zwei Zahlen bis aufs Vorzeichen übereinstimmen.

Assoziiert zu sein ist eine Äquivalenzrelation auf  $R$ . Die Äquivalenzklasse von  $a$  heißt seine *Assoziiertenklasse* und ist genau  $a \cdot R^\times$ . Man sagt auch, die Assoziiertenklasse von  $a$  teile die von  $b$ , wenn  $a$  ein Teiler von  $b$  ist. Es ist klar, dass diese Begriffsbildung nicht von der Wahl der Repräsentanten der Assoziiertenklassen abhängt, denn zwei solche Repräsentanten unterscheiden sich ja nur um eine Einheit.

**Bemerkung 1.2.10 Eine Ordnungsrelation**

Wenn  $R$  kommutativ und nullteilerfrei ist, dann wird durch die Teilbarkeit eine Ordnungsrelation auf der Menge der Assoziiertenklassen festgelegt:

$$aR^\times \preceq bR^\times \iff a \mid b.$$

Transitivität ist klar, dazu braucht man auch weder die Nullteilerfreiheit noch die Bildung der Assoziiertenklassen, das geht schon elementweise.

Interessanter ist es zu zeigen, dass zwei Assoziiertenklassen  $a \cdot R^\times$  und  $b \cdot R^\times$  übereinstimmen, wenn sie sich gegenseitig teilen. Das ist klar, wenn eine der beiden Klassen nur aus der Null besteht. Ansonsten geht es so:  $a$  und  $b$  teilen sich gegenseitig, es gibt also  $c, d \in R$ , sodass

$$a = bc, b = ad.$$

Daraus folgt  $a = acd$ , und da  $R$  nullteilerfrei ist, folgt aus  $a(1 - cd) = 0$ , dass  $1 - cd = 0$ . Daher ist  $cd = 1$ , und auch  $dc = 1$ , da  $R$  kommutativ ist. Es sind also  $c$  und  $d$  Einheiten in  $R$  und folglich  $a$  und  $b$  assoziiert.

<sup>7</sup>  $R^\times = \{a \in R \mid \exists b \in R : ab = 1\}$  ist eine Gruppe bezüglich der Multiplikation aus  $R$ .

**Definition 1.2.11 Noch einmal der ggT**

Es seien  $R$  ein kommutativer und nullteilerfreier Ring und  $a, b \in R$ .

- a) Das Element  $g \in R$  heißt ein *größter gemeinsamer Teiler* von  $a$  und  $b$ , wenn  $g$  ein gemeinsamer Teiler ist und jeder gemeinsame Teiler von  $a$  und  $b$  auch  $g$  teilt.

NB: Das Adjektiv „größter“ bezieht sich also auf die Ordnungsrelation aus 1.2.10.

Wenn man von **dem** ggT sprechen will, so muss man damit eigentlich die Assoziiertenklasse (eines beliebigen ggT) meinen. Im Falle  $R = \mathbb{Z}$  gibt es in einer Assoziiertenklasse  $\{a, -a\}$  immer die naheliegende Wahl, als Vertreter das nicht-negative Element zu wählen.

Wegen 1.2.3 fallen dann für natürliche Zahlen die beiden Definitionen des ggT zusammen.

- b)  $a$  und  $b$  heißen *teilerfremd*, wenn die einzigen gemeinsamen Teiler die Einheiten in  $R$  sind.

**Beispiel 1.2.12 Ein paar ggT**

Es sei  $R$  ein kommutativer und nullteilerfreier Ring.

- a) Der ggT von  $a \in R$  und einer Einheit  $e \in R^\times$  ist immer die Assoziiertenklasse von 1, also  $R^\times$ . Klar, denn nur Einheiten teilen Einheiten.
- b) Der ggT von  $a \in R$  und 0 ist immer  $a \cdot R^\times$ . Klar, denn alles teilt 0.
- c) In  $R = \mathbb{Z}[X]$  ist der ggT von  $X$  und 2 gleich 1. Es gibt kein nichtkonstantes Polynom, das 2 teilen würde, also muss der ggT eine Konstante sein, und die einzigen Teiler von 2 (in  $\mathbb{Z}$ ), die auch  $X$  teilen, sind  $\pm 1$ .

**Hilfssatz 1.2.13 Die Idealisierung**

Es sei  $R$  ein nullteilerfreier kommutativer Ring. Weiter seien  $a, b \in R$ .

- a) Ist  $d$  ein gemeinsamer Teiler von  $a$  und  $b$ , so teilt  $d$  auch jede Linearkombination  $ax + by$ ,  $x, y \in R$ .
- b) Wenn es ein  $g \in R$  gibt, sodass

$$\{ax + by \mid x, y \in R\} = Rg := \{rg \mid r \in R\}$$

gilt, dann ist  $g$  ein ggT von  $a$  und  $b$ .

*Beweis.* a) Das ist klar. Aus  $a = rd, b = sd, r, s \in R$  folgt

$$ax + by = (rx + sy)d.$$

b) Es ist  $g$  ein Teiler von  $a$  und  $b$ , da beide zur linker Hand definierten Menge gehören. Zum Beispiel ist  $a = a \cdot 1 + b \cdot 0$ .

Andererseits gehört  $g$  selber auch zu dieser Menge, und in a) hatten wir gesehen, dass jeder gemeinsame Teiler von  $a$  und  $b$  daher auch  $g$  teilt. Definitionsgemäß ist also  $g$  ein ggT von  $a$  und  $b$ .  $\circ$

### Definition 1.2.14 Ideal

- a) Es sei  $R$  ein kommutativer Ring. Eine Teilmenge  $I \subseteq R$  heißt ein *Ideal* in  $R$ , wenn  $0 \in I$  gilt,  $I$  unter Addition abgeschlossen ist, und außerdem gilt:

$$\forall r \in R, i \in I : ri \in I.$$

Als Beispiel sei für feste  $a, b \in R$  die Menge  $\{ax + by \mid x, y \in R\}$  ins Feld geführt, die gerade eben im Zuge der Teilbarkeit eine Rolle spielte. Tatsächlich kommt der Name „Ideal“ daher, dass Ideale dieser als „Idealisierung“ des Begriffs des ggT zum ersten Male das Licht der Welt erblickten.<sup>8</sup>

Die abstrakte Definition der Ideale, wie sie natürlich auch hier im Text zunächst gegeben wurde, ist erst nachträglich zu Bedeutung gekommen.

- b) Ein Ideal  $I \subseteq R$  heißt ein *Hauptideal*, falls ein  $g \in I$  existiert, sodass  $I = Rg$  gilt.

Ein Element  $g$  mit  $I = Rg$  heißt dann ein *Erzeuger* von  $I$ .

Nicht jedes Ideal ist ein Hauptideal, was auch mit daran liegt, dass nicht in jedem Ring ein ggT für beliebige Elemente existiert.

- c) Ein nullteilerfreier kommutativer Ring  $R$ , in dem jedes Ideal ein Hauptideal ist, heißt sinnvoller Weise ein *Hauptidealring*.

Nach 1.2.13 haben in einem Hauptidealring zwei Elemente stets einen ggT.

### Hilfssatz 1.2.15 Assoziiertenklassen und Ideale

*Es sei  $R$  ein Hauptidealring. Dann gelten:*

- a) *Zwei Elemente  $g, h \in R$  sind genau dann Erzeuger desselben Hauptideals  $Rg = Rh$ , wenn sie assoziiert sind.*

---

<sup>8</sup>Nämlich bei Ernst Eduard Kummer, 1810-1893

b) In jeder nichtleeren Teilmenge  $S \subseteq R$  gibt es ein Element  $m$ , das bezüglich Teilbarkeit minimal ist<sup>9</sup>.

*Beweis.* a) ist klar, denn beide Bedingungen sind in nullteilerfreien Ringen dazu äquivalent, dass  $g$  und  $h$  sich gegenseitig teilen.

b) ist etwas trickreicher. Wir schließen durch einen Widerspruchsbeweis und nehmen dazu an, die Aussage sei falsch.

Es sei  $s_1 \in S$  irgendein Element. Nach Annahme ist es nicht minimal, das heißt, es gibt einen Teiler  $s_2 \in S$  von  $s_1$ , der nicht zu  $s_1$  assoziiert ist. Sukzessive so fortfahrend wählen wir Elemente  $s_i \in S$ , sodass jeweils  $s_{i+1}$  ein Teiler von  $s_i$  ist, aber nicht umgekehrt.

Dann erhalten wir – wegen der Teilbarkeitsbedingung – eine echt aufsteigende Kette von Idealen

$$Rs_1 \subset Rs_2 \subset Rs_3 \subset \dots$$

Die Vereinigung  $I = \cup_{i \in \mathbb{N}} Rs_i$  dieser Ideale ist auch ein Ideal von  $R$ , denn:

- $0 \in I$
- $\forall a, b \in I : \exists i \in \mathbb{N} : a, b \in Rs_i$ , und daher gilt auch  $a + b \in Rs_i \subseteq I$ .
- $\forall a \in I, r \in R : \exists i \in \mathbb{N} : a \in Rs_i$  und daher gilt  $ra \in Rs_i \subseteq I$ .

Da  $R$  ein Hauptidealring ist, gibt es ein  $a \in I$  mit  $I = Ra$ . Dieses  $a$  liegt aber schon in einem der  $Rs_i$ , und es folgt

$$Ra \subseteq Rs_i \subseteq Ra, \text{ also } Ra = Rs_i.$$

Also gilt für alle  $k \geq i$ :

$$Ra \subseteq Rs_k \subseteq Ra,$$

und auch hier herrscht Gleichheit. Daher ist die Kette – entgegen der Konstruktion – nicht echt aufsteigend.

Dies liefert den gewünschten Widerspruch. ○

Wir beschreiben jetzt eine wichtige Klasse von Hauptidealringen.

### Definition 1.2.16 Euklidischer Ring

Es sei  $R$  ein nullteilerfreier kommutativer Ring. Weiter sei  $\varphi : R \rightarrow \mathbb{N}_0$  eine Abbildung.

---

<sup>9</sup>Das soll heißen, dass alle  $s \in S$ , die  $m$  teilen, zu  $m$  assoziiert sind, ist also eigentlich eine Bedingung an die Assoziiertenklassen  $sR^\times$ ,  $s \in S$ .

Dann heißt  $R$  *euklidisch bezüglich*  $\varphi$ , falls  $[\varphi(r) = 0 \iff r = 0]$  und vor allem folgendes gilt: für alle  $a, b \in R, b \neq 0$ , gibt es  $c \in R$ , sodass

$$\varphi(a - bc) < \varphi(b).$$

### Bemerkung 1.2.17 Euklid und die Hauptideale

Jeder euklidische Ring  $(R, \varphi)$  ist ein Hauptidealring. Ist nämlich  $I \subseteq R$  ein Ideal, so ist entweder  $I = \{0\} = R \cdot 0$  – ein Hauptideal – oder es gibt ein  $g \in I$ , sodass

$$\varphi(g) = \min\{\varphi(x) \mid x \in I, x \neq 0\}.$$

Es ist klar, dass dieses  $g$  jedes  $a \in I$  teilen muss, denn  $g$  ist nicht 0, also existiert ein  $c \in R$  mit  $\varphi(a - cg) < \varphi(g)$ , was nach Wahl von  $g$  ja  $\varphi(a - cg) = 0$  erzwingt, denn  $a - cg \in I$ .

Es folgt nach 1.2.13, dass in einem euklidischen Ring je zwei Elemente immer einen ggT haben. Dieser lässt sich wie in 1.2.4 berechnen, wenn man dort die  $k_i$  so wählt, dass  $\varphi(a_{i-1} - k_i a_i) < \varphi(a_i)$  gilt, was geradezu nach Definition der euklidischen Ringe möglich ist.

Es ist übrigens im Allgemeinen sehr schwer zu entscheiden, ob ein gegebener Hauptidealring durch Wahl einer Abbildung  $\varphi$  von  $R$  nach  $\mathbb{N}_0$  zu einem euklidischen Ring gemacht werden kann. Wenn man so ein  $\varphi$  sieht, dann ist alles gut. Aber wenn man keines sieht, könnte es dennoch eines geben. Das zu widerlegen ist schwer, denn die Abbildung  $\varphi$  unterliegt keinen weitreichenden strukturellen Einschränkungen, sodass ein Ansatz sich gar nicht aufdrängt.

### Beispiel 1.2.18 Einige euklidische Ringe

- a)  $\mathbb{Z}$  ist bezüglich  $\varphi(z) = |z|$  euklidisch. Das haben wir im Prinzip gerade beim euklidischen Algorithmus ausgeschlachtet.
- b) Ist  $K$  ein Körper, so ist der Polynomring  $K[X]$  euklidisch, wenn wir

$$\varphi(0) = 0, \quad \text{und sonst } \varphi(f) = \text{grad}(f) + 1$$

setzen.

Noch kohärenter wird das, wenn wir alternativ  $\varphi(f) = 2^{\text{grad}(f)}$  setzen. Dabei ist insbesondere der Grad des Nullpolynoms gleich  $-\infty$ , und  $2^{-\infty} = 0$ .

- c) Der Ring  $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$  ist euklidisch bezüglich der Abbildung

$$\varphi(a + bi) := a^2 + b^2 = |a + bi|^2.$$

Denn: Für  $a + bi, c + di \in \mathbb{Z}[i] \setminus \{0\}$  liegt auch

$$\frac{a + bi}{c + di} = \frac{ac + bd + (bc - ad)i}{c^2 + d^2} =: x + yi \in \mathbb{C}.$$

Wähle nun  $m, n \in \mathbb{Z}$  mit  $|m - x|, |n - y| \leq \frac{1}{2}$ .

Dann gilt

$$a + bi - (c + di)(m + ni) = ((x - m) + (y - n)i)(c + di),$$

und die Multiplikativität des Betrages zeigt dann

$$\varphi(a + bi - (c + di)(m + ni)) \leq \frac{1}{2}\varphi(c + di).$$

- d) Der Ring  $R := \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{R}$  ist kein Hauptidealring, also bezüglich keiner Abbildung  $\varphi$  euklidisch.

Es ist nämlich die Menge

$$I := \{2x + (1 + \sqrt{5})y \mid x, y \in \mathbb{Z}\}$$

ein Ideal in  $R$ , aber kein Hauptideal.

Ideal ist es, da es eine Untergruppe ist und für  $2x + (1 + \sqrt{5})y \in I$  sowie  $a + b\sqrt{5} \in R$  gilt

$$\begin{aligned} (a + b\sqrt{5}) \cdot (2x + (1 + \sqrt{5})y) = \\ (2ax + (1 + \sqrt{5})ay) + (2b(2y - x) + (1 + \sqrt{5})b(2x + y)). \end{aligned}$$

Das ist eine Summe von zwei Elementen in  $I$ , also selbst auch in  $I$ .

Wenn  $I$  ein Hauptideal wäre, so gäbe es ein  $g \in I$  mit  $I = Rg$ . Dann wäre also  $g$  ein Teiler von 2 im Ring  $R$ . Welche gibt es da?

Aus  $(a + b\sqrt{5})(c + d\sqrt{5}) = 2$  folgt  $ad + bc = 0$ , denn  $\sqrt{5}$  ist nicht rational. Also folgt  $\frac{a}{b} = -\frac{c}{d}$ . Wenn nun  $d$  ein gemeinsamer Teiler von  $a$  und  $b$  in  $\mathbb{Z}$  wäre, so würde es auch  $ac + 5bd = 2$  teilen. Es ist also  $\text{ggT}(a, b) = 1$  oder 2. Wäre der ggT 2, dann wäre 2 auch ein Teiler von  $a + b\sqrt{5}$  in  $R$ , und damit wären die beiden assoziiert. Analog wären 2 und  $c + d\sqrt{5}$  assoziiert, wenn  $c, d$  nicht teilerfremd wären.

Wären hingegen  $a, b$  und  $c, d$  jeweils teilerfremd, so folgte aus  $\frac{a}{b} = -\frac{c}{d}$ , dass

$$(a, b) = \pm(c, -d).$$

Eingesetzt in die Zerlegung von 2 impliziert das

$$a^2 - 5b^2 = \pm 2.$$

Diese Gleichung ist in  $\mathbb{Z}$  nicht lösbar, denn eine Zahl der Gestalt

$$\pm 2 - a^2$$

ist niemals durch 5 teilbar, wie eine Fallunterscheidung nach dem Rest der Division von  $a$  durch 5 zeigt.

Die einzigen Teiler von 2 in  $R$  sind also Einheiten und zu 2 assoziierte Elemente. Insbesondere gilt dies für unseren hypothetischen Erzeuger  $g$  von  $I$ , und das würde zeigen, dass  $I = R$  oder  $I = 2R$  gilt.

Der ersten Fall kann nicht auftreten, denn  $1 \notin I$ . Der zweite Fall kann nicht auftreten, denn  $1 + \sqrt{5} \in I$ , aber  $\notin 2R$ .

Daher ist  $I$  kein Hauptideal und mithin auch nicht euklidisch.

## 1.3 Primzahlen

### Definition 1.3.1 Primzahl

Eine Primzahl ist eine natürliche Zahl  $p > 1$ , die sich nicht als Produkt zweier kleinerer natürlicher Zahlen schreiben lässt.

Die Menge der Primzahlen notieren wir mit  $\mathbb{P}$ .

$$\begin{aligned} \mathbb{P} &= \{n \in \mathbb{N} \mid n > 1 \text{ und } \forall d, t < n : d \cdot t \neq n\} \\ &= \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \dots\}. \end{aligned}$$

Es ist eine der vornehmsten Aufgaben der Zahlentheorie, mehr zu den Pünktchen hier zu sagen.

### Hilfssatz 1.3.2 Alternative Charakterisierung

*Eine natürliche Zahl  $n > 1$  ist genau dann eine Primzahl, wenn für jedes Produkt  $a \cdot b$  von natürlichen Zahlen gilt:*

$$n \text{ teilt } ab \iff n \text{ teilt } a \text{ oder } n \text{ teilt } b.$$

*Beweis.* Wenn  $n$  ein Teiler von  $a$  oder  $b$  ist, dann teilt es auch  $ab$ . Nur die andere Richtung ist also überhaupt relevant.

Es sei zunächst  $n$  eine Primzahl, die  $ab$  teilt:  $ab = kn$  für eine natürliche Zahl  $k$ . Ist  $n$  keine Teiler von  $a$ , so sind  $a$  und  $n$  teilerfremd, denn der ggT ist ja ein gemeinsamer Teiler, aber nicht  $\pm n$ .

Wegen des euklidischen Algorithmus in  $\mathbb{Z}$  gibt es ganze Zahlen  $c, d$ , sodass  $ac + nd = 1$ . Wir multiplizieren mit  $b$  durch und erhalten

$$b = abc + bnd = n(kc + bd),$$

also ist  $b$  ein Vielfaches von  $n$ . Analog ist  $a$  ein Vielfaches von  $n$ , wenn  $b$  kein Vielfaches von  $n$  ist.

Umgekehrt erfülle  $n$  die Bedingung aus dem Hilfssatz. Wir müssen zeigen, dass es eine Primzahl ist. Sei also  $n = ab$  für natürliche Zahlen  $a, b$ .

Dann ist aber nach Voraussetzung  $n$  ein Teiler von  $a$  oder von  $b$ , und damit sind nicht beide Faktoren kleiner als  $n$  – das mussten wir zeigen.  $\circ$

### Bemerkung 1.3.3 Klarheiten

Für jede natürliche Zahl  $n$  ist die Menge der Teiler

$$\{d \in \mathbb{N} : d \mid n\} \subseteq \{1, 2, 3, \dots, n\}$$

endlich, hat also ein kleinstes Element – klar: die Eins. Für  $n \geq 2$  hat auch die Menge der von Eins verschiedenen Teiler ein kleinstes Element. Dieser kleinste Teiler ist zwangsläufig eine Primzahl. Wäre er nämlich ein Produkt zweier kleinerer Zahlen, so wären diese ja auch Teiler von  $n$ .

Also wird jede natürliche Zahl  $\geq 2$  von einer Primzahl  $p$  geteilt.

Im Fall  $p \neq n$  wird auch  $n/p$  von einer Primzahl geteilt, und induktiv sieht man, dass  $n$  ein Produkt von Primzahlen ist.

Die 1 ist nach einer sinnvollen Konvention ein leeres Produkt:

$$1 = \prod_{p \in \emptyset \subseteq \mathbb{P}} p.$$

### Satz 1.3.4 Fundamentalsatz der Arithmetik

*Jede natürliche Zahl  $n$  lässt sich als Produkt von Primzahlen schreiben. Diese Darstellung ist eindeutig, wenn die Primfaktoren der Größe nach sortiert werden.*

*Beweis.* Nur die Eindeutigkeit ist noch nicht klar.

Es sei  $n$  eine natürliche Zahl, und es seien

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_s = q_1 \cdot q_2 \cdot \dots \cdot q_t$$

zwei Zerlegungen von  $n$  als Produkt von Primzahlen, wobei

$$p_1 \leq p_2 \leq \dots \leq p_s, \quad q_1 \leq q_2 \leq \dots \leq q_t.$$

Wir müssen zeigen, dass  $s = t$  und  $p_i = q_i$ ,  $1 \leq i \leq s$ , gilt.

Das machen wir durch vollständige Induktion nach  $\min\{s, t\}$ . Ist dieses 0, so ist  $n = 1$ , und hier ist die Eindeutigkeit klar. Ist das Minimum 1, so ist  $n$  eine Primzahl, und die Behauptung ist auch klar.

Ansonsten ist  $p_1$  ein Teiler von  $q_1 \cdot \dots \cdot q_t$ , und da  $p_1$  prim ist ist es nach 1.3.2 ein Teiler eines der Faktoren, also eines  $q_j$ . Da  $q_j$  eine Primzahl ist, folgt  $p_1 = q_j$ , und wegen der Nullteilerfreiheit von  $\mathbb{Z}$  können wir diesen Faktor kürzen. Wir erhalten eine Gleichheit von Produkten von Primzahlen, mit weniger Faktoren, und aus der (unausgesprochenen) Induktionsannahme folgt die gewünschte Identität.  $\circ$

### Folgerung 1.3.5 Die $p$ -adische Bewertung

Es sei  $p \in \mathbb{P}$  eine Primzahl. Dann gibt es für jede ganze Zahl  $k \neq 0$  eine eindeutig bestimmte Zahl  $v_p(k) \in \mathbb{N}_0$ , sodass  $p^{v_p(k)}$  ein Teiler von  $k$  ist, aber  $p^{v_p(k)+1}$  nicht.

Dann gilt insbesondere

$$k = \pm \prod_{p \in \mathbb{P}} p^{v_p(k)}$$

Für  $k = 0$  schreibt man formal  $v_p(0) = \infty$ .

Es gelten für alle  $k, l \in \mathbb{Z}$  die Regeln

$$\begin{aligned} v_p(k+l) &\geq \min\{v_p(k), v_p(l)\}, \\ v_p(k \cdot l) &= v_p(k) + v_p(l). \end{aligned}$$

*Beweis.* Die Zahl  $v_p(k)$  zählt, wie oft die Primzahl  $p$  als Faktor in der Zerlegung von  $|k|$  als Produkt von Primzahlen, vorkommt, wie sie laut 1.3.4 existiert.

Zu begründen sind nur noch die Rechenregeln. Die erste ist wegen des Distributivgesetzes klar, die zweite folgt unmittelbar aus der Eindeutigkeit der Primfaktorzerlegung.  $\circ$

### Folgerung 1.3.6 $v_p$ und der ggT

Es seien  $a, b \in \mathbb{N}$ . Dann gelten:

a)  $b$  teilt  $a$  genau dann, wenn

$$\forall p \in \mathbb{P} : v_p(b) \leq v_p(a).$$

b) Der ggT von  $a$  und  $b$  ist

$$g = \prod_{p \in \mathbb{P}} p^{e_p}, \quad \text{wobei } e_p = \min\{v_p(a), v_p(b)\}.$$

c) Das kgV von  $a$  und  $b$  ist

$$k = \prod_{p \in \mathbb{P}} p^{f_p}, \quad \text{wobei } f_p = \max\{v_p(a), v_p(b)\}.$$

*Beweis.* a) Wenn für alle  $p$  die Bedingung  $v_p(b) \leq v_p(a)$  gilt, dann ist

$$a = b \cdot \prod_{p \in \mathbb{P}} p^{v_p(a) - v_p(b)},$$

und das Produkt ist eine natürliche Zahl.

Ist umgekehrt  $a = bc$  mit  $c \in \mathbb{N}$ , so gilt für alle  $p \in \mathbb{P}$

$$v_p(a) = v_p(b) + v_p(c) \geq v_p(b)$$

und es folgt die Behauptung.

b) und c) sind einfache Konsequenzen hieraus. ○

### Bemerkung 1.3.7 Fortsetzungsgeschichte

Die Abbildung  $v_p : \mathbb{Z} \rightarrow \mathbb{N}_0 \cup \{\infty\}$  heißt die *p-adische Bewertung* auf  $\mathbb{Z}$ . Sie wird durch

$$v_p\left(\frac{z}{n}\right) := v_p(z) - v_p(n)$$

zu einer Abbildung von  $\mathbb{Q}$  nach  $\mathbb{Z} \cup \{\infty\}$  fortgesetzt und behält dabei die beiden Eigenschaften aus der letzten Folgerung bei.

Wir wollen die Eigenschaften dieser Bewertung nicht weiter ausschlichten, die Notation wird aber gelegentlich hilfreich sein.

Als nächstes übertragen wir den arithmetisch motivierten Primzahlbegriff in die Ringtheorie.

### Definition 1.3.8 irreduzibel oder prim?

Es sei  $R$  ein kommutativer Ring.

Ein Element  $m \in R$  heißt *irreduzibel*, wenn  $m \notin R^\times$  und für alle  $a, b \in R$  gilt:

$$m = ab \Rightarrow a \in R^\times \text{ oder } b \in R^\times.$$

Ein Element  $p \in R$  heißt ein *Primelement*, wenn es keine Einheit in  $R$  ist und wenn für  $a, b \in R$  gilt:

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

Irreduzibilität eines Elementes  $r \in R$  heißt also, dass seine Assoziiertenklasse  $rR^\times$  in  $R$  unter den Klassen  $\neq R^\times$  bezüglich der Ordnungsrelation der Teilbarkeit minimal ist: Jeder Teiler von  $r$  ist entweder eine Einheit oder zu  $r$  assoziiert. Die Rechnung unter d) in 1.2.18 zeigt unter anderem, dass 2 in  $\mathbb{Z}[\sqrt{5}]$  irreduzibel ist.

Für die Primzahlen gilt jetzt: Sie sind – laut Vergleich der Definitionen – gerade die positiven irreduziblen Elemente im Ring  $\mathbb{Z}$ , und laut 1.3.2 auch genau die positiven Primelemente in  $\mathbb{Z}$ .

### Hilfssatz 1.3.9 Prim vs. irreduzibel

*Es sei  $R$  ein nullteilerfreier kommutativer Ring.*

- a) *Ein von 0 verschiedenes Primelement in  $R$  ist immer irreduzibel.*
- b) *Wenn  $R$  ein Hauptidealring ist, dann ist ein irreduzibles Element in  $R$  immer auch prim.*

*Beweis.* a) Es sei  $0 \neq p \in R$  prim. Weiter seien  $a, b \in R$  zwei Elemente mit  $p = ab$ .

Da  $p$  prim ist, muss es  $a$  oder  $b$  teilen. Es sei oBdA  $a = cp$ . Dann folgt

$$p = ab = cpb, \quad \text{also } p(1 - bc) = 0,$$

und da  $R$  nullteilerfrei ist, folgt  $1 - bc = 0$ , also ist  $bc = 1$ , und  $b$  ist eine Einheit.

b) Nun seien  $R$  ein Hauptidealring und  $m \in R$  irreduzibel. Weiter seien  $a, b \in R$  Elemente, sodass  $m$  ein Teiler von  $ab$  ist:  $ab = mt$ ,  $t \in R$ . Wenn  $m$  kein Teiler von  $a$  ist, dann sind  $a$  und  $m$  teilerfremd, denn die einzigen Teiler von  $m$  sind Einheiten und zu  $m$  assoziierte Elemente. Aber auch alle zu  $m$  assoziierten können  $a$  nicht teilen. Also ist 1 ein ggT von  $a$  und  $m$ , und nach 1.2.13 lässt sich schreiben als

$$1 = ac + md, \quad c, d \in R \text{ geeignet.}$$

Multiplikation mit  $b$  macht daraus wieder – wie schon für  $\mathbb{Z}$  gesehen –

$$b = abc + mbd = m(tc + bd),$$

also ist  $m$  ein Teiler von  $b$ .

Insgesamt zeigt das, dass  $m$  prim ist. ○

Jetzt können wir den Fundamentalsatz der Arithmetik in die Welt der Hauptidealringe übertragen. Die in  $\mathbb{N}$  geltende Eindeutigkeit muss einem Akt der Willkür weichen – wir müssen erst aus jeder Assoziiertenklassen von Primelementen einen Vertreter wählen.

**Satz 1.3.10 Primzerlegung in Hauptidealringen**

Es sei  $R$  ein Hauptidealring. Weiter sei  $\mathbb{P}_R$  ein Vertretersystem der Assoziertenklassen von Primelementen  $\neq 0$ .

Dann ist jedes  $r \in R \setminus \{0\}$  assoziiert zu einem Produkt von endlich vielen Primelementen.

Sind weiter  $s, t \in \mathbb{N}_0$  und  $p_1, \dots, p_s, q_1, \dots, q_t \in \mathbb{P}_R$  derart, dass eine Einheit  $\varepsilon \in R^\times$  existiert mit

$$r = p_1 \cdot \dots \cdot p_s = \varepsilon \cdot q_1 \cdot \dots \cdot q_t,$$

so gelten  $\varepsilon = 1$ ,  $s = t$  und – bis auf eine Vertauschung der Reihenfolge der Faktoren – es gilt  $p_i = q_i$  für alle  $1 \leq i \leq s$ .

*Beweis.* Die Eindeutigkeit geht im Prinzip genauso wie im Fall  $R = \mathbb{Z}$ , und dazu sage ich jetzt nichts weiter.

Die Existenz der Zerlegung geht für euklidische Ringe mit vollständiger Induktion nach  $\varphi(r)$ , im Prinzip auch genauso wie für  $\mathbb{Z}$ . Der Vollständigkeit halber soll hier noch gezeigt werden, wie man für einen beliebigen Hauptidealring argumentieren kann. Hier braucht man ein etwas anders geartetes Argument, das wir aber schon vorbereitet haben.

Wir nehmen an, die Aussage des Satzes sei falsch, und betrachten die Menge  $S$  aller Elemente  $0 \neq r \in R$ , die nicht zu einem Produkt von Elementen aus  $\mathbb{P}_R$  assoziiert sind. Diese Menge ist dann nicht leer, und es gibt nach 1.2.15 ein minimales Element  $m \in S$ .

Natürlich ist  $m$  kein Primelement, da es sonst ja zu einem  $p \in \mathbb{P}_R$  assoziiert wäre. Es sei  $m = ab$  eine Zerlegung in zwei echte Faktoren, also beide nicht zu  $m$  assoziiert. Dann sind  $a$  und  $b$  im Sinne der Teilbarkeit kleiner als  $m$  und gehören demnach nicht zu  $S$ . Genau hier braucht man übrigens, dass  $m$  nicht 0 ist.

Es gibt also eine Zerlegung

$$a = e \cdot p_1 \cdot \dots \cdot p_k, \quad b = f \cdot q_1 \cdot \dots \cdot q_l$$

mit Primelementen  $p_i, q_j \in \mathbb{P}_R$  und Einheiten  $e, f$  und es folgt

$$m = ef \cdot p_1 \cdot \dots \cdot p_k \cdot q_1 \cdot \dots \cdot q_l$$

entgegen der Annahme. Damit ist diese zum Widerspruch geführt.  $\circ$

**Beispiel 1.3.11 Primelemente in  $\mathbb{Z}[i]$** 

Der Ring  $\mathbb{Z}[i]$  der ganzen Gaußschen Zahlen ist ein Hauptidealring, siehe 1.2.18. Es ist also interessant, eine Übersicht über die Primelemente hier zu bekommen.

Hierzu benutzen wir die Normabbildung  $N : \mathbb{Z}[i] \rightarrow \mathbb{N}_0$ ,  $N(z) := |z|^2$  und die komplexe Konjugation:

$$\overline{x + yi} = x - yi.$$

Diese Abbildung ist insbesondere multiplikativ:

$$\overline{z\bar{w}} = \bar{z} \cdot \bar{w}.$$

Wenn nun  $\pi \in \mathbb{Z}[i]$  ein Primelement  $\neq 0$  ist, dann teilt es also  $N(\pi) = \pi \cdot \bar{\pi}$ , und dies ist eine natürliche Zahl. Da diese natürliche Zahl ein Produkt von Primfaktoren ist, muss  $\pi$  bereits einen dieser Primfaktoren teilen, da es ein Primelement ist. Die Primelemente in  $\mathbb{Z}[i]$  finden sich also gerade als Primteiler der natürlichen Primzahlen.

Es sei  $\pi$  ein Teiler der Primzahl  $p$ . Dann gilt

$$N(\pi) | N(p) = p^2,$$

und wir haben zwei Möglichkeiten:  $N(\pi) = p$  oder  $N(\pi) = p^2$ .

NB:  $N(\pi) = 1$  würde heißen, dass  $\pi\bar{\pi} = 1$ , und dann wäre ja  $\pi$  eine Einheit, was verboten ist.

Weiter sei nun  $\pi = a + bi$ ,  $a, b \in \mathbb{Z}$ . Dann ist  $N(\pi) = a^2 + b^2$ , und wir kommen letztlich zur Frage, wann eine Primzahl  $p \in \mathbb{P}$  sich als Summe von zwei Quadraten schreiben lässt.

Fall 1:  $p = 2$ .

Hier gilt  $2 = -i(1 + i)^2$ , und der einzige Primteiler von 2 in  $\mathbb{Z}[i]$  ist die Assoziiertenklasse von  $1 + i$ . 2 ist assoziiert zum Quadrat eines Primelements.

Fall 2:  $p$  lässt nach Division durch 4 Rest 3.

Wäre hier  $p$  die Norm eines Primelements  $a + bi$ , so folgte aus  $p = a^2 + b^2$ , dass ohne Einschränkung  $a$  gerade und  $b$  ungerade sind (ansonsten wäre die Summe der Quadrate gerade), und  $a = 2s, b = 2t + 1$  liefert

$$a^2 + b^2 = 4(s^2 + t^2 + t) + 1.$$

Daher hat jeder Primteiler  $\pi$  von  $p$  die Norm  $p^2$ , und aus

$$p = z \cdot \pi$$

folgt  $p^2 = N(p) = N(z) \cdot N(\pi) = N(z) \cdot p^2$ , also  $z\bar{z} = N(z) = 1$ , und  $z$  ist eine Einheit. Das heißt, dass  $p$  selbst prim ist in  $\mathbb{Z}[i]$ .

Fall 3:  $p$  lässt nach Division durch 4 Rest 1.

Hier sehen wir schnell Beispiele:

$$5 = 2^2 + 1^2, \quad 13 = 3^2 + 2^2, \quad 17 = 4^2 + 1^2, \quad 29 = 5^2 + 2^2,$$

aber keine Gegenbeispiele. Wir werden in Kürze (siehe 1.3.12) zeigen, dass es eine Zahl  $u \in \{0, \dots, p-1\}$  gibt, sodass  $u^2 + 1$  ein Vielfaches von  $p$  ist:

$$\exists u, k \in \{1, \dots, p-1\} : u^2 + 1 = kp.$$

Ein Primteiler  $\pi$  von  $p$  in  $\mathbb{Z}[i]$  teilt daher auch  $u+i$  oder  $u-i$ , und daher hat  $\pi$  als Norm einen Teiler von  $kp$ . Da aber nach den vorhergehenden Überlegungen die Norm von  $\pi$  ein Teiler von  $p^2$  sein muss, ist die Norm ein gemeinsamer Teiler von  $kp$  und  $p^2$ , also  $p$ , denn 1 ist sie nicht und  $k < p$ .

In diesem Fall hat also  $p$  zwei nicht assoziierte Primteiler

$$a \pm ib, a^2 + b^2 = p.$$

### Hilfssatz 1.3.12 Nachtrag

*Es sei  $p$  eine Primzahl die bei Division durch 4 Rest 1 lässt.*

*Dann gibt es eine Zahl  $u \in \{1, \dots, p-1\}$ , sodass  $p$  ein Teiler von  $u^2 + 1$  ist.*

*Beweis.*

Kurze Vorüberlegung: Gegeben seien natürliche Zahlen  $a, b, c, d$ , sodass  $p$  ein Teiler von  $a - c$  und von  $b - d$  ist. Dann teilt es auch

$$ab - cd = (a - c)b + c(b - d).$$

Hier braucht man übrigens weder, dass  $p$  Primzahl ist, noch dass es bei Division durch 4 Rest 1 lässt... Wir werden das später noch systematisieren.

Wir betrachten nun die Zahl  $v = \frac{p-1}{2}! \in \mathbb{N}$ . Nach Voraussetzung ist  $\frac{p-1}{2}$  gerade, und  $v = (-1) \cdot (-2) \cdot \dots \cdot (-(p-1)/2)$ .

Da für  $1 \leq k \leq \frac{p-1}{2}$

$$\frac{p-1}{2} + k = p - \left(\frac{p-1}{2} - k + 1\right)$$

gilt, folgt aus der Vorüberlegung, dass  $v^2$  und  $(p-1)!$  denselben Rest bei Division durch  $p$  lassen.

Für jedes  $a \in \{1, \dots, p-1\}$  gibt es ein  $b \in \{1, \dots, p-1\}$ , sodass  $ab$  bei Division durch  $p$  den Rest 1 lässt, denn  $a, p$  sind teilerfremd. Für  $a = 1$  ist  $b = 1$ , für

$a = p - 1$  ist  $b = p - 1$ , aber sonst gilt hier  $a \neq b$ . Denn: Aus  $a = b$  folgt, dass  $p$  ein Teiler von  $a^2 - 1$  ist, also entweder  $a - 1$  oder  $a + 1$  teilt. Aber  $a$  liegt zwischen 1 und  $p - 1$ .

Man kann also alle Faktoren in  $(p-1)!$  außer 1 und  $p-1$  so in Paaren gruppieren, dass das Produkt eines jeden Paares bei Division durch  $p$  Rest 1 lässt. Folglich lässt  $(p-1)!$  denselben Rest wie  $1 \cdot (p-1) = p-1$ , also Rest  $-1$ .

Nun weiß man also für  $v$ , dass  $v^2 + 1$  durch  $p$  teilbar ist. Ersetze nun  $v$  durch ein  $u = v - kp$ ,  $0 < u < p$ . Dann haben wir die Behauptung.  $\circ$

### Folgerung 1.3.13 Summen zweier Quadrate

*Eine natürliche Zahl  $n$  ist genau dann als Summe zweier Quadrate von ganzen Zahlen schreibbar, wenn für alle Primzahlen  $p \in \mathbb{P}$ , die bei Division durch 4 Rest 3 lassen, gilt, dass  $v_p(n)$  gerade ist.*

*Beweis.* Die Zahl  $n$  ist genau dann Summe zweier Quadrate, wenn sie die Norm eines Elements  $a + bi \in \mathbb{Z}[i] \setminus \{0\}$  ist.

Nun schreibt man  $a + bi$  als Produkt von Primelementen in  $\mathbb{Z}[i]$  und überlegt sich mit 1.3.11, dass das Betragsquadrat eines Primfaktors entweder 2 oder eine Primzahl  $p = 4k + 1$  oder das Quadrat einer Primzahl  $p = 4k + 3$  ist.

Das zeigt wegen  $|z \cdot w|^2 = |z|^2 \cdot |w|^2$  die Behauptung.  $\circ$

## 1.4 Zur Verteilung der Primzahlen

### Hilfssatz 1.4.1 Noch einmal Euklid

*Es gibt unendlich viele Primzahlen.*

*Beweis.* Es sei  $N \in \mathbb{N}$ . Die Zahl

$$M := N! + 1$$

hat einen Primteiler, aber dieser kann nicht  $\leq N$  sein, denn sonst müsste er mit  $N!$  auch  $1 = M - N!$  teilen. Also gibt es eine Primzahl  $> N$ .  $\circ$

### Hilfssatz 1.4.2 Lückenhaft

*Es sei  $k \in \mathbb{N}$ . Dann gibt es eine natürliche Zahl  $M$ , sodass zwischen  $M$  und  $M + k$  keine Primzahl liegt.*

*Beweis.* Setze  $M = (k + 2)! + 2$ .  $\circ$

Nun könnte man fragen, wie sich bequem eine schöne Liste von Primzahlen erstellen lässt. Auch hier ist die Antwort schon über 2000 Jahre alt.

**Bemerkung 1.4.3 Sieb des Eratosthenes<sup>10</sup>**

Es sei  $M \in \mathbb{N}$  eine natürliche Zahl. Betrachte

$$S_1 := \{n \in \mathbb{N} \mid 2 \leq n \leq M\}.$$

Die kleinste Zahl von  $S_1$  ist  $p_1 := 2$ , eine Primzahl. Setze

$$S_2 := \{n \in S_1 \mid p_1 \text{ teilt nicht } n\}.$$

Das Minimum von  $S_2$  ist  $p_2 := 3$ , eine Primzahl. Setze

$$S_3 := \{n \in S_2 \mid p_2 \text{ teilt nicht } n\}.$$

Das sind die Zahlen aus  $S_1$ , die keine Vielfachen von 2 oder 3 sind. Mache sukzessive so weiter: Setze  $p_i = \min(S_i)$ , solange dies nicht leer ist. Dann ist  $p_i$  eine Primzahl, sonst wäre es vorher schon als Vielfaches einer kleineren Zahl gestrichen worden. Setze weiter

$$S_{i+1} := \{n \in S_i \mid p_i \text{ teilt nicht } n\}.$$

Wenn schließlich  $S_{i+1}$  leer ist, dann gilt

$$\{p_1, p_2, \dots, p_i\} = S_1 \cap \mathbb{P} = \{p \in \mathbb{P} \mid p \leq M\}.$$

Kleine Fußnote am Rande: Sobald  $p_j > \sqrt{M}$  gilt, sind in  $S_j$  nur noch Primzahlen übrig, denn eine natürliche Zahl  $n \geq 2$ , die keine Primzahl ist, hat einen Teiler  $\leq \sqrt{n}$ . Man kann also hier schon mit dem Sieben aufhören. Dann ist

$$\{p_1, \dots, p_j\} \cup S_j$$

die gesuchte Menge der Primzahlen  $\leq M$ .

**Bemerkung 1.4.4 Ein Euler<sup>11</sup>-Produkt**

Leonhard Euler hat das folgende Argument für die Unendlichkeit der Menge der Primzahlen gegeben: Wenn es nur endlich viele Primzahlen  $\{p_1, \dots, p_k\}$  gäbe,  $p_1 < p_2 < \dots < p_k$ , so betrachte die rationale Zahl

$$\begin{aligned} \prod_{i=1}^k \frac{1}{1-p_i^{-1}} &= \prod_{i=1}^k \left( \sum_{j_i=0}^{\infty} p_i^{-j_i} \right) \\ &= \sum_{j_1=0}^{\infty} \sum_{j_2=0}^{\infty} \dots \sum_{j_k=0}^{\infty} p_1^{-j_1} \cdot p_2^{-j_2} \cdot \dots \cdot p_k^{-j_k} \\ &= \sum_{n=1}^{\infty} \frac{1}{n}. \end{aligned}$$

<sup>10</sup>Eratosthenes, ca. 284-200 v.Chr.

<sup>11</sup>Leonhard Euler, 1707-1783

Hier benutzen wir zunächst die geometrische Reihe und dann das Distributivgesetz in seiner Inkarnation als Cauchy-Faltungsvorschrift für das (endliche) Produkt absolut konvergenter Reihen. Schließlich kommt wegen des Fundamentalsatzes der Arithmetik – wir haben ja alle Primzahlen ins Feld geführt! – die harmonische Reihe heraus, die bekanntlich divergiert. Ein Widerspruch!

Über Konvergenzfragen hat Euler sich übrigens nie sehr große Gedanken gemacht. Aber er hatte die entscheidende Einsicht, wie es geht, und mehr noch, wie sich die Dinge mit dieser Art von Argumentation quantitativ genauer fassen lassen. Wir wollen ihm noch etwas dabei zusehen.

Vorher sagen wir schon einmal, dass in der analytischen Zahlentheorie anstelle von  $\ln$  immer  $\log$  gesagt wird; so heißt hier der natürliche Logarithmus.

Außerdem lässt sich jede Zahl  $n \in \mathbb{N}$  auf eindeutig bestimmte Art als Produkt einer Quadratzahl und einer quadratfreien Zahl schreiben, wobei quadratfrei heißt, dass es außer 1 keinen quadratischen Faktor gibt.

Die quadratfreien Zahlen sind also genau die Produkte von endlich vielen paarweise verschiedenen Primzahlen.

$$1, 2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17, 19, 21, \dots$$

#### Hilfssatz 1.4.5 Noch eine Einsicht von Euler

Für jede reelle Zahl  $x > 1$  gilt

$$\sum_{x \geq p \in \mathbb{P}} \frac{1}{p} \geq \log(\log x) - \log 2.$$

*Beweis.* Wir betrachten zunächst

$$\log x = \int_1^x \frac{1}{x} dx < \sum_{x \geq n \in \mathbb{N}} \frac{1}{n}$$

Andererseits ist (wenn wir  $n = m^2 f$  mit quadratfreiem  $f$  als Faktor schreiben)

$$\sum_{x \geq n \in \mathbb{N}} \frac{1}{n} \leq \sum_{m \leq \sqrt{x}} \frac{1}{m^2} \cdot \sum_{f \leq x} \frac{1}{f} \leq 2 \prod_{x \geq p \in \mathbb{P}} \left(1 + \frac{1}{p}\right) \leq 2 \cdot \exp\left(\sum_{x \geq p \in \mathbb{P}} \frac{1}{p}\right),$$

denn  $\exp(t) \leq 1 + t$  für reelles  $t$ .

Hier haben wir die Summe

$$\sum_{m \leq x} \frac{1}{m^2}$$

durch 2 abgeschätzt, was wegen

$$\frac{1}{m^2} < \frac{1}{m-1} - \frac{1}{m} \quad (m \geq 2)$$

und einem Teleskopsummenargument legal ist.

Ziehen des Logarithmus aus der nun resultierende Ungleichung

$$\log x < 2 \exp\left(\sum_{x \geq p \in \mathbb{P}} \frac{1}{p}\right)$$

liefert das gewünschte Ergebnis. ○

### Bemerkung 1.4.6 Die Verteilungsfunktion – der Primzahlsatz

Für eine reelle Zahl  $x$  sei

$$\pi(x) := \#\{p \in \mathbb{P} \mid p \leq x\}.$$

Diese Funktion zählt also, wieviele Primzahlen unterhalb  $x$  es gibt.

Schon Euklid wusste, dass  $\lim_{x \rightarrow \infty} \pi(x) = \infty$ , auch wenn er es so nicht formuliert hätte.

Hätte man für die  $n$ -te Primzahl eine Abschätzung vom Typ

$$p_n \geq C \cdot n^{1/(1-\varepsilon)}, \quad n \gg 0, C \text{ eine Konstante,}$$

so würde dies die Konvergenz der Summe der Kehrwerte der Primzahlen zeitigen. Also gibt es – wegen Eulers Lemma – solch eine Abschätzung nicht, und das zeigt, dass  $\pi(x)$  zum Beispiel immer wieder größer sein muss als  $x^{1-\delta}$  für jedes positive  $\delta$ . Also sogar

$$\limsup_{x \rightarrow \infty} \pi(x) \frac{x^\delta}{x} = \infty.$$

Schon bei Lagrange<sup>12</sup>, spätestens bei Gauß<sup>13</sup> findet sich eine präzise Vermutung, wie schnell  $\pi(x)$  ansteigt. Die Vermutung war

$$\lim_{x \rightarrow \infty} \pi(x) \cdot \frac{\log x}{x} = 1.$$

Das ist nach der Regel von L'Hospital<sup>14</sup> so äquivalent zur eigentlich von Gauß stammenden Formel

$$\lim_{x \rightarrow \infty} \pi(x) \cdot \frac{1}{\int_2^x (\log t)^{-1} dt} = 1.$$

Allerdings liefert der hier im Nenner stehende Integrallogarithmus ein besseres Konvergenzverhalten.

<sup>12</sup>Joseph Louis Lagrange, 1736-1813

<sup>13</sup>Carl Friedrich Gauß, 1777-1855

<sup>14</sup>Guillaume Francois Antoine L'Hospital, 1661-1704

Dass Gauß den richtigen Riecher hatte wurde erst etwa 100 Jahre später bewiesen, und zwar mit Methoden der Funktionentheorie und unabhängig voneinander 1896 von Hadamard<sup>15</sup> und La Vallée-Poussin<sup>16</sup>. Sie benutzten beide die Riemannsche Zetafunktion.

Noch einmal etwa 50 Jahre später gab es einen Beweis ohne Funktionentheorie, den sogenannten elementaren Beweis des Primzahlsatzes, der von Erdős<sup>17</sup> und Selberg<sup>18</sup> auch unabhängig erbracht wurde.

### Definition 1.4.7 Arithmetische Funktionen

Eine *arithmetische Funktion* ist eine Abbildung  $\varphi : \mathbb{N} \rightarrow \mathbb{C}$ .

Die Menge  $\mathcal{A} = \text{Abb}(\mathbb{N}, \mathbb{C})$  aller arithmetischen Funktionen ist mit den üblichen Verknüpfungen ein komplexer Vektorraum.

Wir definieren eine weitere Verknüpfung – die *Faltung* – durch

$$* : \mathcal{A} \times \mathcal{A} \rightarrow \mathcal{A}, (\varphi * \psi)(n) := \sum_{d|n} \varphi(d) \cdot \psi(n/d).$$

Man rechnet leicht nach, dass  $*$  assoziativ ist, und dass  $(\mathcal{A}, +, *)$  ein kommutativer Ring wird, dessen Einselement die Abbildung  $\delta$  mit

$$\delta(n) := \begin{cases} 1, & \text{falls } n = 1, \\ 0, & \text{sonst.} \end{cases}$$

ist.

Eine arithmetische Funktion  $\varphi$  heißt *strikt multiplikativ*, falls  $\varphi(1) = 1$  gilt und  $\forall m, n \in \mathbb{N} : \varphi(mn) = \varphi(m)\varphi(n)$ .

Sie heißt *multiplikativ*, falls  $\varphi(1) = 1$  gilt und

$$\forall m, n \in \mathbb{N} : \text{ggT}(m, n) = 1 \Rightarrow \varphi(mn) = \varphi(m) \cdot \varphi(n).$$

### Bemerkung 1.4.8 Einheiten und Dirichletreihen<sup>19</sup>

- a) Die Einheiten in  $\mathcal{A}$  sind genau die Folgen  $\varphi$  mit  $\varphi(1) \neq 0$ . Der Beweis ist eine leichte Übungsaufgabe.

<sup>15</sup>Jaques Hadamard, 1865 - 1963

<sup>16</sup>Charles Jean Gustav Nicolas, Baron de La Vallée-Poussin, 1866-1962

<sup>17</sup>Paul Erdős, 1913 - 1996

<sup>18</sup>Atle Selberg, 1917 - 2007

<sup>19</sup>Johann Peter Gustav Lejeune Dirichlet, 1805-1859

- b) Die multiplikativen arithmetischen Funktionen bilden eine Untergruppe von  $\mathcal{A}^\times$ .

Insbesondere hat zum Beispiel die (sogar strikt) multiplikative arithmetische Funktion  $\eta(n) = 1$  eine Inverse. Sie ist gegeben durch

$$\mu(n) = \begin{cases} 0, & \text{falls } n \text{ nicht quadratfrei,} \\ (-1)^k, & \text{falls } n = p_1 \cdot \dots \cdot p_k, \text{ } p_i \in \mathbb{P} \text{ paarweise verschieden.} \end{cases}$$

und heißt die Möbius<sup>20</sup>-Funktion. Diese ist übrigens nicht mehr strikt multiplikativ!

Speziell gilt für  $\varphi, \psi \in \mathcal{A}$ :

$$\varphi = \eta * \psi \iff \psi = \mu * \varphi.$$

Diese Formel heißt die Möbius-Inversionsformel.

- c) Für eine arithmetische Funktion  $\varphi = (\varphi(n))_{n \in \mathbb{N}}$  bezeichnen wir mit

$$D(\varphi, s) := \sum_{n \in \mathbb{N}} \frac{\varphi(n)}{n^s}$$

die zugehörige *formale Dirichletreihe*. Falls diese für ein  $\sigma \in \mathbb{R}$  konvergiert, so konvergiert sie auch für alle  $s > \sigma$ , und für alle  $s > \sigma + 1$  konvergiert sie sogar absolut.

Beispiel: Die *Riemannsches*<sup>21</sup> *Zetafunktion*  $\zeta(s) := \sum_{n=1}^{\infty} n^{-s}$  konvergiert (überhaupt, und dann auch absolut) genau dann, wenn  $s > 1$ .

- d) Für zwei arithmetische Funktionen  $\varphi, \psi$  gilt formal

$$D(\varphi, s) \cdot D(\psi, s) = \sum_{m, n \in \mathbb{N}} \frac{\varphi(n) \cdot \psi(m)}{n^s m^s} = D(\varphi * \psi, s).$$

Diese Gleichheit gilt „wirklich“ für diejenigen Werte von  $s$ , wo die Dirichletreihen absolut konvergieren.

Zum Beispiel ist  $1/\zeta(s) = \sum_{n=1}^{\infty} \mu(n)n^{-s}$ .

- e) Für eine multiplikative arithmetische Funktion  $\varphi$  und eine Primzahl  $p$  sei

$$\varphi_p(n) = \begin{cases} \varphi(n), & \text{falls } n = p^k, \text{ } k \in \mathbb{N}_0, \\ 0, & \text{sonst.} \end{cases}$$

<sup>20</sup>August Ferdinand Möbius, 1790-1868

<sup>21</sup>Bernhard Georg Friedrich Riemann, 1826-1866

Das ist der  $p$ -Anteil von  $\varphi$ , und es gilt

$$\varphi = *_{p \in \mathbb{P}} \varphi_p.$$

Das liegt einfach am Fundamentalsatz der Arithmetik. Für jedes  $n$  sind nur endlich viele Primfaktoren beteiligt, und deshalb ist das scheinbar unendliche Faltungsprodukt rechter Hand in Wirklichkeit endlich.

d) impliziert dann – auf zunächst formaler Ebene –

$$D(\varphi, s) = \prod_{p \in \mathbb{P}} D(\varphi_p, s) = \prod_{p \in \mathbb{P}} \sum_{k=0}^{\infty} \frac{\varphi(p^k)}{p^{ks}}.$$

Diese stimmt im Fall der absoluten Konvergenz tatsächlich für die Funktion  $D(\varphi)$ . Statt  $D(\varphi_p, s)$  ist es gebräuchlicher,  $D_p(\varphi, s)$  zu schreiben. Diese Funktion heißt dann ein *Euler-Faktor* von  $D(\varphi, s)$ .

### Bemerkung 1.4.9 Einige Aussagen zur Verteilung der Primzahlen

- a) Neben dem Primzahlsatz an sich gibt es auch den Dirichletschen Primzahlsatz, der besagt, dass es für je zwei teilerfremde ganze Zahlen  $a, b$  (mit  $a \neq 0$ ) unendlich viele Primzahlen der Gestalt  $ak+b$ ,  $k \in \mathbb{Z}$  gibt. Im Beweis benutzte er wesentlich Eigenschaften geeignet gewählter Dirichlet-Reihen, und das ist übrigens häufig eine Methode, um Aussagen zur Verteilung der Primzahlen zu beweisen.

Für  $a \in \{1, 2, 3, 4, 6\}$  kann man Dirichlets Satz für alle relevanten Werte von  $b$  relativ elementar zeigen – im Wesentlichen muss man nur  $b = \pm 1$  ansehen.

Für alle anderen Zahlen  $a$  gibt es mehr als 2 zu  $a$  teilerfremde Reste.

- b) Es wird vermutet, dass es unendlich viele Primzahlen  $p$  gibt, für die auch  $p+2$  eine Primzahl ist. Diese *Primzahlzwillingsvermutung* lässt sich auch quantifizieren.
- c) Es wird vermutet, dass sich jede gerade natürliche Zahl  $\geq 4$  als Summe zweier Primzahlen schreiben lässt. Dies ist die sogenannte Goldbach<sup>22</sup>-Vermutung.
- d) Es ist mittlerweile bekannt, dass es für jedes  $k \in \mathbb{N}$  natürliche Zahlen  $a, b$  gibt, sodass  $a, a+b, 2a+b, \dots, ka+b$  allesamt Primzahlen sind. Dieser Satz von Tao<sup>23</sup> und Green<sup>24</sup> war eine der Arbeiten, für die Tao im Jahre 2006 die Fields<sup>25</sup>-Medaille bekam.

<sup>22</sup>Christian von Goldbach, 1690 - 1764

<sup>23</sup>Terence Tao, geb. 1975

<sup>24</sup>Ben Green, geb. 1977

<sup>25</sup>John Charles Fields, 1863-1932

## 1.5 Gleichungssysteme

### Definition 1.5.1 Basen

Es sei  $A$  eine (additiv geschriebene) abelsche Gruppe. Dann heißt  $B \subseteq A$  eine ( $\mathbb{Z}$ -) *Basis* von  $A$ , wenn sich jedes  $a \in A$  auf eindeutig bestimmte Art als

$$a = \sum_{b \in B} \lambda_b \cdot b, \quad \lambda_b \in \mathbb{Z}, \text{ fast alle } \lambda_b = 0$$

schreiben lässt. Dabei heißt *fast alle* genauer: alle bis auf endlich viele.

Wir werden zumeist endliche Basen  $B$  betrachten, und dann kann man diesen Zusatz auch weglassen.

Wenn  $A$  eine Basis  $B$  hat, dann nennt man  $A$  auch eine *freie abelsche Gruppe über  $B$* .

Ist dann  $G$  irgendeine abelsche Gruppe und  $\varphi : B \rightarrow G$  eine Abbildung, so lässt sich diese Abbildung auf genau eine Art zu einem Gruppenhomomorphismus  $\Phi : A \rightarrow G$  fortsetzen.

### Bemerkung 1.5.2 Ohne jede Basis

- a) Jede Basis einer frei abelschen Gruppe ist insbesondere über  $\mathbb{Z}$  linear unabhängig, denn sonst könnte man die 0 auf zwei verschiedene Arten als Linearkombination schreiben.
- b) Nicht jede abelsche Gruppe hat eine Basis. Zum Beispiel  $\mathbb{Q}$  besitzt keine.
- c) Die positiven rationalen Zahlen sind eine Gruppe bezüglich der Multiplikation. Als Gruppe wird sie von den Primzahlen erzeugt, die – wegen der Eindeutigkeit der Primfaktorzerlegung – eine Basis von  $\mathbb{Q}_{>0}$  bilden.
- d) Es ist nicht immer so, dass ein minimales Erzeugendensystem eine Basis sein muss, selbst wenn es eine solche gibt; auch eine maximale, linear unabhängige Teilmenge ist nicht immer eine Basis. . . es gibt keinen so einfachen Basisergänzungssatz wie in der Linearen Algebra.

Die richtige Definition steht eben da oben, und das ist die Eigenschaft, mit der immer gearbeitet wird.

- e) Eine Basis  $B$  von  $\mathbb{Z}^n$  hat immer  $n$  Elemente, denn die Standardbasis und  $B$  sind dann beide auch  $\mathbb{Q}$ -Basen von  $\mathbb{Q}^n$ .

Da jede abelsche Gruppe mit einer endlichen Basis zu einem  $\mathbb{Z}^r$  isomorph ist, ist die Anzahl der Elemente einer Basis ein Invariante von  $A$ . Sie heißt der *Rang* von  $A$ .

**Hilfssatz 1.5.3 ... und dann doch!**

Es seien  $n \in \mathbb{N}_0$  und  $A \subseteq \mathbb{Z}^n$  eine Untergruppe.

Dann hat  $A$  eine Basis aus höchstens  $n$  Elementen.

*Beweis.* Wir machen vollständige Induktion nach  $n$ .

Für  $n = 0$  ist nichts zu zeigen (die leere Menge ist eine Basis von  $\mathbb{Z}^0$ ), und für  $n = 1$  ist die Aussage auch klar, denn entweder  $A$  ist  $\{0\}$  oder nicht, und im zweiten Fall besteht  $A$  aus allen Vielfachen von  $x_0 := \min\{x \in A \mid x > 0\}$ . Also ist (wegen der Nullteilerfreiheit von  $\mathbb{Z}$ )  $\{a_0\}$  eine Basis von  $A$ .

Nun sei die Behauptung wahr für  $n$  und  $A$  eine Untergruppe von  $\mathbb{Z}^{n+1}$ .

Weiter sei

$$\Phi : \mathbb{Z}^{n+1} \rightarrow \mathbb{Z}, \Phi((z_1, \dots, z_{n+1})^\top) = z_{n+1}.$$

Dann ist  $\Phi(A)$  eine Untergruppe von  $\mathbb{Z}$ .

Fall 1:  $\Phi(A) = \{0\}$ . Dann ist  $A$  in Wirklichkeit eine Untergruppe von  $\mathbb{Z}^n$ , was wir als Untergruppe von  $\mathbb{Z}^{n+1}$  auffassen, und wir können die Induktionsannahme direkt für  $A$  benutzen.

Fall 2:  $\Phi(A) \neq \{0\}$ . Sei dann  $x_0 > 0$  der positive Erzeuger von  $\Phi(A)$ .

Dann gibt es ein  $b_0 \in A$ , sodass  $\Phi(b_0) = x_0$ .

Nun sei  $K := \text{Kern}(\Phi) = \{a \in A \mid \Phi(a) = 0\}$ . Der Kern von  $\Phi$  wird nun wieder mit  $\mathbb{Z}^n$  identifiziert, und das zeigt, dass  $K$  eine Basis  $B$  aus höchstens  $n$  Elementen besitzt.

Dann gilt für  $a \in A$ :

$$a = \frac{\Phi(a)}{x_0} b_0 + \left(a - \frac{\Phi(a)}{x_0} b_0\right) = \frac{\Phi(a)}{x_0} b_0 + \sum_{b \in B} \lambda_b \cdot b$$

für geeignete ganze Zahlen  $\lambda_b, b \in B$ . Es ist klar, dass die Vorfaktoren hierbei eindeutig bestimmt sind (der Vorfaktor vor  $b_0$  ergibt sich aus  $\Phi(a) = \lambda_{b_0} \Phi(b_0)$ , der Rest weil  $B$  linear unabhängig ist).

Also ist  $B \cup \{b_0\}$  eine Basis von  $A$ . ○

**Hilfssatz 1.5.4 Unimodulare Matrizen**

Es sei  $M \in \mathbb{Z}^{n \times n}$  gegeben. Dann sind äquivalent:

- i) Die Spalten von  $M$  bilden eine Basis von  $\mathbb{Z}^n$ .
- ii) Es gibt eine zu  $M$  inverse Matrix mit ganzzahligen Einträgen.
- iii)  $\det(M) = \pm 1$ .

Matrizen, für die eine dieser Aussagen stimmt, heißen unimodulare Matrizen.

*Beweis.*

i)  $\Rightarrow$  ii) Wenn die Spalten von  $M$  eine Basis von  $\mathbb{Z}^n$  bilden, dann lassen sich die Standardbasisvektoren als ganzzahlige Linearkombinationen dieser Spalten schreiben, das heißt es gibt  $v_1, \dots, v_n \in \mathbb{Z}^n$  mit  $Mv_i = e_i$ . Die Matrix  $N$  mit Spalten  $v_1, \dots, v_n$  ist also zu  $M$  invers und ganzzahlig.

ii)  $\Rightarrow$  iii) Aus  $MN = E_n, M, N \in \mathbb{Z}^{n \times n}$ , folgt

$$\det(M) \cdot \det(N) = \det(E_n) = 1,$$

also sind die ganzen Zahlen  $\det(M)$  und  $\det(N)$  Einheiten in  $\mathbb{Z}$ .

iii)  $\Rightarrow$  i)

Sei umgekehrt  $\det(M) = \pm 1$ . Das charakteristische Polynom

$$\text{CP}_M(X) = \det(XE_n - M) = \sum_{i=0}^n a_i X^i$$

ist ein normiertes ganzzahliges Polynom mit konstantem Term  $a_0 = \pm 1$  – das ist gerade die Bedingung an die Determinante von  $M$ .

Der Satz von Cayley<sup>26</sup>-Hamilton<sup>27</sup> sagt dann, dass

$$\sum_{i=0}^n a_i M^i = 0,$$

und daraus folgt

$$M \cdot \left( \sum_{i=1}^n a_i M^{i-1} \right) = \sum_{i=1}^n a_i M^i = \pm E_n.$$

Die Matrix  $\pm \sum_{i=1}^n a_i M^{i-1}$  ist also ganzzahlig und invers zu  $M$ , und damit sind insbesondere die Standardbasisvektoren von  $\mathbb{Z}^n$  in der von den Spalten von  $M$  erzeugten Untergruppe von  $\mathbb{Z}^n$ . Diese Spalten erzeugen also  $\mathbb{Z}^n$ , und da sie linear unabhängig sind, bilden sie eine Basis.

○

### Definition 1.5.5 Nicht alles ist primitiv...

Es sei  $v \in \mathbb{Z}^n$ . Dann heißt der ggT der Einträge von  $v$  auch der *Inhalt* von  $v$ , kurz  $\text{Inh}(v)$ .

Wenn der Inhalt von  $v$  1 ist, dann heißt  $v$  auch ein *primitiver Vektor*.

<sup>26</sup>Arthur Cayley, 1821-1895

<sup>27</sup>William Rowan Hamilton, 1805-1865

**Hilfssatz 1.5.6 Basisergänzung**

Ein Vektor  $v \in \mathbb{Z}^n$  ist genau dann ein Element einer Basis von  $\mathbb{Z}^n$ , wenn  $\text{Inh}(v) = 1$ .

*Beweis.* Es sei  $v \in B$ ,  $B$  eine Basis von  $\mathbb{Z}^n$ . Da dann  $\text{Inh}(v)$  ein Teiler der Determinante der unimodularen Matrix ist, die die Elemente von  $B$  als Spalten hat, ist  $\text{Inh}(v) = 1$ .

Sei umgekehrt  $\text{Inh}(v) = 1$ . Dann ist – wegen Euklid – 1 eine ganzzahlige Linearkombination der Einträge von  $v$ , also

$$\exists w \in \mathbb{Z}^n : w^\top \cdot v = 1.$$

Analog zum Vorgehen im Beweis von 1.5.3 sei

$$K := \{u \in \mathbb{Z}^n \mid w^\top \cdot u = 0\}.$$

Dann findet sich

$$\mathbb{Z}^n = \mathbb{Z} \cdot v + K,$$

und  $\mathbb{Z} \cdot v \cap K = \{0\}$ , und die Hinzunahme von  $v$  zu einer Basis von  $K$  liefert eine Basis von  $\mathbb{Z}^n$ .  $\circ$

**Satz 1.5.7 Elementarteilersatz**

Es seien  $F$  eine freie abelsche Gruppe vom Rang  $n$  und  $U \subseteq F$  eine Untergruppe vom Rang  $r$ .

Dann gibt es eine Basis  $\{b_1, \dots, b_n\}$  von  $F$  und natürliche Zahlen  $e_1 \mid e_2 \mid \dots \mid e_r$ , sodass

$$\{e_1 b_1, e_2 b_2, \dots, e_r b_r\}$$

eine Basis von  $U$  ist.

NB: Dies ist so etwas wie ein Basisergänzungssatz.

*Beweis.* Ohne Einschränkung dürfen wir  $F = \mathbb{Z}^n$  annehmen.

Wir machen wieder vollständige Induktion, dieses Mal aber nach  $r$ . Für  $r = 0$  ist nichts zu zeigen.

Für  $r = 1$  sei  $c$  ein Basisvektor von  $U$  und  $e = \text{Inh}(c)$ . Dann ist  $b_1 := c/e$  ein ganzzahliger Vektor, dessen Einträge teilerfremd sind, der sich also zu einer Basis von  $\mathbb{Z}^n$  ergänzen lässt. Das ist die Behauptung.

Es sei  $r \geq 2$ . Dann gibt es ein  $c_1 \in U$  derart, dass  $\text{Inh}(c_1)$  bezüglich der Division unter den Inhalten von Elementen  $\neq 0$  von  $U$  minimal ist. Diese Inhalte sind ja eine nichtleere Teilmenge von  $\mathbb{N}$ , und man könnte und sollte hier einfach einen

Vektor mit minimalem von 0 verschiedenem Inhalt nehmen. Sei  $e_1$  der Inhalt von  $c_1$ .

Dann gibt es ein  $w \in \mathbb{Z}^n$  mit  $w^\top \cdot c_1 = e_1$ . Das Element  $b_1 := \frac{1}{e_1}c_1$  ist primitiv in  $\mathbb{Z}^n$ , und mit

$$K := \{u \in \mathbb{Z}^n \mid w^\top \cdot u = 0\}$$

gilt

$$U = U \cap \mathbb{Z}^n = U \cap (\mathbb{Z} \cdot b_1 + K) = \mathbb{Z} \cdot c_1 + (U \cap K).$$

Nach Induktionsvoraussetzung gibt es eine Basis  $\{b_2, \dots, b_n\}$  von  $K$  und Zahlen  $e_2 \mid e_3 \mid \dots \mid e_r$ , sodass

$$c_2 := e_2 b_2, \dots, c_r := e_r b_r$$

eine Basis von  $K \cap U$  bilden.

Noch zu zeigen ist nun, dass  $e_1$  ein Teiler von  $e_2$  ist.

Sei dazu  $v \in \mathbb{Z}^n$  mit  $v \cdot c_2 = e_2$  gegeben. Das geht, da  $b_2$  ja primitiv ist und daher  $e_2$  der Inhalt von  $c_2 = e_2 b_2$  ist.

Dann ist aber  $e_1$  ein Teiler von  $v^\top \cdot c_1$ , und wir ersetzen  $v$  durch

$$\tilde{v} := v - \frac{v^\top \cdot c_1}{e_1} w.$$

Dann gilt für  $w$  und  $\tilde{v}$  sogar

$$w^\top c_1 = e_1, w^\top c_2 = 0, \tilde{v}^\top c_1 = 0, \tilde{v}^\top c_2 = e_2.$$

Nun sei  $\text{ggT}(e_1, e_2) = se_1 + te_2$  für geeignete  $s, t \in \mathbb{Z}$ . Dann folgt

$$\text{Inh}(sc_1 + tc_2) \mid (w + \tilde{v})^\top (sc_1 + tc_2) = \text{ggT}(e_1, e_2) \mid e_1.$$

Da aber  $e_1$  unter den Inhalten der Elemente von  $U$  minimal gewählt war, folgt  $\text{Inh}(sc_1 + tc_2) = e_1$ , und damit teilt  $e_1$  auch  $e_2$ .

Damit ist der Satz gezeigt. ○

### Bemerkung 1.5.8 Elementarteiler

Die Zahlen  $e_1, \dots, e_r$  aus dem Satz sind eindeutig durch  $A$  festgelegt; das soll hier nicht vorgeführt werden. Sie heißen die *Elementarteiler* von  $U$  in  $F$ .

Der Elementarteilersatz hat auch folgende Formulierung:

### Satz 1.5.9 Die Matrixversion

Es sei  $M \in \mathbb{Z}^{n \times m}$  eine ganzzahlige Matrix. Dann gibt es unimodulare Matrizen  $S \in \text{GL}_n(\mathbb{Z})$ ,  $T \in \text{GL}_m(\mathbb{Z})$ , sodass

$$S^{-1}MT = \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}, \quad D = \text{diag}(e_1, \dots, e_r), \quad e_1 \mid e_2 \mid \dots \mid e_r \neq 0.$$

Die Nullen hier stehen für Nullmatrizen der jeweils passenden Größe.

*Beweis:* Wir betrachten die Abbildung  $\Phi : \mathbb{Z}^m \rightarrow \mathbb{Z}^n$ , die durch Multiplikation mit  $M$  gegeben ist. Ihr Bild ist eine Untergruppe  $U \subseteq \mathbb{Z}^n$ , und hier gibt es also eine Basis  $\{b_1, \dots, b_r\} \in \mathbb{Z}^n$  sowie die zugehörigen Elementarteiler  $e_1 \mid e_2 \mid \dots \mid e_r$ , sodass  $e_i b_i, 1 \leq i \leq r$ , eine Basis von  $U$  ist. Wir schreiben diese Basisvektoren in dieser Reihenfolge in eine Matrix  $S$ , welche dann natürlich unimodular ist.

Wir wählen Elemente  $v_i \in \mathbb{Z}^m$  mit  $A \cdot v_i = e_i b_i, 1 \leq i \leq r$ . Da die Bilder dieser Elemente eine Basis von  $U$  sind, gilt – analog wie wir das schon für Linearformen zweimal benutzt haben –

$$\mathbb{Z}^m = \mathbb{Z}v_1 + \dots + \mathbb{Z}v_r + \text{Kern}(\Phi).$$

Weiter sind  $v_1, \dots, v_r$  linear unabhängig, und nur ihre triviale Linearkombination liegt im Kern von  $\Phi$ . Wenn wir nun noch eine Basis  $\{v_{r+1}, \dots, v_m\}$  vom Kern von  $\Phi$  wählen, dann ist  $T = (v_1 \ v_2 \ \dots \ v_m)$  unimodular und es gilt

$$MT = (e_1 b_1 \ e_2 b_2 \ \dots \ e_r b_r \ 0 \ 0 \ \dots \ 0) = SE,$$

wobei  $E$  die Elementarteilermatrix aus der Behauptung ist. ○

### Bemerkung 1.5.10 Lineare Gleichungssysteme

Dieser Satz hat für die Theorie der Linearen Gleichungssysteme über  $\mathbb{Z}$  eine ähnliche Bedeutung wie die Gauß-Normalform im Fall von Körpern.

Will man  $Mx = b$  lösen, so löst man stattdessen

$$S^{-1}MTy = S^{-1}b,$$

und rechnet diesen Lösungsraum zurück mithilfe  $T^{-1}$ . Dabei ist  $S^{-1}MTy = S^{-1}b$  genau dann ganzzahlig lösbar, wenn für die Einträge von  $S^{-1}b = (\beta_1, \dots, \beta_n)^\top$  gilt, dass  $\beta_i = 0$  für  $i \geq r + 1$  und  $e_i \mid \beta_i$  für  $1 \leq i \leq r$ .

Für ganzzahlige Lineare Gleichungssysteme weiß man also ganz gut Bescheid, was die Lösungstheorie angeht.

### Beispiel 1.5.11 Mal eines mit Zahlen

Was sind die Elementarteiler der Matrix

$$M := \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}?$$

Klar, der Rang ist 2 und das Bild der Multiplikation mit  $M$  wird von den ersten beiden Spalten erzeugt. Die erste hat Inhalt 1 und taugt von daher als erster Basisvektor  $b_1$ , und  $e_1 = 1$ . Nun muss der zweite Erzeuger so abgeändert werden, wie es Satz 1.5.7 verlangt, das heißt, wir müssen erst eine Spalte  $w \in \mathbb{Z}^3$  finden

mit  $w^\top \cdot b_1 = 1$ . Hier können wir zum Beispiel den ersten Standardbasisvektor benutzen. Wir müssen dann die zweite Spalte  $s_2$  von  $M$  so um ein Vielfaches von  $c_1 := b_1$  abändern, dass der neu erhaltene Vektor mit  $w^\top$  Produkt 0 hat. Konkret:

$$c_2 := s_2 - (w^\top \cdot s_2) \cdot c_1 = (0 \ -3 \ -6)^\top.$$

Dann setzen wir

$$b_2 := \begin{pmatrix} 0 \\ -1 \\ -2 \end{pmatrix}$$

und erhalten  $e_2 = 3$ . Wir ergänzen  $b_1, b_2$  durch  $b_3 := (0 \ 0 \ 1)^\top$  zu einer Basis von  $\mathbb{Z}^3$ . Andererseits ist  $c_1 = M \cdot (1 \ 0 \ 0)^\top$  und  $c_2 = M \cdot (-2 \ 1 \ 0)^\top$ , und der Kern der Multiplikation mit  $M$  wird von  $(1 \ -2 \ 1)^\top$  erzeugt, womit wir die drei Spalten der anderen unimodularen Matrix erhalten. Wir sehen:

$$M \cdot \begin{pmatrix} 1 & -2 & 1 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 4 & -1 & 0 \\ 7 & -2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

### Bemerkung 1.5.12 Nichtlinear?

Wir wissen nun, wie man lineare Gleichungssysteme über  $\mathbb{Z}$  recht übersichtlich lösen kann.

Nun seien allgemeiner  $P_1, \dots, P_m \in \mathbb{Z}[X_1, \dots, X_n]$  Polynome. Dann ist man interessiert an der Menge der ganzzahligen Lösungen des Gleichungssystems

$$P_i(x_1, \dots, x_n) = 0, \quad 1 \leq i \leq m.$$

Solch ein System ganzzahliger Polynomgleichung heißt eine *Diophantische*<sup>28</sup> Gleichung. Im Allgemeinen ist es sehr schwer, sinnvolle Aussagen über die Struktur des Lösungsraums eines solchen Gleichungssystems zu machen.

Man ist an verschiedenen Fragen interessiert:

- Gibt es überhaupt eine Lösung?
- Gibt es unendlich viele ganzzahlige Lösungen?
- Wie viele ganzzahlige Lösungen  $(x_i)$  mit  $\max\{|x_i| \mid 1 \leq i \leq n\} \leq N$  gibt es?
- Lässt sich die letzte Frage wenigstens asymptotisch in den Griff bekommen?

<sup>28</sup>Diophantos von Alexandria, ca. 250

Natürlich kann es keine ganzzahlige Lösung geben, wenn es nicht einmal eine reelle gibt. Das lässt sich bisweilen mit Methoden der Analysis ausschließen. Zum Beispiel hat die Gleichung

$$x^2 + y^2 = -5$$

keine Lösung in  $\mathbb{Z}^2$ .

Aber nicht immer, wenn es eine reelle Lösung gibt, muss es eine ganzzahlige geben. Man denke etwa an die Gleichung  $x^2 + y^2 = 3$ .

Es gibt neben dem Körper der reellen Zahlen noch eine Reihe weiterer Körper, die *p*-*adischen Zahlen* (wobei *p* die Primzahlen durchläuft), die oftmals auch benutzt werden können, um die Existenz einer rationalen Lösung von Polynomgleichungen auszuschließen.

Ein erster Schritt in deren Richtung ist das Rechnen mit Kongruenzen, dem wir uns in Bälde widmen werden.

### Bemerkung 1.5.13 Schinzels Hypothese

Ein prominentes Beispiel für die Verquickung von Diophantischen Problemen und Fragen nach der Verteilung der Primzahlen ist *Schinzels*<sup>29</sup> *Hypothese*. Sie sagt folgendes aus:

Sind  $P_1, \dots, P_m \in \mathbb{Z}[X]$  (nichtkonstante) irreduzible Polynome in einer Variablen mit positiven Leitkoeffizienten, sodass keine Primzahl *p* alle Werte

$$P_1(k) \cdot \dots \cdot P_m(k), \quad k \in \mathbb{Z}$$

teilt, dann gibt es unendliche viele  $k \in \mathbb{Z}$ , sodass alle Werte

$$P_1(k), \dots, P_m(k)$$

Primzahlen sind.

Im allgemeinen ist hier nichts affirmatives bekannt, was den Charakter der Vermutung dieser Aussage unterstreicht.

Zum Beispiel die Primzahlzwillingsvermutung ist ein Spezialfall hiervon. Oder auch (für  $m = 1$ ) die bisher unbewiesene Vermutung, es gebe unendlich viele Primzahlen der Form  $k^2 + 1$ .

Der populärste Fall, in dem man weiß, dass Schinzels Hypothese zutrifft, ist der eines Polynoms der Gestalt  $aX + b$  für teilerfremde ganze Zahlen  $a, b, a > 0$ . Dann ist Schinzels Hypothese gerade die Aussage, die laut Dirichlets Primzahlsatz zutrifft: es gibt unendlich viele Primzahlen, die bei Division durch *a* Rest *b* lassen.

Es gibt auch eine genau quantifizierte Version von Schinzels Vermutung.

---

<sup>29</sup>Andrzej Schinzel, geb. 1935

**Beispiel 1.5.14 Pythagoräische<sup>30</sup> Tripel**

Ein *pythagoräisches Tripel* ist ein von  $(0,0,0)$  verschiedenes Tripel  $(a, b, c) \in \mathbb{Z}^3$  mit

$$a^2 + b^2 = c^2.$$

Da die Vorzeichen von  $a, b, c$  keine Rolle spielen, können wir auch nach  $a, b, c \in \mathbb{N}_0$  suchen. Da mit  $(a, b, c)$  auch  $(a/g, b/g, c/g)$  ein pythagoräisches Tripel ist, wenn  $g = \text{ggT}(a, b, c)$  gilt, dürfen wir  $a, b, c$  als teilerfremd voraussetzen, sogar als paarweise teilerfremd, denn ein gemeinsamer Primteiler von zwei beteiligten Zahlen müsste auch die dritte teilen.

Wenn  $a, b$  beide ungerade sind, dann lässt  $a^2 + b^2$  bei Division durch 4 Rest 2. Das geht also nicht, denn ein gerades Quadrat ist immer durch 4 teilbar. Wir dürfen annehmen, dass  $a$  ungerade und  $b$  gerade ist.

Die pythagoräischen Tripel entsprechen via

$$(a, b, c) \mapsto (a/c, b/c)$$

den rationalen Punkten auf dem Einheitskreis. Diese lassen sich – ausgehend vom Punkt  $(1, 0)$  als (der zweite der) Schnittpunkte von Geraden

$$y = m(x - 1), \quad m \in \mathbb{Q},$$

mit dem Kreis schreiben. Wenn man  $m = \frac{z}{n}$  mit teilerfremden  $z, n$  schreibt und alles ausrechnet, was zu rechnen ist, kommt man auf die folgende Gestalt von pythagoräischen Tripeln:

Entweder  $zn$  ist gerade, dann ist

$$a = z^2 - n^2, b = 2zn, c = z^2 + n^2.$$

Oder  $zn$  ist ungerade, dann ist die teilerfremde Lösung  $(a, b, c)$  gegeben durch

$$a = (z^2 - n^2)/2, b = zn, c = (z^2 + n^2)/2.$$

Aber nun ist  $a$  gerade und  $b$  ungerade, also haben die beiden nur die Rollen getauscht.

Jedes primitive pythagoräische Tripel mit ungeradem  $a$  ist von der ersten Gestalt, wobei  $n < z$  teilerfremde natürliche Zahlen sind, eine davon gerade, die andere ungerade.

Beispiele:  $(3, 4, 5)$ ,  $(5, 12, 13)$ ,  $(7, 24, 25)$  sind pythagoräische Tripel.

---

<sup>30</sup>Pythagoras von Samos, ca. 580 -500 v.Chr.

# Kapitel 2

## Kongruenzrechnung

### 2.1 Die Restklassenringe

#### Definition 2.1.1 Kongruenz

Es seien  $A$  eine abelsche Gruppe und  $U \subseteq A$  eine Untergruppe.

Dann heißen  $a, b \in A$  *kongruent modulo*  $U$ , falls  $a - b \in U$ .

In Zeichen:  $a \equiv b \pmod{U}$ .

Dies ist eine Äquivalenzrelation. Die Äquivalenzklasse von  $a \in A$  wird mit  $a + U$  notiert. Die Menge aller Äquivalenzklassen notieren wir als  $A/U$ .

#### Bemerkung 2.1.2 Addition von Restklassen

a) Wenn  $A$  eine abelsche Gruppe ist und  $U \subseteq A$  eine Untergruppe, dann gilt für  $a, b, c, d \in A$  mit  $a - c, b - d \in U$  :

$$(a + b) - (c + d) \in U.$$

Daher ist durch

$$(a + U) + (b + U) := (a + b) + U$$

eine wohldefinierte Verknüpfung auf  $A/U$  gegeben. Sie ist assoziativ und kommutativ (weil das für die Vertreter der Restklassen schon gilt), und  $0 + U$  ist ein neutrales Element. Da  $(-a) + U$  zu  $a + U$  invers ist, ist insgesamt  $A/U$  eine Gruppe – die *Restklassengruppe* oder auch *Faktorgruppe* von  $A$  modulo  $U$ .

b) Im Gegensatz zur linearen Algebra, wo ein Faktorraum eines Vektorraums immer zu einem Unterraum des Ausgangsraumes isomorph ist, wird  $A/U$  im Allgemeinen nicht zu einer Untergruppe von  $A$  isomorph sein – man kann also durch Quotientenbildung ganz neue Gruppen konstruieren.

c) Wie in der linearen Algebra für Vektorräume, so gilt auch hier die folgende Aussage: Wenn  $A, B$  zwei (abelsche) Gruppen sind und  $\Phi : A \rightarrow B$  ein Homomorphismus, dann induziert  $\Phi$  einen Isomorphismus zwischen  $A/\text{Kern}(\Phi)$  und  $\text{Bild}(\Phi)$ . Dieser kommt durch

$$\tilde{\Phi}(a + \text{Kern}(\Phi)) := \Phi(a)$$

zustande.

Diese Aussage heißt der *Homomorphiesatz*.

### Beispiel 2.1.3 $\mathbb{Z}/N\mathbb{Z}$

Für  $N \in \mathbb{N}$  ist die Gruppe  $\mathbb{Z}/N\mathbb{Z}$  eine endliche Gruppe mit  $N$  Elementen, denn zwei ganze Zahlen sind genau dann modulo  $N\mathbb{Z}$  äquivalent, wenn sie bei Division durch  $N$  denselben Rest in  $\{0, 1, \dots, N-1\}$  lassen. Diese  $N$  Zahlen nimmt man gerne als Vertreter der Restklassen.

Für  $N > 1$  ist diese Gruppe nicht zu einer Untergruppe von  $\mathbb{Z}$  isomorph, denn  $\mathbb{Z}$  hat keine endlichen Untergruppen  $\neq \{0\}$ .

### Definition 2.1.4 Index, Erzeugnis

- Sind  $U \subseteq A$  abelsche Gruppen, so heißt die Kardinalität von  $A/U$  der *Index* von  $U$  in  $A$ . Wir schreiben dafür auch  $(A : U)$ .
- $U$  ist das *Erzeugnis* von  $S \subseteq U$ , wenn jedes Element von  $U$  eine ganzzahlige Linearkombination von Elementen aus  $S$  ist.
- $U$  heißt *endlich erzeugt*, wenn es ein endliches Erzeugendensystem gibt.  
Dies ist genau dann der Fall, wenn es ein  $n \in \mathbb{N}$  und einen surjektiven Gruppenhomomorphismus  $\Phi : \mathbb{Z}^n \rightarrow U$  gibt.
- Die Gruppe  $U$  heißt *zyklisch*, wenn sie von einem einzigen Element erzeugt wird.

Das sind genau die Gruppen, die zu einer Gruppe  $\mathbb{Z}/N\mathbb{Z}$  mit  $N \in \mathbb{N}_0$  isomorph sind.

- Wenn ein Element  $a \in A$  eine endliche Untergruppe von  $A$  erzeugt, so heißt die Kardinalität dieser Untergruppe auch die *Ordnung* von  $a$ . Dies ist dann die kleinste natürliche Zahl  $d$  mit  $da = 0$  (bzw.  $a^d = 1$  in multiplikativer Notation). Ansonsten sagt man,  $a$  habe unendliche Ordnung.

Für jedes  $a \in A$  haben wir einen Gruppenhomomorphismus

$$\Phi : \mathbb{Z} \rightarrow A, \Phi(k) := ka.$$

Das Bild von  $\Phi$  ist gerade die von  $a$  erzeugte Untergruppe, und nach dem Homomorphiesatz ist sie zu  $\mathbb{Z}/\text{Kern}(\Phi)$  isomorph. Der Kern von  $\Phi$  ist entweder  $\{0\}$  oder von der Gestalt  $N\mathbb{Z}$  mit einem  $N \in \mathbb{N}$ . Dieses  $N$  ist (im zweiten Fall) die Ordnung von  $a$ .

### Hilfssatz 2.1.5 Elementarteiler

Es sei  $F$  eine frei abelsche Gruppe von Rang  $n$  und  $U \subseteq F$  eine Untergruppe von endlichem Index.

Dann hat  $U$  Rang  $n$  und  $(F : U)$  ist das Produkt der Elementarteiler von  $U$  in  $F$ .

*Beweis.* Es seien  $r$  der Rang von  $U$ ,  $e_1, \dots, e_r$  die Elementarteiler von  $U$  in  $F$  und  $b_1, \dots, b_n$  eine geeignete Basis von  $F$ , sodass  $c_i := e_i b_i$  ( $1 \leq i \leq r$ ) eine Basis von  $U$  ist.

Wenn  $r$  kleiner als  $n$  wäre, dann wären die Elemente  $mb_n$ ,  $m \in \mathbb{Z}$ , paarweise nicht kongruent modulo  $U$  und damit hätte  $U$  unendlichen Index. Das kann nicht sein. Also gilt  $r = n$ .

Dann lässt sich aber jedes Element  $f \in F$  durch Subtraktion einer ganzzahligen Linearkombination von  $c_1, \dots, c_n$  zu einer Linearkombination

$$\sum_{i=1}^n \lambda_i b_i, \quad 0 \leq \lambda_i \leq e_i - 1,$$

abändern, und man sieht leicht, dass diese  $e_1 \cdot e_2 \cdot \dots \cdot e_n$  Elemente ein Vertretersystem der Restklassen bilden. Das impliziert dann die Behauptung.  $\circ$

### Hilfssatz 2.1.6 Lagrange (für abelsche Gruppen)

a) Es sei  $A$  eine (additiv geschriebene) endliche abelsche Gruppe und  $a \in A$ .  
Dann gilt

$$|A| \cdot a = 0.$$

b) Die Ordnung  $d$  von  $a$  ist ein Teiler von  $|A|$ .

*Beweis.* a) Wir betrachten

$$\sum_{x \in A} x =: s.$$

Da mit  $x$  auch  $x + a$  alle Elemente von  $G$  genau einmal durchläuft, folgt

$$s = \sum_{x \in A} (x + a) = s + |A| \cdot a,$$

und die Aussage folgt durch Kürzen von  $s$ .

b) Aus  $d \cdot a = |A| \cdot a = 0$  folgt natürlich wegen Euklid auch

$$\text{ggT}(d, |A|) \cdot a = 0.$$

○

### Folgerung 2.1.7 kleiner Fermat<sup>1</sup> - abstrakt

Wenn  $F$  ein endlicher Körper mit  $q$  Elementen ist, dann gilt für jedes  $a \in F^\times$ :

$$a^{q-1} = 1.$$

NB: Hier betrachten wir die Einheitengruppe, und daher Produkte statt Summen, und das neutrale Element ist 1.

### Bemerkung 2.1.8 Restklassenringe

Es seien nun  $R$  ein kommutativer Ring,  $I \subseteq R$  ein Ideal. Das ist insbesondere eine Untergruppe von  $R$  bezüglich der Addition, und es gibt die Faktorgruppe  $R/I$ .

Sind nun  $a, b, c, d \in R$  vier Elemente mit  $a - c, b - d \in I$ , dann gilt auch

$$ab - cd = a(b - d) + d(a - c) \in I, \quad \text{also } ab \equiv cd \pmod{I}.$$

Das zeigt, dass auch das Produkt von zwei Äquivalenzklassen in genau einer Äquivalenzklasse enthalten ist. Dies nehmen wir zum Anlass, um auf  $R/I$  die naheliegende Definition

$$(a + I) \cdot (b + I) := (ab) + I$$

zu machen. Man rechnet leicht nach, dass diese Verknüpfung assoziativ und kommutativ ist und  $1 + I$  ein neutrales Element ist. Weiterhin gilt das Distributivgesetz.

Mithin ist  $R/I$  ein kommutativer Ring, der *Restklassenring von  $R$  nach  $I$* .

Auch hier gilt ein Homomorphiesatz: Sind  $R, S$  zwei kommutative Ringe und ist  $\Phi : R \rightarrow S$  ein Ringhomomorphismus, so liefert  $\Phi$  einen Isomorphismus zwischen den Ringen  $R/\text{Kern}(\Phi)$  und  $\text{Bild}(\Phi)$ .

### Hilfssatz 2.1.9 Die Einheitengruppe - kleiner Fermat konkret

a) Es seien  $R$  ein kommutativer Ring und  $I \subseteq R$ . Dann ist  $r + I$  genau dann eine Einheit in  $R/I$ , wenn es ein  $s \in R$  gibt mit  $rs - 1 \in I$ .

---

<sup>1</sup>Pierre de Fermat, 1601-1665

b) Ist  $R$  ein Hauptidealring und  $I = Rm, m \in R$ , dann ist für  $r \in R$  die Restklasse  $r + I$  genau dann in  $R/I$  invertierbar, wenn  $r$  und  $m$  teilerfremd sind.

c) Ist  $R$  ein Hauptidealring und  $I = Rm, m \in R$ , dann ist  $R/I$  genau dann ein Körper, wenn  $m$  irreduzibel ist.

d) Für  $N \in \mathbb{N}$  ist

$$(\mathbb{Z}/N\mathbb{Z})^\times = \{r + N\mathbb{Z} \mid 0 \leq r \leq N - 1, \text{ggT}(r, N) = 1\}.$$

$\mathbb{Z}/N\mathbb{Z}$  ist genau dann ein Körper, wenn  $N$  eine Primzahl ist.

e) Ist  $p \in \mathbb{P}$ , so gilt für alle  $a \in \mathbb{Z}$ :  $p \mid a^p - a$ .

*Beweis.* a) Wenn es so ein  $s$  gibt, dann ist definitionsgemäß  $(r+I) \cdot (s+I) = 1+I$ , und  $r+I$  ist invertierbar.

Umgekehrt muss es im Falle, dass  $r+I$  invertierbar ist, ein  $s \in R$  geben, sodass 1 ein Vertreter von  $(r+I) \cdot (s+I)$  ist, aber das heißt gerade  $rs - 1 \in I$ .

b) Das ist gerade die Aussage 1.2.13, weil wir einen Hauptidealring haben: der ggT von  $r$  und  $m$  ist eine Linearkombination von  $r$  und  $m$ , und wenn 1 sich als Linearkombination schreiben lässt, dann ist es ein ggT.

c) Ist  $m$  eine Einheit, dann ist  $R/Rm = \{0 + Rm\}$ , also kein Körper, denn dieser muss laut Definition mindestens zwei Elemente enthalten.

Ist  $m$  keine Einheit aber nicht irreduzibel, dann lässt es sich in zwei Faktoren zerlegen:  $m = ab$ , wobei weder  $a$  noch  $b$  Einheiten sind. Dann sind die Restklassen  $a + Rm, b + Rm$  nicht die Nullklasse, denn sonst wäre  $a$  oder  $b$  auch Vielfaches von  $m$  und damit zu  $m$  assoziiert. Das Produkt  $(a + Rm)(b + Rm)$  hingegen ist Null in  $R/Rm$ , und damit ist  $R/Rm$  nicht nullteilerfrei, also kein Körper.

Ist  $m$  hingegen irreduzibel, dann gilt für  $r \in R \setminus (Rm)$ , dass  $r$  zu  $m$  teilerfremd ist, also nach Euklid  $s, t \in R$  existieren, sodass  $sr + mt = 1$ , also ist  $(s + Rm)$  zu  $(r + Rm)$  invers, und  $r + Rm$  ist eine Einheit.

d) Hier wird einfach alles aus b) und c) in den Spezialfall übertragen, wobei wir ausnutzen, dass  $\{0, 1, \dots, N - 1\}$  alle Restklassen in  $\mathbb{Z}/N\mathbb{Z}$  repräsentiert.

e) ist dann klar, wenn  $p$  kein Teiler von  $a$  ist, denn wegen 2.1.7 ist  $p$  schon ein Teiler von  $a^{p-1} - 1$ . Wenn  $p$  aber ein Teiler von  $a$  ist, dann ist die Aussage erst recht klar.  $\circ$

### Definition 2.1.10 $\mathbb{F}_p$ , Eulers $\varphi$ -Funktion

a) Für eine Primzahl  $p$  schreiben wir anstelle von  $\mathbb{Z}/p\mathbb{Z}$  auch  $\mathbb{F}_p$  oder gar – wie die Informatiker –  $\text{GF}(p)$  (Galois<sup>2</sup>-Feld).

<sup>2</sup>Evariste Galois, 1811-1832

b) Es sei  $N \in \mathbb{N}$ . Die Einheitengruppe  $(\mathbb{Z}/N\mathbb{Z})^\times$  heißt auch die *prime Restklassengruppe modulo  $N$* .

Die durch

$$\varphi(N) := |(\mathbb{Z}/N\mathbb{Z})^\times|$$

definierte Funktion heißt die *Eulersche  $\varphi$ -Funktion*.

Es gilt also

$$\varphi(N) = |\{x \in \mathbb{N} \mid x \leq N, \text{ggT}(x, N) = 1\}|.$$

Zum Beispiel ist für eine Primzahl  $p$  nach dem letzten Hilfssatz  $\varphi(p) = p - 1$ , während für Potenzen  $p^e$  (mit  $e \geq 1$ ) von  $p$  gilt, dass

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

Man sieht schnell, dass  $\varphi(N)$  genau die Anzahl der Elemente von Ordnung  $N$  in  $\mathbb{Z}/N\mathbb{Z}$  ist.

### Bemerkung 2.1.11 Primzahltest

Aus dem kleinen Satz von Fermat (siehe 2.1.7, 2.1.9) leitet sich auch ein Kriterium dafür her, dass eine gegebene Zahl  $n$  *keine Primzahl* ist. Wenn nämlich  $n$  gegeben ist und für eine Zahl  $a \in \mathbb{Z}$ , die zu  $n$  teilerfremd ist, die Kongruenz

$$a^{n-1} \equiv 1 \pmod{n}$$

nicht erfüllt ist, dann ist  $n$  sicher keine Primzahl.

Die Umkehr stimmt im allgemeinen nicht. Es könnte für eine Zahl  $a$  diese Kongruenz erfüllt sein (zum Beispiel für  $a = 1$ ), ohne dass  $n$  eine Primzahl ist. Zum Beispiel ist 341 eine solche *Pseudoprimzahl zur Basis 2*.

Selbst wenn die Kongruenz für alle  $1 \leq a \leq n$  mit  $\text{ggT}(a, n) = 1$  erfüllt ist, muss  $n$  immer noch keine Primzahl sein. Die Zahl  $n$  heißt dann eine *Carmichael<sup>3</sup>-Zahl*. Es gibt unendlich viele Carmichael-Zahlen, die Folge startet mit 561, 1105, 1729, 2465. . .

### Hilfssatz 2.1.12 Chinesischer Restsatz

*Es seien  $N, M$  zwei teilerfremde natürliche Zahlen. Dann gelten die folgenden Aussagen*

- a) *Die Ringe  $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$  (mit komponentenweiser Addition und Multiplikation) und  $\mathbb{Z}/(MN\mathbb{Z})$  sind isomorph.*

---

<sup>3</sup>Robert Daniel Carmichael, 1879 - 1967

b) Für je zwei Zahlen  $a, b \in \mathbb{Z}$  gibt es eine ganze Zahl  $x$ , sodass simultan

$$x \equiv a \pmod{M} \quad \text{und} \quad x \equiv b \pmod{N}$$

gilt. Zwei Lösungen  $x$  und  $\tilde{x}$  dieser Kongruenzbedingung sind kongruent modulo  $MN$ .

*Beweis.* a) Beide Ringe bestehen aus  $MN$  Elementen. Der Ring  $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$  hat hierbei genau die Elemente

$$(a + M\mathbb{Z}, b + N\mathbb{Z}), \quad 0 \leq a \leq M - 1, \quad 0 \leq b \leq N - 1.$$

Wir betrachten die Abbildung

$$\Phi : \mathbb{Z}/(MN\mathbb{Z}) \rightarrow \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}, \quad \Phi(x + MN\mathbb{Z}) := (x + M\mathbb{Z}, x + N\mathbb{Z}).$$

Diese ist natürlich wohldefiniert und ein Ringhomomorphismus. Außerdem ist  $\Phi$  injektiv, denn aus

$$\Phi(x + MN\mathbb{Z}) = \Phi(y + MN\mathbb{Z})$$

folgt, dass sowohl  $M$  als auch  $N$  die Differenz  $x - y$  teilen, also – wegen der Teilerfremdheit von  $M$  und  $N$  – auch  $MN$  ein Teiler von  $x - y$  ist.

Damit muss wegen der übereinstimmenden Kardinalität die Abbildung  $\Phi$  auch surjektiv sein, und damit ist  $\Phi$  ein Isomorphismus.

b) Folgt sofort aus dem Beweis von a). ○

### Folgerung 2.1.13 $\varphi$ ist multiplikativ

a) Die Eulersche  $\varphi$ -Funktion ist multiplikativ.

b) Für zwei Primzahlen  $p \neq q$  und  $k \in \mathbb{N}$  gilt

$$\forall a \in \mathbb{Z} : a^{k(p-1)(q-1)+1} \equiv a \pmod{pq}.$$

Wegen der Multiplikativität von  $\varphi$  gilt ja  $\varphi(pq) = (p-1)(q-1)$ .

### Bemerkung 2.1.14 RSA

Die letzte Folgerung ist für die Funktionsweise des klassischen RSA-Verfahrens entscheidend. Wenn  $e$  eine zu  $(p-1)(q-1)$  teilerfremde Zahl ist, dann lässt sich mit Euklid die Zahl 1 als  $re - k(p-1)(q-1)$  schreiben, und es folgt

$$a \equiv a^{re} \pmod{pq}.$$

Also lässt sich  $a$  aus  $a^e$  modulo  $pq$  rekonstruieren, wenn man  $p$  und  $q$  – und nicht nur deren Produkt – kennt.

**Bemerkung 2.1.15 Euklid und die Surjektivität**

a) Ein anderes Argument für die Surjektivität im Beweis des Chinesischen Restsatzes geht so: Es sei  $1 = kM + lN$  für ganze Zahlen  $k, l$ . Dann ist die Zahl  $x = bkM + alN$  modulo  $M$  gleich  $a$  und modulo  $N$  gleich  $b$ .

Dieses Argument benutzt nicht wirklich die endliche Kardinalität der beteiligten Ringe und lässt sich daher besser verallgemeinern.

b) Die allgemeinere Aussage sieht so aus: Es seien  $R$  ein kommutativer Ring und  $I, J \subseteq R$  zwei Ideale, sodass es  $\kappa \in I, \lambda \in J$  gibt mit  $\kappa + \lambda = 1$ .

Dann gibt es einen Isomorphismus zwischen den Ringen

$$R/(I \cap J) \quad \text{und} \quad R/I \times R/J.$$

Dieser Isomorphismus wird genauso hingeschrieben wie oben, und die Surjektivität folgt in Analogie zu dem eben mit Euklid gemachten Argument.

Im Fall  $R = \mathbb{Z}, M, N \in \mathbb{N}$  teilerfremd, ist

$$\mathbb{Z}M \cap \mathbb{Z}N = \mathbb{Z}MN,$$

denn das ist das Ideal, das aus allen gemeinsamen Vielfachen besteht.

**Bemerkung 2.1.16 Polynominterpolation**

Es seien zum Beispiel  $R = \mathbb{C}[X]$  und  $\xi \in \mathbb{C}$ . Für  $d \in \mathbb{N}$  ist  $R/((X - \xi)^d R)$  ein komplexer Vektorraum der Dimension  $d$ , als Basis bieten sich – denken Sie an Division mit Rest! – die Restklassen von  $1, (X - \xi), \dots, (X - \xi)^{d-1}$  an.

Ein Element von  $R/((X - \xi)^d R)$  lässt sich also durch eine Polynom

$$\sum_{i=0}^{d-1} a_i (X - \xi)^i$$

repräsentieren. Ein Blick auf die Taylorformel sagt uns, dass die Restklasse von  $f \in R$  sich gerade die Werte  $f^{(i)}(\xi) = i! \cdot a_i$ ,  $0 \leq i \leq d - 1$ , merkt.

Der Chinesische Restsatz wiederum liefert dann, dass für  $k$  Zahlen  $\xi_1, \dots, \xi_k \in \mathbb{C}$  und natürliche Zahlen  $d_1, \dots, d_k$  ein Polynom existiert, das bei den Zahlen  $\xi_j$ ,  $1 \leq j \leq k$ , vorgegebene Ableitungen  $f^{(i)}(x_j)$ ,  $0 \leq i \leq d_j - 1$ , besitzt.

Denn: Die Ideale in  $R$ , die von den Potenzen  $(X - \xi_j)^{d_j}$  erzeugt werden, sind paarweise teilerfremd, und für jedes  $\xi_j$  alleine ist das Problem lösbar.

Wenn speziell alle  $d_j = 1$  sind, dann gibt es eine sehr explizite Formel (von Lagrange), mit der sich ein Polynom mit vorgegebenen Funktionswerten  $f(\xi_j) := w_j$  hinschreiben lässt, nämlich

$$f = \sum_{j=1}^k \left( w_j \cdot \prod_{i \neq j} \frac{X - \xi_i}{\xi_j - \xi_i} \right)$$

Sieht man sich die Formel noch einmal genau an, dann erkennt man auch wieder den Beweis des Chinesischen Restsatzes, und insbesondere den Beweis der Surjektivität mithilfe des Euklidischen Algorithmus.

Summa summarum gibt es für den Polynomring über  $\mathbb{C}$  eine schöne „geometrische“ Interpretation des Chinesischen Restsatzes. Solch eine Interpretation ist für die Situation  $R = \mathbb{Z}$  zunächst nicht vorhanden, denn was sollte schon die Ableitung einer ganzen Zahl bei einer Primzahl  $p$  sein?

In gewisser Weise wird das durch Grothendieck<sup>4</sup>s Schematheorie noch weiter vereinheitlicht. Die Punkte des zu  $\mathbb{Z}$  gehörigen Schemas sind gerade die Primzahlen und die 0, und eine rationale Zahl kann man auffassen wie eine Funktion (wohin auch immer sie geht) mit einigen Polstellen. Das wird alles in der algebraischen Geometrie präzisiert, sprengt aber den Rahmen dieses Skripts.

### Beispiel 2.1.17 Jordan<sup>5</sup>sche Normalform

Es seien  $K$  ein Körper und  $A \in K^{n \times n}$  eine Matrix. Weiter sei  $R = K[X]$  der Polynomring. Schließlich sei  $\Psi : R^n \rightarrow K^n$  die  $K$ -lineare Abbildung, die die Identität auf  $K^n$  fortsetzt und darüberhinaus

$$\forall v \in R^n : \Psi(Xv) = A\Psi(v)$$

erfüllt. Dadurch ist  $\Psi$  eindeutig festgelegt.

Der Kern  $U$  von  $\Psi$  ist das Bild von  $XE_n - A$ ; diese Matrix wird auch die *charakteristische Matrix* von  $A$  genannt.

Die Multiplikation mit  $A$  auf  $K^n$  ist dasselbe wie die Multiplikation mit  $X$  auf  $R^n/U$ .

Der Elementarteilersatz für  $R$  erlaubt es nun, eine Basis von  $R^n$  zu finden, sodass  $U$  eine  $R$ -Basis besitzt, die aus Vielfachen der gefundenen Basisvektoren besteht. Das führt dazu, dass  $K^n \simeq R^n/U$  eine direkte Summe von  $A$ -zyklischen Unterräumen der Gestalt  $R/e_jR$  ist, wobei die  $e_j$  normierte Polynome sind und stets  $e_j \mid e_{j+1}$  gilt.

Dabei gilt insbesondere – der Elementarteilersatz braucht ja invertierbare Matrizen mit Einträgen in  $R$ , ändert also die Determinante nur um Einheiten –  $e_1 \cdot \dots \cdot e_n = \det(XE_n - A) = \text{CP}(A, X)$ . Und  $e_n$  ist übrigens das Minimalpolynom...

<sup>4</sup>Alexander Grothendieck, geb. 1928

<sup>5</sup>Camille Marie Ennemond Jordan, 1838 - 1922

Nun darf man noch die einzelnen zyklischen Unterräume studieren. Dabei benutzen wir noch den Chinesischen Restsatz. Er sagt, dass für zwei teilerfremde Polynome  $f$  und  $g$  die Multiplikation mit  $X$  auf  $R/(fgR)$  dasselbe ist wie die Multiplikation mit  $X$  auf  $R/(fR) \times R/(gR)$ , und wir können  $R/(e_jR)$  noch weiter zerlegen.

Wenn speziell das charakteristische Polynom von  $A$  in Linearfaktoren zerfällt, dann gilt auch für jedes  $j$

$$e_j = (X - \lambda_1)^{d_1} \cdot \dots \cdot (X - \lambda_s)^{d_s}$$

mit paarweise verschiedenen  $\lambda_l \in K$  und geeigneten  $d_l \in \mathbb{N}$ , und wir finden

$$R/(e_jR) = R/((X - \lambda_1)^{d_1}R) \times \dots \times R/((X - \lambda_s)^{d_s}R).$$

Die Multiplikation mit  $X$  auf  $R/((X - \lambda)^dR)$  wird bezüglich der  $K$ -Basis, die aus den Restklassen von  $1, (X - \lambda), (X - \lambda)^2, \dots, (X - \lambda)^{d-1}$  besteht, durch das Jordankästchen der Länge  $d$  zum Eigenwert  $\lambda$  beschrieben, und wir erhalten damit aus dem Elementarteilersatz und dem Chinesischen Restsatz den Satz von der Jordanschen Normalform.

Nach diesem Exkurs machen wir wieder ein bisschen Zahlentheorie.

### Beispiel 2.1.18 Faktorringe von $\mathbb{Z}[i]$

$R := \mathbb{Z}[i]$  ist ein Hauptidealring, und wir können die Ergebnisse von 2.1.9 benutzen, um seine Faktorringe genauer zu studieren.

Es sei  $m = a + bi \in R$  ein von Null verschiedenes Element. Der Index von  $Rm$  in  $R$  ist wegen 2.1.5 gerade die Determinante der Multiplikation mit  $m$  auf  $\mathbb{C}$ , also  $\dots N(m) = a^2 + b^2$ .

Daher ist  $R/Rm$  ein Ring mit  $N(m)$  Elementen.

Ist  $m$  irreduzibel, so gibt es nach 1.3.11 zwei Fälle:

- $N(m)$  ist eine Primzahl  $p = 2$  oder  $\equiv 1 \pmod{4}$ : Hier hat  $R/Rm$  genau  $p$  Elemente und stimmt damit mit  $\mathbb{F}_p$  überein.
- $N(m) = p^2$ ,  $p \in \mathbb{P}$ ,  $p \equiv 3 \pmod{4}$ . Hier ist  $m$  assoziiert zu  $p$ , und  $R/Rm$  hat  $p^2$  Elemente, ist also keiner der Körper  $\mathbb{F}_p$ , wir erhalten einen neuen Körper. Er entsteht aus  $\mathbb{F}_p$  auf dieselbe Art, wie  $\mathbb{C}$  aus  $\mathbb{R}$  entsteht: durch Hinzunahme einer Quadratwurzel von  $-1$ . Die Restklasse von  $i$  ist solch eine Quadratwurzel. In  $\mathbb{F}_p$  gibt es noch keine.

Es gibt also zum Beispiel einen Körper mit 49 Elementen. Welche sonst noch?

## 2.2 Endliche Körper

### Bemerkung 2.2.1 Konstruktion einiger endlicher Körper

Es sei  $F$  ein endlicher Körper,  $q = |F|$ . Dann wissen wir schon, dass der Polynomring  $F[X]$  ein Hauptidealring ist. Er ist also nullteilerfrei und jedes Ideal wird von einem Polynom erzeugt, das bis auf Normierung eindeutig ist.

Nun sei  $I = mF[X]$  von einem irreduziblen Polynom  $m$  vom Grad  $d$  erzeugt. Dann sagt 2.1.9, dass der Faktorring  $F[X]/mF[X]$  ein Körper ist.

In diesem Faktorring wird jedes Element von einem Polynom repräsentiert, dessen Grad kleiner ist als  $d$ . Zwei solche Polynome sind modulo  $m$  unterschiedlich. Es folgt  $|F[X]/mF[X]| = q^d$ , und wir erhalten einen neuen endlichen Körper, wenn  $d > 1$ .

Wer Matrizen liebt kann sich auch ein Modell im Ring der  $d \times d$ -Matrizen  $F^{d \times d}$  verschaffen, indem er den kleinsten Teilring betrachtet, der  $F$  und die Begleitmatrix zu  $m$  enthält.

### Hilfssatz 2.2.2 Primkörper, Einheitengruppe

Es sei  $F$  ein endlicher Körper. Dann gelten:

- a) Die Ordnung von  $1_F$  in der additiven Gruppe von  $F$  ist eine Primzahl  $p$ , und  $\mathbb{Z}/p\mathbb{Z}$  ist ein Teilring von  $F$ .
- b) Die Kardinalität von  $F$  ist eine Potenz von  $p$ .
- c) Die Einheitengruppe von  $F$  ist zyklisch.
- d)  $F$  ist ein Restklassenkörper des Polynomrings  $\mathbb{F}_p[X]$ .

*Beweis.* a) Es sei  $\Phi : \mathbb{Z} \rightarrow F$  der Ringhomomorphismus

$$\Phi(k) := k \cdot 1_F.$$

Der Kern von  $\Phi$  ist das von der Ordnung  $d$  von  $1_F$  erzeugte Ideal in  $\mathbb{Z}$ . Natürlich ist  $d$  größer als 1, denn sonst wäre schon  $1_F$  das Nullelement, was in einem Körper ja verboten ist. Wäre  $d$  keine Primzahl, so könnte man es als  $d = ab$  schreiben mit  $1 < a, b < d$ . Dann wären  $a \cdot 1_F$  und  $b \cdot 1_F$  Elemente  $\neq 0$  von  $F$ , deren Produkt 0 ist... naja, das geht halt nicht.

Also ist  $p := d$  eine Primzahl, und  $\Phi$  liefert wegen des Homomorphiesatzes – siehe 2.1.8 – eine Einbettung von  $\mathbb{F}_p$  nach  $F$ .

b) klar:  $F$  ist ja nun ein endlich dimensionaler  $\mathbb{F}_p$ -Vektorraum.

c) Es sei  $\Pi : \mathbb{Z}^r \rightarrow F^\times$  ein surjektiver Gruppenhomomorphismus. So etwas gibt es, da  $F^\times$  endlich und kommutativ ist.

Es sei  $q$  die Kardinalität von  $F$ .

Weiter sei  $U$  der Kern von  $\Pi$ . Dann hat  $U$  in  $\mathbb{Z}^r$  Index  $q - 1$  und wegen 2.1.5 Rang  $r$ . Wir bezeichnen wie gehabt die Elementarteiler mit  $e_1 \mid e_2 \mid \cdots \mid e_r$  und sehen in 2.1.5, dass

$$q - 1 = e_1 \cdot \dots \cdot e_r.$$

Für jedes  $v \in \mathbb{Z}^r$  gilt  $e_r v \in U$ . Daher gilt für jedes  $\zeta \in F^\times$  auch  $\zeta^{e_r} = 1$ , und ganz  $F^\times$  besteht aus Nullstellen von  $X^{e_r} - 1$ . Es folgt  $e_r \geq q - 1$ , und da  $e_r$  auch ein Teiler von  $q - 1$  ist, müssen die beiden Zahlen gleich sein. Insbesondere sind alle anderen Elementarteiler 1, und es folgt mit dem Beweis von 2.1.5, dass

$$F^\times \cong \mathbb{Z}^r / U \cong \mathbb{Z} / e_r \mathbb{Z}.$$

Das ist eine zyklische Gruppe.

d) Es sei  $\zeta \in F^\times$  ein Erzeuger. Die Abbildung

$$\Psi : \mathbb{F}_p[X] \rightarrow F, \Psi(f) := f(\zeta)$$

ist ein Ringhomomorphismus. Weiterhin ist für alle  $e \in \mathbb{Z}$  das Element  $\zeta^e = \Psi(X^e)$  im Bild von  $\Psi$ . Da  $\Psi(0) = 0$  gilt und  $\zeta$  die Gruppe der von 0 verschiedenen Elemente erzeugt, ist  $\Psi$  surjektiv, und wir finden die Behauptung als Konsequenz des Homomorphiesatzes aus 2.1.8.  $\circ$

### Definition 2.2.3 Charakteristik, primitives Element, Minimalpolynom

Die Primzahl  $p$  aus dem letzten Hilfssatz heißt die *Charakteristik von  $F$* . Sie ist durch  $F$  natürlich eindeutig festgelegt. Allgemeiner ist die Charakteristik eines beliebigen Körpers gleich der additiven Ordnung von 1, wenn diese endlich (und damit eine Primzahl) ist, und ansonsten 0. Im ersten Fall liegt  $\mathbb{F}_p$  im Körper, im zweiten Fall  $\mathbb{Z}$  und damit auch dessen Quotientenkörper  $\mathbb{Q}$ .

Ein Element  $\zeta \in F^\times$ , das die Einheitengruppe erzeugt, heißt auch ein *primitives Element* von  $F$ . Die Anzahl der primitiven Elemente von  $F$  ist  $\varphi(q - 1)$ , wobei  $q$  wieder die Kardinalität von  $F$  ist (siehe 2.1.10 b)).

Der normierte Erzeuger  $m$  des Kerns von  $\Phi$  im Beweis heißt das *Minimalpolynom* von  $\zeta$  (über  $\mathbb{F}_p$ ).

Es ist offensichtlich irreduzibel, denn  $\mathbb{F}_p[X]/(m)$  ist ein Körper. Der Hilfssatz und die Bemerkung vorweg legen nahe, nach Kandidaten für irreduzible Polynome über  $\mathbb{F}_p$  zu suchen.

Bevor wir das tun, sammeln wir noch zwei Sachverhalte am Wegesrand mit ein.

**Bemerkung 2.2.4 Artin<sup>6</sup>s Vermutung**

a) Es ist nun klar, woher in 1.3.12 die Bedingung kommt, dass  $p \equiv 1 \pmod{4}$ . Denn genau dann hat ein Erzeuger  $\zeta$  von  $\mathbb{F}_p^\times$  eine durch 4 teilbare Ordnung, und da die Ordnung von  $-1$  genau 2 ist ( $p$  ist ja ungerade), muss es eine Potenz von  $\zeta^2$  sein, also selbst ein Quadrat.

b) Eine noch immer unbewiesene Vermutung von Emil Artin sagt, dass es für jede ganze Zahl  $a \neq -1$ , die keine ganze Quadratwurzel in  $\mathbb{Z}$  hat, unendlich viele Primzahlen  $p$  gibt, sodass  $a + p\mathbb{Z}$  ein primitives Element in  $\mathbb{F}_p$  ist.

Dies ist für keine einzige Zahl  $a$  bewiesen. Schon der Fall  $a = 2$  ist nicht klar.

Zum Beispiel für  $p = 3$  ist  $a = 2$  primitiv, die Potenzen sind  $2^1 = 2$  und  $2^2 = 4$ .

Auch modulo 5 und 11 ist 2 primitiv.

Modulo  $p = 7$  sind die Potenzen von 2 gerade 2, 4 und  $8 = 1$ , d.h. 2 erzeugt nur eine Untergruppe vom Index 2 in  $\mathbb{F}_7^\times$ . Ein Erzeuger von  $\mathbb{F}_7^\times$  ist zum Beispiel (die Restklasse von) 5.

Modulo 17 ist die Ordnung von 2 gleich 8, also ist 2 hier nicht primitiv und (letztes Beispiel) modulo 31 ist die Ordnung von 2 gleich 5, also erzeugt 2 modulo 31 nur eine Gruppe vom Index 6 in  $\mathbb{F}_{31}^\times$ .

Ein Resultat von Heath-Brown<sup>7</sup> sagt unter anderem, dass höchstens zwei Primzahlen als Werte für  $a$  die Artin-Vermutung falsch ist.

**Hilfssatz 2.2.5 Zyklizität die zweite**

a) *Es sei  $p \geq 3$  eine Primzahl und  $m \in \mathbb{N}$  natürlich. Dann ist die Einheitsgruppe von  $R := \mathbb{Z}/p^m\mathbb{Z}$  zyklisch.*

b) *Für  $p = 2$  und  $m \in \mathbb{N}$  ist  $(\mathbb{Z}/2^m\mathbb{Z})^\times$  genau dann zyklisch, wenn  $m = 1$  oder 2. Für  $m \geq 3$  ist die Einheitsgruppe isomorph zu  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{m-2}\mathbb{Z}$ .*

*Beweis.* a) Wir zeigen zunächst, dass in  $R^\times$  ein Element  $\zeta$  der Ordnung  $p - 1$  liegt. Dies gilt, denn es gibt eine ganze Zahl  $a$ , die modulo  $p$  Ordnung  $p - 1$  hat, und damit ist die Ordnung modulo  $p^m$  ein Vielfaches  $l(p - 1)$  von  $p - 1$ , und  $a^l$  hat Ordnung  $p - 1$  in  $R^\times$ .

Nun sei  $\rho$  die Restklasse von  $1 + p$  in  $R^\times$ . Es ist klar, dass die Ordnung ein Teiler von  $p^{m-1}$  ist, denn  $\rho$  liegt im Kern des surjektiven Gruppenhomomorphismus von  $R^\times$  nach  $\mathbb{F}_p^\times$ , der  $a + p^m\mathbb{Z}$  nach  $a + p\mathbb{Z}$  schickt.

Wir behaupten, dass  $\rho$  die Ordnung  $p^{m-1}$  hat.

Für  $m = 1$  bzw. 2 sieht man sofort, dass die Ordnung von  $\rho$  tatsächlich 1 bzw.  $p$  ist.

<sup>6</sup>Emil Artin, 1898 - 1962

<sup>7</sup>David Rodney „Roger“ Heath-Brown, geb. 1952

Nun sei  $m \geq 3$  und die Behauptung für alle kleineren Werte von  $m$  gezeigt. Wir müssen zeigen, dass die Ordnung von  $(1+p)$  modulo  $p^m$  nicht schon  $p^{m-1}$  teilt. Aber  $1+p$  hat modulo  $p^{m-1}$  Ordnung  $p^{m-2}$ , und das heißt unter Ausnutzung der Induktionsvoraussetzung für  $m-2$  insbesondere auch, dass

$$(1+p)^{p^{m-3}} = 1 + kp^{m-2} \quad \text{für ein } k \notin p\mathbb{Z}.$$

Dann ist aber

$$(1+p)^{p^{m-2}} = ((1+p)^{p^{m-3}})^p = 1 + kp^{m-1} + rp^m,$$

wobei der Rest  $rp^m$  alle übrigen Summanden aus der binomischen Formel aufammelt.

Das zeigt die behauptete Ordnung von  $\rho$ .

Da  $R^\times$  abelsch ist und  $\zeta$  und  $\rho$  jeweils eine zyklische Untergruppe der Ordnung  $p-1$  bzw.  $p^{m-1}$  erzeugen, liegt in  $R^\times$  eine Untergruppe, die zu

$$\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{m-1}\mathbb{Z}$$

isomorph ist. Diese Gruppe hat  $(p-1) \cdot p^{m-1}$  Elemente, ist also gleich  $R^\times$ . Nach dem Chinesischen Restsatz ist sie zyklisch, und wir sind fertig.

b) verbleibt als Übung. ○

### Bemerkung 2.2.6 Kreisteilungspolynom

a) Wir behalten die Notation von Hilfssatz 2.2.2 bei.

Wegen des kleinen Satzes von Fermat ist ein Erzeuger  $\zeta$  von  $F^\times$  eine Nullstelle des Polynoms  $X^{q-1} - 1$ . Dies ist auch ein ganzzahliges Polynom, und als solches wollen wir es erst einmal – und dann auch gleich allgemeiner – untersuchen.

b) Es sei also  $N \in \mathbb{N}$  beliebig. Die komplexen Nullstellen von  $F_N = X^N - 1$  sind die Zahlen der Gestalt

$$c_k := \cos\left(\frac{2\pi k}{N}\right) + i \sin\left(\frac{2\pi k}{N}\right), \quad 1 \leq k \leq N.$$

Für  $g = \text{ggT}(k, N)$  ist hierbei  $c_k$  schon eine Nullstelle von  $F_{N/g}$ , was (siehe Partialsummen der geometrischen Reihe) ein Teiler von  $F_N$  ist.

Die Idee ist nun,  $F_N$  zu modifizieren zu

$$\Phi_N := \prod_{k \bmod N}^* (X - c_k),$$

wobei das Produkt (mit Sternchen) nur noch über die zu  $N$  teilerfremden  $k$  läuft.

$\Phi_N$  heißt das  $N$ -te Kreisteilungspolynom, sein Grad ist  $\varphi(N)$ .

c) Man kann nun offensichtlich  $\Phi_N$  auch rekursiv so gewinnen:

$$\begin{aligned}\Phi_1 &= X - 1 \\ \Phi_N &= (X^N - 1) : \left( \prod_{d|N, d < N} \Phi_d \right)\end{aligned}$$

Es ist klar, dass das dieselben komplexen Polynome gibt. Andererseits sieht man hier rekursiv auch, dass die  $\Phi_N$  sogar normierte ganzzahlige Polynome sind, deren konstanter Term gleich  $-1$  ist für  $N = 1$ , und sonst gleich  $1$ .

Die Polynomdivision geht ganzzahlig auf, da der Leitkoeffizient des Nenners  $1$  ist.

d) Beispiel: Für  $p \in \mathbb{P}$  gilt  $\Phi_p = X^{p-1} + X^{p-2} + \dots + X + 1$ .

Weiter haben wir zum Beispiel  $\Phi_4 = X^2 + 1$ ,  $\Phi_6 = X^2 - X + 1$  und so weiter.

e) Ohne Beweis halten wir fest, dass  $\Phi_N$  über  $\mathbb{Q}$  irreduzibel ist.

### Hilfssatz 2.2.7 Nullstellen des Kreisteilungspolynoms

Es sei  $K$  ein Körper, dessen Charakteristik kein Teiler von  $N \in \mathbb{N}$  ist.

Dann sind äquivalent:

- i) In  $K^\times$  liegt ein Element der Ordnung  $N$ .
- ii) In  $K$  gibt es eine Nullstelle des Kreisteilungspolynoms  $\Phi_N$ .

*Beweis.*

i)  $\Rightarrow$  ii) Es sei  $\zeta \in K^\times$  ein Element der Ordnung  $N$ . Dann hat  $X^N - 1$  die  $N$  paarweise verschiedenen Nullstellen  $1, \zeta, \zeta^2, \dots, \zeta^{N-1}$ , und diese verteilen sich brav auf die Faktoren von

$$X^N - 1 = \prod_{d|N} \Phi_d,$$

also bekommt auch  $\Phi_N$  eine Nullstelle ab.

ii)  $\Rightarrow$  i) Nun sei  $\zeta \in K$  eine Nullstelle von  $\Phi_N$ . Das ist keine mehrfache Nullstelle von  $X^N - 1$ , denn aus  $(X - \zeta)^2 \mid (X^N - 1)$  folgt

$$(X - \zeta) \mid \frac{X^N - 1}{X - \zeta} = X^{N-1} + \zeta X^{N-2} + \zeta^2 X^{N-3} + \dots + \zeta^{N-2} X + \zeta^{N-1}.$$

Also wäre  $\zeta$  eine Nullstelle des rechten Ausdrucks, der bei Einsetzen von  $\zeta$  aber gerade  $N\zeta^{N-1}$  liefert. Da  $\zeta$  nicht  $0$  ist, folgt  $N\zeta^{N-1} \neq 0$ , da die Charakteristik von  $K$  kein Teiler von  $N$  ist.

Da für jeden echten Teiler  $d$  von  $N$  das Produkt  $\Phi_N \cdot (X^d - 1)$  ein Teiler von  $X^N - 1$  ist, haben die zwei Faktoren keine gemeinsame Nullstelle, und deshalb ist die Ordnung von  $\zeta$  größer als  $d$ . Sie muss also  $N$  sein.  $\circ$

**Folgerung 2.2.8 Spezialfall von Dirichlets Primzahlsatz**

*Es sei  $N \in \mathbb{N}$  beliebig.*

*Dann gibt es unendlich viele Primzahlen  $p \equiv 1 \pmod{N}$ .*

*Beweis.* Ohne Einschränkung sei  $N > 1$ .

Es seien  $p_1, \dots, p_k$  irgendwelche Primzahlen. Für  $e \in \mathbb{N}$  sei  $M = (N + e)!$

Das  $N$ -te Kreisteilungspolynom  $\Phi_N$  ist normiert, ganzzahlig, nichtkonstant und hat konstanten Term 1. Daher ist für großes  $e$  die natürliche Zahl

$$L := \Phi_N(M)$$

größer als 1 und zu  $M$  teilerfremd (nämlich kongruent zu 1 modulo  $M$ ).

Es sei  $p$  ein Primteiler von  $L$ . Dann ist  $N$  kein Vielfaches von  $p$ , und die Restklasse von  $M$  modulo  $p$  ist eine Nullstelle von  $\Phi_N$  in  $\mathbb{F}_p$ . Nach dem letzten Hilfssatz hat diese Restklasse Ordnung  $N$  in  $\mathbb{F}_p^\times$ . Wegen des Satzes von Lagrange (vgl. 2.1.6) ist also  $p - 1$  ein Vielfaches von  $N$ , was nichts anderes heißt als

$$p \equiv 1 \pmod{N}.$$

Außerdem ist  $p$  natürlich größer als  $N + e$ , und da dies für alle großen  $e$  geht, folgt die Behauptung.  $\circ$

In 2.2.2 haben wir gesehen, dass die Kardinalität eines endlichen Körpers immer Potenz einer Primzahl ist. Nun gehen wir den umgekehrten Weg und zeigen:

**Hilfssatz 2.2.9 Alle endlichen Körper**

*Es sei  $p$  eine Primzahl und  $e \in \mathbb{N}$ . Dann gibt es einen Körper mit  $p^e$  Elementen und je zwei solche Körper sind zueinander isomorph.*

*Beweis.* Es sei  $q = p^e$  und  $N = q - 1$ . Dann zerlegen wir das Kreisteilungspolynom  $\Phi_N$  in  $\mathbb{F}_p[X]$  in irreduzible Faktoren und wählen einen davon. Er heiße  $m$  und habe Grad  $d$ .

Dann ist  $F := \mathbb{F}_p[X]/(m\mathbb{F}_p[X])$  ein Körper, der  $p^d$  Elemente enthält. Außerdem liegt in  $F$  eine primitive  $N$ -te Einheitswurzel, das heißt  $q \mid p^d$ .

Außerdem gilt für die Restklasse von  $X$  in  $F$ , dass  $X^{q-1} = 1$ , also  $X^q = X$ . Da  $F$  von  $\mathbb{F}_p$  und  $X$  als Körper erzeugt wird, folgt aus den binomischen Formeln, und weil in  $F$  die Gleichung  $p = 0$  gilt, dass alle Elemente  $a \in F$  die Gleichung

$$a^q = a$$

erfüllen.

Demnach besteht  $F$  aus höchstens  $q$  Elementen (Nullstellen eines Polynoms vom Grad  $q$  in einem Körper!), was insgesamt  $|F| = q$  zeigt.

Wenn  $\tilde{F}$  ein weiterer Körper mit  $q$  Elementen ist, dann findet sich in ihm auch eine Nullstelle von  $\Phi_N$ , denn die Einheitengruppe ist zyklisch und besteht aus  $N$  Elementen. Es folgt dann, dass  $\Phi_N$  über  $\tilde{F}$  in Linearfaktoren zerfällt, also auch unser alter Faktor  $m$  eine Nullstelle in  $\tilde{F}$  besitzt. Das Argument aus 2.2.2 d) zeigt dann, dass  $\tilde{F}$  zu  $F$  isomorph ist.  $\circ$

### Bemerkung 2.2.10 Noch mehr Galoisfelder

Der eindeutig bestimmte Körper mit  $q = p^e$  Elementen wird oft als  $\mathbb{F}_q$  notiert, von Informatikern auch gerne als  $GF(q)$ .

Wenn  $\zeta \in \mathbb{F}_q$  ein Element ist und  $m$  sein Minimalpolynom über  $\mathbb{F}_p$ , dann zerfällt  $m$  über  $\mathbb{F}_q$  in paarweise verschiedene Linearfaktoren, denn  $m$  teilt  $X^q - X$ , und dies zerfällt auch.

Die Nullstellen von  $m$  sind genau  $\zeta, \zeta^p, \zeta^{p^2}, \dots, \zeta^{p^{d-1}}$ , wenn  $d$  der Grad von  $m$  ist.

Der Automorphismus Frob von  $\mathbb{F}_q$ , der durch  $\text{Frob}(x) := x^p$  gegeben ist, heißt der *Frobenius<sup>8</sup> automorphismus* von  $\mathbb{F}_q$ . Jeder Automorphismus ist eine Potenz von diesem. Ist  $f \in \mathbb{F}_p[X]$  ein Polynom und  $a \in \mathbb{F}_q$  eine Nullstelle von  $f$ , so ist auch  $a^p = \text{Frob}(a)$  eine Nullstelle von  $f$ . (Das ist ein Pendant zur Tatsache, dass mit jeder komplexen Nullstelle eines reellen Polynoms auch die komplex konjugierte Zahl eine Nullstelle ist.) Es gilt sogar, dass ein irreduzibles normiertes Polynom  $f \in \mathbb{F}_p[X]$  vom Grad  $d$  immer von der Gestalt

$$(X - \alpha) \cdot (X - \alpha^p) \cdot \dots \cdot (X - \alpha^{p^{d-1}})$$

ist, wobei  $\alpha$  irgendeine Nullstelle von  $f$  in  $\mathbb{F}_{p^d}$  bezeichnet. Dass die entsprechenden Potenzen von  $\alpha$  auch Nullstellen sind, wurde gerade gesagt, weiter ist  $\alpha^{p^d} = \alpha$ , da  $\alpha \in \mathbb{F}_{p^d}$  gilt, und die aufgeschriebenen Potenzen sind paarweise verschieden, denn aus  $\alpha^{p^a} = \alpha^{p^b}$ ,  $0 \leq a < b \leq d-1$ , folgt

$$(\alpha^{p^a})^{p^{b-a}} = \alpha^{p^a},$$

also  $\alpha^{p^a} \in \mathbb{F}_{p^{b-a}}$ , aber das Minimalpolynom von  $\alpha^{p^a}$  ist ja  $f$  und hat Grad  $d$ , was einen Widerspruch liefert.

Jeder Teilkörper von  $\mathbb{F}_q$  ist wegen 2.1.7 ein Fixkörper einer Potenz von Frob, und auf diese Art entsprechen die Teilkörper bijektiv den Untergruppen der Automorphismengruppe von  $\mathbb{F}_q$ . Das ist ein Spezialfall des Hauptsatzes der Galoistheorie, den man in der Algebra kennen lernt.

Insbesondere liegt  $\mathbb{F}_{p^e}$  genau dann in  $\mathbb{F}_{p^d}$ , wenn  $e$  ein Teiler von  $d$  ist.

<sup>8</sup>Georg Ferdinand Frobenius, 1849 - 1917

**Bemerkung 2.2.11 Noch ein Primzahlsatz**

Es sei  $p$  eine Primzahl. Für jedes  $d \in \mathbb{N}$  gibt es nur endlich viele normierte irreduzible Polynome vom Grad  $d$  in  $\mathbb{F}_p[X]$ .

Wie viele?

Es sei  $N_d$  ihre Anzahl.

Für  $d = 1$  gilt  $N_1 = p$ , denn die Polynome sind  $X - a$ ,  $a \in \mathbb{F}_p$ .

Für  $d = 2$  gilt  $N_2 = \frac{p^2-p}{2}$ , denn hier sind die gesuchten Polynome gerade die Minimalpolynome der Elemente  $a \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ , also von der Gestalt  $(X - a)(X - a^p)$ .

Analog ist  $N_3 = \frac{p^3-p}{3}$ .

Hingegen findet sich  $N_4 = \frac{p^4-p^2}{4}$ , denn hier liefern nur die Minimalpolynome von  $a \in \mathbb{F}_{p^4} \setminus \mathbb{F}_{p^2}$  etwas, und je vier solcher Elemente teilen sich das Minimalpolynom.

Für allgemeines  $d$  hat ein Element in  $\mathbb{F}_{p^d}$  ein Minimalpolynom über  $\mathbb{F}_p$ , dessen Grad  $t$  ein Teiler von  $d$  ist, denn es liegt dann in  $\mathbb{F}_{p^t} \subseteq \mathbb{F}_{p^d}$ . Je  $t$  dieser Elemente haben dasselbe Minimalpolynom. Und jedes irreduzible Polynom vom Grad  $t \mid d$  in  $\mathbb{F}_p[X]$  hat  $t$  Nullstellen in  $\mathbb{F}_{p^d}$ .

Das zeigt

$$p^d = \sum_{t \mid d} t \cdot N_t,$$

und mit der Möbius-Inversionsformel folgt

$$N_d = \frac{1}{d} \sum_{t \mid d} \mu(t) p^{d/t},$$

wobei  $\mu$  die Möbiussche  $\mu$ -Funktion ist.

## 2.3 Quadratische Reste

**Bemerkung 2.3.1 Die Quadrategruppe**

Es sei  $F$  ein endlicher Körper der Charakteristik  $p > 2$ . Dann heißt ein Element  $a \in F^\times$  ein *Quadrat* in  $F$ , wenn ein  $b \in F$  existiert mit  $b^2 = a$ .

Die Menge der Quadrate ist also das Bild der Abbildung

$$Q : F^\times \rightarrow F^\times, b \mapsto b^2.$$

Diese ist ein Gruppenhomomorphismus, und der Kern von  $Q$  besteht aus allen Elementen, deren Quadrat 1 ist, also aus  $\pm 1$ . Da die Charakteristik nicht 2 ist, sind das 2 verschiedene Elemente, und folglich hat  $\text{Kern}(Q)$  Index  $\frac{q-1}{2}$  in  $F^\times$ . Es folgt, dass  $Q(F^\times)$  auch  $\frac{q-1}{2}$  Elemente besitzt.

**Definition 2.3.2 Legendre<sup>9</sup>-Symbol**

Es sei  $p \geq 3$  eine Primzahl und  $F = \mathbb{F}_p$ . Für  $a \in \mathbb{Z}$  sei

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{falls } p \mid a, \\ 1, & \text{falls } \exists x \in \mathbb{Z} \setminus p\mathbb{Z} : a \equiv x^2 \pmod{p}, \\ -1, & \text{sonst.} \end{cases}$$

Das ist das klassische Legendre-Symbol.

Als Variante hiervon sei  $F$  ein endlicher Körper ungerader Charakteristik. Dann ist

$$\left(\frac{\cdot}{F}\right) : F \rightarrow \{-1, 0, 1\}$$

definiert durch die Bedingung

$$\left(\frac{a}{F}\right) = \begin{cases} 0, & \text{falls } a = 0, \\ 1, & \text{falls } a \in Q(F^\times), \\ -1, & \text{sonst.} \end{cases}$$

Das heißt speziell für  $a \in \mathbb{Z}$ :

$$\left(\frac{a}{p}\right) = \left(\frac{a + p\mathbb{Z}}{\mathbb{F}_p}\right).$$

Hier werden die Zahlen 0 und  $\pm 1$  entweder als ganze Zahlen oder als Elemente des endlichen Körpers aufgefasst. Weil dieser ungerade Charakteristik hat, sind das auch in  $F$  drei verschiedene Elemente.

**Hilfssatz 2.3.3 Von Euler**

a) *Es sei  $F$  ein endlicher Körper mit ungerader Charakteristik und  $q$  Elementen. Dann gilt für  $a \in F$ :*

$$\left(\frac{a}{F}\right) = a^{\frac{q-1}{2}}.$$

b) *Analog gilt für eine ungerade Primzahl  $p$  und  $a \in \mathbb{Z}$ :*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

c) *Die Abbildung  $\left(\frac{\cdot}{F}\right) : F^\times \rightarrow \{\pm 1\}$  ist ein Gruppenhomomorphismus.*

d) *Die Abbildung  $\left(\frac{\cdot}{p}\right) : \mathbb{Z} \rightarrow \{0, \pm 1\}$  ist strikt multiplikativ.*

---

<sup>9</sup>Adrien-Marie Legendre, 1752 - 1833

*Beweis.* Es ist klar, wie b) aus a) folgt.

Um a) zu zeigen, sehen wir erst ein, dass genau für  $a = 0$  auch  $a^{\frac{q-1}{2}} = 0$  gilt, also nur der Fall  $a \neq 0$  interessant ist.

Wegen des kleinen Satzes von Fermat ist hier  $a^{\frac{q-1}{2}}$  eine Quadratwurzel von 1, also 1 oder  $-1$ . Wenn  $a = b^2$  ein Quadrat ist, dann folgt  $a^{\frac{q-1}{2}} = b^{q-1} = 1$ , was die Hälfte der Aussage ist.

Wenn  $a$  kein Quadrat ist, wählen wir einen Erzeuger  $\zeta$  von  $F^\times$  und schreiben

$$a = \zeta^d$$

mit minimalem  $d \in \mathbb{N}$ . Dieser Exponent  $d$  ist ungerade (sonst wäre  $a$  ein Quadrat). Wäre nun  $a^{\frac{q-1}{2}} = 1$ , so wäre

$$\zeta^{d\frac{q-1}{2}} = 1 = \zeta^{q-1}.$$

Da der ggT von  $d\frac{q-1}{2}$  und  $q-1$  gerade  $\frac{q-1}{2}$  ist, wäre damit auch  $\zeta^{\frac{q-1}{2}} = 1$ , was der Tatsache widerspricht, dass  $\zeta$  Ordnung  $q-1$  hat.

c) und d) sind unmittelbare Konsequenzen hieraus, wobei klar sein dürfte, was in d) mit strikt multiplikativ gemeint ist.  $\circ$

### Folgerung 2.3.4 Vorauseilende Ergänzung

Der erste Ergänzungssatz zum quadratischen Reziprozitätsgesetz ist gerade der folgende Spezialfall von Eulers Formel

$$\forall 2 \neq p \in \mathbb{P} : \left( \frac{-1}{p} \right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{falls } p \equiv 1 \pmod{4}, \\ -1, & \text{falls } p \equiv 3 \pmod{4}. \end{cases}$$

### Definition 2.3.5 Halbheiten

a) Es sei  $F$  ein endlicher Körper von ungerader Charakteristik  $p$  und mit  $q$  Elementen. Ein *Halbsystem* in  $F$  ist eine Teilmenge  $H \subseteq F^\times$ , sodass

$$H \cap (-H) = \emptyset \text{ und } F^\times = H \cup (-H).$$

Zum Beispiel für  $F = \mathbb{F}_p$  bilden die Restklassen von  $1, 2, \dots, \frac{p-1}{2}$  ein Halbsystem.

b) Es sei  $H$  ein Halbsystem in  $F$  und  $a \in F^\times$ . Dann heißt

$$F(a, H) := \frac{q-1}{2} - |H \cap (aH)|$$

die *Fehlstandszahl* von  $a$  bezüglich  $H$ .

Zum Beispiel sind für beliebiges  $F$  und  $H$  die Fehlstandsanzahlen

$$F(1, H) = 0, \quad F(-1, H) = \frac{q-1}{2}.$$

Etwas substanzieller ist das Beispiel  $F = \mathbb{F}_p$  mit dem Halbsystem aus a). Hier gilt für  $a = 2 + p\mathbb{Z}$

$$F(a, H) = |\{x \in H \mid 2x \notin H\}| = \begin{cases} \frac{p-1}{4}, & \text{falls } p \equiv 1 \pmod{4}, \\ \frac{p+1}{4}, & \text{falls } p \equiv 3 \pmod{4}. \end{cases}$$

### Hilfssatz 2.3.6 Von Gauß

Es seien  $F$  ein endlicher Körper ungerader Charakteristik,  $H \subset F^\times$  ein Halbsystem in  $F$  und  $a \in F^\times$ .

Dann gilt

$$\left(\frac{a}{F}\right) = (-1)^{F(a,H)}.$$

*Beweis.* Für  $h \in H$  sei  $\sigma(h) \in \{\pm 1\}$  das Vorzeichen, für das  $\sigma ah \in H$  gilt. Es ist also  $\sigma(h) = 1$ , wenn  $ah \in H$  liegt, und sonst ist es  $-1$ . Es gibt also  $F(a, H)$  Werte für  $h \in H$  mit  $\sigma(h) = -1$ .

Daher haben wir

$$\left(\frac{a}{F}\right) \prod_{h \in H} h = a^{\frac{q-1}{2}} \prod_{h \in H} h = \prod_{h \in H} ah = \prod_{h \in H} \sigma(h)h = (-1)^{F(a,H)} \prod_{h \in H} h.$$

Das zeigt die Behauptung. ○

### Bemerkung 2.3.7 Zweite Ergänzung

Das Beispielmateriale aus 2.3.5b) zeigt, dass für eine Primzahl  $p \geq 3$  gilt:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{falls } p \equiv \pm 1 \pmod{8}, \\ -1, & \text{falls } p \equiv \pm 3 \pmod{8}. \end{cases}$$

Denn genau für die  $p$  aus der ersten Zeile ist  $F(2, H)$  gerade.

### Satz 2.3.8 Das quadratische Reziprozitätsgesetz

Es seien  $p \neq \ell$  zwei ungerade Primzahlen. Dann gilt

$$\left(\frac{p}{\ell}\right) \cdot \left(\frac{\ell}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{\ell-1}{2}}.$$

*Beweis.*

Wir arbeiten mit dem Halbsystem  $H = \{1, 2, 3, \dots, \frac{p-1}{2}\}$  modulo  $p$ . Mit  $F := F(H, \ell)$  gilt dann  $\left(\frac{\ell}{p}\right) = (-1)^F$ . Dabei ist

$$F = |\{x \in \{1, \dots, \frac{p-1}{2}\} \subseteq \mathbb{Z} \mid \exists y \in \mathbb{Z} : -\frac{p}{2} < \ell x - py < 0\}|.$$

Für solch ein  $y$  gilt übrigens immer  $1 \leq y \leq \frac{\ell-1}{2}$ . Denn:  $0 < y$  ist klar, und andererseits gilt

$$py < \ell x + \frac{p}{2} < \frac{p}{2}(\ell + 1);$$

Division durch  $p$  ergibt  $y < \frac{\ell+1}{2}$ , und weil  $\ell$  ungerade ist, muss  $y \leq \frac{\ell-1}{2}$  gelten.

Wir können also symmetrischer schreiben

$$F = |\{(x, y) \in \mathbb{Z}^2 \mid 1 \leq x \leq \frac{p-1}{2}, 1 \leq y \leq \frac{\ell-1}{2} : -\frac{p}{2} < \ell x - py < 0\}|.$$

Analog gilt

$$\left(\frac{p}{\ell}\right) = (-1)^{F'},$$

wobei

$$F' = |\{(x, y) \in \mathbb{Z}^2 \mid 1 \leq x \leq \frac{p-1}{2}, 1 \leq y \leq \frac{\ell-1}{2} : 0 < \ell x - py < \frac{\ell}{2}\}|.$$

Das impliziert

$$\left(\frac{\ell}{p}\right) \cdot \left(\frac{p}{\ell}\right) = (-1)^{F+F'}.$$

Nun ist aber

$$F + F' = |S|,$$

für die Menge

$$S := \{(x, y) \in \mathbb{Z}^2 \mid 1 \leq x \leq \frac{p-1}{2}, 1 \leq y \leq \frac{\ell-1}{2} : -\frac{p}{2} < \ell x - py < \frac{\ell}{2}\}.$$

Zu zeigen bleibt noch, dass  $F + F'$  dieselbe Parität hat wie  $\frac{p-1}{2} \cdot \frac{\ell-1}{2}$ .

Um das einzusehen, benutzen wir die Abbildung

$$\sigma : S \rightarrow S, \quad \sigma(x, y) = \left(\frac{p+1}{2} - x, \frac{\ell+1}{2} - y\right).$$

Hierbei gilt  $\sigma^2 = \text{Id}_S$ , und daher hat  $|S|$  dieselbe Parität, wie die Anzahl der Fixpunkte von  $\sigma$  – alle anderen Punkte lassen sich in disjunkten Zweiergruppchen  $\{P, \sigma(P)\}$  gruppieren.

Wenn nun  $\sigma$  einen Fixpunkt  $(x, y)$  hat, dann gilt

$$x = \frac{p+1}{4}, \quad y = \frac{\ell+1}{4},$$

also gibt es höchstens einen Fixpunkt, und das auch nur dann, wenn sowohl  $p$  als auch  $\ell$  kongruent zu 3 modulo 4 sind.

Wenn umgekehrt  $p, \ell \equiv 3 \pmod{4}$  erfüllt ist, dann ist offensichtlich  $(\frac{p+1}{4}, \frac{\ell+1}{4}) \in S$ , und es gibt so einen Fixpunkt.

Daher ist  $|S|$  ungerade genau dann, wenn  $p \equiv \ell \equiv 3 \pmod{4}$ , und das zeigt die Behauptung.  $\circ$

### Bemerkung 2.3.9 Tratsch

a) Die Einsichten aus 2.3.4 und 2.3.7 heißen die beiden Ergänzungen zum quadratischen Reziprozitätsgesetz.

b) Schon Legendre hatte das Reziprozitätsgesetz gesehen, aber mit Hilfsmitteln bewiesen, die zu seiner Zeit noch nicht zur Verfügung standen, insbesondere benutzte er den Dirichletschen Primzahlsatz. Erst Gauß fertigte gleich einige Beweise an, die schon zum Entstehungszeitpunkt streng gültig waren.

c) Ausgehend vom quadratischen Reziprozitätsgesetz wurden noch andere Reziprozitätsgesetze entwickelt. Zum Einen konnte man statt des Ringes  $\mathbb{Z}$  natürlich erst einmal andere Ringe verwenden. Für  $\mathbb{F}_p[X]$  zum Beispiel findet es sich in Aufgabe 9.4 des aktuellen Semesters.

Zum Anderen kann man – wenn der Ring schon größer ist – vielleicht auch kubische Potenzreste untersuchen, zum Beispiel in  $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ , oder biquadratische Potenzreste, z.B. in  $\mathbb{Z}[i]$ .

Es entstand eine ganze Industrie, die Reziprozitätsgesetze fabrizierte, bis hin zum krönenden Abschluss: dem Artinschen Reziprozitätsgesetz in der abelschen Klassenkörpertheorie.

In gewisser Weise erhält unser letzter Satz erst von solch einem höheren Standpunkt aus eine Existenzberechtigung.

Erst einmal nehmen wir den Satz als eine Möglichkeit, Legendre-Symbole zu berechnen.

### Beispiel 2.3.10 Zahlenbeispiele

$$\left(\frac{111}{41}\right) = \left(\frac{3}{41}\right) \cdot \left(\frac{37}{41}\right) = \left(\frac{41}{3}\right) \cdot \left(\frac{41}{37}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{4}{37}\right) = -1.$$

$$\left(\frac{113}{41}\right) = \left(\frac{31}{41}\right) = \left(\frac{10}{31}\right) = \left(\frac{2}{31}\right) \cdot \left(\frac{5}{31}\right) = (-1)^{\frac{31^2-1}{8}} \cdot \left(\frac{31}{5}\right) = 1.$$

Tatsächlich ist  $20^2 - 113 = 7 \cdot 41$ .

Für eine ungerade Primzahl  $p \neq 5$  ist 5 modulo  $p$  ein Quadrat genau dann, wenn  $p$  modulo 5 ein Quadrat ist, also genau dann, wenn  $p \equiv 1$  oder  $-1$  modulo 5 gilt, also  $p \in \{11, 19, 29, 31, 41, 59, 61, \dots\}$ .

Für eine ungerade Primzahl  $p \neq 3$  ist 3 modulo  $p$  ein Quadrat genau dann, wenn  $p$  modulo 3 ein Quadrat und außerdem 1 modulo 4 ist, oder wenn  $p$  modulo 3 kein Quadrat aber dafür selbst kongruent 3 modulo 4 ist, wenn es also  $\pm 1$  modulo 12 ist, also  $p \in \{11, 13, 23, 37, 47, 59, 61, \dots\}$ .

Unter anderem diese Art von Phänomen werden wir im nächsten Kapitel noch einmal von einer anderen Seite aus beleuchten, die einen kleinen Wink in Richtung der oben erwähnten Klassenkörpertheorie gibt.

# Kapitel 3

## Quadratische Zahlkörper

### 3.1 Der Ganzheitsring

#### Definition 3.1.1 Quadratische Zahlkörper

Ein Körper  $K \subseteq \mathbb{C}$  heißt ein *quadratischer Zahlkörper*, wenn er als Vektorraum über  $\mathbb{Q}$  Dimension 2 hat.

#### Hilfssatz 3.1.2 Alle Beispiele auf ein Mal

Es sei  $K$  ein quadratischer Zahlkörper. Dann gibt es genau eine quadratfreie Zahl  $d \in \mathbb{Z}$  sodass

$$K = \mathbb{Q}(\sqrt{d}) := \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}.$$

Ist umgekehrt  $d \neq 1$  eine quadratfreie ganze Zahl, dann ist die eben definierte Menge  $\mathbb{Q}(\sqrt{d})$  ein quadratischer Zahlkörper.

*Beweis.* Es seien zunächst  $K$  ein quadratischer Zahlkörper und  $\alpha \in K \setminus \mathbb{Q}$ . Da  $K$  zweidimensional ist, können  $1, \alpha, \alpha^2$  nicht über  $\mathbb{Q}$  linear unabhängig sein, während  $1$  und  $\alpha$  das sind. Folglich gibt es  $a, b \in \mathbb{Q}$ , sodass

$$\alpha^2 + a\alpha + b = 0.$$

Dann ist aber

$$\alpha = \frac{-a \pm \sqrt{a^2 - 4b}}{2},$$

und in  $K$  liegt auch

$$\pm\sqrt{a^2 - 4b} = 2\alpha + a.$$

Außerdem ist  $\sqrt{a^2 - 4b}$  irrational, denn sonst wäre ja  $\alpha$  rational.

Es gibt also ein  $\delta \in \mathbb{Q}$ , das in  $\mathbb{Q}$  kein Quadrat ist, und so, dass

$$K = \mathbb{Q} + \mathbb{Q} \cdot \sqrt{\delta}.$$

Nun ist aber klar, dass  $\delta$  sich schreiben lässt als

$$\delta = d \cdot m^2, \quad d \in \mathbb{Z} \text{ quadratfrei, } m \in \mathbb{Q}.$$

und dann ist offensichtlich auch  $\sqrt{d} = \frac{1}{m}\sqrt{\delta} \in K$ , und es gilt

$$K = \mathbb{Q}(\sqrt{d}).$$

Dieses  $d$  ist eindeutig, denn wenn  $1 \neq e \in \mathbb{Z}$  eine weitere quadratfreie Zahl ist, deren Wurzel in  $K$  liegt, dann gibt es  $x, y \in \mathbb{Q}$  mit

$$\sqrt{e} = x + y\sqrt{d}.$$

Es folgt

$$e = x^2 + dy^2 + 2xy\sqrt{d},$$

und da  $\sqrt{d}$  irrational ist, muss  $2xy = 0$  gelten

Im Fall  $y = 0$  folgt  $e = x^2$ , aber  $e$  ist kein Quadrat in  $\mathbb{Q}$ .

Im Fall  $x = 0$  folgt  $e = dy^2$ , also  $\frac{e}{d} = y^2$ . Da  $e$  und  $f$  quadratfrei sind, ist  $y = 1$  und  $d = e$  die Konsequenz.

Ist umgekehrt  $d \in \mathbb{Z}$  nicht 1 und quadratfrei, dann ist  $\sqrt{d}$  irrational, aber Nullstelle eines quadratischen rationalen Polynoms, und man rechnet leicht nach, dass  $\mathbb{Q}(\sqrt{d})$  ein Teilkörper von  $\mathbb{C}$  ist.  $\circ$

### Definition 3.1.3 Komplex oder reell

Es sei  $K = \mathbb{Q}(\sqrt{d})$  ein quadratischer Zahlkörper. Im Falle, dass  $d > 0$  gilt, liegt  $K$  schon in  $\mathbb{R}$  und heißt ein reellquadratischer Zahlkörper.

Anderenfalls liegt  $K$  nicht ganz in  $\mathbb{R}$  und heißt ein imaginärquadratischer Zahlkörper.

### Bemerkung 3.1.4 Eine Einbettung

a) Statt von vorneherein  $K$  als Teilkörper von  $\mathbb{C}$  einzuführen, ist es im Nachhinein geschickter, für eine quadratfreie ganze Zahl  $d \neq 1$  den zu  $\mathbb{Q}(\sqrt{d})$  isomorphen Restklassenkörper

$$\mathbb{Q}[X]/(X^2 - d)\mathbb{Q}[X]$$

als den quadratischen Zahlkörper aufzufassen.

Dieser lässt sich dann bequem in

$$K_{\mathbb{R}} := \mathbb{R}[X]/(X^2 - d)\mathbb{R}[X] \cong \begin{cases} \mathbb{C}, & d < 0, \\ \mathbb{R} \times \mathbb{R}, & d > 0, \end{cases}$$

einbetten.

Im zweiten Fall ist die Einbettung von  $\mathbb{Q}(\sqrt{d})$  nach  $\mathbb{R} \times \mathbb{R}$  konkreter gegeben durch

$$a + b\sqrt{d} \mapsto (a + b\sqrt{d}, a - b\sqrt{d}).$$

b) Der Körper  $K = \mathbb{Q}(\sqrt{d})$  hat neben der Identität noch einen Automorphismus, nämlich

$$\kappa : K \rightarrow K, \quad \kappa(a + b\sqrt{d}) = a - b\sqrt{d}.$$

Wie können also die Einbettung von  $K$  nach  $\mathbb{R} \times \mathbb{R}$  im reellquadratischen Fall auch schreiben als

$$K \ni \alpha \mapsto (\alpha, \kappa(\alpha)) \in \mathbb{R} \times \mathbb{R}.$$

Wie bemerken noch, dass  $(1, 1)$  und  $(\sqrt{d}, -\sqrt{d})$  reell linear unabhängig sind. Das werden wir später noch geometrisch ausnutzen.

### Definition 3.1.5 Norm und Spur

Es sei  $K$  ein quadratischer Zahlkörper. Für  $\alpha \in K$  ist die Abbildung

$$\mu : K \rightarrow K, \quad \mu(x) := \alpha \cdot x,$$

$\mathbb{Q}$ -linear.

Ihre Determinante heißt die *Norm*  $N(\alpha)$  von  $\alpha$ , ihre Spur heißt die *Spur*  $\text{Sp}(\alpha)$  von  $\alpha$ .

Konkreter gilt für  $\alpha = a + b\sqrt{d}$ :

$$N(\alpha) = a^2 - db^2, \quad \text{Sp}(\alpha) = 2a.$$

Die Norm ist also eine quadratische Form auf  $K$ . Insbesondere ist für negatives  $d$  die Normenform positiv definit, und  $N(\alpha)$  ist einfach das Quadrat der Länge von  $\alpha \in \mathbb{C}$ . Die Spur ist in diesem Fall das Doppelte des Realteils.

Für positives  $d$  ist die Normenform indefinit.

Mithilfe des Automorphismus  $\kappa$  aus 3.1.4 sieht man

$$N(\alpha) = \alpha \cdot \kappa(\alpha), \quad \text{Sp}(\alpha) = \alpha + \kappa(\alpha).$$

Die Norm ist nur dann 0, wenn  $\alpha = 0$  gilt. Man sagt dann auch, diese quadratische Form sei *anisotrop*.

### Definition 3.1.6 Ganzheit

a) Eine komplexe Zahl  $\alpha$  heißt *ganz über  $\mathbb{Z}$* , wenn sie Nullstelle eines ganzzahligen normierten Polynoms ist.

Man sieht leicht, dass  $\alpha \in \mathbb{Q}$  genau dann ganz über  $\mathbb{Z}$  ist, wenn es schon in  $\mathbb{Z}$  liegt. Das liegt daran, dass  $\mathbb{Z}$  ein Hauptidealring ist.

b) Für einen quadratischen Zahlkörper  $K \subseteq \mathbb{C}$  bezeichnen wir mit  $\mathcal{O}_K$  die Menge aller über  $\mathbb{Z}$  ganzen Elemente in  $K$ .

Sie heißt der *Ganzheitsring* von  $K$ . Das müssen wir gleich rechtfertigen.

### Hilfssatz 3.1.7 Konkreter

Es sei  $d \in \mathbb{Z}$  quadratfrei,  $d \neq 1$ , und  $K = \mathbb{Q}(\sqrt{d})$  der zugehörige quadratische Zahlkörper.

Dann gilt

$$\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\omega_d,$$

wobei

$$\omega_d := \begin{cases} \sqrt{d}, & d \not\equiv 1 \pmod{4}, \\ \frac{1+\sqrt{d}}{2}, & d \equiv 1 \pmod{4}. \end{cases}$$

Insbesondere ist  $\mathcal{O}_K$  ein Ring.

*Beweis.* Wir zeigen zunächst, dass  $\alpha \in K$  genau dann ganz ist, wenn es ganze Norm und Spur hat.

Wenn  $N(\alpha)$  und  $\text{Sp}(\alpha)$  ganz sind, dann sagt der Satz von Cayley-Hamilton, dass  $\alpha$  eine Nullstelle des ganzzahligen Polynoms

$$X^2 - \text{Sp}(\alpha)X + N(\alpha)$$

ist. Das kann man hier natürlich leicht explizit nachrechnen, und es zeigt dass  $\alpha$  tatsächlich ganz ist.

Ist umgekehrt  $\alpha$  ganz, so sei es Nullstelle eines Polynoms

$$f = X^r + \sum_{\nu=0}^{r-1} c_\nu X^\nu \in \mathbb{Z}[X].$$

Die Gruppe  $\Gamma := \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\alpha^2 + \cdots + \mathbb{Z}\alpha^{r-1}$  ist endlich erzeugt und als Untergruppe eines rationalen Vektorraums gibt es darin keine Elemente endlicher Ordnung. Sie ist aber – nach dem Homomorphiesatz – eine Faktorgruppe von  $\mathbb{Z}^r$  nach einer Untergruppe, deren Elementarteiler alle 1 sind, denn sonst gäbe es in der Faktorgruppe Elemente endlicher Ordnung. Also ist  $\Gamma$  frei abelsch. Als Untergruppe von  $K$ , die  $\mathbb{Z}$  enthält, ist ihr Rang 1 oder 2. Im ersten Fall sind  $\alpha$  und 1 linear abhängig, also  $\alpha \in \mathbb{Q}$ , und damit  $\alpha \in \mathbb{Z}$ . Also sind Norm und Spur ganz.

Im zweiten Fall ist die Multiplikation mit  $\alpha$  ein Endomorphismus von  $\Gamma$  und beschreibt sich bezüglich einer Basis von  $\Gamma$  durch eine ganzzahlige  $2 \times 2$ -Matrix, deren Spur und Determinante natürlich auch ganz sind.

Es bleibt also zu zeigen, dass die Elemente von  $K$  mit ganzer Norm und Spur genau die  $\mathbb{Z}$ -Linearkombinationen von 1 und  $\omega_d$  sind.

Dass diese ganze Norm und Spur haben, ist eine leichte Rechnung.

Sei umgekehrt  $\alpha = x + y\sqrt{d}$ ,  $x, y \in \mathbb{Q}$ , ein Element mit ganzer Norm und Spur.

Die Spur ist  $2x$ , also gilt  $x \in \frac{1}{2} \cdot \mathbb{Z}$ .

Fall 1:  $x \in \mathbb{Z}$ . Dann ist wegen  $N(\alpha) = x^2 + y^2d \in \mathbb{Z}$  auch  $y \in \mathbb{Z}$ , da  $d$  quadratfrei ist.

Damit liegt  $\alpha$  in  $\mathbb{Z} + \mathbb{Z}\sqrt{d} \subseteq \mathbb{Z} + \mathbb{Z}\omega_d$ .

Fall 2:  $x - \frac{1}{2} \in \mathbb{Z}$ .

Da die Spur und die Norm von  $2(x + y\sqrt{d})$  auch ganz sind, ist dann nach Fall 1  $2y \in \mathbb{Z}$ . Wäre  $y$  sogar selbst in  $\mathbb{Z}$ , so wäre  $x^2 \in \mathbb{Z}$ , und damit auch  $x$ , was ausgeschlossen war. Es folgt  $y - \frac{1}{2} \in \mathbb{Z}$ .

Wann kann das auftreten?

Seien dazu  $x = k + \frac{1}{2}, y = l + \frac{1}{2}, k, l \in \mathbb{Z}$ . Dann gilt

$$x^2 - dy^2 = k^2 + k + \frac{1}{4} - dl^2 - dl - d\frac{1}{4} \in \mathbb{Z},$$

also

$$\frac{1-d}{4} \in \mathbb{Z}.$$

Das impliziert  $d \equiv 1 \pmod{4}$ , und damit

$$x + y\sqrt{d} = k - l + (2l + 1)\frac{\sqrt{d} + 1}{2} \in \mathbb{Z} + \mathbb{Z}\omega_d.$$

○

### Definition 3.1.8 Diskriminante

Es sei  $K = \mathbb{Q}(\sqrt{d})$  ein quadratischer Zahlkörper,  $d \in \mathbb{Z}$  quadratfrei. Dann heißt der Ausdruck

$$D_K := (\omega_d - \kappa(\omega_d))^2 = \begin{cases} 4d, & d \not\equiv 1 \pmod{4}, \\ d & d \equiv 1 \pmod{4}, \end{cases}$$

die *Diskriminante* von  $K$ .

Im reellquadratischen Fall ist das das Quadrat des Flächeninhalts des von  $(1, 1)$  und  $(\omega, \kappa(\omega))$  aufgespannten Parallelogramms in der Ebene.

Im imaginärquadratischen Fall ist es bis aufs Vorzeichen das Vierfache des Quadrats des in  $\mathbb{C}$  von 1 und  $\omega_d$  aufgespannten Parallelogramms.

**Folgerung 3.1.9 Einheitsnorm**

Die Norm wird am interessantesten, wenn man sie als Abbildung von  $\mathcal{O}_K$  nach  $\mathbb{Z}$  auffasst. Wegen ihrer Multiplikativität hat jede Einheit in  $\mathcal{O}_K$  Norm  $\pm 1$ , denn die Norm ist auch in  $\mathbb{Z}$  invertierbar. Wegen  $N(x) = x \cdot \kappa(x)$  ist umgekehrt auch jedes Element  $x \in \mathcal{O}_K$  mit Norm  $\pm 1$  eine Einheit, ihr Inverses ist ja  $\pm \kappa(x) \in \mathcal{O}_K$ .

Zum Beispiel ist  $1 + \sqrt{2}$  eine Einheit im Ganzheitsring von  $\mathbb{Q}(\sqrt{2})$ , denn die Norm ist  $-1$ .

Auch  $\frac{1+\sqrt{5}}{2}$  ist eine Einheit.

**Beispiel 3.1.10 Alte Bekannte**

Speziell für  $d = -1$  oder  $d = -3$  finden sich als Ganzheitsringe gerade

$$\mathbb{Z}[i], \quad \mathbb{Z}\left[\frac{1 + \sqrt{-3}}{2}\right],$$

die wir in Vorlesung und Übung schon verschiedentlich gesehen hatten. Ihre Diskriminante ist  $-4$  bzw.  $-3$ .

Sie sind sogar Hauptidealringe, aber das stimmt bei weitem nicht für alle Ganzheitsringe.

**Hilfssatz 3.1.11 Die Einheiten**

*Es seien  $0 > d \in \mathbb{Z}$  quadratfrei,  $K = \mathbb{Q}(\sqrt{d})$  der zugehörige imaginärquadratische Zahlkörper,  $\mathcal{O}$  sein Ganzheitsring. Dann ist  $\mathcal{O}^\times$  endlich und zyklisch, und ein Erzeuger hat Ordnung 4, wenn  $d = -1$ , 6, wenn  $d = -3$ , und ansonsten 2.*

*Insbesondere ist  $\mathcal{O}^\times = \{\pm 1\}$ , wenn  $d \neq -1, -3$ .*

*Beweis.* Im imaginärquadratischen Fall ist  $K_{\mathbb{R}} = \mathbb{C}$ , und die Norm ist das Quadrat des Betrages. Da  $\mathcal{O}$  additiv von 1 und  $\omega_d$  erzeugt wird, die reell linear unabhängig sind, ist es diskret. Also liegen auf dem kompakten Einheitskreis nur endlich viele ganze Elemente von  $K$ , und das sind gerade die gesuchten Einheiten.

Wenn  $\alpha \in \mathcal{O} \setminus \mathbb{Z}$  eine Einheit ist, dann ist  $|\alpha| = 1$ , und  $(X - \alpha)(X - \bar{\alpha}) = X^2 - \text{Sp}(\alpha)X + 1$  ist ganzzahlig. Natürlich ist dann die Spur von  $\alpha$  als Summe zweier komplexer Zahlen vom Betrag 1 betragsmäßig kleiner als 2. Da sie ganz ist, ist sie 0 (und  $\alpha = \pm i$ ), 1 (und  $\alpha = \frac{1 \pm \sqrt{-3}}{2}$ ) oder  $-1$  (und  $\alpha = \frac{-1 \pm \sqrt{-3}}{2}$ ).

Man sieht, dass die Einheitengruppe im Fall  $d = -1$  von  $i$  erzeugt wird, im Fall  $d = -3$  von  $\frac{1 + \sqrt{-3}}{2}$  und ansonsten immer von  $-1$ .  $\circ$

Wir werden später noch sehen, dass im reellquadratischen Fall die Einheitengruppe unendlich ist. Dafür langt es dann natürlich, ein von  $\pm 1$  verschiedenes Element zu finden.

**Bemerkung 3.1.12 Norm statt Index**

Es sei  $\mathcal{O}_K$  der Ganzheitsring im quadratischen Zahlkörper  $K = \mathbb{Q}(\sqrt{d})$ .

Ein Ideal in  $\mathcal{O}_K$  ist dann einfach eine Untergruppe von  $\mathcal{O}_K$ , die unter Multiplikation mit  $\omega_d$  in sich selbst abgebildet wird. Als Gruppe ist so ein Ideal wegen 1.5.3 frei abelsch, der Rang ist 0, 1, oder 2. Allerdings ist mit einem von 0 verschiedenen Element  $\alpha \in I$  auch  $\omega_d \cdot \alpha \in I$ , und damit der Rang niemals 1. Insbesondere hat ein von Null verschiedenes Ideal endlichen Index.

Für  $0 \neq \alpha \in \mathcal{O}_K$  hat das Ideal  $\alpha\mathcal{O}_K$  (wegen 2.1.5 und der Matrixversion des Elementarteilersatzes) in  $\mathcal{O}_K$  Index  $|N(\alpha)|$ . Man spricht daher auch von der Norm eines Ideals und meint damit seinen Index im Ganzheitsring, auch wenn es kein Hauptideal ist.

Ist  $I \neq \{0\}$  so ein Ideal, dann ist sein Schnitt mit  $\mathbb{Z}$  nicht  $\{0\}$ , denn in  $I$  liegen auch die Normen seiner Elemente. Ein Erzeuger von  $I \cap \mathbb{Z}$  zusammen mit einem Element  $a + b\omega_d$  mit minimalem positiven  $b$  sind dann eine mögliche Wahl für eine Basis von  $I$  (als frei abelsche Gruppe).

**Hilfssatz 3.1.13 Wieder einmal die Assoziiertenklassen**

Es sei  $K = \mathbb{Q}(\sqrt{d})$  wie gehabt und  $\mathcal{O}_K$  sein Ganzheitsring. Weiter sei  $n \in \mathbb{N}$  gegeben.

Dann gibt es nur endlich viele Assoziiertenklassen in  $\mathcal{O}_K$ , sodass die Repräsentanten Norm  $\pm n$  haben.

*Beweis.* Es sei  $\alpha \in \mathcal{O}$  mit Norm  $\pm n$  gegeben. Dann hat das Ideal  $\alpha\mathcal{O}_K$  Index  $|N(\alpha)|$  in  $\mathcal{O}_K$ . Da es nur endlich viele solcher Ideale gibt (höchstens so viele wie Untergruppen vom Index  $n$ , also höchstens  $\sum_{d|n} d$  Stück), und zwei Elemente von  $\mathcal{O}_K$  genau dann assoziiert sind, wenn sie dasselbe Hauptideal erzeugen (siehe 1.2.15), folgt die Behauptung.  $\circ$

**Definition 3.1.14 Primideal**

Es sei  $R$  ein kommutativer Ring und  $I \subseteq R$  ein Ideal. Dann heißt  $I$  ein *Primideal*, wenn  $I \neq R$  gilt und außerdem für alle  $x, y \in R$ :

$$x \cdot y \in I \Rightarrow x \in I \text{ oder } y \in I.$$

Speziell ist ein Hauptideal  $I = Ra$  genau dann ein Primideal, wenn es von einem Primelement erzeugt wird.

Das Nullideal  $\{0\}$  ist genau dann ein Primideal, wenn  $R$  nullteilerfrei ist.

Ein Ideal, dessen Index in  $R$  eine Primzahl ist, ist ein Primideal.

Die Menge aller Primideale von  $R$  wird oft auch das *Spektrum* von  $R$  genannt.

**Hilfssatz 3.1.15 Zur Übersicht**

Es sei  $K = \mathbb{Q}(\sqrt{d})$  ein quadratischer Zahlkörper.

- a) Ist  $P \subseteq \mathcal{O}_K$  ein von  $\{0\}$  verschiedenes Primideal, so enthält  $P$  genau eine Primzahl.
- b) Ist  $p \in \mathbb{P}$  eine Primzahl, so liegt es in ein oder zwei Primidealen in  $\mathcal{O}_K$ .

*Beweis.*

a) Wenn  $P$  ein Primideal ist, dann ist auch  $P \cap \mathbb{Z}$  ein Primideal  $p \cdot \mathbb{Z}$ , und es ist nicht 0, denn für  $a \in P$  ist auch  $N(a) = a\kappa(a) \in P$ .

b) Wenn  $p$  eine Primzahl ist, dann gibt es zwei Möglichkeiten.

Einerseits könnte  $p$  auch in  $\mathcal{O}_K$  ein Primelement sein, also dort ein Primideal erzeugen, und es gibt genau ein Primideal, das  $p$  enthält, nämlich  $p\mathcal{O}_K$ .

Andererseits könnte  $p$  kein Primideal erzeugen. Dann gibt es  $x, y \in \mathcal{O}_K$ , die beide keine Vielfachen von  $p$  sind aber ihr Produkt schon. Insbesondere sind dann auch beide keine Einheiten und nicht 0. Es sei  $I := \{rp + sx \mid r, s \in \mathcal{O}_K\}$  das von  $p$  und  $x$  erzeugte Ideal. Es umfasst  $p\mathcal{O}_K$  echt, seine Norm ist also ein echter Teiler von  $p^2$ , also 1 oder  $p$ . Wäre die Norm von  $I$  gleich 1, so gäbe es  $r, s \in \mathcal{O}_K$  mit

$$rp + sx = 1.$$

Multipliziert man dies mit  $y$ , so wird daraus

$$rpy + sxy = y.$$

Die linke Seite jedoch wird von  $p$  geteilt, und daher ist  $y$  doch ein Vielfaches von  $p$  entgegen der Annahme. Folglich ist die Norm von  $I$  gleich  $p$ .

Es gibt also ein Primideal, das  $p$  enthält. Da sein Index eine Primzahl ist, kann es auch nicht in einem noch größeren echten Ideal enthalten sein.

Genauso ist das von  $p$  und  $y$  erzeugte Ideal ein Primideal. Da in jedem  $p$  enthaltenden Primideal einer der beiden Faktoren  $x$  und  $y$  enthalten sein muss, sind das die einzigen Primideale, die  $p$  enthalten.  $\circ$

**Folgerung 3.1.16 Noch übersichtlicher**

Es seien  $K$  ein quadratischer Zahlkörper mit Diskriminante  $D$  und  $2 \neq p \in \mathbb{P}$  eine Primzahl. Weiter sei  $M = (X - \omega_d)(X - \kappa(\omega_d))$  das Minimalpolynom von  $\omega_d$ .

Dann gilt für jede Primzahl  $p$  einer der folgenden Sachverhalte:

- a) Liegt in  $\mathbb{F}_p$  eine doppelte Nullstelle von  $M$ , dann liegt  $p$  in genau einem Primideal von  $\mathcal{O}_K$ , und dieses hat Norm  $p$ . Man sagt dann,  $p$  sei in  $K$  verzweigt.
- b) Liegt in  $\mathbb{F}_p$  keine Nullstelle von  $M$ , so erzeugt  $p$  ein Primideal in  $\mathcal{O}_K$ . Man sagt dann,  $p$  sei träge in  $K$ .
- c) Hat  $M$  in  $\mathbb{F}_p$  zwei verschiedene Nullstellen, so liegt  $p$  in genau zwei Primidealen in  $\mathcal{O}_K$ . Man sagt dann,  $p$  sei zerlegt in  $K$ .

*Beweis.* Zum Beweis muss man nur die Argumente aus dem vorherigen Hilfssatz genau analysieren.  $\circ$

### Folgerung 3.1.17 Viele Nichthauptidealringe

Es sei  $d \in \mathbb{Z}$  kleiner als  $-2$ , quadratfrei und  $\not\equiv 1 \pmod{4}$ .

Dann ist der Ganzheitsring  $\mathbb{Z}[\sqrt{d}]$  kein Hauptidealring.

*Beweis.* Die Diskriminante des zugehörigen Hauptidealrings ist  $4d$ , also ist 2 verzweigt in  $K = \mathbb{Q}(\sqrt{d})$ . Das 2 enthaltende Primideal ist eine Untergruppe von Index 2 in  $\mathbb{Z}[\sqrt{d}]$ , also frei in zwei Erzeugern. Man sieht leicht, dass es für gerades  $d$  von 2 und  $\sqrt{d}$  erzeugt wird, und ansonsten von 2 und  $\sqrt{d} - 1$ .

Wenn dieses Ideal ein Hauptideal wäre, dann müsste es in  $\mathcal{O}_K$  ein Element der Norm 2 geben. Die Norm von  $a + b\sqrt{d}$  ist aber

$$a^2 - db^2,$$

und da  $d$  negativ ist, ist dies für  $|b| \geq 2$  größer als 2. Für  $b = 0$  wird die Norm nicht 2, denn 2 ist keine Quadrat in  $\mathbb{Z}$ , und es bleibt nur die Möglichkeit  $b = \pm 1$ . Das liefert Elemente der Norm 2 für  $a = 0$  und  $d = -2$  bzw.  $a = \pm 1$  und  $d = -1$ . Diese Werte negativer  $d$  hatten wir aber mit ausgeschlossen.  $\circ$

### Bemerkung 3.1.18 Wieder einmal Gauß

Es ist spannend zu verfolgen, für welche Werte negativer  $d$  der Ganzheitsring in  $\mathbb{Q}(\sqrt{d})$  ein Hauptidealring ist.

Relativ schnell findet man als Kandidaten die Zahlen

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

Man wusste lange Zeit (seit Gauß) nicht, ob es weitere Werte hierfür gibt. Dann konnte man zeigen, dass es höchstens einen weiteren Wert gibt. Ein erster Beweis

von Heegner<sup>1</sup>, dass die neun Werte die einzigen sind, wurde zunächst nicht akzeptiert. Erst als Stark<sup>2</sup> 1967 einen eigenen Beweis angab, wurde auch Heegners Beweis (rigorosifiziert und) rehabilitiert.

Er funktioniert mithilfe der Theorie der elliptischen Kurven und benutzt eine spezielle Konstruktion von Punkten auf einigen dieser Kurven, die heute Heegner-Punkte genannt werden.

**Noch spannender** aber wäre es, der bis heute ungelösten Frage nachzugehen, ob wirklich – wie auch seit Gauß vermutet wird – unendlich viele reellquadratische Zahlkörper einen Hauptidealring als Ganzheitsring besitzen.

## 3.2 Geometrie der Zahlen

Der Ganzheitsring  $\mathcal{O}_K$  eines quadratischen Zahlkörpers  $K$ , aufgefasst als Untergruppe von  $K_{\mathbb{R}}$  wird von zwei reell linear unabhängigen Elementen erzeugt. Er ist daher eine diskrete Untergruppe von  $K_{\mathbb{R}}$ , das heißt: jeder Punkt der Ebene hat eine Umgebung, die nur endlich viele Elemente aus  $\mathcal{O}_K$  enthält.

Dieses Faktum kann man nun benutzen, um arithmetische Eigenschaften des Ganzheitsrings zu sehen. Wir werden dabei natürlich nicht alle Facetten der Geometrie der Zahlen zur Sprache bringen, sondern nur einen leichten Vorgeschmack geben.

### Definition 3.2.1 Gitter

Ein *Gitter* in einem reellen, endlichdimensionalen Vektorraum  $V$  ist eine Untergruppe  $\Gamma$ , die von einer  $\mathbb{R}$ -Basis von  $V$  erzeugt wird.

### Bemerkung 3.2.2 Ein Fundamentalbereich

Es sei  $\Gamma \subseteq V$  das von der Basis  $B = \{b_1, \dots, b_n\}$  erzeugte Gitter. Dann heißt

$$\mathcal{F}_B := \left\{ \sum_{i=1}^n a_i b_i \mid 0 \leq a_i < 1 \right\}$$

die *Fundamentalmasche* von  $\Gamma$  in  $V$ .

Jeder Punkt  $x \in V$  lässt sich auf eindeutig bestimmte Art schreiben als

$$x = f + \gamma, \quad f \in \mathcal{F}_B, \gamma \in \Gamma,$$

denn zunächst ist  $x$  eine reelle Linearkombination der Basisvektoren, und dann zerlegen wir die Koeffizienten als  $a + z$ ,  $0 \leq a < 1, z \in \mathbb{Z}$ .

<sup>1</sup>Kurt Heegner, 1893 - 1865; Lehrer und Ingenieur

<sup>2</sup>Harold Stark, geb. 1939

Ist  $V$  sogar ein euklidischer Vektorraum, so nennen wir das Volumen von  $\mathcal{F}_B$  auch das *Kovolumen* von  $\Gamma$ , in Zeichen  $\text{cov}(\Gamma)$ .

Ist  $\{\beta_1, \dots, \beta_n\}$  eine Orthonormalbasis von  $V$  und  $A = (\langle \beta_i, b_j \rangle)_{1 \leq i, j \leq n}$  die Basiswechselmatrix von  $\{\beta_j\}$  zu  $\{b_i\}$ , dann ist

$$\text{cov}(\Gamma) = |\det(A)|.$$

Sind nun  $B, C$  zwei Basen des Gitters  $\Gamma$ , so ist die Basiswechselmatrix zwischen ihnen unimodular, denn sie ist ganzzahlig, und ihre Inverse auch. Also hat der Basiswechsel Determinante  $\pm 1$ , und damit haben  $\mathcal{F}_B$  und  $\mathcal{F}_C$  dasselbe Volumen. Das zeigt, dass das Kovolumen des Gitters wohldefiniert ist.

3.1.8 zeigt uns daher, wie die Diskriminante eines Zahlkörpers  $K$  mit dem Kovolumen von  $\mathcal{O}_K$  in  $K_{\mathbb{R}}$  zusammenhängt, wobei wir auf  $K_{\mathbb{R}} = \mathbb{C}$  oder  $\mathbb{R}^2$  das übliche Skalarprodukt wählen.

### Satz 3.2.3 Gitterpunktsatz von Minkowski<sup>3</sup>

Im euklidischen Vektorraum  $E$  sei ein Gitter  $\Gamma$  von Kovolumen  $V$  gegeben. Weiter sei  $S \subseteq E$  eine konvexe, kompakte Menge (eigentlich langt hier messbar) mit  $S = -S$  und Volumen

$$\text{vol}(S) > 2^n \cdot V.$$

Dann liegt in  $S \cap \Gamma$  mindestens ein Element  $\neq 0$ .

*Beweis.* Es sei  $B$  eine Basis von  $\Gamma$  und  $\mathcal{F}_B$  die zugehörige Fundamentalmasche. Wie zeigen zunächst, dass in  $\frac{1}{2}S$  zwei verschiedene Punkte existieren, deren Differenz in  $\Gamma$  liegt.

Um dies zu zeigen, setzen wir

$$C(\gamma) := (\gamma + \mathcal{F}_B) \cap \frac{1}{2}S, \quad \gamma \in \Gamma,$$

und zerlegen  $\frac{1}{2}S$  als

$$\frac{1}{2}S = \bigcup_{\gamma \in \Gamma} C(\gamma).$$

Die Disjunktheit der Mengen  $\gamma + \mathcal{F}_B, \gamma \in \Gamma$ , und die maßtheoretische Freundlichkeit aller beteiligten Mengen zeigen, dass

$$\text{vol}\left(\frac{1}{2}S\right) = \sum_{\gamma \in \Gamma} \text{vol}(C(\gamma)).$$

---

<sup>3</sup>Hermann Minkowski, 1864 - 1909

Nun ist aber  $C(\gamma) - \gamma \subseteq \mathcal{F}_B$ , und wenn diese alle disjunkt wären, dann hätten wir

$$V = \text{vol}(\mathcal{F}_B) \geq \sum_{\gamma \in \Gamma} \text{vol}(C(\gamma)) = \text{vol}\left(\frac{1}{2}S\right) = 2^{-n} \text{vol}(S).$$

Das widerspricht der Annahme an die Größenverhältnisse.

Also gibt es zwei verschiedene Elemente  $\gamma_1, \gamma_2 \in \Gamma$  mit

$$(C(\gamma_1) - \gamma_1) \cap (C(\gamma_2) - \gamma_2) \neq \emptyset,$$

und daher 2 Punkte  $s_1, s_2 \in \frac{1}{2}S$  mit

$$s_1 - \gamma_1 = s_2 - \gamma_2, \quad \text{also} \quad s_1 - s_2 = \gamma_1 - \gamma_2 \in \Gamma.$$

Da  $2s_2$  und  $2s_1$  beide in  $S$  liegen, und damit nach Voraussetzung auch  $-2s_2$ , liegt auch die Konvexkombination

$$s_1 - s_2 = \frac{1}{2}(2s_1 + (-2s_2))$$

in  $S$ . Das zeigt die Behauptung. ○

### Satz 3.2.4 Der Vierquadratesatz von Lagrange

*Jede natürliche Zahl lässt sich als Summe von vier Quadratzahlen schreiben.*

*Beweis.* Zur Vorbereitung überlegen wir uns, dass das Produkt zweier Zahlen, die Summen vierer Quadrate sind, auch eine Summe von vier Quadraten ist. Dazu betrachten wir die Menge

$$\mathcal{Q} := \left\{ \begin{pmatrix} a & -\bar{b} \\ b & \bar{a} \end{pmatrix} \mid a, b \in \mathbb{Z}[i] \right\}.$$

Eine natürliche Zahl  $n$  ist genau dann die Summe vierer Quadratzahlen, wenn sie die Determinante einer Matrix in  $\mathcal{Q}$  ist. Da  $\mathcal{Q}$  ein Ring ist und die Determinante multiplikativ ist, folgt die eingangs aufgestellte Behauptung.

Das zeigt aufgrund des Fundamentalsatzes der Arithmetik (und weil  $1 = 1^2 + 0^2 + 0^2 + 0^2$  Summe vierer Quadratzahlen ist), dass wir die Behauptung des Satzes nur für Primzahlen zu zeigen haben.

Es sei also  $p$  eine Primzahl. Außerdem sei  $p > 2$ , denn für  $p = 2$  sieht jeder, dass es Summe vierer Quadratzahlen ist.

Die Mengen

$$M := \{0^2, 1^2, \dots, \left(\frac{p-1}{2}\right)^2\} \quad \text{und} \quad -1 - M = \{-1 - 0^2, -1 - 1^2, \dots, -1 - \left(\frac{p-1}{2}\right)^2\}$$

enthalten jeweils  $\frac{p+1}{2}$  Elemente, die modulo  $p$  verschiedenen sind. Also können  $M$  und  $-1 - M$  modulo  $p$  nicht disjunkt sein. Daher gibt es ganze Zahlen  $u, v$ , sodass

$$u^2 + v^2 \equiv -1 \pmod{p}$$

gilt. Mit diesen Zahlen definieren wir das Gitter

$$\Gamma := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ u & v & p & 0 \\ -v & u & 0 & p \end{pmatrix} \cdot \mathbb{Z}^4 \subseteq \mathbb{R}^4.$$

Es hat Kovolumen  $p^2 < \text{vol}(B_r(0))/16$ , wenn

$$r = \sqrt[4]{32} \sqrt{\frac{p}{\pi}} + \varepsilon$$

gewählt wird (das Volumen der Kugel im Vierdimensionalen ist  $\frac{\pi^2}{2} \cdot r^4$ ).

Also gibt es für jedes positive  $\varepsilon$  einen von Null verschiedenen Vektor in  $\Gamma$ , der Länge  $< r$  hat.

Es seien  $a, b, c, d \in \mathbb{Z}$  gegeben. Dann ist das Längenquadrat von

$$\gamma = \begin{pmatrix} a \\ b \\ ua + vb + pc \\ -va + ub + pd \end{pmatrix} \in \Gamma$$

modulo  $p$  gleich

$$(1 + u^2 + v^2)a^2 + (1 + v^2 + u^2)b^2,$$

also – wegen unserer Wahl von  $u$  und  $v$  – durch  $p$  teilbar. Andererseits ist für kleines  $\varepsilon$  sicher auch

$$r^2 < 2p,$$

und damit ist das Längenquadrat eines von Null verschiedenen Vektors mit Länge  $< r$  genau  $p$ .

Damit ist die Behauptung gezeigt.  $\circ$

Weniger als 4 Quadrate reichen im allgemeinen nicht, wie der Fall  $n = 7$  lehrt. Man kann präzise sagen, für welche Zahlen man tatsächlich 4 Quadrate braucht.

Nach diesem kleinen Exkurs mit einem konkreten Beispiel, was der Gitterpunktsatz von Minkowski bewirken kann, kehren wir nun zu den quadratischen Zahlkörpern zurück. Es geht uns jetzt um die Einheitengruppe des Ganzheitsrings im reellquadratischen Fall.

**Bemerkung 3.2.5 Vorbereitende Bemerkungen**

Es sei nun  $d > 1$  eine ganze, quadratfreie Zahl,  $K = \mathbb{Q}(\sqrt{d})$  der zugehörige reellquadratische Zahlkörper. Wie bereits gewohnt fassen wir diesen via

$$K \ni \alpha \mapsto (\alpha, \kappa(\alpha)) \in \mathbb{R} \times \mathbb{R} = K_{\mathbb{R}}$$

als Teilring von  $K_{\mathbb{R}}$  auf und betrachten auf diesem reellen Vektorraum das übliche Skalarprodukt. Das Kovolumen des Gitters  $\mathcal{O}_K$  in  $K_{\mathbb{R}}$  ist dann gerade  $\sqrt{D_K}$ .

Die Einheiten von  $\mathcal{O}_K$  liegen wegen 3.1.9 alle in

$$H := \{(x, y) \in K_{\mathbb{R}} \mid xy = \pm 1\}.$$

Dies ist eine Gruppe bezüglich der komponentenweisen Multiplikation. Die Untergruppe

$$H_+ := \{(x, y) \in K_{\mathbb{R}} \mid x, y > 0, xy = 1\}$$

hat hierin Index 4. Sie ist der Kern der surjektiven Abbildung, die  $(x, y) \in H$  auf  $(\operatorname{sgn}(x), \operatorname{sgn}(y)) \in \{\pm 1\}^2$  abbildet.

Da nun  $\mathcal{O}_K$  in  $K_{\mathbb{R}}$  diskret liegt, liegt auch die Einheitengruppe  $\mathcal{O}_K^{\times}$  in  $H$  diskret, denn  $H$  ist abgeschlossen.

Andererseits ist  $H_+$  biestetig isomorph zu  $(\mathbb{R}, +)$ , nämlich vermöge der Abbildung

$$H_+ \ni (x, y) \mapsto \log x \in \mathbb{R}, \quad \mathbb{R} \ni t \mapsto (\exp(t), \exp(-t)) \in H_+.$$

Der Durchschnitt  $\mathcal{O}_K^{\times} \cap H_+$  wird hierbei auf eine diskrete Untergruppe von  $\mathbb{R}$  abgebildet, und diese wird – wenn nichttrivial – zwangsläufig von einem betragsmäßig kleinsten Element erzeugt, ist also zyklisch.

Andererseits ist  $H$  unbeschränkt. Wenn wir nun wissen, dass es ein Kompaktum  $Q \subseteq K_{\mathbb{R}}$  gibt, sodass

$$H \subseteq \bigcup_{\gamma \in \mathcal{O}_K^{\times}} \gamma Q,$$

dann muss  $\mathcal{O}_K^{\times}$  unendlich sein.

Insgesamt folgt aus der Existenz eines solchen Kompaktums also der folgende

**Satz 3.2.6 Spezialfall von Dirichlets Einheitsensatz**

*Es sei  $K$  ein reellquadratischer Zahlkörper.*

*Dann gibt es eine Einheit  $\varepsilon \in \mathcal{O}_K^{\times}$ ,  $\varepsilon \neq \pm 1$ , sodass*

$$\mathcal{O}_K^{\times} = \{\pm \varepsilon^a \mid a \in \mathbb{Z}\} \cong \{\pm 1\} \times \mathbb{Z}.$$

*Beweis.* Wir erinnern an die vorangehende Bemerkung, auch was die Notation angeht, und wählen den Radius  $\delta$  so groß, dass die Kreisscheibe  $B := B_\delta(0)$  Flächeninhalt  $> 2^2 \text{cov}(\mathcal{O}_K)$  hat.

Für jedes  $h \in H$  ist  $h \cdot B$  eine Ellipsenfläche mit demselben Flächeninhalt, und ist symmetrisch zur 0. Es gibt also wegen 3.2.3 ein von 0 verschiedenes  $r_h \in \mathcal{O}_K \cap (hB)$ .

Für die Abbildung

$$N : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}, (x, y) \mapsto xy,$$

die die auf  $K$  definierte Norm fortsetzt und stetig und multiplikativ ist, ist

$$\forall b \in B : |N(hb)| = |N(b)| \leq \delta^2.$$

$|N(r_h)|$  ist also durch eine von  $h$  unabhängige Schranke nach oben beschränkt, und es gibt daher nur endlich viele Werte, die in Frage kommen.

Da es für jede dieser ganzen Zahlen nur endlich viele Assoziiertenklassen in  $\mathcal{O}_K$  gibt, die sie als Norm haben (siehe 3.1.13), gibt es Elemente  $r_1, \dots, r_t \in \mathcal{O}_K$ , sodass für jedes  $h \in H$  ein  $i \in \{1, \dots, t\}$  und ein  $\gamma_h \in \mathcal{O}_K^\times$  existieren mit

$$r_{h^{-1}} = r_i \cdot \gamma_h,$$

also

$$h \in r_{h^{-1}} B = \gamma_h^{-1} r_i^{-1} B \subseteq \bigcup_{\gamma \in \mathcal{O}_K^\times} \gamma \left( \bigcup_{i=1}^t r_i^{-1} B \right).$$

Mit  $Q := \bigcup_{i=1}^t r_i^{-1} B$  folgt die Behauptung. ○

### Folgerung 3.2.7 Die Pellische Gleichung

*Es sei  $d \in \mathbb{N}$  keine Quadratzahl.*

*Dann hat die Gleichung*

$$x^2 - dy^2 = 1$$

*unendlich viele Lösungen  $(x, y) \in \mathbb{Z}^2$ .*

*Beweis.* Naja, eigentlich ist das keine Folgerung, sondern vielmehr lässt sich dasselbe Argument für den Ganzheitsring eben auch für den Teilring

$$R := \mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$$

durchziehen.

Das liefert unendlich viele Einheiten in  $R$ , und das sind dort genau die Elemente mit Norm  $\pm 1$ , also die Elemente  $x + y\sqrt{d} \in R$  mit

$$x^2 - dy^2 = \pm 1.$$

Die Lösungen der Gleichung mit 1 auf der rechten Seite entsprechen dann gerade einer Untergruppe vom Index 1 oder 2 in  $R^\times$ . ○

**Bemerkung 3.2.8 Namensgebend war... Euler**

Die Gleichung

$$x^2 - dy^2 = 1$$

für unquadratisches natürliches  $d$  heißt Pell<sup>4</sup>sche Gleichung, weil Euler sie so genannt hat. Er hätte sie wahrscheinlich eher Rahn<sup>5</sup>sche Gleichung nennen sollen, ließ sich aber wohl davon irritieren, dass Pell Teile des Rahnschen Werkes mit herausgegeben hat.

Im allgemeinen ist es aufwendig, den Erzeuger des zyklischen Anteils der Einheitsgruppe in  $\mathbb{Z}[\sqrt{d}]$  zu finden.

In Abschnitt 3.4 werden wir noch einen konstruktiven Weg zur Lösung dieser Gleichung kennen lernen.

Erst einmal wollen wir uns noch einmal den Idealen zuwenden, und ein Maß dafür angeben, wie weit der Ganzheitsring davon entfernt ist, ein Hauptidealring zu sein.

**3.3 Idealklassen****Definition 3.3.1 Eine Äquivalenzrelation**

Es sei  $\mathcal{O}_K \subseteq K$  der Ganzheitsring im quadratischen Zahlkörper  $K$ . Zwei von Null verschiedene Ideale  $I, J \subseteq \mathcal{O}_K$  heißen *äquivalent*, wenn ein  $\alpha \in K^\times$  existiert mit

$$\alpha I = J.$$

Es ist klar, dass dies eine Äquivalenzrelation ist. Die Äquivalenzklassen heißen zumeist Idealklassen, und die von  $\mathcal{O}_K$  selbst ist die Menge aller Hauptideale in  $\mathcal{O}_K$ .

**Bemerkung 3.3.2 Unimodulare Ähnlichkeit**

Wir bleiben unserer Situation treu.

Wenn  $I \neq \{0\}$  ein Ideal in  $\mathcal{O}_K$  ist, dann wird die Multiplikation mit  $\omega_d$  bezüglich einer Basis von  $I$  durch eine ganzzahlige  $2 \times 2$ -Matrix dargestellt, deren charakteristisches Polynom gerade

$$m := (X - \omega_d)(X - \kappa(\omega_d))$$

ist. Bezüglich einer anderen Basis von  $I$  bekommt man eine Matrix, die vermöge eines unimodularen Basiswechsels zur ersten ähnlich ist. Ist  $J = \alpha I$  ein zu  $I$

---

<sup>4</sup>John Pell, 1611 - 1685

<sup>5</sup>J.H. Rahn, 1622 - 1676

äquivalentes Ideal, so erhält man dieselbe unimodulare Ähnlichkeitsklasse von ganzzahligen  $2 \times 2$ -Matrizen, die  $m$  als Minimalpolynom haben, denn die Multiplikation mit  $\alpha$  ist ein Isomorphismus zwischen  $I$  und  $J$ , der mit der Multiplikation mit  $\omega_d$  vertauscht.

Ist umgekehrt  $A \in \mathbb{Z}^{2 \times 2}$  eine Nullstelle von  $m$ , so gibt es ein Ideal, auf dem  $\omega_d$  via  $A$  wirkt. Je zwei solche Ideale sind zueinander äquivalent.

Denn: Sind  $I = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2$ ,  $J = \mathbb{Z}\beta_1 + \mathbb{Z}\beta_2$  zwei Ideale, sodass die Multiplikation mit  $\omega_d$  sich bezüglich der Basen  $\{\alpha_1, \alpha_2\}$  und  $\{\beta_1, \beta_2\}$  durch dieselbe Matrix  $A$  beschreibt, dann vertauscht die  $\mathbb{Q}$ -lineare Abbildung

$$K \ni x\alpha_1 + y\alpha_2 \mapsto x\beta_1 + y\beta_2 \in K$$

mit der Multiplikation mit  $\omega_d$ , ist also sogar  $K$ -linear, und daher die Multiplikation mit einem Skalar aus  $K$ .

Man erhält also eine Bijektion zwischen den Äquivalenzklassen von Idealen in  $\mathcal{O}_K$  einerseits und unimodularen Ähnlichkeitsklassen von ganzzahligen Matrizen  $A$  mit  $m(A) = 0$ .

Die Frage nach Idealklassen in  $\mathcal{O}_K$  ist also nichts anderes als die Frage nach einer ganzzahligen „Normalform“ von ganzzahligen Matrizen mit gegebenem Minimalpolynom.

Es ist klar, dass alle rationalen  $2 \times 2$ -Matrizen, die  $m$  als Minimalpolynom haben, über  $\mathbb{Q}$  zueinander ähnlich sind.

### Definition 3.3.3 Eine Verknüpfung und eine Gruppe

Für zwei Ideale  $I, J \subseteq \mathcal{O}_K$  definieren wir

$$I \cdot J$$

als das Ideal in  $\mathcal{O}_K$ , das von den Produkten  $xy, x \in I, y \in J$  erzeugt wird.

Diese Verknüpfung ist assoziativ und besitzt ein neutrales Element, nämlich  $\mathcal{O}_K$ .

Übrigens gilt stets  $N(I \cdot J) = N(I) \cdot N(J)$ , was sich für „teilerfremde“ Ideale (wenn es also  $x \in I$  gibt, sodass  $1 - x \in J$  gilt) mit dem chinesischen Restsatz zeigen lässt, denn hier ist  $I \cdot J = I \cup J$ .

Es ist klar, dass diese Verknüpfung eine wohldefinierte Verknüpfung auf den Äquivalenzklassen der von Null verschiedenen Ideale gibt.

Dort besitzt dann jede Klasse ein inverse Klasse, denn man kann mit etwas Mühe nachrechnen, dass für ein Ideal  $I$  das Ideal

$$I \cdot \kappa(I)$$

von der ganzen Zahl  $(\mathcal{O}_K : I) = N(I)$  erzeugt wird, also ein Hauptideal ist.

Das führt dazu, dass die Menge der Idealklassen eine Gruppe ist, die sogenannte *Klassengruppe*  $\text{Cl}_K$  von  $\mathcal{O}_K$ .

$\mathcal{O}_K$  ist genau dann ein Hauptidealring, wenn  $\text{Cl}_K$  die triviale Gruppe ist.

### Satz 3.3.4 Erzeuger

*Jedes von Null verschiedene Ideal in  $\mathcal{O}_K$  ist ein Produkt von Primidealen.*

*Beweis.* Wir nehmen das Gegenteil an, und betrachten ein Ideal  $I$  mit minimalem Index, das sich nicht als Produkt von Primidealen schreiben lässt. Es ist auf jeden Fall in einem Primideal  $P$  von  $\mathcal{O}_K$  enthalten, denn es hat endlichen Index (man kommt hier also ohne das Lemma von Zorn aus, das sonst benutzt wird um diese Aussage für kommutative Ringe allgemein zu zeigen). Wir zeigen, dass es ein Ideal  $J \subseteq \mathcal{O}_K$  gibt, sodass  $I = PJ$ , und dass die Norm von  $J$  kleiner ist als die von  $I$ . Dann lässt sich dieses als Produkt von Primidealen schreiben, und damit auch  $I = PJ$ .

Die Existenz von  $J$  folgt aus  $P \cdot \kappa(P) = N(P) \cdot \mathcal{O}_K$ , denn wir finden dann

$$I = \frac{P \cdot \kappa(P)}{N(P)} \cdot I = P \cdot \frac{\kappa(P) \cdot I}{N(P)}.$$

Da  $I$  in  $P$  liegt, gilt tatsächlich  $\kappa(P) \cdot I \subseteq \kappa(P) \cdot P = N(P) \cdot \mathcal{O}_K$ , und damit ist  $J := \frac{\kappa(P) \cdot I}{N(P)}$  ein Ideal in  $\mathcal{O}_K$ . Seine Norm ist

$$N(J) = N(I) \cdot N(\kappa(P)) / N(N(P)) = N(I) / N(P),$$

denn  $N(\kappa(P)) = N(P)$  und  $N(N(P)) = N(P)^2$ .

Also ist die Norm von  $J$  kleiner als die von  $I$ , und wir sind fertig.  $\circ$

**Bemerkung 3.3.5** Der letzte Satz sollte als Verallgemeinerung des Fundamentalsatzes der Arithmetik angesehen werden. Statt wie dort mit Zahlen hantiert er aber mit Idealen, was für  $\mathbb{Z}$  aber auf dasselbe hinausläuft. Was hier nicht mitbewiesen wurde, aber trotzdem stimmt, ist die Eindeutigkeit der als existent nachgewiesenen Zerlegung.

### Satz 3.3.6 Endlichkeit der Klassengruppe

*Die Klassengruppe eines quadratischen Zahlkörpers  $K$  ist endlich.*

*Beweis.* Wir zeigen, dass es endlich viele Ideale gibt, sodass jedes Ideal zu einem dieser endlich vielen äquivalent ist.

Dabei nutzen wir aus, dass  $\mathcal{O}_K \subseteq K_{\mathbb{R}}$  ein Gitter ist. Es sei  $v$  das Kovolumen.

Es sei  $I \subseteq \mathcal{O}_K$  ein Ideal. Das Ideal  $\kappa(I)$  hat dann in  $\mathcal{O}_K$  den selben Index wie  $I$ , und es hat in  $K_{\mathbb{R}}$  Kovolumen

$$v \cdot N(I).$$

Wir zeigen nun, dass es in  $\kappa(I)$  ein von Null verschiedenes Element  $\alpha$  von „kleiner“ Norm gibt, und dass „klein“ dahingehend präzisiert werden kann, dass die Norm von  $\frac{\alpha}{N(I)}I$  kleiner als eine von  $I$  unabhängige Schranke ist. Da es nur endlich viele Ideale mit Norm kleiner als diese Schranke gibt, folgt die Behauptung.

Um das rigoroser zu gestalten, unterscheiden wir wieder die folgenden Fälle.

Fall 1:  $K$  ist imaginärquadratisch.

Hier ist  $K_{\mathbb{R}} = \mathbb{C}$ , und die Norm eines Elements  $\alpha$  ist  $|\alpha|^2$ .

Im Kreis

$$\{z \in \mathbb{C} \mid |z| \leq \sqrt{\frac{5v}{\pi}N(I)}\},$$

der ja Flächeninhalt  $> 4v \cdot N(I) = 4\text{cov}(\kappa(I))$  hat, liegt ein Element  $\alpha$  aus  $\kappa(I)$ , das nicht 0 ist. Dessen Norm ist also  $\leq \frac{5v}{\pi}N(I)$ , und da

$$\alpha I \subseteq \kappa(I)I = N(I) \cdot \mathcal{O}_K$$

gilt, ist

$$\frac{\alpha}{N(I)}I$$

ein zu  $I$  äquivalentes Ideal mit Norm

$$N\left(\frac{\alpha}{N(I)}I\right) = \frac{N(\alpha)}{N(I)} \leq \frac{5v}{\pi}.$$

Fall 2:  $K$  ist reellquadratisch.

Hier ist  $K_{\mathbb{R}} = \mathbb{R} \times \mathbb{R}$ , und die Norm eines Elements  $(x, y)$  ist  $xy$ . Wir müssen also Rechtecke anstelle von Kreisen benutzen, um eine Abschätzung für Normen zu bekommen.

Das Quadrat

$$\{(x, y) \mid |x|, |y| \leq \sqrt{2vN(I)}\} \subseteq \mathbb{R} \times \mathbb{R}$$

hat Flächeninhalt  $8vN(I)$ , also liegt darin ein Element  $\alpha \neq 0$  aus  $\kappa(I)$ . Der Betrag seiner Norm ist  $\leq 2vN(I)$ , und wir sehen, dass die Norm von  $\frac{\alpha}{N(I)}I$  nach oben durch  $2v$  beschränkt ist.

Das beendet den Beweis auch im reellquadratischen Fall. ○

**Bemerkung 3.3.7** Insbesondere ist  $\mathcal{O}_K$  ein Hauptidealring, wenn alle Ideale mit Norm  $\leq 5v/\pi$  bzw.  $2v$  Hauptideale sind.

Mit etwas mehr Sorgfalt hätten wir diese Schranke noch besser hinbekommen können, wollten aber vor allem die Endlichkeitsaussage an sich begründen.

Wenn man das hat, kann man zum Beispiel einsehen, dass die Ganzheitsringe der reellquadratischen Zahlkörper  $\mathbb{Q}(\sqrt{d})$  mit

$$d = 2, 3, 5, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, 31, 33, 37, 38, \dots$$

Hauptidealringe sind.

Für  $d = 2$  etwa ist die Diskriminante 8, und wir müssen sehen, dass alle Ideale in  $\mathbb{Z}[\sqrt{2}]$  von Norm  $\leq 2\sqrt{8}$  Hauptideale sind.

Machen wir das zunächst für die Primideale.

Das Primideal, das 2 enthält, wird von  $\sqrt{2}$  erzeugt, ist also ein Hauptideal.

Die Primzahlen  $\equiv 3, 5 \pmod{8}$  sind träge, also auch dort das einzige sie enthaltende Primideal ein Hauptideal.

Es verbleiben die Primideale, die Primzahlen  $\equiv \pm 1 \pmod{8}$  enthalten. Da die Norm kleiner als 6 sein soll, gibt es diese nicht.

Da sich jedes Ideal als Produkt von Primidealen kleinerer Norm schreiben lässt (siehe 3.3.4), ist damit jedes Ideal von Norm  $\leq 2\sqrt{8}$  ein Hauptideal, und damit überhaupt jedes Ideal in  $\mathbb{Z}[\sqrt{2}]$ .

## 3.4 Kettenbrüche

### Bemerkung 3.4.1 Soviel vorweg

a) Dieser Abschnitt gehört nur halb in dieses Kapitel, aber für ihn ein neues Kapitel aufzumachen wäre jetzt etwas übertrieben. Auch hier reißen wir nur einige Ergebnisse an, und werden vor allem die Kettenbruchentwicklung behandeln, die nur ein kleines Teilgebiet des großen Gebietes der Diophantischen Approximation ist.

b) Wenn  $(a, b)$  eine nichttriviale (das heißt hier  $b \neq 0$ ) Lösung der Pellischen Gleichung

$$a^2 - db^2 = 1$$

ist, dann ist  $|a - b\sqrt{d}| \cdot |a + b\sqrt{d}| = 1$ , also dürfen wir ohne Einschränkung annehmen, dass

$$|a - b\sqrt{d}| =: u < 1$$

Dann ist  $|b| = \left| \frac{a+b\sqrt{d}-(a-b\sqrt{d})}{2\sqrt{d}} \right| = \left| \frac{1-u}{2\sqrt{d}} \right| < \frac{1}{u}$ .

Daher ist

$$\left| \frac{a}{b} - \sqrt{d} \right| < \frac{1}{b^2}.$$

Um eine Lösung der Pellschen Gleichung zu finden, sollte man also eine rationale Zahl suchen, die – gemessen an ihrem Nenner – nahe bei  $\sqrt{d}$  liegt.

Darum geht es prinzipiell in der Diophantischen Approximation.

### Definition 3.4.2 Kettenbrüche

a) Es seien  $a_0 \in \mathbb{R}$  und  $a_1, a_2, \dots, a_k \in \mathbb{R}_{>0}$ .

Dann definieren wir den *Kettenbruch*  $[a_0; a_1, a_2, \dots, a_k]$  rekursiv durch

$$[a_0] := a_0, [a_0; a_1, a_2, \dots, a_k] := a_0 + \frac{1}{[a_1; a_2, \dots, a_k]}.$$

Es ist zum Beispiel

$$[a_0; a_1] = a_0 + \frac{1}{a_1}, \quad [a_0; a_1, a_2] = a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = a_0 + \frac{a_2}{a_1 a_2 + 1} \dots$$

b) Nun sei  $\alpha \in \mathbb{R}$  irrational und sonst beliebig. Für die Gaußklammer schreiben wir jetzt lieber  $\lfloor \cdot \rfloor$ , um sie nicht mit dem Kettenbruch  $[\cdot]$  zu verwechseln.

Dann definieren wir  $a_0, \beta_1$  durch

$$a_0 := \lfloor \alpha \rfloor, \quad \beta_1 := \frac{1}{\alpha - a_0}.$$

Es gilt  $\alpha = [a_0; \beta_1]$  und  $\beta_1 > 1$ , und wenn

$$a_0, a_1, \dots, a_{n-1} \in \mathbb{Z}, \quad \mathbb{R} \ni \beta_n > 1,$$

gefunden sind mit  $a_1, a_2, \dots > 0$ , und  $\alpha = [a_0; a_1, \dots, a_{n-1}, \beta_n]$  dann definieren wir

$$a_n := \lfloor \beta_n \rfloor, \quad \beta_{n+1} := \frac{1}{\beta_n - a_n}.$$

Dann gilt wieder  $\beta_{n+1} > 1$ ,  $a_n \in \mathbb{N}$ , und

$$\alpha = [a_0; a_1, \dots, a_{n-1}, a_n, \beta_{n+1}].$$

Die rationale Zahl  $[a_0; a_1, \dots, a_n]$  heißt dann die *n-te Konvergente* von  $\alpha$ .

### Beispiel 3.4.3 Fibonacci und der goldene Schnitt

Es sei  $\alpha = \omega_5 = \frac{1+\sqrt{5}}{2}$  der goldene Schnitt. Das ist die positive Nullstelle des Polynoms

$$X^2 - X - 1,$$

das bei 1 den Wert  $-1$  und bei 2 den Wert 1 annimmt. Es gilt

$$\alpha = \frac{1}{\alpha - 1}.$$

Die Kettenbruchentwicklung von  $\alpha$  liefert daher

$$a_0 := \lfloor \alpha \rfloor = 1, \quad \beta_1 = \frac{1}{\alpha - 1} = \alpha,$$

und induktiv sieht man  $a_0 = a_1 = \dots = 1$ .

Die 0-te Konvergente ist 1, die erste ist 2, die dritte ist  $\frac{3}{2}$ , und wegen

$$[1; 1, 1, 1, \dots] = 1 + \frac{1}{[1; 1, 1, \dots, 1]}$$

(wobei rechts der Kettenbruch einen Schritt kürzer ist) folgt für die  $n$ -te Konvergente  $\alpha_n$ :

$$\alpha_n = 1 + \frac{1}{\alpha_{n-1}}.$$

Ist insbesondere  $\alpha_{n-1} = \frac{F_n}{F_{n-1}}$ , so folgt

$$\alpha_n = 1 + \frac{F_{n-1}}{F_n} = \frac{F_{n-1} + F_n}{F_n},$$

weshalb wir  $F_{n-1} + F_n = F_{n+1}$  setzen und die alte Rekursionsvorschrift für die Fibonaccizahlen herausbekommen (mit  $F_0 = 1, F_1 = 1$ ).

Wegen  $F_{n-1}F_{n+1} - F_n^2 = F_{n-1}^2 - F_{n-2}F_n$  folgt induktiv, dass der Betrag von  $F_{n-1}F_{n+1} - F_n^2$  stets 1 ist und vom Vorzeichen her alterniert. Die Differenz

$$\frac{F_{n-1}}{F_n} - \frac{F_n}{F_{n+1}} = \frac{F_{n-1}F_{n+1} - F_n^2}{F_nF_{n+1}}$$

ist daher eine alternierende Nullfolge, und folglich konvergiert die Folge

$$\left(\frac{F_{n-1}}{F_n}\right)_{n \in \mathbb{N}}$$

gegen eine reelle Zahl  $\sigma$ . Offensichtlich muss diese die Gleichung

$$\sigma^{-1} = \sigma - 1$$

erfüllen, und daher – aus Vorzeichenrunden – der goldene Schnitt sein.

Wir lernen also hier, dass die Konvergenten der Kettenbruchentwicklung von  $\alpha$  gegen  $\alpha$  konvergieren und ihren Namen nicht umsonst tragen.

Allerdings wissen wir das bisher nur für den goldenen Schnitt.

### Hilfssatz 3.4.4 Eine Rekursionsvorschrift

*Es seien  $a_0, a_1, \dots$  reelle Zahlen,  $a_i > 0$  für  $i > 0$ .*

Weiter seien  $p_i, q_i$  rekursiv definiert durch

$$p_{-2} = 0, \quad q_{-2} = 1, \quad p_{-1} = 1, \quad q_{-1} = 0$$

und

$$p_i := a_i p_{i-1} + p_{i-2}, \quad q_i := a_i q_{i-1} + q_{i-2}.$$

Dann gilt für  $i \geq 0$  die Gleichung

$$[a_0; a_1, a_2, \dots, a_i] = \frac{p_i}{q_i}.$$

*Beweis.* Wir machen vollständige Induktion nach  $i$ .

Für  $i = 0$  ist  $p_0 = a_0$ ,  $q_0 = 1$ , und wir sehen

$$a_0 = \frac{a_0 \cdot 1 + 0}{a_0 \cdot 0 + 1} = \frac{p_0}{q_0}.$$

Für  $i = 1$  ist  $p_1 = a_0 a_1 + 1$ ,  $q_1 = a_1 \cdot 1 + 0$ , und es folgt

$$a_0 + \frac{1}{a_1} = \frac{p_1}{q_1}.$$

Sei die Behauptung wahr für alle Indizes  $\leq i$ . Dann ist

$$\begin{aligned} [a_0; a_1, \dots, a_i, a_{i+1}] &= [a_0; a_1, \dots, a_i + \frac{1}{a_{i+1}}] \\ &= \frac{(a_i + \frac{1}{a_{i+1}})p_{i-1} + p_{i-2}}{(a_i + \frac{1}{a_{i+1}})q_{i-1} + q_{i-2}} \\ &= \dots = \frac{p_{i+1}}{q_{i+1}}. \end{aligned}$$

Hier benutzen wir beim zweiten Gleichheitszeichen die Induktionsvoraussetzung und formen das dann mit der Definition aller beteiligten Größen um.  $\circ$

### Bemerkung 3.4.5 Fixiere die Notation!

Wir halten im Weiteren die Notation aus dem Hilfssatz fest, und bezeichnen mit  $p_k, q_k$  immer die hier fixierten Zähler und Nenner der Konvergenten. Diese Notation ist in der Literatur sehr einheitlich in Verwendung.

Es gilt stets

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k+1}.$$

Für  $k = -1$  ist das klar, und dann ist induktiv

$$p_{k+1} q_k - p_k q_{k+1} = \det \begin{pmatrix} p_{k+1} & p_k \\ q_{k+1} & q_k \end{pmatrix} = \det \begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix} \cdot \begin{pmatrix} a_{k+1} & 1 \\ 1 & 0 \end{pmatrix}.$$

Das langt. ○

Man sieht auch: Wenn die  $a_i$  für  $i > 0$  mindestens 1 sind, dann gilt mit  $i \geq 0$  stets  $q_i \geq i$  gilt; die  $q_i$  gehen also gegen unendlich.

### Satz 3.4.6 Konvergente konvergieren

Es sei  $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ . Dann konvergieren die Konvergenten der Kettenbruchentwicklung von  $\alpha$  gegen  $\alpha$ .

*Beweis.* Wir nutzen die Notation von 3.4.2 und schreiben

$$\alpha = [a_0; a_1, \dots, a_k, \beta_{k+1}] = \frac{p_k \cdot \beta_{k+1} + p_{k-1}}{q_k \cdot \beta_{k+1} + q_{k-1}}.$$

Hier sind die  $a_i$  ganze Zahlen (sogar natürlich für  $i > 0$ ) und  $\beta_{k+1} > 1$ . Daher ist die Folge der  $q_k$  streng monoton steigend und geht daher gegen unendlich.

Außerdem liegt  $\alpha$  zwischen  $\frac{p_k}{q_k}$  und  $\frac{p_{k-1}}{q_{k-1}}$ , und damit ist

$$\left| \alpha - \frac{p_k}{q_k} \right| \leq \left| \frac{p_{k-1}}{q_{k-1}} - \frac{p_k}{q_k} \right| = \left| \frac{1}{q_{k-1}q_k} \right| \xrightarrow{k \rightarrow \infty} 0.$$

○

### Bemerkung 3.4.7 Allgemein und beispielhaft

a) Der Beweis zeigt sogar, dass

$$\left| \alpha - \frac{p_n}{q_n} \right| \leq \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2}$$

gilt, und das ist genau die Art von Ungleichung, die wir vorher aus der Lösung der Pellschen Gleichung extrahiert hatten.

Der Beweis zeigt auch, dass für beliebige vorgegebene  $a_0 \in \mathbb{Z}$  und  $a_1, a_2, \dots \in \mathbb{N}$  die Folge der Konvergenten gegen eine reelle Zahl  $\alpha$  konvergiert. Genauer sieht das Konvergenzverhalten so aus:

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \dots < \alpha < \dots < \frac{p_5}{q_5} < \frac{p_3}{q_3} < \frac{p_1}{q_1}$$

b) nun sei  $\alpha = \sqrt{3}$ . Wir sehen, dass

$$a_0 = 1, \beta_1 = \frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{2}, a_1 = 1, \beta_2 = \frac{2}{\sqrt{3}-1} = \sqrt{3}+1, a_2 = 2,$$

und insgesamt folgt

$$\sqrt{3} = [1; 1, 2, 1, 2, 1, 2, 1, 2 \dots]$$

Es folgt eine kleine Tabelle mit den Werten für  $a_i, p_i, q_i$  und der Norm der Zahl  $p_i - q_i\sqrt{3} \in \mathbb{Q}(\sqrt{3})$ .

$i$	$a_i$	$p_i$	$q_i$	$N(p_i - q_i\sqrt{3})$
-2		0	1	-3
-1		1	0	1
0	1	1	1	-2
1	1	2	1	1
2	2	5	3	-2
3	1	7	4	1
4	2	19	11	-2
5	1	26	15	1

Das sei ein kleiner Wink dafür, dass die Kettenbruchentwicklung von  $\sqrt{d}$  etwas mit der Pellischen Gleichung zu tun haben könnte, die ja das Einswerden der Norm verlangt.

### Hilfssatz 3.4.8 Herausgepellt

Es seien  $d \in \mathbb{N}$  keine Quadratzahl,  $\alpha = \sqrt{d}$  und  $\alpha = [a_0; a_1, \dots, a_{k-1}, \beta_k]$  wie gehabt.

Dann gilt  $\beta_k = \frac{P_k + \sqrt{d}}{Q_k}$ , wobei die ganzen Zahlen  $P_k, Q_k$  rekursiv wie folgt definiert werden:

$$P_0 = 0, \quad Q_0 = 1, \quad P_{k+1} = a_k Q_k - P_k, \quad Q_{k+1} = \frac{d - P_{k+1}^2}{Q_k}.$$

*Beweis.* Zu Beginn des Beweises setzen wir erst einmal  $\beta_0 = \alpha$  und sehen die Richtigkeit der Behauptung für  $k = 0$ . Dann folgt induktiv

$$\beta_{k+1} = \frac{1}{\beta_k - a_k} = \frac{Q_k}{P_k + \sqrt{d} - Q_k a_k} = \frac{\sqrt{d} + a_k Q_k - P_k}{(d - (P_k - Q_k a_k)^2)/Q_k},$$

und das zeigt die Behauptung schon fast. Nur die Ganzzahligkeit von  $Q_{k+1}$  ist noch zu begründen. Sie folgt daraus, dass *per definitionem*

$$Q_k Q_{k-1} = d - P_k^2$$

gilt,  $Q_k$  also  $d - P_k^2$  teilt, und damit auch  $d - (P_k - Q_k a_k)^2$ . ○

Wir halten jetzt auch die Notation der  $P_k$  und  $Q_k$  fest, speziell  $P_1 = a_0$  und  $Q_1 = d - a_0^2$ .

### Hilfssatz 3.4.9 Periodizitätskriterium

Es gilt  $(P_{k+1}, Q_{k+1}) = (P_1, Q_1)$  genau dann, wenn  $Q_k = 1$ .

*Beweis.*

Aus  $Q_k = 1$  folgt  $\beta_k = P_k + \sqrt{d}$ , also  $a_k = P_k + a_0$ . Das impliziert

$$P_{k+1} = a_0 + P_k - P_k = a_0 = P_1 \quad \text{und} \quad Q_{k+1} = \frac{d - P_{k+1}^2}{Q_k} = d - a_0^2 = Q_1.$$

Ist umgekehrt  $(P_{k+1}, Q_{k+1}) = (P_1, Q_1)$ , dann folgt

$$\frac{d - P_1^2}{Q_0} = Q_1 = Q_{k+1} = \frac{d - P_{k+1}^2}{Q_k},$$

und wegen  $P_1 = P_{k+1}$  folgt  $Q_k = Q_0 = 1$ . ○

### Hilfssatz 3.4.10 Eine Norm

Es gilt  $p_k^2 - dq_k^2 = (-1)^{k+1}Q_{k+1}$ .

*Beweis.* Wir benutzen

$$\alpha = \sqrt{d} = [a_0; a_1, \dots, a_k, \beta_{k+1}] = \frac{p_k \beta_{k+1} + p_{k-1}}{q_k \beta_{k+1} + q_{k-1}}.$$

Hier setzen wir  $\beta_{k+1} = \frac{P_{k+1} + \sqrt{d}}{Q_{k+1}}$  ein und erhalten nach einer Umformung

$$dq_k - P_{k+1}p_k - Q_{k+1}P_{k-1} = (p_k - P_{k+1}q_k - Q_{k+1}q_{k-1})\sqrt{d}.$$

Auf der linken Seite steht eine rationale Zahl, rechts ein Vielfaches von  $\sqrt{d}$ , und demnach müssen beide Seiten 0 sein. Es folgt

$$-q_k(dq_k - P_{k+1}p_k - Q_{k+1}P_{k-1}) + p_k(p_k - P_{k+1}q_k - Q_{k+1}q_{k-1}) = 0,$$

und das impliziert...

$$p_k^2 - dq_k^2 = Q_{k+1}q_{k-1}p_k - Q_{k+1}p_{k-1}q_k = Q_{k+1} \cdot (-1)^{k+1}.$$

○

Wir sehen also schon einmal, dass im Falle  $Q_{k+1} = 1$  tatsächlich  $(p_k - q_k\sqrt{d})$  eine Einheit in  $\mathbb{Z}[\sqrt{d}]$  ist. Jetzt müssen wir noch dafür sorgen, dass irgendwann  $Q_{k+1}$  wirklich 1 ist, was ja zu  $\beta_{k+2} = \beta_1$  äquivalent ist. Also müssen wir auf jeden Fall irgendwie sehen, dass tatsächlich eine Periodizität eintritt, also die Menge der  $\beta_k$  endlich ist. Wir brauchen wieder einmal den Automorphismus  $\kappa$  von  $\mathbb{Q}(\sqrt{d})$ .

### Hilfssatz 3.4.11 Eine Beschränktheitsaussage

Für  $k \geq 1$  gilt  $\beta_k > 1$ ,  $-1 < \kappa(\beta_k) < 0$ .

*Beweis.* Nach Konstruktion ist  $\beta_k$  immer größer als 1. Für  $k = 1$  ist

$$\kappa(\beta_1) = \frac{1}{-\sqrt{d} - \lfloor \sqrt{d} \rfloor}$$

der Kehrwert einer Zahl, die offensichtlich kleiner ist als  $-2$ .

Induktiv folgt

$$-1 < \kappa(\beta_{k+1}) = \frac{1}{\kappa(\beta_k) - \lfloor \beta_k \rfloor} < 0.$$

○

### Hilfssatz 3.4.12 Eine Endlichkeitsaussage

Für  $k \geq 1$  gilt

$$0 < P_k < \sqrt{d}, \quad 0 < Q_k < 2\sqrt{d}.$$

*Beweis.*  $\beta_k = \frac{P_k + \sqrt{d}}{Q_k}$ ,  $\kappa(\beta_k) = \frac{P_k - \sqrt{d}}{Q_k}$ .

Wäre  $Q_k$  negativ, so wäre  $-\sqrt{d} + P_k > \sqrt{d} + P_k$ , was Quatsch ist.

Also ist  $Q_k$  positiv, und es folgt mit dem letzten Hilfssatz

$$\sqrt{d} - P_k < Q_k < P_k + \sqrt{d},$$

was  $P_k > 0$  impliziert.

Wegen  $\kappa(\beta_k) < 0$  muss dann  $P_k < \sqrt{d}$  gelten, und dann wegen  $P_k + \sqrt{d} > Q_k$  auch  $Q_k < 2\sqrt{d}$ . ○

Damit gibt es nur endlich viele Möglichkeiten für die  $\beta_k$ , und es gibt insbesondere ein  $k \geq 1, r \geq 1$ , sodass

$$\beta_r = \beta_{k+r}.$$

Um das für die Pellische Gleichung und vielleicht sonst noch etwas nutzen zu können, wäre es (siehe 3.4.9) schön, dies bereits für  $r = 1$  zu haben.

Die eleganteste Version, in der wir das sehen können, betrachtet die Kettenbruchentwicklung von  $\sqrt{d} + \lfloor \sqrt{d} \rfloor$ , die sich von der von  $\sqrt{d}$  nur an der nullten Stelle unterscheidet und dort den doppelten Eintrag hat.

### Satz 3.4.13 Zieleinlauf

Es gibt ein  $s \geq 1$ , sodass

$$\sqrt{d} + \lfloor \sqrt{d} \rfloor = \overline{[2a_0, a_1, a_2, \dots, a_s]}.$$

Insbesondere ist also

$$\sqrt{d} = [a_0; \overline{a_1, a_2, \dots, a_s, 2a_0}] \quad \text{und} \quad \beta_{s+2} = \beta_1.$$

*Beweis.* Wir setzen

$$y_k := \begin{cases} \frac{1}{\sqrt{d} - \lfloor \sqrt{d} \rfloor}, & k = 0, \\ \frac{Q_k}{\sqrt{d} - P_k}, & k \geq 1. \end{cases}$$

Für  $k \geq 1$  ist das  $\frac{-1}{\kappa(\beta_k)}$ , für  $k = 0$  ist das  $\frac{-1}{\kappa(\beta_0 + \lfloor \sqrt{d} \rfloor)}$ . Wir finden dann

$$y_{k+1} = \begin{cases} 2a_0 + \frac{1}{y_0}, & k = 0, \\ a_k + \frac{1}{y_k}, & k \geq 1. \end{cases}$$

Für  $k \geq 1$  etwa ist die linke Seite gleich  $\frac{Q_{k+1}}{\sqrt{d} - P_{k+1}}$ , die rechte Seite ist

$$a_k + \frac{\sqrt{d} - P_k}{Q_k} = \frac{P_{k+1} + \sqrt{d}}{Q_k},$$

und diese Ausdrücke stimmen überein. Für  $k = 0$  geht das ähnlich.

Wegen 3.4.11 ist  $y_k > 1$ , und das gilt auch für  $k = 0$ . Es folgt

$$\lfloor y_{k+1} \rfloor = \begin{cases} 2a_0, & k = 0, \\ a_k, & k \geq 1. \end{cases}$$

Nun sei  $r \in \mathbb{N}_0$  minimal derart, dass ein  $s \geq 1$  existiert mit  $y_{r+s} = y_r$ .

Annahme:  $r > 0$ . Dann ist aber

$$y_{r-1} = \frac{1}{y_r - \lfloor y_r \rfloor} = \frac{1}{y_{r+s} - \lfloor y_{r+s} \rfloor} = y_{r+s-1},$$

und  $r$  ist doch nicht minimal.

Also gibt es auch ein  $s > 0$  mit  $y_0 = y_s$ .

Das liefert die Periodizität der Kettenbruchentwicklung von  $\sqrt{d} + \lfloor \sqrt{d} \rfloor$ . ○

### Folgerung 3.4.14 Noch mal zur Pellischen Gleichung

Eine Lösung der Pellischen Gleichung findet man also konstruktiv und zielstrebig, indem man die Kettenbruchentwicklung von  $\sqrt{d}$  durchführt, bis man ein  $s$  sieht, für das  $\sqrt{d} = [a_0; \overline{a_1, a_2, \dots, a_s, 2a_0}]$  gilt. Dann ist

$$p_s^2 - dq_s^2 = (-1)^{s+1}.$$

### Bemerkung 3.4.15 Eine Anwendung

Eine der schwierigen Fragen der elementaren Zahlentheorie ist es, gute Verfahren zu finden, die Teiler einer gegebenen Zahl entdecken.

Wenn eine ungerade natürliche Zahl  $d = 2t + 1$  gegeben ist, dann ist sie immer eine Differenz zweier Quadratzahlen,  $d = r^2 - s^2 = (r - s)(r + s)$ , und wir finden

Teiler, die aber meistens triviale Teiler sein werden, denn die Standardwahl für  $r$  und  $s$  wird  $r = t + 1$ ,  $s = t$  sein.

Wenn  $d$  keine Quadratzahl ist, dann können wir immer noch in der Kettenbruchentwicklung von  $\sqrt{d}$  die Konvergenten anschauen. Ist zum Beispiel  $k$  ungerade und  $Q_k = 1$ , so folgt

$$p_k^2 - dq_k^2 = 1,$$

und  $p_k^2 - 1$  ist durch  $d$  teilbar. Der größte gemeinsame Teiler von  $p_k - 1$  und  $d$  könnte also ein nichttrivialer Teiler von  $d$  sein – auch wenn es dafür keine Garantie gibt.

Allgemeiner kann man eine Menge  $F$  endlich vieler Indizes betrachten, sodass

$$\prod_{f \in F} (-1)^{f+1} Q_{f+1}$$

eine Quadratzahl  $u^2$  ist. Dann ist wieder  $d$  ein Teiler von

$$\left( \prod_{f \in F} p_f \right)^2 - u^2,$$

und wir können den ggT von  $\prod_{f \in F} p_f - u$  und  $d$  ermitteln, der vielleicht ein nichttrivialer Teiler von  $d$  ist.

Von dieser Methode gibt es noch einige Varianten.

### Definition 3.4.16 Algebraische Zahlen

Eine komplexe Zahl heißt *algebraisch*, wenn sie Nullstelle eines nichttrivialen rationalen Polynoms ist.

Zum Beispiel sind die rationalen Zahlen selbst algebraisch, oder auch die Elemente eines quadratischen Zahlkörpers.

Nicht algebraische Zahlen heißen *transzendent*. Dazu gehören die Eulersche Zahl  $e$  oder die Kreiszahl  $\pi$ . Der Nachweis deren Transzendenz einfach, aber aufwendig. Eine Konsequenz ist zum Beispiel, dass sich  $\pi$  nicht mit Zirkel und Lineal konstruieren lässt, und damit die *Quadratur des Kreises* nicht mit den klassisch erlaubten Hilfsmitteln möglich ist.

### Hilfssatz 3.4.17 Unbezahlt

*Die Menge der algebraischen Zahlen ist abzählbar.*

*Beweis.* Jede algebraische Zahl ist Nullstelle eines ganzzahligen Polynoms, denn zunächst ist sie Nullstelle eines rationalen Polynoms  $f$ , und dies hat dieselben Nullstellen, wie das ganze Polynom, das durch Multiplikation von  $f$  mit einem gemeinsamen Nenner der Koeffizienten von  $f$  entsteht.

Nun sei für  $d \in \mathbb{N}$  die Menge  $P_d$  definiert als

$$P_d := \left\{ f = \sum_{i=0}^d a_i X^i \in \mathbb{Z}[X] \mid \max\{|a_i| \mid 0 \leq i \leq d\} \leq d \right\} \setminus \{0\}.$$

$P_d$  ist eine endliche Menge, sie hat genau  $(2d+1)^{d+1} - 1$  Elemente. Die Vereinigung der Mengen  $P_d$  ist ganz  $\mathbb{Z}[X] \setminus \{0\}$ , und daher ist die Menge der algebraischen Zahlen gleich

$$\bigcup_{d \in \mathbb{N}} \{ \alpha \in \mathbb{C} \mid \exists f \in P_d : f(\alpha) = 0 \}.$$

Da diese Mengen für jedes  $d$  endlich sind (denn jedes Polynom hat höchstens  $d$  Nullstellen) ist die Menge der algebraischen Zahlen die Vereinigung einer abzählbaren Familie von endlichen Mengen und damit abzählbar.  $\circ$

### Bemerkung 3.4.18 Cantor<sup>6</sup>

Vor 1880 war es nicht bekannt, dass es sinnvoll ist, verschiedene Typen der Unendlichkeit zu unterscheiden. Mit Cantors Nachweis, dass es überabzählbar viele reelle Zahlen gibt, sieht heute jedermann, dass es auch transzendente Zahlen geben muss. Es ist für diemeisten individuellen Zahlen sehr schwer, ihre Transzendenz nachzuweisen oder zu widerlegen. Interessanter Weise tut sich hier wieder eine Verbindung zur Diophantischen Approximation auf.

### Hilfssatz 3.4.19 Liouville<sup>7</sup>

*Es sei  $\alpha$  eine algebraische Zahl, die Nullstelle eines irreduziblen ganzen Polynoms vom Grad  $d$  ist.*

*Dann gibt es nur endlich viele teilerfremde ganze Zahlen  $p, q$ , sodass*

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^{d+1}}.$$

*Beweis.* Wenn  $\alpha$  rational ist, dann schreibe  $\alpha = \frac{k}{l}$ . Aus  $q\alpha \neq p$  folgt dann, dass

$$\left| \alpha - \frac{p}{q} \right| = \left| \frac{kq - pl}{ql} \right| > \frac{1}{ql},$$

also wird die Differenz höchstens dann kleiner als  $1/q^2$ , wenn  $q < l$  gilt. Es ist klar, dass es hier nur endlich viele Brüche geben kann, die  $\alpha$  mit der gewünschten Güte approximieren. Das erledigt den Fall rationaler Zahlen, also  $d = 1$ .

<sup>6</sup>Georg Cantor, 1845-1918

<sup>7</sup>Joseph Liouville, 1809-1882

Nun sei  $\alpha$  irrational, aber algebraisch. Dann gibt es ein irreduzibles Polynom  $f = \sum_{i=0}^d a_i X^i \in \mathbb{Z}[X]$  vom Grad  $d \geq 2$ ,  $a_d > 0$ , das  $\alpha$  als Nullstelle hat. Weiter seien  $p, q$  teilerfremde ganze Zahlen,  $q > 0$ . Dann ist  $f(\frac{p}{q}) \neq 0$ , denn ein irreduzibles Polynom hat keine rationale Nullstelle.

Es folgt ähnlich wie im ersten Fall

$$|f(\frac{p}{q})| = |\frac{\sum_{i=0}^d a_i p^i q^{d-i}}{q^d}| \geq \frac{1}{q^d},$$

denn der Zähler ist eine ganze Zahl und nicht 0.

Nun entwickeln wir  $f$  um  $\alpha$  und sehen

$$f(\frac{p}{q}) = \sum_{i=0}^d \frac{f^{(i)}(\alpha)}{i!} \cdot (\frac{p}{q} - \alpha)^i = \left( \sum_{i=1}^d \frac{f^{(i)}(\alpha)}{i!} \cdot (\frac{p}{q} - \alpha)^{i-1} \right) \cdot (\frac{p}{q} - \alpha).$$

Nun gibt es natürlich eine Konstante  $c$ , sodass für alle Zahlen  $\xi$  aus dem Intervall  $[-1, 1]$  die Ungleichung

$$\left| \sum_{i=1}^d \frac{f^{(i)}(\alpha)}{i!} \cdot \xi^{i-1} \right| < c$$

gilt.

Für  $|\alpha - \frac{p}{q}| \leq 1$  folgt also

$$|\alpha - \frac{p}{q}| > \frac{1}{c} \cdot |f(\frac{p}{q})| \geq \frac{1}{cq^d}.$$

Da wir für  $|\alpha - \frac{p}{q}| > 1$  bereits

$$|\alpha - \frac{p}{q}| > 1 \geq \frac{1}{q^n}$$

wissen, folgt die Existenz einer Konstante  $\tilde{c} > 0$ , sodass für alle  $p, q$  wie gehabt die Ungleichung

$$|\alpha - \frac{p}{q}| > \frac{\tilde{c}}{q^n}$$

gilt, was natürlich die ursprüngliche Behauptung zeigt und sogar verschärft.  $\circ$

### Beispiel 3.4.20 Eine transzendente Zahl

Zum Beispiel zeigt dieser Satz, dass eine Zahl wie

$$\alpha = \sum_{n \in \mathbb{N}} 10^{-n!}$$

transzendent ist. Denn es gibt für jedes  $d \in \mathbb{N}$  teilerfremde ganze Zahlen  $p, q$  mit  $|\alpha - \frac{p}{q}| < \frac{1}{q^d}$ .

Hier könnte man etwa  $q = \frac{1}{10^{d!}}$ ,  $\frac{p}{q} = \sum_{n=1}^d 10^{-n!}$  wählen.

**Bemerkung 3.4.21 Thue<sup>8</sup>-Siegel<sup>9</sup>-Roth<sup>10</sup>**

Der vorangehende Hilfssatz von Liouville lässt sich verschärfen, was sich aus einer Reihe von Arbeiten ergab, die in dem folgenden Resultat von Roth kulminierten:

*Wenn  $\alpha$  eine algebraische Zahl ist, dann gibt es für jedes  $\varepsilon > 0$  nur endlich viele teilerfremde  $p \in \mathbb{Z}$ ,  $q \in \mathbb{N}$ , sodass*

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

Für Roth brachte das 1958 die Fields-Medaille ein!

**Folgerung 3.4.22 Eine maßtheoretische Folgerung**

Es sei  $\Gamma \subseteq \mathbb{R}^2$  ein Gitter und  $K \subseteq \mathbb{R}^2$  ein Kompaktum mit stückweise glattem Rand, zum Beispiel der Einheitskreis.

Nun kann man versuchen, den Flächeninhalt von  $K$  dadurch zu ermitteln, dass man die Gitterpunkte in  $K$  zählt, jedem Gitterpunkt eine Kopie einer Fundamentalmasche anhängt, und dann schätzt, dass

$$\text{vol}(K) \approx |(K \cap \Gamma)| \cdot \text{cov}(\Gamma).$$

Das wird besser, wenn man  $\Gamma$  mit einem Faktor  $\frac{1}{2}$  kleiner macht, und nach besser, wenn man  $\Gamma$  noch weiter schrumpfen lässt, und tatsächlich kann man zeigen, dass

$$\text{vol}(K) = \lim_{\sigma \rightarrow 0^+} |(K \cap \sigma\Gamma)| \cdot \sigma^2 \text{cov}(\Gamma).$$

Die Phänomene, die am Rand von  $K$  auftreten könnten, werden durch dessen Kompaktheit und stückweise Glattheit unter Kontrolle gehalten.

Wenn nun  $K$  nicht mehr kompakt sein muss, dann wird es natürlich noch einmal spannend.

Als Beispiel nehmen wir das Folgende:

Es sei  $K = \{(x, y) \in \mathbb{R}^2 \mid x \geq 0, |y| \leq \min(\frac{1}{x^k}, x)\}$ , wobei  $k \geq 1$  fest gegeben sei. Dann ist das Volumen von  $K$  endlich, nämlich

$$\text{vol}(K) = \int_0^1 2x dx + \int_1^\infty \int \frac{2}{x^k} dx = 1 + \frac{2}{k-1}.$$

Nun sei  $\alpha \in \mathbb{R}$  irrational und  $\Gamma$  das Gitter, das von  $(0, 1)$  und  $(1, \alpha)$  erzeugt wird. Dann liegt

$$\left( \left( \begin{array}{c} m \\ n + m\alpha \end{array} \right) \right) \in \Gamma$$

---

<sup>8</sup>Axel Thue, 1863-1922

<sup>9</sup>Carl Ludwig Siegel, 1896-1981

<sup>10</sup>Klaus Friedrich Roth, geb. 1925

genau dann in  $K$ , wenn  $m = n = 0$  gilt oder wenn  $m > 0$  gilt und

$$|n + m\alpha| < \frac{1}{m^k}, \quad \text{also} \quad \left| \frac{n}{m} + \alpha \right| < \frac{1}{m^{1+k}}.$$

Der Satz von Roth sagt, dass das für algebraisches  $\alpha$  nur endlich oft passiert, und ähnlich sieht man, dass für jeden Skalierungsfaktor  $\sigma$  der Durchschnitt  $K \cap \sigma\Gamma$  endlich ist. Ein noch genauere Analyse zeigt, dass auch hier die Gleichheit

$$\text{vol}(K) = \lim_{\sigma \rightarrow 0^+} |(K \cap \sigma\Gamma)| \cdot \sigma^2 \text{cov}(\Gamma)$$

erfüllt ist.

Solche Phänomene treten häufig im Zusammenhang mit speziellen Werten von Zetafunktionen auf, wie sie etwa im Wechselspiel von hyperbolischer Geometrie und Zahlentheorie eine Rolle spielen.

Andererseits kann man durch Vorschrift der Kettenbruchentwicklung eine transzendente Zahl  $\alpha$  konstruieren, sodass für das zugehörige Gitter der Grenzwert  $\lim_{\sigma \rightarrow 0^+} |(K \cap \sigma\Gamma)| \cdot \sigma^2 \text{cov}(\Gamma)$  eine beliebige vorgegebene Zahl größer als das Volumen von  $K$  ist.

### Bemerkung 3.4.23 Zahlkörper

Zu guter Letzt will ich noch einen kleinen Hinweis auf die algebraische Zahlentheorie geben. Hier studiert man für algebraisches  $\alpha \in \mathbb{C}$  den kleinsten Teilkörper  $K = \mathbb{Q}(\alpha)$  von  $\mathbb{C}$ , der  $\alpha$  enthält. Wenn das Minimalpolynom  $f$  von  $\alpha$  Grad  $d$  hat, ist dies ein Vektorraum über  $\mathbb{Q}$  von Dimension  $d$ , und eine Basis besteht zum Beispiel aus

$$\{1, \alpha, \alpha^2, \dots, \alpha^{d-1}\}.$$

Quadratische Zahlkörper sind Beispiele hierfür, und zwar genau die Beispiele mit  $d = 2$ .

Die Menge  $\mathcal{O}_K$  aller ganz-algebraischen Zahlen in  $K$  ist wieder ein Ring, der als additive Gruppe frei vom Rang  $d$  ist.

Das Analogon zu unserem Satz 3.3.6 gilt auch hier, und es gibt nur endlich viele verschiedene Typen von Idealen in  $\mathcal{O}_K$ .

Das Analogon zum Struktursatz für die Einheitengruppe 3.2.6 ist hier, dass die Einheitengruppe von  $\mathcal{O}_K$  bis auf einen zyklischen Faktor frei abelsch ist, der Rang ist  $r + s - 1$ , wobei  $r$  die Anzahl der reellen Nullstellen von  $f$  ist, und  $2s$  die Anzahl der nichtreellen Nullstellen.

Im Fall  $K = \mathbb{Q}$  ist  $r = 1, s = 0$ . Im Falle eines reellquadratischen Zahlkörpers ist  $r = 2, s = 0$ , und im Falle eines imaginärquadratischen Zahlkörpers ist  $r = 0, s = 1$ .

Es gibt eine Formel, die sogenannte analytische Klassenzahlformel, die die Klassenzahl von  $K$  (Anzahl der Idealklassen) mit dem sogenannten *Regulator* verquickt, der sich aus einer Basis des freien Anteils der Einheitengruppe ergibt. Die weitere Zutat hier ist das Residuum der Dedekindschen Zetafunktion von  $K$  an der Stelle 1.

Es gibt eine ganze Reihe von Vermutungen, die versuchen, dieses Phänomen zu übertragen in andere Situationen. Die berühmteste davon ist die Vermutung von Birch<sup>11</sup> und Swinnerton-Dyer<sup>12</sup>, deren Behandlung ich aber anderen Vorlesungen überlasse.

---

<sup>11</sup>Brian Birch,

<sup>12</sup>Peter Swinnerton-Dyer

## INDEX

algebraisch	3.4.16
Äquivalenz (von Idealen)	3.3.1
arithmetische Funktion	1.4.7
Assoziiertheit	1.2.9
Basis (einer abelschen Gruppe)	1.5.1
Charakteristik	2.2.3
Chinesischer Restsatz	2.1.12
Diophantische Gleichung	1.5.12
Diskriminante	3.1.8
Elementarteilersatz	1.5.7, 1.5.9
Euklidischer Algorithmus	1.2.2, 1.2.4
Euklidischer Ring	1.2.16
Eulers $\varphi$ -Funktion	2.1.10
Faktorgruppe	2.1.2
Faltung	1.4.7
frei abelsche Gruppe	1.5.1
Fundamentalmasche	3.2.2
ganze Zahlen	1.1.3, 1.1.4
ganz über $\mathbb{Z}$	3.1.6
Ganzheitsring	3.1.6
Gitter	3.2.1
größter gemeinsamer Teiler	1.2.1, 1.2.11
Halbsystem	2.3.5
Hauptideal, Hauptidealring	1.2.14
Homomorphiesatz	2.1.2, 2.1.8
Ideal	1.2.14
imaginärquadratisch	3.1.3
Index	2.1.4
Inhalt	1.5.5
irreduzibel	1.3.8
Kettenbruch	3.4.2
Klassengruppe	3.3.3
kleiner Satz von Fermat	2.1.7, 2.1.9
kleinstes gemeinsames Vielfaches	1.2.1
Kongruenz	2.1.1
Konvergente	3.4.2
Kovolumen	3.2.2
Kreisteilungspolynom	2.2.6
Legendre-Symbol	2.3.2

Minkowskis Gitterpunktsatz	3.2.3
Möbius-Inversionsformel	1.4.8
(strikt) multiplikativ	1.4.7
natürliche Zahlen	1.1.1
Norm	3.1.5
$p$ -adische Bewertung	1.3.5
Primelement	1.3.8
Primideal	3.1.14
primitiver Vektor	1.5.5
primitives Element	2.2.3
Primzahl	1.3.1
Primzahlsatz	1.4.6
Produkt zweier Ideale	3.3.3
Pseudoprimzahl	2.1.11
quadratischer Zahlkörper	3.1.1
quadratisches Reziprozitätsgesetz	2.3.8
Rang	1.5.2
rationale Zahlen	1.1.5
reelle Zahlen	1.1.7
reellquadratisch	3.1.3
Restklassenring	2.1.8
Sieb des Eratosthenes	1.4.3
Spur	3.1.5
Teiler	1.2.1, 1.2.8
teilerfremd	1.2.1, 1.2.11
unimodulare Matrizen	1.5.4