Algebraische Zahlentheorie I

Prof. Dr. Alexander Schmidt

Wintersemester 2021/22

Inhaltsverzeichnis

0tens: Begriffe aus der Algebra:

- Ring, hier immer kommutativ mit 1
- R-Modul, $R \times M \to M$
- Ideal: $\mathfrak{a} \subset R$, R-Untermodul
- $x \in R \rightsquigarrow (x) = Rx = \{rx \mid r \in R)$ das von x erzeugte Hauptideal
- R heißt nullteilerfrei: wenn $xy = 0 \Rightarrow x = 0$ oder $y = 0$
- Einheitengruppe: $R^\times = \{r \in R \mid \exists\, s \in R : rs = 1\}$
- R nullteilerfrei: $(x) = (y) \iff x = ey$, $e \in R^\times$
- $\mathfrak{p} \subset R$ heißt Primideal $\iff R/\mathfrak{p}$ nullteilerfrei
- $\mathfrak{m} \subset R$ Maximalideal $\iff R/\mathfrak{m}$ Körper
- $f : R \to R'$ Ringhomomorphismus und $\mathfrak{p}' \subset R'$ Primideal $\Rightarrow f^{-1}(\mathfrak{p}') \subset R'$ Primideal (gilt nicht für Maximalideal).
- jeder Ring $\neq 0$ besitzt ein Maximalideal
- jedes Ideal $\neq R$ ist in einem Maximalideal enthalten
- jede Nichteinheit ist in einem Maximalideal enthalten
- $a, b \in R$, $a \mid b \overset{\text{df}}{=}$ es existiert ein $c \in R$ mit $ac = b \iff (b) \subset (a)$
- $a \mathrel{\hat{=}} b$ (assoziiert) $\overset{\text{df}}{=} a \mid b$ und $b \mid a \iff (a) = (b)$, R nullteilerfrei: $a \mathrel{\hat{=}} b \iff a = be$, $e \in R^\times$.

Definition 0.1. Sei R nullteilerfrei und $a, b \in R$. Ein Element $d \in R$ heißt **größter gemeinsamer Teiler** von a und b, wenn gilt

(i) $d \mid a$ und $d \mid b$
(ii) $(e \mid a$ und $e \mid b)) \Rightarrow e \mid d$.

Der ggT ist, wenn er existiert, bis auf Assoziiertheit eindeutig.

Definition 0.2. R heißt **Hauptidealring** wenn R nullteilerfrei ist, und jedes Ideal in R ist ein Hauptideal.

Bemerkung 0.3. Ist R ein Hauptidealring so existiert der ggT und es gilt

$$(a) + (b) = (\mathrm{ggT}(a, b)).$$

Insbesondere läßt sich $\mathrm{ggT}(a, b)$ linear aus a und b kombinieren. (Erinnerung: $\mathfrak{a} + \mathfrak{b} = \{\alpha + \beta \mid \alpha \in \mathfrak{a},\ \beta \in \mathfrak{b}\}$

Begründung: $(a)+(b) = (d)$ für ein $d \in R$, weil R Hauptidealring. Es gilt also $d|a$, $d|b$. Gilt nun $e|a$ und $e|b$, so folgt $(a) \subset (e)$ und $(b) \subset (e)$ also $(d) = (a) + (b) \subset (e) \Rightarrow e|d$ □

Definition 0.4. Ein nullteilerfreier Ring R heißt **euklidisch**, wenn es eine Funktion $\nu : R \setminus \{0\} \to \mathbb{N}$ gibt, so dass zu $a, b \in R$, $b \neq 0$ stets $q, r \in R$ mit $a = qb + r$ und $r = 0$ oder $\nu(r) < \nu(b)$ gibt $\rightsquigarrow$ erhalten („Euklidischen“) Algorithmus zur Bestimmung des ggT.

Satz 0.5. *(LA 2) Jeder euklidische Ring ist ein Hauptidealring.*

Definition 0.6. R nullteilerfrei $\pi \in R \setminus (\{0\} \cup R^\times)$ heißt

- Primelement, wenn (π) Primideal
- irreduzibel, falls $\pi = ab \Rightarrow a \in R^\times$ oder $b \in R^\times$.

Bemerkung 0.7. Primelemente sind irreduzibel

Grund: $\pi = ab \Rightarrow \pi \mid a$ oder $\pi \mid b$. Gelte OE $\pi \mid a$. Wegen $a \mid \pi$ gilt $a \hat{=} \pi$, also $a = \pi u$, $u \in R^\times$. Nun gilt $\pi = ab = \pi ub$, also $\pi(1 - ub) = 0 \Rightarrow 1 = ub \Rightarrow b \in R^\times$.

Definition 0.8. R (nullteilerfrei) heißt **faktoriell**, wenn jedes $a \in R\backslash\{0\}$ eine bis auf Einheiten und Reihenfolge eindeutige Zerlegung in das Produkt irreduzibler Elemente besitzt.

Satz 0.9. *(i) In einem faktoriellen Ring ist jedes irreduzible Element Primelement. (Algebra 1, 2.20)*

(ii) Hauptidealringe sind faktoriell. (LA 2)

(iii) R faktoriell $\Rightarrow R[T]$ faktoriell. (Algebra 1, 2.42)

Sei R ein Ring und $\mathfrak{a} \subset R$ ein Ideal. Die Elemente des Faktorrings $R/\mathfrak{a}$ heißen Restklassen modulo $\mathfrak{a}$. Die Gruppe $(R/\mathfrak{a})^\times$ heißt Gruppe der *primen Restklassen* modulo $\mathfrak{a}$. Für $\mathfrak{a}, \mathfrak{b} \subset R$ gilt

$$\mathfrak{a}\mathfrak{b} \stackrel{df}{=} \left\{ \sum_{\text{endl.}} a_i b_i \mid a_i \in \mathfrak{a},\ b_i \in \mathfrak{b} \right\}.$$

$\mathfrak{a}$ und $\mathfrak{b}$ heißen teilerfremd (auch koprim), wenn $\mathfrak{a} + \mathfrak{b} = (1)$ gilt.

Lemma 0.10. *(Algebra 2, 1.15 (ii)) Es gilt*

$$(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) \subset \mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}.$$

Insbesondere gilt $\mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}$ falls $\mathfrak{a}$ und $\mathfrak{b}$ teilerfremd sind.

Seien $R_1, \ldots, R_n$ Ringe. Dann ist $R = \prod_{i=1}^{n} R_i$ mit komponentenweiser Addition und Multiplikation ein Ring. Sei R ein Ring und $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subset R$ Ideale. Wir betrachten den Ringhomomorphismus

$$\phi : R \longrightarrow \prod_{i=1}^{n} R/\mathfrak{a}_i$$

der durch $r \mapsto (r + \mathfrak{a}_1, \ldots, r + \mathfrak{a}_n)$ gegeben ist.

Satz 0.11. *(Algebra 2, 1.16)*

(i) *Sind die* $\mathfrak{a}_i$ *paarweise relativ prim, so gilt* $\prod_{i=1}^{n} \mathfrak{a}_i = \bigcap_{i=1}^{n} \mathfrak{a}_i$.

(ii) ϕ *ist surjektiv* $\Longleftrightarrow$ *die* $\mathfrak{a}_i$ *sind paarweise relativ prim.*

(iii) ϕ *ist injektiv* $\Longleftrightarrow \bigcap \mathfrak{a}_i = (0)$.

Als Korollar erhält man:

Chinesischer Restklassensatz: *Seien* $r_1, \ldots, r_n \in R$ *und* $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subset R$ *paarweise teilerfremde Ideale. Dann hat das System von Kongruenzen*

$$\begin{aligned} x &\equiv r_1 \mod \mathfrak{a}_1 \\ &\vdots \\ x &\equiv r_n \mod \mathfrak{a}_n \end{aligned}$$

eine Lösung $x \in R$ *und* x *ist eindeutig bestimmt modulo* $\mathfrak{a}_1 \cdots \mathfrak{a}_n$.

Beweis. Dies ist eine Umformulierung der Tatsache, dass unter den gegebenen Bedingungen $R/(\mathfrak{a}_1 \cdots \mathfrak{a}_n) \longrightarrow \prod_{i=1}^{n} R/\mathfrak{a}_i$ ein Isomorphismus ist. □

1 Elementare Zahlentheorie

1.1 Primzahlen

Notation:
$\mathbb{N} = 1, 2, \ldots$
$\mathbb{N}_0 = 0, 1, 2, \ldots$

Definition 1.1. Eine **Primzahl** ist eine natürliche Zahl $p > 1$ die nur durch 1 und sich selbst teilbar ist.
M.a.W.: Primzahlen sind die positiven irreduziblen Elemente in $\mathbb{Z}$.

Division mit Rest ganzer Zahlen ist wohlbekannt, man erhält daher:

Lemma 1.2. *Die Funktion*

$$\nu : \mathbb{Z} \setminus \{0\} \longrightarrow \mathbb{N}, \qquad a \longmapsto |a|,$$

ist eine euklidische Normfunktion. Insbesondere ist $\mathbb{Z}$ ein Hauptidealring und faktoriell.

Satz 1.3. *Es gibt unendlich viele Primzahlen.*

Beweis. Angenommen es gäbe nur endlich viele und sei P ihr Produkt. Dann ist $P + 1$ durch keine Primzahl teilbar. Widerspruch. □

Frage: Haben wir jetzt gezeigt, dass es in jedem faktoriellen Ring unendlich viele Primelemente gibt?

Antwort: Nein, $P + 1$ könnte eine Einheit sein!

Lemma 1.4. $\mathbb{Z}^\times = \{\pm 1\}$.

Zum Beweis brauchen wir, dass auf $\mathbb{Z}$ eine Anordnung existiert, d.h. die „$\leq$“-Relation mit ihren bekannten Eigenschaften (vgl. Algebra 1, 6.22).
Außerdem brauchen wir: Zu $a \in \mathbb{Z}$ gibt es keine ganze Zahl b mit $a < b < a + 1$.

Beweis von Lemma 1.4. Seien $a, b \in \mathbb{Z}$ mit $ab = 1$. Dann gilt $0 \neq a$, $0 \neq b$. Wäre $a > 1$, so gilt $b > 0$ (sonst $ab < 0$) also $b \geq 1$ und dann $ab > 1 \cdot b = b \geq 1 \Rightarrow 1 > 1$ Widerspruch.
Wäre $a < -1$, so gilt $b < 0$ (sonst $ab < 0$) also $b \leq -1$ und

$$-ab = a(-b) < (-1)(-b) = b \leq -1$$

also $-1 < -1$ Widerspruch. □

Erinnerung:

$$\sum_{n\in\mathbb{N}} \frac{1}{n} = \infty, \qquad \sum_{n\in\mathbb{N}} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

Satz 1.5.

$$\sum_{p \text{ Primzahl}} \frac{1}{p} = \infty.$$

Bemerkung 1.6. Es gibt also „mehr“ Primzahlen als Quadratzahlen.

Beweis. Die Folge $\left(1+\frac{1}{n}\right)^n$ konvergiert von unten gegen e. Insbesondere gilt $\left(1+\frac{1}{p-1}\right)^{p-1} < e$, also $\log\left(1+\frac{1}{p-1}\right) < \frac{1}{p-1} = \frac{1}{p} + \frac{1}{p(p-1)}$. Wegen $\frac{1}{1-\frac{1}{p}} = 1 + \frac{1}{p-1}$ gilt für jedes $N \in \mathbb{N}$:

$$\begin{aligned} \log \prod_{p\le N} \tfrac{1}{1-\frac{1}{p}} &= \sum_{p\le N} \log\left(1+\tfrac{1}{p-1}\right) \\ &< \sum_{p\le N} \tfrac{1}{p} + \sum_{p\le N} \tfrac{1}{p(p-1)}. \end{aligned}$$

Wir setzen: $p_+(1) = 0$ und für $n \ge 2$: $p_+(n) =$ größter Primteiler von n. Mithilfe der geometrischen Reihe $\frac{1}{1-\frac{1}{p}} = 1 + \frac{1}{p} + \frac{1}{p^2} + \dots$ erhalten wir

$$\begin{aligned} \prod_{p\le N} \tfrac{1}{1-\frac{1}{p}} = \prod_{p\le N} (1 + \tfrac{1}{p} + \tfrac{1}{p^2} + \dots) &= \sum_{p_+(n)\le N} \tfrac{1}{n} \\ \ge \sum_{n=1}^{N} \tfrac{1}{n} \ge \int_1^{N+1} \tfrac{dx}{x} &= \log(N+1). \end{aligned}$$

Zusammen:

$$\log\log(N+1) < \sum_{p\le N} \frac{1}{p} + \sum_{p\le N} \frac{1}{p(p-1)}.$$

Nun gilt:

$$\sum_{p\le N} \frac{1}{p(p-1)} \le \sum_{n=2}^{\infty} \frac{1}{n(n-1)} = \sum_{n=2}^{\infty} \frac{1}{n-1} - \frac{1}{n} = 1,$$

also

$$\log\log(N+1) - 1 < \sum_{p\le N} \frac{1}{p}.$$

□

Lemma 1.7. *In $\mathbb{N}$ gibt es beliebig große primzahlfreie Teilabschnitte.*

Beweis. Für jedes $n \in \mathbb{N}$ ist unter den n Zahlen

$$(n+1)!+2, (n+1)!+3, \dots, (n+1)!+n+1$$

keine Primzahl. □

Bemerkung 1.8. Sei $\pi(n) =$ Anzahl der Primzahlen $\le n$. Dann gilt

$$\lim_{n\to\infty} \frac{\pi(n)}{\frac{n}{\log(n)}} = 1.$$

1.2 Die Eulersche φ-Funktion

Definition 1.9. (Eulersche φ-Funktion). Für $n \in \mathbb{N}$ ist

$$\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times.$$

Lemma 1.10. $(n,m) = 1 \Longrightarrow \varphi(nm) = \varphi(n)\varphi(m)$.

Beweis. Nach gilt $\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, also
$(\mathbb{Z}/nm\mathbb{Z})^\times \cong (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$. □

Lemma 1.11. *Für $a \in \mathbb{Z}$, $n > 1$ bezeichne $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ die Restklasse von a* mod *n. Dann gilt*

$$\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times \iff \text{ggT}\,(a,n) = 1.$$

Beweis. Sei $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ und $b \in \mathbb{Z}$ so dass $\bar{a}\bar{b} = 1$. Dann gilt $ab = 1 + cn$, $c \in \mathbb{Z}$, also $\text{ggT}(a,n) \mid 1$.

Gilt $\text{ggT}(a,n) = 1$, so existieren $\alpha, \beta \in \mathbb{Z}$ mit $\alpha a + \beta n = 1$ (lineare Kombinierbarkeit des ggT in Hauptidealringen). Dann gilt $\bar{\alpha}\bar{a} = \bar{1}$, also $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. □

Korollar 1.12. *Sei p eine Primzahl. Dann gilt: $\varphi(p^k) = (p-1)p^{k-1}$.*

Beweis. Unter den p^k Restklassen $\overline{1}, \overline{2}, \ldots, \overline{p^k}$ sind genau die p^{k-1} Restklassen: $\overline{p}, \overline{2p}, \ldots, \overline{p^{k-1}p}$ nicht prim. Also $\varphi(p^k) = p^k - p^{k-1} = (p-1)p^{k-1}$. □

Korollar 1.13. *Für $n = \prod_{i=1}^{r} p_i^{e_i}$ gilt $\varphi(n) = \prod_{i=1}^{r} (p-1)p^{e_i-1}$.*

Bemerkung 1.14. Die Erweiterung $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ (hier: $\zeta_n = e^{2\pi i/n}$) ist vom Grad $\varphi(n)$ mit Galoisgruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ (siehe Algebra 1, 4.47).

Satz 1.15. *Für jede natürliche Zahl m gilt: $\sum_{d|m} \varphi(d) = m$.*

Beweis. Induktion über die Anzahl der verschiedenen Primteiler von m.
$m = 1$ (0 Primteiler). Die Aussage ist trivial (bzw. formal).
Induktionsschritt: $m = np^e$, p Primzahl $n, e \in \mathbb{N}$, $p \nmid n$. Jeder Teiler von m hat eine eindeutige Darstellung der Form dp^i mit $d \mid n$ und $0 \le i \le e$. Wir erhalten

$$\begin{aligned}
\sum_{d|m} \varphi(d) &= \sum_{d|n} \varphi(d) + \sum_{d|n} \varphi(dp) + \cdots + \sum_{d|n} \varphi(dp^e) \\
&= n + n\varphi(p) + \cdots + n\varphi(p^e) \\
&= n(1 + (p-1)p^0 + \cdots + (p-1)p^{e-1}) \\
&= np^e = m.
\end{aligned}$$

□

Bemerkung 1.16. Das Minimalpolynom $\Phi_m(X)$ von ζ_m über $\mathbb{Q}$ heißt das *m-te Kreisteilungspolynom*. Da jede m-te Einheitswurzel primitive d-te Einheitswurzel für genau einen Teiler d von m ist, gilt

$$X^m - 1 = \prod_{d|m} \Phi_d(X)$$

(siehe Algebra 1, §4.5). Grade auswerten liefert einen alternativen Beweis von Satz 1.15.

Satz 1.17 (Kleiner Fermatscher Satz). *Für $(a, m) = 1$ gilt*

$$a^{\varphi(m)} \equiv 1 \mod m$$

Beweis. Es gilt $\bar{a} \in (\mathbb{Z}/m\mathbb{Z})^\times$ und somit gilt $\mathrm{ord}(a) \mid \#(\mathbb{Z}/m\mathbb{Z})^\times = \varphi(m)$. Also folgt $\bar{a}^{\varphi(m)} = \bar{1}$ in $\mathbb{Z}/m\mathbb{Z}$. □

Korollar 1.18. *$a \in \mathbb{Z}$, p Primzahl $\Rightarrow a^p \equiv a \mod p$.*

Beweis. $(a, p) = 1 \Rightarrow a^{p-1} = a^{\varphi(p)} \equiv 1 \mod p \Rightarrow a^p \equiv a$. Ansonsten gilt $p \mid a$ und daher $a^p \equiv 0 \equiv a \mod p$ □

Definition 1.19. $a \in \mathbb{Z}$ heißt **primitive Wurzel** modulo einer Primzahl p, wenn die Restklassen $\bar{a}, \bar{a}^2, \ldots, \bar{a}^{p-1} = 1$ alle Restklassen $\neq 0 \mod p$ durchlaufen.

Satz 1.20 (Gauß). *Es existieren primitive Wurzeln modulo p.*

Beweis. $\mathbb{Z}/p\mathbb{Z}$ ist ein endlicher Körper. Daher ist $(\mathbb{Z}/p\mathbb{Z})^\times$ zyklisch (Algebra 1, 3.103). Wähle $a \in \mathbb{Z}$ so dass $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$ ein Erzeuger ist. □

2 Das Quadratische Reziprozitätsgesetz

Das Quadratische Reziprozitätsgesetz (QRG) wurde von Euler vermutet und zuerst von Gauss bewiesen. Es ist einer der wichtigsten Sätze der klassischen Zahlentheorie. Es setzt die Frage, ob eine Primzahl p quadratischer Rest modulo einer Primzahl q ist, in Beziehung zu der „reziproken“ Frage, ob q quadratischer Rest modulo p ist. Ein solcher Zusammenhang ist erstaunlich und tiefliegend, da eine Aussage über Reste modulo q mit einer über Reste modulo p verknüpft wird. Das Quadratische Reziprozitätsgesetz ist von *globaler* Natur, d.h. nicht durch Rechnen mit Restklassen modulo einer festen Zahl zu verstehen. Ein tieferes Verständnis des QRG erhält man erst im Rahmen seiner modernen Verallgemeinerung, der *Klassenkörpertheorie*.

2.1 Quadratische Reste modulo p

Im Folgenden bezeichne p stets eine von 2 verschiedene Primzahl.

Definition 2.1. Eine ganze Zahl a (bzw. ihre Restklasse modulo p) heißt **quadratischer Rest** modulo p, wenn $p \nmid a$ und $\bar{a} = \bar{b}^2 \in \mathbb{Z}/p\mathbb{Z}$ für ein $b \in \mathbb{Z}$. Wenn $p \nmid a$ und a kein quadratischer Rest ist, dann heißt a **quadratischer Nichtrest**.

Definition 2.2. Für $a \in \mathbb{Z}$ ist das **Legendre-Symbol** $\left(\frac{a}{p}\right)$ folgendermaßen definiert:

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & \text{wenn } a \text{ quadratischer Rest } \bmod p, \\ 0, & \text{wenn } p \mid a, \\ -1, & \text{wenn } a \text{ quadratischer Nichtrest } \bmod p. \end{cases}$$

Aus $a \equiv b \bmod p$ folgt offenbar $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. Wir benutzen daher auch die Notation $\left(\frac{\bar{a}}{p}\right)$, d.h. wir fassen das Legendre-Symbol als Funktion auf den Restklassen modulo p auf. Wir sagen, eine ganze Zahl g sei primitive Wurzel modulo p, wenn ihre Restklasse $\bar{g} \in \mathbb{Z}/p\mathbb{Z}$ eine primitive Wurzel ist.

Lemma 2.3. *Sei g eine primitive Wurzel modulo p. Dann gilt für $r \in \mathbb{N}$*

$$\left(\frac{g^r}{p}\right) = (-1)^r.$$

Beweis. Zu zeigen ist: g^r ist quadratischer Rest $\iff 2|r$.
($\Longrightarrow$): Sei $\bar{g}^r = \bar{h}^2$. Dann ist $\bar{h} = \bar{g}^n$ für ein n. Also ist $\bar{g}^r = \bar{g}^{2n}$. Es gilt somit $p - 1 = \mathrm{ord}(\bar{g}) \mid (r - 2n)$ und folglich ist r gerade.
($\Longleftarrow$): Ist r gerade, so gilt $\bar{g}^r = (\bar{g}^{r/2})^2$. □

Korollar 2.4. *In $\mathbb{Z}/p\mathbb{Z}$ gibt es genau $\frac{p-1}{2}$ quadratische Reste und $\frac{p-1}{2}$ quadratische Nichtreste.*

Beweis. Die Werte g^r, $r = 1, \ldots, p-1$, durchlaufen genau die primen Restklassen modulo p. Nach Lemma 2.3 sind die quadratischen Reste genau die Werte mit geradem Exponenten und die quadratischen Nichtreste genau die Werte mit ungeradem Exponenten. □

Nun zeigen wir die Multiplikativität des Legendre-Symbols.

Satz 2.5.

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Beweis. Es gilt die Implikation $p|ab \Longrightarrow p|a$ oder $p|b$. Daher ist die linke Seite der Gleichung genau dann gleich Null, wenn es die rechte ist. Sei g eine primitive Wurzel modulo p. Sind a und b nicht durch p teilbar, so existieren r, s mit $\bar{a} = \bar{g}^r$, $\bar{b} = \bar{g}^s$, und es gilt

$$\left(\frac{ab}{p}\right) = \left(\frac{g^{r+s}}{p}\right) = (-1)^{r+s}$$

$$= (-1)^r(-1)^s = \left(\frac{g^r}{p}\right)\left(\frac{g^s}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

□

Korollar 2.6. *Das Produkt zweier quadratischer Nichtreste ist ein quadratischer Rest.*

Beweis. Sind a und b quadratische Nichtreste, so gilt $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = (-1)(-1) = 1$. Daher ist ab quadratischer Rest. □

Mit Hilfe des Legendre-Symbols können wir das Lösungsverhalten quadratischer Gleichungen modulo p angeben.

Satz 2.7. *Die quadratische Gleichung $X^2 + aX + b = 0$ hat modulo p*

- *genau zwei verschiedene Lösungen,* *wenn* $\left(\frac{a^2-4b}{p}\right) = +1$,
- *genau eine Lösung,* *wenn* $\left(\frac{a^2-4b}{p}\right) = 0$,
- *keine Lösung,* *wenn* $\left(\frac{a^2-4b}{p}\right) = -1$.

Beweis. Da p als ungerade vorausgesetzt ist, können wir Restklassen modulo p durch 2 teilen. Die gegebene Gleichung ist äquivalent zu

$$\left(X + \frac{a}{2}\right)^2 - \frac{a^2}{4} + b \equiv 0 \mod p$$

bzw. zu

$$(2X + a)^2 \equiv a^2 - 4b \mod p.$$

Hieraus folgt die Behauptung. □

Wegen $p > 2$ sind die Restklassen modulo p der Zahlen -1, 0 und 1 paarweise verschieden. Daher ist das Legendre-Symbol bereits durch seine Restklasse modulo p eindeutig bestimmt. Diese berechnet sich wie folgt.

Satz 2.8 (Euler)**.** *Für $a \in \mathbb{Z}$ gilt*

$$\overline{\left(\frac{a}{p}\right)} = \bar{a}^{\frac{p-1}{2}} \qquad \text{in } \mathbb{Z}/p\mathbb{Z}.$$

Beweis. Ist a durch p teilbar, so sind beide Seiten gleich Null. Also können wir $p \nmid a$ annehmen. Wegen $(\bar{a}^{\frac{p-1}{2}})^2 = \bar{a}^{p-1} = \bar{1}$ nimmt $\bar{a}^{\frac{p-1}{2}}$ nur die Werte $+\bar{1}, -\bar{1}$ an, und wir müssen zeigen: $\left(\frac{a}{p}\right) = 1 \iff \bar{a}^{\frac{p-1}{2}} = \bar{1}$.

($\Longrightarrow$): Ist $\left(\frac{a}{p}\right) = 1$, so ist $\bar{a} = \bar{b}^2$ für ein b. Also ist $\bar{a}^{\frac{p-1}{2}} = \bar{b}^{p-1} = \bar{1}$.

($\Longleftarrow$): Sei g eine primitive Wurzel und $\bar{a} = \bar{g}^r$. Dann gilt $\bar{g}^{r\frac{p-1}{2}} = \bar{1}$, also $(p-1) \mid r\frac{p-1}{2}$, weshalb r gerade ist. Dann ist $\left(\frac{a}{p}\right) = (-1)^r = 1$. □

2.2 Das Quadratische Reziprozitätsgesetz

Theorem 2.9 (Quadratisches Reziprozitätsgesetz)**.** *Es seien $p, q > 2$ Primzahlen. Dann gilt*

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right).$$

Mit anderen Worten: Ist eine der beiden Primzahlen p und q kongruent 1 modulo 4, so gilt $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$. Im verbleibenden Fall gilt $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

Bevor wir das QRG beweisen, formulieren wir noch seine zwei sogenannten Ergänzungssätze. Mit Hilfe des QRG und seiner Ergänzungssätze kann man dann die Legendre-Symbole $\left(\frac{a}{p}\right)$ bequem ausrechnen.

Theorem 2.10 (1. Ergänzungssatz zum QRG)**.**

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Mit anderen Worten: -1 ist genau dann quadratischer Rest modulo einer Primzahl p, wenn p kongruent 1 modulo 4 ist.

Theorem 2.11 (2. Ergänzungssatz zum QRG)**.**

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Mit anderen Worten: 2 ist genau dann quadratischer Rest modulo einer Primzahl p, wenn p kongruent ± 1 modulo 8 ist.

Zum Beweis des QRG benötigen wir das sogenannte Gauß-Lemma. Sei

$$H = \left\{\bar{1}, \bar{2}, \ldots, \overline{\frac{p-1}{2}}\right\}.$$

Dann hat jedes Element aus $(\mathbb{Z}/p\mathbb{Z})^\times$ die Gestalt $\pm\bar{h}$ mit $\bar{h} \in H$. Sei nun $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$ ein fixiertes Element. Dann erhalten wir Gleichungen der folgenden Form

$$\begin{array}{rcll}
\bar{a}\cdot\bar{1} & = & \varepsilon_1\cdot\bar{h}_1, & \bar{h}_1 \in H, \varepsilon_1 \in \{+1,-1\} \\
\bar{a}\cdot\bar{2} & = & \varepsilon_2\cdot\bar{h}_2, & \bar{h}_2 \in H, \varepsilon_2 \in \{+1,-1\} \\
\vdots & & \vdots & \vdots \\
\bar{a}\cdot\overline{\frac{p-1}{2}} & = & \varepsilon_{\frac{p-1}{2}}\cdot\bar{h}_{\frac{p-1}{2}}, & \bar{h}_{\frac{p-1}{2}} \in H, \varepsilon_{\frac{p-1}{2}} \in \{+1,-1\}.
\end{array}$$

Lemma 2.12 (Gauß-Lemma). $$\left(\frac{a}{p}\right) = \prod_{i=1}^{\frac{p-1}{2}} \varepsilon_i.$$

Beweis. Zunächst zeigen wir, dass die $\bar{h}_i$ paarweise verschieden sind. Wäre nämlich $\bar{h}_i = \bar{h}_j$, so schließt man $\bar{a}^2\bar{i}^2 = \bar{a}^2\bar{j}^2$, also $\bar{i}^2 = \bar{j}^2$, also $\bar{i} = \pm\bar{j}$. Wegen $\bar{i}, \bar{j} \in H$ folgt $i = j$. Also taucht jedes Element aus H genau einmal als $\bar{h}_i$ auf, und wir erhalten

$$\bar{a}^{\frac{p-1}{2}} \cdot \prod_{i=1}^{\frac{p-1}{2}} \bar{i} = \prod_{i=1}^{\frac{p-1}{2}} \varepsilon_i \cdot \prod_{i=1}^{\frac{p-1}{2}} \bar{h}_i = \prod_{i=1}^{\frac{p-1}{2}} \varepsilon_i \cdot \prod_{i=1}^{\frac{p-1}{2}} \bar{i}\ .$$

Teilen wir beide Seiten durch $\prod_{i=1}^{\frac{p-1}{2}} \bar{i}$ und wenden Satz 2.8 an, erhalten wir

$$\overline{\left(\frac{a}{p}\right)} = \bar{a}^{\frac{p-1}{2}} = \overline{\left(\prod_{i=1}^{\frac{p-1}{2}} \varepsilon_i\right)} \quad \text{in } \mathbb{Z}/p\mathbb{Z},$$

was wegen $p \geq 3$ die Behauptung zeigt. □

Beweis des QRG und seiner Ergänzungssätze. 1. Schritt: Satz 2.8 für $a = -1$ impliziert die Behauptung des 1. Ergänzungssatzes.

2. Schritt: Wir schreiben für $1 \leq i \leq \frac{p-1}{2}$

$$a \cdot i = \varepsilon_i \cdot h_i + e_i \cdot p$$

mit $1 \leq h_i \leq \frac{p-1}{2}$, $\varepsilon_i \in \{\pm 1\}$ und $e_i \in \mathbb{Z}$. Ist $\varepsilon_i = +1$, so gilt $2ai = 2h_i + 2e_ip$ und daher

$$\frac{2ai}{p} = \frac{2h_i}{p} + 2e_i.$$

Folglich gilt

$$\left[\frac{2ai}{p}\right] = 2e_i,$$

und $\left[\frac{2ai}{p}\right]$ ist in diesem Fall eine gerade ganze Zahl. Ist $\varepsilon_i = -1$, so gilt $2ai = p - 2h_i + (2e_i - 1)p$, und daher

$$\frac{2ai}{p} = \frac{p - 2h_i}{p} + 2e_i - 1.$$

Folglich gilt

$$\left[\frac{2ai}{p}\right] = 2e_i - 1,$$

und $\left[\frac{2ai}{p}\right]$ ist in diesem Fall eine ungerade ganze Zahl. Zusammen erhalten wir die Gleichung

$$\varepsilon_i = (-1)^{\left[\frac{2ai}{p}\right]}.$$

3. Schritt: Nach dem Gauß-Lemma (2.12) und Schritt 2 gilt

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{i=1}^{p_1}\left[\frac{2ai}{p}\right]},$$

wobei $p_1 = \frac{p-1}{2}$ ist.

4. Schritt: Sei a ungerade. Dann gilt

$$\left(\frac{2a}{p}\right) = \left(\frac{2a+2p}{p}\right) = \left(\frac{4\frac{a+p}{2}}{p}\right) = \left(\frac{4}{p}\right)\left(\frac{\frac{a+p}{2}}{p}\right).$$

Beachtet man nun $\left(\frac{4}{p}\right) = 1$, so folgt unter Verwendung der wohlbekannten Formel für die Summe der ersten n natürlichen Zahlen aus Schritt 3 die Formel

$$\begin{aligned}\left(\frac{2a}{p}\right) &= (-1)^{\sum_{i=1}^{p_1}\left[\frac{(a+p)i}{p}\right]} \\ &= (-1)^{\sum_{i=1}^{p_1} i + \sum_{i=1}^{p_1}\left[\frac{ai}{p}\right]} \\ &= (-1)^{\frac{p^2-1}{8}+\sum_{i=1}^{p_1}\left[\frac{ai}{p}\right]}.\end{aligned}$$

Setzt man in dieser Gleichung $a = 1$, so erhält man die Aussage des 2. Ergänzungssatzes.

5. Schritt: Aus der Multiplikativität des Legendre-Symbols, dem 2. Ergänzungssatz und der letzten Gleichung in Schritt 4 erhält man für ungerades a die Gleichung

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{i=1}^{p_1}\left[\frac{ai}{p}\right]}.$$

6. Schritt: Von nun an sei $a = q$ eine von p verschiedene Primzahl größer als 2 und $q_1 = \frac{q-1}{2}$. Wir setzen

$$\begin{aligned}S_1 &= \#\left\{(i,j) \mid 1 \le i \le p_1, 1 \le j \le q_1, qi > pj\right\} \\ S_2 &= \#\left\{(i,j) \mid 1 \le i \le p_1, 1 \le j \le q_1, qi < pj\right\}.\end{aligned}$$

Weil stets $qi \neq pj$ ist, gilt

$$S_1 + S_2 = p_1 q_1.$$

Für ein fest gewähltes i ist $qi > pj$ äquivalent zu $j \le \left[\frac{qi}{p}\right]$. Also gilt

$$S_1 = \sum_{i=1}^{p_1}\left[\frac{qi}{p}\right].$$

Analog erhält man

$$S_2 = \sum_{j=1}^{q_1} \left[\frac{pj}{q}\right].$$

Zusammen mit Schritt 5 zeigt dies

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(\sum_{i=1}^{p_1}\left[\frac{qi}{p}\right]+\sum_{j=1}^{q_1}\left[\frac{pj}{q}\right])} = (-1)^{(S_1+S_2)} = (-1)^{p_1 q_1},$$

und der Beweis des QRG ist erbracht. □

Mit Hilfe dieser Sätze ist das Legendre-Symbol $\left(\frac{a}{p}\right)$ schnell ausgerechnet. Zum Beispiel:

$$\left(\frac{17}{19}\right) = \left(\frac{19}{17}\right) = \left(\frac{2}{17}\right) = +1$$

$$\left(\frac{21}{23}\right) = \left(\frac{3}{23}\right)\left(\frac{7}{23}\right) = (-1)\left(\frac{23}{3}\right)(-1)\left(\frac{23}{7}\right) =$$

$$\left(\frac{2}{3}\right)\left(\frac{2}{7}\right) = (-1)(+1) = -1.$$

2.3 Primzahlen mit vorgegebener Restklasse

Satz 2.13. (i) *Es gibt unendlich viele Primzahlen kongruent* -1 *modulo* 3.

(ii) *Es gibt unendlich viele Primzahlen kongruent* -1 *modulo* 4.

Beweis. (i) Angenommen es gäbe nur endlich viele. Sei P ihr Produkt. Dann ist die Zahl $3P - 1$ durch keine Primzahl kongruent -1 modulo 3 und auch nicht durch 3 teilbar. Daher ist sie Produkt von Primzahlen kongruent 1 modulo 3; sie selbst ist aber kongruent -1 modulo 3. Widerspruch. (ii) Angenommen es gäbe nur endlich viele. Sei P ihr Produkt. Dann ist die Zahl $4P - 1$ durch keine Primzahl kongruent -1 modulo 4 und auch nicht durch 2 teilbar. Daher ist die Produkt von Primzahlen kongruent 1 modulo 4; sie selbst ist aber kongruent -1 modulo 4. Widerspruch. □

Der Beweis von 2.13 war elementar. Um entsprechende Aussagen auch für die $+1$-Restklassen zu bekommen, wenden wir das Quadratische Reziprozitätsgesetz an. Wir beginnen mit einem Lemma.

Lemma 2.14. *Für beliebiges* $a \in \mathbb{Z}$ *hat die Zahl* $n = 4a^2 + 1$ *nur Primteiler kongruent* 1 *modulo* 4.

Beweis. Zunächst ist n stets positiv und ungerade. Ist p ein Primteiler von n, so ist -1 quadratischer Rest modulo p. Nach dem ersten Ergänzungssatz zum QRG folgt $p \equiv 1 \bmod 4$. □

Satz 2.15. *Es gibt unendlich viele Primzahlen kongruent* 1 *modulo* 4.

Beweis. Angenommen es gäbe nur endlich viele. Sei P ihr Produkt. Dann ist die Zahl $4P^2+1$ durch keine Primzahl kongruent 1 modulo 4 teilbar. Nach dem obigen Lemma hat sie aber nur solche Primteiler. Widerspruch. □

Dieses Vorgehen kann verallgemeinert werden.

Satz 2.16. *Zu jeder ganzen Zahl $a \neq 0$ existieren unendlich viele Primzahlen p, so dass a quadratischer Rest modulo p ist.*

Beweis. Wir nehmen an, dass es nur endlich viele (ungerade) Primzahlen $p_1, \ldots, p_n$ mit $\left(\frac{a}{p_i}\right) = 1$ gäbe. Wir wählen eine ganze Zahl A prim zu a. Ist a ungerade, so wählen wir A gerade und umgekehrt. Ferner sei A so groß gewählt, dass die ganze Zahl

$$N = (p_1 \cdots p_n A)^2 - a$$

größer als 1 ist. Entsprechend unseren Wahlen ist N ungerade, durch keines der p_i teilbar und es gilt $(N, a) = 1$. Sei q ein Primteiler von N. Dann ist a quadratischer Rest modulo q. Widerspruch. □

Satz 2.17. *Es gibt unendlich viele Primzahlen kongruent* 1 *modulo* 3.

Beweis. Nach dem letzten Satz gibt es unendlich viele Primzahlen p mit $\left(\frac{-3}{p}\right) = 1$. Daher folgt alles aus dem nächsten Lemma. □

Lemma 2.18. *Eine ungerade Primzahl p ist genau dann $\equiv 1 \bmod 3$, wenn*

$$\left(\frac{-3}{p}\right) = 1.$$

Beweis. Zunächst ist $\left(\frac{-3}{3}\right) = 0$, so dass wir $p > 3$ annehmen können. Dann gilt

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right).$$

Nun ist aber $\left(\frac{p}{3}\right) = +1 \Longleftrightarrow p \equiv 1 \bmod 3$. □

Satz 2.19. *Sei $a \in \mathbb{Z}$ kein Quadrat. Dann existieren unendlich viele Primzahlen p mit $\left(\frac{a}{p}\right) = -1$.*

Beweis. Sei zunächst $a = -1$. Nach dem 1. Ergänzungssatz zum QRG ist $\left(\frac{-1}{p}\right) = -1$ äquivalent zu $p \equiv -1 \bmod 4$. Nach Satz 2.13 gibt es unendlich viele solche Primzahlen. Im Fall $a = 2$ müssen wir nach dem 2. Ergänzungssatz zum QRG zeigen, dass es unendlich viele Primzahlen kongruent ± 3 modulo 8 gibt. Angenommen es gäbe nur endlich viele. Seien $p_1 = 3, p_2, \ldots, p_n$ diese Primzahlen und sei

$$N = 8p_2 \cdots p_n + 3.$$

Dann ist $N > 1$ ungerade und durch keines der p_i teilbar, d.h. N hat nur Primteiler kongruent $\pm 1 \bmod 8$. Das widerspricht $N \equiv 3 \bmod 8$. Daher gibt es unendlich viele Primzahlen p mit $\left(\frac{2}{p}\right) = -1$.

Im Fall $a = -2$ schließen wir so: Seien $p_1 = 5, p_2, \ldots, p_n$ alle ungeraden Primzahlen mit $\left(\frac{-2}{p}\right) = -1$ (das sind die kongruent $-1, -3 \bmod 8$). Sei

$$N = 8p_2 \cdots p_n + 5.$$

Dann ist $N > 1$ ungerade und durch keines der p_i teilbar. Daher hat N nur Primteiler kongruent $1, 3 \bmod 8$. Das widerspricht $N \equiv -3 \bmod 8$. Daher gibt es unendlich viele Primzahlen p mit $\left(\frac{-2}{p}\right) = -1$.

Da sich das Legendre-Symbol nicht ändert, wenn wir a um ein Quadrat abändern, können wir nun annehmen, dass $a = (-1)^\epsilon 2^e q_1 \cdots q_n$ mit paarweise verschiedenen ungeraden Primzahlen q_i und $n \geq 1$, $e, \epsilon \in \{0, 1\}$ gilt. Wir nehmen nun an, dass $p_1, \ldots, p_m$ alle Primzahlen mit $\left(\frac{a}{p}\right) = -1$ sind. Dann gilt insbesondere $p_i \neq q_j$ für beliebige i, j. Sei α ein quadratischer Nichtrest modulo q_n. Mit Hilfe des Chinesischen Restklassensatzes finden wir ein $N \in \mathbb{N}$ mit

$$\begin{aligned} N &\equiv 1 && \bmod 8, \\ N &\equiv 1 && \bmod p_1, \ldots, p_m, \\ N &\equiv 1 && \bmod q_1, \ldots, q_{n-1}, \\ N &\equiv \alpha && \bmod q_n. \end{aligned}$$

Sei

$$N = \ell_1 \cdots \ell_r$$

die Primfaktorzerlegung von N. Da N weder durch 2 noch durch eines der p_i oder q_i teilbar ist, sind die ℓ_i sämtlich ungerade und von den p_i und q_i verschieden. Daher gilt

$$\prod_i \left(\frac{a}{\ell_i}\right) = \prod_i \left(\frac{-1}{\ell_i}\right)^\epsilon \cdot \prod_i \left(\frac{2}{\ell_i}\right)^e \cdot \prod_{i,j} \left(\frac{q_j}{\ell_i}\right).$$

Wegen $N \equiv 1 \bmod 4$ ist eine gerade Anzahl der ℓ_i kongruent -1 modulo 4, weshalb der erste Faktor gleich 1 ist. Wegen $N \equiv 1 \bmod 8$ ist eine gerade Anzahl

der ℓ_i kongruent ± 3 modulo 8. Also ist der zweite Faktor gleich 1. Für festes q_j gilt

$$\prod_i \left(\frac{q_j}{\ell_i}\right) = \prod_i \left(\frac{\ell_i}{q_j}\right).$$

Entsprechend unserer Wahl von N erhalten wir die Gleichung

$$\prod_i \left(\frac{a}{\ell_i}\right) = \prod_{i,j} \left(\frac{\ell_i}{q_j}\right) = \prod_j \left(\frac{N}{q_j}\right) = -1.$$

Daher muss $\left(\frac{a}{\ell_i}\right) = -1$ für mindestens ein i gelten. Widerspruch. □

2.4 Quadratsummen

Wir wollen mit Hilfe des Quadratischen Reziprozitätsgesetzes Darstellungen von Primzahlen als Quadratsummen herleiten. Der folgende Satz ist ein Klassiker.

Satz 2.20 (Lagrange)**.** *Eine ungerade Primzahl ist genau dann als Summe zweier Quadrate darstellbar, wenn sie kongruent* 1 *modulo* 4 *ist.*

Da die Summe zweier Quadrate stets $\equiv 0, 1, 2 \bmod 4$ ist, ist die gegebene Bedingung notwendig. Auch die Primzahlbedingung ist notwendig, wie das Beispiel der Zahl 21 zeigt.

Beweis von Satz 2.20. Die Bedingung ist offenbar notwendig. Es verbleibt zu zeigen, dass die Bedingung hinreichend ist, also sei $p \equiv 1 \bmod 4$ eine Primzahl.

Wir betrachten den Ring der Gaußschen Zahlen $\mathbb{Z}[i] = \{a+bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ und seine Normfunktion $N(a+bi) = a^2 + b^2$. Diese ist eine euklidische Normfunktion, insbesondere ist $\mathbb{Z}[i]$ ein Hauptidealring. Eine Nichteinheit $z = a + bi$ hat stets eine Norm $N(z) > 1$ (ansonsten wäre wegen $N(z) = z\bar{z}$ die komplex Konjugierte $\bar{z}$ von z ein Inverses von z).

Nun ist p kein Primelement in $\mathbb{Z}[i]$. Um dies einzusehen, wähle $x \in \mathbb{Z}$ mit $x^2 \equiv -1 \bmod p$. Dann gilt in $\mathbb{Z}[i]$, dass $p \mid (x^2+1) = (x+i)(x-i)$, aber die Faktoren sind beide nicht durch p teilbar.

Weil p kein Primelement ist, ist es auch nicht irreduzibel, man findet also $z, z' \in \mathbb{Z}[i] \setminus \mathbb{Z}[i]^\times$ mit $zz' = p$. Hieraus folgt $N(z)N(z') = N(p) = p^2$, also $N(z) = N(z') = p$. Mit $z = a + bi$ erhalten wir $p = N(z) = a^2 + b^2$. □

Wir nennen eine ganze Zahl *Quadratzahl*, wenn sie das Quadrat einer ganzen Zahl ist, d.h. wir zählen die Zahl 0 mit zu den Quadratzahlen.

Theorem 2.21 (Lagrange)**.** *Jede natürliche Zahl ist Summe von vier Quadratzahlen.*

Zentral für den Beweis ist die folgende Bemerkung, die besagt, dass das Produkt zweier Summen von vier Quadraten wieder eine Summe von vier Quadraten ist.

Lemma 2.22 (Euler-Identität)**.** *Für $x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4 \in \mathbb{Z}$ gilt die Identität*

$$\begin{aligned}(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2) = \\ (x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2 \\ +(x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2 \\ +(x_1y_3-x_2y_4-x_3y_1+x_4y_2)^2 \\ +(x_1y_4+x_2y_3-x_3y_2-x_4y_1)^2.\end{aligned}$$

Zum Beweis ist nichts zu sagen, man multipliziert einfach aus. Ihren Ursprung hat diese Gleichung in den Quaternionen. Eine **Quaternion** (oder auch **hyperkomplexe Zahl**) ist ein Ausdruck der Form $z = x_1+x_2i+x_3j+x_4k$, wobei x_1, x_2, x_3, x_4 reelle Zahlen und i, j, k Symbole sind, die den Rechenregeln $-1 = i^2 = j^2 = k^2$ und $ij = -ji = k$, $jk = -kj = i$ und $ki = -ik = j$ genügen. Die Norm einer Quaternion ist durch $N(z) = x_1^2 + x_2^2 + x_3^2 + x_4^2$ definiert und die obige Identität entspricht genau dem Multiplikationsgesetz $N(z)N(z') = N(zz')$ für die Quaternionennorm.

Beweis von Theorem 2.21. Wegen der Euler-Identität genügt es zu zeigen, dass jede Primzahl Summe von vier Quadratzahlen ist. Sei p eine Primzahl, die wir ohne Einschränkung als ungerade annehmen können. Es gibt $(p+1)/2$ Quadrate modulo p, also auch genauso viele Restklassen der Form $-1-x^2$. Da es insgesamt nur p verschiedene Restklassen gibt, muss unter diesen wenigstens ein Quadrat sein, d.h. die Gleichung $x^2 + y^2 + 1 = 0$ hat eine Lösung modulo p. Wählen wir Repräsentanten x, y mit $-p/2 < x, y < p/2$, so folgt

$$0 < x^2 + y^2 + 1 < 3\left(\frac{p}{2}\right)^2 < p^2.$$

Also gibt es ein $n \in \mathbb{N}$, $n < p$, so dass np Summe von drei, also insbesondere auch von vier Quadraten ist. Sei m die kleinste natürliche Zahl, so dass mp Summe von vier Quadraten ist. Offenbar gilt $m < p$. Wir zeigen $m = 1$. Angenommen m wäre echt größer als 1 und

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2. \qquad (*)$$

Sei nun $x_i \equiv y_i \bmod m$ mit $-m/2 < y_i \leq m/2$ für $i = 1, 2, 3, 4$. Dann gilt $y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv 0 \bmod m$, also existiert ein $r \in \mathbb{Z}$, $r \geq 0$, mit

$$rm = y_1^2 + y_2^2 + y_3^2 + y_4^2. \qquad (**)$$

Wegen $y_1^2 + y_2^2 + y_3^2 + y_4^2 \leq m^2/4 + m^2/4 + m^2/4 + m^2/4 = m^2$, gilt $r \leq m$. Multiplizieren wir die Gleichungen $(*)$ und $(**)$, so erhalten wir eine Darstellung von rpm^2 als Summe von vier Quadraten

$$rpm^2 = A^2 + B^2 + C^2 + D^2, \qquad (***)$$

wobei A, B, C und D gerade die Terme auf der rechten Seite der Euler-Identität sind. Wegen $x_i \equiv y_i \bmod m$ sind B, C und D durch m teilbar. Außerdem gilt

$$A = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp \equiv 0 \bmod m.$$

Folglich ist auch $rp = (A/m)^2 + (B/m)^2 + (C/m)^2 + (D/m)^2$ Summe von vier Quadraten. Wir zeigen nun, dass r weder gleich 0 noch gleich m sein kann:

Aus $r = 0$ folgt $y_1 = y_2 = y_3 = y_4 = 0$. Daher sind x_1, x_2, x_3, x_4 durch m teilbar und $(*)$ impliziert $m^2 | mp$, also $m|p$.

Aus $r = m$ folgt $y_i = m/2$ für $i = 1, 2, 3, 4$, insbesondere ist m gerade. Es gilt $x_i = m/2 + c_i m$ mit $c_i \in \mathbb{Z}$, $i = 1, 2, 3, 4$. Wir erhalten $x_i^2 = m^2/4 + c_i m^2 + c_i^2 m^2 \equiv m^2/4 \bmod m^2$. Durch Aufsummieren folgt $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv m^2 \bmod m^2$, woraus wieder $m \mid p$ folgt.

In beiden Fällen haben wir $m \mid p$ erhalten, was, da p eine Primzahl ist, im Widerspruch zu $1 < m < p$ steht. Daher gilt $1 \leq r \leq m - 1$. Dies steht wiederum im Widerspruch zur Minimalität von m. Die Annahme $m > 1$ ist damit zum Widerspruch geführt. Es folgt $m = 1$, und der Beweis ist beendet. □

Bemerkung: Wir haben gezeigt, dass jede natürliche Zahl Summe von vier Quadraten ist. Der Beweis benutzte zum einen die entsprechende Aussage über Primzahlen und zum anderen die von den Quaternionen herkommende Euler-Identität. Die Normgleichung $N(z)N(z') = N(zz')$ für komplexe Zahlen $z = x_1 + ix_2$, $z' = y_1 + iy_2$ impliziert die Identität

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1y_2 + x_2y_1)^2 + (x_1y_1 - x_2y_2)^2,$$

und zeigt uns, dass auch das Produkt von Summen zweier Quadrate wieder Summe zweier Quadrate ist. Nach Satz 2.20 ist daher jedes Produkt von Primzahlen inkongruent 3 modulo 4 Summe zweier Quadrate. Um alle natürlichen Zahlen zu bestimmen, die Summe zweier Quadrate sind, brauchen wir allerdings mehr Einsicht in den Ring $\mathbb{Z}[i]$.

Ein Element in $\mathbb{Z}[i]$ ist genau dann Einheit, wenn es Norm 1 hat - dies sind die vier Elemente $\{\pm 1, \pm i\}$. Ein Element mit Primzahlnorm ist automatisch prim (wegen der Multiplikativität der Norm). Allerdings haben nicht alle Primelemente in $\mathbb{Z}[i]$ eine Primzahl als Norm. Zum Beispiel ist $3 \in \mathbb{Z}[i]$ irreduzibel, also ein Primelement, und es gilt $N(3) = 9$.

Satz 2.23. *Sei $\pi \in \mathbb{Z}[i]$ ein Primelement. Dann tritt genau einer der beiden folgenden Fälle auf:*

(a) $N(\pi) = p^2$ für eine Primzahl p und $\pi \mathrel{\hat{=}} p$.

(b) $N(\pi) = \pi\bar{\pi} = p$ ist eine Primzahl.

Umgekehrt ist jede Primzahl p entweder Primelement in $\mathbb{Z}[\,i\,]$ oder von der Form $p = \pi\bar{\pi}$ mit einem Primelement π der Norm p.

Beweis. Sei $p = \pi_1 \cdots \pi_n$ eine Primelementzerlegung der Primzahl p in $\mathbb{Z}[i]$. Dann gilt

$$p^2 = N(p) = N(\pi_1) \cdots N(\pi_n).$$

Es gilt $N(\pi_j) > 1$ für $j = 1, \ldots, n$; folglich ist $n \leq 2$. Im Fall $n = 1$ ist p Primelement. Im Fall $n = 2$ gilt $p = N(\pi_1) = \pi_1\bar{\pi}_1$. Sei nun $\pi \in \mathbb{Z}[i]$ ein Primelement. Dann teilt π die natürliche Zahl $N(\pi) > 1$ und deshalb auch eine Primzahl p. Ist p Primelement in $\mathbb{Z}[i]$, so folgt $\pi \mathrel{\hat{=}} p$ und $N(\pi) = N(p) = p^2$. Gilt $p = \pi_1\bar{\pi}_1$ mit einem Primelement π_1 der Norm p, so ist, wegen der Eindeutigkeit der Primzerlegung, π assoziiert zu π_1 oder zu $\bar{\pi}_1$. In jedem Fall gilt $\pi\bar{\pi} = N(\pi) = N(\pi_1) = p$. □ □

Es verbleibt zu klären, wann welcher Fall eintritt.

Satz 2.24. *Eine Primzahl p ist genau dann ein Primelement in $\mathbb{Z}[i]$, wenn p kongruent 3 modulo 4 ist.*

Beweis. Zunächst ist $2 = (1+i)(1-i)$ kein Primelement in $\mathbb{Z}[i]$. Sei $p \neq 2$ und kein Primelement. Nach Satz 2.23 gilt $p = \pi\bar{\pi}$ für ein Primelement π. Setzt man $\pi = a + bi$, $a, b \in \mathbb{Z}$, so folgt $p = a^2 + b^2$, also $p \equiv 1 \bmod 4$. Dies zeigt eine Richtung. Dass Primzahlen $p \equiv 1 \bmod 4$ keine Primelemente in $\mathbb{Z}[i]$ sind, haben wir bereits im Beweis von 2.20 eingesehen. □

Ist p von der Form $\pi\bar{\pi}$ und gilt $\pi \mathrel{\hat{=}} \bar{\pi}$, so erhalten wir mit $\pi = a + bi$

$$a + bi = u(a - bi), \quad u \in \{\pm 1, \pm i\}.$$

Aus $u = \pm 1$ würde folgen, dass p ein Quadrat ist, also scheidet diese Möglichkeit aus. Für $u = \pm i$ erhalten wir $a = \pm b$. Aus $p = N(\pi) = 2a^2$ folgt dann $p = 2$. In der Tat gilt $2 = (1+i)(1-i)$ und $(1-i) = (-i)(1+i)$.

Zusammenfassend erhalten wir das

Satz 2.25 (Zerlegungsgesetz in $\mathbb{Z}[i]$)**.** *Eine Primzahl p ist in $\mathbb{Z}[i]$*

Produkt zweier assoziierter Primelemente	$\iff$	$p = 2$,
Produkt zweier nicht assoziierter Primelemente	$\iff$	$p \equiv 1 \bmod 4$,
Primelement	$\iff$	$p \equiv 3 \bmod 4$.

Satz 2.26. *Eine natürliche Zahl ist genau dann Summe zweier Quadratzahlen, wenn in ihrer Primfaktorzerlegung jede Primzahl kongruent* 3 *modulo* 4 *in gerader Vielfachheit vorkommt.*

Beweis. Eine natürliche Zahl ist genau dann Summe zweier Quadrate, wenn sie als Norm einer Gaußschen Zahl $\alpha \in \mathbb{Z}[i]$ vorkommt. Sei nun $n = N(\alpha)$ und

$$\alpha = \pi_1 \cdots \pi_r$$

eine Primzerlegung von α in $\mathbb{Z}[i]$. Dann gilt

$$n = N(\alpha) = N(\pi_1) \cdots N(\pi_r).$$

Nach Satz 2.23 und dem Zerlegungsgesetz ist für ein Primelement $\pi \in \mathbb{Z}[i]$ die Norm $N(\pi)$ entweder gleich 2, eine Primzahl kongruent 1 modulo 4 oder das Quadrat einer Primzahl kongruent 3 modulo 4. Dies zeigt, dass die gegebene Bedingung notwendig ist.
Sei nun

$$n = (p_1 \cdots p_r) \cdot (n')^2$$

mit Primzahlen $p_i \not\equiv 3 \bmod 4$, $i = 1, \ldots, r$. Nach dem Zerlegungsgesetz finden wir Primelemente $\pi_i \in \mathbb{Z}[i]$ mit $N(\pi_i) = p_i$, $i = 1, \ldots, r$. Wir erhalten $n = N(\alpha)$ mit $\alpha = \pi_1 \cdots \pi_r \cdot n'$. □ □

Die Frage, welche natürlichen Zahlen sich als Summe dreier Quadrate darstellen lassen, lässt sich nicht durch Normgleichungen behandeln.

3 Ringe ganzer Zahlen

3.1 Quadratische Zahlringe

Wir betrachten nun allgemeinere Zahlbereiche. Sei $d \in \mathbb{Z}$ quadratfrei (d.h. durch keine Quadratzahl > 1 teilbar) und von 0 und 1 verschieden. Mit $\sqrt{d}$ bezeichnen wir eine (willkürlich, aber fest gewählte) komplexe Lösung der Gleichung $X^2 = d$ (die andere ist dann $-\sqrt{d}$). Die Menge der komplexen Zahlen

$$a + b\sqrt{d}, \quad a, b \in \mathbb{Z},$$

ist ein Ring und wird mit $\mathbb{Z}[\sqrt{d}]$ bezeichnet. Da d als quadratfrei angenommen ist, ist $\sqrt{d}$ keine rationale Zahl. Ist $a+b\sqrt{d} = a'+b'\sqrt{d}$, so gilt $(b'-b)\sqrt{d} = (a-a')$ und daher $a = a'$ und $b = b'$, d.h. die Darstellung ist eindeutig. Wir betrachten nun die folgende Normfunktion auf $\mathbb{Z}[\sqrt{d}]$:

$$N(a + b\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2.$$

Ist d negativ, so ist $N(z)$, wie im Falle der Gaußschen Zahlen, gerade das Quadrat des Absolutbetrages von z als komplexe Zahl. Für positives d ist das nicht richtig, die Norm kann sogar negativ sein. So hat $\sqrt{2}-1 \in \mathbb{Z}[\sqrt{2}]$ die Norm $(-1)^2 - 2 \cdot 1^2 = -1$. Unabhängig vom Vorzeichen von d verifiziert man leicht die Regel $N(zz') = N(z)N(z')$. Ist $N(z) = 0$, so folgt aus der Quadratfreiheit von d, dass $z = 0$ ist.

Satz 3.1. *Die Funktion*

$$\nu : \mathbb{Z}[\sqrt{d}] \setminus \{0\} \longrightarrow \mathbb{N},\ z \longmapsto |N(z)|,$$

ist eine euklidische Normfunktion, falls

$$|x^2 - dy^2| < 1$$

für alle rationalen Zahlen $x, y \in \mathbb{Q}$ mit $|x| \leq \frac{1}{2}$, $|y| \leq \frac{1}{2}$ gilt.

Beweis. Wir bemerken zunächst, dass für komplexe Zahlen $x, y \in \mathbb{C}$ der Form $x = a + b\sqrt{d}$, $y = a' + b'\sqrt{d}$ mit $a, a', b, b' \in \mathbb{Q}$ auch die komplexen Zahlen $x + y$, xy und x/y von dieser Gestalt sind. Für den Quotienten (wir nehmen natürlich $y \neq 0$ an) sieht man das durch

$$\frac{x}{y} = \frac{a + b\sqrt{d}}{a' + b'\sqrt{d}} = \frac{(a + b\sqrt{d})(a' - b'\sqrt{d})}{a'^2 - db'^2} = \frac{aa' - bb'd}{a'^2 - db'^2} + \frac{a'b - ab'}{a'^2 - db'^2}\sqrt{d}.$$

Seien $a, b \in \mathbb{Z}[\sqrt{d}]$, $b \neq 0$. Wie wir gerade gesehen haben, hat die komplexe Zahl a/b die Gestalt

$$\frac{a}{b} = u + v\sqrt{d}$$

mit $u, v \in \mathbb{Q}$. Nun wählen wir ganze Zahlen $x, y \in \mathbb{Z}$ mit $|u - x| \leq 1/2$, $|v - y| \leq 1/2$. Mit $q = x + y\sqrt{d}$ erhalten wir nach Voraussetzung

$$\left|N\left(\frac{a}{b} - q\right)\right| = \left|(u - x)^2 - d(v - y)^2\right| < 1.$$

Setzen wir $r = a - bq \in \mathbb{Z}[\sqrt{d}]$, so gilt

$$\nu(r) = |N(r)| = \left|N(b)N\left(\frac{a}{b} - q\right)\right| < |N(b)| = \nu(b).$$

Also erfüllen q und r das Gewünschte. □

Korollar 3.2. *Für $d = -2, -1, 2, 3$ ist der Ring $\mathbb{Z}[\sqrt{d}]$ euklidisch und daher auch faktoriell.*

Beweis. Es gilt in den verschiedenen Fällen:

$$d = -2: \quad |x^2 + 2y^2| \leq \tfrac{3}{4} < 1; \qquad d = -1: \quad |x^2 + y^2| \leq \tfrac{1}{2} < 1;$$
$$d = +2: \quad |x^2 - 2y^2| \leq \tfrac{1}{2} < 1; \qquad d = +3: \quad |x^2 - 3y^2| \leq \tfrac{3}{4} < 1.$$

□

Leider ist der Ring $\mathbb{Z}[\sqrt{d}]$ oft nicht faktoriell (und damit insbesondere nicht euklidisch). So haben wir beispielsweise im Ring $\mathbb{Z}[\sqrt{-5}]$ die Zerlegung

$$(1+\sqrt{-5})(1-\sqrt{-5}) = 6 = 2 \cdot 3.$$

Die Elemente $1+\sqrt{-5}$, $1-\sqrt{-5}$, 2, 3 sind sämtlich irreduzibel, also ist $\mathbb{Z}[\sqrt{-5}]$ nicht faktoriell. Ein weiteres, ganz praktisches Problem ist das folgende. Die dritte Einheitswurzel

$$\zeta_3 = e^{2\pi i/3} = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$$

liegt nicht im Ring $\mathbb{Z}[\sqrt{-3}]$. Wir würden aber gerne mit ζ_3 arbeiten, um zum Beispiel zur Lösung der Fermat-Gleichung $X^3 + Y^3 = Z^3$ die Identität

$$X^3 + Y^3 = (X+Y)(X+\zeta_3 Y)(X-\zeta_3 Y)$$

heranziehen zu können. Wir werden uns diesem Problem im nächsten Abschnitt widmen.

3.2 Ganzheit

Sei $\phi : A \to B$ ein Ringhomomorphismus. Dann nennt man B eine A-Algebra. B wird zum A-Modul durch $a \cdot b \stackrel{df}{=} \phi(a) \cdot b$.
Insbesondere ist für $f \in A[X]$ und $b \in B$ das Element $f(b) \in B$ definiert

Definition 3.3. ϕ heißt endlich (und B endliche A-Algebra) wenn B als A-Modul endlich erzeugt ist.

Satz 3.4. *Sei $\phi : A \to B$ ein Ringhomomorphismus und $b \in B$. Dann sind äquivalent*

(i) *es existiert ein normiertes Polynom $f \in A[X]$ mit $f(b) = 0$.*

(ii) *der Unterring $A[b] \subset B$ ist als A-Modul endlich erzeugt.*

(iii) *es existiert ein endlich erzeugter A-Untermodul $M \subset B$ mit $1 \in M$ und $b \cdot M \subset M$.*

Beweis. Siehe Algebra 1, 3.3 oder beliebiges Algebra-Buch. □

Definition 3.5. $b \in B$ heißt **ganz** über A, wenn es die äquivalenten Bedingungen von 3.4 erfüllt. ϕ heißt **ganz** (bzw. B heißt ganz über A), wenn jedes Element $b \in B$ ganz über A ist.

Bemerkung 3.6. Endliche Ringhomomorphismen sind ganz (setze $M = B$ in (iii).

Satz 3.7. *Seien $A \xrightarrow{\phi} B \xrightarrow{\psi} C$ Ringhomomorphismen.*

(i) *sind ψ und ϕ endlich, so auch $\psi \circ \phi$.*

(ii) *sind ψ und ϕ ganz, so auch $\psi \circ \phi$.*

Beweis. Siehe Algebra 1, 3.49 und 3.52 oder beliebiges Algebra-Buch. □

Satz 3.8. *Sei $\phi : A \to B$ ein Ringhomomorphismus und $B = A[b_1, \ldots, b_n]$, also B ist e.e. A-Algebra. Sind $b_1, \ldots, b_n$ ganz über A, so ist B eine endliche A-Algebra.*

Beweis. Siehe Algebra 1, 3.50 oder beliebiges Algebra-Buch. □

Korollar 3.9. *Sind $b_1, b_2 \in B$ ganz über A, so auch $b_1 + b_2$ und $b_1 b_2$.*

Sei nun A nullteilerfrei und $K = Q(A)$ der Quotientenkörper. Sei $L|K$ eine algebraische Körpererweiterung

Definition 3.10.

$$A_L = \{x \in L \mid x \text{ ganz über } A\}$$

heißt der **Ganzabschluss** von A in L. A heißt ganzabgeschlossen, wenn $A = A_K$.

Bemerkung 3.11. Nach 3.9 ist A_L ein Ring. L ist der Quotientenkörper von A_L und A_L ist ganzabgeschlossen.

Beispiel 3.12 (eines nicht ganzabgeschlossenen Ringes). Sei $f = X^2 - Y^3 \in \mathbb{C}[X, Y]$ und $A = \mathbb{C}[X, Y]/(f)$. A ist nullteilerfrei weil f irreduzibel ist.

Sei x das Bild von X in A; wegen $f \nmid X$ gilt $x \neq 0$. Analog sei y das Bild von Y in A; wegen $f \nmid Y$ gilt $y \neq 0$. Es gilt $x^2 = y^3$ in A. Daher gilt

$$\left(\frac{x}{y}\right)^2 - y = \frac{x^2}{y^2} - y = \frac{x^2 y}{y^3} - y = y - y = 0.$$

Also ist $\frac{x}{y} \in Q(A)$ ganz über A. Aber $\frac{x}{y} \notin A$. Ansonsten wäre nämlich $x = y \cdot \frac{x}{y} \in Ay$ und somit $X \in (Y, X^2 - Y^3)$. Aber $(Y, X^2 - Y^3) = (Y, X^2) \not\ni X$. Also ist A nicht ganzabgeschlossen.

Satz 3.13. *Jeder faktorielle Ring ist ganzabgeschlossen.*

Beweis. Sei $\alpha \in K$ mit $\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_0 = 0$, wobei $c_0, \ldots, c_{n-1} \in A$. Z.z.: $\alpha \in A$. Sei $\alpha = \frac{a}{b}$, $a, b \in A$, $\mathrm{ggT}(a,b) = 1$. Dann gilt

$$a^n + c_{n-1}ba^{n-1} + \cdots + c_0 b^n = 0.$$

Ist nun $p \in A$ ein Primelement mit $p \mid b$, so folgt $p \mid a^n$, also $p \mid a$ WID. Also existiert so ein p nicht und es gilt $b \in A^\times$. Folglich gilt $\alpha \in A$. □

Bemerkung 3.14. Wir sehen somit, dass $\mathbb{C}[X,Y]/(X^2 - Y^3)$ ein nullteilerfreier, nicht faktorieller Ring ist.

Satz 3.15. *Sei A ganzabgeschlossen und $L|K$ endlich. Sei $x \in L$ und*

$$f = X^r + a_{r-1}X^{r-1} + \cdots + a_0$$

das Minimalpolynom von x über K. Dann gilt

$$x \in A_L \Longleftrightarrow a_{r-1}, \ldots, a_0 \in A.$$

Beweis. $\Longleftarrow$ per definitionem
$\Longrightarrow$ $L|K$ normal. Sei $x \in A_L$ und $g \in A[X]$ normiert mit $g(x) = 0$. Dann gilt $f|g$ in $K[X]$, also $g(y) = 0$ für jede Nullstelle y von f, d.h. diese liegen alle in A_L. Die Koeffizienten von f sind die elementarsymmetrischen Polynome in den Nullstellen $\Rightarrow a_{r-1}, \ldots, a_0 \in A_L \cap K = A$. □

Erinnerung: Sei $L|K$ endlich, $x \in L$. Dann ist

$$\varphi_x : L \to L,\ y \mapsto xy$$

ein Endomorphismus des endlichdimensionalen K-Vektorraums L.

Definition 3.16.

$$\begin{aligned} \mathrm{Sp}_{L|K}(x) &= \mathrm{Sp}(\varphi_x) \in K \\ N_{L|K}(x) &= \det(\varphi_x) \in K. \end{aligned}$$

Satz 3.17. *Sind $\sigma_1, \ldots, \sigma_n$ die endlich vielen K-Einbettungen $L \to \overline{K}$ in einen festen algebraischen Abschluss von K, so gilt*

$$\begin{aligned} \mathrm{Sp}_{L|K}(x) &= [L:K]_i \cdot \sum_{i=1}^{n} \sigma_i x \\ N_{L|K}(x) &= \left(\prod_{i=1}^{n} \sigma_i x \right)^{[L:K]_i}. \end{aligned}$$

Beweis. Siehe Algebra 1, 4.62. □

Korollar 3.18. *A ganzabgeschlossen, $K = Q(A)$, $L|K$ endlich, $x \in A_L \Longrightarrow$ $\mathrm{Sp}_{L|K}(x)$, $N_{L|K}(x) \in A$.*

Beweis. $N_{L|K}(x) = N_{K(x)/K}(x)^{[L:K(x)]} = \pm a_0^{[L:K(x)]}$ wobei $X^r + a_{r-1}X^{r-1} + \cdots + a_0$ das Minimalpolynom von x über K ist. Desweiteren gilt

$$\begin{aligned} \mathrm{Sp}_{L|K}(x) = [L : K(x)] \cdot \quad & \mathrm{Sp}_{K(x)/K}(x) \\ & \| \\ & -a_{r-1}. \end{aligned}$$

Schließlich gilt $a_0, a_{r-1} \in A$. □

Erinnerung: (Algebra 1, 4.64) $L|K$ endlich, separabel. Dann ist die **Spurform**

$$\begin{aligned} \mathrm{Sp} : L \times L &\longrightarrow K, \\ (x, y) &\longmapsto \mathrm{Sp}_{L|K}(xy), \end{aligned}$$

eine nicht-ausgeartete Bilinearform.

Definition 3.19. Für eine K-Basis $\alpha_1, \ldots, \alpha_n$, $n = [L : K]$, von L ist die **Diskriminante** definiert durch

$$d(\alpha_1, \ldots, \alpha_n) = \det(\mathrm{Sp}(\alpha_i \alpha_j)).$$

Mit $\mathrm{Hom}_K(L, \overline{K}) = \{\sigma_1, \ldots, \sigma_n\}$ gilt

$$\mathrm{Sp}(\alpha_i \alpha_j) = \sum_k \sigma_k(\alpha_i)\sigma_k(\alpha_j)$$

Daher gilt die Gleichheit von Matrizen

$$(\mathrm{Sp}(\alpha_i \alpha_j))_{ij} = (\sigma_k \alpha_i)^t_{k,i} \cdot (\sigma_k \alpha_j)_{k,j},$$

und wir erhalten

Lemma 3.20.

$$d(\alpha_1, \ldots, \alpha_n) = \big(\det(\sigma_i \alpha_j)_{ij}\big)^2.$$

Im Spezialfall $(\alpha_1, \ldots, \alpha_n) = (1, \alpha, \ldots, \alpha^{n-1})$ erhält man

$$d(1, \alpha, \ldots, \alpha^{n-1}) = \prod_{i<j} (\sigma_j(\alpha) - \sigma_i(\alpha))^2.$$

Beweis. Die erste Aussage haben wir schon. Die zweite folgt aus

$$\det \begin{pmatrix} 1, \sigma_1(\alpha), \sigma_1(\alpha)^2, \ldots, \sigma_1(\alpha)^{n-1} \\ \ddots \\ 1, \sigma_n(\alpha), \sigma_n(\alpha)^2, \ldots, \sigma_n(\alpha)^{n-1} \end{pmatrix} = \prod_{i<j} (\sigma_i(\alpha) - \sigma_j(\alpha))$$

(Vandermondsche Matrix). □

Sei $L|K$ endlich separabel, A ganzabgeschlossen mit $K = Q(A)$ und sei $B = A_L$. Jedes $x \in L$ erfüllt eine Gleichung

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0.$$

Durch Multiplikation erhalten wir $ax \in A_L$ für $a \in A$ geeignet. Insbesondere existieren in B enthaltene K-Basen von L.

Satz 3.21. *A ganzabgeschlossen, $K = Q(A)$, $L|K$ endlich separabel, $B = A_L$. Sei $\alpha_1, \ldots, \alpha_n$ eine in B gelegene K-Basis von L. Dann gilt*

$$d(\alpha_1, \ldots, \alpha_n) \cdot B \subset A\alpha_1 + \cdots + A\alpha_n.$$

Insbesondere ist B ein Untermodul eines e.e. A-Moduls.

Beweis. Sei $\alpha \in B$ beliebig. $\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n$, $a_1, \ldots, a_n \in K$.
Dann gilt $\mathrm{Sp}_{L|K}(\alpha_i\alpha) = \sum_{j=1}^{n} \mathrm{Sp}_{L|K}(\alpha_i\alpha_j)a_j$.
Also sind die a_i Lösungen eines linearen Gleichungssystems der Form

$$M \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

mit $b_i \in A$, $M = (m_{ij}) \in M_{n,n}(A)$.

Cramersche Regel: $\det(M)a_i \in A$ (multipliziere mit Adjunkter von M). Es gilt $\det M = d(\alpha_1, \ldots, \alpha_n) =: d$. Also gilt $d\alpha = da_1\alpha_1 + \cdots + da_n\alpha_n \in B$. Schließlich erhalten wir die Inklusion

$$B \subset A\frac{\alpha_1}{d} + \cdots + A\frac{\alpha_n}{d},$$

was das „Insbesondere“ zeigt. □

Korollar 3.22. *Ist A ein Hauptidealring, so ist B ein freier A-Modul vom Rang $n = [L : K]$.*

Beweis. Sei $\alpha_1, \ldots, \alpha_n$ eine in B enthaltene K-Basis von L und $d = d(\alpha_1, \ldots, \alpha_n)$. Dann gilt nach 3.21

$$B \subset A\frac{\alpha_1}{d} + \cdots + A\frac{\alpha_n}{d}.$$

Die Elemente $\frac{\alpha_i}{d}$ sind K-linear unabhängig, also auch A-linear unabhängig. Daher ist B Untermodul eines freien A-Moduls vom Rang n und somit frei vom Rang $\leq n$. Jede A-Basis von B ist auch K-Basis von $L \Rightarrow \mathrm{Rang}_A B = n$. □

Definition 3.23. Eine A-Basis von B (wenn sie existiert) heißt **Ganzheitsbasis** von B über A.

3.3 Dedekindringe

Satz 3.24 (Algebra 2, 19.1)**.** *Für einen A-Modul M sind die folgenden Eigenschaften äquivalent.*

(i) *Jede aufsteigende Kette $M_1 \subset M_2 \subset \cdots \subset M$ von Untermoduln in M wird stationär.*

(ii) *jeder Untermodul von M ist endlich erzeugt.*

Definition 3.25. Ein Modul M der den Bedingungen von 3.24 genügt heißt **noetherscher** A-Modul. A heißt **noetherscher Ring**, wenn A noethersch als A-Modul ist (d.h. jedes Ideal ist endlich erzeugt).

Beispiel 3.26. Jeder Hauptidealring ist noethersch.

Satz 3.27 (Algebra 2, 19.10)**.** *Sei A ein noetherscher Ring. Dann ist ein A-Modul M genau dann noethersch, wenn er endlich erzeugt ist.*

Satz 3.28 (Hilbertscher Basissatz, Algebra 2, 19.15)**.** *Ist A noethersch und B eine endlich erzeugte A-Algebra, so ist auch B ein noetherscher Ring.*

Satz 3.29. *Sei A ein nullteilerfreier ganzabgeschlossener noetherscher Ring, $K = Q(A)$ und $L|K$ endlich separabel. Dann ist $B = A_L$ eine endliche A-Algebra und insbesondere selbst wieder noethersch.*

Beweis. Nach 3.21 ist B Untermodul eines e.e. A-Moduls, also selbst e.e. A-Modul. □

Definition 3.30 (Algebra 2, 26.10)**.** Die **Dimension** $\dim A$ eines Ringes ist das Supremum über alle $n \in \mathbb{N}_0$ mit der Eigenschaft: es existiert eine Kette (der Länge n)

$$\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_n \subset A$$

von Primidealen in A.

Bemerkungen 3.31. • A Körper $\Rightarrow \dim A = 0$
• A nullteilerfrei und $\dim A = 0 \Rightarrow A$ Körper
• $n \in \mathbb{N},\ n \geq 2 \Rightarrow \dim \mathbb{Z}/n\mathbb{Z} = 0$
• A Hauptidealring $\Rightarrow \dim A \leq 1$.
Grund: z.z.: jedes Primideal $\neq 0$ ist maximal: Gilt $\mathfrak{p}_1 \subsetneqq \mathfrak{p}_2$, so gilt $\mathfrak{p}_i = (\pi_i)$ für Primelemente $\pi_1, \pi_2 \in A$. Es folgt $\pi_2 \mid \pi_1$. Da die π_i prim, insbesondere irreduzibel sind, folgt $\pi_1 \mathrel{\hat{=}} \pi_2 \Rightarrow \mathfrak{p}_1 = \mathfrak{p}_2$. Widerspruch.
• es gibt noethersche Ringe der Dimension ∞.

Definition 3.32. Ein nullteilerfreier, ganzabgeschlossener noetherscher Ring der Dimension ≤ 1 heißt **Dedekindring**.

Beispiel 3.33. Jeder Hauptidealring ist ein Dedekindring.

Satz 3.34. *Sei A ein Dedekindring, $K = Q(A)$, $L|K$ endlich separabel, und $B = A_L$. Dann ist B ein Dedekindring und es gilt* $\dim B = \dim A$.

Bemerkung 3.35. Die Separabilitätsforderung ist entbehrlich, dann wird aber der Beweis schwerer.

Beweis von 3.34. B ist ganzabgeschlossen und noethersch nach 3.29. Bleibt z.z.: $\dim B = \dim A$.

1. Fall: $\dim A = 0$. Dann ist A ein Körper. B ist endliche nullteilerfreie A-Algebra. Für $b \in B$, $b \neq 0$, ist $\cdot b : B \to B$ ein injektiver Endomorphismus des e.d. A-Vektorraums B, also ein Isomorphismus. Folglich ist jedes $b \neq 0$ invertierbar und somit B ein Körper.

2. Fall: $\dim A = 1$. Z.z.:
   a) es gibt in B ein Primideal $\neq 0$.
   b) jedes Primideal $\neq 0$ in B ist maximal.

Zu a) Sei $a \in A \setminus (\{0\} \cup A^\times)$. Dann gilt $a \in B \setminus (\{0\} \cup B^\times)$.
Grund: Offenbar gilt $a \neq 0$ trivial. Angenommen es existiert $b \in B$ mit $ba = 1$. Dann gilt $b \in B \cap K = A$ im Widerspruch zu $a \notin A^\times$. Folglich gilt $(0) \subsetneqq aB \subsetneqq B$ und aB ist in einem Maximalideal $\neq (0)$ enthalten.

Zu b) Sei $\mathfrak{P} \subset B$ ein Primideal $\neq 0$. Dann ist das Primideal $\mathfrak{p} := \mathfrak{P} \cap A$ ungleich 0: Grund: Sei $b \in \mathfrak{P}$, $b \neq 0$. Dann existiert eine Gleichung

$$b^r + a_{r-1}b^{r-1} + \cdots + a_0 = 0,\ a_i \in A,\ a_0 \neq 0$$

$\Rightarrow a_0 \in \mathfrak{P} \cap A = \mathfrak{p}$.
Nun ist B, also auch $B/\mathfrak{P}$ eine endliche A-Algebra. Daher ist $B/\mathfrak{P}$ ist endliche Algebra über dem Körper $A/\mathfrak{p}$. Außerdem ist $B/\mathfrak{p}$ nullteilerfrei $\Rightarrow B/\mathfrak{P}$ ist Körper (siehe oben). □

Definition 3.36. Ein **Zahlkörper** ist ein endlicher Erweiterungskörper $K|\mathbb{Q}$. Der Ganzabschluss $\mathcal{O}_K$ von $\mathbb{Z}$ in K heißt **Ring der ganzen Zahlen** von K.

Korollar 3.37. *Für jeden Zahlkörper K ist $\mathcal{O}_K$ ein Dedekindring.*

Beweis. $\mathbb{Z}$ ist Hauptidealring also Dedekindring. Das Ergebnis folgt aus 3.34. □

Beispiel 3.38. Gilt $[K : \mathbb{Q}] = 2$, so heißt K **quadratischer Zahlkörper**. Es gilt $K = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Q}^\times \setminus \mathbb{Q}^{\times 2}$. Stillschweigend nehmen wir d stets als ganzzahlig und quadratfrei an.

Jedes Element von K hat eine eindeutige Darstellung $x = a + b\sqrt{d}$, $a, b \in \mathbb{Q}$. Es gilt

$$N_{K|\mathbb{Q}}(x) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2,$$

$$\mathrm{Sp}_{K|\mathbb{Q}}(x) = (a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a.$$

Da x Nullstelle des Polynoms $X^2 - \mathrm{Sp}(x)X + N(x)$ ist gilt

$$x \in \mathcal{O}_K \iff N(x), \mathrm{Sp}(x) \in \mathbb{Z}.$$

Satz 3.39. *Sei $K = \mathbb{Q}(\sqrt{d})$ ein quadratischer Zahlkörper.*

Ist $d \not\equiv 1 \bmod 4$ so gilt $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{d}$.

Für $d \equiv 1 \bmod 4$ gilt

$$\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right) = \left\{\frac{a+b\sqrt{d}}{2} \mid a, b \in \mathbb{Z},\ a \equiv b \bmod 2\right\}$$

Beweis. Sei $x = a + b\sqrt{d}$, $a, b \in \mathbb{Q}$. Nach den obigen Bemerkungen gilt

$$x \in \mathcal{O}_K \Longleftrightarrow 2a, a^2 - db^2 \in \mathbb{Z}$$

Für $a, b \in \mathbb{Z}$, d beliebig folgt $x \in \mathcal{O}_K$.
Sei $d \equiv 1 \bmod 4$ und $a = \frac{1}{2}A$, $b = \frac{1}{2}B$, $A, B \in \mathbb{Z}$, $A \equiv B \bmod 2$. Dann ist $a^2 - db^2 = \frac{1}{4}(A^2 - dB^2) \in \mathbb{Z}$ und $2a = A \in \mathbb{Z}$. Die angegebenen Elemente sind daher ganz.

Umgekehrt: Wegen $2a \in \mathbb{Z}$ ist $4db^2 = (2a)^2 - 4(a^2 - db^2) \in \mathbb{Z}$. Da d quadratfrei ist, folgt $2b \in \mathbb{Z}$. Also existieren $A, B \in \mathbb{Z}$, $2a = A$, $2b = B$. Aus $a^2 - db^2 \in \mathbb{Z}$ folgt $4 \mid (A^2 - dB^2)$. Für $d \not\equiv 1 \bmod 4$ ist dies nur für gerades A, B möglich, also $a, b \in \mathbb{Z}$. Ist $d \equiv 1 \bmod 4$ folgt $A \equiv B \bmod 2$. □

Bemerkung 3.40. Für $d = -5$ erhalten wir $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Dieser Ring ist nicht faktoriell, insbesondere kein Hauptidealring, aber ein Dedekindring.

Sei nun K wieder ein beliebiger Zahlkörper. Da $\mathbb{Z}$ ein Hauptidealring ist, existiert eine Ganzheitsbasis von $\mathcal{O}_K$ (über $\mathbb{Z}$) der Länge $n = [K : \mathbb{Q}]$. Sei

$$\mathcal{O}_K = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n.$$

Definition/Lemma 3.41. *Die Diskriminante $d(\alpha_1, \ldots, \alpha_n)$ hängt nicht von der Wahl der Basis ab. Sie heißt die* **Diskriminante des Zahlkörpers** *K. Bezeichnung $d_K = d(\alpha_1, \ldots, \alpha_n)$.*

Beweis. Es gilt

$$d(\alpha_1, \ldots, \alpha_n) = \det(\sigma_i \alpha_j)^2,$$

wobei $\{\sigma_1, \ldots, \sigma_n\} = \mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})$. Sei $(\alpha'_1, \ldots, \alpha'_n)$ eine andere Ganzheitsbasis und M die Übergangsmatrix. Es gilt $M \in Gl_n(\mathbb{Z})$, also gilt $\det(M) \in \mathbb{Z}^\times = \{\pm 1\}$ und

$$\begin{aligned} d(\alpha'_1, \ldots, \alpha'_n) &= \det(M)^2 \cdot d(\alpha_1, \ldots, \alpha_n) \\ &= d(\alpha_1, \ldots, \alpha_n) \end{aligned}$$

□

Beispiel 3.42. Ist $K = \mathbb{Q}(\sqrt{d})$ ein quadratischer Zahlkörper so gilt

$$d_K = \begin{cases} 4d, & d \not\equiv 1 \bmod 4, \\ d, & d \equiv 1 \bmod 4. \end{cases}$$

(Man benutze die angegebene Ganzheitsbasis).

3.4 Primzerlegung in Dedekindringen

Sei A ein Dedekindring. A ist nicht notwendig ein Hauptidealring. Aber wir werden im Laufe dieses Abschnitts das folgende Theorem zeigen:

Theorem 3.43. *Jedes Ideal $\mathfrak{a} \subset A$, $\mathfrak{a} \neq 0$ hat eine bis auf Reihenfolge eindeutige Zerlegung*

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n$$

in das Produkt von Primidealen $\neq 0$.

Konvention: Wenn nicht explizit anders gesagt, meinen wir von jetzt an mit Primideal stets Primideal $\neq 0$.

Lemma 3.44. *Jedes Ideal $\mathfrak{a} \neq 0$ umfaßt ein Produkt von Primidealen.*

Beweis. Angenommen $\mathfrak{a} \neq 0$ sei ein Ideal für das die Aussage falsch ist. Offenbar gilt $\mathfrak{a} \neq A$ und $\mathfrak{a}$ ist kein Primideal. Daher existieren $b_1, b_2 \in A$, $b_1, b_2 \notin \mathfrak{a}$, aber $b_1 b_2 \in \mathfrak{a}$. Setze

$$\begin{aligned} \mathfrak{a}_1 &= \mathfrak{a} + (b_1) \supsetneq \mathfrak{a} \\ \mathfrak{a}_2 &= \mathfrak{a} + (b_2) \supsetneq \mathfrak{a}. \end{aligned}$$

Es gilt

$$\begin{aligned} \mathfrak{a}_1\mathfrak{a}_2 &= (\mathfrak{a} + (b_1))(\mathfrak{a} + (b_2)) \\ &= \mathfrak{a}^2 + \mathfrak{a}(b_1) + \mathfrak{a}(b_2) + (b_1 b_2) \\ &\subset \mathfrak{a}. \end{aligned}$$

Enthalten $\mathfrak{a}_1$ und $\mathfrak{a}_2$ ein Produkt von Primidealen, so auch $\mathfrak{a}_1\mathfrak{a}_2$, also auch $\mathfrak{a}$. Daher ist die Aussage des Lemmas für mindestens eines der Ideale $\mathfrak{a}_1$, $\mathfrak{a}_2$ auch falsch. Wir erhalten induktiv eine nicht stationär werdende aufsteigende Folge von Idealen. Widerspruch zu A noethersch. □

Lemma 3.45. *Sei $\mathfrak{p}$ ein Primideal und $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ Ideale mit*

$$\mathfrak{a}_1 \cdots \mathfrak{a}_n \subset \mathfrak{p}.$$

Dann gilt $\mathfrak{a}_i \subset \mathfrak{p}$ für ein i.

Beweis. Anderenfalls können wir für jedes $i = 1, \ldots, n$ ein $a_i \in \mathfrak{a}_i \setminus \mathfrak{p}$ wählen und es würde $a_1 \cdots a_n \in \mathfrak{p}$ gelten. Aber $\mathfrak{p}$ ist prim. Widerspruch. □

Lemma 3.46. *Für einen A-Untermodul M von $K = Q(A)$ sind äquivalent*

(i) *M ist endlich erzeugter A-Modul.*
(ii) *es existiert ein $\alpha \in A$, $\alpha \neq 0$, mit $\alpha M \subset A$.*

Beweis. (i) $\Rightarrow$ (ii). Ist $M = Am_1 + \cdots + Am_n$ und $\alpha \in A$ so gewählt, dass $\alpha m_i \in A$, $i = 1, \ldots, n$, so gilt $\alpha M \subset A$.
(ii) $\Rightarrow$ (i). Gilt $\alpha M \subset A$ so ist αM als Ideal in A e.e. Sei $\alpha M = Aa_1 + \cdots + Aa_n$. Dann gilt $M = A\frac{a_1}{\alpha} + \cdots + A\frac{a_n}{\alpha}$. □

Definition 3.47. Ein A-Untermodul $M \subset K$, der die äquivalenten Bedingungen von 3.46 erfüllt heißt **gebrochenes Ideal** in K.

Bemerkung 3.48. Jedes Ideal $\mathfrak{a} \subset A$ ist ein gebrochenes Ideal. Zur besseren Unterscheidung werden wir diese oft als „ganze Ideale“ bezeichnen.

Definition 3.49. Für $x \in K$ heißt

$$xA = \{xa \mid a \in A\}$$

das zu x assoziierte **gebrochene Hauptideal**.

Operationen auf gebrochenen Idealen:

$$\begin{aligned} \mathfrak{a}_1 + \mathfrak{a}_2 &= \{a_1 + a_2 \mid a_1 \in \mathfrak{a}_1, a_2 \in \mathfrak{a}_2\} \\ \mathfrak{a}_1 \cap \mathfrak{a}_2 &= \text{was sonst} \\ \mathfrak{a}_1\mathfrak{a}_2 &= \{\sum_{\text{endl.}} a_i b_i \mid a_i \in \mathfrak{a}_1, b_i \in \mathfrak{a}_2\} \end{aligned}$$

d.h. genauso wie für gewöhnliche Ideale. Für Hauptideale gilt

$$(xA)(yA) = (xy)A.$$

Insbesondere gilt für $x \neq 0$:

$$(xA)(x^{-1}A) = A = (1).$$

d.h. von 0 verschiedene gebrochene Hauptideale haben ein Inverses bzgl. Multiplikation.

Definition 3.50. Für ein gebrochenes Ideal $\mathfrak{a} \subset K$, $\mathfrak{a} \neq 0$, sei $\mathfrak{a}^* = \{a \in K \mid a\mathfrak{a} \subset A\}$.

Lemma 3.51. *$\mathfrak{a}^*$ ist ein gebrochenes Ideal.*

Beweis. Zunächst ist $\mathfrak{a}^* \subset K$ ein A-Untermodul. Sei $x \in \mathfrak{a}$, $x \neq 0$, beliebig gewählt. Dann gilt $x\mathfrak{a}^* \subset A$. □

Lemma 3.52. (i) $\mathfrak{a} \subset \mathfrak{b} \Longrightarrow \mathfrak{b}^* \subset \mathfrak{a}^*$.

(ii) $\mathfrak{a} \subset A \Longleftrightarrow \mathfrak{a}^* \supset A$

(iii) *Für ein Primideal* $\mathfrak{p}$ *gilt* $\mathfrak{p}^* \supsetneq A$.

Beweis. (i) ist folgt durch Auswertung der Definitionen.
(ii) $\mathfrak{a} \subset A \Rightarrow 1 \in \mathfrak{a}^* \Rightarrow A \subset \mathfrak{a}^*$. Gilt $\mathfrak{a}^* \supset A$ folgt $1 \in \mathfrak{a}^*$, also $\mathfrak{a} = 1\mathfrak{a} \subset A$.
(iii) Sei $a \in \mathfrak{p}$, $a \neq 0$. Nach 3.44 existieren Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ mit $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subset (a) \subset \mathfrak{p}$. OE sei n minimal gewählt. Nach 3.45 gilt $\mathfrak{p}_i \subset \mathfrak{p}$ für ein i, etwa $\mathfrak{p}_1 \subset \mathfrak{p}$. Wegen $\dim A \leq 1$ folgt $\mathfrak{p}_1 = \mathfrak{p}$. Wegen $\mathfrak{p}_2 \cdots \mathfrak{p}_n \not\subset (a)$ (Im Fall $n = 1$ ist das leere Produkt gleich A) existiert ein $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_n$ mit $b \notin aA$ also $a^{-1}b \notin A$. Aber $b\mathfrak{p} \in \mathfrak{p}_2 \cdots \mathfrak{p}_n \cdot \mathfrak{p}_1 \subset (a)$, also $a^{-1}b \in \mathfrak{p}^*$. □

Lemma 3.53. *Sei* $\mathfrak{a} \subset A$ *und* $\mathfrak{a}^* = A$. *Dann gilt* $\mathfrak{a} = A$.

Beweis. Wäre $\mathfrak{a} \neq A$, so existierte ein Primideal $\mathfrak{p} \subset A$ mit $\mathfrak{a} \subset \mathfrak{p}$. Wir erhalten $\mathfrak{a}^* \supset \mathfrak{p}^* \supsetneq A$. Widerspruch □

Lemma 3.54. *Für* $\mathfrak{a} \subset A$ *gilt* $\mathfrak{a}\mathfrak{a}^* = A$.

Beweis. Sei $\mathfrak{b} = \mathfrak{a}\mathfrak{a}^* \subset A$. Z.z.: $\mathfrak{b} = A$. Es gilt

$$\mathfrak{a}(\mathfrak{a}^*\mathfrak{b}^*) = \mathfrak{b}\mathfrak{b}^* \subset A.$$

Daher gilt $\mathfrak{a}^*\mathfrak{b}^* \subset \mathfrak{a}^*$. Sei nun $\beta \in \mathfrak{b}^*$ beliebig. Wegen $1 \in \mathfrak{a}^*$ und $\beta \cdot \mathfrak{a}^* \subset \mathfrak{a}^*$ ist nach 3.4 (iii) (mit $M = \mathfrak{a}^*$) β ganz über A, also in A. Daher gilt $\mathfrak{b}^* \subset A$. Wegen $\mathfrak{b} \subset A$ folgt $\mathfrak{b}^* \supset A$, also $\mathfrak{b}^* = A$. Nach 3.53 folgt $\mathfrak{b} = A$. □

Theorem 3.55. *Die Menge der von* 0 *verschiedenen gebrochenen Ideale eines Dedekindrings bildet bzgl. Multiplikation eine abelsche Gruppe. Das Inverse zu* $\mathfrak{a}$ *ist durch*

$$\mathfrak{a}^{-1} = \{a \in K \mid a\mathfrak{a} \subset A\} \qquad [= a^*]$$

gegeben.

Bezeichnung dieser Gruppe: $J(A)$.

Beweis. Die gebrochenen Ideale bilden ein abelsches Monoid. Z.z. ist die Existenz Inverser. Sei $\mathfrak{a} \neq 0$ beliebig. Für $0 \neq x \in K$ gilt $\mathfrak{a}^* = (xA)(x\mathfrak{a})^*$.
Wählen wir x so, dass $x\mathfrak{a} \subset A$ gilt, so folgt nach 3.54

$$\mathfrak{a}^*\mathfrak{a} = (xA)(x\mathfrak{a})^*\mathfrak{a} = (x\mathfrak{a})^*(x\mathfrak{a}) = A.$$ □

Definition 3.56. Seien $\mathfrak{a}, \mathfrak{b} \subset A$ Ideale. Wir sagen $\mathfrak{a}$ teilt $\mathfrak{b}$ ($\mathfrak{a} \mid \mathfrak{b}$), wenn ein ganzes Ideal $\mathfrak{c} \subset A$ mit $\mathfrak{a}\mathfrak{c} = \mathfrak{b}$ existiert.

Satz 3.57. *Es gilt*

$$\mathfrak{a} \mid \mathfrak{b} \Longleftrightarrow \mathfrak{b} \subset \mathfrak{a}.$$

Beweis. $\Rightarrow$: Aus $\mathfrak{ac} = \mathfrak{b}$ und $\mathfrak{c} \subset A$ folgt $\mathfrak{b} = \mathfrak{ac} \subset \mathfrak{a}A = \mathfrak{a}$.
$\Leftarrow$ $\mathfrak{a} = (0)$ teilt nur sich selbst, also sei $\mathfrak{a} \neq 0$. Sei $\mathfrak{b} \subset \mathfrak{a}$. Dann ist

$$\mathfrak{c} = \mathfrak{a}^{-1}\mathfrak{b} \subset \mathfrak{a}^{-1}\mathfrak{a} = A$$

ein ganzes Ideal und es gilt $\mathfrak{ac} = \mathfrak{b}$. □

Korollar 3.58. *Für ein ganzes Ideal $0 \neq \mathfrak{a} \subsetneqq A$ gilt $\mathfrak{a}^{n+1} \subsetneqq \mathfrak{a}^n$ für alle $n \in \mathbb{N}$. D.h. wir erhalten eine strikt fallende Folge von Idealen*

$$A \supsetneqq \mathfrak{a} \supsetneqq \mathfrak{a}^2 \supsetneqq \mathfrak{a}^3 \supsetneqq \cdots$$

Beweis. Es gilt $\mathfrak{a}^{n+1} = \mathfrak{a}^n\mathfrak{a} \subset \mathfrak{a}^n A = \mathfrak{a}^n$. Aus $\mathfrak{a}^n = \mathfrak{a}^{n+1}$ würde durch Multiplikation mit $\mathfrak{a}^{-n}$ die Gleichheit $A = \mathfrak{a}$ folgen. □

Beweis von Theorem 3.43. Sei $\mathfrak{a} \subset A$, $\mathfrak{a} \neq 0$, ein ganzes Ideal. Der Fall $\mathfrak{a} = A$ ist formal (A =leeres Produkt von Primidealen). Sei $\mathfrak{a} \subsetneqq A$. Da jedes echte Ideal in einem Primideal liegt und wegen 3.44 finden wir Primideale $\mathfrak{p}, \mathfrak{p}_1, \ldots, \mathfrak{p}_n$ mit

$$\mathfrak{p}_1 \cdots \mathfrak{p}_n \subset \mathfrak{a} \subset \mathfrak{p}.$$

Nach 3.45 ist (OE) $\mathfrak{p}_1 \subset \mathfrak{p}$ und daher $\mathfrak{p}_1 = \mathfrak{p}$. Dann gilt

$$\mathfrak{p}_2 \cdots \mathfrak{p}_n \subseteq \mathfrak{p}_1^{-1}\mathfrak{a} \subset A.$$

Gilt $\mathfrak{p}_1^{-1}\mathfrak{a} = A$, so folgt $\mathfrak{a} = \mathfrak{p}_1$. Ansonsten ist $\mathfrak{p}_1^{-1}A$ in einem Primideal enthalten und wir erhalten induktiv nach $r \leq n$ Schritten

$$\mathfrak{p}_r^{-1}\mathfrak{p}_{r-1}^{-1} \ldots \mathfrak{p}_1^{-1}\mathfrak{a} = A,$$

also $\mathfrak{a} = \mathfrak{p}_1, \ldots, \mathfrak{p}_r$. Es verbleibt die Eindeutigkeit zu zeigen. Sei

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n = \mathfrak{q}_1 \cdots \mathfrak{q}_m.$$

Es gilt $\mathfrak{a} \subset \mathfrak{p}_1$ und nach 3.45 gilt (OE) $\mathfrak{q}_1 \subset \mathfrak{p}_1$, also $\mathfrak{p}_1 = \mathfrak{q}_1$. Multiplikation mit $\mathfrak{p}_1^{-1}$ gibt

$$\mathfrak{p}_2 \cdots \mathfrak{p}_n = \mathfrak{q}_2 \cdots \mathfrak{q}_m.$$

Dieser Prozess bricht ab und wir erhalten $n = m$ und nach Umnummerierung $\mathfrak{p}_i = \mathfrak{q}_i$. □

Korollar 3.59. *Jedes gebrochene Ideal $\mathfrak{a} \neq 0$ hat eine eindeutige Darstellung der Form*

$$\mathfrak{a} = \prod_{\mathfrak{p}\, PI} \mathfrak{p}^{v_\mathfrak{p}}, \quad v_\mathfrak{p} \in \mathbb{Z},\ v_\mathfrak{p} = 0 \ \textit{ f.f.a. } \mathfrak{p}.$$

Mit anderen Worten: $J(A)$ ist die freie abelsche Gruppe über der Menge der Primideale von A.

Beweis. Schreibe $\mathfrak{a} = \mathfrak{b} \cdot \mathfrak{c}^{-1}$ mit $\mathfrak{b}, \mathfrak{c} \subset A$ und wende 3.43 an. □

Beispiel 3.60. Wir betrachten die Zerlegung

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

in $\mathbb{Z}[\sqrt{-5}] = \mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$.

Sei

$$\mathfrak{p} = (2, 1 + \sqrt{-5}) = 2\mathbb{Z}[\sqrt{-5}] + (1 + \sqrt{-5})\mathbb{Z}[\sqrt{-5}]$$

und

$$\begin{aligned} \mathfrak{q}_1 &= (3, 1 + \sqrt{-5}), \\ \mathfrak{q}_2 &= (3, 1 - \sqrt{-5}). \end{aligned}$$

Dann gilt mit $A = \mathbb{Z}[\sqrt{-5}]$:

$$\begin{aligned} \mathfrak{p}^2 &= (4, 2(1 + \sqrt{-5}), (1 + \sqrt{-5})^2) \\ &= (4, 2 + 2\sqrt{-5}, -4 + 2\sqrt{-5}) \\ &\subset (2). \end{aligned}$$

Wegen $2 = (2 + 2\sqrt{-5}) - 4 - (-4 + 2\sqrt{-5}) \in \mathfrak{p}^2$, folgt $\mathfrak{p}^2 = (2)$.

Analog

$$\begin{aligned} \mathfrak{q}_1\mathfrak{q}_2 &= (9, 3(1 + \sqrt{-5}), 3(1 - \sqrt{-5}), 6) \\ &\subset (3) \end{aligned}$$

und $3 = 9 - 6 \in \mathfrak{q}_1\mathfrak{q}_2$, also $\mathfrak{q}_1\mathfrak{q}_2 = (3)$.

Außerdem berechnet man leicht:

$$\begin{aligned} \mathbb{Z}[\sqrt{-5}]/\mathfrak{p} &\cong \mathbb{Z}/2\mathbb{Z} \\ \mathbb{Z}[\sqrt{-5}]/\mathfrak{q}_i &\cong \mathbb{Z}/3\mathbb{Z} \quad \text{für} \quad i = 1, 2, \end{aligned}$$

also sind $\mathfrak{p}, \mathfrak{q}_1, \mathfrak{q}_2$ Primideale.

Wegen $2 \notin \mathfrak{q}_1$ (sonst $1 = 3 - 2 \in \mathfrak{q}_1$) gilt $1 - \sqrt{-5} = 2 - (1 + \sqrt{-5}) \notin \mathfrak{q}_1$ also $\mathfrak{q}_2 \neq \mathfrak{q}_1$. Folglich ist

$$(6) = \mathfrak{p}^2\mathfrak{q}_1\mathfrak{q}_2$$

die eindeutige Primidealzerlegung von (6). Schon berechnet: $(2) = \mathfrak{p}^2$, $(3) = \mathfrak{q}_1\mathfrak{q}_2$. Zudem gilt

$$\begin{aligned} (1 + \sqrt{-5}) &= \mathfrak{p}\mathfrak{q}_1, \\ (1 - \sqrt{-5}) &= \mathfrak{p}\mathfrak{q}_2. \end{aligned}$$

Z.B.

$$\mathfrak{p}\mathfrak{q}_1 = (6, 2(1 + \sqrt{-5}), 3(1 + \sqrt{-5}), (1 + \sqrt{-5})^2),$$

also $\mathfrak{p}\mathfrak{q}_1 \subset (1 + \sqrt{-5})$. Andererseits gilt

$$(1 + \sqrt{-5}) = 3(1 + \sqrt{-5}) - 2(1 + \sqrt{-5}) \in \mathfrak{p}\mathfrak{q}_1.$$

Für ganze Ideale $0 \neq \mathfrak{a}, \mathfrak{b} \subset A$ kann man nun mit Hilfe von 3.43 in natürlicher Weise den ggT definieren. Ist $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$, $\mathfrak{b} = \mathfrak{p}_1^{f_1} \cdots \mathfrak{p}_n^{f_n}$ (Exponent $= 0$ erlaubt), so setzt man

$$\mathrm{ggT}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{p}_1^{\min(e_1, f_1)} \cdots \mathfrak{p}_n^{\min(e_n, f_n)}.$$

Satz 3.61. *Für $0 \neq \mathfrak{a}, \mathfrak{b} \subset A$ gilt* $\mathrm{ggT}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$.

Beweis. Nach 3.57 ist der ggT das kleinste Ideal, das sowohl $\mathfrak{a}$ also auch $\mathfrak{b}$ umfasst, also $\mathfrak{a} + \mathfrak{b}$. □

Satz 3.62. *Für ein ganzes Ideal $\mathfrak{a} \subsetneq A$ gilt*

$$\bigcap_{n=1}^{\infty} \mathfrak{a}^n = (0).$$

Beweis. $\mathfrak{b} := \bigcap_{n=1}^{\infty} \mathfrak{a}^n$ ist ein Ideal, das durch beliebige Potenzen von $\mathfrak{a}$ teilbar ist. Für $\mathfrak{b} \neq (0)$ würde dies der eindeutigen Primzerlegung widersprechen. □

Bemerkung 3.63. Die Eigenschaft aus 3.62 heißt: „A ist $\mathfrak{a}$-adisch separiert“. Sie gilt allgemeiner für nullteilerfreie noethersche Ringe (siehe Algebra 2, 24.17).

Um nun doch effektiv mit Elementen von A rechnen zu können muss man die folgenden Effekte untersuchen:

1) Wie weit weichen Ideale davon ab Hauptideal zu sein?
2) Wie weit bestimmt ein Hauptideal seinen Erzeuger?

Zu 2) Wegen $(x) = (y) \Longleftrightarrow x = uy$, $u \in A^\times$ müssen wir die Einheitengruppe von A bestimmen.

Zu 1)

Definition 3.64. Sei $P(A) \subset J(A)$ die Untergruppe der gebrochenen Hauptideale $\neq 0$. Die Faktorgruppe

$$Cl(A) := J(A)/P(A)$$

heißt die **Idealklassengruppe** von A.

Wir werden $A^\times$ und $Cl(A)$ im Fall $A = \mathcal{O}_K$, K Zahlkörper genauer untersuchen.

3.5 Idealnorm

Im ganzen Abschnitt sei $K|\mathbb{Q}$ eine endliche Erweiterung. Dann ist $\mathcal{O}_K$ ein Dedekindring. Als abelsche Gruppe gilt (nach 3.22) $\mathcal{O}_K \cong \mathbb{Z}^n$, $n = [K : \mathbb{Q}]$. Ist $\mathfrak{a} \subset \mathcal{O}_K$, $\mathfrak{a} \neq (0)$ ein Ideal und $0 \neq \alpha \in \mathfrak{a}$, so gilt

$$\alpha\mathcal{O}_K \subset \mathfrak{a} \subset \mathcal{O}_K$$

und deshalb auch $\mathfrak{a} \cong \mathbb{Z}^n$. Folglich ist $\mathrm{Rg}_{\mathbb{Z}}(\mathcal{O}_K/\mathfrak{a}) = n - n = 0$ und deshalb ist $\mathcal{O}_K/\mathfrak{a}$ als endlich erzeugte abelsche Gruppe vom Rang Null endlich.

Definition 3.65. Die **Norm** eines Ideals $\mathfrak{a} \subset \mathcal{O}_K$ ist definiert durch

$$\mathfrak{N}(\mathfrak{a}) = \begin{cases} 0, & \mathfrak{a} = 0, \\ \#\mathcal{O}_K/\mathfrak{a}, & \mathfrak{a} \neq 0. \end{cases}$$

Satz 3.66. *Für $a \in \mathcal{O}_K$ gilt*

$$\mathfrak{N}(a\mathcal{O}_K) = |N_{K|\mathbb{Q}}(a)|.$$

Beweis. Es gilt $\mathfrak{N}(a\mathcal{O}_K) = \#\mathrm{coker}\,(\varphi_a)$,

$$\varphi_a : \mathcal{O}_K \hookrightarrow \mathcal{O}_K,\ x \longmapsto ax.$$

Wir stellen φ_a bzgl. einer $\mathbb{Z}$-Basis von $\mathcal{O}_K$ als Matrix dar. Basiswechsel in Quelle und Ziel mit Matrizen aus $Gl_n(\mathbb{Z})$ lassen $\mathrm{coker}\,\varphi_a$ invariant und ändern $\det\varphi_a$ höchstens um ein Vorzeichen. Nach dem Elementarteilersatz für den Hauptidealring $\mathbb{Z}$ hat φ_a nach geeignetem Basiswechsel die Matrixform

$$\begin{pmatrix} e_1 & & \\ & \ddots & \\ & & e_n \end{pmatrix}, \quad e_1 \mid e_2 \mid \cdots \mid e_n.$$

Es gilt $N_{K|\mathbb{Q}}(a) = \det\varphi_a = \pm e_1 \cdots e_n$ und

$$\mathrm{coker}\,\varphi_a = \mathbb{Z}/e_1\mathbb{Z} \times \cdots \times \mathbb{Z}/e_n\mathbb{Z},$$

also $\#\mathrm{coker}\,\varphi_a = |e_1 \cdots e_n| = |N_{K|\mathbb{Q}}(a)|$. □

Lemma 3.67. *Für $\mathfrak{a}, \mathfrak{b} \subset \mathcal{O}_K$ teilerfremd gilt $\mathfrak{N}(\mathfrak{ab}) = \mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{b})$.*

Beweis. Nach dem Chinesischen Restsatz gilt

$$\mathcal{O}_K/\mathfrak{ab} \cong \mathcal{O}_K/\mathfrak{a} \times \mathcal{O}_K/\mathfrak{b}.$$ □

Jetzt eliminieren wir die Voraussetzung der Teilerfremdheit.

Lemma 3.68. *Sei A ein Dedekindring und $\mathfrak{a}, \mathfrak{b} \subset A$ Ideale $\neq 0$. Dann existiert ein zu $\mathfrak{a}$ teilerfremdes Ideal $\mathfrak{c} \subset A$, $\mathfrak{c} \neq 0$, so dass $\mathfrak{bc}$ ein Hauptideal ist.*

Beweis. Sei $\mathfrak{a} = \mathfrak{p}_1^{a_1} \dots \mathfrak{p}_n^{a_n}$, $\mathfrak{b} = \mathfrak{p}_1^{b_1} \dots \mathfrak{p}_n^{b_n}$ (Exponent 0 zugelassen). Nach 3.62 existiert für jedes i ein $\alpha_i \in \mathfrak{p}_i^{b_i} \smallsetminus \mathfrak{p}_i^{b_i+1}$. Nach dem Chinesischen Restsatz finden wir $\alpha \in A$ mit $\alpha \equiv \alpha_i \bmod \mathfrak{p}_i^{b_i+1}$, $i = 1, \dots, n$. Die Primidealzerlegung von (α) sieht so aus:

$$(\alpha) = \mathfrak{p}_1^{b_1} \cdots \mathfrak{p}_n^{b_n} \cdot (\text{Produkt von Primidealen die nicht in } \mathfrak{a} \text{ und } \mathfrak{b} \text{ vorkommen})$$

Wir benennen das letzte Produkt mit $\mathfrak{c}$, also $(\alpha) = \mathfrak{p}_1^{b_1} \cdots \mathfrak{p}_n^{b_n} \cdot \mathfrak{c}$.

Dann gilt $\mathfrak{a} + \mathfrak{c} = A$ und $\mathfrak{bc} = (\alpha)$. □

Lemma 3.69. *Seien $\mathfrak{a}$, $\mathfrak{b} \subset A$ Ideale $\neq 0$. Dann gibt es einen Isomorphismus von A-Moduln $A/\mathfrak{a} \xrightarrow{\sim} \mathfrak{b}/\mathfrak{ab}$.*

Beweis. Wir wählen $\mathfrak{c}$ wie in 3.68: $\mathfrak{a} + \mathfrak{c} = A$, $\mathfrak{bc} = (\alpha)$, $\alpha \in A$. Wir betrachten die Abbildung

$$\varphi : A \longrightarrow \mathfrak{b}/\mathfrak{ab}, \quad x \longmapsto \alpha x \bmod \mathfrak{ab}.$$

Wegen $\alpha \in \mathfrak{bc} \subset \mathfrak{b}$ ist die Abbildung definiert. Nun gilt

$$\begin{aligned} \ker(\varphi) &= \{x \in A \mid \alpha x \in \mathfrak{ab}\} \\ &= \mathfrak{ab} \cdot (\alpha)^{-1} \cap A \\ &= \mathfrak{ac}^{-1} \cap A \\ &= \mathfrak{c}^{-1}(\mathfrak{a} \cap \mathfrak{c}) \\ (\mathfrak{a} + \mathfrak{c} = (1)): \quad &= \mathfrak{c}^{-1}(\mathfrak{ac}) = \mathfrak{a}. \end{aligned}$$

Bleibt die Surjektivität von φ zu zeigen: Es gilt $\mathfrak{a} + \mathfrak{c} = A \Rightarrow \mathfrak{ab} + \mathfrak{bc} = \mathfrak{b} \Rightarrow \mathfrak{ab} + (\alpha) = \mathfrak{b}$. □

Satz 3.70. *Für Ideale $\mathfrak{a}, \mathfrak{b} \subset \mathcal{O}_K$ gilt $\mathfrak{N}(\mathfrak{ab}) = \mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{b})$.*

Beweis. Ist $\mathfrak{a} = 0$ oder $\mathfrak{b} = 0$, so ist die Aussage trivial. Sei $\mathfrak{a} \neq 0 \neq \mathfrak{b}$. Dann gilt:

$$\begin{aligned} \mathfrak{N}(\mathfrak{ab}) = \#\mathcal{O}_K/\mathfrak{ab} &= (\#\mathcal{O}_K/\mathfrak{b})\#(\mathfrak{b}/\mathfrak{ab}) \\ 3.69: &= \mathfrak{N}(\mathfrak{b}) \cdot \#(\mathcal{O}_K/\mathfrak{a}) \\ &= \mathfrak{N}(\mathfrak{a}) \cdot \mathfrak{N}(\mathfrak{b}). \end{aligned}$$

□

Satz 3.71. *Sei $K|\mathbb{Q}$ galoissch. Dann gilt*

$$\prod_{\sigma \in \mathrm{Gal}(K|\mathbb{Q})} \sigma(\mathfrak{a}) = \mathfrak{N}(\mathfrak{a}) \cdot \mathcal{O}_K.$$

Erläuterung: Für $\sigma \in \mathrm{Gal}(K|\mathbb{Q})$ und $\alpha \in \mathcal{O}_K$ gilt $\sigma(\alpha) \in \mathcal{O}_K$. Daher ist mit $\mathfrak{a}$ auch $\sigma(\mathfrak{a}) \subset \mathcal{O}_K$ ein Ideal: $\alpha \in \mathcal{O}_K$, $a \in \sigma(\mathfrak{a}) \Rightarrow \alpha a = \sigma(\sigma^{-1}(\alpha)a) \in \sigma(\mathfrak{a})$.

Wir beweisen den Satz später.

Jetzt verallgemeinern wir den Begriff der Diskriminante. Wie oben sehen wir: Jedes gebrochene Ideal $0 \neq \mathfrak{a} \subset K$ ist als abelsche Gruppe $\cong \mathbb{Z}^n$ und für $\mathfrak{a} \subset \mathfrak{a}'$ gilt: $(\mathfrak{a}' : \mathfrak{a}) < \infty$

Definition 3.72. Sei $0 \neq \mathfrak{a} \subset K$ ein gebrochenes Ideal und

$$\mathfrak{a} = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n.$$

Wir setzen

$$d(\mathfrak{a}) = d(\alpha_1, \ldots, \alpha_n) = \det(\mathrm{Sp}_{K|\mathbb{Q}}(\alpha_i\alpha_j)).$$

Diese Definition hängt nicht von der Wahl der Basis $\alpha_1, \ldots, \alpha_n$ ab. Nach 3.20 gilt $d(\alpha_1, \ldots, \alpha_n) = \det(\sigma_i\alpha_j)^2$ wobei $\{\sigma_1, \ldots, \sigma_n\} = \mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})$.

Satz 3.73. *Sind $0 \neq \mathfrak{a} \subset \mathfrak{a}' \subset K$ gebrochene Ideale, so gilt*

$$d(\mathfrak{a}) = (\mathfrak{a}' : \mathfrak{a})^2 d(\mathfrak{a}').$$

Insbesondere gilt für ein ganzes Ideal $\mathfrak{a} \subset \mathcal{O}_K$

$$d(\mathfrak{a}) = \mathfrak{N}(\mathfrak{a})^2 \cdot d_K.$$

Beweis. Sei $M \in Gl_n(\mathbb{Q})$ die Basiswechselmatrix von einer Basis von $\mathfrak{a}'$ zu einer von $\mathfrak{a}$. Wegen $\mathfrak{a} \subset \mathfrak{a}'$ gilt $M \in M_{n,n}(\mathbb{Z})$. Wir erhalten $d(\mathfrak{a}) = \det(M)^2 \cdot d(\mathfrak{a}')$. Durch Ändern der Basen bekommen wir M auf Diagonalform (Elementarteilersatz) und sehen

$$|\det(M)| = (\mathfrak{a}' : \mathfrak{a}).$$

Dies zeigt die erste Behauptung. Die zweite folgt, da per definitionem $d_K = d(\mathcal{O}_K)$, $\mathfrak{N}(\mathfrak{a}) = (\mathcal{O}_K : \mathfrak{a})$. □

4 Endlichkeitssätze für Zahlkörper

4.1 Gitter

Definition 4.1. Sei V ein n-dimensionaler $\mathbb{R}$-Vektorraum. Ein **Gitter** in V ist eine Untergruppe der Form

$$\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m$$

mit linear unabhängigen Vektoren $v_1, \ldots, v_m$ in V. Das m-Tupel $(v_1, \ldots, v_m)$ heißt **Basis** von Γ und die Menge

$$\Phi = \Phi(v_1, \ldots, v_m) = \{x_1v_1 + \cdots + x_mv_m \mid x_i \in \mathbb{R} \quad 0 \leq x_i \leq 1\}$$

heißt **Grundmasche**. Das Gitter heißt **vollständig**, wenn $m = n$.

Bemerkungen 4.2. 1) Begriffe wie beschränkt in V, abgeschlossen in V usw. hängen nicht von der Identifikation $V \cong \mathbb{R}^n$ ab!
2) Γ ist genau dann vollständig, wenn die Translate $\Phi + \gamma$, $\gamma \in \Gamma$, ganz V überdecken.
3) nicht jede e.e. Untergruppe von V ist ein Gitter, z.B. $\mathbb{Z} + \mathbb{Z}\sqrt{2} \subset \mathbb{R}$ ist kein Gitter.
4) Ein Gitter ist eine *diskrete Teilmenge*, d.h. zu $\gamma \in \Gamma$ existiert eine offene Umgebung U von γ in V mit $U \cap \Gamma = \{\gamma\}$.

Grund: Ergänze $v_1, \ldots, v_m$ durch Vektoren $v_{m+1}, \ldots, v_n$ zu einer Basis von V. Für $\gamma = a_1 v_1 + \cdots + a_m v_m \in \Gamma$ setze

$$U = \{x_1 v_1 + \cdots + x_n v_n \mid |a_i - x_i| < 1, \quad i = 1, \ldots, m\}.$$

Satz 4.3. *Eine Untergruppe $\Gamma \subset V$ ist genau dann ein Gitter, wenn sie diskret ist.*

Beweis. Gitter sind diskret. Sei $\Gamma \subset V$ eine diskrete Untergruppe.
Behauptung: Γ hat keine Häufungspunkte in V.
Grund: Da

$$V \times V \longrightarrow V, \ (v, w) \longmapsto v - w,$$

stetig ist, gibt es zu jeder offenen Umgebung U der 0 eine offene Umgebung U' der 0 mit $v, w \in U' \Rightarrow v - w \in U$. Wäre nun $x \in V$ ein Häufungspunkt von Γ, so ist nach der Definition der Durchschnitt $(x + U') \cap \Gamma$ unendlich. Insbesondere existieren $\gamma_1, \gamma_2 \in (x + U') \cap \Gamma$, $\gamma_1 \neq \gamma_2$, also $0 \neq \gamma_1 - \gamma_2 \in U' - U' \subset U$. Wählen wir nun U so klein, dass $U \cap \Gamma = \{0\}$ ist, erhalten wir ein Widerspruch.

Sei nun V_0 der von Γ in V erzeugte $\mathbb{R}$-Untervektorraum und $m = \dim_{\mathbb{R}} V_0$. Sei $u_1, \ldots, u_m$ eine in Γ gelegene Basis von V_0. Setze

$$\Gamma_0 = \mathbb{Z}u_1 + \cdots + \mathbb{Z}u_m \subset \Gamma.$$

Dann ist Γ_0 ein vollständiges Gitter in V_0.

Behauptung: $(\Gamma : \Gamma_0) < \infty$.

Beweis der Behauptung: Sei $\Phi_0 \subset V_0$ die Grundmasche zur Basis $u_1, \ldots, u_m$ von Γ_0. Da Γ_0 vollständiges Gitter in V_0 ist, gilt

$$V_0 = \bigcup_{\gamma \in \Gamma_0} \gamma + \Phi_0.$$

Möge $\gamma_i \in \Gamma$ über ein Repräsentantensystem von Γ/Γ_0 laufen. Dann schreiben wir $\gamma_i = \mu_i + \gamma_{0i}$ mit $\mu_i \in \Phi_0$, $\gamma_{0i} \in \Gamma_0$. Die $\mu_i = \gamma_i - \gamma_{0i} \in \Gamma$ liegen in der beschränkten Menge Φ_0 und haben keine Häufungspunkt in $V \Rightarrow$ es sind nur endlich viele.

Sei nun $q = (\Gamma : \Gamma_0)$. Dann gilt $q\Gamma \subset \Gamma_0$, also $\Gamma \subset \frac{1}{q}\Gamma_0$. Daher ist Γ als Untergruppe einer freien abelschen Gruppe von endlichem Rang selbst frei, d.h. es existiert eine $\mathbb{Z}$-Basis $v_1, \ldots, v_r$ von Γ, $r \leq m$. Nun erzeugt Γ den Vektorraum V_0, also erzeugen $v_1, \ldots, v_r$ ganz $V_0 \Rightarrow r = m$ und $v_1, \ldots, v_m$ sind linear unabhängig. □

Lemma 4.4. *Ein Gitter $\Gamma \subset V$ ist genau dann vollständig wenn eine beschränkte Teilmenge $M \subset V$ existiert, so dass*

$$V = \bigcup_{\gamma \in \Gamma} \gamma + M.$$

Beweis. Ist Γ vollständig, so wähle für M eine Grundmasche. Umgekehrt sei M wie oben. Sei V_0 der durch Γ aufgespannte Unterraum. Gilt $V_0 = V$, sind wir fertig. Ansonsten wählen wir eine beliebige Metrik auf V, d.h. wir machen V zu einem euklidischen Vektorraum. Da M beschränkt ist liegt jeder Punkt $x \in V$ mit $d(x, V_0)$ hinreichend groß nicht in $V_0 + M \supset \Gamma + M$. Widerspruch. □

Definition 4.5. Eine Teilmenge $X \subset V$ heißt **zentralsymmetrisch**, wenn gilt:

$$x \in X \Rightarrow -x \in X,$$

und **konvex**, falls

$$x, y \in X \Rightarrow \{\lambda x + (1-\lambda)y \mid 0 \leq \lambda \leq 1\} \subset X.$$

Theorem 4.6 (Minkowskischer Gitterpunktsatz)**.** *Sei Γ ein vollständiges Gitter in einem euklidischen Vektorraum V und sei X eine (meßbare) zentralsymmetrische, konvexe Teilmenge in V. Gilt*

$$\mathrm{vol}(X) > 2^n \mathrm{vol}(\Gamma),$$

so enthält X mindestens einen von 0 verschiedenen Gitterpunkt $\gamma \in \Gamma$.

Beweis. Es g.z.z., dass $\gamma_1, \gamma_2 \in \Gamma$, $\gamma_1 \neq \gamma_2$, mit $(\frac{1}{2}X + \gamma_1) \cap (\frac{1}{2}X + \gamma_2) \neq \varnothing$ existieren (nutze konvex + zentralsymmetrisch). Wären diese Teilmengen alle disjunkt, so gilt nach Schneiden mit der Grundmasche Φ:

$$\mathrm{vol}(\Phi) \geq \sum_{\gamma \in \Gamma} \mathrm{vol}(\Phi \cap (\tfrac{1}{2}X + \gamma)).$$

Nun induziert Translation mit $-\gamma$:

$$\mathrm{vol}(\Phi \cap (\frac{1}{2}X + \gamma)) = \mathrm{vol}((\Phi - \gamma) \cap \frac{1}{2}X),$$

und weil die $(\Phi - \gamma) \cap \frac{1}{2}X$ die Menge $\frac{1}{2}X$ disjunkt zerlegen, folgt

$$\begin{aligned} \mathrm{vol}(\Phi) &\geq \sum_{\gamma \in \Gamma} \mathrm{vol}((\Phi - \gamma) \cap \tfrac{1}{2}X) \\ &= \mathrm{vol}(\tfrac{1}{2}X) = \tfrac{1}{2^n}\mathrm{vol}(X), \end{aligned}$$

im Widerspruch zur Annahme. □

4.2 Minkowski-Theorie

(altmodisch: „Geometrie der Zahlen“)

Sei $K|\mathbb{Q}$ ein Zahlkörper, $n = [K : \mathbb{Q}]$. Dann gilt $\#\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C}) = n$.

Ziel: Wir machen den n-dimensionalen $\mathbb{R}$-Vektorraum $K_{\mathbb{R}} := K \otimes_{\mathbb{Q}} \mathbb{R}$ zu einem euklidischen Vektorraum.

Zunächst erinnern wir an die lineare Unabhängigkeit von *Charakteren*: Sei G eine Gruppe und K ein Körper. Dann bezeichnet man einen Gruppenhomorphismus $G \to K^\times$ als K-wertigen Charakter der Gruppe G.

Die Menge der Abbildungen $\mathrm{Abb}(G, K)$ wird zum K-Vektorraum durch wertweise Addition und Skalarmultiplikation, d.h.

$$(a_1\phi_1 + a_2\phi_2)(g) := a_1\phi_1(g) + a_2\phi_2(g)$$

$\phi_1, \phi_2 \in \mathrm{Abb}(G, K),\ a_1, a_2 \in K,\ g \in G$. Über die (Mengen)abbildung $K^\times \hookrightarrow K$ können K-wertige Charaktere von G als Elemente des Vektorraums $\mathrm{Abb}(G, K)$ aufgefasst werden.

Satz 4.7. *Verschiedene Charaktere $\chi_1, \ldots, \chi_n$ einer Gruppe G mit Werten in einen Körper K sind linear unabhängig als Elemente im K-Vektorraum* $\mathrm{Abb}(G, K)$.

Beweis. Siehe Algebra 1, 4.53 oder Bosch: „Algebra“ §4.6. Satz 2. □

Sei nun $L|K$ und $M|K$ Körpererweiterungen. Die Menge $\mathrm{Hom}_K(L, M)$ (Körperhomorphismen) ist eine Teilmenge des K-Vektorraums $\mathrm{Hom}_{K\text{-VR}}(L, M)$ (K-Vektorraumhomomorphismen). Die K-Vektorraumstruktur setzt sich zu einer M-Vektorraumstruktur fort durch

$$(\alpha\phi)(x) = \alpha\phi(x), \quad \alpha \in M,\ x \in L,\ \phi \in \mathrm{Hom}_{K\text{-VR}}(L, M).$$

Auf diese Weise wird $\mathrm{Hom}_{K\text{-VR}}(L, M)$ ein M-Untervektorraum von $\mathrm{Abb}(L, M)$. Die Menge $\mathrm{Hom}_{K\text{-VR}}(L, M)$ der K-Vektorraumhomomorphismen von L nach M ist in natürlicher Weise ein K-Vektorraum. Die K-Vektorraumstruktur setzt sich zu einer M-Vektorraumstruktur fort durch

$$(\alpha\phi)(a) = \alpha\phi(a), \quad \alpha \in M,\ a \in L,\ \phi \in \mathrm{Hom}_K(L, M).$$

Auf diese Weise wird $\mathrm{Hom}_{K\text{-VR}}(L, M)$ ein M-Untervektorraum von $\mathrm{Abb}(L, M)$.

Satz 4.8 (Algebra 2, 4.54)**.** *Es ist* $\mathrm{Hom}_K(L, M)$ *eine linear unabhängige Menge von Vektoren im M-Vektorraum* $\mathrm{Hom}_{K\text{-}VR}(L, M) \subset \mathrm{Abb}(L, M)$.

Sei nun K wieder ein Zahlkörper, die Rolle von M wird durch den Körper $\mathbb{C}$ übernommen. Wir betrachten die $\mathbb{Q}$-Bilinearform

$$K \times \mathbb{C} \to \prod_{\tau \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})} \mathbb{C}, \qquad (x, \alpha) \mapsto ((\tau x) \cdot \alpha)_\tau.$$

Diese induziert

$$\phi : K \otimes_{\mathbb{Q}} \mathbb{C} \longrightarrow \prod_\tau \mathbb{C}, \quad x \otimes \alpha \longmapsto (\tau x \cdot \alpha)_\tau$$

Es ist ϕ bezüglich der natürlichen $\mathbb{C}$-Vektorraum-Strukturen von Quelle und Ziel ein $\mathbb{C}$-Vektorraumhomomorphismus.

Lemma 4.9. *Es ist*

$$\phi : K_{\mathbb{C}} := K \otimes_{\mathbb{Q}} \mathbb{C} \xrightarrow{\sim} \prod_{\tau \in \mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C})} \mathbb{C} \quad \cong \mathbb{C}^n$$

ein Isomorphismus von $\mathbb{C}$*-Vektorräumen.*

Beweis. Es gilt

$$\dim(\prod_{\tau} \mathbb{C}) = n \quad \text{und} \quad \dim_{\mathbb{C}}(K \otimes_{\mathbb{Q}} \mathbb{C}) = \dim_{\mathbb{Q}} K = n.$$

Daher genügt es zu zeigen, dass ϕ injektiv ist. Sei $x_1, \ldots, x_n$ eine $\mathbb{Q}$-Basis von K. Nach Satz 4.8 sind die n Vektoren $(\tau x_1, \ldots, \tau x_n)_{\tau \in \mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C})}$ linear unabhängig im $\mathbb{C}^n$ (sonst gäbe es eine lineare Abhängigkeit der τ in $\mathrm{Hom}_{\mathbb{Q}\text{-VR}}(K, \mathbb{C})$). Also hat die Matrix

$$(\tau x_i)_{\substack{\tau \in \mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C}) \\ i=1,\ldots,n}} \in M_{n,n}(\mathbb{C})$$

eine Determinante $\neq 0$, weshalb auch die Vektoren $(\tau x_i)_\tau$, $i = 1, \ldots, n$, linear unabhängig im $\mathbb{C}^n$ sind. Nun ist $(x_1 \otimes 1, \ldots, x_n \otimes 1)$ eine $\mathbb{C}$-Basis von $K_{\mathbb{C}}$ und da die Vektoren

$$\phi(x_i \otimes 1) = (\tau x_i)_\tau, \quad i = 1, \ldots, n,$$

linear unabhängig sind, ist ϕ injektiv. □

Nun betrachten wir die komplexe Konjugation

$$F : \mathbb{C} \longrightarrow \mathbb{C},\ z \longmapsto \bar{z}, \quad \mathrm{Gal}(\mathbb{C}|\mathbb{R}) = \langle F \rangle.$$

F induziert durch Wirkung auf der zweiten Komponente einen Automorphismus von $K_{\mathbb{C}} = K \otimes_{\mathbb{Q}} \mathbb{C}$

$$F : K_{\mathbb{C}} \longrightarrow K_{\mathbb{C}}.$$

Lemma 4.10. *Bezüglich des natürlichen Isomorphismus* $\phi : K_{\mathbb{C}} \cong \prod_{\tau} \mathbb{C}$ *aus Lemma 4.9, ist* $F \in \mathrm{Aut}(\prod_{\tau} \mathbb{C})$ *gegeben durch*

$$F(z)_\tau = \bar{z}_{\overline{\tau}},$$

wobei $\overline{\tau} = F \circ \tau \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$.

Beweis. Klar nach Definition des natürlichen Isomorphismus ϕ. □

Lemma 4.11. *Die natürliche Inklusion* $\mathbb{R} \hookrightarrow \mathbb{C}$ *definiert eine natürliche Inklusion*

$$K_{\mathbb{R}} := K \otimes_{\mathbb{Q}} \mathbb{R} \hookrightarrow K_{\mathbb{C}} = K \otimes_{\mathbb{Q}} \mathbb{C},$$

deren Bild $K_{\mathbb{C}}^+ \subset K_{\mathbb{C}}$ *genau aus den* F*-invarianten Elementen besteht.*

Beweis. Wir betrachten den (üblichen) Isomorphismus

$$\mathbb{C} \cong \mathbb{R} \oplus \mathbb{R}, \ z \longmapsto (\mathrm{Re}(z), \mathrm{Im}(z)).$$

Dies ist ein Isomorphismus von $\mathbb{R}$- und insbesondere von $\mathbb{Q}$-Vektorräumen. Daher gilt ($\otimes$ vertauscht mit $\oplus$)

$$\begin{aligned} K \otimes_{\mathbb{Q}} \mathbb{C} &\cong K \otimes_{\mathbb{Q}} \mathbb{R} \oplus K \otimes_{\mathbb{Q}} \mathbb{R} \\ x \otimes z &\longmapsto (x \otimes \mathrm{Re}(z), \ x \otimes \mathrm{Im}(z)). \end{aligned}$$

Auf der rechten Seite operiert F so:

- trivial auf der 1. Komponente.
- Multiplikation mit -1 auf der 2. Komponente.

$\Rightarrow$ die erste Komponente $=$ $\mathrm{im}(K_{\mathbb{R}} \to K_{\mathbb{C}})$ besteht genau aus den F-invarianten Elementen. □

Wir erhalten hieraus das

Korollar 4.12. *Bezüglich der natürlichen Identifikation ϕ aus Lemma 4.9 und der Inklusion aus Lemma 4.11 gilt*

$$\begin{aligned} K_{\mathbb{R}} &\cong [\prod_{\tau} \mathbb{C}]^+ \\ &= \{z \in \prod_{\tau} \mathbb{C} \mid z_{\bar{\tau}} = \bar{z}_{\tau} \quad \forall \tau\}. \end{aligned}$$

Auf $K_{\mathbb{C}} \cong \prod_{\tau} \mathbb{C}$ haben wir das Standard-Hermitesche Skalarprodukt

$$\langle x, y \rangle = \sum_{\tau} x_{\tau} \bar{y}_{\tau}.$$

Lemma 4.13. *Dieses Skalarprodukt ist F-äquivariant, d.h. es gilt*

$$\langle Fx, Fy \rangle = F\langle x, y \rangle.$$

Beweis. Klar nach Einsetzen aller Definitionen. □

Nach Einschränkung auf $[\prod_{\tau} \mathbb{C}]^+ = K_{\mathbb{R}}$ erhalten wir daher eine symmetrische, positiv definite Bilinearform auf $K_{\mathbb{R}}$, d.h. $K_{\mathbb{R}}$ wird zum euklidischen Vektorraum.

Definition 4.14. Der so definierte euklidische Vektorraum $K_{\mathbb{R}} = [\prod_{\tau} \mathbb{C}]^+$ heißt **Minkowski-Raum** und sein Skalarprodukt die **kanonische Metrik**. Das assoziierte Maß heißt das **kanonische Maß** auf $K_{\mathbb{R}}$.

Auf $K_{\mathbb{C}}$ haben wir die natürliche („Spur“)Abbildung

$$\mathrm{Sp} : \prod_{\tau} \mathbb{C} \longrightarrow \mathbb{C}, \quad z \longmapsto \sum_{\tau} z_{\tau}.$$

Sei $j : K \to K_{\mathbb{C}}$, $x \mapsto x \otimes 1 = (\tau x)_{\tau}$ die natürliche Inklusion. Nach Satz 3.17 gilt

$$\mathrm{Sp} \circ j(x) = \mathrm{Sp}_{K|\mathbb{Q}}(x).$$

Man rechnet leicht nach: $F \circ \mathrm{Sp} = \mathrm{Sp} \circ F$. Daher erhalten wir die Abbildung

$$\mathrm{Sp} : K_{\mathbb{R}} \to \mathbb{R}$$

und für die natürliche Inklusion $j : K \to K_{\mathbb{R}}$ gilt $\mathrm{Sp} \circ j(x) = \mathrm{Sp}_{K|\mathbb{Q}}(x)$ für $x \in K$.

Wir suchen nun eine Identifikation

$$K_{\mathbb{R}} \cong \mathbb{R}^n, \quad n = [K : \mathbb{Q}].$$

(jede $\mathbb{Q}$-Basis von K gibt uns eine solche, aber die wollen wir nicht). Wir unterteilen die Menge $\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ in zwei Teilmengen. Die erste besteht aus

$$\rho_1, \ldots, \rho_{r_1} : K \longrightarrow \mathbb{R}$$

(alle die in $\mathbb{R}$ landen). Die anderen tauchen im Paaren auf:

$$\sigma_1, \bar{\sigma}_1, \ldots, \sigma_{r_2}, \bar{\sigma}_{r_2} : K \longrightarrow \mathbb{C}.$$

Wir haben also $r_1 + 2r_2 = n = [K : \mathbb{Q}]$. Der Buchstabe ρ bezeichne jetzt immer reelle Einbettungen. Aus jedem Paar konjugiert komplexer Einbettungen wählen wir uns willkürlich eine und bezeichnen diese stets mit σ. Wir erhalten (trivialerweise)

$$K_{\mathbb{R}} = \{(z)_{\tau} \in \prod_{\tau} \mathbb{C} \mid z_{\rho} \in \mathbb{R}, \quad z_{\bar{\sigma}} = \bar{z}_{\sigma}\}.$$

Satz 4.15. *Die Abbildung*

$$f : K_{\mathbb{R}} \longrightarrow \prod_{\tau} \mathbb{R} = \mathbb{R}^n,$$

die durch

$$(z)_{\tau} \in [\prod_{\tau} \mathbb{C}]^{+} \longmapsto (x)_{\tau} \in \prod_{\tau} \mathbb{R}$$

mit $x_{\rho} = z_{\rho}$, $x_{\sigma} = Re(z_{\sigma})$, $x_{\bar{\sigma}} = Im(z_{\sigma})$ gegeben ist, ist ein Isomorphismus. Es transformiert f die kanonische Metrik auf $K_{\mathbb{R}}$ in das Skalarprodukt

$$\langle x, y \rangle = \sum_{\tau} \varepsilon_{\tau} x_{\tau} y_{\tau},$$

wobei

$$\varepsilon_{\tau} = \begin{cases} 1 & \text{wenn } \tau \text{ reell} \\ 2 & \text{wenn } \tau \text{ komplex.} \end{cases}$$

Beweis. Offenbar ist f injektiv und daher ein Isomorphismus. Ist nun $(z)_\tau = (x)_\tau + i(y)_\tau \in [\prod_\tau \mathbb{C}]^+$, und $(z')_\tau = (x')_\tau + i(y')_\tau$, so gilt $z_\rho z'_\rho = x_\rho x'_\rho$ und wegen

$$y_\sigma = \mathrm{Im}(z_\sigma),\ y_{\bar\sigma} = \mathrm{Im}(z_{\bar\sigma}) = -\mathrm{Im}(z_\sigma) = -y_\sigma, \quad x_{\bar\sigma} = x_\sigma$$

erhält man

$$\begin{aligned} z_\sigma \bar z'_\sigma + z_{\bar\sigma}\bar z'_{\bar\sigma} &= (x_\sigma + iy_\sigma)(x'_\sigma - iy_\sigma) + (x_\sigma - iy_\sigma)(x'_\sigma + iy'_\sigma) \\ &= 2(x_\sigma x'_\sigma + y_\sigma y'_\sigma). \end{aligned}$$

□

Wir identifizieren nun $K_\mathbb{R}$ über f mit dem $\mathbb{R}^n$. Das kanonische Maß einer Teilmenge $X \subset K_\mathbb{R} \cong \mathbb{R}^n$ hängt mit dem Standard-Lebesgue-Maß durch die Regel

$$\mathrm{vol}_{\mathrm{kan}}(X) = 2^{r_2}\mathrm{vol}_{\mathrm{Lebesgue}}(f(X))$$

zusammen.

Satz 4.16. *Sei $0 \neq \mathfrak{a} \subset \mathcal{O}_K$ ein Ideal. Das Bild $\Gamma = j(\mathfrak{a})$ unter der natürlichen Abbildung $j : K \to K_\mathbb{R}$ ist ein vollständiges Gitter in $K_\mathbb{R}$. Die Grundmasche hat den Inhalt*

$$\mathrm{vol}(\Gamma) = \sqrt{|d_K|}\mathfrak{N}(\mathfrak{a}).$$

Beweis. Sei $\alpha_1, \ldots, \alpha_n$ eine $\mathbb{Z}$-Basis von $\mathfrak{a}$ so dass $\Gamma = \mathbb{Z}j\alpha_1 + \cdots + \mathbb{Z}j\alpha_n$. Wir numerieren die Einbettungen $\tau : K \to \mathbb{C}$, $\tau_1, \ldots, \tau_n$, und bilden die Matrix $A = (\tau_k\alpha_\ell)$. Dann gilt nach Satz 3.73

$$\det(A)^2 = d(\mathfrak{a}) = \mathfrak{N}(\mathfrak{a})^2 \cdot d_K.$$

Außerdem gilt

$$\begin{aligned} (\langle j\alpha_k, j\alpha_\ell\rangle)_{k,\ell} &= (\sum_{i=1}^n \tau_i\alpha_k\bar\tau_i\alpha_\ell)_{k,\ell} \\ &= A \cdot \bar A^t. \end{aligned}$$

So erhält man

$$\mathrm{vol}(\Gamma) = |\det(\langle j\alpha_k, j\alpha_\ell\rangle)_{k,\ell}|^{1/2} = |\det A| = \sqrt{|d_K|} \cdot \mathfrak{N}(\mathfrak{a}).$$

Insbesondere gilt $\det A \neq 0$, weshalb $j\alpha_1, \ldots, j\alpha_n$ linear unabhängig, also Γ ein vollständiges Gitter ist. □

Theorem 4.17. *Sei $0 \neq \mathfrak{a} \subset \mathcal{O}_K$ ein Ideal und seien $c_\tau > 0$, $\tau \in \mathrm{Hom}(K, \mathbb{C})$, reelle Zahlen mit $c_\tau = c_{\bar\tau}$ und*

$$\prod_\tau c_\tau > \left(\frac{2}{\pi}\right)^{r_2} \cdot \mathfrak{N}(\mathfrak{a})\sqrt{|d_K|}.$$

Dann gibt es ein $a \in \mathfrak{a}$, $a \neq 0$, mit

$$|\tau a| < c_\tau \text{ für alle } \tau \in \mathrm{Hom}(K, \mathbb{C}).$$

Beweis. Die Menge $X := \{(z_\tau) \in K_{\mathbb{R}} \mid |z_\tau| < c_\tau\}$ ist zentralsymmetrisch und konvex. Mit Hilfe der Abbildung $f : K_{\mathbb{R}} \xrightarrow{\sim} \prod_\tau \mathbb{R}$ aus Satz 4.15 ergibt sich

$$\mathrm{vol}_{\mathrm{kan}}(X) = 2^{r_2}\mathrm{vol}_{\mathrm{Lebesgue}}(f(X)).$$

Nun ist

$$f(X) = \{(x_\tau) \in \prod_\tau \mathbb{R} \mid |x_\rho| < c_\rho,\ x_\sigma^2 + x_{\overline{\sigma}}^2 < c_\sigma^2\}$$

(= Produkt von r_1 Intervallen und r_2 Kreisschreiben). Also gilt

$$\mathrm{vol}_{\mathrm{kan}}(X) = 2^{r_2}\prod_\rho (2c_\rho) \cdot \prod_\sigma (\pi c_\sigma^2) = 2^{r_1+r_2}\pi^{r_2}\prod_\tau c_\tau.$$

Der Grundmascheninhalt von $\Gamma = j\mathfrak{a}$ ist $\sqrt{|d_K|} \cdot \mathfrak{N}(\mathfrak{a})$. Also gilt

$$\begin{aligned}\mathrm{vol}_{\mathrm{kan}}(X) = 2^{r_1+r_2}\pi^{r_2}\prod_\tau c_\tau &> 2^{r_1+2r_2} \cdot \mathfrak{N}(\mathfrak{a})\sqrt{|d_K|} \\ &= 2^n \mathrm{vol}(\Gamma).\end{aligned}$$

Nach dem Minkowskischen Gitterpunktsatz enthält X ein $\gamma \in \Gamma$, $\gamma \neq 0$. Nun ist per definitionem $\gamma = ja$ für ein $a \in \mathfrak{a}$, und dieses a ist das Gesuchte. □

4.3 Die Endlichkeit der Klassenzahl

Sei $K|\mathbb{Q}$ ein Zahlkörper. Wir setzen $J_K = J(\mathcal{O}_K)$, $P_K = P(\mathcal{O}_K)$, $Cl_K = J_K/P_K$. Wir nennen Cl_K die **Idealklassengruppe von K**. Unser Ziel ist der Beweis des folgenden Theorems.

Theorem 4.18. *Cl_K ist endlich.*

Definition 4.19. $h_K = \#Cl_K$ heißt die **Klassenzahl** von K.

Lemma 4.20. *In jedem Ideal $0 \neq \mathfrak{a} \subset \mathcal{O}_K$ gibt es ein $0 \neq a \in \mathfrak{a}$ mit*

$$|N_{K|\mathbb{Q}}(a)| \ \leq\ \left(\frac{2}{\pi}\right)^{r_2}\sqrt{|d_K|}\mathfrak{N}(\mathfrak{a}).$$

Beweis. Zu vorgegebenem $\varepsilon > 0$ wählen wir $c_\tau > 0$, $\tau \in \mathrm{Hom}(K, \mathbb{C})$, mit $c_\tau = c_{\overline{\tau}}$ und

$$\prod_\tau c_\tau = \left(\frac{2}{\pi}\right)^{r_2}\sqrt{|d_K|}\,\mathfrak{N}(\mathfrak{a}) + \varepsilon$$

und finden nach Theorem 4.17 ein $0 \neq a \in \mathfrak{a}$ mit $|\tau a| < c_\tau$ für alle τ, also

$$|N_{K|\mathbb{Q}}(a)| = \prod_\tau |\tau a| < \left(\frac{2}{\pi}\right)^{r_2}\sqrt{|d_K|}\,\mathfrak{N}(\mathfrak{a}) + \varepsilon.$$

Nun gilt $N_{K|\mathbb{Q}}(a) \in \mathbb{Z}$. Ist $\left(\frac{2}{\pi}\right)^{r_2}\sqrt{|d_K|}\,\mathfrak{N}(\mathfrak{a}) \notin \mathbb{Z}$, so erhält man (wähle $\varepsilon > 0$ hinreichend klein) die Ungleichung (sogar mit $<$). Gilt $\left(\frac{2}{\pi}\right)^{r_2}\sqrt{|d_K|}\,\mathfrak{N}(\mathfrak{a}) \in \mathbb{Z}$, so wählt man $\varepsilon < 1$, um die Ungleichung zu erhalten. □

Beweis von Theorem 4.18. Sei $\mathfrak{p} \subset \mathcal{O}_K$ ein Primideal. Wegen

$$\mathfrak{N}(\mathfrak{p}) = \#(\mathcal{O}/\mathfrak{p}) \cdot 1 = 0 \in \mathcal{O}_K/\mathfrak{p}$$

gilt $\mathfrak{N}(\mathfrak{p}) \in \mathfrak{p} \cap \mathbb{Z}$. Daher gilt $\mathfrak{p} \cap \mathbb{Z} \neq 0$, also $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ für eine Primzahl p und $\mathfrak{p} \mid p\mathcal{O}_K$. Außerdem ist $\mathcal{O}_K/\mathfrak{p}$ ein endlicher Körper der Charakteristik p, weshalb $\mathfrak{N}(\mathfrak{p}) = p^f$ für ein $f \in \mathbb{N}$ gilt. Da nun $p\mathcal{O}_K$ nur endlich viele Primteiler hat, gilt für jedes $N \in \mathbb{N}$, dass $\#\{\mathfrak{p} \subset \mathcal{O}_K \mid N(\mathfrak{p}) \leq N\} < \infty$.
Für beliebiges $0 \neq \mathfrak{a} \subset \mathcal{O}_K$ gilt

$$\mathfrak{a} = \mathfrak{p}_1^{v_1} \cdots \mathfrak{p}_n^{v_n}, \quad \mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{p}_1)^{v_1} \cdots N(\mathfrak{p}_n)^{v_n}$$

$\Rightarrow$ für jedes $N \in \mathbb{N}$ ist

$$\#\{\mathfrak{a} \subset \mathcal{O}_K \mid \mathfrak{N}(\mathfrak{a}) \leq N\} < \infty.$$

Daher folgt das Theorem aus dem folgenden Lemma. □

Lemma 4.21. *Jede Idealklasse enthält ein ganzes Ideal $\mathfrak{a} \subset \mathcal{O}_K$ mit*

$$\mathfrak{N}(\mathfrak{a}) \leq \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|d_K|}.$$

Beweis. Sei $\mathfrak{a}_1 \subset K$ ein beliebiger Repräsentant einer Idealklasse und $0 \neq \gamma \in \mathcal{O}_K$ mit $\mathfrak{b} = \gamma\mathfrak{a}_1^{-1} \subset \mathcal{O}_K$. Nach Lemma 4.20 gibt es ein $\alpha \in \mathfrak{b}$, $\alpha \neq 0$, mit

$$|N_{K|\mathbb{Q}}(\alpha)| \leq \left(\frac{2}{\pi}\right)^{r_2} \mathfrak{N}(\mathfrak{b}) \sqrt{|d_K|}\,.$$

Das ganze Ideal $\mathfrak{a} := \alpha\gamma^{-1}\mathfrak{a}_1 = \alpha\mathfrak{b}^{-1}$ liegt in der gleichen Idealklasse wie $\mathfrak{a}_1$ und es gilt

$$\mathfrak{N}(\mathfrak{a}) = |\,N_{K|\mathbb{Q}}(\alpha)| N(\mathfrak{b})^{-1} \leq \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|d_K|}.$$ □

Bemerkung 4.22. Mit etwas mehr Aufwand kann die Schranke verbessert werden zu

$$\mathfrak{N}(\mathfrak{a}) \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} \sqrt{|d_K|}.$$

Beispiele 4.23. 1.) $K = \mathbb{Q}(\sqrt{-3})$. Wir haben $r_1 = 0$, $r_2 = 1$, $d_K = -3$. Jede Idealklasse enthält ein ganzes Ideal der Norm $\leq \left(\frac{2}{\pi}\right)\sqrt{3} = 1,10\ldots$
Davon gibt es nur eines, nämlich $\mathcal{O}_K$ selbst $\Rightarrow h_K = 1$, $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$ ist Hauptidealring.

Bemerkung: $\mathbb{Z}[\sqrt{-3}]$ ist kein Hauptidealring!

2) $K = \mathbb{Q}(\sqrt{-5})$. $r_1 = 0$, $r_2 = 1$, $d_K = -20$. Wir wissen schon, dass $\mathcal{O}_K$ *kein* Hauptidealring ist, also $h_K \geq 2$. Jede Idealklasse enthält ein ganzes Ideal der Norm $\leq \left(\frac{2}{\pi}\right)\sqrt{20} = 2,84\ldots$

$\mathfrak{N}(\mathfrak{a}) = 1 \Longleftrightarrow \mathfrak{a} = \mathcal{O}_K$

$\mathfrak{N}(\mathfrak{a}) = 2 \Longrightarrow \mathfrak{a} \mid (2)$. Wegen $(2) = \mathfrak{p}^2$ mit $\mathfrak{p} = (2, 1 + \sqrt{-5})$ und $\mathfrak{N}(\mathfrak{p}) = 2$ folgt $\mathfrak{a} = \mathfrak{p} \Rightarrow h_K \leq 2$, also $h_K = 2$.

3) Wir betrachten für eine Primzahl $p > 2$ die Fermatgleichung $X^p + Y^p = Z^p$. Über $\mathcal{O}_{\mathbb{Q}(\zeta_p)} = \mathbb{Z}[\zeta_p]$ (Beweis später) können wir umformen

$$X^p = Z^p - Y^p = (Z - Y)(Z - \zeta_p Y) \dots (Z - \zeta_p^{p-1} Y).$$

Ist nun (x, y, z) eine nichttriviale (also $xyz \neq 0$) ganzzahlige Lösung, so erhalten wir eine Zerlegung von x^p, die man, wenn $\mathbb{Z}[\zeta_p]$ ein Hauptidealring ist (d.h. $h_{\mathbb{Q}(\zeta_p)} = 1$) zum Widerspruch führen kann. Nun gilt

$$h_{\mathbb{Q}(\zeta_p)} = 1 \Longleftrightarrow p \in \{3, 5, 7, 11, 13, 17, 19\}.$$

Kummer hat gezeigt, dass man die Bedingung $h_{\mathbb{Q}(\zeta_p)} = 1$ zu $p \nmid h_{\mathbb{Q}(\zeta_p)}$ abschwächen kann. Eine solche Primzahl heißt *reguläre Primzahl*. Die anderen Primzahlen heißen *irregulär*. Die irregulären Primzahlen < 100 sind $37, 59$ und 67.

Wie prüft man nun nach, ob p regulär ist?

Definition. Die rationale Zahl B_n in der Potenzreihenentwicklung

$$\frac{X}{e^X - 1} = \sum_{n=0}^{\infty} B_n \cdot \frac{X^n}{n!}$$

heißen **Bernoulli-Zahlen**.

Es gilt $B_0 = 1$, $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_3 = 0$ und allgemeiner $B_{2n+1} = 0$ für $n \geq 1$. Die nächsten geraden Werte sind: $B_4 = -\frac{1}{30}$, $B_6 = \frac{1}{42}$, $B_8 = -\frac{1}{30}$, $B_{10} = \frac{5}{66}$, $B_{12} = -\frac{691}{2730}$. Nun gilt der

Satz (von Staudt-Clausen). *Für gerades positives n gilt*

$$B_n + \sum_{(p-1) \mid n} \frac{1}{p} \in \mathbb{Z}.$$

Insbesondere ist der Nenner von B_n (in gekürzter Schreibweise) genau durch die Primzahlen p mit $(p-1) \mid n$ teilbar.

Wir sehen:

- 2 und 3 teilen den Nenner stets.
- n gerade $n < p - 1 \Rightarrow$ der Nenner von B_n ist prim zu p.