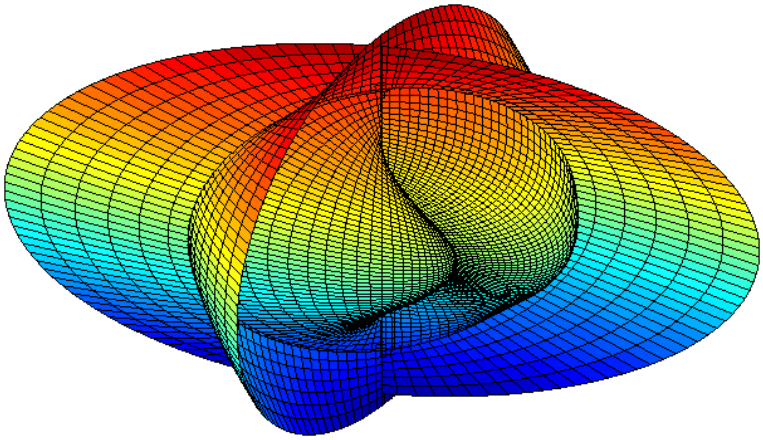
Sktiprum zur Vorlesung

Algebraische Zahlentheorie

Private Mitschrift



gelesen von

Prof. Dr. Alexander Prestel

Martin Gubisch

Konstanz, Sommersemester 2007

Inhaltsverzeichnis

Problemstellungen der Zahlenthorie

Die Zahlentheorie beschäftigt sich mit der Theorie der ganzen rationalen Zahlen $\mathbb{Z}$:

1. Die Suche nach ganzzahligen Lösungen von diophantischen Gleichungen, also Gleichungen mit ganzzahligen Koeffizienten. Ein bekanntes historisches Beispiel ist die Fermatsche Gleichung

$$X^n + Y^n = Z^n.$$

   Diese hat offensichtlich die trivialen Lösungen $(a, 0, a)$ und $(0, a, a)$. Auch trivial ist der Fall $n = 1$. Weitere Lösungen: Für $n = 2$ gibt es unendlich viele (ganzzahlige) Lösungen, zum Beispiel $3^2+4^4 = 5^2$. Für $n \geq 3$ hingegen gibt es keine nicht-triviale Lösung (Fermatsches Problem). Fermat schrieb dazu an den Rand von Diophants Arithmetica:

   Es ist unmöglich, einen Kubus in zwei Kuben zu teilen, eine vierte Potenz in zwei vierte Potenzen oder, allgemeiner gesagt, irgendeine Potenz über der zweiten in zwei Potenzen des gleichen Grades: Ich habe eine wahrhaft wunderbare Beweisführung entdeckt, die auf diesem Rand keinen Platz findet.

   Die Nichtlösbarkeit der Gleichung konnte für viele einzelne n gezeigt werden; endgültig gelöst wurde das Problem aber erst 1995 von Andrew Wiles und Richard Taylor.

2. Wann ist eine Primzahl Summe zweier Quadrate, d.h.

$$p = x^2 + y^2?$$

   Genau dann, wenn $p \equiv 1 \bmod 4$, z.B. $5 = 1^2 + 2^2$ oder $13 = 3^2 + 2^2$. Der Beweis dazu ist etwas komplizierter und setzt folgendermaßen an: Zu $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q} + \sqrt{-1}\mathbb{Q}$ betrachte $N : \mathbb{Q}(i) \to \mathbb{Q}$ mit $N(a+ib) = a^2+b^2 = (a+ib)(a-ib)$. Dies ist eine (multiplikative) Normabbildung, d.h. es gelten die Axiome einer Norm und $N(\alpha\beta) = N(\alpha)N(\beta)$ für alle $\alpha, \beta \in \mathbb{Q}(i)$. Beachte dabei: $\sigma : \mathbb{Q}(i) \to \mathbb{Q}(i)$ mit $a+ib \mapsto a-ib$ ist ein Homomorphismus. Also: Eine Primzahl ist genau dann Summe zweier Quadrate, wenn sie eine Norm ist: $N(n+im) = n^2+m^2 \in \mathbb{Z}$. Betrachte zur Lösung weiter den faktoriellen Ring $\mathbb{Z} + i\mathbb{Z} \subseteq \mathbb{Q}(i)$. Allgemein: $\mathbb{Z} \subseteq \mathbb{Q} \subseteq K$ mit Grad $[K : \mathbb{Z}] = n$, d.h. K ist eine Körpererweiterung $K = \mathbb{Q}(\alpha) \subseteq \mathbb{C}$ (Satz vom primitiven Element). Wir kommen auf dieses Problem später zurück.

3. Die Goldbachsche Vermutung, dass jede gerade Zahl sich als Summe zweier Primzahlen darstellen lässt, konnte bis heute weder bewiesen noch widerlegt werden und ist eines der sogenannten Hilbertschen Probleme.

4. Bereits Euklid konnte zeigen, dass es unendlich viele Primzahlen gibt: Angenommen, es gäbe nur endlich viele Primzahlen, etwa $p_1, ..., p_n$. Dann kann $p = p_1 \cdots p_n + 1$ nicht prim sein, muss also einen Primteiler haben. $p_1 \cdots p_n$ hat diesen ebenso als Primteiler, also wird auch 1 von ihm geteilt, ein Widerspruch.

1. Kongruenzen und Moduln

1.1. Lineare Kongruenzen

Wiederholung 1.1.

1. Sei ab jetzt R stets ein kommutativer Ring mit Eins. Weiter sei I ein R-Ideal, d.h. $I \subseteq R$ mit $I+I \subseteq I$ und $RI \subseteq I$.

2. Mit $\overline{R}$ bezeichnen wir den Restklassenring $R/I = \{a + I \mid a \in R\}$.

3. Für Hauptideale (b) in R setzen wir $a \bmod (b) = a \bmod Rb = a \bmod b$. $a \equiv b \bmod I$ bedeutet dabei, dass $a - b \in I$. Wir schreiben $\overline{a} = \overline{b}$, wenn klar ist, dass Restklassen bzgl. des Ideals I gemeint sind.

4. Im Fall $R = \mathbb{Z}$ und $I = n\mathbb{Z}$ für ein $n \in \mathbb{Z}$ ist beispielsweise $\bar{R} = \mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, ..., (n-1) + n\mathbb{Z}\}$ die Menge $\{\overline{0}, ..., \overline{n-1}\}$ (welche nicht notwendig aus n ELementen bestehen muss). Wir bezeichnen diese auch mit $\mathbb{Z}_n$. $a \equiv b \bmod n\mathbb{Z}$ bedeutet dabei $a - b \in n\mathbb{Z}$, d.h. n ist ein Teiler von $a - b$.

5. Die Restklassenabbildung $R \to R/I$ mit $a \mapsto a + I = \overline{a}$ ist ein Ringhomomorphismus, der kanonische Homomorphismus, denn es gelten $\overline{a+b} = \overline{a} + \overline{b}$ sowie $\overline{ab} = \overline{a}\overline{b}$.

6. Mit $(a, b) = (\mathrm{ggT}(a, b))$ ist das Ideal, das vom größten gemeinsamen Teiler der Zahlen a, b erzeugt wird. Wir bezeichnen auch $\mathrm{ggT}(a, b)$ selbst mit (a, b). ◊

Satz 1.2. (Chinesischer Restsatz, ca. 3. Jh. n. Chr.)

Seien R ein kommutativer Ring mit Eins und seien $I_1, ..., I_n$ Ideale in R mit $I_i + I_j = R$ für alle $i \neq j$.

Zu $x_1, ..., x_n \in R$ gibt es dann ein $x \in R$ mit $x \equiv x_i \bmod I_i$ für alle $1 \leq i \leq n$.

Beweis. (per Induktion über n)

1. $n = 2$: Seien $a_1 \in I_1$ und $a_2 \in I_2$ mit $a_1 + a_2 = 1$. Setze $x = x_1a_2 + x_2a_1$. Dann gelten
$$x \equiv x_1a_2 = (1 - a_1)x_1 = x_1 - a_1x_1 \equiv x_1 \bmod I_1,$$
$$x \equiv x_2a_1 = (1 - a_2)x_2 = x_2 - a_2x_2 \equiv x_2 \bmod I_2.$$

2. $n > 2$: Wir betrachten den Fall $I_1 + I_i = R$. Für $i \geq 2$ gibt es $a_i \in I_1$ und $b_i \in I_i$ mit $a_i + b_i = 1$. Dann ist
$$1 = \prod_{i\geq 2}(a_i + b_i) = \prod_{i\geq 2} a_i + \cdots + \prod_{i\geq 2} b_i,$$
wobei alle Faktoren bis auf den letzten in I_1 liegen und der letzte in $I = \bigcap\{I_i \mid i \geq 2\}$, d.h. $I_1 + I = R$. Nach Induktionsvoraussetzung gibt es $y_1 \in R$ mit $y_1 \equiv 1 \bmod I_1$ und $y_1 \equiv 0 \bmod I$. Analog gibt es $y_j \in R$ mit $y_j \equiv 1 \bmod I_j$ und $y_j \equiv 0 \bmod \bigcap\{I_i \mid i \neq j\}$ für alle $1 \leq j \leq n$. Setze $x = x_1y_1 + \cdots + x_ny_n$, dann $x \equiv x_jy_j \bmod I_j$ (denn $x_i \in I_j$ für alle $i \neq j$) und $x_jy_j \equiv x_j1 = x_j \bmod I_j$. □

Korollar 1.3.

Seien R ein Hauptidealring und $p_1, ..., p_n \in R$ paarweise verschiedene Primelemente.

Dann gibt es zu $\nu_1, ..., \nu_n \in \mathbb{N}$ und $x_1, ..., x_n \in R$ ein $x \in R$ mit $x \equiv x_i \bmod p_i^{\nu_i}$.

Beweis.

Für $I_i = Rp_i^{\nu_i}$ gilt: Ist $i \neq j$, dann $I_i + I_j = R$, denn $(p_i^{\nu_i}, p_j^{\nu_j}) = (1)$. Die Behauptung folgt somit mit dem Chinesischen Restsatz 1.2. □

Satz 1.4. (Lösbarkeit linearer Kongruenzgleichungen in $\mathbb{Z}$)

1. Die Kongruenzgleichung $ax \equiv b \bmod n$ ist genau dann lösbar, wenn (a, n) ein Teiler von b ist.
2. Ist (a, n) ein Teiler von b, so gibt es genau (a, n) viele Lösungen modulo n.

Beweis.

1. a) Gelte $ac \equiv b \bmod n$, dann ist $ac - b = dn$ für ein $d \in R$, also $b \in (a, n)$ und damit $(a, n) \mid b$.
   b) Sei umgekehrt $b = cd$ mit $d = (a, n)$. Dann ist $d = ax_0 + ny_0$, d.h. $b = cd = acx_0 + ncy_0$, also $b \equiv a(cx_0) \bmod n$, also ist $a(cx_0)$ eine Lösung der Kongruenzgleichung.

2. Bezeichne $d = (a, n)$, sei x_0 eine Lösung der Kongruenzgleichung und sei $n = dc$. Dann gilt für jedes $0 \leq i < d$, dass $a(x_0 + i\frac{n}{d}) \equiv ax_0 \equiv b \bmod n$, denn $a\frac{n}{d} = \frac{a}{d}n$. Seien also x_1, x_2 zwei Lösungen der Kongruenzgleichung, dann existieren $0 \leq i \leq j < d$ mit $x_1 = x_0 + i\frac{n}{d}$ und $x_2 = x_0 + j\frac{n}{d}$. Für diese gilt:
$$\begin{aligned} x_0 + i\frac{n}{d} \equiv x_0 + j\frac{n}{d} \bmod n \quad &\iff \quad (i - j)\frac{n}{d} \equiv 0 \bmod n \\ &\iff \quad n \mid (i - j)\frac{n}{d} \\ &\iff \quad dc \mid (i - j)c \\ &\iff \quad i \equiv j \bmod d \\ &\iff \quad i = j. \end{aligned}$$
Also gibt es genau d Lösungen. □

Korollar 1.5.

1. Sind a, n teilerfremd, so besitzt die Gleichung $ax \equiv b \bmod n$ genau eine Lösung.
2. Es gilt: $ax \equiv 1 \bmod n$ ist lösbar g.d.w. $ax \equiv 1 \bmod n$ ist eindeutig lösbar g.d.w. $(a, n) = 1$.

Bemerkung 1.6.

$\overline{m} \in \mathbb{Z}_n$ ist genau dann eine Einheit, wenn $mx \equiv 1 \bmod n$ lösbar ist. Nach Korollar 1.5 ist dies genau dann der Fall, wenn $(m, n) = 1$, d.h. $\mathbb{Z}_n^\times$ besteht genau aus den zu n teilerfremden Resten. ◊

Definition 1.7.

Die Abbildung $\varphi : \mathbb{Z} \to \mathbb{N}$ mit $\varphi(n) = \sharp\mathbb{Z}_n^\times$ heißt die Eulersche φ-Funktion.

Bemerkung 1.8.

Genau dann ist $n \in \mathbb{Z}$ prim, wenn $\varphi(n) = n - 1$:

$$\begin{aligned} \varphi(n) = n - 1 \quad &\iff \quad ax \equiv 1 \bmod n \text{ ist für alle } \overline{a} \neq \overline{0} \text{ lösbar} \\ &\iff \quad \text{für alle } a \in \mathbb{Z}, \text{ die nicht von } n \text{ geteilt werden, gilt } (a, n) = 1 \\ &\iff \quad n \text{ ist eine Primzahl.} \end{aligned}$$

Folglich erhalten wir daraus, dass $\mathbb{Z}_n$ genau dann ein Körper ist, wenn n prim ist. ◊

Satz 1.9. (Euler, 1763)

Seien $a, n \in \mathbb{Z}$ mit $(a, n) = 1$. Dann ist $a^{\varphi(n)} \equiv 1 \bmod n$.

Beweis.

Aus $(a, n) = 1$ folgt $\overline{a} \in \mathbb{Z}_n^\times$, d.h. $\overline{a}^{\varphi(n)} = \overline{a}^{\sharp\mathbb{Z}_n^\times} = \overline{1}$ in $\mathbb{Z}_n$. □

Beispiel 1.10.

Es gilt $5^6 \equiv 1 \bmod 7$, da $(5, 7) = 1$. Da $19, 23$ teilerfremd, ist $19^{22} \equiv 1 \bmod 23$. ◊

Lemma 1.11.

Ist K ein endlicher Körper, dann gilt $\prod\limits_{a \in K^\times} a = \prod\limits_{a \neq 0} a = -1$.

Beweis.

Sei $\sharp K = q$, dann ist q eine Primzahlpotenz, d.h. es gibt ein primes $p \in \mathbb{N}$ und einen Exponenten $m \in \mathbb{N}$ mit $q = p^m$, und es gilt $\sharp K^\times = q - 1$.

1. Für $p \neq 2$ ist $q - 1$ gerade. Das Polynom $X^{q-1} - 1$ hat alle $a \neq 0$ als Nullstellen, denn $\mathrm{Ord}(a) \mid \sharp K^\times$ in der multiplikativen Gruppe $K^\times$, d.h. $a^{q-1} = 1$. Dann ist

$$X^{q-1} - 1 = (X - a_1) \cdots (X - a_{q-1}) \quad \Longrightarrow \quad -1 = \prod_{i=1}^{q-1} (-a_i) = \prod_{a \neq 0} a.$$

2. Ist $p = 2$, dann gilt $-a_i = a_i$ für alle i, also $-1 = \prod\limits_{a \neq 0} a$. □

Satz 1.12. (Wilson, 1771)

Für $n \in \mathbb{N}$ gilt: n ist genau dann prim, wenn $(n - 1)! \equiv -1 \bmod n$.

Beweis.

1. Sei n prim, dann ist $\mathbb{Z}_n$ ein endlicher Körper und die Behauptung folgt aus Lemma 1.11.
2. Nehmen wir umgekehrt an, $n = pq$ mit p prim und $q \neq 1$. Dann ist $(n-1)! \equiv 0 \bmod p$. Aus $(n-1)! \equiv -1 \bmod n$ folgt dann $(n-1)! \equiv -1 \bmod p$, d.h. $0 \equiv -1 \bmod p$, ein Widerspruch. □

Satz 1.13.

1. Es gibt $\varphi(n)$ viele Erzeugende von $(\mathbb{Z}_n, +)$.
2. Sei p prim. Dann hat $(\mathbb{Z}_p^\times, \cdot)$ $\varphi(p-1)$ viele Erzeugende.
3. Es gibt $\varphi(n)$ viele primite n-te Einheitswurzeln.
4. Besitzt $n \in \mathbb{N}$ die Primfaktorzerlegung $n = p_1^{\nu_1} \cdots p_m^{\nu_m}$. Dann gilt $\varphi(n) = \varphi(p_1^{\nu_1}) \cdots \varphi(p_m^{\nu_m})$.
5. Seien p prim und $\nu \in \mathbb{N}$. Dann ist $\varphi(p^\nu) = p^{\nu-1}(p-1)$.
6. Insbesondere ist $\varphi(n) = p_1^{\nu_1}(1-p_1^{-1}) \cdots p_m^{\nu_m}(1-p_m^{-1}) = n \prod_{p|n}(1-p^{-1})$.

Beweis.

1. $(\mathbb{Z}_n, +)$ ist eine zyklische Gruppe der Ordnung n, welche beispielsweise von $\overline{1}$ erzeugt wird. Sei $\overline{m}$ ein beliebiger Erzeuger der Gruppe, dann ist $\mathbb{Z}_n = \{\overline{m}, 2\overline{m}, ..., n\overline{m}\}$, d.h. die Abbildung $\rho : \mathbb{Z}_n \to \mathbb{Z}_n$ mit $\overline{s} \mapsto m\overline{s} = \overline{ms}$ ist ein Gruppenisomorphismus. Damit gilt: $\overline{m}$ erzeugt $\mathbb{Z}_n$ g.d.w. $\overline{mx} = \overline{1}$ ist eindeutig lösbar g.d.w. $\overline{m} \in \mathbb{Z}_n^\times$. Also besitzt $(\mathbb{Z}_n, +)$ genau $\varphi(n)$ viele erzeugende Elemente.
2. Jede endliche Untergruppe der multiplikativen Gruppe eines Körpers ist zyklisch. Damit ist speziell $\mathbb{Z}_p^\times$ eine zyklische Gruppe der Ordnung $p-1$ und hat somit $\varphi(p-1)$ Erzeuger.
3. Bezeichne $\zeta_n = e^{\frac{2\pi i}{n}}$ und $U_n = \{\zeta_n^m \mid m \in \mathbb{Z}\}$ die (zyklische) Gruppe der n-ten Einheitswurzeln. Dann definiert $\rho : (\mathbb{Z}_n, +) \to (U_n, \cdot)$ mit $m \mapsto e^{\frac{2\pi i}{n}m} = \zeta_n^m$ einen Isomorphismus, denn $\rho(r+s) = \zeta_n^r \zeta_n^s$. Dann ist ζ_n^m eine primitive n-te Einheitswurzel, d.h. ein Erzeuger von U_n, g.d.w. $\overline{m} \in \mathbb{Z}_n^\times$.
4. $\rho : \mathbb{Z} \to \mathbb{Z}_{p_1^{\nu_1}} \times \cdots \times \mathbb{Z}_{p_m^{\nu_m}}$ mit $a \mapsto (a_1, ..., a_m)$, $a_i \equiv a \bmod p_i^{\nu_i}$, ist ein Ringhomomorphismus (im Fall $m = 1$ der kanonische Homomorphismus). ρ ist surjektiv, denn nach Korollar 1.3 zum Chinesischen Restsatz gibt es zu $a_i \in \mathbb{Z}_{p_i^{\nu_i}}$ ein $a \in \mathbb{Z}$ mit $a \equiv a_i \bmod p_i^{\nu_i}$, $i = 1, ..., m$, d.h. $\rho(a) = (a_1, ..., a_m)$. Weiter ist $\mathrm{Kern}(\rho) = (p_1^{\nu_1}) \cap \cdots \cap (p_m^{\nu_m}) = (n)$. Nach dem Homomorphiesatz ist somit $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\nu_1}} \times \cdots \times \mathbb{Z}_{p_m^{\nu_m}}$. Damit gilt: $(a_1, ..., a_m)$ ist eine Einheit in $\mathbb{Z}_{p_1^{\nu_1}} \times \cdots \times \mathbb{Z}_{p_m^{\nu_m}}$ g.d.w. alle a_i sind Einheiten in $\mathbb{Z}_{p_i^{\nu_i}}$. Dies liefert einen kanonischen Isomorphismus $\mathbb{Z}_n^\times \cong \mathbb{Z}_{p_1^{\nu_1}}^\times \times \cdots \times \mathbb{Z}_{p_m^{\nu_m}}^\times$, d.h. $\varphi(n) = \varphi(p_1^{\nu_1}) \cdots \varphi(p_m^{\nu_m})$.
5. Für alle $0 \leq a \leq p^\nu$ gilt: $\overline{a} \in \mathbb{Z}_{p^\nu}^\times$ g.d.w. $(a, p^\nu) = 1$. Gelte nun $a = pb$, dann ist $0 \leq b < p^{\nu-1}$, also $\sharp\{\overline{a} \mid (a, p^\nu) = 1\} = p^\nu - p^{\nu-1} = p^{\nu-1}(p-1)$. □

1.2. Höhere Kongruenzen

Satz 1.14.

Besitze $m \in \mathbb{Z}$ die Primfaktorzerlegung $m = p_1^{\nu_1} \cdots p_s^{\nu_s}$ und sei $f \in \mathbb{Z}[X]$. Dann sind äquivalent:

1. Die Kongruezgleichung $f(X) \equiv 0 \bmod m$ ist lösbar.
2. Die Kongruenzgleichungen $f(X) \equiv 0 \bmod p_i^{\nu_i}$ sind lösbar für alle $1 \leq i \leq s$.

Beweis.

1. Sei $a \in \mathbb{Z}$ mit $f(a) \equiv 0 \bmod m$, dann gilt $f(a) \mid m$, somit auch $p_i^{\nu_i} \mid m$ für alle i, d.h. $f(a) \equiv 0 \bmod p_i^{\nu_i}$.
2. Seien umgekehrt $a_1, ..., a_s \in \mathbb{Z}$ mit $p_i^{\nu_i} \mid f(a_i)$. Mit dem Chinesischen Restsatz 1.2 wählen wir ein $a \in \mathbb{Z}$, das alle Kongruenzgleichungen $a \equiv a_i \bmod p_i^{\nu_i}$ erfüllt, d.h. $\overline{a_i} = \overline{a}$ in $\mathbb{Z}_{p_i^{\nu_i}}$. Aus $\overline{f(a_i)} = \overline{0}$ in $\mathbb{Z}_{p_i^{\nu_i}}$ folgt dann $\overline{f(a)} = \overline{0}$ in $\mathbb{Z}_{p_i^{\nu_i}}$ für alle $1 \leq i \leq s$, d.h. $m = p_1^{\nu_1} \cdots p_s^{\nu_s}$ ist ein Teiler von $f(a)$ und somit $f(a) \equiv 0 \bmod m$. □

Satz 1.15. (Euler-Kriterium)

Seien $p \neq 2$ prim und $a \in \mathbb{Z}$ mit $p \nmid a$. Dann sind äquivalent:

1. a ist ein quadratischer Rest modulo p, d.h. die Kongruenzgleichung $X^2 - a \equiv 0 \bmod p$ ist lösbar.
2. $a^{\frac{p-1}{2}}$ löst die Kongruenzgleichung $X \equiv 1 \bmod p$.

Beweis.

1. Seien $b \in \mathbb{Z}$ mit $a \equiv b^2 \bmod p$ und ζ ein Erzeugendes von $\mathbb{Z}_p^\times$, d.h. $\mathrm{Ord}(\zeta) = p-1$. Dann existieren Exponenten $0 \leq r, s \leq p-1$ mit $\overline{a} = \zeta^r$ und $\overline{b} = \zeta^s$; wegen $\zeta^r = \zeta^{2s}$ ist $r \equiv 2s \bmod p-1$. Da $p-1$ ungerade, ist r somit gerade, d.h. $\overline{a}$ liegt in der Untergruppe der Quadrate $U = \{\zeta^{2s} \mid 0 \leq s < \frac{p-1}{2}\}$ von $\mathbb{Z}_p^\times$. Damit teilt $\mathrm{Ord}(\overline{a})$ die Gruppenordnung $\mathrm{Ord}(U) = \frac{p-1}{2}$, d.h. $\overline{a}^{\frac{p-1}{2}} = \overline{1}$.
2. Sei wieder $\overline{a} = \zeta^r$. Wir müssen zeigen, dass r gerade ist. Wegen $\mathrm{Ord}(\overline{a}) \mid \frac{p-1}{2}$ ist $(\zeta^r)^{\frac{p-1}{2}} = \overline{1}$, d.h. $(p-1) \mid r\frac{p-1}{2}$ und damit $2 \mid r$. □

Definition 1.16. (1798)

Seien p prim, $p \neq 2$, und $a \in \mathbb{Z}$.

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p \mid a \\ 1 & a \text{ ist quadratischer Rest mod } p \\ -1 & \text{sonst} \end{cases}$$

heißt das Legendre-Symbol von a über p.

Bemerkung 1.17. (Rechenregeln für das Legendre-Symbol)

1. Gelte $p \nmid a$. Dann ist $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \bmod p$:

   Wegen $\overline{a}^{p-1} = \overline{1}$ ist $\overline{a}^{\frac{p-1}{2}} = \pm\overline{1}$. Mit dem Euler-Kriterium 1.15 folgt: $(\frac{a}{p}) = +1$ g.d.w. $\overline{a}^{\frac{p-1}{2}} = +\overline{1}$.
2. Speziell gilt $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$.
3. Gelte $a \equiv b \bmod p$, dann ist $(\frac{a}{p}) = (\frac{b}{p})$:

   Wegen $\overline{a} = \overline{b}$ ist $a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \bmod p$, d.h. $(\frac{a}{p}) = (\frac{b}{p})$.
4. $(\frac{\cdot}{p})$ ist multiplikativ, d.h. $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$:

   Gelte Œ $p \nmid a$, $p \nmid b$, dann ist $(\frac{ab}{p}) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv (\frac{a}{p})(\frac{b}{p}) \bmod p$, d.h. $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$.
5. $(\frac{q}{p}) = (\frac{p}{q})(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ für $q \neq 2$ prim und $(\frac{q}{p}) = (-1)^{\frac{p^2-1}{8}}$ für $q = 2$.

   Dies ist das sogenannte quadratische Reziprozitätsgesetz und wird in Kapitel 4.5 bewiesen.

Beispiel 1.18.

1. $(\frac{60}{67}) = (\frac{4}{67})(\frac{5}{67})(\frac{3}{67}) = (\frac{5}{67})(\frac{3}{67}) = (\frac{67}{5})(1)(\frac{67}{3})(-1) = (-1)(\frac{2}{5})(\frac{1}{3}) = (-1)(\frac{2}{5}) = (-1)(-1)^{\frac{5^2}{8}} = 1.$
2. $(\frac{60}{67}) = (\frac{-7}{67}) = (\frac{-1}{67})(\frac{67}{7})(-1) = (-1)(\frac{67}{7})(-1) = (\frac{67}{7}) = (\frac{4}{7}) = 1.$ ◊

Bemerkung 1.19.

1. Seien $m = p_1^{\nu_1} \cdots p_s^{\nu_s}$ und $a \in \mathbb{Z}$. Dann gilt: a ist quadratischer Rest modulo m g.d.w. a ist quadratischer Rest modulo $p_i^{\nu_i}$ für alle $1 \leq i \leq s$.
2. Sei $p \neq 2$ mit $p \nmid a$. Dann gilt: a ist quadratischer Rest modulo p^ν g.d.w. a ist quadratischer Rest modulo p.
3. Gelte $2 \nmid a$. Dann gilt: a ist quadratischer Rest modulo 2^2 g.d.w. $a \equiv 1 \bmod 2^2$ und a ist quadratischer Rest modulo 2^ν g.d.w. a ist quadratischer Rest modulo 2^r für alle $r \geq 3$. ◊

Bemerkung 1.20. (Dirichletscher Primzahlsatz)

Seien $r, s \in \mathbb{Z}$ mit $(r, s) = 1$. Dann gibt es unendlich viele Primzahlen p mit $p \equiv r \bmod s$.

Der Beweis ist ziemlich kompliziert und findet sich in Kapitel 3.5. ◊

Korollar 1.21.

Sei a quadratischer Rest modulo p für fast alle Primzahlen p. Dann ist a ein Quadrat in $\mathbb{Z}$.

Beweis.

Habe $a \in \mathbb{Z}$ die Darstellung $a = \pm b^2 p_1 \cdots p_{m+1}$ für ein $m \in \mathbb{N}_0$ und paarweise verschiedene Primzahlen $p_1, ..., p_{m+1}$. Wir suchen unendlich viele Primzahlen p mit $(\frac{p_i}{p}) = 1$ für alle $i = 1, ..., m$ und $(\frac{p_{m+1}}{p}) = -1$, $(\frac{-1}{p}) = 1$, denn dann gilt nach den Rechenregeln für das Legendre-Symbol, dass $(\frac{a}{p}) = -1$ und somit ist a kein Quadrat modulo p.

1. Sei $m \geq 1$ und seien alle p_i ungerade. Sei $u \in \mathbb{Z}$ mit $(\frac{u}{p_{m+1}}) = -1$. Mit dem Chinesischen Restsatz 1.2 wählen wir ein $r \in \mathbb{Z}$ mit $r \equiv 1 \bmod 4p_1 \cdots p_m$ und $r \equiv u \bmod p_{m+1}$. Dann gilt für $s = 4p_1 \cdots p_{m+1}$, dass $(r, s) = 1$. Nach dem Dirichletschen Primzahlsatz 1.20 gibt es somit unendlich viele Primzahlen p mit $p \equiv r \bmod s$. Also gelten $p \equiv 1 \bmod 4p_1 \cdots p_m$, d.h. es gilt $(\frac{p}{p_i}) = 1$ für alle $1 \leq i \leq m$, und $p \equiv u \bmod p_{m+1}$, d.h. $(\frac{p}{p_{m+1}}) = -1$. Außerdem ist $(\frac{-1}{p}) = 1$, da $4 \mid (p-1)$, d.h. $\frac{p-1}{2}$ ist gerade. Mit dem quadratischen Reziprozitätsgesetz 1.17 erhalten wir schließlich $1 = (\frac{p}{p_i}) = (\frac{p_i}{p})$ und $-1 = (\frac{p}{p_{m+1}}) = (\frac{p_{m+1}}{p})$.
2. Seien $m \geq 1$ und $p_{m+1} = 2$. Wähle $r \equiv 5 \bmod 8$ und $r \equiv 1 \bmod p_1 \cdots p_m$. Setze $s = 8p_1 \cdots p_m$, dann ist $(r, s) = 1$, also sind die Voraussetzungen des Dirichletschen Primzahlsatzes 1.20 erfüllt. Mit den Rechenregeln für das Legendre-Symbol erhalten wir: $p \equiv 5 \bmod 8$, d.h. $p \equiv 1 \bmod 8$, also $(\frac{p}{p_i}) = (\frac{p_i}{p})$, und $p \equiv 1 \bmod p_1 \cdots p_m$, d.h. $(\frac{p}{p_i}) = 1$. Wie eben ist $(\frac{-1}{p}) = 1$. Aus $p \equiv 5 \bmod 8$ folgt schließlich, dass $(\frac{2}{p}) = -1$, da $\frac{p^2-1}{8}$ ungerade ist.
3. Der letzte zu betrachtende Fall ist $a = -b^2$. Wähle $p \equiv 3 \bmod 4$, dann ist $p - 1 = 2$, d.h. $\frac{p-1}{2} = 1$ bzw. $(\frac{-1}{p}) = -1$, also $(\frac{a}{p}) = -1$. Nach dem Dirichletschen Primzahlsatz 1.20 finden wir unendlich viele solche p. □

1.3. Moduln

Wiederholung 1.22.

1. Sei stets A ein kommutativer Ring mit Eins. Beispiele für A-Moduln sind:
   a) $(A, +)$ selbst mit der Multiplikation $ax = a \cdot x$.
   b) Jeder A-Vektorraum mit der Skalarmultiplikation, falls A ein Körper ist.
   c) Im Fall $A = \mathbb{Z}$ wird jede abelsche Gruppe $(G, +)$ mit $mx = x + \cdots + x$ zu einem A-Modul.
   d) Seien V ein K-Vektorraum und $f \in \mathrm{End}(V)$. Dann ist V mit $p(f)x = p(f)(x)$ ein $K[f]$-Modul.
   e) Sei I ein A-Ideal, dann ist A/I mit $\alpha\overline{a} = \overline{\alpha a}$ ein A-Modul.
2. Es gilt der Homomorphiesatz: Ist $f : L \to M$ ein Modulhomomorphismus, dann ist $L/\mathrm{Kern}(f) \cong f(L)$ via des kanonischen Homomorphismus $\overline{f} : \overline{x} \mapsto f(x)$.

Bemerkung 1.23.

1. Sei M ein R-Modul und sei $(U_\lambda)_{\lambda \in \Lambda}$ eine Familie von R-Untermoduln von M. Dann ist

$$\sum_{\lambda \in \Lambda} U_\lambda = \left\{ \sum_{\lambda \in \Lambda} u_\lambda \mid u_\lambda \in U_\lambda \text{ und fast alle } u_\lambda = 0 \right\}$$

   ein R-Untermodul von M.

2. Sei $(M_\lambda)_{\lambda\in\Lambda}$ eine Familie von R-Moduln. Dann ist

$$\prod_{\lambda\in\Lambda} M_\lambda = \{(m_\lambda)_{\lambda\in\Lambda} \mid m_\lambda \in M_\lambda\}$$

mit komponentenweiser Addition und komponentenweiser skalarer Multiplikation ein R-Modul.

3. Ein R-Untermodul von $\prod_{\lambda\in\Lambda} M_\lambda$ ist gegeben durch

$$\bigoplus_{\lambda\in\Lambda} M_\lambda = \{(m_\lambda)_{\lambda\in\Lambda} \mid m_\lambda \in M_\lambda \text{ und fast alle } m_\lambda = 0\}. \qquad \Diamond$$

Wiederholung 1.24. (Erzeugendensystem und Basis)

1. Seien M ein R-Modul und $U_1, ..., U_m$ R-Untermoduln von M. Dann gelten:
   a) $M = U_1 + \cdots + U_m$ g.d.w. jedes $a \in M$ besitzt eine Darstellung $a = u_1 + \cdots + u_m$ mit $u_i \in U_i$.
   b) $M = U_1 \oplus \cdots \oplus U_m$ g.d.w. jedes $a \in M$ besitzt eine eindeutige Darstellung $a = u_1 + \cdots + u_m$ mit $u_i \in U_i$.
2. Ein Erzeugendensystem eines R-Moduls ist eine Familie $(v_\lambda)_{\lambda\in\Lambda}$ mit $M = \sum_{\lambda\in\Lambda} Rv_\lambda$.
3. M heißt endlich erzeugt, falls es ein Erzeugendensystem endlicher Länge gibt, d.h. falls es eine endliche Indexmenge Λ gibt, so dass $(v_\lambda)_{\lambda\in\Lambda}$ ein Erzeugendensystem von M ist.
4. Eine Basis von M ist eine Familie $(v_\lambda)_{\lambda\in\Lambda}$ mit

$$M = \sum_{\lambda\in\Lambda} Rv_\lambda \qquad \text{und} \qquad \sum_{\lambda\in\Lambda} \alpha_\lambda v_\lambda = 0 \text{ impliziert } \alpha_\lambda = 0 \text{ für alle } \lambda \in \Lambda.$$

5. M heißt ein freier Modul, falls M eine Basis besitzt. Ist M ein freier Modul mit Basis $\{v_1, ..., v_m\}$, dann heißt m der Rang von M. Der Rang eines endlich erzeugten Moduls ist eindeutig bestimmt, aber nicht jeder Modul ist frei.
6. Sei M ein freier R-Modul mit Basis $\{v_1, ..., v_m\}$. Dann ist die Koordinatenabbildung $\phi : M \to R^m$ mit $\phi(v_i) = e^i$ ein R-Modul-Isomorphismus. Es gilt $R^n \cong R^m$ g.d.w. $n = m$.
7. $M = Rv_1 + \cdots + Rv_m$ ein freier R-Modul mit Basis $\{v_1, ..., v_m\}$. Dann ist $M = Rv_1 \oplus \cdots \oplus Rv_m$. Die Umkehrung ist falsch: Sei $M = Rv_1 \oplus \cdots \oplus Rv_m$, dann folgt aus $\sum \alpha_i v_i = \sum \beta_i v_i$ nur $\alpha_i v_i = \beta_i v_i$, aber nicht unbedingt $\alpha_i = \beta_i$, d.h. $\{v_1, ..., v_m\}$ ist dann im Allgemeinen keine Basis von M.
8. Sind $L \subsetneq M$ zwei R-Moduln, so können beide die gleiche Basislänge haben: Beispielsweise haben $\mathbb{Z}$ und $n\mathbb{Z}$ beide die Basislänge 1, denn (1) ist eine Basis von $\mathbb{Z}$ und (n) ist eine Basis von $n\mathbb{Z}$. $\Diamond$

Bemerkung 1.25. (Annihilator)

1. Zu dem Homomorphismus $f : R \to Rv$ mit $\alpha \mapsto \alpha v$ heißt das R-Ideal $\mathrm{Kern}(f) = \{\alpha \in R \mid \alpha v = 0\}$ der Annihilator von v und wird mit $\mathrm{Ann}(v)$ bezeichnet.
2. In dem $\mathbb{Z}$-Modul $\mathbb{Z}/n\mathbb{Z}$ ist $\mathrm{Ann}(\overline{1}) = n\mathbb{Z}$. $\mathbb{Z}/n\mathbb{Z}$ ist nicht frei: $(\overline{1})$ ist ein Erzeugendensystem von $\mathbb{Z}/n\mathbb{Z}$, aber $n\overline{1} = 0$ für $n \neq 0$. $\Diamond$

Wiederholung 1.26. (Modul-Struktursätze)

1. Seien R ein Hauptidealring, M ein freier R-Modul mit Basis $\{v_1, ..., v_n\}$ und $M' \neq \{0\}$ ein R-Untermodul von M. Dann ist M' frei vom Rang $m \leq n$ und es existiert eine Basis $\{e_1, ..., e_n\}$ von M und eine Teilerkette von Koeffizienten $\alpha_1 \mid \cdots \mid \alpha_m \in R\backslash\{0\}$, so dass eine Basis von M' gegeben ist durch $\{\alpha_1 e_1, ..., \alpha_m e_m\}$. (Elementarteilersatz)
2. Seien R ein Hauptidealring und M ein endlich erzeugter R-Modul. Dann existieren $v_1, ..., v_m \in M$ und eine Teilerkette $\alpha_1 \mid \cdots \mid \alpha_m \in R$ mit $M = Rv_1 \oplus \cdots \oplus Rv_m$ und $\mathrm{Ann}(v_i) = R\alpha_i$, speziell $\mathrm{Ann}(v_{i+1}) \subseteq \mathrm{Ann}(v_i)$, für alle $i = 1, ..., m$. (Erster Struktursatz für endlich erzeugte Moduln)

3. $\{v_1, ..., v_m\}$ muss keine R-Basis von M sein. Es gilt stattdessen:

$$\sum_{i=1}^{m} \gamma_i v_i = \sum_{i=1}^{m} \beta_i v_i \iff (\gamma_i - \beta_i)v_i = 0 \iff (\gamma_i - \beta_i) \in \mathrm{Ann}(v_i) \iff \gamma_i \equiv \beta_i \bmod \alpha_i.$$

4. Sei R ein Hauptidealring und Integritätsbereich und sei M ein endlich erzeugter R-Modul. Dann gibt es $v_1, ..., v_m \in M$, $p_1, ..., p_m \in R$ prim (bzw. irreduzibel) und $\nu_1, ..., \nu_m \in \mathbb{N}_0$ mit $M = Rv_1 \oplus \cdots \oplus Rv_m$ und $\mathrm{Ann}(v_i) = Rp_i^{\nu_i}$ oder $\{0\}$. (Zweiter Strukturtsatz für endlich erzeugte Moduln)

5. Jede endlich erzeugte abelsche Gruppe ist direkte Summe von endlich vielen Kopien von $\mathbb{Z}$ und von gewissen zyklischen Gruppen $\mathbb{Z}/p_i^{\nu_i}\mathbb{Z}$. (Struktursatz für endlich erzeugte, abelsche Gruppen)

Beweise der Struktursätze finden sich in [6], Kapitel 4.6. ◊

Korollar 1.27.

Sei G eine endlich erzeugte, abelsche Gruppe. Dann gibt es $v \in G$ mit $\mathrm{Ord}(v) = \mathrm{kgV}\{\mathrm{Ord}(w) \mid w \in G\}$.

Beweis.

G ist ein endlich erzeugter $\mathbb{Z}$-Modul. Nach dem Ersten Struktursatz für endlich erzeugte Moduln 1.26 besitzt G dann eine Darstellung $G = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_n \cong m_1\mathbb{Z} \oplus \cdots \oplus m_n\mathbb{Z}$ mit $\mathrm{Ann}(v_1) \supseteq \cdots \supseteq \mathrm{Ann}(v_n)$ bzw. $m_1 \mid \cdots \mid m_n$ und $\mathrm{Ord}(v_n) = m_n$ für gewisse $v_1, ..., v_n \in G$. Sei $w \in G$. Dann ist $w = \alpha_1 v_1 + \cdots + \alpha_n v_n$ für gewisse $\alpha_1, ..., \alpha_n$. Damit ist $m_n w = \alpha_1 m_n v_1 + \cdots + \alpha_n m_n v_n = 0$, denn $m_n \in \mathrm{Ann}(v_n)$, d.h. $m_n \in \mathrm{Ann}(v_i)$ für $i = 1, ..., n$. Also ist auch $m_n \in \mathrm{Ann}(w) \cong \mathrm{Ord}(w)\mathbb{Z}$, d.h. $\mathrm{Ord}(w)$ ist Teiler von m_n. □

2. Ganze algebraische Zahlen

2.1. Ganze Größen

Definition 2.1.

Seien L ein Körper, R ein Unterring von L und $\alpha \in L$. Dann heißt α ganz über R, falls es ein normiertes Polynom $f \in R[X]$ gibt mit $f(\alpha) = 0$. α heißt ganz algebraisch, falls $R = \mathbb{Z}$ ist.

Beispiel 2.2.

1. Sei $\alpha \in \mathbb{Z}$, dann annuliert α das normierte Polynom $f(X) = X - \alpha \in \mathbb{Z}[X]$, d.h. die "ganzen" Zahlen $\mathbb{Z}$ sind ganz im Sinne der obigen Definition.

2. Sei $\alpha \in \mathbb{Q}\backslash\mathbb{Z}$, etwa $\alpha = \frac{\beta}{\gamma\pi}$ mit $\pi, \beta, \gamma \in \mathbb{Z}$, π prim und $\pi \nmid \beta$. Dann ist α nicht ganz: Angenommen, für das Polynom $f(X) = X^n + a_{n-1}X^{n-1} + a_0 \in \mathbb{Z}[X]$ gilt $f(\alpha) = 0$. Multiplikation mit $(\gamma\pi)^n$ liefert: $\beta^n + a_{n-1}\beta^{n-1}(\gamma\pi) + \cdots + a_0(\gamma\pi)^n = 0$. π teilt alle Summanden außer dem ersten und π teilt auch 0. Also muss auch $\pi \mid \beta^n$ gelten, d.h. $\pi \mid \beta$, ein Widerspruch.

3. Wir haben dabei nur benutzt: $\mathbb{Q} = \mathrm{Quot}(\mathbb{Z})$ und $\mathbb{Z}$ ist faktoriell, d.h. ist allgemein L der Quotientenkörper eines faktoriellen Ringes R, dann gilt: $\alpha \in L$ ist ganz über R g.d.w. $\alpha \in R$. ◊

Lemma 2.3.

Seien L ein Körper, R ein Unterring von L und $\alpha \in L$. Dann sind äquivalent:

1. α ist ganz über R.
2. $R[\alpha]$ ist ein endlich erzeugter R-Modul.
3. Es gibt einen nicht trivialen, endlich erzeugten R-Modul M mit $\alpha M \subseteq M$.

Beweis.

Wir zeigen die Implikationen (1) ⇒ (2), (2) ⇒ (3) und (3) ⇒ (1).

1. Sei α ganz über R, etwa $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$ für gewisse Koeffizienten $a_i \in R$. Also liegt $\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_0$ im endlich erzeugten R-Modul $M = R\alpha^{n-1} + \cdots + R$. Per Induktion folgt: Alle α^m liegen in M, also $R[\alpha] \subseteq M \subseteq R[\alpha]$, d.h. $M = R[\alpha]$.
2. Sei $M = R[\alpha]$ ein endlich erzeugter R-Modul. Wegen $1 \in M$ ist $M \neq \{0\}$. Weiter ist $\alpha R[\alpha] \subseteq R[\alpha]$.
3. Sei $M = R\beta_1 + \cdots + R\beta_n$, $M \neq \{0\}$, mit $\alpha M \subseteq M$, etwa $\alpha\beta_i = a_{i1}\beta_1 + \cdots + \alpha_{in}\beta_n$, $1 \leq i \leq n$, mit nicht notwendig eindeutig bestimmten $a_{ij} \in R$. Bezeichne A die Matrix $(a_{ij})_{1\leq i\leq n}^{1\leq j\leq n}$. Dann gilt für das normierte Polynom $f(X) = \det(X\mathrm{Id} - A) \in R[X]$, dass $f(\alpha) = 0$, d.h. α ist ganz über R. □

Definition 2.4.

1. Seien M ein R-Modul und $\alpha \in R$ mit $\alpha M \subseteq M$. Dann heißt α ein Stabilisator von M.
2. $\overline{R} = \{\alpha \in L \mid \alpha \text{ ist ganz über } R\}$ heißt der ganze Abschluss von R in L.
3. R heißt ganz abgeschlossen in L, falls $R = \overline{R}$ erfüllt ist.

Bemerkung 2.5.

1. $\overline{R}$ ist Teilring von L mit $R \subseteq \overline{R}$:

   Wir zeigen, dass $\overline{R}$ abgeschlossen ist unter den Ringoperationen. Seien dafür $\alpha, \beta \in \overline{R}$. Dann existieren nichttriviale, endlich erzeugte R-Moduln M_1, M_2 mit $\alpha M_1 \subseteq M_1$ und $\beta M_2 \subseteq M_2$. Setze $M = M_1 M_2$, dann gelten $(\alpha+\beta)M \subseteq M$ und $(\alpha\beta)M \subseteq M$, d.h. $\alpha+\beta \in \overline{R}$ und $\alpha\beta \in \overline{R}$. Also ist der ganze Abschluss von R in L ein Ring.
2. Sei R faktoriell mit $L = \mathrm{Quot}(R)$. Dann gilt $R = \overline{R}$.

   Der Beweis wurde bereits in Beispiel 2.2 geführt.
3. Es gilt: $\overline{\overline{R}} = \overline{R}$:

   Wir zeigen $\overline{\overline{R}} \subseteq \overline{R}$. Sei $\alpha \in \overline{\overline{R}}$. Dann gibt es einen nichttrivialen $\overline{R}$-Modul $M = \overline{R}\beta_1 + \cdots + \overline{R}\beta_n$ mit $\alpha M \subseteq M$, d.h. $\alpha\beta_i = a_{i1}\beta_1 + \cdots + a_{in}\beta_n$ für gewisse $a_{ij} \in \overline{R}$, $1 \leq i, j \leq n$. Dann ist $R' = R[a_{ij}]_{1\leq j\leq n}^{1\leq i\leq n}$ ein endlich erzeugter R-Modul. Setze $M' = R'\beta_1 + \cdots + R'\beta_n$. Dies ist ein endlich erzeugter R'-Modul, also auch R-Modul, mit $\alpha M' \subseteq M'$. Also ist α ganz über R, d.h. $\alpha \in \overline{R}$. ◊

Definition 2.6.

1. Eine Erweiterung von $\mathbb{Q}$ durch Quadratwurzeladjunktion nennt man eine quadratische Erweiterung.
2. $d \in \mathbb{Z}$ heißt quadratfrei, falls für alle $a \in \mathbb{Z}$ aus $a^2 \mid d$ folgt, dass $a = \pm 1$.
3. Der Körper $K = \mathbb{Q}(\sqrt{d})$ mit $d \in \mathbb{Z}$ quadratfrei heißt quadratischer Zahlkörper.
4. Wir bezeichnen den ganzen Abschluss von $\mathbb{Z}$ in K mit $\mathcal{O}_K$.

Beispiel 2.7.

1. Im Fall $K = \mathbb{Q}(\sqrt{-1})$ ist $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}(\sqrt{-1})$ ein Hauptidealring.
2. Für $K = \mathbb{Q}(\sqrt{5})$ ist $\mathcal{O}_K = \mathbb{Z} + \frac{1+\sqrt{5}}{2}\mathbb{Z}$ ebenfalls ein Hauptidealring.
3. Für $K = \mathbb{Q}(\sqrt{-5})$ ist $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}(\sqrt{-5})$ dagegen kein Hauptidealring.

Allgemein gilt: ◊

Satz 2.8.

1. Es ist $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{d}$, falls $d \equiv 2 \bmod 4$ oder $d \equiv 3 \bmod 4$.
2. Es ist $\mathcal{O}_K = \mathbb{Z} + \frac{1+\sqrt{d}}{2}\mathbb{Z}$, falls $d \equiv 1 \bmod 4$.

Beweis.

Sei $\alpha = a + b\sqrt{d} \in K$ mit $a, b \in \mathbb{Q}$ und $\kappa : K \to K$ mit $a + b\sqrt{d} \mapsto a - b\sqrt{d}$ die Konjunktion in K; wir setzen $\overline{\alpha} = \kappa(\alpha)$. Dann gilt:

$$\begin{aligned} \alpha \text{ ist ganz über } \mathbb{Z} &\iff \operatorname{Irr}(\alpha, \mathbb{Q}) \in \mathbb{Z}[X] \\ &\iff (X - \alpha)(X - \overline{\alpha}) \in \mathbb{Z}[X] \\ &\iff \alpha + \overline{\alpha},\ \alpha\overline{\alpha} \in \mathbb{Z} \\ &\iff 2a,\ a^2 - b^2 d \in \mathbb{Z}. \end{aligned}$$

Setze $a = \frac{u}{2}$ und $b = \frac{v}{2}$ mit $u, v \in \mathbb{Q}$. Dann ist $\alpha = \frac{u}{2} + \frac{v}{2}\sqrt{d}$ ganz g.d.w. $u \in \mathbb{Z}$, $u^2 - v^2 d \in 4\mathbb{Z}$ und $v \in \mathbb{Z}$.

1. Gelte $d \equiv 2$ oder $d \equiv 3 \bmod 4$. Dann ist $v^2u^2 \equiv 0$ oder $v^2u^2 \equiv 1 \bmod 4$. Es ist

   $$u^2 - v^2 d \equiv 0 \bmod 4 \iff u^2 \equiv 0 \equiv v^2 \bmod 4 \iff 2 \mid u,\ 2 \mid v \iff a, b \in \mathbb{Z}.$$

   Also ist $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{d}$.

2. Gelte $d \equiv 1 \bmod 4$. Dann gilt

   $$u^2 - v^2 d \equiv 0 \bmod 4 \iff u \equiv v \equiv 0 \bmod 2 \text{ und } u \equiv v \equiv 1 \bmod 2.$$

   Damit ist $\mathcal{O}_K = (\mathbb{Z} + \mathbb{Z}\sqrt{d}) \cup ((\frac{1}{2}\mathbb{Z}) + (\frac{\sqrt{d}}{2} + \mathbb{Z}\sqrt{d})) = \mathbb{Z} + \frac{1+\sqrt{d}}{2}\mathbb{Z}$. □

2.2. Dedekind-Ringe

Definition 2.9.

Seien K ein Körper und R ein Teilring von K. Dann heißt R ein Dedekind-Ring, falls R ganz abgeschlossen in K ist, nicht-triviale Primideale von R maximal sind und R Noethersch ist, d.h. alle R-Ideale endlich erzeugt sind.

Bemerkung 2.10.

1. In Hauptidealringen sind Primideale maximal: Seien nämlich p prim und $\mathfrak{p} = Rp \subsetneq Ra$, dann wäre a ein echter Teiler von p, ein Widerspruch.
2. Genau dann ist R ein Hauptidealring, wenn R faktoriell ist und Primideale von R maximal sind.
3. Ein Dedekind-Ring ist genau dann faktoriell, wenn er ein Hauptidealring ist.
4. Seien R ein Hauptidealring und $K = \operatorname{Quot}(R)$. Dann ist R ein Dedekind-Ring.
5. Der ganze Abschluss $\mathcal{O}_K$ von $\mathbb{Z}$ im quadratischen Zahlkörper K ist ein Dedekind-Ring, vgl. Satz 2.23.
6. Ideale in einem Dedekind-Ring R haben die Gestalt $Ra_1 + \cdots + Ra_m$ mit $a_i \in R$.
7. Ein R-Modul in K ist $Rb_1 + \cdots + Rb_m$ mit $b_i = \frac{a_i}{c}$ für $a_i \in R$ und $c \in R$, also $\frac{1}{c}(Ra_1 + \cdots + Ra_m)$.◊

Definition 2.11.

$A \subseteq K$ heißt gebrochenes R-Ideal, falls es ein $c \in R\backslash\{0\}$ gibt, so dass cA ein R-Ideal ist, und ganzes R-Ideal, falls bereits $A \subseteq R$ gilt.

Bemerkung 2.12.

1. Sei R Noethersch. Da alle R-Ideale endlich erzeugt sind, gilt: A ist ein gebrochenes R-Ideal genau dann, wenn A ein endlich erzeugter R-Modul ist.
2. Seien A, B gebrochene R-Ideale und C ein ganzes R-Ideal. Wir setzen

   $$A \cdot B = \left\{ \sum_{i=1}^{m} a_i b_i \;\middle|\; m \in \mathbb{N},\ a_i \in A,\ b_i \in B \right\} \quad \text{und} \quad C^{-1} = \left\{ \alpha \in K \;\middle|\; \alpha A \subseteq R \right\}.$$

   Es gelten:

a) Ist $A \subseteq K$ ein gebrochenes R-Ideal, dann $aA \subseteq A$ für alle $a \in R$. Da A ein R-Modul ist, gilt außerdem $A + A \subseteq A$.

b) Sind $A \subseteq K$ ein gebrochenes R-Ideal und $aA \subseteq A$, dann ist $a \in R$, denn da A endlich erzeugter R-Modul, ist a ganz über R und damit $a \in \overline{R} = R$.

c) Sind A, B gebrochene R-Ideale, dann ist auch AB ein gebrochenes Ideal.

d) Seien $A, B, C \subseteq K$ gebrochene R-Ideale. Dann gelten $A(BC) = (AB)C$ und $AB = BA$ sowie $RA = A$.

e) Seien A, B ganze R-Ideale, dann ist $AB \subseteq A \cap B$.

f) Sei A ein ganzes R-Ideal, dann ist A^{-1} ein gebrochenes R-Ideal, denn aus $d \in A$ folgt stets $A^{-1}d = dA^{-1} \subseteq R$.

g) Es sind $R \subseteq A^{-1}$, $RA^{-1} \subseteq A^{-1}$ und $A^{-1} + A^{-1} \subseteq A^{-1}$ sowie $A^{-1}A \subseteq R$.

3. Für ganze R-Ideale $A, B \subseteq K$ setzen wir $A \mid B :\Leftrightarrow B \subseteq A$. Dann gilt speziell in Hauptidealringen: $(a) \mid (b) \Leftrightarrow a \mid b \Leftrightarrow (b) \subseteq (a)$. ◊

Proposition 2.13.

Sei $\mathfrak{p}$ ein Primideal in R und seien A, B ganze R-Ideale. Dann gilt $\mathfrak{p} \mid AB \Longleftrightarrow \mathfrak{p} \mid A$ oder $\mathfrak{p} \mid B$.

Beweis.

Gelte zunächst $AB \subseteq \mathfrak{p}$. Angenommen, $A \nsubseteq \mathfrak{p}$ und $B \nsubseteq \mathfrak{p}$, dann gibt es $a \in A$ und $b \in B$ mit $a, b \notin \mathfrak{p}$. Wegen $ab \in AB \subseteq \mathfrak{p}$ folgt aber $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$, ein Widerspruch.

Die Rückrichtung ist trivial, denn es gilt $AB \subseteq A$. □

Lemma 2.14.

Sei R ein Dedekind-Ring. Für nicht-triviale Primideale $\mathfrak{p}$ gilt dann: $\mathfrak{p}\mathfrak{p}^{-1} = R$.

Beweis.

Schritt 1: Sei $A \neq \{0\}$ ein ganzes Ideal. Angenommen, es gibt keine Primideale $\mathfrak{p}_1, ..., \mathfrak{p}_n \neq \{0\}$ mit $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subseteq A$. Sei $\mathcal{M}$ die Menge aller solchen A. Dann $\mathcal{M} \neq \emptyset$ und da R Noetschersch, gibt es ein maximales $A \in \mathcal{M}$. A ist nicht prim, d.h. es gibt $a, b \in R$ mit $ab \in A$ und $a, b \notin A$. Setze $A_1 = A + Ra \supsetneq A$ und $A_2 = A + Rb \supsetneq A$. Also gibt es Primideale $\mathfrak{p}_1, ..., \mathfrak{p}_s$ und $\mathfrak{q}_1, ..., \mathfrak{q}_t$ mit $\mathfrak{p} = \mathfrak{p}_1 \cdots \mathfrak{p}_s \subseteq A_1$ und $\mathfrak{q} = \mathfrak{q}_1 \cdots \mathfrak{q}_t \subseteq A_2$. Also $\mathfrak{p} \cdot \mathfrak{q} \subseteq A_1 A_2 \subseteq A + aA + bA + abR \subseteq A$, ein Widerspruch.

Schritt 2: Seien $a \in \mathfrak{p}$ und r minimal mit $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq Ra \subseteq \mathfrak{p}$. Wegen $\mathfrak{p} \mid \mathfrak{p}_1 \cdots \mathfrak{p}_r$, etwa $\mathfrak{p} \mid \mathfrak{p}_1$, folgt also $\mathfrak{p} = \mathfrak{p}_1$, da $\mathfrak{p}_1$ maximal ist, also $\mathfrak{p}_2 \cdots \mathfrak{p}_r \nsubseteq Ra$. Damit gibt es ein $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ mit $b \notin Ra$, d.h. $\frac{b}{a} \notin R$. $\mathfrak{p}b \subseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r$ impliziert $\mathfrak{p}\frac{b}{a} \subseteq R$, d.h. $\frac{b}{a} \in \mathfrak{p}^{-1} \backslash R$. Wegen $\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq R$ und $\mathfrak{p}$ maximal folgt somit $\mathfrak{p} = \mathfrak{p}\mathfrak{p}^{-1}$ oder $\mathfrak{p}\mathfrak{p}^{-1} = R$. Allerdings kann $\mathfrak{p} = \mathfrak{p}\mathfrak{p}^{-1}$ nicht sein, sonst wäre $\frac{b}{a}\mathfrak{p} \subseteq \mathfrak{p}$, d.h. $\frac{b}{a} \in \overline{R} = R$, ein Widerspruch. □

Satz 2.15.

Sei R ein Dedekind-Ring. Für jedes ganze $A \neq \{0\}$ gilt dann: $AA^{-1} = R$.

Beweis.

Angenommen, $AA^{-1} \neq R$. Da R Noethersch, besitzt A eine Darstellung $A = \frac{1}{c}(Ra_1 + \cdots + Ra_m) \neq \{0\}$ maximal. Speziell ist A nicht prim, d.h. es gibt ein Primideal $\mathfrak{p}$ mit $A \subsetneq \mathfrak{p}$, insbesondere $\mathfrak{p}^{-1} \subsetneq A^{-1}$, d.h. $A \subseteq \mathfrak{p}^{-1}A \subseteq A^{-1}A \subseteq R$. Wäre $A = A\mathfrak{p}^{-1}$, dann $A\mathfrak{p}\mathfrak{p}^{-1} = A\mathfrak{p}$ und für $ba^{-1} \in \mathfrak{p}^{-1} \backslash R$ würde folgen $(ba^{-1})A\mathfrak{p} \subseteq A\mathfrak{p}$, d.h. ba^{-1} würde den endlich erzeugten Modul $A\mathfrak{p}$ erzeugen, d.h. $\frac{b}{a} \in \overline{R} = R$, ein Widerspruch. Also gilt $A \subsetneq B$ für $B = A\mathfrak{p}^{-1}$. Damit ist $A\mathfrak{p}^{-1}B^{-1} = BB^{-1} \subseteq R$. Es gilt sogar Gleichheit, denn $A\mathfrak{p}^{-1} \supsetneq A$ und A maximal mit $AA^{-1} \neq R$, also $BB^{-1} = R$. Damit $A(\mathfrak{p}^{-1}B^{-1}) = R$. Zu zeigen

ist also nur noch: $C = A^{-1}$ für $C = \mathfrak{p}^{-1}B^{-1}$. Dazu: $AC \subseteq R \Rightarrow C \subseteq A^{-1}$. Für die andere Inklusion sei $\alpha \in A^{-1}$. Dann ist $\alpha A \subseteq R$, d.h. $\alpha R = \alpha AC \subseteq RC = C$, also $\alpha \cdot 1 = \alpha \in C$ und damit $C = A^{-1}$, d.h. $AA^{-1} = R$, ein Widerspruch. Für alle $A \neq \{0\}$ gilt somit: $AA^{-1} = R$. □

Bemerkung 2.16.

1. Für $d \in R$ gilt $(dR)^{-1} = d^{-1}R$, denn $\alpha \in (dR)^{-1} \Leftrightarrow \alpha d \in R \Leftrightarrow \alpha \in d^{-1}R$.
2. Jedes von $\{0\}$ verschiedene, gebrochene Ideal A ist invertierbar: Sei $dA \subseteq R$, dann gilt für $B = (dA)^{-1}$, dass $(dA)B = A(dB) = R$. Die Menge der von $\{0\}$ verschiedenen, gebrochenen R-Ideale bilden folglich eine multiplikative Gruppe, die wir mit $\mathcal{I}(R)$ bezeichnen.
3. Seien A, B ganze R-Ideale. Dann gilt $A \mid B \Leftrightarrow$ es gibt ein ganzes R-Ideal C mit $AC = B$: Gelte zunächst $B = AC$, dann $B \subseteq A \cap C \subseteq A$, d.h. $A \mid B$. Sei umgekehrt A ein Teiler von B, dann setze $C = BA^{-1} \subseteq AA^{-1} = R$, d.h. C ist ganz und $AC = A(A^{-1}B) = (AA^{-1})B = RB = B$. ◊

Satz 2.17. (Hauptsatz für Dedekind-Ringe)

Seien R ein Dedekind-Ring und $K = \mathrm{Quot}(R)$. Dann bilden die von $\{0\}$ verschiedenen gebrochenen Ideale von K eine multiplikative Gruppe $\mathcal{I}(R)$. Und jedes ganze Ideal lässt sich bis auf Permutationen eindeutig als endliches Produkt von Primidealen schreiben.

Beweis.

Existenz: Sei A ganz und nicht von dieser Gestalt. Dann gibt es ein maximales A, das sich so nicht schreiben lässt. A kann nicht prim sein. Also gibt es ein Primideal $\mathfrak{p}$ mit $A \subsetneq \mathfrak{p}$, d.h. es gelten die Inklusionen $A \subseteq \mathfrak{p}^{-1}A \subseteq A^{-1}A = R$. Nun ist $A = \mathfrak{p}^{-1}A$ unmöglich, da $\mathfrak{p}^{-1} \neq R$: Multipliziere dazu beide Seiten mit A^{-1}. Also muss gelten $A \subsetneq A\mathfrak{p}^{-1} \subseteq R$. Damit ist $A\mathfrak{p}^{-1} = \mathfrak{p}_2 \cdots \mathfrak{p}_r$, d.h. $A = \mathfrak{p}\mathfrak{p}_2 \cdots \mathfrak{p}_r$, ein Widerspruch.

Eindeutigkeit: Sei $A = \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$. Es gilt also $\mathfrak{p}_1 \mid A = \mathfrak{q}_1 \cdots \mathfrak{q}_s$, etwa $\mathfrak{p}_1 \mid \mathfrak{q}_1$. Da $\mathfrak{q}_1$ maximal, folgt $\mathfrak{p}_1 = \mathfrak{q}_1$. Also ist $\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s$ und per Induktion folgen $r = s$ und $\mathfrak{p}_i = \mathfrak{q}_i$ für $1 \leq i \leq r$. □

Bemerkung 2.18.

1. Bilden die gebrochenen Ideale von $K = \mathrm{Quot}(R)$ eine multiplikative Gruppe, so ist R Dedekind-Ring.
2. Sei A gebrochenes Ideal, d.h. es gibt B ganz und $d \in R\backslash\{0\}$ mit $A = \frac{B}{d}$. Dann $A = B(Rd)^{-1} = \frac{\mathfrak{p}_1 \cdots \mathfrak{p}_r}{\mathfrak{q}_1 \cdots \mathfrak{q}_s}$.
3. Über einem Dedekind-Ring $R \subseteq K = \mathrm{Quot}(R)$ ist die Gruppe $\mathcal{I}(R)$ eindeutig erzeugt von den Primidealen, d.h. die abelsche Gruppe $\mathcal{I}(R)$ ist frei.
4. Wir schreiben $(\alpha_1, ..., \alpha_n)$ für das endlich erzeugte Ideal $R\alpha_1 + \cdots + R\alpha_n$. Speziell ist $(\alpha) = R\alpha$ ein Hauptideal für $\alpha \in K$. Es gilt $(\alpha)^{-1} = (\alpha^{-1})$ für alle $\alpha \neq 0$. ◊

Definition 2.19.

Sei R ein Dedekind-Ring. Bezeichne $\mathcal{I}_0$ die Untergruppe der Hauptideale von $\mathcal{I}$.

Dann heißt $\mathcal{I}/\mathcal{I}_0$ die Idealklassengruppe und $\mathrm{h}(R) = \sharp(\mathcal{I}/\mathcal{I}_0)$ die Klassenzahl von R.

Bemerkung 2.20.

Gelte $[K : \mathbb{Q}] < \infty$, d.h. K sei eine endliche algebraische Erweiterung von $\mathbb{Q}$. Dann ist auch die Klassenzahl $\mathrm{h}(\mathcal{O}_K)$ endlich, vgl. Satz 3.24. ◊

Korollar 2.21.

Zu jedem $A \subseteq \mathcal{O}_K$ gibt es eine Erweiterung $L = K(\alpha)$ mit $A = K \cap \mathcal{O}_L\omega$ für ein $\omega \in \mathcal{O}_L$.

Speziell gilt für $\gamma \in \mathcal{O}_K$, dass $\gamma \in A \Leftrightarrow \omega \mid \gamma$ in $\mathcal{O}_L$.

Beweis.

Bezeichne $h = \mathrm{h}(\mathcal{O}_K)$ die Klassenzahl von $\mathcal{O}_K$. Nach dem kleinen Satz von Fermat [6], Kapitel 2.3, ist dann $A^h = \mathcal{O}_K\beta$ für ein $\beta \in \mathcal{O}_K$ Hauptideal. Setze $\omega = \sqrt[h]{\beta}$ und $L = K(\omega)$. In $\mathcal{O}_K$ gilt dann:

$$\gamma \in A \Leftrightarrow (\gamma) \subseteq A \Leftrightarrow A \mid (\gamma) \Leftrightarrow A^h \mid (\gamma^h) \Leftrightarrow \left(\frac{\gamma}{\omega}\right)^h = \frac{\gamma^h}{\beta} \in \mathcal{O}_L \Leftrightarrow \frac{\gamma}{\omega} \in \mathcal{O}_L \Leftrightarrow \omega \mid \gamma \text{ in } \mathcal{O}_L,$$

denn allgemein gilt $\delta^k \in \mathcal{O}_L \Rightarrow X^k - \delta^k \in \mathcal{O}_L[X] \Rightarrow \delta \in \overline{\mathcal{O}}_L = \mathcal{O}_L$. Beachte dabei: $\mathcal{O}_L \cap K = \mathcal{O}_K$. □

Bemerkung 2.22.

Es gilt sogar: Zu jedem $A \subseteq \mathcal{O}_K$ gibt es eine Erweiterung $L = K(\alpha)$ mit $A = K \cap \mathcal{O}_L\alpha$, d.h. man kann $\omega = \alpha$ wählen. ◊

Satz 2.23.

Seien o ein Dedekind-Ring mit $K = \mathrm{Quot}(o)$ und $L|K$ eine endliche separable Erweiterung. Dann ist der ganze Abschluss O von o in L ein Dedekind-Ring von L.

Beweis.

1. O ist ganz abgeschlossen in $L = \mathrm{Quot}(O)$.
2. Sei $\mathfrak{P} \neq \{0\}$ prim in O. Dann ist $\mathfrak{P} \cap o = \mathfrak{p}$ prim in o. Sei $\alpha \in \mathfrak{P}$, dann $0 = \alpha^m + a_{m-1}\alpha^{m-1} + \cdots + a_0$ mit Koeffizienten $a_i \in o$ für alle i; o.B.d.A. $a_0 \neq 0$. Dann $a_0 = \alpha^m + \cdots + a_1\alpha \in \mathfrak{P} \cap o = \mathfrak{p}$. Also $\mathfrak{p} \neq \{0\}$. Dann ist $k = o/\mathfrak{p}$ ein Körper. Betrachte den Homomorphismus $\sigma : o \to O/\mathfrak{P}$ mit $\sigma(a) = a + \mathfrak{P}$. Es ist $\mathrm{Kern}(\sigma) = o \cap \mathfrak{P} = \mathfrak{p}$ und damit ist $o/\mathfrak{p} \hookrightarrow O/\mathfrak{P}$ eine Einbettung. Sei $\alpha \in O$, d.h. $\overline{\alpha} = \alpha + \mathfrak{P} \in O/\mathfrak{P}$. Wegen $0 = \alpha^m + a_{m-1}\alpha^{m-1} + \cdots + a_0$ mit $a_i \in o$ ist $0 = \overline{\alpha}^m + \overline{a}_{m-1}\overline{\alpha}^{m-1} + \cdots + \overline{a}_0$, d.h. $\overline{\alpha}$ ist algebraisch über $o/\mathfrak{p} = k$, also ist $k[\overline{\alpha}]$ ein Körper und damit $\overline{\alpha}^{-1} \in k[\overline{\alpha}]$. Also ist auch $O/\mathfrak{P}$ ein Körper, d.h. $\mathfrak{P}$ ist ein maximales Ideal.
3. Sei $A \subseteq O$ ein O-Ideal. Wir zeigen: O ist ein endlich erzeugter o-Modul, denn dann folgt aus o ist ein Noetherscher Ring, dass O Noetherscher o-Modul ist, d.h. $A = o\alpha_1 + \cdots + o\alpha_m$ ist endlich erzeugter o-Modul und damit $A = O\alpha_1 + \cdots + O\alpha_m$. In Proposition 2.39 zeigen wir dafür, dass in der Tat ein endlich erzeugter o-Modul $M = o\mathfrak{p}_1 + \cdots + o\mathfrak{p}_n$ existiert mit $O \subseteq M \subseteq L$. □

Bemerkung 2.24.

Es gilt $L = \mathrm{Quot}(\mathcal{O}_L)$: Sei $\alpha \in L$, dann ist α algebraisch über $\mathbb{Q}$, d.h. es gibt $a_i \in \mathbb{Q}$, $i = 0, ..., n-1$, mit $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$. Wegen $\mathbb{Q} = \mathrm{Quot}(\mathbb{Z})$ gibt es dann $b_0, ..., b_n$ mit $b_n \neq 0$ und $b_n\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_0 = 0$. Multiplikation mit b_n^{n-1} ergibt: $(b_n\alpha)^n + b_{n-1}(b_n\alpha)^{n-1} + \cdots + b_n^{n-1}a_0 = 0$. Also ist $b_n\alpha = \beta \in \mathcal{O}_L$. ◊

2.3. Spuren und Normen

Bemerkung 2.25.

Seien $A \subseteq B$ kommutative Ringe mit Eins, so dass B über A ein freier A-Modul ist. Sei $E = (e_1, ..., e_n)$ eine Basis von B über A, d.h. $B = Ae_1 \oplus \cdots \oplus Ae_n$ mit $\alpha_1e_1 + \cdots + \alpha_ne_n = 0$ nur wenn bereits $\alpha_1, ..., \alpha_n = 0$. Sei $u : B \to B$ ein Modul-Endomorphismus, d.h. eine A-lineare Abbildung: $u(\alpha b_1 + \beta b_2) = \alpha u(b_1) + \beta u(b_2)$ für alle $\alpha, \beta \in A$ und alle $b_1, b_2 \in B$. Sei $\mathrm{Mat}_E^E(u) = (a_{ij}) \in A^{n\times n}$ die Darstellungsmatrix von u bzgl. der Basis E, d.h. $a_{ij} = u_i(e_j)$. Dann ist das charakteristische Polynom χ_u, gegeben als die Determinante $\chi_u(t) = \det(t\mathrm{Id} - \mathrm{Mat}_E^E(u)) = t^n - a_{n-1}t^{n-1} + \cdots + (-1)^n a_0$, unabhängig von der Wahl der Basis. ◊

Definition 2.26.

Die Spur $\mathrm{S}(u) \in A$ und die Norm $\mathrm{N}(u) \in A$ des Endomorphismus u sind gegeben durch

$$\mathrm{S}(u) = a_{n-1} = \sum_{i=1}^{n} a_{ii} \qquad \text{und} \qquad \mathrm{N}(u) = a_0 = \det((a_{ij})).$$

Bemerkung 2.27.

1. Norm und Spur sind unabhängig von der Wahl der Basis. Sei nämlich $F = (f_1, ..., f_n)$ eine andere Basis über A, d.h. es gibt Matrizen $\beta = \mathrm{Mat}_F^E(\mathrm{Id})$ und $\gamma = \mathrm{Mat}_E^F(\mathrm{Id})$ mit $\beta\gamma = \mathrm{Id}$, d.h. $\det(\beta)\det(\gamma) = 1$, also sind die Determinanten der Basiswechselmatrizen Einheiten in A. Insbesondere gilt:

$$\det(\mathrm{Mat}_F^F(u)) = \det(\gamma \mathrm{Mat}_E^E(u)\beta) = \det(\beta)^{-1}\det(\mathrm{Mat}_E^E(u))\det(\beta) = \det(\mathrm{Mat}_E^E(u)),$$

   d.h. die Determinante ist unabhängig von der der Darstellungsmatrix zugrunde liegenden Basis, und

$$\det(t\mathrm{Id} - \mathrm{Mat}_F^F(u)) = \det(\gamma(t\mathrm{Id})\beta - \gamma\mathrm{Mat}_E^E(u)\beta) = \det(\gamma(t\mathrm{Id} - \mathrm{Mat}_E^E(u))\beta) = \det(t\mathrm{Id} - \mathrm{Mat}_E^E(u)),$$

   d.h. auch das charakteristische Polynom und insbesondere a_0, a_{n-1} hängen nicht von E ab.

2. Für $x \in B$ betrachten wir $m_x : B \to B$ mit $m_x(y) = yx$. Dies ist ein Endomorphismus:

$$m_x(\alpha y + \beta z) = x(\alpha y + \beta z) = \alpha xy + \beta xz = \alpha m_x(y) + \beta m_x(z) \quad \text{für alle } y, z \in B \text{ und } \alpha, \beta \in A.$$

   Weiter gelten $m_{x+x'} = m_x + m_{x'}$ und $m_{xx'} = m_{x'} \circ m_x$ sowie $m_{ax} = am_x$ für alle $a \in A$. ◊

Definition 2.28.

Sei $x \in B$, dann heißt $\mathrm{S}_{B|A}(x) = \mathrm{S}(m_x)$ die Spur von x, $\mathrm{N}_{B|A}(x) = \mathrm{N}(m_x)$ die Norm von x und $\chi_{B|A}(x) = \chi(m_x)$ das charakteristisches Polynom von x.

Bemerkung 2.29.

1. Für alle $x, x' \in B$ und alle $a \in A$ gelten $\mathrm{S}(x+x') = \mathrm{S}(x)+\mathrm{S}(x')$ und $\mathrm{S}(ax) = a\mathrm{S}(x)$, speziell $\mathrm{S}(a) = na$.
2. Außerdem gelten $\mathrm{N}(xx') = \mathrm{N}(x)\mathrm{N}(x')$ und $\mathrm{N}(ax) = a^n\mathrm{N}(x)$, insbesondere $\mathrm{N}(a) = a^n$. ◊

Satz 2.30.

Sei $L|K$ eine algebraische Körpererweiterung vom Grad n. Weiter seien $x \in L$, $f = \mathrm{Irr}(x, K) \in K[t]$ und $x_1, ..., x_n$ seien alle Nullstellen von f im algebraischen Abschluss von K, wobei jede Nullstelle $\deg(f) = [K : K(x)]$ oft wiederholt wird. Dann gelten:

$$\mathrm{S}_{L|K}(x) = x_1 + \cdots + x_n, \qquad \mathrm{N}_{L|K}(x) = x_1 \cdots x_n \qquad \text{und} \qquad \chi_{L|K}(x) = f^{[L:K(x)]}.$$

Beweis.

Fall 1: Gelte $L = K(x) = K + Kx + \cdots + Kx^{n-1}$, d.h. $[L : K(x)] = 1$ und $[K(x) : K] = \deg(f) = n$. Dann ist $1, x, ..., x^{n-1}$ eine K-Basis von L und f lässt sich schreiben als $f = t^n + a_{n-1}t^{n-1} + \cdots + a_1t + a_0$, $f(x) = 0$ und alle $a_i \in K$. Es gelten $m_x(x^m) = x^{m+1}$, $m < n-1$ und $m_x(x^{n-1}) = x^n = -a_0 - a_1x - \cdots - a_{n-1}x^{n-1}$. Bzgl. der gewählten Basis erhalten wir die Darstellungen

$$m_x = \begin{pmatrix} 0 & \cdots & \cdots & 0 & -a_0 \\ 1 & \ddots & 0 & \vdots & -a_1 \\ 0 & \ddots & \ddots & \vdots & -a_2 \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix} \quad \text{und} \quad t\mathrm{Id} - m_x = \begin{pmatrix} t & 0 & \cdots & 0 & a_0 \\ -1 & \ddots & \ddots & \vdots & a_1 \\ 0 & \ddots & \ddots & 0 & a_2 \\ \vdots & \ddots & \ddots & t & \vdots \\ 0 & \cdots & 0 & -1 & t + a_{n-1} \end{pmatrix}$$

Entwicklung nach der letzten Spalte liefert:

$$\begin{aligned} &\det(t\mathrm{Id} - m_x) \\ &= (-1)^{n-1}a_0(-1)^{n-1} + (-1)^{n-2}a_1t(-1)^{n-2} + \cdots + (-1)^1a_{n-1}t^{n-2}(-1)^1 + (t + a_{n-1})t^{n-1} \\ &= a_0 + a_1t + \cdots + a_{n-1}t^{n-1} + t^n = f(t) = \mathrm{Irr}(x, K) = (t - x_1)\cdots(t - x_n) \end{aligned}$$

im algebraischen Abschluss, also speziell $\mathrm{S}(x) = -a_{n-1} = x_1 + \cdots + x_n$ und $\mathrm{N}(x) = (-1)^n a_0 = x_1 \cdots x_n$.

Fall 2: Seien $[L : K(x)] = r$, $[K(x) : K] = m$ und $[L : K] = n$, d.h. $r = \frac{n}{m}$. Dann ist $1, x, ..., x^{m-1}$ eine Basis von $K(x)$ über K. Wähle als Basis von L über $K(x)$ eine Basis $z_1, ..., z_r$, dann ist eine K-Basis von L gegeben durch $1z_1, ..., x^{m-1}z_1, 1z_2, ..., x^{m-1}z_2, ..., ..., 1z_r, ..., x^{m-1}z_r$ eine Basis von L über K. Die Matrix m_x von $y \mapsto xy$ in L hat die Gestalt

$$\begin{pmatrix} \square & 0 & \cdots & 0 \\ 0 & \square & \ddots & 0 \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \square \end{pmatrix} \quad \text{mit} \quad \square = \begin{pmatrix} 0 & \cdots & \cdots & 0 & -a_0 \\ 1 & \ddots & 0 & \vdots & -a_1 \\ 0 & \ddots & \ddots & \vdots & -a_2 \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix}.$$

Also folgt: $\chi_{L|K}(x) = \det(t\mathrm{Id} - m_x) = \det(t\mathrm{Id} - \square)^r = \mathrm{Irr}(x, K)^r = \mathrm{Irr}(x, K)^{[L:K(x)]}$. Desweiteren sind $\mathrm{S}_{L|K}(x) = \mathrm{S}(m_x) = r\mathrm{S}(\square) = x_1 + \cdots + x_n$ und $\mathrm{N}_{L|K}(x) = \det(m_x) = \det(\square^r) = x_1 \cdots x_n$. □

Proposition 2.31.

Sei o in K ganz abgeschlossen und sei $x \in L$ ganz über o.

Dann ist $\chi_{L|K}(x) \in o[X]$, insbesondere $\mathrm{S}_{L|K}(x) \in o$ und $\mathrm{N}_{L|K}(x) \in o$.

Beweis.

Zu zeigen ist: Alle x_i von eben sind ganz über o, denn dann liegen die Koeffizienten von f in $\mathcal{O} \cap K = o$, da sie ganz über o und aus K sind. Es sind $f = (t - x_1) \cdots (t - x_n)$ und $\chi_{L|K}(x) = \det(t\mathrm{Id} - m_x) = f^r \in o[X]$. Wir zeigen also: Alle Nullstellen von f sind Nullstellen gewisser normierter Polynome über o. Sei $x \in L$ dazu ganz über o, dann ist $g(x) = 0$ für ein normiertes $g \in o[X]$. Mit $f = \mathrm{Irr}(x, K)$ wird durch $f(x) = x_i$ eine Einbettung über K von $K(x)$ in den algebraischen Abschluss von K induziert. Also gilt $g(x_i) = 0$; da g normiert mit Koeffizienten aus o, sind die x_i damit ganz über o. □

Satz 2.32.

Sei $L|K$ separabel vom Grad n und sei $N \supseteq L$ eine Galoiserweiterung von K. Seien $L^{(i)} = \sigma_i(L)$, $1 \leq i \leq n$, die n verschiedenen Einbettungen von K in N und $x^{(i)} = \sigma_i(x)$. Dann gelten für $x \in L$:

$$\mathrm{N}_{L|K}(x) = x^{(1)} \cdots x^{(n)} \qquad \text{und} \qquad \mathrm{S}_{L|K}(x) = x^{(1)} + \cdots + x^{(n)}.$$

Beweis.

Seien $L = K(z)$ und $\mathrm{Irr}(z, K) = (X - \sigma_1(z)) \cdots (X - \sigma_n(z))$. Wir betrachten die beiden Galoisgruppen $G = \mathrm{Gal}(N|K) > H = \mathrm{Gal}(N|L)$.Dann zerlegt G sich disjunkt in $G = \sigma_1 H \cup \cdots \cup \sigma_n H$. Weiter sind die $\sigma_i : L \hookrightarrow N$ definiert durch $z \mapsto z^{(i)} = \sigma_i(z)$. Zu $x \in L$ ist $\mathrm{Irr}(x, K) = (X - x_1) \cdots (X - x_r)$; für die Erweiterungsgrade $r = [K(x) : K]$ und $s = [L : K(x)]$ gilt $rs = [L : K] = n$. $K(x)$ hat r Einbettungen über K in N und L hat s Einbettungen über $K(x)$ in N sowie $rs = n$ Einbettungen über K in N. Jedes x_j taucht dabei s-mal als Bild auf. Also gelten

$$\mathrm{S}_{L|K}(x) = s\sum_{j=1}^{n} x_j = \sum_{i=1}^{n} \sigma_i(x) = \sum_{i=1}^{n} x^{(i)} \qquad \text{und} \qquad \mathrm{N}_{L|K}(x) = s\prod_{j=1}^{n} x_j = \prod_{i=1}^{n} \sigma_i(x) = \prod_{i=1}^{n} x^{(i)},$$

womit alles gezeigt ist. □

Satz 2.33.

Spur und Norm sind transitiv: Seien $K \subseteq L \subseteq L'$ separabel und endlich, dann gelten für $x \in L'$:

$$\mathrm{N}_{L'|K}(x) = \mathrm{N}_{L|K}(\mathrm{N}_{L'|L}(x)) \qquad \text{und} \qquad \mathrm{S}_{L'|K}(x) = \mathrm{S}_{L|K}(\mathrm{S}_{L'|L}(x)).$$

Beweis.

Wähle $N \supseteq L'$ mit $N|K$ Galoisch. Dann gelten für die Galoisgruppen $G = \mathrm{Gal}(N|K)$, $H = \mathrm{Gal}(N|L)$ und $H' = \mathrm{Gal}(N|L')$, dass $G > H > H'$. Weiter lassen sich G, H zerlegen in $G = \sigma_1 H \cup \cdots \cup \sigma_n H$ und $H = \sigma'_1 \cup \cdots \cup \sigma'_m H'$, d.h. $G = \sigma_1\sigma'_1 H' \cup \cdots \cup \cdots \cup \sigma_n\sigma'_m H'$. Also

$$\begin{aligned}
\mathrm{S}_{L'|K} &= \sum_{i,j} \sigma_j \circ \sigma'_i(x) = \sum_j \sum_i \sigma_j \circ \sigma'_i(x) = \sum_j \sigma_j(\sigma_i\sigma'_i(x)) = \sum_j \sigma_j(\mathrm{S}_{L'|L}(x)) = \mathrm{S}_{L|K}(\mathrm{S}_{L'|L}(x)),\\
\mathrm{N}_{L'|K} &= \prod_{i,j} \sigma_j \circ \sigma'_i(x) = \prod_j \prod_i \sigma_j \circ \sigma'_i(x) = \prod_j \sigma_j(\sigma_i\sigma'_i(x)) = \prod_j \sigma_j(\mathrm{N}_{L'|L}(x)) = \mathrm{N}_{L|K}(\mathrm{N}_{L'|L}(x)).
\end{aligned}$$

□

Bemerkung 2.34.

Sei wieder B ein freier A-Modul und sei $(e_1, ..., e_n)$ eine Basis von B über A, d.h. $B = Ae_1 \oplus \cdots \oplus Ae_n$. Dann ist $\sigma : B \times B \to A$ mit $(x, y) \mapsto \mathrm{S}_{B|A}(xy)$ eine symmetrische Bilinearform:

σ ist symmetrisch, da A kommutativ, und bilinear, da für alle $a_1, a_2 \in A$ und alle $x_1, x_2, y \in B$ gilt

$$\begin{aligned}
\sigma(a_1x_1 + \sigma_2x_2, y) = \ & \mathrm{S}((a_1x_1 + a_2x_2)y) \ = \ \mathrm{S}(a_1(x_1y) + a_2(x_2y))\\
& = a_1\mathrm{S}(x_1y) + a_2\mathrm{S}(x_2y) = a_2\sigma(x_1, y) + a_2\sigma(x_2, y)
\end{aligned}$$

◊

Definition 2.35.

Für $x_1, ..., x_n \in B$ heißt $\mathrm{D}_{A|B}(x_1, ..., x_n) = \det(\mathrm{S}(x_ix_j))_{1\le j\le n}^{1\le i\le n}$ die Diskriminante von $x_1, ..., x_n$.

Bemerkung 2.36.

1. Seien $(a_{ij}) \in A^{n\times n}$ und $y_1, ..., y_n \in B$ gegeben durch $y_i = a_{i1}x_1 + \cdots + a_{in}x_n$. Dann gilt

$$\mathrm{D}(y_1, ..., y_n) = \det(a_{ij})^2\mathrm{D}(x_1, ..., x_n) :$$

   Es ist $(\mathrm{S}(y_iy_j)) = (a_{ij})^{\mathrm{T}}(\mathrm{S}(x_ix_j))(a_{ij})$, also $\det(\mathrm{S}(y_iy_j)) = (\det(a_{ij}))^2 \det(\mathrm{S}(x_ix_j))$.

2. Seien $(x_1, ..., x_n)$ und $(y_1, ..., y_n)$ zwei A-Basen von B. Dann ist $\det((a_{ij})_{1\le j\le n}^{1\le i\le n})$ eine Einheit in A, d.h.

$$A\mathrm{D}(x_1, ..., x_n) = A\mathrm{D}(y_1, ..., y_n).$$

3. Seien $L|K$ eine endliche Körpererweiterung und $(x_1, ..., x_n), (y_1, ..., y_n)$ Basen von $L|K$. Dann gilt

$$\mathrm{D}(x_1, ..., x_n) \neq 0 \quad \Longleftrightarrow \quad \mathrm{D}(y_1, ..., y_n) \neq 0.$$

◊

Satz 2.37.

Sei $[L : K] = n$. Dann gilt für jede Basis $(x_1, ..., x_n)$ von $L|K$: $L|K$ ist separabel $\Leftrightarrow \mathrm{D}(x_1, ..., x_n) \neq 0$.

Beweis.

Sei zunächst $L|K$ separabel, o.B.d.A. $L = K(x) = K \oplus \cdots \oplus Kx^{n-1}$ mit Basis $(1, x, ..., x^{n-1})$. Seien $x_1, ..., x_n$ die Konjugierten von x (d.h. die anderen Nullstellen von $\mathrm{Irr}(x, K) = (X - x_1)\cdots(X - x_n)$). Setze $y_l = \sigma_l(y)$, dann $(x^ix^j)_l = x_l^ix_l^j$ und es gilt mit der van-der-Monde-Entwicklungsformel

$$\mathrm{D}(1, x, ..., x^{n-1}) = \det(\mathrm{S}_{L|K}(x^i \cdot x^j)_{0\le j\le n-1}^{0\le i\le n-1}) = \det\left(\sum_{l=1}^n x_l^ix_l^j\right) = \prod_{i<j}(x_i - x_j)^2 \neq 0.$$

Nehmen wir umgekehrt an, $L|K$ wäre nicht separabel. Sei $\mathrm{char}(K) = p$. Dann ist $\mathrm{S}_{L|K}(z) = 0$ für alle $z \in L$: Ist z separabel, dann $\mathrm{S}_{L|K}(z) = [L : K(z)] \cdot (z_1 + \cdots + z_{[K(z):K]})$; da $L|K(z)$ aufgrund der Transitivität der Separabilität selbst nicht separabel sein kann, folgt somit $p \mid [L : K(z)]$ und wegen $\mathrm{char}(K) = p$ also $\mathrm{S}(z) = 0$. Ist dagegen z nicht separabel, dann hat jede Nullstelle von $\mathrm{Irr}(z, K)$ die Vielfachheit p, also auch in dem Fall $\mathrm{S}(z) = 0$. □

Satz 2.38. (duale Basis)

Sei $L|K$ endlich und separabel mit Basis $x_1, ..., x_n$. Dann existiert eine duale Basis $x_1^*, ..., x_n^*$ mit $\mathrm{S}_{L|K}(x_i x_j^*) = \delta_{ij}$, wobei δ das Kronecker-Symbol bezeichnet.

Beweis.

Setze $x_j^* = \xi_1^j x_1 + \cdots + \xi_n^j x_n$ und löse die j linearen Gleichungssysteme

$$\xi_1^j \mathrm{S}(x_i x_1) + \cdots + \xi_n^j \mathrm{S}(x_i x_n) = 0 \ (i \neq j), \qquad \xi_1^j \mathrm{S}(x_j x_1) + \cdots + \xi_n^j \mathrm{S}(x_j x_n) = 0.$$

Die Systeme sind universell lösbar, da für die zugehörigen Koeffizientenmatrizen nach Satz 2.37 gilt $\det(\mathrm{S}(x_i x_j)) = \mathrm{D}(x_1, ..., x_n) \neq 0$. Noch zu zeigen: $x_1^*, ..., x_n^*$ sind K-linear unabhängig. Gelte hierfür $0 = a_1 x_1^* + \cdots + a_n x_n^*$, dann

$$0 = \mathrm{S}(0) = \mathrm{S}((a_1 x_1^* + \cdots + a_n x_n^*)(x_i)) = \mathrm{S}(a_i x_i^* x_i) = a_i \mathrm{S}(x_i x_i^*) = a_i. \qquad \square$$

Proposition 2.39.

Seien $L|K$ separabel und endlich, o ein Dedekind-Ring, $K = \mathrm{Quot}(o)$ und O der ganze Abschluss von o in L. Dann gibt es einen endlich erzeugten o-Modul $M \subseteq L$ mit $O \subseteq M$.

Beweis.

Wähle $x_1, ..., x_n \in O$ als Basis von $L|K$ (Genauer: Wähle die Basis $y_1, ..., y_n \in K$ und multipliziere dann mit dem Hauptnenner). Sei $(x_1^*, ..., x_n^*)$ die duale Basis von $(x_1, ..., x_n)$. Setze $M = o x_1^* + \cdots + o x_n^*$. Zu $\alpha \in O$ gibt es dann $a_1, ..., a_n \in K$ mit $\alpha = a_1 x_1^* + ... + a_n x_n^*$, also $a_i = a_i \mathrm{S}(x_i x_i^*) = \mathrm{S}(\alpha x_i) \in o$, da $\alpha, x_i \in O$, und somit $O \subseteq M$. $\square$

2.4. Lokalisierung

Definition 2.40.

Seien R ein Integritätsbereich, $K = \mathrm{Quot}(R)$ und $S \subseteq R\backslash\{0\}$, $S \neq \emptyset$ multiplikativ abgeschlossen, d.h. $SS \subseteq S$ und $1 \in S$. Dann heißt $S^{-1}R = \{\frac{a}{s} \mid a \in R,\ s \in S\}$ der Fraktionsring von R nach S.

Ist $\mathfrak{p} \subseteq R$ ein Primideal, dann ist $S = R\backslash\mathfrak{p}$ multiplikativ abgeschlossen und $R_\mathfrak{p} = S^{-1}R$ heißt die Lokalisierung von R nach $\mathfrak{p}$.

Beispiel 2.41.

1. Ist $S \subseteq R^\times$, dann $S^{-1}R = R$. Für $S = R\backslash\{0\}$ ist $S^{-1}R = \mathrm{Quot}(R) = K$.
2. $\mathrm{Quot}(R) = R_{(0)}$ und z.B. $\mathbb{Z}_{(3)} = \{\frac{n}{m} \mid n, m \in \mathbb{Z},\ 3 \nmid m\}$. Beachte aber: $\frac{3}{6} \in \mathbb{Z}_{(3)}$. Präziser müssten wir also schreiben $\mathbb{Z}_{(3)} = \{x \in K \mid \text{es gibt } n, m \in \mathbb{Z} \text{ mit } x = \frac{m}{n} \text{ und } 3 \nmid m\}$. $\lozenge$

Lemma 2.42.

Seien R ein Integritätsbereich, $S \subseteq R\backslash\{0\}$, $S \neq \emptyset$ multiplikativ abgeschlossen und $K = \mathrm{Quot}(R)$. Für $R' = S^{-1}R$ gelten dann:

1. Jedes R'-Ideal $\mathfrak{b}$ erfüllt $(\mathfrak{b} \cap R)R' = \mathfrak{b}$.
2. Die Abbildung $\psi : \mathfrak{p}' \mapsto \mathfrak{p}' \cap S$ ist bijektiv und inklusionserhaltend von $\{\mathfrak{p}' \subsetneq R' \text{ Primideal von } R'\}$ auf $\{\mathfrak{p} \text{ Primideal von } R \text{ mit } \mathfrak{p} \cap S = \emptyset\}$.

   Wir identifizieren hierbei R mit seinem Bild unter Einbettung $R \hookrightarrow R'$, definiert durch $a \mapsto \frac{a}{1}$, d.h. wir nehmen an $R \subseteq R'$.

Beweis.

1. $(\mathfrak{b} \cap R)R' \subseteq \mathfrak{b}$ ist klar. Zu $\supseteq$: Habe $x \in \mathfrak{b}$ die Darstellung $x = \frac{a}{s}$ mit $s \in S$ und $a \in R$. Dann gilt $a = xs \in \mathfrak{b} \cap R$, d.h. $x = a\frac{1}{s} \in (\mathfrak{b} \cap R)R'$. Insbesondere ist die Abbildung $\mathfrak{b} \mapsto \mathfrak{b} \cap R$ injektiv und inklusionserhaltend.
2. Sei $\mathfrak{p}'$ ein Primideal in R', dann ist $\mathfrak{p} = \mathfrak{p}' \cap R$ ein Primideal in R. Die Surjektivität wird in Aufgabe 20 gezeigt. Schließlich ist $\mathfrak{p} \cap S = \emptyset$, denn angenommen, $s \in \mathfrak{p} \cap S = \mathfrak{p}' \cap S$, dann $1 = \frac{1}{s}s \in R'\mathfrak{p}' = \mathfrak{p}'$, ein Widerspruch. □

Korollar 2.43.

Sei der Integritätsbereicht R Noethersch, dann ist auch R' Noethersch.

Beweis.

Gelte $\mathfrak{a}'_1 \subseteq \mathfrak{a}'_2 \subseteq \mathfrak{a}'_3 \subseteq ...$ in R', dann bricht die Kette $\mathfrak{a}'_1 \cap R \subseteq \mathfrak{a}'_2 \cap R \subseteq \mathfrak{a}'_3 \cap R \subseteq ...$ in R ab, d.h. es gibt ein $n \in \mathbb{N}$ mit $\mathfrak{a}'_k \cap R = \mathfrak{a}'_n \cap R$ für alle $k \geq n$. Mit Lemma 2.42 folgt dann $\mathfrak{a}'_n = \mathfrak{a}'_k$ für alle $k \geq n$. □

Lemma 2.44.

Seien R ein Integritätsbereich, $K = \mathrm{Quot}(R)$ der Quotientenkörper von R, $L|K$ eine Körpererweiterung und $\overline{R}$ der ganzer Abschluss von R in L. Dann ist $S^{-1}\overline{R}$ der ganze Abschluss von $S^{-1}R$ in L.

Beweis.

Sei zunächst $bs^{-1} \in S^{-1}\overline{R}$ mit $b \in \overline{R}$ und $s \in S$. Dann gilt $b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0$ für gewisse $a_0, ..., a_{n-1}$. Multiplikation mit s^{-n} ergibt: bs^{-1} ist eine Nullstelle von $X^n + (a_{n-1}s^{-1})x^{n-1} + \cdots + (a_0 s^{-n})$, d.h. bs^{-1} ist ganz über $S^{-1}R$.

Sei umgekehrt $x^n + (a_{n-1}s_{n-1}^{-1})x^{n-1} + \cdots + (a_0 s_0^{-1}) = 0$. Durchmultiplizieren mit $(s_{n-1} \cdots s_0)^n$ ergibt $(xs_0 \cdots s_{n-1})^n + a_{n-1}(s_0 \cdots s_{n-1})(xs_0 \cdots s_{n-1})^{n-1} + \cdots = 0$. Also ist $xs_0 \cdots s_{n-1}$ ein Element aus $\overline{R}$, d.h. $x = (xs_0 \cdots s_{n-1})(s_0 \cdots s_{n-1})^{-1} \in S^{-1}\overline{R}$. □

Korollar 2.45.

Ist der Integrationsbereich R ein Dedekind-Ring, so ist auch R' ein Dedekind-Ring.

Beweis.

Nach Korollar 2.43 ist R' Noethersch. Da R ganz algebraisch, liefert Lemma 2.44: $\overline{S^{-1}\overline{R}} = S^{-1}\overline{R} = S^{-1}R$, d.h. auch $S^{-1}R = R'$ ist ganz algebraisch. Sei schließlich $\mathfrak{p}'$ prim in R', dann ist $\mathfrak{p}' \cap R = \mathfrak{p}$ prim in R, wegen der Injektivität der Abbildung ψ in Lemma 2.42 ist damit $\mathfrak{p}'$ maximal in R'. □

Lemma 2.46.

Seien R ein Integritätsbereich und $\mathfrak{p} \subseteq R$ prim. Dann ist $\mathfrak{p}R_\mathfrak{p}$ das einzige maximale Ideal von $R_\mathfrak{p}$, d.h. $R_\mathfrak{p}$ ist ein lokaler Ring. Es gilt $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} \cong \mathrm{Quot}(R/\mathfrak{p})$.

Beweis.

Es gilt $S = R \backslash \mathfrak{p}$ und $\mathfrak{p}$ ist maximal mit $\mathfrak{p} \cap S = \emptyset$. Dann ist $\mathfrak{p}$ eindeutig bestimmt mit dieser Eigenschaft und wegen der Bijektion $\mathfrak{p} \mapsto \mathfrak{p} \cap S$ ist $\mathfrak{p}R_\mathfrak{p}$ das einzige maximale Ideal von $R_\mathfrak{p}$. Betrachte den Homomorphismus $\phi : R_\mathfrak{p} \to \mathrm{Quot}(R/\mathfrak{p})$, definiert durch $\phi(as^{-1}) = (a + \mathfrak{p})(s + \mathfrak{p})^{-1}$. Dieser ist surjektiv, da $\overline{s} = s + \mathfrak{p} \neq 0$, d.h. $s \notin \mathfrak{p}$ und damit $\in S$, und es gilt $\mathrm{Kern}(\phi) = \mathfrak{p}R_\mathfrak{p}$, denn $(as^{-1}) \mapsto 0$ genau dann, wenn $a \in \mathfrak{p}$. □

Lemma 2.47.

Sind R ein Dedekind-Ring und $\mathfrak{p} \subseteq R$ prim, $\mathfrak{p} \neq (0)$, so gilt $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} \cong R/\mathfrak{p}$ und es gibt ein $\pi \in R_\mathfrak{p}$, so dass jedes Ideal in $R_\mathfrak{p}$ von der Form $\pi^m R_\mathfrak{p}$ ist.

Beweis.

Die erste Behauptung folgt wegen $R/\mathfrak{p} = \text{Quot}(R/\mathfrak{p})$ aus Lemma 2.46. Weiter besitzt $R_\mathfrak{p}$ nur ein maximales Ideal, also auch nur ein von $\{0\}$ verschiedenes Primideal, nämlich $\mathfrak{p}R_\mathfrak{p} = \mathfrak{p}'$, denn ist $\mathfrak{q}'$ prim in $R_\mathfrak{p}$, dann ist $\mathfrak{q} = (\mathfrak{q}' \cap R)$ prim in R und wegen $\mathfrak{q} \cap S \neq \emptyset$ folgt $\mathfrak{q} \subseteq \mathfrak{p}$, d.h. $\mathfrak{q} = \mathfrak{p}$ und damit auch $\mathfrak{q}' = \mathfrak{p}'$. Sei nun $\mathfrak{o}'$ ein Ideal im Dedekind-Ring $R_\mathfrak{p}$, dann gilt $\mathfrak{o}' = (\mathfrak{p}')^m$. Sei $\pi \in \mathfrak{p}' \backslash (\mathfrak{p}')^2$, dann $(\pi) \subseteq \mathfrak{p}'$ und $(\pi) \nsubseteq (\mathfrak{p}')^2$. Aus $(\pi) = (\mathfrak{p}')^n$ folgt $n = 1$. □

Bemerkung 2.48.

Seien R ein Dedekind-Ring, $K = \text{Quot}(R)$ und $\{0\} \neq \mathfrak{p} \subseteq R$ prim. Dann definiert die Abbildung $r_\mathfrak{p} : K \to \mathbb{Z} \cup \{\infty\}$ mit $ab^{-1} \mapsto n - m$, $a, b \in R\backslash\{0\}$ und $r_\mathfrak{p}(0) = \infty$, wobei $R_\mathfrak{p}a = (\mathfrak{p}')^n$ und $R_\mathfrak{p}b = (\mathfrak{p}')^m$, eine Bewertung [5] von K, d.h. es gelten $r_\mathfrak{p}(\alpha\beta) = r_\mathfrak{p}(\alpha) + r_\mathfrak{p}(\beta)$ und $r_\mathfrak{p}(\alpha + \beta) \geq \min(r_\mathfrak{p}(\alpha), r_\mathfrak{p}(\beta))$ für alle $\alpha, \beta \in K$.

Setze $|\alpha|_\mathfrak{p} = \exp(-r_\mathfrak{p}(\alpha))$, dann gelten $|0|_\mathfrak{p} = 0$, $|\alpha\beta|_\mathfrak{p} = |\alpha|_\mathfrak{p}|\beta|_\mathfrak{p}$ und $|\alpha + \beta|_\mathfrak{p} \leq \max(|\alpha|_\mathfrak{p}, |\beta|_\mathfrak{p})$. Aus Letzterem folgt die ultrametrische Dreiecksungleichung: $|\alpha + \beta|_\mathfrak{p} \leq |\alpha|_\mathfrak{p} + |\beta|_\mathfrak{p}$. ◊

3. Geometrie der ganzen Zahlen

3.1. Gitter im $\mathbb{R}^n$

Definition 3.1.

Ein Gitter G im $\mathbb{R}^n$ ist ein $\mathbb{Z}$-Modul, der von endlich vielen $\mathbb{R}$-linear unabhängigen Elementen des $\mathbb{R}^n$ erzeugt wird, d.h.$G = \mathbb{Z}\beta_1 \oplus \cdots \oplus \mathbb{Z}\beta_m$ mit $\mathbb{R}$-linear unabhängigen Erzeugern $\beta_1, ..., \beta_m \in \mathbb{R}^n$. G heißt vollständig, falls $r = n$ ist. $M \subseteq \mathbb{R}^n$ heißt diskret, falls $U_r(\alpha) \cap M$ endlich ist für alle $\alpha \in \mathbb{R}^n$ und alle $r > 0$, wobei $U_r(\alpha) = \{\beta \in \mathbb{R}^n \mid \|\beta - \alpha\| < r\}$ die offene Umgebung um α vom Radius r bzgl. der euklidischen Metrik bezeichnet. $\mathcal{T} = \{r_1\beta_1 + \cdots + r_m\beta_m \mid 0 \leq r_i < 1\}$ heißt die Grundmasche des Gitters bzgl. $\beta_1, ..., \beta_m$. Sofern existent, wird mit $\text{v}(\mathcal{T})$ das Volumen (bzgl. eines geeigneten Maßes) von $\mathcal{T}$ bezeichnet.

Bemerkung 3.2.

Ist G vollständig, so lässt sich der $\mathbb{R}^n$ disjunkt zerlegen in die Menge der Maschen $\mathbb{R}^n = \bigcup\{\alpha + \mathcal{T} \mid \alpha \in G\}$ des Gitters, wobei $\alpha + \mathcal{T} = \{\alpha + \tau \mid \tau \in \mathcal{T}\}$. ◊

Beispiel 3.3.

Sei $\mathcal{T}$ die Grundmasche des vollständigen Gitters $\mathbb{Z}\beta_1 \oplus \cdots \oplus \mathbb{Z}\beta_n$, wobei $\beta_1, ..., \beta_n$ eine Basis des $\mathbb{R}^n$ bilden. Dann ist $\mathcal{T} = \text{Bild}\{(r_1, ..., r_n) \mid 0 \leq r_i < 1\}$ unter der $\mathbb{R}$-linearen Koordinatenabbildung $e_i \mapsto \beta_i$. Sei dazu $\beta_i = (b_{1i}, ..., b_{ni})$. Dann ist das Volumen von $\mathcal{T}$ gegeben durch $\text{v}(\mathcal{T}) = |\det(b_{ij})|$. Insbesondere ist das Volumen der Grundmasche von G unabhängig von der Wahl der Basis $\beta_1, ..., \beta_n$. ◊

Lemma 3.4.

Sei G ein Gitter im $\mathbb{R}^n$. Dann ist G vollständig genau dann, wenn es eine beschränkte Menge $M \subseteq \mathbb{R}^n$ gibt mit $\mathbb{R}^n = \bigcup\{\alpha + M \mid \alpha \in G\}$.

Beweis.

Ist G vollständig, dann wähle $M = T$. Nehmen wir dagegen an, G ist unvollständig und habe die Darstellung $G = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_m$ mit $m < n$. Setze $W = \text{span}(G) \subsetneq \mathbb{R}^n$ und wähle $r > 0$ mit $M \subseteq U_r(0)$ sowie ein $\gamma \in W^\perp$ mit $\|\gamma\| \geq r$. Dann folgt $\gamma \in \bigcup\{\alpha + M \mid \alpha \in G\} \subseteq \bigcup\{\alpha + U_r(0) \mid \alpha \in G\}$, also $\gamma \in \alpha + U_r(0)$ für ein $\alpha \in G$. Damit ist $\gamma = \alpha + \beta$ mit $\beta \in U_r(0)$. Dann können wir abschätzen $\|\gamma\|^2 = |\gamma \circ \gamma| \leq \|\gamma\|\|\beta\| < r\|\gamma\|$, d.h. $\|\gamma\| < r$, ein Widerspruch. □

Satz 3.5.

Eine Untergruppe G des $\mathbb{R}^n$ ist genau dann diskret, wenn G ein Gitter ist.

Beweis.

1. Sei zunächst G ein Gitter vom Rang m. Ergänze $\alpha_1, ..., \alpha_m$ mit $\alpha_{m+1}, ..., \alpha_n$ zu einer Basis, dann ist $G \subseteq G_1$ für das vollständige Gitter $G_1 = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \alpha_n$. Sei $\alpha_1^*, ..., \alpha_n^* \in \mathbb{R}^n$ dual zu $\alpha_1, ..., \alpha_n$ bzgl. $\circ$, d.h. $\alpha_i \alpha_j^* = \delta_{ij}$. Beachte dabei, dass $\det(\alpha_i \circ \alpha_j)_{1\le j\le n}^{1\le i\le n} \neq 0$ gilt. Sei nun eine Kugel $U_r(\alpha) \subseteq U_{r_1}(0)$ gegeben und sei $\gamma \in U_{r_1}(0)$. Dann ist $\gamma = a_1\alpha_1 + \cdots + a_n\alpha_n \in G_1$, d.h. alle $a_i \in \mathbb{Z}$. Dann ist die folgende Abschätzung erfüllt: $|a_j| = |\gamma \circ \alpha_j^*| \le \|\gamma\|\|\alpha_j^*\| < r_1\|\alpha_j^*\| \le r_1 \max(\|\alpha_i^*\|)$. Da es nur endlich viele $a_j \in \mathbb{Z}$ mit dieser Eigenschaft gibt und damit auch nur endlich viele $\gamma \in U_{r_1}(0) \cap G_1$, ist das Gitter diskret.

2. Sei nun G eine diskrete Gruppe im $\mathbb{R}^n$ und sei $S = \operatorname{span}(G)$ mit $\dim(S) = m$, d.h. $S = \mathbb{R}\beta_1 \oplus \cdots \oplus \mathbb{R}\beta_m$ mit $\beta_1, ..., \beta_m \in G$. Setze $M = \mathbb{Z}\beta_1 \oplus \cdots \oplus \mathbb{Z}\beta_m$. Dann ist M ein Gitter in $\mathbb{R}^n$ mit $M \subseteq G$. Die Gruppe G/M ist endlich, denn jedes $\alpha \in G$ lässt sich schreiben als $\alpha = t_1\beta_1 + \cdots + t_m\beta_m$ mit $t_1, ..., t_m \in \mathbb{R}$. Dann $\alpha = \mu + \delta$ mit $\mu = a_1\beta_1 + \cdots + a_m\beta_m$ und $\delta = r_1\beta_1 + \cdots + r_m\beta_m$, wobei $a_i \in \mathbb{Z}$ und $0 \le r_i < 1$. Also ist $\alpha \equiv \delta \bmod M$ für ein $\delta \in \{r_1\beta_1 + \cdots + r_m\beta_m \mid 0 \le r_i < 1\} \subseteq U_r(0)$ mit geeignetem $r > 0$, d.h. $\delta = \alpha - \mu$ liegt in der endlichen Menge $G \cap U_r(0)$. Sei $|G/M| = d$. Dann gilt $\alpha d \in M$ für alle $\alpha \in G$. Also $\alpha = (a_1d^{-1})\beta_1 + \cdots + (a_nd^{-1})\beta_m$ mit $a_1, ..., a_m \in \mathbb{Z}$, d.h. G ist ein Untermodul des freien $\mathbb{Z}$-Moduls $\mathbb{Z}\beta_1 d^{-1} \oplus \cdots \oplus \mathbb{Z}\beta_m d^{-1}$. Nach dem Elementarteilersatz 1.26 gibt es eine $\mathbb{Z}$-Basis $\gamma_1, ..., \gamma_{m'}$ für G mit $m' \le m$. Schließlich gilt $\dim(\operatorname{span}(G)) = m' = m$; insbesondere sind $\gamma_1, ..., \gamma_{m'}$ auch $\mathbb{R}$-linear unabhängig. Damit ist G ein Gitter. □

3.2. Darstellung von $\mathcal{O}_K$ als Gitter

Definition 3.6.

Seien $[K : \mathbb{Q}] = n$ und $\rho_1, ..., \rho_n$ die Einbettungen von K in $\mathbb{Z}$. ρ_i heißt reelle Einbettung, falls $K^{(i)} = \rho_i(K) \subseteq \mathbb{R}$. Andernfalls heißt ρ_i komplexe Einbettung.

Bemerkung 3.7.

Falls $\rho_i : K \to \mathbb{Z}$ eine komplexe Einbettung ist, so definiert auch $\overline{\rho}_i : K \to \mathbb{Z}$ mit $\beta \mapsto \overline{\rho_i(\beta)}$ eine komplexe Einbettung, die von ρ_i verschieden ist. Es gibt also $s, t \in \mathbb{N}$ mit $n = s+2t$, so dass $\rho_1, ..., \rho_s$ die reellen und $\rho_{s+1}, ..., \rho_{s+t}, \overline{\rho_{s+1}}, ..., \overline{\rho_{s+t}}$ die komplexen Einbettungen von K in $\mathbb{C}$ sind. Wir schreiben $\alpha^{(i)}$ für $\rho_i(\alpha)$. und betrachten die $\mathbb{Q}$-lineare Abbildung $\rho : K \to \mathbb{R}^s \times \mathbb{C}^t$, definiert durch $\alpha \mapsto (\alpha^{(1)}, ..., \alpha^{(s+t)})$. Bzgl. komponentenweiser Multiplikation in $\mathbb{K}^{s,t} = \mathbb{R}^s \times \mathbb{C}^t$ ist ρ multiplikativ, d.h. es gilt $\rho(\alpha\beta) = \rho(\alpha)\rho(\beta)$. $\mathbb{K}^{s,t}$ ist eine n-dimensionale $\mathbb{R}$-Algebra, die als Vektorraum isomorph ist zu $\mathbb{R}^n$. ◊

Beispiel 3.8.

Sei $K = \mathbb{Q}(\sqrt{d})$ für ein quadratfreies $d \in \mathbb{Z}$. Beachte: $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}[X]/(X^2 - d) = \mathbb{Q} + \overline{X}\mathbb{Q}$. Ist $d > 0$, dann gelten $s = 2$ und $t = 0$. Andernfalls sind $s = 0$ und $t = 1$. Für $\alpha = a + b\sqrt{d}$ mit $a, b \in \mathbb{Q}$ sind $\alpha^{(1)} = a + b\sqrt{d}$ und $\alpha^{(2)} = a - b\sqrt{d}$. ρ ist eindeutig definiert durch seine Werte auf der $\mathbb{Q}$-Basis $1, \sqrt{d}$ von $\mathbb{Q}(\sqrt{d})$: $\rho(1) = (1, 1)$ und $\rho(\sqrt{d}) = (\sqrt{d}, -\sqrt{d})$. ◊

Satz 3.9.

$\alpha_1, ..., \alpha_n \in K$ sind linear abhängig über $\mathbb{Q}$ g.d.w. $\rho(\alpha_1), ..., \rho(\alpha_n)$ linear abhängig über $\mathbb{R}$ sind.

Beweis.

Sind $\alpha_1, ..., \alpha_n$ linear abhängig über $\mathbb{Q}$, d.h. gilt $\sum a_i\alpha_i = 0$ für gewisse $a_i \in \mathbb{Q}$, die nicht alle Null sind, dann auch $0 = \rho(\sum a_i\alpha_i) = \sum a_i\rho(\alpha_i)$, d.h. die $\rho(\alpha_1), ..., \rho(\alpha_n)$ sind linear abhängig über $\mathbb{R}$.

Seien dagegen $\rho(\alpha_1), ..., \rho(\alpha_n)$ $\mathbb{R}$-linear abhängig. Für gewisse $x_j^{(1)}, ..., x_j^{(s)} \in \mathbb{R}$, $u_j^{(s+1)}, ..., u_j^{s+t} \in \mathbb{R}$, $v_j^{(s+1)}, ..., v_j^{(s+t)} \in \mathbb{R}$ ist dann

$$\rho(\alpha_j) = (\alpha_j^{(1)}, ..., \alpha_j^{(s+t)}) = (x_j^{(1)}, ..., x_j^{(s)}, u_j^{(s+1)} + iv_j^{(s+t)}, ..., u_j^{(s+t)} + iv_j^{(s+t)})$$

in $\mathbb{R}^s \times \mathbb{C}^t = \mathbb{K}^{s,t}$.

Es gilt

$$
\begin{aligned}
0 &= \det \begin{pmatrix} x_1^{(1)} & x_1^{(2)} & \dots & x_1^{(s)} & u_1^{(s+1)} & v_1^{(s+1)} & \dots & u_1^{(s+t)} & v_1^{(s+t)} \\ \vdots & & & & & & & & \vdots \\ x_n^{(1)} & & \dots & & \dots & & \dots & & v_n^{(s+t)} \end{pmatrix}^2 2^{2t}(-i)^{2t} \\
&= \det \begin{pmatrix} x_1^{(1)} & \dots & x_1^{(s)} & (u_1^{(s+1)} + iv_1^{(s+1)}) & (u_1^{(s+1)} - iv_1^{(s+1)}) & \dots & (u_1^{(s+t)} - iv_1^{(s+t)}) \\ \vdots & & & & & & \vdots \\ x_n^{(1)} & \dots & & \dots & & \dots & (u_n^{(s+t)} - iv_n^{(s+t)}) \end{pmatrix}^2 \\
&= \det \begin{pmatrix} \alpha_1^{(1)} & \alpha_1^{(2)} & \dots & \alpha_1^{(s)} & \alpha_1^{(s+1)} & \overline{\alpha}_1^{(s+1)} & \dots & \alpha_1^{(s+t)} & \overline{\alpha}_1^{(s+t)} \\ \vdots & & & & & & & & \vdots \\ \alpha_n^{(1)} & & \dots & & \dots & & \dots & & \overline{\alpha}_n^{(s+t)} \end{pmatrix}^2 \\
&= \det \begin{pmatrix} \alpha_1^{(1)} & \dots & \alpha_1^{(n)} \\ \vdots & \ddots & \vdots \\ \alpha_n^{(1)} & \dots & \alpha_n^{(n)} \end{pmatrix}^2 = \det \left(\begin{pmatrix} \alpha_1^{(1)} & \dots & \alpha_1^{(n)} \\ \vdots & \ddots & \vdots \\ \alpha_n^{(1)} & \dots & \alpha_n^{(n)} \end{pmatrix} \begin{pmatrix} \alpha_1^{(1)} & \dots & \alpha_1^{(n)} \\ \vdots & \ddots & \vdots \\ \alpha_n^{(1)} & \dots & \alpha_n^{(n)} \end{pmatrix}^{\mathrm{T}} \right) \\
&= \det \left(\sum_{l=1}^{n} \alpha_i^{(l)} \alpha_j^{(l)} \right)_{1 \le i \le n}^{1 \le j \le n} = \det(\mathrm{S}(\alpha_i \alpha_j))_{1 \le j \le n}^{1 \le i \le n} = \mathrm{D}(\alpha_1, \dots, \alpha_n).
\end{aligned}
$$

Aus $\mathrm{D}(\alpha_1, \dots, \alpha_n) = 0$ folgt dann mit Satz 2.37, dass $\alpha_1, \dots, \alpha_n$ linear abhängig sind. □

Bemerkung 3.10.

1. Insbesondere haben wir eine Formel zur Berechnung der Diskriminante über die Koeffizienten der $\rho(\alpha_j)$ gefunden. Sei $\mathcal{T}_K$ die Grundmasche von $\rho(\mathcal{O}_K)$, dann ist speziell $\mathrm{v}(\mathcal{T}_K) = 2^{-t}\sqrt{|\mathrm{D}(\alpha_1, \dots, \alpha_n)|}$.
2. $\mathcal{O}_K$ ist ein freier $\mathbb{Z}$-Modul vom Rang n: Mit $o = \mathbb{Z}$ und $K = \mathrm{Quot}(\mathcal{O}_K)$ (Bemerkung 2.24) liefert Proposition 2.39, dass $\mathcal{O}_K$ in einem freien $\mathbb{Z}$-Modul von Rang n liegt und nach dem Elementarteilersatz 1.26 daher selbst ein freier $\mathbb{Z}$-Modul vom Rang $m \le n$ ist; da $\mathcal{O}_K$ eine Basis von $K|\mathbb{Q}$ enthält, ist zugleich $m \ge n$. Daraus folgt: $\rho(\mathcal{O}_K)$ ist ein vollständiges Gitter im $\mathbb{R}^n$, denn sei $\mathcal{O}_K = \mathbb{Z}\alpha_1 \oplus \dots \oplus \mathbb{Z}\alpha_n$ als $\mathbb{Z}$-Modul. Dann ist $\rho(\mathcal{O}_K) = \mathbb{Z}\rho(\alpha_1) \oplus \dots \oplus \rho(\alpha_n)$ mit $\rho(\alpha_1), \dots, \rho(\alpha_n)$ linear unabhängig über $\mathbb{R}$.
3. Sei A ein gebrochenes Ideal von K. Dann folgt für jedes $\gamma \in A\backslash\{0\}$, dass $\gamma\alpha_1, \dots, \gamma\alpha_n$ linear unabhängig über $\mathbb{Q}$ ist. Also ist A ein freier $\mathbb{Z}$-Modul vom Rang n und damit $A = \mathbb{Z}\beta_1 \oplus \dots \oplus \mathbb{Z}\beta_n$. Wir setzen $\mathrm{D}(A) = \mathrm{D}(\beta_1, \dots, \beta_n)$, speziell $\mathrm{D}(\mathcal{O}_K) = \mathrm{D}(\alpha_1, \dots, \alpha_n)$. Also ist $\rho(A)$ ein vollständiges Gitter im $\mathbb{R}^n$ und es gilt $\mathrm{v}(\rho(A)) = 2^{-t}\sqrt{|\mathrm{D}(A)|}$. ◊

Beispiel 3.11.

Sei $K = \mathrm{Quot}(\sqrt{d})$ mit d quadratfrei. Dann lässt sich $\mathcal{O}_K$ als $\mathbb{Z}$-Modul darstellen über $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\omega$ mit $\omega = \sqrt{d}$ für $d \equiv 2, 3 \bmod 4$ und $\omega = \frac{1+\sqrt{d}}{2}$ für $d \equiv 1 \bmod 4$, vgl. Satz 2.8. Mit $\mathrm{D}(1, \omega) = (\omega^{(1)} - \omega^{(2)})^2$ gelten

$$
\omega^{(1)} = \begin{cases} \sqrt{d} & d \equiv 2, 3 \bmod 4 \\ \frac{1+\sqrt{d}}{2} & d \equiv 1 \bmod 4 \end{cases}, \quad \omega^{(2)} = \begin{cases} \sqrt{d} & d \equiv 2, 3 \bmod 4 \\ \frac{1-\sqrt{d}}{2} & d \equiv 1 \bmod 4 \end{cases}, \quad \mathrm{D}(1, \omega) = \begin{cases} 4d & d \equiv 2, 3 \bmod 4 \\ d & d \equiv 1 \bmod 4 \end{cases}.
$$

Speziell für $d = 2$ ist $\mathrm{v} = \sqrt{\mathrm{D}} = \sqrt{8} = 2\sqrt{2}$ und für $d = -2$ ist $\mathrm{v} = \frac{1}{2}\sqrt{-\mathrm{D}} = \sqrt{2}$. ◊

3.3. Der Minkowskische Gitterpunktsatz

Definition 3.12.

$M \subseteq \mathbb{R}^n$ heißt zentralsymmetrisch, falls $-M = M$, und konvex, falls mit $\alpha, \beta \in M$ auch $t\alpha + (1-t)\beta \in M$ für alle $0 \le t \le 1$.

Lemma 3.13. (Blickfeld)

Sei $A \subseteq \mathbb{R}^n$ messbar und beschränkt mit $\mathrm{v}(A) > \mathrm{v}(\mathcal{T})$, wobei $\mathcal{T}$ die Grundmasche eines vollständigen Gitters G im $\mathbb{R}^n$ sei. Dann gibt es $\alpha, \beta \in A$ mit $\alpha \neq \beta$ und $\alpha - \beta \in G$.

Beweis.

Wegen $\mathbb{R}^n = \bigcup\{\{\alpha+\mathcal{T} \mid \alpha \in G\}$ ist $A = \bigcup\{\alpha+\mathcal{T} \mid \alpha \in G\} \cap A$, also gilt für das Volumen der Grundmasche $\mathcal{T}$ die Abschätzung $\mathrm{v}(\mathcal{T}) < \mathrm{v}(A) = \sum\{\mathrm{v}(A \cap (\alpha + \mathcal{T})) \mid \alpha \in G\} = \sum\{\mathrm{v}((A-\alpha) \cap \mathcal{T}) \mid \alpha \in G\}$. Wegen $(A-\alpha) \cap \mathcal{T} \subseteq \mathcal{T}$ sind die $(A-\alpha) \cap \mathcal{T}$ mit $\alpha \in G$ in $\mathcal{T}$ nicht alle disjunkt. Also gibt es $\alpha_1 \neq \alpha_2$ in G mit $((A-\alpha_1) \cap \mathcal{T}) \cap ((A-\alpha_2) \cap \mathcal{T}) \neq \emptyset$. Damit ist auch $(A-\alpha_1) \cap (A-\alpha_2) \neq \emptyset$, d.h. es gibt $\alpha, \beta \in A$ mit $\alpha - \alpha_1 = \beta - \alpha_2$ bzw. $\alpha - \beta = \alpha_1 - \alpha_2 \in G\backslash\{0\}$. □

Satz 3.14. (Minkowskischer Gitterpunktsatz, 1889)

Sei G ein vollständiges Gitter im $\mathbb{R}^n$ mit Grundmascheninhalt $\mathrm{v}(\mathcal{T}) = \Delta$. Ist dann $M \subseteq \mathbb{R}^n$ zentralsymmetrisch, messbar, beschränkt und konvex mit $\mathrm{v}(M) > 2^n\Delta$, so ist $M \cap (G\backslash\{0\}) \neq \emptyset$.

Beweis.

Wir führen die Situation auf das Lemma von Blickfeld 3.13 zurück. Die Menge $A = \frac{1}{2}M = \{\frac{1}{2}\gamma \mid \gamma \in M\}$ ist messbar und beschränkt. Weiter ist $\mathrm{v}(A) = \frac{1}{2^n}\mathrm{v}(M) > \Delta$. Also gibt es zwei verschiedene Elemente $\gamma_1, \gamma_2 \in M$ mit $\frac{1}{2}\gamma_1 - \frac{1}{2}\gamma_2 \in G\backslash\{0\}$. Da M zentralsymmetrisch, liegt auch $-\gamma_2$ in M. Beide Summanden von $\frac{1}{2}\gamma_1 - \frac{1}{2}\gamma_2 = \frac{1}{2}\gamma_1 + \frac{1}{2}(-\gamma_2)$ liegen in A, also auch in M, und wegen der Konvexität von M liegt dann auch die Summe in M, also ist $\frac{1}{2}\gamma_1 - \frac{1}{2}\gamma_2 \in M \cap G\backslash\{0\}$. □

Beispiel 3.15.

Wir betrachten das Gitter $G = \mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z} \subseteq \mathbb{R}^2$ und die zentralsymmetrische, messbare, beschränkte, konvexe Menge $M = \{\alpha \in \mathbb{R}^2 \mid \|\alpha\|_\infty < 1\}$, wobei die Maximumsnorm $\|\cdot\|_\infty$ auf $\mathbb{R}^2$ gegeben ist durch $\|\alpha\|_\infty = |\alpha_1| + |\alpha_2|$. Dann ist $M \cap \mathbb{Z}^2 = \{0\}$, d.h. $M \cap (G\backslash\{0\}) = \emptyset$. Dies widerspricht nicht dem Minkowskischer Gitterpunktsatz 3.14, da $\mathrm{v}(M) = 2^2 = 2^2\Delta$. ◊

Korollar 3.16.

Sei G ein vollständiges Gitter im $\mathbb{K}^{s,t} \cong \mathbb{R}^n$ mit Grundmascheninhalt Δ und gelte für $c_1, ..., c_{s+t} > 0$, dass $\Delta(\frac{4}{\pi})^t < c_1 \cdots c_{s+t}$. Dann gibt es im Gitter G einen Vektor $(a_1, ..., a_{s+t}) \neq 0$ mit $|a_i| < c_i$ für $1 \leq i \leq s$ und $|a_j|^2 < c_j$ für $s+1 \leq j \leq s+t$.

Beweis.

Die Menge $M = \{(a_1, ..., a_n) \in \mathbb{K}^{s,t} \mid |a_1| < c_1, ..., |a_{s+t}|^2 < c_{s+t}\}$ ist zentralsymmetrisch und konvex. Weiter gilt

$$\mathrm{v}(M) = \int_{-c_1}^{c_1} \mathrm{d}x_1 \quad \cdots \quad \int_{-c_s}^{c_s} \mathrm{d}x_s \iint\limits_{u_{s+1}^2+v_{s+1}^2<c_{s+1}} \mathrm{d}(u_{s+1}, v_{s+1}) \quad \cdots \iint\limits_{u_{s+t}^2+v_{s+t}^2<c_{s+t}} \mathrm{d}(u_{s+t}, v_{s+t})$$

$$= (2c_1)\cdots(2c_s)(\pi c_{s+1})\cdots(\pi c_{s+t}) = 2^s\pi^t \prod_{i=1}^{s+t} c_i > 2^s\pi^t\left(\frac{4}{\pi}\right)^t \Delta = 2^{s+2t}\Delta = 2^n\Delta.$$

Nach dem Minkowskischer Gitterpunktsatz 3.14 gibt es dann ein $(a_1, ..., a_{s+t}) \in M \cap (G\backslash\{0\})$. □

Korollar 3.17.

Sei A ein gebrochenes $\mathcal{O}_K$-Ideal. Dann existiert ein $\alpha \in A$, welches der folgenden Abschätzung genügt:

$$0 < |\mathrm{N}_{K|\mathbb{Q}}(\alpha)| \leq \left(\frac{2}{\pi}\right)^t \sqrt{|\mathrm{D}(A)|}.$$

Beweis.

$\rho(A)$ ist ein vollständiges Gitter in $\mathbb{K}^{s,t}$, vgl. Bemerkung 3.10, mit $\Delta = \mathrm{v}(\mathcal{T}) = 2^{-t}\sqrt{|\mathrm{D}(A)|}$. Für beliebiges $c \in \mathbb{R}_+^{s+t}$ mit $c_1 \cdots c_{s+t} > (\frac{4}{\pi})^t \Delta = (\frac{2}{\pi})^t \sqrt{|\mathrm{D}(A)|}$. Dann existiert gemäß Korollar 3.16 ein $\alpha \in A \backslash \{0\}$ derart, dass $|\alpha^{(i)}| < c_i$ für alle $1 \leq i \leq s$ gilt sowie $|\alpha^{(s+i)}|^2 < c_{s+i}$ für alle $1 \leq i \leq t$ erfüllt ist, d.h. wir haben $|\mathrm{N}(\alpha)| = \alpha^{(1)} \cdots \alpha^{(s+t)} < c_1 \cdots c_{s+t}$. Da $\rho(A)$ diskret ist, existiert weiter ein $\alpha \neq 0$ aus A, sodass gilt $|\mathrm{N}(\alpha)| \leq \prod c_i$ für unendlich viele solche Produkte, o.B.d.A. mit Infimum $(\frac{2}{\pi})^t \sqrt{|\mathrm{D}(A)|}$. Sei dazu $(c^{(j)})_{j\in\mathbb{N}}$ eine komponentenweise streng monoton fallende Folge, d.h. es gelte $(\prod c_i^{(j)})_{j\in\mathbb{N}} \to (\frac{2}{\pi})^t \sqrt{|\mathrm{D}(A)|}$, dann folgt $\mathrm{N}(\alpha) \leq (\frac{2}{\pi})^t \sqrt{|D(A)|}$. □

3.4. Endlichkeit der Klassenzahl

Definition 3.18.

Seien $\mathcal{O}_K = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$ und $A = \mathbb{Z}\beta_1 \oplus \cdots \oplus \mathbb{Z}\beta_n$ ein gebrochenes Ideal in $\mathcal{O}_K$. Dann setzen wir $\mathcal{N}(A) = |\det(a_{ij})|$, wobei (a_{ij}) die zu β gehörige Koeffizientenmatrix bezeichnet: $\beta_i = \sum a_{ij}\alpha_j$.

Bemerkung 3.19.

Die Definition von $\mathcal{N}(A)$ ist unabhängig von der Wahl der Basis α, da der Wert der Determinante invariant unter Basistransformationen ist. ◊

Lemma 3.20.

Sei $A = \mathbb{Z}\beta_1 \oplus \cdots \oplus \mathbb{Z}\beta_n$ ein gebrochenes Ideal in $\mathcal{O}_K$. Dann gelten:

1. Ist A ganz, dann ist $\mathcal{N}(A) = |\mathcal{O}/A|$.
2. $\mathcal{N}(\alpha A) = |\mathrm{N}_{K|\mathbb{Q}}(\alpha)|\mathcal{N}(A)$.
3. $\mathcal{N}$ ist multiplikativ: $\mathcal{N}(AB) = \mathcal{N}(A)\mathcal{N}(B)$.
4. $\mathrm{D}(A) = \mathrm{D}(\mathcal{O})(\mathcal{N}(A))^2$.

Beweis.

1. Es gibt nach dem Elementarteilersatz 1.26 eine Basis $\alpha_1, ..., \alpha_n$ von $\mathcal{O}$ mit $A = \mathbb{Z}d_1\alpha_1 + \cdots + \mathbb{Z}d_n\alpha_n$ für gewisse $d_1, ..., d_n \in \mathbb{Z}$. Dann ist $(a_{ij}) = \mathrm{diag}(d_1, ..., d_n)$ bzw. $a_{ij} = d_i\delta_{ij}$, d.h. $\mathcal{N}(A) = |d_1| \cdots |d_n|$. Weiter gilt für $\alpha \in \mathcal{O}$: $\alpha \equiv \nu_1\alpha_1 + \cdots + \nu_n\alpha_n \bmod A$ mit $0 \leq \nu_i < |d_i|$, d.h. es gibt $|d_1| \cdots |d_n|$ viele Elemente in $\mathcal{O}/A$.

2. Mit $\mathcal{O} = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$ und $A = \mathbb{Z}\beta_1 \oplus \cdots \oplus \mathbb{Z}\beta_n$ ist $\alpha\beta_1, ...\alpha\beta_n$ eine Basis von αA und für alle i gilt $\beta_i = \sum a_{ij}\alpha_j$, also $\alpha\beta_i = \alpha \sum a_{ij}\alpha_j$. Die Übergangsmatrix von $\alpha_1, ..., \alpha_n$ zu $\alpha\beta_1, ..., \alpha\beta_n$ ist $m_\alpha(a_{ij})$, wobei m_α die bzgl. $\alpha_1, ..., \alpha_n$ ist. Also gilt $\mathcal{N}(\alpha A) = |\det m_\alpha|\,|\det(a_{ij})| = |\mathrm{N}_{K|\mathbb{Q}}(\alpha)|\mathcal{N}(A)$.

3. Seien zuerst A, B ganz. Zu zeigen ist: $|\mathcal{O}/AB| = |\mathcal{O}/A|\,|\mathcal{O}/B|$. Wir zeigen nur: $|\mathcal{O}/A\mathfrak{p}| = |\mathcal{O}/A|\,|\mathcal{O}/\mathfrak{p}|$ mit $\mathfrak{p}$ prim, dann können wir mit Induktion auf den allgemeinen Fall schließen. Für additive Gruppen gilt mit dem Zweiten Isomorphiesatz [7], Kapitel 1.1: $\mathcal{O}/A = (\mathcal{O}/A\mathfrak{p})/(A/A\mathfrak{p})$. Es genügt also zu zeigen: $A/A\mathfrak{p} = \mathcal{O}/\mathfrak{p}$. $A/A\mathfrak{p}$ ist ein endlich dimensionaler $\mathcal{O}/\mathfrak{p}$-Vekrorraum, wenn wir als skalare Multiplikation wählen $(\alpha + \mathfrak{p})(a + A\mathfrak{p}) = \alpha a + A\mathfrak{p}$ für $\alpha \in \mathcal{O}$ und $a \in A$. Diese Operation ist wohldefiniert: Falls $\alpha - \alpha' \in \mathfrak{p}$ und $a - a' \in A\mathfrak{p}$, so gilt $\alpha a - \alpha' a' = (\alpha - \alpha')a + \alpha'(a - a') \in A\mathfrak{p}$. Wir zeigen nun, dass $A/A\mathfrak{p}$ über $\mathcal{O}/\mathfrak{p}$ die Dimension 1 hat. Sei hierfür W ein Untervektorraum von $A/A\mathfrak{p}$, dann setze $C = \bigcup\{\alpha + A\mathfrak{p} \mid \overline{\alpha} \in W\}$. C ist ein Ideal, denn für $\overline{\alpha}_1, \overline{\alpha}_2 \in W$ ist $\overline{\alpha}_1 + \overline{\alpha}_2 = \overline{\alpha_1 + \alpha_2} \in W$ und mit $\overline{\alpha} \in W$, $\overline{\beta} \in \mathcal{O}/\mathfrak{p}$ ist $\overline{\beta\alpha} \in W$. Aus $A\mathfrak{p} \subseteq C \subseteq A$ folgt dann $C = A\mathfrak{p}$ oder $C = A$, d.h. $W = \{0\}$ oder $W = A/A\mathfrak{p} \Rightarrow \dim W \leq 1$, es gilt also $|A/A\mathfrak{p}| = |\mathcal{O}/\mathfrak{p}|$. Seien A, B gebrochene Ideale mit $dA, d'B \subseteq \mathcal{O}$ für $d, d' \in \mathcal{O}$. Mit (2) folgt $\mathrm{N}(dd')\mathcal{N}(AB) = \mathcal{N}(dAd'B) = \mathcal{N}(dA)\mathcal{N}(d'B) = \mathrm{N}(d)\mathcal{N}(A)\mathrm{N}(d')\mathcal{N}(B)$, d.h. $\mathcal{N}(AB) = \mathcal{N}(A)\mathcal{N}(B)$.

4. Mit $(\mathrm{S}(\beta_i\beta_j)) = (a_{ij})(\mathrm{S}(\alpha_i\alpha_j))(a_{ij})^{\mathrm{T}}$ folgt $\mathrm{D}(A) = \det(a_{ij})^2\mathrm{D}(\mathcal{O})$. □

Bemerkung 3.21.

Als Folgerung erhalten wir, dass $\mathcal{N}$ normiert und verträglich bzgl. der Invertierung ist, d.h. es gelten $\mathcal{N}(\mathcal{O}) = 1$ und $\mathcal{N}(A^{-1}) = \mathcal{N}(A)^{-1}$. ◊

Satz 3.22.

Zu jeder Idealklasse $A\mathcal{I}_0 \in \mathcal{I}/\mathcal{I}_0$ gibt es ein ganzes Ideal C mit $\mathcal{N}(C) \leq (\frac{2}{\pi})^t \sqrt{|\mathrm{D}(\mathcal{O})|}$.

Beweis.

Setze $B = A^{-1}$. Nach Korollar 3.17 gibt es $0 \neq \beta \in B$ mit $|\mathrm{N}(\beta)| \leq (\frac{2}{\pi})^t \sqrt{|\mathrm{D}(B)|} = (\frac{2}{\pi})^t \mathcal{N}(B)\sqrt{|\mathrm{D}(\mathcal{O})|}$, d.h. $\mathcal{N}(\beta B^{-1}) = |\mathrm{N}(\beta)|\mathcal{N}(B)^{-1} \leq (\frac{2}{\pi})^t \sqrt{|\mathrm{D}(\mathcal{O})|}$. Wegen $\beta \in B$ ist $(\beta) \subseteq B$, d.h. $\beta A = \beta B^{-1} \subseteq \mathcal{O}$, also erfüllt das ganze Ideal $C = \beta A$ die geforderte Normabschätzung. □

Bemerkung 3.23.

Die Schranke $(\frac{2}{\pi})^t$ kann verbessert werden zu $(\frac{4}{\pi})^t \frac{n!}{n^n} = (\frac{2}{\pi})^t \frac{2^t n!}{n^n}$, siehe [13], Satz 2.23. ◊

Satz 3.24. (Endlichkeit der Klassenzahl)

Die Klassenzahl $\mathrm{h} = |\mathcal{I}/\mathcal{I}_0|$ eines algebraischen Zahlkörpers K ist endlich.

Beweis.

Setze $c = (\frac{2}{\pi})^t \sqrt{|\mathrm{D}(\mathcal{O})|}$. Es gibt nur endlich viele Normen $\mathcal{N}(A) \leq c$ für ganze Ideale A, da $\mathcal{N}(A) \in \mathbb{N}$. Sei $m = \mathcal{N}(A)$, d.h. $m = |\mathcal{O}/A|$ nach Lemma 3.20; mit dem Kleinen Satz von Fermat [6], Kapitel 2.3, folgt dann $m\mathcal{O} \subseteq A$. Damit gilt $A \mid m\mathcal{O} = \mathfrak{p}_1^{\nu_1} \cdots \mathfrak{p}_s^{\nu_s}$, d.h. es gibt nur endlich viele Teiler A von $m\mathcal{O}$. Also ist die Klassenzahl endlich. □

Korollar 3.25.

Es gibt nur endlich viele nicht assoziierte Elemente $\alpha \in \mathcal{O}_K$ mit $|\mathrm{N}(\alpha)| \leq c$.

Beweis.

Es gilt $\mathrm{N}(\alpha) = \mathcal{N}(\alpha\mathcal{O})$, da $\mathcal{N}(\mathcal{O}) = 1$. Also existieren nur endlich viele Hauptideale $a\mathcal{O}$ mit $|\mathcal{N}(a\mathcal{O})| < c$; wegen $\alpha_1 \sim \alpha_2 \Leftrightarrow \alpha_1\mathcal{O} = \alpha_2\mathcal{O}$ folgt die Behauptung. □

3.5. Der Dirichletsche Einheitensatz

Lemma 3.26.

Seien $K|k$ endlich, o ein Dedekind-Ring in k und $\mathcal{O}$ der ganze Abschluss von o in K. Dann gilt:

$$\alpha \in \mathcal{O} \text{ ist eine Einheit in } \mathcal{O} \quad \Longleftrightarrow \quad \mathrm{N}_{K|k}(\alpha) \in o \text{ ist eine Einheit in } o.$$

Beweis.

Sei zunächst $\alpha \in \mathcal{O}^\times$, d.h. es gibt $\beta \in \mathcal{O}^\times$ mit $\alpha\beta = 1$. Dann ist $\mathrm{N}(\alpha)\mathrm{N}(\beta) = 1$, d.h. $N(\alpha) \in o^\times$. Sei dagegen $\mathrm{N}(\alpha) = \alpha^{(1)} \cdots \alpha^{(n)} \in o^\times$. Wegen $\alpha = \alpha^{(1)}$ ist dann $\alpha(\alpha^{(2)} \cdots \alpha^{(n)}\mathrm{N}(\alpha)^{-1}) = 1$. Da $\alpha^{(2)} \cdots \alpha^{(n)}\mathrm{N}(\alpha)^{-1}$ ganz über o in K, d.h. eine Einheit in $\mathcal{O}$ ist, folgt $\alpha \in \mathcal{O}^\times$. □

Satz 3.27. (Dirichletscher Einheitensatz, 1837)

Sei $\mathcal{O}_K$ der Ring der ganzen Zahlen des algebraischen Zahlkörpers K mit $[K : \mathbb{Q}] = n = s + 2t$, wobei s die Anzahl der reellen Einbettungen in $\mathbb{Z}$ bezeichnet.

Dann gibt es in $\mathcal{O}_K$ Einheiten $\epsilon_1, ..., \epsilon_r$ mit $r = s + t - 1$, so dass sich jede Einheit $\epsilon \in \mathcal{O}_K^\times$ eindeutig in der Form $\epsilon = \zeta \epsilon_1^{m_1} \cdots \epsilon_r^{m_r}$ darstellen lässt, wobei $m_i \in \mathbb{Z}$ und ζ eine Einheitswurzel ist.

Die ϵ_i heißen Fundamentaleinheiten und $\{\epsilon_i \mid 1 \leq i \leq r\}$ ein Einheiten-Fundamentalsystem von K.

Beweis.

Betrachte die Einbettung $\rho : K \hookrightarrow \mathbb{K}^{s,t}$ mit $\rho(\alpha) = (\alpha^{(1)}, ..., \alpha^{(s+t)})$ und die logarithmische Darstellung $\ell : \rho(K^\times) \subseteq \mathbb{K}^{s,t} \to \mathbb{R}^{s+t}$, gegeben durch $\ell(x_1, ..., x_{s+t}) = (\ln|x_1|, ..., \ln|x_{s+t}|^2)$. Via Identifikation mit den Bildern unter der Einbettung schreiben wir $\ell(\alpha)$ statt $(\ell \circ \rho)(\alpha)$, dann ist $\ell(\alpha\beta) = \ell(\alpha) + \ell(\beta)$ für $\alpha, \beta \in K^\times$, d.h. ℓ vermittelt einen Gruppenhomomorphismus von $(K^\times, \cdot)$ nach $(\mathbb{R}^{s+t}, +)$. Für $\alpha \in \mathcal{O} \backslash \{0\}$ gilt laut Lemma 3.26: $\alpha \in \mathcal{O}^\times \Leftrightarrow |\mathrm{N}(\alpha)| = 1 \Leftrightarrow |\alpha^{(1)} \cdots \alpha^{(s)} \alpha^{(s+1)} \overline{\alpha^{(s+1)}} \cdots \alpha^{(s+t)} \overline{\alpha^{(s+t)}}| = 1 \Leftrightarrow$ alle $|\alpha^{(i)}| = 1$ sowie $\ell(\alpha) \bullet (1, ..., 1) = 0 \Leftrightarrow \ln|\alpha^{(1)}| + \cdots + \ln|\alpha^{(s+t)}|^2 = 0$, d.h. $\ell(\mathcal{O}^\times) = \ell(\mathcal{O} \backslash \{0\}) \cap (1, ..., 1)^\perp$. Dabei ist $W = (1, ..., 1)^\perp$ eine Hyperebene im $\mathbb{R}^{s+t}$ der $\mathbb{R}$-Dimension $s + t - 1 = r$.

1. *$\ell(\mathcal{O}^\times)$ ist ein Gitter im $\mathbb{R}^{s+t}$:* Wir zeigen dazu, dass $\ell(\mathcal{O}^\times)$ diskret ist. Seien $r > 0$ und $\epsilon \in \mathcal{O}^\times$ mit $\|\ell(\epsilon)\| < r$, dann ist $|\ln|\epsilon^{(i)}|^{1,2}| < r$ für alle $1 \leq i \leq s + t$, d.h. $\rho(\epsilon) = (\epsilon^{(1)}, ..., \epsilon^{(s+t)})$ liegt in einer beschränkten Teilmenge von $\mathbb{K}^{s,t}$. Da $G = \rho(\mathcal{O})$ ein Gitter im $\mathbb{K}^{s,t}$ ist, gibt es nur endlich viele solche $\epsilon \in \mathcal{O}^\times$, d.h. $\ell(\mathcal{O}^\times) \cap U_r(0)$ ist endlich.

2. *$\ell(\mathcal{O}^\times)$ ist ein vollständiges Gitter in W:* Wir zeigen, dass es eine beschränkte Menge S in W gibt, so dass $W = \bigcup\{l(\epsilon) + S \mid \epsilon \in \mathcal{O}^\times\}$ gilt. Wir weisen dazu die Existenz einer beschränkte Menge $S_0 \subseteq \mathbb{K}^{s,t}$ nach mit $\ell^{-1}(W) \subseteq \bigcup\{\rho(\epsilon) S_0 \mid \epsilon \in \mathcal{O}^\times\}$, denn dann gilt $W = \bigcup\{\ell(\epsilon) + S \mid \epsilon \in \mathcal{O}^\times\}$ mit $S = \ell(S_0) \cap W$ und S ist beschränkt: Gelte $\|(x_1, ..., x_{s+t})\| < r$, dann sind alle $|x_i| < r$, also auch $\ln|x_i| < \ln(r)$, ohne Einschränkung $\ln|x_i|^{1,2} < \ln(r)$, und mit $\ell(x_1, ..., x_{s+t}) \in W$ erhalten wir $\ln|x_i|^{1,2} = \sum\{-\ln|x_j|^{1,2} \mid i \neq j\} > -(s + t - 1)\ln(r)$.

   Bleibt also die Existenz von S_0 zu zeigen. Bezeichne Δ den Grundmascheninhalt von G. Gilt für den Zylinder $M = \{(x_1, ..., x_{s+t}) \mid |x_1| < c_1, ..., |x_{s+t}|^2 < c_{s+t}\} \subseteq \mathbb{K}^{s,t}$, dass $c = c_1 \cdots c_{s+t} > (\frac{4}{\pi})^t \Delta$, dann ist laut Korollar 3.16 $\rho(\mathcal{O}) \backslash \{0\} \cap M \neq \emptyset$. Es gilt im Übrigen bereits $\rho(\mathcal{O}) \backslash \{0\} \cap M' \neq \emptyset$ mit $M' = \{(x_1, ..., x_{s+t}) \in M \mid \prod x_i \neq 0\}$, denn aus $\alpha \neq 0$ folgt stets auch $\prod \alpha^{(i)} \neq 0$. Sei $\eta = (y_1, ..., y_{s+t}) \in \ell^{-1}(W) \subseteq \mathbb{K}^{s,t}$, d.h. $|y_1| \cdots |y_{s+t}|^2 = 1$. Wir betrachten die komponentenweise Multiplikation $\eta : \mathbb{K}^{s,t} \to \mathbb{K}^{s,t}$ mit $(x_1, ..., x_{s+t}) \mapsto (x_1 y_1, ..., x_{s+t} y_{s+t})$. η ist $\mathbb{R}$-linear und injektiv, also bijektiv. Damit ist auch $\eta(G)$ ein vollständiges Gitter im $\mathbb{K}^{s,t}$. Die Übergangsmatrix ist gegeben durch $M = \mathrm{diag}(y_1, ..., y_s, \square_1, ..., \square_t)$ mit $\square_j = \left(\begin{smallmatrix} u_{s+j} & -v_{s+j} \\ v_{s+j} & u_{s+j} \end{smallmatrix}\right)$, wobei $y_{s+j} = u_{s+j} + i v_{s+j}$, $1 \leq j \leq t$.

   Wegen $\det(M) = y_1 \cdots y_s (u_{s+1}^2 + v_{s+1}^2) \cdots (u_{s+t}^2 + v_{s+t}^2) = y_1 \cdots y_s |y_{s+1}|^2 \cdots |y_{s+t}|^2 = \pm 1$ gilt für das Grundmaschenvolumen von $\eta(G)$, dass $\mathrm{v}(\mathcal{T}_{\eta(G)}) = \mathrm{v}(\mathcal{T}_G) = \Delta$. Mit Hilfe von Korollar 3.16 finden wir ein $\alpha \in \mathcal{O} \backslash \{0\}$ mit $\eta(\rho(\alpha)) \in M'$. Dann ist $|y_1 \alpha^{(1)}| \cdots |y_{s+t} \alpha^{(s+t)}|^2 < \prod c_i = c$, d.h. es gilt auch $|\alpha^{(1)}| \cdots |\alpha^{(s+t)}|^2 = \mathrm{N}(\alpha) < c$. Laut Korollar 3.25 gibt es nur endlich viele nicht-assoziierte Elemente $\alpha \in \mathcal{O}$ mit $|\mathrm{N}(\alpha)| < c$, etwa $\alpha_1, ..., \alpha_n$. Also gilt $\alpha \sim \alpha_i$ für ein $i \in \{1, ..., n\}$, etwa $\alpha = \alpha_i \epsilon^{-1}$ mit $\epsilon \in \mathcal{O}^\times$. Dann ist $\eta(\rho(\alpha_i)) \rho(\epsilon^{-1}) \in M'$. Wir setzen nun $S_0 = \bigcup\{\rho(\alpha_i^{-1}) M' \mid 1 \leq i \leq m\}$, dann gilt $\eta \in \ell^{-1}(W) \subseteq \bigcup\{\rho(\epsilon) S_0 \mid \epsilon \in \mathcal{O}\}$. Wegen der Submultiplikativität $\|x\|\|y\| \geq \|xy\|$ (bzgl. komponentenweiser Multiplikation η) impliziert die Beschränktheit von M: S_0 ist beschränkt.

3. *$Kern(\ell) \cap \mathcal{O}$ besteht aus Einheitswurzeln* und bildet damit eine endliche Gruppe: Sei $\alpha \in K^\times$ eine Einheitswurzel, dann ist $\alpha^m = 1$ für ein $m \in \mathbb{N}$, d.h. α ist ganz und erfüllt $|\alpha^{(i)}| = 1$ für alle $1 \leq i \leq n$. Sei umgekehrt $\alpha \in \mathcal{O}$ mit $\ell(\alpha) = (0, ..., 0)$. Dann ist $|\alpha^{(i)}| = 1$ für alle i, d.h. es gilt $|\mathrm{N}(\alpha)| = 1$ und mit Lemma 3.26 folgt $\alpha \in \mathcal{O}^\times$. Weiter sind die $\alpha \in \mathcal{O}$ mit $|\alpha^{(i)}| = 1$ beschränkt in $\mathbb{K}^{s,t}$ und da $\mathcal{O}$ diskret in $\mathbb{K}^{s,t}$, ist $\ell^{-1}(\{0\}) \cap \mathcal{O}$ eine endliche Untergruppe von $K^\times$, also zyklisch.

4. *Jedes $\epsilon \in \mathcal{O}^\times$ lässt sich eindeutig schreiben als $\epsilon = \zeta \epsilon_1^{m_1} \cdots \epsilon_r^{m_r}$:* Seien $\epsilon_1, ..., \epsilon_r \in \mathcal{O}^\times$ mit $r = s + t - 1$ und $\ell(\mathcal{O}^\times) = \mathbb{Z}\ell(\epsilon_1) \oplus \cdots \oplus \mathbb{Z}\ell(\epsilon_r)$. Da $\ell(\epsilon) = m_1 l(\epsilon_1) + \cdots + m_r l(\epsilon_r)$, mit eindeutig bestimmten $m_1, ..., m_r$, ist $\epsilon^{-1} \epsilon_1^{m_1} \cdots \epsilon_r^{m_r} \in \mathrm{Kern}(\ell) \cap \mathcal{O}$, d.h. es gibt eine Einheitswurzel ζ mit $\epsilon = \zeta \epsilon_1^{m_1} \cdots \epsilon_r^{m_r}$. Diese ist eindeutig bestimmt, denn aus $\epsilon = \zeta' \epsilon_1^{m_1} \cdots \epsilon_r^{m_r}$ folgt sofort, dass $\zeta' = \zeta$. □

Bemerkung 3.28.

Zu jedem algebraischen Zahlkörper K existieren also ein Einheiten-Fundamentalsystem $\epsilon_1, ..., \epsilon_r$ der Länge $r = s + t - 1$ sowie eine m-te Einheitswurzel ζ_m mit $\mathcal{O}_K^\times \cong \mathbb{Z}^r \times \langle \zeta_m \rangle \cong \langle \epsilon_1 \rangle \times \cdots \times \langle \epsilon_r \rangle \times \langle \zeta_m \rangle$. ◊

Bemerkung 3.29. (Einheiten in komplex-quadratischen Zahlkörpern)

Sei $K = \mathbb{Q}(\sqrt{d})$ mit $d \in -\mathbb{N}$ quadratfrei. Dann sind $s = 0$ und $t = 1$, d.h. $\mathcal{O}^\times = \zeta^{\mathbb{Z}}$ für eine geeignete Einheitswurzel ζ. Wegen $\mathcal{O} = \mathbb{Z} \oplus \omega\mathbb{Z}$, vgl. Beispiel 3.11, existieren $a, b \in \mathbb{Z}$ mit $\zeta = a + b\omega$, und mit Lemma 3.26 folgt $\pm 1 = \mathrm{N}(\zeta) = a^2 + \mathrm{S}(\omega)ab + \mathrm{N}(\omega)b^2$, speziell $\mathrm{N}(\zeta) = +1$. Für $d \equiv 2, 3 \bmod 4$ folgt $\pm 1 = a^2 - b^2 d$, sonst $\pm 1 = a^2 + ab + \frac{1-d}{4}b^2$. Wir unterscheiden vier Fälle:

1. $d = -1$, dann sind $\omega = i$ und $1 = a^2 + b^2$ hat genau die Lösungen $(\pm 1, 0)$ und $(0, \pm 1)$, die zugehörigen vierten Einheitswurzeln sind $1, -1, i, -i$.
2. Ist $d \equiv 2, 3 \bmod 4$ mit $d \neq -1$, dann $\omega = \sqrt{d}$ und $1 = a^2 - db^2$ hat die Lösungen $(\pm 1, 0)$ mit zugehörigen Einheitswurzeln $1, -1$.
3. Für $d = -3$ ist $\omega = \frac{1+\sqrt{-3}}{2}$ und $1 = a^2 + ab + b^2$ besitzt genau die Lösungen $(\pm 1, 0)$, $(0, \pm 1)$, $(\pm 1, \mp 1)$; wegen $1 - ab = a^2 + b^2 \geq -2ab \Rightarrow -1 \leq ab$ gibt es keine weiteren. Dies impliziert, dass ζ eine sechste Einheitswurzel ist.
4. Sei $d \equiv 1 \bmod 4$ mit $d \neq -3$, dann folgt $b = 0$, denn es ist $1 = a^2 + ab + \frac{1-d}{4}b^2 \geq a^2 + ab + b^2 > 0$ und $a = 0$ ist wegen $d \neq -3$ unmöglich. Also gilt $(a, b) = (\pm 1, 0)$ und ζ ist eine zweite Einheitswurzel. ◊

Bemerkung 3.30. (Einheiten in reell-quadratischen Zahlkörpern)

Sei $K = \mathbb{Q}(\sqrt{d})$ mit $d \in \mathbb{N}$ quadratfrei. Dann gibt es nur die beiden Einheitswurzeln $\zeta = \pm 1$ in $\mathcal{O}^\times$ und es sind $s = 2$, $t = 0$, d.h. $r = 1$. Also besitzt $\mathcal{O}^\times$ die Darstellung $\mathcal{O}^\times = \epsilon^{\mathbb{Z}}$ für eine geeignete Fundamentaleinheit $\epsilon \in \mathcal{O}^\times$. Die Pellsche Gleichung $X^2 - dY^2$ besitzt für jedes quadratfreie $d > 0$ eine nicht-triviale Lösung $(a, b) \in \mathbb{Z}$, vgl. [1], Satz 10.3 oder [13], Satz 2.4 (ist $d = \delta^2$ ein Quadrat, dann ist $X^2 - dY^2 = (X - \delta Y)(X + \delta Y)$ offenbar nur trivial lösbar durch $a = \pm 1$ und $b = 0$). Sei also $\epsilon = a + b\omega \in \mathcal{O}^\times$ eine nicht-triviale Einheit. Unter den Einheiten $\pm\epsilon, \pm\epsilon^{-1}$ existiert eine, welche größer als 1 ist, o.B.d.A. ϵ selbst. Die nicht-leere Menge $E = \{\varepsilon \in \mathcal{O}^\times \mid 1 < \varepsilon \leq \epsilon\}$ ist endlich, denn sei $\varepsilon \in E$, dann ist $\mathrm{N}(\varepsilon) = \pm 1$, d.h. $\varepsilon^{(2)} = \pm\varepsilon^{-1}$. Weiter ist $|\varepsilon^{(2)}| < 1$, d.h. es gilt $|\mathrm{S}(\varepsilon)| = |\varepsilon^{(1)} + \varepsilon^{(2)}| \leq |\varepsilon| + |\varepsilon^{-1}| \leq \epsilon + 1$; da $\mathrm{S}(\varepsilon) \in \mathbb{Z}$, kommen also nur die Spuren $s \in \mathbb{Z}$ mit $|s| \leq \epsilon + 1$ in Frage. Das Minimalpolynom von ε hat somit die Gestalt $m(X) = X^2 + \mathrm{S}(\varepsilon)X \pm \mathrm{N}(\varepsilon) = X^2 \pm sX \pm 1$. Also liegt ε in der endlichen Menge $\{\varepsilon \in \mathcal{O}^\times \mid X^2 \pm sX \pm 1 = 0\} \supseteq E$.

Damit existiert ein kleinstes $\epsilon > 1$, welches die Pellsche Gleichung löst. Offenbar ist dieses ϵ eine Fundamentaleinheit, denn sei $\varepsilon \in \mathcal{O}^\times$, $\varepsilon > 1$ beliebig, dann existiert ein $n \in \mathbb{Z}$ mit $\varepsilon \in [\epsilon^n, \epsilon^{n+1})$. Dann ist auch $\varepsilon\epsilon^{-n} \in \mathcal{O}^\times$ und da $1 \leq \varepsilon\epsilon^{-n} < \epsilon$, folgt aus der Minimalität von ϵ, dass $\varepsilon\epsilon^{-n} = 1$, d.h. $\varepsilon = \epsilon^n$. Die Forderung $\varepsilon > 1$ stellt dabei keine Einschränkung dar, da wieder eines der Elemente $\pm\varepsilon, \pm\varepsilon^{-1}$ in $(1, \infty)$ liegt. Zur Berechnung der Fundamentaleinheit $\epsilon = a + b\sqrt{d}$ im Fall $d \equiv 2, 3 \bmod 4$ bzw. $\epsilon = \frac{1+b\sqrt{d}}{2}$ im Fall $d \equiv 1 \bmod 4$ bestimmen wir $a, b \in \mathbb{Z}$ mit $a, b > 0$ und b minimal, welche eine der diophantischen Gleichungen $a^2 - db^2 = \pm 1$ bzw. $a^2 - db^2 = \pm 4$ lösen, vgl. [1], Satz 10.8:

1. Für $d = 2$ ist $\epsilon = 1 + \sqrt{2}$ mit $\mathrm{N}(\epsilon) = -1$.
2. Im Fall $d = 3$ sind $\epsilon = 2 + \sqrt{3}$ und $\mathrm{N}(\epsilon) = +1$.
3. Mit $d = 5$ erhalten wir $\epsilon = \frac{1+\sqrt{5}}{2}$ mit $\mathrm{N}(\epsilon) = -1$.
4. Für $d = 7$ berechnen wir zu $b = 1, 2, \ldots$ die zugehörigen $a_+^2(b) = db^2 + 1$ und $a_-^2(b) = db^2 - 1$. Wir erhalten die Paare $(a_+^2, b) = (8, 1), (29, 2), (64, 3), \ldots$ und $(a_-^2, b) = (6, 1), (27, 2), (53, 3), \ldots$, also ist die gesuchte Lösung $(a_+(3), 3) = (8, 3)$ und die Fundamentaleinheit zu $d = 7$ somit $\epsilon = 8 + 3\sqrt{7}$ mit $\mathrm{N}(\epsilon) = 1$. ◊

4. Zerlegungstheorie

4.1. Fortsetzung von Idealen

Definition 4.1.

Seien o ein Dedekind-Ring mit Quotientenkörper $K = \mathrm{Quot}(o)$, $L|K$ eine separable Körpererweiterung vom Grad n, $\mathcal{O}$ der ganze Abschluss von o in L und $\mathfrak{p} \neq (0)$ ein Primideal in o.

$\mathfrak{P} = \mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ mit paarweise verschiedenen $\mathcal{O}$-Primidealen $\mathfrak{P}_i$ liegt über $\mathfrak{p}$, falls $\mathfrak{P} \cap o = \mathfrak{p}$.

Bemerkung 4.2.

1. Es gelten die Äquivalenzen $\mathfrak{P}$ liegt über $\mathfrak{p}$ g.d.w. $\mathfrak{p} \in \{\mathfrak{P}_1, ..., \mathfrak{P}_r\}$ g.d.w. $\mathfrak{p} \mid \mathfrak{P}$:

   Liege $\mathfrak{P}$ über $\mathfrak{p}$, dann $\mathfrak{P} \cap o = \mathfrak{p}$, also $\mathfrak{p} \subseteq \mathfrak{P}$, d.h. $\mathfrak{p} = \mathfrak{P}_i$ für ein $i \in \{1, ..., r\}$. Auch klar: Aus $\mathfrak{p} \subseteq \mathfrak{P}$ folgt $\mathfrak{p} \mid \mathfrak{P}$. Gelte schließlich $\mathfrak{p} \mid \mathfrak{P}$, dann liefert $\mathfrak{p} \subseteq \mathfrak{P} \cap o$ mit der Maximalität von $\mathfrak{p}$, dass schon $\mathfrak{p} = \mathfrak{P} \cap o$.

2. Der kanonische Homomorphismus $o \mapsto \mathcal{O}/\mathfrak{P}$ mit $a \mapsto a + \mathfrak{P}$ hat den Kern $o \cap \mathfrak{P} = \mathfrak{p}$, d.h. $o/\mathfrak{p} \to \mathcal{O}/\mathfrak{P}$ ist eine Einbettung. Wir identifizieren dann $o/\mathfrak{p}$ mit seinem Bild: $o/\mathfrak{p} \subseteq \mathcal{O}/\mathfrak{P}$.

3. Der Grad der Körpererweiterung $f_i = [\mathcal{O}/\mathfrak{P}_i : o/\mathfrak{p}]$ heißt der Restklassengrad. ◊

Satz 4.3. (Fortsetzungssatz)

Mit $[L : K] = n$, $f_i = [\mathcal{O}/\mathfrak{P}_i : o/\mathfrak{p}]$ und $\mathfrak{P} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ gilt die Gradormel $n = e_1 f_1 + \cdots + e_r f_r$.

Beweis.

1. Sei $k = o/\mathfrak{p}$. Wir zeigen zuerst, dass $\mathcal{O}/\mathfrak{p}\mathcal{O}$ die k-Dimension $\dim \mathcal{O}/\mathfrak{p}\mathcal{O} = e_1 f_1 + \cdots + e_r f_r$ besitzt. Wegen $\mathfrak{p}\mathcal{O} \cap o = \mathfrak{p}$ ist $\mathcal{O}/\mathfrak{p}\mathcal{O}$ ein k-Vektorraum mit

$$\mathcal{O} \supseteq \mathfrak{P}_1 \supseteq \mathfrak{P}_1^2 \supseteq \cdots \supseteq \mathfrak{P}_1^{e_1} \supseteq \mathfrak{P}_1^{e_1}\mathfrak{P}_2 \supseteq \cdots \supseteq \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} = \mathfrak{p}\mathcal{O} \supseteq o.$$

   Dann sind die $\mathcal{O}/\mathfrak{p}\mathcal{O} \supseteq \mathfrak{P}_1/\mathfrak{p}\mathcal{O} \supseteq \cdots$, die wir mit $U_1 \supseteq U_2 \supseteq \cdots$ bezeichnen, alles k-Vektorräume; beachte dabei: aus $A_m \mid \mathfrak{p}\mathcal{O}$ folgt $A_m \cap o = \mathfrak{p}$, wobei $U_m = A_m/\mathfrak{p}\mathcal{O}$. Für deren k-Dimensionen gilt $\dim \mathcal{O}/\mathfrak{p}\mathcal{O} = U_1/U_2 + \cdots + U_m/U_{m+1}$. Die Kette der Untervektorräume hat $e_1 + \cdots + e_r$ viele Glieder. Es bleibt also zu zeigen, dass $\dim U_m/U_{m+1} = f_i$. Wir betrachten dazu den Epimorphismus $U_m = A_m/\mathfrak{p}\mathcal{O} \to A_m/A_m\mathfrak{P}_i$ mit $a + \mathfrak{p}\mathcal{O} \mapsto a + A_m\mathfrak{P}_i$; dieser hat den Kern $A_m\mathfrak{P}_i/\mathfrak{p}\mathcal{O} = U_{m+1}$. Also ist U_m/U_{m+1} als Vektorraum isomorph zu $A_m/A_m\mathfrak{P}_i$. Weiter ist $A_m/A_m\mathfrak{P}_i$ ein $\mathcal{O}/\mathfrak{P}_i$-Vektorraum der Dimension 1, vgl. den Beweis zu Lemma 3.20. Wegen $\dim \mathcal{O}/\mathfrak{P}_i = f_i$ folgt daraus $\dim A_m/A_m\mathfrak{P}_i = f_i$.

2. Wir lokalisieren nach $S = o\backslash\mathfrak{p}$ und schreiben $\mathcal{O}_\mathfrak{p}$ für $S^{-1}\mathcal{O}$. Wir haben bereits in Lemma 2.44 bewiesen, dass $\mathcal{O}_\mathfrak{p}$ der ganze Abschluss von $o_\mathfrak{p}$ in L ist. Weiter ist der Bewertungsring $o_\mathfrak{p}$ ein faktorieller Hauptidealring und damit $\mathcal{O}_\mathfrak{p}$ ein Dedekind-Ring, vgl. Korollar 2.45. Wir setzen $\mathfrak{P}_i' := \mathfrak{P}_i\mathcal{O}_\mathfrak{p}$, dann ist $\mathfrak{p}\mathcal{O}_\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}\mathcal{O}_\mathfrak{p} = \mathfrak{P}_1'^{\,e_1} \cdots \mathfrak{P}_r'^{\,e_r}$. Wegen $\mathfrak{P}_i \cap o = \mathfrak{p}$ ist $\sigma : \mathcal{O}_\mathfrak{p} \to \mathrm{Quot}(\mathcal{O}/\mathfrak{P}_i) = \mathcal{O}/\mathfrak{P}_i$ mit $as^{-1} \mapsto \overline{a}\overline{s}^{-1}$ ein Epimorphismus mit Kern $\mathfrak{P}_i\mathcal{O}_\mathfrak{p} = \mathfrak{P}_i'$. Also ist $\mathfrak{P}_i'$ ein Primideal und es gilt $\mathcal{O}_\mathfrak{p}/\mathfrak{P}_i\mathcal{O}_\mathfrak{p} \cong \mathcal{O}/\mathfrak{P}_i$. Für die Einschränkung von σ auf $o_\mathfrak{p}$ gilt: $o_\mathfrak{p}/\mathfrak{p}o_\mathfrak{p} \cong o/\mathfrak{p}$, woraus wir folgern $f_i = [\mathcal{O}/\mathfrak{P} : o/\mathfrak{p}] = [\mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p} : o_\mathfrak{p}/\mathfrak{p}o_\mathfrak{p}]$ und mit Teil (1): $e_1 f_1 + \cdots + e_r f_r$ ist die $o_\mathfrak{p}/\mathfrak{p}o_\mathfrak{p}$-Dimension von $\mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p}$.

3. Bleibt zu zeigen, dass n die $o_\mathfrak{p}/\mathfrak{p}o_\mathfrak{p}$-Dimension von $\mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p}$ ist. Wir lassen die Lokalisierung wieder weg und setzen voraus, dass o ein Hauptidealring ist. Wir wissen: $\mathcal{O}/\mathfrak{p}\mathcal{O}$ ist ein o/p-Vektorraum und müssen zeigen, dass $\dim \mathcal{O}/\mathfrak{p}\mathcal{O} = n$ über dem Körper $k = o/\mathfrak{p}$. Da o Hauptidealring, ist $\mathcal{O}$ ein freier o-Modul vom Rang r, denn $\mathcal{O} \subseteq M \subseteq L$ mit M freier o-Modul vom Rang n, vgl. Proposition 2.39. Es gibt also eine Basis $(\alpha_1, ..., \alpha_n)$ mit $\mathcal{O} = o\alpha_1 \oplus \cdots \oplus o\alpha_n$, d.h. $\mathcal{O}/\mathfrak{p}\mathcal{O} = o/\mathfrak{p}\overline{\alpha}_1 + \cdots + o/\mathfrak{p}\overline{\alpha}_n$ mit $\overline{\alpha} = \alpha + \mathfrak{p}\mathcal{O}$. Falls nun $a_1\alpha_1 + \cdots + a_n\alpha_n \in \mathfrak{p}\mathcal{O}$, d.h. $\overline{a}_1\overline{\alpha}_1 + \cdots + \overline{a}_n\overline{\alpha}_n = 0$ für gewisse $a_1, ..., a_n \in o$, dann ist zu zeigen, dass alle $\overline{a}_i = \overline{0}$, d.h. $a_i \in \mathfrak{p}$. Mit $a_1\alpha_1 + \cdots + a_n\alpha_n = p_1\alpha_1 + \cdots + p_n\alpha_n$ für $p_i \in \mathfrak{p}$ folgt $a_i = p_i$, also ist $\overline{\alpha}_1, ..., \overline{\alpha}_n$ eine k-Basis von $\mathcal{O}/\mathfrak{p}\mathcal{O}$, d.h. $\mathcal{O}/\mathfrak{p}\mathcal{O} = o/\mathfrak{p}\overline{\alpha}_1 \oplus \cdots \oplus o/\mathfrak{p}\overline{\alpha}_n$. Folglich gilt $\dim \mathcal{O}/\mathfrak{p}\mathcal{O} = n$ und damit $e_1 f_1 + \cdots + e_r f_r = n$. □

Beispiel 4.4.

Seien wieder $o = \mathbb{Z}$, $K = \mathbb{Q}$ und $L = K(\sqrt{d})$ mit $d \in \mathbb{Z}$ quadratfrei. Dann ist $\mathcal{O} = \mathbb{Z} + \mathbb{Z}\omega$ mit $\omega = \sqrt{d}$ für $d \equiv 2, 3 \bmod 4$ und $\omega = \frac{1+\sqrt{d}}{2}$, falls $d \equiv 1 \bmod 4$. Weiter seien $\mathfrak{p} = \mathbb{Z}p$ für eine Primzahl $p \in \mathbb{Z}$ und $\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ mit $f_i = [\mathcal{O}/\mathfrak{P}_i : \mathbb{Z}/p\mathbb{Z}]$. Dann ist $[L : K] = 2$ und es bestehen folgende Möglichkeiten:

1. $\mathfrak{p}\mathcal{O} = p\mathcal{O} = \mathfrak{P}^1$ mit $[\mathcal{O}/\mathfrak{P} : \mathbb{Z}/p\mathbb{Z}] = 2$, man nennt p dann träge;

2. $p\mathcal{O} = \mathfrak{P}^2$ mit $\mathcal{O}/\mathfrak{P} = \mathbb{Z}/p\mathbb{Z}$, dann nennt man p verzweigt;

3. $p\mathcal{O} = \mathfrak{P}^1\mathfrak{P}^2$ mit $\mathcal{O}/\mathfrak{P}_i = \mathbb{Z}/p\mathbb{Z}$; dann heißt p zerlegt. ◊

Satz 4.5.

Gibt es ein $\alpha \in \mathcal{O}$ mit $\mathcal{O}/\mathfrak{p}\mathcal{O} = k \oplus \cdots \oplus k\overline{\alpha}^{n-1}$, wobei $k = \mod o/\mathfrak{p}$ und $\overline{\alpha} = \alpha + \mathfrak{p}\mathcal{O}$. Gelte für das Polynom $f = \mathrm{Irr}(\alpha, k)$, dass $\overline{f} = \overline{g}_1^{e_1} \cdots \overline{g}_r^{e_r}$ über k, wobei $g_i \in o[X]$ und $\overline{g}_i$ irreduzibel sowie paarweise verschieden seien. Dann ist

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} \qquad \text{mit} \qquad \mathfrak{P}_i = \mathfrak{p}\mathcal{O} + g_i(\alpha)\mathcal{O} \qquad \text{und} \qquad f_i = [\mathcal{O}/\mathfrak{P}_i : o/\mathfrak{p}] = \deg g_i.$$

Beweis.

Es gilt $f \in o[X]$, da $\alpha \in \mathcal{O}$, also sind auch alle Konjugierten von α ganz über o; die Koeffizienten von f sind Linearkombinationen dieser Konjugierten. $R = \mathcal{O}/\mathfrak{p}\mathcal{O} = k \oplus \cdots \oplus k\overline{\alpha}^{n-1}$ ist isomorph zu $k[X]/(f)$: Der Epimorphismus $\varphi : k[X] \to R$ mit $g(X) \mapsto g(\overline{\alpha})$ hat den Kern $(\overline{f})$. Offenbar gilt $\overline{f} \in \mathrm{Kern}(\varphi)$, denn $\varphi(\overline{f}(X)) = \overline{f}(\overline{\alpha}) = 0$. Weiter ist $\dim(R) = n$. Setze $\mathrm{Kern}(\varphi) = (\overline{h})$ prim und normiert, dann gilt $\overline{h} \mid \overline{f}$ und wegen $\deg \overline{h} = n$, dass $\overline{h} \sim \overline{f}$; da $\overline{h}$ normiert, folgt also $\overline{f} = \overline{h}$.

Setze $A_i = \mathfrak{p}\mathcal{O} + g_i(\alpha)\mathcal{O}$, dann $\overline{A}_i = (\overline{g}_i(\overline{\alpha}))$. Also ist $\overline{g}_i(\overline{\alpha})$ keine Einheit in R, sonst gäbe es Polynome $h_1, h_2 \in o[X]$ mit $\overline{g}_i\overline{h}_1 = 1 + \overline{f}\overline{h}_2$. Wegen $\overline{g}_i \mid \overline{f}$ würde dann gelten $\overline{g}_i \mid 1$ in $k[X]$, ein Widerspruch. Weiter ist $\overline{A}_i$ ein Primideal in R: falls $\overline{h_1 h_2} = \overline{g_i h_3 + f h_4}$ mit $h_j \in o[X]$, $j = 1, ..., 4$, dann gilt $\overline{g}_i \mid \overline{h}_1$ oder $\overline{g}_i \mid \overline{h}_2$, d.h. $\overline{h}_1(\overline{\alpha}) \in \overline{A}_i$ oder $\overline{h}_2(\overline{\alpha}) \in \overline{A}_i$. A_i ist prim in $\mathcal{O}$, denn $O/A_i \cong R/\overline{A}_i$ (ein Integritätsbereich) und die Abbildung $\mathcal{O} \to R/\overline{A}_i$ mit $\beta \mapsto \overline{\beta} + \overline{A}_i$ hat den Kern A_i. Schließlich ist $\overline{A}_i \neq \overline{A}_j$ für alle $i \neq j$, insbesondere $A_i \neq A_j$. Sonst wäre etwa $\overline{g}_i(\overline{\alpha}) \in \overline{A}_j$, d.h. es gibt $h_1, h_2 \in o[X]$ mit $\overline{g}_i = \overline{g}_j\overline{h}_1 + \overline{f}\overline{h}_2$, also $\overline{g}_j \mid \overline{g}_i$, ein Widerspruch zur Irreduzibilität.

Wir schreiben $\mathfrak{P}_i$ für A_i; wegen $\mathfrak{P}_i \supseteq \mathfrak{p}\mathcal{O}$ wird $\mathfrak{p}\mathcal{O}$ von $\mathfrak{P}_i$ geteilt. Weiter gilt $g_i(\alpha) \in \mathfrak{P}_i$ und folglich $\mathcal{O}/\mathfrak{P}_i = k + k(\alpha + \mathfrak{P}_i) + \cdots + k(\alpha + \mathfrak{P}_i)^{f_i - 1}$, also $f_i' = [\mathcal{O}/\mathfrak{P}_i : k] \leq f_i = \deg g_i$. Beachte dabei: $g_i(\alpha) \in \mathfrak{P}_i \Rightarrow g_i(\alpha) + \mathfrak{P}_i = 0 + \mathfrak{P}_i)$. Wegen $\mathfrak{P}_i \subseteq \mathfrak{p}\mathcal{O} + g_i(\alpha)\mathcal{O}$ ist $\mathfrak{P}_i^{e_i} \subseteq \mathfrak{p}\mathcal{O} + g_i(\alpha)^{e_i}\mathcal{O}$. Also gelten die Inklusionen $\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} \subseteq \mathfrak{p}\mathcal{O} + g_1(\alpha)^{e_1} \cdots g_r(\alpha)^{e_r}\mathcal{O} \subseteq \mathfrak{p}\mathcal{O}$. Folglich ist $\mathfrak{p}\mathcal{O} = \mathfrak{P}_1'^{e_1} \cdots \mathfrak{P}_r'^{e_r}$ mit $e_i' \leq e_i$ und der Fortsetzungssatz 4.3 liefert $n = e_1'f_1' + \cdots + e_r'f_r' \leq e_1 f_1 + \cdots + e_r f_r = \deg f = n$, also gilt Gleichheit und damit $e_i = e_i'$ sowie $f_i = f_i'$. Es folgen $\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ und $\deg g_i = [\mathcal{O}/\mathfrak{P}_i : k]$. □

Beispiel 4.6. (Fortsetzung in quadratischen Zahlkörpern)

Sei wieder $d \in \mathbb{Z}$ quadratfrei. Dann gelten:

1. Sind $d \equiv 2, 3 \bmod 4$ und $p \neq 2$ eine Primzahl in $\mathbb{Z}$, dann können für das über $\mathbb{Q}$ irreduzible Polynom $f(X) = \mathrm{Irr}(\omega, \mathbb{Q}) = X^2 - d$ mit $\omega = \sqrt{d}$ die folgenden Fälle auftreten:

   a) $X^2 - d$ ist irreduzibel in $k = \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$. Dann ist d kein quadratischer Rest modulo p und es gelten $(\frac{d}{p}) = -1$, $p \nmid d$. Also $r = 1$, $e_1 = 1$, $f_1 = 2$, d.h. $p\mathcal{O} = \mathfrak{P}_1$ ist träge und $[\mathcal{O}/\mathfrak{P}_1 : \mathbb{Z}_p] = 2$.

   b) $X^2 - d = (X - a)(X - b)$ über $\mathbb{Z}_p$ mit $a \neq b \Leftrightarrow d$ ist quadratischer Rest und $p \nmid d \Leftrightarrow (\frac{d}{p}) = 1$ und $p \nmid d$. Also $r = 2$, $e_1 = e_2 = 1 = f_1 = f_2 = 1$ und $p\mathcal{O} = \mathfrak{P}_1\mathfrak{P}_2$ zerlegt mit $\mathcal{O}/\mathfrak{P}_i = \mathbb{Z}_p$, $i = 1, 2$.

   c) $X^2 - d = (X - a)^2$ über $\mathbb{Z}_p \Leftrightarrow p \mid d$, d.h. $\overline{d} = 0$. Dann sind $r = 1$, $e_1 = 2$ und $f_1 = 1$, d.h. $\mathcal{O}/\mathfrak{P}_1 = \mathbb{Z}_p$ und $p\mathcal{O} = \mathfrak{P}_1^2$ ist verzweigt.

2. Sind $d \equiv 2, 3 \bmod 4$ und $p = 2$, dann $X^2 - d = (X - d)^2$ über $\mathbb{Z}_2$, also ist $2\mathcal{O}$ verzweigt in L.

3. Im Fall $d \equiv 1 \bmod 4$ mit $p \neq 2$ prim ist $\mathcal{O}/p\mathcal{O} = \mathbb{Z} + \mathbb{Z}\sqrt{d}/p\mathcal{O} \cong \mathbb{Z}/p\mathbb{Z}[\sqrt{\overline{d}}] = \mathbb{Z}/p\mathbb{Z} + \mathbb{Z}/p\mathbb{Z}\sqrt{\overline{d}}$, denn ist $u \in \mathbb{Z}$ ungerade, dann $u + p \equiv u \bmod p$ und $u + p$ ist gerade. Also $\frac{u}{2}(1 + \sqrt{d}) \in \mathbb{Z} + \mathbb{Z}\sqrt{d} \bmod p$. Ist dann $f(X) = X^2 - d$, dann gelten (a),(b),(c) wie eben.

4. Sind $d \equiv 2, 3 \bmod 4$ und $p = 2$, dann $f(X) = X^2 - X - \frac{d-1}{4}$. Weiter sind $\frac{d-1}{4} \equiv 1 \bmod 2$, falls $d \equiv 5 \bmod 8$, und $\frac{d-1}{4} \equiv 0 \bmod 2$ für $d \equiv 1 \bmod 8$, modulo 2 gilt also: $f(X) = X^2 - X = X(X - 1)$ zerlegt für $d \equiv 5 \bmod 8$ und $f(X) = X^2 - X - 1$ ist träge, da irreduzibel, für $d \equiv 1 \bmod 8$.

Mit $\mathrm{D}_L = 4d$ für $d \equiv 2, 3 \bmod 4$ und $\mathrm{D}_L = d$ im Fall $d \equiv 1 \bmod 4$ erhalten wir:

$$p \text{ verzweigt} \Leftrightarrow p \mid \mathrm{D}_L, \quad p \text{ zerlegt} \Leftrightarrow \begin{cases} p \neq 2, & (\frac{d}{p}) = +1 \\ p = 2 & d \equiv 1 \bmod 8 \end{cases}, \quad p \text{ träge} \Leftrightarrow \begin{cases} p \neq 2, & (\frac{d}{p}) = -1 \\ p = 2, & d \equiv 5 \bmod 8 \end{cases}. \quad \Diamond$$

Korollar 4.7. (Primzahlen als Quadratsummen)

Sei $p \neq 2$ prim. Dann gilt: $p = X_1^2 + X_2^2$ ist lösbar in $\mathbb{Z} \Leftrightarrow p \equiv 1 \bmod 4$.

Beweis.

Setze $L = \mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$, dann $\mathcal{O} = \mathbb{Z} + \mathbb{Z}i$, $\mathrm{h}(\mathcal{O}) = 1$ und $\mathrm{D}_2 = -4$. Wegen $p \neq 2$ gilt $(p)_\mathcal{O} = (\pi)$ oder $(p)_\mathcal{O} = (\pi_1\pi_2)$. Sei $\alpha \in \mathcal{O}$, dann $\alpha^{(1)} = a+ib$ und $\alpha^{(2)} = a-ib$ mit $a, b \in \mathbb{Z}$, also $\mathrm{N}(\alpha) = \alpha^{(1)}\alpha^{(2)} = a^2+b^2$. Gilt nun $(p) = (\pi)$, so $\mathrm{N}(\pi) = \pm p^2$ und $p = \epsilon\pi$. Andernfalls ist $(p) = (\pi_1\pi_2) \Rightarrow p^2 = \pm\mathrm{N}(\pi_1)\mathrm{N}(\pi_2)$, d.h. $|\mathrm{N}(\pi_1)| = |\mathrm{N}(\pi_2)| = p$. Damit gilt mit Bemerkung 1.17:

$$\begin{array}{lll} p = X_1^2 + X_2^2 \text{ lösbar} & \iff & p = N(a+ib) \iff p \text{ ist zerlegt in } \mathcal{O} \text{ (da } \mathrm{N}(p) = p^2) \\ & \iff & (\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = 1 \iff p \equiv 1 \bmod 4. \end{array}$$

□

4.2. Verzweigung von Primidealen

Definition 4.8.

Seien o ein Dedekind-Ring mit Quotientenkörper $K = \mathrm{Quot}(o)$, $L|K$ eine separable Körpererweiterung vom Grad n, $\mathcal{O}$ der ganze Abschluss von o in L und $\mathfrak{p} \neq (0)$ ein Primideal in o.

$\mathfrak{p}$ heißt verzweigt in L, wenn $e_i > 1$ gilt oder $\mathcal{O}/\mathfrak{P}_i$ inseparabel über $o/\mathfrak{p}$ ist für ein $i \in \{1, ..., r\}$. e_i heißt dann der Verzweigungsindex von $\mathfrak{P}_i$ über $\mathfrak{p}$.

Die Relativdiskriminante $\mathcal{D}(\mathcal{O}/o)$ ist dasjenige o-Ideal, das von $\mathrm{D}_{L|K}(\alpha_1, ..., \alpha_n)$ erzeugt wird, wobei $\alpha_1, ..., \alpha_n \in \mathcal{O}$ alle Basen von $L|K$ durchläuft.

Bemerkung 4.9.

1. Falls $K = \mathbb{Q}$ und L eine endliche Erweiterung von $\mathbb{Q}$), dann ist $o/\mathfrak{p}$ endlich, also perfekt, und damit $\mathcal{O}/\mathfrak{P}_i$ stets separabel über $o/\mathfrak{p}$.
2. Ist o ein Hauptidealring, so ist $\mathcal{O}$ ein freier o-Modul vom Rang $n = [L : K]$. Sei $\alpha_1, ..., \alpha_n$ eine o-Basis von $\mathcal{O}$, dann ist $\mathcal{D}(\mathcal{O}/o) = o\mathrm{D}(\alpha_1, ..., \alpha_n)$. ◊

Lemma 4.10.

$\mathfrak{p}$ ist genau dann verzweigt in L, wenn $\mathcal{D}(\alpha_1, ..., \alpha_n) = 0$ für eine $o/\mathfrak{p}$-Basis von $\mathcal{O}/\mathfrak{p}\mathcal{O}$.

Beweis.

Habe $\mathfrak{P} = \mathfrak{p}\mathcal{O}$ die Darstellung $\mathfrak{P} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$. Dann ist $\mathcal{O}/\mathfrak{p}$ isomorph zu $\mathcal{O}/\mathfrak{P}_1^{e_1} \oplus \cdots \oplus \mathcal{O}/\mathfrak{P}_r^{e_r}$: Betrachte den Homomorphismus $\sigma : \mathcal{O} \to \mathcal{O}/\mathfrak{P}_1^{e_1} \oplus \cdots \oplus \mathcal{O}/\mathfrak{P}_r^{e_r}$ mit $a \mapsto a/\mathfrak{P}_1^{e_1} + \cdots + a/\mathfrak{P}_r^{e_r}$. Dann ist σ ein wohldefinierter Homomorphismus mit $\mathrm{Kern}(\sigma) = \mathfrak{P}_1^{e_1} \cap \cdots \cap \mathfrak{P}_r^{e_r} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_e^{e_r}$. Wegen $\mathfrak{P}_i^{e_i} + \mathfrak{P}_j^{e_j} = \mathcal{O}$ für $i \neq j$ folgt mit dem Chinesichen Restsatz 1.2 die Surjektivität von σ und mit dem Homomorphiesatz die Bijektivität. Setze $k = o/\mathfrak{p}$ und $d_i = \dim \mathcal{O}/\mathfrak{P}_i^{e_i} = e_i f_i$. Sei $\alpha_{i1}, ..., \alpha_{id_i}$ eine k-Basis von $\mathcal{O}/\mathfrak{P}_i^{e_i}$. Dann gilt $\alpha_{is}\alpha_{jt} = 0$ für alle $i \neq j$, $1 \leq i, j \leq r$. Also ist

$$\det(\mathrm{S}(\alpha_{is}\alpha_{jt}))_{1\leq i\leq n}^{1\leq j\leq n} = \prod_{i=1}^{r} \det(\mathrm{S}(\alpha_{is}\alpha_{it}))_{1\leq s\leq d_i}^{1\leq t\leq d_i} = \prod_{i=1}^{r} \mathrm{D}(\alpha_{i1}, ..., \alpha_{id_i})$$

und damit $\mathcal{D}(\mathcal{O}/\mathfrak{p}\mathcal{O}) \neq 0$ genau dann, wenn $\mathcal{D}(o/\mathfrak{P}_i^{r_i}) \neq 0$ für alle $1 \leq i \leq r$. Wir unterscheiden:

1. Sind $e_i = 1$ und $\mathcal{O}/\mathfrak{P}_i^{e_i}$ separabel über $o/\mathfrak{p}$, so folgt $\mathcal{D}(\mathcal{O}/\mathfrak{P}_i^{e_i}) \neq 0$.
2. Im Fall $e_i = 1$ und $\mathcal{O}/\mathfrak{P}_i^{e_i}$ inseparabel über $o/\mathfrak{p}$ folgt $\mathcal{D}(\mathcal{O}/\mathfrak{P}_i^{e_i}) = 0$.
3. Ist hingegen $e_i > 1$ für ein i, existieren nilpotente Elemente in $B = \mathcal{O}/\mathfrak{P}_i^{e_i}$, denn sei $b \in \mathfrak{P}_i \backslash \mathfrak{P}_i^2$, dann gilt für $\beta = b/\mathfrak{P}_i^{e_i}$, dass $\beta^{e_i} = 0$ und außerdem $\beta \neq 0$. Wähle eine k-Basis von B mit $\beta_1, ..., \beta_{d_i}$ mit $\beta_1 = \beta$. Dann ist $\beta\beta_i$ nilpotent, d.h. $m_{\beta\beta_i}$ eine nilpotente Matrix. Eigenwerte nilpotenter Matrizen sind alle 0, also ist auch $\mathrm{Spur}(m_{\beta\beta_i}) = 0$. Dann folgt $(\mathrm{S}(\beta_e\beta_j)) = (0|*)$, also $\mathrm{D}(\beta_1, ..., \beta_{d_i}) = 0$. □

Satz 4.11.

$\mathfrak{p}$ ist in L genau dann verzweigt, wenn gilt $\mathfrak{p} \mid \mathcal{D}(\mathcal{O}/o)$.

Beweis.

Wir lokalisieren nach $S = o\backslash\mathfrak{p}$. Dann folgt aus $\mathfrak{P} = \mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$, dass $\mathfrak{p}\mathcal{O}_\mathfrak{p} = \mathfrak{P}_1'^{e_1} \cdots \mathfrak{P}_r'^{e_r}$ mit $\mathfrak{P}_i' = \mathfrak{P}_i\mathcal{O}_\mathfrak{p}$. Wir zeigen: $\mathcal{D}(\mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p}) = 0$ über $k = o/\mathfrak{p} \cong o_\mathfrak{p}/\mathfrak{p}'$, wobei $\mathfrak{p}' = \mathfrak{p}o_\mathfrak{p}$ und $\mathcal{O}_\mathfrak{p}/\mathfrak{p}'\mathcal{O}_\mathfrak{p} \cong \mathcal{O}/\mathfrak{p}\mathcal{O}$. Da $o_\mathfrak{p}$ ein Hauptidealring ist, also $\mathcal{O}_\mathfrak{p} = o_\mathfrak{p}\alpha_1 \oplus \cdots \oplus o_\mathfrak{p}\alpha_n$, gilt gemäß dem Beweis des Fortsetzungssatzes 4.3, dass $\mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p} = k\overline{\alpha}_1 \oplus \cdots \oplus k\overline{\alpha}_n$, also ist $\mathfrak{p}$ genau dann verzweigt, wenn $\mathrm{D}(\overline{\alpha}_1, ..., \overline{\alpha}_n) = 0$ über k.

1. Es gilt $\mathrm{D}(\alpha_1, ..., \alpha_n) = \det(\mathrm{S}(\alpha_i\alpha_j))$ in $\mathcal{O}_\mathfrak{p}$ als $o_\mathfrak{p}$-Modul und damit
$$\overline{\mathrm{D}(\alpha_1, ..., \alpha_n)} = \det(\overline{\mathrm{S}(\alpha_i\alpha_j)}) = \mathrm{Spur}(m_{\overline{\alpha_i\alpha_j}}) = \det(\mathrm{S}(\overline{\alpha_i\alpha_j})) = \mathrm{D}(\overline{\alpha}_1, ..., \overline{\alpha}_n).$$
2. Es ist $\mathcal{D}(\mathcal{O}_\mathfrak{p}/o_\mathfrak{p}) = \mathcal{D}(\mathcal{O}/o)o_\mathfrak{p}$: $\supseteq$ gilt wegen $\mathcal{O} \subseteq \mathcal{O}_\mathfrak{p}$; zu $\subseteq$: Seien $\alpha_1, ..., \alpha_n \in \mathcal{O}_\mathfrak{p}$ mit $\alpha_i = \frac{\beta_i}{s}$, $\beta_i \in \mathcal{O}$, $s \in S$. Dann ist $s\alpha_1, ..., s\alpha_n \in \mathcal{O}$ und damit gilt $\mathrm{D}(\alpha_1, ..., \alpha_n) \in \mathcal{D}(\mathcal{O}/o)o_\mathfrak{p}$:
$$\mathrm{D}(s\alpha_1, ..., s\alpha_n) = \det(\mathrm{S}(s\alpha_i, s\alpha_j)) = s^{2n}\mathrm{D}(\alpha_1, ..., \alpha_n) \in \mathcal{D}(\mathcal{O}/o).$$

Wir erhalten

$$\begin{aligned} \mathfrak{p} \text{ verzweigt} &\iff \mathrm{D}(\alpha_1, ..., \alpha_n) \in \mathfrak{p}\mathcal{O}_\mathfrak{p} \cap K = \mathfrak{p}o_\mathfrak{p} = \mathfrak{p}' \\ &\iff \mathfrak{p}' \mid \mathcal{D}(\mathcal{O}_\mathfrak{p}/o_\mathfrak{p}) = \mathcal{D}(\mathcal{O}/o)o_\mathfrak{p} \\ &\iff \mathfrak{p} \mid \mathcal{D}(\mathcal{O}/o), \end{aligned}$$

denn falls $\mathcal{D}(\mathcal{O}/o) = \mathfrak{p}_1^{\nu_1} + \cdots + \mathfrak{p}_s^{\nu_s}$, so gilt $\mathcal{D}(\mathcal{O}/o)o_\mathfrak{p} = \mathfrak{p}_1'^{\nu_1} \cdots \mathfrak{p}_s'^{\nu_s}$ mit $\mathfrak{p}_i' = \mathfrak{p}_i o_\mathfrak{p}$ für alle i. □

Korollar 4.12.

Es gibt nur endlich viele verzweigte Primideale von o in L.

4.3. Zerlegung und Verzweigung in Galoiserweiterungen

Satz 4.13.

Seien o ein Dedekind-Ring mit Quotientenkörper $K = \mathrm{Quot}(o)$, $L|K$ eine separable Galoiserweiterung vom Grad n mit zugehöriger Galoisgruppe $G = \mathrm{Gal}(L|K)$, $\mathcal{O}$ der ganze Abschluss von o in L und $\mathfrak{p} \neq (0)$ ein Primideal in o.

Sei $\mathfrak{P} = \mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$. Dann sind alle $\mathfrak{P}_i$ konjugiert, d.h. für alle $i, j \in \{1, ..., r\}$ gibt es ein $\sigma \in G$ mit $\mathfrak{P}_i = \sigma(\mathfrak{P}_j)$, und es existieren $e, f \in \mathbb{N}$ mit $e_i = e$ sowie $f_i = f$ für alle i; speziell ist $n = ref$.

Beweis.

Wegen $\mathfrak{P} \cap o = \mathfrak{p}$ ist auch $\sigma(\mathfrak{P}) \cap o = \mathfrak{p}$. Sei $\{\sigma(\mathfrak{P}) \mid \sigma \in G\} = \{\mathfrak{P}^{(1)}, ..., \mathfrak{P}^{(m)}\}$. Wähle $\xi_{ij} \in \mathfrak{P}^{(i)}\backslash\mathfrak{P}^{(j)}$ für $i \neq j$. Angenommen, $\mathfrak{P}' \cap o = \mathfrak{p}$, aber $\mathfrak{P}' \not\subseteq \mathfrak{P}^{(i)}$ für alle $1 \leq i \leq m$. Wähle dann $\alpha_i \in \mathfrak{P}'\backslash\mathfrak{P}^{(i)}$ und setze $\beta_i = \alpha_i \prod\{\xi_{ij} \mid j \neq i\} \in \mathfrak{P}', \mathfrak{P}^{(j)}$, aber $\beta_i \notin \mathfrak{P}^{(i)}$, da kein Faktor in $\mathfrak{P}^{(i)}$ liegt. Setze $\beta = \beta_1 + \cdots + \beta_m \in \mathfrak{P}'$, dann liegt β in keinem $\mathfrak{P}^{(i)}$, denn es gelten $\beta_j \in \mathfrak{P}^{(i)}$ und $\beta_i \notin \mathfrak{P}^{(j)}$ für $j \neq i$. Die Norm von β ist ein Element aus $\mathfrak{P}$, denn $\mathrm{N}(\beta) = \beta^{(1)} \cdots \beta^{(n)} = \prod\{\sigma(\beta) \mid \sigma \in G\} \in \mathfrak{P}'$ impliziert $\mathrm{N}(\beta) \in \mathfrak{P}' \cap o = \mathfrak{p} \subseteq \mathfrak{P}$. Andererseits ist $\beta \notin \sigma^{-1}(\mathfrak{P})$ für alle $\sigma \in G$, also $\sigma(\beta) \notin \mathfrak{P}$ für alle $\sigma \in G$. Dann kann auch nicht $\mathrm{N}(\beta) = \prod\{\sigma(\beta) \mid \sigma \in G\}$ in $\mathfrak{P}$ liegen, ein Widerspruch. Damit sind alle $\mathfrak{P}_i$ konjugiert zueinander.

Wegen $\mathfrak{P}^s \mid \mathfrak{p}\mathcal{O} \Leftrightarrow \sigma(\mathfrak{P}^s) = \sigma(\mathfrak{P})^s \mid \mathfrak{p}\mathcal{O}$ sind alle e_i identisch. Weiter hat der Epimorphismus $\mathcal{O} \to \mathcal{O}/\sigma(\mathfrak{P})$ mit $\alpha \mapsto \sigma(\alpha) + \sigma(\mathfrak{P})$ den Kern $\mathfrak{P}$, also gilt mit dem Homomorphiesatz $\mathcal{O}/\mathfrak{P} \cong \mathcal{O}/\sigma(\mathfrak{P})$, d.h. alle f_i sind gleich. □

Definition 4.14.

Sei $\mathfrak{P}$ ein $\mathcal{O}$-Primideal. Dann heißt $\mathrm{Z}(\mathfrak{P}) = \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$ die Zerlegungsgruppe von $\mathfrak{P}$. $K_\mathrm{Z} = \mathrm{Fix}(\mathrm{Z}(\mathfrak{P}))$ nennt man den Zerlegungskörper von $\mathfrak{P}$.

Bemerkung 4.15.

1. $\mathcal{O}$ ist invariant unter G, d.h. $\sigma(\mathcal{O}) = \mathcal{O}$ für alle $\sigma \in G$, denn aus $\alpha \in L$ ganz über o folgt $\sigma(\alpha)$ ganz über o, also $\sigma(\mathcal{O}) \subseteq \mathcal{O}$, und analog $\sigma^{-1}(\mathcal{O}) \subseteq \mathcal{O}$, d.h. $\mathcal{O} = \sigma(\mathcal{O})$.
2. $\mathrm{Z}(\mathfrak{P})$ ist eine Untergruppe von G.
3. Aus $\mathfrak{P}' = \tau(\mathfrak{P})$ folgt $\mathrm{Z}(\mathfrak{P}') = \tau\mathrm{Z}(\mathfrak{P})\tau^{-1}$, denn $\sigma(\mathfrak{P}') = \mathfrak{P}'$ genau dann, wenn $(\tau^{-1}\sigma\tau)(\mathfrak{P}) = \mathfrak{P}$, d.h. $\sigma \in \mathrm{Z}(\mathfrak{P}')$ genau dann, wenn $(\tau^{-1}\sigma\tau) \in \mathrm{Z}(\mathfrak{P})$.
4. Sei $\mathfrak{p}\mathcal{O} = (\mathfrak{P}^{(1)} \cdots \mathfrak{P}^{(r)})^e$ mit $\mathfrak{P}^{(i)} = \sigma_i(\mathfrak{P})$ und $\mathfrak{P} \cap o = \mathfrak{p}$. Dann bildet $\{\sigma_1, ..., \sigma_r\}$ ein Vertretersystem modulo $\mathrm{Z}(\mathfrak{P})$, d.h. G lässt sich darstellen als disjunkte Vereinigung $G = \sigma_1\mathrm{Z} \cup \cdots \cup \sigma_r\mathrm{Z}$. Also ist $|G| = n = efr$, d.h. $|\mathrm{Z}(\mathfrak{P})| = \frac{1}{r}|G| = ef$. Damit haben wir gezeigt: $|\mathrm{Z}(\mathfrak{P})| = ef$ für $\mathfrak{P} \cap o = \mathfrak{p}$.
5. Sei nun $\sigma \in \mathrm{Z}(\mathfrak{P})$. Dann gelten $\sigma(\mathcal{O}) = \mathcal{O}$ und $\sigma(\mathfrak{P}) = \mathfrak{P}$. Definiere die Abbildung $\overline{\sigma} : \mathcal{O}/\mathfrak{P} \to \mathcal{O}/\mathfrak{P}$ mit $\alpha + \mathfrak{P} \mapsto \sigma(\alpha) + \mathfrak{P}$. Dies ist unabhängig vom Vertreter:

$$\alpha + \mathfrak{P} = \alpha' + \mathfrak{P} \Leftrightarrow \alpha - \alpha' \in \mathfrak{P} \Leftrightarrow \sigma(\alpha) - \sigma(\alpha') = \sigma(\alpha - \alpha') \in \sigma(\mathfrak{P}) = \mathfrak{P}.$$

   $\overline{\sigma}$ ist ein Automorphismus von $\mathcal{O}/\mathfrak{P}$ über $o/\mathfrak{p}$: Offenbar ist $\overline{\sigma}$ ein (Körper-)Epimorphismus und damit ein Automorphismus. Weiter ist $\sigma_{|o} = \mathrm{id}$. Setze $\overline{L}_\mathfrak{P} = \overline{L} = \mathcal{O}/\mathfrak{P}$ und $\overline{K}_\mathfrak{p} = \overline{K} = o/\mathfrak{p}$.

   Dabei ist $\bar{\cdot} : \mathrm{Z}(\mathfrak{P})/\mathrm{Aut}(\overline{L}|\overline{K})$ mit $\sigma \mapsto \bar{\sigma}$ ein Gruppenhomomorphismus, denn $\overline{\sigma \circ \tau} = \overline{\sigma} \circ \overline{\tau}$. ◊

Definition 4.16.

Der Normalteiler $\mathrm{T}(\mathfrak{P}) = \mathrm{Kern}(\bar{\cdot})$ in $\mathrm{Z}(\mathfrak{P})$ heißt die Trägheitsgruppe von $\mathfrak{P}$.

Bemerkung 4.17.

1. Es gilt $\sigma \in \mathrm{T}(\mathfrak{P}) \Leftrightarrow \sigma(\mathfrak{P}) = \mathfrak{P}$ und $\sigma(\alpha) \equiv \alpha \bmod \mathfrak{P}$ für alle $\alpha \in \mathcal{O} \Leftrightarrow \sigma(\alpha) = \alpha \bmod \mathfrak{P}$ für alle $\alpha \in \mathcal{O}$, denn $\sigma(\mathfrak{P}) \subseteq \mathfrak{P}$ impliziert bereits die Gleichheit $\sigma(\mathfrak{P}) = \mathfrak{P}$.
2. $\mathrm{T}(\mathfrak{P}) = \{\sigma \in G \mid \sigma(\alpha) \equiv \alpha \bmod \mathfrak{p} \text{ für alle } \alpha \in \mathcal{O}\} \lhd \mathrm{Z}(\mathfrak{P})$, d.h. $\mathrm{T}(\mathfrak{P})$ ist ein Normalteiler von $\mathrm{Z}(\mathfrak{P})$, da Kern eines Homomorphismus.
3. $\mathcal{O}_\mathrm{Z} = K_\mathrm{Z} \cap \mathcal{O}$ ist der ganze Abschluss von o in K_Z.
4. $\mathfrak{P}$ ist die einzige Fortsetzung von $\mathfrak{P}_\mathrm{Z} = \mathfrak{P} \cap \mathcal{O}_\mathrm{Z}$ auf L, da $L|K_\mathrm{Z}$ Galoisch mit $\mathrm{Gal}(L|K_\mathrm{Z}) = \mathrm{Z}(\mathfrak{P})$ (Zerlegungsgruppe auch über K_Z). Falls $\mathfrak{P}' \cap \mathcal{O} = \mathfrak{P}_\mathrm{Z}$, so ist $\mathfrak{P}' = \tau(\mathfrak{P})$ für ein $\tau \in \mathrm{Gal}(L|K_\mathrm{Z}) = \mathrm{Z}(\mathfrak{P})$. Dann liegt τ in $\mathrm{Z}(\mathfrak{P})$ und damit $\tau(\mathfrak{P}) = \mathfrak{P}$, also $\mathfrak{P}_\mathrm{Z}\mathcal{O} = \mathfrak{P}^{e'}$ für irgendein e'.
5. Allgemein sind die Zerlegungsindizes e, f transitiv: Seien $K''|K'|K$ Galoisch und $\mathcal{O}'' \supseteq \mathcal{O}' \supseteq \mathcal{O}$ die zugehörigen ganzen Abschlüsse von o sowie $\mathfrak{P}'' \supseteq \mathfrak{P}' = \mathfrak{P}'' \cap \mathcal{O}' \supseteq \mathfrak{P} = \mathfrak{P}' \cap \mathcal{O}$, dann sind $\mathfrak{P}\mathcal{O} \subseteq \mathfrak{P}\mathcal{O}' = \cdots \mathfrak{P}'^{ee'} \subseteq \mathfrak{P}''^{e''e'}$, $\mathfrak{P}' \subseteq \mathfrak{P}'\mathcal{O}' = \mathfrak{P}''^{e'}$. Mit den Inklusionen $\mathcal{O}/\mathfrak{P} \subseteq \mathcal{O}'/\mathfrak{P}' \subseteq \mathcal{O}''/\mathfrak{P}''$ erhalten wir für die Erweiterungsgrade $[\mathcal{O}''/\mathfrak{P}'' : \mathcal{O}'/\mathfrak{P}'] \cdot [\mathcal{O}'/\mathfrak{P}' : \mathcal{O}/\mathfrak{P}] = [\mathcal{O}''/\mathfrak{P}'' : \mathcal{O}/\mathfrak{P}]$, d.h. $f(\mathfrak{P}''/\mathfrak{P}')f(\mathfrak{P}'/\mathfrak{P}) = f(\mathfrak{P}''/\mathfrak{P})$ und weiter $e(\mathfrak{P}''/\mathfrak{P}')e(\mathfrak{P}'/\mathfrak{P}) = e(\mathfrak{P}''/\mathfrak{P})$.
6. Zurück zum K_Z: Es gilt $e = e'$ und $f = [\mathcal{O}/\mathfrak{P} : \mathcal{O}_\mathrm{Z}/\mathfrak{P}_\mathrm{Z}] = f'$, denn $ef = |\mathrm{Z}(\mathfrak{P})| = [L : K_\mathrm{Z}] = e'f'$ und $e' \le e$, $f' \le f$, also $e = e'$ und $f = f'$. Insbesondere sind $e(\mathfrak{P}_\mathrm{Z}/\mathfrak{p}) = 1$ und $f(\mathfrak{P}_\mathrm{Z}/\mathfrak{p}) = 1$.
7. Volle Verzweigung, d.h. $e = f = 1$ und $r' = r$, liegt dann vor, wenn K_Z über K eine Galoiserweiterung ist. Dann ist $\mathrm{Z}(\mathfrak{P}) = \mathrm{Z}(\mathfrak{P}')$ für alle $\mathfrak{P}' \cap o = \mathfrak{p}$. Dies ist zum Beispiel dann der Fall, wenn die Galoisgruppe G abelsch ist. ◊

Definition 4.18.

$\mathfrak{P}$ heißt unverzweigt über $\mathfrak{p}$, wenn $e(\mathcal{O}/\mathfrak{p}) = 1$ und $(\mathcal{O}/\mathfrak{P})|(o/\mathfrak{p})$ separabel ist.

Bemerkung 4.19.

$\mathfrak{p}$ ist genau dann unverzweigt in $\mathcal{O}$, wenn alle $\mathfrak{P}_i$ unverzweigt über $\mathfrak{p}$ sind, wobei $\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$. ◊

Satz 4.20.

Sei $\overline{L} = \mathcal{O}/\mathfrak{P}$ separabel über $\overline{K} = o/\mathfrak{p}$. Dann ist $\bar{\cdot} : \mathrm{Z}(\mathfrak{P}) \to \mathrm{Gal}(\overline{L}/\overline{K})$ ein Epimorphismus und $|\mathrm{T}(\mathfrak{P})| = e$. Speziell gilt dies, wenn $\mathfrak{P}$ unverzweigt ist über $\mathfrak{p}$; in dem Fall ist $\bar{\cdot}$ ein Isomorphismus.

Beweis.

Es gilt $\overline{K} = \overline{K}_\mathrm{Z}$ und $\overline{L}|\overline{K}$ ist endlich und separabel. Sei $\overline{L} = \overline{K}(\overline{\alpha})$ für ein $\alpha \in \mathcal{O}$. Sei $g \in \mathcal{O}_\mathrm{Z}[X]$ das irreduzible Polynom von α über K_Z. Da g in L zerfällt, zerfällt $\overline{g}$ in $\overline{L}$. Die Nullstellen von g haben die Gestalt $\sigma(\alpha)$ mit $\sigma \in \mathrm{Z}(\mathfrak{P})$. Also sind auch die Nullstellen von $\overline{g}$ von der Gestalt $\overline{\sigma}(\overline{\alpha})$, d.h. die Abbildung $\bar{\cdot} : \mathrm{Z}(\mathfrak{P}) \to \mathrm{Gal}(\overline{L}|\overline{K})$ ist surjektiv. Weiter ist

$$|\mathrm{T}(\mathfrak{P})| = |\mathrm{Kern}(\bar{\cdot})| = \frac{|\mathrm{Z}(\mathfrak{P})|}{|\mathrm{Gal}(\overline{L}|\overline{K})|} = \frac{ef}{f} = e.$$

Ist speziell $\mathfrak{P}$ unverzweigt, dann ist $|\mathrm{Kern}(\bar{\cdot})| = |\mathrm{T}(\mathfrak{P})| = e(\mathcal{O}/\mathfrak{p}) = 1$, d.h. $\bar{\cdot}$ ist auch injektiv. □

Korollar 4.21.

Seien $L|K$ zwei Zahlkörper, d.h. endliche Erweiterungen von $\mathbb{Q}$. Ist $e(\mathfrak{P}/\mathfrak{p}) = 1$, so ist $\mathrm{Z}(\mathfrak{P})$ zyklisch.

Beweis.

Aus $e = 1$ folgt $\mathrm{Z}(\mathfrak{P}) \cong G(\overline{L}|\overline{K})$. Diese Gruppe ist zyklisch, da der Restklassenkörper $\overline{M}$ eines Zahlkörpers M endlich ist: $|\overline{M}| = [\mathcal{O}/\mathfrak{P} : \mathbb{Z}/\mathfrak{p}]$. □

Beispiel 4.22.

Seien $K = \mathbb{Q}$, $\mathfrak{p} = (p)$ und $\mathfrak{P}$ über G unverzweigt. Der erzeugende Automorphismus von $\mathrm{Gal}(\overline{L}|\mathbb{Z}_p)$ ist $x \mapsto x^p$, der Frobenius-Automorphismus von $\overline{L}|\mathbb{Z}_p$. Also wird $\mathrm{Z}(\mathfrak{P})$ erzeugt von σ mit $\sigma(\alpha) \equiv \alpha^p \bmod \mathfrak{P}$ für alle $\alpha \in \mathcal{O}$. Dann heißt $\mathrm{Frob}(\mathfrak{P}) = \sigma$ der Frobenius-Automorphismus von $\overline{L}|\mathbb{Q}$ zu $\mathfrak{P}$. Ist $G = \mathrm{Gal}(L|\mathbb{Q})$ abelsch, dann nennt man $\mathrm{Frob}(p) = \sigma$ auch den Frobenius-Automorphismus von p. ◊

Bemerkung 4.23.

1. Gilt $\sigma'(\alpha) \equiv \alpha^p \bmod \mathfrak{P}$, dann ist $\sigma^{-1}\sigma'(\alpha) \equiv \alpha \bmod \mathfrak{P}$, d.h. $\sigma = \sigma'$. Also ist σ eindeutig bestimmt (bzgl. $\mathfrak{P}$).
2. Ist $\mathrm{Gal}(L|\mathbb{Q})$ abelsch und $p \in \mathbb{Z}$ unverzweigt in L, dann gilt für $\mathfrak{P} \cap o = \mathfrak{p} = \mathfrak{P}' \cap o$, dass $\mathrm{Z}(\mathfrak{P}) = \mathrm{Z}(\mathfrak{P}')$ und $\mathrm{Frob}(\mathfrak{P}) = \mathrm{Frob}(\mathfrak{P}')$, denn sei $\mathfrak{P}' = \tau(\mathfrak{P})$. Dann gilt mit $\sigma(\beta) \equiv \beta^p \bmod \mathfrak{P}_i$ für $\alpha \in \mathfrak{P}$, dass
$$\sigma(\tau(\alpha)) - (\tau(\alpha))^p = \tau(\sigma(\alpha)) - \tau(\alpha^p) \in \tau(\mathfrak{P}) = \mathfrak{P}'.$$
Also ist σ in der Tat schon durch p eindeutig festgelegt.
3. Sei $[\overline{K} : \mathbb{Z}_p] = f_0$. Dann ist ein erzeugender Automorphismus der Galoisgruppe $\mathrm{Gal}(\overline{L}|\overline{K})$ gegeben durch $x \mapsto x^{p^{f_0}} = x^{\mathrm{N}(\mathfrak{p})}$. Also wird $\mathrm{Z}(\mathfrak{P})$ erzeugt von σ mit $\sigma(\alpha) \equiv \alpha^{\mathrm{N}(\mathfrak{p})} \bmod \mathfrak{P}$ ($\mathfrak{P}$ unverzweigt). ◊

Definition 4.24.

Sei $L|K$ Galoiserweiterung von Zahlkörpern. Dann heißt $K_\mathrm{T} = \mathrm{Fix}(\mathrm{T}(\mathfrak{P}))$ der Trägheitskörper von $\mathfrak{P}$.

Bemerkung 4.25.

1. Für eine Galoiserweiterung $L|K$ von Zahlkörpern sind $K \subseteq K_\mathrm{Z} \subseteq K_\mathrm{T} \subseteq L$ und $o \subseteq \mathcal{O}_\mathrm{Z} \subseteq \mathcal{O}_\mathrm{T} \subseteq \mathcal{O}$ sowie $\mathfrak{p} \subseteq \mathfrak{P}_\mathrm{Z} \subseteq \mathfrak{P}_\mathrm{T} \subseteq \mathfrak{P}$. Es gelten $[L : K_\mathrm{T}] = e$ und $[K_\mathrm{T} : K_\mathrm{Z}] = f$. Mit dem Epimorphismus $\bar{\cdot} : \mathrm{Gal}(L|K_\mathrm{T}) \to \mathrm{Gal}(\overline{L}|\overline{K}_\mathrm{T})$ gilt für $\sigma \in \mathrm{Gal}(L|K_\mathrm{T})$, dass $\sigma \in \mathrm{Kern}(\bar{\cdot}) \Leftrightarrow \sigma(\alpha) \equiv \alpha \bmod \mathfrak{P}$ für alle α, d.h. $\mathrm{Gal}(\overline{L}|\overline{K}_\mathrm{T}) = (\mathrm{id})$. Also ist $\overline{L} = \overline{K}_\mathrm{T}$, d.h. $f(\mathfrak{P}_\mathrm{T}/\mathfrak{P}_\mathrm{Z}) = f$ und damit $e(\mathfrak{P}_\mathrm{T}/\mathfrak{P}_\mathrm{Z}) = 1$.

2. Seien weiter $\mathfrak{p} \subseteq o$ unverzweigt in L $\mathfrak{P}_1 \mid \mathfrak{p}$ (d.h. $\mathfrak{p}$ liegt über $\mathfrak{p}$) und $n = [L : K]$. Dann gilt $\mathfrak{p} = \mathfrak{P}_1 \cdots \mathfrak{P}_r$ mit $r = \frac{n}{f}$ und f ist minimal mit $(\alpha^{N(\mathfrak{p})})^f \equiv \alpha \bmod \mathfrak{P}_1$ für alle $\alpha \in \mathcal{O}$, d.h. f ist die Ordnung des Frobenius-Automorphismus:

$$f = [\overline{L} : \overline{K}] = |\mathrm{Z}(\mathfrak{P}_1)| = \text{ Ordnung des Frobenius-Automorphismus } \sigma = \mathrm{Frob}(\mathfrak{P}_1).$$

3. Im abelschen Fall gilt für den Frobenius-Automorphismus $\sigma = \mathrm{Frob}(p)$ sogar, dass

$$\alpha^{\mathrm{N}(\mathfrak{p})} \equiv \sigma(\alpha) \bmod \mathfrak{p}\mathcal{O} = \mathfrak{P}_1 \cap \cdots \cap \mathfrak{P}_r = \mathfrak{P}_1 \cdots \mathfrak{P}_r. \qquad \Diamond$$

4.4. Zerlegung und Verzweigung in Kreisteilungskörpern

Wiederholung 4.26.

Seien $\zeta = \exp(\frac{2\pi i}{m})$ eine primitive m-te Einheitswurzel, $K = \mathbb{Q}$ und $L = K(\zeta)$. Dann gelten:

1. ζ^μ ist eine m-te Einheitswurzel. ζ^μ ist primitiv $\Leftrightarrow \nu\mu \equiv 1 \bmod m$ für ein $\mu \Leftrightarrow \overline{\nu} \in \mathbb{Z}_m^\times$.
2. Es gibt $\varphi(m) = |\mathbb{Z}_m^\times|$ viele primitive m-te Einheitswurzeln.
3. $f = \mathrm{Irr}(\zeta, \mathbb{Q})$ teilt das Polynom $X^m - 1 = (X-1)(X^{m-1} + X^{m-2} + \cdots + X + 1)$, also auch $X^{m-1} + \cdots + 1$.
4. $L|K$ ist eine Galoiserweiterung mit Galoisgruppe $G = \mathrm{Gal}(L|\mathbb{Q})$.
5. Die Abbildung $\nu : G \to \mathbb{Z}_m^\times$ mit $\sigma \mapsto \nu(\sigma)$, wobei $\sigma(\zeta) = \zeta^{\nu(\sigma)}$ primitive m-te Einheitswurzel ist ein Monomorphismus: $(\sigma \circ \tau)(\zeta) = \sigma(\zeta^{\nu(\tau)}) = \sigma(\zeta)^{\nu(\tau)} = \sigma^{\nu(\sigma)\nu(\tau)}$, also $\nu(\sigma \circ \tau) = \nu(\sigma)\nu(\tau)$ und aus $\nu(\sigma) \equiv 1 \bmod m.$ folgt $\sigma(\zeta) = \zeta$, d.h. $\sigma = \mathrm{id}$. Also ist G abelsch und es gilt $[L : K] \mid \varphi(m)$. $\Diamond$

Satz 4.27.

1. In L sind die Primzahlen p mit $p \nmid m$ unverzweigt.
2. Für $p^s \parallel m$, d.h. $p^s \mid m$ und $p^{s+1} \nmid m$ $(s \geq 1)$, gilt $p\mathcal{O}_L = [(1 - \zeta^{\frac{m}{p^s}})\mathcal{O}_L]^{\varphi(p^s)}$.

   Speziell ist p für $\varphi(p^s) > 1$ verzweigt.
3. Falls $s = 1$ und $p = 2$, so ist p unverzweigt in L.

Beweis.

1. Seien $\zeta^{(1)}, ..., \zeta^{(d)}$ alle Konjugierten von ζ, dann gilt $d = \deg f = [L : K]$. Für die Diskriminante $\mathrm{D}_\zeta = \mathrm{D}(1, \zeta, ..., \zeta^{d-1})$ gilt dann mit nach Van-der-Monde die Formel $\mathrm{D}_\zeta = \prod\{(\zeta^{(j)} - \zeta^{(k)})^2 \mid j < k\}$ mit $\zeta^{(j)} = \zeta^{\nu_j}$, vgl. den Beweis zu Satz 2.37. Damit folgt $(\zeta^{(j)} - \zeta^{(k)})\mathcal{O}_L = (1 - \zeta^{\nu_k - \nu_j})\mathcal{O}_L$, wobei $\zeta^{\nu_k - \nu_j}$ eine m-te Einheitswurzel ist. Weiter ist

$$X^{m-1} + \cdots + 1 = \prod_{\nu=1}^{m-1}(X - \zeta^\nu) \qquad \Longrightarrow \qquad m = \prod_{\nu=1}^{m-1}(1 - \zeta^\nu),$$

   also $(1 - \zeta^\nu) \mid m$ in $\mathcal{O}_L \Rightarrow \mathrm{N}(1 - \zeta^\nu) \mid \mathrm{N}(m) = m^d$ in $\mathbb{Z} \Rightarrow \mathrm{D}_\zeta^d = \mathrm{N}(D_\zeta) \mid m^l$ für ein $l \in \mathbb{N}$, $k \geq 1$. Wegen $\mathbb{Z} + \mathbb{Z}\zeta + \cdots + \mathbb{Z}\zeta^{d-1} \subseteq \mathcal{O}_L$ ist $\mathrm{D}_\zeta \in \mathrm{D}(\mathcal{O}_L)\mathbb{Z}$. Wäre nun p verzweigt, dann $p \mid \mathrm{dD}(\mathcal{O}_L)$, also auch $p \mid \mathrm{D}_\zeta$, d.h. $p \mid \mathrm{N}(\mathrm{D}_\zeta) \mid m^l$ und damit $p \mid m$, ein Widerspruch.

2. Gelte jetzt $p \mid m$, etwa $p^s \parallel m$. Wir setzen $\xi = \zeta^{\frac{m}{p^s}}$, dann sind $\xi^p = 1$ und $\xi^{p^{s-1}} \neq 1$. Dieses ξ ist eine Nullstelle von $X^{p^s} - 1 = Y^p - 1 = (Y-1)(Y^{p-1} + \cdots + 1)$ mit $Y = X^{p^{s-1}}$. Also ist ξ eine Nullstelle von $Y^{p-1} + \cdots + 1 = (X^{p^{s-1}})^{p-1} + \cdots + 1$; das gleiche gilt für alle ξ^ν mit $p \mid \nu$, wobei die Anzahl der ν gerade $\varphi(p^s) = p^{s-1}(p-1)$ beträgt. Damit gilt

$$Y^{p-1} + \cdots + 1 = \prod_{p \nmid \nu}(X - \xi^\nu) \qquad \Longrightarrow \qquad p = \prod_{p \nmid \nu}(1 - \xi)^\nu.$$

   Gilt $p \nmid \nu$, dann ist $1 - \xi^\nu$ assoziiert zu $1 - \xi$ in $\mathcal{O}_L$, denn $(1 - \xi^\nu)(1 - \xi)^{-1} = 1 + \cdots + \xi^{\nu-1} \in \mathcal{O}_L$. Wähle μ derart, dass $\xi = \xi^{\nu\mu}$, d.h. $\nu\mu \equiv 1 \bmod p^s$ bzw. $\overline{\nu} \in \mathbb{Z}_{p^s}^\times$. Also ist

$$(1 - \xi)(1 - \xi^\nu)^{-1} = (1 - (\xi^\nu)^\mu)(1 - xi^\nu)^{-1} = 1 + \cdots + (\xi^\nu)^{\mu-1} \in \mathcal{O}_L.$$

   Damit ist $p\mathcal{O}_L = ((1 - \xi)\mathcal{O}_L)^{\varphi(p^s)}$, d.h. p ist für $\varphi(p^s) > 1$ in L verzweigt.

3. Sei $m = 2u$ mit u ungerade. Dann ist $\zeta_u = e^{\frac{2\pi i}{u}}$ eine primitive u-te Einheitswurzel, also $-\zeta_u$ primitive $2u$-te Einheitswurzel, d.h. $\mathbb{Q}(\zeta_u) = \mathbb{Q}(\zeta_m)$. Mit (1) angewendet auf $\zeta = \zeta_u$ und $2 \nmid u$ folgt, dass 2 unverzweigt in L ist. □

Satz 4.28.
Gelte $p \nmid m$, dann $G \cong \mathbb{Z}_m^\times$, speziell $[L : \mathbb{Q}] = \varphi(m)$ und $\mathrm{Irr}(\zeta, \mathbb{Q}) = \prod_{1 \le \nu \le m-1}^{(\nu,m)=1} (X - \zeta^\nu) \in \mathbb{Z}[X]$.

Beweis.

Zu zeigen: Der Monomorphismus $\sigma \mapsto \overline{\nu(\sigma)} \in \mathbb{Z}_m^\times$ ist surjektiv. Sei also p teilerfremd zu m. Es genügt zu zeigen, dass es ein $\sigma \in G$ gibt mit $\zeta^{\nu(\sigma)} = \sigma^p$. Wegen $p \nmid m$ ist p unverzweigt in L, es gibt also einen Frobenius-Automorphismus σ mit $\sigma(\zeta) \equiv \zeta^p \bmod \mathfrak{P}$, wobei $\mathfrak{P} \cap \mathbb{Z} = (p)$. Also gilt $\zeta^{\nu(\sigma)} \equiv \zeta^p \bmod \mathfrak{P}$, d.h. $1 - \zeta^{\nu(\sigma)-p} \in \mathfrak{P}$ für alle $\mathfrak{P}$ mit $\mathfrak{P} \cap \mathbb{Z} = (p)$, also $1 - \zeta^{\nu(\sigma)-p} \in (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^1 = p\mathcal{O}_L$, d.h. $p \mid 1 - \zeta^{\nu(\sigma)-p}$ in $\mathcal{O}_L$ und damit $p \mid \mathrm{N}(1 - \zeta^{\nu(\sigma)-1}) \mid m^d$ in $\mathbb{Z}$, falls $1 - \zeta^{\nu(\sigma)-p} \neq 0$. Dies ist aber unmöglich, also $1 - \zeta^{\nu(\sigma)-p} = 0$, d.h. $\zeta^\nu = \zeta^p$. □

Bemerkung 4.29.

1. Für $p \nmid m$ definiert $\zeta \mapsto \zeta^p$ den Frobenius-Automorphismus von p. Seine Ordnung ist das kleinste f mit $p^f \equiv 1 \bmod m$.
2. Für jede Primzahl $p \equiv 1 \bmod m$ ist $f = 1$, d.h. p ist voll zerlegt in L. Ist dagegen $m = p^s$, so ist p in L voll verzweigt, d.h. $e = \varphi(m) = [L : \mathbb{Q}]$. ◊

4.5. Das quadratische Reziprozitätsgesetz

Satz 4.30. (quadratisches Reziprozitätsgesetz)
Sei $q \neq 2$ prim. Dann gelten $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ für $p \neq q$, $p \neq 2$ und $\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}}$.

Beweis.

Setze $q^* = q(-1)^{\frac{q-1}{2}}$. Dann gilt

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

Also ist zu zeigen: $\left(\frac{q^*}{p}\right) = \left(\frac{p}{q}\right)$. Betrachte dazu $L = \mathbb{Q}(\zeta)$ mit $\zeta = \exp(\frac{2\pi i}{q})$. Sei G die Galoisgruppe $\mathrm{Gal}(L|\mathbb{Q})$. Diese ist zyklisch von der Ordnung $q-1$, denn $G \cong \mathbb{Z}_q^\times$ via $\sigma \mapsto \zeta^{\nu(\sigma)}$; da $\mathbb{Z}_q$ ein endlicher Körper ist, ist seine multiplikative Gruppe zyklisch. Sei U die einzige Untergruppe vom Index 2, d.h. $|U| = \frac{q-1}{2}$. Dann $U \cong (\mathbb{Z}_q^\times)^2$, vgl. Aufgabe 31. Setzen wir $F = \mathrm{Fix}(U)$, dann $[F : \mathbb{Q}] = 2$ und $\mathrm{Gal}(F|\mathbb{Q}) = \{\mathrm{id}, \tau\}$. Also ist $F = \mathbb{Q}(\sqrt{d})$ mit $d \in \mathbb{Z}$ quadratfrei. Damit gilt $\mathrm{D}_F = 4d$ für $d \equiv 2, 3 \bmod 4$ und $\mathrm{D}_F = d$ im Fall $d \equiv 1 \bmod 4$.

1. *Es gilt $d = q^*$:* Sei p verzweigt in F, dann auch in L, d.h. $p = q$ mit $q \neq 2$. Mit $d \equiv 1 \bmod 4$, $d = \pm q$ folgt $d = q$ für $q \equiv 1 \bmod 4 \Leftrightarrow \mathrm{D}_F = q$ und $d = -q$ für $q \equiv 3 \bmod 4 \Leftrightarrow \mathrm{D}_F = -q$, d.h. $d = q(-1)^{\frac{q-1}{2}} = q^*$.
2. *Es gilt $\left(\frac{p}{q}\right) = 1 \Leftrightarrow p$ zerlegt in $\mathcal{O}_F$:* Wegen $p \neq q$ ist p unverzweigt in L, d.h. es gibt einen Frobenius-Automorphismus σ zu p, festgelegt durch $\sigma(\zeta) = \zeta^p$, $\sigma \mapsto \nu(\sigma) = p$. Weiter ist $\sigma(\alpha) \equiv \alpha^p \bmod \mathfrak{P}$ für alle $\alpha \in \mathcal{O}_L$. Damit $\sigma_F(\alpha) \equiv \alpha^p \bmod \mathfrak{P}$ für alle $\alpha \in \mathcal{O}_F$, d.h. $\sigma_{|F}$ ist der Frobenius-Automorphismus von p in F. Also $\left(\frac{p}{q}\right) = 1 \Leftrightarrow \overline{p} \in (\mathbb{Z}_q^\times)^2 \cong U \Leftrightarrow \sigma_F = \mathrm{id} \Leftrightarrow p$ zerlegt in $\mathcal{O}_F$.
3. *Es gilt $\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right)$:* Für $p \neq 2$ gilt: p zerlegt in F g.d.w. $\left(\frac{d}{q}\right) = 1$. Also $\left(\frac{p}{q}\right) = 1 \Leftrightarrow \left(\frac{q^*}{p}\right) = 1$.
4. *Es gilt $\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}}$:* Für $p = 2$ gilt: p zerlegt in F g.d.w. $d \equiv 1 \bmod 8 \Leftrightarrow (-1)^{\frac{d^2}{8}} = 1$, also $\left(\frac{2}{q}\right) = 1 \Leftrightarrow (-1)^{\frac{q^{*2}-1}{8}} = 1$, d.h. mit $q^{*2} = q^2$: $\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}}$. □

Lemma 4.31. (Nakayama)

Seien R ein Ring, A ein R-Ideal, das in allen maximalen Idealen von R enthalten ist, und M ein endlich erzeugter R-Modul mit $AM = M$. Dann gilt $M = \{0\}$.

Beweis.

Sei $M = R\omega_1 + \cdots + R\omega_n$. Aus $AM \supseteq M$ folgt $\omega_1 = a_1\omega_1 + \cdots + a_n\omega_n$ für gewisse $a_i \in A$, also $(1-a_1)\omega_1 = a_2\omega_2 + \cdots + a_n\omega_n$. Setze $M_{n-1} = R\omega_2 + \cdots + R\omega_n$, dann $1 - a_1 \in R^\times$, sonst gäbe es ein maximales Ideal J mit $1 - a_1 \in J$ und $A \subseteq J \Rightarrow a_1 \in J$, d.h. $1 \in J$, Widerspruch. Also $\omega_1 \in M_{n-1}$ u.s.w. bis $\omega_n \in M_1 = R\omega_1$, d.h. $M \subseteq M_0 = \{0\}$. □

Satz 4.32.

Sei $m = p^s$ mod ζ, ζ primitive m-te Einheitswurzel, dann $\mathcal{O}_L = \mathbb{Z} \oplus \mathbb{Z}\zeta \oplus \cdots \oplus \mathbb{Z}\zeta^{\varphi(m)-1}$ in $L = \mathbb{Q}(\zeta)$.

Beweis.

Für $\phi = \varphi(m)$ setze $M = \mathbb{Z} \oplus \mathbb{Z}\zeta \oplus \cdots \oplus \mathbb{Z}\zeta^{\phi-1} \subseteq \mathcal{O}_L$ und wähle $\omega_1, ..., \omega_\phi$ mit $\mathcal{O} = \mathbb{Z}\omega_1 \oplus \cdots \oplus \mathbb{Z}\omega_\phi$. Für geeignete $c_{ij} \in \mathbb{Z}$ ist $\zeta^{i-1} = c_{i1}\omega_1 + \cdots + c_{i\phi}\omega_\phi$. Also $\mathrm{D}(M) = \mathcal{D}(\mathcal{O}) \det^2(c_{ij})$ nach Lemma 3.20. Wir zeigen: $\mathrm{D}(M) = \mathrm{D}(\mathcal{O}) \Rightarrow |\det(c_{ij})| = 1$, dann bildet $1, \zeta, ..., \zeta^{n-1}$ eine $\mathbb{Z}$-Basis von $\mathcal{O}$. Nach Satz 4.27 gilt $\mathrm{D}(M) = \mathrm{D}_\zeta \mid p^l$ für ein $l \in \mathbb{N}$, d.h. $\det(c_{ij}) = \pm p^h$. Wir zeigen $h = 0$ durch den Nachweis $\det(c_{ij}) \in \mathbb{Z}_{(p)}^\times$. Wir lokalisieren dazu nach $\mathfrak{p} = (p) = o\mathbb{Z}$, d.h. mittels der multiplikativen Menge $S = \mathbb{Z}\backslash p\mathbb{Z}$. Dann $o_\mathfrak{p} = \mathbb{Z}_{(p)}$ und es ist zu zeigen: $M_\mathfrak{p} = S^{-1}M = \mathbb{Z}_{(p)} \oplus \cdots \oplus \mathbb{Z}_{(p)}\zeta^{n-1}$ und $\mathcal{O}_\mathfrak{p} = S^{-1}\mathcal{O} = \mathbb{Z}_{(p)}\omega_1 \oplus \cdots \oplus \mathbb{Z}_{(p)}\omega_n$ erfüllen $M_\mathfrak{p} = \mathcal{O}_\mathfrak{p}$; dies liefert $h = 0$. Es gilt $k = o/\mathfrak{p} =$ mod $o_\mathfrak{p}/\mathfrak{p}o_\mathfrak{p} = \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$, vgl. den Beweis zum Fortsetzungssatz 4.3, und $\dim(\mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p}) = n = [L : \mathbb{Q}] = \varphi(m) = \varphi(p^s) = (p-1)p^{s-1}$. Weiter ist $n = \varphi(m)$, $\mathfrak{p}\mathcal{O}_\mathfrak{p} = \mathfrak{P}^e \subseteq \mathfrak{P}^{e-1} \subseteq \cdots \subseteq \mathfrak{P} \subseteq \mathcal{O}_\mathfrak{p}$, da $\mathfrak{p} = (p)$ in $\mathcal{O}_\mathfrak{p}$ voll verzweigt ist. Wir erhalten die Kette $\mathcal{O}_\mathfrak{p}/\mathfrak{P}^e \supseteq \mathfrak{P}/\mathfrak{P}^e \supseteq \mathfrak{P}^2/\mathfrak{P}^e \supseteq \cdots \supseteq \mathfrak{P}^e/\mathfrak{P}^e = \{0\}$ von k-Vektorräumen. Setze $\omega = 1 - \zeta$, dann $\mathfrak{P} = \omega\mathcal{O}_\mathfrak{p}$. Wir schreiben $\overline{a} = a + \mathfrak{P}^e = a + \mathfrak{p}\mathcal{O}_\mathfrak{p}$, dann $\omega^\nu \subseteq \mathfrak{P}^\nu \backslash \mathfrak{P}^{\nu-1}$, d.h. $\overline{\omega} \in \mathfrak{P}^{\nu-1}/\mathfrak{P}^e$, also bilden die $\overline{\omega}^0, ..., \overline{\omega}^{e-1}$ eine k-Basis von $\mathcal{O}_\mathfrak{p}/\mathfrak{P}^e \backslash \mathfrak{P}^{\nu-1}/\mathfrak{P}^e$, d.h. $\overline{\zeta}^0, ..., \overline{\zeta}^{e-1}$ bildet eine k-Basis von $\mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p}$. Daraus folgt $\mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p} = o_\mathfrak{p}/\mathfrak{p}\overline{\zeta}^0 \oplus \cdots \oplus o_\mathfrak{p}/\mathfrak{p}\overline{\zeta}^{e-1}$, d.h. $\mathcal{O}_\mathfrak{p} = M_\mathfrak{p} + \mathfrak{p}\mathcal{O}_\mathfrak{p}$. Also ist $\mathfrak{p}\mathcal{O}_\mathfrak{p}/M_\mathfrak{p} = \mathcal{O}_\mathfrak{p}/M_\mathfrak{p}$ als $o_\mathfrak{p}$-Modul. Mit $R = o_\mathfrak{p}$ und $\mathfrak{p} = \mathfrak{p}o_\mathfrak{p}$ einziges maximales Ideal folgt aus Nakayamas Lemma 4.31: $\mathcal{O}_\mathfrak{p}/M_\mathfrak{p} = \{0\}$, also $\mathcal{O}_\mathfrak{p} = M_\mathfrak{p}$. □

Bemerkung 4.33.

Der Satz gilt auch für allgemeines m. ◊

4.6. Der Satz von Kummer

Definition 4.34.

$p \in \mathbb{P}$ ist regulär, wenn p nicht die Klassenzahl des p-ten Kreisteilungskörpers teilt: $p \nmid \mathrm{h}(\mathbb{Q}(\exp(\frac{2\pi i}{p})))$.

Bemerkung 4.35.

1. Es gibt unendlich viele irreguläre Primzahlen (Satz von Jensen, 1915). Man vermutet, dass ca. 60% der Primzahlen regulär sind. Alle Primzahlen kleiner als 100 sind regulär außer 37, 59, 67.
2. Für die Primzahlen 3, 5, 7, 11, 13, 17, 19 gilt $\mathrm{h} = 1$.
3. Kummer bewies die Fermatsche Vermutung für alle regulären Primzahlen [8]. Wir studieren in diesem Kapitel die Teilaussage, dass $X^p + Y^p = Z^p$ für $p \geq 3$ regulär keine nicht-triviale Lösung (x, y, z) besitzt mit $p \mid xyz$.
4. Es genügt, die allgemeine Gleichung $X^n + Y^n = Z^n$, $n \in \mathbb{N}$, nur für $n \in \mathbb{P}$ und $n = 4$ zu betrachten, denn gilt $n = mp$ mit $p \in \mathbb{P}$, so ist $x^n + y^n = z^n \Leftrightarrow (x^m)^p + (y^m)^p = (z^m)^p$. ◊

Bemerkung 4.36.

Seien $L = \mathbb{Q}(\zeta)$ mit $\zeta = \exp(\frac{2\pi i}{m})$ primitive m-te Einheitswurzel und $m = p^s$ mit $p \in \mathbb{P}\backslash\{2\}$. Dann ist $L \subseteq \mathbb{C}$ und $L|\mathbb{Q}$ ist eine Galoiserweiterung mit $[L:\mathbb{Q}] = \varphi(m) = p^{s-1}(p-1)$. Weiter gelten:

1. $p\mathcal{O}_L = (1-\zeta)^{\varphi(m)}\mathcal{O}_L$ ist voll verzweigt.
2. $1-\zeta$ ist prim in $\mathcal{O}_L$.
3. $\mathcal{O}_L = \mathbb{Z} \oplus \zeta\mathbb{Z} \oplus \cdots \oplus \zeta^{\varphi(m)-1}\mathbb{Z} = \mathbb{Z}[\zeta]$.
4. $1, \zeta, ..., \zeta^{\varphi(m)-1}$ bildet eine $\mathbb{Z}_p$-Basis von $\mathcal{O}_L/p\mathcal{O}_p$.
5. $p \nmid \nu \Rightarrow 1-\zeta \sim 1-\zeta^\nu$ in $\mathcal{O}_L$.

Sei $\rho : \mathbb{C} \to \mathbb{C}$ die komplexe Konjugation, dann ist $\rho \in \mathrm{Gal}(L|\mathbb{Q})$ mit $\mathrm{Ord}(\rho) = 2$. Bezeichne $F = \mathrm{Fix}(\rho)$ den zugehörigen Fixkörper, dann gilt $= L \cap \mathbb{R}$. Weiter sind $\rho(\zeta) = \zeta^{-1}$ und $\mathbb{Q}(\zeta + \zeta^{-1}) \subseteq L \cap \mathbb{R} = F$. ζ ist eine Nullstelle von $X^2 - (\zeta + \zeta^{-1})X + 1$ und aus Gradgründen folgt $F = \mathbb{Q}(\zeta + \zeta^{-1})$. ◊

Satz 4.37.

Die Einheiten ϵ von $\mathcal{O}_L$ sind von der Gestalt $\epsilon = (-\zeta)^r\epsilon_0$ mit $r \in \mathbb{Z}$ und $\epsilon_0 \in \mathcal{O}_F^\times$.

Beweis.

Sei zunächst ϵ selbst eine Einheitswurzel in L. ξ primitive n-te Einheitswurzel aus L, dann $\varphi(n) \mid \varphi(m)$. Also ist die Gruppe aller Einheitswurzeln in L endlich, d,h, von der Gestalt $\xi^{\mathbb{Z}}$. $-\zeta \in \xi^{\mathbb{Z}}$ ist $2m$-te Einheitswurzel, d.h. $2m \mid n$, denn $\mathrm{Ord}(-\zeta) = 2m$ und $\varphi(n) \mid \varphi(m) = p^{s-1}(p-1)$, d.h. $n = 2mn_0 = 2p^s n_0$ und $\varphi(n) = 1p^{s-1}(p-1)u \Rightarrow u = 1 \Rightarrow n_0 = 1 \Rightarrow n = 2m$. Damit ist $\epsilon \in \xi^{\mathbb{Z}} = (-\zeta)^{\mathbb{Z}}$; setze $\epsilon_0 = 1$.

Sei nun $\epsilon \in \mathcal{O}_L^\times$ beliebig. Nach Bemerkung 4.36 (3) ist $\epsilon = a_0 + a_1\zeta + \cdots + a_{\varphi(m)-1}\zeta^{\varphi(m)-1} = -f(\zeta)$ mit $a_0, ..., a_{\varphi(m)-1} \in \mathbb{Z}$. Dann $\rho(\epsilon) = f(\rho(\zeta)) = f(\zeta^{-1})$. Zu $\mu = \epsilon\rho(\epsilon)^{-1} \in \mathcal{O}_L^\times$ betrachte die Konjugierten $\mu^{(1)}, ..., \mu^{(\varphi(m)-1)}$ von μ:

$$\mu^{(j)} = \frac{f(\zeta)^{(j)}}{f(\zeta^{-1})^{(j)}} = \frac{f(\zeta^{(j)})}{f(\zeta^{(j)^{-1}})} = \frac{f(\zeta^{\nu_j})}{f(\zeta^{(-\nu_j)})} = \frac{f(\zeta^{(\nu_j)})}{\rho(f(\zeta^{(\nu_j)}))}$$

mit $\nu_j \in \mathbb{N}$, $0 \le \nu_j \le m$. Also $\mu^{(j)}\rho(\mu^{(j)}) = 1$, d.h. $|\mu^{(j)}| = 1$. Mit Aufgabe 29 folgt, dass μ eine Einheitswurzel ist, also $\mu(-\zeta)^{\mathbb{Z}}$, etwa $\mu = (-\zeta)^r = (-1)^r\zeta^r$. r ist gerade, sonst $\mu = -\zeta^r \Rightarrow \epsilon = -\zeta^r\rho(\epsilon)$. Setze $\omega = 1-\zeta$; mit Bemerkung 4.36 (1) folgt, dass $p\mathcal{O}_L = (\omega\mathcal{O}_L)^{\varphi(m)}$ und damit ω prim. Wegen $\zeta \equiv 1 \bmod \omega$ ist $\zeta^t \equiv 1 \bmod \omega$ mit $t \in \mathbb{Z}$, also $\epsilon = f(\zeta) \equiv a_0 + \cdots + a_{\varphi(m)-1} = M \bmod \omega$. Zugleich ist auch $\rho(\epsilon) = f(\zeta^{-1}) \equiv M \bmod \omega$, d.h. $\epsilon = (-\zeta^r)\rho(\epsilon)$, also $M \equiv -M \bmod \omega$ und damit $2M \equiv 0 \bmod \omega$. Da ω prim mit $\omega \nmid 2$, ist dann $\epsilon \equiv 0 \bmod \omega$, d.h. $b\epsilon \in \omega\mathcal{O}_L \subsetneq \mathcal{O}_L$, ein Widerspruch dazu, dass ϵ eine Einheit ist. Also ist $r = 2t$ gerade, $\mu = \zeta^r = \zeta^{2t}$. Dann $\epsilon = \zeta^t\rho(\epsilon)\rho(\zeta^t)^{-1}$, d.h. $\epsilon\zeta^{-t} = \rho(\epsilon)\rho(\zeta^t)^{-1} \in \mathbb{R} \cap L = F$. Setze $\epsilon_0 = \rho(\frac{\epsilon}{\zeta^t})$, dann $\epsilon\mu\rho(\epsilon) = \zeta^t\epsilon \in \mathcal{O}_F^\times$. □

Satz 4.38. (Kummer, erster Fall, 1849)

Ist p eine reguläre Primzahl und gilt für $x, y, z \in \mathbb{Z}$, dass $x^p + y^p = z^p$, dann $p \mid xyz$.

Beweis.

Setze $L = \mathbb{Q}(\zeta)$ mit $\zeta = \exp(\frac{2\pi i}{p})$. Angenommen, es gäbe $x, y, z \in \mathbb{Z}$ mit $x^p + y^p = z^p$ und $p \nmid xyz$. O.B.d.A. gelte $(x, y) = 1$; setze $u = \frac{x}{-y}$. Dann

$$x^p + y^p = (-y)^p(u^p - 1) = (-y)^p \prod_{n=0}^{p-1}(u - \zeta^n) = \prod_{n=0}^{p-1}(x + \zeta y) = z^p.$$

Gilt $n \not\equiv m \bmod p$, dann ist $(x + \zeta^n y, x + \zeta^m y) = (1)$, denn setze $A = (x + \zeta^n y, x + \zeta^m y)$. Dann gilt $(x+\zeta^m y)-(x+\zeta^n y) = \zeta^m(1-\zeta^{n-m})y \in A$ und damit $(x+\zeta^m y)\zeta^n-(x+\zeta^n y)\zeta^m = -\zeta^m(1-\zeta^{n-m})x \in A$, also auch $(1-\zeta)y \in A$ und $(1-\zeta)x \in A$, vgl. Bemerkung 4.36 (5). Wegen $(x, y) = 1$ gibt es $a, b \in \mathbb{Z}$ mit $ax + by = 1$, also $(1-\zeta) = a(1-\zeta)x + b(1-\zeta)y \in A$ und da nach Bemerkung 4.36 (1) gilt

$a-\zeta \mid p$, folgt $p \in A$. Damit $x+y = (x+\zeta^{n-m}y)+(1-\zeta^{n-m})y \in A$ (beachte: $n-m \not\equiv 0 \bmod p$) und daher $(x+y)^p \equiv x^p+y^p = z^p \not\equiv 0 \bmod p$, speziell $x+y \not\equiv 0 \bmod p$ in $\mathbb{Z}$, also $(x+y,p) \subseteq A$ und damit $A = (1) = \mathcal{O}_L$. Also $(\mathfrak{P}_1 \cdots \mathfrak{P}_r)^p = (z)^p = (z^p) = (x^p+y^p) = (x+\zeta^0 y)\cdots(x+\zeta^{p-1}y)$. Wegen $n \not\equiv m \bmod p$ und $\mathrm{ggT}((x+\zeta^n y),(x+\zeta^m y)) = (1)$ folgt aus $\mathfrak{P}_i \mid x+\zeta^n y$, dass auch $\mathfrak{P}_i \nmid (x+\zeta^m y)$, also $(x+\zeta^n y) = B_n^p$ für ein Ideal B_n von $\mathcal{O}_L$. Es gelten $\mathrm{Ord}(B_i) \mid p$ in der Idealklassengruppe und $\mathrm{Ord}(B_i) \mid \mathrm{h}(L)$. Wegen $(p, \mathrm{h}(L)) = 1$ folgt $\mathrm{Ord}(B_i) = 1$, d.h. jedes B_i ist ein Hauptideal.

Es gibt ein $\alpha \in \mathcal{O}_L$ und eine Einheit $\epsilon \in \mathcal{O}_L^\times$ mit $x+\zeta y = \epsilon\alpha^p$, da $(x+\zeta y) = (\alpha)^p = (\alpha^p)$, d.h. $(x+\zeta y) \sim \alpha^p$. Analog gilt $x^p+(-z)^p = (-y)^p$ und $(x,y) = 1$ impliziert $(x,z) = 1$. Analog gibt es ein $\alpha' \in \mathcal{O}_L$ und ein $\epsilon' \in \mathcal{O}_L'^\times$ mit $x-\zeta z = \alpha'\epsilon'$. Wegen Bemerkung 4.36 (3) ist $\alpha = a_0 + \cdots + a_{p-2}\zeta^{p-2}$ mit $a_0, ..., a_{p-2} \in \mathbb{Z}$. Also gilt $\alpha^p \equiv a_o^p + a_1^p\zeta^p + \cdots + a_{p-2}^p\zeta^{p(p-2)} \equiv M \bmod p$ mit $M = a_o^p + \cdots + a_{p-2}^p$, da $\zeta^p = 1$. Weiter ist $\epsilon = \zeta^s\eta$ mit $\eta \in \mathbb{R} \cap \mathcal{O}_L^\times$ nach Satz 4.37, also $x+\zeta y \equiv \zeta^s\eta M = \zeta^s\xi \bmod p$ mit $\zeta = \eta M \in \mathbb{R} \cap \mathcal{O}_L$. Bezeichne ρ die komplexe Konjugation $a+ib \mapsto a-ib$, dann ist $\zeta^{-s}(x+\zeta y) \equiv \xi \bmod p$ und damit $(*)$ $\rho(\zeta^{-s}(x+\zeta y)) = \zeta^s(x+\zeta^{-1}y) \equiv \rho(\xi) = \xi \bmod p$, d.h. $\zeta^{-s}(x+\zeta y) \equiv \zeta^s(x+\zeta^{-1}y) \bmod p$. Wir erhalten die Gleichung $x\zeta^s + y\zeta^{s-1} - x\zeta^{-s} - y\zeta^{1-s} \equiv 0 \bmod p$. Beachte: Nach Bemerkung 4.36 (4) gilt für $b_0, ..., b_{p-2} \in \mathbb{Z}$, dass

$$b_0 + b_1\zeta + \cdots + b_{p-2}\zeta^{p-2} \equiv 0 \bmod p \quad \Longleftrightarrow \quad b_0, ..., b_{p-2} \equiv 0 \bmod p.$$

1. $s, s-1, -s, 1-s$ können nicht modulo p paarweise inkongruent und zugleich inkongruent zu $p-1$ sein, sonst $x, y \equiv 0 \bmod p$, was $(x,y) = 1$ widerspricht.
2. Sei $p \geq 5$ (den Fall $p = 3$ betrachten wir separat). Ist genau ein Exponent kongruent 0 mod p, dann ist ζ wegen $X^p - 1 = (X-1)(X^{p-1}+X^{p-2}+\cdots+1)$ Nullstelle des Polynoms $X^{p-1}+X^{p-2}+\cdots+1 = 0$. Wir ersetzen ζ^{p-1} durch $-1-\zeta-\cdots-\zeta^{p-2}$ in $(*)$ (beachte: $p-1$ sind mindestens 4 Summanden). Mindestens ein Koeffizient der resultierenden Summe ist $\pm x$ oder $\pm y$. Mit Bemerkung 4.36 (4) folgt: $p \mid x$ oder $p \mid y$ im Widerspruch zu $p \nmid xyz$.
3. Sind schließlich zwei Exponenten kongruent modulo p, dann führt $s \equiv s-1$ zu dem Widerspruch $1 \equiv 0 \bmod p$, $s \equiv -s \Rightarrow s \equiv 0 \bmod p$ kann wegen $s-1 \not\equiv p-1 \bmod p$ nicht sein, weiterhin scheidet $s-1 \equiv 1-s \Rightarrow s-1 \equiv 0 \bmod p$ wegen $-s \not\equiv p-1 \bmod p$ aus und auch $-s \equiv 1-s \bmod p$ ist nicht möglich.
4. Also gilt entweder $s \equiv 1-s \bmod p$ oder $s-1 \equiv -s \bmod p$. Wegen $2s \equiv 1 \equiv p+1 \bmod p$ folgt mit $(*)$ daraus aber:

$$s \equiv \frac{p+1}{2} \bmod p \quad \Longrightarrow \quad (x-y)\zeta^{\frac{p+1}{2}} + (y-x)\zeta^{\frac{p-1}{2}} \equiv 0 \bmod p \quad \Longrightarrow \quad x \equiv y \bmod p.$$

   Zugleich erhalten wir aber aus $x-\zeta z = \alpha'^p\epsilon'$ mit $\alpha' \in \mathcal{O}_L$, $\epsilon' \in \mathcal{O}_L^\times \cap \mathbb{R}$, dass $x \equiv -z \bmod p$ und wegen $x^p+y^p = z^p$ folgt $x^p+x^p = (x+x)^p = (-x)^p \bmod p$, d.h. $3x^p \equiv 0 \bmod p$ und damit $p \mid x$, Widerspruch.
5. Bleibt also nur noch der Fall $p = 3$. Es ist $x+y \equiv x^3+y^3 = z^3 \equiv z \bmod 3$, $X^p \equiv X \bmod p$. Es gibt also ein $a \in \mathbb{Z}$ mit $z = x+y+3a$. Damit $x^3+y^3 = (x+y+3a)^3 \equiv x^3+y^3+3x^2y+3xy^2 \bmod 9$, d.h. $0 \equiv 3x^2y+3xy^2 \bmod 9$, d.h. $0 \equiv 3(x^2y+xy^2)$, also $x^2y+xy^2 \equiv 0 \bmod 3$. Daraus folgt aber $0 \equiv xy(x+y) \equiv xyz \bmod 3$ und auch das ist ein Widerspruch. □

5. Der Primzahlsatz von Dirichlet

5.1. Dirichlet-Dichten und Dirichlet-Reihen

Definition 5.1.

Seien f_1, f_2 stetig für $x > 1$. Wir setzen $f_1 \sim f_2$, falls $\sup\limits_{x>1} |f_1(x) - f_2(x)| < \infty$.

Sei $M \subseteq \mathbb{P}$. Gibt es ein $\delta \in [0,1]$ mit $\wp(M) = \sum\limits_{p \in M} \frac{1}{p^x} \sim \delta\ell$, so heißt $\delta(M)$ die Dirichlet-Dichte von M.

Sei $(a,m) = 1$. Die natürliche Dichte von $M = \{p \in \mathbb{P} \mid p \equiv a \bmod m\}$ ist

$$\eta(M) = \lim_{r\to\infty} \frac{\sharp\{p \in M \mid p \leq r\}}{\sharp\{p \in \mathbb{P} \mid p \leq r\}} > 0.$$

Bemerkung 5.2.

1. Die Reihe $\ell(x) = \sum\{p^{-x} \mid p \in \mathbb{P}\}$ ist stetig für $x > 1$ und konvergiert gleichmäßig für $x > x_0 > 1$. Für $x = 1$ ist sie divergent.
2. Falls existent, so ist $\delta(M)$ eindeutig bestimmt: $|\delta_1\ell(s) - \delta_2\ell(s)|$ ist beschränkt für $x \searrow 1 \Rightarrow \delta_1 = \delta_2$.
3. Ist M endlich, dann ist $\delta(M) = 0$. Für $M \subseteq M'$ ist $\delta(M) \leq \delta(M')$. Aus $M \cap M' = \emptyset$ folgt $\delta(M) + \delta(M') = \delta(M \cap M')$.
4. Gilt $\wp(M) \sim \delta\ell$, dann lässt sich δ berechnen mittels $\delta = \lim\limits_{x\searrow 1} \frac{\wp(M)}{\ell}(x) = \lim\limits_{x\searrow 1} \frac{\wp(M)}{\wp(\mathbb{P})}(x)$.
5. Falls existent, stimmen die Dirichlet-Dichte und die natürliche Dichte überein:

$$\eta(M) = \lim_{r\to\infty} \frac{\#\{p \in M \mid p \leq r\}}{\#\{p \in \mathbb{P} \mid p \leq r\}} = \lim_{x\searrow 1} \frac{\sum\{p^{-x} \mid x \in M\}}{\sum\{p^{-x} \mid x \in \mathbb{P}\}} = \delta(M). \qquad \lozenge$$

Definition 5.3.

Seien $(a_n)_{n\in\mathbb{N}} \subseteq \mathbb{C}$ und $s \in \mathbb{C}$. Dann heißt $f(s) = \sum\limits_{n=1}^{\infty} \frac{a_n}{n^s}$ eine Dirichlet-Reihe.

Bemerkung 5.4.

1. Das Produkt zweier Dirichlet-Reihen berechnet sich über die diskrete Faltung der Koeffizientenfolgen:

$$\left(\sum_{n=1}^{\infty} \frac{a_n}{n^s}\right)\left(\sum_{m=1}^{\infty} \frac{b_m}{m^s}\right) = \sum_{n=1}^{\infty}\sum_{m=1}^{\infty} \frac{a_n b_m}{(nm)^s} = \sum_{k=1}^{\infty} \frac{1}{k^s} \sum_{n|k} a_n b_{\frac{k}{n}} = \sum_{k=1}^{\infty} \frac{(a * b)_k}{k^s}.$$

2. Nach dem Identitätssatz für Dirichlet-Reihen [12], Satz 3.3, sind die Koeffizienten von f eindeutig.
3. Der Konvergenzbereich einer Dirichlet-Reihe f ist stets eine rechte Halbebene. Ist $(a_n)_{n\in\mathbb{N}}$ beschränkt, so ist $f(s)$ für $\mathrm{Re}(s) > 1$ absolut konvergent und holomorph. Sind sogar die Partialsummen von $(a_n)_{n\in\mathbb{N}}$ beschränkt, so konvergiert $f(s)$ für alle $\mathrm{Re}(s) > 0$. Ist $(a_n)_{n\in\mathbb{N}} \subseteq \mathbb{R}$ mit $a_n > 0$ für alle $n \in \mathbb{N}$, dann ist die Konvergenzhalbebene von f durch eine Singularität auf der reellen Achse begrenzt. Beweise finden sich in [10], Kapitel 3.

5.2. Die Riemannsche ζ-Funktion

Definition 5.5.

Die Dirichlet-Reihe $\zeta(s) = \sum\limits_{n=1}^{\infty} \frac{1}{n^s}$ heißt Riemannsche Zeta-Funktion.

Bemerkung 5.6.

1. ζ ist holomorph und konvergiert gleichmäßig für $\mathrm{Re}(s) > 1$.
2. $\zeta(s) = \frac{1}{s-1} + \phi(s)$ für eine Funktion ϕ, die für $\mathrm{Re}(s) > 0$ holomorph ist.
3. Es gelten für $\mathrm{Re}(s) > 1$ die beiden Darstellungsformeln

$$\zeta(s) = \prod_{p\in\mathbb{P}} \frac{1}{1 - \frac{1}{p^s}}, \qquad \log(\zeta(s)) = \sum_{p\in\mathbb{P}} \frac{1}{p^s} + \psi(s),$$

   wobei $\psi(s)$ für $\mathrm{Re}(s) > 1$ beschränkt ist. Genauer:

$$\log\zeta(s) = \sum_{p\in\mathbb{P}} -\log\left(1 - \frac{1}{p^s}\right) = \sum_{p\in\mathbb{P}}\sum_{k=1}^{\infty} \frac{1}{kp^{ks}} \leq \sum_{p\in\mathbb{P}} \frac{1}{p^s} + \sum_{p\in\mathbb{P}} \frac{2}{p^2} \sim \sum_{p\in\mathbb{P}} \frac{1}{p^s}.$$

4. Die Riemannsche Vermutung besagt: $\mathrm{Re}(s) = \frac{1}{2}$ für alle nicht-trivialen Nullstellen s von ζ. $\lozenge$

Bemerkung 5.7. (Eulersche Produktformel)

Sei $s \in \mathbb{C}$ mit $\mathrm{Re}(s) > 1$. Dann gilt

$$\prod_{p\in\mathbb{P}} \frac{1}{1-\frac{1}{p^s}} = \left(1+\frac{1}{2^s}+\frac{1}{4^s}+\cdots\right)\left(1+\frac{1}{3^s}+\frac{1}{9^s}+\cdots\right)\cdots = 1+\frac{1}{2^s}+\frac{1}{3^s}+\cdots. \qquad \Diamond$$

5.3. L-Reihen und Charaktere

Definition 5.8.

$\chi : \mathbb{Z} \to \mathbb{C}$ heißt Zahlcharakter oder modularer Charakter, falls für $m \geq 2$ gelten:

$$\chi(a) = \chi(b) \text{ für } a \equiv b \bmod m, \qquad \chi(ab) = \chi(a)\chi(b), \qquad \chi(1) = 1 \text{ und } \chi(p) = 0 \text{ für alle } p \mid m.$$

Sei G eine Gruppe. $\chi : G \to \mathbb{C}^\times$ heißt ein Gruppencharakter, falls $\chi(ab) = \chi(a)\chi(b)$.

Bemerkung 5.9.

1. Ist $(a,m) = 1$, dann $\chi(a) \neq 0$: $ab \equiv 1 \bmod m \Rightarrow \chi(a)\chi(b) = \chi(1) = 1 \Rightarrow \chi(a) \neq 0$.
2. Für $(a,m) > 1$ ist $\chi(a) = 0$: $p \mid (a,m) \Rightarrow \chi(a) = \chi(p)\chi(\frac{a}{p}) = 0$.
3. Sei G eine abelsche Gruppe der Ordnung n und $\hat{G} = \mathrm{Hom}(G, \mathbb{Z}^\times)$. Dann gelten $|\hat{G}| = n$ und
$$\sum_{a\in G} \chi(a) = \begin{cases} n, & \chi = 1 \\ 0 & \text{sonst} \end{cases}, \qquad \sum_{\chi\in\hat{G}} \chi(n) = \begin{cases} n, & n = 1 \\ 0 & \text{sonst} \end{cases}. \qquad \text{(Charakterrelationen)}$$
4. Die Zahlcharaktere entsprechen bijektiv den Gruppencharakteren von $\mathbb{Z}_m^\times$: Seien $G = \mathbb{Z}_m^\times$ die Einheitengruppe des Restklassenrings, $G = \{\bar{a} \in \mathbb{Z}_m \mid (a,m) = 1\}$, und $\chi \in \hat{G}$, dann definiert die Fortsetzung $\chi \in \mathbb{Z}_m$, $\chi(\bar{a}) = 0$ für $(a,m) \neq 1$ einen Zahlcharakter $\mathbb{Z} \to \mathbb{C}$ via $a \mapsto \chi(\bar{a})$.
5. Der zum Gruppencharakter $\chi_0 = \mathrm{id} \in \hat{G}$ gehörige Zahlcharakter $\chi_0 = \mathbb{Z} \to \mathbb{C}$ ist gegeben durch $\chi_0(a) = 1$ für $(a,m) = 1$ und $\chi_0(a) = 0$ sonst. χ_0 heißt der Hauptcharakter. $\Diamond$

Definition 5.10.

Die Dirichlet-Reihe $L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ heißt die L-Reihe des Zahlcharakters χ.

Bemerkung 5.11.

$L(s,\chi)$ ist für $\mathrm{Re}(s) > 1$ absolut konvergent und damit holomorph: Es gilt

$$\sum_{n=1}^{\infty} \left|\frac{\chi(n)}{n^s}\right| \leq \sum_{n=1}^{\infty} \frac{1}{|n^s|} \leq \sum_{n=1}^{\infty} \frac{1}{n^{\mathrm{Re}(s)}} = \zeta(\mathrm{Re}(s)). \qquad \Diamond$$

Lemma 5.12.

Die L-Reihe $L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ besitzt die Produktdarstellung $L(s,\chi) = \prod_{p\in\mathbb{P}} \frac{1}{1-\frac{\chi(p)}{p^s}}$.

Beweis.

Sei $M = \{n \in \mathbb{N} \mid n \text{ ist nur durch Primzahlen} \leq N \text{ teilbar}\}$. Für die Partialprodukte gilt nach der Entwicklung der Faktoren als geometrische Reihen

$$P_N(s,\chi) = \prod_{\substack{p\in\mathbb{P}\\ p\leq N}} \frac{1}{1-\chi(p)p^{-s}} = \prod_{\substack{p\in\mathbb{P}\\ p\leq N}} \sum_{k=0}^{\infty} \frac{\chi(p)^k}{p^{ks}} = \sum_{p\in M} \frac{\chi(n)}{n^s},$$

also $|L(s,\chi) - P_N(s,\chi)| \leq \sum_{n>N} \frac{1}{n^s} \longrightarrow 0$ für $N \to \infty$. $\square$

Lemma 5.13.

Das Produkt $I(s) = \prod_\chi L(s,\chi)$ über alle Dirichletreihen erfüllt $I(s) \geq 1$ für alle $s \geq 1$.

Beweis.

Wir zeigen, dass der Logarithmus von I nichtnegativ ist:

$$\log I(s) = \prod_\chi \prod_p \frac{1}{1-\chi(p)p^{-1}} = \sum_\chi \sum_p \sum_k \frac{1}{k}\left(\frac{\chi(p)}{p^s}\right)^k = \sum_p \sum_k \frac{1}{kp^{ks}} \sum_\chi \chi(p^k) \geq 0,$$

da $\sum_\chi \chi(p^k) = \varphi(m)$ für $p^k \equiv 1 \bmod m$ und 0 sonst nach der Charakterrelation. □

Lemma 5.14.

Die Dirichletreihe zu I hat nur Koeffizienten in $\mathbb{R}_0^+$, ist also holomorph für alle $\mathrm{Re}(s) > 0$.

Beweis.

Zu $\overline{p} \in \mathbb{Z}_m^\times$ setze $f(p) = \mathrm{Ord}(\overline{p})$, $d = \mathrm{Ord}(\mathbb{Z}_m^\times) = \varphi(m)$ und $r(p) = \frac{d}{f(p)}$, dann folgt mit Aufgabe 50:

$$I(s) = \prod_\chi \prod_p \frac{1}{1-\chi(p)p^{-s}} = \prod_{p\nmid m} \prod_\chi \frac{1}{1-\chi(p)p^{-s}} = \prod_{p\nmid m} \frac{1}{(1-p^{-sf(p)})^{r(p)}} = \prod_{p\nmid m} \left(\sum_{k=0}^\infty p^{-skf(p)}\right)^{r(p)}.$$ □

Bemerkung 5.15.

Mit der Riemannschen ζ-Funktion besthehen die Zusammenhänge

$$L(s,\chi_0) = \zeta(s) \prod_{p\,|\,m} \left(1-\frac{1}{p^s}\right), \qquad I(s) = \zeta(s) \prod_{\chi\neq\chi_0} L(s,\chi) \prod_{p\,|\,m} \left(1-\frac{1}{p^s}\right).$$

Speziell hat $L(s,\chi_0)$ in $s=1$ einen Pol erster Ordnung. ◊

Satz 5.16.

Für alle Charaktere $\chi \neq \chi_0$ gilt $L(1,\chi) \neq 0$.

Beweis.

Angenommen, es gibt ein $\chi \neq \chi_0$ mit $L(1,\chi) = 0$. Da $L(s,\chi_0)$ in $s=1$ einen Pol erster Ordnung hat, konvergiert die Dirichletreihe zu I also für alle $\mathrm{Re}(s) > 0$. Mit der Ungleichung $(1-a^r) \geq (1-a)^r$ und $s = \frac{1}{d}$ folgt dann die Konvergenz von

$$\prod_{p\nmid m} \frac{1}{1-p^{-sf(p)r(p)}} = \prod_{p\nmid m} \frac{1}{1-p^{-1}} \sim \prod_{p\in\mathbb{P}} \frac{1}{1-p^{-1}} = \zeta(1) = \sum_{n=1}^\infty \frac{1}{n},$$

ein Wiederspruch. □

5.4. Der Dirichletsche Primzahlsatz

Satz 5.17. (Dirichletscher Primzahlsatz)

Sei $(a,m) = 1$. Dann gilt $\delta(\{p \in \mathbb{P} \mid p \equiv a \bmod m\}) = \frac{1}{\varphi(m)}$.

Beweis.

Setze $f_\chi(s) = \sum_{p\in\mathbb{P}} \frac{\chi(p)}{p^s}$. Wegen $f_\chi(s) \sim \log L(s,\chi)$ ist dann $f_\chi(s)$ für $s \searrow 1$

1. im Fall $\chi \neq \chi_0$ beschränkt, da $L(1,\chi) \neq 0$, d.h. der Logarithmus fortsetzbar ist auf $s=1$, und
2. im Fall $\chi = \chi_0$ unbeschränkt: $f_{\chi_0} = \sum_{p\in\mathbb{P}} \frac{1}{p^s} - \sum_{p\,|\,m} \frac{1}{p^s} \sim \sum_{p\in\mathbb{P}} \frac{1}{p^s}$.

Setze $M = \{p \in \mathbb{P} \mid p \equiv a \bmod m\}$. Wegen $\sum_\chi \chi(\overline{pa}^{-1}) = \varphi(m)$ für $\overline{pa}^{-1} \equiv 1 \bmod m$ und 0 sonst ist

$$f_{\chi_0}(s) \sim f_{\chi_0}(s) + \sum_{\chi \neq \chi_0} \frac{f_\chi(s)}{\chi(a)} = \sum_\chi \frac{f_\chi(s)}{\chi(a)} = \sum_\chi \sum_{p \nmid m} \frac{\chi(p)}{\chi(a) p^s} = \sum_{p \nmid m} \sum_\chi \frac{\chi(\overline{pa}^{-1})}{p^s} = \sum_M \frac{\varphi(m)}{p^s},$$

also $\sum_M \frac{1}{p^s} \sim \frac{1}{\varphi(m)} \sum_{\mathbb{P}} \frac{1}{p^s}$ und damit $\delta(M) = \frac{1}{\varphi(m)}$. □

Korollar 5.18.

Zu $(a, m) = 1$ gibt es stets unendlich viele Primzahlen $p \in \mathbb{P}$ mit $p \equiv a \bmod p$.

Bemerkung 5.19.

Im Zusammenhang mit der Riemannschen ζ-Funktion ergibt sich [14]

$$\sum_{p \in M} \frac{1}{p^s} \sim \frac{1}{\varphi(m)} \sum_{p \in \mathbb{P}} \frac{1}{p^s} \sim \frac{1}{\varphi(m)} \log \zeta(s) \sim \frac{1}{\varphi(m)} \log \frac{1}{s-1}.$$ ◊

Übungsaufgaben

Aufgabe 1.

Bestimmen Sie die Lösungsmengen der folgenden linearen Kongruenzen:

$25x \equiv 1 \bmod 29$,	$5x \equiv 2 \bmod 26$,	$6x \equiv 15 \bmod 21$,
$36x \equiv 8 \bmod 102$,	$34x \equiv 60 \bmod 98$,	$140x \equiv 133 \bmod 301$.

Aufgabe 2.

Bestimmen Sie die Lösungsmengen der folgenden linearen diophantischen Gleichungen:

$$4x + 51y = 9, \qquad 12x + 25y = 331.$$

Aufgabe 3.

Seien $m, n \in \mathbb{N}$ mit $m \geq 1$ und $m \mid n$. Zeigen Sie

1. Die Zuordnung $\rho : \mathbb{Z}_n \to \mathbb{Z}_m$ mit $k + n\mathbb{Z} \mapsto k + m\mathbb{Z}$ definiert einen Ringhomomorphismus.
2. Durch ρ wird ein surjektiver Gruppenhomomorphismus $\varphi : \mathbb{Z}_n^\times \to \mathbb{Z}_m^\times$ induziert.

Aufgabe 4.

Seien a, b, c drei paarweise verschiedene natürliche Zahlen. Zeigen Sie, dass es eine natürliche Zahl n gibt, so dass $a + n$, $b + n$ und $c + n$ paarweise teilerfremd sind.

Aufgabe 5. (Eine Aufgabe aus dem alten China)

Eine wilde Horde von 17 Piraten hatte bei einem Raubzug einen Sack voller Goldmünzen erbeutet. Nach einem gleichmäßigen Verteilen der Beute blieben zwei Münzen übrig. Uneinig darüber, was mit diesen Münzen zu geschehen hätte, gerieten sie in einen erbitterten Streit, in dessen Verlauf ein Pirat getötet wurde. Erneut wurden die Münzen gleichmäßig unter den noch lebenden Piraten verteilt, wobei diesmal zehn Münzen übrig blieben. Da die Piraten unfähig waren, dieses Problem mit friedlichen Mitteln zu lösen, musste noch ein Pirat sein Leben lassen. Glücklicherweise ließ sich nun die Beute ohne Rest verteilen.

Wie viele Münzen hatten die Piraten mindestens erbeutet?

Aufgabe 6.

1. Zeigen Sie, dass $(x^2 - 13)(x^2 - 17)(x^2 - 221) \equiv 0 \bmod p$ für jede Primzahl p lösbar ist.
2. Ist 2007 ein quadratischer Rest modulo 1291?

Aufgabe 7.

1. Seien $p_1, ..., p_n$ paarweise verschiedene Primzahlen, $\nu_1, ..., \nu_n \in \mathbb{N}$ und $a_1, ..., a_n, b_1, ..., b_n \in \mathbb{Z}$ derart, dass $(a_i, p_i^{\nu_i}) \mid b_i$ für $i = 1, ..., n$.

   Zeigen Sie, dass eine Lösung des folgenden Kongruenzsystems existiert:

   $$a_1 \equiv b_1 \bmod p_1^{\nu_1}, \qquad ... \qquad a_n x \equiv b_n \bmod p_n^{\nu_n}$$

2. Bestimmen Sie die Lösungsmenge des folgenden Kongruenzsystems:

   $$7x \equiv 2 \bmod 9, \qquad 11x \equiv 3 \bmod 25, \qquad 13x \equiv 5 \bmod 19$$

Aufgabe 8.

Für den Ring der ganzen Gaußschen Zahlen $\mathbb{Z}[i]$ definieren wir $N : \mathbb{Z}[i] \to \mathbb{N}_0$ durch $a + bi \mapsto a^2 + b^2$.

1. Zeigen Sie, dass N multiplikativ ist, d.h. dass für beliebige $x, y \in \mathbb{Z}[i]$ gilt: $N(xy) = N(x)N(y)$.
2. Bestimmen Sie alle Einheiten von $\mathbb{Z}[i]$.
3. Zeigen Sie, dass $\mathbb{Z}[i]$ ein euklidischer Ring bzgl. N ist.
4. Als euklidischer Ring ist $\mathbb{Z}[i]$ insbesondere faktoriell. Erklären Sie, wie sich das mit der Gleichung $(2 + i)(2 - i) = 5 = (1 + 2i)(1 - 2i)$ verträgt.

Aufgabe 9.

Zeigen Sie: Eine Primzahl p ist genau dann Summe zweier Quadrate natürlicher Zahlen, wenn $p \equiv 1 \bmod 4$.

Aufgabe 10.

Seien R ein kommutativer Ring, M ein R-Modul. Zeigen Sie, dass folgende Aussagen äquivalent sind:

1. Jede aufsteigende Kette von Untermoduln $U_1 \subseteq U_2 \subseteq \cdots$ in M wird stationär.
2. Jede nichtleere Menge von Untermoduln von M enthält ein maximales Element.
3. M ist Noethersch, d.h. jeder Untermodul von M ist endlich erzeugt.

Aufgabe 11.

Seien R ein kommutativer Ring und M ein R-Modul. Zeigen Sie:

1. Ist U ein Untermodul von M, so ist M genau dann Noethersch, wenn U und M/U Noethersch sind.
2. Sind R Noethersch und M endlich erzeugt, so ist auch M Noethersch.
3. Finden Sie einen endlich erzeugten Modul mit einem nicht endlich erzeugten Untermodul.

Aufgabe 12.

Zeigen Sie, dass $\frac{\sqrt{2}}{3}$ algebraisch über $\mathbb{Q}$, aber keine ganze algebraische Zahl ist.

Aufgabe 13.

Sei R ein in seinem Quotientenkörper K ganz abgeschlossener Integritätsbereich. Zeigen Sie:

1. Sind $f, g \in K[X]$ normiert mit $fg \in R[X]$, so sind auch $f, g \in R[X]$.
2. Sind $L|K$ Körpererweiterung & $\alpha \in L$ ganz über R, so sind α algebraisch über K & $\mathrm{Irr}(\alpha, K) \in R[X]$.
3. $\alpha = \sqrt{\frac{-1+\sqrt{-3}}{2}} \in \mathbb{Z}$ ist ganz über $\mathbb{Z}[\sqrt{-3}]$, aber $\mathrm{Irr}(\alpha, \mathbb{Q}(\sqrt{-3})$ liegt nicht in $\mathbb{Z}[\sqrt{-3}][X]$.

Aufgabe 14.

Seien $K|\mathbb{Q}$ eine endliche Körpererweiterung vom Grad $[K:\mathbb{Q}] = n$, $\tilde{K}$ ein algebraischer Abschluss von K und $\sigma_1, ..., \sigma_n : K \hookrightarrow \tilde{K}$ die n verschiedenen Einbettungen von K in $\tilde{K}$. Zeigen Sie:

1. Ist $\alpha \in \mathcal{O}_K$, so sind auch die Konjugierten $\sigma_1(\alpha), ..., \sigma_n(\alpha)$ in $\tilde{K}$ ganz über $\mathbb{Z}$.
2. Für $\alpha_1, ..., \alpha_n \in K$ ist $d = \det((\sigma_i(\alpha_j))_{1\le i\le n}^{1\le j\le n})^2 \in \mathbb{Q}$.
3. Für $\alpha_1, ..., \alpha_n \in \mathcal{O}_K$ gilt $d \in \mathbb{Z}$.
4. Berechnen Sie d im Fall $\alpha_j = \alpha^{j-1}$.

Aufgabe 15.

Betrachten Sie die Ideale $\mathfrak{p} = (2, 1+\sqrt{-5})$, $\mathfrak{q} = (3, 1+\sqrt{-5})$, $\mathfrak{r} = (3, 1-\sqrt{-5})$ im Dedekind-Ring $\mathbb{Z}[\sqrt{-5}]$.

1. Zeigen Sie, dass $(6) = \mathfrak{p}^2\mathfrak{q}\mathfrak{r}$ die eindeutige Zerlegung von (6) in Primideale von $\mathbb{Z}[\sqrt{-5}]$ ist.
2. Bestimmen Sie die Zerlegung in Primideale von $(1+\sqrt{-5})$ und von $(1-\sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$.

Aufgabe 16.

1. Finden Sie eine Bijektion zwischen der Potenzmenge der Primzahlen und den Teilringen von $\mathbb{Q}$.
2. Zeigen Sie, dass jeder Teilring von $\mathbb{Q}$ ganz abgeschlossen ist.

Aufgabe 17.

Ein Primideal eines Ringes heißt minimal, wenn es vom Nullideal verschieden ist und außer dem Nullideal kein anderes Primideal echt enthält. Sei R ein faktorieller Ring. Zeigen Sie:

1. Jedes nicht prime Hauptideal $\neq \{0\}$ in R, ist minimal und jedes minimale Primideal ist Hauptideal.

Sei nun jedes vom Nullideal verschiedene Primideal in R maximal ist. Zeigen Sie:

3. Jedes Primideal ist ein Hauptideal und jedes Ideal ist in einem echten Hauptideal enthalten.
4. R ist ein Hauptidealring.

Aufgabe 18.

Seien R kommutativer Ring mit 1 und $n \in \mathbb{N}$. Bezeichne $\mathfrak{M}_n(R)$ den Ring der $n \times n$-Matrizen über R.

1. Sei $A \in \mathfrak{M}_n(R)$. Zeigen Sie: A ist invertierbar in $\mathfrak{M}_n(R) \Leftrightarrow \det(A) \in R^\times$.
2. Sei M ein freier R-Modul mit Basis $v_1, ..., v_n$ und seien $w_1, ..., w_n \in M$ mit

$$w_1 = a_{11}v_1 + \cdots + a_{1n}v_n, \qquad ... \qquad w_n = a_{n1}v_1 + \cdots + a_{nn}v_n$$

   für gewisse $a_{ij} \in R$, $1 \le i, j \le n$. Zeigen Sie: $w_1, ..., w_n$ ist eine Basis von $M \Leftrightarrow \det(a_{ij})_{1\le j\le n}^{1\le i\le n} \in R^\times$.

Aufgabe 19.

Sei R ein kommutativer Ring mit 1. Zeigen Sie, dass für einen endlich erzeugten R-Modul und ein multiplikatives System S von R, d.h. $S \subseteq R$ mit $1 \in S$ und $SS \subseteq S$, gilt:

1. Auf $M \times S$ wird eine Äquivalenzrelation erklärt durch $(m, s) \sim (n, t) \iff \exists u \in S : u(mt - ns) = 0$. Wir bezeichnen die Äquivalenzklasse von (m, s) mit $\frac{m}{s}$.
2. Auf der Menge der Äquivalenzklassen $S^{-1}M = (M \times S)/_\sim$ wird eine Gruppenstruktur eingeführt durch $\frac{m}{s} + \frac{n}{t} = \frac{mt+ns}{st}$.
3. Eine Skalarmultiplikation mit Skalaren aus R wird auf $S^{-1}M$ definiert durch $r\frac{m}{s} = \frac{rm}{s}$.
4. Mit der additivien Verknüpfung und der Skalarmultiplikation wird $S^{-1}M$ zu einem R-Modul. $S^{-1}M$ wird die Lokalisierung von M nach S genannt.
5. $S^{-1}R$ wird ein kommutativer Ring mit 1 via $\frac{a}{s}\frac{b}{t} = \frac{ab}{st}$ und ein $S^{-1}R$-Modul durch $\frac{r}{s}\frac{m}{t} := \frac{rm}{st}$.

Aufgabe 20.

Seien R ein kommutativer Ring mit 1 und $S \subseteq R$ multiplikativ. Zeigen Sie:

1. $\iota : M \to S^{-1}M$, $m \mapsto \frac{m}{1}$, ist ein R-Modul-Homomorphismus mit Kern $\{m \in M \mid \exists s \in S : sm = 0\}$.
2. Seien R' ein Ring und $\varphi : R \to T'$ ein Ringhomomorphismus mit $\varphi(S) \subseteq (R')^\times$. Dann existiert genau ein Ringhomomorphismus $\psi : S^{-1}R \to R'$ mit $\varphi = \psi \circ \iota$, wobei $\iota : R \to S^{-1}R$, $r \mapsto \frac{r}{1}$.
3. Die Primideale $\mathfrak{p}$ von R mit $\mathfrak{p} \cap S = \emptyset$ entsprechen vermöge den Abbildungen $I \mapsto S^{-1}I$ und $J \mapsto \iota^{-1}(J)$ eineindeutig den Primidealen von $S^{-1}R$.
4. Die Nicht-Nullteiler in R bilden ein multiplikatives System S. R nullteilerfrei impliziert $S^{-1}R$ Körper.

Aufgabe 21.

Seien $\alpha = \sqrt[3]{2} \in \mathbb{R}$ und $R = \mathbb{Z}[\alpha]$. Zeigen Sie:

1. Es gilt die Gleichheit $5R = (5, \alpha + 2)(5, \alpha^2 + 3\alpha - 1)$.
2. Es gibt einen surjektiven Ringhomomorphismus $\mathbb{Z}[T]/(5, T^2 + 3T - 1) \to R/(5, \alpha^2 + 3\alpha - 1)$.
3. R stimmt nicht mit $(5, \alpha^2 + 3\alpha - 1)$ überein.

Aufgabe 22.

Sei $R \subseteq R'$ eine Erweiterung von Dedekind-Ringen. Zeigen Sie die Äquivalenz folgender Aussagen:

1. Für jedes Ideal A von R gilt $AR' \cap R = A$.
2. Für Ideale A, B von R mit $AR' \subseteq BR'$ gilt stets $A \subseteq B$.
3. Für jedes Primideal $\mathfrak{p}$ von R ist $\mathfrak{p}R' \neq R'$.

Finden Sie jeweils ein einfaches Beispiel für eine Erweiterung von Dedekind-Ringen, für die diese Aussagen erfüllt sind bzw. nicht erfüllt sind.

Aufgabe 23.

Sei R ein kommutativer Ring mit 1. Zeigen Sie die Äquivalenz der folgenden Aussagen:

1. R ist ein lokaler Ring, d.h. R besitzt genau ein maximales Ideal.
2. $R \backslash R^\times$ ist ein Ideal von R.
3. R besitzt ein maximales Ideal $\mathfrak{m}$, für welches $1 + \mathfrak{m} \subseteq R^\times$ gilt.

Zeigen Sie, dass für jedes Primideal $\mathfrak{p}$ von R der Ring $R_\mathfrak{p}$ lokal ist.

Aufgabe 24.

Sei $R \subseteq R'$ eine ganze Ringerweiterung. Zeigen Sie:

1. Ist $R' \subseteq R''$ eine ganze Ringerweiterung, so ist auch $R \subseteq R''$ ganz.
2. Für jedes Ideal I von R' ist $R/(I \cap R) \hookrightarrow R'/I$ eine ganze Ringerweiterung.
3. Für jedes Primideal $\mathfrak{p}$ von R ist die Erweiterung $S^{-1}R \subseteq S^{-1}R'$ mit $S = R \backslash \mathfrak{p}$ ganz.
4. Ist $R \subseteq R'$ ganze Erweiterung von Dedekind-Ringen, dann gilt $\mathfrak{p}R' \neq R'$ für jedes Primideal $\mathfrak{p}$ von R.

Aufgabe 25.

Seien R ein Integritätsbereich, Ω die Menge der maximalen Ideale von R. Zeigen Sie:

1. $R = \bigcap \{R_\mathfrak{m} \mid \mathfrak{m} \in \Omega\}$.
2. R ist ganz abgeschlossen $\iff$ für jedes Primideal $\mathfrak{p}$ von R ist $R_\mathfrak{p}$ ganz abgeschlossen.
3. Es gibt einen lokalen Ring, der nicht ganz abgeschlossen ist.

Aufgabe 26.

Zeigen Sie für einen algebraischen Zahlkörper K und seinen Ring der ganzen Zahlen $\mathcal{O}_K$:

1. $\mathcal{O}_K^\times = \{\alpha \in \mathcal{O}_K \mid \mathrm{N}_{K|\mathbb{Q}}(\alpha) = \pm 1\}$.
2. $\mathcal{O}_K$ ist bzgl. der Abbildung $|\mathrm{N}_{K|\mathbb{Q}}|$ euklidisch $\iff \forall x \in K : \exists a \in \mathcal{O}_K : |\mathrm{N}_{K|\mathbb{Q}}(x-a)| < 1$.
3. Sei nun $K = \mathbb{Q}(\sqrt{-d})$ quadratfrei. Bestimmen Sie $\mathcal{O}_K^\times$ und alle quadratfreien $d \in \mathbb{N}$, für die $\mathcal{O}_K$ euklidisch bzgl. der Normabbildung $\mathrm{N}_{K|\mathbb{Q}}$ ist.

Aufgabe 27.

Sei K ein algebraischer Zahlkörper vom Grad n über $\mathbb{Q}$. Zeigen Sie:

1. Für jede Basis $(\alpha_1, ..., \alpha_n)$ des $\mathbb{Z}$-Moduls $\mathcal{O}_K$ hat $\mathrm{D}_{K|\mathbb{Q}}(\alpha_1, ..., \alpha_n)$ den selben Wert.
2. Sind $\alpha_1, ..., \alpha_n \in \mathcal{O}_K$, sodass $\mathrm{D}_{K|\mathbb{Q}}(\alpha_1, ..., \alpha_n)$ quadratfrei ist, so ist $(\alpha_1, ..., \alpha_n)$ eine $\mathbb{Z}$-Basis von $\mathcal{O}_K$.
3. Ist $n = 2$ und (α_1, α_2) eine $\mathbb{Z}$-Basis von $\mathcal{O}_K$, so gilt $K = \mathbb{Q}(\sqrt{D_{K|\mathbb{Q}}(\alpha_1, \alpha_2)})$.

Aufgabe 28.

Seien $f \in \mathbb{Z}[X]$ irreduzibel und normiert vom Grad n, $\alpha \in \mathbb{Z}$ Nullstelle von f und $K = \mathbb{Q}(\alpha)$. Zeigen Sie:

1. $\mathrm{D}_{K|\mathbb{Q}}(1, \alpha, ..., \alpha^{n-1}\} = (-1)^{\frac{n(n-1)}{2}} \mathrm{N}_{K|\mathbb{Q}}(f'(\alpha))$.
2. Ist $f = X^3 + aX + b$, $a, b \in \mathbb{Z}$, so gilt $\mathrm{D}_{K|\mathbb{Q}}(1, \alpha, \alpha^2) = -(4a^3 + 27b^2)$.
3. Für $a, b \in \{\pm 1\}$ ist $f = X^3 + aX + b \in \mathbb{Z}[X]$ irreduzibel über $\mathbb{Z}$ und $(1, \alpha, \alpha^2)$ eine $\mathbb{Z}$-Basis von $\mathcal{O}_K$.

Aufgabe 29.

Zeigen Sie: $\zeta \in \mathbb{Z}$ ist eine Einheitswurzel $\Leftrightarrow$ ζ ist ganz über $\mathbb{Z}$ und $|\bar{\zeta}| = 1$ für alle Konjugierten von ζ.

Aufgabe 30.

Für jede messbare Menge $\mathcal{B} \subseteq \mathbb{R}^n$ und jede Matrix $A \in \mathbb{R}^{n \times n}$ gelte $\mathrm{vol}(A\mathcal{B}) = \det(A) \cdot \mathrm{vol}(\mathcal{B})$, wobei $A \cdot \mathcal{B} = \{A \cdot b \mid b \in \mathcal{B}\}$.

1. Seien $a, b \in \mathbb{Z}$ und $m \in \mathbb{N}_{>0}$ sowie $\mathcal{B} = \{x \in \mathbb{R}^4 \mid \|Ax\|^2 < 2m\}$ mit

$$A = \begin{pmatrix} m & 0 & a & -b \\ 0 & m & b & a \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

   Zeigen Sie, dass $\mathrm{vol}(\mathcal{B}) > 16$ ist.

2. Zeigen Sie unter Verwendung des Minkowskischen Gitterpunktsatzes, dass $p \in \mathbb{N}$ Summe von vier Quadraten in $\mathbb{Z}$ ist, wenn es $u, v \in \mathbb{Z}$ mit $-1 \equiv u^2 + v^2 \bmod m$ gibt.

Aufgabe 31.

1. Zeigen Sie, dass für jede Primzahl $p \in \mathbb{Z}$ im Körper $\mathbb{Z}_p$ jedes Element Summe von zwei Quadraten ist.
2. Zeigen Sie, dass jede natürliche Zahl Summe von vier Quadratzahlen ist.

Aufgabe 32.

Seien $K = \mathbb{Q}(\sqrt{-6})$. Beweisen Sie die folgenden Aussagen:

1. In $\mathcal{O}_K$ gelten $(2) = (2, \sqrt{-6})^2$ und $(3) = (3, \sqrt{-6})^2$.

2. Die einzigen Ideale in $\mathcal{O}_K$ mit Norm 2 oder 3 sind $(2, \sqrt{-6})$ und $(3, \sqrt{-6})$.
3. $(2, \sqrt{-6})$ und $(3, \sqrt{-6})$ sind keine Hauptideale.
4. In jeder Idealklasse von $\mathcal{O}_K$ liegt ein ganzes Ideal A mit $\mathrm{N}(A) \leq 3$.
5. Die Klassenzahl $\mathrm{h}(\mathcal{O}_K)$ von K beträgt 2.

Aufgabe 33.

Seien R' ein kommutativer Ring mit 1 und R ein Teilring von R', sodass der Quotient der additiven Gruppe R/R' die endliche Ordnung n hat. Zeigen Sie, dass für jede Primzahl $p \in \mathbb{Z}$, welche n nicht teilt, die natürliche Abbildung $fR/pR \to R'/pR'$ mit $f(r + pR) = r + pR'$ ein Isomorphismus ist.

Aufgabe 34.

Sei K ein algebraischer Zahlkörper vom Grad n über $\mathbb{Q}$. Zeigen Sie:

1. Für jedes Ideal A von $\mathcal{O}_K$ gilt $\mathrm{N}(A)\mathcal{O}_K \subseteq A$.
2. Für jedes Primideal $\mathfrak{p} \neq (0)$ von $\mathcal{O}_K$ ist $\mathrm{N}(\mathfrak{p}) = p^r$ für ein $r \in \mathbb{N}$
3. Im Fall $p \nmid n$ hat dieses r den Wert 1.

Aufgabe 35.

Ein Integritätsbereich R mit $K = \mathrm{Quot}(R)$ heißt Bewertungsring, wenn $\forall x \in K^\times : x \in R$ oder $x^{-1} \in R$.

Beweisen Sie die folgenden Aussagen über Bewertungsringe:

1. Ein Integritätsbereich ist ein Bewertungsring $\Leftrightarrow$ die Menge der R-Ideale ist durch $\subseteq$ total geordnet.
2. Bewertungsringe sind ganz abgeschlossen und lokal.
3. Die Bewertungsringe von $\mathbb{Q}$ sind die Lokalisierungen von $\mathbb{Z}$ nach (p) mit p prim oder $p = 0$.

Aufgabe 36.

Sei K ein Körper, dann heißt $v : K \to \overline{\mathbb{Z}} = \mathbb{Z} \cup \{\infty\}$ diskrete Bewertung von K, falls für alle $x, y \in K$

$$v(x) < \infty \Leftrightarrow x = 0, \qquad v(xy) = v(x) + v(y), \qquad v(x + y) \geq \min\{v(x), v(y)\}.$$

Dabei ist stets $\infty + m = m + \infty = \infty$ für alle $m \in \overline{\mathbb{Z}}$ und $m < \infty$ für alle $m \in \mathbb{Z}$.

Seien K ein algebraischer Zahlkörper und $\mathfrak{P}$ ein Primideal von $\mathcal{O}_K$. Weiter sei $x \in K^\times$, d.h. $x = ab^{-1}$ für gewisse $a, b \in \mathcal{O}_K$. Die Primidealzerlegungen von (a) und (b) besitzen die Gestalt $(a) = \mathfrak{P}^r\mathfrak{Q}_1^{r_1} \cdots \mathfrak{Q}_n^{r_n}$ und $(b) = \mathfrak{P}^s\mathfrak{Q}_1^{s_1} \cdots \mathfrak{Q}_n^{s_n}$, $r, r_1, ..., r_n, s, s_1, ..., s_n \in \mathbb{N}$. Dann hat das gebrochene Ideal (x) die eindeutige Zerlegung $(x) = \mathfrak{P}^m\mathfrak{Q}_1^{m_1} \cdots \mathfrak{Q}_n^{m_n}$, $m, m_1, ..., m_n \in \mathbb{Z}$. Wir bezeichnen die eindeutig bestimmte Zahl $m \in \mathbb{Z}$ mit $f_{\mathfrak{P}}(x)$ und setzen $v_{\mathfrak{P}}(0) = \infty$. Wir erhalten so eine Abbildung $v_{\mathfrak{P}} : K \to \overline{\mathbb{Z}}$.

Seien nun K ein algebraischer Zahlkörper und $\mathfrak{p}$ ein Primideal von $\mathcal{O}_K$. Zeigen Sie:

1. Die Abbildung $v_{\mathfrak{p}}$ ist eine diskrete Bewertung von K.
2. $\mathcal{O}_{\mathfrak{p}} = \{x \in K \mid v_{\mathfrak{p}} > 0\}$ ist ein Bewertungsring von K und die Lokalisierung von $\mathcal{O}_K$ nach $\mathfrak{p}$.
3. $\mathcal{M}_{\mathfrak{p}} = \{x \in K \mid v_{\mathfrak{p}}(x) > 0\}$ ist das maximale Ideal von $\mathcal{O}_{\mathfrak{p}}$.
4. Der Restklassenkörper $\mathcal{O}_{\mathfrak{p}}/\mathcal{M}_{\mathfrak{p}}$ ist endlich.

Aufgabe 37.

Seien $K = \mathbb{Q}(\sqrt{2})$ und $\mathfrak{p} = (\sqrt{2}) \subseteq \mathcal{O}_K$.

1. Zeigen Sie, dass $\mathfrak{p}$ ein Primideal von $\mathcal{O}_K$ ist.
2. Berechnen Sie $v_{\mathfrak{p}}(\sqrt{2})$, $v_{\mathfrak{p}}(1 + \sqrt{2})$, $v_{\mathfrak{p}}(\frac{5}{6} - \frac{1}{8}\sqrt{2})$ und $v_{\mathfrak{p}}((4 - \sqrt{2})^{100})$.
3. Beschreiben Sie $\mathcal{O}_{\mathfrak{p}}$ und den Restklassenkörper $\mathcal{O}_{\mathfrak{p}}/\mathcal{M}_{\mathfrak{p}}$.

Aufgabe 38.

Sei K ein Körper. Ein Absolutbetrag $|\cdot| : K \to \mathbb{R}_0^+$ heißt nicht archimedisch, falls die ultrametrische Dreiecksungleichung $|x+y| \leq \max\{|x|,|y|\}$ für $x,y \in K$ gilt. Andernfalls heißt $|\cdot|$ archimedisch.

Sei $p \in \mathbb{Z}$ eine Primzahl. Dann heißt $v_p = v_{(p)}$ die p-adische Bewertung von $\mathbb{Q}$. Die Funktion $|\cdot|_p : \mathbb{Q} \to \mathbb{R}_0^+$ mit $x \mapsto p^{-v_p(x)}$ für $x \in \mathbb{Q}^\times$ und $|0|_p = 0$ wird der p-adische Absolutbetrag von $\mathbb{Q}$ genannt.

1. Beschreiben Sie den Bewertungsring $\mathcal{O}_p$ von v_p, sein maximales Ideal $\mathcal{M}_p$ und den Körper $\mathcal{O}_p/\mathcal{M}_p$.
2. Zeigen Sie: Die Abbildung $|\cdot|_p$ ist ein nicht archimedischer Absolutbetrag von $\mathbb{Q}$.
3. Finden Sie zu $p_1,...,p_n \in \mathbb{Z}$ paarweise verschiedene Primzahlen, $x_1,...,x_n \in \mathbb{Z}$ und $\epsilon_1,...,\epsilon_n \in \mathbb{R}^+$ ein $x \in \mathbb{Z}$ mit $|x-x_i|_{p_i} \leq \epsilon_i$, $i = 1,...,n$.

Aufgabe 39.

Seien K ein algebraischer Zahlkörper vom Grad n und p eine Primzahl.

1. Finden Sie einen solchen Körper K mit einer Primzahl p, bei dem $n > 1$ ist und p nicht n teilt, aber $p\mathcal{O}_K$ ein Primideal in $\mathcal{O}_K$ ist, also speziell ein Primideal $\mathfrak{P}$ in $\mathcal{O}_K$ mit $\mathrm{N}_{K|\mathbb{Q}}(\mathfrak{P}) = p^n$.
2. Zeigen Sie: Für alle $\alpha \in \mathcal{O}_K$ mit $K = \mathbb{Q}(\alpha)$ und $p \nmid [\mathcal{O}_K : \mathbb{Q}(\alpha)]$ ist $\mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{Z}_p \oplus \mathbb{Z}_p\overline{\alpha} \oplus \cdots \oplus \mathbb{Z}_p\overline{\alpha}^{n-1}$.

Aufgabe 40.

Sei $\alpha \in \mathbb{Z}$ eine Nullstelle des Polynoms $f = X^3 - X + 1 \in \mathbb{Z}[X]$ und sei $K = \mathbb{Q}(\alpha)$.

Bestimmen Sie die Primidealzerlegung von (5) und (7) in $\mathcal{O}$.

Aufgabe 41.

Seien $\alpha \in \mathbb{Z}$ ganz über $\mathbb{Z}$ und $K = \mathbb{Q}(\alpha)$, $n = [K:\mathbb{Q}]$, $m = |\mathcal{O} : \mathbb{Z}[\alpha]|$.

1. Zeigen Sie die Gleichheit $\mathrm{D}_{K|\mathbb{Q}}(1,\alpha,...,\alpha^{n-1}) = m^2\mathrm{D}_K$.
2. Sei $\alpha \in \mathbb{Z}$ eine Nullstelle von $X^5 - 5X - 5$. Bestimmen Sie die Primidealzerlegung von (2) in $\mathcal{O}$.

Aufgabe 42.

Seien $p \in \mathbb{Z}$ eine Primzahl, $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$ ein normiertes Eisensteinpolynom, d.h. irreduzibel nach dem Eisenstein-Kriterium, $\alpha \in \mathbb{Z}$ eine Nullstelle von f und $K = \mathbb{Q}(\alpha)$.

Zeigen Sie: $p \nmid |\mathcal{O} : \mathbb{Z}[\alpha]|$ und das Ideal $\mathfrak{p} = (p,\alpha)$ ist ein Primideal in $\mathcal{O}$ mit $\mathfrak{p}^n = p\mathcal{O}$.

Aufgabe 43.

Seien $m \in \mathbb{N}^* = \mathbb{N}\backslash\{0\}$ und $Z(m) = \{e^{\frac{2\pi i k}{m}} \mid (k,m) = 1\}$ die Menge der primitiven m-ten Einheitswurzeln, $\Phi_m(X) = \prod_{\zeta \in Z(m)} (X-\zeta) \in \mathbb{Z}[X]$ das m-te Kreisteilungspolynom. Für alle $n \in \mathbb{N}^*$ ist $X^n - 1 = \prod_{m|n} \Phi_m(X)$.

Beweisen Sie die folgenden Aussagen:

1. Zu $f \in \mathbb{Z}[X]$, $\deg(f) > 1$ gibt es unendlich viele Primzahlen p, sodass f eine Nullstelle mod p hat.
2. Zu jedem $m \in \mathbb{Z}$ gibt es eine Primzahl p mit $p \equiv 1 \bmod m$.
3. Zu jedem $m \in \mathbb{Z}$ gibt es unendlich viele Primzahlen p mit $p \equiv 1 \bmod m$.
4. Zu jedem Zahlring gibt es unendlich viele Primideale $\mathfrak{P}$ mit $f(\mathfrak{P}|(p)) = 1$, wobei $(p) = \mathfrak{P} \cap \mathbb{Z}$.

Aufgabe 44.

Seien $L|K$ Zahlkörper. Ein Primideal in $\mathcal{O}_K$ ist voll zerlegt, falls es in L genau $[L:K]$ Fortsetzungen hat.

1. Zeigen Sie, dass es unendlich viele Primideale $\mathfrak{p}$ in $\mathcal{O}_K$ gibt, die in L voll zerlegt sind.
2. Seien $\mathcal{O}_K$ ein Zahlring und $f \in \mathcal{O}_K[X]\backslash\mathcal{O}_K$ normiert und irreduzibel. Zeigen Sie, dass es unendlich viele Primideale $\mathfrak{p}$ in $\mathcal{O}_K$ gibt, für die f modulo $\mathfrak{p}$ in Linearfaktoren zerfällt.

Aufgabe 45.

Sei $L|K$ eine Erweiterung von Zahlkörpern und sei N die normale Hülle von $L|K$. Zeigen Sie, dass jedes Primideal $\mathfrak{p}$ in $\mathcal{O}_K$, das in L voll zerlegt ist, auch in N voll zerlegt ist.

Aufgabe 46.

Beweisen Sie die folgenden Aussagen:

1. Sei Ω die Menge aller diskreten Bewertungen eines algebraischen Zahlkörpers K. Dann lässt sich $\mathcal{O}_K$ schreiben als $\mathcal{O}_K = \bigcap\{\mathcal{O}_v \mid v \in \Omega\}$, wobei $\mathcal{O}_v = \{x \in K \mid v(x) \geq 0\}$ der Bewertungsring zu v ist.
2. Seien K ein algebraischer Zahlkörper, $v : K \to \mathbb{Z} \cup \{\infty\}$ eine diskrete, surjektive Bewertung von K mit $v(K^\times) = \mathbb{Z}$. Dann gibt es ein Primideal $\mathfrak{P}$ in $\mathcal{O}_K$ mit v die $\mathfrak{P}$-adische Bewertung $v_\mathfrak{P}$ von K.

Aufgabe 47.

Sei G eine endliche abelsche Gruppe. Ein Gruppenhomomorphismus $\chi : G \to \mathbb{Z}^\times$ wird Gruppencharakter von G genannt. Die Menge der Charaktere von G bezeichnen wir mit $\hat{G}$.

Seien jetzt G und H endliche abelsche Gruppen. Zeigen Sie:

1. Die Multiplikation in $\mathbb{Z}$ induziert eine Gruppenoperation auf $\hat{G}$.
2. Ist G zyklisch, so ist $\hat{G}$ ebenfalls zyklisch und von der selben Ordnung wie G.
3. Es gilt $\widehat{G \times H} \cong \hat{G} \times \hat{H}$.
4. Es gilt $G \cong \hat{G}$.

Aufgabe 48.

Sei G eine endliche abelsche Gruppe. Zeigen Sie:

1. Für jeden Charakter $\chi \in \hat{G}$, $\chi \neq \chi_0$, gilt $\sum\{\chi(a) \mid a \in G\} = 0$.
2. Für jedes Element $a \in G$, $a \neq 1$, gilt $\sum\{\chi(a) \mid \chi \in \hat{G}\} = 0$.
3. Ist H eine Untergruppe von G, so hat jeder Charakter von H genau $|G/H|$ Fortsetzungen auf G.

Aufgabe 49.

Sei $m \in \mathbb{N}_{\geq 2}$. Eine Abbildung $\chi : \mathbb{Z} \to \mathbb{Z}$ heißt Zahlcharakter modulo m, falls gelten:

$$\chi(a) = \chi(b) \text{ für } a \equiv b \bmod m, \quad \chi(ab) = \chi(a)\chi(b) \text{ für } a, b \in \mathbb{Z}, \quad \chi(1) = 1 \;\&\; \chi(p) = 0 \text{ für } p \in \mathbb{P},\ p \mid m.$$

Beweisen Sie die folgenden Aussagen:

1. Ist $\chi : \mathbb{Z} \to \mathbb{Z}$ ein Zahlcharakter modulo m und ist $a \in \mathbb{Z}$, so gilt: $\chi(a) \neq 0 \Leftrightarrow (a, m) = 1$.
2. Die Zahlcharaktere modulo m stehen in Bijektion zu den Gruppencharakteren von $\mathbb{Z}/(m\mathbb{Z})^\times$.
3. Für jede Primzahl $p \in \mathbb{Z}$ definiert das Legendre-Symbol $(\frac{\cdot}{p})$ einen Zahlcharakter modulo p.

Aufgabe 50.

Seien $m \in \mathbb{N}$, $m \geq 2$, $G = \mathbb{Z}/(m\mathbb{Z})^\times$, $d = \varphi(m)$, $p \in \mathbb{Z}$ prim mit $p \nmid m$, $f = \mathrm{Ord}(\overline{p})$ in G und $r = \frac{d}{f} \in \mathbb{N}$.

Zeigen Sie, dass in $\mathbb{Z}[X]$ gilt: $\prod_{\chi \in \hat{G}} (1 - \chi(p)X) = (1 - X^f)^r$.

Index

Literaturverzeichnis

[1] Bruns, W.: *Zahlentheorie.* Osnabrücker Schriften zur Mathematik, Reihe V, Heft 146, 2000.

[2] Dieckmann, T.: *Dirichletsche L-Reihen*, 2008.

[3] Dirichlet, P. G. L.: *Beweis des Satzes, daß jede unbegrenzte arithmetische Progrssion, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält.* Abh. Ak. Wiss. Berlin, **vol. 39**: pp. 45–71, 1837.

[4] Elstrodt, J.: *The Life and Work of Gustav Lejeune Dirichlet (1805-1859).* Clay Mathematics Proceedings, **vol. 7**, 2007.

[5] Engler, A. J. & Prestel, A.: *Valued fields.* Springer Verlag Berlin Heidelberg, 2005.

[6] Gubisch, M.: *Lineare Algebra II.* Vorlesungsskript, Universität Konstanz, 2006.

[7] Gubisch, M.: *Algebra.* Vorlesungsskript Universität Konstanz, 2007.

[8] Kummer, E. E.: *Allgemeiner Beweis des Fermatschen Satzes, daß die Gleichung $x^\lambda + y^\lambda = z^\lambda$ durch ganze Zahlen unlösbar ist, für alle diejenigen Potenz-Exponenten λ, welche ungerade Primzahlen sind und in den Zählern der ersten $\frac{1}{2}(\lambda - 3)$ Bernouillschen Zahlen als Factoren nicht vorkommen.* J. d. Math., **vol. 40**: pp. 138–146, 1850.

[9] Leutbecher, A.: *Zahlentheorie – Eine Einführung in die Algebra.* Springer-Lehrbuch, 1996.

[10] Müller, P.: *Analytische Zahlentheorie.* Vorlesungsskript Universität Würzburg, 2005.

[11] Nickel, M.: *Der Dirichletsche Primzahlsatz.* Bachelorarbeit, Universität Mainz, 2012.

[12] Sander, J.: *Analytische Zahlentheorie.* Vorlesungsskript Universität Hannover, 2001.

[13] Sander, J.: *Algebraische Zahlentheorie.* Vorlesungsskript Universität Hannover, 2002.

[14] Werner, F.: *Die Riemannsche Zetafunktion.* Vorlesungsskript Universität Göttingen, 2007.