Algebraische Zahlentheorie

Benjamin Sambale

14. September 2019

1 Zahlkörper

Ein *Zahlkörper* K ist eine endliche (und damit algebraische) Körpererweiterung von $\mathbb{Q}$. Nach dem Fundamentalsatz der Algebra kann man K als Teilkörper von $\mathbb{C}$ auffassen. Man nennt $x \in K$ *ganz-algebraisch*, falls das Minimalpolynom von x über $\mathbb{Q}$ in $\mathbb{Z}[X]$ liegt. Die ganz-algebraischen Elemente in K bilden den *Ganzheitsring* (oder *Hauptordnung*) $\mathbb{Z}_K$. Wegen $K = \{\frac{x}{y} : x, y \in \mathbb{Z}_K,\, y \neq 0\}$ ist K der Quotientenkörper von $\mathbb{Z}_K$.

Ein *Gitter* von K ist eine freie abelsche Gruppe $\Gamma \leq (K, +)$ vom Rang $|K : \mathbb{Q}|$. Die *Ordnung* von Γ ist der Teilring

$$\mathfrak{o}_\Gamma := \{x \in K : x\Gamma \subseteq \Gamma\} \subseteq \mathbb{Z}_K.$$

Gitter Γ und Δ heißen *äquivalent* (im weiteren Sinn), falls $x \in K$ mit $x\Gamma = \Delta$ existiert. Die Gitter mit Ordnung $\mathbb{Z}_K$ nennt man *gebrochene Ideale*. Die in $\mathbb{Z}_K$ enthaltenen gebrochenen Ideale sind die gewöhnlichen Ideale außer dem Nullideal. Die vom Nullideal verschiedenen Primideale in $\mathbb{Z}_K$ sind genau die maximalen Ideale. Sie bilden eine Basis der freien abelschen Gruppe J_K aller gebrochenen Ideale bzgl. Multiplikation (dies gilt allgemeiner für *Dedekindringe*). Für $\mathfrak{a} \in J_K$ und $\mathfrak{P} \trianglelefteq \mathbb{Z}_K$ maximal sei $v_\mathfrak{P}(\mathfrak{a}) \in \mathbb{Z}$ der Exponent von $\mathfrak{P}$ in der Primfaktorzerlegung von $\mathfrak{a}$. Dies liefert eine Bewertung mit folgenden Rechenregeln:

$$v_\mathfrak{P}(\mathfrak{ab}) = v_\mathfrak{P}(\mathfrak{a}) + v_\mathfrak{P}(\mathfrak{b}), \qquad v_\mathfrak{P}(\mathfrak{a} + \mathfrak{b}) \leq \min\{v_\mathfrak{P}(\mathfrak{a}), v_\mathfrak{P}(\mathfrak{b})\}, \qquad \mathfrak{a} \subseteq \mathfrak{b} \Longrightarrow v_\mathfrak{P}(\mathfrak{b}) \leq v_\mathfrak{P}(\mathfrak{a}).$$

Man setzt außerdem $v_\mathfrak{P}(x) := v_\mathfrak{P}(x\mathbb{Z}_K)$ für $x \in \mathbb{Z}_K$.

Die gebrochenen *Hauptideale* der Form $(x) = x\mathbb{Z}_K$ für $x \in K$ bilden einen Normalteiler $H_K \trianglelefteq J_K$. Die *Idealklassengruppe*

$$C_K := J_K/H_K$$

ist endlich und ihre Ordnung $h_K := |C_K|$ heißt *Klassenzahl* von K. Die Elemente von C_K sind Äquivalenzklassen im obigen Sinn. Es gilt

$$\mathbb{Z}_K \text{ faktoriell} \iff \mathbb{Z}_K \text{ Hauptidealring} \iff h_K = 1.$$

Ist K kein imaginär-quadratischer Zahlkörper (siehe unten), so würde die verallgemeinerte riemannsche Vermutung außerdem implizieren:

$$\mathbb{Z}_K \text{ euklidisch} \implies h_K = 1.$$

2 Erweiterungen von Zahlkörpern

Seien nun $K \subseteq L \subseteq M$ Zahlkörper. Dann gilt der *Gradsatz* $|M : K| = |M : L||L : K|$. Jedes maximale Ideal $\mathfrak{P} \trianglelefteq \mathbb{Z}_L$ bestimmt durch $\mathfrak{p} := \mathfrak{P} \cap \mathbb{Z}_K$ ein maximales Ideal von $\mathbb{Z}_K$. Für jedes maximale Ideal $\mathfrak{p} \trianglelefteq \mathbb{Z}_K$ gibt es umgekehrt eine eindeutige Zerlegung

$$\mathfrak{p}\mathbb{Z}_L = \sum_{\mathfrak{p} \subseteq \mathfrak{P} \trianglelefteq \mathbb{Z}_L} \mathfrak{P}^{v_{\mathfrak{P}}(\mathfrak{p}\mathbb{Z}_L)},$$

wobei man $e(\mathfrak{P}|\mathfrak{p}) := v_{\mathfrak{P}}(\mathfrak{p}\mathbb{Z}_L)$ den *Verzweigungsindex* von $\mathfrak{P}$ über $\mathfrak{p}$ nennt. Im Fall $e(\mathfrak{P}|\mathfrak{p}) > 1$ nennt man $\mathfrak{P}$ *verzweigt* und anderenfalls *unverzweigt* bzgl. K. Durch die natürliche Einbettung $\mathbb{Z}_K/\mathfrak{p} \to \mathbb{Z}_L/\mathfrak{P}$ wird $\mathbb{Z}_L/\mathfrak{P}$ zu einer endlichen Körpererweiterung über $\mathbb{Z}_K/\mathfrak{p}$, deren Grad man *Restklassenindex* $f(\mathfrak{P}|\mathfrak{p})$ nennt. Es gilt die *fundamentale Gleichung*

$$|L : K| = \sum_{\mathfrak{P} \supseteq \mathfrak{p}} e(\mathfrak{P}|\mathfrak{p}) f(\mathfrak{P}|\mathfrak{p}). \tag{2.1}$$

Im Fall $|L : K| = e(\mathfrak{P}|\mathfrak{p})$ (bzw. $e(\mathfrak{P}|\mathfrak{p}) = f(\mathfrak{P}|\mathfrak{p}) = 1$ für alle $\mathfrak{P}$) nennt man $\mathfrak{p}$ *voll verzweigt* (bzw. *voll zerlegt*) bzgl. L. Sei p die einzige Primzahl in $\mathfrak{p}$, also $\mathbb{Z} \cap \mathfrak{p} = (p)$. Ist $p \nmid e(\mathfrak{P}|\mathfrak{p})$ für alle $\mathfrak{P}$, so heißt $\mathfrak{p}$ *zahm* und anderenfalls *wild* bzgl. L.

Sind $\mathfrak{P}_K \subseteq \mathfrak{P}_L \subseteq \mathfrak{P}_M$ maximale Ideale, so gilt die Transitivität

$$e(\mathfrak{P}_M|\mathfrak{P}_K) = e(\mathfrak{P}_M|\mathfrak{P}_L)e(\mathfrak{P}_L|\mathfrak{P}_K), \qquad f(\mathfrak{P}_M|\mathfrak{P}_K) = f(\mathfrak{P}_M|\mathfrak{P}_L)f(\mathfrak{P}_L|\mathfrak{P}_K). \tag{2.2}$$

Durch $\mathfrak{N}_{L|K}(\mathfrak{P}) := \mathfrak{p}^{f(\mathfrak{P}|\mathfrak{p})}$ erhält man einen inklusionserhaltenden Homomorphismus $\mathfrak{N}_{L|K} : J_L \to J_K$, der *Relativnorm* heißt. Für $\mathfrak{a} \trianglelefteq \mathbb{Z}_K$ gilt $\mathfrak{N}_{L|K}(\mathfrak{a}\mathbb{Z}_L) = \mathfrak{a}^{|L:K|}$. Außerdem ist die Relativnorm transitiv

$$\mathfrak{N}_{M|K} = \mathfrak{N}_{L|K}\mathfrak{N}_{M|L}.$$

Im Fall $K = \mathbb{Q}$ ist $\mathfrak{p} = (p)$ für eine Primzahl p und man erhält die *Absolutnorm* $\mathfrak{N}(\mathfrak{a}) := |\mathbb{Z}_L : \mathfrak{a}|$ von $\mathfrak{a} \trianglelefteq \mathbb{Z}_L$ mit $\mathfrak{N}_{L|\mathbb{Q}}(\mathfrak{a}) = (\mathfrak{N}(\mathfrak{a}))$ (chinesischer Restsatz).

Jedes $x \in L$ induziert eine K-lineare Abbildung $f_x : L \to L$, $a \mapsto xa$. Man nennt $S_{L|K}(x) := \operatorname{tr} f_x \in K$ die (relative) *Spur* und $N_{L|K}(x) := \det f_x \in K$ die (relative) *Norm* von x über K. Wie üblich gilt

$$S_{L|K}(\lambda x + \mu y) = \lambda S_{L|K}(x) + \mu S_{L|K}(y), \qquad N_{L|K}(\lambda xy) = \lambda^{|L:K|} N_{L|K}(x)\, \mathrm{N}_{L|K}(y)$$

für $x, y \in L$ und $\lambda, \mu \in K$. Man kann L stets in einer Galois-Erweiterung $\widehat{L}$ einbetten. Es gilt dann

$$S_{L|K}(x) = \sum_{\sigma \in \mathrm{Gal}(\widehat{L}|K)/\,\mathrm{Gal}(\widehat{L}|L)} \sigma(x), \qquad N_{L|K}(x) = \prod_{\sigma \in \mathrm{Gal}(\widehat{L}|K)/\,\mathrm{Gal}(\widehat{L}|L)} \sigma(x).$$

Daraus erhält man

$$S_{M|K} = S_{L|K}S_{M|L}, \qquad N_{M|K} = N_{L|K}N_{M|L}.$$

Im Fall $K = \mathbb{Q}$ ist außerdem $|N(x)| := |N_{L|\mathbb{Q}}(x)| = \mathfrak{N}(x\mathbb{Z}_L)$ für $x \in L$. Ist dann r die Anzahl der Nebenklassen $\sigma \in \mathrm{Gal}(\widehat{L}|\mathbb{Q})/\,\mathrm{Gal}(\widehat{L}|L)$ mit $\sigma(L) \subseteq \mathbb{R}$, so ist die Einheitengruppe $\mathbb{Z}_L^\times$ ein direktes Produkt einer endlichen zyklischen Gruppe (Einheitswurzeln) mit einer freien abelschen Gruppe vom Rang $\frac{1}{2}(|L : \mathbb{Q}| + r) - 1$ (*Dirichletscher Einheitensatz*).

3 Diskriminanten

Eine $\mathbb{Z}$-Basis $b_1, \ldots, b_n$ von $\mathbb{Z}_K$ nennt man *Ganzheitsbasis* (existiert stets). Mit der Abkürzung $S := S_{K|\mathbb{Q}}$ ist

$$d_K := \det(S(b_i b_j)_{i,j})$$

die *Diskriminante* von K. Diese hängt nicht von der Wahl der Ganzheitsbasis ab. Nach dem *Stickelberger Diskriminantensatz* ist $d_K \equiv 0, 1 \pmod 4$.

Als separable Körpererweiterung besitzt K ein primitives Element $x \in \mathbb{Z}_K$, d. h. $K = \mathbb{Q}(x)$. Gilt $\mathbb{Z}_K = \mathbb{Z}[x]$, so nennt man K *monogen* (für eine Nullstelle x von X^3+X^2-2X+8 ist $\mathbb{Q}(x)$ beispielsweise nicht monogen). Sei $f \in \mathbb{Q}[X]$ das Minimalpolynom von x mit Nullstellen $x_1, \ldots, x_n \in \mathbb{C}$. Dann nennt man

$$\Delta(f) := \prod_{i<j} (x_i - x_j)^2 \in \mathbb{Z}$$

die *Diskriminante* von f. Sei lässt sich mittels elementarsymmetrischer Funktionen durch die Koeffizienten von f ausdrücken. Es gilt

$$\Delta(f) = |\mathbb{Z}_K : \mathbb{Z}[x]|^2 d_K.$$

Man nennt

$$\mathbb{Z}_L^* := \{x \in L : S_{L|K}(x\mathbb{Z}_L) \subseteq \mathbb{Z}_K\}$$

das zu $\mathbb{Z}_L$ *duale* Gitter bzgl. K. Die *Relativdifferente* $\mathfrak{D}_{L|K} \trianglelefteq \mathbb{Z}_L$ wird durch die Gleichung

$$\mathfrak{D}_{L|K}\mathbb{Z}_L^* = \mathbb{Z}_L$$

in J_L definiert. Man nennt $\mathfrak{d}_{L|K} := \mathfrak{N}_{L|K}(\mathfrak{D}_{L|K})$ die *Relativdiskriminante* von L über K. Im Fall $K = \mathbb{Q}$ nennt man $\mathfrak{D}_L := \mathfrak{D}_{L|\mathbb{Q}}$ *Differente* von L. Es gilt der *erste Dedekind-Hauptsatz* $\mathfrak{N}(\mathfrak{D}_L) = |d_L|$ und $\mathfrak{d}_{L|\mathbb{Q}} = (d_L)$. Im Allgemeinen gilt die Transitivität

$$\mathfrak{D}_{M|K} = \mathfrak{D}_{L|K}\mathfrak{D}_{M|L}, \qquad \mathfrak{d}_{M|K} = \mathfrak{d}_{L|K}^{|M:L|}\mathfrak{N}_{L|K}(\mathfrak{d}_{M|L}).$$

Speziell für $K = \mathbb{Q}$ ergibt sich $d_L^{|M:L|} \mid d_M$. Sei $x \in \mathbb{Z}_L$ primitiv über K (d. h. $L = K(x)$) mit Minimalpolynom $f \in K[X]$. Dann heißt $\delta_{L|K}(x) := f'(x) \in \mathbb{Z}_L$ *Zahldiskriminante* von x, wobei $f' \in K[X]$ die Ableitung von f bezeichnet. Es gilt

$$\delta_{L|K}(x)\mathbb{Z}_L = \mathfrak{D}_{L|K}\mathfrak{F},$$

wobei $\mathfrak{F} \trianglelefteq \mathbb{Z}_L$ *Führer* von x genannt wird. Der *zweite Dedekind-Hauptsatz* besagt

$$\mathfrak{D}_{L|K} = \sum_{\substack{x \in \mathbb{Z}_L \\ L = K(x)}} \delta_{L|K}(x)\mathbb{Z}_L.$$

Für maximale Ideale $\mathfrak{p} \subseteq \mathfrak{P}$ von K und L gilt der *dritte Dedekind-Hauptsatz* (*Differentensatz*)

$$v_{\mathfrak{P}}(\mathfrak{D}_{L|K}) \geq e(\mathfrak{P}|\mathfrak{p}) - 1$$

mit Gleichheit genau dann, wenn $e(\mathfrak{P}|\mathfrak{p})$ nicht durch die in $\mathfrak{p}$ enthaltene Primzahl p teilbar ist. Durch Normbildung erhält man den *Diskriminantensatz*

$$v_{\mathfrak{p}}(\mathfrak{d}_{L|K}) \geq \sum_{\mathfrak{P} \supseteq \mathfrak{p}} f(\mathfrak{P}|\mathfrak{p})(e(\mathfrak{P}|\mathfrak{p}) - 1)$$

mit Gleichheit genau dann, wenn $\mathfrak{p}$ zahm bzgl. L ist. Insbesondere treten genau die (endlich vielen) verzweigten Ideale in $\mathfrak{d}_{L|K}$ auf. Der *Hermitesche Diskriminantensatz* besagt, dass nur endlich viele Zahlkörper mit vorgegebener Diskriminante existieren. Nach *Minkowskis Diskriminantensatz* ist $\mathbb{Q}$ der einzige Zahlkörper mit $|d_K| = 1$.

Ist $L = K_1K_2$ das Kompositum von Zahlkörpern K_1 und K_2 über K, so gilt außerdem

$$v_\mathfrak{p}(\mathfrak{d}_{L|K}) > 0 \iff v_\mathfrak{p}(\mathfrak{d}_{K_1|K}) + v_\mathfrak{p}(\mathfrak{d}_{K_2|K}) > 0$$

und $\mathfrak{D}_{K_2|K} \subseteq \mathfrak{D}_{L|K_1}$. Im Fall $K = \mathbb{Q}$ stimmen die Primteiler von d_L und $d_{K_1}d_{K_2}$ überein. Ist in diesem Fall sogar $\mathrm{ggT}(d_{K_1}, d_{K_2}) = 1$, so gilt $K_1 \cap K_2 = \mathbb{Q}$ und $d_L = d_{K_1}^{|K_2:\mathbb{Q}|} d_{K_2}^{|K_1:\mathbb{Q}|}$. Eine Ganzheitsbasis von L erhält man dann wie beim Gradsatz durch Multiplikation von Ganzheitsbasen von K_1 und K_2 (die entsprechende Diskriminantenmatrix ist ein Kroneckerprodukt).

4 Polynome

Sei x ein ganzes primitives Element des Zahlkörpers K mit Minimalpolynom $\mu \in \mathbb{Z}[X]$. Sei p eine Primzahl, die $|\mathbb{Z}_K : \mathbb{Z}[x]|$ nicht teilt. Sei $\overline{\mu} \in \mathbb{F}_p[X]$ die Reduktion modulo p mit Primfaktorzerlegung

$$\overline{\mu} = \prod_{i=1}^{n} \overline{\gamma}_i^{e_i}.$$

Seien $\gamma_i \in \mathbb{Z}[X]$ mit Reduktion $\overline{\gamma}_i$ modulo p. Dann ist $p\mathbb{Z}_K = \prod \mathfrak{p}_i^{e_i}$ die fundamentale Gleichung bzgl. p mit $\mathfrak{p}_i = \gamma_i(x)\mathbb{Z}[x] + p\mathbb{Z}_K$ für $i = 1, \ldots, n$. Die Restklassengrade sind außerdem $f(\mathfrak{p}_i|p) = \deg \overline{\gamma}_i$.

Ist allgemeiner $\mu \in \mathbb{Z}[X]$ ein (irreduzibles) Eisensteinpolynom zur Primzahl p mit Nullstelle x, so ist p voll verzweigt im Ganzheitsring $\mathbb{Z}_K$ von $K = \mathbb{Q}(x)$ und $|\mathbb{Z}_K : \mathbb{Z}[x]| \not\equiv 0 \pmod{p}$. Ist umgekehrt $p\mathbb{Z}_K = \mathfrak{P}^{|K:\mathbb{Q}|}$ für einen Zahlkörper K, so ist $K = \mathbb{Q}(x)$ für alle $x \in \mathfrak{P} \setminus \mathfrak{P}^2$ und das Minimalpolynom von x ist ein Eisensteinpolynom bzgl. p.

5 Galois-Erweiterungen

Sei nun $K \subseteq L$ eine Galois-Erweiterung mit $G := \mathrm{Gal}(L|K)$. Dann operiert G transitiv auf der Menge der maximalen Ideale von L, die ein festes maximales Ideal von K enthalten. In (2.1) sind daher e und f konstant; es gilt also $|G| = |L : K| = efg$, wobei g die Anzahl der maximalen Ideale von $\mathbb{Z}_L$ ist, die $\mathfrak{p}$ enthalten. Für ein maximales Ideal $\mathfrak{P} \trianglelefteq \mathbb{Z}_L$ sei

$$G_{-1} := \{\sigma \in G : \sigma(\mathfrak{P}) = \mathfrak{P}\} \leq G$$

die *Zerlegungsgruppe* und

$$G_k := \{\sigma \in G_{-1} : \sigma(x) \equiv x \pmod{\mathfrak{P}^{i+1}}\ \forall x \in \mathbb{Z}_L\} \leq G_{-1}$$

die k-te *Verzweigungsgruppe* für $k \geq 0$ (G_0 heißt auch *Trägheitsgruppe*). Die entsprechenden Fixkörper heißen *Zerlegungskörper* $K_{-1} := L^{G_{-1}}$, *Trägheitskörper* $K_0 := L^{G_0}$ und *Verzweigungskörper* $K_1 := L^{G_1}$. Es existiert ein k mit $G \geq G_{-1} \geq \ldots \geq G_k = 1$. Des Weiteren gilt

$$|G : G_{-1}| = g, \qquad G_{-1}/G_0 \cong \mathbb{Z}/f\mathbb{Z}, \qquad |G_0| = e,$$
$$G_0/G_1 \leq (\mathbb{Z}_L/\mathfrak{P})^\times \cong \mathbb{Z}/(\mathfrak{N}(\mathfrak{p})^f - 1)\mathbb{Z}, \qquad G_l/G_{l+1} \leq \mathbb{Z}_L/\mathfrak{P}$$

für $l \geq 1$. Insbesondere ist G_0/G_1 eine zyklische p'-Gruppe und G_l/G_{l+1} eine elementarabelsche p-Gruppe für die in $\mathfrak{P}$ enthaltene Primzahl p. Aus (2.2) folgt, dass $\mathfrak{p}$ bzgl. K_0 unverzweigt ist. Schließlich ist

$$v_{\mathfrak{P}}(\mathfrak{D}_{L|K}) = \sum_{n=0}^{\infty}(|G_n| - 1).$$

Sei nun $\mathfrak{p}$ unverzweigt, d. h. $G_0 = 1$. Dann ist $G_{-1} \cong \mathrm{Gal}(\mathbb{Z}_L/\mathfrak{P}|\mathbb{Z}_K/\mathfrak{p}) \cong \mathbb{Z}/f\mathbb{Z}$ und es existiert ein *Frobenius-Element* $\gamma \in G_{-1}$ mit $\gamma(x) \equiv x^{|\mathbb{Z}_K/\mathfrak{p}|} \pmod{\mathfrak{P}}$ für alle $x \in \mathbb{Z}_L$. Da die $\mathfrak{p}$ enthaltenden maximalen Ideale von $\mathbb{Z}_L$ in G konjugiert sind, bestimmt $\mathfrak{p}$ auf diese Weise eine Konjugationsklasse von Frobenius-Elementen in G. Der *Dichtigkeitssatz von Tschebotarjoff* besagt, dass der Anteil aller unverzweigten Primideale von $\mathbb{Z}_K$, die die Konjugationsklasse von γ bestimmen genau $\frac{1}{|\mathrm{C}_G(\gamma)|}$ beträgt. Im Spezialfall $K = \mathbb{Q}$ und $L = \mathbb{Q}_n$ erhält man den *Dirichletschen Primzahlsatz*: Für $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, n) = 1$ beträgt der Anteil aller Primzahlen $p \in a + n\mathbb{Z}$ genau $\frac{1}{\varphi(n)}$. Speziell für $n = 10$ erhält man: Eine zufällig gewählte Primzahl endet zu je 25% auf eine der Ziffern 1, 3, 7 oder 9.

6 Quadratische Zahlkörper

Schließlich sei K ein *quadratischer* Zahlkörper, d. h. $|K : \mathbb{Q}| = 2$. Dann existiert genau eine quadratfreie Zahl $m \in \mathbb{Z}$ mit $K = \mathbb{Q}(\sqrt{m}) = \mathbb{Q} + \mathbb{Q}\sqrt{m}$. Im Fall $m < 0$ nennt man K *imaginär-quadratisch* und anderenfalls *reell-quadratisch*. Es gilt

$$d_K = \begin{cases} m & \text{falls } m \equiv 1 \pmod 4, \\ 4m & \text{sonst} \end{cases}$$

und

$$\mathbb{Z}_K = \mathbb{Z} + \mathbb{Z}\frac{d_K + \sqrt{d_K}}{2}.$$

Bekanntlich ist $\mathbb{Q} \subseteq K$ eine Galois-Erweiterung mit nicht-trivialem Automorphismus $\sigma : \sqrt{m} \mapsto -\sqrt{m}$. Damit ergibt sich $S(a + b\sqrt{m}) = 2a$ sowie $N(a + b\sqrt{m}) = a^2 - b^2 m$. Die Einheitengruppe hängt wie folgt von m ab:

$$\mathbb{Z}_K^\times = \{x \in \mathbb{Z}_K : N(x) = \pm 1\} = \begin{cases} \langle -1\rangle \cong \mathbb{Z}/2\mathbb{Z} & \text{falls } m < -3, \\ \langle \frac{1}{2}(1 + \sqrt{-3})\rangle \cong \mathbb{Z}/6\mathbb{Z} & \text{falls } m = -3, \\ \langle \sqrt{-1}\rangle \cong \mathbb{Z}/4\mathbb{Z} & \text{falls } m = -1, \\ \langle -1\rangle \times \langle \epsilon_K\rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z} & \text{falls } m > 0. \end{cases}$$

Dabei ist ϵ_K durch die Bedingung $\epsilon_K > 1$ eindeutig bestimmt und heißt *Grundeinheit* von K. Mit dem *Kettenbruchalgorithmus* lässt sich ϵ_K berechnen (z. B. $1 + \sqrt{2}$; Stichwort: *Pellsche Gleichung*).

Für eine Primzahl p hat die fundamentale Gleichung nur drei Lösungen:

- p ist genau dann (voll) verzweigt, wenn $p \mid d_K$,
- p ist genau dann (voll) zerlegt, wenn $p \neq 2$, $\left(\frac{d_K}{p}\right) = 1$ oder $p = 2$, $d_k \equiv 1 \pmod 8$ gilt,
- p ist genau dann *träge*, wenn $p \neq 2$, $\left(\frac{d_K}{p}\right) = -1$ oder $p = 2$, $d_k \equiv 5 \pmod 8$ gilt.

Hierbei ist $\left(\frac{d_K}{p}\right)$ das *Legendre-Symbol*, also $\left(\frac{d_K}{p}\right) = 1$ genau dann, wenn $d_k \equiv x^2 \pmod p$ für ein $x \in \mathbb{Z}$ gilt.

Gebrochene Ideale $\mathfrak{a}, \mathfrak{b} \in J_K$ heißen *äquivalent im engeren Sinn*, falls ein $x \in K$ mit $\mathfrak{a} = x\mathfrak{b}$ und $N(x) > 0$ existiert. Die gebrochenen Hauptideale (x) mit $N(x) > 0$ bilden eine Untergruppe $H_K^+ \leq H_K$. Man nennt $C_K^+ := J_K/H_K^+$ Gruppe der *engeren Idealklassen* und setzt $h_K^+ := |C_K^+| \in \{h_K, 2h_K\}$. Genau dann gilt $h_K = h_K^+$, wenn $d_K > 0$ und $N(\epsilon_K) = -1$. Für die Anzahl der Primteiler s von d_K gilt

$$C_K^+/(C_K^+)^2 \cong (\mathbb{Z}/2\mathbb{Z})^{s-1}.$$

Im Fall $s = 1$ ist $h_K = h_K^+ \equiv 1 \pmod 2$. Im Fall $s > 2$ folgt $h_K > 1$. Die imaginär-quadratischen Zahlkörper mit Klassenzahl 1 sind durch

$$-m \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$$

gegeben (*Heegner-Zahlen*). Unter denen entsprechen die euklidischen Zahlkörper den Werten $-m \in \{1, 2, 3, 7, 11\}$. Man vermutet, dass es unendlich viele reellquadratische Zahlkörper mit Klassenzahl 1 gibt (z. B. $m = 2, 3, 5, 6, 7, \ldots$; für $m = 3$ ist $h_K^+ = 2$). In jedem Fall ist $\mathbb{Z}_K$ genau dann euklidisch bzgl. der Norm N, wenn

$$m \in \{-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}.$$

Wie oben erwähnt sind vermutlich auch die anderen reell-quadratischen Zahlkörper mit Klassenzahl 1 euklidisch (bzgl. einer anderen Norm). Dies wurde bis auf höchstens zwei Ausnahmen bewiesen.

Jedes Gitter von K hat bis auf Äquivalenz die Form $\Gamma = \mathbb{Z} + \alpha\mathbb{Z}$ wobei $\alpha = a + b\omega$ mit $a, b \in \mathbb{Q}$, $b \neq 0$ und

$$\omega := \begin{cases} \frac{1+\sqrt{m}}{2} & \text{falls } m \equiv 1 \pmod 4, \\ \sqrt{m} & \text{sonst.} \end{cases}$$

Die entsprechende Ordnung ist $\mathbb{Z} + f\omega\mathbb{Z}$, wobei $f \in \mathbb{N}$ durch

$$v_p(f) = v_p(b) - \min\{0, v_p(a), v_p(b), v_p(N(\alpha))\}$$

für jede Primzahl p bestimmt ist. Man nennt f den *Führer* von Γ.

7 Kreisteilungskörper

Sei $n = \prod_{i=1}^s p_i^{a_i}$ die Primfaktorzerlegung von $n \neq 1$. Der n-te Kreisteilungskörper $\mathbb{Q}_n = \mathbb{Q}(\zeta_n)$ ist eine Galois-Erweiterung über $\mathbb{Q}$ vom Grad $\varphi(n) = \prod p_i^{a_i-1}(p_i - 1)$ (*eulersche* φ-Funktion). Für die Galoisgruppe gilt

$$\mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times \cong \prod (\mathbb{Z}/p_i^{a_i}\mathbb{Z})^\times.$$

Für $p > 2$ ist $(\mathbb{Z}/p^a\mathbb{Z})^\times$ zyklisch der Ordnung $\varphi(p^a) = p^{a-1}(p-1)$ (die p-Sylowgruppe wird von $1 + p + p^a\mathbb{Z}$ erzeugt). Für $p = 2$ ist

$$(\mathbb{Z}/2^a\mathbb{Z})^\times = \langle -1 + 2^a\mathbb{Z}\rangle \times \langle 5 + 2^a\mathbb{Z}\rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{a-2}\mathbb{Z}.$$

Insbesondere ist $\mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q})$ abelsch. Nach dem Hauptsatz der Galoistheorie ist jeder Teilkörper von $\mathbb{Q}_n$ (*Kreiskörper*) ebenfalls eine Galois-Erweiterung von $\mathbb{Q}$ mit abelscher Galoisgruppe. Nach *Kronecker-Weber* ist umgekehrt jeder abelsche Zahlkörper (Galois-Erweiterung mit abelscher Galoisgruppe) ein Kreiskörper.

Der Ganzheitsring von $\mathbb{Q}_n$ ist $\mathbb{Z}_{\mathbb{Q}_n} = \mathbb{Z}[\zeta_n]$ mit Diskriminante

$$d_{\mathbb{Q}_n} = (-1)^{\varphi(n)s/2} \prod p_i^{\varphi(n)(a_i - 1/(p_i-1))}.$$

Insbesondere ist $\mathbb{Q}_n$ monogen. Außerdem ist auch $\mathbb{Q}_n \cap \mathbb{R}$ monogen mit Ganzheitsring $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$.

Nach Dirichlet hat $\mathbb{Z}_{\mathbb{Q}_n}^\times$ Rang $\frac{1}{2}\varphi(n) - 1$. Insbesondere ist $\mathbb{Z}_{\mathbb{Q}_n}^\times$ unendlich, falls $n > 6$. Die Untergruppe der *Kreisteilungseinheiten*

$$U_n := \mathbb{Z}_{\mathbb{Q}_n}^\times \cap \langle \pm\zeta_n^i, 1 - \zeta_n^i : i = 0, \ldots, n-1 \rangle$$

hat endlichen Index in $\mathbb{Z}_{\mathbb{Q}_n}^\times$, falls $n \not\equiv 2 \pmod 4$. Für jede Primzahlpotenz p^m stimmt der Index $|\mathbb{Z}[\zeta_{p^m} + \zeta_{p^m}^{-1}]^\times : U_{p^m} \cap \mathbb{R}|$ mit der Klassenzahl von $\mathbb{Q}_{p^m} \cap \mathbb{R}$ überein.

Nach Dedekind ist jede Primzahl $p \nmid n$ unverzweigt in $\mathbb{Q}_n$. In (2.1) ist f die Ordnung von $p + n\mathbb{Z}$ in $(\mathbb{Z}/n\mathbb{Z})^\times$ und $g = \varphi(n)/f$. Insbesondere ist p genau dann voll zerlegt, wenn $p \equiv 1 \pmod n$ gilt. Andererseits ist

$$p_i \mathbb{Z}_{\mathbb{Q}_n} = \prod_{j=1}^{g} \mathfrak{P}_j^{\varphi(p_i^{a_i})}$$

mit Restklassengrad $f = |\langle p_i + n'\mathbb{Z} \rangle|$, wobei $n' = n/p_i^{a_i}$. Wie jede Galois-Erweiterung besitzt auch $\mathbb{Q}_n$ eine *Normalbasis* über $\mathbb{Q}$ (d. h. $\mathrm{Gal}(\mathbb{Q}_n|\mathbb{Q})$ permutiert die Basisvektoren). Der Ganzheitsring $\mathbb{Z}_{\mathbb{Q}_n}$ besitzt genau dann eine Normalbasis, wenn n quadratfrei ist. Der Satz von *Hilbert-Speiser* besagt allgemeiner, dass der Ganzheitsring eines abelschen Zahlkörpers K genau eine Normalbasis besitzt, wenn jede Primzahl zahm bzgl. K ist. In jedem Fall wird $\mathbb{Z}_K$ als abelsche Gruppe von den Bahnensummen der Einheitswurzeln unter der Galoisgruppe erzeugt.

Genau dann ist $\mathbb{Z}_{\mathbb{Q}_n}$ ein Hauptidealring, wenn

$$n \in \{1, \ldots, 22\} \cup \{24, 25, 26, 27, 28, 30, 32, 33, 34, 35, 36, 38, 40, 42, 44, 45, 48, 50, 54, 60, 66, 70, 84, 90\}$$

(dies liefert nur 30 verschiedene Körper wegen $\mathbb{Q} = \mathbb{Q}_2$ usw.). Für eine Primzahl p ist $\mathbb{Z}_{\mathbb{Q}_p}$ also genau dann ein Hauptidealring, wenn $p \leq 19$.