1 Einheitengruppe der ganzalgebraischen Zahlen im quadratischen Zahlkörper

Wir betrachten den quadratischen Zahlkörper, also $F = \mathbb{Q}(\sqrt{d})$, wobei $d \in \mathbb{Z}$ und quadratfrei ist. Wir bestimmen darin die Einheitengruppe U_d der ganzalgebraischen Zahlen $D \subset F$. Zunächst bemerkt man folgendes Lemma:

Lemma 1.1. *$\alpha \in D$ ist eine Einheit genau dann, wenn $N(\alpha) = \pm 1$.*

Zur Erinnerung: $N(\alpha) = \alpha \cdot \sigma(\alpha)$, wobei $\sigma(\alpha)$ das Konjugierte zu α ist.

Beweis. ($\Rightarrow$) Sei $\alpha \in D$ eine Einheit. Dann existiert ein α^{-1} mit $\alpha^{-1}\alpha = 1$. Also ist auch $N(\alpha^{-1}\alpha) = 1$, da $N(1) = 1$. Nun gilt aber

$$N(\alpha^{-1}\alpha) = N(\alpha^{-1})N(\alpha) = 1$$

Da $N(\alpha^{-1}), N(\alpha) \in \mathbb{Z}$, muss $N(\alpha) = \pm 1$.
($\Leftarrow$) Wenn $N(\alpha) = 1$ folgt, dass $\sigma(\alpha) = \alpha^{-1}$.
Wenn $N(\alpha) = -1$ folgt, dass $\sigma(\alpha) = \alpha^{-1}$ □

Nun beobachten wir im Fall, dass F ein imaginärer quadratischer Körper ist, das heißt $d < 0$, dass für Einheitengruppe U_d von D folgendes gilt:

Satz 1.2. *Wenn $d < 0$ und quadratfrei, dann ist*
(a) $U_{-1} = \{\pm 1, \pm i\}$
(b) $U_{-3} = \{\pm 1, \pm\omega, \pm\omega^2\}$, *wobei* $\omega = \frac{(-1+\sqrt{-3})}{2}$
(c) $U_d = \{\pm 1\}$, *für* $d < -3$ *oder* $d = -2$.

Beweis. Betrachte zwei Fälle:
1. Fall: $d \equiv 2$ oder $3(4)$:
Wie im vorherigen Vortrag gezeigt, kann jedes Elemtent $\alpha \in D$ in der Form $\alpha = x + \sqrt{d}y, x, y \in \mathbb{Z}$ dargestellt werden. Nun ist $N(\alpha) = \pm 1$ äquivalent zu $x^2 + |d|y^2 = 1$. Wenn nun $d = -1$ ist, dann erhält man (a). Wenn $|d| > 1$, dann ist $U_d = \{\pm 1\}$.
2. Fall: $d \equiv 1(4)$:
Nun ist jedes Element $\alpha \in D$ der Form $\alpha = (x + \sqrt{d}y)/2$, wobei $x, y \in \mathbb{Z}$ und $x \equiv y(2)$ (vgl. letzter Vortrag). Dann ist $N(\alpha) = \pm 1$ äquivalent zu $x^2 + |d|y^2 = 4$. Wenn nun $d = -3$, dann hat $x^2+3y^2 = 4$ genau die Lösungen $\{(2,0), (-2,0), (1,1), (1,-1), (-1,1), (-1,-1)\}$, also erhält (b). Wenn $|d| > 3$, gibt es keine nichttriviale Lösungen für die Gleichung $x^2 + |d|y^2 = 1$, also erhält man wieder (c). □

Nun betrachten wir den reellen quadratischen Körper $F = \mathbb{Q}(\sqrt{d})$ mit $d > 0$. Hierfür benötigen wir zunächst zwei Vorüberlegungen:

Satz 1.3. *Wenn d eine positive quadratfreie ganze Zahl ist, so hat $x^2 - y^2 = 1$ (Pell'sche Gleichung) unendlich viele ganzzahlige Lösungen. Des Weiteren exisitert eine Lösung (x_1, y_1), sodass jede Lösung die Form $\pm(x_n, y_n)$ hat, wobei $x_n + \sqrt{d}y_n = (x_1 + \sqrt{d}y_1)^n, n \in \mathbb{Z}$*

Beweis. Kapitel 17, Abschnitt 5. □

Lemma 1.4. *Sei $d > 0$ und $M \in \mathbb{R}$. Dann existieren nur endlich viele $\alpha \in D$, sodass $|\alpha| < M$ und $|\sigma(\alpha)| < M$.*

Beweis. Das Lemma folgt schon aus der allgemeineren Betrachtung von Elementen der Form $\alpha = x + \sqrt{d}y$, wobei $x, y \in \frac{1}{2}\mathbb{Z}$ und den dazugehörigem $\alpha' = x - \sqrt{d}y$. Hier sieht man schnell, dass es nicht unendlich viele Möglichkeiten für $x, y \in \mathbb{Z}$ geben kann, sodass $|\alpha| < M$ und $|\alpha'| < M$. □

Nun bestimmen wir die Einheitengruppe von D im reellen quadratischen Körper F:

Satz 1.5. *Wenn $d > 0$, dann exisitiert eine Einheit $\epsilon > 1$, sodass jede Einheit von der Form $\pm\epsilon^m, m \in \mathbb{Z}$. Diese nennt man Fundamentaleinheit. Also $U_d \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.*

Beweis. Nach Satz 1.3 exisitieren $x, y \in \mathbb{Z}$, sodass $x^2 - dy^2 = 1$ und $u = x + \sqrt{d}y > 1$ ist. Nach Lemma 1.1 ist u dann eine Einheit.
Sei $M \in \mathbb{R}$ eine fixe reelle Zahl. Nach Lemma 1.4 existieren nur endlich viele $\alpha \in D$, sodass $|\alpha| < M$ und $|\sigma(\alpha)| < M$, also auch nur endlich viele Einheiten $\beta \in U_d$ mit dieser Eigenschaft. Jedoch sieht man leicht, dass für alle Einheiten $\beta \in U_d$ mit $1 < \beta < M$ gilt, dass $|\sigma(\beta)| < M$. Also gibt es nur endlich viele Einheiten $\beta \in U_d$ mit $1 < \beta < M$ und mindestens eine (u).
Sei ϵ die kleinste Einheit die größer als 1 ist und sei ß*tau* eine weitere Einheit > 0. Es existiert nun ein $s \in \mathbb{Z}$, sodass $\epsilon^s \leq \tau < \epsilon$. Durch multiplizieren mit ϵ^{-s} erhält man

$$1 \leq \tau\epsilon^{-s} < \epsilon.$$

$\tau\epsilon^{-s}$ ist eine Einheit. Deshalb muss $\tau\epsilon^{-s} = 1$ sein, also $\tau = \epsilon^s$.
Für negative τ kann man die gleiche Argumentation mit $-\tau$ durchführen. □

2 Kreisteilungskörper

Sei $m \in \ltimes$ und $\zeta_m = e^{2\pi i/m}$. Die Zahl und alle Potenzen dieser erfüllen $x^m - 1 = 0$. Folglich haben wir $x^m - 1 = (x-1)(x-\zeta_m)\dots(x-\zeta_m^{m-1})$. Also ist $F = \mathbb{Q}(\zeta_m)$ der Zerfällungskörper von $x^m - 1$. Da $x^m - 1$ seperabel ist, ist $F/\mathbb{Q}(\zeta_m)$ eine Galoiserweiterung. Wir nennen $F = \mathbb{Q}(\zeta_\gg)$ den Kreisteilungskörper der m-ten Einheitswurzel.

Satz 2.1. *Sei G die Galoisgruppe von $F/\mathbb{Q}$. Dann existiert ein Monomorphismus $\Theta : G \longrightarrow (\mathbb{Z}/m\mathbb{Z})^x$, sodass für alle $\sigma \in G$ gilt:*

$$\zeta_m = \zeta_m^{\Theta(\sigma)}. \tag{1}$$

Beweis. Sei Θ so definiert wie in (1). Zeige zunächst, dass $\Theta : G \longrightarrow \mathbb{Z}/m\mathbb{Z}$.
Da $\zeta_m^m = 1$, haben wir $(\sigma\zeta_m)^m = 1$. Also muss $\Theta(\sigma)$ eine ganze Zahl $\bmod m$ sein.
Nun muss noch gezeigt werden, dass $\Theta(\sigma) \in (\mathbb{Z}/m\mathbb{Z})^x$ also invertierbar ist. Dafür betrachtet man

$$\zeta_m = \sigma^{-1}\sigma\zeta_m = \sigma^{-1}(\sigma\zeta_m^{\Theta(\sigma)}) = \zeta_m^{\Theta(\sigma^{-1})\Theta(\sigma)}.$$

Also ist $\Theta(\sigma^{-1})\Theta(\sigma) \cong 1 \mod m$, also ist $\Theta : G \longrightarrow (\mathbb{Z}/m\mathbb{Z})^x$.
Dass Θ ein Homomorphismus ist, ist klar. Dass Θ injektiv ist, sieht man ein durch $\Theta^{-1}(\{1\}) = \{\sigma \in G | \sigma\zeta_m = \zeta_m\} = \{id\}$ □

Korollar 2.2. $[\zeta_> : \mathbb{Q}]$ *teilt* $\phi(m)$

Beweis. Wie in Algebra gesehen, ist $[\zeta_> : \mathbb{Q}] = |G|$ Nach Isomorphiesätzen, dem Satz von Lagrange und Satz 2.1 folgt die Behauptung. □

Definition 2.3. *Sei* $\Phi_m(x) = \prod_{(a,m)=1}(x - \zeta_m^a)$*, wobei* $1 \leq a < m$*. Dieses Polynom nennt man das Kreisteilungspolynom.*

Bemerkung: Die Wurzeln von $\Phi_m(x)$ sind genau die primitiven m-ten Einheitswurzeln, d.d. m-te Einheitswurzeln von Ordnung m. Der Grad des Polynoms ist $\phi(m)$.

Satz 2.4. $x^m - 1 = \prod_{d|m} \Phi_m(x) = \prod_{d|m} \Phi_{m/d}(x)$

Beweis.

$$x^m - 1 = \prod_{i=0}^{m-1}(x - \zeta_m^i) = \prod_{d|m} \prod_{(i,m)=d} (x - \zeta_m^i)$$

Behauptung: $\prod_{(i,m)=d}(x - \zeta_m^i) = \Phi_{m/d}(x)$
Um dies zu zeigen, beachten wir, dass $(i, m) = d$ impliziert, dass $i = dj$ für ein $j \in \mathbb{N}$. Dann gilt

$$\zeta_m^i = \zeta_m^{dj} = \zeta_{m/d}^j.$$

Des Weiteren ist $(j, m/d) = 1$. Also gilt

$$\prod_{(i,m)=d} (x - \zeta_m^i) = \prod_{(j,m/d)=1} (x - \zeta_m^j) = \Phi_{m/d}$$

□

Korollar 2.5. $\Phi_m \in \mathbb{Z}[X]$

Beweis. Wir führen eine Induktion über m durch. Wenn $m = 1$ ist, dann ist $\Phi_1(x) = x - 1 \in \mathbb{Z}$. Sei nun $m > 1$ und die Behauptung gelte für alle kleineren m. Nach Satz 2.4 gilt nun

$$x^m - 1 = \prod_{d|m} \Phi_m(x) = \prod_{\substack{d|m \\ d \neq m}} \Phi_d(x) \cdot \Phi_m(x).$$

Da $x^m - 1 \in \mathbb{Z}[X]$ und $\prod_{\substack{d|m \\ d \neq m}} \Phi_d(x) \in \mathbb{Z}[X]$ nach Induktionsvorraussetzung, ist nun $\Phi_m(x) \in \mathbb{Q}[X]$.
Behauptung: Die Koeffizienten von Φ_m sind ganzalgebraisch.
Dies gilt, da die Koeffizienten Summen von Zahlen der Form $k\zeta_m^a, 0 \leq a \leq m - 1$ sind. Da diese Zahlen klar ganzalgebraisch sind und Summen von ganzalgebraischen Zahlen auch ganzalgebraisch sind, sind die Koeffizienten ganzalgebraisch.
Nun wissen wir, dass die einzigen ganzalgebraischen Zahlen in $\mathbb{Q}$ in $\mathbb{Z}$ liegen. Also sind die Koeffizienten in $\mathbb{Z}$ und die Behauptung ist gezeigt. □