Prof. Dr. H. Brenner **Osnabrück WS 2020/2021**

Algebraische Zahlentheorie

Vorlesung 29

Wir besprechen in verschiedenen Beispielen genauer, wie die Einheitengruppe eines Zahlbereiches aussieht und wie Fundamentaleinheiten zu finden sind. Nach dem Dirichletschen Einheitensatz, den wir in der letzten Vorlesung bewiesen haben, ist der Rang der Einheitengruppe eines Zahlbereichs R mit r reellen Einbettungen und s Paaren von komplexen Einbettungen gleich $r+s-1$.

Der Rang der Einheitengruppe $r+s-1$ ist in zwei Fällen gleich 0, nämlich bei $R = \mathbb{Z}$ und wenn R ein imaginär-quadratischer Zahlbereich ist. In diesem Fall wurden die möglichen Einheitengruppen (= Einheitswurzelgruppen) in Lemma 27.7 besprochen. Für den Rang $r+s-1 = 1$, also $r+s = 2$, gibt es die folgenden Möglichkeiten:

(1) $r = 2$ und $s = 0$. Dann ist der Grad der Körpererweiterung gleich 2 und es handelt sich um eine reell-quadratische Körpererweiterung.
(2) $r = 1$ und $s = 1$. Dann ist der Grad der Körpererweiterung gleich 3. Das Minimalpolynom der Körpererweiterung ist ein kubisches Polynom mit genau einer reellen Nullstelle, beispielsweise $\mathbb{Q} \subset K \cong \mathbb{Q}[X]/(X^3-2)$.
(3) $r = 0$ und $s = 2$. Dann ist der Grad der Körpererweiterung gleich 4. Das Minimalpolynom der Körpererweiterung ist ein Polynom vom Grad 4 ohne reelle Nullstelle. Ein Beispiel ist $\mathbb{Q} \subset K \cong \mathbb{Q}[X]/(X^4+X^3+X^2+X+1)$, der fünfte Kreisteilungskörper.

Fundamentaleinheiten im reell-quadratischen Fall

LEMMA 29.1. *Es sei A_D ein reell-quadratischer Zahlbereich zu quadratfreiem $D \geq 2$ und sei $A_D \subseteq \mathbb{R}$ eine fixierte reelle Einbettung. Dann besitzt $A_D^\times \cap \mathbb{R}_{>1}$ ein Minimum und dieses ist eine Fundamentaleinheit.*

Beweis. Die Einheitengruppe von A_D ist nach Korollar 28.10 isomorph zu $\{1,-1\} \times \mathbb{Z}$, alle Einheiten sind von der Form $\pm u^n$ mit $n \in \mathbb{Z}$ und einer Fundamentaleinheit u. Diese Beschreibung gilt auch in der Einbettung nach $\mathbb{R}$. Mit u ist genauso $-u$ und u^{-1} eine Fundamentaleinheit. Damit können wir $u > 1$ annehmen. Zwischen 1 und u kann es keine weitere Einheit aus A_D geben, da sie ja die Form $\pm u^n$ besitzt, was bei negativem Vorzeichen negativ ist und bei (positivem Vorzeichen und) $n \leq 0$ zwischen 0 und 1 liegt. Für $n \geq 2$ ist $u^n > u$. □

Wir werden die Fundamentaleinheit > 1 (bezüglicher einer reellen Einbettung) häufig als die Fundamentaleinheit schlechthin bezeichnen. Man beachte, dass das Bild der Einbettung $A_D \subseteq \mathbb{R}$ eine dichte Teilmenge ist. Zwischen 1 und der gewählten Fundamentaleinheit u gibt es also unendlich viele Zahlen aus A_D, aber eben keine weiteren Einheiten.

LEMMA 29.2. *Es sei A_D ein reell-quadratischer Zahlbereich zu quadratfreiem $D \geq 2$ und sei $A_D \subseteq \mathbb{R}$ eine fixierte reelle Einbettung. Dann sind für jede Einheit $a + b\sqrt{D} \in A_D^\times \cap \mathbb{R}_{>1}$ die Komponenten a und b positiv.*

Beweis. Mit $a + b\sqrt{D}$ sind auch $-a - b\sqrt{D}, a - b\sqrt{D}, -a + b\sqrt{D}$ Einheiten, wobei diese drei Elemente kleiner als 1 sind, da konjugierte Elmente im quadratischen Fall bis eventuell auf das Vorzeichen invers zueinander sind. Deshalb ist $a+b\sqrt{D} > a-b\sqrt{D}$, woraus $b > 0$ folgt, und $a+b\sqrt{D} > -a+b\sqrt{D}$, woraus $a > 0$ folgt. □

LEMMA 29.3. *Es sei A_D ein reell-quadratischer Zahlbereich zu quadratfreiem $D \geq 2$ und sei $A_D \subseteq \mathbb{R}$ eine fixierte reelle Einbettung. Dann ist die Fundamentaleinheit $a + b\sqrt{D} \in A_D^\times \cap \mathbb{R}_{>1}$ dadurch charakterisiert, dass bei ihr unter allen Einheiten $a' + b'\sqrt{D} \in A_D^\times \cap \mathbb{R}_{>1}$ die erste Komponente minimal ist.*

Beweis. Nach Lemma 29.1 gibt es eine Fundamentaleinheit $a + b\sqrt{D}$, und diese ist unter den Einheiten oberhalb von 1 minimal. Sei $a' + b'\sqrt{D}$ eine weitere solche Einheit > 1. Dann ist diese von der Form

$$\begin{aligned} a' + b'\sqrt{D} &= \left(a + b\sqrt{D}\right)^n \\ &= a^n + \binom{n}{2} a^{n-2} b^2 D + \ldots \left(\binom{n}{1} a^{n-1} b^1 + \ldots \right) \sqrt{D} \end{aligned}$$

mit $n \geq 2$. Bei $a \geq 1$ folgt daraus sofort, dass $a' \geq a$, und bei $a < 1$ kommt wegen Lemma 29.2 nach Satz 9.8 nur $a = \frac{1}{2}$ in Frage, was überhaupt (unabhängig von der Einheitenbedingung) das Minimum für die erste Komponente ist. □

Explizit geht es bei $D = 2, 3 \mod 4$ um die Lösungen der Gleichung

$$a^2 - Db^2 = \pm 1$$

mit a, b ganzzahlig und bei $D = 1 \mod 4$ um Lösungen der Gleichung

$$\left(\frac{a}{2}\right)^2 - D\left(\frac{b}{2}\right)^2 = \pm 1$$

mit a, b ganzzahlig mit $a + b$ geradzahlig, was auf die ganzzahlige Gleichung

$$a^2 - Db^2 = \pm 4$$

führt. Diese Gleichung (en) nennt man auch die *Pellsche Gleichung*, wobei der Sprachgebrauch nicht einheitlich ist. Die Gleichung in der letzten Form

erfasst jedenfalls alle Möglichkeiten, wobei nicht jede Lösung zu einer Einheit führt, beispielsweise entspricht

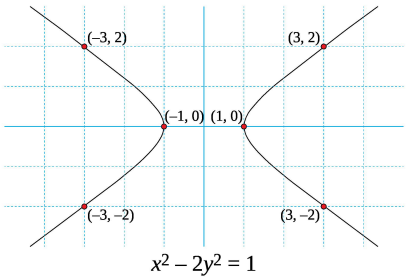
$$(a, b) \;=\; (2, 0)$$

direkt keiner Lösung (die Hälfte davon aber wiederum schon).

Bemerkung 29.4. Mit Lemma 29.3 kann man prinzipiell konstruktiv eine Fundamentaleinheit bestimmen, indem man zu aufsteigendem $a > 0$ (ganzzahlig oder ein ganzzahliges Vielfaches von $\frac{1}{2}$) untersucht, ob die Gleichung

$$a^2 - b^2 D \;=\; \pm 1$$

eine Lösung in b besitzt, wofür nur endlich viele Kandidaten zu überprüfen sind. Man hat aber von vornherein keine Schranke für a, daher weiß man nicht, wie schnell diese Methode zum Erfolg führt.



Beispiel 29.5. In $\mathbb{Z}[\sqrt{2}]$ ist wegen

$$(1 + \sqrt{2})(1 - \sqrt{2}) \;=\; 1 - 2 \;=\; -1$$

das Element $1 + \sqrt{2}$ eine Einheit. Nach Lemma 29.3 handelt es sich um die eindeutig bestimmte Fundamentaleinheit > 1.

Beispiel 29.6. Wir suchen in $\mathbb{Z}[\sqrt{3}]$ gemäß Bemerkung 29.4 nach der Fundamentaleinheit, nach Satz 9.8 müssen wir nur $a + b\sqrt{3}$ mit ganzzahligen $a, b \geq 1$ überprüfen, ob

$$N(a + b\sqrt{3}) \;=\; a^2 - 3b^2 \;=\; \pm 1$$

gilt. Für $a = 1$ gibt es keine Lösung, und bei $a = 2$ ist mit $b = 1$ eine Lösung gefunden. Somit ist $2 + \sqrt{3}$ die Fundamentaleinheit. Die anderen Einheiten oberhalb von 1 sind $\left(2 + \sqrt{3}\right)^2 = 7 + 4\sqrt{3}$, $\left(2 + \sqrt{3}\right)^3 = 26 + 15\sqrt{3}$, u.s.w.

Für quadratfreies $D \geq 2$ kann man so algorithmisch die Fundamentaleinheit $u > 1$ des quadratischen Zahlbereiches A_D bestimmen. Für kleine D ergibt sich die folgende Tabelle.

D	2	3	5	6	7	10	11	13	14	15
u	$1+\sqrt{2}$	$2+\sqrt{3}$	$\frac{1+\sqrt{5}}{2}$	$5+2\sqrt{6}$	$8+3\sqrt{7}$	$3+\sqrt{10}$	$10+3\sqrt{11}$	$18+5\sqrt{13}$	$15+4\sqrt{14}$	$4+\sqrt{15}$

Die Norm der Fundamentaleinheit ist wie von jeder Einheit gleich 1 oder -1. Es ist eine interessante Frage, ob die Fundamentaleinheit die Norm 1 oder -1 ist. Für $D = 2, 5, 10, 13, 17, ...$ ist die Norm der Fundamentaleinheit gleich -1.

Weitere Beispiele

Beispiel 29.7. Wir betrachten den Zahlbereich $R = \mathbb{Z}[\sqrt[3]{2}]$ vom Grad 3, eine Ganzheitsbasis ist $1, \sqrt[3]{2}, \sqrt[3]{2}^2$ nach Korollar 16.2. Es ist

$$(1-\sqrt[3]{2})(1+\sqrt[3]{2}+\sqrt[3]{2}^2) = 1-\sqrt[3]{2}^3 = 1-2 = -1.$$

d.h. das Element $1-\sqrt[3]{2}$ ist eine Einheit, und zwar keine Einheitswurzel.

In Fröhlich/Taylor wird erwähnt, dass in $\mathbb{Q}[\sqrt[3]{23}]$ das Element

$$2166673601 + 761875860\sqrt[3]{23} + 267901370\sqrt[3]{23}^2$$

eine Fundamentaleinheit ist.

Beispiel 29.8. Der fünfte Kreisteilungskörper (vergleiche Beispiel 17.5) die Gestalt

$$K_5 \cong \mathbb{Q}[X]/\left(X^4+X^3+X^2+X+1\right)$$

und die komplexen Einbettungen sind durch $X \mapsto e^{j2\pi \mathrm{i}/5}$ mit $j = 1, 2, 3, 4$ gegeben, wobei die Einbettungen zu 1 und 4 und zu 2 und 3 zueinander komplex-konjugiert sind. Es gibt keine reelle Einbettung und es ist $r = 0$ und $s = 2$. Der Rang der Einheitengruppe ist also 1 nach Satz 28.7. Wegen $\mathbb{Q} \subset \mathbb{Q}[\sqrt{5}] \subset K_5$ gibt es einen reellen Zwischenkörper und dieser enthält auch schon eine Einheitengruppe vom Rang 1. Es ist

$$\frac{1+\sqrt{5}}{2} = x^4+x+1 = -x^2-x^3$$

und wegen

$$\frac{1+\sqrt{5}}{2} \cdot \frac{1-\sqrt{5}}{2} = -1$$

ist dies eine Einheit im quadratischen Zahlbereich zu 5, und zwar nach Lemma 29.3 die Fundamentaleinheit > 1.

Der Regulator

Definition 29.9. Es sei R ein Zahlbereich mit r reellen Einbettungen und s Paaren von komplexen Einbettungen und es sei $u_1, \ldots, u_{r+s-1}$ ein System

von Fundamentaleinheiten. Dann nennt man den Betrag der Determinante der reellen $(r+s-1)\times(r+s-1)$-Matrix

$$\begin{pmatrix} L_1(u_1) & \dots & L_1(u_{r+s-1}) \\ \vdots & \ddots & \vdots \\ L_{r+s-1}(u_1) & \dots & L_{r+s-1}(u_{r+s-1}) \end{pmatrix},$$

wobei $L = (L_1, \dots, L_{r+s})$ die logarithmische Gesamtabbildung bezeichnet, den *Regulator* von R. Er wird mit $\mathrm{Reg}(R)$ bezeichnet.

Man beachte, dass in der Definition des Regulators nur $r+s-1$ Komponenten der (logarithmischen) Gesamtabbildung verwendet werden. Das Bild der Einheiten liegt ja in einer Hyperebene des $\mathbb{R}^{r+s}$, ist also dort nicht volldimensional. Wir werden gleich sehen, dass es zur Berechnung egal ist, welche Komponente man weglässt. Wenn $r+s=1$ ist (wie bei $\mathbb{Z}$ oder einem imaginär-quadratischen Zahlbereich), so ist die Definition als 1 zu interpretieren (Determinante der leeren Matrix).

Lemma 29.10. *Es sei R ein Zahlbereich mit r reellen Einbettungen und s Paaren von komplexen Einbettungen und es sei $u_1, \dots, u_{r+s-1}$ ein System von Fundamentaleinheiten von R. Es sei Λ das von $L(u_1), \dots, L(u_{r+s-1})$ im Untervektorraum $H = \left\{(v_1, \dots, v_{r+s}) \mid \sum_{j=1}^{r+s} v_j = 0\right\} \subset \mathbb{R}^{r+s}$ erzeugte Gitter. Dann besteht zwischen dem Regulator und dem Volumen einer Grundmasche $\mathfrak{M}$ von Λ der Zusammenhang*

$$\sqrt{r+s} \cdot \mathrm{Reg}(R) = \mathrm{vol}(\mathfrak{M}).$$

Beweis. Siehe Aufgabe 29.13. □

Dies zeigt insbesondere, dass es bei der Definition des Regulators auf die Reihenfolge der Einbettungen nicht ankommt und man eine beliebige Komponente weglassen kann.

Bemerkung 29.11. Es sei $D \geq 2$ quadratfrei und A_D der zugehörige reell-quadratische Zahlbereich. Es sei $A_D \subseteq \mathbb{R}$ eine reelle Einbettung und sei u eine Fundamentaleinheit von R. Dann ist der Regulator von A_D gleich

$$\mathrm{Reg}(A_D) = |\ln |u||.$$

An dieser Definition sieht man direkt, dass wenn man u durch eine der anderen Fundamentaleinheiten $-u, u^{-1}, -u^{-1}$ ersetzt, dies zum gleichen Ergebnis führt: Das Vorzeichen wird durch den inneren Betrag und die Inversenbildung durch den äußeren Betrag aufgefangen. Auch von der gewählten Einbettung hängt es nicht ab, da ja die andere Einbettung aus der gegebenen Einbettung durch einen Automorphismus hervorgeht und dabei u auf eines der drei Elemente abgebildet wird.

Abbildungsverzeichnis