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

Algebraische Zahlentheorie

Vorlesung 27

Einheitswurzeln in Zahlbereichen

Eine Einheitswurzel in einem kommutativen Ring R ist das gleiche wie eine Torsionseinheit, also ein Element $x \in R$ mit $x^n = 1$ für ein $n \in \mathbb{N}_+$. Die Menge aller Einheitswurzeln bilden eine Untergruppe der Einheitengruppe $R^\times$. Wir bezeichnen sie mit $\mu(R)$. Ebenso bildet die Menge aller n-ten Einheitswurzeln eine Untergruppe, die wir mit $\mu_n(R)$ bezeichnen. Da eine n-te Einheitswurzel eine Nullstelle des Polynoms $X^n - 1$ ist, gibt es über einem Körper und damit auch über einem Integritätsbereich nach Korollar 19.9 (Lineare Algebra (Osnabrück 2017-2018)) maximal n Nullstellen. Für einen Integritätsbereich ist also $\mu_n(R)$ eine endliche Gruppe mit höchstens n Elementen. Nach Satz 9.5 (Körper- und Galoistheorie (Osnabrück 2018-2019)) handelt es sich um eine zyklische Gruppe. Wenn sie die Ordnung n besitzt, so nennt man einen Erzeuger eine *primitive Einheitswurzel*. Für die abstrakte multiplikative geschrieben zyklische Gruppe mit n Elementen schreiben wir μ_n und die Eigenschaft, dass ein Körper K n n-te Einheitswurzeln besitzt schreiben wir kurz als $\mu_n \subseteq K$.

Lemma 27.1. *Es sei R ein normaler Integritätsbereich mit Quotientenkörper $Q(R)$. Dann ist $\mu(R) = \mu(Q(R))$.*

Beweis. Die Inklusion $\mu(R) \subseteq \mu(Q(R))$ ist klar. Sei $q \in \mu(Q(R))$, sagen wir $q^n = 1$. Da q die Ganzheitsgleichung

$$X^n - 1 = 0$$

erfüllt, folgt aus der Normalität direkt, dass $q \in R$ gehört. □

Diese Beobachtung kann man für Zahlbereiche anwenden. Wir werden im Folgenden die Aussagen für die Zahlbereiche formulieren, wobei die Argumente teilweise über die Quotientenkörper, also über endliche Erweiterungen von $\mathbb{Q}$, gehen, teilweise über den Zahlbereich selbst. Ohne die Voraussetzung normal ist die Aussage nicht richtig, wie das folgende Beispiel zeigt.

Beispiel 27.2. Wir betrachten den Ring

$$R = \mathbb{Z}[2\mathrm{i}] \subseteq \mathbb{Z}[\mathrm{i}] \subseteq \mathbb{Q}[\mathrm{i}] = K.$$

Der Quotientenkörper von R ist $\mathbb{Q}[\mathrm{i}]$, R ist nicht normal. In R gibt es nur die Einheitswurzeln 1 und -1, im Quotientenkörper gibt es dagegen die Einheitswurzeln $1, -1, \mathrm{i}, -\mathrm{i}$.

Lemma 27.3. *Es sei R ein Zahlbereich, für den es zumindest eine reelle Einbettung gebe. Dann ist die Gruppe der Einheitswurzeln $\mu(R)$ gleich $\{1,-1\}$.*

Beweis. Dies folgt direkt aus einer Inklusion $R \subseteq Q(R) \subseteq \mathbb{R}$, da es in $\mathbb{R}$ nur die beiden Einheitswurzeln 1 und -1 gibt und da Einheitswurzeln unter einem Ringhomomorphismus auf Einheitswurzeln abgebildet werden. □

In den komplexen Zahlen gibt es alle Einheitswurzeln. Die Kreisteilungskörper und Kreisteilungsringe zeigen, dass man Einheitswurzeln in endlichen Erweiterungen von $\mathbb{Q}$ bzw. $\mathbb{Z}$ realisieren lassen. Die folgenden Aussagen zeigen, dass die Kreisteilungskörper im Wesentlichen durch ihre enthaltenen Einheitswurzeln bestimmt sind.

Lemma 27.4. *Es sei K ein Körper der Charakteristik 0 und sei $n \in \mathbb{N}$. Dann enthält K genau dann eine primitive n-te Einheitswurzel, wenn für den n-ten Kreisteilungskörper $K_n \subseteq K$ gilt.*

Beweis. Die eine Richtung ist klar. Für die Rückrichtung sei $\zeta \in K$ eine primitive n-te Einheitswurzel. Dies definiert einen Einsetzungshomomorphismus

$$\mathbb{Q}[X]/(X^n-1) \longrightarrow K,\, X \longmapsto \zeta.$$

Somit gibt es nach Lemma 19.9 (Körper- und Galoistheorie (Osnabrück 2018-2019)) einen induzierten Ringhomomorphismus

$$\mathbb{Q}[X]/(\Phi_d) \longrightarrow K$$

mit einem Teiler d von n. Doch dann gibt es auch einen Ringhomomorphismus

$$\mathbb{Q}[X]/(X^d-1) \longrightarrow K,\, X \longmapsto \zeta.$$

Bei $d < n$ ist dies ein Widerspruch zur Ordnung von ζ. Also ist $d = n$ und es gibt einen Ringhomomorphismus

$$K_n = \mathbb{Q}[X]/(\Phi_n) \longrightarrow K.$$

□

Lemma 27.5. *Die Einheitswurzelgruppe des n-ten Kreisteilungskörpers K_n ist*

$$\mu(K_n) = \mu_n$$

bei n gerade und

$$\mu(K_n) = \mu_{2n}$$

bei n ungerade.

Beweis. Nach Konstruktion der Kreisteilungskörper ist klar, dass K_n die n-ten Einheitswurzeln enthält. Wenn n ungerade und ζ eine primitive n-te Einheitswurzel ist, so ist $-\zeta$ eine primitive $2n$-te Einheitswurzel und somit sind die Inklusionen $\supseteq$ klar. Es ist also noch zu zeigen, dass die Kreisteilungskörper keine weiteren Einheitswurzeln enthält. Dazu können wir annehmen, dass n gerade ist. Sei ξ eine zusätzliche Einheitswurzel der Ordnung m. Wir können

annehmen, dass m gerade und ein echtes Vielfaches von n ist, da die von ξ und einer primitiven n-ten Einheitswurzel ζ erzeugte Untergruppe wieder endlich und zyklisch und ihre Ordnung ein Vielfaches der beiden Ordnungen sein muss. Aus $\mu_m \subseteq K_n$ folgt $K_m \subseteq K_n$ nach Lemma 27.4. Es ist $m = 2^r p_1^{r_1} \cdots p_k^{r_k}$ und $n = 2^s p_1^{s_1} \cdots p_k^{s_k}$ mit $r \geq s \geq 1$ und $r_j \geq s_j \geq 1$. Da ein Exponent echt größer ist, ergibt sich ein Widerspruch zu Satz 17.10. □

LEMMA 27.6. *Es sei R ein Zahlbereich. Dann ist $\mu(R)$ endlich und zyklisch.*

Beweis. Wir argumentieren in der endlichen Erweiterung $\mathbb{Q} \subseteq K = Q(R)$, die den Grad d habe. Wir behaupten zunächst, dass die Ordnungen in $\mu(K)$ beschränkt ist. Nehmen wir an, dass dies nicht der Fall ist, und sei r_n, $n \in \mathbb{N}$, eine streng wachsende (und damit unbeschränkte) Folge von natürlichen Zahlen, die als Ordnungen von Elementen aus $\mu(K)$ vorkommen. Dann gilt nach Lemma 27.4 für die Kreisteilungskörper

$$K_{r_n} \subseteq K.$$

Für der Grad d gilt dann unter Verwendung von Satz 17.10

$$d \geq \operatorname{grad}_{\mathbb{Q}} K_{r_n} = \varphi(r_n).$$

Wenn in den Primfaktorzerlegungen der Folgenglieder r_n unendlich viele Primzahlen p_m vorkommen, so ist

$$d \geq p_m - 1.$$

Wenn hingegen in den Primfaktorzerlegungen nur endlich viele Primzahlen vorkommen, so gibt es darin eine Teilfolge mit Primzahlpotenzen p^{s_k} als Teiler mit $s_k \to \infty$. In diesem Fall ist $d \geq (p-1)p^{s_k-1}$. In beiden Fällen ergibt sich ein Widerspruch zur Endlichkeit von d. Die Endlichkeit der Gruppe folgt daher mit Korollar 19.9 (Lineare Algebra (Osnabrück 2017-2018)). Die Zyklizität folgt aus Satz 9.5 (Körper- und Galoistheorie (Osnabrück 2018-2019)). □

LEMMA 27.7. *Es sei R der imaginär-quadratische Zahlbereich mit Diskriminante $\triangle$. Dann stimmt die Einheitengruppe $R^\times$ mit der Einheitswurzelgruppe $\mu(R)$ überein. Für diese gibt es die folgenden drei Möglichkeiten.*

(1) *Bei $\triangle = -3$ ist $\mu(R) \cong \mathbb{Z}/(6)$.*
(2) *Bei $\triangle = -4$ ist $\mu(R) \cong \mathbb{Z}/(4)$.*
(3) *Bei $\triangle \leq -5$ ist $\mu(R) = \{1, -1\} \cong \mathbb{Z}/(2)$.*

Beweis. Wegen der expliziten Gestalt der Norm und Lemma 10.1 ist die Einheitengruppe endlich, stimmt also mit der Einheitswurzelgruppe überein. Es sei A der quadratische Zahlbereich zur quadratfreien Zahl $D \leq -1$. Bei $D = -1$ ist A der Ring der Gaußschen Zahlen und es gibt die vier Einheiten $1, -1, \mathrm{i}, -\mathrm{i}$, und es ist $\triangle = -4$ nach Lemma 9.9. Dies ist der einzige quadratische Zahlbereich mit Diskriminante -4. Bei $D = \triangle = -3$

liegt der Ring der Eisensteinzahlen vor, siehe Beispiel 7.4. Er ist zugleich der dritte und der sechste Kreisteilungsring und seine Einheitswurzelgruppe ist nach Lemma 27.5 gleich $\mathbb{Z}/(6)$. Sei also die Diskriminante ≤ -5. Die Norm von $a+b\sqrt{D} \in \mathbb{Q}[\sqrt{D}]$ (mit $a,b \in \mathbb{Q}$) ist durch $a^2+b^2\,|D|$ gegeben. Wenn das Element zum Ganzheitsring gehört, so sind bei $D = 2,3 \mod 4$ nach Satz 9.8 die Koeffizienten a,b ganzzahlig und aus $|D| \geq 2$ folgt $b=0$ und aus Lemma 10.1 folgt $a = \pm 1$. Bei $D = 1 \mod 4$ sind ebenfalls nach Satz 9.8 die Koeffizienten a,b ganzzahlige Vielfache von $1/2$ und aus $|D| \geq 7$ folgt wieder $b=0$ und $a = \pm 1$. □

Zu einer kommutativen Gruppe H bezeichnen wir die Menge der Automorphismen mit $\mathrm{Aut}(H)$. Dies ist selbst eine Gruppe mit der Hintereinanderschaltung als Verknüpfung. Für die kommutative Gruppe $\mathbb{Z}/(n)$ ist ein Gruppenhomomorphismus in sich durch das Bild des Erzeugers festgelegt, und ein Automorphismus liegt genau dann vor, wenn der Erzeuger auf einen Erzeuger abgebildet wird. Deshalb ist

$$\mathrm{Aut}\,(\mathbb{Z}/(n)) \cong (\mathbb{Z}/(n))^\times,$$

einer Einheit a rechts entspricht der Gruppenhomomorphismus $x \mapsto ax$. Für μ_n, die multiplikativ geschriebene zyklische Gruppe der Ordnung n, gilt entsprechend

$$\mathrm{Aut}\,(\mu_n) \cong (\mathbb{Z}/(n))^\times,$$

und der Einheit a entspricht das Potenzieren $x \mapsto x^a$. Die Beschreibung der Galoisgruppe für Kreisteilungskörper aus Satz 17.11 kann man somit als einen Gruppenisomorphismus

$$\mathrm{Gal}\,(K_n|\mathbb{Q}) \cong \mathrm{Aut}(\mu_n)$$

verstehen. Zwischen diesen beiden Gruppen besteht nun stets der folgende Zusammenhang.

Lemma 27.8. *Es sei $\mathbb{Q} \subseteq K$ eine endliche Körpererweiterung mit der Galoisgruppe G und es sei*

$$\mu(K) = \mu_n$$

die Einheitswurzelgruppe zu K. Dann operiert G in natürlicher Weise auf $\mu(K)$, d.h. es gibt einen Gruppenhomomorphismus

$$G \longrightarrow \mathrm{Aut}(\mu(K)) = (\mathbb{Z}/(n))^\times,\ \sigma \longmapsto (\zeta \mapsto \sigma(\zeta)).$$

Wenn eine Galoiserweiterung vorliegt, so ist diese Abbildung surjektiv.

Beweis. Nach Voraussetzung enthält K die n-ten Einheitswurzeln und damit ist $K_n \subseteq K$ nach Lemma 27.4. Insbesondere ist $\mu(K) = \mu(K_n)$. Die Abbildung

$$\mathrm{Gal}\,(K_n|\mathbb{Q}) \longrightarrow \mathrm{Aut}(\mu(K)) \cong (\mathbb{Z}/(n))^\times$$

ist nach Satz 17.11 ein Isomorphismus. Wenn $\mathbb{Q} \subseteq K$ galoissch ist, so ist K nach Korollar 16.7 (Körper- und Galoistheorie (Osnabrück 2018-2019)) auch galoissch über K_n und die $\mathbb{Q}$-Automorphismen lassen sich wegen Korollar

15.8 (Körper- und Galoistheorie (Osnabrück 2018-2019)) nach K fortsetzen.
□

Abbildungsverzeichnis

Erläuterung: Die in diesem Text verwendeten Bilder stammen aus Commons (also von http://commons.wikimedia.org) und haben eine Lizenz, die die Verwendung hier erlaubt. Die Bilder werden mit ihren Dateinamen auf Commons angeführt zusammen mit ihrem Autor bzw. Hochlader und der Lizenz. 7

Lizenzerklärung: Diese Seite wurde von Holger Brenner alias Bocardodarapti auf der deutschsprachigen Wikiversity erstellt und unter die Lizenz CC-by-sa 3.0 gestellt. 7