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

Algebraische Zahlentheorie

Vorlesung 28

Der Dirichletsche Einheitensatz

Es sei R der Ganzheitsring zur endlichen Körpererweiterung $\mathbb{Q} \subseteq K$. In Satz 25.2 haben wir gesehen, dass das Bild der reellen Gesamteinbettung

$$\tau^{\mathbb{R}}(R) = \Gamma_R \subset \mathbb{R}^r \times \mathbb{C}^s$$

ein Gitter in $\mathbb{R}^r \times \mathbb{C}^s$ ist, wobei r die Anzahl der reellen Einbettungen und s die Anzahl der Paare von komplexen Einbettungen bezeichnet. Zu jedem von 0 verschiedene Element $f \in R$ ist $\tau^{\mathbb{R}}(f)$ in jeder reellen Komponente und in jeder komplexen Komponente von 0 verschieden (Real- oder Imaginäreteil kann aber 0 sein). Um die Einheitengruppe von R zu verstehen, betrachten wir die Abbildung

$$\left(\mathbb{R}^\times\right)^r \times \left(\mathbb{C}^\times\right)^s \longrightarrow \mathbb{R}^{r+s}, (x_1, \ldots, x_r; z_{r+1}, \ldots, z_{r+s}) \longmapsto$$
$$(\ln|x_1|, \ldots, \ln|x_r|; \ln|z_{r+1}|^2, \ldots, \ln|z_{r+s}|^2).$$

Man beachte, dass man für die komplexen Einbettungen die Werte

$$\ln|z_j\overline{z_j}| = \ln|z_j|^2 = 2\ln|z_j|$$

heranzieht. Insgesamt haben wir die Verknüpfung der folgenden Abbildungen

$$K^\times \xrightarrow{\tau^{\mathbb{R}}} \left(\mathbb{R}^\times\right)^r \times \left(\mathbb{C}^\times\right)^s \xrightarrow{|-|} \left(\mathbb{R}^\times\right)^r \times \left(\mathbb{R}^\times\right)^s \xrightarrow{\ln(-),2\ln(-)} \mathbb{R}^r \times \mathbb{R}^s,$$

wobei die funktionalen Ausdrücke komponentenweise zu verstehen sind. Da die Einbettungen und der Betrag multiplikativ sind und der Logarithmus die Multiplikation in die Addition überführt, liegt insgesamt ein Gruppenhomomorphismus

$$(K^\times, 1, \cdot) \longrightarrow (\mathbb{R}^{r+s}, 0, +)$$

vor. Wir sprechen von der *logarithmischen Gesamtabbildung* und bezeichnen sie mit L. Diese ist insbesondere für die Einheitengruppe $R^\times \subseteq K^\times$ wichtig.

Lemma 28.1. *Es sei R der Ganzheitsring zu einer endlichen Körpererweiterung $\mathbb{Q} \subseteq K$ mit r reellen Einbettungen und s Paaren von komplexen Einbettungen. Dann besitzt die logarithmische Gesamtabbildung*

$$L\colon K^\times \longrightarrow \mathbb{R}^{r+s}$$

die folgenden Eigenschaften.

(1) *Der Kern von L eingeschränkt auf $R^\times$ ist die Gruppe der Einheitswurzeln $\mu(R)$ und insbesondere eine endliche zyklische Gruppe.*

(2) *Das Bild $L(R^\times)$ liegt in der Hyperebene*

$$\begin{aligned} H &= \left\{ (u_1, \ldots, u_{r+s}) \mid \sum_{j=1}^{r+s} u_j = 0 \right\} \\ &\subset \mathbb{R}^{r+s}. \end{aligned}$$

(3) *Das Bild $L(R^\times)$ ist eine diskrete Untergruppe von $H \subset \mathbb{R}^{r+s}$.*

Beweis. (1) Es liegt eine Faktorisierung

$$R^\times \xrightarrow{\tau} \Gamma \setminus \{0\} \xrightarrow{\ell} \mathbb{R}^{r+s}$$

vor. Ein Element $f \in K^\times$ wird genau dann unter L auf den Nullvektor abgebildet, wenn $\tau(f)$ in jeder reellen oder komplexen Komponente den Betrag 1 besitzt. Diese Elemente liegen somit alle in einer beschränkten Teilmenge von $\mathbb{R}^r \times \mathbb{C}^s$ aber ja auch im Gitter Γ. Daher ist diese Menge endlich und daher ist wegen der Injektivität von τ auch die zugrunde liegende Menge in R endlich. Also haben diese Elemente endliche Ordnung und sind Einheitswurzeln. Umgekehrt ist ein Torsionselement der Einheitengruppe von R in jeder Einbettung ein Torsionselement und hat daher den Betrag 1, wird also unter L auf 0 abgebildet.

(2) Sei $f \in R^\times$ eine Einheit und sei

$$(\rho_1(f), \ldots, \rho_r(f); \sigma_{r+1}(f), \overline{\sigma_{r+1}}(f), \ldots, \sigma_{r+s}(f), \overline{\sigma_{r+s}}(f)$$

das totale komplexe Einbettungstupel. Nach Lemma 7.14 ist die Norm von f gleich

$$\begin{aligned} & \rho_1(f) \cdots \rho_r(f) \sigma_{r+1}(f) \cdot \overline{\sigma_{r+1}}(f) \cdots \sigma_{r+s}(f) \cdot \overline{\sigma_{r+s}}(f) \\ = \; & \rho_1(f) \cdots \rho_r(f) \left|\sigma_{r+1}(f)\right|^2 \cdots \left|\sigma_{r+s}(f)\right|^2. \end{aligned}$$

Nach Lemma 10.1 ist der Betrag davon gleich 1. Unter der logarithmischen Abbildung

$$\ln(|-|) : \left(\mathbb{R}^\times\right)^r \times \left(\mathbb{C}^\times\right)^{2s} \longrightarrow \mathbb{R}^r \times \mathbb{R}^{r+2s}$$

wird dieses Produkt auf die Summe abgebildet, somit gilt

$$\begin{aligned} & \sum_{j=1}^{r} \ln|\rho_j(f)| + \sum_{i=1}^{s} \ln|\sigma_{r+i}(f)| + \sum_{i=1}^{s} \ln|\overline{\sigma}_{r+i}(f)| \\ = \; & \sum_{j=1}^{r} \ln|\rho_j(f)| + 2\sum_{i=1}^{s} \ln|\sigma_{r+i}(f)| \\ = \; & 0. \end{aligned}$$

Die letzte Gleichung bedeutet gerade, dass $L(f)$ auf der Hyperebene H liegt.

(3) Es ist zu zeigen, dass das Bild $L(R^\times)$ mit jeder beschränkten Teilmenge von H einen endlichen Durchschnitt besitzt. Das Urbild einer beschränkten Teilmenge unter ℓ ist aber auch beschränkt, und der Durchschnitt mit dem Gitter Γ ist endlich.

□

Die Hyperebene im vorstehenden Lemma hat die reelle Dimension $r+s-1$, und darin ist das Bild eine diskrete Untergruppe. Es wird sich herausstellen, dass das Bild in dieser Hyperebene sogar ein Gitter ist, also von $r+s-1$ linear unabhängigen Vektoren erzeugt wird. Wir erläutern die Situation anhand von Beispielen kleinen Grades.

Beispiel 28.2. Zu quadratfreiem $D < 0$ und zugehörigem imaginär-quadratischen Zahlbereich $A_D \subseteq \mathbb{C}$ (vergleiche Beispiel 25.3) ist die logarithmische Gesamtabbildung durch

$$A_D \setminus \{0\} \longrightarrow \mathbb{R},\ (a+b\mathrm{i}\sqrt{|D|}) \longmapsto \ln\left(a^2+b^2\,|D|\right),$$

gegeben. Der minimale Wert von $a^2+b^2\,|D|$ ist 1 und das Bild der logarithmischen Abbildung liegt in $\mathbb{R}_{\geq 0}$. Hieran sieht man erneut, dass es in A_D nur Einheitswurzeln als Einheiten gibt, vergleiche Lemma 27.7.

Beispiel 28.3. Zu quadratfreiem $D \geq 2$ und zugehörigem reell-quadratischen Zahlbereich A_D mit der Gitterrealisierung

$$A_D \longrightarrow \mathbb{R}^2,\ (a+b\sqrt{D}) \longmapsto \begin{pmatrix} a+b\sqrt{D} \\ a-b\sqrt{D} \end{pmatrix},$$

(vergleiche Beispiel 25.4) ist die logarithmische Gesamtabbildung durch

$$A_D \setminus \{0\} \longrightarrow \mathbb{R}\times\mathbb{R},\ (a+b\sqrt{D}) \longmapsto \begin{pmatrix} \ln\left|a+b\sqrt{D}\right| \\ \ln\left|a-b\sqrt{D}\right| \end{pmatrix},$$

gegeben. Diese induziert für die Einheiten den Gruppenhomomorphismus

$$A_D^\times \longrightarrow \mathbb{R}\times\mathbb{R},\ (a+b\sqrt{D}) \longmapsto \begin{pmatrix} \ln\left|a+b\sqrt{D}\right| \\ \ln\left|a-b\sqrt{D}\right| \end{pmatrix},$$

wobei das Bild (wegen Lemma 28.1 (2) oder direkt) auf der Gegendiagonalen landet. Somit liegt ein Gruppenhomomorphismus $\left(A_D^\times,\cdot,1\right) \to (\mathbb{R},+,0)$ vor. Der Kern besteht aus $\{1,-1\}$ und das Bild ist eine diskrete Untergruppe von $\mathbb{R}$. Wir werden gleich sehen, dass das Bild die Form $\mathbb{Z}v$ mit $v \neq 0$ besitzt.

Beispiel 28.4. Wir knüpfen an Beispiel 25.5 an, also

$$R = \mathbb{Z}[X]/\left(X^3-3X+1\right).$$

Unter der logarithmischen Gesamtabbildung wird das Ringelement $a+b\alpha+c\alpha^2$ auf

$$\begin{pmatrix} \ln|a+b\alpha+c\alpha^2| \\ \ln|a+b(\alpha^2-2)+c(-\alpha^2-\alpha+4)| \\ \ln|a+b(-\alpha^2-\alpha+2)+c(\alpha+2)| \end{pmatrix}$$

bzw. $a+b\alpha+d\beta$ auf

$$\begin{pmatrix} \ln|a+b\alpha+d\beta| \\ \ln|a+b\beta+d(-\alpha-\beta)| \\ \ln|a+b(-\alpha-\beta)+d\alpha| \end{pmatrix}$$

abgebildet. Die Einheiten α bzw. β werden auf

$$\begin{pmatrix} \ln|\alpha| \\ \ln|\beta| \\ \ln|-\alpha-\beta| \end{pmatrix}$$

bzw.

$$\begin{pmatrix} \ln|\beta| \\ \ln|-\alpha-\beta| \\ \ln|\alpha| \end{pmatrix}$$

und diese Vektoren liegen auf der durch $x+y+z=0$ definierten Ebene. Die lineare Unabhängigkeit dieser beiden Vektoren kann man über die Determinante zeigen.

Die numerischen Werte der Nullstellen des Polynoms sind ungefähr

$$\alpha \sim 1,532,\ \beta \sim 0,347,\ \gamma \sim -1,879\,.$$

Die Determinante der oberen 2×2-Untermatrix ist ungefähr

$$\begin{aligned} \ln|\alpha|\ln|\alpha+\beta| - \ln\left(|\beta|\right)^2 &\sim 0,426\cdot 0,631-(-1.058)^2 \\ &\sim 0,89 \\ &\neq 0. \end{aligned}$$

Die Bilder der beiden Einheiten α und β sind also linear unabhängig und daher besteht zwischen den Einheiten selbst in R keine Beziehung der Form

$$\alpha^m = \beta^n$$

für $(m,n)\neq(0,0)$.

Bemerkung 28.5. Zu einem Körperautomorphismus φ der Ordnung $k\neq 1,2$ auf einer endlichen Körpererweiterung $\mathbb{Q}\subseteq K$ mit einer reellen Einbettung $K\subseteq\mathbb{R}$ und einem Element $\alpha\in K$ mit

$$\varphi(\alpha)\neq\pm\alpha$$

sind α und $\varphi(\alpha)$ exponentiell unabhängig, d.h. es besteht keine Relation der Form

$$\alpha^m = \varphi(\alpha)^n$$

mit $(m,n)\neq(0,0)$. Aus

$$\varphi(\alpha) = \alpha^q$$

mit einem positiven rationalen Exponenten $q = \frac{m}{n}$ folgt ja

$$\alpha = \varphi^k(\alpha) = \alpha^{q^k},$$

woraus sich wegen der reellen Einbettung $q^k = 1$ ergibt, was ausgeschlossen ist. Daher sind auch die Logarithmen der Beträge von α und $\varphi(\alpha)$ linear unabhängig über $\mathbb{Q}$. Wenn die Einheitengruppe den Rang 1 besitzt, so muss bei rein reellen Erweiterungen zwischen den Einheiten α und $\varphi(\alpha)$ bis auf das Vorzeichen eine exponentielle Relation bestehen. Im reell-quadratischen Fall sind in der Tat für eine Einheit $a + b\sqrt{D}$ wegen

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

die beiden zueinander konjugierten Elemente auch bis eventuell auf das Vorzeichen zueinander invers.

Lemma 28.6. *Es sei R ein Zahlbereich mit dem zugehörigen Gitter $\Gamma \subset \mathbb{R}^r \times \mathbb{C}^s$ und der Teilmenge*

$$\begin{aligned} U &= \{(x_1, \ldots, x_r; z_{r+1}, \ldots, z_{r+s}) \in \mathbb{R}^r \times \mathbb{C}^s \\ &\quad \mid |x_1| \cdots |x_r| \cdot |z_{r+1}|^2 \cdots |z_{r+s}|^2 = 1\} \end{aligned}$$

.

Dann gibt es eine beschränkte Teilmenge $T \subseteq U$ mit

$$U = \bigcup_{u \in R^\times} T \cdot \tau^{\mathbb{R}}(u).$$

Beweis. Es sei $d = r + 2s$ der Grad der Körpererweiterung, wir arbeiten in

$$\Gamma \subset \mathbb{R}^r \times \mathbb{C}^s = \mathbb{R}^d.$$

Es seien $c_1, \ldots, c_d$ positive reelle Zahlen mit $c_j = c_{j+1}$ für die konjugierten Stellen und mit

$$c := c_1 \cdots c_d > \left(\frac{2}{\pi}\right)^s \sqrt{|\triangle_K|}.$$

Wir betrachten die durch c definierte beschränkte Teilmenge

$$A := \{(x_1, \ldots, x_d) \in \mathbb{R}^d \mid |x_j| < c_j \text{ alle } j\}.$$

Zu einem Element $y = (y_1, \ldots, y_d) \in \mathbb{R}^d$ ohne Nulleintrag ist die mit y multiplizierte Menge gleich

$$\begin{aligned} yA &= \{(y_1 x_1, \ldots, y_d x_d) \in \mathbb{R}^d \mid |x_j| < c_j \text{ alle } j\} \\ &= \{(z_1, \ldots, z_d) \in \mathbb{R}^d \mid |z_j| < |y_j|\, c_j \text{ alle } j\}. \end{aligned}$$

Nach Lemma 10.8 gibt es in R für jede vorgegebene Norm bis auf Assoziiertheit nur endlich viele Elemente mit dieser Norm. Da als Norm nur ganze Zahlen auftreten, gilt dies auch für die Elemente unterhalb einer fixierten Norm. Deshalb gibt es von 0 verschiedene Elemente $f_1, \ldots, f_n \in R$ derart, dass jedes Element $g \in R$ mit $N(g) \leq c$ zu einem der f_i assoziiert ist.

Wir betrachten nun

$$T := U \cap \left(\bigcup_{i=1}^{n} \tau^{\mathbb{R}}(f_i^{-1})A \right)$$

und behaupten

$$U = \bigcup_{u \in R^\times} T \cdot \tau^{\mathbb{R}}(u),$$

wobei die Inklusion $\supseteq$ klar ist. Zum Beweis der anderen Inklusion sei $y \in U$. Wir betrachten $y^{-1}A$. Wegen $|y_1| \cdots |y_d| = 1$ gilt, dass das Produkt der Grenzen in $y^{-1}A$ wieder gleich c ist und damit die eingangs fixierte Bedingung erfüllt. Nach Korollar 26.3 gibt es ein von 0 verschiedenes $f \in R$ mit $\tau^{\mathbb{R}}(f) \in y^{-1}A$, sagen wir

$$\tau^{\mathbb{R}}(f) = y^{-1}x$$

mit $x \in A$. Da die $\tau^{\mathbb{R}}(f)$ komponentenweise durch die c_j beschränkt sind, ist der Betrag der Norm von f durch c beschränkt. Daher gibt es ein f_i aus unserer endlichen Auswahlmenge und eine Einheit u mit $f = uf_i$. Somit ist

$$y = x\tau^{\mathbb{R}}(f^{-1}) = \tau^{\mathbb{R}}(f_i^{-1})x\tau^{\mathbb{R}}(u^{-1})$$

und

$$x\tau^{\mathbb{R}}(u^{-1}) \in A.$$

□

Der folgende Satz heißt *Dirichletscher Einheitensatz*.

Satz 28.7. *Es sei R ein Zahlbereich mit r reellen Einbettungen und s Paaren von komplexen Einbettungen. Dann ist*

$$R^\times = \mathbb{Z}^{r+s-1} \times \mu$$

mit einer endlichen zyklischen Gruppe μ.

Beweis. Die logarithmische Gesamtabbildung

$$L\colon\ R^\times \longrightarrow \mathbb{R}^{r+s}$$

hat nach Lemma 28.1 den Kern

$$\mu = \mu(R)$$

und das Bild $L(R^\times)$ ist eine diskrete Untergruppe von

$$H = \left\{ (u_1, \ldots, u_{r+s}) \mid \sum_{j=1}^{r+s} u_j = 0 \right\} \subset \mathbb{R}^{r+s}.$$

Nach Lemma 28.6 in Verbindung mit Aufgabe 28.2 ist die Bildgruppe ein Gitter. Es liegt also eine kurze exakte Sequenz

$$0 \longrightarrow \mu(R) \longrightarrow R^\times \longrightarrow L(R^\times) \cong \mathbb{Z}^{r+s-1} \longrightarrow 0$$

vor. Indem man für die Standardvektoren rechts Urbilder in $R^\times$ wählt, erhält man auch eine Darstellung

$$R^\times \cong \mu(R) \times \mathbb{Z}^{r+s-1}.$$

□

DEFINITION 28.8. Eine Familie von Einheiten $u_1, \ldots, u_m \in R$ in einem Zahlbereich R heißt ein System von *Fundamentaleinheiten*, wenn man jede Einheit u von R in eindeutiger Weise als

$$u = \zeta u_1^{n_1} \cdots u_m^{n_m}$$

mit einer Einheitswurzel ζ und ganzzahligen Exponenten n_j schreiben kann.

BEMERKUNG 28.9. Satz 28.7 besagt insbesondere, dass es Systeme von Fundamentaleinheiten gibt, und dass stets

$$m = r + s - 1$$

ist, wenn wieder r die Anzahl der reellen und s die Anzahl der Paare von komplexen Einbettungen bezeichnet. Bei einer Zerlegung

$$R^\times = \mu(R) \times \mathbb{Z}^m$$

kann man eine Basis von $\mathbb{Z}^m$ und insbesondere die Standardbasis als System von Fundamentaleinheiten nehmen. Man beachte, dass weder die Zerlegung noch die dazu äquivalente Auswahl von Fundamentaleinheiten in irgendeiner Form kanonisch ist. Es liegt eine natürliche Untergruppenbeziehung

$$\mu(R) \subseteq R^\times$$

vor und damit gibt es auch einen natürlichen Restklassenhomomorphismus

$$R^\times \longrightarrow \mu(R)/R^\times,$$

und der Satz besagt eben, dass diese Restklassengruppe eine freie kommutative Gruppe vom Rang $r + s - 1$ ist, also isomorph zu $\mathbb{Z}^{r+s-1}$, es gibt aber keine natürliche Identifizierung dieser Restklassengruppe mit $\mathbb{Z}^{r+s-1}$. Aus einer surjektiven Gesamtabbildung

$$R^\times \longrightarrow \mu(R)/R^\times \xrightarrow{\cong} \mathbb{Z}^{r+s-1}$$

erhält man eine freie Untergruppe von $R^\times$, indem man jedem Element der Standardbasis rechts ein Urbild aus $R^\times$ zuordnet und von dieser Abbildung das Bild nimmt. Dies führt dann zu einer Zerlegung

$$R^\times \cong \mu(R) \times \mathbb{Z}^m.$$

KOROLLAR 28.10. *Es sei D eine quadratfreie Zahl und $R = A_D$ der zugehörige quadratische Zahlbereich.*

(1) *Wenn D positiv ist, so ist die Einheitengruppe isomorph zu $\{1, -1\} \times \mathbb{Z}$.*
(2) *Wenn D negativ ist, so ist die Einheitengruppe endlich.*

Beweis. Dies folgt unmittelbar aus Satz 28.7 in Verbindung mit Lemma 27.3. □

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. 9

Lizenzerklärung: Diese Seite wurde von Holger Brenner alias Bocardodarapti auf der deutschsprachigen Wikiversity erstellt und unter die Lizenz CC-by-sa 3.0 gestellt. 9