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

Algebraische Zahlentheorie

Vorlesung 23

Zerlegung im Kreisteilungsring

Wir besprechen die Ergebnisse der letzten Vorlesungen genauer anhand der Kreisteilungsringe. Nach Satz 17.11 liegt eine Galoiserweiterung vor. Auf das Verständnis der Kreisteilungsringe bauen wir einen Beweis des quadratischen Reziprozitätsgesetzes auf.

LEMMA 23.1. *Es sei $R_n = \mathbb{Z}[X]/(\Phi_n)$ der n-te Kreisteilungsring. Dann sind für eine ungerade Primzahl q folgende Aussagen äquivalent.*

(1) *q ist ein Teiler von n.*
(2) *Das Primideal (q) verzweigt in R_n.*
(3) *Das Kreisteilungspolynom Φ_n ist über $\mathbb{Z}/(q)$ nicht separabel.*
(4) *Das Polynom $X^n - 1$ ist über $\mathbb{Z}/(q)$ nicht separabel.*
(5) *Der Ring $\mathbb{Z}/(q)[X]/(X^n - 1)$ ist nicht reduziert.*

Beweis. Von (1) nach (2). Wenn q ein Teiler von n ist, so ist eine q-te Einheitswurzel auch eine n-te Einheitswurzel. Die q-ten Einheitswurzeln lassen sich also als eine Potenz einer primitiven n-ten Einheitswurzel erhalten und deshalb gilt für die Kreisteilungskörper $K_q \subseteq K_n$. Damit ist auch $R_q \subseteq R_n$. Nach Lemma 17.16 in Verbindung mit Satz 18.15 und Satz 18.10 verzweigt (q) in R_q und damit auch in R_n.

Die Äquivalenz von (2) und (3) ist klar aufgrund von Satz 18.10, Aufgabe 15.3 und Satz 17.18. Von (3) nach (4) ist klar wegen Aufgabe 15.4. Die Äquivalenz von (4) und (5) ist klar.

Von (4) nach (1). Wenn q kein Teiler von n ist, so ist n eine Einheit in $\mathbb{Z}/(q)$ und somit sind $X^n - 1$ und $(X^n - 1)' = nX^{n-1}$ teilerfremd über $\mathbb{Z}/(q)$, was nach Aufgabe 15.3 die Separabilität bedeutet. □

SATZ 23.2. *Es sei $R_n = \mathbb{Z}[X]/(\Phi_n)$ der n-te Kreisteilungsring und es sei q eine Primzahl, die kein Teiler von n sei. Es sei f die multiplikative Ordnung von q in $(\mathbb{Z}/(n))^\times$. Dann liegen oberhalb von (q) in $\operatorname{Spek}(R_n)$ genau $\frac{\varphi(n)}{f}$ Primideale, deren Restekörper gleich $\mathbb{F}_{q^f}$ sind.*

Beweis. Nach Voraussetzung ist q kein Teiler von n und damit eine Einheit in $\mathbb{Z}/(n)$. Es gibt deshalb eine wohldefinierte Ordnung f, also die kleinste positive Zahl mit $q^f = 1 \mod n$. Dabei ist f ein Teiler von $\varphi(n)$, der Ordnung der Einheitengruppe $(\mathbb{Z}/(n))^\times$. Nach Aufgabe 17.16 ist $\mathbb{F}_{q^f}$ der kleinste Erweiterungskörper von $\mathbb{Z}/(q)$, der n verschiedene Einheitswurzeln enthält.

Wegen Lemma 22.1 und Lemma 23.1 ist lediglich zu zeigen, dass $\mathbb{F}_{q^f}$ der Restekörper der Primideale oberhalb von (q) ist. Betrachten wir also $\mathbb{Z}/(q)[X]/(\Phi_n)$. Da $\mathbb{F}_{q^f}$ eine primitive n-te Einheitswurzel enthält, gibt es eine surjektive Abbildung

$$\mathbb{Z}/(q)[X]/(X^n-1) \longrightarrow \mathbb{F}_{q^f}.$$

Diese faktorisiert nach Lemma 19.9 (Körper- und Galoistheorie (Osnabrück 2018-2019)) durch

$$\mathbb{Z}/(q)[X]/(\Phi_m) \longrightarrow \mathbb{F}_{q^f},$$

wobei m ein Teiler von n ist und dann gibt es auch eine Surjektion

$$\mathbb{Z}/(q)[X]/(X^m-1) \longrightarrow \mathbb{F}_{q^f}.$$

Wenn m ein echter Teiler von n wäre, so würde sich ein Widerspruch ergeben, da dann das Bild von X eine Ordnung $< n$ hätte. □

Die beiden Extremfälle des Zerlegungsverhaltens kann man folgendermaßen herausarbeiten.

KOROLLAR 23.3. *Es sei $R_n = \mathbb{Z}[X]/(\Phi_n)$ der n-te Kreisteilungsring. Dann sind für eine ungerade Primzahl q folgende Aussagen äquivalent.*

(1) *n ist ein Teiler von $q-1$.*
(2) *$q = 1 \mod n$.*
(3) *In $\mathbb{Z}/(q)$ gibt es n n-te Einheitswurzeln.*
(4) *Das Polynom X^n-1 zerfällt über $\mathbb{Z}/(q)$ in verschiedene Linearformen.*
(5) *Das Kreisteilungspolynom Φ_n zerfällt über $\mathbb{Z}/(q)$ in verschiedene Linearformen.*
(6) *Über (q) liegen $\varphi(n)$ Primideale von R_n.*
(7) *Das Kreisteilungspolynom Φ_n hat eine Nullstelle in $\mathbb{Z}/(q)$ und q ist nicht verzweigt.*

Beweis. Die Äquivalenz von (1) und (2) und die von (3) und (4) ist klar. Die Einheitengruppe von $\mathbb{Z}/(q)$ ist nach Satz 9.7 (Körper- und Galoistheorie (Osnabrück 2018-2019)) zyklisch mit $q-1$ Elementen, das n-te Potenzieren wird unter dieser Identifizierung zum n-ten Multiplizieren,

$$\mathbb{Z}/(q-1) \longrightarrow \mathbb{Z}/(q-1),\ y \longmapsto ny.$$

Die n-ten Einheitswurzeln entsprechen dabei dem Kern dieser Abbildung. Wenn n ein Teiler von $q-1$ ist, so sei $q-1 = na$. In diesem Fall sind $0, a, 2a, \ldots, (n-1)a$ die verschiedenen Elemente des Kerns, was die Implikation von (1) nach (3) beweist. Umgekehrt besitzt der Kern wie jede Untergruppe von $\mathbb{Z}/(q-1)$ einen Erzeuger a, der ein Teiler von $q-1$ ist. Wenn der Kern aus n Elementen besteht, so ist $an = q-1$, was die andere Implikation beweist.

Von (4) nach (5) ist klar, da das Kreisteilungspolynom ein Teiler von $X^n - 1$ ist. Die Äquivalenz von (5) und (6) ist auch klar, da $\mathbb{Z}/(q)[X]/(\Phi_n)$ der Faserring über (q) ist und da das Kreisteilungspolynom den Grad $\varphi(n)$ besitzt. Die Eigenschaft (5) impliziert unmittelbar den ersten Teil von (7). Wäre q verzweigt in R_n, so wäre q nach Lemma 23.1 ein Teiler von n, sagen wir $n = qc$, und dann wäre

$$X^n - 1 = (X^c - 1)^q$$

über $\mathbb{Z}/(q)$. Doch dann hätte das Kreisteilungspolynom mehrfache Nullstellen.

Von (7) nach (3). Zunächst ist nach Lemma 23.1 q kein Teiler von n, d.h. q ist eine Einheit in $\mathbb{Z}/(n)$. Es sei f die (multiplikative) Ordnung von q in $(\mathbb{Z}/(n))^\times$. Dann gibt es in $\mathbb{F}_{q^f}$ n verschiedene n-te Einheitswurzeln. Nach Voraussetzung gibt es eine Nullstelle ζ des Kreisteilungspolynoms Φ_n über $\mathbb{Z}/(p)$. Dessen Potenzen durchlaufen in $\mathbb{F}_{q^f}$ die n-ten Einheitswurzeln. Da die Potenzen aber zu $\mathbb{Z}/(q)$ gehören, ist $f = 1$. □

Korollar 23.4. *Es sei $R_n = \mathbb{Z}[X]/(\Phi_n)$ der n-te Kreisteilungsring und es sei q eine Primzahl, die kein Teiler von n sei. Dann sind folgende Aussagen äquivalent.*

(1) *Das Element q erzeugt die Einheitengruppe von $\mathbb{Z}/(n)$.*
(2) *Über (q) liegt ein Primideal in R_n, d.h. (q) ist unzerlegt im Kreisteilungsring.*
(3) *Das Kreisteilungspolynom Φ_n ist irreduzibel über $\mathbb{Z}/(q)$.*

Beweis. Die Eigenschaft (1) bedeutet, dass die Ordnung von q in der Einheitengruppe $(\mathbb{Z}/(n))^\times$ gleich $\varphi(n)$ ist. Somit folgt die Äquivalenz von (1) und (2) aus Satz 23.2. Die Äquivalenz zu (3) ist angesichts der Voraussetzung über die Unverzweigtheit und der expliziten Beschreibung der Kreisteilungsringe klar. □

Bemerkung 23.5. Nach Satz 17.11 in Verbindung mit Satz 21.2 und Satz 17.18 operiert die Galoisgruppe

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

auf dem n-ten Kreisteilungsring

$$R_n = \mathbb{Z}[X]/(\Phi_n)$$

derart, dass $a \in (\mathbb{Z}/(n))^\times$ durch die Substitution $X \mapsto X^a$ wirkt. Es sei q eine Primzahl, die kein Teiler von n sei, und es sei $\mathfrak{q}$ mit ein Primideal oberhalb von (q). Das Element q gehört zur Einheitengruppe $(\mathbb{Z}/(n))^\times$, seine Ordnung sei f, vergleiche Satz 23.2. Zu q gehört der Automorphismus ψ von R_d, der X auf die q-te Potenz von X abbildet, wobei dies nur von der Restklasse von q modulo n abhängt. Dieser stimmt auf dem Faserring $R_d/(q)R_d$ der Charakteristik q mit dem Frobenius-Homomorphismus überein, da er auf einem Erzeuger damit übereinstimmt und da der Frobenius auf $\mathbb{Z}/(q)$ die

Identität ist. Daher gilt $\psi(\mathfrak{q}) = \mathfrak{q}$ nach Aufgabe 5.36 und ψ gehört zur Zerlegungsgruppe $G_{\mathfrak{q}}$. Da q die Ordnung f besitzt, und die Zerlegungsgruppe nach Lemma 22.3 (4) f Elemente besitzt, wird die Zerlegungsgruppe von diesem Element erzeugt. Da ψ auf dem Faserring den Frobenius induziert, gilt dies auch auf dessen Restekörpern. Somit wird unter der in Lemma 22.5 (3) beschriebenen natürlichen Korrespondenz zwischen der Zerlegungsgruppe und der Galoisgruppe der Restekörpererweiterungen die Substitution $X \mapsto X^q$ auf den Frobenius abgebildet. Damit ist insbesondere zu jeder Primzahl q das Frobenius-Element (siehe Bemerkung 22.10) im Fall von Kreisteilungsringen explizit gegeben.

Der in der letzten Vorlesung erwähnte Dichtigkeitssatz von Tschebotarjowsch beinhaltet unter Verwendng der vorstehenden Bemerknug im Fall von Kreisteilungsringen den Satz von Dirichlet über Primzahlen in einer arithmetischen Progression. Er besagt, dass die Primzahlen modulo den teilerfremden Resten zu einer gegebenen Zahl n gleichverteilt sind.

Das quadratische Reziprozitätsgesetz

Das quadratische Reziprozitätsgesetz gehört zu den Hauptresultaten der Zahlentheorie und wurde erstmals von Gauß bewiesen. Es seien p und q verschiedene ungerade Primzahlen. Es geht dann um die Frage, ob p in $\mathbb{Z}/(q)$ ein Quadrat ist, also eine Quadratwurzel besitzt, oder eben nicht. Die Aussage des Satzes ist nun, dass dies in einer direkten Beziehung zu der „reziproken Eigenschaft“ steht, ob q in $\mathbb{Z}/(p)$ ein Quadrat ist. Es gibt eine Reihe von ziemlich verschiedenen Beweise für diesen Satz, auch relativ elementare, siehe beispielsweise die Einführung in die elementare und algebraische Zahlentheorie. Der Nachteile dieser elementaren Beweise ist, dass sie konzeptionell eher undurchsichtig sind. Man kann die Beweise Zeile für Zeile nachprüfen, fragt sich letztlich aber dennoch, warum die Aussage überhaupt stimmt.

Definition 23.6. Für eine ungerade Primzahl p und eine zu p teilerfremde Zahl $k \in \mathbb{Z}$ definiert man das *Legendre-Symbol*, geschrieben $\left(\frac{k}{p}\right)$ (sprich „k nach p“), durch

$$\left(\frac{k}{p}\right) := \begin{cases} 1, \text{ falls } k \text{ quadratischer Rest modulo } p \text{ ist,} \\ -1, \text{ falls } k \text{ kein quadratischer Rest modulo } p \text{ ist.} \end{cases}$$

Für einfache Eigenschaften des Legendre-Symbols siehe den Anhang. Für Vielfache von p im Zähler setzt man das Legendre-Symbol gleich 0. Für die Beziehung zwischen quadratischen Resten und Kreisteilungsringen ist das folgende Konzept entscheidend.

DEFINITION 23.7. Es sei p eine ungerade Primzahl und $\zeta = e^{2\pi \mathrm{i}/p}$ die erste primitive komplexe Einheitswurzel. Dann nennt man

$$g = \sum_{r=0}^{p-1} \left(\frac{r}{p}\right) \zeta^r$$

die (erste) *quadratische Gaußsumme*.

LEMMA 23.8. *Es sei p eine ungerade Primzahl. Dann gilt für das Quadrat der ersten quadratischen Gaußsumme die Gleichung*

$$g^2 = (-1)^{(p-1)/2} p = \left(\frac{-1}{p}\right) p.$$

Beweis. Die hintere Gleichung beruht auf Satz Anhang 10.8. Nach Definition ist

$$g = \sum_{r=0}^{p-1} \left(\frac{r}{p}\right) \zeta^r = \sum_{r=1}^{p-1} \left(\frac{r}{p}\right) \zeta^r.$$

Daher ist

$$\begin{aligned} g^2 &= \left(\sum_{r=1}^{p-1} \left(\frac{r}{p}\right) \zeta^r\right) \left(\sum_{s=1}^{p-1} \left(\frac{s}{p}\right) \zeta^s\right) \\ &= \sum_{1 \le r,s \le p-1} \left(\frac{rs}{p}\right) \zeta^{r+s}. \end{aligned}$$

Mit der neuen Variablen

$$s = rt$$

können wir dies als

$$\begin{aligned} \sum_{1 \le r,t \le p-1} \left(\frac{rrt}{p}\right) \zeta^{r+rt} &= \sum_{1 \le r,t \le p-1} \left(\frac{t}{p}\right) \zeta^{r(1+t)} \\ &= \sum_{1 \le r,t \le p-1,\, t \ne p-1} \left(\frac{t}{p}\right) \zeta^{r(1+t)} + \sum_{1 \le r \le p-1} \left(\frac{-1}{p}\right) \zeta^0 \\ &= \sum_{1 \le r,t \le p-1,\, t \ne p-1} \left(\frac{t}{p}\right) \zeta^{r(1+t)} + (p-1) \left(\frac{-1}{p}\right). \end{aligned}$$

Für $t \ne -1$, also t zwischen 1 und $p-2$, ist jedenfalls $\xi = \zeta^{1+t}$ auch eine primitive p-te Einheitswurzel. Für ein solches fixiertes t ist

$$\sum_{1 \le r \le p-1} \left(\frac{t}{p}\right) \xi^r = \left(\frac{t}{p}\right) \sum_{1 \le r \le p-1} \xi^r = -\left(\frac{t}{p}\right).$$

Die obige Summe ist also

$$-\sum_{1 \le t \le p-2} \left(\frac{t}{p}\right) + (p-1) \left(\frac{-1}{p}\right) = -\sum_{1 \le t \le p-1} \left(\frac{t}{p}\right) + p \left(\frac{-1}{p}\right) = p \left(\frac{-1}{p}\right),$$

da es nach Satz Anhang 10.1 gleich viele Quadrate wie Nichtquadrate in $(\mathbb{Z}/(p))^\times$ gibt. □

Diese Aussage bedeutet insbesondere, dass im p-ten Kreisteilungsring die quadratische Erweiterung zu p oder $-p$ liegt, wobei das Vorzeichen im Lemma mitbestimmt wird.

LEMMA 23.9. *Es seien p und q verschiedene ungerade Primzahlen. Es sei S der quadratische Zahlbereich zu $\left(\frac{-1}{p}\right)p$ und es sei R_p der p-te Kreisteilungsring. Es sei f die multiplikative Ordnung von q in $(\mathbb{Z}/(p))^\times$. Dann sind folgende Aussagen äquivalent.*

(1) *Es ist $\left(\frac{-1}{p}\right)p$ ein Quadrat in $\mathbb{Z}/(q)$.*
(2) *Über (q) liegen in $\operatorname{Spek}(S)$ zwei Primideale.*
(3) *Über (q) liegt in $\operatorname{Spek}(R_p)$ eine gerade Anzahl von Primidealen.*
(4) *Es ist f ein Teiler von $\frac{p-1}{2}$*
(5) *q ist ein Quadrat in $\mathbb{Z}/(p)$.*

Beweis. Die Äquivalenz von (1) und (2) ist klar nach Aufgabe 9.19. Von (2) nach (3). Nach Lemma 23.8 gilt $S \subseteq R_p$, sodass diese Richtung aus Lemma 22.1 folgt, da sich der nichttrivale Automorphismus der quadratischen Erweiterung zu einem Automorphismus des Kreisteilungsringes fortsetzt, der die beiden Fasern vertauscht. Von (3) nach (2). Es sei $\mathfrak{q}$ ein Primideal über (q). Nach Lemma 22.3 (3) ist

$$\#(G_{\mathfrak{q}}) = \operatorname{grad}_{\mathbb{Z}/(q)} \kappa(\mathfrak{q}) = f$$

und nach Voraussetzung ist wegen Lemma 22.1 $\frac{p-1}{f}$ gerade. Nach Aufgabe 22.6 ist $\frac{p-1}{f}$ auch die Anzahl der Primideale über (q) im Zerlegungsring und die Restekörper sind $\mathbb{Z}/(q)$. Da der Index der Zerlegungsgruppe in der zyklischen Galoisgruppe

$$\operatorname{Aut}(R_p) \cong (\mathbb{Z}/(p))^\times \cong (\mathbb{Z}/(p-1), +, 0)$$

gerade ist, umfasst der Zerlegungskörper den quadratischen Zahlbereich. Deshalb sind auch dessen Restekörper gleich dem Grundkörper und es liegt im Zahlbereich Zerlegung vor.

Die Äquivalenz von (3) und (4) ist klar aufgrund von Satz 23.2. (4) bedeutet, dass

$$q^{\frac{p-1}{2}} = 1 \mod p,$$

deshalb folgt die Äquivalenz von (4) und (5) aus dem Euler-Kriterium. □

SATZ 23.10. *Es seien p und q verschiedene ungerade Primzahlen. Dann gilt:*

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = \begin{cases} -1\,, & \text{wenn } p = q = 3 \mod 4\,, \\ 1\,, & \text{sonst}\,. \end{cases}$$

Beweis. Nach Lemma 23.9 ist unter Verwendung von Lemma Anhang 10.4 und Satz Anhang 10.8

$$\begin{aligned}
\left(\frac{q}{p}\right) &= \left(\frac{\left(\frac{-1}{p}\right)p}{q}\right) \\
&= \left(\frac{\left(\frac{-1}{p}\right)}{q}\right)\cdot\left(\frac{p}{q}\right) \\
&= \left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right)\cdot\left(\frac{p}{q}\right) \\
&= \left(\frac{-1}{q}\right)^{\frac{p-1}{2}}\cdot\left(\frac{p}{q}\right) \\
&= \left((-1)^{\frac{q-1}{2}}\right)^{\frac{p-1}{2}}\cdot\left(\frac{p}{q}\right) \\
&= (-1)^{\frac{q-1}{2}\cdot\frac{p-1}{2}}\cdot\left(\frac{p}{q}\right).
\end{aligned}$$

□

Abbildungsverzeichnis