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

Algebraische Zahlentheorie

Vorlesung 17

Kreisteilungskörper

Wir rekapitulieren ohne Beweis die wichtigsten Ergebnisse über Kreisteilungskörper, wie sie in der Galoistheorie bewiesen werden.

DEFINITION 17.1. Der n-te *Kreisteilungskörper* ist der Zerfällungskörper des Polynoms

$$X^n - 1$$

über $\mathbb{Q}$.

Die Kreisteilungskörper über $\mathbb{Q}$ bezeichnen wir mit K_n. Offenbar ist 1 eine Nullstelle von $X^n - 1$, daher kann man $X^n - 1$ durch $X - 1$ teilen und erhält

$$X^n - 1 = (X-1)\big(X^{n-1} + X^{n-2} + \cdots + X + 1\big).$$

Wegen $1 \in \mathbb{Q}$ ist daher der n-te Kreisteilungskörper auch der Zerfällungskörper von

$$X^{n-1} + X^{n-2} + \cdots + X + 1\,.$$

Da $X^n - 1$ auf die in Lemma 2.10 (Körper- und Galoistheorie (Osnabrück 2018-2019)) beschriebene Art über $\mathbb{C}$ in Linearfaktoren zerfällt, nämlich

$$X^n - 1 = \prod_{k=0}^{n-1} (X - e^{k2\pi \mathrm{i}/n}),$$

kann man K_n als Unterkörper von $\mathbb{C}$ realisieren, und zwar ist K_n der von allen n-ten Einheitswurzeln erzeugte Unterkörper von $\mathbb{C}$. Dieser wird sogar schon von einer einzigen primitiven Einheitswurzel erzeugt.

LEMMA 17.2. *Es sei $n \in \mathbb{N}_+$. Dann wird der n-te Kreisteilungskörper über $\mathbb{Q}$ von $e^{2\pi \mathrm{i}/n}$ erzeugt. Der n-te Kreisteilungskörper ist also*

$$K_n = \mathbb{Q}\big(e^{2\pi \mathrm{i}/n}\big) = \mathbb{Q}[e^{2\pi \mathrm{i}/n}].$$

Insbesondere ist jeder Kreisteilungskörper eine einfache Körpererweiterung von $\mathbb{Q}$.[1]

Statt $e^{\frac{2\pi \mathrm{i}}{n}}$ kann man auch jede andere n-te primitive Einheitswurzel aus $\mathbb{C}$ als Erzeuger nehmen.

[1] Dies ist natürlich auch klar aufgrund des Satzes vom primitiven Element.

Beispiel 17.3. Wir bestimmen einige Kreisteilungskörper für kleine n. Bei $n = 1$ oder 2 ist der Kreisteilungskörper gleich $\mathbb{Q}$. Bei $n = 3$ ist

$$X^3 - 1 = (X-1)\big(X^2+X+1\big)$$

und der zweite Faktor zerfällt

$$X^2+X+1 = \left(X+\frac{1}{2}-\mathrm{i}\frac{\sqrt{3}}{2}\right)\left(X+\frac{1}{2}+\mathrm{i}\frac{\sqrt{3}}{2}\right).$$

Daher ist der dritte Kreisteilungskörper der von $\sqrt{-3} = \sqrt{3}\mathrm{i}$ erzeugte Körer, es ist also $K_3 = \mathbb{Q}[\sqrt{-3}]$ eine quadratische Körpererweiterung der rationalen Zahlen.

Bei $n = 4$ ist natürlich

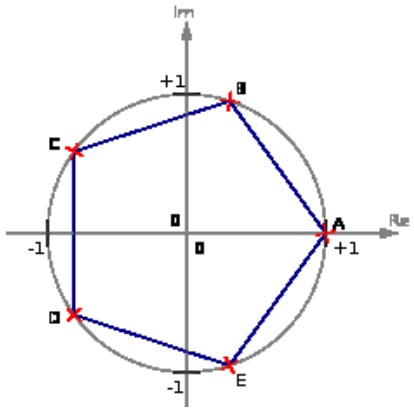
$$\begin{aligned} X^4-1 &= \big(X^2-1\big)\big(X^2+1\big) \\ &= (X-1)(X+1)\big(X^2+1\big) \\ &= (X-1)(X+1)(X-\mathrm{i})(X+\mathrm{i}). \end{aligned}$$

Der vierte Kreisteilungskörper ist somit $\mathbb{Q}[\mathrm{i}] \cong \mathbb{Q}[X]/(X^2+1)$, also ebenfalls eine quadratische Körpererweiterung von $\mathbb{Q}$.

Lemma 17.4. *Es sei p eine Primzahl. Dann ist der p-te Kreisteilungskörper gleich*

$$\mathbb{Q}[X]/\big(X^{p-1}+X^{p-2}+\cdots+X^1+1\big).$$

Insbesondere besitzt der p-te Kreisteilungskörper den Grad $p-1$ über $\mathbb{Q}$.



Beispiel 17.5. Der fünfte Kreisteilungskörper wird von der komplexen Zahl $e^{2\pi\mathrm{i}/5}$ erzeugt. Er hat aufgrund von Lemma 17.4 die Gestalt

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

wobei die Variable X als $e^{2\pi \mathrm{i}/5}$ (oder eine andere primitive Einheitswurzel) zu interpretieren ist. Sei $x = e^{2\pi \mathrm{i}/5}$ und setze $v = 2x^3 + 2x^2 + 1$. Aus Symmetriegründen muss dies eine reelle Zahl sein. Es ist

$$\begin{aligned} v^2 &= 4x^6 + 4x^4 + 1 + 8x^5 + 4x^3 + 4x^2 \\ &= 4x + 4x^4 + 1 + 8 + 4x^3 + 4x^2 \\ &= 5 + 4\big(x^4 + x^3 + x^2 + x + 1\big) \\ &= 5. \end{aligned}$$

Es ist also $v = \sqrt{5}$ (die positive Wurzel) und somit haben wir eine Folge von quadratischen Körpererweiterungen

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt{5}] \subset K_5.$$

Die Menge der n-ten Einheitswurzeln in $\mathbb{C}$ bilden eine zyklische Gruppe der Ordnung n und die primitiven Einheitswurzeln sind die Erzeuger davon. Ihre Anzahl stimmt damit generell mit der Anzahl der Erzeuger der additiven Gruppe $(\mathbb{Z}/(n), \cdot, 0)$ überein. Diese Anzahl bekommt einen eigenen Namen.

Definition 17.6. Zu einer natürlichen Zahl n bezeichnet $\varphi(n)$ die Anzahl der Elemente von $(\mathbb{Z}/(n))^\times$. Man nennt $\varphi(n)$ die *Eulersche Funktion*.

Definition 17.7. Es sei $n \in \mathbb{N}_+$ und seien $z_1, \ldots, z_{\varphi(n)}$ die primitiven komplexen Einheitswurzeln. Dann heißt das Polynom

$$\Phi_n = \prod_{i=1}^{\varphi(n)} (X - z_i) \in \mathbb{C}[X]$$

das n-te *Kreisteilungspolynom*.

Lemma 17.8. *Die Koeffizienten der Kreisteilungspolynome liegen in* $\mathbb{Z}$.

Satz 17.9. *Die Kreisteilungspolynome* Φ_n *sind irreduzibel über* $\mathbb{Q}$.

Satz 17.10. *Der* n*-te Kreisteilungskörper* K_n *über* $\mathbb{Q}$ *hat die Beschreibung*

$$K_n = \mathbb{Q}[X]/(\Phi_n),$$

wobei Φ_n *das* n*-te Kreisteilungspolynom bezeichnet. Der Grad des* n*-ten Kreisteilungskörpers ist* $\varphi(n)$.

Satz 17.11. *Es sei* K_n *der* n*-te Kreisteilungskörper. Dann ist* $\mathbb{Q} \subseteq K_n$ *eine Galoiserweiterung mit der Galoisgruppe*

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

Dabei entspricht der Einheit $a \in (\mathbb{Z}/(n))^\times$ *derjenige Automorphismus* $\varphi_a \in \mathrm{Gal}\,(K_n|\mathbb{Q})$, *der eine* n*-te Einheitswurzel* ζ *auf* ζ^a *abbildet.*

Kreisteilungsringe

Definition 17.12. Es sei $n \in \mathbb{N}_+$. Der Ring der ganzen Zahlen im n-ten Kreisteilungskörper heißt n-ter *Kreisteilungsring*.

Wir bezeichnen diesen Kreisteilungsring mit R_n und möchten die Gleichheit $R_n = \mathbb{Z}[X]/(\Phi_n)$ nachweisen, was bedeutet, dass der Kreisteilungsring durch die selbe Gleichung beschrieben wird wie der Kreisteilungskörper. Für $n = 3$ ist der Kreisteilungsring der Ring der Eisensteinzahlen, und für diesen gilt in der Tat die Beschreibung $\mathbb{Z}[u]/(u^2+u+1)$ und für $n = 4$ ist der vierte Kreisteilungsring der Ring der Gaußschen Zahlen $\mathbb{Z}[u]/(u^2+1)$, und u^2+1 ist das vierte Kreisteilungspolynom. Aber schon für diese niedrigen Zahlen ist das Resultat nicht selbstverständlich, sondern beruht auf der expliziten Beschreibung der quadratischen Zahlbereiche im Sinne von Satz 9.8.

Wir werden die Behauptung zuerst für eine Primzahl $n = p$ zeigen. Wenn ζ eine primitive p-te Einheitswurzel ist, so spielt das Element $1-\zeta$ eine besondere Rolle.

LEMMA 17.13. *Es sei p eine Primzahl und sei $\zeta \in \mathbb{C}$ eine primitive p-te Einheitswurzel. Dann ist das einzige Primideal im p-ten Kreisteilungsring oberhalb von (p) das Primhauptideal $(1-\zeta)$.*

Beweis. Wir setzen

$$S := \mathbb{Z}[\zeta] \cong \mathbb{Z}[Y]/(Y^{p-1}+Y^{p-2}+\cdots+Y^2+Y+1) \subseteq R_p \subseteq \mathbb{C}.$$

Das p-te Kreisteilungspolynom zerfällt

$$X^{p-1}+X^{p-2}+\cdots+X^2+X+1 = \prod_{k=1}^{p-1}(X-\zeta^k),$$

über $\mathbb{C}$ und auch über S. Für $X = 1$ ergibt sich speziell die Gleichung

$$p = \prod_{k=1}^{p-1}(1-\zeta^k).$$

Aufgrund der endlichen geometrischen Reihe ist

$$\frac{1-\zeta^k}{1-\zeta} = 1+\zeta+\zeta^2+\cdots+\zeta^{k-1}$$

und dieses Element gehört zu S. Da k zwischen 1 und $p-1$ ist, gibt es jeweils ein ℓ mit $k\cdot\ell = 1 \mod p$. Wegen $\zeta^p = 1$ und

$$\begin{aligned}\frac{1-\zeta}{1-\zeta^k} &= \frac{1-\zeta^{k\ell}}{1-\zeta^k}\\ &= \frac{1-(\zeta^k)^\ell}{1-\zeta^k}\\ &= 1+\zeta^k+(\zeta^k)^2+\cdots+(\zeta^k)^{\ell-1}\end{aligned}$$

gehört dieses Element ebenfalls zu S, d.h. die Elemente $\frac{1-\zeta^k}{1-\zeta}$ sind Einheiten in S. Deshalb ist

$$p = \prod_{k=1}^{p-1}(1-\zeta^k) = \prod_{k=1}^{p-1}\frac{1-\zeta^k}{1-\zeta}(1-\zeta) = u\cdot(1-\zeta)^{p-1}$$

mit einer Einheit u aus S. Deshalb gilt in S und damit auch im ganzen Abschluss R_p die Idealgleichheit $(p) = ((1-\zeta)^{p-1})$.

Im ganzen Abschluss liegt nach Satz 12.2 eine Idealzerlegung

$$(1-\zeta) = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

vor und daher gilt dort

$$(p) = ((1-\zeta)^{p-1}) = \mathfrak{p}_1^{p-1} \cdots \mathfrak{p}_r^{p-1}.$$

Da der Grad der Erweiterung gleich $p-1$ ist, folgt direkt $r = 1$ und somit, dass $(1-\zeta)$ ein Primideal ist, und zwar das einzige über (p). □

LEMMA 17.14. *Es sei p eine Primzahl und sei $\zeta \in \mathbb{C}$ eine primitive p-te Einheitswurzel. Dann ist der p-te Kreisteilungsring gleich $\mathbb{Z}[\zeta]$.*

Beweis. Wir zeigen, dass

$$\mathbb{Z}[\zeta] \cong \mathbb{Z}[Y]/(Y^{p-1} + Y^{p-2} + \cdots + Y^2 + Y + 1)$$

bereits normal ist, also mit seinem ganzen Abschluss übereinstimmt. Dazu genügt es zu zeigen, dass die Lokalisierung von $\mathbb{Z}[\zeta]$ an jedem Primideal $\mathfrak{q}$ ein diskreter Bewertungsring ist. Es sei

$$\mathfrak{q} \cap \mathbb{Z} = (q)$$

mit einer Primzahl q und wir machen eine Fallunterscheidung je nachdem, ob $q = p$ ist oder nicht. Bei $q = p$ zeigt Lemma 17.13, dass $\mathfrak{q} = (\zeta - 1)$ ein Hauptideal ist, was sich auf die Lokalisierung überträgt. Bei $q \neq p$ lokalisieren wir die Situation an (q). Da $X^p - 1$ und seine Ableitung pX^{p-1} teilerfremd in $\mathbb{Z}_{(q)}[X]$ sind, gilt dies auch für das Kreisteilungspolynom und seine Ableitung. Deshalb sind die Primteiler des Kreisteilungspolynoms in $\mathbb{Z}/(q)[X]$ einfach. Somit sind die Lokalisierungen oberhalb von (q) nach Lemma 15.1 diskrete Bewertungsringe. □

Insbesondere ist $1, \zeta, \zeta^2, \ldots, \zeta^{p-2}$ eine Ganzheitsbasis des Kreisteilungsringes.

BEISPIEL 17.15. Es sei $R = \mathbb{Z}[X]/(X^4+X^3+X^2+X+1) = \mathbb{Z}[x]$ der fünfte Kreisteilungsring. Wir verwenden den Zwischenring (vergleiche Beispiel 17.5)

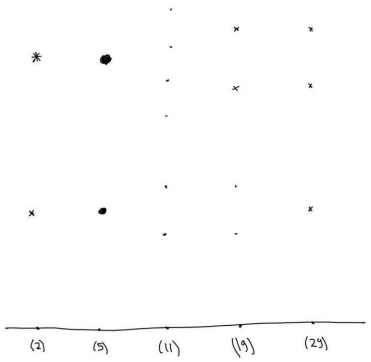
$$\begin{array}{rcl} \mathbb{Z} & \subseteq & \mathbb{Z}[\sqrt{5}] \\ & \subseteq & \mathbb{Z}[W]/(W^2 - W - 1) \\ & = & S \\ & \subseteq & \mathbb{Z}[X]/(X^4 + X^3 + X^2 + X + 1) \\ & = & S[X]/(X^2 + XW + 1) \end{array}$$

mit

$$w = \frac{v+1}{2} = x^3 + x^2 + 1$$

und $v^2 = 5$. Wir beschreiben exemplarisch das Verhalten von Primzahlen in diesem Zahlbereich. Zu einer Primzahl p kommen als Restekörper der Primideale in R oberhalb von (p) nach Korollar 8.8 nur die Körper

$\mathbb{Z}/(p), \mathbb{F}_{p^2}, \mathbb{F}_{p^3}, \mathbb{F}_{p^4}$ in Frage (die Möglichkeit $\mathbb{F}_{p^3}$ werden wir gleich ausschließen), und zwar muss es in den Restekörpern fünf Einheitswurzeln (über (5) fallen die zusammen) geben. Wegen Satz 9.6 (Körper- und Galoistheorie (Osnabrück 2018-2019)) ist dies genau dann der Fall, wenn $p^e - 1$ ein Vielfaches von 5 ist. Daraus ergeben sich die Möglichkeiten $e = 1, 2, 4$. Wir geben Beispiele für typisches Zerlegungsverhalten.



Das exemplarische Zerlegungsverhalten im fünften Kreisteilungsring umd im quadratischen Zahlbereich zu $\sqrt{5}$.

Sei $p = 2$. Es ist $S/2S$ ein Körper mit vier Elementen und es ist $R/2S$ ein Körper mit 16 Elementen.

Sei $p = 5$. Hier ist über $\mathbb{Z}/(5)$

$$(X-1)(X^4+X^3+X^2+X+1) = X^5-1 = (X-1)^5$$

und somit $X^4+X^3+X^2+X+1 = (X-1)^4$. Es gibt also nur ein Primideal oberhalb von (5) und dessen Restklassenkörper ist $\mathbb{Z}/(5)$, was auch von Lemma 17.13 her klar ist.

Bei $q = 11$ sind $1, 3, 4, 5, 9$ fünfte Einheitswurzeln und das Kreisteilungspolynom hat die Zerlegung

$$X^4+X^3+X^2+X+1 = (X-3)(X+2)(X-4)(X-5).$$

Oberhalb von (11) liegen in $\operatorname{Spek}(R)$ vier Primideale, alle mit dem Restekörper $\mathbb{Z}/(11)$. Dabei liegen $(X-3)$ und $(X-4)$ über $(W-4)$ und $(X+2)$ und $(X-5)$ über $(W-8)$ in S.

Bei $p = 19$ ist $9^2 = 5 = 10^2$, in S gibt es somit zwei Primideale oberhalb von (19), beide mit dem Restekörper $\mathbb{Z}/(19)$. In $\mathbb{Z}/(19)$ gibt es aber keine fünfte Einheitswurzeln, deshalb liegen oberhalb von (19) in R zwei Primideale, beide

mit dem Restekörper $\mathbb{F}_{361}$. Über (19) liegt die Faktorzerlegung

$$X^4 + X^3 + X^2 + X + 1 = \big(X^2 + 5X + 1\big)\big(X^2 + 15X + 1\big)$$

vor.

Bei $p = 29$ liegt in S nur ein Primideal oberhalb von (29), da 5 kein Quadrat in $\mathbb{Z}/(29)$ ist. Der Restekörper ist $\mathbb{F}_{841}$. Da es in $\mathbb{F}_{841}$ fünfte Einheitswurzeln gibt, liegen darüber in R zwei Primideale mit diesem Restekörper.

LEMMA 17.16. *Es sei p eine Primzahl und ζ eine primitive p-te Einheitswurzel. Dann ist die Diskriminante der $\mathbb{Q}$-Basis $1, \zeta, \zeta^2, \ldots, \zeta^{p-2}$ des p-ten Kreisteilungskörpers gleich*

$$\triangle(1, \zeta, \zeta^2, \ldots, \zeta^{p-2}) = \pm p^{p-2}.$$

Beweis. Das p-te Kreisteilungspolynom ist

$$\Phi_p = X^{p-1} + X^{p-2} + \cdots + X^2 + X + 1 = (X - \zeta)(X - \zeta^2)\cdots(X - \zeta^{p-1}).$$

Es ist nach Lemma 8.11

$$\begin{aligned} \triangle(1, \zeta, \zeta^2, \ldots, \zeta^{p-2}) &= \prod_{0 \le i < j \le p-2} (\zeta^i - \zeta^j)^2 \\ &= \pm \prod_{0 \le i, j \le p-2,\, i \ne j} (\zeta^i - \zeta^j). \end{aligned}$$

Wenn man die Übergangsmatrix zwischen den beiden Basen $1, \zeta, \zeta^2, \ldots, \zeta^{p-2}$ und $\zeta, \zeta^2, \ldots, \zeta^{p-2}, \zeta^{p-1}$ betrachtet, so ist deren Determinante gleich ± 1 und deshalb kann man wegen Lemma 8.2 genauso gut $\pm \prod_{1 \le i, j \le p-1,\, i \ne j} (\zeta^i - \zeta^j)$ berechnen.

Wir verwenden nun zwei verschiedene Möglichkeiten, die Ableitung des Kreisteilungspolynoms zu bestimmen. Die Ableitung von Φ_p ist nach der Produktregel gleich

$$\sum_{k=1}^{p-1} (X - \zeta)(X - \zeta^2)\cdots(X - \zeta^{p-1})/(X - \zeta^k)\,.$$

Wenn man darin ζ^i, $i = 1, \ldots, p-1$, einsetzt, so werden alle Summanden mit der einzigen Ausnahme für $k = i$ zu 0, und der verbleibende Summand ist

$$\Phi_p'(\zeta^i) = \prod_{1 \le j \le p-1,\, j \ne i} (\zeta^i - \zeta^j).$$

Somit ist die Diskriminante gleich

$$\pm \prod_{i=1}^{p-1} \Phi_p'(\zeta^i) = \pm \prod_{\varphi} \Phi_p'(\varphi(\zeta)) = \pm \prod_{\varphi} \varphi(\Phi_p'(\zeta)) = \pm N(\Phi_p'(\zeta)),$$

wobei φ die Galoisgruppe durchläuft und Lemma 7.14 verwendet wurde. Aufgrund von

$$X^p - 1 = (X - 1)\Phi_p$$

gilt für die Ableitung auch die Beziehung

$$pX^{p-1} = (X-1)\Phi_p' - \Phi_p.$$

Wenn man darin ζ einsetzt, so erhält man

$$p\zeta^{p-1} = p\zeta^{-1} = (\zeta-1)\Phi_p'(\zeta)$$

und somit

$$\Phi_p'(\zeta) = p\zeta^{-1}(\zeta-1)^{-1}.$$

Die Norm von $\zeta - 1$ ist

$$N(\zeta-1) = \prod_{k=1}^{p-1}(\zeta^k - 1) = \pm\Phi_p(1) = \pm p.$$

Deshalb ist die Diskriminante nach Lemma 8.7 (Körper- und Galoistheorie (Osnabrück 2018-2019)) und Lemma 10.2 gleich

$$\begin{aligned} \pm N(\Phi_p'(\zeta)) &= \pm N(p\zeta^{-1}(\zeta-1)^{-1}) \\ &= \pm N(p)N(\zeta^{-1})N((\zeta-1)^{-1}) \\ &= \pm p^{p-1}\cdot\frac{1}{p} \\ &= \pm p^{p-2} \end{aligned}$$

□

Lemma 17.17. *Es sei p eine Primzahl, $q = p^r$ und ζ eine primitive p^r-te Einheitswurzel und Dann ist die Diskriminante der $\mathbb{Q}$-Basis $1, \zeta, \zeta^2, \ldots, \zeta^{\varphi(p^r)-1}$ des p^r-ten Kreisteilungskörpers gleich*

$$\triangle(1, \zeta, \zeta^2, \ldots, \zeta^{\varphi(p^r)-1}) = \pm p^{p^{r-1}(rp-r-1)}.$$

Beweis. Dies wird ähnlich wie Lemma 17.16 bewiesen. □

Satz 17.18. *Sei $n \in \mathbb{N}_+$ und sei $\zeta \in \mathbb{C}$ eine primitive n-te Einheitswurzel. Dann ist der n-te Kreisteilungsring gleich $\mathbb{Z}[\zeta]$.*

Beweis. Dies wird zuerst ausgehend von Lemma 17.14 für Primzahlpotenzen bewiesen. Bei $n = p_1^{r_1}\cdot p_k^{r_k}$ ergibt sich eine Ganzheitsbasis des Ganzheitsringes wegen der nach Lemma 17.17 teilerfremden Diskiminanten aus den Produkten der Ganzheitsbasen der einzelnen Kreisteilungsringen zu den Primzahlpotenzen. □

Es ist also

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

wobei Φ_n das n-te Kreisteilungspolynom bezeichnet.

Abbildungsverzeichnis