Zu §6.6: Kreisteilungskörper

Satz: $\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times$.

Beweis: Betrachte das n-te Kreisteilungspolynom

$$\Phi_n(X) := \prod_{\substack{\zeta \in \mu_n \\ \mathrm{ord}\,\zeta = n}} (X - \zeta)$$

Da es immer n-te Gal$(\mathbb{Q}(\mu_n)/\mathbb{Q})$ ist, liegt es in $\mathbb{Q}[X]$. Weiter ist $\deg(\Phi_n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$, und jede einzelne Nullstelle von Φ_n erzeugt schon $\mathbb{Q}(\mu_n)$. Folglich ist der Satz äquivalent zu: $\Phi_n(X)$ ist irreduzibel in $\mathbb{Q}[X]$.

Beweis nur für $n = p^k$ für p prim und $k \geq 1$:

Dann ist $\Phi_{p^k}(X) = \dfrac{X^{p^k}-1}{X^{p^{k-1}}-1} = X^{p^k-p^{k-1}} + \dots + X^{p^{k-1}} + 1$

$$\Rightarrow \Phi_{p^k}(1+Y) = (1 + \text{höhere Terme})^{p^k-p^{k-1}} + \dots + (1) = p + \text{höhere Terme}$$

$$\equiv \frac{(1+Y)^{p^k}-1}{(1+Y)^{p^{k-1}}-1} \equiv \frac{1+Y^{p^k}-1}{1+Y^{p^{k-1}}-1} = Y^{p^k-p^{k-1}} \text{ mod } p.$$

Nach dem Eisensteinkriterium bei $p=2$ ist also Φ_{p^k} irreduzibel. qed.

Satz: Ein regelmäßiges n-Eck ist mit Zirkel und Lineal konstruierbar g.d.w. $|(\mathbb{Z}/n\mathbb{Z})^\times|$ eine Zweierpotenz ist.

Beweis: Sei $n = p_1^{k_1} \cdots p_r^{k_r}$ mit p_i paarweise verschieden. Dann ist $\mu_n = \mu_{p_1^{k_1}} \times \cdots \times \mu_{p_r^{k_r}}$. Also ist das n-Eck konstruierbar g.d.w. die $p_i^{k_i}$-Ecke konstruierbar sind für alle i.

Nach §5.5 ist dies der Fall g.d.w. $\mathbb{Q}(\mu_{p_i^{k_i}})/\mathbb{Q}$ eine Folge von Körpererweiterungen vom Grad 2 ist. Da dessen Galoisgruppe abelsch ist, ist das äquivalent dazu, dass $[\mathbb{Q}(\mu_{p_i^{k_i}})/\mathbb{Q}]$ eine Zweierpotenz ist. Schließlich ist

$$(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} \bigoplus_{i=1}^r (\mathbb{Z}/p_i^{k_i}\mathbb{Z})^\times.$$

qed.

Bemerkung: Betrachte K und n wie im Satz. Ist K_n der Zerfällungskörper des Polynoms $X^n - 1$ über K, so gilt also $|\mu_n(K_n)| = n$ und $\mu_n(K_n) \cong \mathbb{Z}/n\mathbb{Z}$. Da $\mu_n(K) \subset \mu_n(K_n)$ ist, folgt $\mu_n(K) \cong \mathbb{Z}/d\mathbb{Z}$ für einen Teiler d von n. Die Menge der primitiven n–ten Einheitswurzeln in K_n werde mit $\mu_n^*(K_n)$ bezeichnet; es ist also $|\mu_n^*(K_n)| = \varphi(n)$.

2.3. Das n–te *Kreisteilungspolynom* $\Phi_n \in \mathbb{C}[X]$ ist definiert als Produkt aller Polynome $X - \zeta$ über die primitiven n–ten Einheitswurzeln $\zeta \in \mathbb{C}$:

$$\Phi_n := \prod_{\zeta \in \mu_n^*(\mathbb{C})} (X - \zeta). \tag{1}$$

Es ist ein normiertes Polynom vom Grad $\varphi(n)$. Da die Ordnung einer n–ten Einheitswurzel ein Teiler von n ist, kann man $\mu_n(\mathbb{C})$ als disjunkte Vereinigung schreiben: $\mu_n(\mathbb{C}) = \bigcup_{d|n} \mu_d^*(\mathbb{C})$. Es folgt die Zerlegung

$$X^n - 1 = \prod_{\zeta \in \mu_n(\mathbb{C})} (X - \zeta) = \prod_{d|n} \Phi_d. \tag{2}$$

Satz 2.4. *Das n–te Kreisteilungspolynom Φ_n hat ganzzahlige Koeffizienten, d.h., es gilt $\Phi_n \in \mathbb{Z}[X]$.*

Beweis: Wir benützen Induktion über n. Man hat $\Phi_1 = X - 1 \in \mathbb{Z}[X]$. Nach Induktionsvoraussetzung ist das normierte Polynom $f = \prod_{d|n,\, d \neq n} \Phi_d$ ein Element in $\mathbb{Z}[X]$. Zu $X^n - 1$ existieren dann eindeutig bestimmte Polynome $q, r \in \mathbb{Z}[X]$ mit $X^n - 1 = qf + r$ und $\operatorname{grad} r < \operatorname{grad} f$. Andererseits gilt auch die Identität $X^n - 1 = \Phi_n f$ in $\mathbb{C}[X]$, also folgt $r = f(\Phi_n - q)$. Da $\operatorname{grad} r < \operatorname{grad} f$ gilt, muß $\Phi_n = q \in \mathbb{Z}[X]$ sein. ∎

Beispiele: (1) Die Formel $\Phi_n = (X^n - 1)/\prod_{d|n,\, d \neq n} \Phi_d$ erlaubt die rekursive Berechnung von Kreisteilungspolynomen. Man erhält: $\Phi_1 = X - 1$, $\Phi_2 = X + 1$, $\Phi_3 = X^2 + X + 1$, $\Phi_4 = X^2 + 1$, $\Phi_5 = X^4 + X^3 + X^2 + X + 1$, $\Phi_6 = X^2 - X + 1$, $\Phi_7 = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$, $\Phi_8 = X^4 + 1, \ldots$

(2) Für eine Primzahl p gilt allgemein $\Phi_p = X^{p-1} + X^{p-2} + \cdots + X + 1$. Ist $\alpha \in \mathbb{N}$ eine positive natürliche Zahl, so gilt $X^{p^\alpha} - 1 = (X^{p^{\alpha-1}} - 1)\Phi_{p^\alpha}$, also folgt

$$\Phi_{p^\alpha} = (X^{p^\alpha} - 1)/(X^{p^{\alpha-1}} - 1) = \Phi_p(X^{p^{\alpha-1}}) = (X^{p^{\alpha-1}})^{p-1} + \cdots + X^{p^{\alpha-1}} + 1.$$

(3) Ist $n > 1$ ungerade, so ist $\zeta \in \mathbb{C}$ genau dann eine primitive n–te Einheitswurzel, wenn $-\zeta$ eine primitive $2n$–te Einheitswurzel in $\mathbb{C}$ ist. Dies folgt aus dem Isomorphismus $(\mathbb{Z}/2n\mathbb{Z})^* \cong (\mathbb{Z}/2\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/n\mathbb{Z})^*$. Für das Kreisteilungspolynom Φ_{2n} gilt

$$\Phi_{2n}(-X) = \prod_j (-X - (-\zeta)^j) = \prod_j (X - \zeta^j) = \Phi_n(X).$$

2.5. Sei K ein Körper mit $\operatorname{char} K \nmid n$. Bezeichne mit χ den einzigen Ringhomomorphismus $\chi : \mathbb{Z} \longrightarrow K$, siehe III.3.5. Aus 2.3(2) folgt, daß

$$X^n - 1 = \prod_{d|n} \chi^*(\Phi_d) \tag{1}$$

in $K[X]$ gilt. Sei K_n ein Zerfällungskörper von $X^n - 1$ über K. Das zum Beweis von 2.3(2) benützte Argument zeigt, daß in $K_n[X]$

$$X^n - 1 = \prod_{d|n} \prod_{\zeta \in \mu_d^*(K_n)} (X - \zeta). \tag{2}$$

Mit Induktion über n folgt daraus

$$\chi^*(\Phi_n) = \prod_{\zeta \in \mu_n^*(K_n)} (X - \zeta). \tag{3}$$

(Der Fall $n = 1$ ist klar.) Dies bedeutet, daß $\chi^*(\Phi_n)$ das Analogon zu Φ_n über K ist; wir bezeichnen deshalb $\chi^*(\Phi_n)$ auch mit $\Phi_{n,K}$.

Satz 2.6. *Das n-te Kreisteilungspolynom Φ_n ist irreduzibel über $\mathbb{Z}$ und über $\mathbb{Q}$.*

Beweis: Das Polynom Φ_n ist normiert; also ist Φ_n genau dann über $\mathbb{Q}$ irreduzibel, wenn Φ_n über $\mathbb{Z}$ irreduzibel ist.

Sei K_n Zerfällungskörper von Φ_n über $\mathbb{Q}$. Der entscheidende Schritt im Beweis des Satzes ist die folgende Behauptung:

(*) *Sei $\zeta \in K_n$ eine primitive n-te Einheitswurzel. Ist p eine Primzahl, die n nicht teilt, so stimmen die Minimalpolynome $m_{\zeta,\mathbb{Q}}$ von ζ und $m_{\zeta^p,\mathbb{Q}}$ von ζ^p über $\mathbb{Q}$ überein.*

Nehmen wir diese Behauptung an, so ergibt sich der Satz aus dem folgenden Argument: Wir wählen eine feste primitive n-te Einheitswurzel $\zeta \in K_n$. Eine beliebige primitive n-te Einheitswurzel hat dann die Form ζ^m mit $\operatorname{ggT}(m, n) = 1$. Nun wählen wir eine Primfaktorzerlegung $m = p_1 \dots p_k$. Dann gilt $p_i \nmid n$ für alle i; mit ζ ist auch jedes $\zeta^{p_1 \cdots p_j}$ mit $1 \leq j \leq k$ primitive n-te Einheitswurzel. Wenden wir (*) auf alle $\zeta^{p_1 \cdots p_{j-1}}$ an, so folgt induktiv, daß alle $\zeta^{p_1 \cdots p_j}$ dasselbe Minimalpolynom wie ζ haben. Insbesondere folgt $m_{\zeta,\mathbb{Q}}(\zeta^m) = 0$. Daher hat $m_{\zeta,\mathbb{Q}}$ mindestens $\varphi(n)$ Nullstellen, nämlich alle primitiven n-ten Einheitswurzeln in K_n. Da ζ auch eine Nullstelle von Φ_n ist, wird Φ_n von $m_{\zeta,\mathbb{Q}}$ geteilt. Weil Φ_n normiert ist und Grad $\varphi(n)$ hat, folgt nun $\Phi_n = m_{\zeta,\mathbb{Q}}$; insbesondere ist Φ_n irreduzibel.

Wir müssen nun (*) beweisen. Zunächst bemerken wir, daß $m_{\zeta,\mathbb{Q}}$ und $m_{\zeta^p,\mathbb{Q}}$ ganzzahlige Koeffizienten haben: Φ_n zerlegt sich in $\mathbb{Z}[X]$ in der Form $\Phi_n = \prod_{i=1}^k f_i$ mit irreduziblen $f_i \in \mathbb{Z}[X]$. Da Φ_n normiert ist und die f_i

Koeffizienten in $\mathbb{Z}$ haben, sind die höchsten Koeffizienten der f_i gleich ± 1. Daher sind die f_i auch in $\mathbb{Q}[X]$ irreduzibel. Indem wir notfalls einige f_i durch $-f_i$ ersetzen, können wir annehmen, daß alle f_i normiert sind. Nun ist ζ eine Nullstelle von einem der Polynome f_i. Dieses f_i ist dann, da normiert und irreduzibel über $\mathbb{Q}$, gerade $m_{\zeta,\mathbb{Q}}$. Ebenso findet man ein j mit $m_{\zeta^p,\mathbb{Q}} = f_j \in \mathbb{Z}[X]$.

Um $m_{\zeta,\mathbb{Q}} = m_{\zeta^p,\mathbb{Q}}$ nachzuweisen, müssen wir $i = j$ zeigen. Gilt dies nicht, so ist $m_{\zeta,\mathbb{Q}} \cdot m_{\zeta^p,\mathbb{Q}} = f_i f_j$ ein Teiler von Φ_n in $\mathbb{Z}[X]$, also auch ein Teiler von $X^n - 1$.

Wir setzen zur Abkürzung $f := f_i = m_{\zeta,\mathbb{Q}}$ und $g := f_j = m_{\zeta^p,\mathbb{Q}}$. Wir nehmen an, daß $fg \mid X^n - 1$ in $\mathbb{Z}[X]$ und suchen einen Widerspruch. Wegen $g(\zeta^p) = 0$ ist ζ eine Wurzel des Polynoms $g(X^p)$. Also teilt f als Minimalpolynom von ζ das Polynom $g(X^p)$ in $\mathbb{Q}[X]$, aber dann auch in $\mathbb{Z}[X]$, vergleiche den Beweis von Satz 2.4. Es gibt also ein $h \in \mathbb{Z}[X]$ mit $g(X^p) = f\,h$.

Man betrachte jetzt den natürlichen Homomorphismus $\pi : \mathbb{Z} \longrightarrow \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ und den zugehörigen Homomorphismus $\pi^* : \mathbb{Z}[X] \longrightarrow \mathbb{F}_p[X]$. Schreibt man $g = \sum_{j=0}^{m} a_j X^j$ mit $a_j \in \mathbb{Z}$, so folgt, da $\pi(a_j) = \pi(a_j)^p$ in $\mathbb{F}_p$ gilt,

$$\begin{aligned} \pi^*(g)^p &= \Big(\sum \pi(a_j) X^j\Big)^p = \sum \pi(a_j) X^{jp} = \pi^*(g(X^p)) \\ &= \pi^*(f)\,\pi^*(h), \end{aligned}$$

d.h., $\pi^*(f)$ teilt $\pi^*(g)^p$ in $\mathbb{F}_p[X]$. Ist $q \in \mathbb{F}_p[X]$ ein irreduzibler Faktor von $\pi^*(f)$, dann teilt q auch $\pi^*(g)$. Daher teilt q^2 das Produkt $\pi^*(f)\pi^*(g)$, also auch $X^n - 1 = \pi^*(X^n - 1)$, da wir $fg \mid X^n - 1$ annehmen. Man kann also $X^n - 1 = q^2 s$ mit irgendeinem $s \in \mathbb{F}_p[X]$ schreiben. Bildet man die Ableitung, so erhält man

$$D(X^n - 1) = nX^{n-1} = 2qD(q)s + q^2 D(s).$$

Dies zeigt, daß das Polynom q das Polynom nX^{n-1} teilt. Da p eine Primzahl ist, die n nicht teilt, gilt $n \neq 0$ in $\mathbb{F}_p$. Also muß q das Polynom X^{n-1} teilen. Weil q irreduzibel ist, stimmt es (bis auf einen Faktor $\neq 0$) mit X überein. Auf diese Weise erhält man einen Widerspruch, da einerseits q das Polynom $X^n - 1$ teilt, andererseits aber X das Polynom $X^n - 1$ nicht teilt. ∎

Der folgende Satz gibt Auskunft über die Primfaktorzerlegung der Kreisteilungspolynome über endlichen Primkörpern.

Satz 2.7. *Seien n eine positive ganze Zahl und p eine Primzahl, die n nicht teilt. Sei e die Ordnung der Restklasse von p in $(\mathbb{Z}/n\mathbb{Z})^*$, also $e := \operatorname{ord}(p \bmod n)$ in $(\mathbb{Z}/n\mathbb{Z})^*$. Dann zerfällt das n-te Kreisteilungspolynom $\Phi_{n,\mathbb{F}_p}$ in $\varphi(n)/e$ verschiedene irreduzible Faktoren vom Grad e. Insbesondere ist $\Phi_{n,\mathbb{F}_p}$ genau dann irreduzibel, wenn die Restklasse von p modulo n die Einheitengruppe $(\mathbb{Z}/n\mathbb{Z})^*$ erzeugt.*