Kreisteilungskörper

Sei $n \geq 1$ natürliche Zahl und k ein Körper. Wir bezeichnen mit $k[n]$ den Zerfällungskörper von $X^n - 1$. Die Menge $\mu_n \subset k[n]^\times$ der Nullstellen von $X^n - 1$ ist dann eine endliche Untergruppe von $k[n]^\times$ und daher zyklisch. Wir benennen "n-te primitive Einheitswurzel" die ~~Generatoren~~ Erzeugenden von μ_n.

Von jetzt an nehmen wir an, dass entweder $\mathrm{Char}\, k = 0$ oder $\mathrm{Char}\, k$ nicht n teilt. Das ist nach Lemma II. 10

equivalent zur Bedingung dass $X^n - 1$ keine mehrfachen Nullstellen besitzt; insbesondere ist $X^n - 1$ separabel und daher (Def. IV. 12, Thm IV. 11) ist dann $k[n]$ eine Galois Erweiterung von k.

Sei $\zeta \in \mu_n$ eine primitive Einheits-Wurzel; mittels des Isomorphismus

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &\longrightarrow \mu_n \\ h &\longmapsto \zeta^h \end{aligned}$$

können wir $\mathrm{Gal}(k[n]/k)$ als Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^\times$ betrachten: jedes $\sigma \in \mathrm{Gal}(k[n]/k)$ ist eindeutig bestimmt durch $\sigma(\zeta) = \zeta^{a_\sigma}$, $a_\sigma \in (\mathbb{Z}/n\mathbb{Z})^\times$.

und damit erhalten wir einen injektiven Gruppenhomomorphismus:

$$Gal(k[n]/k) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$$
$$\sigma \longmapsto a_\sigma .$$

In diesem Abschnitt werden wir das Bild dieses Homomorphismus für $k = \mathbb{Q}$ und $k = \mathbb{F}_p$, $p \nmid n$ bestimmen.

Thm IV.26 $Gal(\mathbb{Q}[n]/\mathbb{Q}) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ ist ein Isomorphismus.

Der folgende Beweis stammt von Dedekind (1857); er benützt das

Gauß Lemma: Falls $p = Q \cdot R$ wobei $p \in \mathbb{Z}[x]$, Q und $R \in \mathbb{Q}[x]$

so gibt es $\lambda, \mu \in \mathbb{Q}^\times$ mit $q := \lambda Q \in \mathbb{Z}[x]$ $r := \mu R \in \mathbb{Z}[x]$ und $p = q \cdot r$. Insbesondere, falls p, Q, R unitäre Polynome sind, so folgt $Q, R \in \mathbb{Z}[x]$.

Beweis von Thm IV.26.

Sei $\zeta \in \mu_n$ primitive Einheitswurzeln wobei ~~und~~ $(a, n) = 1$; sei $f = \operatorname{irr}(\zeta, \mathbb{Q})$ $g = \operatorname{irr}(\zeta^a, \mathbb{Q})$ deren Minimalpolynome über $\mathbb{Q}$. Wir werden zeigen, dass $f = g$.

Daraus folgt dann $f(\zeta^a) = 0$; da f irreduzibel ist und $\mathbb{Q}[n]$ Zerfällungskörper von f ist, folgt aus Korollar IV.13, dass $\operatorname{Gal}(\mathbb{Q}[n]/\mathbb{Q})$ transitiv auf den Nullstellen von f

wirkt, insbesondere gibt es $\sigma \in Gal(\mathbb{Q}[\zeta]/\mathbb{Q})$ mit $\sigma(\zeta) = \zeta^a$. Daraus folgt dann die Surjektivität von $Gal(\mathbb{Q}[\zeta]/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$ und somit das Theorem.

Sei $a = p_1 \cdots p_r$ die Primzahlzerlegung von a. Wir betrachten die Folge:

$$\zeta,\ \zeta^{p_1},\ \zeta^{p_1 p_2} = (\zeta^{p_1})^{p_2},\ \zeta^{p_1 p_2 p_3} = (\zeta^{p_1 p_2})^{p_3},\ \ldots$$

Dann sind $\zeta^{p_1}, \zeta^{p_1 p_2}, \ldots, \zeta^{p_1 \cdots p_{r-1}}$ immer noch primitive Einheitswurzeln. Falls wir also zeigen dass für jede primitive Einheitswurzel ζ und Primzahl p mit $(p, n) = 1$, $\operatorname{irr}(\zeta, \mathbb{Q}) = \operatorname{irr}(\zeta^p, \mathbb{Q})$ dann haben alle Elemente obiger Folge dasselbe Minimalpolynom und

daraus folgt $f = g$.

Sei also $f = \mathrm{irr}(\zeta, \mathbb{Q})$, $g = \mathrm{irr}(\zeta^p, \mathbb{Q})$

$(p, n) = 1$ und p Primzahl.

Annahme: $f \neq g$.

Nun sind f, g irreduzible Faktoren von $X^n - 1$ und unitär; ~~daraus~~ $f \neq g$ folgt $X^n - 1 = f(x) g(x) h(x)$ wobei $h \in \mathbb{Q}[x]$, h unitär. Aus dem Gauss Lemma folgt dann, $f, g, h \in \mathbb{Z}[x]$. Jetzt reduzieren wir alles modulo p:

$$X^n - 1 = \bar{f}(x) \bar{g}(x) \bar{h}(x).$$

Da $(p, n) = 1$ hat $X^n - 1 \in \mathbb{F}_p[X]$ keine mehrfachen Nullstellen; daraus

folgt, dass $\bar{f}$ und $\bar{g}$ Teilerfremd sind.

Andererseits ist $g(s^p) = 0$, also ist s eine Nullstelle von $g(x^p)$.

Daraus folgt

$$g(x^p) = f(x) \cdot k(x)$$

wobei (Gauss Lemma) $k \in \mathbb{Z}[x]$, k unitär. Modulo p folgt:

$$(\bar{g}(x))^p = \bar{g}(x^p) = \bar{f}(x)\,\bar{k}(x).$$

Ein Widerspruch mit der Tatsache, dass $\bar{f}$ und $\bar{g}$ Teilerfremd sind.

□

Sei $\zeta \in \mathbb{C}$ eine primitive n-te Einheitswurzel. Wir identifizieren $\mathbb{Q}[n]$ mit einem Unterkörper von $\mathbb{C}$.

Def. IV.27 Das n-te Zyklotomische Polynom ist

$$\Phi_n(X) = \prod_{(a,n)=1} (X - \zeta^a) .$$

Korollar IV.28 $\Phi_n \in \mathbb{Z}[X]$ und ist irreduzibel.

Beweis:

Da $\mathbb{Q}[n] = \mathbb{Q}[\zeta]$, folgt aus Thm IV.26:

$$\Phi_n(X) = \prod_{\sigma \in Gal(\mathbb{Q}[n]/\mathbb{Q})} (X - \sigma(\zeta))$$

und somit $\Phi_n \in \mathbb{Q}[X]$, da

$$\mathbb{Q} = \mathbb{Q}[n]^{Gal(\mathbb{Q}[n]/\mathbb{Q})} .$$

Nun gilt $X^n - 1 = \phi_n(X) \cdot h(X)$

mit $\phi_n, h \in \mathbb{Q}[X]$ beide unitär.

Aus dem Gauss Lemma folgt $\phi_n \in \mathbb{Z}[X]$.

□

Grad $\phi_n = \varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^\times|$,

die Euler φ-Funktion. Diese läßt sich bekanntlich wie folgt berechnen:

(1) $\varphi(nm) = \varphi(n)\varphi(m)$ falls $(n,m)=1$.

(2) $\varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$,

p Primzahl, $r \geq 1$.

Beispiele:

$\phi_1(X) = X - 1$, $\phi_2(X) = X + 1$

$\phi_3(X) = X^2 + X + 1$, $\phi_4(X) = X^2 + 1$

$\phi_5(X) = X^4 + X^3 + X^2 + X + 1$, $\phi_6(X) = X^2 - X + 1$

$$\phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

$$\phi_8(x) = x^4 + 1$$

$$\phi_9(x) = x^6 + x^3 + 1$$

Prop. IV. 29

(1) $$x^n - 1 = \prod_{d \mid n} \phi_d(x)$$

(2) p Primzahl:

$$\phi_p(x) = x^{p-1} + \cdots + 1$$

(3) $$\phi_n(x) = x^{\varphi(n)} \phi_n\left(\tfrac{1}{x}\right) \qquad n \geq 2.$$

(4) $$\phi_{p^r}(x) = \phi_p(x^{p^{r-1}})$$ p prim, $r \geq 1$.

(5) Falls p Primzahl, $(p, n) = 1$

$$\phi_{pn}(x) = \frac{\phi_n(x^p)}{\phi_n(x)}$$

(6) $$\Phi_n(X) = \prod_{d \mid n} (X^{n/d} - 1)^{\mu(d)}$$

Wobei μ die Möbius Funktion bezeichnet.

$$\mu : \mathbb{N}^* \longrightarrow \{-1, 0, 1\}.$$

$$\mu(n) = \begin{cases} 0 & \text{falls } n \text{ nicht quadratfrei} \\ (-1)^r & n = p_1 \cdots p_r, \text{ quadratfrei} \\ 1 & n = 1. \end{cases}$$

Beweis:

(1) $$X^n - 1 = \prod_{\zeta \in \mu_n} (X - \zeta)$$

Für jedes m, sei μ_m^{Prim} die Menge der primitiven m-ten Einheitswurzeln.

Dann folgt: $$\mu_n = \bigsqcup_{d \mid n} \mu_d^{\text{Prim}}$$

woraus (1) folgt.

(2) Falls p Primzahl folgt aus (1):

$$X^p - 1 = (X-1) \underbrace{\prod_{\substack{\zeta \in \mu_p \\ \text{prim}}} (X - \zeta)}_{\Phi_p(X)}$$

(3) ~~[illegible]~~

$$\Phi_n(X) = \prod_{\substack{\zeta \in \mu_n \\ \text{prim}}} (X - \zeta)$$

$$= X^{\varphi(n)} \prod (1 - \zeta X^{-1})$$

$$= T^{\varphi(n)} \underbrace{\prod (-\zeta)}_{\Phi_n(0)} \underbrace{\prod (X^{-1} - \zeta^{-1})}_{\Phi_n(X^{-1})}$$

Nun folgt aus

$$X^n - 1 = (X-1) \prod_{\substack{d \mid n \\ d > 1}} \Phi_d(X)$$

dass $\prod_{d \mid n,\ d>1} \phi_d(0) = 1$. (*)

Aus $\phi_p(0) = 1$ folgt mithilfe (*)

und Induktion über n, dass für $n \geq 2$:

$$\phi_n(0) = 1.$$

□

Wir enden diesen Abschnitt mit:

Thm IV.30:

Falls $(p, n) = 1$ dann ist das Bild

$$\mathrm{Gal}(\mathbb{F}_p[n]/\mathbb{F}_p) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$$

die durch p modulo erzeugte zyklische Untergruppe.

Beweis: Wir wissen, dass $\mathrm{Gal}(\mathbb{F}_p[n]/\mathbb{F}_p) = \langle \varphi_p \rangle$, erzeugt vom Frobenius

Automorphismus $\varphi_p(\zeta) = \zeta^p$.

Unter obiger Abbildung geht φ_p zu

$p \in (\mathbb{Z}/n\mathbb{Z})^\times$ ∎