Der Frobenius-Automorphismus endlicher Körper

Erinnerung: Sei p eine Primzahl.

- Für jeden Ring R ist durch $x \mapsto x^p$ ein Endomorphismus gegeben, der sog. Frobenius-Endomorphismus.
- Ist K ein endlicher Körper, dann ist dieser Endomorphismus auf K sogar ein Automorphismus.

Definition (23.1)

Sei $n \in \mathbb{N}$ und φ der Frobenius-Automorphismus von $\mathbb{F}_{q^n}$. Dann bezeichnen wir $\varphi_{\mathbb{F}_{q^n}|\mathbb{F}_q} = \varphi^r$ als den Frobenius-Automorphismus der Körpererweiterung $\mathbb{F}_{q^n}|\mathbb{F}_q$.

Satz (23.2)

Sei $n \in \mathbb{N}$.

(i) Die Erweiterung $\mathbb{F}_{q^n}|\mathbb{F}_q$ ist eine Galois-Erweiterung.

(ii) Die Galois-Gruppe $G = \mathrm{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$ wird vom Frobenius-Automorphismus $\varphi_{\mathbb{F}_{q^n}|\mathbb{F}_q}$ der Erweiterung $\mathbb{F}_{q^n}|\mathbb{F}_q$ erzeugt.

(iii) Durch $\mathbb{Z}/n\mathbb{Z} \to G$, $a + n\mathbb{Z} \mapsto \varphi^a$ ist ein Isomorphismus von Gruppen definiert.

Die Galoisgruppe von Kreisteilungskörpern

Satz (23.3)

Sei $n \in \mathbb{N}$ mit $n \geq 2$ und $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q})$.

(i) Für jedes $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, n) = 1$ gibt es ein eindeutig bestimmtes Element $\sigma_a \in G$ definiert durch $\sigma_a(\zeta_n) = \zeta_n^a$.

(ii) Es gibt einen Gruppenisomorphismus $\phi_n : (\mathbb{Z}/n\mathbb{Z})^\times \to G$ mit $\phi_n(a + n\mathbb{Z}) = \sigma_a$ für alle $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, n) = 1$.

Verallgemeinerung auf beliebige Grundkörper

Satz (23.4)

Sei $n \in \mathbb{N}$ mit $n \geq 2$, K ein Körper der Charakteristik 0, $L|K$ eine Körpererweiterung und $\zeta_n \in L$ eine primitive n-te Einheitswurzel. Dann ist $K(\zeta_n)|K$ eine Galois-Erweiterung, und die Galoisgruppe $G = \mathrm{Gal}(K(\zeta_n)|K)$ ist isomorph zu einer Untergruppe der primen Restklassengruppe $(\mathbb{Z}/n\mathbb{Z})^\times$.

Beweis von Satz 23.4

geg: K Körper, $\operatorname{char} K = 0$, $n \in \mathbb{N}$, $n \geq 2$

$\Leftrightarrow$ ζ_n primitive n-te Einheitswurzel in einer alg. Erweiterung von K $\Leftrightarrow$ $\mathrm{Gal}(K(\zeta_n)|K)$ ist isomorph zu einer Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^\times$

Sei $G = \mathrm{Gal}(K(\zeta_n)|K)$ und $\sigma \in G$. „Nullstellen auf Nullst." $\rightarrow$ Mit ζ_n ist auch $\sigma(\zeta_n)$ eine Nullstelle von $X^n - 1$. σ ist injektiv (als Körperhom.) $\rightarrow$ $\sigma|_{K(\zeta_n)^\times} : K(\zeta_n)^\times \to K(\zeta_n)^\times$ injektiv $\Rightarrow$ Mit ζ_n ist auch

$\sigma(\zeta_n)$ in $K(\zeta_n)^\times$ ein Elt. der Ordn. n Da die n-ten Einheitswurzeln im $K(\zeta_n)^\times$ eine zykl. Gruppe der Ordn. n bilden, existiert also ein $a \in \mathbb{Z}$ mit $ggT(a,n) = 1$ und $\sigma(\zeta_n) = \zeta_n^a$

$\Rightarrow$ Jedem Element σ aus G kann auf eindeutige Weise ein Element $a \in \mathbb{Z}$ mit $ggT(a,n) = 1$ und $1 \leq a < n$ zugeordnet werden. Dieses a ist durch σ eindeutig bestimmt. Sei $U = \{a + n\mathbb{Z} \mid \exists \sigma \in G$ mit $\sigma = \sigma_a\} \subseteq (\mathbb{Z}/n\mathbb{Z})^\times$ und definiere $\phi: G \to U$ durch $\sigma_a \mapsto (\mathbb{Z}/n\mathbb{Z})^\times$ Diese Abb. ist injektiv, denn Seien $\sigma, \tau \in G$ mit $\phi(\sigma) = \phi(\tau) = a + n\mathbb{Z}$, $a \in \{1, \dots, n-1\}$, $ggT(a,n) = 1 \Rightarrow \sigma = \sigma_a = \tau$ Außerdem $(\sigma_a \circ \sigma_b)(\zeta_n) = \sigma_a(\zeta_n^b) = \sigma_a(\zeta_n)^b = (\zeta_n^a)^b = \zeta_n^{ab} \Rightarrow ab + n\mathbb{Z} \in \phi(G)$, und $\phi(\sigma_a \circ \sigma_b) = \phi(\sigma_a)\,\phi(\sigma_b)$ jeweils für $a, b \in \{1, \dots, n-1\}$ und

$ggT(a,n) = ggT(b,n) = 1$ Dies zeigt, dass ϕ ein Homomorphismus, U eine Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^\times$ und ϕ insgesamt ein Isom. zwischen G und U ist. □

Definition der n-ten Wurzeln

Definition (23.5)

Sei K ein Körper, $a \in K$ und $n \in \mathbb{N}$. Ein Element $\alpha \in K$ wird eine n-te Wurzel von a genannt, falls $\alpha^n = a$ gilt. Im Fall $n = 2$ spricht man von Quadrat-, im Fall $n = 3$ von Kubikwurzeln.

Ein Element α ist also genau dann n-te Wurzel von a, wenn es die Gleichung $x^n - a = 0$ löst. Eine solche Gleichung wird als reine Gleichung bezeichnet.

Die Galoisgruppe der reinen Gleichung

Satz (23.6)

Sei $n \in \mathbb{N}$ mit $n \geq 2$ und K ein Körper mit $\mathrm{char}(K) \nmid n$, was $\mathrm{char}(K) = 0$ einschließt. Wir setzen voraus, dass K eine primitive n-te Einheitswurzel ζ enthält. Weiter sei $a \in K^\times$, L ein Erweiterungskörper von K und $\alpha \in L$ eine n-te Wurzel von a.

(i) Die Erweiterung $K(\alpha)|K$ ist eine Galois-Erweiterung.

(ii) Sei G die Galoisgruppe von $K(\alpha)|K$. Dann gibt es einen Teiler d von n mit der Eigenschaft, dass G isomorph zu $\mathbb{Z}/d\mathbb{Z}$ ist.

(iii) Es gilt $G \cong \mathbb{Z}/n\mathbb{Z}$ genau dann, wenn das Polynom $f = x^n - a$ in $K[x]$ irreduzibel ist.

Beweis von Satz 23.6.

geg. Körper K, $n \in \mathbb{N}$, $n \geq 2$ mit $\mathrm{char}(K) \nmid n$
ζ primitive n-te Einheitswurzel in K
$a \in K^\times$, $f = x^n - a \in K[x]$, α Nullstelle von f

zu zeigen: $K(\alpha)/K$ ist eine Galois-Erw.

Zeige zunächst, dass $K(\alpha)$ Zerf.körper von f ist.
Für $0 \leq k < n$ gilt $f(\zeta^k \alpha) = (\zeta^k \alpha)^n - a =$
$(\zeta^n)^k \alpha^n - a = 1^k \cdot a - a = 0$. Außerdem sind die Elemente $\zeta^k \alpha$ diese Form alle verschieden, denn:
$\mathrm{ord}(\zeta) = n$ in $K(\zeta)^\times \Rightarrow 1, \zeta, \dots, \zeta^{n-1}$ alle verschieden, außerdem: $a \neq 0 \underset{\alpha^n = a}{\Rightarrow} \alpha \neq 0 \Rightarrow$ Elemente $\alpha, \zeta\alpha, \dots, \zeta^{n-1}\alpha$

alle verschieden. Also hat f in $K(\alpha)$ n verschiedene Nullstellen $\xrightarrow{\text{grad}(f)=n}$ f zerfällt über $K(\alpha)$ in Linearfaktoren. Außerdem wird $K(\alpha)|K$ von den Nullstellen von f in $K(\alpha)$ erzeugt, weil sie bereits von $\{\alpha\}$ erzeugt wird.
$\rightarrow$ $K(\alpha)$ ist Zerf.körp. von f über $K \Rightarrow K(\alpha)|K$ ist normal

noch zu zeigen: $K(\alpha)|K$ ist separabel

genügt: α ist separabel über K (weil die über K sep. Elemente einen Zwischenkörper von $K(\alpha)|K$ bilden) Sei $g = \mu_{\alpha,K}$. $f(\alpha)=0$, $f \in K[x]$

$\Rightarrow g \mid f$ $\quad ggT(f,f') = ggT(x^n - a,\ nx^{n-1})$

$= 1 \Rightarrow f$ hat in keiner Erw. von K mehrfache

$\uparrow_{n \neq 0 \text{ in } K}$
$a \neq 0$

Nullst., das Element g wg. g | f sonst auch nicht
$\Rightarrow$ g ist separabel $\rightarrow$ α ist sep. über K.

zu (ii) Sei $G = Gal(K(S)|K)$ und $\sigma \in G$
„Nullst. auf Nullst." $\rightarrow$ $\sigma(\alpha)$ ist Nullst. von f
$\Rightarrow \sigma(\alpha)^n = a = \alpha^n \Rightarrow \left(\frac{\sigma(\alpha)}{\alpha}\right)^n = 1 \rightarrow$
$\frac{\sigma(\alpha)}{\alpha}$ ist n-te Einheitswurzel $\rightarrow$ $\exists\, k \in \{0,1,\dots,n-1\}$
$\mu_n = \langle S \rangle$
mit $\sigma(\alpha) = S^k \alpha$. Wie im Beweis von Satz 23.4
können wir jedem Element von G also ein $k \in \{0,\dots,n-1\}$
zuordnen, das umgekehrt ein Element $\sigma_k \in G$
eindeutig festlegt. Definiere $U = \{k + n\mathbb{Z} \mid$
$\exists\, \sigma \in G$ mit $\sigma = \sigma_k\}$ und $\phi : G \to U, \sigma_k \mapsto k + n\mathbb{Z}$
leicht zu sehen: ϕ ist injektiv und ein Gruppen-

Isomorphismus, U also eine Untergr. von $(\mathbb{Z}/n\mathbb{Z}, +)$ und ϕ ein Isomorphismus (u.a. Seien $k, l \in \{0, \dots, n-1\}$

$(\sigma_k \circ \sigma_l)(\alpha) = \sigma_k(\beta^l \alpha) = \sigma(\beta)^l \sigma(\alpha) = \beta^l \sigma(\alpha) =$
$\Delta \beta \in K$

$\beta^l \cdot \beta^k \alpha = \beta^{l+k} \alpha \Rightarrow k+l+n\mathbb{Z} \in U, \ \sigma_k \circ \sigma_l = \sigma_{k+l}$)

zu (iii) z.Zg: f ist irreduzibel in $K[x] \Leftrightarrow G \cong \mathbb{Z}/n\mathbb{Z}$

Sei $g = M_{\alpha, K} \in K[x]$, $f \in K[x]$, $f(\alpha) = 0 \Rightarrow g \mid f$

„$\Rightarrow$" f irred., $g \mid f \Rightarrow f = g \Rightarrow [K(\alpha) : K] =$
$\operatorname{grad}(f) = n. \Rightarrow |G| = |\mathrm{Gal}(K(\alpha) \mid K)| = n$

bekannt aus (i): G ist isomorph zu einer Untergr. von $(\mathbb{Z}/n\mathbb{Z}, +)$
$\overset{|G|=n}{\Rightarrow} G \cong \mathbb{Z}/n\mathbb{Z}$.

"$\Leftarrow$" $\forall \alpha \Rightarrow |G| = n \Rightarrow \operatorname{grad}(g) = n = \operatorname{grad}(f)$

$g \mid f$ $f = g \Rightarrow f$ stirred in $K[x]$. $\square$

g, normiert

Das Dedekindsche Lemma

Satz (23.7)

Sei H eine Halbgruppe und K ein Körper. Dann ist jede endliche Menge von Halbgruppen-Homomorphismen $H \to K^\times$ im K-Vektorraum $\mathrm{Abb}(H, K)$ der Abbildungen $H \to K$ linear unabhängig.

Beweis des Dedekindschen Lemmas:

geg.: Halbgruppe H, K Körper

z.zg.: Jede endliche Menge von Halbgruppen-Hom. $H \to K^\times$ ist in $Abb(H, K)$ linear unabh.

Beweis über die Mächtigkeit n der Menge

Ind.-Anf. $n = 1$ Sei σ ein Halbgruppen-Hom

$\sigma(H) \subseteq K^\times \Rightarrow \sigma \neq 0$ in $Abb(H, K)$

$\Rightarrow \{\sigma\}$ ist linear unabh. Teilm. von $Abb(H, K)$

Ind.-Schritt $n \mapsto n+1$:

Seien $\tau_1, \dots, \tau_{n+1}$ $n+1$ verschiedene Halbg. -

Beh. $\tau_1 \neq \tau_{n+1} \Rightarrow \exists a \in H$ mit $\tau_1(a) \neq \tau_{n+1}(a)$

Seien $c_1, \dots, c_{n+1} \in K$ mit $\sum_{k=1}^{n+1} c_k \tau_k = 0$

z.zg.: $c_1 = \dots = c_{n+1} = 0$

Für bel. $b \in H$ gilt $\sum_{k=2}^{n+1} c_k (\tau_k(a) - \tau_1(a)) \tau_k(b)$

$$= \sum_{k=2}^{n+1} c_k \tau_k(a) \tau_k(b) - \sum_{k=2}^{n+1} c_k \tau_1(a) \tau_k(b)$$

$$= \sum_{k=2}^{n+1} c_k \tau_k(ab) - \tau_1(a) \sum_{k=2}^{n+1} c_k \tau_k(b)$$

$$= -c_1 \tau_1(ab) + \tau_1(a) c_1 \tau_1(b)$$

$$= -c_1 \tau_1(a) \tau_1(b) + c_1 \tau(ab) = 0$$

$$\Rightarrow \sum_{k=2}^{n+1} c_k \left(\tau_k(a) - \tau_1(a)\right) \cdot \tau_k = 0 \text{ in } \mathrm{Abb}(H, K)$$

Ind.-V. (jede n-elem. Teilm. ist lin. unabh.) $\Rightarrow$

$$c_k\left(\tau_k(a) - \tau_1(a)\right) = 0 \quad \text{für } 2 \le k \le n+1$$

$\tau_{n+1}(a) - \tau_1(a) \neq 0 \Rightarrow c_{n+1} = 0 \overset{\text{s.o.}}{\Rightarrow} \sum_{k=1}^{n} c_k \tau_k = 0$

n-malige Anwendung der Ind.-V. liefert $c_1 = \ldots = c_n = 0$.

□

Definition der Lagrangeschen Resolventen

Definition (23.8)

Sei $L|K$ eine endliche Galois-Erweiterung mit einer zyklischen Galoisgruppe G der Ordnung n, wobei K ein primtive n-te Einheitswurzel ζ enthält. Sei $\sigma \in G$ ein Element mit $G = \langle \sigma \rangle$. Dann nennt man für beliebiges $\alpha \in L$ das Element

$$\vartheta(\sigma, \alpha) \quad = \quad \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + ... + \zeta^{n-1}\sigma^{n-1}(\alpha)$$

die Lagrangesche Resolvente von α bezüglich σ.

Bem: Aus dem Dedekindschen Lemma folgt, dass $\vartheta(\sigma, \alpha)$ für mind. ein $\alpha \in L^\times$ ungleich null ist. Denn ansonsten wäre in $\mathrm{Abb}(L^\times, L^\times)$ die Linearkomb. $1 \cdot \sigma^0 + 1 \cdot \sigma + \dots + \varphi^{n-1} \sigma^{n-1}$ gleich Null, die Menge $\{\sigma^0, \sigma, \dots, \sigma^{n-1}\}$ der Halbgruppen-Hom. $L^\times \to L^\times$ also linear abhängig

Zyklische Galois-Erweiterungen und Wurzeln

Satz (23.9)

Sei $n \in \mathbb{N}$, K ein Körper, der eine primitive n-te Einheitswurzel ζ enthält, und $L|K$ eine Galois-Erweiterung vom Grad n mit zyklischer Galoisgruppe G. Dann gibt es ein Element $\vartheta \in L$ mit $L = K(\vartheta)$ und $\vartheta^n \in K$.

Beweis von Satz 23.9

geg: Körpererweiterung $L|K$, $n \in \mathbb{N}$

ζ primitive n-te Einheitswurzel in K

Vor: $L|K$ ist galoissch mit zyklischer Galoisgruppe G der Ordnung n

Beh: $\exists \vartheta \in L$ mit $L = K(\vartheta)$ und $\vartheta^n \in K$

Dedekindsches Lemma (wird nachgeliefert) $\Rightarrow \exists \alpha \in L$, so dass die Lagrange'sche Resolvente

$$\vartheta = \vartheta(\alpha, \sigma) = \alpha + \zeta\sigma(\alpha) + \ldots + \zeta^{n-1}\sigma^{n-1}(\alpha) = \sum_{k=0}^{n-1} \zeta^k \sigma^k(\alpha)$$

Beh. $\exists \vartheta \in L$ mit $L = K(\vartheta)$ und $\vartheta^n \in K$

ungleich Null ist, wobei σ einen bel. gewählten Erzeuger der Gruppe G bezeichnet.

Wende σ auf ϑ an. $\Rightarrow \sigma(\vartheta) = \sum_{k=0}^{n-1} \sigma(\zeta^k \sigma^k(\alpha)) =$

$\sum_{k=0}^{n-1} \sigma(\zeta)^k \sigma^{k+1}(\alpha) = \underset{\zeta \in K}{=} \sum_{k=0}^{n-1} \zeta^k \sigma^{k+1}(\alpha) = \zeta^{-1} \sum_{k=0}^{n-1} \zeta^{k+1} \sigma^{k+1}(\alpha)$

$= \zeta^{-1} \sum_{k=1}^{n} \zeta^k \sigma^k(\alpha) \underset{\substack{\uparrow \zeta^n = 1 = \zeta^0 \\ \sigma^n = id = \sigma^0}}{=} \zeta^{-1} \sum_{k=0}^{n-1} \zeta^k \sigma^k(\alpha) = \zeta^{-1} \vartheta$

$\Rightarrow \sigma(\vartheta^n) = \sigma(\vartheta)^n = (\zeta^{-1})^n \vartheta^n = 1 \cdot \vartheta^n = \vartheta^n \overset{G = \langle \sigma \rangle}{\Rightarrow} \vartheta^n \in L^G$

Auf Grund der Galoistheorie gilt $L^G = K \Rightarrow \vartheta^n \in K$

Sei nun $g = \mu_{\vartheta, K}$ „Nullst. auf Nullst.", ϑ Nullst. von $g \Rightarrow$

$\sigma^k(\vartheta)$ ist Nullst. von g für $1 \le k \le n$ Für $1 \le k \le n$ gilt

$\sigma^k(v) = \vartheta^{-k} v \overset{\vartheta^n = 1}{=} \vartheta^{n-k} v$ Also ist

$\vartheta^k v$ für $0 \leq k < n$ Nullst. von g.

$v \neq 0$, $\operatorname{ord}(\vartheta) = n$ in $K^\times$ $\Rightarrow$ g hat mind.

n verschiedene Nullst. $\Rightarrow \operatorname{grad}(g) \geq n$

andererseits: $K(v)$ ist Zwischenkörp. von $L|K$

Gradformel $\Rightarrow$ $n = |G| = [L:K] =$

$[L:K] \cdot [K(v):K] = [L:K] \cdot \operatorname{grad}(g)$

$\Rightarrow$ erhalte $[K(v):K] = \operatorname{grad}(g) = n =$

$[L:K] \overset{K(v) \leq L}{\Rightarrow} L = K(v)$ $\square$