Der Frobenius-Automorphismus endlicher Körper

Erinnerung: Sei p eine Primzahl.

- Für jeden Ring R mit $\mathrm{char}(R) = p$ ist durch $x \mapsto x^p$ ein Endomorphismus von R gegeben, der sog. Frobenius-Endomorphismus.
- Ist K darüber hinaus ein endlicher Körper, dann ist dieser Endomorphismus auf K sogar ein Automorphismus.

Sei nun $r \in \mathbb{N}$ und $q = p^r$.

Definition (22.1)

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 (22.2)

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 $\mathbb{Z}/n\mathbb{Z} \to G$, $a + n\mathbb{Z} \mapsto \varphi^a_{\mathbb{F}_{q^n}|\mathbb{F}_q}$ ist ein Isomorphismus von Gruppen definiert.

Bem: Sei $n \in \mathbb{N}$, $n \geq 2$ und $\zeta_n = e^{2\pi i/n}$ (primitive n-te Einheitswurzel, d.h. ein Element der Ordnung n in $\mathbb{C}^\times$).

Dann ist $\mathbb{Q}(\zeta_n)|\mathbb{Q}$ eine Galois-Erweiterung, denn:

Die Gleichung $\Phi_n = \prod_{\substack{0 \leq a < n \\ \text{ggT}(a,n)=1}} (x - \zeta_n^a)$ zeigt, dass

$\mathbb{Q}(\zeta_n)$ Zerfällungskörper von Φ_n über $\mathbb{Q}$ ist $\Rightarrow \mathbb{Q}(\zeta_n)|\mathbb{Q}$ ist normal $\Rightarrow \mathbb{Q}(\zeta_n)|\mathbb{Q}$ algebraisch $\overset{\text{char}(\mathbb{Q})=0}{\Rightarrow}$ $\mathbb{Q}(\zeta_n)|\mathbb{Q}$ ist separabel. Da Φ_n über $\mathbb{Q}$ irreduzibel ist, gilt außerdem $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \text{grad}(\Phi_n) = \varphi(n)$.

Die Galoisgruppe von Kreisteilungskörpern

Satz (22.3)

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 $\mathrm{ggT}(a, n) = 1$.

Beweis von Satz 22.3:

geg: $n \in \mathbb{N}$, $n \geq 2$. $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n) | \mathbb{Q})$

zu (i) Sei $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,n) = 1 \Rightarrow \zeta_n^a$ ist primitive n-te Einheitswurzel, also eine Nullstelle von Φ_n; ebenso wie ζ_n selbst. Fortsetzungssatz (der Galoistheorie), Irreduzibilität von $\Phi_n \Rightarrow$ $\exists \sigma_a \in G$ mit $\sigma_a(\zeta_n) = \zeta_n^a$. Da $\mathbb{Q}(\zeta_n)$ über $\mathbb{Q}$ durch ζ_n erzeugt wird, ist σ_a durch diese Eig. eindeutig bestimmt.

zu (ii) Definiere $\phi : (\mathbb{Z}/n\mathbb{Z})^\times \to G$ durch $\phi(a) = \sigma_a$ für alle $a \in \{0, 1, \ldots, n-1\}$ mit $\mathrm{ggT}(a,n) = 1$. Beh.:

(1) $\forall a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,n) = 1$ gilt $\phi(a) = \sigma_a$

(2) ϕ ist Gruppenhom.

(3) ϕ ist bijektiv

zu (1) Sei $a \in \mathbb{Z}$ mit $ggT(a,n) = 1$. Div. mit Rest $\rightarrow$ $\exists q, r \in \mathbb{Z}$ mit $a = qn + r$ und $0 \leq r \leq n-1$ Aus $ggT(a,n) = 1$ folgt $ggT(r,n) = 1$ $\Rightarrow \phi(r + n\mathbb{Z}) = \sigma_r$

$\sigma_a(\zeta_n) = \zeta_n^a = \zeta_n^{qn+r} = (\zeta_n^n)^q \cdot \zeta_n^r = 1^q \cdot \zeta_n^r$

$= \zeta_n^r = \sigma_r(\zeta_n) \Rightarrow \sigma_r = \sigma_a$ (da jedes $\sigma \in G$ durch $\sigma(\zeta_n)$ eind. (best.) insgesamt:

$\phi(a + n\mathbb{Z}) \overset{a \equiv r \bmod n}{=} \phi(r + n\mathbb{Z}) = \sigma_r = \sigma_a$

zu (2) Seien $a, b \in \mathbb{Z}$ mit $ggT(a,n) = ggT(b,n) = 1$ Dann gilt $(\sigma_a \circ \sigma_b)(\zeta_n) = \sigma_a(\sigma_b(\zeta_n))$

$= \sigma_a(\zeta_n^b) = \sigma_a(\zeta_n)^b = (\zeta_n^a)^b = \zeta_n^{ab}$

$= \sigma_{ab}(\zeta_n) \Rightarrow \sigma_a \circ \sigma_b = \sigma_{ab} \Rightarrow$

$\phi(a+n\mathbb{Z}) \circ \phi(b+n\mathbb{Z}) = \sigma_a \circ \sigma_b = \sigma_{ab} =$

$\phi(ab+n\mathbb{Z}) = \phi((a+n\mathbb{Z})(b+n\mathbb{Z}))$

$z_n(b)$ Injektivität: Sei $a \in \mathbb{Z}$ mit $ggT(a,n) = 1$

und $a+n\mathbb{Z} \in \ker(\phi)$ z.zg: $a+n\mathbb{Z} = 1+n\mathbb{Z}$

$a+n\mathbb{Z} \in \ker(\phi) \Rightarrow \phi(a+n\mathbb{Z}) = id_{\mathbb{Q}(\zeta_n)}$

$\Rightarrow \sigma_a = \sigma_1 \Rightarrow \zeta_n^a = \sigma_a(\zeta_n) = id_{\mathbb{Q}(\zeta_n)}(\zeta_n)$

$= \zeta_n \Rightarrow \zeta_n^{a-1} = 1 \overset{\text{ord}(\zeta_n)=n \text{ in } \mathbb{C}^\times}{\Rightarrow} n \mid (a-1) \Rightarrow$

$a \equiv 1 \bmod n \Rightarrow a+n\mathbb{Z} = 1+n\mathbb{Z}$

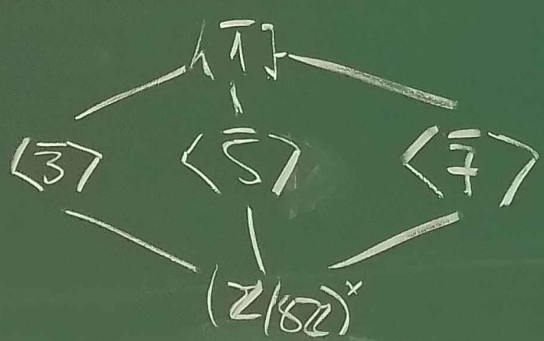
Wegen $|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = |G|$

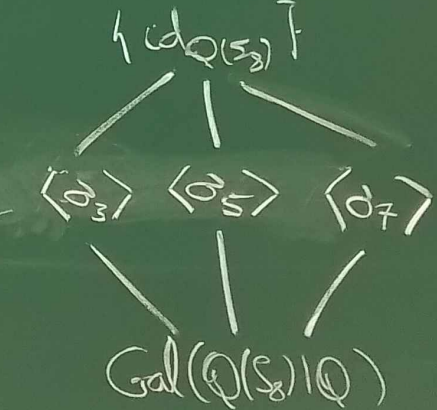
ist die Abbildung damit auch surjektiv, insgesamt bijektiv. □

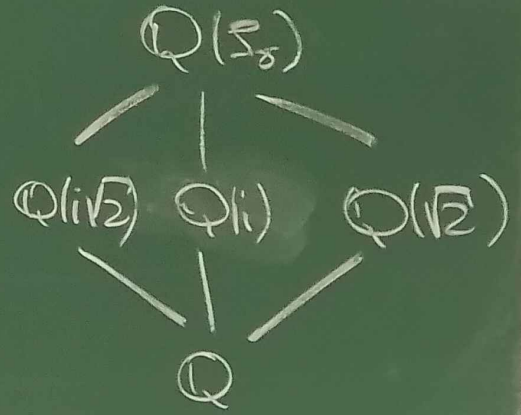
Beispiel: Zwischenkörperstruktur von $\mathbb{Q}(\zeta_8)|\mathbb{Q}$

(Es ist $\zeta_8 = \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}$.)

Untergruppen von $(\mathbb{Z}/8\mathbb{Z})^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$	Untergruppen von $\mathbb{Q}(\zeta_8)|\mathbb{Q}$	Zwischenkörper von $\mathbb{Q}(\zeta_8)|\mathbb{Q}$







Für jede n-te Einheitswurzel ζ gilt $\zeta^{-1} = \bar{\zeta}$ (Grund: $\zeta\bar{\zeta} = |\zeta|^2 = 1^2 = 1$). $\sigma_7(\zeta_8) = \zeta_8^7 = \zeta_8^{-1} = \bar{\zeta}_8$

$\Rightarrow$ σ_7 ist die Einschränkung der komplexen Konjugation auf $\mathbb{Q}(\zeta_8)$

$\Rightarrow \sigma_7(\sqrt{2}) = \sqrt{2} \Rightarrow \sqrt{2} \in \mathbb{Q}(\zeta_8)^{\langle\sigma_7\rangle}$

$\sigma_5(i) = \sigma_5(\zeta_8^2) = \sigma_5(\zeta_8)^2 = (\zeta_8^5)^2 = \zeta_8^{10} = \zeta_8^2 = i$

$\Rightarrow i \in \mathbb{Q}(\zeta_8)^{\langle\sigma_5\rangle}$

Übungsaufgabe: $\sigma_3(i\sqrt{2}) = i\sqrt{2}$ (Hinweis: $\sqrt{2} = \zeta_8 + \zeta_8^{-1}$)

(Früher gezeigt: $i, \sqrt{2}, i\sqrt{2} \in \mathbb{Q}(\zeta_8)$)

Die Galoisgruppe von Kreisteilungskörpern

Satz (22.4)

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, also ein Element in $L^\times$ der Ordnung n. Dann ist $K(\zeta_n)|K$ eine Galois-Erweiterung, und die Galoisgruppe $G = \mathrm{Gal}(K(\zeta_n)|K)$ ist isomorph zu einer Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^\times$.

Beweis von Satz 22.4

geg.: Körper K mit $\mathrm{char}(K) = 0$, $n \in \mathbb{N}$ mit $n \geq 2$

$L | K$ Körpererw., $\zeta_n \in L^\times$ primitive n-te Einheitswurzel

z.zg.: (1) $K(\zeta_n) | K$ ist galoisch

(2) Die Galoisgruppe $G = \mathrm{Gal}(K(\zeta_n) | K)$ ist isomorph zu einer Untergr. von $(\mathbb{Z}/n\mathbb{Z})^\times$.

zu (1) Überprüfe, dass $K(\zeta_n)$ Zerfällungskörper von $x^n - 1 \in K[x]$ über K ist (Grund: $x^n - 1 = \prod_{a=0}^{n-1} (x - \zeta_n^a)$)

$\Rightarrow K(\zeta_n) | K$ ist normal $\longrightarrow K(\zeta_n) | K$ ist algebraisch

$\overset{\mathrm{char}(K)=0}{\Rightarrow}$ $K(\zeta_n) | K$ ist separabel, insgesamt galoisch

zu (2) Definition einer Abbildung $\phi : G \to (\mathbb{Z}/n\mathbb{Z})^*$

Sei $\sigma \in G$. Mit ζ_n ist auch $\sigma(\zeta_n)$ eine Nullstelle von $x^n - 1$

$\Rightarrow \exists a \in \{0, 1, \ldots, n-1\} : \sigma(\zeta_n) = \zeta_n^a$ Da σ ein Automorphismus ist, gilt $\mathrm{ord}(\zeta_n^a) = \mathrm{ord}(\zeta_n) = n \Rightarrow \mathrm{ggT}(a, n) = 1$ (gzsd:

$\mathrm{ord}(\zeta_n^a) = \frac{\mathrm{ord}(\zeta_n)}{\mathrm{ggT}(\mathrm{ord}(\zeta_n), a)} = \frac{n}{\mathrm{ggT}(a, n)}$) $\Rightarrow a + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^*$

Definiere nun $\phi(\sigma) = a + n\mathbb{Z}$ zu überprüfen ist:

(2.1) ϕ ist ein Gruppenhom. (2.2) ϕ ist injektiv

zu (2.1) Seien $\sigma, \tau \in G \Rightarrow \exists a, b \in \mathbb{Z}$ mit $\phi(\sigma) = a + n\mathbb{Z}$, $\phi(\tau) = b + n\mathbb{Z}$, $\mathrm{ggT}(a, n) = \mathrm{ggT}(b, n) = 1$ Es gilt außerdem $\sigma(\zeta_n) = \zeta_n^a$ und $\tau(\zeta_n) = \zeta_n^b \Rightarrow (\sigma \circ \tau)(\zeta_n) = \sigma(\tau(\zeta_n)) = \sigma(\zeta_n^b) = \sigma(\zeta_n)^b = (\zeta_n^a)^b = \zeta_n^{ab} \Rightarrow \phi(\sigma\tau) = ab + n\mathbb{Z} = (a + n\mathbb{Z})(b + n\mathbb{Z})$

$= \phi(\sigma) \cdot \phi(\tau)$

zu (2.2) Sei $\sigma \in \ker(\phi)$. zzg $\sigma = id_{K(\zeta_n)}$

$\phi(\sigma) = 1 + n\mathbb{Z} \Rightarrow \sigma(\zeta_n) = \zeta_n^1 = \zeta_n \Rightarrow$

$\sigma = id_{K(\zeta_n)}$ (da σ durch $\sigma(\zeta_n)$ eindeutig bestimmt ist)

Also ist G isomorph zur Untergruppe $\phi(G)$ von $(\mathbb{Z}/n\mathbb{Z})^\times$. □

Definition der n-ten Wurzeln

Definition (22.5)

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.

Bedeutung des Wurzelsymbols in dieser Vorlesung

geg: Körper K mit $\mathrm{char}(K) = 0$

Sei $n \in \mathbb{N}$, $n \geq 2$ und

$$R_K^{(n)} = \{ a \in K \mid \exists\, \beta \in K \text{ mit } \beta^n = a \}$$

Im Folgenden bezeichnet $\sqrt[n]{\ }$ stets eine (bel. gewählte) Abbildung $R_K^{(n)} \to K$ mit der Eigenschaft $(\sqrt[n]{a})^n = a$. Dabei ist $\sqrt{\ }$ gleichbedeutend mit $\sqrt[2]{\ }$.

(Achtung: Nicht vorausgesetzt wird

$\sqrt[n]{a^n} = a \quad \forall a \in R_K^{(n)}$, und auch nicht

$\sqrt[n]{ab} = \sqrt[n]{a} \cdot \sqrt[n]{b}$.)

Bsp. (1) $K = \mathbb{R}$, n gerade. Dann ist $R_K^{(n)} = \mathbb{R}_+$.
Man kann dann z.B. $\sqrt[n]{a}$ definieren als die eindeutig bestimmte Zahl $\alpha \in \mathbb{R}_+$ mit $\alpha^n = a$. ($\sqrt[4]{16} = 2$).

(2) $K = \mathbb{R}$, n ungerade. Dann ist $R_K^{(n)} = \mathbb{R} = K$.
Man kann dann die Fkt. $\sqrt[n]{\ }$ für alle $a \in \mathbb{R}$ mit $a \geq 0$ definieren wie unter (1), und für $a < 0$ durch $\sqrt[n]{a} = -\sqrt[n]{|a|}$. ($\sqrt[3]{8} = 2$, $\sqrt[3]{-8} = -2$)

(3) $K = \mathbb{C}$, $n \in \mathbb{N}$, $n \geq 2$ beliebig. Dann ist $R_K^{(n)} = \mathbb{C}$

Eine Standard-Definition für die n-te Wurzelfunktion auf $\mathbb{C}$ ist gegeben durch $\sqrt[n]{z} = \begin{cases} e^{\frac{1}{n}\ln(z)} & \text{falls } z \neq 0 \\ 0 & \text{falls } z = 0 \end{cases}$

wobei $\ln : \mathbb{C}^\times \to \mathbb{C}$ den komplexen Logarithmus bezeichnet. zu beachten: $\mathrm{Im}(\ln(z)) = \arg(z) \in]-\pi, \pi]$ für alle $z \in \mathbb{C}^\times$

Hinweis: $\sqrt[3]{-8}$ im Sinne von Def. (3) ist keine reelle Zahl, insb. ist $\sqrt[3]{-8} \neq -2$