

Die Galoisgruppe eines Polynoms

Definition (22.7)

Sei K ein Körper und $f \in K[x]$ ein nicht-konstantes Polynom, dessen irreduzible Faktoren alle separabel sind, und sei L ein Zerfällungskörper von f über K . Dann bezeichnet man $\text{Gal}(L|K)$ auch als die Galoisgruppe $\text{Gal}(f|K)$ des Polynoms f .

Satz (22.8)

Sei $f \in K[x]$ ein Polynom wie in Def. 22.7 und L ein Zerfällungskörper von f über K . Seien $\alpha_1, \dots, \alpha_n \in L$ die verschiedenen Nullstellen von f in L . Dann gibt es einen injektiven Homomorphismus $\phi : \text{Gal}(f|K) \rightarrow S_n$ mit

$$\sigma(\alpha_k) = \alpha_{\phi(\sigma)(k)} \quad \text{für} \quad 1 \leq k \leq n.$$

Beweis von Satz 22.8

geg. $f \in K[X] \setminus K$, L Zerf.-korp. von f über K
so dass $L|K$ galois'sch $S = \{\alpha_1, \dots, \alpha_n\}$ n -elem Menge
der Nullstellen ($\Rightarrow L = K(S)$)

Schritt 1: Jedes $\sigma \in G$ liefert ein Element aus $\text{Per}(S)$.

Jede Nullst. von f muss auf eine Nullst. von f abgebildet
werden (da σ -Hom.). $\Rightarrow \sigma(S) \subseteq S \Rightarrow$ können $\sigma|_S$
als Abb. $S \rightarrow S$ betrachten σ invertierbar $\Rightarrow \sigma|_S$ ist
Sendf.
 $\Rightarrow \sigma|_S$ bijektiv $\Rightarrow$ erhalten Abb. $\phi: G \rightarrow \text{Per}(S)$.

durch $\sigma \mapsto \sigma|_S$ Es gilt $(\sigma|_S \circ \tau|_S) = (\sigma \circ \tau)|_S$

$\forall \sigma, \tau \in G \rightarrow \phi$ ist Hom. Da jedes σ durch $\sigma(x_k)$ ($1 \leq k \leq n$)
eindeut. bestimmt ist, ist ϕ injektiv

Sei $L: M_n \rightarrow S$ geg. durch $L(k) = x_k$ für $1 \leq k \leq n$, diese ist
offenbar bijektiv $\rightarrow$ erhalte einen Isom. $\tilde{\tau}$ zwischen $S_n =$
 $\text{Per}(M_n)$ und $\text{Per}(S)$ durch $\sigma \mapsto L \circ \sigma \circ L^{-1}$

$\rightarrow$ erhalte ein Hom. $\psi: G \rightarrow S_n$ durch $\psi = \tilde{\tau}^{-1} \circ \phi$

noch z.zg. $\sigma(x_k) = x_{\psi(\sigma)(k)}$ für $1 \leq k \leq n, \sigma \in G$ $\text{Per}(S) \rightarrow S_n$ $G \rightarrow \text{Per}(S)$

Sei also $k \in M_n, \sigma \in G$ Sei $l \in M_n$ geg. durch $\sigma(x_k) = x_l$.

z.zg. $\psi(\sigma)(k) = l$ Es gilt $\psi(\sigma)(k) = (\tilde{\tau}^{-1} \circ \phi)(\sigma)(k)$

$$= \tilde{\tau}^{-1}(\phi(\sigma))(k) = (L^{-1} \circ \sigma \circ L)(k) = (L^{-1} \circ \sigma)(x_k) = L^{-1}(x_l) = l \quad \square$$

Anwendungsbeispiel 2:

Die Galoisgruppe von $f = x^3 - 2 \in \mathbb{Q}[x]$

komplexe Nullst. von f : $\alpha_1 = \alpha$, $\alpha_2 = \zeta\alpha$, $\alpha_3 = \zeta^2\alpha$
wobei $\alpha = \sqrt[3]{2}$, $\zeta = -\frac{1}{2} + \frac{1}{2}\sqrt{3}i$ primitive dritte
Einheitswurzel

bekannt: $L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) = \mathbb{Q}(\alpha, \zeta)$ ist Zer-
fällungskörper von f über $\mathbb{Q}$, außerdem:

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 3 = 6$$

Sei $G = \text{Gal}(L/\mathbb{Q}) = \text{Gal}(f/\mathbb{Q})$

$$|G| = [L : \mathbb{Q}] = 6 \quad \text{Nach Satz 22.8 ist}$$

G isomorph zu einer Untergr. von S_3 .

$$|G| = 6 = |S_3| \Rightarrow G \leq S_3$$

Untergr. von S_3 : id , $\langle (12) \rangle$, $\langle (13) \rangle$, $\langle (23) \rangle$,
 $\langle (123) \rangle$, S_3

6 Untergruppen $\xrightarrow{\text{Hauptsatz der Galoistheorie}}$ $L/\mathbb{Q}$ hat genau 6
Zwischkörper (4 echte)

Zwei der echten Zwischkörper sind $\mathbb{Q}(\alpha)$ und
 $\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{-3})$, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ und $[\mathbb{Q}(\beta) : \mathbb{Q}]$
 $= 2$. Beh.: Die anderen beiden echten Zwischkör-
per sind $\mathbb{Q}(\beta\alpha)$, $\mathbb{Q}(\beta^2\alpha)$ klar.

$[\mathbb{Q}(\beta\alpha) : \mathbb{Q}] = [\mathbb{Q}(\beta^2\alpha) : \mathbb{Q}] = \text{grad}(f) = 3$ (weil
 f das Min. pol. von $\beta\alpha$, $\beta^2\alpha$ ist)

Wegen $x \in \mathbb{R}$ und $\sqrt[3]{x}, \sqrt[5]{x} \in \mathbb{C} \setminus \mathbb{R}$ gilt

$\mathbb{Q}(x) \neq \mathbb{Q}(\sqrt[3]{x}), \mathbb{Q}(\sqrt[5]{x})$ noch zu überprüfen:

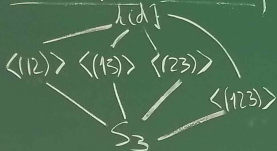
$\mathbb{Q}(\sqrt[3]{x}) \neq \mathbb{Q}(\sqrt[5]{x})$ Ang. $\mathbb{Q}(\sqrt[3]{x}) = \mathbb{Q}(\sqrt[5]{x}) \Rightarrow$

$\sqrt[3]{x}, \sqrt[5]{x} \in \mathbb{Q}(\sqrt[3]{x}) \Rightarrow \sqrt[5]{x} = \frac{\sqrt[5]{x}}{\sqrt[3]{x}} \in \mathbb{Q}(\sqrt[3]{x}), x = \frac{\sqrt[3]{x}}{\sqrt[5]{x}} \in \mathbb{Q}(\sqrt[3]{x})$

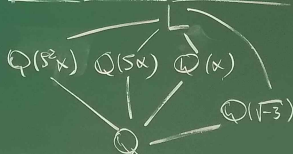
$\Rightarrow L = \mathbb{Q}(x, \sqrt[3]{x}) \subseteq \mathbb{Q}(\sqrt[3]{x}) \nmid$ da $[L:\mathbb{Q}] = 6, [\mathbb{Q}(\sqrt[3]{x}):\mathbb{Q}] = 3$

Damit sind alle Zwischenkörper von $L|\mathbb{Q}$ gefunden.

Untergruppen von S_3



Zwischenkörper von $L|\mathbb{Q}$



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 $G = \text{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$ wird vom **Frobenius-Automorphismus** $\varphi_{\mathbb{F}_{q^n}|\mathbb{F}_q}$ der Erweiterung $\mathbb{F}_{q^n}|\mathbb{F}_q$ erzeugt.
- (iii) Durch $\mathbb{Z}/n\mathbb{Z} \rightarrow G, a + n\mathbb{Z} \mapsto \varphi^a$ ist ein Isomorphismus von Gruppen definiert.

Ergänzung zu Def. (23.1)

$r \in \mathbb{N}$ ist geg. durch $q = p^r \Rightarrow \varphi_{\mathbb{F}_{q^n} | \mathbb{F}_q} = \varphi^r$ bildet
 α auf $\alpha^{p^r} = \alpha^q$ ab

Beweis von Satz 23.2

zu i) bekannt: $\mathbb{F}_{q^n}$ ist Zerf.-körper von $f = x^q - x$ über $\mathbb{F}_p$
und damit auch über $\mathbb{F}_q \Rightarrow \mathbb{F}_{q^n} | \mathbb{F}_q$ ist eine normale Er-
weiterung. Außerdem ist jede alg. Erw. eines endlichen
Körpers separabel. Insg. ist $\mathbb{F}_{q^n} | \mathbb{F}_q$ also galoissch.

zu ii) Sei $G = \text{Gal}(\mathbb{F}_{q^n} | \mathbb{F}_q)$ z.zg. $G = \langle \varphi_{\mathbb{F}_{q^n} | \mathbb{F}_q} \rangle$

" $\supseteq$ " bekannt: $\mathbb{F}_q$ besteht aus den Nullstellen von $x^q - x$

weiterung. Außerdem ist jede alg. Erw. eines endlichen Körpers separabel. Insg. ist $\mathbb{F}_{q^n} / \mathbb{F}_q$ also galois'sch.

$$\Rightarrow x^q = x \quad \forall x \in \mathbb{F}_q \Rightarrow \varphi_{\mathbb{F}_{q^n} / \mathbb{F}_q} \text{ ist ein } \mathbb{F}_q\text{-Automorphismus}$$

$$\Rightarrow \varphi_{\mathbb{F}_{q^n} / \mathbb{F}_q} \in G \Rightarrow \langle \varphi_{\mathbb{F}_{q^n} / \mathbb{F}_q} \rangle \subseteq G$$

"=" Da $\mathbb{F}_{q^n} / \mathbb{F}_q$ galois'sch ist, gilt $|G| = [\mathbb{F}_{q^n} : \mathbb{F}_q] = n$

$$\text{Sei } m = \text{ord}(\varphi_{\mathbb{F}_{q^n} / \mathbb{F}_q}) \Rightarrow \varphi_{\mathbb{F}_{q^n} / \mathbb{F}_q}^m = \text{id}_{\mathbb{F}_{q^n}} \text{ Sei } x \in \mathbb{F}_{q^n} \text{ mit}$$

$$\mathbb{F}_{q^n} = \mathbb{F}_q(x) \quad \text{Ang. } m < n \quad x^{q^m} = x \Rightarrow x \in \mathbb{F}_{q^m} \Rightarrow$$

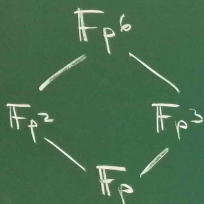
$$\mathbb{F}_q(x) \subseteq \mathbb{F}_{q^m} \Rightarrow \mathbb{F}_{q^n} \subseteq \mathbb{F}_{q^m} \quad \text{da } m < n$$

$$\text{also: } n = \text{ord}(\varphi_{\mathbb{F}_{q^n} / \mathbb{F}_q}) \Rightarrow |\langle \varphi_{\mathbb{F}_{q^n} / \mathbb{F}_q} \rangle| = n = |G| \Rightarrow$$

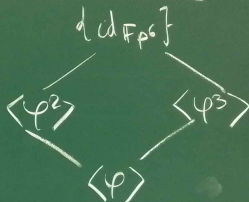
$$G = \langle \varphi_{\mathbb{F}_{q^n} / \mathbb{F}_q} \rangle$$

zuletzt z.zg.: $\exists$ Isom. $\mathbb{Z}/n\mathbb{Z} \rightarrow G, a+n\mathbb{Z} \mapsto \varphi_{\mathbb{F}_{q^n} / \mathbb{F}_q}^a$
Da G zyklisch von Ordnung n und $\varphi_{\mathbb{F}_{q^n} / \mathbb{F}_q}$ ein Element der Ordnung n ist, folgt die Existenz aus Prop 4.12. $\square$

Zwischenkörper von $\mathbb{F}_{p^6} | \mathbb{F}_p$ (p Primzahl)

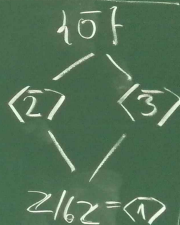


Unterg. der
Galoisgr.



wobei $\varphi = \text{Frob}_{\mathbb{F}_{p^6} | \mathbb{F}_p}$

Unterg.
von $\mathbb{Z}/6\mathbb{Z}$



zu
v
Da
ge
gt
lie
und
ist
 $\sigma_i =$
 φ_n^r
 (S_n^n)

Satz (23.3)

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

- (i) Für jedes $a \in \mathbb{Z}$ mit $\text{ggT}(a, n) = 1$ gibt es ein eindeutig bestimmtes Element $\sigma_a \in G$ definiert durch $\sigma_a(\zeta_n) = \zeta_n^a$.
- (ii) Es gibt einen Gruppenisomorphismus $\phi_n : (\mathbb{Z}/n\mathbb{Z})^\times \rightarrow G$ mit $\phi_n(a + n\mathbb{Z}) = \sigma_a$ für alle $a \in \mathbb{Z}$ mit $\text{ggT}(a, n) = 1$.

Beweis von Satz 23.2

geg: $n \in \mathbb{N}$, $n \geq 2$, $\zeta_n = e^{2\pi i/n}$, $G = \text{Gal}(\mathbb{Q}(\zeta_n) | \mathbb{Q})$
(Es ist $|G| = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \text{grad } \Phi_n = \varphi(n)$.)

zuli) geg. $a \in \mathbb{Z}$ mit $\text{ggT}(a, n) = 1$ $\uparrow$ Kreisteilungs-
polynom

z.zg: Es gibt ein eindeutiges $\sigma_a \in G$ mit $\sigma_a(\zeta_n) = \zeta_n^a$.

Die Eindeutigkeit ist klar, da $\mathbb{Q}(\zeta_n) | \mathbb{Q}$ von ζ_n erzeugt wird.

zur Existenz: $\text{ord}(\zeta_n) = n$ in $\mathbb{C}^\times$, $\text{ggT}(a, n) = 1 \Rightarrow$

$\text{ord}(\zeta_n^a) = n \Rightarrow \zeta_n^a$ ist prim. n -te Einheitswurzel

$\Rightarrow \zeta_n^a$ ist Nullst. von Φ_n

ζ_n, ζ_n^a sind beides Nullst. von Φ_n , Φ_n ist irred. in

$\mathbb{Q}[x]$ $\xRightarrow{\text{Fortsetzungssatz}} \exists \mathbb{Q}$ -Hom $\sigma_a: \mathbb{Q}(\zeta_n) \rightarrow \mathbb{C}$

mit $\sigma_a(\zeta_n) = \zeta_n^a$ Da $\mathbb{Q}(\zeta_n) | \mathbb{Q}$ normal ist, liegt

Abg. 101

2/6Z

101

7 < 3

7

2/6Z = < 1

σ_a in $\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(S_n))$, also in G

zu ii) z.zeg. Es gibt einen Isom. $\phi: (\mathbb{Z}/n\mathbb{Z})^* \rightarrow G$
mit $\phi(a+n\mathbb{Z}) \stackrel{101}{=} \sigma_a \forall a \in \mathbb{Z}$ mit $\text{ggT}(a, n) = 1$

Definiere ϕ durch $\phi(a+n\mathbb{Z}) = \sigma_a$ für $0 \leq a < n$ und
 $\text{ggT}(a, n) = 1$. Überprüfe, dass (*) für alle $a \in \mathbb{Z}$ mit
 $\text{ggT}(a, n) = 1$ gilt. Ist ein solches a vorgeg., dann
liefert Division mit Rest $q, r \in \mathbb{Z}$ mit $a = qn + r$
und $0 \leq r < n$ bzw. $\text{ggT}(r, n) = 1$. Nach Def.

ist $\phi(a+n\mathbb{Z}) = \phi(r+n\mathbb{Z}) = \sigma_r$. z.zeg:

$\sigma_r = \sigma_a$, genügt: $\sigma_r(S_n) = \sigma_a(S_n)$, gleichbed.:

$S_n^r = S_n^a$ Tatsächlich gilt $S_n^a = S_n^{qn+r} =$

$(S_n^n)^q S_n^r = 1^q S_n^r = S_n^r$

$\sigma_r = \partial_a$, genügt: $\partial_r(S_n) = \partial_a(S_n)$, gleichbed.:

Hom-Eigenschaft: Seien $a, b \in \mathbb{Z}$ mit $\text{ggT}(a, n) = \text{ggT}(b, n) = 1$. z.zg. $\phi((a+n\mathbb{Z}) \cdot (b+n\mathbb{Z})) = \phi(a+n\mathbb{Z}) \cdot \phi(b+n\mathbb{Z})$, gleichbed. $\partial_{ab} = \partial_a \circ \partial_b$, genügt:

$$\partial_{ab}(S_n) = (\partial_a \circ \partial_b)(S_n) \quad \text{Es gilt tatsächlich}$$
$$(\partial_a \circ \partial_b)(S_n) = \partial_a(S_n^b) = \partial_a(S_n)^b = (S_n^a)^b = S_n^{ab} = \partial_{ab}(S_n)$$

bleibt z.zg. ϕ ist bijektiv. Es gilt $|\mathbb{Z}/n\mathbb{Z}^\times| = \varphi(n) = |\mathcal{G}|$. Es genügt also z.zg., dass ϕ injektiv ist.

Sei $a \in \mathbb{Z}$ mit $\text{ggT}(a, n) = 1$ und $\phi(a+n\mathbb{Z}) = \text{id}_{\mathcal{Q}(S_n)}$

$$\Rightarrow \partial_a = \text{id}_{\mathcal{Q}(S_n)} \Rightarrow S_n^a = \partial_a(S_n) = \text{id}_{\mathcal{Q}(S_n)}(S_n) = S_n$$

$$\Rightarrow S_n^{a-1} = 1 \quad \text{und } S_n = 1 \quad n \mid (a-1) \Rightarrow a \equiv 1 \pmod{n}$$

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

www.arxiv.org



Beispiel: Die Galois-Erweiterung $\mathbb{Q}(\zeta_8)/\mathbb{Q}$

$(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}$ adites Kreisteilungspolynom:

$$\Phi_{\mathbb{Z}_8} = x^4 + 1 \quad \text{leicht zu sehen: } \zeta_8 = e^{2\pi i/8} = \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}$$

Satz 23.2 $\Rightarrow G = \text{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})$ ist isomorph zu $(\mathbb{Z}/8\mathbb{Z})^\times$

Die Gruppe $(\mathbb{Z}/8\mathbb{Z})^\times$ hat außer $\{1\}$ und $(\mathbb{Z}/8\mathbb{Z})^\times$ die Untergruppen $\langle 3 \rangle$, $\langle 5 \rangle$, $\langle 7 \rangle$. Hauptsatz der Galoistheorie $\Rightarrow \mathbb{Q}(\zeta_8)/\mathbb{Q}$

hat genau drei echte Zwischenkörper. $\zeta_8^2 = i \Rightarrow$ Einer davon

ist $\mathbb{Q}(i)$. $\zeta_8 \bar{\zeta}_8 = |\zeta_8|^2 = 1 \Rightarrow \bar{\zeta}_8 = \zeta_8^{-1} = \zeta_8^7$

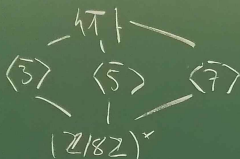
$$\zeta_8 + \zeta_8^{-1} = \zeta_8 + \bar{\zeta}_8 = \left(\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right) + \left(\frac{1}{\sqrt{2}} - \frac{i}{\sqrt{2}}\right) = \frac{2}{\sqrt{2}} = \sqrt{2}$$

$\Rightarrow \mathbb{Q}(\sqrt{2})$ ist echter Zwischenkörper der Erw., $\mathbb{Q}(\sqrt{2})$ ist ein weiterer, wegen $\sqrt{-2} = i\sqrt{2}$.

$(-16\mathbb{Z})$... Restteilungsgradpolynom:

$$\Phi_8 = x^4 + 1 \text{ leicht zu sehen } \zeta_8 = e^{2\pi i/8} = \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}$$

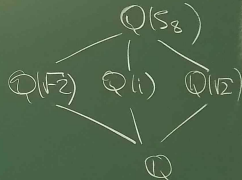
Untergruppen von
 $(\mathbb{Z}/8\mathbb{Z})^\times$



Untergruppen
von $G = \text{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})$



Zwischenkörper
von $\mathbb{Q}(\zeta_8)/\mathbb{Q}$



$$\zeta_8^2 = i \mapsto \zeta_8^{10} = \zeta_8^2 = i$$

$$\begin{aligned} \sqrt{-2} &= \zeta_8 - \bar{\zeta}_8 = \zeta_8 - \zeta_8^7 \xrightarrow{\sigma_3} \zeta_8^3 - \zeta_8^{21} \\ &= \zeta_8^3 - \zeta_8^5 = \zeta_8 - \zeta_8^7 = \sqrt{-2} \\ &\quad \uparrow \zeta_8 \text{ Nullst. von } x^4 + 1 \end{aligned}$$