§ Galoistheorie

Definition 4.1 Eine normale und separable Körpererweiterung L/K heißt GALOISERWEITERUNG. Die GALOISGRUPPE der Galoiserw. L/K ist $\mathrm{Gal}(L/K) = \mathrm{Aut}_K(L)$.

Bemerkungen: a) Galoiserweiterungen sind, wie jede normale Erw. algebraisch.

b) Ist L/K normal so gilt $|\mathrm{Aut}_K(L)| = |\mathrm{Hom}_K(L,\bar{K})| = [L:K]_s \leq [L:K]$ und $[L:K]_s = [L:K]$, wenn L/K separabel.
$\Rightarrow$ ist L/K Galois $\Rightarrow |\mathrm{Gal}(L/K)| = [L:K]$.

c) ist L/K endlich, $L = K(a_1,\dots,a_n)$ und $\sigma \in \mathrm{Aut}_K(L)$. ist f_i das minimalpolynom von a_i so ist $\sigma(a_i)$ wieder eine Nullstelle von f_i d.h. σ permutiert die Nullstellen aller f_i.

Beispiele 4.2 a) p prim, $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$ ist Galois mit $|\mathrm{Gal}(\mathbb{Q}(\sqrt{p})/\mathbb{Q})| = 2$ und daher $\mathrm{Gal}(\mathbb{Q}(\sqrt{p})/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$. Ein erzeuger σ ist gegeben durch $\sigma(\sqrt{p}) = -\sqrt{p}$ (minimalpolynom ist X^2-p).

b) sei $f = (X^2-2)(X^2-3) \in \mathbb{Z}[X]$. Dann ist $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ zerfällungskörper von f, also normal. $\mathrm{char}(\mathbb{Q}) = 0 \Rightarrow \mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ auch separabel und daher Galois und $|\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})| = 4$.
Für $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3}))$ gilt, dass σ die Nullstellen von X^2-2 und X^2-3 permutiert. Die möglichkeiten sind also $\begin{cases}\sqrt{2} \mapsto \pm\sqrt{2} \\ \sqrt{3} \mapsto \pm\sqrt{3}\end{cases}$

und man sieht dass es einen Gruppenhom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$ gibt, welcher injektiv und somit eine Bijektion ist.

c) sei $f = X^3-2 \in \mathbb{Z}[X]$. f ist irreduzibel nach Eisenstein.
sei $\sqrt[3]{2} \in \mathbb{R}$ und ω eine NS von X^2+X+1 in $\mathbb{C}$ (d.h. eine nicht reelle NS von $X^3-1 = (X-1)(X^2+X+1)$).
Dann ist $L = \mathbb{Q}(\sqrt[3]{2},\omega)$ ein Zerfällungskörper von f.
(NS von f sind $\omega^i \cdot \sqrt[3]{2}$ für $i = 0,1,2$)

da $\sigma \in Gal(L/\mathbb{Q})$ die Nullstellen von f permutiert, und die NS von f die Menge $\{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\}$ ist, können wir $Gal(L/\mathbb{Q})$ als Untergruppe von S_3 auffassen. (bijektionen der Menge $\{1,2,3\}$)

wir haben $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq L$ und $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 3$, $[L:\mathbb{Q}(\sqrt[3]{2})] = 2$

also gilt $[L:\mathbb{Q}] = 6$. es folgt, dass $|Gal(L/\mathbb{Q})| = 6 = |S_3|$ und somit (da $Gal(L/\mathbb{Q}) \subseteq S_3$) dass $Gal(L/\mathbb{Q}) = S_3$.

wir bemerken, dass $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ nicht normal, also nicht Galois ist. außerdem $Aut_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2})) = \{id\}$ (via σA) während $|[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]| = 3$.

d) p prim $r, n \in \mathbb{N}_{\geq 1}$, $q = p^r$, $q' = p^{rn}$. Wir haben dann

$\mathbb{F}_{q'}/\mathbb{F}_q$: dies ist normal (Zerfällungskörper von $X^{q'} - X$) und separabel (endl. Körper wie $\mathbb{F}_q$ sind perfekt). Daher gilt

$[\mathbb{F}_{q'}:\mathbb{F}_q] = |Gal(\mathbb{F}_{q'}/\mathbb{F}_q)|$

Betrachte den r-fachen Frobenius $\varphi^r : \mathbb{F}_{q'} \to \mathbb{F}_{q'}$, $\varphi^r(x) = x^{p^r} = x^q$

es gilt $\varphi^r|_{\mathbb{F}_q} = id$, denn $\mathbb{F}_q$ = NS von $X^q - X$ in $\overline{\mathbb{F}_p}$

wir bekommen eine Abbildung $\mathbb{Z} \xrightarrow{k \mapsto \varphi^{rk}} Gal(\mathbb{F}_{q'}/\mathbb{F}_q)$

Beh: kern dieses Homom. ist genau $n\mathbb{Z} \subseteq \mathbb{Z}$:

wegen $|Gal(\mathbb{F}_{q'}/\mathbb{F}_q)| = n$ ist der kern erzeugt von einem Teiler k von n.

also hat man $\varphi^{rk}(x) = x$ $\forall x \in \mathbb{F}_{q'}$. es folgt, dass alle $a \in \mathbb{F}_{q'}$ NS des Polynoms $X^{p^{rk}} - X$ sind. Da $|\mathbb{F}_{q'}| = q' = p^{rn}$ gilt also $p^{rn} \leq p^{rk} = grad(X^{p^{rk}} - X)$ und somit $n \leq k$. Daher $n = k$.

Es folgt, dass $\mathbb{Z}/n\mathbb{Z} \xrightarrow{k \mapsto \varphi^{rk}} Gal(\mathbb{F}_{q'}/\mathbb{F}_q)$ ein Isomorphismus ist.

Gegeben nun eine Galoiserweiterung L/K mit Galoisgruppe $Gal(L/K)$.

Lemma 4.3 Sei $K \subseteq E \subseteq L$ ein Zwischenkörper, L/K Galois.

a) L/E ist Galois und $Gal(L/E) \subseteq Gal(L/K)$ ist eine Untergruppe

b) ist E/K Galois, so ist $Gal(L/K) \to Gal(E/K)$, $\varphi \mapsto \varphi|_E$ ein surjektiver Gruppenhomom.

Bemerkung: 1) Sei K ein Körper, $f \in K[X]$ ein Polynom, $L(f)/K$ ein Zerfällungskörper von f über K, und $\{\alpha_1, \dots, \alpha_n\}$ die Menge der Nullstellen von f in $L(f) = L$ ($\alpha_i \neq \alpha_j$ für $i \neq j$).

Dann definiert die Zuordnung

$$\begin{array}{ccc} \mathrm{Aut}_K(L) & \longrightarrow & \mathrm{Bijektionen}(\{\alpha_1, \dots, \alpha_n\}) \cong S_n \\ \sigma & \longmapsto & \sigma|_{\{\alpha_1, \dots, \alpha_n\}} \end{array}$$

einen wohldefinierten und injektiven Gruppenhomomorphismus:

- Wohldefiniert: es genügt zu sehen, dass σ zu einer Abbildung $\{\alpha_1, \dots, \alpha_n\} \xrightarrow{*} \{\alpha_1, \dots, \alpha_n\}$ einschränkt, diese ist dann bijektiv mit Inverser induziert von $\sigma^{-1} \in \mathrm{Aut}_K(L)$. Dass σ zu $*$ einschränkt folgt, da $\sigma(\alpha_i)$ eine Nullstelle von $\sigma(f) = f$ ist.
- Gruppenhom: ist offenbar (in beiden Fällen ist die Gruppenstruktur durch Komposition von Abbildungen gegeben)
- injektiv: angenommen $\sigma|_{\{\alpha_1, \dots, \alpha_n\}} = \sigma'|_{\{\alpha_1, \dots, \alpha_n\}}$. Dann folgt $\sigma = \sigma'$ denn $\{\alpha_1, \dots, \alpha_n\} \subseteq L(f)$ erzeugt $L(f)$ als Ring (nach Definition von Zerfällungskörpern.

2) Ist f zusätzlich irreduzibel, so ist die induzierte Wirkung von $\mathrm{Aut}_K(L(f))$ auf $\{\alpha_1, \dots, \alpha_n\}$ transitiv: Seien $\alpha_i, \alpha_j \in \{\alpha_1, \dots, \alpha_n\}$. Dann haben wir $K(\alpha_i) \cong K[X]/(f) \cong K(\alpha_j)$ (da f das Minimalpolynom von allen seiner Nullstellen ist). Betrachte dann

$$\begin{array}{ccccc} K(\alpha_i) & \xrightarrow{\cong} & K(\alpha_j) & \subseteq & L \\ \| & & & & \\ L & - - - & - - - & \xrightarrow{\exists \varphi} & \end{array} \quad : \exists \varphi \in \mathrm{Hom}_K(L)$$

welches den Isomorphismus φ erweitert. Per Konstruktion ist $\varphi(\alpha_i) = \alpha_j$ und somit $\varphi(\alpha_i) = \alpha_j$. Da L/K normal ist φ ein Isomorphismus und somit $\varphi \in \mathrm{Aut}_K(L)$ und $\varphi(\alpha_i) = \alpha_j$.

Die Wirkung von $\mathrm{Aut}_K(L)$ auf $\{\alpha_1, \dots, \alpha_n\}$ ist daher transitiv.

Lemma 4.3

Beweis: a) ist L/K normal, so auch L/E normal (ist z.B. L Zerfällungskörper von $\{f_i\}_{i\in I}$ mit $f_i \in K[X]$, so auch von $\{f_i\}_{i\in I}$ mit $f_i \in E[X]$).

Ist L/K separabel, so auch L/E (3.35) und man hat:

$$\mathrm{Gal}(L/E) = \mathrm{Aut}_E(L) \subseteq \mathrm{Aut}_K(L) = \mathrm{Gal}(L/K)$$

(Untergruppe)

b) die Abbildung $\mathrm{Aut}_K(L) \to \mathrm{Aut}_K(E)$, $\varphi \mapsto \varphi|_E$ ist wohldefiniert und Gruppenhom.

Zu zeigen ist hier nur, dass $\varphi|_E$ ein K-Homomorphismus von E definiert; wir haben $\varphi|_E : E \to L \to \bar{L}$ ist K-Homomorphismus. Nach 3.23 c) und der Voraussetzung, dass E/K normal ist, folgt $\varphi|_E(E) = E$.

nun zur Surjektivität. Sei $\varphi : E \to E$ K-Automorphismus. Betrachte

$$\begin{array}{ccc} E & \xrightarrow{\varphi} & E \to \bar{L} \\ \downarrow & & \\ L & & \end{array}$$

Dies hat nach 3.19 a) eine Erweiterung zu einem E-Hom. $L \xrightarrow{\bar{\varphi}} \bar{L}$. da L/K normal folgt $\bar{\varphi}(L) = L$ und $\bar{\varphi} \in \mathrm{Aut}_K(L)$ mit $\bar{\varphi}|_E = \varphi$. □

Bemerkung: Ist L/K Galois und $K \subseteq E \subseteq L$, so ist nicht notwendigerweise E/K Galois (siehe Bsp 4.2 c)): es ist E/K zwar separabel (3.35) aber nicht notwendigerweise normal.

Ist L/K und E/K Galois, so ist der Kern der Surjektion $\mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(E/K)$ gegeben durch die $\varphi \in \mathrm{Gal}(L/K)$ mit $\varphi|_E = \mathrm{id}$, d.h. genau durch die Untergruppe $\mathrm{Gal}(L/E)$

Lemma 4.4 Sei L ein Körper, $G \subseteq \mathrm{Aut}(L)$ eine Untergruppe. Sei

$$K = L^G = \{a \in L \mid \forall g \in G : g(a) = a\}.$$

Dann ist $K \subseteq L$ ein Unterkörper.

Außerdem gelten

a) ist G endlich, so ist L/K Galois mit $\mathrm{Gal}(L/K) = G$

b) ist G unendlich, so ist L/K Galois falls L/K algebraisch ist und $G \subsetneq \mathrm{Gal}(L/K)$ ist eine Untergruppe.

Beweis: Sind $a,b \in K$ und $\sigma \in G$, so gilt $\sigma(a+b) = \sigma(a) + \sigma(b) = a+b$ und analog $\sigma(ab) = ab$, $\sigma(a^{-1}) = a^{-1} \Rightarrow K \subseteq L$ Unterkörper.

Sei nun $\alpha \in L$. Dann ist die Menge $\{\sigma(\alpha)\}_{\sigma \in G}$ endlich: (klar falls G endlich) α ist NS seines minimalpolynoms q_α (falls $|G| = \infty$ ist L/K algebraisch angenommen) und damit auch $\sigma(\alpha)$ NS, es gibt aber nur endlich viele NS von q_α.

Sei $\{\sigma_1, \dots, \sigma_n\}$ eine max. Teilmenge von G, sodass $\{\sigma_i(\alpha)\}_{i=1,\dots,n} \neq \{\sigma(\alpha)\}_{\sigma \in G}$

betrachte $f_\alpha = \prod_{i=1}^{n} X - \sigma_i(\alpha)$. Dann ist für alle $\sigma \in G$ $\sigma(f) = f$ und somit $f \in K[X]$. Dann ist f separabel, α NS von f und daher L/K separabel. Außerdem ist L Zerfällungskörper der Polynome f_α und daher normal. $\Rightarrow$ L/K ist Galois. Per Konstruktion bildet $G \subseteq \mathrm{Aut}(L)$ aus solchen Automorphismen, die K fixieren $\Rightarrow$ $G \leq \mathrm{Aut}_K(L) = \mathrm{Gal}(L/K)$.

es verbleibt zu zeigen, dass $G = \mathrm{Gal}(L/K)$ falls G endlich ist.

Da aus $G \leq \mathrm{Gal}(L/K)$ und $|\mathrm{Gal}(L/K)| = [L:K]$ folgt, dass es genügt zu zeigen dass $[L:K] \leq |G|$, selbst, dass für jede endliche Teilerweiterung $K \subseteq E \subseteq L$ gilt, dass $[E:K] \leq |G|$.

E/K endl. ist separabel und endlich, also gibt es nach dem Satz vom primitiven Element (3.37) ein $\alpha \in E$ sodass $E = K(\alpha)$.

da α NS von f_α wie oben folgt $q_\alpha \mid f_\alpha$ (q_α das minimalpolynom) und daher $[E:K] = \mathrm{grad}(q_\alpha) \leq \mathrm{grad}(f_\alpha) \leq |G|$ ∎

Lemma 4.5 Sei L/K normal und $G = \mathrm{Aut}_K(L)$

a) $K \subseteq L^G \subseteq L$, L/L^G ist Galois und $\mathrm{Gal}(L/L^G) = G$

b) ist L/K separabel, so ist $K = L^G$.

Beweis a) offenbar ist $K \subseteq L^G$. L/L^G ist algebraisch und somit nach 4.4 Galois, außerdem $G \leq \mathrm{Gal}(L/L^G)$. Wegen $K \subseteq L^G$ ist $\mathrm{Aut}_{L^G}(L) \leq \mathrm{Aut}_K(L) = G$.

also $\mathrm{Gal}(L/L^G) \leq G$.

b) da L/K sep $\Rightarrow$ L^G/K separabel, daher $[L^G:K]_s = [L^G:K]$. (wähle $K \subseteq L^G \subseteq L \subseteq \bar{K}$) Wir zeigen, dass $[L^G:K]_s = |\mathrm{Hom}_K(L^G, \bar{K})|$. Sei $\tau: L^G \to \bar{K}$ K-Hom. nach 3.19 a) $\exists$ erweiterung zu $\bar{\tau}: L \to \bar{K}$ (L/L^G alg.). Da L normal/K faktorisiert $\bar{\tau}$ über $L \subseteq \bar{K}$

und definiert ein Element von $\mathrm{Aut}_K(L) = G$. Nach Def. von L^G gilt also $\bar{\tau}|_{L^G} = \mathrm{id}|_{L^G}$ und somit τ = kanonische Abbildung.
$\Rightarrow \mathrm{Hom}_K(L^G, \bar{K}) = \{\text{kan. Inklusion}\}$ und somit $[L^G : K]_s = 1$ ✓

Sei nun L/K Galoiserweiterung mit Galoisgruppe $\mathrm{Gal}(L/K)$.
Ist $K \subseteq E \subseteq L$ ein Zwischenkörper, so ist nach 4.3 a) L/E Galois und $\mathrm{Gal}(L/E) \subseteq \mathrm{Gal}(L/K)$ eine Untergruppe. Betrachte nun:

$$\left\{\begin{array}{l}\text{Zwischenkörper } E \\ \text{von } L/K\end{array}\right\} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \left\{\begin{array}{l}\text{Untergruppen } H \\ \text{von } \mathrm{Gal}(L/K)\end{array}\right\}$$

$$E \longmapsto \mathrm{Gal}(L/E)$$
$$L^H \longleftarrow H$$

Satz 4.6 (Galoiskorrespondenz) Sei L/K Galoiserweiterung. Φ und Ψ sind inklusionsumkehrende Abbildungen. $\Psi \circ \Phi = \mathrm{id}$, $\Phi \circ \Psi = \mathrm{id}$ falls L/K endlich ✓
Des weiteren ist L^H/K normal $\Leftrightarrow H \trianglelefteq \mathrm{Gal}(L/E)$ Normalteiler. Gilt dies, so ist H der Kern der Surjektion $\mathrm{Gal}(L/K) \to \mathrm{Gal}(L^H/K)$.

Beweis: Für $H \subseteq H' \subseteq \mathrm{Gal}(L/K)$ gilt offenbar $L^{H'} \subseteq L^H$. Umgekehrt gilt für $K \subseteq E \subseteq E' \subseteq L$, dass $\mathrm{Gal}(L/E') \subseteq \mathrm{Gal}(L/E)$. Φ und Ψ sind also inklusionsumkehrend.
Sei nun $K \subseteq E \subseteq L$. Dann ist $\Psi(\Phi(E)) = L^{\mathrm{Gal}(L/E)}$. Da $\mathrm{Gal}(L/E) = \mathrm{Aut}_E(L)$ und L/E Galois folgt mit 4.5 b), dass $L^{\mathrm{Gal}(L/E)} = E$, somit $\Psi \circ \Phi = \mathrm{id}$.
Für $H \subseteq \mathrm{Gal}(L/K)$ gilt $\Phi(\Psi(H)) = \mathrm{Gal}(L/L^H)$. Da $\mathrm{Gal}(L/K)$ endlich ist auch H endlich. 4.4 a) sagt, dass $\mathrm{Gal}(L/L^H) = H$.
Ist L^H/K normal, so ist $\mathrm{Gal}(L/L^H) = \ker(\mathrm{Gal}(L/K) \to \mathrm{Gal}(L^H/K))$ also eine normale UG von $\mathrm{Gal}(L/K)$ (siehe Bem. vor Lemma 4.4)
Sei nun $H \trianglelefteq \mathrm{Gal}(L/K)$ Normalteiler. Zz: L^H/K ist normal
Sei $\sigma : L^H \to \bar{L}$ ein K-Hom. nach 3.23 c) genügt es zz, dass $\sigma(L^H) = L^H$.
nach 3.19 a) $\exists$ K-hom. $\bar{\sigma} : L \to \bar{L}$ mit $\bar{\sigma}|_{L^H} = \sigma$. Da L/K normal gilt

$\bar{\sigma}(L) = L$ und $\bar{\sigma} \in \mathrm{Aut}_K(L) = \mathrm{Gal}(L/K)$. mit anderen Worten:
σ ist die Komposition $L^H \subseteq L \xrightarrow{\bar{\sigma}} L$.

zz: $\bar{\sigma}(L^H) = L^H$. da $\bar{\sigma}$ invertierbar (klar) genügt es zz $\bar{\sigma}(L^H) \subseteq L^H$ für alle $\bar{\sigma} \in \mathrm{Gal}(L/K)$. sei also $\tau \in H$, $x \in L^H$. zz dann gilt:
$\tau(\bar{\sigma}(x)) = \bar{\sigma}(\tau'(x)) = \bar{\sigma}(x)$ für $\tau' \in H$ (da $H \subseteq \mathrm{Gal}(L/K)$ normal)
also $\bar{\sigma}(L^H) \subseteq L^H$.

Bemerkung: Ist L/K Galois, so gilt $L = \bigcup_{\substack{K \subseteq L' \subseteq L \\ L'/K \text{ Galois} \\ \text{und endlich}}} L'$, denn:

jedes Element lebt in einer endlichen Erweiterung E/K. für diese gibt es nach 3.25 c) einen normalen Abschluss L'/K, $K \subseteq E \subseteq L'$. und L'/K ist wieder endlich, normal, und als Teilerweiterung von L separabel. Also ist jedes Element in einer endl. Galoiserw. enthalten.

Sei L'/K nun eine endl. Teil-Galoiserweiterung ($K \subseteq L' \subseteq L$) L/K endl. Galois. Dann definiert $\mathrm{Aut}_K(L) \xrightarrow{\sigma \mapsto \sigma|_{L'}} \mathrm{Hom}_K(L', L)$ eine wohldefinierte Abb.

$\exists$ da L' normal/K. $\to \mathrm{Hom}_K(L', L')$

$\mathrm{Gal}(L/K) \to \mathrm{Gal}(L'/K)$ (die Surjektion in der Aussage von 4.6)

Wir bekommen also insgesamt einen Gruppenhomom.

$$\mathrm{Gal}(L/K) \longrightarrow \prod_{\substack{L' \subseteq L \\ L'/K \text{ endl.} \\ \text{Galois}}} \mathrm{Gal}(L'/K)$$

dieser ist injektiv ($f: L \to L$ ist durch seine Einschränkung auf alle L' bestimmt). Die Gruppe $\prod_{L'} \mathrm{Gal}(L'/K)$ trägt eine Topologie (die Produkttopologie, wobei $\mathrm{Gal}(L'/K)$ diskret sei). Ist L/K nicht endlich, so ist die Topologie auf $\prod \mathrm{Gal}(L'/K)$ nicht diskret.
Als UG von $\prod \mathrm{Gal}(L'/K)$ trägt $\mathrm{Gal}(L/K)$ dann auch eine Topologie

Die Galoiskorrespondenz im unendlichen Fall sagt dann dass

$$\left\{\begin{array}{c}\text{Zwischenkörper } E \\ \text{von } L/K\end{array}\right\} \quad \overset{1:1}{\longleftrightarrow} \quad \left\{\begin{array}{c}\text{abgeschlossene UG} \\ H \text{ von } \mathrm{Gal}(L/K)\end{array}\right\}$$

$$\begin{array}{ccc} E & \longmapsto & \mathrm{Gal}(L/E) \leq \mathrm{Gal}(L/K) \\ L^H & \longleftarrow & H \end{array}$$

wir werden dies aber nicht in dieser Vorlesung diskutieren.

Bem: Für $H \leq \mathrm{Gal}(L/K)$ UG mit Abschluss $\overline{H}$ gilt $L^H = L^{\overline{H}}$.

Korollar 4.7 Eine endl. separable Erw. L/K hat nur endl. viele Zwischenkörper.

Ist N/K ein normaler Abschluss, so ist N/K Galois ($\Leftrightarrow$: N/K separabel)

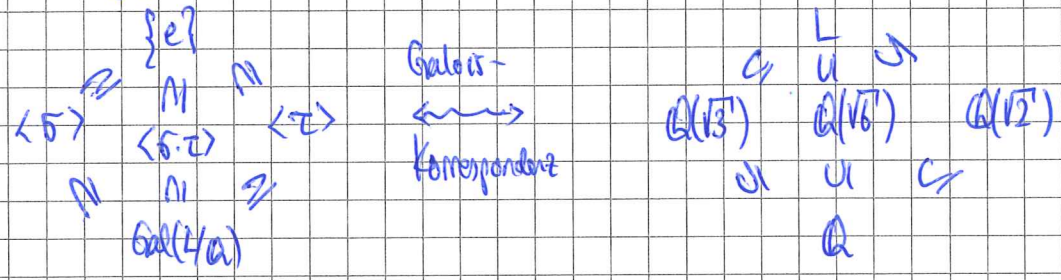
und endlich. $\left\{\begin{array}{c}\text{Zwischenkörper von} \\ L/K\end{array}\right\} \subseteq \left\{\begin{array}{c}\text{Zwischenkörper} \\ \text{von } N/K\end{array}\right\} \overset{1:1}{\longleftrightarrow} \left\{\begin{array}{c}\text{UG von} \\ \mathrm{Gal}(N/K)\end{array}\right\}$

und $\mathrm{Gal}(N/K)$ ist endlich, hat daher auch nur endl. Viele UG.

Beispiele 4.8 a) $L = \mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ ist eine endl. Galoiserweiterung mit $\mathrm{Gal}(L/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

erzeugt von σ, τ $\sigma(\sqrt{2}) = -\sqrt{2}$, $\sigma(\sqrt{3}) = \sqrt{3}$, $\tau(\sqrt{2}) = \sqrt{2}$, $\tau(\sqrt{3}) = -\sqrt{3}$

die Untergruppen von $\mathrm{Gal}(L/\mathbb{Q})$ (mit Inklusionen) sehen also so aus:



Beachte: $\mathrm{Gal}(L/\mathbb{Q})$ abelsch, also $H \leq \mathrm{Gal}(L/\mathbb{Q})$ normalteiler $\Rightarrow L^H/\mathbb{Q}$ normal

Um zu sehen, dass obiges Diagram von Körpererw. korrekt ist, berechnet man, dass $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ ein $\mathbb{Q}$-Basis von L bilden.

b) $L = \mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$ wie in 4.2 b) ist Galois mit $\mathrm{Gal}(L/\mathbb{Q}) = S_3$.

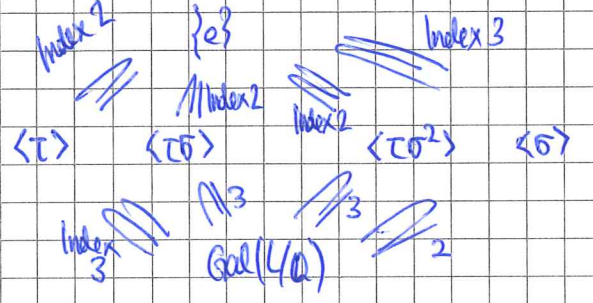
eine $\mathbb{Q}$-basis ist gegeben durch $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2, \omega, \omega\sqrt[3]{2}, \omega(\sqrt[3]{2})^2\}$

die Nullstellen von $X^3 - 2$ sind $\{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\} \cong \{1,2,3\}$

seien $\sigma, \tau \in \mathrm{Gal}(L/\mathbb{Q})$ gegeben durch $\sigma(\sqrt[3]{2}) = \omega\sqrt[3]{2}$, $\sigma(\omega) = \omega$, $\tau(\sqrt[3]{2}) = \sqrt[3]{2}$, $\tau(\omega) = \omega^2$

(unter dem Isomorphismus $\mathrm{Gal}(L/\mathbb{Q}) \cong S_3$ korrespondieren σ und τ zu dem 3-Zykel (123) und der Transposition (23)).

Die Untergruppen von $Gal(L/\mathbb{Q})$ sehen so aus:



und $\langle\sigma\rangle \trianglelefteq Gal(L/\mathbb{Q})$ normal, während $\langle\tau\rangle, \langle\tau\sigma\rangle, \langle\tau\sigma^2\rangle$ nicht normal in $Gal(L/\mathbb{Q})$ sind. Durch betrachten der $\mathbb{Q}$-Basis von L ergeben sich folgende Fixkörper:

- $L^{\langle\tau\rangle} = \mathbb{Q}(\sqrt[3]{2})$ ($\tau(\sqrt[3]{2}) = \sqrt[3]{2}$ und beider Ew. $/\mathbb{Q}$ sind vom grad 3)
- $L^{\langle\tau\sigma\rangle} = \mathbb{Q}(\sqrt[3]{2}\cdot\omega)$
- $L^{\langle\tau\sigma^2\rangle} = \mathbb{Q}(\sqrt[3]{2}\cdot\omega^2)$
- $L^{\langle\sigma\rangle} = \mathbb{Q}(\omega)$

Notation: Ist $f \in K[X]$ ein separables Polynom, $L(f)/K$ ein Zerfällungskörper (separabel, da f separabel), so schreiben wir auch $Gal(f)$ statt $Gal(L(f)/K)$.

Ist $grad(f) = n$, so gilt (Bem. S.59) $Gal(f) \leq S_n$ und somit ist $|Gal(f)| = [L(f):K]$ ein Teiler von $n!$

Auf dem Übungszettel 8 haben wir gesehen, dass $f = X^5 - 4X + 2$ erfüllt, dass $Gal(f) = S_5$. Wir werden später zeigen, dass für alle $n \geq 1$ ein f existiert mit $Gal(f) = S_n$ und auch ein g mit $Gal(g) = A_n$ wobei $A_n = \ker\left(S_n \leq GL_n(\mathbb{Z}) \xrightarrow{det} \mathbb{Z}^\times = \mathbb{Z}/2\right)$

Einheitswurzeln

Def. 4.9 Sei K ein Körper und $\bar{K}$ ein alg. Abschluss von K. Eine n-te Einheitswurzel in K ist eine Nullstelle des Polynoms $X^n - 1 \in K[X]$ in $\bar{K}$.

Wir bezeichnen die Menge dieser n-ten Einheitswurzeln in $\bar{K}$ mit $\mu_n(\bar{K}) \leq \bar{K}^\times$.

Bemerkung: da für $\zeta, \zeta' \in \mu_n(\bar{K})$ gilt, dass $(\zeta\cdot\zeta')^n = \zeta^n\cdot(\zeta')^n = 1$ und $(\zeta^{-1})^n = (\zeta^n)^{-1} = 1$ folgt, dass $\mu_n(\bar{K})$ eine endliche Untergruppe von $(\bar{K})^\times$ ist, und daher nach 3.36 eine zyklische Gruppe ist.

- ~~ist~~ gilt $\mathrm{char}(K) \nmid n$ so haben X^n-1 und $(X^n-1)' = nX^{n-1}$ keine gemeinsamen Nullstellen: ist ζ NS von X^n-1 so ist $\zeta^{n-1} = \zeta^{-1} \neq 0$ und somit ($\mathrm{char}(K)\nmid n$) auch $n\cdot\zeta^{n-1} \neq 0$. in diesem Fall ist also X^n-1 separabel und $|\mu_n(\bar{K})| = n$ also $\mu_n(\bar{K}) \cong \mathbb{Z}/n\mathbb{Z}$.

- gilt $\mathrm{char}(K) = p \mid n$, sagen wir $n = p^r\cdot n'$, $p\nmid n'$ so ist $X^{n'}-1$ nach obigem separabel und wegen $X^n-1 = (X^{n'}-1)^{p^r}$ haben X^n-1 und $X^{n'}-1$ die gleichen Nullstellen in $\bar{K}$. Im folgenden nehmen wir daher immer (ohne große Probleme) an, dass $\mathrm{char}(K)\nmid n$.

Definition 4.10 K Körper, $\overset{n\geq 1}{\mathrm{char}(K)\nmid n}$, Eine n-te Einheitswurzel $\zeta \in \mu_n(\bar{K})$ heißt primitiv, falls sie ein Erzeuger der zyklischen Gruppe $\mu_n(\bar{K}) \cong \mathbb{Z}/n\mathbb{Z}$ ist.

Ist $\zeta \in \mu_n(\bar{K})$ primitiv, so ist $K(\zeta)/K$ Zerfällungskörper von X^n-1 und somit ist $K(\zeta)/K$ eine Galoiserweiterung (X^n-1 separabel).

ÜA: $[m] \in \mathbb{Z}/n\mathbb{Z}$ ist erzeuger $\Leftrightarrow [m] \in (\mathbb{Z}/n\mathbb{Z})^\times \Leftrightarrow \mathrm{ggT}(n,m) = 1$.

Definition 4.11 Die Eulersche φ-Funktion ist: $\varphi: \mathbb{N}_{\geq 0} \to \mathbb{N}$:

$$\varphi(n) = \left|\{m \mid 1\leq m\leq n \mid \mathrm{ggT}(m,n)=1\}\right| \overset{\text{ÜA}}{=} \left|\mathbb{Z}/n\mathbb{Z}\right|^\times.$$

mit anderen Worten, $\varphi(n)$ ist die Anzahl der primitiven n-ten Einheitswurzeln in $\mu_n(\bar{K})$ ($\mathrm{char}(K)\nmid n$).

Sei nun wieder $\mathrm{char}(K)\nmid n$, $\zeta_1, \dots, \zeta_r$ die primitiven n-ten Einheitswurzeln, $r = \varphi(n)$

Definition 4.12 K Körper, $\mathrm{char}(K) \nmid n$. Definiere $\phi_n \in \bar{K}[X]$ durch

$$\phi_n = \prod_{i=1}^{\varphi(n)} (X - \zeta_i) = \prod_{\substack{\zeta \in \mu_n(\bar{K}) \\ \text{primitiv}}} (X - \zeta)$$

Lemma 4.13 $\phi_n \mid (X^n - 1)$ und $\phi_n \in K[X]$.

Beweis: Per Konstruktion gilt $X^n - 1 = \prod_{\zeta \in \mu_n(\bar{K})} (X - \zeta)$, also $\phi_n \mid (X^n - 1)$.

Außerdem gilt offenbar $\phi_n \in K(\zeta)[X]$ für jede primitive Einheitswurzel ζ und $K = K(\zeta)^{\mathrm{Aut}_K(K(\zeta))}$. Sei also $\sigma \in \mathrm{Aut}_K(K(\zeta))$, dann ist $\sigma(\zeta)$ eine primitive n-te Einheitswurzel wenn ζ eine solche ist $\Rightarrow \sigma(\phi_n) = \phi_n$ und somit $\phi_n \in K[X]$. ∎

Bem: später: $\phi_n \in \mathbb{Z}[X]$ und gilt via der Abb. $\mathbb{Z}[X] \to K[X]$ das zu K gehörige ϕ_n.

Lemma 4.14 Sei $n \in \mathbb{N} \setminus \{0\}$

a) ist $m \geq 1$, $\mathrm{ggT}(m,n) = 1$ so gilt $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$

b) ist $n = \prod_{i=1}^{r} p_i^{\nu_i}$ p_i paarw. versch. Primzahlen $\Rightarrow \varphi(n) = \prod_{i=1}^{r} p_i^{\nu_i - 1}(p_i - 1)$

c) $n = \sum_{\substack{d \geq 1 \\ d \mid n}} \varphi(d)$.

Beweis: a) ist $\mathrm{ggT}(m,n) = 1$ so folgt aus dem chinesischen Restsatz $\mathbb{Z}/nm\mathbb{Z} = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$

b) wieder chin. Restsatz: $\mathbb{Z}/n\mathbb{Z} \cong \prod_{i=1}^{r} \mathbb{Z}/p_i^{\nu_i}$; $|(\mathbb{Z}/p^n)^\times| = p^{n-1}(p-1)$

c) Übungsaufgabe.

Beispiele 4.15
- $\varphi(1) = 1$, $\varphi(p) = p - 1$ für p prim
- $\varphi(6) = \varphi(2 \cdot 3) \overset{a)}{=} \varphi(2) \cdot \varphi(3) = 1 \cdot 2 = 2$
- $\varphi(140) = \varphi(2^2 \cdot 5 \cdot 7) \overset{b)}{=} 2 \cdot 4 \cdot 6 = 48$

Beispiele 4.16
- $\phi_1 = X - 1$
- $\phi_2 = X + 1$
- ϕ_4 = produkt von zwei Linearfaktoren ($\varphi(4) = 2$), mit NS primitive 4-Einheitswurzeln also z.B. für $K = \mathbb{C}$ $\phi_4 = (X - i)(X + i) = X^2 + 1$

Lemma 4.17 $X^n - 1 = \prod_{d \mid n} \prod_{\substack{\zeta \in \mu_d(\bar{K}) \\ \text{primitiv}}} (\phi_d X - \zeta) = \prod_{d \mid n} \phi_d$

Beweis: wir haben $X^n - 1 = \prod_{\zeta \in \mu_n(\bar{K})} (X - \zeta)$.

nun gilt: $\mu_n(\bar{K}) = \coprod_{d|n} \{\text{primitive } d\text{-te Einheitswurzel in } \bar{K}\}$

denn eine n-te Einheitswurzel hat eine Ordnung welche ein Teiler von n ist.

also folgt $\prod_{\zeta \in \mu_n(\bar{K})} (X - \zeta) = \prod_{d|n} \prod_{\substack{\zeta' \in \mu_d(\bar{K}) \\ \text{primitiv}}} (X - \zeta') = \prod_{d|n} \Phi_d$ wie behauptet ☐

Korollar 4.18 Für p prim gilt $\Phi_p = X^{p-1} + X^{p-2} + \dots + 1$.

Beweis: nach 4.17 ist $X^p - 1 = \prod_{d|p} \Phi_d = \Phi_1 \cdot \Phi_p$ und $\Phi_1 = (X-1)$ nach 4.16.

daher $\Phi_p = X^{p-1} + \dots + 1$ wie behauptet. ☐

Beispiel 4.19 $\Phi_6 = X^2 - X + 1$. denn

$$X^6 - 1 = \Phi_1 \Phi_2 \Phi_3 \Phi_6 = \underbrace{(X-1)(X+1)(X^2+X+1)}_{} \cdot \Phi_6$$
$$= (X^2-1)(X^2+X+1) \cdot \Phi_6$$
$$= (X^4 + X^3 - X - 1) \cdot \Phi_6$$

und $\Phi_6 = X^2 - X + 1$ erfüllt die Gleichung.

Bem
Sei $n \geq 1$, $\text{char}(K) \nmid n$, $\zeta \in \mu_n(\bar{K})$ primitiv. Dann ist $K(\zeta)/K$ Galois.

Sei f das minimalpolynom von ζ. da $\Phi_n(\zeta) = 0$ folgt dass $f \mid \Phi_n$ und $\text{grad}(f) = d$ ($[K(\zeta):K] = d$) und somit $d \leq \varphi(n) = \text{grad}(\Phi_n)$

es gilt $d = \varphi(n)$ genau dann wenn Φ_n irreduzibel ist. Ob dies so ist hängt vom Körper K ab:

Beispiel 4.20 ähnlich wie in 4.19 sieht man, dass $\Phi_{12} = X^4 - X^2 + 1$

in $\mathbb{F}_{11}$ haben wir aber $(X^2 - 5X + 1)(X^2 + 5X + 1) = X^4 - X^2 + 1$ ☐

Satz 4.21 Sei $n \geq 1$, $\zeta \in \mu_n(\mathbb{Q})$ primitiv. Dann ist Φ_n das minimalpolynom von ζ (also irreduzibel) und $\Phi_n \in \mathbb{Z}[X]$.

Beweis: Sei f das minimalpolynom von ζ. es gilt dass $f \mid (X^n - 1)$, also gibt es $h \in \mathbb{Q}[X]$ mit $f \cdot h = (X^n - 1)$. Folglich ist h normiert, und folglich $f, h \in \mathbb{Z}[X]$ (siehe Bem. nach Gauß Lemma 2.32) Sei p prim mit $\text{ggT}(p, n) = 1$. Dann ist ζ^p wieder eine primitive Einheitswurzel, wir zeigen $f(\zeta^p) = 0$.

angenommen $f(\zeta^p) \neq 0$ da $(\zeta^p)^n - 1 = 0$ folgt, dass $h(\zeta^p) = 0$
folglich ist ζ eine NS von $h(X^p)$. daher gilt $f \mid h(X^p)$
es gibt also $g \in \mathbb{Q}[X]$ mit $f \cdot g = h(X^p)$. wieder folgt, dass g normiert und
dann, dass $g \in \mathbb{Z}[X]$. sei $\pi : \mathbb{Z}[X] \to \mathbb{F}_p[X]$ die von der Projektion induzierte Abb.
dann gilt $\pi(h)^p = \pi(h(X^p)) = \pi(f) \cdot \pi(g)$, außerdem $\pi(h)$ reduktion eines
normierten Polynoms mit NS $\zeta^p \Rightarrow \operatorname{grad}(\pi(h)) > 0$.
wegen $\pi(h)^p = \pi(f) \cdot \pi(g)$ haben $\pi(f)$ und $\pi(h)$ eine gemeinsame Nullstelle
in $\overline{\mathbb{F}_p}$, wegen $X^n - 1 = \pi(f) \cdot \pi(h)$ hat dann $X^n - 1$ eine mehrfache NS
in $\overline{\mathbb{F}_p}$ im Widerspruch zu $\operatorname{char}(k) \nmid n$ ($\Rightarrow X^n - 1$ separabel über $\mathbb{F}_p$).
also gilt $f(\zeta^p) = 0$. Eine allgemeine primitive n-te Einheitswurzel ζ'
ist von der Form ζ^m mit $\operatorname{ggT}(m,n) = 1$.
da $m = p_1^{\nu_1} \cdots p_k^{\nu_k}$ folgt aus obigem Argument induktiv ($\zeta^m = (\zeta^{m'})^{p_k}$)
dass $f(\zeta') = f(\zeta^m) = 0$. es folgt, dass f $\varphi(n)$ viele NS in $\overline{\mathbb{Q}}$ hat,
daher, dass $\operatorname{grad}(f) = \operatorname{grad}(\phi_n) = \varphi(n)$. Da $\phi_n(\zeta) = 0$ folgt
$f \mid \phi_n$ und da f und ϕ_n normiert folgt aus $\operatorname{grad}(f) = \operatorname{grad}(\phi_n)$, dass
$f = \phi_n$.

zz

Korollar 4.22 sei $\zeta \in \mu_n(\overline{\mathbb{Q}})$ primitiv. Dann ist $\mathbb{Q}(\zeta)/\mathbb{Q}$ Galois,
$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$ und $\operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times$.

Beweis: Da $\mathbb{Q}(\zeta)$ Zerfällungskörper von $X^n - 1$ folgt dass $\mathbb{Q}(\zeta)/\mathbb{Q}$ Galois.
aus 4.20 folgt, dass das minimalpolynom von ζ gleich ϕ_n ist, also
gilt $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$. Ist $\zeta' \in \mu_n(\overline{\mathbb{Q}})$ primitiv, so $\exists\, m$, $\operatorname{ggT}(m,n) = 1$
und $\zeta' = \zeta^m$. Für jedes $1 \leq m \leq n$ mit $\operatorname{ggT}(m,n) = 1$ existiert also
$\sigma_m \in \operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ mit $\sigma_m(\zeta) = \zeta^m$ (und umgekehrt ist $\forall \sigma \in \operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$
$\sigma(\zeta)$ eine prim. Einheitswurzel)
Behauptung: die Abbildung

$$\begin{array}{ccc} (\mathbb{Z}/n\mathbb{Z})^\times & \longrightarrow & \operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \\ \downarrow\wr & & \downarrow\wr \\ [m] & \longmapsto & \sigma_m \end{array}$$

ist ein surjektiver Gruppenhomomorphismus:

$\sigma_{mm'}(\zeta) = \zeta^{mm'} = (\zeta^m)^{m'} = \sigma_{m'}(\sigma_m(\zeta))$ und surjektivität folgt aus
da $|\operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})| = |(\mathbb{Z}/n\mathbb{Z})^\times|$ folgt, dass obige Abbildung ein Isom. ist.

zz

Definition 4.23 Eine Galoiserw. L/K heißt ABELSCH, falls $\mathrm{Gal}(L/K)$ eine abelsche Gruppe ist.

Bemerkungen:
- Klassenkörpertheorie studiert abelsche Erweiterungen von sogenannten lokalen und globalen Körpern (wie z.B. endl. Erweiterungen von $\mathbb{Q}$, den Zahlkörpern). Dies studiert man in Vorlesungen zur alg. Zahlentheorie.
- Nach Sätzen von Weber (1886) und Hilbert (1896) ist jede endliche abelsche Erweiterung enthalten in einem Körper der Form $\mathbb{Q}(\zeta)$, $\zeta \in \mu_n(\overline{\mathbb{Q}})^{\text{prim}}$, $n \in \mathbb{N}$ geeign.

Beispiel 4.24 a) Sei ζ_{12} eine primitive 12te Einheitswurzel. Dann ist $\mathbb{Q}(\zeta_{12})/\mathbb{Q}$ Galois mit $\mathrm{Gal}(\mathbb{Q}(\zeta_{12})/\mathbb{Q}) \cong (\mathbb{Z}/12\mathbb{Z})^\times = (\mathbb{Z}/12\mathbb{Z})^\times$ (a wirkt wie folgt $a(\zeta_{12}) = (\zeta_{12})^a$)

$\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ und somit

$5 \mapsto (1,-1)$
$7 \mapsto (-1,1)$ $\mathrm{Gal}(\mathbb{Q}(\zeta_{12})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$11 \mapsto (-1,-1)$

Die 3 nicht-trivialen Zwischenkörper von $\mathbb{Q}(\zeta_{12})/\mathbb{Q}$ sind dann
- $\mathbb{Q}(\zeta_{12}^3 = i)$ (Fixkörper von $[5]$)
- ζ_{12}^4 wird von $[7]$ fixiert, $\zeta_{12}^4 = \frac{-1+\sqrt{-3}}{2}$
- und der Fixkörper von $[7]$ ist $\mathbb{Q}(\sqrt{-3})$

es folgt durch Gradvergleich dass $\mathbb{Q}(i, \sqrt{-3}) = \mathbb{Q}(\zeta_{12})$
und damit auch $i\sqrt{-3} = \sqrt{3} \in \mathbb{Q}(\zeta)$. $\sqrt{3}$ wird von $[11] \in (\mathbb{Z}/12\mathbb{Z})^\times$ fixiert und ist somit der Fixkörper von $[11]$

b) Sei ζ_8 ein primitive 8te Einheitswurzel. Dann ist $\mathbb{Q}(\zeta_8)/\mathbb{Q}$ Galois von grad $\varphi(8) = 4$, $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) = (\mathbb{Z}/8\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
(die Einheiten von $\mathbb{Z}/8\mathbb{Z}$ sind $1,3,5,7$ und $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \bmod 8$, $3 \cdot 7 = 5 \bmod 8$)
ÜA: Beschreibe analog zu oben die Fixkörper.

Radikalerweiterungen

Erinnerung zu allgemeinen Lösungsformeln:

grad 2: ein Polynom X^2+aX+b hat die Lösungen ($a,b \in \mathbb{Q}(R)$)

$$X_{1,2} = -\frac{a}{2} \pm \sqrt{\frac{a^2}{4}-b}$$

grad 3: $X^3+a_1X^2+a_2X+a_3$, $a_i \in R$ hat folgende 3 Nullstellen (Cardano)

zunächst setze $p = a_2 - \frac{a_1^2}{2}$, $q = \frac{2a_1^3}{27} - \frac{a_1a_2}{3} + a_3$, $r = \frac{p^3}{27} + \frac{q^2}{4}$

$P = \sqrt[3]{-\frac{q}{2}+r}$, $Q = \sqrt[3]{-\frac{q}{2}-r}$, $\zeta = e^{\frac{2\pi i}{3}}$

Die 3 Nullstellen sind dann

$$X_1 = P+Q-\frac{a_1}{3}, \quad X_2 = \zeta P + \zeta^2 Q - \frac{a_1}{3}, \quad X_3 = \zeta^2 P + \zeta Q - \frac{a_1}{3}$$

Ein Radikal von $a \in K$ ist eine Nullstelle eines Polynoms $X^n - a \in K[X]$ für ein $n \geq 2$. Wir betrachten Körpererweiterungen L/K welche von Radikalen auf folgende Art erzeugt werden können

Definition 4.25 K Körper, $\mathrm{char}(K)=0$. L/K Körpererweiterung heißt RADIKAL, falls es einen endlichen Turm von Körpererweiterungen gibt

$$K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_n = L$$ sodass gilt, dass $\forall i \geq 0$

$K_{i+1} = K_i(\sqrt[n_i]{a_i})$ für $n_i \geq 1$, $a_i \in K_i$

Bemerkung:
- Radikalerweiterungen sind endlich
- ist $f \in K[X]$, so existiert allg. Lösungsformel für NS von f durch Operationen wie $\cdot, +, -, /, (-)^n, \sqrt[n]{\ }$ genau falls ein Zerfällungskörper von f in einer Radikalerweiterung enthalten ist. ($\Leftrightarrow \exists$ Radikalerw. welche alle NS von f enthält) Ist dies der Fall so sagen wir das Polynom f ist durch RADIKALE LÖSBAR.

Beispiel 4.26
- $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ ist Radikal aber nicht Galois.
- $\mathbb{Q}(\sqrt[3]{2}, i)/\mathbb{Q}$ ist Radikal und Galois.

Lemma 4.27 Ist L/K radikal, so existiert eine Erw. M/L sodass M/K radikal und Galois ist.

Beweis: Induktion über die Länge eines Turms einfacher Radikalerweiterungen: zunächst betrachten wir den Fall $L = K(\sqrt[n]{a})$. Sei $\zeta \in \mu_n(\bar{K})$ primitiv und betrachte $M = L(\zeta) = K(\sqrt[n]{a}, \zeta)$. Dann ist M/K radikal ($K \subseteq L \subseteq M$) und Zerfällungskörper von $X^n - a$, damit Galoisch.

Sei nun $K = K_0 \subseteq \dots \subseteq K_{n-1} \subseteq K_n = L$ wie in der Def. von Radikalerw.

Per Induktion existiert N/K_{n-1} sodass N/K radikal und Galois ist.

sei $L = K_{n-1}(\sqrt[m]{a})$ für $a \in K_{n-1}$. Betrachte das Polynom

$$f = \prod_{\sigma \in \mathrm{Gal}(N/K)} (X^m - \sigma(a)) \in N[X].$$

nach Konstruktion gilt $\forall \sigma \in \mathrm{Gal}(N/K)$ dass $\sigma(f) = f$, also $f \in N^{\mathrm{Gal}(N/K)}[X] = K[X]$

sei M ein Zerfällungskörper von f über N, dann ist M/N Galois und da N/K Galois ist auch M/K Galois. Per Konstruktion ist M/N radikal und damit auch M/K radikal. Des weiteren ist $\sqrt[m]{a}$ eine Nullstelle von f, sodass L als Unterkörper von M aufgefasst werden kann. ☐

Definition 4.28 Eine Gruppe G heißt AUFLÖSBAR falls es einen Turm

$$\{e\} = G_n \trianglelefteq G_{n-1} \trianglelefteq \dots \trianglelefteq G_1 \trianglelefteq G_0 = G \text{ gibt } (G_i \trianglelefteq G_{i-1} \text{ normalteiler})$$

sodass $\forall i$ gilt, dass G_{i-1}/G_i eine abelsche Gruppe ist.

Lemma 4.29 Sei G eine Gruppe, $H \subseteq G$ UG, $N \trianglelefteq G$ Normalteiler.

1) Ist G auflösbar, so sind H und G/N auflösbar
2) Ist N und G/N auflösbar, dann auch G.

Beweis: ÜA.

Satz 4.30 Sei L/K radikal und Galois. Dann ist $\mathrm{Gal}(L/K)$ auflösbar.

Beweis: sei $K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_r = L$ und $K_{i+1} = K_i(\sqrt[n_i]{a_i})$ $a_i \in K_i$

sei $n = \prod_{i=0}^{r-1} n_i$ und $\zeta \in \mu_n(\bar{K})$ primitiv.

Setze für $i = 0, \dots, r$ $K_i' = K_i(\zeta)$. Dann gilt $K_{i+1}' = K_i'(\sqrt[n_i]{a_i})$.

und K_{i+1}'/K_i' ist Galois, denn ein Zerfällungskörper von $X^{n_i}-a_i$ (dessen Nullstellen sind $\sqrt[n_i]{a_i}\cdot(\zeta')^j$ mit ζ' eine primitive n_i-te Einheitswurzel und $\zeta^{s_i} \in K_i'$ ist eine solche, s_i sodass $n = s_i \cdot n_i'$.)

außerdem ist K_i'/K_i Galois (siehe kurz nach Def. 4.16) und insbesondere L'/L Galois und L/K Galois nach Voraussetzung. Daher gilt:

$\mathrm{Gal}(L'/K) \twoheadrightarrow \mathrm{Gal}(L/K)$ (mit Kern $\mathrm{Gal}(L'/L)$) also genügt es noch 4.29 zz, dass $\mathrm{Gal}(L'/K)$ auflösbar ist. Betrachte nun

$K = K_0 \subseteq K_0' \subseteq K_1' \subseteq \dots \subseteq K_r' = L'$ und betrachte

$\mathrm{Gal}(L'/K_i') \leq \mathrm{Gal}(L'/K)$, da es gilt:

$\mathrm{Gal}(L'/K_{i+1}') \subseteq \mathrm{Gal}(L'/K_i')$ und stimmt überein mit dem Kern der Surjektion $\mathrm{Gal}(L'/K_i') \twoheadrightarrow \mathrm{Gal}(K_{i+1}'/K_i')$, denn K_{i+1}'/K_i' ist Galois.

es gilt also $\mathrm{Gal}(L'/K_{i+1}') \trianglelefteq \mathrm{Gal}(L'/K_i')$ und auch

$\mathrm{Gal}(L'/K_0') \trianglelefteq \mathrm{Gal}(L'/K)$ (wieder der Kern der Surj. $\mathrm{Gal}(L'/K) \twoheadrightarrow \mathrm{Gal}(K_0'/K)$).

Wir bekommen

$\{e\} = \mathrm{Gal}(L'/K_r') \trianglelefteq \mathrm{Gal}(L'/K_{r-1}') \trianglelefteq \dots \trianglelefteq \mathrm{Gal}(L'/K_0') \trianglelefteq \mathrm{Gal}(L'/K)$

genügt nun

es zu zeigen dass $\forall i$ $\mathrm{Gal}(K_{i+1}'/K_i')$ und $\mathrm{Gal}(K_0'/K)$ abelsch sind.

Wegen K_{i+1}' = Zerfällungskörper von $X^{n_i}-a_i$ dessen NS $\{\sqrt[n_i]{a_i}\cdot(\zeta^{s_i})^j\}_{j=1,\dots,n_i}$ sind gilt für $\sigma \in \mathrm{Gal}(K_{i+1}'/K_i') \leq S_{n_i}$, dass $\sigma(\zeta^{s_i}) = \zeta^{f_i}$ und

$\sigma(\sqrt[n_i]{a_i}\cdot(\zeta^{s_i})) = \sqrt[n_i]{a_i}\cdot(\zeta^{s_i})^j$ für ein! $j \in \mathbb{Z}/n_i\mathbb{Z}$

$\Rightarrow \mathrm{Gal}(K_{i+1}'/K_i') \leq \mathbb{Z}/n_i\mathbb{Z}$ und somit abelsch als UG einer ab. Gruppe.

Analog ist $\mathrm{Gal}(K_0'/K) = \mathrm{Gal}(K(\zeta)/K)$ eine UG von $\mathbb{Z}/n\mathbb{Z}$

(für $\sigma \in \mathrm{Gal}(K(\zeta)/K)$ ist $\sigma(\zeta) = \zeta^j$ für ein $j \in \mathbb{Z}/n\mathbb{Z}$ und dieses j bestimmt σ eindeutig). ∎

Korollar 4.31 Sei K Körper, $\mathrm{char}(K) = 0$, $f \in K[X]$. Ist f durch Radikale lösbar, so ist $\mathrm{Gal}(f)$ auflösbar.

nach 4.27

Beweis: ist f durch Radikale lösbar, so existiert eine Radikal und Galoiserweiterung M/K sodass $L(f) \subseteq M$, $L(f)$ ein Zerfällungskörper von f.

Da $L(f)/K$ auch Galois folgt, dass man eine Surjektion

$$\mathrm{Gal}(M/K) \twoheadrightarrow \mathrm{Gal}(L(f)/K)$$

hat. $\mathrm{Gal}(M/K)$ ist nach 4.30 auflösbar, also auch $\mathrm{Gal}(L(f)/K)$ nach 4.29. □

Wir werden später zeigen, dass es Polynome f von grad ≥ 5 gibt, sodass $\mathrm{Gal}(f)$ nicht auflösbar ist (zB werden wir zeigen, dass für $n \geq 5$ A_n und S_n nicht auflösbar sind).