

20. Der Hauptsatz der Galoistheorie

Lemma 20.1 Sei L_f der Zerfällungskörper des separablen Polynoms $f \in K[X]$ und sei $G = \text{Gal}(L_f:K)$.
Dann ist $L_f^G = K$.

Beweis: Mit Prop. 19.8 gilt $|\text{Gal}(L_f:K)| = [L_f:K] =: n$.

Sei $K' := L_f^G$, also

$$K' = \{a \in L_f : \forall \sigma \in G (\sigma(a) = a)\}.$$

- Dann ist $K \subseteq K' \subseteq L_f$ und somit $[L_f:K'] =: m \leq n$.
- L_f ist der Zerfällungskörper von $f \in K'[X]$ und mit Prop. 19.8 gilt $[L_f:K'] = m = |\text{Gal}(L_f:K')|$. ($\leq n$)
- Mit Satz 19.1 ist $G \leq \text{Gal}(L_f:K') = \text{Gal}(L_f:L_f^G)$. $\Rightarrow n \leq m$
($H=G$)
- Somit ist $G = \text{Gal}(L_f:K) = \text{Gal}(L_f:K')$, d.h. $m = n$
und aus $\underbrace{[L_f:K]}_{=n} = \underbrace{[L_f:K']}_{=n} \cdot \underbrace{[K':K]}_{\Rightarrow =1}$ folgt $K' = K$.

Bem. Unter der Voraussetzung von Lemma 20.1 ist der Fixkörper zur Galoisgruppe $\text{Gal}(L_f:K)$ der Körper K .

Korollar 20.2 Ist L_f der Zerfällungskörper eines sep. Polynoms $f \in K[X]$, dann ist die Körpererweiterung $L_f:K$ separabel.

Beachte: Die Körpererweiterung $L_f:K$ ist normal (Satz 18.1).

Beweis: Sei $\alpha \in L_f$ beliebig. Zu zeigen: α ist separabel. Seien $\alpha_1, \dots, \alpha_r$ die in L_f zu α konj. Elemente, wobei wir jede Nullstelle nur einmal aufführen, und sei $g := (X - \alpha_1) \cdots (X - \alpha_r)$.

- Da nun jedes $\sigma \in \text{Gal}(L_f:K) =: G$ die Nullstellen $\alpha_1, \dots, \alpha_r$ permutiert, ist $\sigma(g) = g$, d.h. die Koeffizienten von g liegen in L_f^G ; mit Lemma 20.1 also in K und somit ist $g \in K[X]$ separabel.

Bem. Aus Satz 18.1 und Kor. 20.2 folgt, dass eine Körpererweiterung $L:K$ genau dann endl., normal und separabel ist, wenn der Körper L der Zerfällungskörper eines separablen Polynoms $f \in K[X]$ ist. Solche Körpererweiterungen heißen endl. Galoiserweiterungen oder kurz galoisch.

Lemma 20.3 Es sei L ein Körper und $H \leq \text{Aut}(L)$.

Dann gilt $[L:L^H] \leq |H|$.

Beweis: Sei $K := L^H$ und $m := |H|$, wobei $H = \{\sigma_1, \dots, \sigma_m\}$.

Wir führen die Annahme $[L:K] > m$ zu einem Widerspruch.

- Ist $[L:K] > m$, so ex. in L Elemente $\alpha_0, \dots, \alpha_m$ die über K lin. unabh. sind. Für jedes der m Elemente $\sigma_i \in H$ betrachten wir die Gleichung

$$\sigma_i(\alpha_0) \cdot x_0 + \dots + \sigma_i(\alpha_m) \cdot x_m = 0$$

in L in den Unbekannten $x_0, \dots, x_m$.

- Wir erhalten m Gleichungen (für jedes $\sigma_i \in H$ eine Gleichung) mit $m+1$ Unbekannten, welche in L eine nicht-triviale Lösung hat.
- Wir wählen die ^{nicht-triviale} Lösung mit den meisten k 's mit $x_k = 0$ und nummerieren die x_i und α_i so, dass $x_0 \neq 0, \dots, x_q \neq 0, x_{q+1} = 0, \dots, x_m = 0$.
[Beachte: $x_0 \neq 0$ weil Lösung nicht-trivial]
- Ist $\tau \in H$ (also $\tau = \sigma_j$), so ist $\tau(0) = 0$. Für alle $1 \leq i \leq m$ gilt somit

$$\underbrace{\tau \sigma_i(\alpha_0)}_{= \sigma_i \in H} \cdot \tau(x_0) + \dots + \underbrace{\tau \sigma_i(\alpha_m)}_{= \sigma_i \in H} \cdot \tau(x_m) = 0$$

- Die Matrix dieses Gleichungssystems ist bis auf Vertauschung der Zeilen dieselbe wie für das ursprüngliche Gleichungssystem, also ist auch $\tau(x_0), \dots, \tau(x_m)$ eine Lösung des ursprünglichen Systems. [Beachte: Die Spalten werden nicht vertauscht.]

- Weil $x_0 \neq 0$ und $\tau \in \text{Aut}(L)$, ist $\tau(x_0) \neq 0$. Mit x_i ($0 \leq i \leq m$) $\tau(x_i)$ ($0 \leq i \leq m$), sind auch $\tau(x_0) \cdot x_i$ und $x_0 \cdot \tau(x_i)$ ($0 \leq i \leq m$) Lösungen, und somit auch die Differenz

$$x'_i := \tau(x_0) \cdot x_i - x_0 \cdot \tau(x_i) \quad (0 \leq i \leq m).$$

- Weil $x'_0 = \tau(x_0) \cdot x_0 - x_0 \cdot \tau(x_0) = 0$ und weil die Spalten nicht vertauscht wurden, muss es sich nach Voraussetzung (max. Anzahl 0'en) um die triviale Lösung handeln. Also gilt $x'_0 = \dots = x'_m = 0$.

- D.h. $\tau(x_0) \cdot x_i = x_0 \cdot \tau(x_i)$ und weil $x_0 \neq 0$, ist

$$x_i \cdot x_0^{-1} = \tau(x_i \cdot x_0^{-1}) \quad \text{für alle } \tau \in H.$$

- Somit gilt: $x_i \cdot x_0^{-1} \in L^H = K$. Für jedes x_i ex. ein $z_i := x_i \cdot x_0^{-1} \in K$ mit $x_i = x_0 \cdot z_i$. [$x_0 = x_0 \cdot z_0 \Rightarrow z_0 \neq 0$]

- Für $\sigma = \tau$ ($\tau = \text{Identität}$) erhalten wir

$$\alpha_0 x_0 + \dots + \alpha_m x_m = 0 = x_0 (\alpha_0 z_0 + \dots + \alpha_m z_m)$$

mit $z_i \in K$. Somit ist, weil $x_0 \neq 0$, $\alpha_0 z_0 + \dots + \alpha_m z_m = 0$,

und weil $z_0 \neq 0$ sind $\alpha_0, \dots, \alpha_m$ über K lin. abh. $\swarrow$ zu $[L:K] > m$

—

Satz 20.4 (Hauptsatz der Galois-theorie)

Die Körpererweiterung $L:K$ sei galoisch (d.h. endl., normal und separabel) mit Galoisgruppe $G = \text{Gal}(L:K)$.

Dann ist die Zuordnung

$$\begin{array}{ccc} \{H: H \leq G\} & \longleftrightarrow & \{M: K \subseteq M \subseteq L\} \\ \text{Untergruppen} & & \text{Zwischenkörper} \\ H & \longmapsto & L^H \\ \text{Gal}(L:M) & \longleftarrow & M \end{array}$$

eine Bijektion zwischen den Untergruppen von G und den Zwischenkörpern von $L:K$.

Beweis: Sei $K \subseteq M \subseteq L$. Da $L:K$ endl., normal, separabel, ist auch (unter anderem mit Bem. zu Kor. 20.2) $L:M$ endl., normal und separabel. [Bem. $M:K$ ist ebenfalls separabel, aber nicht notwendigerweise normal.]

$$\bullet \quad H \longmapsto L^H \longmapsto \text{Gal}(L:L^H) \leq G$$

L^H ist Zw.-Körper
mit Satz 19.1

$$\begin{aligned} H \leq \text{Gal}(L:L^H) \text{ mit Satz 19.1} &\Rightarrow |H| \leq |\text{Gal}(L:L^H)| \\ &\leq [L:L^H] \stackrel{\text{Prop. 19.6}}{\leq} |H| \stackrel{\text{Lem. 20.3}}{\leq} |H| \\ &\Rightarrow H = \text{Gal}(L:L^H) \end{aligned}$$

$$\bullet \quad M \longmapsto \underbrace{\text{Gal}(L:M)}_{\leq G \text{ mit Satz 19.2}} \longmapsto L^H = M \text{ mit Lem. 20.1}$$

Das folgende Korollar ist eine Folgerung aus Satz 19.10 (über primitive Elemente).

Korollar 20.5 Ist $L:K$ eine endl. separable Körpererweiterung.

Dann ist $L:K$ einfach (d.h. es ex. $\alpha \in L$ mit $L = K(\alpha)$).

Beweis: Ist $L:K$ endl. und separabel, dann ist $L = K(\alpha_1, \dots, \alpha_n)$ für $\alpha_i \in L$. Sei N der Zerfällungskörper von $\prod_{i=1}^n f_i$ über K , wobei f_i das Min.-Poly. von α_i über K ist.

- Dann ist $N:K$ galoisch (also endl., normal und separabel).
- Mit dem Hauptsatz der Galoistheorie 20.4 entspricht jeder Zwischenkörper $K \subseteq M \subseteq N$ in bijektiver Weise einer Untergruppe von $\text{Gal}(N:K)$.
- Weil $[N:K]$ endlich ist, ist auch $|\text{Gal}(N:K)|$ endlich und somit kann es nur endl. viele Zwischenkörper $K \subseteq M \subseteq N$ (bzw. Untergruppen $H \leq \text{Gal}(N:K)$) geben. Insbesondere gibt es nur endl. viele Zwischenkörper $K \subseteq M \subseteq L \subseteq N$ und mit Satz 19.10 ist $L = K(\alpha)$.

[für die folgenden Korollare]

Im folgenden sei $L:K$ galoisch (d.h. endl., normal und separabel).

Korollar 20.6 Ist M ein Zwischenkörper, d.h. $K \subseteq M \subseteq L$,

$$\text{so ist } \underbrace{[M:K]}_{\substack{\text{nicht notwendig} \\ \text{galoisch}}} = \underbrace{[\text{Gal}(L:K)]}_{\text{galoisch}} : \underbrace{[\text{Gal}(L:M)]}_{\text{galoisch}}$$

Beweis: Sei M ein Zwischenkörper und sei

$$H := \text{Gal}(L:M) \leq \text{Gal}(L:K) =: G.$$

- Es gilt $|G| = [L:K]$ und $|H| = [L:M]$ (mit Satz 18.1)
- Aus $[L:K] = [L:M] \cdot [M:K]$ folgt:

$$[M:K] = \frac{[L:K]}{[L:M]} = \frac{|G|}{|H|} = [G:H] \quad \begin{array}{l} [H \trianglelefteq G \Rightarrow \\ |G/H| = [G:H] \end{array}$$

└

Korollar 20.7 Jeder aufsteigenden Folge von Zwischenkörpern

$$K \subseteq M_1 \subseteq \dots \subseteq M_n \subseteq L$$

entspricht eine absteigende Folge von Untergruppen von $\text{Gal}(L:K)$:

$$\text{Gal}(L:K) \geq \text{Gal}(L:M_1) \geq \dots \geq \text{Gal}(L:M_n) \geq \text{Gal}(L:L)$$

$$G \geq H_1 \geq \dots \geq H_n \geq \{e\}$$

bzw. $\{e\}$ mit
 $z \in \text{Aut}(L)$

Beweis: • Die Körpererweiterungen $L:M_i$ sind endl., normal und separabel, also galoisch.

- M_{i+1} ist ein Zwischenkörper der Körpererweiterung $L:M_i$, d.h. $M_i \subseteq M_{i+1} \subseteq L$.

- Somit ist $\text{Gal}(L:M_{i+1}) = H_{i+1} \leq H_i = \text{Gal}(L:M_i)$.

└

Ein einfaches Beispiel: Sei $L = K(\alpha)$ mit $[K(\alpha):K] = 2$.

Dann ist $\{1, \alpha\}$ eine Basis des VR $K(\alpha)$ über K und $\alpha^2 = p + q \cdot \alpha$ für $p, q \in K$.

Dann ist $\alpha^2 - q\alpha - p = 0$ und $\alpha_{1,2} = \frac{q \pm \sqrt{q^2 + 4p}}{2}$. Für $a := q^2 + 4p \in K$ ist

$L = K(\alpha)$ somit der Zerfällungskörper von $X^2 - a$. Somit gilt $|\text{Gal}(L:K)| = [L:K] = 2$, d.h. $\text{Gal}(L:K) \cong C_2$ und für $H \leq G$ ist $H = \{e\}$ oder $H = G$. Somit hat $L:K$ keine nicht-trivialen Zwischenkörper.

Korollar 20.8 Ist M ein Zwischenkörper, $K \subseteq M \subseteq L$, und ist $\sigma \in \text{Gal}(L:K)$, so ist $\sigma[M]$ ein Körper mit $K \subseteq \sigma[M] \subseteq L$ und es gilt:

$$\text{Gal}(L: \sigma[M]) = \sigma \underbrace{\text{Gal}(L: M)}_{\text{konj. Untergruppe}} \sigma^{-1} \leq \text{Gal}(L: K) \leq \text{Gal}(L: K)$$

Beweis: • Weil $\sigma \in \text{Gal}(L:K)$ ein K -Automorphismus von L ist, ist $\sigma[M]$ ein Körper und weil $K \subseteq M$ und $\sigma|_K = \text{id}$, ist $\sigma[M] \supseteq K$.

- Ist $\tau \in \text{Gal}(L: M)$ und $x \in M$, so ist $\tau(x) = x$ (weil τ ein M -Autom. von L ist) und $\sigma(x) \in \sigma[M]$ (nach Def.). Somit ist $\sigma \tau \sigma^{-1}(\sigma x) = \sigma \tau(x) = \sigma(x)$, also

$$\sigma \tau \sigma^{-1} \in \text{Gal}(L: \sigma[M])$$

und es gilt: $\sigma \text{Gal}(L: M) \sigma^{-1} \leq \text{Gal}(L: \sigma[M])$
 $\tau \in \text{Gal}(L: M)$

- Ist $\tilde{\tau} \in \text{Gal}(L: \sigma[M])$ (und ^{wieder} $\sigma(x) \in \sigma[M]$, $x \in M$), so ist $\tilde{\tau}(\sigma(x)) = \sigma(x)$ (weil $\tilde{\tau}$ ein $\sigma[M]$ -Autom. von L ist). D.h. $\sigma^{-1} \tilde{\tau}(\sigma(x)) = \sigma^{-1} \tilde{\tau} \sigma(x) = \sigma^{-1}(\sigma(x)) = x$, und somit ist $\sigma^{-1} \tilde{\tau} \sigma$ ein M -Autom. von L , also

$$\sigma^{-1} \tilde{\tau} \sigma \in \text{Gal}(L: M). \text{ d.h. } \tilde{\tau} \in \sigma \text{Gal}(L: M) \sigma^{-1}$$

Es gilt somit: $\text{Gal}(L: \sigma[M]) \leq \sigma \text{Gal}(L: M) \sigma^{-1}$
 $\tilde{\tau} \in \text{Gal}(L: \sigma[M])$

- Damit ist $\text{Gal}(L: \sigma[M]) = \sigma \text{Gal}(L: M) \sigma^{-1}$.

—

Def. Ist $\sigma \in \text{Gal}(L: K)$ und M ein Zwischenkörper, so heisst $\sigma[M]$ der unter σ zu M konjugierte Körper.

Korollar 20.9 Ist M ein Zwischenkörper, $K \subseteq M \subseteq L$, dann ist die Körpererweiterung $M:K$ genau dann normal, wenn $\text{Gal}(L: M) \trianglelefteq \text{Gal}(L: K)$.

Beweis: • Ist die Körpererweiterung $M:K$ normal, so liegt mit Kor. 19.3 jedes ^(in L) zu $a \in M$ konjugierte Element wiederum in M . D.h. für alle $\sigma \in \text{Gal}(L:K)$ ist $\sigma(a) \in M$, also gilt $\sigma[M] = M$. Mit Kor. 20.8 gilt nun (für alle $\sigma \in \text{Gal}(L:K)$)

$$\sigma \text{Gal}(L:M) \sigma^{-1} = \text{Gal}(L: \sigma[M]) = \text{Gal}(L:M),$$
d.h. $\text{Gal}(L:M) \trianglelefteq \text{Gal}(L:K)$.

• Sei umgekehrt $H \trianglelefteq \text{Gal}(L:K)$ und sei $M := L^H$. Dann ist $K \subseteq M \subseteq L$. Für $\sigma \in \text{Gal}(L:K)$ gilt:

$$\sigma[M] = L^{\sigma H \sigma^{-1}} = L^H = M$$

$\uparrow$
 $H \trianglelefteq \text{Gal}(L:K)$

Somit enthält der Körper M mit jedem $a \in M$ auch alle ^{(in L (!))} zu a konj. Elemente (weil $L:K$ normal ist und $\sigma \in \text{Gal}(L:K)$ beliebig ist). D.h. die Körpererweiterung $M:K$ ist normal. —

Bem. Wenn $M:K$ normal ist, dann ist $M:K$ auch galoissch (weil $L:K$ galoissch ist). Mit dem folgenden Korollar können wir $\text{Gal}(M:K)$ bestimmen.

Korollar 20.10 Ist M ein Zwischenkörper, $K \subseteq M \subseteq L$, und ist $M:K$ normal, dann gilt:

$$\text{Gal}(L:K) / \text{Gal}(L:M) \cong \text{Gal}(M:K)$$

Beweis: Ist $M:K$ normal, so gilt für alle $\sigma \in \text{Gal}(L:K)$, $\sigma[M] = M$. Damit ist $\pi: \text{Gal}(L:K) \rightarrow \text{Gal}(M:K)$

$$\sigma \mapsto \sigma|_M \quad \text{z = Identität}$$

ein Gruppenhomom. Es ist $\ker(\pi) = \{\sigma \in \text{Gal}(L:K) : \sigma|_M = z\}$, d.h. $\ker(\pi) = \text{Gal}(L:M)$. Damit induziert π einen Isom.

$$\text{Gal}(L:K) / \text{Gal}(L:M) \xrightarrow{\sim} \text{Gal}(M:K)$$

und wir erhalten $\text{Gal}(L:K) / \text{Gal}(L:M) \cong \text{Gal}(M:K)$. —

Ein Beispiel Sei L der normale Abschluss von $\mathbb{Q}(\sqrt{2}, \sqrt{3})$,
d.h. $L:\mathbb{Q}$ ist die kleinste normale Körpererweiterung
mit $\sqrt{2}, \sqrt{3} \in L$.

- $L = \mathbb{Q}(a_1)$ mit $a_1 = \sqrt{2} + \sqrt{3}$. Das Min.-Poly. von a_1 über $\mathbb{Q}$
ist
$$f = \prod (X - (\pm\sqrt{2} \pm \sqrt{3})) = 1 - 10X^2 + X^4.$$

mit den 4 Nullstellen: $a_1 = \sqrt{2} + \sqrt{3}$, $a_2 = \sqrt{2} - \sqrt{3}$,
(Bem. $a_1 + a_2 = 2\sqrt{2} \Rightarrow \sqrt{2} \in L$) $a_3 = -\sqrt{2} + \sqrt{3}$, $a_4 = -\sqrt{2} - \sqrt{3}$

$$\bullet [L:\mathbb{Q}] = \underbrace{[L:\mathbb{Q}(\sqrt{2})]}_{=2} \cdot \underbrace{[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]}_{=2} = 4 = |\text{Gal}(L:\mathbb{Q})|$$

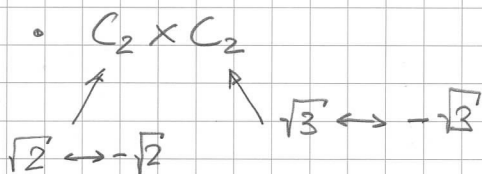
Somit ist $\text{Gal}(L:\mathbb{Q}) \cong \begin{cases} C_4 & \text{(nicht möglich, warum?)} \\ C_2 \times C_2 \end{cases}$

- Sei $C_2 \times C_2 = \{(\varepsilon_1, \varepsilon_2) : \varepsilon_1, \varepsilon_2 \in \{0, 1\}\}$, dann sind

$$\tilde{A} = \langle (0, 1) \rangle, \quad \tilde{B} = \langle (1, 1) \rangle, \quad \tilde{C} = \langle (1, 0) \rangle$$

die drei nicht-trivialen Untergruppen von $C_2 \times C_2$, und
weil $C_2 \times C_2$ abelsch ist, sind $\tilde{A}, \tilde{B}, \tilde{C}$ Normalteiler von $C_2 \times C_2$.

- Es gilt $C_2 \times C_2 / \tilde{A}, \tilde{B}, \tilde{C} \cong C_2$ und $\tilde{A}, \tilde{B}, \tilde{C} \cong C_2$.



- Die Elemente $\alpha \in \text{Gal}(L:\mathbb{Q})$ sind bestimmt durch
 $\alpha(a_1):$

	Bild von $\sqrt{2}$		$\sqrt{3}$	
$\alpha(a_1) =$	a_1	$\sqrt{2}$	$\sqrt{3}$	$\Rightarrow \alpha = 1, \alpha \hat{=} (0, 0)$
	a_2	$\sqrt{2}$	$-\sqrt{3}$	$\Rightarrow \alpha^2 = 1, \alpha \hat{=} (0, 1)$
	a_3	$-\sqrt{2}$	$\sqrt{3}$	$\Rightarrow \alpha^2 = 1, \alpha \hat{=} (1, 0)$
	a_4	$-\sqrt{2}$	$-\sqrt{3}$	$\Rightarrow \alpha^2 = 1, \alpha \hat{=} (1, 1)$

Seien $A, B, C \leq \text{Gal}(L:\mathbb{Q})$ die Untergruppen von $\text{Gal}(L:\mathbb{Q})$ welche den Untergruppen von $\tilde{A}, \tilde{B}, \tilde{C} \leq C_2 \times C_2$ entsprechen.

$$\bullet L^A = \{a \in L: \forall \sigma \in A (\sigma(a) = a)\}$$

$$\Rightarrow \text{Gal}(L:L^A) = \{\sigma \in G: \sigma(\sqrt{2}) = -\sqrt{2}\}$$

$$\text{und es gilt } L^A = \mathbb{Q}(\sqrt{2}).$$

Weil $\tilde{A} \cong C_2 \times C_2$ ist $\mathbb{Q}(\sqrt{2}):\mathbb{Q}$ galoissch mit

$\text{Gal}(\mathbb{Q}(\sqrt{2}):\mathbb{Q}) \cong C_2 \times C_2 / \tilde{A} \cong C_2$ und $\mathbb{Q}(\sqrt{2})$ ist der Zerfällungskörper von $f = X^2 - 2$ über $\mathbb{Q}$.

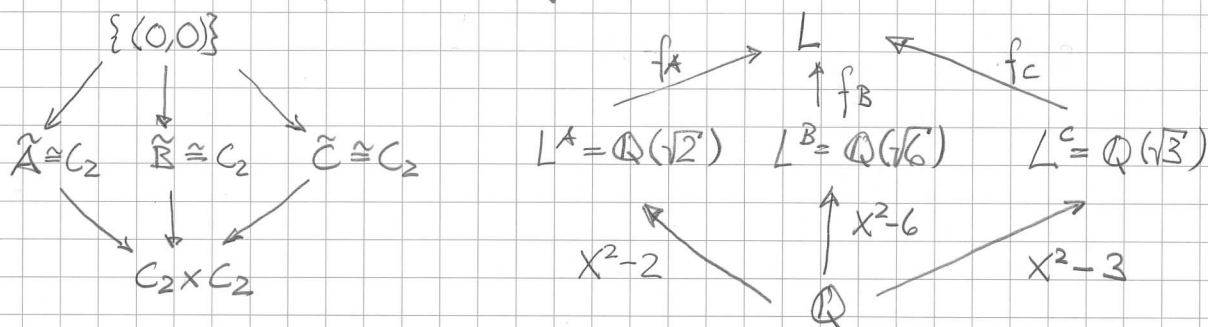
• Analog erhalten wir $L^C = \mathbb{Q}(\sqrt{3})$ mit $\text{Gal}(\mathbb{Q}(\sqrt{3}):\mathbb{Q}) \cong C_2$ und $\mathbb{Q}(\sqrt{3})$ ist Zerfällungskörper von $X^2 - 3$ über $\mathbb{Q}$.

$$\bullet L^B = \{a \in L: \forall \sigma \in B (\sigma(a) = a)\}:$$

$$\sigma \in B, \sigma \neq 1, \text{ dann ist } \sigma(\sqrt{2}) = -\sqrt{2} \text{ und } \sigma(\sqrt{3}) = -\sqrt{3}.$$

Somit ist $L^B = \mathbb{Q}(\sqrt{6})$, denn $\sqrt{6} = \sqrt{2} \cdot \sqrt{3}$ und für $\sigma \neq 1$ ist $\sigma(\sqrt{6}) = \sigma(\sqrt{2} \cdot \sqrt{3}) = \sigma(\sqrt{2}) \cdot \sigma(\sqrt{3}) = -\sqrt{2} \cdot -\sqrt{3} = \sqrt{6}$.

• Wir erhalten folgendes Diagramm:



• Da $L:\mathbb{Q}(\sqrt{2})$ galoissch ist, ex. $b \in L$ mit $L = \mathbb{Q}(\sqrt{2})(b)$.

Das Min.-Poly. eines solchen b über $\mathbb{Q}(\sqrt{2})$ ist $f_A = -1 + 2\sqrt{2}X + X^2 \in \mathbb{Q}(\sqrt{2})[X]$

• Analog ist $f_C = 1 - 2\sqrt{3}X + X^2 \in \mathbb{Q}(\sqrt{3})[X]$

• Für f_B betrachten wir $1 - 10X^2 + X^4 = 1 - 10Y + Y^2$ mit $Y = 5 \pm 2\sqrt{6}$ und erhalten $X = \pm\sqrt{5 \pm 2\sqrt{6}}$

Somit ist $f_B = X^2 - \underbrace{(5 + 2\sqrt{6})}_{=(\sqrt{2} + \sqrt{3})^2} \in \mathbb{Q}(\sqrt{6})[X]$

Beachte: $\sqrt{6} \cdot (\sqrt{2} + \sqrt{3}) = 2\sqrt{3} + 3\sqrt{2}$
 $\Rightarrow 3 \cdot (\sqrt{2} + \sqrt{3}) - (2\sqrt{3} + 3\sqrt{2}) = \sqrt{2} \in L$