Ein Isom. $Gal(L/\mathbb{Q}) \to S_3$ ist gegeben durch $\varphi \mapsto$ Perm. induziert auf $\{\alpha_1,\alpha_2,\alpha_3\} \cong \{1,2,3\}$ also $\sigma \mapsto (23)$, $\tau\sigma \mapsto (12)$, $\tau^2\sigma \mapsto (13)$, $\tau \mapsto (123)$, $\tau^2 \mapsto (132)$

Galois-Korrespondenz

$$\begin{tikzcd}
 & & S_3 & & \\
\{e,\sigma\} \arrow[urr] & \{e,\tau\sigma\} \arrow[ur] & \{e,\tau^2\sigma\} \arrow[u] & \{e,\tau,\tau^2\} \arrow[ul, "3"'] & \\
 & & \{e\} \arrow[ull] \arrow[ul] \arrow[u] \arrow[ur] & &
\end{tikzcd}
\longleftrightarrow
\begin{tikzcd}
 & & \mathbb{Q} \arrow[dll] \arrow[dl] \arrow[d] \arrow[dr] & \\
\mathbb{Q}(\sqrt[3]{2}) \arrow[drr] & \mathbb{Q}(\zeta^2\sqrt[3]{2}) \arrow[dr] & \mathbb{Q}(\zeta\sqrt[3]{2}) \arrow[d] & \mathbb{Q}(\zeta) \arrow[dl] \\
 & & \mathbb{Q}(\sqrt[3]{2},\zeta) &
\end{tikzcd}$$

Von der oberen Inkl. nur $\{e,\tau,\tau^2\} \cong A_3 \subset S_3$ ist normal $\rightsquigarrow$ von den oberen Inkl. nur $\mathbb{Q} \subset \mathbb{Q}(\zeta)$ galois, mit $Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$

4.1.11 Korollar (Rechenregel)

Sei $K \subset L$ galois, $E_1, E_2 \in \mathcal{K}$, $H_1 = Gal(L/E_1)$, $H_2 = Gal(L/E_2)$
(i) $E_1 \subset E_2 \iff H_2 \subset H_1$ (ii) Sei E_1E_2 das Kompositum von E_1, E_2, d.h. kleinste Teilkörper von L, der E_1, E_2 enthält. Dann $Gal(L/E_1E_2) = H_1 \cap H_2$ (iii) $Gal(L/E_1 \cap E_2) = \langle H_1 \cup H_2 \rangle$

Beweis Übung.

4.1.12 Satz Sei $K \subset L$ Körpererw, E_1, E_2 Zwischenkörper $K \subset E_1$, $K \subset E_2$ seien galois. Dann
(i) $K \subset E_1E_2$ galois (ii) $\varphi : Gal(E_1E_2/E_1) \to Gal(E_2/E_1 \cap E_2)$, $\sigma \mapsto \sigma|_{E_2}$ wohldef und Isom.
(iii) $\psi: Gal(E_1E_2/K) \to Gal(E_1/K) \times Gal(E_2/K)$, $\sigma \mapsto (\sigma|_{E_1}, \sigma|_{E_2})$ ist wohldef. und injektiv. Falls $K = E_1 \cap E_2$, so ψ Isom.

Beweis (i) $E_1 = K(\alpha_1,\dots,\alpha_n)$, $E_2 = K(\beta_1,\dots,\beta_m)$, wobei α_i, β_j Nst von sep. Polynome sind (s. 4.1.2(ii)). Dann $E_1E_2 = E_1(\beta_1,\dots,\beta_m)$ und
$\underbrace{K \subset E_1}_{sep} \underbrace{\subset E_1(\beta_1,\dots,\beta_m)}_{sep} \underset{3.5.11}{\rightsquigarrow} K \subset E_1E_2$ sep.
E_1 Zerfkörper von $f_1 \in K[X]$, E_2 Zerfkörper von $f_2 \in K[X] \rightsquigarrow E_1E_2$ Zerfkörper von $f_1f_2 \in K[X] \rightsquigarrow K \subset E_1E_2$ normal. (ii),(iii) Übung. ∎

4.2. Die Galois-Gruppe einer Gleichung

4.2.1 Def Sei $f \in K[X]$ separabel und $\operatorname{grad} f \geq 1$.
Die Galoisgruppe von f über K (oder der Gleichung $f(x)=0$) ist $\operatorname{Gal}(L/K)$, wobei L der Zerfällungskörper von f über K ist ($K \subset L$ galois wegen 4.1.2).

4.2.2 Satz Sei $f \in K[X]$ separabel, $n = \operatorname{grad} f \geq 1$, L ein Zerf.kö von f über K, $\alpha_1, \dots, \alpha_n$ Nst. von f in L. Dann gilt:
(i) $\varphi : \operatorname{Gal}(L/K) \longrightarrow S(\{\alpha_1, \dots, \alpha_n\}) \cong S_n$, $\sigma \mapsto \sigma|_{\{\alpha_1, \dots, \alpha_n\}}$
ist ein injektiver Homom. Insb. $\operatorname{Gal}(L/K) = [L:K] \mid n!$
(ii) f irred $\Longleftrightarrow$ $\operatorname{Gal}(L/K)$ operiert transitiv auf $\{\alpha_1, \dots, \alpha_n\}$
Insb.: $[L:K] = n! \Rightarrow f$ irred.

Beweis (i) Ist $\varphi(\alpha_i) = \alpha_i$ für alle $i \overset{\varphi|_K = Id}{\rightsquigarrow} \varphi = Id_L$
(ii) „$\Rightarrow$" Seien $1 \leq i, j \leq n$ gegeben. Lemma 3.3.10 $\rightsquigarrow \exists$ K-Homom $\sigma : K(\alpha_i) \to K(\alpha_j)$ mit $\sigma(\alpha_i) = \alpha_j$. Satz 3.3.11 $\rightsquigarrow \sigma$ hat eine Fortsetzung $\sigma : L \to \bar{L}$. Satz 3.4.6 $\rightsquigarrow \operatorname{Im} \sigma = L$ also $\sigma \in \operatorname{Gal}(L/K)$ und $\sigma(\alpha_i) = \alpha_j$
„$\Leftarrow$" Ist $f = g \cdot h \rightsquigarrow$ Jedes $\sigma \in \operatorname{Gal}(L/K)$ lässt die Nstmenge von g und Nstmenge von h invariant. Diese zwei Mengen sind disjunkt (da f separabel) $\rightsquigarrow$ Die Operation ist nicht transitiv. ▨

4.2.3 Bem. $K \subset L$ galois $\overset{3.5.12}{\rightsquigarrow} \exists \alpha \in L : L = K(\alpha)$. Sei $f \in K[X]$ Minpol. zu $\alpha \rightsquigarrow \operatorname{grad} f = n = [L:K]$. Nun ist L Zerf.kö von f
$\overset{4.2.2}{\rightsquigarrow} \operatorname{Gal}(L/K) \hookrightarrow S_n$ aber $\underset{\text{ord } n}{\operatorname{Gal}(L/K)} \neq \underset{\text{ord } n!}{S_n}$

4.2.4 Bsp. (i) Sei $\operatorname{char} K \neq 2$, $f = X^2 + aX + b \in K[X]$ habe keine Nst. in K. $\operatorname{grad} f = 2 \rightsquigarrow f$ irred. Außerdem ist f separabel (3.5.4: falls $\operatorname{char} K = 0$ oder Blatt 12 falls $\operatorname{char} K = p \neq 2$). Sei $\alpha \in \bar{K}$ eine Nst. von $f \rightsquigarrow L = K(\alpha)$ schon