Sei nun $f \in K[X]$ ein separables Polynom vom Grad $n \geqslant 0$. Seien $a_1, \ldots, a_n$ die Nullstellen von f in einem Zerfällungskörper $L = K(a_1, \ldots, a_n)$ von f über K. Dann ist L/K galoissch, und wir nennen seine Galoisgruppe $\mathrm{Gal}(L/K)$ auch die *Galoisgruppe von f über K*.

7.2.4 Proposition: Es existiert eine eindeutige Linksoperation von Γ auf $\{1, \ldots, n\}$ mit der Eigenschaft

$$\forall \gamma \in \mathrm{Gal}(L/K)\ \forall 1 \leqslant i \leqslant n\colon \gamma(a_i) = a_{\gamma i}.$$

Diese ist treu, entspricht also einem injektiven Homomorphismus $\mathrm{Gal}(L/K) \hookrightarrow S_n$.

Injektivität: $\forall \sigma \in \mathrm{Gal}: \forall i : \sigma(a_i) = a_i \Rightarrow \sigma$ auf $K(a_1, \ldots, a_n)$ trivial.

Dadurch können wir $\mathrm{Gal}(L/K)$ mit einer Untergruppe von S_n identifizieren. Die Identifikation hängt allerdings von der gewählten Reihenfolge der Nullstellen ab. Jede andere Reihenfolge hat die Form $a_{\sigma 1}, \ldots, a_{\sigma n}$ für eine Permutation $\sigma \in S_n$, und die Umordnung ändert den Homomorphismus ab um den inneren Automorphismus int_σ von S_n und sein Bild somit um Konjugation mit σ.

7.2.5 Proposition: Die Bahnen der Operation von $\mathrm{Gal}(L/K)$ auf $\{1, \ldots, n\}$ entsprechen genau den normierten irreduziblen Faktoren von f in $K[X]$. Insbesondere ist die Operation transitiv genau dann, wenn f irreduzibel ist.

Beweis: A Bahn $\Rightarrow g(X) := \prod_{i \in A} (X - a_i) \in L[X]$ invariant unter $\mathrm{Gal}(L/K)$, denn:

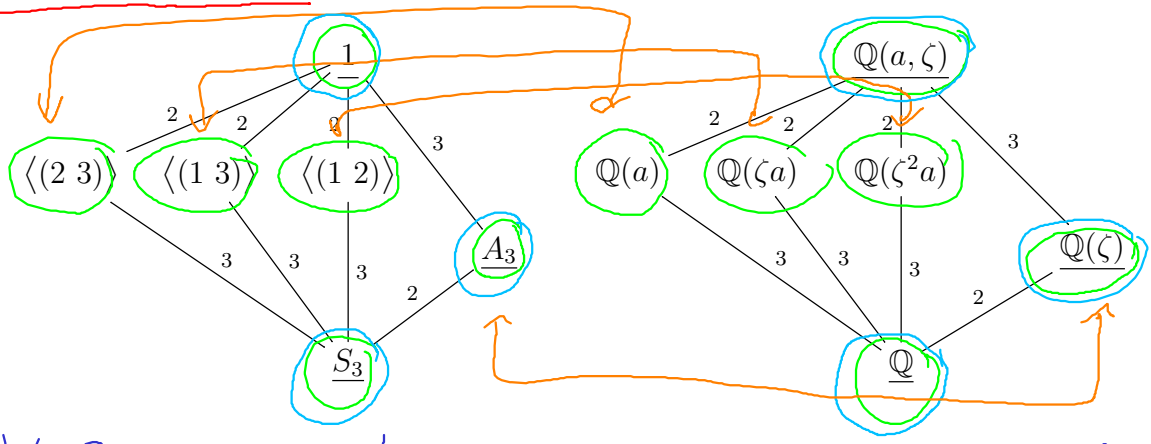
$\sigma\left(\prod_{i \in A}(X - a_i)\right) = \prod_{i \in A}(X - \sigma(a_i)) = \prod_{i \in A}(X - a_{\sigma i}) = \prod_{j \in A}(X - a_j) \Rightarrow \sigma(g) = g$ für alle $\sigma \in \mathrm{Gal}(L/K)$

$\Rightarrow g \in K[X]$ und $g \mid f$ in $L[X] \Rightarrow g \mid f$ in $K[X]$.

Ist $h \in K[X]$ mit $h \mid g$, existiert $i \in A$ mit $X - a_i \mid h \Rightarrow \forall \sigma : X - \sigma(a_i) \mid h \Rightarrow g \mid h \Rightarrow g = h$. Also ist g irred.

irred. nach Eisenstein für $p=2$.

7.2.6 Beispiel: Das Polynom $f(X) := X^3 - 2 \in \mathbb{Q}[X]$ hat die Galoisgruppe S_3. Genauer seien $a := \sqrt[3]{2} \in \mathbb{R}$ und $\zeta := \exp\frac{2\pi i}{3} \in \mathbb{C}$. Die komplexen Nullstellen von f sind dann $(a_1, a_2, a_3) := (a, \zeta a, \zeta^2 a)$. Mit $L := \mathbb{Q}(a_1, a_2, a_3) = \mathbb{Q}(a, \zeta)$ liefert die Galoiskorrespondenz die folgenden Entsprechungen, wobei normale Untergruppen bzw. Erweiterungen unterstrichen sind:



$\mathbb{Q}(a)$

$[\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}] = 3$.

$\gamma \notin \mathbb{R} \Rightarrow \gamma \notin \mathbb{Q}(\sqrt[3]{2})$

$\Rightarrow [\mathbb{Q}(\sqrt[3]{2}, \gamma)/\mathbb{Q}(\sqrt[3]{2})] = 2$

$\Rightarrow [L/\mathbb{Q}] = 6 = |\Gamma|$

$\Gamma := \mathrm{Gal}(L/\mathbb{Q}) \subset S_3$.

$\Rightarrow \Gamma \xrightarrow{\sim} S_3$.

$\mathbb{Q}(a)$ enthält eine Untergruppe vom Index 3 $\Rightarrow$ Ordnung 2.

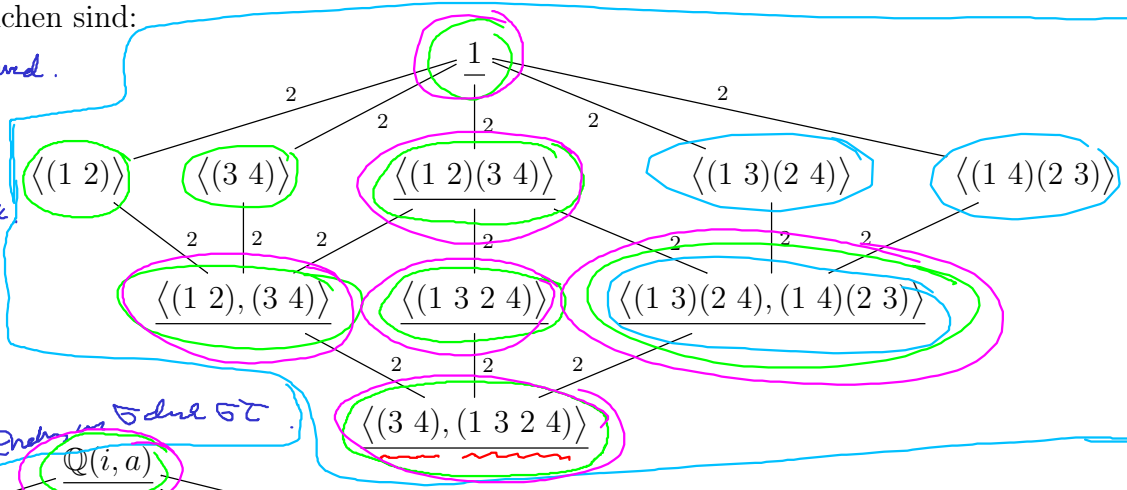
$a = a_1$ fest unter $(2\,3)$. $\Rightarrow (2\,3) \in \mathrm{Gal}(L/\mathbb{Q}(a))$. (Ordnung 2)

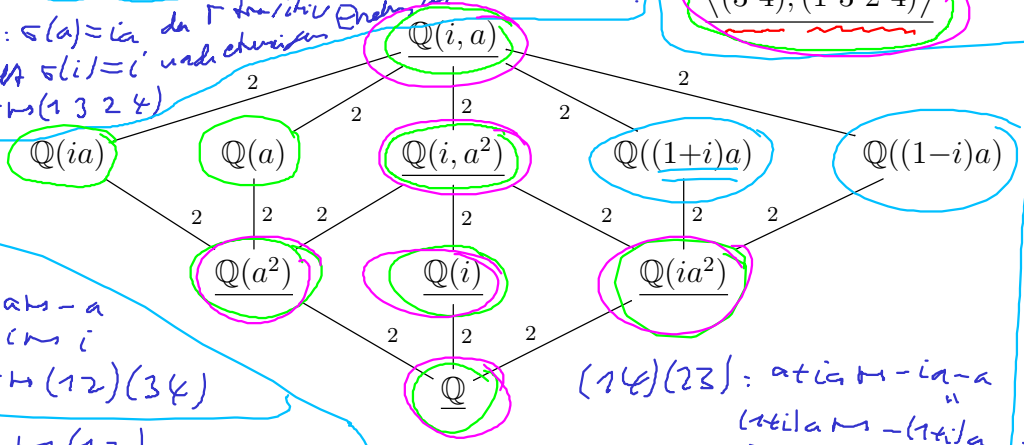
$\exists a = a_2$ fest unter $(1\,3)$

$\mathbb{Q}(\gamma) = \mathbb{Q}(i\sqrt{3})$ vom Grad 2 über $\mathbb{Q}$

$\Rightarrow$ enthält eine Untergruppe vom Index 2.

7.2.7 Beispiel: Das Polynom $f(X) := X^4 - 2 \in \mathbb{Q}[X]$ hat Galoisgruppe D_4. Genauer sei $a := \sqrt[4]{2} \in \mathbb{R}$; die komplexen Nullstellen von f sind dann $(a_1, a_2, a_3, a_4) := (a, -a, ia, -ia)$. Mit $L := \mathbb{Q}(a_1, a_2, a_3, a_4) = \mathbb{Q}(i, a)$ liefert die Galoiskorrespondenz die folgenden Entsprechungen, wobei normale Untergruppen bzw. Erweiterungen unterstrichen sind:





$[\mathbb{Q}(a)/\mathbb{Q}] = 4$ da f irred.
$i \notin \mathbb{Q}(a) \Rightarrow [L/\mathbb{Q}(a)] = 2$
$\Rightarrow [L/\mathbb{Q}] = 8$.
$\Gamma := \mathrm{Gal}(L/\mathbb{Q}) \subset S_4$ $\Big\}$ $\Gamma \cong D_4$

$\tau :=$ komplexe Konjugation:
$\tau(a) = a, \tau(i) = -i$
$\Rightarrow \tau \mapsto (34)$

$\exists \sigma : \sigma(a) = ia$ da Γ transitiv auf Nullstellen von f und $\sigma\tau$
OBdA $\sigma(i) = i$ sonst ersetze σ durch $\sigma\tau$.
$\Rightarrow \sigma \mapsto (1324)$

σ^2: $a \mapsto -a$
$i \mapsto i$
$\Rightarrow \sigma \mapsto (12)(34)$
$\sigma^2\tau \mapsto (12)$

$(14)(23)$: $a + ia \mapsto -ia - a$
$(1+i)a \mapsto -(1+i)a$
$\Rightarrow$ nicht invariant.

$ia^2 = a \cdot (ia)$
$(13)(24)$: $a + ia \mapsto a$
$\Rightarrow a + ia = (1+i)a$ invariant.

$a - ia$ invariant unter $(14)(23)$.
$ia^2 = a \cdot (ia) = -a \cdot (-ia)$
$\Rightarrow ia^2$ invariant bei Γ.
$ia^2 \notin \mathbb{Q}$