$G \subset \mathrm{Aut}(L)$, $K = \mathrm{Fix}(G)$

$[L : \mathrm{Fix}(G)] \geq |G|$

Ungleichheit zu zeigen, verwenden wir die G-Spur:

8.7 Def L Körper, $G \subset \mathrm{Aut}(L)$ endliche Untergruppe, $K = \mathrm{Fix}(G)$. Dann heißt

$$\mathrm{Tr}_G : L \to K, \quad a \mapsto \sum_{\varphi \in G} \varphi(a)$$

die G-Spur von L

Für $\psi \in G$ gilt

$$\psi\Big(\sum_{\varphi \in G} \varphi(a)\Big) = \sum_{\varphi \in G} (\psi \circ \varphi)(a) = \sum_{\varphi \in G} \varphi(a)$$

da mit φ auch $\psi \circ \varphi$ G durchläuft. Also $\mathrm{Tr}_G(a) \in \mathrm{Fix}(G) = K$

$\mathrm{Tr}_G(L) \supsetneq \{0\}$ denn wäre $\mathrm{Tr}_G(a) = 0$ $\forall a \in L$, dann wäre $\sum_{\varphi \in G} \varphi|_{L^\times} = 0 \in \mathrm{Abb}(L^\times, L)$ was der linearen Unabhängigkeit von paarweise verschiedenen Charakteren widerspricht.

Beweis von Satz 8.2 $[L : \mathrm{Fix}(G)] = |G|$

Es bleibt $[L : \mathrm{Fix}(G)] \leq |G|$ zu zeigen. Sei $G = \{\varphi_1, \dots, \varphi_n\}$, $n = |G|$ z.z. ist für $m > n$ sind die m-Elemente $a_1, \dots, a_m \in L$ linear abhängig über $K = \mathrm{Fix}(G)$. Wegen $m > n$ hat das Gleichungssystem

$$\varphi_1^{-1}(a_1)x_1 + \dots + \varphi_1^{-1}(a_m)x_m = 0$$
$$\vdots$$
$$\varphi_n^{-1}(a_1)x_1 + \dots + \varphi_n^{-1}(a_m)x_m = 0$$

eine nichttriviale Lösung $y = \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} \in L^m$

Ist $z \in L$ ein Element $\mathrm{Tr}_G(z) \neq 0$ und $y_e \neq 0$ so können wir y durch $\frac{z}{y_e} y$ ersetzen um $\mathrm{Tr}_G(y_e) \neq 0$ zu erreichen.

$\varphi_1, \dots, \varphi_n$ angewendet liefert

$$a_1\varphi_1(y_1) + \dots + a_m\varphi_1(x_m) = 0$$
$$\vdots$$
$$a_1\varphi_n(y_1) + \dots + a_m\varphi_n(x_m) = 0$$

Aufsummieren gibt $a_1 Tr_G(y_1) + \dots + a_m Tr_G(y_m) = 0$
also wegen $Tr_G(y_\ell)$ sind $a_1, \dots, a_m$ linear abh. über K □

8.8 Satz Ist $L \supset K$ ein Zerfällungskörper eines Polynoms $f \in K[x]$ und sind $\{a_1, \dots, a_r\}$ die paarweise verschiedenen Nullstellen von f in L, dann operiert $Aut(L;K)$ auf $\{a_1, \dots, a_r\}$ durch Permutationen. Die Bahnen der Operation entsprechen dabei eindeutig den irreduziblen Faktoren von f.

Beweis: Sei g ein irreduzibler Faktor von f und etwa a_1 eine Nullstelle von g. Dann ist $\varphi(a_1)$ ebenfalls eine Nullstelle von g, da $g(\varphi(a_1)) = \varphi(g(a_1)) = \varphi(0) = 0$
Also $\varphi(a_1) \in \{a_1, \dots, a_r\}$. Umgekehrt ist
a_ℓ eine weitere Nullstelle von g, dann lässt sich der Automorphismus

$$\begin{array}{ccc} K & \subset & K[a_1] \\ \| & & \wr\| \\ K & \subset & K[a_\ell] = K[x]/(g) \end{array}$$

zu einem Automorphismus von L sukzessive fortsetzen.

$$\begin{array}{l} K \subset K[a_1] \subset K[a_1, a_2] \subset \dots \subset L = K[a_1, \dots, a_r] \\ \| \qquad \wr\| \qquad\qquad\qquad\qquad\qquad \wr\| \\ K \subset K[a_1'] \subset K[a_1', a_2'] \subset \dots \subset L = K[a_1', \dots, a_r'] \end{array}$$

wobei $a_1' = a_\ell$ und a_2' eine Nullstelle des Minimalpolynoms von a_2 über $K[a_1]$ transportiert nach $K[a_1'][x]$ ist usw

8.9 Satz + Def Eine endliche Körpererweiterung $L \supset K$ heißt normal, falls die folgenden äquivalenten Bedingungen erfüllt sind.

1) Für jede endliche Körpererweiterung $M \supset L$ und jeden Automorphismus $\varphi \in Aut(M;K)$ gilt:
$\varphi(L) = L$

2) Jedes irreduzible Polynom $g \in K[x]$ welches in L eine

Nullstelle hat zerfällt über L in Linearfaktoren
3) L ist der Zerfällungskörper eines Polynoms $f \in K[x]$

Bem 1) $M \supset L \supset K$ ein Turm in Körpererweiterung. Dann ist $Aut(M;L) \subset Aut(M;K)$ eine Untergruppe.
Ist $L \supset K$ normal, dann ist wegen 1) die Abbildung

$$Aut(M;K) \longrightarrow Aut(L;K),$$
$$\varphi \longmapsto \varphi|_L$$

ein wohldefinierter Gruppenhomomorphismus. Der Kern dieses Gruppenhomomorphismus ~~bei~~ ist $Aut(M;L)$. Also $Aut(M;L) \subset Aut(M;K)$ ist für $L \supset K$ normal ein Normalteiler.
Daher der Name.

Beweis 1) $\Rightarrow$ 2) Sei $L = K[a_1, \dots, a_n]$ und $b \in L$ und eine Nullst. in g.
Es sei f_k das Minimalpolynom von a_k über K und g ~~das Minpolynom von b~~. Wir betrachten $M \supset L$ den Zerfällungskörper von $f = g f_1 \dots f_n$ über L. Dann ist M auch ein Zerfällungskörper von f über K. Sei b' eine weitere Nullstelle von g. Dann gibt es einen Automorphismus $\varphi \in Aut(M,K)$, der $\varphi(b) = b'$ erfüllt.
Nach 1) liegt $b' \in L$.
Sämtliche Faktoren von $g \in M[x]$ liegen schon in $L[x]$, also g zerfällt schon über $L[x]$.
2) $\Rightarrow$ 3). Es sei $L = K[a_1, \dots, a_n]$, $f_1, \dots, f_n$ die Minimalpolynome von $a_1, \dots, a_n$. Nach 2) zerfällt $f = f_1 \dots f_n$ über L in Linearfaktoren
Also L ist ein Zerfällungskörper von f über K.
3) $\Rightarrow$ 1) Sei L ~~der~~ ein Zerfällungskörper von $f \in K[x]$ und $M = L[b_1, \dots, b_m]$. Es seien $g_1, \dots, g_m$ die Minimalpolynome von $b_1, \dots, b_m$ über K und $\bar{M}$ der Zerfällungskörper von $g_1 \dots g_m$ über M.

Dann M der Zerfällungskörper von $f g_1 \cdots g_m$. Sind $c_1, \dots, c_r$ die Nullstellen dieses Polynoms in M dann lässt sich jeder Automorphismus $\varphi \in \mathrm{Aut}(M, K)$ entlang des Turms

$$\begin{array}{ccccccc} M & \subseteq & M[c_1] & \subseteq \dots \subseteq & M[c_1, \dots, c_r] & = & M \\ \varphi \downarrow & & \wr\wr & & \varphi \quad \wr\wr & & \\ K_1 & \subset & M[c_1'] & \dots \subset & \tilde{M} & & \end{array}$$

zu einem Automorphismus φ fortsetzen.

Da $L = K[a_1, \dots, a_n]$ ein Zerfällungskörper von f über K ist gilt $\varphi(a_i) \in L$ also $\varphi_{|L} = \varphi|_L \in \mathrm{Aut}(L; K)$ d.h. $\varphi(L) = L$ $\square$

8.10 <u>Def</u> K Körper $f \in K[x]$ ein nicht konstantes Polynom. f heißt separabel über K, wenn jeder irreduzible Faktor g von f in seinem Zerfällungskörper nur einfache Nullstellen hat. Äquivalent wenn $\mathrm{ggT}(g, g') = 1$

Sei $L \supset K$ eine algebraische Körpererweiterung. (lokale Abl vorig)

$a \in L$ heißt separabel, wenn das Minimalpolynom von a über K separabel ist.

$L \supset K$ heißt separabel, wenn jedes Element $a \in L$ separabel ist

<u>Bem</u> Ist $f = \lambda f_1^{\nu_1} \cdots f_r^{\nu_r}$ die Faktorisierung von f in paarweise verschiedene Faktoren, $\lambda \in K$ der Leitkoeffizient, dann stimmt der Zerfällungskörper von f mit dem von $f_1 \cdots f_r$ überein. Ist f separabel dann $f_1 \cdots f_r$ separabel und demzufolge ein Polynom, das über seinem Zerfällungskörper $L \supset K$ ~~in das $(f_1, \dots, f_r)$~~ keine mehrfachen Nullstellen hat. Für solche Polynome haben wir $[L;K] = \mathrm{Aut}(L;K)$ gezeigt und deshalb

$$\mathrm{Fix}(\mathrm{Aut}(L;K)) = K$$

$L \supset K$ ist also eine Galoiserweiterung. Dies zeigt die Implikation $2) \Rightarrow 1)$ in folgendem Satz.

8.11 Satz Sei $L \supset K$ eine Körpererweiterung. Äquivalent sind 1) $L \supset K$ ist Galoisch 2) $L \supset K$ ist endlich, normal und separabel 3) L ist der Zerfällungskörper eines separablen Polynoms.

Beweis 1) ⇒ 2)

Sei $G \subset \mathrm{Aut}(L)$ endliche Gruppe mit $K = \mathrm{Fix}(G)$.

Dann gilt $[L:K] = |G|$, $L \supset K$ ist also endlich

Sei $a \in L$ und $\underbrace{\{a_1, \dots, a_r\}}_{= Ga = \{\varphi(a) \mid \varphi \in G\}}$ die Bahn von a unter G, $a_1, \dots, a_r$ paarweise verschieden. Ist $\varphi \in G$ ein Automorph. dann gilt $\{\varphi(a_1), \dots, \varphi(a_r)\} = \{a_1, \dots, a_r\}$ da G transitiv auf der Bahn operiert.

Sei $f = \prod_{i=1}^{r} (x - a_i)$. Wenden φ auf Koeffizienten des Polynoms an, so erhalten wir

$$\varphi(f) = \prod_{i=1}^{r} (x - \varphi(a_i)) = \prod_{i=1}^{r} (x - a_i) = f$$

Die Koeffizienten von f sind also invariant unter $\varphi \in G$ also liegen sie in

$$\mathrm{Fix}(G) = K$$

f stimmt also mit Minimalpolynom von a über K überein da mit a auch ~~gleich~~ jedes Element $\varphi(a)$ eine Nullstelle d. Minimalpolynoms ist.

~~Da $a \in L$ beliebig war~~ Also $a \in L$ ist separabel über K.

Ferner jedes irreduzible Polynom f, dass in L eine Nullstelle hat zerfällt über L in Linearfaktoren. $L \supset K$ ist auch normal.

2) ⇒ 3) Da L eine endliche normale Körpererweiterung ist, ist L Zerfällungskörper eines Polynoms.

Dieses ist separabel, da $L \supset K$ separabel ist.

3) ⇒ 1) haben wir schon eingesehen. □

8.12 Korollar Sei $L = K[a_1, \dots, a_n] \supset K$ eine algebr. Körpererweiterung mit $a_1, \dots, a_n$ separabel über K. Dann ist $L \supset K$ separabel.

Beweis Es seien $f_1, \dots, f_n$ die Minimalpolynome von $a_1, \dots, a_n$ über K und $\bar{L}$ der Zerfällungskörper von $f = f_1 \cdots f_n$ über L. Dann $\bar{L}$ auch Zerfällungskörper von f über K. Da f separabel ist, ist $\bar{L} \supset K$ galoisch und daher jedes Element $a \in L \subset \bar{L}$ separabel über K. $\square$

8.13 Hauptsatz der Galoistheorie

Es sei $K \subset L$ eine Galoiserweiterung mit Gruppe $G = \mathrm{Aut}(L; K)$. Es sei

$$\mathcal{Z} = \{ Z \mid K \subset Z \subset L \text{ ist Zwischenkörper} \}$$

die Menge der Zwischenkörper und

$$\mathcal{H} = \{ H \subset G, H \text{ Untergruppe} \}$$ die Menge der Untergruppen von G.

Dann induzieren die Abbildungen $\mathrm{Aut}(L; \_): \mathcal{Z} \to \mathcal{H}$, $Z \mapsto \mathrm{Aut}(L; Z)$,

$\mathrm{Fix}(\_): \mathcal{H} \to \mathcal{Z}$, $H \mapsto \mathrm{Fix}(H)$ zueinander inverse inklusionsumkehrende Bijektionen.

Für ein Paar H, Z, $H = \mathrm{Aut}(L; Z)$, $Z = \mathrm{Fix}(H)$ gilt

$$[L : Z] = |H|$$

$$[Z : K] = [G : H]$$

und $L \supset Z$ ist galoisch mit Gruppe H.

Für $\varphi \in \mathrm{Aut}(L; K) = G$ ~~und $Z \in \mathcal{Z}$~~ gilt

$\mathrm{Aut}(L, \varphi(Z)) = \varphi H \varphi^{-1}$

Schließlich $Z \supset K$ ist galoisch genau dann, wenn $H \subset G$ ein Normalteiler ist und in diesem Fall ist die Galoisgruppe $\mathrm{Aut}(Z; K) \cong G/H$

<u>Beweis</u>: Da $L \supset K$ galoisch, ist L der Zerfällungskörper eines separablen Polynoms $f \in K[x]$.
Für jeden Zwischenkörper Z ist dann L auch der Zerfällungskörper von $f \in Z[x]$. Also auch $L \supset Z$ ist galoisch mit Galoisgruppe $H = Aut(L; Z)$ und daher $Z = Fix(H)$
Also $Fix(Aut(L; Z)) = Z$, und umgekehrt $H \in \mathcal{H}$
$Z = Fix(H)$, $Aut(L; Fix(H)) = H$.
die Abbildungen sind zueinander inverse.
inklusionsumkehrend ist klar, da
$Z_1 \subset Z_2 \Rightarrow Aut(L; Z_2) \subset Aut(L; Z_1)$ jeder Automorphismus der Z_2 festhält, hält auch die Teilmenge Z_1 fest.
$H_1 \subset H_2 \Rightarrow Fix(H_1) \supset Fix(H_2)$, da die Elemente $a \in L$, die von H_2 festgehalten werden erst recht von H_1 festgehalten werden.
$[L:Z] = |H|$ gilt für jede Galoiserweiterung
$[Z:K] = [G:H]$ folgt aus

$$\underbrace{[L:Z]}_{=H}[Z:K] = [L:K] = |G| = [G:H] \cdot |H|$$

$\varphi \in Aut(L; K) = G$; dann lässt jedes Element von $\varphi H \varphi^{-1}$ den Zwischenkörper $\varphi(Z) \subset L$ fest: ist $a \in \varphi(Z)$ etwa $a = \varphi(b)$ und $\varphi H \varphi^{-1} = \varphi h \varphi^{-1}$ $h \in H$, so gilt

$$(\varphi h \varphi^{-1})(a) = \varphi h \varphi^{-1} \varphi(b) = \varphi h(b) = \varphi(b) = a$$

Also $\varphi H \varphi^{-1} \subset Aut(L; \varphi(Z))$
Da $|Aut(L; \varphi(Z))| = |Aut(\varphi(L); \varphi(Z))|$
$= |Aut(L; Z)|$
und $|\varphi H \varphi^{-1}| = |H|$ gilt Gleichheit.

Ist $Z \supset K$ galoisch $\Rightarrow$ $Z \supset K$ ist normal und daher $\varphi(Z) = Z$ $\forall \varphi \in Aut(L;K)$. Der Gruppenhomom.

$$Aut(L;K) \to Aut(Z,K)$$
$$\varphi \mapsto \varphi(Z)$$

ist dann definiert und hat $Aut(L;Z)$ als Kern, also $H \subset G$ ist ein Normalteiler. Umgekehrt ist $H \subset G$ ein Normalteiler, dann

$\varphi(Z) = Fix(\varphi H \varphi^{-1}) = Fix(H) = Z$ und der obige Gruppenhomomorphismus existiert auch in diesem Fall.

Da $[Aut(L;K) : Aut(L;Z)] = [Z:K]$ hat das Bild von $Aut(L;K) \to Aut(Z;K)$, $\varphi \mapsto \varphi|_Z$

Ordnung $[Z:K]$. Der Fixkörper unter der Bildgruppe hat also Index $[Z : Fix(Bild\, \mathcal{G})] = [Z:K]$

$\Rightarrow K = Fix(Bild\, \mathcal{G})$ und $\mathcal{G}$ ist surjektiv und $Z \supset K$ galoisch.

Nach dem Homomorphiesatz folgt

$$Aut(Z;K) \cong G/H = \frac{Aut(L;K)}{Aut(L;Z)} \qquad \square$$

<u>8.14 Beispiel</u> $f = x^4 - x^2 + 1 \in \mathbb{Q}[x]$

1) f ist irreduzibel: Lineare Faktoren kommen nicht in Frage, da ± 1 keine Nullstellen sind.

Angenommen, $x^4 + x^2 - 1 = (x^2 + ax + 1)(x^2 + bx - 1)$

dann Koeffizientenvergleich

$$\left.\begin{array}{ll} (x^3) & 0 = a+b \\ (x) & 0 = b-a \end{array}\right\} a = b = 0$$

$$x^2 \quad -1 = ab \quad \lightning$$

2) Benutzung der Wurzeln Substitution $y = x^2$ und Lösen zunächst $y^2 - y - 1 = 0$

$$y_{1,2} = \frac{1}{2} \pm \sqrt{\frac{1}{4} + 1} = \frac{1}{2}(1 \pm \sqrt{5})$$

$a_1 = \frac{\sqrt{1+\sqrt{5}}}{\sqrt{2}}$, $a_2 = -\frac{\sqrt{1+\sqrt{5}}}{\sqrt{2}}$, $a_3 = \frac{\sqrt{1-\sqrt{5}}}{\sqrt{2}}$

$a_4 = \frac{-\sqrt{1-\sqrt{5}}}{\sqrt{2}}$

$[\mathbb{Q}[a_1] : \mathbb{Q}] = 4$, da f irreduzibel ist.

Da $a_1^2 = \frac{1+\sqrt{5}}{2}$, gilt $\frac{1-\sqrt{5}}{2} \in \mathbb{Q}[a_1]$

$[\mathbb{Q}[a_1, a_3] : \mathbb{Q}[a_1]] \leq 2$

Es gilt Gleichheit, da $\mathbb{Q}[a_1] \subset \mathbb{R}$ aber $a_3 \notin \mathbb{R}$, da $1-\sqrt{5} < 0$. Es folgt

$[\mathbb{Q}[a_1, a_3] : \mathbb{Q}] = 8$ und $\mathbb{Q}[a_1, a_3]$ ist der Zerfällungskörper von f

3) Die Galoisgruppe $G = Gal(f)$ ist eine Untergruppe der S_4 von der Ordnung 8, also eine der 2-Sylow-Untergruppen von S_4

$\Longrightarrow G \cong D_4$ Symmetriegruppe des regulären 4-Ecks (Quadrat) □

4) Beschreibung von G als Permutationsgruppe von $\{a_1, \dots, a_4\}$. id auf $\mathbb{Q}[a_3]$ lässt sich auf zwei Weisen zu einem $p \in G$ fortsetzen

id $\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_1 & a_2 & a_4 & a_3 \end{pmatrix} = (34)$

Ebenso lässt sich $\begin{pmatrix} a_1 & a_2 \\ a_2 & a_1 \end{pmatrix}$ auf zwei Weisen

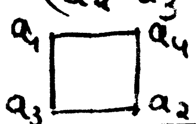
fortsetzen $\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_1 & a_3 & a_4 \end{pmatrix} = (12)$ $\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_1 & a_4 & a_3 \end{pmatrix} = (12)(34)$

Der Isomorphismus $\mathbb{Q}[a_1] \cong \mathbb{Q}[a_3]$ mit $a_1 \mapsto a_3$ lässt sich auf 2 Weisen fortsetzen

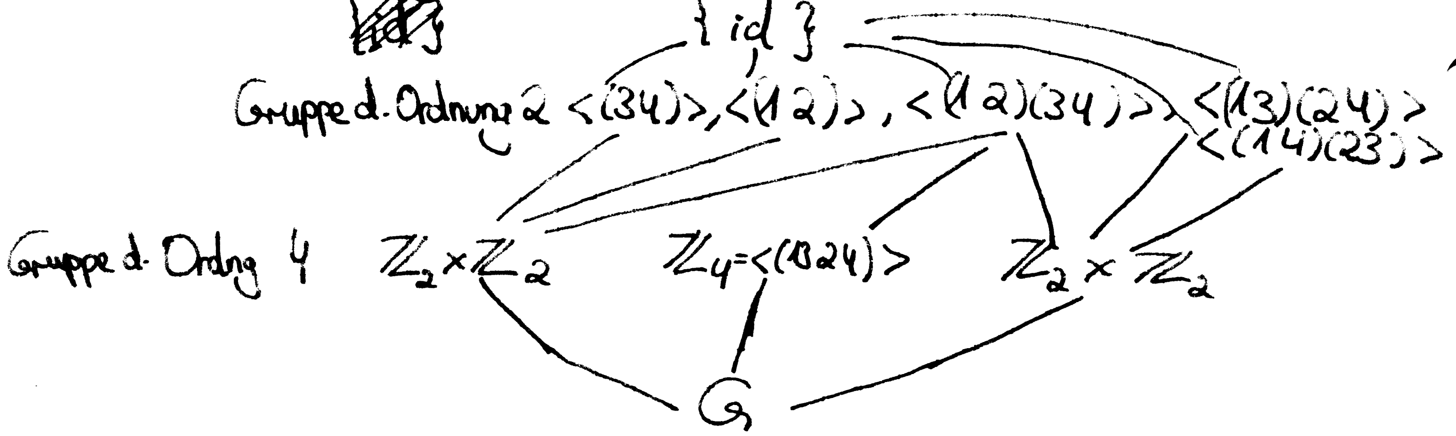
$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_1 & a_2 \end{pmatrix} = (13)(24)$ oder $\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_2 & a_1 \end{pmatrix} = (1324)$

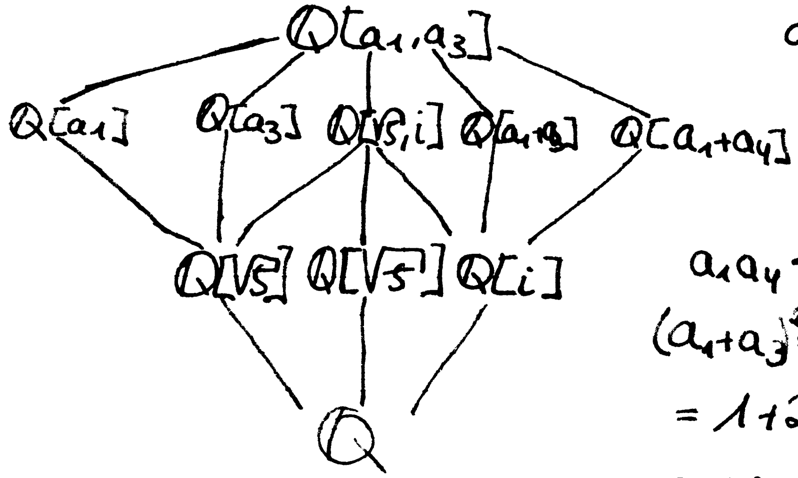
$\mathbb{Q}[a_1] \Rightarrow \mathbb{Q}[a_3]$, $a_1 \mapsto a_3 = a_4$ setzt sich fort zu

$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_3 & a_2 & a_1 \end{pmatrix} = (14)(23)$, $\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_3 & a_1 & a_2 \end{pmatrix} = (1423)$



5) Untergruppen und Unterkörperverband





$a_1a_3 = a_2a_4$
$= \frac{\sqrt{1+\sqrt5}}{\sqrt2}\,\frac{\sqrt{1-\sqrt5}}{\sqrt2} = \frac{\sqrt{1-5}}{2}$
$= \frac{\sqrt{-4}}{2} = \sqrt{-1} = i$

$a_1a_4 - a_2a_3 = -i$

$(a_1+a_3)^2 = \frac{1+\sqrt5}{2} + \frac{1-\sqrt5}{2} + 2i$
$= 1+2i$

$a_1+a_3 \notin \mathbb{Q}[i]$.

Minimalpolynom von a_1+a_3: $(x^2-1)^2 = -4$,
$x^4 - 4x^2 + 5 = 0$

Koeff. vergl. $(x^2+ax \pm 5)(x^2+bx \pm 1)$

$(x^2+5)(x^2+1)$
$(x^2-5)(x^2-1) \neq x^4-4x^2+5$

Nur $\mathbb{Q}[\sqrt5, i]$ ist Galoisch mit Gruppe
$D_4 / \langle (12)(34) \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$