Bevor wir 1.5, den Hauptsatz der Galoistheorie, beweisen, betrachten wir ausführlich ein großes Beispiel, in dem wir auch $\mathcal{U}$, $\mathcal{Z}$, α und β bestimmen. was war nochmal $\mathcal{U}$, $\mathcal{Z}$, α und β?

Sei $K = \mathbb{Q}$ und L der Zerfällungskörper von $f(x) = x^4 - 2 \in \mathbb{Q}[x]$.

In $L \subset \mathbb{C}$ liegen die vier Nullstellen $\pm\sqrt[4]{2} \in \mathbb{R}$ und $\pm i \cdot \sqrt[4]{2}$

Einen Zwischenkörper können wir erraten: $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$, also $L \supset \mathbb{Q}(\sqrt[4]{2}) \supset \mathbb{Q}$. Diesen benutzen wir, um $[L:\mathbb{Q}]$ mit der Gradformel zu berechnen: $\pm i \sqrt[4]{2} \notin \mathbb{R} \Rightarrow \mathbb{Q}(\sqrt[4]{2}) \subsetneq L$.

Außerdem ist $\pm i = \pm i\sqrt[4]{2} / \sqrt[4]{2} \in L$. $\Rightarrow L = \mathbb{Q}(\sqrt[4]{2}, i)$

$\mathbb{Q}(\sqrt[4]{2})$ ist eine einfache Erweiterung, deshalb suchen wir das Minimalpolynom von $\sqrt[4]{2}$.

$f(x) = x^4 - 2$ ist irreduzibel über $\mathbb{Q}$: ist das Kriterium von Eisenstein anwendbar?

Verwende z.B. Reduktion modulo 3:

$x^4 - 2 \in \mathbb{F}_3[x]$ hat keine Nullstellen (warum nicht?)

$\Rightarrow$ könnte nur in ein Produkt zweier quadratischer Polynome faktorisiert werden, also $(x^2+ax+b)(x^2+cx+d) \rightsquigarrow$ Gleichungen für a,b,c,d ↯ Details?

Noch ein Argument: Polynomdivision $\Rightarrow$ über $\mathbb{R}$ zerfällt f in

$$x^4 - 2 = \underbrace{(x-\sqrt[4]{2})(x+\sqrt[4]{2})}_{x^2-\sqrt{2}}(x^2+\sqrt{2})$$

$\Rightarrow$ Faktoren in einer Zerlegung über $\mathbb{Q}$ müssen Produkte dieser Faktoren sein warum?

Aber das geht nicht ↯

Ergebnis: $f(x) = x^4 - 2$ ist irreduzibel in $\mathbb{Q}[x] \Rightarrow \mathbb{Q}(\sqrt[4]{2}) \cong \mathbb{Q}[x]/(x^4-2)$

$f(x) = m_{\sqrt[4]{2},\mathbb{Q}}(x)$, Grad 4 $\Rightarrow [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$

Als nächstes: $[L = \mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] = ?$

i hat über $\mathbb{Q}$ Minimalpolynom $m_{i,\mathbb{Q}}(x) = x^2+1$. Wegen $m_{i,\mathbb{Q}(\sqrt[4]{2})}(x) \mid m_{i,\mathbb{Q}}(x)$ und $i \notin \mathbb{Q}(\sqrt[4]{2})$ muß $m_{i,\mathbb{Q}(\sqrt[4]{2})} = m_{i,\mathbb{Q}}$ gelten

$m_{i,\mathbb{Q}}(x) = x^2+x+1$, Grad 2 $\Rightarrow [L : \mathbb{Q}(\sqrt[4]{2})] = 2$

Ergebnis: $[L:\mathbb{Q}] = [L : \mathbb{Q}(\sqrt[4]{2})] \cdot [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}]$
$= 2 \cdot 4 = 8$

$\operatorname{char} \mathbb{Q} = \operatorname{char} L = 0 \Rightarrow [L:\mathbb{Q}]$ ist separabel
L Zerfällungskörper $\Rightarrow L/\mathbb{Q}$ normal
Insgesamt also: $L/\mathbb{Q}$ Galoiserweiterung
Also: $\operatorname{Aut}_{\mathbb{Q}}(L) = \operatorname{Gal}(L/\mathbb{Q})$, $|\operatorname{Gal}(L/\mathbb{Q})| = [L:\mathbb{Q}] = 8$
Aus Algebra kennen wir alle Gruppen der Ordnung 8. Bis auf Isomorphie gibt es drei abelsche Gruppen nämlich?
und zwei nichtabelsche: eine Diedergruppe (welche genau?)
und die Quaternionengruppe
Wir versuchen, die acht $\mathbb{Q}$-Automorphismen von L zu bestimmen.
Dabei können wir zwei Ketten von Erweiterungen verwenden

$$\underbrace{L \supset \mathbb{Q}(\sqrt[4]{2})}_{4} \underbrace{\supset \mathbb{Q}}_{2} \quad \text{und} \quad \underbrace{L \supset \mathbb{Q}(i)}_{?} \underbrace{\supset \mathbb{Q}}_{?}$$

Wie sehen die $\mathbb{Q}$-Automorphismen von $\mathbb{Q}(\sqrt[4]{2})$ aus?
$\varphi: \mathbb{Q}(\sqrt[4]{2}) \to \mathbb{Q}(\sqrt[4]{2})$ schickt $\sqrt[4]{2}$ auf eine Nullstelle von x^4-2, die auch in $\mathbb{Q}(\sqrt[4]{2})$ liegt, also $\pm\sqrt[4]{2}$. Dadurch ist φ festgelegt.
$\varphi: \sqrt[4]{2} \mapsto \sqrt[4]{2}$ ist die Identität. $\mathrm{Id}: L \to L$ ist natürlich ein Automorphismus.
Zu welchem Automorphismus von L, wenn es einen gibt, $\varphi: \sqrt[4]{2} \to -\sqrt[4]{2}$ gehört, wissen wir noch nicht. Auch nicht, ob vielleicht mehrere Automorphismen von L zu diesem φ einschränken.
Wie sehen die $\mathbb{Q}$-Automorphismen von $\mathbb{Q}(i)$ aus? $\mathbb{Q}(i)/\mathbb{Q}$ ist eine Galoiserweiterung. Es gibt zwei Automorphismen $\psi: \mathbb{Q}(i) \to \mathbb{Q}(i)$. Einer ist die Identität, der andere ist $\psi: i \mapsto -i$. Das ist die Einschränkung der komplexen Konjugation $z \mapsto \bar{z}$ auf $\mathbb{Q}(i)$. woher wissen wir das? (mehrere Begründungen möglich)
Das hilft uns zunächst nicht viel.
Aber wir können auch noch die anderen beiden Erweiterungen betrachten, z.B. $L/\mathbb{Q}(i)$. Das sieht erstmal schwieriger aus, hat aber einen großen Vorteil: Nach Definition ist $\operatorname{Aut}_{\mathbb{Q}(i)}(L) \subset \operatorname{Aut}_{\mathbb{Q}}(L)$ warum?
$ \| $
Elemente in $\operatorname{Aut}_{\mathbb{Q}(i)}(L)$ liefern also $\quad \operatorname{Gal}(L/\mathbb{Q})$
sofort Elemente in $\operatorname{Gal}(L/\mathbb{Q})$

$L = \mathbb{Q}(\sqrt[4]{2}, i) = (\mathbb{Q}(i))(\sqrt[4]{2})$ und $[L : \mathbb{Q}(i)] = 4 \Rightarrow \sqrt[4]{2}$ hat Grad 4 über $\mathbb{Q}(i)$, d.h. $x^4 - 2$ bleibt irreduzibel über $\mathbb{Q}(i)$

L ist Zerfällungskörper von $x^4 - 2$ über $\mathbb{Q}(i)$ warum?

also normal, und separabel $\Rightarrow L / \mathbb{Q}(i)$ ist eine Galoiserweiterung folgt das aus 1.5?

$Gal(L/\mathbb{Q}(i)) = Aut_{\mathbb{Q}(i)}(L)$ hat also 4 Elemente, die dann auch Elemente in $Aut_{\mathbb{Q}}(L)$ sind.

$\sigma \in Gal(L/\mathbb{Q}(i))$ ist durch $\sigma(\sqrt[4]{2})$ festgelegt, dafür gibt es vier Möglichkeiten. Da es auch 4 solche σ gibt, kommt jede Wahl von $\sigma(\sqrt[4]{2})$ auch vor.

Zum Beispiel $\sigma : \sqrt[4]{2} \to i\sqrt[4]{2}$ muß existieren. $\sigma \in Aut_{\mathbb{Q}(i)}(L)$, d.h. $\sigma(i) = i$.

Mit σ finden wir gleich weitere Elemente: $\sigma^2, \sigma^3, \sigma^4$ – (endlich viele).

$\sigma : i \mapsto i, \ \sqrt[4]{2} \mapsto i\sqrt[4]{2} \quad \Rightarrow \sigma^n : i \mapsto i \ \forall n$

$\sigma^2 : \sqrt[4]{2} \mapsto i\sqrt[4]{2} \mapsto i \cdot i \sqrt[4]{2} = -\sqrt[4]{2}$

$\sigma^3 : \sqrt[4]{2} \longmapsto -i\sqrt[4]{2}$

$\sigma^4 : \sqrt[4]{2} \longmapsto -i^2\sqrt[4]{2} = \sqrt[4]{2}, \ \sigma^4(i) = i \Rightarrow \sigma^4 = \text{Identität}$ warum ist das ohne Rechnung klar?

Sei $H = \langle\sigma\rangle$ die von σ erzeugte Untergruppe von $Gal(L/\mathbb{Q})$. ($H = Gal(L/\mathbb{Q}(i))$ nach Konstruktion)

H ist zyklisch von Ordnung 4, also $H \cong \mathbb{Z}/4\mathbb{Z}$ was sagt 1.5 dazu?

$[Gal(L/\mathbb{Q}) : H] = \frac{8}{4} = 2 \Rightarrow H$ ist normale Untergruppe, $H \trianglelefteq Gal(L/\mathbb{Q})$, es gibt zwei Nebenklassen, H und eine weitere, in der die restlichen Elemente von $Gal(L/\mathbb{Q})$ liegen müssen

$Gal(L/\mathbb{Q})/H$ ist eine Gruppe (warum?) mit 2 Elementen, also $\cong \mathbb{Z}/2\mathbb{Z}$

Kann man mit $L/\mathbb{Q}(\sqrt[4]{2})$ Ähnliches erwarten?

Wir brauchen ein Element in $Gal(L/\mathbb{Q})$, der nicht in H liegt. Da bietet sich die komplexe Konjugation τ an: $z \mapsto \bar{z}$. τ bildet L auf L ab und läßt $\mathbb{Q}(\sqrt[4]{2})$ punktweise fest, liegt also in $\underset{\{Id, \tau\}}{\overset{\text{warum}}{Aut_{\mathbb{Q}(\sqrt[4]{2})}(L)}} \subset Aut_{\mathbb{Q}}(L) = Gal(L/K)$

$\sigma(i) = i \Rightarrow \tau \notin H = \langle\sigma\rangle$

Ergebnis: $G = Gal(L/\mathbb{Q})$

$\quad = H \,\dot\cup\, \tau \circ H \ (= H \,\dot\cup\, H \circ \tau)$ (Nebenklassen)

$\Rightarrow G = H \,\dot\cup\, \{\tau, \tau\circ\sigma, \tau\circ\sigma^2, \tau\circ\sigma^3\}$, damit sind die Elemente von G bestimmt

Genauer:	$\sqrt[4]{2}$	i		
τ	$\sqrt[4]{2}$	$-i$		
$\tau\circ\sigma$	$-i\sqrt[4]{2}$	$-i$	$\sigma^3\circ\tau = \tau\circ\sigma$	
$\tau\circ\sigma^2$	$-\sqrt[4]{2}$	$-i$	$\sigma^2\circ\tau = \tau\circ\sigma^2$	nachrechnen
$\tau\circ\sigma^3$	$i\sqrt[4]{2}$	$-i$	$\sigma\circ\tau = \tau\circ\sigma^3$	

Insbesondere: $\sigma^4 = \mathrm{Id} = \tau^2$, $\tau = \tau^{-1}$; $\tau\circ\sigma\circ\tau = \sigma^3 = \sigma^{-1}$

$\Rightarrow$ G ist die Diedergruppe D_8, die Symmetriegruppe des Quadrats

welche Elemente sind Drehungen, welche sind Spiegelungen?

Jetzt kommt der zweite Teil des Beispiels: Wir bestimmen die Untergruppen von $G = \mathrm{Gal}(L|\mathbb{Q})$, die Inklusionen zwischen diesen, und danach die Körper zwischen $\mathbb{Q}$ und L als Fixkörper der Untergruppen.

$|G| = 8 \Rightarrow$ mögliche Untergruppen U haben Ordnung 1, 2, 4 oder 8

$|U| = 1 \Rightarrow U = \{\mathrm{Id}\}$, $|U| = 8 \Rightarrow U = G$

$|U| = 2 \Rightarrow U = \{\mathrm{Id}, g\}$ mit $g^2 = \mathrm{Id}$, d.h. g Spiegelung

Das sind alle $g \in G - \{\mathrm{Id}, \sigma, \sigma^3\}$ nachprüfen

welche Spiegelung fehlt hier?

Also gibt es 5 Untergruppen der Ordnung 2

$$I_1 = \{\mathrm{id}, \sigma^2\},\ I_2 = \{\mathrm{id}, \tau\},\ I_3 = \{\mathrm{id}, \sigma\circ\tau\},\ I_4 = \{\mathrm{id}, \sigma^2\circ\tau\},\ I_5 = \{\mathrm{id}, \sigma^3\circ\tau\}$$

$|U| = 4$: Wir kennen schon $H_1 = H = \langle\sigma\rangle = \langle\sigma^3\rangle$ zyklisch der Ordnung 4

Weitere Untergruppen der Ordnung 4?

Gruppen der Ordnung 4 sind abelsch (in Algebra-Skript nachschauen)

Genauer: $\mathbb{Z}/4\mathbb{Z}$ oder $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (bis auf Isomorphie)

Falls $U \cong \mathbb{Z}/4\mathbb{Z}$: $U = \langle g\rangle$ mit $\mathrm{ord}(g) = 4$. Aber nur σ und σ^3 haben Ordnung 4. Also bleibt nur $U \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \Rightarrow U = \langle a, b : a^2 = b^2 = \mathrm{id}, ab = ba\rangle =$
$= \{\mathrm{id}, a, b, ab = ba\}$

z.B. $a = \tau$, $b = \sigma^2$ oder $a = \tau\circ\sigma$, $b = \sigma\circ\tau$ nachprüfen

Weitere Paare a, b gibt es nicht nachprüfen

Also erhalten wir noch $H_2 = \{\mathrm{id}, \sigma^2, \tau, \sigma^2\circ\tau = \tau\circ\sigma^2\}$

und $H_3 = \{\mathrm{id}, \sigma^2, \tau\circ\sigma = \sigma^2\circ\tau, \tau\circ\sigma^3 = \sigma\circ\tau\}$

Damit sind alle Untergruppen bestimmt und die Inklusionen direkt ablesbar:

U

$$
\begin{tikzcd}
 & & G = \mathrm{Gal}(L/\mathbb{Q}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & & \\
 & H_2 = \{id, \sigma^2, \tau, \sigma^2\circ\tau\} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & H_1 = \{id, \sigma, \sigma^2, \sigma^3\} \arrow[d, dash] & H_3 = \{id, \sigma^2, \tau\circ\sigma, \tau\circ\sigma^3\} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
Z_4 = \{id, \tau\circ\sigma^2\} \arrow[drr, dash] & Z_2 = \{id, \tau\} \arrow[dr, dash] & Z_1 = \{id, \sigma^2\} \arrow[d, dash] & Z_3 = \{id, \sigma\circ\tau\} \arrow[dl, dash] & Z_5 = \{id, \sigma^3\circ\tau\} \arrow[dll, dash] \\
 & & \{id\} & &
\end{tikzcd}
$$

(Striche bedeuten Inklusionen.) stimmt das Diagramm

Der Hauptsatz der Galoistheorie sagt, daß ein analoges Diagram für Z gibt, wobei die Inklusionen umgedreht sind.

Ganz oben steht $L^G = \mathbb{Q}$ (warum?), ganz unten $L^{\{id\}} = L$. Alle anderen Fixkörper müssen wir erraten oder berechnen.

Bestimmung von L^{H_1}: $|H_1| = 4$. Proposition 1.4 $\Rightarrow [L : L^{H_1}] = |H_1| = 4$

$K = \mathbb{Q}$, $\dim_{\mathbb{Q}} L = 8$, $\underset{\mathbb{Q}}{\overset{}{K}} \subset \underbrace{L^{H_1} \subset L}_{4} \Rightarrow [L^{H_1} : \mathbb{Q}] = 2$

$H_1 = \langle \sigma \rangle$, $\sigma(i) = i \Rightarrow i \in L^{H_1}$

$\Rightarrow \mathbb{Q}(i) \subset L^{H_1}$, aber $[\mathbb{Q}(i) : \mathbb{Q}] = 2 = [L^{H_1} : \mathbb{Q}] \Rightarrow \boxed{L^{H_1} = \mathbb{Q}(i)}$

Bestimmung von L^{H_2}: wieder zweidimensional über $\mathbb{Q}$ weil $2 = \frac{8}{4}$ genauer?

$H_2 = \langle \tau, \sigma^2 \rangle$. Hier ist es nicht so leicht, ein unter H_2 invariantes Element zu erraten. Deshalb gehen wir zu Fuß:

Ein Element $a \in L$ ist eine $\mathbb{Q}$-Linearkombination von Basiselementen, Invarianz unter H_2, d.h. unter τ und σ^2 bedeutet Gleichungen an die Koeffizienten.

Als Basis wählen wir $1, \sqrt[4]{2}, \sqrt{2}, \sqrt[4]{8}, i, i\sqrt[4]{2}, i\sqrt{2}, i\sqrt[4]{8}$ warum ist das eine Basis?

$\rightsquigarrow a = \lambda_1 \cdot 1 + \lambda_2 \sqrt[4]{2} + \lambda_3 \sqrt{2} + \lambda_4 \sqrt[4]{8} + \lambda_5 i + \lambda_6 i \sqrt[4]{2} + \lambda_7 i \sqrt{2} + \lambda_8 i \sqrt[4]{8}$

$(\lambda_1, \ldots, \lambda_8 \in \mathbb{Q})$ $\quad a \in L^{H_1} \Leftrightarrow \tau(a) = a = \sigma^2(a)$

$\tau : \sqrt[4]{2} \longmapsto \sqrt[4]{2}, i \longmapsto -i \rightsquigarrow \tau(a) = \lambda_1 \cdot 1 + \lambda_2 \sqrt[4]{2} + \lambda_3 \sqrt{2} + \lambda_4 \sqrt[4]{8}$
$\qquad - \lambda_5 i - \lambda_6 i \sqrt[4]{2} - \lambda_7 i \sqrt{2} - \lambda_8 i \sqrt[4]{8}$

Koeffizientenvergleich: $a = \tau(a) \Leftrightarrow \lambda_5 = \lambda_6 = \lambda_7 = \lambda_8 = 0$

Analog für $a = \sigma^2(a)$, ~~denn~~ mit $\sigma^2 : \sqrt[4]{2} \mapsto -\sqrt[4]{2}$

Für $a = \tau(a)$ ist $\sigma^2(a) = \lambda_1 \cdot 1 - \lambda_2 \sqrt[4]{2} + \lambda_3 \sqrt{2} - \lambda_4 \sqrt[4]{8}$

Koeffizientenvergleich $\Rightarrow \lambda_2 = \lambda_4 = 0$ nötig für $a = \sigma^2(a)$

1 ist (wie immer) H_2-invariant und $\sqrt{2}$ auch $\Rightarrow \boxed{L^{H_2} = \mathbb{Q}(\sqrt{2})}$

Bestimmung von L^{H_3}: auch zwei-dimensional

$H_3 = \langle \sigma^2, \sigma \circ \tau \rangle : \sigma^2(i) = i,\ \sigma^2(\sqrt[4]{2}) = -\sqrt[4]{2},\ \sigma \circ \tau : i \mapsto -i,\ \sqrt[4]{2} \mapsto i\sqrt[4]{2}$

wie bei H_2 Gleichungen aufstellen $\Rightarrow 1, i\sqrt{2}$ sind H_3-invariant nachvollziehen

Probe: $\sigma \circ \tau : i(\sqrt[4]{2})^2 \mapsto -i \cdot i^2 (\sqrt[4]{2})^2 \;(= i(\sqrt[4]{2})^2)$

$\sigma^2 : i(\sqrt[4]{2})^2 \mapsto i \cdot (-\sqrt[4]{2})^2$

$\Rightarrow \boxed{L^{H_3} = \mathbb{Q}(i\sqrt{2})}$

weitere Probe: das ist wirklich eine quadratische Erweiterung von $\mathbb{Q}$, denn $(i\sqrt{2})^2 = -2$, also ist $i\sqrt{2}$ Nullstelle von x^2+2 ist das der Minimalpolynom?

Mit der gleichen Methode kann man auch die Fixkörper von $J_1, \dots, J_5$ berechnen.

Der Hauptsatz 1.5 vereinfacht die Situation aber deutlich:

J_1 ist eine Untergruppe von H_1, H_2 und $H_3 \overset{1.5}{\Rightarrow}$ (wegen der Inklusionsumkehrung) L^{J_1} enthält L^{H_1}, L^{H_2} und L^{H_3}, also insbesondere die Elemente $i, \sqrt{2}$ und (dann natürlich auch) $i\sqrt{2}$ $\Rightarrow L^{J_1} \supset \mathbb{Q}(i, \sqrt{2})$

Die Dimension von L^{J_1} ist $4 = \frac{8}{2}$, die von $\mathbb{Q}(i, \sqrt{2})$ auch warum? (ohne Rechnung)

$\Rightarrow \boxed{L^{J_1} = \mathbb{Q}(i, \sqrt{2})}$

Eine andere 4-dimensionale Erweiterung, $\mathbb{Q}(\sqrt[4]{2})$, muß jetzt als ein $L^?$ vorkommen – für welches J? $(\sqrt[4]{2})^2 = \sqrt{2} \in \mathbb{Q}(\sqrt[4]{2})$, also $\mathbb{Q}(\sqrt[4]{2}) \supset \mathbb{Q}(\sqrt{2}) = L^{H_2}$

$\Rightarrow$ nur L^{J_4}, L^{J_2} oder L^{J_1} kommen in Frage, aber L^{J_1} ist es nicht

ausprobieren: $J_2 = \langle \tau \rangle,\ \tau(\sqrt[4]{2}) = \sqrt[4]{2} \Rightarrow \boxed{L^{J_2} = \mathbb{Q}(\sqrt[4]{2})}$

wie könnte man J_4 direkt ausschliessen?

Eine weitere 4-dimensionale Erweiterung können wir auch noch erraten:

$x^4 - 2$ ist irreduzibel über $\mathbb{Q}$, die Nullstelle $\sqrt[4]{2}$ führt zu $\mathbb{Q}(\sqrt[4]{2})$

Eine weitere Nullstelle ist $i\sqrt[4]{2} \Rightarrow \mathbb{Q}(i\sqrt[4]{2}) \cong \mathbb{Q}(\sqrt[4]{2})$ warum?

$\Rightarrow [\mathbb{Q}(i \cdot \sqrt[4]{2}) : \mathbb{Q}] = 4$, und $\mathbb{Q}(i\sqrt[4]{2}) \neq \mathbb{Q}(\sqrt[4]{2})$ und $\neq \mathbb{Q}(i, \sqrt{2})$ warum?

$(i\sqrt[4]{2})^2 = -\sqrt{2} \Rightarrow \mathbb{Q}(i \cdot \sqrt[4]{2}) \supset \mathbb{Q}(\sqrt{2})$

$\Rightarrow \boxed{L^{J_4} = \mathbb{Q}(i\sqrt[4]{2})}$

Jetzt fehlen noch L^{Z_3} und L^{Z_5}, die beide $\mathbb{Q}(i\sqrt{2})$ enthalten müssen (laut Hauptsatz ist die Liste der Zwischenkörper dann vollständig).

Bestimmung von L^{Z_3}: $Z_3 = \{id, \sigma\circ\tau = \tau\circ\sigma^3\}$

$\sigma\circ\tau: \sqrt[4]{2} \mapsto \sqrt[4]{2}\cdot i,\ i \mapsto -i,\ i\sqrt[4]{2} \mapsto \sqrt[4]{2}$ ⇒ $\sqrt[4]{2}$ und $i\sqrt[4]{2}$ werden vertauscht

⇒ die Summe der beiden, $(1+i)\sqrt[4]{2}$ ist invariant ⇒ $(1+i)\sqrt[4]{2} \in L^{Z_3}$

⇒ $\mathbb{Q}((1+i)\sqrt[4]{2}) \subset L^{Z_3}$

⇓

$(1+i)\sqrt[4]{2},\ ((1+i)\sqrt[4]{2})^2,\ ((1+i)\sqrt[4]{2})^3$ usw – was ist der Grad von $(1+i)\sqrt[4]{2}$ bzw seines Minimalpolynoms?

$\mathbb{Q}((1+i)\sqrt[4]{2}) \supsetneq \mathbb{Q}$ ⇒ kann nur Grad 2 oder 4 haben

Rechnen: $((1+i)\sqrt[4]{2})^2 = (1+2i-1)\cdot\sqrt{2} = 2i\sqrt{2}$ ⇒ warum? $1,\ (1+i)\sqrt[4]{2}$ und $((1+i)\sqrt[4]{2})^2$ sind linear unabhängig über $\mathbb{Q}$ ⇒ $[\mathbb{Q}((1+i)\sqrt[4]{2}):\mathbb{Q}] = 4$

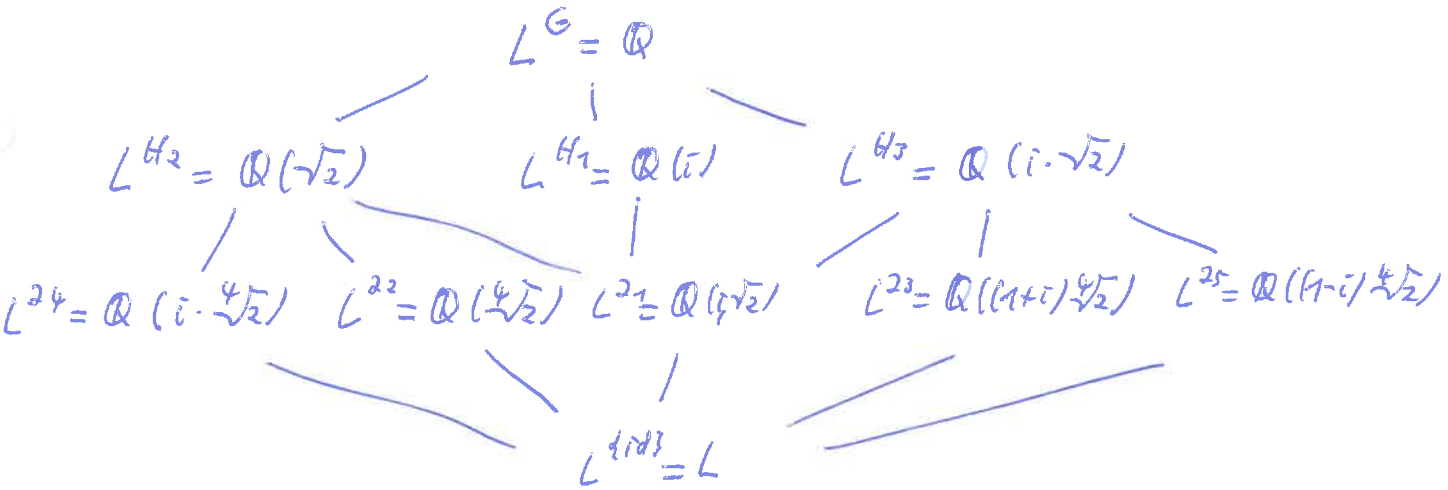
⇒ $\boxed{L^{Z_3} = \mathbb{Q}((1+i)\sqrt[4]{2})}$

Jetzt fehlt noch L^{Z_5}, das geht ähnlich: $Z_5 = \{id, \tau\circ\sigma = \sigma^3\circ\tau\}$

$\tau\circ\sigma: \sqrt[4]{2} \mapsto -i\sqrt[4]{2},\ i \mapsto -i,\ i\sqrt[4]{2} \mapsto (-i)\cdot(-i\sqrt[4]{2}) = -\sqrt[4]{2}$

⇒ $(1-i)\sqrt[4]{2}$ ist $(\tau\circ\sigma)$-invariant und hat auch Grad 4 nachprüfen

⇒ $\boxed{L^{Z_5} = \mathbb{Q}((1-i)\sqrt[4]{2})}$ Damit ist $\mathfrak{Z}$ laut 1.5 bestimmt.



tragen Sie bei allen Inklusionen noch die Erweiterungsgrade ein

Jetzt kommt der Beweis von 1.5, der im Vergleich zu den Vorbereitungen und zum Beispiel fast schon einfach wirkt.

Sei also $L|K$ eine Galoiserweiterung und M ein Zwischenkörper: $K < M < L$.

Behauptung 1: $L|M$ ist eine Galoiserweiterung, d.h. endlich, normal und separabel.

wirklich?

Beweis: $L|K$ endlich $\Rightarrow L|M$ endlich (Gradformel)

nachschauen

$L|K$ separabel $\Rightarrow L|M$ und $M|K$ separabel (Algebra, Theorem 6.12(e))

$L|K$ normal $\Rightarrow \exists\, S \subset \bar{K}$, S eine Menge, deren Elemente genau die Nullstellen in $\bar{K}$ einer Menge von Polynomen in $K[x]$ sind, sodaß $L = K(S)$

$K[x] \subset M[x] \Rightarrow L = M(S) \Rightarrow L|M$ normal

$\Rightarrow$ Behauptung 1 ✓

Die Abbildungen α und β sind $\mathcal{Z} \underset{\beta:\, H \mapsto L^H}{\overset{\alpha:\, M \mapsto Gal(L|M)}{\rightleftarrows}} \mathcal{U}$ (α ist nach Behauptung 1 wohldefiniert)

Behauptung 2: α und β sind zueinander inverse Bijektionen

Beweis: Sei $M \in \mathcal{Z}$. $\alpha: M \longmapsto Gal(L|M) =: H$, $\beta: H \longmapsto L^H = L^{Gal(L|M)}$

$L|M$ Galoiserweiterung $\overset{\text{Prop 1.3}}{\Longrightarrow} M = L^{Gal(L|M)}$, also $\beta(\alpha(M)) = M$

Gegenrichtung: Sei $H \in \mathcal{U}$. $H \overset{\beta}{\longmapsto} \underset{M}{\overset{}{L^H}} \overset{\alpha}{\longmapsto} Gal(L|M)$, $L^H =: M$

$Gal(L|K)$ endlich $\Rightarrow H$ endlich

$\overset{\text{Prop 1.3}}{\Longrightarrow} L|L^H$ galoisch und $H = Gal(L|L^H) = Gal(L|M)$

$\Rightarrow \alpha(\beta(H)) = H \Rightarrow$ Behauptung 2 ✓

Behauptung 3: Die Abbildungen α und β kehren Inklusionen um.

Beweis: $M_1 \subset M_2$, $\alpha(M_1) = Gal(L|M_1) = \{\sigma: L \xrightarrow{\sim} L \text{ mit } \sigma|_{M_1} = id_{M_1}\}$

$\alpha(M_2) = Gal(L|M_2) = \{\tau: L \xrightarrow{\sim} L \text{ mit } \underbrace{\tau|_{M_2} = id_{M_2}}_{\Rightarrow\, \tau|_{M_1} = id_{M_1}}\}$

$\Rightarrow \alpha(M_2) \subset \alpha(M_1)$

$H_1 \subset H_2$, $\beta(H_1) = L^{H_1} = \{a \in L : h(a) = a\ \forall h \in H_1\}$

$\beta(H_2) = L^{H_2} = \{b \in L : h(b) = b\ \underbrace{\forall h \in H_2}_{\Rightarrow\, \forall h \in H_1}\}$

$\Rightarrow \beta(H_2) \subset \beta(H_1)$

$\Rightarrow$ Behauptung 3 ✓

Behauptung 4: Sei $H \in \mathcal{U}$ und $\sigma \in Gal(L/K)$. Dann ist $\underbrace{\sigma(L^H)}_{\substack{=\text{Bild von} \\ L^H \text{ unter } \sigma}} = L^{\overbrace{\sigma H \sigma^{-1}}^{\{\sigma \circ h \circ \sigma^{-1} : h \in H\}}}$

Beweis: Sei $a \in L$. Dann: $a \in L^H \Leftrightarrow \varphi(a) = a \ \forall \varphi \in H \Leftrightarrow$

warum

$\Leftrightarrow \sigma\varphi(a) = \sigma(a) \ \forall \varphi \in H$

$\Leftrightarrow \underbrace{\sigma\varphi(\sigma^{-1}(\sigma(a)))}_{=(\sigma\circ\varphi\circ\sigma^{-1})(\sigma(a))} = \sigma(a) \ \forall \varphi \in H \quad \Leftrightarrow \sigma(a) \in L^{\sigma H \sigma^{-1}}$

$\Rightarrow$ Behauptung 4 ✓

Behauptung 5: $\underset{L^H}{M}/K$ ist normale Erweiterung $\Leftrightarrow \underset{H}{Gal(L/M)} \trianglelefteq Gal(L/K)$ (normale Untergruppe)

In diesem Fall gilt die "Kürzungsregel" $Gal(L/K)/_{Gal(L/M)} \simeq \underbrace{Gal(M/K)}_{\substack{\text{nur definiert,} \\ \text{wenn } M/K \text{ normal}}}$

Beweis: Die Hauptarbeit ist der Beweis der Äquivalenz. Die Kürzungsregel folgt dann schnell.

"$\Rightarrow$" $\underset{L^H}{M}/K$ normal $\Leftrightarrow \forall$ K-Homomorphismen $\varphi: M \to \bar{K}$ gilt $\varphi(M) = M$

↑ Algebra, Theorem 6.7 nachschauen

Sei $\tau \in Gal(L/K)$ und definiere $\varphi: M \to \bar{K}$ als Komposition

$$\begin{tikzcd} M \arrow[r, hook, "\text{Inklusion}"] \arrow[rrr, bend right, "\varphi"'] & L \arrow[r, "\tau"] & L \arrow[r, hook, "\text{Inklusion}"] & \bar{K} \end{tikzcd}$$

Dafür gilt $\varphi(M) = M$, also auch $\tau(M) = M$. Das definiert einen Gruppenhomomorphismus $Gal(L/K) \xrightarrow{\pi} Gal(M/K)$.

$\underset{H}{Gal(L/M)}$ ist eine Untergruppe von $Gal(L/K)$. Für $\tau \in Gal(L/M)$ ist das π-Bild in $Gal(M/K)$ die Identität. warum?

Für allgemeines $\tau \in Gal(L/K)$ ist $\tau(M) = M = \tau^{-1}(M)$

$\Rightarrow$ für $h \in H$: $h(M) = M$, da $h|_M = id_M \Rightarrow \tau H \tau^{-1}(M) = \tau\tau^{-1}(M) = M$ und

$\forall m \in M$: $\tau h \tau^{-1}(m) = \tau(\tau^{-1}(m)) = m$, d.h. m ist $\tau H \tau^{-1}$-invariant

Also: $L^H = L^{\tau H \tau^{-1}} \Rightarrow \underbrace{\alpha(\underset{M}{L^H})}_{=H} = \alpha(\underbrace{L^{\tau H \tau^{-1}}}_{\tau H \tau^{-1}}) \Rightarrow H = \tau H \tau^{-1}$ (für jedes $\tau \in Gal(L/K)$)

$\Rightarrow H = Gal(L/M)$ ist normal in $Gal(L/K$

"$\Leftarrow$" Sei $H = Gal(L/M) \trianglelefteq Gal(L/K)$ mit $M = L^H$ und $L/M = L/L^H$

Mit Proposition 1.4 ist L/L^H eine Galoiserweiterung mit Galoisgruppe H, die nach Voraussetzung normal in $G = Gal(L/K)$ ist

$\Rightarrow G/H$ (die Menge der Linksnebenklassen) ist auch eine Gruppe, mit der von G induzierten Multiplikation auf den Nebenklassen: $g_1H \cdot g_2H = g_1g_2H$.
Die Gruppe G/H operiert auf der Menge L^H in der folgenden Weise:
Sei $a \in L^H$ und $\bar{g} = gH \in G/H$. Definiere $\bar{g} \cdot a := g(a)$ ($g \in G = Gal(L|K)$ ist eine Abbildung $g: L \to L$, also auf a anwendbar). Wir müssen nachprüfen, daß die Operation wohldefiniert ist: Sei $h \in H$, dann ist
$(gh)(a) = g(h(a)) = g(a)$ weil $a \in L^H$, also kann der Repräsentant der Nebenklasse beliebig gewählt werden. Außerdem ist $hg(a) = gh'(a)$ für ein $h' \in H$ warum?
$\Rightarrow hg(a) \overset{\text{warum?}}{=} gh'(a) = g(a) \Rightarrow g(a) \in L^H \Rightarrow G/H$ operiert wirklich auf L^H.
$M = L^H \Rightarrow$ für die G/H-Invarianten von M, dh die $m \in M$ mit $G/H \cdot m = m$, gilt: $M^{G/H} = (L^H)^{G/H} = L^G = K$

das ist nicht offensichtlich – nachprüfen

G/H ist eine endliche Gruppe $\overset{\text{Prop 1.4}}{\Longrightarrow} M/M^{G/H}$ ist eine Galoiserweiterung mit Galoisgruppe $Gal(M|M^{G/H}) = G/H$. Aus galoisch folgt normal, d.h. $M/M^{G/H} = M/K$ ist normal, was zu beweisen war, also "$\Leftarrow$" ✓
Wir machen gleich weiter, um zur Kürzungsregel zu kommen:

$$Gal(M/M^{G/H}) = G/H = Gal(L^H|K)$$

$$G/H = Gal(L|K)/Gal(L|L^H), \quad L^H = M, \quad K = M^{G/H} \Rightarrow \text{Kürzungsregel ✓}$$

Damit ist der Hauptsatz der Galoistheorie bewiesen □
Dieser Beweis verdient es, ein zweites Mal gelesen zu werden.

Daß der Hauptsatz nicht nur schön, sondern auch sehr nützlich ist, haben wir schon im Beispiel gesehen und werden es in den nächsten Kapiteln noch mehr sehen.