4. Körper und Konstruierbarkeit

Vorwissen: Def Körper, Charakteristik

4.1 Körpererweiterungen

4.1.1 Def

Sei L ein Körper und $K \subset L$ mit den Verknüpfungen von L ein Körper, so ist K Unterkörper und $K \subset L$ eine Körpererweiterung, L ein Oberkörper.

L ist ein K-Vektorraum mit Skalarmultiplikation $K \times L \to L : (k, e) \mapsto ke$

$[L:K] := \dim_K L$ ist der Grad der Körpererweiterung.

Man schreibt L/K.

4.1.2 Bsp

1) $\mathbb{R} \subset \mathbb{C}$, $[\mathbb{C}:\mathbb{R}] = 2$.

2) $\mathbb{Q} \subset \mathbb{R}$, $[\mathbb{R}:\mathbb{Q}] = \infty$

3) $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2},\ a, b \in \mathbb{Q}\}$

$\mathbb{Q}[\sqrt{2}]$ ist das Bild des Einsetzhomomorphismus $\varphi: \mathbb{Q}[x] \to \mathbb{R}$:

$x \mapsto \sqrt{2}$

Beh: $\ker(\varphi) = \langle x^2 - 2 \rangle$

Angenommen, x^2-2 wäre zerlegbar über $\mathbb{Q}$, dann existieren $a,b,c,d \in \mathbb{Q}$ mit

$$(x^2-2) = (ax+b)(cx+d) =$$
$$ac\,x^2 + (ad+bc)x + bd$$

$$\Rightarrow c = \frac{1}{a},\ d = \frac{-2}{b} \text{ und}$$

$$\frac{-2a}{b} + \frac{b}{a} = 0 \Rightarrow \frac{-2a^2+b^2}{ab} = 0$$

$$\Rightarrow -2a^2+b^2 = 0 \Rightarrow 2a^2 = b^2 \Rightarrow 2 = \frac{b^2}{a^2}$$

$$\Rightarrow \sqrt{2} = \frac{b}{a} \in \mathbb{Q} \quad \lightning$$

$\Rightarrow$ x^2-2 ist irreduzibel

$\Rightarrow$ $\langle x^2-2 \rangle$ ist maximal

Es gilt $x^2-2 \in \ker(\varphi) \Rightarrow$
$\langle x^2-2 \rangle \subset \ker(\varphi) \Rightarrow \langle x^2-2 \rangle = \ker(\varphi)$

$\Rightarrow \mathbb{Q}[x]/\langle x^2-2 \rangle \cong \mathbb{Q}[\sqrt{2}]$ ist ein Körper

$[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$, denn eine $\mathbb{Q}$-Basis von $\mathbb{Q}[x]/\langle x^2-2 \rangle$ ist $1, x$.

Die Tatsache, daß $\mathbb{Q}[\sqrt{2}]$ ein Körper ist, kann man auch direkt sehen:
Die Ringstruktur wird von $\mathbb{Q}[x]$ geerbt, zu zeigen ist die Existenz von Inversen.

$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$$

$$\in \mathbb{Q}[\sqrt{2}],$$

denn $a^2-2b^2 \neq 0$, da $\sqrt{2}$ irrational.

4.1.3 Satz (Turmsatz)

Seien $K \subset L \subset M$ Körpererweiterungen (L ist Zwischenkörper). Dann gilt

$$[M:K] = [M:L] \cdot [L:K].$$

Beweis:
Sei $\{v_i\}$ eine L-Vektorraumbasis von M,
$\{w_j\}$ eine K-Vektorraumbasis von L.
Sei $m \in M \Rightarrow m = \sum l_i v_i$, $l_i \in L$.
Für $l_i \in L$ gilt $l_i = \sum k_{ij} w_j$ mit
$k_{ij} \in K \Rightarrow m = \sum_{i,j} k_{ij} w_j v_i \Rightarrow$

Die $\{w_j v_i\}$ erzeugen M als K-Vektorraum.

Ist $\sum k_{ij} w_j v_i = 0 \Rightarrow \sum_i \left(\sum_j k_{ij} w_j\right) v_i = 0$

$\overset{\{v_i\} \text{ Basis}}{\Longrightarrow} \sum_j k_{ij} w_j = 0 \ \forall i \overset{\{w_j\} \text{ Basis}}{\Longrightarrow} k_{ij} = 0 \ \forall i,j.$

$\Rightarrow \{w_j v_i\}$ linear unabhängig.

$\{w_j v_i\}$ ist eine Basis, $|\{w_j v_i\}| = |\{w_j\}| \cdot |\{v_i\}| \Rightarrow [M:K] = [M:L] \cdot [L:K]$. □

4.1.4 Korollar

Ist $[L:K]$ eine Primzahl, so hat $K \subset L$ keine echten Zwischenkörper.

Bemerkung: $K \subset L \Rightarrow \operatorname{char}(K) = \operatorname{char}(L)$, denn $1_K = 1_L$.

Ist $|K| < \infty \Rightarrow \operatorname{char}(K)$ prim

Ist $\operatorname{char}(K) = 0 \Rightarrow |K| = \infty$.

Es gibt unendlich viele Körper der Charakteristik p, z.B. $\operatorname{Quot}(\mathbb{Z}_p[x])$.

4.1.5 Def

K heißt Primkörper $:\Leftrightarrow$ K besitzt keine echten Unterkörper

K Körper, $P(K) := \bigcap_{\substack{U \subset K \\ U \text{ Unterkörper}}} U$

ist Primkörper von K.

4.1.6 Satz

$\operatorname{char} K = 0 \iff P(K) \cong \mathbb{Q}$

$\operatorname{char} K = p \iff P(K) \cong \mathbb{Z}_p$

Beweis: $\mathbb{Q}$ ist ein Primkörper, $\mathbb{Z}_p$ auch. Die charakteristische Abbildung $\mathbb{Z} \to K$: $n \mapsto n \cdot 1_K$ liefert uns diese als Unterkörper von K. □

4.1.7 Lemma

Sei $K \subset L$, $\alpha_1, \dots, \alpha_n \in L$,

$\varphi: K[x_1, \dots, x_n] \longrightarrow L : x_i \mapsto \alpha_i$

der Einsetzehomomorphismus,

$\operatorname{Im}(\varphi) =: K[\alpha_1, \dots, \alpha_n]$.

$K[\alpha_1, \dots, \alpha_n]$ ist der Durchschnitt aller Unterringe von L, die K und die α_i enthalten.

Beweis: $K[\alpha_1, \dots, \alpha_n]$ ist in jedem Unterring von L, der K und α_i enthält, enthalten, außerdem ist es selbst ein solcher Unterring. □

4.1.8 Def Sei $K \subset L$, $\alpha_1, \dots, \alpha_n \in L$,

$$K(\alpha_1, \dots, \alpha_n) := \bigcap_{\substack{U \subset L \text{ Unterkörper} \\ K \subset U,\ \alpha_1, \dots, \alpha_n \in U}} U$$

der kleinste Körper, der K und α_i enthält.

4.1.9 Lemma

$$K(\alpha_1, \dots, \alpha_n) = \operatorname{Quot}(K[\alpha_1, \dots, \alpha_n])$$

Beweis: $K[\alpha_1, \dots, \alpha_n]$ ist Unterring von L und daher nullteilerfrei. Die Inklusion $K[\alpha_1, \dots, \alpha_n] \hookrightarrow K(\alpha_1, \dots, \alpha_n)$ können wir auf $\operatorname{Quot}(K[\alpha_1, \dots, \alpha_n])$ fortsetzen und erhalten $\operatorname{Quot}(K[\alpha_1, \dots, \alpha_n]) \subset K(\alpha_1, \dots, \alpha_n)$. Andererseits ist $\operatorname{Quot}(K[\alpha_1, \dots, \alpha_n])$ ein Unterkörper, der K und α_i enthält, also gilt auch $K(\alpha_1, \dots, \alpha_n) \subset \operatorname{Quot}(K[\alpha_1, \dots, \alpha_n])$. □

4.1.10 Satz Sei $K \subset L$, $\alpha \in L$.

Dann sind äquivalent:

1) $\exists\ g \in K[X] \setminus \{0\}$ mit $g(\alpha) = 0$
2) $\ker(\varphi_\alpha : K[X] \to K[\alpha] : X \mapsto \alpha) \neq \{0\}$
3) $K[\alpha] = K(\alpha)$
4) $K[\alpha]$ ist Körper.

Falls 1)-4) gilt, folgt, daß m_α normierte Erzeuger von $\ker(\varphi_\alpha)$, m_α, irreduzibel ist.
Außerdem gilt $[K[\alpha]:K] = \deg(m_\alpha)$, $\{1, \alpha, \dots, \alpha^{\deg(m_\alpha)-1}\}$ ist eine K-Vektorraumbasis von $K[\alpha]$.

4.1.11 Def m_α heißt das Minimalpolynom von α, $\deg(m_\alpha)$ der Grad von α, α heißt algebraisch/K. Elemente $\alpha \in L$, die nicht algebraisch /K sind, heißen transzendent/K.

Beweis von 4.1.10:

1) $\Rightarrow$ 2): $g \in \ker(\varphi_\alpha)$

2) $\Rightarrow$ 1): $\exists\, g \neq 0$, $g \in \ker(\varphi_\alpha)$, mit $g(\alpha) = 0$.

Beh. Falls (2) gilt, so ist m_α irreduzibel.

Sei $m_\alpha = g_1 \cdot g_2 \Rightarrow 0 = m_\alpha(\alpha) = g_1(\alpha) \cdot g_2(\alpha) \in L \Rightarrow \Leftarrow g_1(\alpha) = 0$

$\Rightarrow g_1 \in \ker(\varphi_\alpha) = \langle m_\alpha \rangle \Rightarrow$

$m_\alpha \mid g_1 \Rightarrow \exists\, h: \; h \cdot m_\alpha = g_1$

$\Rightarrow m_\alpha = h \cdot m_\alpha \cdot g_2 \Rightarrow h \cdot g_2 = 1$

$\Rightarrow g_2$ ist Einheit.

2) $\Rightarrow$ 4): $K[\alpha] = \operatorname{Im}(\varphi_\alpha) \cong K[x] / \ker(\varphi_\alpha)$

$= K[x] / \langle m_\alpha \rangle$ und $\langle m_\alpha \rangle$ ist

maximal, da m_α irreduzibel

$\Rightarrow K[x] / \langle m_\alpha \rangle$ ist Körper

$\Rightarrow K[\alpha]$ ist Körper.

4) $\Rightarrow$ 2) Sei $\ker(\varphi_\alpha) = \{0\} \Rightarrow$

$K[\alpha] = \operatorname{Im}(\varphi_\alpha) = K[x] / \ker(\varphi_\alpha) = K[x] / \{0\}$

$= K[x]$ ist kein Körper.

4) $\Rightarrow$ 3) nach Definition.

3) $\Rightarrow$ 4) klar

In $K[x] / \langle m_\alpha \rangle$ bilden die Klassen

von $1, x, x^2, \dots, x^{\deg(m_\alpha)-1}$ eine

K- Vektorraumbasis, also entsprechend $1, \alpha, \dots, \alpha^{\deg(\alpha)-1}$ in $K[\alpha]$. □

4.1.12 Bsp 1) $\sqrt{2} \in \mathbb{R}$ ist algebraisch / $\mathbb{Q}$, $\deg(\sqrt{2}) = 2$

2) $i \in \mathbb{C}$ ist algebraisch / $\mathbb{R}$, $\deg(i) = 2$

3) π ist transzendent über $\mathbb{Q}$ (ohne Beweis).

4.1.13 Def

$K \subset L$ heißt algebraisch $:\Leftrightarrow$
$\forall \alpha \in L$: α ist algebraisch / K.

Falls $K \subset L$ nicht algebraisch, so heißt $K \subset L$ transzendent.

Bsp: $K \subset K(x) = \mathrm{Quot}(K[x])$ ist transzendent, denn die Potenzen von x erfüllen keine K-lineare Relation.

4.1.14 Satz Sei $K \subset L$.
Dann sind äquivalent:

1) $[L : K] < \infty$

2) $K \subset L$ ist algebraisch und $\exists$ $\alpha_1, \dots, \alpha_n \in L$: $K(\alpha_1, \dots, \alpha_n) = L$

3) $\exists$ $\alpha_1, \dots, \alpha_n \in L$ algebraisch mit $L = K(\alpha_1, \dots, \alpha_n)$.

4.1.15 Def Eine Körpererweiterung, die 4.1.14 1)–3) erfüllt, heißt endlich.

Insbesondere gilt: endliche Körpererweiterungen sind algebraisch.

Beweis von 4.1.14:

1) $\Rightarrow$ 2): Sei $[L:K] = n$, $\alpha \in L$

$\Rightarrow$ $1, \alpha, \dots, \alpha^n$ sind linear abhängig/K

$\Rightarrow$ $\exists$ $\lambda_i \in K$: $\sum_{i=0}^{n} \lambda_i \alpha^i = 0$.

Setze $g = \sum_{i=0}^{n} \lambda_i x^i$, dann gilt

$g(\alpha) = 0$ $\Rightarrow$ α ist algebraisch

Sei $\alpha_1, \dots, \alpha_n$ eine K-Vektorraum Basis von L, dann ist $K(\alpha_1, \dots, \alpha_n) \subset L$ (per Def) und $L \subset K(\alpha_1, \dots, \alpha_n)$, da $\ell \in L$ sich schreiben läßt

als $\sum \lambda_i \alpha_i = l$ mit $\alpha_i \in K$

$\Rightarrow L = K(\alpha_1, \dots, \alpha_n)$.

2) $\Rightarrow$ 3) klar

3) $\Rightarrow$ 1) $[L:K] = [K(\alpha_1, \dots, \alpha_n) : K] \overset{4.1.3}{=}$

$[K(\alpha_1, \dots, \alpha_n) : K(\alpha_1, \dots, \alpha_{n-1})] \cdot \dots \cdot [K(\alpha_1) : K]$

und jeder Faktor ist $< \infty$, da jedes α_i algebraisch $/K$ ist. □

4.1.16 Lemma

Ist $K \subset L$, $N \subset L$ eine Teilmenge von Elementen, die algebraisch über K sind, so ist $K(N) = K[N]$ und die Körpererweiterung $K(N)/K$ ist algebraisch.

(Der Fall $|N| < \infty$ folgt aus 4.1.10 per Induktion.)

Beweis:

Wir zeigen, daß $K[N]$ ein Körper ist. Dazu müssen wir ein Inverses für jedes $g \in K[N]$, $g \neq 0$, finden.

g ist ein Polynom in endlich vielen $\alpha_1, \dots, \alpha_n \in N$ mit Koeffizienten in K, und die α_i sind algebraisch $/K$.

$\Rightarrow g \in K[\alpha_1, \dots, \alpha_n] = K(\alpha_1, \dots, \alpha_n)$

$\Rightarrow \exists\, g^{-1} \in K[\alpha_1, \dots, \alpha_n] \subset K[N]$.

Da $K(\alpha_1, \dots, \alpha_n)$ algebraisch ist, ist g algebraisch $/K$ und damit $K[N]$ algebraisch $/K$. □

4.2 Zerfällungskörper und algebraischer Abschluß

4.2.1 Satz (Kronecker)

Sei K ein Körper, $f \in K[x]$, $f = g \cdot h$, g irreduzibel, $L = K[x]/\langle g \rangle$

Dann hat f in L eine Nullstelle $\alpha = [x] = x + \langle g \rangle \in L$, $L \cong K[\alpha]$.

Beweis: $f(\alpha) = f([x]) = [f(x)] \in L = K[x]/\langle g \rangle$, $[f(x)] = [g \cdot h] = [g] \cdot [h] = 0$. Das Minimalpolynom von α teilt g, da beide irreduzibel sind, sind sie bis auf konstanten Faktor gleich und damit $L \cong K[\alpha]$. □

4.2.2 Korollar

Sei K ein Körper, $f \in K[x]$, $d = \deg f > 0$.

1) $\exists\ K \subset L$, so daß f/L in Linearfaktoren zerfällt

2) Sind $\alpha_1, \dots, \alpha_d \in L$ Nullstellen, dann ist $K[\alpha_1, \dots, \alpha_d]$ der kleinste solche Körper

3) $K[\text{Nullstellen}]$ ist bis auf Isomorphie eindeutig und heißt Zerfällungskörper von f.

Beweis:

1) Satz von Kronecker 4.1.15 und Induktion.

2) Seien $\alpha_1, \dots, \alpha_d \in L$ Nullstellen

$\Rightarrow f = c(x-\alpha_1)\cdots(x-\alpha_d) \in K[\alpha_1, \dots, \alpha_d][x]$

Nach Def ist $K(\alpha_1, \dots, \alpha_n)$ der kleinste Körper, der K und die α_i

enthält. Wegen 4.1.10 (mit Induktion) gilt $K[\alpha_1, \dots, \alpha_n] = K(\alpha_1, \dots, \alpha_n)$, da jedes α_i als Nullstelle eines Polynoms in $K[X]$ per Def algebraisch ist. □

3) f zerfalle über $L' > K$, das heißt, in L' hat f d Nullstellen $\alpha_1', \dots, \alpha_d'$. Dann ist wegen 2) $K[\alpha_1', \dots, \alpha_d']$ ein Körper (der kleinste in L', über dem f zerfällt).

zu zeigen: $K[\alpha_1', \dots, \alpha_d'] \cong K[\alpha_1, \dots, \alpha_d]$.

Sei $f = g \cdot h$, $g, h \in K[X]$, g irreduzibel und normiert, dann hat wegen des Satzes von Kronecker 4.2.1 f eine Nullstelle α_1 in $K[X]/\langle g \rangle \cong K[\alpha_1]$.

Als Faktor von f zerfällt auch g über L' in Linearfaktoren und die Nullstellen von g in L'

sind auch Nullstellen von f in L'

$\Rightarrow$ OE α_1' ist eine Nullstelle von g in L'.

Das Minimalpolynom von α_1' über K ist, da $g(\alpha_1') = 0$, ein Faktor von g, und da g irreduzibel und normiert gleich g.

$$\Rightarrow K[\alpha_1'] \cong K[X]/\langle g \rangle \cong K[\alpha_1].$$

f hat in $K[\alpha_1][X]$ und $K[\alpha_1'][X]$ den Linearfaktor $(X-\alpha_1)$ bzw. $(X-\alpha_1')$, $f = (X-\alpha_1) \cdot f_1$, $f = (X-\alpha_1') \cdot f_1'$.

Der Isomorphismus $K[\alpha_1] \cong K[\alpha_1']$ induziert einen Ringhomomorphismus

$$K[\alpha_1][X] \xrightarrow{\cong} K[\alpha_1'][X],$$

der f festhält (da der Isomorphismus $K[\alpha_1] \cong K[\alpha_1']$ K festhält)

Da außerdem $x-\alpha_1 \longmapsto x-\alpha_1'$ muß auch f_1 auf f_1' überführt werden.
Wir führen Induktion über den Grad von f und können daher per Induktions-voraussetzung annehmen, daß der Zerfällungskörper von $f_1 \in K[\alpha_1][x]$ (bzw. $f_1' \in K[\alpha_1'][x]$) eindeutig ist, damit ist auch der Zerfällungs-körper von f eindeutig. □

4.2.3 Korollar
Sei $f \in K[x]$, der Zerfällungskörper L von f hat höchstens Grad $[L:K] \leq d!$ über K.

Beweis: Folgt durch sukzessives Adjungieren von Nullstellen aus 4.1.10 und 4.2.1 □

Bsp:
1) Der Zerfällungskörper von $x^2+1 \in \mathbb{R}[x]$ ist $\mathbb{C}$.

2) Sei $f = x^d - 1 \in \mathbb{Q}[x]$.

Über $\mathbb{C}$ zerfällt f, die Nullstellen sind $\alpha_j = e^{\frac{2\pi i}{d} \cdot j}$, $j = 0, \dots, d-1$,

die d-ten Einheitswurzeln.

Die $\{\alpha_j\} \subset \mathbb{C}^*$ sind eine zyklische Untergruppe, erzeugt von beliebigen α_j mit $ggT(j, d) = 1$,

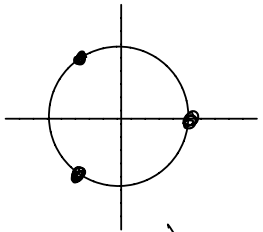
z.B. von α_1.

Daher ist der Zerfällungskörper von f gleich $\mathbb{Q}[\alpha_1, \dots, \alpha_{d-1}] = \mathbb{Q}[\alpha_j]$ $\forall$ j mit $ggT(j, d) = 1$.

3) Sei $f = x^3 - 2 \in \mathbb{Q}[x]$.

$\mathbb{Q}[\sqrt[3]{2}]$ ist nicht der Zerfällungskörper von f, denn die Nullstellen von f in $\mathbb{C}$ sind $\alpha_1 = \sqrt[3]{2}$,

$\alpha_2 = \sqrt[3]{2} \cdot e^{\frac{2\pi i}{3}}$, $\alpha_3 = \sqrt[3]{2} \cdot e^{\frac{4\pi i}{3}}$



Der Zerfällungskörper ist $\mathbb{Q}[\alpha_1, \alpha_2, \alpha_3]$ $(\neq \mathbb{Q}[\alpha_i]$ für jedes $i)$.

4.2.4 Lemma Sei K ein Körper. Dann sind äquivalent:

1) $\forall f \in K[x]$, $\deg f \geq 1$ gilt: f hat eine Nullstelle in K.

2) $f \in K[x]$ ist irreduzibel $\Leftrightarrow$ $\deg f = 1$

3) $\forall K \subset L$ algebraisch $\Rightarrow K = L$

4.2.5 Def

Ein K, daß 4.2.4 1)–3) erfüllt, heißt **algebraisch abgeschlossen.**

Beweis von 4.2.4:

1) $\Rightarrow$ 2) „$\Rightarrow$" Sei $\deg f > 1$, wegen 1) hat f eine Nullstelle α in K, der Linearfaktor $(x-\alpha)$ spaltet ab
$\Rightarrow$ f ist nicht irreduzibel

„$\Leftarrow$" Sei $\deg f = 1$, $f = g \cdot h$
$\Rightarrow$ o.E. $\deg g = 1$, $\deg h = 0$ $\Rightarrow$
h Einheit $\Rightarrow$ f irreduzibel.

2) $\Rightarrow$ 3) Sei $K \subset L$ algebraisch, $\alpha \in L$.
Das Minimalpolynom m_α ist irreduzibel
(4.1.10) $\Rightarrow$ $\deg m_\alpha = 1$ $\Rightarrow$
$m_\alpha = X - \alpha$, da $m_\alpha \in K[X]$ folgt
$\alpha \in K$ $\Rightarrow$ $L \subset K$ $\Rightarrow$ $K = L$.

3) $\Rightarrow$ 1) Wegen des Satzes von
Kronecker 4.2.1 gibt es für jedes
$f \in K[X]$ mit $\deg(f) \geq 1$ eine
Nullstelle in

$$L = K[\alpha] \cong K[X]/\langle g \rangle$$

(wobei g ein irreduzibler Faktor von
f ist), und $K \subset L$ ist algebraisch
$\Rightarrow$ $K = L$ $\Rightarrow$ $\alpha \in K$ $\Rightarrow$
f hat eine Nullstelle in K. □

Bsp: $\mathbb{Q}$, $\mathbb{R}$ sind nicht
algebraisch abgeschlossen, da $X^2 + 1$
keine Nullstelle hat.

4.2.6 (Fundamentalsatz der Algebra)

$\mathbb{C}$ ist algebraisch abgeschlossen.

Beweis in Funktionentheorie, bzw. später.

Für K wollen wir die Existenz des algebraischen Abschlusses $\overline{K}$ zeigen.

Zur Vorbereitung:

4.2.7 Zornsches Lemma

Sei $(M, \leq)$, $M \neq \emptyset$, partiell geordnet. Besitzt jede Kette in M eine obere Schranke, so besitzt M ein maximales Element.

Das Zornsche Lemma ist äquivalent zum Auswahlaxiom und zum Wohlordnungssatz (Lineare Algebra).

4.2.8 Prop

Sei R ein Ring und $I \subsetneq R$ ein Ideal. Dann $\exists$ maximales Ideal

m mit $I \subset m \subsetneq R$.

Beweis:

Sei $M = \{ J \subsetneq R \text{ Ideal}, I \subset J \}$

$M \neq \emptyset$, da $I \in M$.

M ist bezüglich $\subset$ partiell geordnet.

Sei K eine nicht-leere Kette in M, setze $S = \bigcup_{J \in K} J$

Beh: $S \in M$.

Da die Kette nicht-leer ist, gibt es $J \in K$ und $I \subset J \subset S$.

Seien $x, x' \in S$, $r \in R$.

Dann $\exists\ J, J' \in K$ mit $x \in J$, $x' \in J'$, $O.E.\ J \subset J'$, da K total geordnet $\Rightarrow$ $x + x' \in J' \subset S$.

Außerdem $r \cdot x \in J \subset S$

$\Rightarrow$ S ist ein Ideal.

Wäre $S = R$, so gäbe es ein $J \in K$ mit $1 \in J$ ↯

$\Rightarrow \quad S \subsetneq R \quad \Rightarrow \quad S \in M.$

Damit besitzt K eine obere Schranke $S \in M$ $\overset{\text{Zornsches Lemma}}{\Longrightarrow}$ M besitzt ein maximales Element m.

Es gilt $I \subset m$, da $m \in M$.

Wäre m kein maximales Ideal, so gäbe es ein Element in M echt größer m $\lightning$ zu Maximalität von m in M

$\Rightarrow$ m ist ein maximales Ideal, das I enthält. $\square$

4.2.9 Prop (Artin)

Sei K ein Körper. Dann $\exists$ algebraische Körpererweiterung $L > K$, so daß jedes nicht-konstante Polynom $f \in K[x]$ eine Nullstelle in L hat.

Beweis: Sei $\Lambda = K[x] \setminus K$

die Menge alle nicht-konstanten Polynome.

Betrachte $R = K[x_f \mid f \in \Lambda]$ den Polynomring mit Variablen für jedes $f \in \Lambda$.

Betrachte

$$I = \langle f(x_f) \mid f \in \Lambda \rangle \subset R.$$

$f(x_f)$ entsteht aus $f(x) \in \Lambda$, indem wir die Variable umbenennen als x_f.

Die Erzeuger von I hängen also von verschiedenen Variablen ab.

Angenommen, $I = R$.

Dann $\exists\ f_1, \dots, f_k \in \Lambda,\ g_1, \dots, g_k \in R$:

$$1 = \sum_{i=1}^{k} g_i f_i(x_{f_i}). \qquad (*)$$

Im Zerfällungskörper L von $f = f_1 \cdots f_k \in K[x]$ wählen

wir für jedes f_i eine Nullstelle α_i.

Wir wenden den Einsetzehomomorphismus

$$\varphi: R \longrightarrow L : \begin{cases} X_{f_i} \longmapsto \alpha_i \\ X_f \longmapsto 0 \quad f \neq f_i \end{cases}$$

auf (*) an und erhalten

$$1 = \sum_{i=1}^{k} \varphi(g_i) f_i(\varphi(X_{f_i})) =$$

$$\sum_{i=1}^{k} \varphi(g_i) f_i(\alpha_i) = \sum_{i=1}^{k} \varphi(g_i) \cdot 0 = 0$$

↯ $\Rightarrow$ $I \subsetneq R$.

Wegen 4.2.8 $\exists$ ein maximales Ideal $I \subset m \subsetneq R$.

Setze $L = R/m$, dann ist L ein Körper mit $K \subset L$.

Für $f \in K[X] \setminus K$ $\exists$ eine

Nullstelle in L, da $f(x_f) \in I \subset m$

$\Rightarrow [f(x_f)] = [0] \Rightarrow$

$f([x_f]) = 0 \Rightarrow [x_f]$ ist

Nullstelle.

Noch zu zeigen: L ist algebraisch.

Da $f([x_f]) = 0$ ist $[x_f]$

algebraisch. Aus 4.1.15 folgt

dann, daß

$L = K[x_f]/m = K[[x_f]]$

algebraisch ist. □

4.2.10 Satz

Jeder Körper besitzt einen algebraischen Abschluß $\overline{K}$.

Beweis: Setze $K_0 = K$ und

konstruiere mit 4.2.9

$K_0 \subset K_1$, so daß jedes Polynom

in $K_0[x] \setminus K_0$ in K_1 eine

Nullstelle hat.

Konstruiere rekursiv

$K_0 \subset K_1 \subset K_2 \subset \dots$

und setze $\overline{K} := \bigcup_{i=0}^{\infty} K_i$.

Beh: $\overline{K}$ ist der algebraische Abschluß von K.

Seien $\alpha, \beta, \gamma \in \overline{K}$, dann $\exists$ K_i mit $\alpha, \beta, \gamma \in K_i$, da die K_i eine Kette bilden.

Die Körperaxiome für α, β, γ ($(\alpha+\beta)\gamma = \alpha\gamma + \beta\gamma$ usw.) gelten also, da sie in K_i gelten

$\Rightarrow$ $\overline{K}$ ist ein Körper,

es gilt $K \subset \overline{K}$.

Ist $\alpha \in \overline{K}$ $\exists$ K_i : $\alpha \in K_i$ $\Rightarrow$

α algebraisch $/K$ $\Rightarrow$ $\overline{K}$ algebraisch $/K$.

Sei $f \in \overline{K}[x] \setminus \overline{K}$.

f hat endlich viele Koeffizienten

$\Rightarrow$ $\exists$ K_i : $f \in K_i[x] \setminus K_i$

Dann hat f nach Konstruktion

eine Nullstelle in $K_{i+1} \subset \overline{K}$

$\Rightarrow$ $\overline{K}$ ist algebraisch abgeschlossen.

□

4.3 Konstruktionen mit Zirkel und Lineal

4.3.1 Def

Wir identifizieren $\mathbb{R}^2 \cong \mathbb{C}$.

$k(a,r)$ bezeichne den Kreis um a mit Radius r, $a \in \mathbb{C}$, $r \in \mathbb{R}$.

$g(p,q)$ bezeichne die Gerade durch p und $q \in \mathbb{C}$

4.3.2 Def

Sei $M \subset \mathbb{C}$, $0,1 \in M$.

$G(M)$ = Menge der Geraden durch 2 Punkte von M

$K(M)$ = Menge der Kreise mit Mittelpunkt aus M und Radius = Entfernung zweier Punkte von M

$A(M)$ = Menge der Schnittpunkte zweier Geraden $= \{ z \in \mathbb{C} \mid \exists\, g_1, g_2 \in G(M), g_1 \neq g_2, z \in g_1 \cap g_2 \}$

$B(M)$ = Menge der Schnittpunkte einer

Geraden mit einem Kreis =

$$\{z \in \mathbb{C} \mid \exists\, g \in G(M),\ k \in K(M),\ z \in g \cap k\}$$

$C(M)$ = Menge der Schnittpunkte zweier Kreise

$$= \{z \in \mathbb{C} \mid \exists\, k_1, k_2 \in K(M),\ k_1 \neq k_2,\ z \in k_1 \cap k_2\}$$

$$M' = A(M) \cup B(M) \cup C(M)$$

Rekursiv $M_0 := M$, $M_1 = M'$, $M_2 = M_1'$, ...

$$\tilde{M} = \bigcup_{n \geq 0} M_n$$

$\tilde{M}$ ist die Menge der aus M konstruierbaren Punkte.

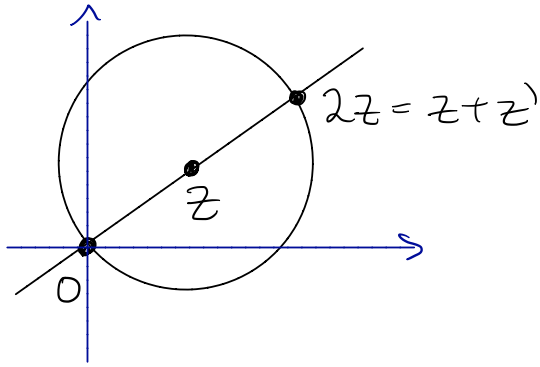
4.3.3 Satz $\tilde{M}$ ist ein Unterkörper von $\mathbb{C}$.

Beweis:

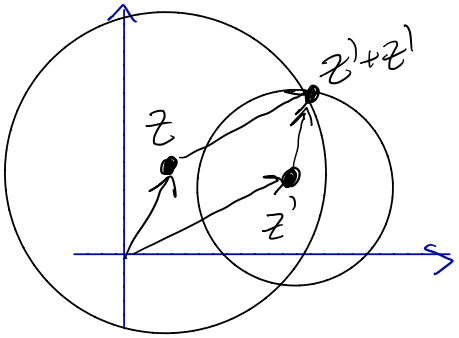
Behauptung: $(\tilde{M}, +)$ ist eine Untergruppe von $(\mathbb{C}, +)$.

$\tilde{M} \neq \emptyset$. Seien $z, z' \in \tilde{M}$.

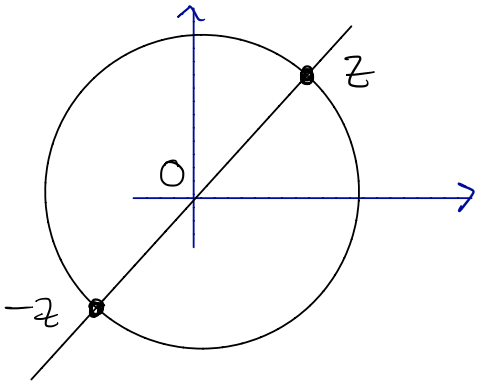
Falls $z = z'$ $\Rightarrow$ $z + z' \in k(z, |z|) \cap g(0, z) \subset \tilde{M}$



Falls $z \neq z' \Rightarrow z+z' \in k(z, |z'|) \cap k(z', |z|) \subset \tilde{M}$



$-z \in k(0, |z|) \cap g(0, z) \subset \tilde{M}$



Beh $(\tilde{M} \setminus \{0\}, \cdot)$ ist Untergruppe von $(\mathbb{C} \setminus \{0\}, \cdot)$

Dazu:

1) $z, z' \in \tilde{M} \setminus \{0\} \cap \mathbb{R}_{>0} \Rightarrow zz' \in \tilde{M} \setminus \{0\}$
2) $z \in \tilde{M} \setminus \{0\} \cap \mathbb{R}_{>0} \Rightarrow \frac{1}{z} \in \tilde{M} \setminus \{0\}$
3) $z \in \tilde{M} \setminus \{0\} \cap \mathbb{R}_{>0} \Rightarrow i \cdot z \in \tilde{M} \setminus \{0\}$
4) $z \in \tilde{M} \setminus \{0\} \Rightarrow |z|, \bar{z}, \mathrm{Re}\, z, \mathrm{Im}\, z \in \tilde{M}$
5) $\lambda \in \mathbb{R}_{>0} \cap \tilde{M} \setminus \{0\}, z \in \tilde{M} \setminus \{0\} \Rightarrow \lambda z \in \tilde{M} \setminus \{0\}$

Daraus folgt:
$\tilde{M} \setminus \{0\} \neq \emptyset$, da $1 \in \tilde{M} \setminus \{0\}$.
Für $z, z' \in \tilde{M} \setminus \{0\}$ beliebig gilt

$$z \cdot z' = \mathrm{Re}(z) \cdot \mathrm{Re}(z') - \mathrm{Im}(z) \cdot \mathrm{Im}(z') + i \cdot (\mathrm{Im}(z')\,\mathrm{Re}(z) + \mathrm{Re}(z')\,\mathrm{Im}(z))$$

Da Produkte aus $|\mathrm{Re}(z)|, |\mathrm{Re}(z')|, |\mathrm{Im}(z)|, |\mathrm{Im}(z')|$ wegen 1) in $\tilde{M}\setminus\{0\}$ sind und Negative da $(\tilde{M},+)$ Untergruppe von $(\mathbb{C},+)$ ist, und ein Produkt von i mit einer Zahl aus $\tilde{M}\setminus\{0\}$ in $\tilde{M}\setminus\{0\}$ ist wegen 3) folgt $z \cdot z' \in \tilde{M}\setminus\{0\}$.

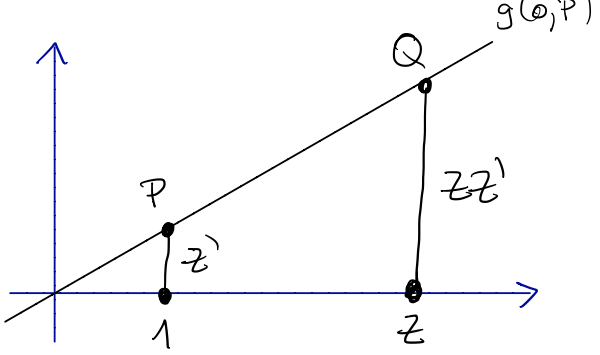
$\frac{1}{z} = \frac{1}{|z|^2} \cdot \bar{z} \in \tilde{M}\setminus\{0\}$, denn

$\frac{1}{|z|} \in \tilde{M}\setminus\{0\}$ wegen 2), $\frac{1}{|z|} \cdot \frac{1}{|z|}$ wegen 1),

$\bar{z} \in \tilde{M}\setminus\{0\}$ wegen 4)

und reelles Vielfaches einer Zahl in $\tilde{M}\setminus\{0\}$ wegen 5).

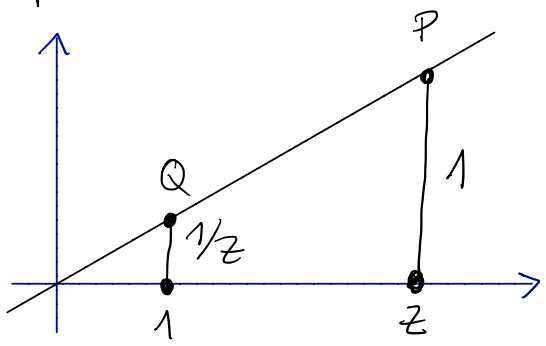
1)



- Lot fällen auf 1, z' abtragen liefert P
- Lot fällen auf z
- Schnittpunkt von $g(0,P)$ mit Lot auf z sei Q

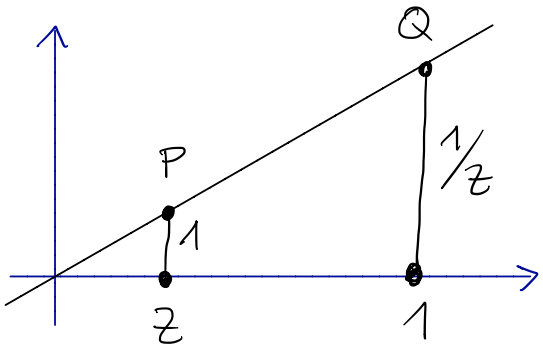
Dann gilt $|zQ| = zz'$ wegen Strahlensatz.

2) falls $z > 1$:

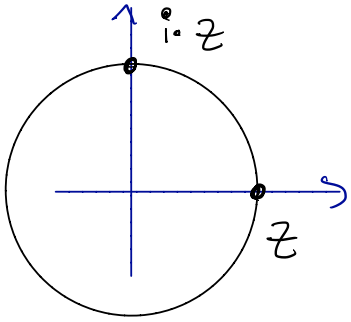


- Lot fällen auf z, 1 abtragen liefert P
- Lot fällen auf 1
- Schnittpunkt von $g(0,P)$ mit Lot auf 1 liefert Q. Dann gilt $|1Q| = 1/z$ wegen Strahlensatz.

falls $z < 1$



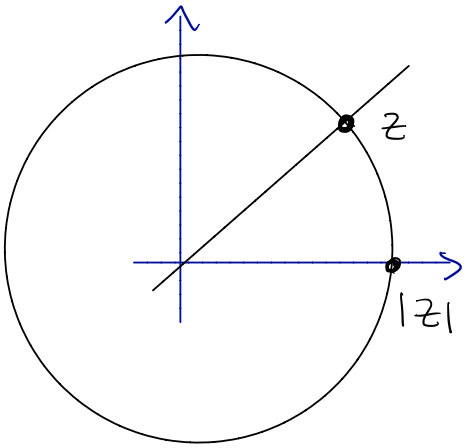
3) $i \cdot z \in g(0,i) \cap k(0,|z|) \subset \tilde{M} \setminus \{0\}$



4) $\cdot\ |z| \in$

$k(0,|z|) \cap$

$g(0,1) \in \tilde{M} \setminus \{0\}$



- $\mathrm{Re}\, z$ = Lot von z auf $g(0,1)$
- $\mathrm{Im}\, z$ = Lot von z auf $g(0,i)$
  ($i \in \tilde{M} \setminus \{0\}$ wegen 3))
- $\bar{z}$ = Spiegelung von z an $g(0,1)$

5) $|\lambda \cdot z| = \lambda \cdot |z| \in \tilde{M} \setminus \{0\}$ wegen 1), 4)
$\lambda \cdot z \in k(0, \lambda \cdot |z|) \cap g(0,z)$ □

Bemerkung: $\mathbb{Q} \subset \tilde{M}$, da man über die Strahlensätze jedes bekommt

4.3.4 Def

1) Eine Körpererweiterung $K \subset L$ heißt quadratisch abgeschlossen in $L :\Leftrightarrow$
$\forall\, \alpha \in L$ mit $\alpha^2 \in K$ gilt $\alpha \in K$

2) $K \subset L$ heißt Quadratwurzelerweiterung
$:\Leftrightarrow \exists\, \alpha_1, \dots, \alpha_n \in L$ mit
$L = K(\alpha_1, \dots, \alpha_n)$, $\alpha_i^2 \in K(\alpha_1, \dots, \alpha_{i-1})$,
$\alpha_i \notin K(\alpha_1, \dots, \alpha_{i-1})$.

Bemerkung
Der Grad einer Quadratwurzelerweiterung ist eine Zweierpotenz.

Bsp: $\mathbb{R} \subset \mathbb{C}$ ist nicht quadratisch abgeschlossen, denn $i^2 = -1 \in \mathbb{R}$, $i \notin \mathbb{R}$.

$\mathbb{R} \subset \mathbb{C}$, $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ sind Quadratwurzelerweiterungen.

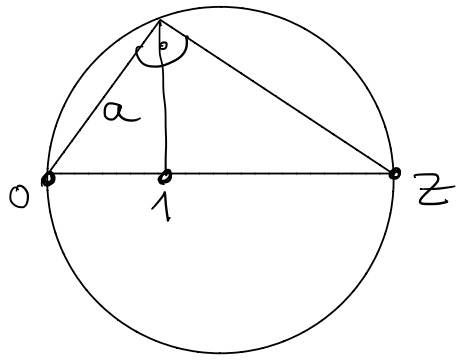
4.3.5 Satz

$\tilde{M}$ ist quadratisch abgeschlossen in $\mathbb{C}$.

Beweis:

Sei $z \in \tilde{M} \cap \mathbb{R}_{>0}$, $z > 1$.

Konstruiere mit dem Kathetensatz a mit $1 \cdot z = a^2 \Rightarrow \sqrt{z} = a \in \tilde{M}$:



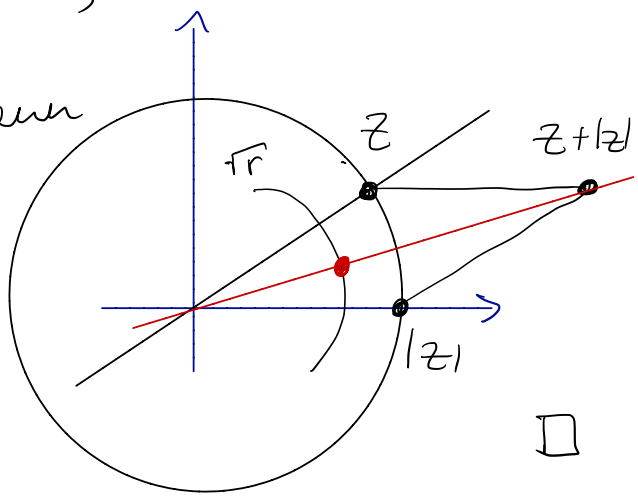
Sei $z \in \tilde{M} \cap \mathbb{R}_{>0}$, $z < 1 \Rightarrow$

$\frac{1}{z} > 1 \Rightarrow \sqrt{\frac{1}{z}} \in \tilde{M} \Rightarrow \sqrt{z} = \frac{\wedge}{\sqrt{\frac{1}{z}}} \in \tilde{M}$.

Sei $z = r \cdot e^{i\varphi} \in \tilde{M} \Rightarrow$

$\pm \sqrt{r} \cdot e^{i\varphi/2} \in \tilde{M}$, denn

$\sqrt{r} \cdot e^{i\varphi/2} \in K(0, \sqrt{r}) \cap g(0, z+|z|) \subset \tilde{M}$



□

4.3.6 Satz

$z \in \tilde{M} \Leftrightarrow \exists\ \mathbb{Q}(M \cup \bar{M}) \subset L \subset \mathbb{C}$
mit $z \in L$ und $K = \mathbb{Q}(M \cup \bar{M}) \subset L$
ist Quadratwurzelerweiterung.

Insbesondere: für $M = \{0,1\}$,
$z \in \tilde{M} \Rightarrow [\mathbb{Q}(z) : \mathbb{Q}] = 2^r$ ist
Zweierpotenz.

Beweis:

„$\Leftarrow$" Sei $\mathbb{Q}(M \cup \bar{M}) \subset L \subset \mathbb{C}$ mit
$z \in L$ und $K = \mathbb{Q}(M \cup \bar{M}) \subset L$ sei
Quadratwurzelerweiterung.
$\Rightarrow L = K(\alpha_1, \dots, \alpha_n)$, $\alpha_i^2 \in K(\alpha_1, \dots, \alpha_{i-1})$

Induktion über n.
$n = 0$: $L = K \subset \tilde{M}$.
$n-1 \to n$: Nach Induktionsvoraussetzung gilt
$K(\alpha_1, \dots, \alpha_{n-1}) \subset \tilde{M}$.
$\alpha_n^2 \in K(\alpha_1, \dots, \alpha_{n-1}) \Rightarrow \alpha_n^2 \in \tilde{M} \Rightarrow$
$\alpha_n \in \tilde{M}$, da $\tilde{M}$ quadratisch
abgeschlossen $\Rightarrow L \subset \tilde{M} \Rightarrow z \in \tilde{M}$.

„$\Rightarrow$" Wir verfolgen die Konstruktions-
schritte, um z zu erreichen und

adjungieren die neuen Elemente schrittweise zu $K = \mathbb{Q}(M \cup \bar{M})$ dazu, $K = K_0 \subset K_1 \subset \cdots$.

Schneiden wir zwei Geraden, so erhalten wir die Koordinaten $(\mathrm{Re}\, z, \mathrm{Im}\, z)$ des Schnittpunkt z durch ein lineares Gleichungssystem über K – dies läßt sich über K schon lösen und wir müssen nichts dazuadjungieren.

Schneiden wir eine Gerade mit der Gleichung $y = mx + b$ mit einem Kreis mit der Gleichung $(x-a_1)^2 + (y-a_2)^2 = r^2$, so erfüllt x die quadratische Gleichung

$$f = (x-a_1)^2 + (mx+b-a_2)^2 - r^2 = 0.$$

Falls f irreduzibel $/K_i$ adjungieren wir eine Nullstelle dazu und erhalten $K_{i+1} = K_i[x]/\langle f \rangle$ mit $[K_{i+1} : K_i] = 2$.

Falls f reduzibel $/K_i$ ist, ist $K_{i+1} = K_i$.

Schneiden wir zwei Kreise mit den Gleichungen $(x-a_1)^2 + (y-b_1)^2 = r_1^2$, $(x-a_2)^2 + (y-b_2)^2 = r_2^2$, ersetzen wir zunächst die zweite Gleichung durch die Differenz beider:

$$2(a_1-a_2)x + 2(b_1-b_2)y = -r_1^2 + r_2^2 + a_1^2 + b_1^2 - a_2^2 - b_2^2$$

Dies ist eine Geradengleichung.

Wir haben also wie vorher jetzt eine Kreis- und eine Geradengleichung und verfahren wie im Fall vorher.

Wir erhalten schließlich L im letzten Konstruktionsschritt als Quadratwurzelerweiterung von K mit $z \in L$. □

4.3.7 Korollar

Würfelverdopplung ist durch Konstruktion nicht möglich.

Beweis: Um einen Würfel des Volumens 2 zu konstruieren, müssten wir die Kantenlänge $\alpha = \sqrt[3]{2}$ konstruieren.

Beh $m_\alpha = x^3 - 2 \in \mathbb{Q}[x]$ ist Minimalpolynom

Wäre m_α reduzibel, $m_\alpha = g \cdot h$ mit $\deg g > 0$, $\deg h > 0$, dann folgt, da $\deg(g) + \deg(h) = \deg(m_\alpha) = 3$ $\Leftrightarrow$ $\deg g = 1$ $\Rightarrow$ g ist ein Linearfaktor $\Rightarrow$ die Nullstelle von g (die auch Nullstelle von m_α ist) muss in $\mathbb{Q}$ sein. Aber die Nullstellen von m_α sind $\sqrt[3]{2}$, $\sqrt[3]{2} \cdot e^{2\pi i/3}$, $\sqrt[3]{2} \cdot e^{4\pi i/3}$ und keine davon ist in $\mathbb{Q}$.

Damit gilt $\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}[x]/\langle x^3 - 2 \rangle$ und

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

Wäre α konstruierbar, also $\alpha \in \tilde{M}$, so gäbe es nach 4.3.6 eine Quadratwurzelerweiterung $\mathbb{Q} \subset L$ mit $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset L$, aber $[L : \mathbb{Q}] = 2^r$ ↯

da $3 \nmid 2$. □

4.3.8 Bemerkung:

π ist transzendent / $\mathbb{Q}$ (Bsp. 4.1.12 3)), damit auch $\sqrt{\pi}$ $\Rightarrow$ Ein Quadrat der Fläche π = Kreisfläche eines Kreises von Radius 1 ist nicht konstruierbar $\Rightarrow$ die Quadratur des Kreises ist nicht möglich.

In Korollar 4.3.7 war es wichtig, die Irreduzibilität von $x^3 - 2$ zeigen zu können. Für weitere Aussagen dieser Art:

4.3.9 Satz (Eisenstein-Kriterium)

Sei R faktoriell, $f \in R[x] \setminus R$ primitiv.

$f = \sum_{i=0}^{n} a_i x^i$.

$\exists\, p \in R$ prim mit $p \mid a_0, \dots, a_{n-1}$

$p^2 \nmid a_0$ $\Rightarrow$ f irreduzibel in $R[x]$.

Beweis:

Sei $f = g \cdot h$, $g = \sum_{i=0}^{k} b_i x^i$, $h = \sum_{j=0}^{\ell} c_j x^j$.

Falls $k = 0$, so ist $g \in R$, $g \mid a_i$ $\forall i$

$\Rightarrow$ $g \in R^*$, da f primitiv.

Genauso folgt $h \in R^*$, falls $\ell = 0$.

Sei $k, \ell > 0$.

Da $f = g \cdot h$ gilt $a_k = \sum_{i+j=k} b_i c_j$

für $k = 0, \dots, n$.

$p \mid a_0 = b_0 c_0$, da p prim folgt

O.E. $p \mid b_0$. Da $p^2 \nmid a_0$ folgt

$p \nmid c_0$.

Beh: $p \mid b_i \ \forall i = 0, \dots, k$.

Per Induktion, $p \mid b_0$ gilt.

Es gelte $p \mid b_0, \dots, b_{i-1}$.

Da $a_i = b_0 c_i + b_1 c_{i-1} + \dots + b_i c_0$

$\Rightarrow b_i c_0 = a_i - b_0 c_i - \dots - b_{i-1} c_1$

und alle Summanden rechts werden von p geteilt $\Rightarrow p \mid b_i c_0$, da

p prim und $p \nmid c_0$ folgt $p \mid b_i$.

Damit folgt $p \mid a_n = b_k c_\ell$

$\Rightarrow p \mid a_0, \dots, a_n$ ↯ zu f primitiv.

□

Bsp: $f = X^5 - 4X + 2 \in \mathbb{Z}[X]$ ist primitiv,
$2 \mid a_0, \dots, a_{n-1}$, $2^2 \nmid a_0$ $\Rightarrow$ f ist irreduzibel.

4.3.10 Satz

Sei R faktoriell, $f \in R[X] \setminus R$.
f ist irreduzibel in $R[X]$ $\Longleftrightarrow$
f primitiv in $R[X]$ und irreduzibel
in $\mathrm{Quot}(R)[X]$

Beweis:
Wegen des Satzes von Gauß (2.1) ist
$R[X]$ faktoriell, $\mathrm{Quot}(R)[X]$ ist auch
faktoriell, daher sind irreduzibel und
prim äquivalent.

Sei f primitiv in $R[X]$ und irreduzibel
in $\mathrm{Quot}(R)[X]$ $\overset{\text{Lemma 2.6}}{\Longrightarrow}$ f irreduzibel
in $R[X]$.

Sei f irreduzibel in $R[X]$, $f = g \cdot h$
mit $g, h \in \mathrm{Quot}(R)[X]$. Wie in
Lemma 2.3 2) schreiben wir g
und h als $g = c \cdot p$, $h = d \cdot q$

mit $p, q \in R[X]$ primitiv und $c, d \in \mathrm{Quot}(R)$.

Wegen Lemma 2.5 ist $p \cdot q$ primitiv.

$$\Rightarrow \quad f = (c \cdot d) \cdot p \cdot q \overset{2.3.\ 1)}{\Rightarrow}$$

$(c \cdot d) \in R$.

Diese Gleichung ist also in $R[X]$, und f ist irreduzibel in $R[X]$ $\Rightarrow$ zwei der drei Faktoren (cd), p, q sind Einheiten.

Dann folgt $\not\in \quad g = c \cdot p$ ist Einheit in $\mathrm{Quot}(R)[X]$

$\Rightarrow$ f ist irreduzibel.

f muß primitiv sein, da für einen Teiler $e \in R \setminus R^*$ aller Koeffizienten $f = e \cdot \frac{f}{e}$ sonst eine Zerlegung in Nichteinheiten wäre. □

Bsp: $X^5 - 4X + 2 \in \mathbb{Q}[X]$ ist irreduzibel.

4.3.11 Satz

Sei $e^{i\varphi}$ transzendent $/\mathbb{Q}$, dann ist die 3-Teilung des Winkels φ nicht möglich.

Beweis:

Sei $z = e^{i\varphi}$. Das Bild des Einsetzehomomorphismus $\varphi: \mathbb{Q}[x] \longrightarrow \mathbb{C} : x \mapsto z$ ist isomorph zu $\mathbb{Q}[x]$, da u. z transzendent, also keine algebraische Gleichung erfüllt, also $\ker(\varphi) = \{0\}$.

$\Rightarrow \mathbb{Q}[z]$ ist faktoriell und $z \in \mathbb{Q}[z]$ ist prim.

Betrachte $f = x^3 - z \in \mathbb{Q}[z][x]$

f ist primitiv, z teilt alle Koeffizienten außer a_3, $z^2 \nmid a_0$ $\overset{\text{Eisenstein}}{\underset{4.3.9}{\Longrightarrow}}$ f ist irreduzibel in $\mathbb{Q}[z][x]$ $\overset{4.3.10}{\Longrightarrow}$ f ist irreduzibel in $\mathrm{Quot}(\mathbb{Q}[z])[x] = \mathbb{Q}(z)[x]$ $\Rightarrow$ $x^3 - z$ ist Minimalpolynom von $e^{i\varphi/3}$ und $[\mathbb{Q}(z)(e^{i\varphi/3}) : \mathbb{Q}(z)] = 3$. $\lightning$ zu 4.3.6 (Quadratwurzelerweiterung). $\square$

4.3.12 Beispiel

Das regelmäßige 5-Eck ist konstruierbar.

Zunächst: Für $z = e^{\frac{2\pi i}{5}}$ und

$f = \frac{x^5-1}{x-1} = x^4 + x^3 + x^2 + 1$ gilt $f(z) = 0$.

Für $\varphi: \mathbb{Z}[x] \xrightarrow{\cong} \mathbb{Z}[x] : x \mapsto x+1$

gilt $\varphi(f) = f(x+1) = \frac{(x+1)^5 - 1}{x+1-1} =$

$$\frac{\sum_{i=0}^{5} \binom{5}{i} x^i - 1}{x} = \frac{1 + 5x + 10x^2 + 10x^3 + 5x^4 + x^5 - 1}{x}$$

$$= 5 + 10x + 10x^2 + 5x^3 + x^4$$

Da φ Isomorphismus gilt f irreduzibel

$\Leftrightarrow \varphi(f)$ irreduzibel.

Da $5 \mid$ alle Koeff außer a_n, $5^2 \nmid a_0$

folgt mit Eisenstein (4.3.9) $\varphi(f)$

irreduzibel

$\Rightarrow f$ irreduzibel

$\Rightarrow$ das Minimalpolynom von z ist f

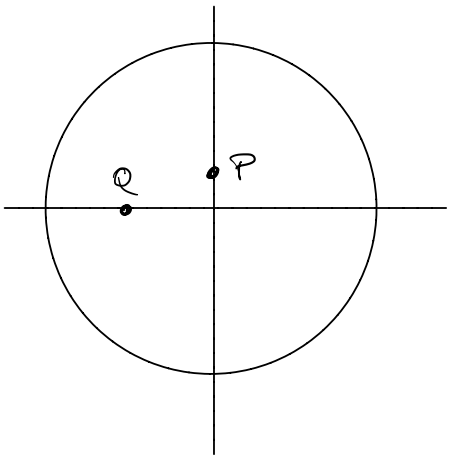
und hat Grad 4.

Wir können also keinen Widerspruch

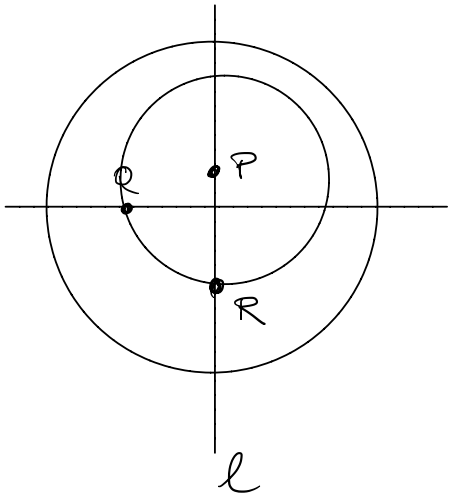
zu Satz 4.3.6 erzeugen.

Um die Konstruierbarkeit zu zeigen, müssen wir ein Konstruktionsverfahren angeben:

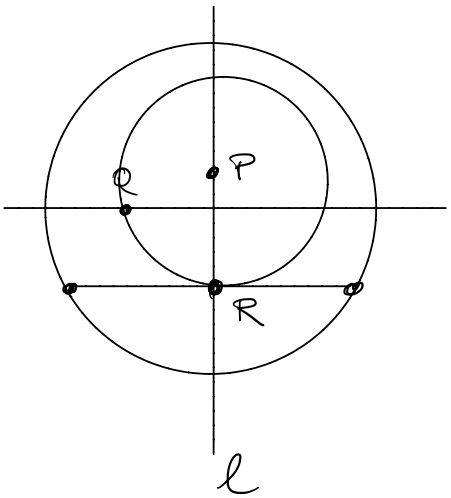
- Zwei aufeinander senkrecht stehenden Geraden durch den Mittelpunkt eines Kreises

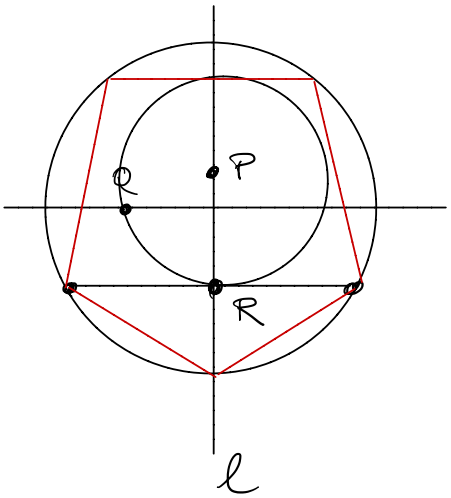


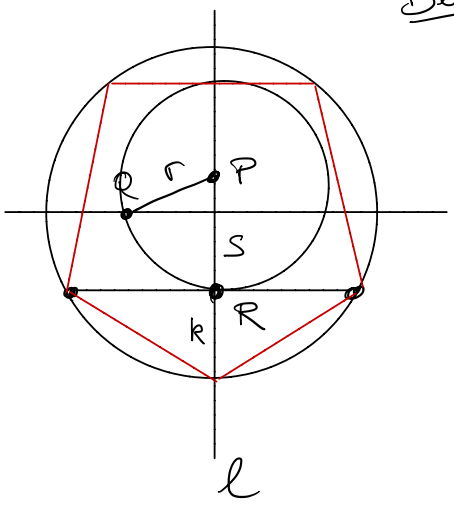
- Halbiere Radius, erhalte Q
- Viertele Radius, erhalte P
- Kreis mit Mittelpunkt P durch Q schneidet Gerade l in Punkt R



- Die Strecke durch R orthogonal zu l ist die Diagonale eines regelmäßigen 5-Ecks, trage ihre Länge 5 mal ab.







Beh Die Konstruktion funktioniert

Wir konstruieren die Längen:

$$r^2 = \left(\frac{1}{2}\right)^2 + \left(\frac{1}{4}\right)^2 = \frac{5}{16} \Rightarrow$$

$$r = \frac{\sqrt{5}}{4}$$

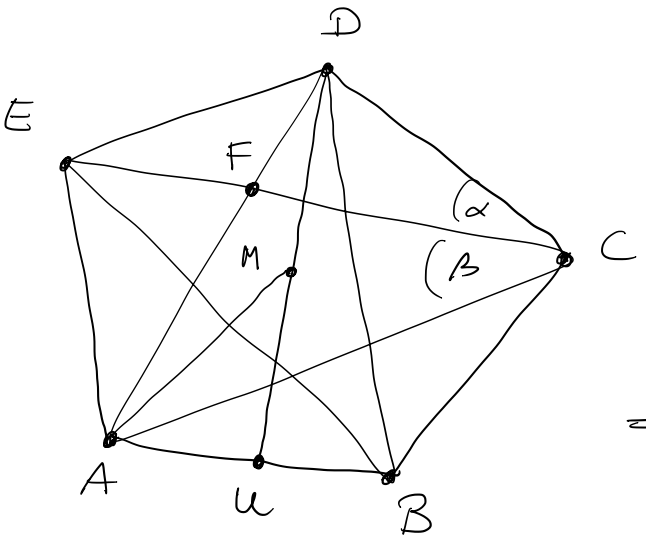
$$s = \frac{\sqrt{5}}{4} - \frac{1}{4},$$

$$k = 1 - s = \frac{5}{4} - \frac{\sqrt{5}}{4}$$

In einem regelmäßigen 5-Eck gilt:

Innenwinkel 72°, Außenwinkel 108°

Sei a die Seitenlänge, d die Diagonalenlänge.



$$\alpha = (180° - 108°)\frac{1}{2} = 36°$$

$$\beta = 108° - 2 \cdot 36° = 36°$$

$\Rightarrow$ $\triangle ABD$, $\triangle CDF$, $\triangle AEF$ sind ähnlich

$$\Rightarrow \overline{CF} = a, \quad \frac{d}{a} = \frac{\overline{AD}}{\overline{AB}} = \frac{\overline{AE}}{\overline{EF}} = \frac{a}{d-a}$$

Durch Lösen dieser quadratischen Gleichung für d in a erhalten wir

$$d = \frac{a}{2}\left(1 + \sqrt{5}\right)$$

Für die Höhe $h = \overline{DU}$ gilt dann

$$h^2 = a^2 - \frac{a^2}{4} = \frac{a^2}{4}(1+\sqrt{5})^2 - \frac{a^2}{4} =$$

$$a^2\left(\frac{1}{4}(1+2\sqrt{5}+5-1)\right) = a^2 \cdot \frac{1}{4}(5+2\sqrt{5})$$

Weiter gilt $\overline{MU} = h-1$ und in $\triangle AUM$

$$1 = \frac{a^2}{4} + (h-1)^2 =$$

$$\frac{a^2}{4} + h^2 - 2h + 1 = \frac{a^2}{4} + \frac{a^2}{4}(5+2\sqrt{5}) - a\sqrt{5+2\sqrt{5}} + 1$$

$$= \frac{a^2}{4}(6+2\sqrt{5}) - a\sqrt{5+2\sqrt{5}} + 1$$

$$\Rightarrow \frac{a^2}{4}(6+2\sqrt{5}) - a\sqrt{5+2\sqrt{5}} = 0$$

$$\Rightarrow a \cdot \frac{3+\sqrt{5}}{2} - \sqrt{5+2\sqrt{5}} = 0$$

$$\Rightarrow a \cdot \frac{3+\sqrt{5}}{2} = \sqrt{5+2\sqrt{5}}$$

$$\Rightarrow a = \frac{2\sqrt{5+2\sqrt{5}}}{3+\sqrt{5}} = \frac{2\sqrt{5+2\sqrt{5}}\,(3-\sqrt{5})}{4}$$

$$= \frac{1}{2}\sqrt{(5+2\sqrt{5})(14-6\sqrt{5})} =$$

$$\frac{1}{2}\sqrt{10-2\sqrt{5}} = \sqrt{\frac{10-2\sqrt{5}}{4}} = \sqrt{\frac{5-\sqrt{5}}{2}}$$

Für k gilt damit

$$k^2 = a^2 - \frac{d^2}{4} = a^2 - \frac{a^2}{16}(6+2\sqrt{5}) =$$

$$a^2\left(\frac{10-2\sqrt{5}}{16}\right) = \frac{5-\sqrt{5}}{2} \cdot \frac{10-2\sqrt{5}}{16} =$$

$$\frac{60-20\sqrt{5}}{2\cdot 16} = \frac{30-10\sqrt{5}}{16} = \frac{25-10\sqrt{5}+5}{16} =$$

$\left(\frac{5-\sqrt{5}}{4}\right)^2$, also haben wir für k die richtige Länge konstruiert.

4.3.13 Satz

Das regelmäßige g-Eck ist nicht konstruierbar.

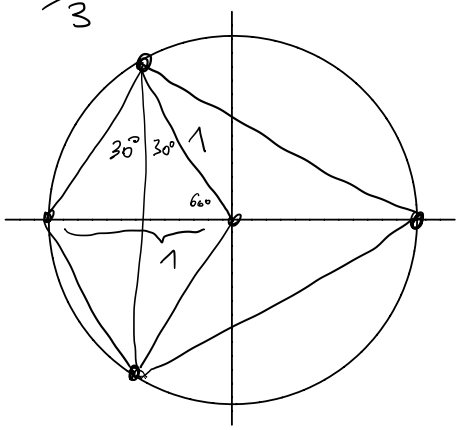
Beweis:

Angenommen, $e^{\frac{2\pi i}{g}} \in \tilde{M}$ (für $M = \{0,1\}$).

$$\Rightarrow a = e^{\frac{2\pi i}{g}} + e^{\frac{-2\pi i}{g}} = 2\,\mathrm{Re}\left(e^{\frac{2\pi i}{g}}\right) \in \tilde{M}$$

$$a^3 = e^{2\pi i/3} + 3e^{\frac{2\pi i}{g}} + 3e^{\frac{-2\pi i}{g}} + e^{-2\pi i/3}$$

$$= 3a + \underbrace{e^{2\pi i/3} + e^{-2\pi i/3}}_{-1}$$



$= 3a - 1$

Sei $f = x^3 - 3x + 1 \in \mathbb{Z}[x] \Rightarrow f(a) = 0$

Beh: f irreduzibel.

Wäre $f = g \cdot h = (c_1 x + c_0)(d_2 x^2 + d_1 x + d_0)$

$\Rightarrow c_0 d_0 = 1 \Rightarrow c_0 \in \mathbb{Z}^* = \{\pm 1\}$

und $c_1 d_2 = 1 \Rightarrow c_1 \in \mathbb{Z}^* = \{\pm 1\}$

$\Rightarrow$ Die möglichen Linearfaktoren sind $\pm(x \pm 1)$, aber ± 1 sind nicht Nullstellen von f ↯.

Mit 4.3.10 folgt $f \in \mathbb{Q}[x]$ ist irreduzibel $\Rightarrow f$ ist Minimalpolynom von $a \Rightarrow [\mathbb{Q}(a) : \mathbb{Q}] = 3$ ↯

wegen Satz 4.3.6. □

4.4 Die Galoisgruppe

4.4.1 Def Sei $K \subset L$ eine Körpererweiterung. Ein K-*Automorphismus* ist $\varphi: L \to L$ mit $\varphi|_K = id_K$.

Bsp Sei $\mathbb{R} \subset \mathbb{C}$, dann ist die komplexe Konjugation ein $\mathbb{R}$-Automorphismus von $\mathbb{C}$.

4.4.2 Bemerkung Jeder Automorphismus von K ist ein $P(K)$-Automorphismus für den Primkörper $P(K)$, denn $\varphi(1) = 1 \Rightarrow \varphi(a \cdot 1) = a \cdot 1 = a \quad \forall a \in \mathbb{Z}$, falls $P(K) = \mathbb{Q}$ außerdem $\varphi\left(\frac{p}{q}\right) = \frac{\varphi(p)}{\varphi(q)} = \frac{p}{q}$. □

4.4.3 Lemma Sei $K \subset L$, φ ein K-Automorphismus. Dann ist φ ein K-Vektorraumhomomorphismus. Falls $[L:K] < \infty$, ist φ K-Vektorraum-Isomorphismus.

Beweis: $\varphi(l_1+l_2) = \varphi(l_1) + \varphi(l_2)$ für $l_i \in L$, da φ Körperautomorphismus.
Sei $\lambda \in K$, $l \in L$, dann gilt
$\varphi(\lambda l) = \varphi(\lambda) \cdot \varphi(l) = \lambda \cdot \varphi(l)$,
↑ da φ Körperautomorphismus
da $\varphi|_K = id_K$. Als Körperautomorphismus ist φ injektiv. Falls $[L:K] < \infty \Rightarrow \dim_K L < \infty$ folgt damit, daß φ Isomorphismus ist. □

4.4.4 Def
Sei $K \subset L$ eine Körpererweiterung.
$Aut_K(L) = \{\varphi \in Aut(L) \mid \varphi|_K = id_K\}$
heißt die Gruppe der K-Automorphismen von L oder die Galoisgruppe von $K \subset L$.

Bsp: Für $\mathbb{R} \subset \mathbb{C}$ gilt
$Aut_{\mathbb{R}}(\mathbb{C}) = \{id, konj.\} \cong \mathbb{Z}_2$,
denn für $\varphi \in Aut_{\mathbb{R}}(\mathbb{C})$ gilt
$-1 = \varphi(-1) = \varphi(i^2) = \varphi(i) \cdot \varphi(i) = \varphi(i)^2$
$\Rightarrow \varphi(i) \in \{\pm i\}$.

4.4.5 Def:

Sei $K \subset L$ eine Körpererweiterung und $U \subset Aut_K(L)$ eine Untergruppe.

Dann ist

$$Fix(U) := \{a \in L \mid \varphi(a) = a \ \forall \varphi \in U\}$$

der Fixkörper von U, $K \subset Fix(U) \subset L$

Für einen Zwischenkörper M, $K \subset M \subset L$ ist

$Aut_M(L) \subset Aut_K(L)$

die Fixgruppe von M.

Bsp $\mathbb{R} \subset \mathbb{C}$,

$U = \{id\} \subset \mathbb{Z}_2$, $Fix(U) = \mathbb{C}$.

$Fix(\mathbb{Z}_2) = \mathbb{R}$.

4.4.6 Prop Sei $K \subset L$, $f \in K[x]$, $\varphi \in \mathrm{Aut}_K(L)$.
Dann bildet φ die Nullstellen von f auf die Nullstellen von f ab.

Beweis:
Sei $f = a_n x^n + \dots + a_0 \in K[x]$, seien $\alpha_1, \dots, \alpha_n$ die Nullstellen von f $\Rightarrow$

$$0 = \varphi(0) = \varphi(f(\alpha_i)) =$$
$$\varphi(a_n \alpha_i^n + \dots + a_0) = a_n \varphi(\alpha_i)^n + \dots + a_0$$
$$= f(\varphi(\alpha_i)).$$

□

4.4.7 Lemma
Sei $K \subset K[\alpha_1, \dots, \alpha_r]$ algebraisch.
$\varphi \in \mathrm{Aut}_K(K[\alpha_1, \dots, \alpha_r])$ ist eindeutig durch die Bilder $\varphi(\alpha_1), \dots, \varphi(\alpha_r)$ festgelegt.

Beweis: Für $r = 0$ ist $\varphi = \mathrm{id}_K$.

Induktion nach r.

Sei $\ell \in K[\alpha_1, \dots, \alpha_r]$, dann läßt sich ℓ schreiben als

$$\ell = c_d \alpha_r^d + \dots + c_1 \alpha_r + c_0$$

mit $c_i \in K[\alpha_1, \dots, \alpha_{r-1}]$.

$$\Rightarrow \varphi(\ell) = \varphi(c_d)\, \varphi(\alpha_r)^d + \dots + \varphi(c_1)\varphi(\alpha_r) + \varphi(c_0)$$

ist eindeutig bestimmt durch die $\varphi(\alpha_i)$, da die $\varphi(c_i)$ durch $\varphi(\alpha_1), \dots, \varphi(\alpha_{r-1})$ nach Induktionsvoraussetzung eindeutig bestimmt sind. □

4.4.8 Prop Sei $f \in K[x]$ mit Zerfällungskörper L.
Seien $\alpha_1, \dots, \alpha_n$ die Nullstellen von f.
Dann ist $\mathrm{Aut}_K(L) \subset S_n = S(\{\alpha_1, \dots, \alpha_n\})$
Die Operation

$$\mathrm{Aut}_K(L) \times \{\alpha_1, \dots, \alpha_n\} \to \{\alpha_1, \dots, \alpha_n\}$$
$$(\varphi, \alpha_i) \longmapsto \varphi(\alpha_i)$$

ist treu.

Beweis:
Nach 4.4.6 gilt $\varphi(\alpha_i) = \alpha_j$,
wir können φ also mit einer

Permutation der α_i identifizieren.
Nach 4.4.7 ist φ durch die Permutation eindeutig.
Gibt es ein φ so daß $\forall i$ $\varphi(\alpha_i) = \alpha_i$ so folgt $\varphi = id \Rightarrow$ die Gruppenwirkung ist treu. □

Bsp: Sei $f = x^3 - 2 \in \mathbb{Q}[X]$,
$L = \mathbb{Q}[\alpha_1, \alpha_2, \alpha_3]$ mit $\alpha_j = \sqrt[3]{2} \cdot e^{\frac{2\pi i}{3} j}$.

Es gilt $[L : \mathbb{Q}] = 6$, denn
$\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset L$,
$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, $\mathbb{Q}(\sqrt[3]{2}) \neq L$,
$f / x - \sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2})[X]$ ist Minimalpolynom von $\alpha_2 \in L$.
$\mathrm{Aut}_{\mathbb{Q}}(L) \cong S_3$, da f keine mehrfachen Nullstellen hat.

4.4.9 Prop

Ist $K \subset L$ endlich, so gilt
$|\mathrm{Aut}_K(L)| \leq [L : K]$.

Beweis:

Sei $L = K[\alpha_1, \dots, \alpha_n]$, sei f_j das Minimalpolynom von α_j über $K[\alpha_1, \dots, \alpha_{j-1}]$.

Die Inklusion $\varphi_0 : K \hookrightarrow L$ ist der einzige Körperhomomorphismus $K \to L$, der K festhält.

Sei $\varphi_{j-1} : K[\alpha_1, \dots, \alpha_{j-1}] \to L$ ein Körperhomomorphismus, der K festhält.

Beh $\exists$ höchstens $\deg(f_j)$ Körperhomomorphismen $\varphi_j : K[\alpha_1, \dots, \alpha_j] \to L$ mit $\varphi_j|_{K[\alpha_1, \dots, \alpha_{j-1}]} = \varphi_{j-1}$

Wie in 4.4.7 ist φ_j durch das Bild $\varphi_j(\alpha_j)$ festgelegt, und $\varphi_j(\alpha_j)$ muß eine Nullstelle von $\varphi_{j-1}(f_j)$ sein, denn für $f_j = c_r x^r + \dots + c_0$ mit $c_i \in K[\alpha_1, \dots, \alpha_{j-1}]$ gilt

$$\varphi_{j-1}(f_j)(\varphi_j(\alpha_j)) =$$
$$\varphi_{j-1}(c_r)\,\varphi_j(\alpha_j)^r + \dots + \varphi_{j-1}(c_0) =$$
$$\varphi_j(c_r\alpha_j^r + \dots + c_0) = \varphi_j(f_j(\alpha_j))$$
$$= 0$$

Wir bekommen damit insgesamt höchstens $\prod_j \deg(f_j)$ Möglichkeiten für Elemente in $\mathrm{Aut}_K(L)$. Es gilt

$$[L:K] = [K(\alpha_1,\dots,\alpha_n):K] =$$
$$[K(\alpha_1,\dots,\alpha_n):K(\alpha_1,\dots,\alpha_{n-1})] \cdot \dots \cdot [K(\alpha_1):K]$$
$$= \prod_j \deg(f_j),$$

also folgt die Aussage. □

4.4.10 Korollar:
Sei $f \in K[X]$, L der Zerfällungskörper. Dann gilt $|\mathrm{Aut}_K(L)| \leq [L:K]$ und Gleichheit, wenn jeder irreduzible Faktor von f keine mehrfachen Nullstellen hat.

Beweis: Wie im vorherigen Beweis durch Adjunktion der Nullstellen von f. Jedes Minimalpolynom f_j ist ein Teiler des Minimalpolynoms m_{α_j} von α_j über K. Da $f = c \cdot m_{\alpha_1} \cdots m_{\alpha_n}$ über K die Zerlegung in irreduzible Faktoren ist, und die m_{α_j} nach Voraussetzung keine mehrfachen Nullstellen haben, haben auch die f_j keine mehrfachen Nullstellen und wir haben in jedem Schritt zur Konstruktion der Elemente von $\mathrm{Aut}_K(L)$ die volle Auswahl. □

4.5 Normale und separable Körpererweiterungen

4.5.1 Def

Eine algebraische Körpererweiterung heißt normal, wenn jedes irreduzible Polynom $g \in K[X]$ mit einer Nullstelle in L schon über L in Linearfaktoren zerfällt.

Bsp 1) $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ ist nicht normal, da $x^3 - 2 \in \mathbb{Q}[X]$ irreduzibel ist, aber die weiteren Nullstellen $\sqrt[3]{2}\, e^{2\pi i/3}$, $\sqrt[3]{2}\, e^{4\pi i/3} \notin \mathbb{Q}(\sqrt[3]{2})$ liegen.

2) $\mathbb{R} \subset \mathbb{C}$ ist normal, da jedes irreduzible Polynom in $\mathbb{R}[X]$ über $\mathbb{C}$ in Linearfaktoren zerfällt.

4.5.2 Lemma

Sei $\varphi : K \xrightarrow{\cong} K'$, L Zerfällungskörper von $f \in K[X]$, L' Zerfällungskörper von $\varphi(f) \in K'[X]$

Dann $\exists\ \Psi : L \to L'$ mit $\Psi|_K = \varphi$.

Beweis:

Induktion nach $d = \deg(f)$.

Für $d = 1$ ist $L = K$, $L' = K'$, $\Psi = \varphi$.

Sei $d > 1$, sei α_1 eine Nullstelle von f mit Minimalpolynom $g \in K[X]$.

g ist ein irreduzibler Faktor von f, und $\varphi(g)$ damit ein irreduzibler Faktor von $\varphi(f)$. Da L' Zerfällungskörper von $\varphi(f)$ $\exists\ \alpha_1' \in L'$ mit $\varphi(g)(\alpha_1') = 0$.

$$\varphi_1 : K[\alpha_1] \cong \frac{K[X]}{\langle g \rangle} \cong \frac{K'[X]}{\varphi(g)} \cong K'[\alpha_1']$$

ist ein Isomorphismus mit $\varphi_1|_K = \varphi$.

Es gilt $f = (X - \alpha_1) \cdot f_1$ mit $\deg(f_1) < d$ und $\varphi(f) = \varphi_1(f) = (X - \alpha_1') \cdot \varphi_1(f_1)$ $\in K'[\alpha_1'][X]$.

Damit ist L Zerfällungskörper von $f_1 \in K[\alpha_1][X]$ und L' Zerfällungskörper von $\varphi_1(f_1) \in K'[\alpha_1'][X]$. Per Induktion können wir φ_1 zu

$\Psi : L \longrightarrow L'$ fortsetzen. □

4.5.3 Prop

Sei L = Zerfällungskörper von $f \in K[X]$, dann ist $K \subset L$ normal.

Beweis:

Sei $L = K[\alpha_1, \dots, \alpha_n]$ mit Nullstellen $\alpha_1, \dots, \alpha_n$ von f.

Sei $g \in K[X]$ irreduzibel mit Nullstelle $\beta \in L$, und M der Zerfällungskörper von $g \in L[X]$.

Sei $y \in M$ eine Nullstelle von g.

Da g irreduzibel ist gilt

$K[\beta] \cong K[X]/\langle g \rangle \cong K[y]$,

mit Isomorphismus $\varphi: K[\beta] \to K[\gamma]$

und $\varphi|_K = id_K$.

$L[\gamma] = K[\gamma][\alpha_1, \dots, \alpha_n]$ ist

Zerfällungskörper von $f \in K[\gamma][x]$

genauso ist $L = L[\beta] = K[\beta][\alpha_1, \dots, \alpha_n]$

Zerfällungskörper von $f \in K[\beta][x]$.

Wegen 4.5.2 läßt sich φ zu

einem Isomorphismus

$\varphi: L \to L[\gamma]$ erweitern.

Da $L \subset L[\gamma]$ folgt $L = L[\gamma]$

und $\gamma \in L$. □

4.5.4 Prop Eine endliche Erweiterung

$K \subset L$ ist normal $\Leftrightarrow$

L ist Zerfällungskörper eines Polynoms

$f \in K[x]$.

Beweis:

„$\Leftarrow$" 4.5.3

„$\Rightarrow$" $\exists$ algebraische $\alpha_i \in L$ mit

$L = K[\alpha_1, \dots, \alpha_n]$.
Sei $g_i \in K[x]$ das Minimalpolynom von α_i. Da $K \subset L$ normal und g_i die Nullstelle $\alpha_i \in L$ hat, zerfällt g_i über L in Linearfaktoren.
Damit ist L der Zerfällungskörper von $f = g_1 \cdot \dots \cdot g_r$. □

4.5.5 Korollar

Ist $K \subset L$ eine endliche, normale Körpererweiterung und $K \subset M \subset L$ ein Zwischenkörper, dann ist auch $M \subset L$ normal.

Beweis: Wegen 4.5.4 ist L der Zerfällungskörper von $f \in K[x] \subset M[x]$. □

4.5.6 Def

1) Ein irreduzibles Polynom heißt separabel, wenn es keine mehrfachen Nullstellen im Zerfällungskörper besitzt. Ein Polynom heißt separabel, wenn seine irreduziblen Faktoren separabel sind.

2) Eine algebraische Körpererweiterung $K \subset L$ heißt <u>separabel</u>, wenn für jedes $\alpha \in L$ das Minimalpolynom m_α separabel ist.

<u>4.5.7 Lemma</u>

Sei $f \in K[x]$, $K \subset L$, $\alpha \in L$

α ist mehrfache Nullstelle von f

$\Longleftrightarrow$ $f(\alpha) = 0$ und $f'(\alpha) = 0$.

<u>Beweis:</u>

Sei $f = (x-\alpha)^m \cdot g$ mit $g(\alpha) \neq 0$

$\Rightarrow f' = (x-\alpha)^{m-1} \cdot (mg + (x-\alpha) g')$.

„$\Rightarrow$" $m \geq 2 \Rightarrow f'(\alpha) = 0$.

„$\Leftarrow$" Da $g(\alpha) \neq 0$ ist $f'(\alpha) = 0$ nur wenn $m - 1 \geq 1$. □

<u>4.5.8 Lemma</u>: Ein irreduzibles $f \in K[x]$ hat eine mehrfache Nullstelle

$\Longleftrightarrow$ $f' = 0$.

<u>Beweis:</u> „$\Rightarrow$" Sei α die mehrfache

Nullstelle, dann gilt $f'(\alpha)=0$
Da $\deg(f') < \deg(f)$ und f das Minimalpolynom von α ist, folgt $f'=0$.
"$\Leftarrow$" Wenn $f'=0$ gilt insbesondere $f'(\alpha)=0$ für jede Nullstelle α von f und damit hat f eine mehrfache Nullstelle nach 4.5.7. □

4.5.9 Lemma

Ist $K \subset L$ separabel und $K \subset M \subset L$ ein Zwischenkörper, dann sind auch $K \subset M$ und $M \subset L$ separabel.

Beweis: Für $K \subset M$ nach Def.
Das Minimalpolynom von $\alpha \in L$ über M ist ein Teiler des Minimalpolynoms über K, daher auch $M \subset L$. □

4.5.10 Prop

Sei $\operatorname{char}(K)=0$, dann ist jede algebraische Körpererweiterung $K \subset L$ separabel.

Beweis:

Sei $\alpha \in L$, $m_\alpha \in K[x]$ das Minimalpolynom, $m_\alpha = x^n + a_{n-1}x^{n-1} + \dots + a_0$.

Da $n \neq 0$ gilt $m_\alpha' = n x^{n-1} + \dots \neq 0$

$\Rightarrow$ m_α hat keine mehrfache Nullstelle wegen 4.5.8. □

4.5.11 Korollar

Sei $\mathrm{char}(K) = 0$, dann ist jedes Polynom separabel.

Beweis: Sei $f = c f_1 \cdots f_r$ die Zerlegung in irreduzible Faktoren.

Wie eben gilt $f_i' \neq 0 \Rightarrow f_i$ hat keine mehrfache Nullstelle

wegen 4.5.8 $\Rightarrow$ f ist separabel. □

Bsp Sei $K = \mathbb{Z}_p(t)$ der Körper der rationalen Funktionen über $\mathbb{Z}_p$.

Dann ist $f = x^p - t \in K[x]$ irreduzibel, denn f ist irreduzibel in $\mathbb{Z}_p[t][x]$: $\mathbb{Z}_p[t]$ ist faktoriell, $t \in \mathbb{Z}_p[t]$ ist prim, $t \mid a_0$, $t^2 \nmid a_0$, f ist primitiv, also folgt die Irreduzibilität mit Eisenstein 4.3.9.

$\Rightarrow$ f ist Minimalpolynom von $[x]$ in $K[x]/\langle f \rangle = L$.

$K \subset L$ ist nicht separabel, denn f ist nicht separabel : f hat eine mehrfache Nullstelle, da

$f' = p x^{p-1} = 0$ (4.5.8.)

4.6 Endliche Körper

4.6.1 Satz

Sei F ein Körper mit endlich vielen Elementen.
Dann $\exists$ p Primzahl mit
$\operatorname{char}(F) = p$, $|F| = p^r$ wobei
$r = [F : \mathbb{Z}_p] < \infty$, wobei $\mathbb{Z}_p$ der Primkörper $P(F)$ ist.

Beweis: $P(F) = \mathbb{Z}_p$ und $\operatorname{char}(F) = p$
wegen Satz 4.1.6. F ist endlicher $\mathbb{Z}_p$-Vektorraum, also $[F : \mathbb{Z}_p] = r < \infty$
$\Rightarrow$ $F \cong (\mathbb{Z}_p)^r$ als $\mathbb{Z}_p$-Vektorraum
$\Rightarrow$ $|F| = p^r$. □

Bsp:

1) $x^2 + x + 1 \in \mathbb{Z}_2[x]$ ist irreduzibel, denn die einzigen Polynome vom Grad 1 in $\mathbb{Z}_2[x]$ sind $x+1$ und x und $x^2 + x + 1$ ist

kein Produkt mit diesen Faktoren.

$\Rightarrow F_4 = \mathbb{Z}_2[X] / \langle X^2+X+1 \rangle$ ist ein

endlicher Körper mit $2^2 = 4$ Elementen

der Char 2.

Seine Verknüpfungstafeln sind:

+	0	1	X	X+1
0	0	1	X	X+1
1	1	0	X+1	X
X	X	X+1	0	1
X+1	X+1	X	1	0

·	1	X	X+1
1	1	X	X+1
X	X	X+1	1
X+1	X+1	1	X

4.6.2 Def Sei $\operatorname{char}(L) = p$.

$Fr: L \to L: a \mapsto a^p$

heißt Frobenius homomorphismus und

ist Körper monomorphismus, für L

endlich Automorphismus.

Beweis: Für $a, b \in L$ ist

$Fr(a \cdot b) = (a \cdot b)^p = a^p \cdot b^p =$

$Fr(a) \cdot Fr(b)$ und

$$Fr(a+b) = (a+b)^p =$$
$$a^p + \binom{p}{1} a^{p-1}b + \cdots + \binom{p}{j} a^{p-j}b^j + \cdots + \binom{p}{p-1} ab^{p-1} + b^p$$
$$= a^p + b^p = Fr(a) + Fr(b).$$

Falls $a^p = 0$ ist $a = 0$. $\Rightarrow$
Fr injektiv $\square$

4.6.3 Satz

Zu jeder Primzahlpotenz gibt es bis auf Isomorphie genau einen Körper F mit p^r Elementen, den Zerfällungskörper von $f = X^{p^r} - X \in \mathbb{Z}_p[X]$.

Beweis:

$f' = p^r \cdot X^{p^r - 1} - 1 = -1 \in \mathbb{Z}_p[X]$

hat keine Nullstellen, also hat f keine mehrfachen Nullstellen und ist separabel.

Der Zerfällungskörper L von f enthält die p^r Nullstellen von f und ist der kleinste solche Körper.

Beh: Die Menge der Nullstellen von f ist ein Körper (damit gleich L, und $|L| = p^r$).

Es gilt: α Nullstelle von $f \iff$
$f(\alpha) = 0 \iff \alpha^{p^r} - \alpha = 0 \iff$
$\alpha^{p^r} = \alpha \Rightarrow Fr^r(\alpha) = \alpha \iff$
α ist Fixpunkt von Fr^r.

Seien α, β Nullstellen von f.
$Fr^r(\alpha+\beta) = Fr^r(\alpha) + Fr^r(\beta) = \alpha+\beta$
$\Rightarrow \alpha+\beta$ ist Nullstelle.
0 ist Nullstelle von f.
$Fr^r(-\alpha) = -Fr^r(\alpha) = -\alpha \Rightarrow$
$-\alpha$ ist Nullstelle von f
$\Rightarrow \{\text{Nullstellen}\} \subset (L, +)$ ist Untergruppe.

$Fr^r(\alpha \cdot \beta) = Fr^r(\alpha) \cdot Fr^r(\beta)$,
$Fr^r\left(\frac{1}{\alpha}\right) = \frac{1}{Fr^r(\alpha)}$, $Fr^r(1) = 1$

$\Rightarrow \{\text{Nullstellen}\} \subset (L \setminus \{0\}, \cdot)$ ist Untergruppe.

Damit ist L = Zerfällungskörper von f = $\{$Nullstellen von $f\}$ ein Körper mit $|L| = p^r$.

Sei F ein beliebiger Körper mit $|F| = p^r$. $|F^*| = p^r - 1 \Rightarrow$

$\forall a \in F^* : (a)^{p^r-1} = 1$

da die Ordnung eines Elements in F^* die Gruppenordnung teilt

$\Rightarrow a^{p^r} = a \quad \forall a \in F^*$

$\Rightarrow a^{p^r} = a \quad \forall a \in F$

$\Rightarrow F \subset \{$Nullstellen von $f\}$

$\Rightarrow F = \{$Nullstellen von $f\} = L$.

□

Wir schreiben $\mathbb{F}_{p^r}$ für den Körper mit p^r Elementen.

4.6.4 Def $\varphi : \mathbb{N} \to \mathbb{Z}$,

$\varphi(n) := \#\{ r \in \mathbb{Z} \mid 1 \leq r \leq n, \ ggT(r,n) = 1\}$

Die Eulersche Phifunktion.

4.6.5 Korollar

Sei $G = \langle g \rangle$ eine zyklische Gruppe. Sei $|G| = n$, $d \mid n$. Dann gibt es $\varphi(d)$ Elemente der Ordnung d in G, $\{g^{r \cdot \frac{n}{d}} \mid 1 \leq r \leq d, ggT(r,d) = 1\}$.

Insbesondere gibt es $\varphi(n)$ Elemente der Ordnung n, also Erzeuger.

Folgt aus dem Satz über Untergruppen zyklischer Gruppen.

Bsp.

$(\mathbb{Z}_{12}, +)$

Element	0	1	2	3	4	5	6	7	8	9	10	11
Ordnung	1	12	6	4	3	12	2	12	3	4	6	12

$\varphi(12) = 4$

Erzeuger von $\mathbb{Z}_{12}$: 1, 5, 7, 11

$\varphi(6) = 2$,

Elemente der Ordnung 6:

$(1 \cdot \frac{12}{6}) \cdot 1 = 2$, $(5 \cdot \frac{12}{6}) \cdot 1 = 10$,

denn $\{1,5\} = \{r \mid 1 \leq r \leq 6, ggT(r,6) = 1\}$

$\varphi(2) = 1$, Element der Ordnung 2:

$(1 \cdot \frac{12}{2}) \cdot 1 = 6$

4.6.6 Korollar

Sei $n \in \mathbb{N}$.

$$\sum_{d|n} \varphi(d) = n.$$

Beweis: Sei G die zyklische Gruppe der Ordnung n. Jedes Element hat als Ordnung einen Teiler d von n, für jeden Teiler gibt es $\varphi(d)$ Elemente dieser Ordnung. Daher ist $\sum_{d|n} \varphi(d)$ die Anzahl der Elemente von G. □

4.6.7 Satz

Sei K ein Körper, $H \subset K^*$ endliche Untergruppe $\Rightarrow$ H zyklisch.

Beweis: Sei $|H| = n$, $d \mid n$, $a \in H$ mit Ordnung d.

Dann ist $a^d = 1$, $(a^2)^d = 1$, ..., $(a^{d-1})^d = 1$

$\Rightarrow$ $1, a, \ldots, a^{d-1}$ sind Nullstellen von $f = x^d - 1 \in K[X]$. Da $\deg(f) = d$ sind dies alle Nullstellen und

$\{ b \in K \mid b^d = 1 \} = \{1, a, \ldots, a^{d-1}\}$ ist eine zyklische Untergruppe von H der Ordnung d.

Unter diesen Elementen sind $\varphi(d)$ Elemente der Ordnung d.

Setze $\Psi(d) = \#$Elemente der Ordnung d in H

Dann gilt

$$\Psi(d) = \begin{cases} \varphi(d) & \exists \text{ Element der Ordnung } d \\ 0 & \text{sonst} \end{cases}$$

$$\Rightarrow \quad n = |H| = \sum_{d \mid n} \Psi(d) \leq \sum_{d \mid n} \varphi(d)$$

$$\overset{4.6.6}{=} n \quad \Rightarrow \quad \Psi(d) = \varphi(d) \ \forall d \ \Rightarrow$$

$\exists$ Elemente der Ordnung d $\forall d \mid n$,
insbesondere $\exists$ Element der Ordnung
n und H ist zyklisch. $\square$

4.6.8 Def Eine Körpererweiterung der Form $K \subset K(\alpha)$ heißt *einfach*.
α heißt primitives Element.

4.6.9 Satz (Satz vom primitiven Element)
Jede endliche Erweiterung eines endlichen Körpers ist einfach.

Beweis: Sei $K \subset L$ endlich, $|K| < \infty$
$\Rightarrow |L| < \infty \overset{4.6.7}{\Rightarrow} L^*$ ist zyklisch,
also $L^* = \langle \alpha \rangle$ und $L = K(\alpha)$.
$\square$

4.6.10 Korollar

In $\mathbb{Z}_p[x]$ gibt es irreduzible Polynome vom Grad r $\forall r \in \mathbb{N}_{>0}$.

Beweis: Sei F_{p^r} der Körper mit p^r Elementen. $\mathbb{Z}_p = P(F_{p^r}) \subset F_{p^r}$ ist eine einfache Erweiterung

wegen 4.6.9 $\Rightarrow$ $F_{p^r} = \mathbb{Z}_p(\alpha) = \mathbb{Z}_p[\alpha]$, da α algebraisch und

$r = [F_{p^r} : \mathbb{Z}_p] = [\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] = \deg(m_\alpha)$ für das Minimalpolynom m_α von α $\Rightarrow$ m_α ist ein irreduzibles Polynom in $\mathbb{Z}_p[x]$ vom Grad r. □

In 4.4.5 haben wir Fixkörper eingeführt. Wir untersuchen jetzt Fixkörper von endlichen Körpern.

Bsp

$F_4 = F_2[x]/\langle x^2+x+1 \rangle = \{0, 1, x, x+1\}$

$Fr: \quad 0 \mapsto 0, \quad 1 \mapsto 1, \quad x \mapsto x^2 = x+1$

$x+1 \mapsto (x+1)^2 = x^2+2x+1 = x+1+1$

$= x$

$\Rightarrow \quad Fix(Fr) = F_2$

(Beachte, allgemein ist Fr ein $\mathbb{Z}_p$-Automorphismus von F_{p^r} wegen 4.4.2)

$Fr^2: \quad 0 \mapsto 0, \quad 1 \mapsto 1, \quad x \mapsto x^4 = (x+1)^2$

$= x$

$x+1 \mapsto (x+1)^4 = x^2 = x+1$

$\Rightarrow \quad Fix(Fr^2) = F_4.$

4.6.11 Satz

In F_{p^r} $\exists$ zu $s \mid r$ genau ein Zwischenkörper $\mathbb{Z}_p \subset F_{p^s} \subset F_{p^r}$ mit p^s Elementen, nämlich

$F_{p^s} = Fix(Fr^s) = \{a \in F_{p^r} \mid a^{p^s} = a\}.$

Beweis: $|F_{p^r}^*| = p^r - 1$, wegen 4.6.7 ist $F_{p^r}^* = \langle \alpha \rangle$ zyklisch.

$$p^r - 1 = p^{s \cdot k} - 1 = (p^s - 1) \cdot (p^{(k-1)s} + \dots + p^s + 1)$$

$$\Rightarrow p^s - 1 \mid p^r - 1$$

In zyklischen Gruppen $\exists$ zu jedem Teiler der Gruppenordnung genau eine Untergruppe dieser Ordnung

$\Rightarrow \exists!$ Untergruppe U der Ordnung $p^s - 1$ von $\mathbb{F}_{p^r}^*$, wobei

$$U = \langle \alpha^{\frac{p^r-1}{p^s-1}} \rangle .$$

Für jedes $\beta \in U$ gilt $\beta^{p^s-1} = 1$ und jedes Element, dessen Ordnung $p^s - 1$ teilt, liegt in $U \Rightarrow$

$$\beta^{p^s} = \beta \iff Fr^s(\beta) = \beta \iff \beta \in U \cup \{0\}$$

$$\Rightarrow U \cup \{0\} = \mathrm{Fix}(Fr^s)$$

ist der eindeutige Unterkörper mit p^s Elementen. □

Bsp: Durch Probieren sieht man, daß $x^4 + x + 1 \in \mathbb{F}_2[X]$ irreduzibel ist. Damit gilt

$F_{16} = \{0, 1, x, x+1, x^2, x^2+x, x^2+1, x^2+x+1,$
$x^3, x^3+x^2, x^3+x^2+x, x^3+x, x^3+x^2+x+1,$
$x^3+x+1, x^3+x^2+1, x^3+1\}$

$F_{16} = \mathrm{Fix}(Fr^4) = \{a \mid a^{16} = a\}$

$F_2 = \mathrm{Fix}(Fr)$

$Fr^2: (x^2+x)^4 = x^8 + x^4 = x^4 \cdot x^4 + x^4$
$= (x+1)(x+1) + x+1 = x^2 + 1 + x + 1 = x^2 + x$
$(x^2+x+1)^4 = x^8 + x^4 + 1 = (x+1)^2 + x + 1 + 1$
$= x^2 + 1 + x$
$0^4 = 0$, $1^4 = 1$, alle anderen werden nicht festgehalten
$\Rightarrow \mathrm{Fix}(Fr^2) = \{0, 1, x^2+x, x^2+x+1\}$

4.6.12 Satz

$x^{p^r} - x \in F_p[x]$ ist das Produkt aller irreduziblen normierten Polynome vom Grad d mit $d \mid r$.

Beweis: Sei f irreduzibel und normiert vom Grad d.

Wir zeigen: $f \mid x^{p^r} - x \iff d \mid r$

Da $x^{p^r} - x$ nur einfache Nullstellen hat, folgt dann die Behauptung.

"$\Leftarrow$" Sei $d \mid r$. Sei α eine Nullstelle von f. Sei $K = \mathbb{F}_p(\alpha)$. Es gilt $[K : \mathbb{F}_p] = d$, also $|K| = p^d \overset{4.6.11}{\Longrightarrow} K \cong \mathrm{Fix}(\mathrm{Fr}^d) \subset \mathbb{F}_{p^r}$. Das Polynom

$$x^{p^r} - x = \prod_{a \in \mathbb{F}_{p^r}} (x - a)$$

hat α als Nullstelle. Damit wird es vom Minimalpolynom f von α geteilt.

"$\Longrightarrow$" $f \mid x^{p^r} - x$. In $\mathbb{F}_{p^r}$ zerfällt $x^{p^r} - x$ und damit auch f in Linearfaktoren. Sei α eine Nullstelle von f, dann ist $r = [\mathbb{F}_{p^r} : \mathbb{F}_p] = [\mathbb{F}_{p^r} : \mathbb{F}_p(\alpha)] \cdot \underbrace{[\mathbb{F}_p(\alpha) : \mathbb{F}_p]}_{d}$, also $d \mid r$. □

4.6.13 Satz

$\mathrm{Aut}(\mathbb{F}_{p^r})$ ist zyklisch der Ordnung r mit Erzeuger Fr.

Beweis:

F_r hat die Ordnung r, denn

$F_r^r(\alpha) = \alpha^{p^r} = \alpha \Rightarrow F_r^r = id$

aber $F_r^k \neq id$ für $k < r$, denn

$Fix(F_r^k) \subsetneq F_{p^r}$.

Damit ist $\langle F_r \rangle \subset Aut(F_{p^r})$

eine zyklische Untergruppe der Ordnung r.

Es gilt $F_{p^r} = F_p(\alpha)$ und das Minimalpolynom m_α von α hat Grad $r = [F_{p^r} : F_p] = [F_p(\alpha) : F_p]$.

$m_\alpha \in F_p[X]$ und F_r ist F_p-Automorphismus wegen 4.4.2 $\Rightarrow$

$F_r(m_\alpha) = m_\alpha$. Damit ist mit α auch $F_r(\alpha)$ eine Nullstelle von m_α und $F_r^j(\alpha)$, $j > 0$ auch

$\Rightarrow m_\alpha = \prod_{j=1}^{r} (X - F_r^j(\alpha))$

Sei $\varphi \in Aut_{F_p}(F_{p^r})$, dann

gilt wegen 4.4.7 $\varphi(\alpha)$ ist Nullstelle von $m_\alpha \Rightarrow \exists j: \varphi(\alpha) = Fr^j(\alpha)$

Wegen 4.4.8 ist φ eindeutig durch $\varphi(\alpha)$ festgelegt, also folgt $\varphi = Fr^j$.

$\Rightarrow Aut_{F_p}(F_{p^r}) = \langle Fr \rangle$ □

4.6.14 Satz

Sei $K \subset L$ eine endliche Erweiterung endlicher Körper, also $K = F_q$, $L = F_{q^n}$ mit $q = p^r$ Primzahlpotenz, dann ist $K = Fix(Fr_q)$ mit

$Fr_q: L \to L: a \mapsto a^q$ $(Fr_q = Fr^r)$

$\langle Fr_q \rangle = Aut_K(L)$, $|Aut_K(L)| = n$.

Beweis:

$F_p \subset K = F_q = F_{p^r} \subset L = F_{q^n} = F_{p^{r \cdot n}}$

$Fix(Fr^r) = K$ wegen 4.6.11.

$Aut(L) \overset{4.6.13}{=} \langle Fr \rangle$, $|Aut(L)| = n \cdot r$.

Wie in 4.6.11 ist $L^* = \langle \alpha \rangle$,

$K^* = \langle \beta \rangle$ mit $\beta = \alpha^{p^{rn}-1/p^r-1}$

und $\operatorname{ord}(\beta) = p^r - 1 \Rightarrow Fr^j \notin$ $Aut_K(L)$ für $j < r$ (denn $\beta^{p^j - 1} \neq 1$ $\Rightarrow \beta^{p^j} = Fr^j(\beta) \neq \beta$) aber $Fr^r \in Aut_K(L)$, also $Aut_K(L) = \langle Fr^r \rangle$. □

Bemerkung:

Damit erhalten wir Bijektionen

$$\{\text{Teiler von } n\} \xleftrightarrow{1:1} \{\text{Zwischenkörper } K \subset M \subset L\}$$
$$s \longmapsto \operatorname{Fix}(Fr_q^s) \cong \mathbb{F}_{q^s}$$

denn $q^n = p^{rn}$ und die Zwischenkörper kommen von Teilern von rn, die Vielfache von r sind

$$\{\text{Teiler von } n\} \xleftrightarrow{1:1} \{\text{Untergruppen von } Aut_K(L)\}$$
$$s \longmapsto \langle Fr_q^s \rangle$$

da $Aut_K(L)$ zyklisch der Ordnung n.

Zusammen ergibt sich damit:

4.6.15 Satz (Hauptsatz der Galoistheorie für endliche Körper)

Sei $K \subset L$ eine endliche Erweiterung endlicher Körper. Dann ist

$$\{ \text{Untergruppen von } \mathrm{Aut}_K(L) \} \overset{1:1}{\longleftrightarrow} \{ \text{Zwischenkörper } K \subset M \subset L \}$$

$$U \longmapsto \mathrm{Fix}(U)$$

$$\mathrm{Aut}_M(L) \longmapsto M$$

eine Bijektion.

Außerdem gilt $\mathrm{Aut}_K(L) / \mathrm{Aut}_M(L) \cong \mathrm{Aut}_K(M)$.

Beweis: $K = \mathbb{F}_q$, $L = \mathbb{F}_{q^n}$, die Bijektion folgt aus der vorangegangenen Bemerkung.

Genauer: Sei M ein Zwischenkörper, $K \subset M \subset L$

Da $q = p^r$ ist $\mathbb{F}_p \subset K \subset M \subset L$

$\Rightarrow$ M ist Zwischenkörper von $\mathbb{F}_p \subset L$

$\Rightarrow$ M ist von der Form $\mathrm{Fix}(\mathrm{Fr}_p^{s'})$ (4.6.11) und hat $p^{s'}$ Elemente, wobei s' Teiler von rn ist, denn L hat $q^n = p^{rn}$ Elemente.

Da $K \subset M$ muß M q^s Elemente haben für ein s $\Rightarrow$ $q^s = p^{rs} = p^{s'}$ $\Rightarrow$ s' ist ein Teiler von rn, der Vielfaches

von r ist $\Rightarrow$ s ist ein Teiler von n.
Umgekehrt können wir für jeden Teiler s von n den Teiler rs von rn betrachten und erhalten mit 4.6.11 ein Körper M
$= \mathrm{Fix}(\mathrm{Fr}_p^{rs}) = \mathrm{Fix}(\mathrm{Fr}_q^{s})$ mit $\mathbb{F}_p \subset M \subset L$, da außerdem $K = \mathrm{Fix}(\mathrm{Fr}_p^{r}) = \mathrm{Fix}(\mathrm{Fr}_q)$ gilt $K \subset M$.

Aus 4.6.14 folgt $\mathrm{Aut}_K(L) = \langle \mathrm{Fr}_q \rangle$ ist zyklisch der Ordnung n, die Untergruppen von $\mathrm{Aut}_K(L)$ sind also genau die $\langle \mathrm{Fr}_q^s \rangle$ mit $s \mid n$.

Für einen Zwischenkörper $K \subset M \subset L$ gilt dabei

$$\frac{\mathrm{Aut}_K(L)}{\mathrm{Aut}_M(L)} = \frac{\langle \mathrm{Fr}_q \rangle}{\langle \mathrm{Fr}_q^s \rangle} =$$

die Untergruppe $\langle \mathrm{Erzeuger}^s \rangle$ ist zyklisch der Gruppenordnung n/s

$$\cong \frac{\mathbb{Z}_n}{\mathbb{Z}_{\frac{n}{s}}} \cong \mathbb{Z}_s \cong$$

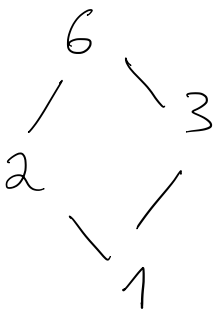
$\mathrm{Aut}_K(M)$, denn mit $K = \mathbb{F}_q$, $M = \mathbb{F}_{q^s}$ ist $\mathrm{Aut}_K(M)$ zyklisch der Ordnung s. □

Bsp $q=4$, $n=6$: $p=2$, $q=2^2$, $r=2$

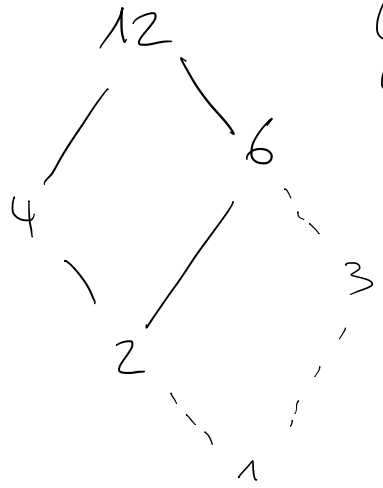
$q^6 = 4^6 = 2^{12}$. $K = F_4 = F_{2^r}$, $L = F_{4^6} = F_{2^{12}}$

Teiler von 6: 1, 2, 3, 6

Wir zeichnen ein Unterkörper-, Untergruppen- und Teilerdiagramm:



wir fassen diese wie im obigen Beweis als Teiler von 12 auf, die Vielfache von 2 sind:



(gestrichelt: weitere Teiler von 12)

$\mathrm{Aut}_K(L) \cong \mathbb{Z}_6$, $\mathrm{Aut}_K(L) \subset \mathrm{Aut}_{F_2}(L) \cong \mathbb{Z}_{12}$,

$G_1 = \mathrm{Aut}_{F_2}(L)$ wird erzeugt von Fr_2, d.h.

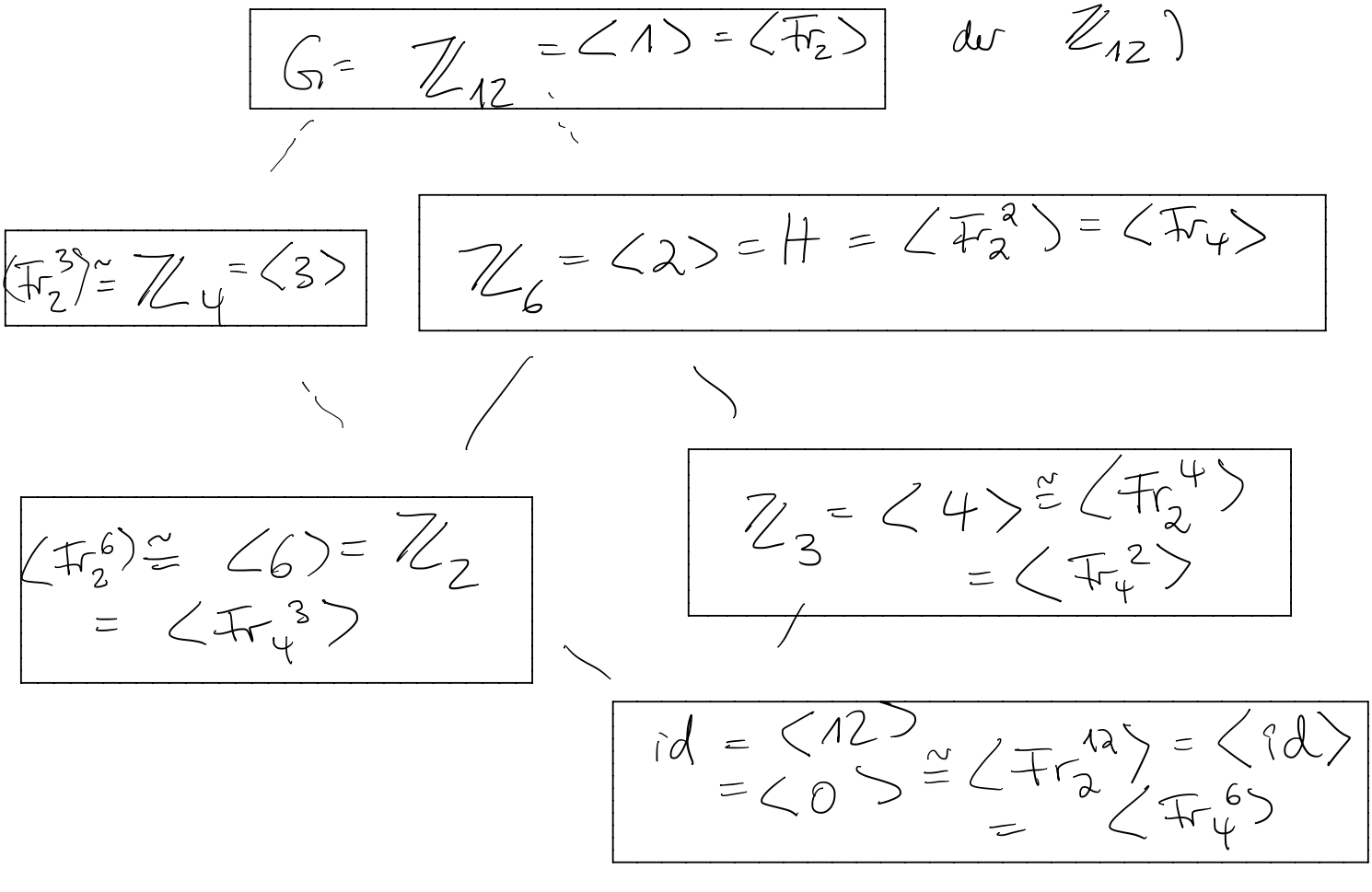
$$\mathrm{Aut}_{F_2}(L) \xrightarrow{\cong} \mathbb{Z}_{12}$$
$$Fr_2 \longmapsto 1$$

$H = \mathrm{Aut}_K(L)$ ist erzeugt von $Fr_2^2 = Fr_4$.

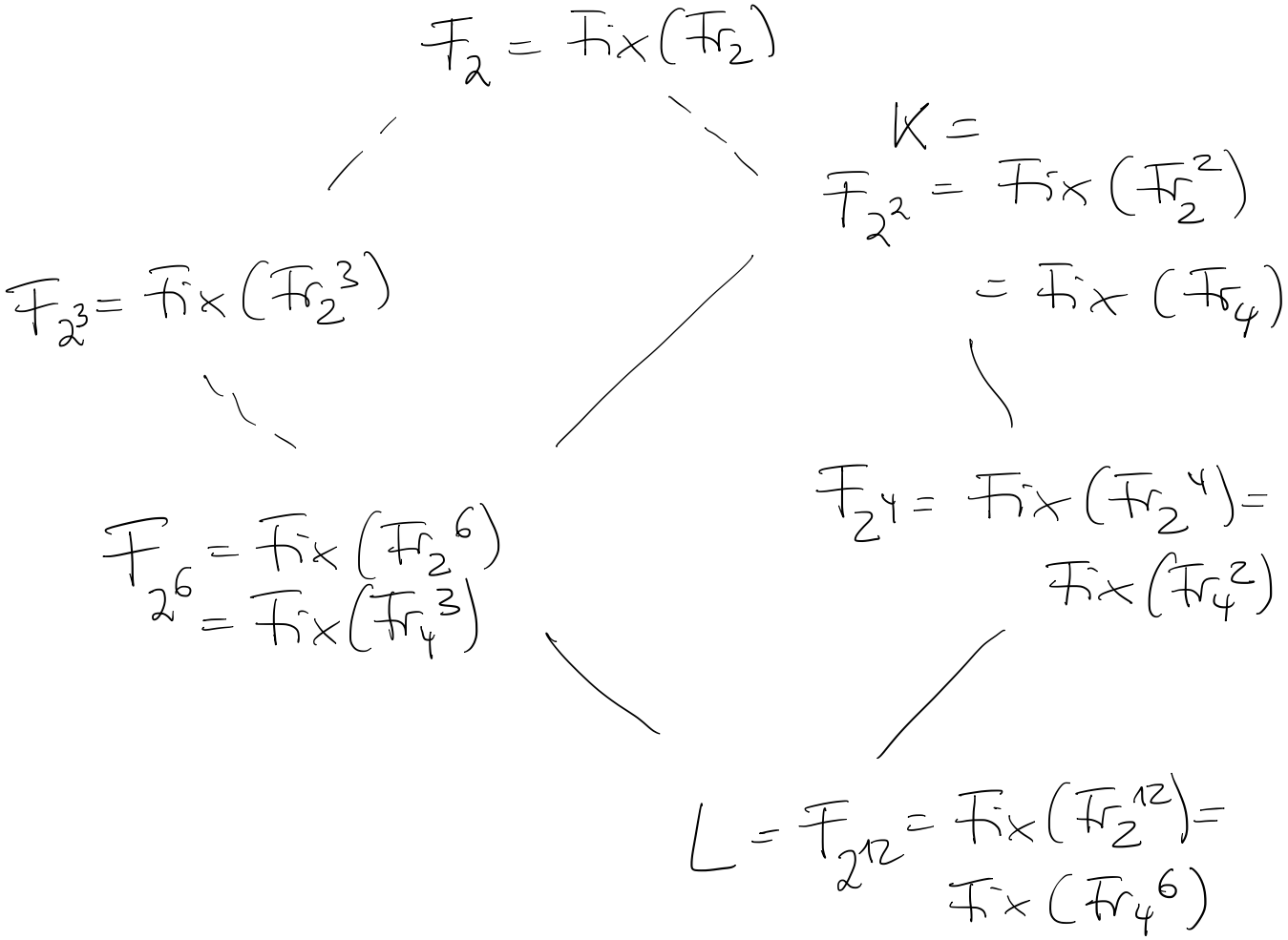
$$\Rightarrow H = \mathrm{Aut}_K(L) \subset \mathrm{Aut}_{F_2}(L) = G_1$$
$$\| \qquad\qquad \|$$
$$\mathbb{Z}_6 = \langle 2 \rangle \subset \mathbb{Z}_{12}$$

Untergruppen der $\mathbb{Z}_{12}$, die auch Untergruppen der $\mathbb{Z}_6 \cong \langle 2 \rangle \subset \mathbb{Z}_{12}$ sind:

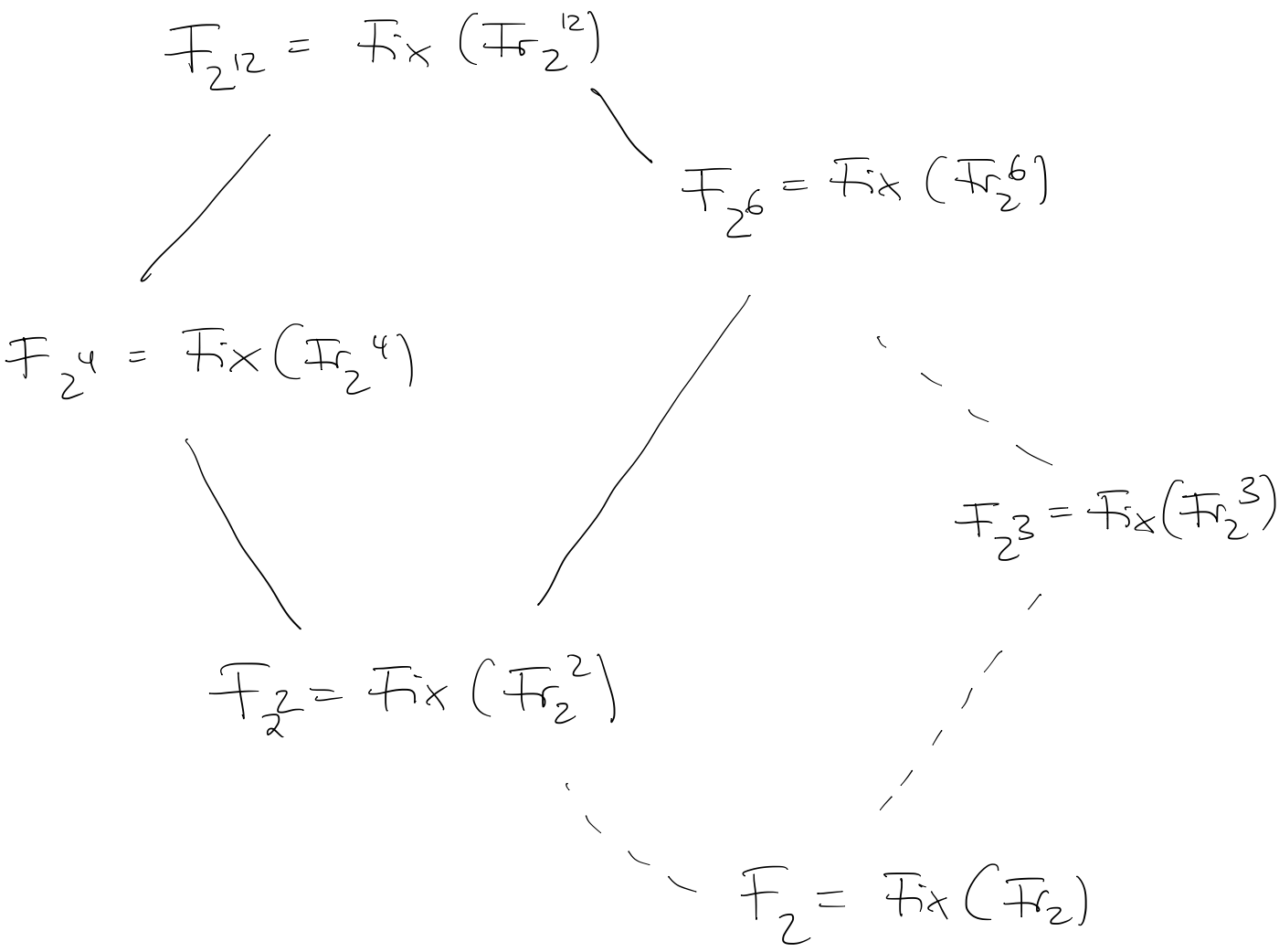
(gestrichelt: alle Untergruppen der $\mathbb{Z}_{12}$)



Das dazugehörige Zwischenkörperdiagramm (gestrichelt: Zwischenkörper von $F_2 \subset L$, die nicht Zwischenkörper von $K \subset L$ sind). Achtung, dieses Diagramm muß man von oben nach unten lesen (i.e. oben steht der kleinste Körper, unten der größte), wenn man es analog zum Untergruppendiagramm betrachten will (mit id unten, G oben), denn "je größer die Gruppe, desto kleiner der Fixkörper".



Wenn man das Unterkörper von unten nach oben (vom kleinsten zum größten Körper) sympathischer findet, dreht man es um:



Dann paßt es so nicht mehr zum Untergruppendiagramm, aber das Untergruppendiagramm läßt sich hier auch in sinnvoller Weise umdrehen, indem wir zu einem Teiler d/n nicht die Untergruppe der Ordnung d listen, sondern die Untergruppe der Ordnung $\frac{n}{d}$, die von $d \cdot 1 \triangleq (\text{Erzeuger})^d$ erzeugt wird:

$id = \langle 12 \rangle = \langle 0 \rangle \cong \langle Fr_2^{12} \rangle = \langle id \rangle = \langle Fr_4^6 \rangle$

(gestrichelt: alle Untergruppen der $\mathbb{Z}_{12}$)

$\langle Fr_2^6 \rangle \cong \langle 6 \rangle = \mathbb{Z}_2 = \langle Fr_4^3 \rangle$

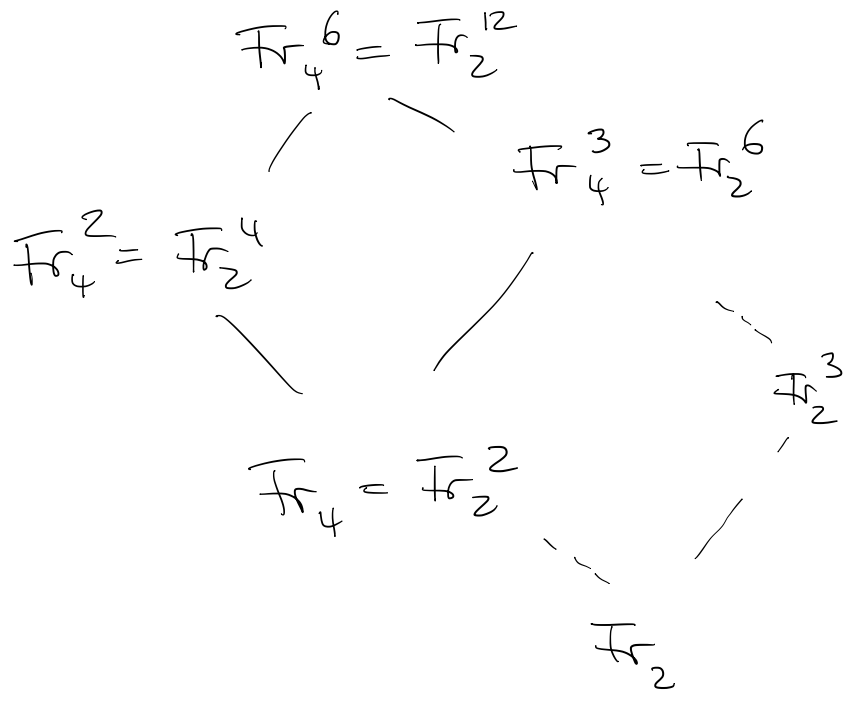
$\mathbb{Z}_3 = \langle 4 \rangle \cong \langle Fr_2^4 \rangle = \langle Fr_4^2 \rangle$

$\mathbb{Z}_6 = \langle 2 \rangle = H = \langle Fr_2^2 \rangle = \langle Fr_4 \rangle$

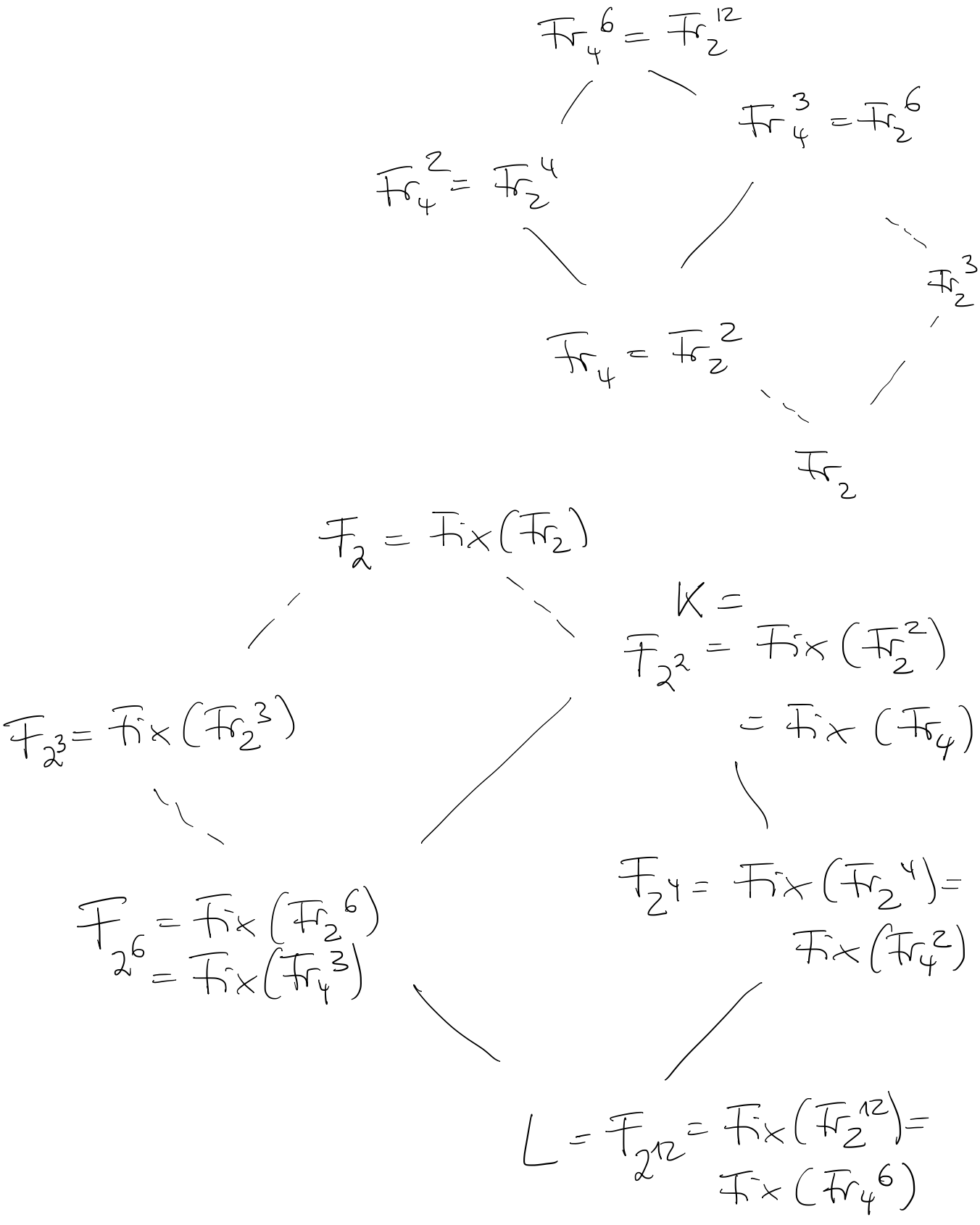
$\langle Fr_2^3 \rangle \cong \mathbb{Z}_4 = \langle 3 \rangle$

$G = \mathbb{Z}_{12} = \langle 1 \rangle = \langle Fr_2 \rangle$

oder kurz gefaßt:



Damit kann man sich das (umgedrehte) Untergruppendiagramm und das Zwischenkörperdiagramm nebeneinanderhalten und sehen, daß es dasselbe ist:



4.7 Die Galoiskorrespondenz

4.7.1 Satz (Satz vom primitiven Element)
Jede endliche separable Körpererweiterung ist einfach.

Beweis: Für endliche Körper: 4.6.9.

Sei $|K| = \infty$.

Beh: Falls $K \subset K[\alpha_1, \beta_1]$, so ist die Erweiterung einfach.
Dann folgt die Aussage mit Induktion.

Seien f, g die Minimalpolynome von α_1, β_1 vom Grad d bzw. e.
Da f und g separabel sind,
gibt es im Zerfällungskörper von $f \cdot g$
d verschiedene Nullstellen $\alpha_1, \dots, \alpha_d$ von f
und e " " $\beta_1, \dots, \beta_e$ von g.

Da $|K| = \infty$ $\exists\, \lambda \in K$ mit

$$\lambda \neq \frac{\alpha_i - \alpha_1}{\beta_1 - \beta_j} \quad \forall\ 1 \leq i \leq d,\ 2 \leq j \leq e.$$

Setze $\gamma = \alpha_1 + \lambda \beta_1$.

Beh: $K[\alpha_1, \beta_1] = K[\gamma]$

„$\supseteq$" klar

„$\subseteq$" Sei $h = f(\gamma - \lambda x) \in K[\gamma][x]$

Dann ist $h(\beta_1) = f(\gamma - \lambda \beta_1) = f(\alpha_1) = 0$.

Das Minimalpolynom von β_1 über $K[\gamma]$ ist also ein Teiler von h und von g. h und g können außer β_1 keine weitere gemeinsame Nullstelle haben, denn wäre $h(\beta_j) = 0$ für $j \geq 2$, so gilt für ein i: $0 = f(\alpha_i) = f(\gamma - \lambda \beta_j) = h(\beta_j)$

$$\Rightarrow \alpha_i = \gamma - \lambda \beta_j = (\alpha_1 + \lambda \beta_1) - \lambda \beta_j$$

$$\alpha_1 + \lambda(\beta_1 - \beta_j)$$

$$\Rightarrow \frac{\alpha_i - \alpha_1}{\beta_1 - \beta_j} = \lambda \quad \lightning$$

Damit hat das Minimalpolynom von β_1 über $K[\gamma]$ Grad 1

$\Rightarrow \beta_1 \in K[\gamma] \Rightarrow \alpha_1 = \gamma - \lambda \beta_1 \in K[\gamma]$.

□

4.7.2 Lemma

Sei $U \subset \mathrm{Aut}(L)$ eine endliche Untergruppe, $\alpha \in L$.
Dann ist α algebraisch über $\mathrm{Fix}(U)$ mit separablem Minimalpolynom

$$f = \prod_{\beta \in U\alpha} (x-\beta) \in \mathrm{Fix}(U)[x]$$

$U\alpha$ ist die Bahn von α unter der Operation von U: $U\alpha = \{\varphi(\alpha) \mid \varphi \in U\}$.

Beweis:

$f(\alpha) = 0$. Für $\varphi \in U$ gilt

$$\varphi(f) = \prod_{\beta \in U\alpha} (x - \varphi(\beta)) = \prod_{\beta \in U\alpha} (x-\beta) = f,$$

denn φ permutiert die Elemente der Bahn.

$\Rightarrow f \in \mathrm{Fix}(U)[x]$

f ist normiert und separabel und wird vom Minimalpolynom $m_\alpha \in \mathrm{Fix}(U)[x]$ geteilt.

Es gilt $m_\alpha(\varphi(\alpha)) = \varphi(m_\alpha(\alpha)) = m_\alpha(\alpha) = 0 \quad \forall \varphi \in U$. Somit sind alle $\beta \in U\alpha$ Nullstellen von $m_\alpha \Rightarrow m_\alpha = f$. □

4.7.3 Satz Sei $K \subset L$ endlich und $U \subset \mathrm{Aut}_K(L)$ eine Untergruppe, dann ist $\mathrm{Fix}(U) \subset L$ eine einfache, normale und separable Erweiterung.

Beweis: Für jedes $\alpha \in L$ ist $m_\alpha \in \mathrm{Fix}(U)[X]$ separabel wegen 4.7.2
$\Rightarrow$ $\mathrm{Fix}(U) \subset L$ separabel.
Wegen 4.7.1 ist $\mathrm{Fix}(U) \subset L$ einfach
$\Rightarrow \exists\, \gamma \in L$: $L = \mathrm{Fix}(U)[\gamma]$.
Sei $m_\gamma \in \mathrm{Fix}(U)[X]$ das Minimalpolynom von γ. Aus 4.7.2 folgt $m_\gamma = \prod_{\beta \in U\gamma} (X-\beta)$, und da $\beta = \varphi(\gamma) \in L$ folgt m_γ zerfällt über L.
Der Zerfällungskörper von m_γ muß die Nullstelle γ enthalten, also $L \subset$ Zerfällungskörper $\Rightarrow$ $L =$ Zerfällungskörper von m_γ
$\overset{4.5.3}{\Rightarrow}$ $\mathrm{Fix}(U) \subset L$ normal. □

4.7.4 Prop Sei $K \subset L$ endlich, $U \subset \mathrm{Aut}_K(L)$ eine Untergruppe.

Dann gilt $\mathrm{Aut}_{\mathrm{Fix}(U)}(L) = U$

und $|U| = [L : \mathrm{Fix}(U)]$.

Beweis: Nach 4.7.1 ∃ $\gamma \in L$ mit $L = \mathrm{Fix}(U)[\gamma]$. Das Minimalpolynom m_γ von γ über $\mathrm{Fix}(U)$ hat den Grad $[L : \mathrm{Fix}(U)]$

$\overset{4.4.10}{\Rightarrow}$ $|\mathrm{Aut}_{\mathrm{Fix}(U)}(L)| \leq [L : \mathrm{Fix}(U)]$

Es gilt $U \subset \mathrm{Aut}_{\mathrm{Fix}(U)}(L)$, denn die Elemente aus U halten $\mathrm{Fix}(U)$ fest.

Mit 4.7.2 folgt $[L : \mathrm{Fix}(U)] = \deg(m_\gamma) = |U\gamma| \leq |U|$

$\Rightarrow |U| \leq |\mathrm{Aut}_{\mathrm{Fix}(U)}(L)| \leq [L : \mathrm{Fix}(U)] \leq |U|$

$\Rightarrow$ Gleichheit, und $U = \mathrm{Aut}_{\mathrm{Fix}(U)}(L)$.

□

4.7.5 Def

Eine endliche, normale, separable Körpererweiterung heißt Galoiserweiterung.

Bsp $\mathrm{char}(K)=0$, $f \in K[X]$, L = Zerfällungskörper, dann ist $K \subset L$ Galoiserweiterung.

4.7.6 Lemma

Sei $K \subset L$ normal und endlich, $L \subset F$ eine Erweiterung. Sei $\varphi: L \hookrightarrow F$ ein Körpermonomorphismus mit $\varphi|_K = id_K$, dann ist $\varphi \in \mathrm{Aut}_K(L)$.

Beweis:

Wegen 4.5.4 ist L Zerfällungskörper eines Polynoms $f \in K[X]$, über L gilt $f = a \cdot \prod (x-\alpha_i)$ und $L = K(\alpha_1, \dots, \alpha_n)$.

Sei $\varphi: L \to F$.

Da $f \in K[X]$ und $\varphi|_K = id_K$ gilt

$0 = \varphi(0) = \varphi(f(\alpha_i)) = f(\varphi(\alpha_i))$

$\Rightarrow \varphi(\alpha_i) \in \{\alpha_1, \dots, \alpha_n\} \quad \forall i$

$\Rightarrow \varphi : L \to L$

und $\varphi|_{\{\alpha_1,\dots,\alpha_n\}} : \{\alpha_1,\dots,\alpha_n\} \to \{\alpha_1,\dots,\alpha_n\}$,

da φ injektiv gilt $\varphi(\{\alpha_1,\dots,\alpha_n\}) = \{\alpha_1,\dots,\alpha_n\}$

$\Rightarrow \forall i : \alpha_i \in \mathrm{Im}(\varphi)$

$\Rightarrow L \subset \mathrm{Im}\,\varphi$

$\Rightarrow \varphi \in \mathrm{Aut}_K(L)$. □

4.7.7 Prop

Sei $K \subset L$ Galoiserweiterung und $K \subset M \subset L$ Zwischenkörper.

Dann gilt $\mathrm{Fix}(\mathrm{Aut}_M(L)) = M$.

Beweis: Da alle M-Automorphismen M festhalten, gilt $M \subset \mathrm{Fix}(\mathrm{Aut}_M(L))$.

Sei $\alpha \in L \setminus M$ und $m_\alpha \in M[x]$ das Minimalpolynom, dann ist $\deg(m_\alpha) \geq 2$.

Wegen 4.5.9 ist $M \subset L$ separabel, insbesondere ist m_α separabel.

Wegen 4.5.5 ist $M \subset L$ normal (insbesondere ist $M \subset L$ Galoiserweiterung). Daher $\exists\, \beta \neq \alpha$, $\beta \in L$, β Nullstelle von m_α. Es gilt

$\varphi: M[\alpha] \cong M[\beta]$. Da $M[\alpha] \subset L$ wegen 4.5.9 separabel ist, $\exists$ mit 4.7.1 γ mit $L = M[\alpha][\gamma]$. Sei $m_\gamma \in M[\alpha][x]$ das Minimalpolynom. Dann ist

$$\Psi: L = M[\alpha][\gamma] \cong M[\alpha][x]/m_\gamma \cong$$

$$M[\beta][x]/\varphi(m_\gamma) = M[\beta][\gamma']$$

ein Isomorphismus, wobei γ' eine Nullstelle von $\varphi(m_\gamma)$ ist.

Damit ist $\Psi: L \xrightarrow{\Psi'} M[\beta][\gamma'] \subset L[\gamma']$ ein Körpermonomorphismus mit $\Psi|_K = id_K$ und $K \subset L$ ist normal

$\overset{4.7.6}{\Rightarrow} \Psi \in Aut_K(L)$. Wir

erhalten so einen Automorphismus
$\varphi : L \to L$, der α nicht festhält,
aber M.

$\Rightarrow \quad \alpha \notin Fix(Aut_M(L))$

$\Rightarrow \quad Fix(Aut_M(L)) \subset M$

$\Rightarrow \quad Fix(Aut_M(L)) = M$ □

4.7.8 Korollar

$K \subset L$ Galoiserweiterung $\Leftrightarrow$
$Fix(Aut_K(L)) = K$

Beweis: „$\Rightarrow$" 4.7.7
„$\Leftarrow$" 4.7.3 ($Fix(U) \subset L$ ist Galoiserweiterung) □

4.7.9 Satz (Hauptsatz der Galoistheorie)

Sei $K \subset L$ Galoiserweiterung.

1) $\{$Untergruppen von $Aut_K(L)\}$ $\overset{1:1}{\longleftrightarrow}$ $\{$Zwischenkörper von $K \subset L\}$

$U \longmapsto Fix(U)$

$Aut_M(L) \longleftarrow M$

2) $|Aut_M(L)| = [L:M]$

3) $M \subset L$ ist Galoiserweiterung.

4) $K \subset M$ ist Galoiserweiterung $\Leftrightarrow$ $Aut_M(L) \subset Aut_K(L)$ Normalteiler, dann gilt $Aut_K(M) \cong Aut_K(L) / Aut_M(L)$.

Beweis:

1) Wegen 4.7.4 gilt $U = Aut_{Fix(U)}(L)$, wegen 4.7.7 $Fix(Aut_M(L)) = M$ $\Rightarrow$ die beiden Abb. $U \mapsto Fix(U)$ und $M \mapsto Aut_M(L)$ sind inves zueinander und liefern daher die Bijektion.

2) Folgt aus 4.7.4, da jeder Zwischenkörper ein Fixkörper ist.

3) $M \subset L$ ist endlich, normal (4.5.5), separabel (4.5.9).

4) „$\Leftarrow$" Wegen 4.5.9 ist $K \subset M$ separabel.
$K \subset M$ ist endlich.

Beh.: $K \subset M$ ist normal.

Sei $g \in K[X]$ irreduzibel mit Nullstelle $\alpha \in M$. Da $K \subset L$ normal, zerfällt g über L in Linearfaktoren.
Sei $\beta \in L$ eine Nullstelle.
Wir zeigen $\beta \in \mathrm{Fix}(\mathrm{Aut}_M(L)) = M$.
Sei $\varphi \in \mathrm{Aut}_M(L)$.
Wie im Beweis von 4.7.7 $\exists$ $\Psi: L \to L$ mit $\Psi|_K = \mathrm{id}_K$ und $\Psi(\alpha) = \beta$. Es gilt
$\Psi^{-1} \circ \varphi \circ \Psi = \varphi' \in \mathrm{Aut}_M(L)$ (Normalteiler),
also $\varphi(\beta) = \varphi(\Psi(\alpha)) = \Psi(\varphi'(\alpha)) \overset{\alpha \in M}{=}$
$\Psi(\alpha) = \beta \Rightarrow \beta \in \mathrm{Fix}(\mathrm{Aut}_M(L))$.
Damit ist $K \subset M$ normal und daher Galoiserweiterung.

"$\Rightarrow$" Sei $K \subset M$ normal. Betrachte

$$\pi : \mathrm{Aut}_K(L) \longrightarrow \mathrm{Aut}_K(M)$$
$$\varphi \longmapsto \varphi|_M$$

- Wohldefiniert, i.e. $\varphi|_M : M \xrightarrow{\sim} M$ wegen Lemma 4.7.6
- Gruppenhomomorphismus
- $\ker(\pi) = \{\varphi \mid \varphi|_M = id\} = \mathrm{Aut}_M(L)$
- π ist surjektiv, da sich jeder Automorphismus von M zu einem von L erweitern läßt, da $M \subset L$ endlich.

$\Rightarrow \mathrm{Aut}_M(L)$ ist Normalteiler als Kern eines Gruppenhomomorphismus und

$$\mathrm{Aut}_K(L) / \mathrm{Aut}_M(L)$$
$$= \mathrm{Aut}_K(L) / \ker(\pi) \cong \mathrm{Im}(\pi)$$
$$= \mathrm{Aut}_K(M).$$

□

4.7.10 Korollar Sei $K \subset L$ endlich.

$K \subset L$ ist Galoiserweiterung $\Leftrightarrow$

$|\mathrm{Aut}_K(L)| = [L : K]$

Beweis:

„$\Rightarrow$" Aus dem Hauptsatz der Galoistheorie 4.7.9 (2).

„$\Leftarrow$" sei $F = \mathrm{Fix}(\mathrm{Aut}_K(L))$, aus 4.7.4 folgt $\mathrm{Aut}_F(L) =$

$\mathrm{Aut}_{\mathrm{Fix}(\mathrm{Aut}_K(L))}(L) = \mathrm{Aut}_K(L)$.

und $|\mathrm{Aut}_K(L)| = [L : \mathrm{Fix}(\mathrm{Aut}_K(L))]$

$= [L : F]$.

Es gilt

$[L : F] \cdot [F : K] = [L : K] =$

$|\mathrm{Aut}_K(L)| = |\mathrm{Aut}_F(L)| = [L : F]$

$\Rightarrow [F : K] = 1 \Rightarrow K = F$

$\overset{4.7.3}{\Rightarrow}$ $K \subset L$ ist Galoiserweiterung. $\square$

4.7.11 Korollar:

Sei $K \subset L$ endlich.
$K \subset L$ ist Galoiserweiterung $\Leftrightarrow$
L ist Zerfällungskörper eines
separablen Polynoms $f \in K[X]$.

Beweis:

„$\Rightarrow$" $K \subset L$ ist normal $\overset{4.5.4}{\Rightarrow}$ L ist
Zerfällungskörper eines Polynoms $f \in K[X]$.
Sei $f = c \cdot f_1 \cdots f_r$ mit normierten
irreduziblen Faktoren f_i. Sei
$\alpha_i \in L$ eine Nullstelle von f_i.
Dann ist f_i das Minimalpolynom
von α_i, und da $K \subset L$ separabel
ist, ist jedes f_i separabel und
damit f.

„$\Leftarrow$" Aus 4.5.4 folgt $K \subset L$ normal.
Aus 4.4.10 folgt $|\mathrm{Aut}_K(L)| =$
$[L:K]$ und mit 4.7.10 daher
$K \subset L$ ist Galoiserweiterung. □

4.7.12 Bsp

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

$\mathbb{Q} \subset L$ ist Galoiserweiterung.

Die Nullstellen von f sind

$\alpha_1 = \sqrt[4]{2}$, $\alpha_2 = i\sqrt[4]{2}$, $\alpha_3 = -\sqrt[4]{2}$,

$\alpha_4 = -i\sqrt[4]{2}$.

$L = \mathbb{Q}(\alpha_1, \dots, \alpha_4) = \mathbb{Q}[i, \sqrt[4]{2}]$.

$|\mathrm{Aut}_{\mathbb{Q}}(L)| = [L : \mathbb{Q}] =$

$[L : \mathbb{Q}[\sqrt[4]{2}]] \cdot [\mathbb{Q}[\sqrt[4]{2}] : \mathbb{Q}] =$

$2 \cdot 4 = 8,$

da x^4-2 das Minimalpolynom von $\sqrt[4]{2}$ über $\mathbb{Q}$ ist und x^2+1 das von i über $\mathbb{Q}[\sqrt[4]{2}]$.

Ein $\mathbb{Q}$-Automorphismus muß Nullstellen der Minimalpolynome auf Nullstellen abbilden, somit gibt es folgende Möglichkeiten:

$$\begin{array}{lcccccccc} i & \mapsto & i & i & i & i & -i & -i & -i & -i \\ \sqrt[4]{2} & \mapsto & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ & & \varphi_1 & \varphi_2 & \varphi_3 & \varphi_4 & \varphi_5 & \varphi_6 & \varphi_7 & \varphi_8 \end{array}$$

Es gilt $\varphi_1 = id$.

Um $\mathrm{Aut}_{\mathbb{Q}}(L) \subset S_4$ darzustellen, bestimmen wir die Operation der φ_i auf der Nullstellenmenge $\{\alpha_1, \dots, \alpha_4\}$:

$\varphi_1 = id$,

φ_2: $\alpha_1 \mapsto \alpha_2$, $\alpha_2 = i\sqrt[4]{2} \mapsto i \cdot i\sqrt[4]{2} = -\sqrt[4]{2} = \alpha_3$

$\alpha_3 = -\sqrt[4]{2} \mapsto -i\sqrt[4]{2} = \alpha_4$

$\alpha_4 = -i\sqrt[4]{2} \mapsto -i \cdot i\sqrt[4]{2} = \alpha_1 \Rightarrow \varphi_2 = (1234)$

φ_3: $\alpha_1 \longmapsto \alpha_3$

$\alpha_2 = i\sqrt[4]{2} \longmapsto i(-\sqrt[4]{2}) = \alpha_4$

$\alpha_3 = -\sqrt[4]{2} \longmapsto -(-\sqrt[4]{2}) = \alpha_1$

$\alpha_4 = -i\sqrt[4]{2} \longmapsto -(-i\sqrt[4]{2}) = \alpha_2$

$\Rightarrow \varphi_3 = (13)(24)$

φ_4: $\alpha_1 \longmapsto \alpha_4$

$\alpha_2 = i\sqrt[4]{2} \longmapsto i(-i\sqrt[4]{2}) = \alpha_1$

$\alpha_3 = -\sqrt[4]{2} \longmapsto -(-i\sqrt[4]{2}) = \alpha_2$

$\alpha_4 = -i\sqrt[4]{2} \longmapsto -i(-i\sqrt[4]{2}) = \alpha_3$

$\Rightarrow \varphi_4 = (1432)$

φ_5: $\alpha_1 \longmapsto \alpha_1$

$\alpha_2 = i\sqrt[4]{2} \longmapsto -i\sqrt[4]{2} = \alpha_4$

$\alpha_3 = -\sqrt[4]{2} \longmapsto \alpha_3$

$\alpha_4 = -i\sqrt[4]{2} \longmapsto i\sqrt[4]{2} = \alpha_2$

$\Rightarrow \varphi_5 = (24)$

φ_6: $\alpha_1 \longmapsto \alpha_2$

$\alpha_2 = i\sqrt[4]{2} \longmapsto (-i)(i\sqrt[4]{2}) = \sqrt[4]{2} = \alpha_1$

$\alpha_3 = -\sqrt[4]{2} \longmapsto -i\sqrt[4]{2} = \alpha_4$

$\alpha_4 = -i\sqrt[4]{2} \longmapsto -(-i)(i\sqrt[4]{2}) = -\sqrt[4]{2} = \alpha_3$

$\Rightarrow \varphi_6 = (12)(34)$

φ_7: $\alpha_1 \longmapsto \alpha_3$

$\alpha_2 = i\sqrt[4]{2} \longmapsto (-i)(-\sqrt[4]{2}) = i\sqrt[4]{2} = \alpha_2$

$\alpha_3 = -\sqrt[4]{2} \longmapsto \sqrt[4]{2} = \alpha_1$

$\alpha_4 = -i\sqrt[4]{2} \longmapsto -(-i)(-\sqrt[4]{2}) = \alpha_4$

$\Rightarrow \varphi_7 = (13)$

φ_8 : $\alpha_1 \longmapsto \alpha_4$

$\alpha_2 = i\sqrt[4]{2} \mapsto (-i)(-i\sqrt[4]{2}) = \alpha_3$

$\alpha_3 = -\sqrt[4]{2} \mapsto -(-i\sqrt[4]{2}) = i\sqrt[4]{2} = \alpha_2$

$\alpha_4 = -i\sqrt[4]{2} \mapsto -(-i)(-i\sqrt[4]{2}) = \sqrt[4]{2} = \alpha_1$

$\Rightarrow \varphi_8 = (14)(23)$

$\Rightarrow \mathrm{Aut}_{\mathbb{Q}}(L) =$

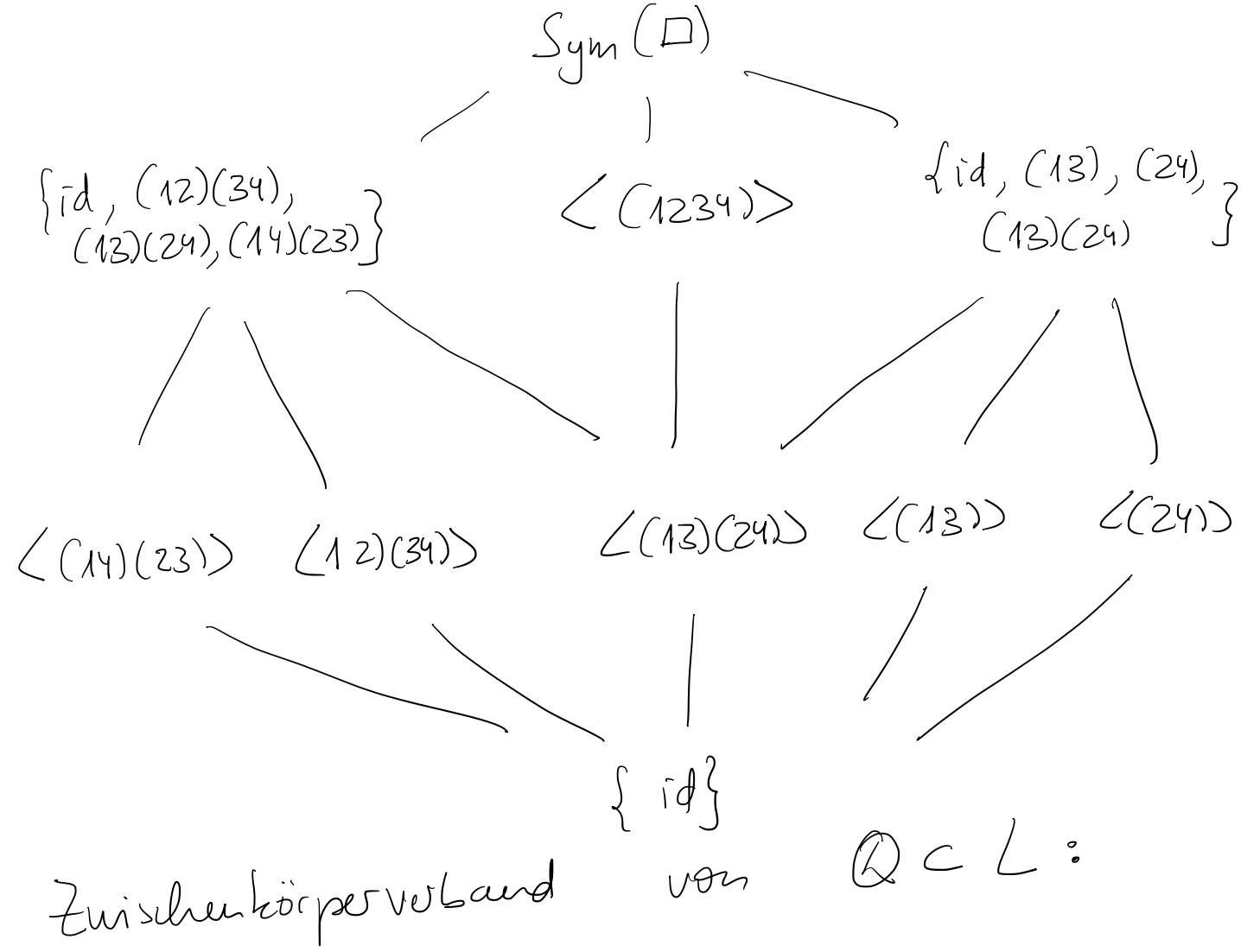
$\{ id, (1234), (13)(24), (1423), (13), (24), (14)(23), (12)(34) \}$

$\mathrm{Sym}(\text{Quadrat}) = \mathrm{Sym}\left(\begin{smallmatrix} 1 & & 4 \\ 2 & & 3 \end{smallmatrix}\right)$

$= \mathrm{Sym}\left(\begin{smallmatrix} \alpha_1 & & \alpha_4 \\ \alpha_2 & & \alpha_3 \end{smallmatrix}\right)$

wobei die Automorphismen mit $i \mapsto -i$ genau die Spiegelungen sind, die mit $i \mapsto i$ genau die Drehungen.

Untergruppenverband der $\mathrm{Sym}\left(\begin{smallmatrix}1&&4\\&\square&\\2&&3\end{smallmatrix}\right)$:



Zwischenkörperverband von $\mathbb{Q} \subset L$: