1. Gruppen

Als bekannt vorausgesetzt werden

- Gruppen, Untergruppen, Homomorphismen
- Normalteiler, Faktorgruppen, Homomorphiesatz
- symmetrische Gruppe
- zyklische Gruppen
- Ordnungen und der Satz von Lagrange

1.1 Operationen

1.1.1 Def Sei $(G, *)$ eine Gruppe, M eine Menge. Eine **Operation** von G auf M ist eine Abbildung

$$\cdot : G \times M \longrightarrow M :$$
$$(g, m) \longmapsto g \cdot m$$

die folgende Eigenschaften erfüllt:

1) $e \cdot m = m \quad \forall\, m \in M$

2) $(a * b) \cdot m = a \cdot (b \cdot m)$
$\forall\, a, b \in G, \quad m \in M$

1.1.2 Bemerkung: Man kann eine Operation als einen Gruppenhomomorphismus

$$\varphi : G \longrightarrow S(M) = \{ f : M \to M, f \text{ bijektiv} \}$$
$$g \longmapsto \varphi(g) : M \longrightarrow M$$
$$m \longmapsto g \cdot m$$

auffassen:

- φ ist wohldefiniert:

$\varphi(g)$ ist injektiv, denn aus $g \cdot m_1 = g \cdot m_2$ folgt

$$g^{-1} \cdot (g \cdot m_1) = g^{-1} \cdot (g \cdot m_2) \Rightarrow$$

$$(g^{-1} * g) \cdot m_1 = (g^{-1} * g) \cdot m_2 \Rightarrow$$

$$e \cdot m_1 = e \cdot m_2 \Rightarrow$$

$$m_1 = m_2$$

$\varphi(g)$ ist surjektiv, denn für $m \in M$ ist $g^{-1} \cdot m \in M$ und

$$\varphi(g)(g^{-1} \cdot m) = g \cdot (g^{-1} \cdot m) =$$

$$(g * g^{-1}) \cdot m = e \cdot m = m$$

$$\Rightarrow \varphi(g) \in \mathfrak{S}(M)$$

- φ ist Gruppenhomomorphismus:

$$\varphi(g*h) : M \longrightarrow M : m \longmapsto (g*h) \cdot m = g \cdot (h \cdot m)$$

$=$

$$\varphi(g) \circ \varphi(h) : M \longrightarrow M : m \longmapsto \varphi(g)(\varphi(h)(m)) = g \cdot (h \cdot m)$$

Umgekehrt liefert ein Gruppenhomomorphismus
$\varphi: G \longrightarrow \mathfrak{S}(M)$ durch
$g \cdot m := \varphi(g)(m)$ eine Operation,
denn $e \cdot m = \varphi(e)(m) = id(m) = m$
und $(g * h) \cdot m = \varphi(g * h)(m) = \varphi(g) \circ \varphi(h)(m)$
$= g \cdot (h \cdot m)$

1.1.3 Beispiele

1) $GL_n(K)$ (= invertierbare $n \times n$-Matrizen über einem Körper K)

operiert auf K^n durch
$A \cdot x := A \cdot x$ (Matrixmultiplikation),
denn $\mathbb{1}_n \cdot x = x$ und
$(A \cdot B) \cdot x = A \cdot (B \cdot x)$.

2) $\mathfrak{S}_n$ (= $\mathfrak{S}(\{1, \dots, n\})$) operiert auf $\{1, \dots, n\}$ durch
$\sigma \cdot i := \sigma(i)$, denn
$id \cdot i = id(i) = i$ und
$(\sigma \circ \sigma') \cdot i = \sigma(\sigma'(i)) = \sigma \cdot (\sigma' \cdot i)$.

3) $\mathfrak{S}_n$ operiert auf $\mathbb{R}^n$, indem wir für $\sigma \in \mathfrak{S}_n$ die Permutation der Einheitsvektoren $e_i \longmapsto e_{\sigma(i)}$

linear fortsetzen, zu einer Permutationsmatrix A_b (in jeder Zeile und Spalte eine 1 und sonst nur Nullen).

Bsp: $n=3$, $A_{(12)} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

Für $x \in K^n$ gilt

$$id \cdot x = A_{id} \cdot x = 1_n \cdot x = x$$

und

$$(b \circ b') \cdot x = (A_b \cdot A_{b'}) \cdot x = A_b \cdot (A_{b'} \cdot x)$$
$$= b \cdot (b' \cdot x).$$

4) Eine Gruppe operiert durch die Gruppenoperation auf sich selbst:

$$G \times G \longrightarrow G : (g, h) \longmapsto g \cdot h$$

denn $e \cdot h = h$, $(g_1 \cdot g_2) \cdot h = g_1 \cdot (g_2 \cdot h)$.

5) Sei $U \subset G$ eine Untergruppe, dann operiert U auf G durch die Gruppenoperation:

$$U \times G \longrightarrow G : (u, g) \longmapsto u \cdot g$$

denn $e \cdot g = g$, $(u_1 \cdot u_2) \cdot g = u_1 \cdot (u_2 \cdot g)$.

1.1.4 Def Eine Operation von G auf M heißt treu, wenn der zugehörige Gruppenhomomorphismus φ injektiv ist, i.e. $\ker(\varphi) = \{e\}$, i.e. nur e wird auf id_M abgebildet durch φ, i.e. $\forall\, g \neq e \quad \exists\, m : g \cdot m \neq m$.

1.1.5 Bsp Wir betrachten die Bsp von eben:

1) Damit $A \cdot x = x \;\forall x \in K^n$ gilt, muss $A = \mathbb{1}_n \Rightarrow$ treu

2) Damit $\sigma \cdot i = i \;\forall i \in \{1, \dots, n\} \Rightarrow$ $\sigma(i) = i \Rightarrow \sigma = id \Rightarrow$ treu

3) wie 1)

4) $g \cdot h = h \;\forall\, h \in G \Rightarrow g = e$

$\Rightarrow$ treu

5) genauso

6) Sei

$G = \{\text{obere Dreiecksmatrizen}, \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}\} \subset GL_2(K)$

↑ Untergruppe

$U = \langle e_1 \rangle \subset K^2$.

$G \times U \to U : (A, x) \mapsto A \cdot x$

ist eine Operation, denn

für $x \in U$ ist $A \cdot x \in U$

$\left(\begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} * \\ 0 \end{pmatrix} \in U \right)$

$1\!\!1_2 \cdot x = x \quad \forall x \in U$ und

$(A \cdot B) \cdot x = A \cdot (B \cdot x)$.

Als Gruppenhomomorphismus betrachtet:

$\varphi : G \to S(U) : A \mapsto f_A$

mit $f_A : U \to U : x \mapsto A \cdot x$

$\ker(\varphi) = \{ A \mid f_A = id|_U \} =$

$\left\{ \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \right\} \supsetneq \{ 1\!\!1_2 \}$

Die Operation ist also nicht treu.

Anders gesagt: $\exists\, A \neq 1\!\!1_2$ mit

$A \cdot x = x \quad \forall x \in U$, z. B.

$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, denn

$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ 0 \end{pmatrix}$.

Erinnerung: $\mathbb{R}^n$ ist ein euklidischer Vektorraum.

Die orthogonale Gruppe ist

$O(n) = \{$ orthogonale Matrizen $\}$

(Spalten sind Orthonormalbasis, $A \cdot A^T = \mathbb{1}_n$).

A orthogonal $\Leftrightarrow$ f_A orthogonal $\Leftrightarrow$

$\langle x, x \rangle = \langle f_A(x), f_A(x) \rangle \quad \forall x \in \mathbb{R}^n$

$\Leftrightarrow$ f_A ist längen- und winkelerhaltend.

1.1.6 Def: Die Menge der affinen Isometrien auf $\mathbb{R}^n$ ist

$E(n) := \{ x \longmapsto Ax + b, \; A \in O(n), b \in \mathbb{R}^n \}$

Durch Hintereinanderausführung ist $E(n)$ eine Gruppe.

Für $M \subset \mathbb{R}^n$ definieren wir eine Untergruppe von $E(n)$, die auf M operiert:

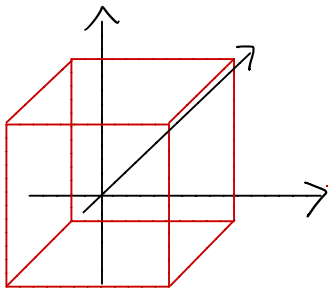
1.1.7 Def: Sei $M \subset \mathbb{R}^n$ eine Teilmenge.

$\mathrm{Sym}(M) = \{ f \in E(n) \mid f(M) = M \}$

heißt die Symmetriegruppe von M, ihre Elemente Symmetrien.

Bsp:

$Q = \{ x \in \mathbb{R}^3 \mid |x_i| \leq 1 \ \forall i \}$ = Würfel



Da Symmetrien abstandserhaltend sind, muß die Teilmenge der Punkte größten Abstands zu 0 (= Eckpunkte) auf sich selbst überführt werden. Damit ist

$$\mathrm{Sym}(Q) \subset \left\{ \begin{pmatrix} \pm 1 & & \\ & \pm 1 & \\ & & \pm 1 \end{pmatrix} \cdot A_\sigma \mid \sigma \in S_3 \right\}$$

und da jede solche Abb in $\mathrm{Sym}(Q)$ ist gilt Gleichheit.

Bsp: Die Symmetriegruppe eines gleichseitigen Dreiecks $\triangle \subset \mathbb{R}^2$ ist

$S_3 = \{ \mathrm{id}, (123), (132), (12), (13), (23) \}$

und besteht aus Drehungen

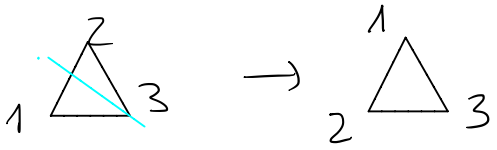
id (um 0°),

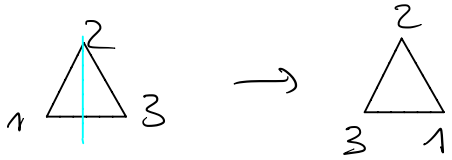
(123): $_1\triangle_3 \to {}_3\triangle_2$ (um 120°)

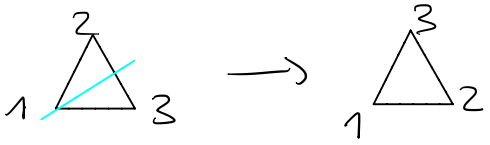
(132): $_1\triangle_3 \to {}_2\triangle_1$ (um 240°)

sowie

Spiegelungen

(12): 

(13): 

(23): 

1.1.8 Bem Für $M \subset \mathbb{R}^n$ definiert

$$\begin{aligned} \mathrm{Sym}(M) \times M &\longrightarrow M : \\ (f, m) &\longmapsto f \cdot m := f(m) \end{aligned}$$

eine Operation, denn $id \cdot m = m$ und $(f \circ g) \cdot m = f(g(m)) = f \cdot (g \cdot m)$.

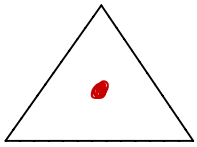
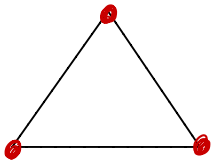
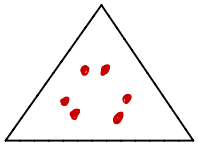
1.1.9 Def Sei $G \times M \to M$ eine Operation.

$Gm := \{ g \cdot m \mid g \in G \} \subset M$ heißt die Bahn von m.

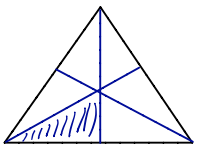
1.1.10 Bsp: Sei $\triangle$ ein gleichseitiges Dreieck in $\mathbb{R}^2$, wir betrachten

die Operation $\mathrm{Sym}(\triangle) \times \triangle \to \triangle$

und Bahnen für verschiedene Punkte:

Man kann die Operation auf die Potenzmenge von $\triangle$ fortsetzen und hier Bahnen betrachten: die Bahn des kleinen Dreiecks ist $\triangle$ z.B.



1.1.11 Bsp $m\mathbb{Z} \subset \mathbb{Z}$ ist Untergruppe bezüglich $+$.

Betrachte die dadurch induzierte Operation $m\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$: $(mz, a) \mapsto mz + a$.

Die Bahnen dieser Operation sind die Restklassen mod m.

1.1.12 Bemerkung: Man kann eine Untergruppe $U \subset G$ auch von rechts operieren lassen

durch $U \times G \to G : (u,g) \mapsto gu$.

Die Bahnen dieser Operation sind $gU = \{gu \mid u \in U\}$, die Linksnebenklassen.

Für die übliche Operation von links sind die Bahnen die $Ug = \{ug \mid u \in U\}$, die Rechtsnebenklassen.

Normalteiler sind also Untergruppen, für die die Bahnen unter Operation von links und rechts gleich sind.

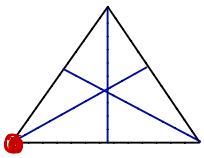
1.1.13 Def Sei $G \times M \to M$ eine Operation.

Für $N \subset M$ ist

$\mathrm{Stab}(N) := \{g \in G \mid \{gn \mid n \in N\} =: gN = N\}$

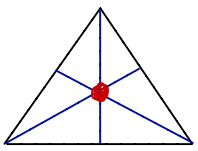
der Stabilisator von N.

1.1.14 Bsp: (siehe Bsp 1.1.10):

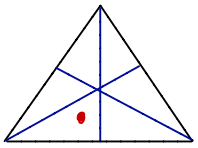


1

$\mathrm{Stab}(1) = \{id, (23)\}$



$\mathrm{Stab} = S_3$



$\mathrm{Stab} = \{id\}$

1.1.15 Bem $\bigcap_{n \in M} \mathrm{Stab}(n)$ ist die Untergruppe von $\mathrm{Sym}(M)$, die M punktweise festhält.

1.1.16 Lemma: Sei $G \times M \to M$ eine Operation, $N \subset M$. $\mathrm{Stab}(N)$ ist eine Untergruppe.

Beweis: Seien $a, b \in \mathrm{Stab}(N) \Rightarrow$
$aN = N$, $bN = N \Rightarrow (ab)N = a(bN) =$
$aN = N \Rightarrow ab \in \mathrm{Stab}(N)$ und
$a^{-1}(aN) = a^{-1}N = (a^{-1}a)N = eN = N$
$\Rightarrow a^{-1} \in \mathrm{Stab}(N)$.
$\mathrm{Stab}(N) \neq \emptyset$, denn $id \in \mathrm{Stab}(N)$. □

1.1.17 Lemma Sei $G \times M \to M$ eine Operation, $m_1, m_2 \in M$. Die Bahnen von m_1 und m_2 sind entweder gleich oder disjunkt, i.e.
$Gm_1 = Gm_2$ oder $Gm_1 \cap Gm_2 = \emptyset$.

Beweis: Angenommen, $Gm_1 \cap Gm_2 \neq \emptyset$
$\Rightarrow \exists\, m_3 \in Gm_1 \cap Gm_2 \Rightarrow$
$\exists\, g_1, g_2 \in G$: $m_3 = g_1 m_1 = g_2 m_2$

$\Rightarrow m_2 = g_2^{-1} g_1 m_1 \in G m_1$

$\Rightarrow G m_2 \subset G m_1$ und analog

$G m_1 \subset G m_2$, also Gleichheit. □

1.1.18 Bsp S_n operiert auf $\{1, \dots, n\}$.

Sei $n=4$, $\sigma = (123)$, dann zerlegt σ $\{1, \dots, n\}$ in die disjunkten Bahnen $\{1,2,3\} \dot\cup \{4\}$.

Sei $n=5$, $\sigma = (123)(45)$, dann zerlegt σ $\{1, \dots, n\}$ in die disjunkten Bahnen $\{1,2,3\} \dot\cup \{4,5\}$.

Allgemeiner entspricht die Zerlegung in Bahnen der Zerlegung in Zykel.

1.1.19 Satz (Satz von Cayley)

Sei G eine Gruppe. Dann existiert eine Menge M und ein injektiver Gruppenhomomorphismus $f: G \longrightarrow S(M)$.
Ist G endlich, so kann man M auch endlich wählen.
Insbesondere kann man jede Gruppe als Untergruppe der Permutationsgruppe einer Menge auffassen.

Beweis: Wir lassen G durch Gruppenoperation auf sich selbst operieren und erhalten dadurch den Gruppenhomomorphismus

$$\varphi: G \longrightarrow S(G): g \longmapsto \sigma_g$$

mit $\sigma_g: G \longrightarrow G: h \longmapsto gh$

Da die Gruppenoperation treu ist, ist φ injektiv. □

Bemerkung: Man betrachtet oft Monomorphismen $\varphi: G \longrightarrow GL_n(K)$

So erhält man Darstellungen von G durch Matrizen, diese heißen lineare Darstellungen von G.

1.1.20 Satz Sei $G \times M \to M$ eine Operation, $m \in M$, $U = \mathrm{Stab}(m)$.

$$G/U \longrightarrow Gm : gU \mapsto gm$$

ist bijektiv.

Beweis: Wohldefiniert:
Sei $g \sim h$, also $gU = hU \Rightarrow$
$\exists u \in U: gu = h \Rightarrow$
$hm = (gu)m = g(um) = gm$,
da m von U stabilisiert wird.

Injektiv: $gm = hm \Rightarrow h^{-1}gm = m$
$\Rightarrow h^{-1}g$ stabilisiert $m \Rightarrow$
$h^{-1}g \in U \Rightarrow g \sim h \Rightarrow gU = hU$.

Surjektiv klar. □

1.1.21 Korollar: Sei $G \times M \to M$ eine Operation, $m \in M$, dann gilt

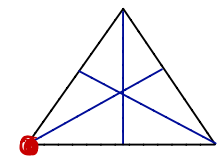
$$|Gm| \cdot |\mathrm{Stab}(m)| = |G|.$$

Beweis: Sei $U = \mathrm{Stab}(m)$.

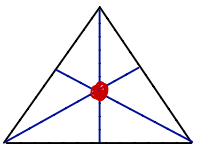
$$|G_m| \cdot |U| \overset{1.1.20}{=} |G/U| \cdot |U|$$

$$= |G| \quad \text{wegen Satz von Lagrange.} \quad \square$$

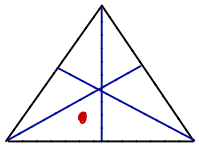
1.1.22 Bsp Im gleichseitigen Dreieck $\triangle \subset \mathbb{R}^2$ mit der Operation von $\mathrm{Sym}(\triangle)$ gilt: (siehe 1.1.10 und 1.1.14)



Bahnlänge = 3
$|\mathrm{Stab}| = 2$



1
6



6
1

1.1.23 Satz (Bahnengleichung)

Sei M endlich, $G \times M \to M$ eine Operation, $R \subset M$ eine Teilmenge, die aus jeder Bahn genau ein Element enthält. Dann gilt

$$|M| = \sum_{r \in R} |G| / |\mathrm{Stab}(r)|$$

Beweis: M ist die disjunkte Vereinigung

seiner Bahnen. Für $r \in R$ hat die Bahn Gr $|G|/|\mathrm{Stab}(r)|$ Elemente wegen Satz 1.1.20. □

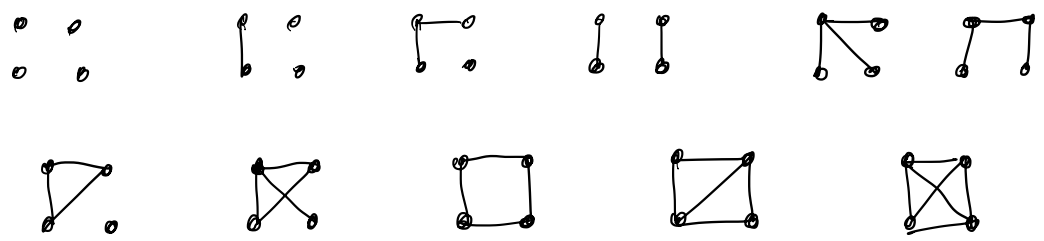
Anwendung der Bahnengleichung:
Klassifikation von Graphen bis auf Isomorphie:

1.1.24 Def Ein Graph ist ein Paar $G = (V, E)$ aus einer Menge V von Ecken und E von Kanten, $E \subset V \times V$. Wir betrachten ungerichtete Graphen, d.h. wir fordern, daß E symmetrisch ist, also aus $(i,j) \in E$ folgt $(j,i) \in E$ – dies steht dann für die Kante zwischen i und j. Wir erlauben keine mehrfachen Kanten und keine Schleifen – $(i,i) \notin E$ $\forall i$.
Ein Isomorphismus von Graphen (V,E), (V',E') ist eine Bijektion $\varphi: V \to V'$, die eine Bijektion

$E \longrightarrow E'$ induziert.

1.1.25 Satz Es gibt 11 Isomorphieklassen von Graphen mit 4 Ecken.

Beweis:

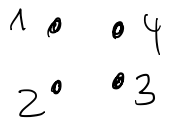
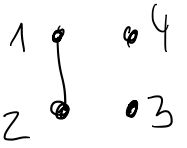
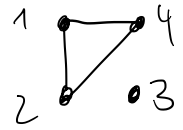
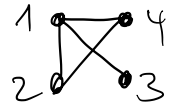
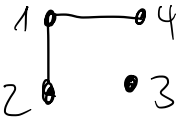
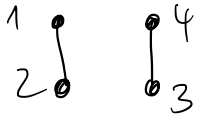
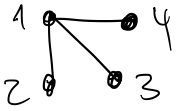
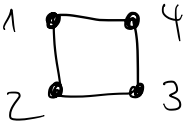
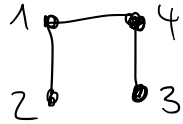
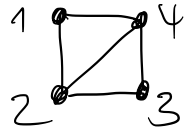
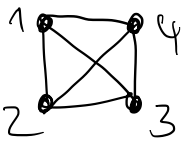


sind paarweise nicht isomorph.

Sei $V = \{1,2,3,4\}$, $M = \{(V,E) \text{ Graph}\}$

$\#M = 2^6 = 64$, da jede der Kanten 12, 13, 14, 23, 24, 34 dabei sein kann oder nicht.

S_4 operiert auf M durch Permutation der Ecken. Wir gesen für jeden der 11 Typen den Stabilisator und dann mit Hilfe von Satz 1.1.20 die Länge der Bahn an:

Graph	Stabilisator	$\lvert Stab \rvert$	Bahnlänge
	S_4	24	1
	$\{id, (12), (34), (12)(34)\}$	4	6
	$S_3 = S(1,2,4)$	6	4
	$\{id, (24)\}$	2	12
	$\{id, (24)\}$	2	12
	$\{id, (1324), (13)(24), (1423), (12), (34), (12)(34), (14)(23)\}$	8	3
	$S(2,3,4)$	6	4
	$\{id, (1234), (13)(24), (1432), (13), (24), (12)(34), (14)(23)\}$	8	3
	$\{id, (14)(23)\}$	2	12
	$\{id, (24), (13), (13)(24)\}$	4	6
	S_4	24	1

(Beachte,  und  liefern die Symmetriegruppe des Quadrats.)

Wir addieren die Bahnenlängen:

$$1+6+4+12+12+3+4+12+3+6+1$$

$$= 64 = |M|$$

Damit haben wir alle Isomorphieklassen gefunden. □

1.2. Konjugation

1.2.1 Def Sei G eine Gruppe. Die Operation

$$G \times G \longrightarrow G : (g,h) \mapsto ghg^{-1}$$

von G auf sich selbst heißt **Konjugation**.

Die Bahnen $h^G = \{ghg^{-1} \mid g \in G\}$ heißen **Konjugationsklassen**.

Wohldefiniert:

$$(e,g) \longmapsto ege^{-1} = g$$

$$(g_1 g_2, h) \longmapsto g_1 g_2 h (g_1 g_2)^{-1} =$$

$$g_1 g_2 h g_2^{-1} g_1^{-1} = g_1 (g_2 h g_2^{-1}) g_1^{-1}.$$

1.2.2 Bsp:

Konjugationsklassen der S_n:

Sei $n = 3$.

$\{id\}$ ist eine Klasse.

Klasse von (12):

$$(12)(12)(12)^{-1} = (12)$$
$$(13)(12)(13)^{-1} = (23)$$
$$(23)(12)(23)^{-1} = (13)$$
$$(123)(12)(123)^{-1} =$$
$$(123)(12)(132) = (23)$$
$$(132)(12)(132)^{-1} = (13)$$

$\Rightarrow$ Wir erhalten alle Transpositionen,

$\{(12), (13), (23)\}$

Klasse von (123):

$$(12)(123)(12) = (132)$$
$$(13)(123)(13) = (132)$$
$$(23)(123)(23) = (132)$$
$$(123)(123)(132) = (123)$$
$$(132)(123)(123) = (123)$$

$\Rightarrow$ Wir erhalten alle 3-Zykel,

$\{(123), (132)\}$

Allgemein gilt:

Die Zerlegung in Konjugationsklassen ist die Zerlegung in Zyklentypen:

Für $\sigma = c_1 \cdots c_s$ Zerlegung in disjunkte Zykel der Länge $\ell(c_i) = l_i$ setzen wir $p(\sigma) = (l_1, \ldots, l_s)$, dies ist eine Partition von n.

z.B. für $n=4$:

$p((123)) = (3,1)$

$p((12)(34)) = (2,2)$.

$p(b)$ heißt der <u>Zykeltyp</u> von b.

<u>1.2.3 Satz:</u>

$\{$ Konjugationsklassen der S_n $\}$ $\overset{1:1}{\longleftrightarrow}$ $\{$ Partitionen von n $\}$

durch den Zykeltyp.

<u>1.2.4 Def</u>

Sei G eine Gruppe, $g \in G$.

$i_g : G \to G : h \mapsto ghg^{-1}$

bezeichnet den inneren Automorphismus zu g.

Wohldefiniert:

Homomorphismus: $i_g(h_1 \cdot h_2) = g h_1 h_2 g^{-1} = g h_1 g^{-1} g h_2 g^{-1} = i_g(h_1) \cdot i_g(h_2)$

Injektiv: $g h_1 g^{-1} = g h_2 g^{-1} \Rightarrow h_1 = h_2$

Surjektiv: $h = i_g(g^{-1} h g) = g g^{-1} h g g^{-1}$

1.2.5 Def Sei $U \subset G$ eine Untergruppe, $g \in G$, dann ist die Konjugation von U mittels g,

$$gUg^{-1} = \{ gug^{-1} \mid u \in U \}.$$

1.2.6 Lemma: $gUg^{-1} \cong U$

Beweis: Da $gUg^{-1} = i_g(U)$ das Bild unter dem inneren Automorphismus zu g.

1.2.7 Def Sei

$$S = \{ U \mid U \text{ in } G \text{ Untergruppe} \}.$$

G operiert auf S durch Konjugation

$$G \times S \to S : (g, U) \longmapsto gUg^{-1}$$

Die Bahnen U^G dieser Operation heißen die Konjugationsklassen von Untergruppen.

Wohldefiniert: $(e, U) \mapsto eUe^{-1} = U$

$(gh, U) \mapsto ghU(gh)^{-1} = ghUh^{-1}g^{-1}$

Bem Ein Normalteiler ist eine Untergruppe, die invariant unter Konjugation ist, d.h. deren Konjugationsklasse $U^G = \{U\}$ nur aus einem Element besteht.

1.2.8 Satz Sei $G \times M \to M$ eine Operation, $n, m \in Gm$ in derselben Bahn mit $n = gm$. Dann sind die Stabilisatoren konjugiert,

$$Stab(n) = g\, Stab(m)\, g^{-1}.$$

Beweis: „$\supset$" Sei $u \in Stab(m)$, $u' = gug^{-1}$. Dann gilt $u' \cdot n = gug^{-1} \cdot n = gum = gm = n$ (da $u \in Stab(m)$)

$\Rightarrow u' \in Stab(n)$.

„$\subset$" Analog mit $m = g^{-1}n$ zeigen wir $g^{-1} Stab(n) g \subset Stab(m)$, daraus folgt „$\subset$" nach Multiplikation von rechts mit g^{-1} und von links mit g. □

Bsp S_3 hat 4 Konjugationsklassen von Untergruppen, $\{id\}$,

$\{\langle(12)\rangle, \langle(13)\rangle, \langle(23)\rangle\}$

$\{\langle(123)\rangle\}$, $\{S_3\}$.

Damit besitzt S_3 Untergruppen jeder Größe, die nach Lagrange theoretisch möglich, i.e. für jeden Teiler von 6.

1.2.9 Def Sei G eine Gruppe.

Das Zentrum $Z(G)$ ist

$$Z(G) = \{g \mid hg = gh \quad \forall h \in G\}$$
$$= \{g \mid h = ghg^{-1} \quad \forall h \in G\}$$

1.2.10 Lemma Sei G eine Gruppe

Sei $\varphi: G \longrightarrow Aut(G): g \mapsto ig$.

Dann ist φ ein Homomorphismus mit $\ker(\varphi) = Z(G)$.

Insbesondere ist $Z(G)$ ein Normalteiler.

Beweis: Homomorphismus:

$\varphi(g_1) \circ \varphi(g_2)\ (h) = i_{g_1} \circ i_{g_2}\ (h) = i_{g_1}(i_{g_2}(h)) =$

$g_1 (g_2 h g_2^{-1}) g_1^{-1} = g_1 g_2 h (g_1 g_2)^{-1} = i_{g_1 g_2}(h)$

$= \varphi(g_1 g_2)(h)$

$\ker(\varphi) = Z(G)$:

$g \in \ker(\varphi) \iff i_g = id \iff$

$\forall h \in G: ghg^{-1} = h \iff g \in Z(G)$ □

1.2.11 Def

Der Stabilisator der Konjugationsoperation heißt Zentralisator:

$Z_G(h) = \{ g \mid ghg^{-1} = h \}$

Auch für Teilmengen $M \subset G$:

$Z_G(M) = \{ g \mid ghg^{-1} = h \ \forall h \in M \}$

der Zentralisator von M.

Der Zentralisator von $M = G$ ist das Zentrum.

1.2.12 Satz (Klassengleichung)

Sei G eine Gruppe, $R \subset G$ eine Teilmenge, die aus jeder Konjugationsklasse genau ein Element enthält.

Dann gilt die Klassengleichung:

$$|G| = |Z(G)| + \sum_{r \in R \setminus Z(G)} |G| / |Z_G(r)|$$

Beweis: Aus der Bahngleichung 1.1.23 folgt

$$|G| = \sum_{r \in R} |G| / |\mathrm{Stab}(r)| = \sum_{r \in R} |G| / |Z_G(r)| .$$

Die Konjugationsklassen von Elementen im Zentrum sind einelementig, denn aus $gh = hg \ \forall h$ folgt $g = hgh^{-1} \ \forall h$

$\Rightarrow g^G = \{g\} \Rightarrow Z(G) \subset R$

Falls r invariant unter Konjugation folgt $Z_G(r) = G$ und

$|G| / |Z_G(r)| = |G| / |G| = 1$.

$$\Rightarrow |G| = \sum_{r \in Z(G)} 1 + \sum_{r \in R \setminus Z(G)} |G| / |Z_G(r)|$$

$$= |Z(G)| + \sum_{r \in R \setminus Z(G)} |G| / |Z_G(r)|$$

□

Bsp Sei G die Symmetriegruppe eines Quadrats.

$G = \{ id, (1234), (13)(24), (1432), (13), (24),$



$(12)(34), (14)(23) \}$



Betrachte die Konjugation von G.

	r	Konj.-klasse r^G	Zentralisator $Z_G(r)$
$Z(G)$	id	$\{id\}$	G
$Z(G)$	$(13)(24)$	$\{(13)(24)\}$	G
	(13)	$\{(13), (24)\}$	$\{id, (13), (24), (13)(24)\}$
	$(12)(34)$	$\{(12)(34), (14)(23)\}$	$\{id, (12)(34), (13)(24), (14)(23)\}$
	(1234)	$\{(1234), (1432)\}$	$\{id, (1234), (13)(24), (1432)\}$

Bahnengleichung: $8 = 1 + 1 + 2 + 2 + 2$

Klassengleichung: $8 = 2 + 2 + 2 + 2$

1.2.13 Korollar

Sei G eine Gruppe der Ordnung p^k, p Primzahl, $k>0$, dann wird $|Z(G)|$ von p geteilt.

Beweis: $r \notin Z(G) \Leftrightarrow \exists g$ mit $r \neq grg^{-1} \Leftrightarrow g \notin Z_G(r) \Leftrightarrow Z_G(r) \subsetneq G \Leftrightarrow |G|/|Z_G(r)| > 1$

Da $|G|/|Z_G(r)|$ wie $|Z_G(r)|$ ein Teiler von $|G| = p^k$ ist, folgt $p \mid |G|/|Z_G(r)|$

Damit wird auch

$$|Z(G)| = |G| - \sum_{r \in R \setminus Z(G)} |G|/|Z_G(r)|$$

(Klassengleichung 1.2.12, R ist eine Menge, die aus jeder Konjugationsklasse genau ein Element enthält)

$= p^k -$ durch p teilbare Zahlen

von p geteilt. □

Bemerkung:

Daraus folgt, daß die Symmetriegruppe des Quadrats der Ordnung $8 = 2^3$ mindestens ein weiteres Element neben id im Zentrum besitzt.

Wir haben im Bsp gesehen, daß dies die Drehung um 180° ist.

1.2.14 Korollar

Sei G eine Gruppe der Ordnung p^2, p prim. Dann ist G abelsch.

Beweis: Wegen 1.2.13 wird $|Z(G)|$ von p geteilt, ist also p oder p^2.

Falls $|Z(G)| = p^2 \Rightarrow G = Z(G)$ und G ist abelsch.

Falls $|Z(G)| = p \Rightarrow |G| / |Z(G)| = p$

$\Rightarrow |G/Z(G)| = p$. Da $Z(G)$ Normalteiler, ist $G/Z(G)$ eine Gruppe.

Eine Gruppe von Primzahlordnung ist zyklisch.

$\Rightarrow \exists g: \quad G/Z(G) = \langle g Z(G) \rangle$.

Seien $g_1, g_2 \in G$, schreibe

$g_i = g^{k_i} \cdot z_i$ mit $z_i \in Z(G)$.

Dann ist $g_1 g_2 = g^{k_1} z_1 g^{k_2} z_2$

$= g^{k_1+k_2} z_1 z_2 = g^{k_1+k_2} z_2 z_1$

$= g^{k_2} z_2 g^{k_1} z_1 = g_2 g_1$, da die

z_i mit jedem Element vertauschen.

Damit ist G abelsch und

$G = Z(G)$, $|Z(G)| = p^2$. $\square$

1.3. Isomorphiesätze

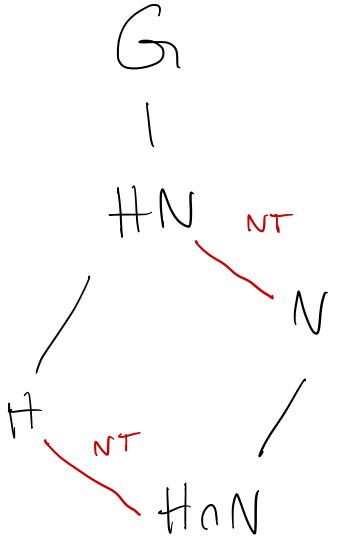
1.3.1 Def Sei G eine Gruppe, H, N Untergruppen.
Wenn $\forall h \in H \quad hNh^{-1} \subset N$
so wird N von H normalisiert.

Bsp Falls N Normalteiler so wird N von jeder Untergruppe normalisiert.

1.3.2 Lemma G Gruppe, H, N Untergruppen, N wird von H normalisiert. Dann:

1) $H \cap N$ ist Normalteiler in H
2) $HN = \{hn \mid h \in H, n \in N\}$ ist Untergruppe von G, N ist Normalteiler von HN.

Ein Teil des Untergruppenverbands ist also:



Beweis:

1) Sei $h \in H$, $n \in H \cap N$, dann

gilt $hnh^{-1} \in N$ da N normalisiert

und $hnh^{-1} \in H$, da alle in H sind.

$\Rightarrow hnh^{-1} \in H \cap N$

Also ist $H \cap N$ Normalteiler in H.

2) $HN \neq \emptyset$. Sei $hn \in HN$, dann

ist $(hn)^{-1} = n^{-1}h^{-1} = h^{-1}\underbrace{hn^{-1}h^{-1}}_{\in N, \text{ da } N \text{ von } H \text{ normalisiert wird}} \in HN$

Seien h_1n_1, $h_2n_2 \in HN$. Dann ist

$h_1n_1h_2n_2 = h_1h_2\underbrace{h_2^{-1}n_1h_2}_{\in N}n_2 \in HN$

Untergruppenkriterium $\Rightarrow$ HN ist Untergruppe.

Sei $hn_1 \in HN$, $n_2 \in N$, dann gilt

$hn_1n_2(hn_1)^{-1} = \underbrace{h\underbrace{n_1n_2n_1^{-1}}_{\in N}h^{-1}}_{\in N} \in N$

$\Rightarrow$ N ist Normalteiler. $\square$

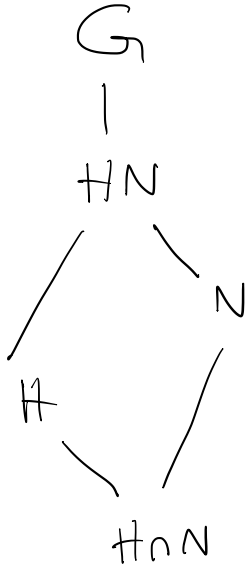
Bsp

1) $G = S_3$, $H = \{id, (12)\}$, $N = \{id, (123), (132)\}$
$= A_3$. Dann ist $G = HN$, da (12) und (123) G erzeugen. N ist Normalteiler in $HN = G$.

2) $G = S_4$, $H = \{id, (14)\}$, $N = \{id, (123), (132)\}$
Dann wird N nicht von H normalisiert, denn z.B. ist
$(14)(123)(14)^{-1} = (14)(123)(14) = (234) \notin N$.
Die Menge $HN = N \cup \{(14), (1234), (1324)\}$
ist keine Untergruppe, da z.B.
$(1234)^2 = ((14)(123))^2 = (13)(24) \notin HN$.

1.3.3 Satz (1. Isomorphiesatz):

Sei G eine Gruppe, H, N Untergruppen, so daß N von H normalisiert wird.
Dann gilt $HN/N \cong H/H \cap N$



Beweis:
Wegen 1.3.2 ist N in HN und $H \cap N$ in H Normalteiler.
Setze
$\varphi: H \hookrightarrow HN \longrightarrow HN/N$

φ ist surjektiv, denn für $[hn] = hnN \in {}^{HN}/_{N}$ ist $hnN = hN = \varphi(h)$.

$$\ker(\varphi) = \{h \in H \mid [h] = hN = [e] = N\}$$
$$= \{h \in H \mid h \in N\} = H \cap N.$$

Aus dem Homomorphiesatz folgt

$${}^{H}/_{\ker\varphi} = {}^{H}/_{H\cap N} \cong \operatorname{Im}(\varphi) = {}^{HN}/_{N}.$$

□

Bsp $G = \mathbb{Z}$, $H = a\mathbb{Z}$, $N = b\mathbb{Z}$

$H + N = d\mathbb{Z}$ mit $d = ggT(a,b)$

$H \cap N = m\mathbb{Z}$ mit $m = kgV(a,b)$

$${}^{H+N}/_{N} = {}^{d\mathbb{Z}}/_{b\mathbb{Z}} \cong {}^{\mathbb{Z}}/_{b/d\,\mathbb{Z}}$$

$${}^{H}/_{H\cap N} = {}^{a\mathbb{Z}}/_{m\mathbb{Z}} \cong {}^{\mathbb{Z}}/_{m/a\,\mathbb{Z}}$$

Der 1. Isomorphiesatz 1.3.3 besagt hier

$${}^{b}/_{d} = {}^{m}/_{a} \iff \frac{ab}{d} = m.$$

1.3.4 Lemma

Seien $H_2 \subset H_1$ Untergruppen von G. Dann gilt $|G/H_2| = |G/H_1| \cdot |H_1/H_2|$.

Beweis:

Wähle einen Vertreter x_i für jede Äquivalenzklasse $[x_i] = x_i H_1$ in G/H_1 und einen Vertreter y_j für jede Äquivalenzklasse $[y_j] = y_j H_2$ in H_1/H_2.

Beh $[x_i y_j] \neq [x_k y_e]$ in G/H_2 $\forall (i,j) \neq (k,e)$.

Angenommen $[x_i y_j] = [x_k y_e] \Rightarrow$

$x_i y_j H_2 = x_k y_e H_2 \Rightarrow x_k^{-1} x_i y_j H_2 = y_e H_2$.

Da $y_e \in H_1$ und $H_2 \subset H_1$ folgt

$x_k^{-1} x_i y_j \in H_1$ und da $y_j \in H_1$

$x_k^{-1} x_i \in H_1 \Rightarrow [x_i] = x_i H_1 = [x_k] = x_k H_1$

$\Rightarrow x_i = x_k$ nach Wahl der x_m

Aus $[x_i y_j] = x_i y_j H_2 = [x_k y_e] = x_k y_e H_2$

folgt dann durch Kürzen $y_j H_2 = y_e H_2$

und nach Wahl der y_n damit $y_j = y_e$.

Beh Für $g \in G \; \exists (i,j)$: $[g] = g H_2 =$
$x_i y_j H_2 = [x_i y_j]$.

$\exists x_i$: $[g] = g H_1 = x_i H_1 \quad \Rightarrow$
$x_i^{-1} g \in H_1$.

Für $x_i^{-1} g \; \exists y_j$: $x_i^{-1} g H_2 = y_j H_2$

$\Rightarrow g H_2 = x_i y_j H_2$.

Aus den beiden Behauptungen folgt

$$|G/H_2| = |\{(i,j)\}| = |\{i\}| \cdot |\{j\}| = |G/H_1| \cdot |H_1/H_2|.$$

□

1.3.5 Satz (2. Isomorphiesatz)

Seien H_1, H_2 Normalteiler von G, $H_2 \subset H_1$. Dann ist H_1/H_2 Normalteiler in G/H_2 und

$$\frac{G/H_2}{H_1/H_2} \cong G/H_1.$$

Beweis: $\varphi: G/H_2 \longrightarrow G/H_1 : aH_2 \longmapsto aH_1$

φ ist wohldefiniert: falls $aH_2 = bH_2$

$\Rightarrow b^{-1}a \in H_2 \subset H_1 \Rightarrow bH_1 = aH_1$

φ ist ein surjektiver Gruppenhomomorphismus.

$\ker(\varphi) = \{ aH_2 \in G/H_2 \mid aH_1 = [a] = [e] = H_1 \}$

$= \{ aH_2 \in G/H_2 \mid a \in H_1 \} = H_1/H_2$

Aus dem Homomorphiesatz folgt

$$G/H_2 \,/\, \ker\varphi = G/H_2 \,/\, H_1/H_2 \cong \operatorname{Im}(\varphi) = G/H_1$$

□

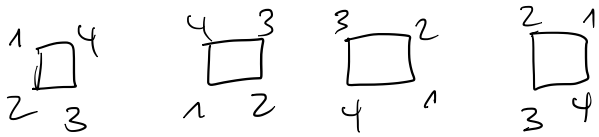
Bsp $G = \mathbb{Z}$, $H_2 = ab\mathbb{Z}$, $H_1 = a\mathbb{Z}$

$\Rightarrow G/H_2 = \mathbb{Z}/ab\mathbb{Z}$, $H_1/H_2 = a\mathbb{Z}/ab\mathbb{Z} \cong \mathbb{Z}/b\mathbb{Z}$,

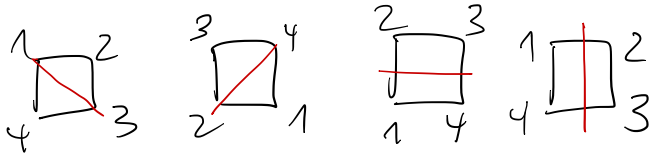
$$\mathbb{Z}/ab\mathbb{Z} \,/\, \mathbb{Z}/b\mathbb{Z} \cong \mathbb{Z}/a\mathbb{Z} = G/H_1 .$$

1.3.6 Bsp

Sei G_1 = Symmetriegruppe des Quadrats $\subset S_4$

Drehungen 

$$G_1 = \{ id, (1234), (13)(24), (1432),$$

Spiegelungen 

$$(24), (13), (12)(34), (14)(23) \}$$

Sei H_1 die Untergruppe der Drehungen.

Da $|G_1/H_1| = 2$ ist H_1 Normalteiler.

Sei $H_2 = \{ id, (13)(24) \}$.

$H_2 = Z(G_1)$, also ist auch H_2 Normalteiler.

G_1/H_2 hat 4 Elemente:

$e := H_2 = \{ id, (13)(24) \}$ Drehung um 0°, 180°

$a := (1234) H_2 = \{ (1234), (1432) \}$ " 90°, 270°

$b := (13) H_2 = \{ (13), (24) \}$ Diagonalenspiegelungen

$c := (12)(34) H_2 = \{ (12)(34), (14)(23) \}$ Seitenmitten-spiegelungen

Wir analysieren die Gruppenstruktur von G/H_2. Die möglichen Ordnungen der Elemente sind 1, 2, 4. Falls ein Element der Ordnung 4 existierte, würde folgen G/H_2 zyklisch, also $\mathbb{Z}/4\mathbb{Z}$.

Aber a, b, c haben Ordnung 2.

Wir erstellen die Gruppenverknüpfungstafel:

	e	a	b	c
e	e	a	b	c
a	a	e		
b	b		e	
c	c			e

Es gilt

$ab \neq a$, denn $b \neq e$ und

$ab \neq b$, denn $a \neq e \Rightarrow ab = c$

Genauso $ac = b$, $ba = c$, $ca = b$, $bc = a$, $cb = a$.

Also:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Vergleiche dazu die Verknüpfungstafel der zyklischen Gruppe der Ordnung 4 mit Erzeuger a, $b = a^2$, $c = a^3$:

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

An der Verknüpfungstabelle erkennen wir: $G/H_2 \cong$

$\{ id, (12), (34), (12)(34) \} \subset S_4$

Kleinsche Vierergruppe K_4.

Oder: $\mathbb{Z}_2 \times \mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

$= \{ (0,0), (1,0), (0,1), (1,1) \}$

$G/H_2 \Big/ H_1/H_2 = \{e,a,b,c\} \Big/ \{e,a\}$

$= \{ \{e,a\}, b \cdot \{e,a\} \} \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \Big/ \mathbb{Z}_2$

$\cong \mathbb{Z}_2 \cong G/H_1$.

Hierbei ist ein direktes Produkt von Gruppen aufgetaucht, dies wollen wir im folgenden weiter untersuchen.

1.4 Direktes und Semidirektes Produkt von Gruppen

1.4.1 Def Seien $(H_1, \circ)$, $(H_2, *)$ Gruppen. Das direkte Produkt $H_1 \times H_2$ ist eine Gruppe mit
$(h_1, h_2) \circ (g_1, g_2) = (h_1 g_1, h_2 * g_2)$.

1.4.2 Lemma Seien H_1, H_2 Gruppen.

1) $\tilde{H}_1 := \{(h_1, e_2) \mid h_1 \in H_1\}$ und
$\tilde{H}_2 := \{(e_1, h_2) \mid h_2 \in H_2\}$
sind Normalteiler in $H_1 \times H_2$ mit $\tilde{H}_1 \cap \tilde{H}_2 = \{(e_1, e_2)\}$. Je zwei Elemente von $\tilde{H}_1$ und $\tilde{H}_2$ vertauschen:
$\tilde{h}_1 \tilde{h}_2 = \tilde{h}_2 \tilde{h}_1 \quad \forall \tilde{h}_1 \in \tilde{H}_1, \tilde{h}_2 \in \tilde{H}_2$.

2) $H_1 \times H_2 = \tilde{H}_1 \tilde{H}_2$

3) $H_1 \times H_2 / \tilde{H}_1 \cong \tilde{H}_2$,

$H_1 \times H_2 / \tilde{H}_2 \cong \tilde{H}_1$.

Beweis:

1) Sei $(g_1, g_2) \in H_1 \times H_2$ und $(h_1, e_2) \in \tilde{H}_1$, dann gilt

$$(g_1, g_2) \cdot (h_1, e_2) \cdot (g_1, g_2)^{-1} =$$

$$(g_1, g_2) \cdot (h_1, e_2) \cdot (g_1^{-1}, g_2^{-1}) =$$

$$(g_1 h_1 g_1^{-1}, g_2 e_2 g_2^{-1}) =$$

$$(g_1 h_1 g_1^{-1}, e_2) \in \tilde{H}_1$$

$\Rightarrow \tilde{H}_1$ ist Normalteiler.

$\tilde{H}_2$ ebenso.

Sei $\tilde{h}_1 = (h_1, e_2)$, $\tilde{h}_2 = (e_1, h_2)$

$$\Rightarrow \tilde{h}_1 \tilde{h}_2 = (h_1, e_2)(e_1, h_2) = (h_1, h_2)$$

$$= (e_1, h_2)(h_1, e_2) = \tilde{h}_2 \tilde{h}_1.$$

2) „$\supseteq$" klar

„$\subseteq$" Sei $(h_1, h_2) \in H_1 \times H_2$

$$\Rightarrow (h_1, h_2) = (h_1, e_2) \cdot (e_1, h_2) \in$$

$$\tilde{H}_1 \cdot \tilde{H}_2.$$

3) Aus dem 1. Isomorphiesatz 1.3.3 folgt $H_1 \times H_2 / \tilde{H}_1 = \tilde{H}_1 \tilde{H}_2 / \tilde{H}_1 \cong \tilde{H}_2 / \tilde{H}_1 \cap \tilde{H}_2$

$= \tilde{H}_2 / \{e\} = \tilde{H}_2$. □

Diese Eigenschaften sind charakteristisch für das direkte Produkt:

1.4.3 Proposition

Sei G eine Gruppe mit Untergruppen H_1, H_2. Es gelte

1) $H_1 \cap H_2 = \{e\}$
2) je zwei Elemente von H_1, H_2 vertauschen
3) $H_1 H_2 = G$

Dann ist $\varphi: H_1 \times H_2 \xrightarrow{\cong} G$, $(h_1, h_2) \longmapsto h_1 h_2$

und H_1, H_2 sind Normalteiler mit $G/H_1 \cong H_2$ und $G/H_2 \cong H_1$.

Beweis:

φ ist Homomorphismus, denn

$\varphi((h_1,h_2)\cdot(g_1,g_2)) = \varphi((h_1g_1, h_2g_2)) =$

$h_1g_1h_2g_2 \overset{2)}{=} h_1h_2g_1g_2 = \varphi((h_1,h_2))\cdot\varphi((g_1,g_2))$.

Wegen 3) ist φ surjektiv.

Sei $(h_1,h_2) \in \ker(\varphi) \Rightarrow h_1h_2 = e$

$\Rightarrow h_1 = h_2^{-1}$ mit $h_1 \in H_1$, $h_2^{-1} \in H_2$

$\Rightarrow h_1, h_2 \in H_1 \cap H_2 \overset{1)}{=} \{e\}$

$\Rightarrow \ker(\varphi) = \{(e,e)\}$.

$\Rightarrow \varphi$ ist Isomorphismus

Unter φ gehen $\tilde{H}_1$, $\tilde{H}_2$ aus 1.4.2 auf H_1, H_2, daher folgt der Rest aus 1.4.2. □

Wir betrachten jetzt eine allgemeinere Konstruktion, bei der 2) weggelassen wird.

1.4.4 Bsp

Sei $G = S_n$, $N = A_n$.

N ist Normalteiler in G, da $|G/N| = 2$, bzw. da $N = \ker(\mathrm{sgn})$.

$H = \langle(12)\rangle \cong \mathbb{Z}_2$.

Es gilt $S_n = NH$, denn jede Permutation b ist entweder gerade (und damit in $A_n = N = Ne$) oder ungerade, aber dann ist $b \circ (12)$ gerade und in Ne, und damit

$$b = b \circ id = (b \circ (12)) \circ (12) \in N(12).$$

Aber es gilt nicht $S_n \cong N \times H$, denn die Tupel vertauschen nicht: Im direkten Produkt $NH \cong N \times H$ würde gelten

$$n_1 h_1 \cdot n_2 h_2 \cong (n_1, h_1)(n_2, h_2) = (n_1 n_2, h_1 h_2)$$
$$\cong n_1 h_2 \, h_1 h_2,$$ aber hier gilt

z. B. für $h_1 = h_2 = (12)$, $n_1 = n_2 = (123)$:

$(123)(12)(123)(12) = (13)(13) = id$ aber

$(12)(12)(123)(123) = (132) \neq id$

Wir versuchen, $n_1 h_1 \cdot n_2 h_2$ anders umzuformen:

$$n_1 h_1 n_2 h_2 = n_1 \underbrace{h_1 n_2 h_1^{-1}}_{\in N,\ \text{da } N \text{ Normalteiler}} h_1 h_2$$

$$= n_1 \, i_{h_1}(n_2) \, h_1 h_2$$

Dies motiviert die folgende Def.

1.4.5 Def und Satz

Seien H, N Gruppen,
$\varphi: H \longrightarrow Aut(N)$ ein Homomorphismus.
Dann ist die Menge $N \times H$
mit der Verknüpfung
$(n_1, h_1) \cdot (n_2, h_2) := (n_1 \varphi(h_1)(n_2), h_1 h_2)$
eine Gruppe, das <u>semidirekte Produkt</u>
$N \rtimes_\varphi H$ von N und H bez. φ.
Man schreibt oft $N \rtimes H$.
$N \cong N \times \{e_H\} \subset N \rtimes H$ ist
Normalteiler in $N \rtimes H$ und
$N \rtimes H / N \cong H$.

<u>Beweis:</u>

Assoziativität:

$((n_1, h_1) \cdot (n_2, h_2)) \cdot (n_3, h_3) =$
$(n_1 \cdot \varphi(h_1)(n_2), h_1 h_2) \cdot (n_3, h_3) =$
$(n_1 \varphi(h_1)(n_2) \cdot \varphi(h_1 h_2)(n_3), h_1 h_2 h_3) =$
$(n_1 \cdot \varphi(h_1)(n_2) \cdot \varphi(h_1) \circ \varphi(h_2)(n_3), h_1 h_2 h_3) =$

$$(n_1 \cdot \varphi(h_1)(n_2) \cdot \varphi(h_1)(\varphi(h_2)(n_3)),\ h_1 h_2 h_3)$$

$$= (n_1 \cdot \varphi(h_1)(n_2 \varphi(h_2)(n_3)),\ h_1 h_2 h_3)$$

$$= (n_1, h_1)\ (n_2 \varphi(h_2)(n_3),\ h_2 h_3)$$

$$= (n_1, h_1)\ ((n_2, h_2) \cdot (n_3, h_3))$$

Neutrales:

$$(e_N, e_H) \cdot (n, h) =$$

$$(e_N \cdot \varphi(e_H)(n),\ e_H \cdot h) = (e_N \cdot \mathrm{id}(n),\ h)$$

$$= (n, h)$$

Inverse:

$\varphi(h) \in \mathrm{Aut}(N)$, $\varphi(h)^{-1}$ bezeichne sein Inverses.

Damit gilt:

$$((\varphi(h)^{-1}(n))^{-1},\ h^{-1}) \cdot (n, h) =$$

$$((\varphi(h)^{-1}(n))^{-1} \cdot \varphi(h^{-1})(n),\ h^{-1} h) \overset{\text{da } \varphi \text{ Homomorphismus}}{=}$$

$$((\varphi(h)^{-1}(n))^{-1} \cdot \varphi(h)^{-1}(n),\ e_H) =$$

$$(e_N, e_H).$$

Damit ist $N \rtimes H$ eine Gruppe.

N ist Normalteiler:

Für $(n,h) \in N \rtimes H$ und $(m, e_H) \in N$ gilt:

$$(n,h)(m,e_H)\cdot(n,h)^{-1} =$$

$$(n,h)(m,e_H)\cdot((\varphi(h)^{-1}(n))^{-1}, h^{-1}) =$$

$$(\dots, h e_H h^{-1}) = (\dots, e_H) \in N.$$

$$\Psi : \{e_N\} \times H \hookrightarrow N \rtimes H \longrightarrow N \rtimes H / N$$

ist surjektiv, denn jede Klasse

$(h,h)\cdot N \times \{e_H\}$ kann man schreiben als $(e_N, h)\cdot N \times \{e_H\}$, indem man den Vertreter mit

$$(\varphi(h)^{-1}(n^{-1}), e_H) \in N \times \{e_H\}$$

multipliziert:

$$(n,h)\cdot(\varphi(h)^{-1}(n^{-1}), e_H) =$$

$$(n\cdot\varphi(h)(\varphi(h)^{-1}(n^{-1})), h e_H) =$$

$$(n\cdot\varphi(h)\circ\varphi(h)^{-1}(n^{-1}), h) =$$

$$(n\cdot id(n^{-1}), h) = (n n^{-1}, h) =$$

$$(e_N, h)$$

$\ker(\Psi) =$

$\{(e_N, h) \mid [(e_N, h)] = (e_N, h) \cdot N \times \{e_H\}$

$= (e_N, e_H) \cdot N \times \{e_H\} = [(e_N, e_H)]\}$

$= \{(e_N, h) \mid (e_N, h) \in N \times \{e_H\}\}$

$= \{(e_N, e_H)\}$

Aus dem Homomorphiesatz folgt

$H \cong \{e_N\} \times H = {}^{\{e_N\} \times H}/_{\ker \Psi}$

$\cong \operatorname{Im} \Psi = {}^{N \rtimes H}/_{N}$ □

1.4.6 Bsp

1) Für $\varphi: H \to \mathrm{Aut}(N)$

$h \mapsto id_N$

ist das semidirekte Produkt gleich dem direkten Produkt

2) Bsp. 1.4.4 zeigt

$S_n = A_n \rtimes_\varphi \mathbb{Z}_2$

mit $\varphi: \mathbb{Z}_2 \longrightarrow \mathrm{Aut}(A_n)$:

$0 \longmapsto \mathrm{id}$

$1 \longmapsto i_{(12)}$, Konjugation mit (12)

denn $\langle (12) \rangle \cong \mathbb{Z}_2$

3) Sei $N = \mathbb{Z}_3$, $H = \mathbb{Z}_2$,

$\varphi: H \longrightarrow \mathrm{Aut}(N)$:

$0 \longmapsto \mathrm{id}$

$1 \longmapsto \begin{pmatrix} N \longrightarrow N \\ x \longmapsto -x \end{pmatrix}$

Setze $\Psi: \mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_2 \xrightarrow{\Psi} S_3$

$(a, 0) \longmapsto (123)^a$

$(a, 1) \longmapsto (123)^a (12)$

<u>Beh</u>: Ψ ist Isomorphismus.

Homomorphismus:

Fallunterscheidung nach dem 2. Eintrag:

1) $\Psi((a,0) + (b,0)) = \Psi(a+b, 0) =$

$(123)^{a+b} = (123)^a \circ (123)^b = \Psi(a,0) \circ \Psi(b,0)$

2) $\Psi((a,0)+(b,1)) =$

$\Psi((a+b,1)) = (123)^{a+b}(12) =$

$(123)^a \circ (123)^b(12) =$

$\Psi(a,0) \circ \Psi(b,1)$

3) $\Psi((a,1)+(b,0)) =$

$\Psi(a+\varphi(1)(b),1) =$

$\Psi(a-b,1) = (123)^{a-b}(12)$

$\Psi(a,1) \circ \Psi(b,0) = (123)^a(12)(123)^b$

$= (123)^a(12)\left((123)(12)(12)\right)^b$

$= (123)^a\Big((12)(123)(12)\Big)\Big((12)(123)(12)\Big)\Big((12)\cdots$

$(123)(12)\Big)(12)$

$= (123)^a(132)^b(12)$

$= (123)^a((123)^{-1})^b(12)$

$= (123)^a(123)^{-b}(12)$

$= (123)^{a-b}(12)$

4) $\Psi((a,1)+(b,1)) =$

$\Psi(a-b,0) = (123)^{a-b}$

$\Psi(a,1) \circ \Psi(b,1) =$ wie in 3)

$(123)^a (12) (123)^b (12) =$

$(123)^{a-b} (12)(12) = (123)^{a-b}$

Ψ ist surjektiv, denn

$(123) = \Psi(1,0)$, $(12) = \Psi(0,1)$

sind im Bild und diese erzeugen S_3.

Ψ ist injektiv:

$\Psi(a,0) = \Psi(a',0) \Rightarrow$

$(123)^a = (123)^{a'} \Rightarrow a \equiv a' \bmod 3$

$\Rightarrow a = a'$ in $\mathbb{Z}/3\mathbb{Z} = \mathbb{Z}_3$

$\Psi(a,1) = \Psi(a',1)$ genauso

$\Psi(a,0) = \Psi(a',1) \Rightarrow$

$(123)^a = (123)^{a'}(12)$ ↯

denn links ist eine gerade Permutation, rechts eine ungerade.

1.5 Sylowsätze

Die Ordnung einer Untergruppe teilt die Gruppenordnung.
Gibt es für jeden Teiler der Gruppenordnung eine Untergruppe?
I.A. unklar, Ergebnisse für Primzahlpotenzen.

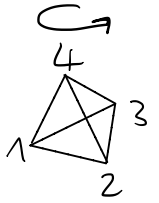
1.5.1 Bsp

S_4 = Symmetriegruppe des Tetraeders

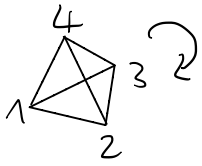
Ordnung $24 = 2^3 \cdot 3$

Untergruppen der Ordnung 3 sind zyklisch, erzeugt von einem 3-Zykel.
Es gibt $8 = \frac{4 \cdot 3 \cdot 2}{3}$ 3-Zykel,
jeweils zwei sind zueinander invers,
damit gibt es 4 Untergruppen der Ordnung 3:

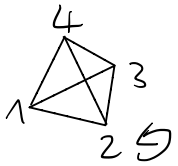
$\{id, (123), (132)\}$



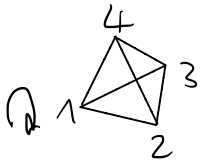
$\{id, (124), (142)\}$



$\{id, (134), (143)\}$

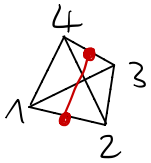


$\{id, (234), (243)\}$



jeweils erzeugt von einer Drehung um eine Ecke um 120°.

Kantenmittendiagonalen:



z.B. 12 nach 34.

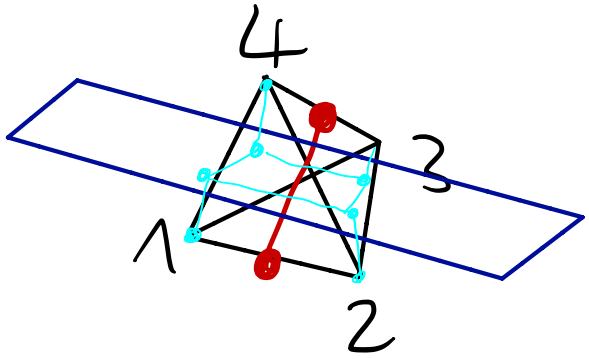
Betrachte den Stabilisator der Kantenmittendiagonale. Die Kante 12 muß festgehalten werden (1, 2 fest oder 1, 2 vertauscht), 34 genauso, oder 12 geht auf 34:

$\{id, (12), (34), (12)(34), (1324),$
$(1423), (13)(24), (14)(23)\}$

= Symmetriegruppe des Quadrats.

Geometrisch sieht man das, indem man den Tetraeder auf die Ebene senkrecht zur Kantenmittendiagonalen durch den Mittelpunkt der Kantenmittendiagonalen

projiziert: der gesuchte Stabilisator hält die Kantenmittendiagonale fest und wirkt nur auf der Projektion des Tetraeders auf die senkrechte Ebene, dies ist ein Quadrat:



Es gibt 3 Kantenmittendiagonalen und 3 zugehörige Stabilisatoren, damit 3 Untergruppen der Ordnung 8:

$\{id, (12), (34), (12)(34), (1324), (1423), (13)(24), (14)(23)\}$

$\{id, (13), (24), (13)(24), (1234), (1432), (12)(34), (14)(23)\}$

$\{id, (14), (23), (14)(23), (1342), (1243), (13)(24), (12)(34)\}$

Untergruppen der Ordnung 4:

Drei erzeugt von Drehspiegelungen:

$\{id, (1234), (13)(24), (1432)\}$

$\{id, (1243), (14)(23), (1342)\}$

$\{id, (1324), (12)(34), (1423)\}$

Vier Kleinsche Vierergruppen:

$\{id, (12), (34), (12)(34)\}$

$\{id, (13), (24), (13)(24)\}$

$\{id, (14), (23), (14)(23)\}$

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

6 Untergruppen der Ordnung 2 erzeugt von Spiegelungen:

$\langle(12)\rangle, \langle(13)\rangle, \langle(14)\rangle, \langle(23)\rangle, \langle(24)\rangle, \langle(34)\rangle$

4 Untergruppen der Ordnung 6 = Stabilisatoren von Ecken $\cong S_3$:

$S(1,2,3), S(1,3,4), S(1,2,4), S(2,3,4)$

1 Untergruppe der Ordnung 12: A_4.

24 hat die Teiler

24, 12, 8, 6, 4, 3, 2, 1

Zu jedem Teiler haben wir Untergruppen gefunden.

1.5.2 Bsp $|A_4| = 12$

$6 \mid 12$ aber A_4 hat keine Untergruppe der Ordnung 6.

Angenommen, sie hätte, N, N ist Normalteiler, dann $|A_4/N| = 2$.

Sei H eine Untergruppe der Ordnung 3, erzeugt von einer Drehung, z.B. $\langle (123) \rangle = H$.

Mit dem 1. Isomorphiesatz 1.3.3 folgt

$$HN/N \cong H/H \cap N \Rightarrow$$

$$|HN/N| = |H/H \cap N| \Rightarrow$$

$$|HN|/|N| = |H|/|H \cap N| \Rightarrow$$

$$12 = |A_4| \geq |HN| = \frac{|H| \cdot |N|}{|H \cap N|} = \frac{3 \cdot 6}{|H \cap N|}$$

$$= \frac{18}{|H \cap N|}$$

$\Rightarrow H \cap N \supsetneq \{id\}$, damit existiert ein 3-Zykel in $H \cap N$. Da $H \cap N$ eine Untergruppe ist, liegt auch sein Inverses in $H \cap N \Rightarrow |H \cap N| = 3$

$\Rightarrow H \subset H \cap N \Rightarrow H \subset N$

Da dieses Argument für jede Wahl von H greift, folgt

$\{3\text{-Zykel}\} \subset N$.

Es gibt 8 3-Zykel ↯.

1.5.3 Def Sei G eine endliche Gruppe, p eine Primzahl.

1) G heißt p-Gruppe, falls $|G| = p^r$ für ein $r \in \mathbb{N}$.

2) Ist $|G| = p^k \cdot m$ mit $p \nmid m$, so heißt eine Untergruppe $H \subset G$ mit $|H| = p^k$ eine p-Sylow-(Unter-)Gruppe von G.

Bsp: Stab(Kantenmitten diagonalen) = Sym(Quadrat) sind 2-Sylowgruppen der S_4, denn $|S_4| = 24 = 2^3 \cdot 3$

Erzeugnisse von Drehungen (z.B. $\langle(1234)\rangle$) sind 3-Sylowgruppen der S_4.

1.5.4 Satz

Sei G endlich, p eine Primzahl mit $p \mid |G|$, $|G| = p^k \cdot m$, $p \nmid m$.

Dann gibt es zu jedem r mit $1 \leq r \leq k$ eine Untergruppe H von G mit $|H| = p^r$.

Insbesondere hat G für jedes p eine p-Sylowuntergruppe.

1.5.5 Def

Sei G eine Gruppe, der <u>Exponent</u> von G ist $\min\{k \in \mathbb{N}_{>0} \mid g^k = e \ \forall g \in G\}$

<u>Bsp</u> $Exp(\mathbb{Z}_2 \times \mathbb{Z}_2) = 2$, $Exp(\mathbb{Z}_4) = 4$,
$Exp(S_3) = 6$, $Exp(Sym(\square)) = 4$

1.5.6 Lemma

Sei $|G| = n$.

1) Der Exponent m von G ist das kgV der Ordnungen der Elemente von G.
2) Falls $g^k = e \ \forall g \in G \Rightarrow m \mid k$.
3) $m \mid n$.

Beweis:

1) $g^k = e \iff \operatorname{ord}(g) \mid k$

m wird also von allen $\operatorname{ord}(g)$ geteilt und das es nach Def das kleinste ist, folgt $m = \operatorname{kgV}(\operatorname{ord}(g) \mid g \in G)$.

2) folgt aus 1).

3) folgt, da n ein Vielfaches von $\operatorname{ord}(g)$ ist $\forall g \in G$. □

1.5.7 Lemma Sei G endlich und abelsch, $m = \operatorname{Exp}(G)$. Dann $\exists$ $k \in \mathbb{N}_{>0}$: $|G| \mid m^k$.

Beweis: Induktion nach $|G|$.

Induktionsanfang: $|G| = 1$ klar.

Induktionsvoraussetzung: Die Behauptung gelte $\forall$ abelschen G' mit $|G'| < |G|$.

Induktionsschluß:

Sei $e \neq g \in G$, $H = \langle g \rangle$, $|H| = \operatorname{ord}(g) \mid m$.

Da G abelsch, ist H Normalteiler und G/H eine Gruppe.

Sei $g'H \in G/H$, dann ist

$(g'H)^m = g'^m H = eH = H$

also teilt der Exponent von G/H m nach Lemma 1.5.6 2).

Da $|G/H| < |G|$ greift die Induktionsvoraussetzung und wir erhalten k' mit $|G/H| \mid \mathrm{Exp}(G/H)^{k'} \Rightarrow$

$$|G/H| \mid m^{k'}$$

Setze $k = k' + 1$, dann gilt

$$|G| = |H| \cdot |G/H| = \mathrm{ord}(g) \cdot |G/H| \mid$$

$$m \cdot m^{k'} = m^{k'+1} = m^k$$

□

1.5.8 Lemma Sei G endlich und abelsch, p Primzahl, $p \mid |G|$, dann hat G eine Untergruppe der Ordnung p.

Beweis: $p \mid |G|$ und $|G| \mid m^k$, wobei $m = \mathrm{Exp}(G) \Rightarrow p \mid m^k$

$\Rightarrow p \mid m$ da p prim

Da $m = \mathrm{kgV}(\mathrm{ord}(g) \mid g \in G)$ $\exists\, g$: $p \mid \mathrm{ord}(g)$. Sei $\mathrm{ord}(g) = r \cdot p$.

Dann hat g^r Ordnung p und $\langle g^r \rangle$ ist eine (notwendigerweise zyklische) Untergruppe der Ordnung p. □

Beweis von Satz 1.5.4:

Induktion nach $n = |G|$.

Induktionsanfang: $n = 1$, $n = 2$ klar.

Induktionsvoraussetzung: Die Behauptung gelte für alle G' mit $|G'| < n$.

Induktionsschluß:

Hat G eine echte Untergruppe U mit $p^k \mid |U|$, so wenden wir die Induktionsvoraussetzung auf U an und die Behauptung folgt, da Untergruppen von U auch Untergruppen von G sind.

Hat G keine solche Untergruppe, so folgt aus $|G| = |U| \cdot |G/U|$

$p \mid |G/U|$ $\forall$ echten Untergruppen U.

Betrachte die Konjugation von G,

Sei $R \subset G$ eine Teilmenge, die aus jeder Konjugationsklasse genau ein Element enthält. Nach der Klassengleichung 1.2.12 gilt

$$|G| = |Z(G)| + \sum_{r \in R \setminus Z(G)} |G / Z_G(r)|$$

wobei für $r \in R \setminus Z(G)$ der Zentralisator $Z_G(r)$ eine echte Untergruppe ist, daher gilt $p \mid |G / Z_G(r)|$

$$\Rightarrow \quad p \mid |Z(G)|.$$

Da $Z(G)$ abelsch ist, folgt mit Lemma 1.5.8, daß $Z(G)$ eine Untergruppe N der Ordnung p hat.

Als Untergruppe des Zentrums, das Normalteiler in G und abelsch ist, ist N Normalteiler in G und wir können G/N betrachten.

Es gilt $|G/N| = \frac{|G|}{|N|} = \frac{p^k m}{p} =$

$p^{k-1} \cdot m$.

Nach Induktionsvoraussetzung hat G/N für jedes r' mit $1 \leq r' \leq k-1$ eine Untergruppe H' der Ordnung $p^{r'}$. G/N hat auch die Untergruppe $\{e\}$ der Ordnung $1 = p^0$.

Sei $\pi : G \longrightarrow G/N$, setze

$H = \pi^{-1}(H')$.

Dann ist H eine Untergruppe von G der Ordnung $p^{r'+1}$, und mit $r = r'+1$ haben wir solche $\forall \; 1 \leq r \leq k$. □

1.5.9 Korollar

Für jede Primzahl $p \mid |G|$ $\exists$ ein Element der Ordnung p.

Beweis: Aus Satz 1.5.4 folgt, daß es für jedes $p \mid |G|$ eine Untergruppe der Ordnung p gibt, diese ist notwendigerweise zyklisch und daher erzeugt von einem Element der Ordnung p. □

1.5.10 Satz (Sylowsche Sätze)

Sei G endlich, $p \mid |G|$, p prim.

1) Jede p-Untergruppe H ist in einer p-Sylowgruppe enthalten.
2) Alle p-Sylowgruppen sind zueinander konjugiert
3) Die Anzahl n_p der p-Sylowgruppen von G ist ein Teiler von $|G|$ mit $n_p \equiv 1 \mod p$.

Bsp $G = S_4$, $|G| = 24 = 2^3 \cdot 3$

Die 2-Sylowgruppen haben Ordnung 8.

$n_2 \mid 24$ und $n_2 \equiv 1 \mod 2$

$\Rightarrow n_2 \mid 3$

Wir kennen 3 2-Sylowgruppen (Bsp. 1.5.1), die drei $\mathrm{Sym}(\square)$, also $n_2 = 3$.

Die 3-Sylowgruppen haben Ordnung 3.

$n_3 \mid 24$, $n_3 \equiv 1 \mod 3$

$\Rightarrow n_3 \in \{1, 4\}$

Wir kennen schon 4 Untergruppen der Ordnung 3 - die 4 Sym(3) der Seiten, erzeugt von einer Drehung,
$\langle (123) \rangle$, $\langle (124) \rangle$, $\langle (134) \rangle$, $\langle (234) \rangle$
$\Rightarrow \quad n_3 = 4.$

1.5.11 Korollar

Sei $|G| = p^k \cdot m$, $p \nmid m$,
so gilt $n_p \mid m$.

Beweis: $n_p \equiv 1 \mod p \Rightarrow$
$p \nmid n_p$, aber $n_p \mid |G| = p^k \cdot m$ □

1.5.12 Def

Sei G eine Gruppe, S eine Untergruppe.
Der Normalisator von S,
$N_G(S) = \{ g \in G \mid gSg^{-1} = S \}.$

1.5.13 Lemma

Sei $H \subset G$ eine p-Gruppe,
S eine p-Sylowgruppe von G.

Ist H im Normalisator $N_G(S)$ enthalten, so gilt schon $H \subset S$.

Beweis: Sei $|G| = p^k \cdot m$, $p \nmid m$.

Da $H \subset N_G(S)$ wird S von H normalisiert.

Mit dem 1. Isomorphiesatz 1.3.3 erhalten wir

$$HS/S \cong H/H \cap S$$

Damit ist $|HS/S|$ ein Teiler von $|H|$ und daher eine p-Potenz.

Also ist auch $|HS| = |HS/S| \cdot |S|$ eine p-Potenz, größer gleich $|S| = p^k$.

Wegen 1.3.2 2) (Vorbereitung zum 1. Isomorphiesatz) ist HS eine Untergruppe von G $\Rightarrow |HS| \mid |G|$

$\Rightarrow |HS| \mid p^k \cdot m \Rightarrow |HS| = p^k$

$\Rightarrow |HS/S| = 1 \Rightarrow HS = S$

$\Rightarrow hs \in S \quad \forall h \in H, s \in S \Rightarrow$

$h = (hs)s^{-1} \in S \quad \forall h \in H$

$\in S \quad \in S$

$\Rightarrow H \subset S.$ □

1.5.14 Def Eine Gruppenoperation mit nur einer Bahn heißt transitiv.

1.5.15 Prop Sei $U \subset G$ eine p-Sylowgruppe, $H \subset G$ eine p-Gruppe, dann $\exists g \in G: H \subset gUg^{-1}$ und gUg^{-1} ist auch p-Sylowgruppe.

Beweis:

Sei U^G = Menge der Konjugationsklassen von U

$= \{gUg^{-1} \mid g \in G\}$

Betrachte die Konjugationsoperation von G auf U^G:

$G \times U^G \longrightarrow U^G : (g, S) \mapsto gSg^{-1}$

Sie ist per Def transitiv.

Aus Korollar 1.1.21 folgt

$|G| =$ Bahnlänge $\cdot$ $|\text{Stab}| =$

$|U^G| \cdot |\text{Stab}(U)| =$

$|U^G| \cdot |N_G(U)|$, da der Normalisator $N_G(U)$ per Def der Stabilisator dieser Operation ist.

Sei $|G| = p^k \cdot m$, $p \nmid m$, dann ist $|U| = p^k$. Da $U \subset N_G(U)$ Untergruppe gilt $p^k \mid |N_G(U)|$

$\Rightarrow p \nmid |U^G|$

Wir schränken die Operation jetzt auf H ein:

$H \times U^G \longrightarrow U^G : (h, S) \mapsto hSh^{-1}$

Dann zerfällt U^G in eine disjunkte Vereinigung von Bahnen.

Sei $R \subset U^G$ eine Menge, die aus jeder Bahn genau ein Element enthält. Dann gilt mit der

Bahnengleichung 1.1.23

$$|U^G| = \sum_{S \in R} |H| / |\mathrm{Stab}_H(S)| = \sum_{S \in R} p^{j_S}$$

für geeignete $j_S \geq 0$, da H eine p-Gruppe ist und daher die Ordnungen von Untergruppen und Faktorgruppen auch p-Potenzen sind.

Da $p \nmid |U^G| \quad \exists S: j_S = 0$

Wir schreiben dieses $S \in R \subset U^G$ als gUg^{-1} für ein $g \in G$.

Für dieses S gilt:

$$\Rightarrow |H| / |\mathrm{Stab}_H(S)| = 1$$

$$\Rightarrow H = \mathrm{Stab}_H(S) = \{h \in H \mid hSh^{-1} = S\} \subset \mathrm{Stab}_G(S) = N_G(S)$$

1.5.13

$$\Rightarrow H \subset S = gUg^{-1}$$

S ist das Bild von U unter

eine Konjugation und damit isomorph zu U, insbesondere ist S eine p-Sylowgruppe. □

Beweis des Sylowschen Sätze 1.5.10:

1) Wegen Satz 1.5.4 $\exists$ eine p-Sylowgruppe $U \subset G$. Wegen Prop 1.5.15 $\exists$ g mit $H \subset gUg^{-1}$ und dies ist eine p-Sylowgruppe.

2) Sei H eine (weitere) p-Sylowgruppe, dann ist H eine p-Gruppe und wir können Prop 1.5.15 auf H anwenden. Wir erhalten g mit $H \subset gUg^{-1}$, und

$$p^k = |H| = |gUg^{-1}| \Rightarrow H = gUg^{-1}$$

Damit ist H zu U konjugiert.

3) Sei U p-Sylowgruppe, jede zu U konjugierte Untergruppe ist auch p-Sylowgruppe, aus 2) folgt

$U^G = \{$ p-Sylowgruppen von $G\}$

$\Rightarrow n_p = |U^G|$.

Wie in 1.5.15 sehen wir

$|G| = |U^G| \cdot |\mathrm{Stab}(U)| = n_p \cdot |\mathrm{Stab}(U)|$

$\Rightarrow n_p \mid |G|$.

Wir schränken die Konjugation auf U ein:

$U \times U^G \longrightarrow U^G : (u, S) \mapsto uSu^{-1}$

Sei $R \subset U^G$ eine Teilmenge, die aus jeder Bahn genau ein Element enthält.

Die Bahn von U ist

$\{uUu^{-1} \mid u \in U\} = \{U\}$.

Angenommen, es gäbe eine weitere Bahn mit nur einem Element, also $S \in U^G$ mit

$uSu^{-1} = S \quad \forall\, u \in U$.

Dann wäre $U \subset N_G(S)$ und mit 1.5.13 folgte $U \subset S$

$\Rightarrow U = S$ da beides p-Sylowgruppen sind.

Mit der Bahnengleichung 1.1.23 gilt also

$$n_p = |U^G| = \sum_{S \in R} |U| / |\mathrm{Stab}_U(S)| =$$

$$\sum_{S \in R} p^{j_S} \quad \text{mit geeigneten } j_S \geq 0,$$

da U p-Gruppe.

Weiter gilt $U \in R$ und $j_U = 0$

sowie $j_S > 0 \quad \forall \quad S \neq U$,

denn $|U| / |\mathrm{Stab}_U(S)| =$ Bahnlänge (S)

nach 1.1.21 und damit

$$n_p = 1 + \sum_{S \in R \setminus \{U\}} p^{j_S} \equiv 1 \bmod p \qquad \square$$

Die Sylowsätze sind wichtig bei der Klassifikation der endlichen Gruppen.
Eine Anwendung:

1.5.16 Satz Seien p, q prim, $p<q$, $p \nmid q-1$. Dann ist jede Gruppe G der Ordnung pq zyklisch, $G \cong \mathbb{Z}_{pq}$.

Beweis $n_p = 1 + k \cdot p$ wegen der Sylowsätze 1.5.10 3) und $n_p \mid q$ wegen Korollar 1.5.11.

$\Rightarrow n_p \in \{1, q\}$

Wäre $n_p = q \Rightarrow q = 1 + kp$

$\Rightarrow q - 1 = kp \Rightarrow p \mid q-1$ ↯.

$\Rightarrow n_p = 1$.

Sei P die einzige p-Sylowgruppe.

$n_q = 1 + lq$, $n_q \mid p \Rightarrow n_q \in \{1, p\}$

Wäre $n_q = p \Rightarrow p = 1 + lq \not\leq$ zu $p < q$

$\Rightarrow n_q = 1.$

Sei Q die einzige q-Sylowgruppe.

P und Q haben Primzahlordnung p bzw. q, sind also zyklisch:

$P \cong \mathbb{Z}_p$, $Q \cong \mathbb{Z}_q$.

Betrachte die Bahnen von P und Q unter Konjugation.

Nach 1.5.10 2) sind es jeweils alle p- bzw. q-Sylowgruppen, also ein elementig.

$\Rightarrow gPg^{-1} = P$, $gQg^{-1} = Q$

$\forall g \in G$

$\Rightarrow P, Q$ Normalteiler

Da P und Q teilerfremde Ordnungen

haben, gilt $P \cap Q = \{e\}$.

Mit 1.3.2 2) und dem 1. Isomophiesatz

folgt PQ ist Untergruppe von G

und $PQ/P \cong Q/P \cap Q \cong Q$

$$\Rightarrow \frac{|PQ|}{|P|} = |Q| \Rightarrow |PQ| = p \cdot q$$

$$\Rightarrow PQ = G.$$

Sei $g \in P, h \in Q \Rightarrow$

$ghg^{-1} \in Q$, da Q Normalteiler

$\Rightarrow ghg^{-1}h^{-1} \in Q$

Andererseits ist

$hg^{-1}h^{-1} \in P$, da P Normalteiler

$\Rightarrow ghg^{-1}h^{-1} \in P$

$\Rightarrow ghg^{-1}h^{-1} \in P \cap Q = \{e\}$

$\Rightarrow gh = hg \Rightarrow g$ und h vertauschen

1.4.3, Charakterisierung des direkten Produkts

$\Rightarrow$

$$G = P \times Q \cong \mathbb{Z}_p \times \mathbb{Z}_q.$$

Beh $\mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q$

Dies folgt aus dem chinesischen Restsatz:

Betrachte $\varphi: \mathbb{Z} \longrightarrow \mathbb{Z}_p \times \mathbb{Z}_q$

$a \longmapsto (a+p\mathbb{Z}, a+q\mathbb{Z})$

φ ist Homomorphismus.

φ ist surjektiv wegen des chinesischen Restsatzes: Für $(a_1, a_2) \in \mathbb{Z}_p \times \mathbb{Z}_q$ suchen wir a mit $a \equiv a_1 \bmod p$, $a \equiv a_2 \bmod q$, dies existiert nach dem chinesischen Restsatz und ist eindeutig mod pq.

$\ker \varphi = pq\mathbb{Z}$

$\overset{\text{Homomorphie-satz}}{\Longrightarrow} \mathbb{Z}_{pq} = \mathbb{Z}/pq\mathbb{Z} = \mathbb{Z}/\ker\varphi \cong \operatorname{Im}\varphi = \mathbb{Z}_p \times \mathbb{Z}_q.$

$\Longrightarrow G \cong \mathbb{Z}_{pq}$ ist zyklisch. □

1.5.17 Korollar Jede Gruppe der Ordnung 15 ist zyklisch.

Anders gesagt: Bis auf Isomorphie

$\exists!$ Gruppe der Ordnung 15, $\mathbb{Z}_{15}$.

1.6 Auflösbare Gruppen

1.6.1 Def

Eine Gruppe G heißt einfach, wenn sie nur die Normalteiler $\{e\}$ und G besitzt.

1.6.2 Lemma

Eine abelsche Gruppe $G \neq \{e\}$ ist einfach $\Leftrightarrow$ G zyklisch von Primzahlordnung

Beweis:

"$\Leftarrow$" Eine zyklische Gruppe von Primzahlordnung hat nur $\{e\}$ und G als Untergruppen

"$\Rightarrow$" Ist $|G|$ keine Primzahl, so existiert eine Primzahl p mit $p \mid |G|$.

Nach Satz 1.5.4 $\exists$ Untergruppe U mit $|U| = p$, da G abelsch, ist U Normalteiler. $\square$

1.6.3 Prop

Die alternierende Gruppe A_5 ist einfach.

Beweis:

A_5 hat $\frac{5!}{5} = 24$ 5-Zykel und

$\frac{5 \cdot 4 \cdot 3}{3} = 20$ 3-Zykel.

$|A_5| = 60 = 2^2 \cdot 3 \cdot 5$

$\Rightarrow$ Die 5-Sylowgruppen haben Ordnung 5, sind zyklisch von einem 5-Zykel erzeugt und enthalten je 4 5-Zykel.

$\Rightarrow \exists$ 6 5-Sylowgruppen.

Genauso: die 3-Sylowgruppen haben Ordnung 3, sind zyklisch und enthalten je 2 3-Zykel

$\Rightarrow \exists$ 10 3-Sylowgruppen.

Sei $\{e\} \subsetneq N \subsetneq A_5$ ein Normalteiler.

Angenommen, $5 \mid |N|$. Dann enthält N eine 5-Sylowuntergruppe, die auch 5-Sylowgruppe von A_5 ist.

Da alle 5-Sylowgruppen konjugiert sind, und $gNg^{-1} \subset N$, da N Normalteiler

folgt, alle 5-Sylowgruppen der A_5 sind in N $\Rightarrow$ $|N| \geq 1 + 24 = 25$

$\Rightarrow$ $|N| \in \{30, 60\}$. $\Rightarrow$ $3 \mid |N|$.

Damit enthält N auch eine (und damit alle) 3-Sylowgruppen, also folgt

$|N| \geq 1 + 24 + 20 = 45$ $\Rightarrow$ $|N| = 60$

$\Rightarrow$ $N = A_5$. ↯

Angenommen, $3 \nmid |N|$.

$\Rightarrow$ N enthält eine (und damit alle) 3-Sylowgruppen $\Rightarrow$ $|N| \geq 1 + 20 = 21$

$\Rightarrow$ $|N| \in \{30, 60\}$ $\Rightarrow$ $5 \mid |N|$

Dann folgt wieder $N = A_5$. ↯

Angenommen, $|N| = 4$.

Dann ist N 2-Sylowgruppe. Da die 2-Sylowgruppen konjugiert sind, und N Normalteiler ist, ist N die einzige 2-Sylowgruppe.

Aber alle $(2,2)$-Zykel haben Ordnung 2, also $\frac{5 \cdot 4}{2} \cdot \frac{3 \cdot 2}{2} \cdot \frac{1}{2} = 15$

Elemente, und jeweils 3 davon

liegen in einer Kleinschen Vierergruppe
$\Rightarrow$ $\exists$ 5 4- Sylowgruppen $\lightning$.

Angenommen, $|N| = 2$.
Dann ist $N = \langle n \rangle$ für ein Element n der Ordnung 2, also einen (2,2)- Zykel.
Da N Normalteiler gilt $gng^{-1} = n$ $\forall\, g \in A_5$, aber für $n = (ab)(cd)$ und $g = (abe)$ gilt
$gng^{-1} = (abe)(ab)(cd)(aeb) = (be)(cd) \neq n$
$\lightning$
Also gibt es keinen solchen Normalteiler und A_5 ist einfach. □

1.6.4 Def
Eine Gruppe G heißt auflösbar, wenn es eine Kette
$\{e\} = G_k \subset G_{k-1} \subset \dots \subset G_0 = G$
gibt, so daß $G_i \subset G_{i-1}$ Normalteiler und G_{i-1}/G_i abelsch $\forall\, i = 1, \dots, k$.

Eine solche Kette heißt Subnormalteiler-kette mit abelschen Faktoren.

Bsp

1) Abelsche Gruppen G sind auflösbar mit $\{e\} \subset G$.

2) S_4 ist auflösbar mit Subnormalteilerkette

$\{id\} \subset K_4 \subset A_4 \subset S_4$,

wobei K_4 die kleinsche Vierergruppe $\{id, (12)(34), (13)(24), (14)(23)\}$ ist.

Da $|S_4/A_4| = 2$, ist A_4 in S_4 Normalteiler. Daß K_4 in A_4 Normalteiler ist, läßt sich nachrechnen.

(Es gilt sogar $K_4 \subset S_4$ ist Normalteiler, man kann dies geometrisch begründen, da $S_4 = \mathrm{Sym}(\text{Tetraeder})$, und $K_4 = \ker(\varphi)$ für $\varphi: S_4 \to S_3 = S(\text{Kantenmitten diagonalen})$.)

$S_4/A_4 \cong \mathbb{Z}_2$ ist abelsch,

$A_4/K_4 \cong \mathbb{Z}_3$ " ,

K_4 ist auch abelsch.

3) A_5 ist einfach, nicht abelsch, also auch nicht auflösbar.

1.6.5 Prop

Sei G endlich, $U \subset G$ Untergruppe, N Normalteiler.

1) G auflösbar $\Rightarrow$ U auflösbar
2) G auflösbar $\Leftrightarrow$ N, G/N auflösbar.

Beweis:

1) Sei G auflösbar mit Subnormalteiler-kette

$$\{e\} = G_k \subset G_{k-1} \subset \dots \subset G_0 = G.$$

Setze $U_i := G_i \cap U$.

Dann ist

$$\{e\} \subset U_k \subset U_{k-1} \subset \dots \subset U_0 = U$$

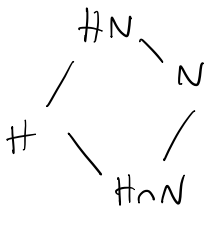
eine Kette von Untergruppen in U.

Dabei gilt

$$U_i = G_i \cap U = G_i \cap G_{i-1} \cap U = G_i \cap U_{i-1}$$

Wegen 1.3.2 1) ($H \cap N$ Normalteiler in H)

folgt $U_i = G_i \cap U_{i-1}$ ist Normalteiler in U_{i-1} (denn G_i ist Normalteiler in G_{i-1}).



Außerdem gilt

$$U_{i-1}/U_i = U_{i-1}/G_i \cap U_{i-1} \overset{\text{1. Isom. satz 1.3.3}}{\cong} G_i U_{i-1}/G_i$$

$\subset G_{i-1}/G_i$ ist Untergruppe, denn

$G_i U_{i-1} \subset G_{i-1}$ ist Untergruppe wegen 1.3.2.

Aber G_{i-1}/G_i ist abelsch, damit auch U_{i-1}/U_i.

2) $\Leftarrow$" N ist auflösbar wegen 1).

Sei $\{e\} = G_k \subset G_{k-1} \subset \dots \subset G_0 = G$ Subnormalteilerkette von G

Durch Multiplikation mit N erhalten wir wegen 1.3.2 eine Kette von Untergruppen

$N = G_k N \subset G_{k-1} N \subset \dots \subset G_0 N = G$.

Beh: $G_i N \subset G_{i-1} N$ ist Normalteiler.

Sei $g_1 n_1 \in G_i N$ und $g_2 n_2 \in G_{i-1} N$

Dann gilt

$$g_2 n_2 (g_1 n_1)(g_2 n_2)^{-1} = g_2 n_2 g_1 n_1 n_2^{-1} g_2^{-1}$$

Da N Normalteiler in G gilt

$g_1 n_1 g_1^{-1} \in N \Rightarrow \exists\ n_3 \in N:$

$g_1 n_1 g_1^{-1} = n_3 \Rightarrow g_1 n_1 = n_3 g_1$

$\Rightarrow g_2 n_2 g_1 n_1 n_2^{-1} g_2^{-1} = g_2 n_2 n_3 g_1 n_2^{-1} g_2^{-1}$

Genauso $\exists\ n_4 \in N:$

$g_2 (n_2 n_3) g_2^{-1} = n_4 \Rightarrow g_2 n_2 n_3 = n_4 g_2$

$\Rightarrow g_2 n_2 n_3 g_1 n_2^{-1} g_2^{-1} = n_4 g_2 g_1 n_2^{-1} g_2^{-1}$

Da $G_i \subset G_{i-1}$ Normalteiler, $g_1 \in G_i$,

$g_2 \in G_{i-1}$, $\exists\ g_3 \in G_i:$

$g_2 g_1 g_2^{-1} = g_3 \Rightarrow g_2 g_1 = g_3 g_2$

$\Rightarrow n_4 g_2 g_1 n_2^{-1} g_2^{-1} = n_4 g_3 g_2 n_2^{-1} g_2^{-1}$

Weiterhin $\exists\ n_5 \in N:\ g_3^{-1} n_4 g_3 = n_5$

$\Rightarrow n_4 g_3 = g_3 n_5$

$\Rightarrow n_4 g_3 g_2 n_2^{-1} g_2^{-1} = g_3 n_5 \underbrace{g_2 n_2^{-1} g_2^{-1}}_{\in N,\ \text{da } N \text{ Normalteiler}}$

$\in G_i N.$

Mit dem 1. und 2. Isomorphiesatz (1.3.3, 1.3.5)

folgt

$$G_{i-1}N/G_iN = G_{i-1}G_iN/G_iN \overset{1.}{\cong} G_{i-1}/G_{i-1}\cap G_iN$$

$$\overset{2.}{\cong} G_{i-1}/G_i \Big/ G_{i-1}\cap G_iN/G_i$$

$\Rightarrow$ $G_{i-1}N/G_iN$ ist isomorph zu einer Faktorgruppe der abelschen Gruppe G_{i-1}/G_i und damit selbst abelsch.

$\Rightarrow$ $N = G_kN \subset G_{k-1}N \subset \dots \subset G_0N = G$

ist Subnormalteilerreihe

$\Rightarrow$ $\{e_{G/N}\} = N/N = G_kN/N \subset \dots \subset G_0N/N = G/N$

ist Subnormalteilerreihe mit abelschen Faktoren $G_{i-1}N/N \Big/ G_iN/N \overset{2.}{\cong} G_{i-1}N/G_iN$.

$\Rightarrow$ G/N ist auflösbar.

"$\Leftarrow$" Seien N und G/N auflösbar mit

$$\{e\} = N_k \subset N_{k-1} \subset \cdots \subset N_0 = N \quad \text{und}$$

$$\{e_{G/N}\} = G_\ell/N \subset G_{\ell-1}/N \subset \cdots \subset G_0/N = G/N.$$

Dann ist

$$\{e\} = N_k \subset \cdots \subset N_0 = N = G_\ell \subset G_{\ell-1} \subset \cdots \subset G_0 = G$$

eine Subnormalteilerkette mit abelschen Faktoren, denn $G_{i-1}/G_i \overset{2.}{\cong} G_{i-1}/N \,/\, G_i/N$ □

1.6.6 Korollar

Für $n \geq 5$ sind S_n, A_n nicht auflösbar.

Beweis: Da $A_5 \subset A_n \subset S_n$ Untergruppe ist und A_5 nicht auflösbar ist. □

1.6.7 Korollar

Sei G eine p-Gruppe, dann ist G auflösbar.

Beweis: Sei $|G| = p^n$, p Primzahl.

Induktion nach n.

$n = 0$: nichts zu zeigen.

$n = 1$: G ist zyklisch und auflösbar.

Sei $n>0$. Nach 1.2.13 gilt $p \mid |Z(G)|$

$\Rightarrow \{e\} \subsetneq Z(G) \subset G$.

Falls $Z(G) = G \Rightarrow G$ ist abelsch $\Rightarrow G$ auflösbar.

Falls $Z(G) \subsetneq G$, so sind $Z(G)$ und $G/Z(G)$ selbst p-Gruppen, die nach 1.6.5 2) Induktionsvoraussetzung auflösbar sind $\Rightarrow$ G ist auflösbar. □

1.6.8 Def Sei G eine endliche Gruppe. Eine Kette $\{e\} \subset G_k \subset G_{k-1} \subset \dots \subset G_0 = G$ von Untergruppen, so daß $G_i \subset G_{i-1}$ Normalteiler ist und G_{i-1}/G_i zyklisch von Primzahlordnung, heißt Kompositionsreihe.

1.6.9 Satz Sei G endliche Gruppe.

G auflösbar $\Leftrightarrow$ G besitzt eine Kompositionsreihe

Beweis: „$\Leftarrow$" klar.

"$\Rightarrow$" Wir müssen eine Subnormalteilerkette zu einer Kompositionsreihe verfeinern.

Falls G_{i-1}/G_i nicht Primzahlordnung hat, so ist G_{i-1}/G_i nach Lemma 1.6.2 nicht einfach, besitzt also einen echten Normalteiler, mit dem wir verfeinern können. Die Ordnungen der Faktorgruppen werden dabei echt kleiner, nach endlich vielen Schritten erhalten wir also Faktorgruppen von Primzahlordnung. □

Bsp 1) S_4 hat die Kompositionsreihe

$\{id\} \subset \langle (12)(34) \rangle \subset K_4 \subset A_4 \subset S_4$.

2) Gruppen der Ordnung pq mit p, q prim sind auflösbar:

Wie in Satz 1.5.16 folgt für $p \neq q$, daß es nur eine q-Sylowgruppe gibt, diese ist somit Normalteiler, und

$\{e\} \subset Q \subset G$ ist Kompositionsreihe, da $|Q| = q$ und $|G/Q| = \frac{pq}{q} = p$.

2. Ringe

Vorwissen:

nullteilerfreie Ringe

$K[x,y,z,w]/(2xy-2w)$

$\mathbb{Z}[\sqrt{-3}]$

Noethersch, nicht faktoriell: $\mathbb{Z}[i\sqrt{5}]$

Faktoriell, nicht noethersch: $K[x_1, x_2, \dots]$

$\cup$

Faktorielle Ringe

$K[x_1, \dots, x_n]$

$\mathbb{Z}[x]$

($\langle 2, x \rangle$ ist kein Hauptideal)

(ohne Beweis: Satz von Gauß: R faktoriell $\Rightarrow$ R[x] faktoriell)

$\cup$

Noethersche Ringe

$K[x_1, \dots, x_n]$

$\cup$

Hauptidealringe

$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$

(ohne Beweis)

$\cup$

euklidische Ringe

$\mathbb{Z}$, $\mathbb{Z}[i]$, $K[x]$

Vorwissen:

Faktorielle Ringe,
Primelemente, irreduzible Elemente,
Einheiten,
Primfaktorzerlegung,
ggT und kgV
Quotientenkörper

Polynomringe
K-Algebra

in Kapitel 3 auch:
euklidische Ringe
Ideale
Noethersche Ringe
chinesischer Restsatz

in Kapitel 4 auch:
maximale Ideale

Notation: R bezeichnet einen kommutativen Ring mit 1.

Der Satz von Gauß und allgemeine Polynomringe

2.1 Satz (Satz von Gauß)

R faktoriell $\Rightarrow$ $R[X]$ faktoriell.

2.2 Def

Sei R nullteilerfrei,

$0 \neq f = \sum_{i=0}^{n} a_i X^i \in R[X]$ ein Polynom. f heißt primitiv, falls

$1 = ggT(a_0, \dots, a_n)$.

2.3 Lemma

Sei R faktoriell.

1) Ist $f \in R[X]$ primitiv und $c \in Quot(R)$ mit $c \cdot f \in R[X]$, so ist $c \in R$.

2) Für $f \in Quot(R)[X]$ $\exists$ $0 \neq c \in Quot(R)$ und $g \in R[X]$ primitiv mit $f = c \cdot g$.

Beweis:

1) Sei $f = \sum_{i=0}^{n} a_i x^i$, $c = \frac{a}{b}$ mit $a, b \in R$ teilerfremd. Da $cf \in R[x] \Rightarrow$

$\frac{a a_i}{b} \in R \quad \forall i = 0, \dots, n.$

Sei $p \in R$ prim mit $p \mid b$.

Da $p \nmid a$ folgt aus $\frac{a a_i}{b} \in R$

$p \mid a_i \quad \forall i = 0, \dots, n$

$\Rightarrow p \mid ggT(a_0, \dots, a_n)$

$\Rightarrow ggT(a_0, \dots, a_n) \neq 1 \Rightarrow f$ nicht primitiv

$\Rightarrow \nexists$ solches p

$\Rightarrow b \in R^* \Rightarrow c = \frac{a}{b} \in R.$

2) Sei $f = \sum_{i=0}^{n} \frac{a_i}{b_i} \cdot x^i$ mit

$a_i \in R$, $b_i \in R \setminus \{0\}$.

$\Rightarrow b_0 \cdots b_n \cdot f \in R[x]$ und für

$d = ggT(\text{Koeffizienten von } b_0 \cdots b_n f)$ gilt

$g := \frac{b_0 \cdots b_n \cdot f}{d} \in R[x]$ ist

primitiv und $c \cdot g = f$ mit

$c = \frac{d}{b_0 \cdots b_n} \in \mathrm{Quot}(R)$. □

Bsp:

Sei $f = x^3 - 3x + \frac{1}{4} \in \mathbb{Q}[x]$,

dann ist $g = 4x^3 - 12x + 1 \in \mathbb{Z}[x]$

primitiv und für $c = \frac{1}{4} \in \mathrm{Quot}(\mathbb{Z}) = \mathbb{Q}$

gilt $c \cdot g = f$.

2.4 Lemma Sei R nullteilerfrei, $p \in R$

prim $\Rightarrow$ p ist prim in $R[x]$.

Beweis: Seien $f = \sum_{i=0}^{n} a_i x^i$ und

$g = \sum_{j=0}^{m} b_j x^j \in R[x]$ mit

$p \mid f \cdot g = \sum_{k=0}^{m+n} c_k x^k$ mit

$$c_k = \sum_{l=0}^{k} a_l b_{k-l}.$$

$\Rightarrow \quad p \mid c_k \quad \forall k \quad (*)$

Angenommen, $p \nmid f$ und $p \nmid g$.

Dann $\exists\ i_0, j_0 : p \nmid a_{i_0}, p \nmid b_{j_0}$.

Wähle i_0, j_0 minimal.

Dann gilt

$$a_{i_0} b_{j_0} = c_{i_0+j_0} - \sum_{\ell=0}^{i_0-1} a_\ell b_{i_0+j_0-\ell} - \sum_{\ell=i_0+1}^{i_0+j_0} a_\ell b_{i_0+j_0-\ell}$$

und p teilt jeden Summanden auf der rechten Seite:

- $c_{i_0+j_0}$ wegen $(*)$
- $a_\ell b_{i_0+j_0-\ell}$ für $\ell < i_0-1$, da dann a_ℓ von p geteilt wird, da i_0 minimal mit $p \nmid a_{i_0}$
- $a_\ell b_{i_0+j_0-\ell}$ für $\ell > i_0+1$, da dann $b_{i_0+j_0-\ell}$ von p geteilt wird

da j_0 minimal mit $p \nmid b_{j_0}$.

$\Rightarrow \quad p \mid a_{i_0} b_{j_0}$

p prim $\Rightarrow \quad p \mid a_{i_0}$ oder $p \mid b_{j_0}$ $\lightning$

zur Wahl von a_{i_0}, b_{j_0} □

2.5 Lemma

Sei R faktoriell, $f, g \in R[x]$ primitiv, dann ist auch $f \cdot g$ primitiv.

Beweis: Angenommen, $f \cdot g$ ist nicht primitiv $\Rightarrow \exists$ Primelement $p \in R$, das jeden Koeffizienten von $f \cdot g$ teilt

$\Rightarrow p \mid f \cdot g \overset{2.4}{\Rightarrow} p \mid f$ oder $p \mid g$, da p auch in $R[x]$ prim ist

↯ zu f, g primitiv. □

2.6 Lemma

Sei R faktoriell, $f \in R[x]$ primitiv, f prim in $\mathrm{Quot}(R)[x]$. Dann ist f prim in $R[x]$.

Beweis: Da f primitiv ist, ist $f \neq 0$.

Da $f \in \mathrm{Quot}(R)[x]$ prim ist, ist $f \notin R^* = (R[x])^*$, also keine Einheit

in $R[x]$.

Seien $g, h \in R[x]$ mit $f \mid g \cdot h$ in $R[x]$.

Dann gilt auch $f \mid g \cdot h$ in $\mathrm{Quot}(R)[x]$,

und da f dort prim ist, folgt $\in$

$f \mid g$ in $\mathrm{Quot}(R)[x] \Rightarrow \exists\, q \in \mathrm{Quot}(R)[x]$:

$$f \cdot q = g.$$

Wie in 2.3 schreiben wir q als

$q = c \cdot \tilde{q}$ mit $\tilde{q} \in R[x]$ primitiv

und $c \in \mathrm{Quot}(R)$.

Dann gilt $g = f \cdot q = c \cdot f \cdot \tilde{q}$.

Wegen $f, \tilde{q}$ primitiv in $R[x]$ folgt

mit 2.5 : $f \cdot \tilde{q}$ primitiv in $R[x]$.

Damit folgt aus 2.3.1) $c \in R$

$\Rightarrow q \in R[x] \Rightarrow f \mid g$ in $R[x]$

□

Beweis von Satz 2.1 (Gauß):

Sei $0 \neq f \in R[x]$, $f \notin (R[x])^* \cup \{0\}$.

Zu zeigen: f besitzt eine Darstellung

als Produkt von Primelementen.

Ist $f \in R$, so folgt dies aus der Tatsache, daß R faktoriell ist, und Lemma 2.4.

Sei $\deg(f) \geq 1$.

Da $\mathrm{Quot}(R)$ ein Körper ist, ist $\mathrm{Quot}(R)[X]$ euklidisch, daher Hauptidealring, daher faktoriell.

In $\mathrm{Quot}(R)[X]$ können wir f also schreiben als

$f = q_1 \cdots q_k$ mit $q_i \in \mathrm{Quot}(R)[X]$ prim.

Wie in 2.3. 2) schreiben wir

$q_i = c_i \cdot p_i$ mit $c_i \in \mathrm{Quot}(R)$ und $p_i \in R[X]$ primitiv.

p_i und q_i sind assoziiert in $\mathrm{Quot}(R)[X]$ (da $c_i \in \mathrm{Quot}(R)$ Einheit, da $c_i \neq 0$ und $\mathrm{Quot}(R)$ Körper),

also ist mit q_i auch p_i prim in $\mathrm{Quot}(R)[x]$.

Wegen 2.6 ist p_i prim in $R[x]$.

Wegen 2.5 ist

$$p := p_1 \cdots p_k \in R[x]$$

primitiv.

Da $f = c \cdot p \in R[x]$ mit $c := c_1 \cdots c_k \in \mathrm{Quot}(R)$ und p primitiv folgt aus 2.3 1) $c \in R$.

Da R faktoriell ist, können wir $c = b_1 \cdots b_e$ in Primfaktoren b_i zerlegen, die wegen 2.4 prim in $R[x]$ sind.

Damit ist $f = b_1 \cdots b_e \cdot p_1 \cdots p_k$ eine Zerlegung in Primfaktoren in $R[x]$.

Die Eindeutigkeit der Zerlegung

bis auf Anordnung und Einheiten folgt per Induktion über die Anzahl der Faktoren und der definierenden Eigenschaft der Primelemente. □

Bsp

1) $\mathbb{Z}[x]$ ist faktoriell.

2) Ist K ein Körper, so ist $K[x_1, \dots, x_n]$ faktoriell.

2.7 Def

Sei I eine beliebige Menge.

$$R[x_i \mid i \in I] = \left\{ \sum_{\alpha = (\alpha_1, \dots, \alpha_k) \in \mathbb{N}^k} a_\alpha \, x_{i_1}^{\alpha_1} \cdots x_{i_k}^{\alpha_k} \;\middle|\; k \in \mathbb{N},\ \{i_1, \dots, i_k\} \subset I,\ a_\alpha \in R,\ \text{nur endlich viele } a_\alpha \neq 0 \right\}$$

ist der Polynomring in den Variablen x_i mit $i \in I$.

Für $|I| < \infty$, o.E. $I = \{1, \dots, n\}$ ist es $R[x_1, \dots, x_n]$.

Multiindexnotation:

Für $(i_1, \dots, i_k)$ fest und $\alpha \in \mathbb{N}^k$ schreiben wir

$$X^\alpha := X_{i_1}^{\alpha_1} \cdots X_{i_k}^{\alpha_k}.$$

Für $f \in R[X_i, i \in I]$ ist die Menge der vorkommenden Variablen (i.e. ij: $\exists\, \alpha : a_\alpha \neq 0, \alpha_j \neq 0$) $\{i_1, \dots, i_k\}$ der <u>Support</u> von f, $\operatorname{supp}(f)$.

Durch Hinzufügen von Nullen als Exponenten können wir ein Polynom immer bezüglich einer größeren Variablenmenge darstellen.
Durch Hinzufügen von Nullen als Koeffizienten können wir auch die Exponentenmenge erweitern.

Für $f, g \in R[X_i \mid i \in I]$ schreiben wir f und g bezüglich derselben Variablenmenge $(\operatorname{supp}(f) \cup \operatorname{supp}(g))$ sowie derselben Exponentenmenge,

$$f = \sum_\alpha a_\alpha X^\alpha, \quad g = \sum_\alpha b_\alpha X^\alpha$$

und definieren

$$f+g = \sum_{\alpha} (a_\alpha + b_\alpha) x^\alpha \quad \text{und}$$

$$f \cdot g = \sum_{\beta} \left(\sum_{\alpha+\alpha'=\beta} a_\alpha b_{\alpha'} \right) x^\beta$$

wobei die zweite Summe über alle β geht, die als Summen von Exponenten in f und g vorkommen.

Durch diese Verknüpfungen wird $R[x_i \mid i \in I]$ ein kommutativer Ring mit 1.

2.8 Lemma

Sei R nullteilerfrei, I eine Menge, $J \subset I$ eine endliche Teilmenge.

1) $(R[x_i \mid i \in I])^* = R^*$

2) Sei $p \neq 0$, $p \in R[x_j \mid j \in J] \setminus R^*$.

p prim in $R[x_j \mid j \in J] \iff$
p prim in $R[x_i \mid i \in I]$.

Beweis: Sei $f \in (R[x_i \mid i \in I])^*$

$\Rightarrow \exists\, g \in R[x_i \mid i \in I] : f \cdot g = 1$.

In f und g kommen nur endlich viele Variablen x_j mit $j \in J$ vor, daher gilt $f \cdot g = 1$ in $R[x_j \mid j \in J]$

$\Rightarrow f \in R^*$.

2) „$\Rightarrow$" Sei p prim in $R[x_j \mid j \in J]$.

Seien $f, g \in R[x_i \mid i \in I]$ mit $p \mid f \cdot g$. Es gibt eine endliche Menge $J' \supset J$, die alle Variablen von p, f und g enthält ($J' = J \cup \operatorname{supp} f \cup \operatorname{supp} g$)

$\Rightarrow p \mid f \cdot g$ in $R[x_j \mid j \in J']$

Durch Induktion folgt mit 2.4, daß p prim in $R[x_j \mid j \in J']$ ist

$\Rightarrow 0 = p \mid f$.

$\Rightarrow p$ prim in $R[x_i \mid i \in I]$.

„$\Leftarrow$" Sei p prim in $R[x_i \mid i \in I]$.

Seien $f, g \in R[x_j \mid j \in J]$ mit

$p \mid f \cdot g \Rightarrow p \mid f \cdot g$ in $R[x_i \mid i \in I]$

$\overset{p \text{ prim}}{\Rightarrow} 0 = p \mid f$ in $R[x_i \mid i \in I] \Rightarrow$

$\exists\ q \in R[x_i \mid i \in I]$:

$q \cdot p = f$.

Da $p, f \in R[x_j \mid j \in J]$ kann q keine Variable x_i mit $i \notin J$ enthalten, also folgt $q \in R[x_j \mid j \in J]$ und $p \mid f$ in $R[x_j \mid j \in J] \Rightarrow$ p prim in $R[x_j \mid j \in J]$. □

2.9 Proposition

Sei I eine Menge. Sei R faktoriell. $R[x_i \mid i \in I]$ ist faktoriell.

Beweis:

Sei $0 \neq f \in R[x_i \mid i \in I] \setminus R^*$.

Dann ist $J = \mathrm{supp}(f)$ endlich und $f \in R[x_j \mid j \in J]$. In diesem Ring hat f durch Induktion und den Satz von Gauß eine eindeutige Primfaktorzerlegung, die wegen 2.8 2) eine Primfaktorzerlegung in $R[x_i \mid i \in I]$ ist. □

2.10 Satz (Universelle Eigenschaft von Polynomringen)

Sei I eine Menge, A eine R-Algebra, $a_i \in A \quad \forall i \in I$.

Dann $\exists!$ R-Algebrenhomomorphismus $\varphi: R[X_i \mid i \in I] \longrightarrow A$ mit $X_i \longmapsto a_i$, der Einsetzehomomorphismus.

Das Bild von φ heißt die von den a_i erzeugte Unteralgebra $\langle a_i \mid i \in I \rangle \subset A$.

Man schreibt auch $\langle a_i \mid i \in I \rangle_R$ oder $R[a_i \mid i \in I]$ für $\mathrm{Im}(\varphi)$, also für die von den a_i erzeugte Unter(-R-)Algebra von A.

Beweis: Durch

$$\varphi\Big(\sum_{\alpha} b_\alpha X_{i_1}^{\alpha_1} \cdots X_{i_k}^{\alpha_k}\Big) = \sum_{\alpha} b_\alpha a_{i_1}^{\alpha_1} \cdots a_{i_k}^{\alpha_k}$$

ist der eindeutige Homomorphismus gegeben. □

3. Moduln und der Elementarteilersatz

3.1 Matrizen über Ringen und die Smith-Normalform

In Lineare Algebra 1 haben wir für $A \in Mat(m \times n, K)$ (K Körper) mit Hilfe des Gauß-Algorithmus eine Normalform $SAT = \left(\begin{array}{c|c} 1\!\!1_r & 0 \\ \hline 0 & 0 \end{array}\right)$ erzielt, wobei $S \in GL(m, K)$, $T \in GL(n, K)$, $r = rang(A)$.

Def Adjunkte:

$A^{\#} = (a_{ij}^{\#})_{ij}$, $a_{ij}^{\#} = (-1)^{i+j} \det(A_{ji})$

wobei A_{ji} die Streichungsmatrix von A ist, bei der die j-te Zeile und die i-te Spalte gestrichen wird.

3.1.1 Satz Sei R ein kommutativer Ring mit 1, $A \in Mat(n, R)$.

$A^{\#} \cdot A = A \cdot A^{\#} = \det(A) \cdot 1\!\!1_n$.

Beweis wie in lineare Algebra, mit Verallgemeinerung.

3.1.2 Korollar

$A \in Mat(n, R)$ invertierbar $\Leftrightarrow$ $\det(A) \in R^*$

Beweis: „$\Leftarrow$" $\det(A) \in R^* \Rightarrow$ $\frac{1}{\det(A)} \cdot A^\#$ ist die Inverse von A.

„$\Rightarrow$" $A^{-1} \cdot A = 1_n \Rightarrow \det(A)^{-1} \cdot \det(A) = 1$

$\Rightarrow \det(A) \in R^*$. □

Bemerkung:
Über Ringen gilt nicht: voller Rang $\Rightarrow$ invertierbar.

z.B. $(2) \in Mat(1, \mathbb{Z})$ hat vollen Rang, aber $\det(2) = 2 \notin \mathbb{Z}^*$

$\Rightarrow (2)$ ist nicht invertierbar

(über $\mathbb{Q}$ wäre $(1/2)$ die inverse Matrix).

3.1.3 Satz (Smith-Normalform)

Sei R ein euklidischer Ring, $A \in \mathrm{Mat}(m \times n, R)$. Dann $\exists$ $S \in GL(m, R)$, $T \in GL(n, R)$, $r \leq \min\{m, n\}$ mit

$$SAT = D = \left(\begin{array}{c|c} \begin{matrix} d_1 & & \\ & \ddots & \\ & & d_r \end{matrix} & 0 \\ \hline 0 & 0 \end{array}\right)$$

mit $d_i \mid d_{i+1}$ $\forall$ $i = 1, \ldots, r-1$.

Die d_i sind (bis auf Einheiten) durch A eindeutig bestimmt und heißen Elementarteiler von A.

D heißt Smith-Normalform von A.

Bem Der Satz gilt allgemeiner für Hauptidealringe R, wir werden ihn jedoch nur für euklidische Ringe beweisen.

Der Beweis ist konstruktiv:

3.1.4 Algorithmus (Smith-Normalform)

Sei R mit $v: R \to \mathbb{N}$ euklidischer Ring, $A \in \mathrm{Mat}(m \times n, R)$, $A \neq 0$.

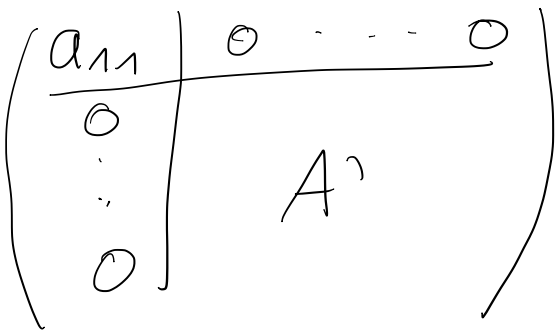
1. Schritt: Zeilen- und Spaltenvertauschungen, so daß $a_{11} \neq 0$ und $v(a_{11}) \leq v(a_{ij})$ $\forall\, a_{ij} \neq 0$ $\forall\, (i,j) \neq (1,1)$.

2. Schritt: Schreibe jedes a_{1j} und a_{j1}, das nicht durch a_{11} teilbar ist, als $a_{1j} = q \cdot a_{11} + r$ mit $v(r) < v(a_{11})$ und reduziere entsprechend mit der 1. Zeile bzw. Spalte.

Zurück nach Schritt 1.

Da $v(a_{11})$ in jedem Schritt echt kleiner wird, terminiert der Prozeß und wir enden mit einer Matrix, in der alle Einträge der 1. Zeile und Spalte durch a_{11} teilbar sind.

3. Schritt Addiere Vielfache der 1. Zeile bzw. Spalte und erhalte



Sind nicht alle Einträge von A' durch a_{11} teilbar, z.B. a_{ij} nicht teilbar, so addiere die i-te zur 1. Zeile und gehe wieder nach Schritt 2.

Der nicht teilbare Eintrag ist jetzt in der 1. Zeile, wir verwenden wieder Division mit Rest und gehen zurück nach Schritt 1 usw. Da $\min\{v(a_{ij})\}$ bei jedem Durchlaufen von Schritt 2 echt kleiner wird, terminiert dieser Prozeß und wir enden mit einem A', in dem alle Einträge durch a_{11} teilbar sind.

Sind alle Einträge von A' durch a_{11} teilbar, beginne mit A' bei Schritt 1.

Beweis: Terminierung siehe Zwischenkommentare. Korrektheit: Rekursiv erhalten wir

$$\left(\begin{array}{c|c|c} a_{11} & 0 \cdots 0 & \\ \hline 0 & a_{22} & 0 \cdots 0 \\ \hline \vdots & 0 & a_{33} \cdots \\ 0 & \vdots & \end{array}\right) \Big\} \text{ Output von } A'$$

Da alle Einträge von A' durch a_{11} teilbar sind, sind auch alle Einträge, die während des Prozesses auftauchen, durch a_{11} teilbar, insbesondere a_{22}. Die Korrektheit folgt per Induktion. Für den Induktionsanfang beachte, daß für $n=1$ oder $m=1$ der Algorithmus einfach Division mit Rest ist und den ggT der Einträge der Zeile bzw. Spalte produziert. □

Bem Die Matrizen S, T erhält man durch Mitprotokollieren der Zeilen- bzw. Spaltenoperationen.

Bsp: $A = \begin{pmatrix} 6 & 9 & 6 \\ 6 & 6 & 7 \end{pmatrix} \in \mathrm{Mat}(2\times 3, \mathbb{Z})$

Die euklidische Norm ist

$v: \mathbb{Z} \to \mathbb{N}: a \mapsto |a|$.

Schritt 1: 6 hat schon kleinste Norm, weiter nach Schritt 2.

Schritt 2: $9 = 1 \cdot 6 + 3$, reduziere mit

1. Spalte:

$$\left(\begin{array}{cc|ccc} 1 & 0 & 6 & 9 & 6 \\ 0 & 1 & 6 & 6 & 7 \\ \hline & & 1 & 0 & 0 \\ & & 0 & 1 & 0 \\ & & 0 & 0 & 1 \end{array}\right) \xrightarrow{\substack{\text{Spalte} \\ \text{II} \mapsto \\ \text{II} - \text{I}}} \left(\begin{array}{cc|ccc} 1 & 0 & 6 & 3 & 6 \\ 0 & 1 & 6 & 0 & 7 \\ \hline & & 1 & -1 & 0 \\ & & 0 & 1 & 0 \\ & & 0 & 0 & 1 \end{array}\right)$$

Zurück nach Schritt 1, Spalten vertauschen:

$$\xrightarrow{\substack{\text{Spalte} \\ \text{I} \leftrightarrow \text{II}}} \left(\begin{array}{cc|ccc} 1 & 0 & 3 & 6 & 6 \\ 0 & 1 & 0 & 6 & 7 \\ \hline & & -1 & 1 & 0 \\ & & 1 & 0 & 0 \\ & & 0 & 0 & 1 \end{array}\right)$$

Jetzt sind alle in der 1. Zeile und Spalte durch 3 teilbar, reduziere mit Schritt 3:

$$\xrightarrow{\substack{\text{Spalte} \\ \text{II} \mapsto \text{II} - 2\text{I} \\ \text{III} \mapsto \text{III} - 2\text{I}}} \left(\begin{array}{cc|ccc} 1 & 0 & 3 & 0 & 0 \\ 0 & 1 & 0 & 6 & 7 \\ \hline & & -1 & 3 & 2 \\ & & 1 & -2 & -2 \\ & & 0 & 0 & 1 \end{array}\right)$$

$A' = (6\ 7)$, 7 ist nicht durch 3 teilbar, addiere 2. Zeile zu 1. und weiter mit Schritt 1

$$\xrightarrow{\substack{\text{Zeile} \\ \text{I} \mapsto \text{I} + \text{II}}} \left(\begin{array}{cc|ccc} 1 & 1 & 3 & 6 & 7 \\ 0 & 1 & 0 & 6 & 7 \\ \hline & & -1 & 3 & 2 \\ & & 1 & -2 & -2 \\ & & 0 & 0 & 1 \end{array}\right)$$

3 ist das kleinste, Schritt 2:

$7 = 3 \cdot 2 + 1$, reduziere mit Spalte 1:

$$\left(\begin{array}{cc|ccc} 1 & 1 & 3 & 6 & 7 \\ 0 & 1 & 0 & 6 & 7 \\ \hline & & -1 & 3 & 2 \\ & & 1 & -2 & -2 \\ & & 0 & 0 & 1 \end{array}\right)$$

Spalte
$\text{III} \mapsto \text{III} - 2\,\text{I}$ ⟶

$$\left(\begin{array}{cc|ccc} 1 & 1 & 3 & 6 & 1 \\ 0 & 1 & 0 & 6 & 7 \\ \hline & & -1 & 3 & 4 \\ & & 1 & -2 & -4 \\ & & 0 & 0 & 1 \end{array}\right)$$

Schritt 1: vertausche III und I Spalte, damit 1 als kleinstes nach vorne kommt

Spalte
$\text{III} \hookrightarrow \text{I}$ ⟶

$$\left(\begin{array}{cc|ccc} 1 & 1 & 1 & 6 & 3 \\ 0 & 1 & 7 & 6 & 0 \\ \hline & & 4 & 3 & -1 \\ & & -4 & -2 & 1 \\ & & 1 & 0 & 0 \end{array}\right)$$

alle in 1. Zeile & Spalte teilbar durch 1 → Schritt 3, reduziere

Spalte
$\text{II} \mapsto \text{II} - 6\,\text{I}$
$\text{III} \mapsto \text{III} - 3\,\text{I}$ ⟶

$$\left(\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 7 & -36 & -21 \\ \hline & & 4 & -21 & -13 \\ & & -4 & 22 & 13 \\ & & 1 & -6 & -3 \end{array}\right)$$

Zeile
$\text{II} \mapsto \text{II} - 7 \cdot \text{I}$ ⟶

$$\left(\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ -7 & -6 & 0 & -36 & -21 \\ \hline & & 4 & -21 & -13 \\ & & -4 & 22 & 13 \\ & & 1 & -6 & -3 \end{array}\right)$$

$A' = (-36 \quad -21)$
alle Einträge durch 1 teilbar
weiter mit A' nach Schritt 1

$v(-21) = 21$ ist das kleinste tausche Spalten:

$$\left(\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ -7 & -6 & 0 & -36 & -21 \\ & & 4 & -21 & -13 \\ & & -4 & 22 & 13 \\ & & 1 & -6 & -3 \end{array}\right) \xrightarrow{\text{Spalte II} \hookrightarrow \text{III}} \left(\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ -7 & -6 & 0 & -21 & -36 \\ & & 4 & -13 & -21 \\ & & -4 & 13 & 22 \\ & & 1 & -3 & -6 \end{array}\right)$$

Schritt 2: Division mit Rest

$-36 = -21 - 15$

$$\xrightarrow{\text{Spalte III} \mapsto \text{III} - \text{II}} \left(\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ -7 & -6 & 0 & -21 & -15 \\ & & 4 & -13 & -8 \\ & & -4 & 13 & 9 \\ & & 1 & -3 & -3 \end{array}\right)$$

Schritt 1: tausche Spalten

$$\xrightarrow{\text{Spalte II} \hookrightarrow \text{III}} \left(\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ -7 & -6 & 0 & -15 & -21 \\ & & 4 & -8 & -13 \\ & & -4 & 9 & 13 \\ & & 1 & -3 & -3 \end{array}\right)$$

Schritt 2: Division mit Rest

$-21 = -15 - 6$

reduziere

$$\xrightarrow{\text{Spalte III} \mapsto \text{III} - \text{II}} \left(\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ -7 & -6 & 0 & -15 & -6 \\ & & 4 & -8 & -5 \\ & & -4 & 9 & 4 \\ & & 1 & -3 & 0 \end{array}\right)$$

Schritt 1: tausche Spalten

$$\xrightarrow{\text{Spalte III} \hookrightarrow \text{II}}$$

$$\left(\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ -7 & -6 & 0 & -6 & -15 \\ \hline & & 4 & -5 & -8 \\ & & -4 & 4 & 9 \\ & & 1 & 0 & -3 \end{array}\right)$$

Schritt 2:
Division mit Rest
$-15 = 2 \cdot (-6) - 3$

Spalte III $\mapsto$ III -2 II $\longrightarrow$

$$\left(\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ -7 & -6 & 0 & -6 & -3 \\ \hline & & 4 & -5 & 2 \\ & & -4 & 4 & 1 \\ & & 1 & 0 & -3 \end{array}\right)$$

Schritt 1:
Spalten tauschen

Spalte II $\leftrightarrow$ III $\longrightarrow$

$$\left(\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ -7 & -6 & 0 & -3 & -6 \\ \hline & & 4 & 2 & -5 \\ & & -4 & 1 & 4 \\ & & 1 & -3 & 0 \end{array}\right)$$

alle Einträge durch -3 teilbar, reduziere mit Schritt 3:

Spalte III $\mapsto$ III -2 II $\longrightarrow$

$$\left(\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ -7 & -6 & 0 & -3 & 0 \\ \hline & & 4 & 2 & -9 \\ & & -4 & 1 & 2 \\ & & 1 & -3 & 6 \end{array}\right)$$

Die Elementarteiler sind 1, 3
(bis auf Einheiten in $\mathbb{Z}$, i.e. Vorzeichen).

Es gilt $\begin{pmatrix} 1 & 1 \\ -7 & -6 \end{pmatrix} \cdot \begin{pmatrix} 6 & 9 & 6 \\ 6 & 6 & 7 \end{pmatrix} \cdot \begin{pmatrix} 4 & 2 & -9 \\ -4 & 1 & 2 \\ 1 & -3 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & 0 \end{pmatrix}$.

Zur Eindeutigkeit der Elementarteiler:

3.1.5 Satz

Sei $A \in \mathrm{Mat}(m \times n, R)$.

Für $I \subset \{1, \dots, m\}$, $J \subset \{1, \dots, n\}$ sei $A_{I,J}$ die Streichungsmatrix mit den Zeilen in I und Spalten in J.

Die Menge $\{ \det(A_{I,J}) \mid |I| = |J| = i \}$ ist die Menge aller $i \times i$- Minoren von A.

Seien $d_1, \dots, d_r$ die Elementarteiler von A

Dann gilt:

$$d_1 \cdots d_i = gg^T \left(\det(A_{I,J}) \mid (|I| = |J| = i) \right) =: D_i$$

Insbesondere sind die Elementarteiler bis auf Einheiten eindeutig, und

$d_1 = D_1 = gg^T$ (alle Einträge von A).

Beweisidee: (benötigt äußere Algebra, LA2)

Die Einträge der i-ten äußeren Potenz $\Lambda^i A$ sind genau die $i \times i$- Minoren von A (bei geeigneter Basiswahl).

Es gilt $\Lambda^i S \cdot \Lambda^i A = \Lambda^i (S \cdot A)$

Beh: $ggT(\text{Einträge von } \Lambda^i(SA)) = ggT(\text{Einträge } \Lambda^i(A))$ für S invertierbar

Jeder Eintrag von $\Lambda^i(S\cdot A) = \Lambda^i S \cdot \Lambda^i A$ ist eine Linearkombination von Einträgen von $\Lambda^i A \Rightarrow ggT(\Lambda^i A) \mid ggT(\Lambda^i(SA))$

Da S invertierbar ist, gilt $A = S^{-1}(SA)$ und wir können mit demselben Argument folgern, daß

$ggT(\Lambda^i(SA)) \mid ggT(\Lambda^i A)$.

Analog gilt $ggT(\Lambda^i A) = ggT(\Lambda^i(AT))$ für T invertierbar.

Damit folgt für $SAT = D = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_r \end{pmatrix}$

mit $d_i \mid d_{i+1}$ $\quad i = 1, \dots, r-1$

$ggT(\Lambda^i A) = ggT(\Lambda^i(SAT)) =$

$ggT(\Lambda^i D) = ggT(d_{j_1} \cdots d_{j_i} \mid 1 \le j_1 < \cdots < j_i \le r)$

$= d_1 \cdots d_i$, denn $d_j \mid d_k$ für $j \le k$ □

Bsp: $A = \begin{pmatrix} 6 & 9 & 6 \\ 6 & 6 & 7 \end{pmatrix}$

$d_1 = ggT(\text{alle Einträge}) = 1$

2×2-Minoren sind $\det\begin{pmatrix} 6 & 9 \\ 6 & 6 \end{pmatrix} = -18$,

$\det\begin{pmatrix} 6 & 6 \\ 6 & 7 \end{pmatrix} = 6$, $\det\begin{pmatrix} 9 & 6 \\ 6 & 7 \end{pmatrix} = 27$,

$ggT(-18, 6, 27) = d_1 \cdot d_2 = 3$

$\Rightarrow d_2 = 3.$

3.2 Moduln

3.2.1 Def Sei R ein Ring.

Ein **R-Modul** $(M,+,\cdot)$ ist eine Menge M mit zwei Verknüpfungen

$+ : M \times M \longrightarrow M$ und

$\cdot : R \times M \longrightarrow M$ so daß

1) $(M,+)$ ist abelsche Gruppe

2) $r \cdot (m_1 + m_2) = rm_1 + rm_2$ (Distributivität)

$(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$

3) $(r_1 \cdot r_2) \cdot m = r_1 \cdot (r_2 \cdot m)$ (Assoziativität)

4) $1 \cdot m = m$

3.2.2 Bsp

1) Sei $R = K$ ein Körper, dann ist jeder K-Vektorraum ein K-Modul.

2) $\{$ abelsche Gruppen $\} \overset{1:1}{\longleftrightarrow} \{\mathbb{Z}\text{-Moduln}\}$

Sei $(G,+)$ abelsche Gruppe.

Setze $\mathbb{Z} \times G \to G$:

$(n, g) \mapsto \underbrace{g + \dots + g}_{n\text{-Mal}}$ für $n \geq 0$

$(-1) \cdot g \mapsto -g$

Dann gilt die Distributivität:

$n(g_1 + g_2) = g_1 + g_2 + \dots + g_1 + g_2 =$ (↙ abelsch)

$g_1 + \dots + g_1 + g_2 + \dots + g_2 = n g_1 + n g_2$

$(n_1 + n_2) g = \underbrace{g + \dots + g}_{n_1 + n_2} = \underbrace{g + \dots + g}_{n_1} + \underbrace{g + \dots + g}_{n_2} =$

$n_1 g + n_2 g$

Assoziativität:

$(n_1 \cdot n_2) \cdot g = \underbrace{g + \dots + g}_{n_1 \cdot n_2} = \underbrace{(\underbrace{g + \dots + g}_{n_2}) + \dots + (\underbrace{g + \dots + g}_{n_2})}_{n_1}$

$= n_1 \cdot (n_2 \cdot g)$

und $1 \cdot g = g$ $\Rightarrow$ G ist ein $\mathbb{Z}$-Modul

Umgekehrt ist jeder $\mathbb{Z}$-Modul abelsche Gruppe $(G, +)$.

3) Sei R ein Ring,

$I \subset R$ ist Ideal $\Leftrightarrow$ I ist R-Modul

„$\Rightarrow$" $(I, +)$ ist abelsche Gruppe

Distributivität, Assoziativität und $1 \cdot m = m$ gelten, da dies Rechnungen in R sind

"$\Leftarrow$" Die Abgeschlossenheit bezüglich der R-Skalarmultiplikation folgt aus der Def.

Insbesondere ist R selbst ein R-Modul.

4) Sei I ein Ideal, dann ist R/I ein R-Modul.

5) Seien M_1, M_2 R-Moduln, dann ist $M_1 \times M_2$ mit komponentenweise definierter Addition und Skalarmultiplikation ein Modul.
Insbesondere ist $R^n = R \times \cdots \times R$ ein R-Modul.

6) Sei $\varphi : R \longrightarrow S$ ein Ringhomomorphismus, dann ist S mit der Addition und mit der Skalarmultiplikation definiert durch $r \circ s := \varphi(r) \cdot s$ ein R-Modul, denn $(S,+)$ ist abelsche Gruppe,
$r \circ (s_1 + s_2) = \varphi(r) \cdot (s_1 + s_2) = \varphi(r) \cdot s_1 + \varphi(r) \cdot s_2$,
$(r_1 + r_2) \circ s = \varphi(r_1 + r_2) \cdot s = (\varphi(r_1) + \varphi(r_2)) \cdot s$
$= \varphi(r_1) \cdot s + \varphi(r_2) \cdot s$,

$(r_1 \cdot r_2) \circ s = \varphi(r_1 \cdot r_2) \circ s = \varphi(r_1) \circ \varphi(r_2) \circ s =$
$r_1 \circ (r_2 \cdot s)$ und $1 \circ s = \varphi(1) \circ s = 1 \circ s = s$.

Insbesondere sind $\mathbb{Q}$, $\mathbb{R}$ $\mathbb{Z}$-Moduln.

7) Sei $R = K[X]$, V ein K-Vektorraum
$\varphi : V \longrightarrow V$ ein Endomorphismus.

Wir definieren
$X \cdot v := \varphi(v) \in V$ für $v \in V$
und erhalten einen $K[X]$-Modul V:
$(V, +)$ ist abelsche Gruppe,

$f(X) \circ (v_1 + v_2) = (a_n X^n + \dots + a_0) \cdot (v_1 + v_2)$
$= (a_n X \cdots X + \cdots + a_0)(v_1 + v_2) =$
$a_n \cdot (X \cdots X) \cdot (v_1 + v_2) + \cdots + a_0 (v_1 + v_2) =$
$a_n \varphi^n (v_1 + v_2) + \cdots + a_0 (v_1 + v_2) =$
$a_n (\varphi^n(v_1) + \varphi^n(v_2)) + \cdots + a_0 (v_1 + v_2) =$
$a_n \varphi^n(v_1) + a_n \varphi^n(v_2) + \cdots + a_0 v_1 + a_0 v_2 =$
$a_n \varphi^n(v_1) + \cdots + a_0 v_1 + a_n \varphi^n(v_2) + \cdots + a_0 v_2 =$
$f(X) \cdot v_1 + f(X) \circ v_2$

$(f(x)+g(x))\cdot v = f(x)\cdot v + g(x)\cdot v$

und $(f(x)\cdot g(x))\cdot v = f(x)\cdot(g(x)\cdot v)$

analog, $1\cdot v = v$.

Umgekehrt, gegeben ein $K[x]$-Modul V, so erhalten wir durch die Einschränkung der Skalarmultiplikation auf K einen K-Vektorraum V, und durch

$\varphi: V \longrightarrow V;\ v \longmapsto x\cdot v$

einen Endomorphismus, denn

$\varphi(v+w) = x\cdot(v+w) = x\cdot v + x\cdot w = \varphi(v) + \varphi(w)$ und $\varphi(\lambda\cdot v) = x\cdot\lambda\cdot v = \lambda\cdot x\cdot v = \lambda\cdot\varphi(v)$.

$$\left\{\begin{array}{l}\text{Tupel } (V,\varphi)\\ \text{mit } V \text{ } K\text{-Vektorraum},\\ \varphi: V\longrightarrow V\\ \text{Endomorphismus}\end{array}\right\} \overset{1:1}{\longleftrightarrow} \left\{\begin{array}{c}K[x]\text{-}\\ \text{Moduln}\\ V\end{array}\right\}$$

3.2.3 Lemma

Sei M ein R-Modul, $m \in M$.

Es gilt $0_R\cdot m = 0_M$ und

$-m = (-1_R)\cdot m$.

Beweis: $0 \cdot m = (0+0) \cdot m = 0 \cdot m + 0 \cdot m \Rightarrow$
$0 \cdot m = 0$. $0 = 0 \cdot m = (1-1) \cdot m = 1 \cdot m + (-1) \cdot m =$
$m + (-1) \cdot m \Rightarrow -m = -1 \cdot m$. □

3.2.4 Def Ein Untermodul $U \subset M$ ist eine Teilmenge, die selbst wieder ein Modul ist.

3.2.5 Lemma (Untermodulkriterium)

Sei $U \subset M$ eine Teilmenge.

U ist Untermodul $\Leftrightarrow$

$U \neq \emptyset$, $m_1 + m_2 \in U \; \forall \; m_1, m_2 \in U$

und $r \cdot m \in U \; \forall \; r \in R, \; m \in U$.

Beweis: „$\Rightarrow$" Da $+ : U \times U \to U$,

$\cdot : R \times U \to U$.

„$\Leftarrow$" Aus dem Untergruppenkriterium folgt, dass $(U, +)$ eine Untergruppe bezüglich $+$ ist, denn $m_1 + m_2 \in U$ und $-m = (-1) \cdot m \in U$.

Distributivität, Assoziativität und $1 \cdot m = m$ $\forall m \in U$ gelten, da sie in M gelten. □

3.2.6 Lemma

Sei $U \subset M$ Untermodul, dann ist M/U mit $r \cdot [m] = [r \cdot m]$ ein R-Modul.

Beweis: $(M/U, +)$ ist abelsche Gruppe.

Die Skalarmultiplikation ist wohldefiniert, denn falls $[m_1] = [m_2] \Rightarrow m_1 - m_2 \in U$

$\Rightarrow r \cdot (m_1 - m_2) \in U \Rightarrow rm_1 - rm_2 \in U$

$\Rightarrow [rm_1] = [rm_2]$.

Die Rechenregeln werden vererbt. □

3.2.7 Def

Ein R-Modul-Homomorphismus $f: M \to N$ ist ein R-linearer Gruppenhomomorphismus, i.e.

$f(m_1 + m_2) = f(m_1) + f(m_2) \quad \forall m_1, m_2 \in M$

$f(r \cdot m) = r \cdot f(m) \quad \forall r \in R, m \in M.$

3.2.8 Satz (Homomorphiesatz)

Sei $f: M \to N$ ein R-Modulhomomorphismus. $\ker(f)$, $\mathrm{Im}(f)$ sind Untermoduln von M bzw. N und es gilt

$$\tilde{f}: M/\ker(f) \xrightarrow{\cong} \mathrm{Im}(f)$$

$$[m] \longmapsto f(m)$$

Beweis: Folgt aus dem Homomorphiesatz für Gruppen, nur die Verträglichkeit mit der Skalarmultiplikation ist zu prüfen:

$$\tilde{f}(r \cdot [m]) = \tilde{f}([r \cdot m]) = f(r \cdot m) = r \cdot f(m) = r \cdot \tilde{f}([m]).$$ □

3.2.9 Def

M heißt endlich erzeugt $\Leftrightarrow$

$\exists$ $f: R^n \twoheadrightarrow M$

(surjektiver Modulhomomorphismus).

3.2.10 Bemerkung

Seien $e_1, \dots, e_n$ die Standard-Einheits-Vektoren von R^n, setze $m_i := f(e_i)$.

f surjektiv $\Leftrightarrow$ jedes Element von M läßt sich in der Form

$$f(r) = f(r_1 e_1 + \dots + r_n e_n) = r_1 f(e_1) + \dots + r_n f(e_n) = r_1 m_1 + \dots + r_n m_n$$

schreiben, also als R-Linearkombination der m_i. $\Leftrightarrow$ die m_i erzeugen M als R-Modul, $M = \langle m_1, \dots, m_n \rangle_R$

Die m_i müssen keine Basis bilden, die Darstellung als R-Linearkombination der m_i muß nicht eindeutig sein:

Bsp $\mathbb{Z}_3$ ist ein $\mathbb{Z}$-Modul, und endlich erzeugt, denn $\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} = \mathbb{Z}_3$ ist ein surjektiver $\mathbb{Z}$-Modulhomomorphismus. Aber $[0] = 3 \cdot [1] = 0 \cdot [1]$ hat keine eindeutige Darstellung als $\mathbb{Z}$-Linearkombination des Erzeugers $[1]$.

3.2.11 Def Ein endlich erzeugter R-Modul M heißt frei $\iff$
$\exists$ Isomorphismus $M \cong R^n$
Insbesondere bilden die Bilder m_i der e_i dann eine Basis von M, i.e. jedes Element von M läßt sich eindeutig als R-Linearkombination der m_i darstellen.

Bsp
1) $\mathbb{Q}$ als $\mathbb{Z}$-Modul ist nicht endlich erzeugt: Angenommen, $\mathbb{Q}$ wäre von $r_1, \dots, r_n$ erzeugt. Wähle d teilerfremd zu den Nennern der r_i. Sei

$a \in \langle r_1, \dots, r_n \rangle_{\mathbb{Z}} \Rightarrow a = a_1 r_1 + \dots + a_n r_n$
mit $a_i \in \mathbb{Z}$. Sei $r_i = \frac{p_i}{q_i} \Rightarrow$

$$a = a_1 \frac{p_1}{q_1} + \dots + a_n \frac{p_n}{q_n} = \frac{\dots}{kgV(q_1, \dots, q_n)} \neq \frac{1}{d}$$

$$\Rightarrow \frac{1}{d} \notin \langle r_1, \dots, r_n \rangle_{\mathbb{Z}}.$$

2) Ein K- Vektorraum ist ein freier K- Modul.

3) Sei $R = K[x_i \mid i \in \mathbb{N}]$ der Polynomring in abzählbar vielen Variablen.
R als R- Modul ist endlich erzugt, sogar frei mit Basis 1.
Betrachte $U = \{ f \in R \mid f(0) = 0 \}$ die Polynome ohne konstanten Koeffizienten.
Da $0 \in U$ ist $U \neq \emptyset$.
Sind $f, g \in U \Rightarrow f+g\,(0) =$
$f(0) + g(0) = 0+0 = 0 \Rightarrow f+g \in U$.
Ist $f \in U$ und $r \in R \Rightarrow r \cdot f(0) =$
$r \cdot 0 = 0 \Rightarrow r \cdot f \in U$
Nach dem Untermodulkriterium 3.2.5

ist U ein Untermodul.

Beh.: U ist nicht endlich erzeugt

($U = \langle x_i \mid i \in \mathbb{N} \rangle_R$)

Angenommen, $U = \langle f_1, \dots, f_k \rangle_R$.

In jedem f_i gibt es nur endlich viele Variablen, seien $x_1, \dots, x_n$ die Variablen, die in allen f_i vorkommen.

Betrachte eine R-Linearkombination $r_1 f_1 + \dots + r_k f_k$ mit $r_i \in R$.

Die f_i haben keinen konstanten Anteil, i.e. jeder Term eines f_i enthält ein x_j, $j = 1, \dots, n$. Damit enthält auch jeder Term von $r_1 f_1 + \dots + r_k f_k$ ein x_j, $j = 1, \dots, n$.

Aber $x_{n+1} \in U$ und x_{n+1} läßt sich nicht als Summe von Termen darstellen, von denen jeder ein x_j, $j = 1, \dots, n$ enthält.

$\Rightarrow U \neq \langle f_1, \dots, f_k \rangle_R$.

U ist nicht endlich erzeugt.

Insbesondere können Untermoduln von endlich erzeugten Moduln selbst nicht endlich erzeugt sein.

3.2.12 Def (Exakte Sequenzen)

Eine Sequenz von R-Moduln und R-Modul-Homomorphismen

$$\dots \longrightarrow M_{i-1} \xrightarrow{\varphi_{i-1}} M_i \xrightarrow{\varphi_i} M_{i+1} \longrightarrow \dots$$

heißt exakt bei M_i $:\Leftrightarrow$

$$\ker(\varphi_i) = \operatorname{Im}(\varphi_{i-1})$$

Eine Sequenz heißt exakt, wenn sie exakt bei jedem inneren Eintrag ist.

Bsp

1) $N \xrightarrow{\varphi} M \longrightarrow 0$ ist exakt $\Leftrightarrow$

$\ker$(Nullabbildung) $= M = \operatorname{Im}\varphi$ $\Leftrightarrow$

φ surjektiv

2) $0 \longrightarrow N \xrightarrow{\varphi} M$ ist exakt $\Leftrightarrow$

Bild(Inklusion der 0) $= \{0\} = \ker(\varphi)$ $\Leftrightarrow$

φ injektiv.

3.3 Endlich präsentierte Moduln

3.3.1 Def M heißt *endlich präsentiert* wenn M durch $\varphi: R^m \to M$ endlich erzeugt wird und $\ker(\varphi)$ selbst wieder endlich erzeugt wird.

3.3.2 Lemma

M endlich präsentiert $\iff$
$\exists$ exakte Sequenz $R^n \xrightarrow{f} R^m \to M \to 0$

Beweis:

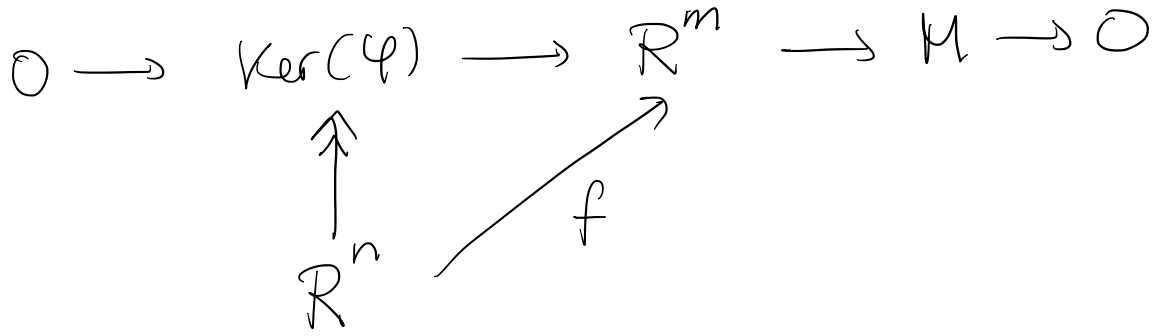
"$\Rightarrow$" M ist endlich erzeugt durch $\varphi: R^m \to M$, φ ist surjektiv $\Rightarrow$

$R^m \xrightarrow{\varphi} M \to 0$ ist exakt

$\Rightarrow 0 \to \ker(\varphi) \to R^m \to M \to 0$ ist exakt.

Da $\ker(\varphi)$ endlich erzeugt, $\exists$

$R^n \twoheadrightarrow \ker(\varphi)$



Damit existiert

$$R^n \xrightarrow{f} R^m \longrightarrow M \longrightarrow 0$$

und ist exakt.

„⇐" Sei $R^n \xrightarrow{f} R^m \xrightarrow{\varphi} M \longrightarrow 0$ exakt $\Rightarrow$ φ ist surjektiv $\Rightarrow$ M ist endlich erzeugt.

Außerdem gilt $\ker(\varphi) = \operatorname{Im}(f)$

$\Rightarrow$ $R^n \xrightarrow{f} \operatorname{Im}(f)$ zeigt, daß $\ker(\varphi)$ selbst endlich erzeugt ist

$\Rightarrow$ M ist endlich präsentiert. □

3.3.3 Def Die Abb $R^n \xrightarrow{f} R^m$ ist ein Morphismus freier Moduln und daher durch die Bilder $f(e_1), \dots, f(e_n)$ festgelegt. Diese Bilder schreiben wir in der Basis

$e_1, \dots, e_m$ und erhalten so eine eine $m \times n$ Matrix $A \in Mat(m \times n, R)$, die Präsentationsmatrix von M.

Es gilt $M = Im\varphi \cong R^m / ker(\varphi) = R^m / Im(f) = R^m / Im(A)$,

das heißt, M ist durch A vollständig beschrieben.

$Im(A)$ liefert alle Relationen zwischen den Erzeugen $\varphi(e_i)$ von M, i.e. für alle Gleichungen $r_1 \varphi(e_1) + \dots + r_m \varphi(e_m) = 0$ die die Erzuger $\varphi(e_i)$ erfüllen, gilt $\begin{pmatrix} r_1 \\ \vdots \\ r_m \end{pmatrix} \in Im(A)$.

3.3.4 Satz

M sei ein R-Modul. Äquivalent sind:

1) Jede aufsteigende Kette von Untermoduln wird stationär.
2) Jedes Untermodul von M ist endlich erzugt
3) Jede Teilmenge von Untermoduln enthält ein maximales Element.

Beweis wie bei Ringen.

3.3.5 Def

Ein Modul, der die Eigenschaften aus 3.3.4 erfüllt, heißt noethersch.

3.3.6 Prop

Sei $0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{\pi} M'' \longrightarrow 0$ eine exakte Sequenz von R-Moduln.

M noethersch $\Leftrightarrow$ M', M'' noethersch.

Beweis:

Beh: $N_1, N_2 \subset M$ Untermoduln mit $N_1 \subset N_2$, $\pi(N_1) = \pi(N_2)$, $i(M') \cap N_1 = i(M') \cap N_2 \Rightarrow N_1 = N_2$

Sei $x \in N_2 \Rightarrow \pi(x) \in \pi(N_2) = \pi(N_1)$

$\Rightarrow \exists\, x' \in N_1 : \pi(x) = \pi(x') \Rightarrow$

$\pi(x - x') = 0 \Rightarrow x - x' \in \ker(\pi) = \operatorname{Im}(i) = i(M')$.

Da $x' \in N_1 \subset N_2$, $x \in N_2$

$\Rightarrow x - x' \in N_2 \Rightarrow x - x' \in N_2 \cap i(M') = N_1 \cap i(M') \Rightarrow x - x' \in N_1$, da $x' \in N_1 \Rightarrow x \in N_1$.

"$\Leftarrow$" Seien M', M'' noethersch,

$M_1 \subset M_2 \subset \dots$ eine Kette von Untermoduln in M $\Rightarrow$

$\pi(M_1) \subset \pi(M_2) \subset \dots$ ist eine Kette in M''

$i(M') \cap M_1 \subset i(M') \cap M_2 \subset \dots$ " " M'

Da beide noethersch, stabilisieren beide Ketten

Wähle n groß genug, daß beide stabil sind $\Rightarrow$ $\pi(M_N) = \pi(M_n) \quad \forall N \geq n$

$i(M') \cap M_N = i(M') \cap M_n \quad \forall N \geq n$

Beh $\Rightarrow$ $M_N = M_n \quad \forall N \geq n$

$\Rightarrow$ die Kette wird stationär

$\Rightarrow$ M ist noethersch.

"$\Rightarrow$" Sei M noethersch.

Jede Kette in M' oder M'' induziert eine Kette in M via i bzw. π^{-1}, die stationär wird, die ursprüngliche deshalb auch. □

3.3.7 Lemma

R noethersch $\Rightarrow$ R^n noethersch

Beweis Induktion über n.

$n=1$ klar. Sei R^{n-1} noethersch.

Betrachte

$$R^{n-1} \xrightarrow{i} R^n \xrightarrow{\pi} R$$

$$\begin{pmatrix} x_1 \\ \vdots \\ x_{n-1} \end{pmatrix} \longmapsto \begin{pmatrix} x_1 \\ \vdots \\ x_{n-1} \\ 0 \end{pmatrix} \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \longmapsto v_n$$

i ist injektiv, π ist surjektiv,

$\ker(\pi) = \operatorname{Im}(i)$ $\Rightarrow$

$0 \to R^{n-1} \to R^n \to R \to 0$ ist exakt, da R^{n-1}, R noethersch folgt mit Prop. 3.3.6 R^n noethersch. □

3.3.8 Satz

Endlich erzeugte Moduln über noetherschen Ringen sind schon endlich präsentiert.

Beweis:

M endlich erzeugt $\Rightarrow \exists\ R^m \twoheadrightarrow M$.

Dann ist

$$0 \longrightarrow \ker(\varphi) \longrightarrow R^m \longrightarrow M \longrightarrow 0$$

exakt, R^m ist noethersch wegen 3.3.7
$\overset{3.3.6}{\Longleftarrow}$ $\ker(\varphi)$ noethersch $\overset{3.3.4}{\Longrightarrow}$
$\ker(\varphi)$ endlich erzeugt $\Rightarrow$ M endlich präsentiert. □

3.3.9 Korollar

Endlich erzeugte Moduln über noetherschen Ringen sind noethersch.

Beweis:
Mit derselben exakten Sequenz

$$0 \longrightarrow \ker(\varphi) \longrightarrow R^m \longrightarrow M \longrightarrow 0$$

folgt auch M ist noethersch. □

3.4 Der Elementarteilersatz

3.4.1 Bsp Eine endlich erzeugte abelsche Gruppe (i.e. ein endlich erzeugter $\mathbb{Z}$-Modul, siehe Bsp 3.2.2 2)) lässt sich durch eine Präsentationsmatrix beschreiben (Satz 3.3.8), z.B.:

$$0 \to \mathbb{Z}^3 \xrightarrow{A} \mathbb{Z}^4 \xrightarrow{\varphi} G \to 0$$

$$A = \begin{pmatrix} 1 & 1 & 1 \\ -3 & 1 & 1 \\ 1 & -3 & 1 \\ 1 & 1 & -3 \end{pmatrix} \quad \text{dann ist} \quad G = \mathbb{Z}^4/\ker\varphi = \mathbb{Z}^4/\mathrm{im}A$$

Bestimme die Smith-Normalform von A, und die Basiswechsel:

$$\left(\begin{array}{cccc|ccc} 1&0&0&0 & 1&1&1 \\ 0&1&0&0 & -3&1&1 \\ 0&0&1&0 & 1&-3&1 \\ 0&0&0&1 & 1&1&-3 \\ & & & & 1&0&0 \\ & & & & 0&1&0 \\ & & & & 0&0&1 \end{array}\right) \quad \begin{matrix} II \mapsto II+3I \\ III \mapsto III - I \\ \longrightarrow \\ IV \mapsto IV - I \\ \text{Zeilen} \end{matrix}$$

$$\left(\begin{array}{cccc|ccc} 1&0&0&0 & 1&1&1 \\ 3&1&0&0 & 0&4&4 \\ -1&0&1&0 & 0&-4&0 \\ -1&0&0&1 & 0&0&-4 \\ & & & & 1&0&0 \\ & & & & 0&1&0 \\ & & & & 0&0&1 \end{array}\right) \quad \begin{matrix} \text{Spalten} \\ II \mapsto \\ II - I \\ \longrightarrow \\ III \mapsto \\ III - I \end{matrix}$$

$$\left(\begin{array}{cccc|ccc} 1&0&0&0 & 1&0&0 \\ 3&1&0&0 & 0&4&4 \\ -1&0&1&0 & 0&-4&0 \\ -1&0&0&1 & 0&0&-4 \\ & & & & 1&-1&-1 \\ & & & & 0&1&0 \\ & & & & 0&0&1 \end{array}\right)$$

Weiter mit $A^1 = \begin{pmatrix} 4 & 4 \\ -4 & 0 \\ 0 & -4 \end{pmatrix}$

$$\left(\begin{array}{cccc|ccc} 1&0&0&0&1&0&0 \\ 3&1&0&0&0&4&4 \\ -1&0&1&0&0&-4&0 \\ -1&0&0&1&0&0&-4 \\ & & & &1&-1&-1 \\ & & & &0&1&0 \\ & & & &0&0&1 \end{array}\right) \xrightarrow{\text{Zeile III} \mapsto \text{III} + \text{II}} \left(\begin{array}{cccc|ccc} 1&0&0&0&1&0&0 \\ 3&1&0&0&0&4&4 \\ 2&1&1&0&0&0&4 \\ -1&0&0&1&0&0&-4 \\ & & & &1&-1&-1 \\ & & & &0&1&0 \\ & & & &0&0&1 \end{array}\right)$$

Spalte $\text{III} \mapsto \text{III} - \text{II}$

$$\left(\begin{array}{cccc|ccc} 1&0&0&0&1&0&0 \\ 3&1&0&0&0&4&0 \\ 2&1&1&0&0&0&4 \\ -1&0&0&1&0&0&-4 \\ & & & &1&-1&0 \\ & & & &0&1&-1 \\ & & & &0&0&1 \end{array}\right)$$

Weiter mit $A^1 = \begin{pmatrix} 4 \\ -4 \end{pmatrix}$

Zeile $\text{IV} \mapsto \text{IV} + \text{III}$

$$\left(\begin{array}{cccc|ccc} 1&0&0&0&1&0&0 \\ 3&1&0&0&0&4&0 \\ 2&1&1&0&0&0&4 \\ 1&1&1&1&0&0&0 \\ & & & &1&-1&0 \\ & & & &0&1&-1 \\ & & & &0&0&1 \end{array}\right)$$

$$\Rightarrow \underbrace{\begin{pmatrix} 1&0&0&0 \\ 3&1&0&0 \\ 2&1&1&0 \\ 1&1&1&1 \end{pmatrix}}_{S} \cdot \underbrace{\begin{pmatrix} 1&1&1 \\ -3&1&1 \\ 1&-3&1 \\ 1&1&-3 \end{pmatrix}}_{A} \cdot \underbrace{\begin{pmatrix} 1&-1&0 \\ 0&1&-1 \\ 0&0&1 \end{pmatrix}}_{T} = \underbrace{\begin{pmatrix} 1&0&0 \\ 0&4&0 \\ 0&0&4 \\ 0&0&0 \end{pmatrix}}_{D}$$

Die Elementarteiler sind 1, 4, 4.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}^3 & \xrightarrow{A} & \mathbb{Z}^4 & \longrightarrow & G & \longrightarrow & 0 \\ & & \cong\uparrow T & & \cong\downarrow S & & \cong & & \\ 0 & \longrightarrow & \mathbb{Z}^3 & \xrightarrow{D} & \mathbb{Z}^4 & \longrightarrow & G' & \longrightarrow & 0 \end{array}$$

$$G' \cong \mathbb{Z}^4/\mathrm{Im}D = \mathbb{Z}^4/\left\langle \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \\ 0 & 0 & 0 \end{pmatrix} \right\rangle_{\mathbb{Z}} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}$$

das heißt, die Erzeuger $e_1, \dots, e_4$ von G' gegeben durch die kanonische Basis von $\mathbb{Z}^4$ erfüllen $e_1 = 0$, $4 \cdot e_2 = 0$, $4 \cdot e_3 = 0$.

$$G \cong \mathbb{Z}^4/\mathrm{Im}(A) = \mathbb{Z}^4/\mathrm{Im}(AT) = \mathbb{Z}^4/\mathrm{Im}(S^{-1}D) \cong \mathbb{Z}^4/\mathrm{Im}(D) \cong G'$$

Verwende die Spalten von S^{-1} als Basis,

$$S^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -3 & 1 & 0 & 0 \\ 1 & -1 & 1 & 0 \\ 1 & 0 & -1 & 1 \end{pmatrix},$$

setze $v_1 = \begin{pmatrix} 1 \\ -3 \\ 1 \\ 1 \end{pmatrix}$, $v_2 = \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix}$, $v_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ -1 \end{pmatrix}$, $v_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

Dann gilt $v_1, 4 \cdot v_2, 4 \cdot v_3 \in \mathrm{Im}(A)$,

denn $e_1, 4e_2, 4e_3 \in \mathrm{Im}(D) \Rightarrow \exists\, w_1, w_2, w_3 \in \mathbb{Z}^3$:

$D \cdot w_1 = e_1$, $D \cdot w_2 = 4e_2$, $D \cdot w_3 = 4e_3$

$\Rightarrow$ $SATw_1 = e_1$, $SATw_2 = 4e_2$, $SATw_3 = 4e_3$

$\Rightarrow$ $A(Tw_1) = S^{-1}e_1 = v_1$, $A(Tw_2) = 4v_2$, $A(Tw_3) = 4v_3$.

3.4.2 Bemerkung

Allgemein: Sei R euklidischer Ring (bzw allgemeiner: Hauptidealring), M endlich erzeugter R-Modul. Wegen Satz 3.3.8 ist M dann schon endlich präsentiert

$$R^n \xrightarrow{A} R^m \xrightarrow{\pi} M \to 0, \quad A \in Mat(m \times n, R)$$

Der Satz über die Smith-Normalform 3.1.3 liefert $S \in GL(m,R)$, $T \in GL(n,R)$ mit

$$\begin{array}{ccccccc} R^n & \xrightarrow{A} & R^m & \xrightarrow{\pi} & M & \longrightarrow & 0 \\ T \uparrow \cong & & \cong \downarrow S & & \cong & & \\ R^n & \xrightarrow{D} & R^m & \longrightarrow & M' & \longrightarrow & 0 \end{array}$$

mit $D = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_r \end{pmatrix}$

Dann sind die $v_i = \pi(S^{-1} \cdot e_i)$ Erzeuger von M mit Relationen $d_1 v_1 = 0, \ldots, d_r v_r = 0$.

Ist d_i eine Einheit, so folgt aus

$d_i v_i = 0$ schon $v_i = 0$ und wir können den Erzeuger v_i streichen.

3.4.3 Def (R nullteilerfrei Ring)

1) Sei M ein Modul, $U_i \subset M$ Untermoduln, wir schreiben $M = U_1 \oplus \dots \oplus U_m$ falls sich jedes Element in M als Summe von Elementen in den U_i schreiben läßt und falls aus $u_1 + \dots + u_m = 0$ mit $u_i \in U_i$ folgt $u_i = 0 \ \forall i$.

2) M heißt <u>zyklisch</u>, wenn es von einem Element erzeugt wird.

3) $T = \{ m \in M \mid \exists\, 0 \neq r \in R \text{ mit } r \cdot m = 0 \} \subset M$ heißt <u>Torsionsuntermodul</u>.

3.4.4 Satz (Elementarteilersatz)

Sei R ein euklidischer Ring (bzw. allgemeiner: Hauptidealring), sei M ein endlich erzeugter Modul.

1) $\exists\ v_1, \dots, v_m$ Erzeuger von M und $d_1, \dots, d_r \in R$ (die (nicht Einheiten) Elementarteiler), $r \leq m$, $d_i \in R^*$, $d_i \mid d_{i+1}$ $i = 1, \dots, r-1$, so daß M durch die Relationen

$d_i \cdot v_i = 0$ beschrieben wird.

2) $M = U_1 \oplus \dots \oplus U_m$ ist direkte Summe zyklischer Untermoduln U_i und

$$U_i \cong \begin{cases} R/d_i R & i \le r \\ R & i > r \end{cases}$$

Anders gesagt:

$$M \cong R/\langle d_1 \rangle \times \dots \times R/\langle d_r \rangle \times R^{m-r}$$

Der Rang $m-r$ und die Elementarteiler sind durch M eindeutig bestimmt.

Beweis:

Konstruktiv, wie in Bemerkung 3.4.2 mit dem Smith-Normalform Algorithmus (Satz 3.1.3):

$$M = R^m/\mathrm{Im}(A) \cong M' = R^m/\mathrm{Im}(D)$$

$$= \frac{R^m}{\langle d_1 e_1, \dots, d_r e_r \rangle}$$

↳ wobei Einheiten schon weggelassen werden

Für die Basiswechsel S, T mit $SAT = D$ gilt $v_i = \pi(S^{-1} e_i)$ sind Erzeuger von M, die $d_i \cdot v_i = 0$ erfüllen, also

$$M = \frac{R^m}{\langle d_1 v_1, \dots, d_r v_r \rangle} = \frac{\langle v_1 \rangle \oplus \dots \oplus \langle v_m \rangle}{\langle d_1 v_1, \dots, d_r v_r \rangle}$$

$$= \frac{\langle v_1 \rangle}{\langle d_1 v_1 \rangle} \oplus \cdots \oplus \frac{\langle v_r \rangle}{\langle d_r v_r \rangle} \oplus \langle v_{r+1} \rangle \oplus \cdots \oplus \langle v_m \rangle$$

$$\cong \frac{R}{d_1 R} \times \cdots \times \frac{R}{d_r R} \times R^{m-r}$$ □

3.4.5 Korollar

Sei R euklidischer Ring (Hauptidealring), M endlich erzeugter Modul.
Sei T der Torsionsmodul von M, dann $\exists$ freier Untermodul $F \subset M$ mit $M = T \oplus F$.

Beweis: Mit dem Elementarteilersatz 3.4.4 gilt $T = U_1 \oplus \cdots \oplus U_r \cong \frac{R}{d_1 R} \times \cdots \times \frac{R}{d_r R}$
und $F = U_{r+1} \oplus \cdots \oplus U_m \cong R^{m-r}$ □

Bsp (Siehe Bsp. 3.4.1)

$$A = \begin{pmatrix} 1 & 1 & 1 \\ -3 & 1 & 1 \\ 1 & -3 & 1 \\ 1 & 1 & -3 \end{pmatrix}, \qquad G_1 = \frac{\mathbb{Z}^4}{\mathrm{Im}(A)},$$

G_1 wird erzeugt von $v_2 = \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix}$, $v_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ -1 \end{pmatrix}$,

$v_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$ mit $4 \cdot v_2 = 0$, $4 \cdot v_3 = 0$

$\Rightarrow G_1 = \langle v_2 \rangle \oplus \langle v_3 \rangle \oplus \langle v_4 \rangle$

Der Torsionsmodul T ist $T = \langle v_2, v_3 \rangle$,

$T \cong \mathbb{Z}_4 \times \mathbb{Z}_4$, $\langle v_4 \rangle$ ist frei.
Statt v_4 kann man als freie Erzeuger auch e_2 oder e_3 wählen z.B.
T ist eindeutig.

3.4.6 Def

M heißt torsionsfrei, wenn $T = \{0\}$
und Torsionsmodul, wenn $M = T$.

3.4.7 Korollar

Sei R euklidischer Ring (Hauptidealring),
M endlich erzeugter Modul.

M frei $\Leftrightarrow$ M torsionsfrei

3.4.8 Korollar

Sei R euklidischer Ring (Hauptidealring).
Jeder Untermodul eines freien
R-Moduls ist wieder frei.

Beweis: M frei $\Rightarrow$ M torsionsfrei
$\Rightarrow U \subset M$ enthält auch keine
Torsionselemente $\Rightarrow$ U frei. □

Wir können die Zerlegung
$M \cong R/\langle d_1 \rangle \times \cdots \times R/\langle d_r \rangle \times R^{m-r}$ aus dem

Elementarteilersatz 3.4.4 noch weiter verfeinern mit dem chinesischen Restsatz:

Ist $d \in R$ und $d = p_1^{r_1} \cdots p_e^{r_e}$ eine Primfaktorzerlegung mit $r_i > 0$, dann folgt mit dem chinesischen Restsatz

$$R/\langle d \rangle \cong R/\langle p_1^{r_1} \rangle \times \cdots \times R/\langle p_e^{r_e} \rangle$$

da die Ideale $\langle p_i^{r_i} \rangle$ coprim sind.

Daher folgt folgender Satz direkt aus dem Elementarteilersatz und dem chinesischen Restsatz:

3.4.9 Satz

Sei R euklidisch (bzw. allgemeiner: Hauptidealring), sei M ein endlich erzeugter R-Modul. Dann $\exists\, t \in \mathbb{N}_{\geq 0}$ und Primelemente $p_1, \ldots, p_k \in R$, $r_1, \ldots, r_k \in \mathbb{N}_{>0}$ mit

$$M \cong R/\langle p_1^{r_1} \rangle \times \cdots \times R/\langle p_k^{r_k} \rangle \times R^t$$

und diese Darstellung ist eindeutig bis auf Reihenfolge der Faktoren.

Da $\mathbb{Z}$-Moduln abelsche Gruppen sind (Bsp 3.2.2 2)) folgt insbesondere:

Satz 3.4.10 (Klassifikation der endlich erzeugten abelschen Gruppen)

Sei G eine endlich erzeugte abelsche Gruppe.

1) G ist direkte Summe von zyklischen Untergruppen.

2) $\exists\ 0 \leq r \leq m,\ d_1, \dots, d_r \geq 2,$
$d_i \mid d_{i+1}\ \forall\ i = 1, \dots, r-1$ mit
$$G \cong \mathbb{Z}_{d_1} \times \dots \times \mathbb{Z}_{d_r} \times \mathbb{Z}^{m-r}$$

3) $\exists$ Primzahlen $p_1, \dots, p_k$ und $r_1, \dots, r_k > 0$ mit
$$G \cong \mathbb{Z}_{p_1^{r_1}} \times \dots \times \mathbb{Z}_{p_k^{r_k}} \times \mathbb{Z}^{m-r}$$

Dabei sind r, m, d_i, p_i, r_i bis auf Reihenfolge (und Einheiten) eindeutig bestimmt.

Bsp Sei G gegeben durch die Präsentationsmatrix $\begin{pmatrix} 2 & 3 & 4 & 18 \end{pmatrix} \in \mathrm{Mat}(4, \mathbb{Z})$.

$\mathrm{ggT}(\text{Einträge}) = 1 \Rightarrow d_1 = 1$

$\mathrm{ggT}(2\times 2\text{-Minoren}) = \mathrm{ggT}(6, 8, 36, 12, 54, 72)$
$= 2 \Rightarrow d_2 = 2$

$\mathrm{ggT}(3\times 3\text{-Minoren}) = \mathrm{ggT}(24, 108, 144, 216)$
$= 12 \Rightarrow d_3 = 6$

$\det = 2 \cdot 3 \cdot 4 \cdot 18 \Rightarrow d_4 = 2 \cdot 18 = 36$

$\Rightarrow D = \begin{pmatrix} 1 & & & \\ & 2 & & \\ & & 6 & \\ & & & 36 \end{pmatrix}$

$\Rightarrow G \cong \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{36}$

$6 = 2 \cdot 3, \quad 36 = 2^2 \cdot 3^2$

$\Rightarrow G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_9$

3.5 Die Jordannormalform

Bsp 3.2.27):

$$\left\{\begin{array}{l}\text{Tupel } (V,\varphi)\\ \text{mit } V \text{ } K\text{-Vektorraum},\\ \varphi: V \longrightarrow V\\ \text{Endomorphismus}\end{array}\right\} \overset{1:1}{\longleftrightarrow} \left\{\begin{array}{c}K[x]\text{-}\\ \text{Moduln}\\ V\end{array}\right\}$$

wobei die Modulstruktur durch

$x \cdot v = \varphi(v)$ gegeben ist.

Sei $V = K^n$ und φ durch die Matrix A gegeben.

Für $f \in K[x]$ gilt dann

$f \cdot v = f(A) \cdot v$.

3.5.1 Lemma:

Sei K^n mittels $A \in Mat(n, K)$ ein $K[x]$-Modul. Ein Unterraum $U \subset K^n$ ist $K[x]$-Untermodul $\Leftrightarrow A \cdot U \subset U$.

Beweis: „$\Leftarrow$" Summen sind in U, da es ein Unterraum ist.

$K[x]$-Vielfache $f \cdot v = f(A) \cdot v$ sind in U, da $A \cdot U \subset U$.

"$\Rightarrow$" $x \cdot u \in U \quad \forall u \in U \Rightarrow A \cdot u \in U$

$\forall u \in U \Rightarrow A \cdot U \subset U$. $\square$

3.5.2 Lemma

Sei K^n ein $K[x]$-Modul mittels A.

Dann ist

$$K[x]^n \xrightarrow{x \cdot \mathbb{1}_n - A} K[x]^n \longrightarrow K^n \longrightarrow 0$$

eine endliche Präsentation von K^n.

Beweis:

$e_1, \dots, e_n \in K^n$ erzeugen K^n als $K[x]$-Modul, denn $\forall\, v \in K^n \ \exists$ $\lambda_i \in K \subset K[x]$: $v = \lambda_1 e_1 + \dots + \lambda_n e_n$

$$K[x]^n \xrightarrow{\pi} K^n : \begin{pmatrix} f_1(x) \\ \vdots \\ f_n(x) \end{pmatrix} \longmapsto f_1(x) \cdot e_1 + \dots + f_n(x) \cdot e_n = f_1(A) \cdot e_1 + \dots + f_n(A) \cdot e_n$$

Beh $\ker(\pi)$ wird von $x \cdot e_j - A \cdot e_j$ erzeugt.

Dies folgt, da wir jeden Vektor $\begin{pmatrix} f_1(x) \\ \vdots \\ f_n(x) \end{pmatrix}$ durch ersetzen von $x \cdot e_j = A \cdot e_j$ in einen Vektor $\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} \in K^n$ überführen können.

Damit $\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = 0 \iff \begin{pmatrix} f_1(x) \\ \vdots \\ f_n(x) \end{pmatrix} \in \ker(\pi) \iff$

$$\begin{pmatrix} f_1(x) \\ \vdots \\ f_n(x) \end{pmatrix} = \sum \lambda_j (x \cdot e_j - A \cdot e_j).$$

Damit gilt $\operatorname{Im}(x \mathbb{1}_n - A) = \ker(\Pi)$, ist also exakt und die Sequenz liefert eine endliche Präsentation. □

Bsp: Sei $n = 3$ $A = (a_{ij})$.

Betrachte den Vektor $\begin{pmatrix} x^2 \\ 2x+1 \\ 2 \end{pmatrix} \in K[x]^3$.

Wir wollen ihn durch Ersetzungen $x e_j = A e_j$ in einen Vektor in K^3 überführen. Dazu:

$$x^2 \cdot e_1 + (2x+1) \cdot e_2 + 2 \cdot e_3 =$$

$$x \cdot (x \cdot e_1) + 2 \cdot (x \cdot e_2) + e_2 + 2 \cdot e_3 =$$

$$x \cdot (a_{11} e_1 + a_{21} e_2 + a_{31} e_3) + 2(a_{12} e_1 + a_{22} e_2 + a_{32} e_3)$$

$$+ e_2 + 2e_3 = a_{11} \cdot (x e_1) + a_{21} (x e_2) +$$

$$a_{31} (x e_3) + 2a_{12} e_1 + (2a_{22}+1) e_2 + (2a_{32}+2) e_3$$

$$= a_{11} (a_{11} e_1 + a_{21} e_2 + a_{31} e_3) + a_{21} (a_{12} e_1 + a_{22} e_2 + a_{32} e_3)$$

$$+ a_{31} (a_{13} e_1 + a_{23} e_2 + a_{33} e_3) + 2a_{12} e_1 + (2a_{22}+1) e_2 +$$

$$(2a_{32}+2) e_3 = (a_{11}^2 + a_{21} a_{12} + a_{31} a_{13} + 2a_{12}) e_1$$

$$+ (a_{11} a_{21} + a_{21} a_{22} + a_{31} a_{23} + 2a_{22} + 1) e_2 +$$

$$\left(a_{11}a_{31} + a_{21}a_{32} + a_{31}a_{33} + 2a_{32} + 2\right) e_3 =$$

$$\begin{pmatrix} a_{11}^2 + a_{21}a_{12} + a_{31}a_{13} + 2a_{12} \\ a_{11}a_{21} + a_{21}a_{22} + a_{31}a_{23} + 2a_{22} + 1 \\ a_{11}a_{31} + a_{21}a_{32} + a_{31}a_{33} + 2a_{32} + 2 \end{pmatrix} \in K^3$$

3.5.3 Lemma

Das $K[x]$-Modul K^n (mittels A) ist ein Torsionsmodul.

Beweis: Nach dem Satz von Cayley-Hamilton gilt $\chi_A(A) = 0$ für das charakteristische Polynom $\chi_A = \det(x \cdot \mathbb{1}_n - A)$.

$\Rightarrow \chi_A \cdot v = \chi_A(A) \cdot v = 0 \cdot v = 0$

$\forall v \in V \Rightarrow v$ ist Torsionselement

$\forall v \in V$. □

Bemerkung: Der Kern des Einsetzehomomorphismus

$\varphi_A : K[x] \longrightarrow \mathrm{Mat}(n, K) : f \mapsto f(A)$

ist ein Hauptideal, erzeugt vom Minimalpolynom p_A.

Es gilt auch $p_A \cdot v = 0 \quad \forall v \in V$.

$p_A \mid \chi_A$ folgt aus dem Satz von Cayley-Hamilton.

3.5.4 Lemma

χ_A zerfalle in Linearfaktoren. Dann ist K^n als $K[X]$-Modul mittels A eine direkte Summe

$K^n = U_1 \oplus \cdots \oplus U_k$ zyklischer Untermoduln U_i mit $U_i \cong \frac{K[X]}{\langle (X-\lambda_i)^{r_i} \rangle}$,

wobei $\chi_A = \prod_i (X-\lambda_i)^{r_i}$.

Beweis:

Bestimme die Smith-Normalform von $X \cdot \mathbb{1}_n - A$ (3.1.4), $D = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix}$, wobei $d_i \neq 0$ gelten muß, da K^n Torsionsmodul ist (Elementarteilersatz 3.4.4, 3.4.5).

Wir zerlegen weiter mit dem chinesischen Restsatz (3.4.9) und erhalten

$K^n = U_1 \oplus \cdots \oplus U_k$ mit $U_i \cong \frac{K[X]}{\langle p_i^{r_i} \rangle}$

mit Primelementen $p_i \in K[X]$.

Es gilt $\prod p_i^{r_i} = d_1 \cdots d_r = \det(D)$

$= \det(X \mathbb{1}_n - A) = \chi_A$.

Da χ_A zerfällt, müssen die p_i von der Form $p_i = X - \lambda_i$ sein. □

3.5.5 Satz (Jordannormalform)

Sei $A \in Mat(n, K)$, χ_A zerfalle in Linearfaktoren über K.
Dann $\exists$ Basis B bezüglich der A die Form $\begin{pmatrix} J(\lambda_1, r_1) & & \\ & \ddots & \\ & & J(\lambda_k, r_k) \end{pmatrix}$ hat,

wobei die $J(\lambda_i, r_i)$ Jordankästchen der Größe r_i sind, $J(\lambda_i, r_i) = \begin{pmatrix} \lambda_i & & \\ 1 & \ddots & \\ & 1 & \lambda_i \end{pmatrix}$,

die λ_i nicht notwendig verschieden.
Bis auf Reihenfolge ist die Darstellung eindeutig.

Beweis: Wir betrachten die Zerlegung $K^n = U_1 \oplus \dots \oplus U_k$ aus Lemma 3.5.4.
mit $U_i \overset{\varphi_i}{\cong} K[X] / \langle (X - \lambda_i)^{r_i} \rangle$.

Betrachte $K[x]/\langle (x-d_i)^{r_i} \rangle$ als K-Vektorraum, eine Basis ist $1, x-d_i, (x-d_i)^2, \dots, (x-d_i)^{r_i-1}$.

Die Bilder dieser Basis unter dem Isomorphismus φ_i nennen wir $v_{ij} \in U_i$, $j = 0, \dots, r_i - 1$.

$$(A - \lambda_i \cdot \mathbb{1}_n) \cdot v_{ij} = (x - \lambda_i) \cdot \varphi_i\left((x-d_i)^j\right)$$

φ_i $K[x]$-linear

$$\varphi_i\left((x-d_i)^{j+1}\right) = \begin{cases} v_{i\,j+1} & j = 0, \dots, r_i - 2 \\ 0 & j = r_i - 1 \end{cases}$$

$$\Rightarrow \quad A \cdot v_{ij} = \begin{cases} \lambda_i \cdot v_{ij} + v_{ij+1} & j = 0, \dots, r_i - 2 \\ \lambda_i \cdot v_{ij} & \text{sonst.} \end{cases}$$

Bezüglich der Basis $\{v_{ij}\}$ hat $A|_{U_i}$ also die Form

$$\begin{pmatrix} \lambda_i & & \\ 1 & \ddots & \\ & 1 & \lambda_i \end{pmatrix}$$

und insgesamt hat A die gewünschte Form. $\square$

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 <u>Körpererweiterung</u>, 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 <u>Grad</u> 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 $\varphi: \mathbb{Q}[x] \to \mathbb{R}$:

$x \mapsto \sqrt{2}$

<u>Beh:</u> $\ker(\varphi) = \langle x^2 - 2 \rangle$

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

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

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

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

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

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

$\Rightarrow x^2-2$ 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: $K \subset L \Rightarrow \text{char}(K) = \text{char}(L)$, denn $1_K = 1_L$.

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

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

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

4.1.5 Def

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

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

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 $\mathrm{Quot}(K[\alpha_1, \dots, \alpha_n])$ fortsetzen und erhalten $\mathrm{Quot}(K[\alpha_1, \dots, \alpha_n]) \subset K(\alpha_1, \dots, \alpha_n)$. Andererseits ist $\mathrm{Quot}(K[\alpha_1, \dots, \alpha_n])$ ein Unterkörper, der K und α_i enthält, also gilt auch $K(\alpha_1, \dots, \alpha_n) \subset \mathrm{Quot}(K[\alpha_1, \dots, \alpha_n])$. □

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 $m_\alpha = g_1 \cdot g_2 \Rightarrow 0 = m_\alpha(\alpha) = g_1(\alpha) \cdot g_2(\alpha) \in L \Rightarrow$ o.E. $g_1(\alpha) = 0$

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

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

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

$\Rightarrow g_2$ 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 $\lambda_i \in K$

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

2) $\Rightarrow$ 3) klar

3) $\Rightarrow$ 1) $[L:K] = [K(\alpha_1, \dots, \alpha_n) : K] =$ 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 $/K$. $\square$

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'

$\Rightarrow \in \alpha_1'$ 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 $ggT(j, d) = 1$,

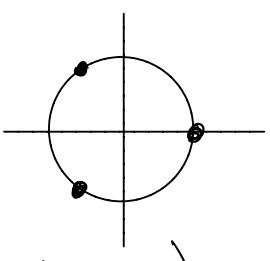
z.B. von α_1.

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 $\deg f = 1$, $f = g \cdot h$
$\Rightarrow$ OE $\deg g = 1$, $\deg h = 0$ $\Rightarrow$
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. $\square$

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

$\mathfrak{m}$ mit $I \subset \mathfrak{m} \subsetneq R$.

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 $x \in J$, $x' \in J'$, OE $J \subset J'$, 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 $1 \in J$ $\lightning$

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

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 Einsetzhomomorphismus

$$\varphi: R \longrightarrow L' : \begin{cases} x_{f_i} \longmapsto \alpha_i \\ x_f \longmapsto 0 \quad f \neq f_i \end{cases}$$

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.

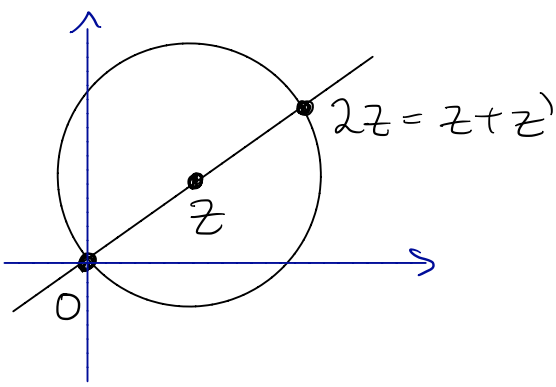
4.3.3 Satz $\tilde{M}$ ist ein Unterkörper von $\mathbb{C}$.

Beweis:

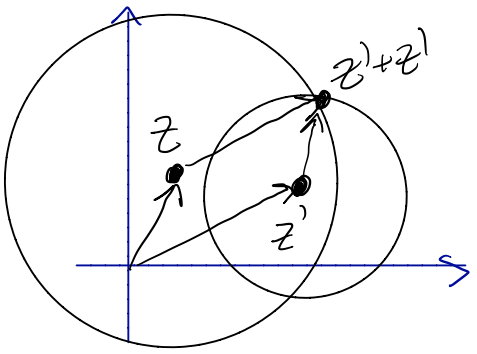
Beh: $(\tilde{M}, +)$ ist eine Untergruppe von $(\mathbb{C}, +)$.

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

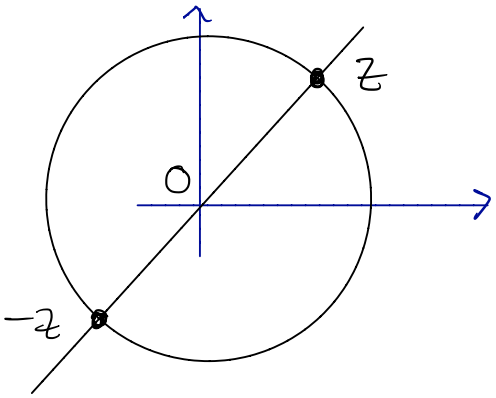
Falls $z = z' \Rightarrow z + z' \in k(z, |z|) \cap g(0, z) \subset \tilde{M}$



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) $z, z' \in \tilde{M} \setminus \{0\} \cap \mathbb{R}_{>0} \Rightarrow z z' \in \tilde{M} \setminus \{0\}$
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) $z \in \tilde{M} \setminus \{0\} \Rightarrow |z|, \bar{z}, \operatorname{Re} z, \operatorname{Im} z \in \tilde{M}$
5) $\lambda \in \mathbb{R}_{>0} \cap \tilde{M} \setminus \{0\}, z \in \tilde{M} \setminus \{0\} \Rightarrow \lambda z \in \tilde{M} \setminus \{0\}$

Dann 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 da $(\tilde{M}, +)$ Untergruppe von $(\mathbb{C}, +)$ ist, und ein Produkt von i mit einer Negative Zahl aus $\tilde{M} \setminus \{0\}$ in $\tilde{M} \setminus \{0\}$ ist wegen 3) folgt $z \cdot z' \in \tilde{M} \setminus \{0\}$.

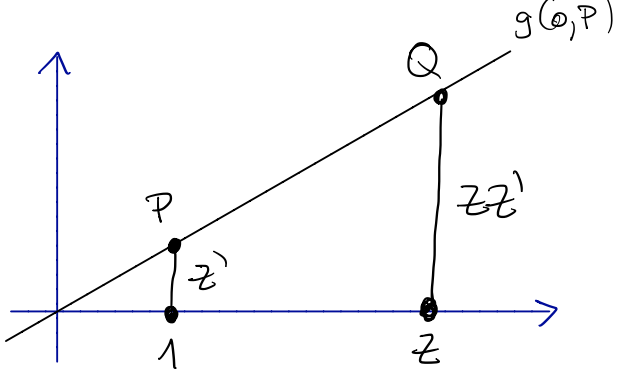
$\frac{1}{z} = \frac{1}{|z|^2} \cdot \bar{z} \in \tilde{M} \setminus \{0\}$, denn

$\frac{1}{|z|} \in \tilde{M} \setminus \{0\}$ 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).

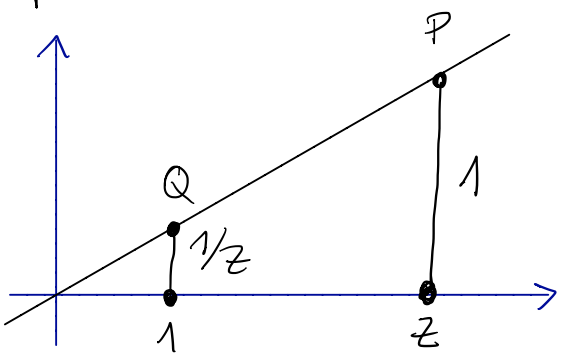
1)



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

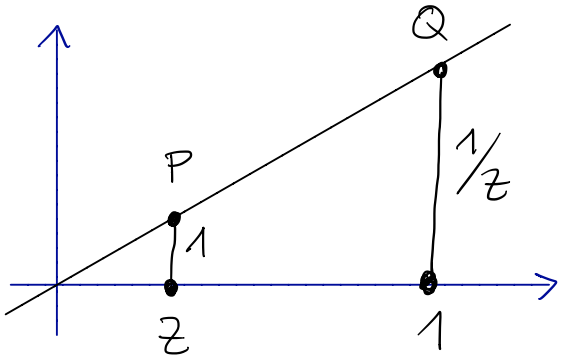
Dann gilt $|zQ| = zz'$ wegen Strahlensatz.

2) falls $z > 1$:

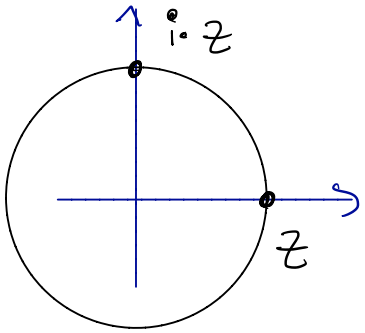


- Lot fällen auf z, 1 abtragen liefert P
- Lot fällen auf 1
- Schnittpunkt von $g(0,P)$ mit Lot auf 1 liefert Q. Dann gilt $|1Q| = 1/z$ wegen Strahlensatz.

falls $z < 1$



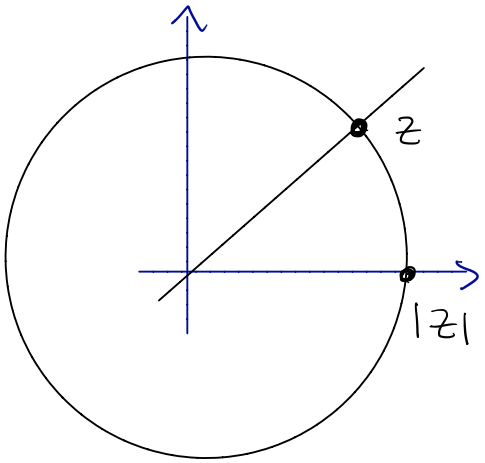
3) $i \cdot z \in g(0,i) \cap k(0,|z|) \subset \tilde{M} \setminus \{0\}$



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.

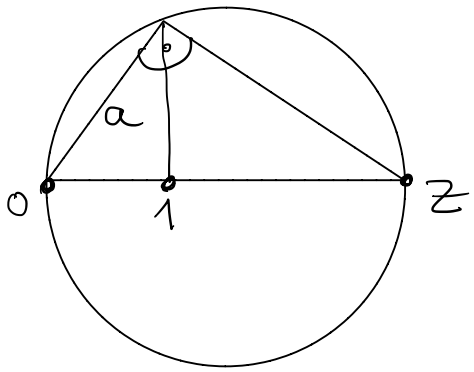
4.3.5 Satz

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

Beweis:

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

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



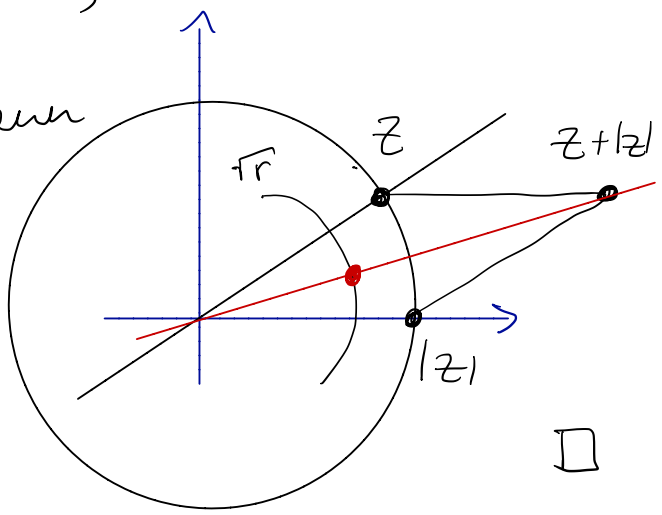
Sei $z \in \tilde{M} \cap \mathbb{R}_{>0}$, $z < 1 \Rightarrow$

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

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

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

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 $l = 0$.

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

OE $p \mid b_0$. 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 $R[x] \iff$
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.

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

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

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 $\mathbb{O}$ $g = c \cdot p$ 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. $\square$

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 n. V. 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_n, $z^2 \nmid a_0 \overset{\text{Eisenstein}}{\underset{4.3.9}{\Longrightarrow}}$ 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

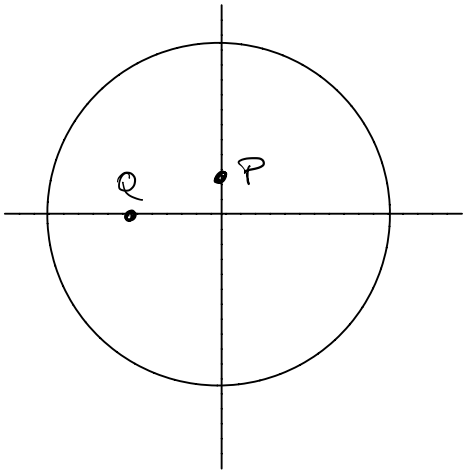
$\Rightarrow$ das Minimalpolynom von z ist f
und hat Grad 4.

Wir können also keinen Widerspruch

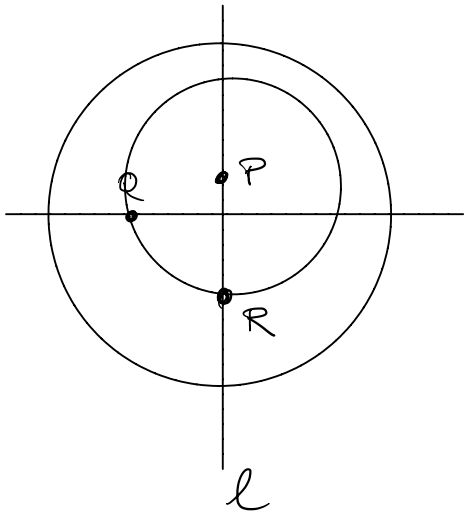
zu Satz 4.3.6 erzeugen.

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

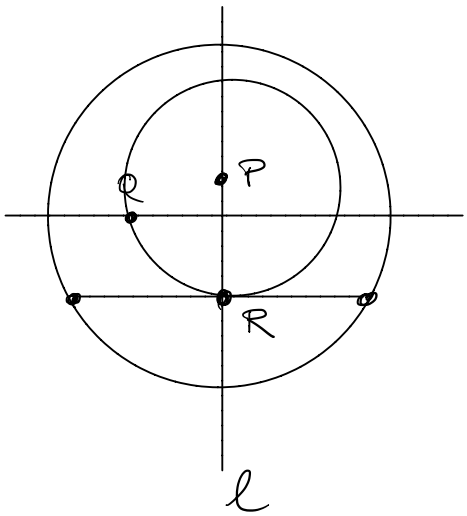
- Zwei aufeinander senkrecht stehenden Geraden durch den Mittelpunkt eines Kreises

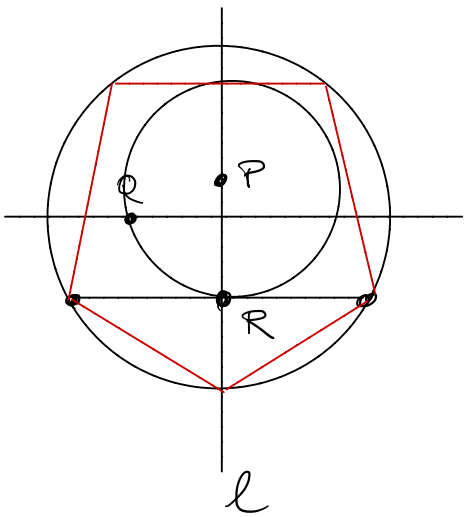


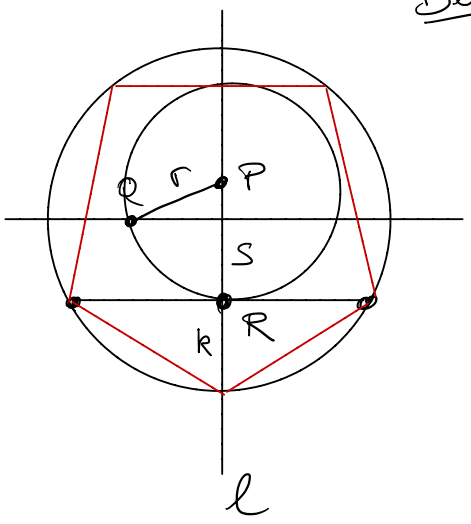
- Halbiere Radius, erhalte Q
- Viertele Radius, erhalte P
- Kreis mit Mittelpunkt P durch Q schneidet Gerade l in Punkt R



- 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:

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

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

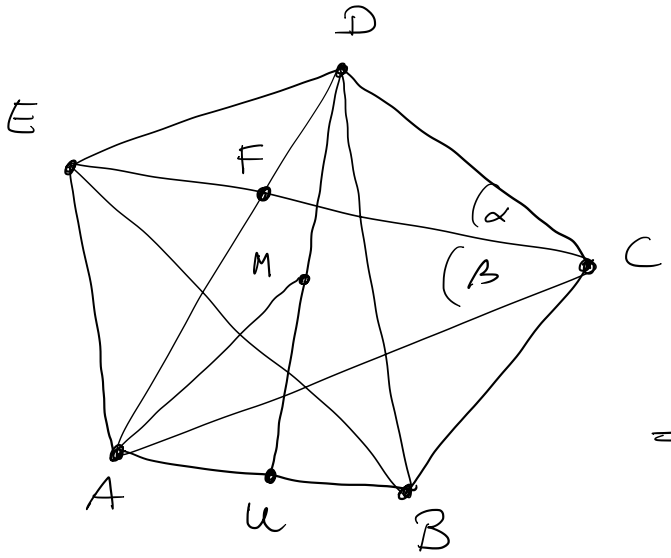
$$s = \frac{\sqrt{5}}{4} - \frac{1}{4},$$

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

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

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

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

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.

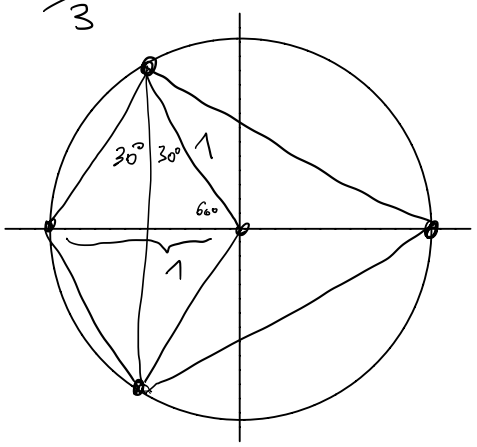
Beweis:

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 $\varphi(\frac{p}{q}) = \frac{\varphi(p)}{\varphi(q)} = \frac{p}{q}$. □

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 $U \subset \mathrm{Aut}_K(L)$ eine Untergruppe.

Dann ist

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

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

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

ist

$\mathrm{Aut}_M(L) \subset \mathrm{Aut}_K(L)$

die Fixgruppe von M.

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

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

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

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 <u>normal</u>, wenn jedes irreduzible Polynom $g \in K[X]$ mit einer Nullstelle in L schon über L in Linearfaktoren zerfällt.

<u>Bsp</u> 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 $\gamma \in M$ eine Nullstelle von g.

Da g irreduzibel ist gilt

$$K[\beta] \cong \frac{K[X]}{\langle g \rangle} \cong K[\gamma],$$

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
$\Psi: L \to L[\gamma]$ 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

$\Leftrightarrow$ $f(\alpha) = 0$ 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

$\Leftrightarrow$ $f' = 0$.

<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
$\mathrm{char}(F) = p$, $|F| = p^r$ wobei
$r = [F : \mathbb{Z}_p] < \infty$, wobei $\mathbb{Z}_p$ der Primkörper $P(F)$ ist.

Beweis: $P(F) = \mathbb{Z}_p$ und $\mathrm{char}(F) = p$
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
$\Rightarrow$ $|F| = p^r$. $\square$

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

$Fr: L \longrightarrow L: a \longmapsto a^p$

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

$$Fr(a+b) = (a+b)^p =$$

$$a^p + \binom{p}{1} a^{p-1}b + \cdots + \binom{p}{j} a^{p-j}b^j + \cdots + \binom{p}{p-1} a b^{p-1} + b^p$$

$$= a^p + b^p = Fr(a) + Fr(b).$$

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. $\square$

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

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

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

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

$\exists$ Elemente der Ordnung d $\forall d \mid n$,

insbesondere $\exists$ Element der Ordnung n und H ist zyklisch. □

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 $L = K(\alpha)$.

□

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 zyklischer Gruppe $\exists$ 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

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

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

Bemerkung:

Damit erhalten wir Bijektionen

$$\{\text{Teiler von } n\} \overset{1:1}{\longleftrightarrow} \{\text{Zwischenkörper } K \subset M \subset L\}$$

$$s \longmapsto \operatorname{Fix}(Fr_q^s) \cong \mathbb{F}_{q^s}$$

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

$$\{\text{Teiler von } n\} \overset{1:1}{\longleftrightarrow} \{\text{Untergruppen von } \operatorname{Aut}_K(L)\}$$

$$s \longmapsto \langle Fr_q^s \rangle$$

da $\operatorname{Aut}_K(L)$ 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

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

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

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

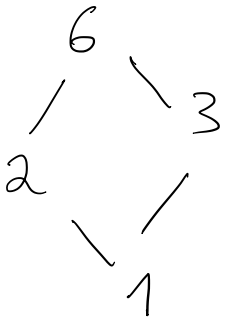
$\mathrm{Aut}_K(M)$, denn mit $K = \mathbb{F}_q$, $M = \mathbb{F}_{q^s}$ ist $\mathrm{Aut}_K(M)$ zyklisch der Ordnung s. □

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

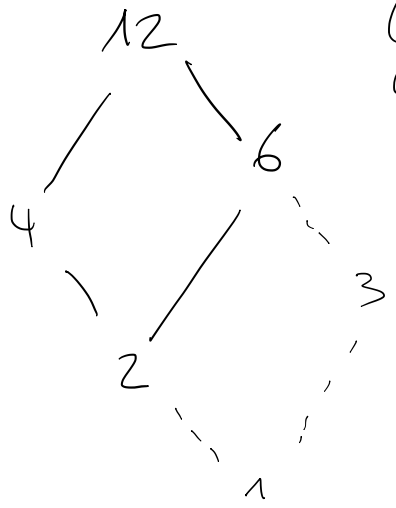
$q^6 = 4^6 = 2^{12}$. $K = F_4 = F_{2^r}$, $L = F_{4^6} = F_{2^{12}}$

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:



(gestrichelte Kante Teiler von 12)

$\mathrm{Aut}_K(L) \cong \mathbb{Z}_6$, $\mathrm{Aut}_K(L) \subset \mathrm{Aut}_{\mathbb{F}_2}(L) \cong \mathbb{Z}_{12}$,

$G = \mathrm{Aut}_{\mathbb{F}_2}(L)$ wird erzeugt von Fr_2, d.h.

$$\begin{array}{ccc} \mathrm{Aut}_{\mathbb{F}_2}(L) & \xrightarrow{\cong} & \mathbb{Z}_{12} \\ \mathrm{Fr}_2 & \longmapsto & 1 \end{array}$$

$H = \mathrm{Aut}_K(L)$ ist erzeugt von $\mathrm{Fr}_2^2 = \mathrm{Fr}_4$.

$$\Rightarrow \begin{array}{ccc} H = \mathrm{Aut}_K(L) & \subset & \mathrm{Aut}_{\mathbb{F}_2}(L) = G \\ \cong & & \cong \\ \mathbb{Z}_6 = \langle 2 \rangle & \subset & \mathbb{Z}_{12} \end{array}$$

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 $\mathbb{Z}_{12}$)

$$\boxed{G = \mathbb{Z}_{12} = \langle 1 \rangle = \langle \mathrm{Fr}_2 \rangle}$$

$$\boxed{\langle \mathrm{Fr}_2^3 \rangle \cong \mathbb{Z}_4 = \langle 3 \rangle}$$

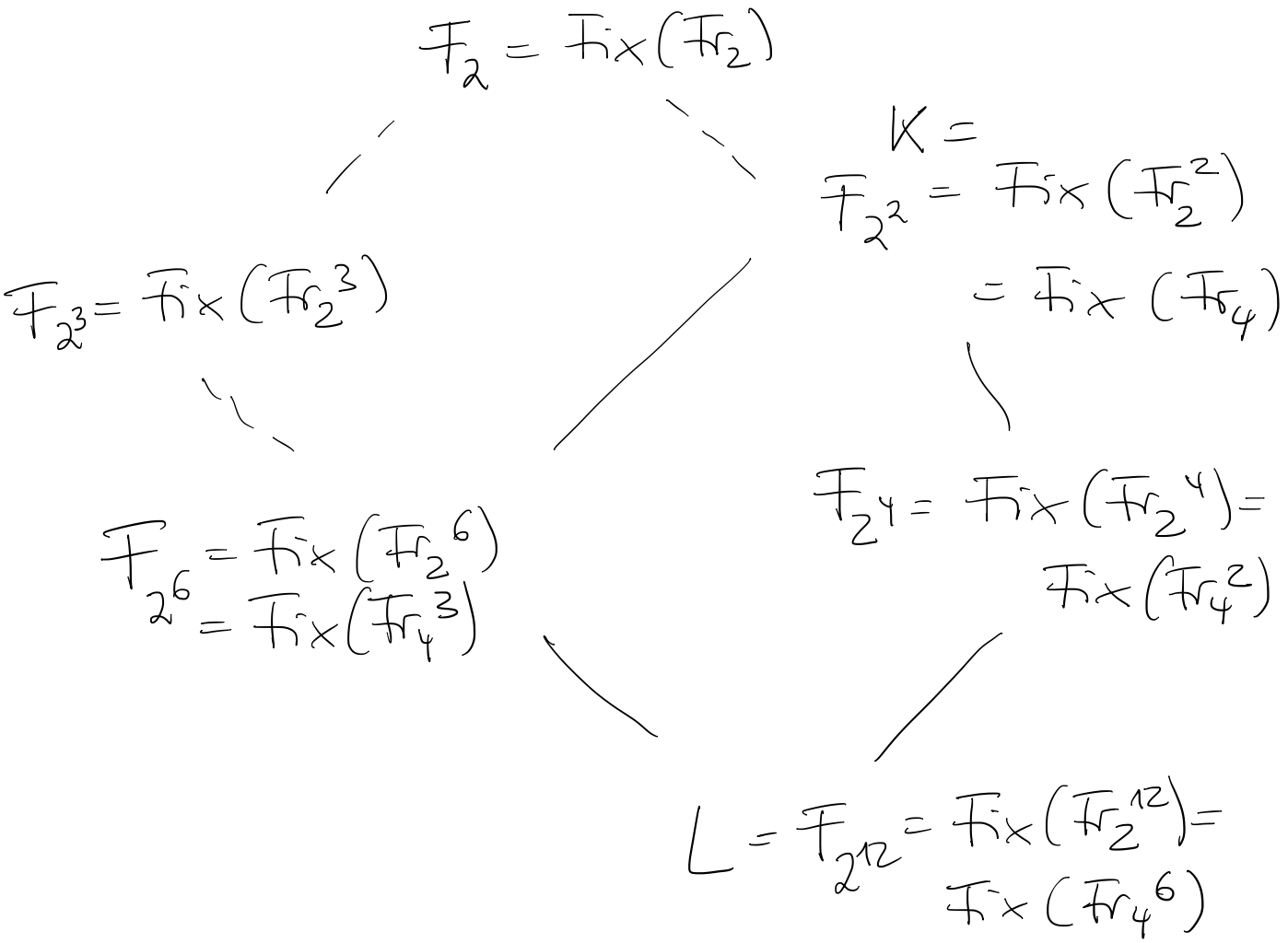
$$\boxed{\mathbb{Z}_6 = \langle 2 \rangle = H = \langle \mathrm{Fr}_2^2 \rangle = \langle \mathrm{Fr}_4 \rangle}$$

$$\boxed{\langle \mathrm{Fr}_2^6 \rangle \cong \langle 6 \rangle = \mathbb{Z}_2 = \langle \mathrm{Fr}_4^3 \rangle}$$

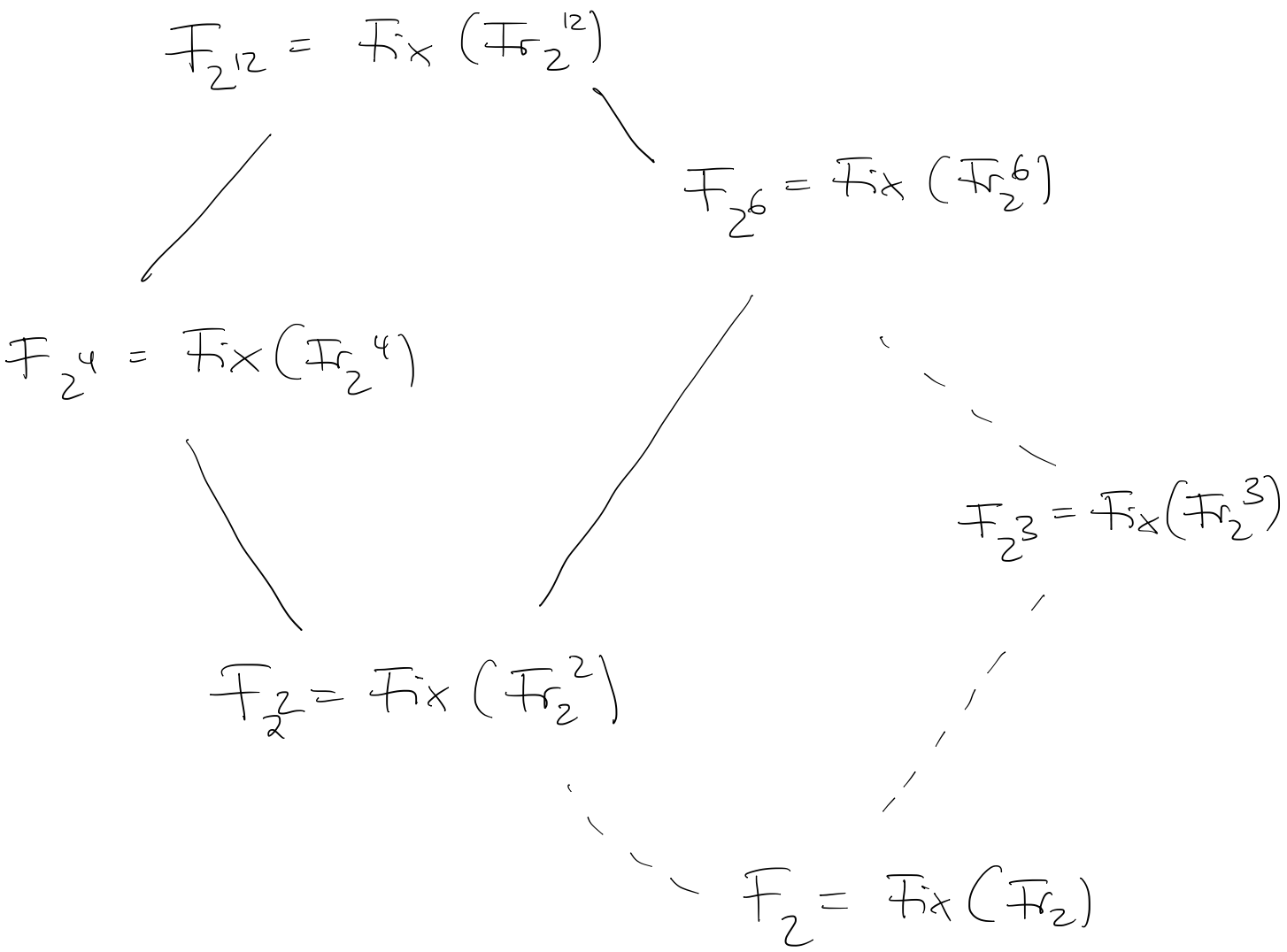
$$\boxed{\mathbb{Z}_3 = \langle 4 \rangle \cong \langle \mathrm{Fr}_2^4 \rangle = \langle \mathrm{Fr}_4^2 \rangle}$$

$$\boxed{\mathrm{id} = \langle 12 \rangle = \langle 0 \rangle \cong \langle \mathrm{Fr}_2^{12} \rangle = \langle \mathrm{id} \rangle = \langle \mathrm{Fr}_4^6 \rangle}$$

Das dazugehörige Zwischenkörperdiagramm (gesucht: 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 Untekörper 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 $\mathbb{Z}_{12}$)

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

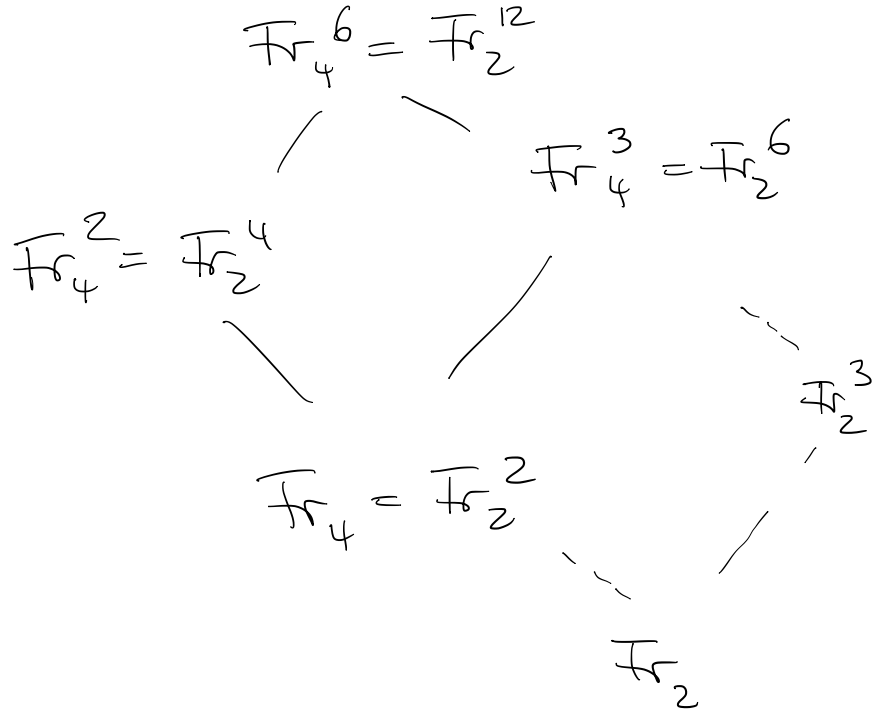
$\mathbb{Z}_3 = \langle 4 \rangle \cong \langle Fr_2^4 \rangle = \langle Fr_4^2 \rangle$

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

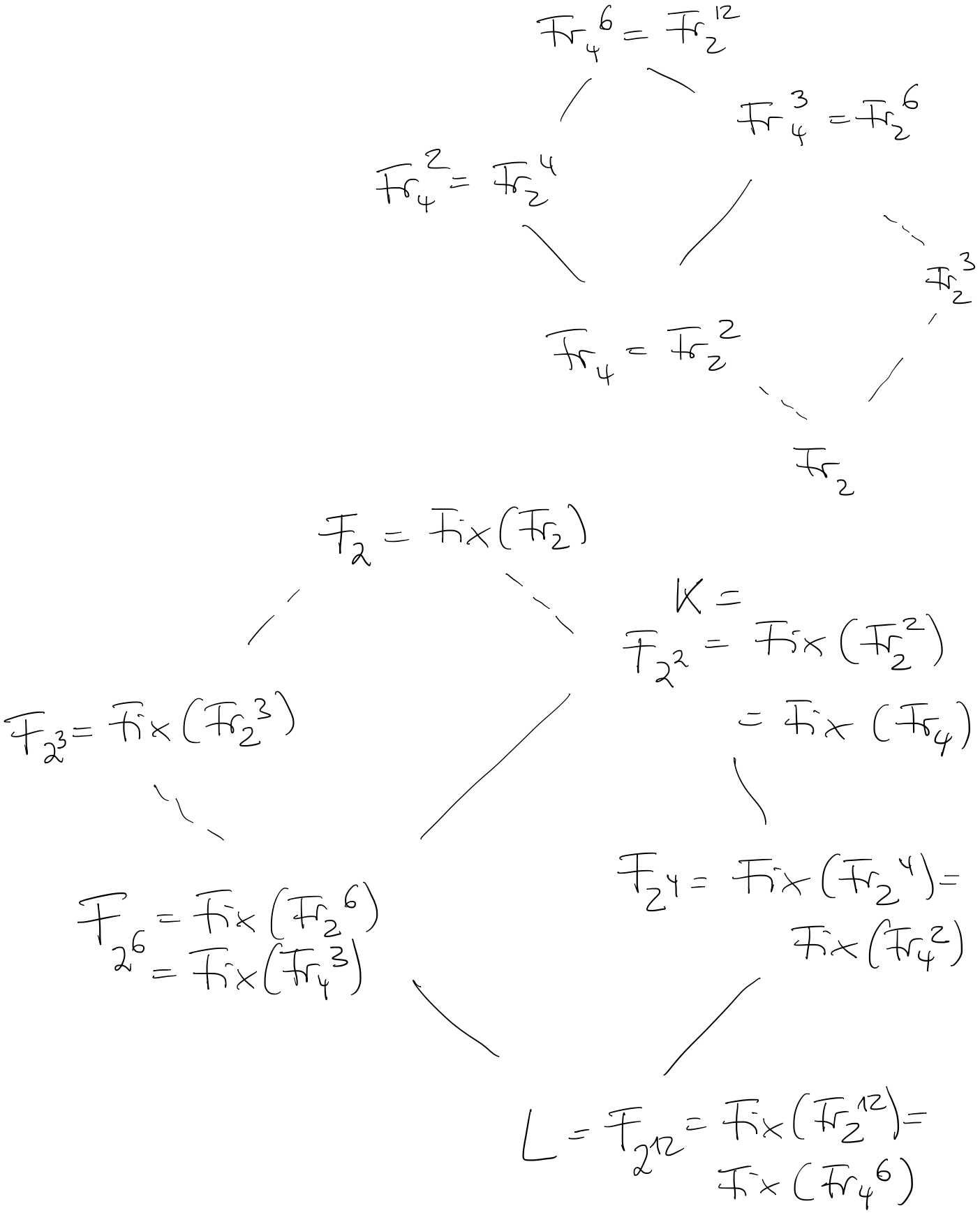
$\langle Fr_2^3 \rangle \cong \mathbb{Z}_4 = \langle 3 \rangle$

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

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. $\square$

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 $[L : \mathrm{Fix}(U)]$

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

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.

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

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

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

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) $\{\text{Untergruppen von } Aut_K(L)\} \xleftrightarrow{1:1} \{\text{Zwischenkörper von } K \subset L\}$

$$U \longmapsto Fix(U)$$

$$Aut_M(L) \longleftarrow M$$

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
- $\ker(\pi) = \{\varphi \mid \varphi|_M = \mathrm{id}\} = \mathrm{Aut}_M(L)$
- 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. $\square$

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:

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

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

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

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

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 :

$\alpha_1 \longmapsto \alpha_4$

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

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

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

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

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

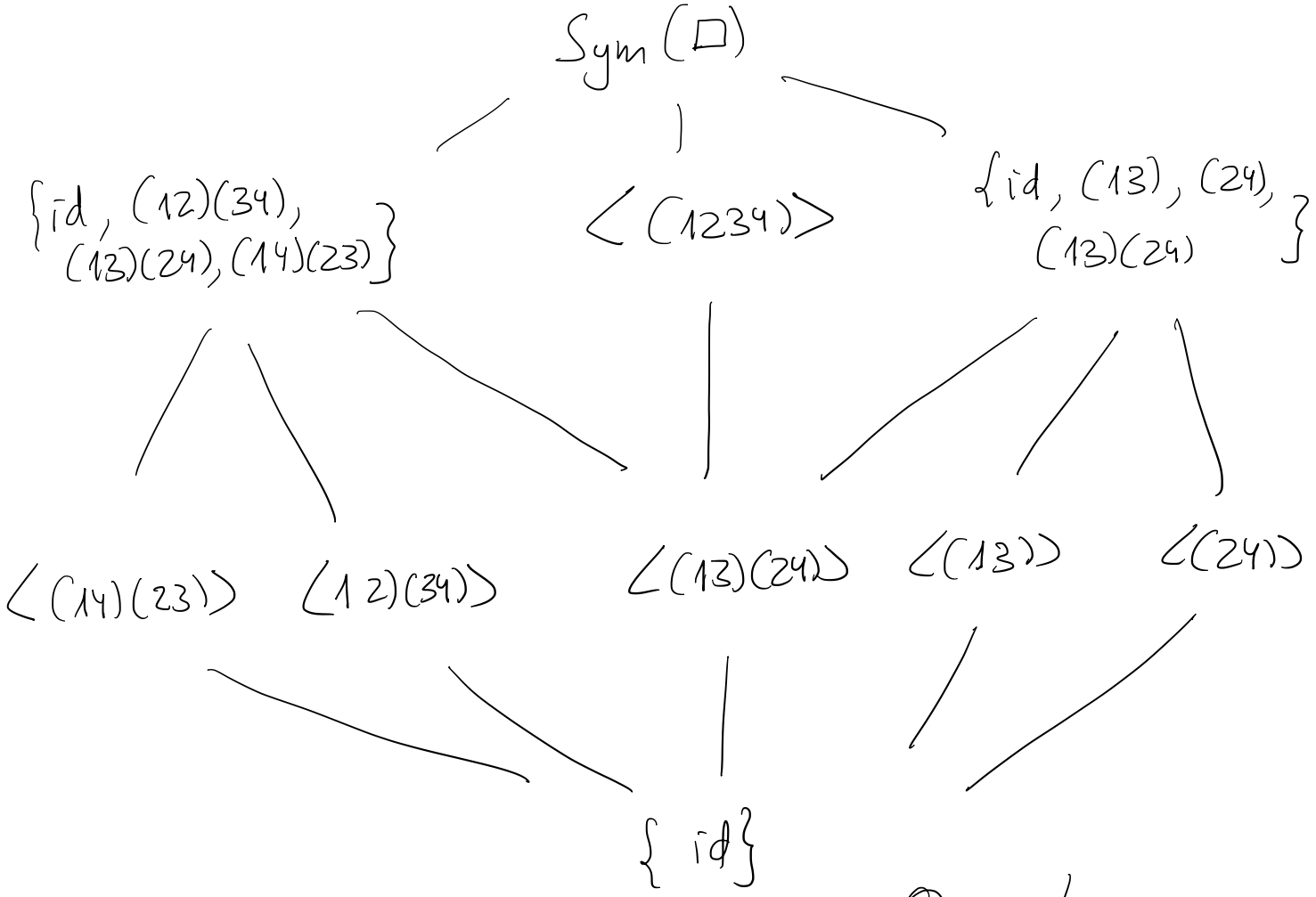
$\{ id, (1234), (13)(24), (1423), (13), (24), (14)(23), (12)(34) \}$

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

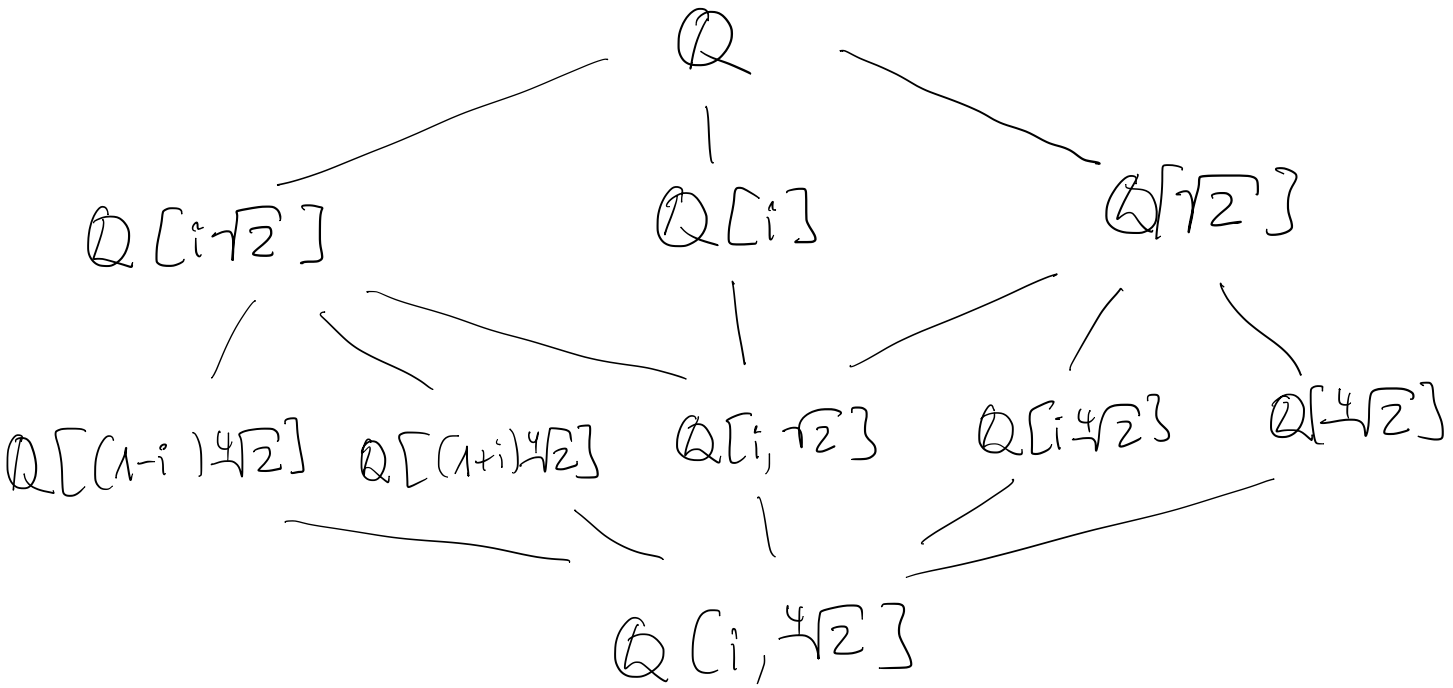
$= \mathrm{Sym}\left(\begin{smallmatrix} \alpha_1 & & \alpha_4 \\ \alpha_2 & & \alpha_3 \end{smallmatrix}\right)$

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

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



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



5. Anwendungen

5.1 Der Fundamentalsatz der Algebra

5.1.1 Lemma

1) $\mathbb{R}$ besitzt keine Körpererweiterung von ungeradem Grad $n > 1$.

2) $\mathbb{C}$ besitzt keine Körpererweiterung vom Grad 2.

Beweis:

1) Sei $\mathbb{R} \subset L$ eine Körpererweiterung vom Grad n. Wegen 4.5.10 ist $\mathbb{R} \subset L$ separabel. Aus dem Satz vom primitiven Element 4.7.1 folgt: $\exists\, \alpha \in L : L = \mathbb{R}(\alpha)$, und das Minimalpolynom $m_\alpha \in \mathbb{R}[X]$ ist irreduzibel von ungeradem Grad n. Dann gilt $\lim_{x \to -\infty} m_\alpha(x) = -\infty$, $\lim_{x \to \infty} m_\alpha(x) = \infty$. Aus dem

Zwischenwertsatz folgt, daß m_α eine Nullstelle in $\mathbb{R}$ hat. Da m_α irreduzibel ist, muß damit $m_\alpha = X - \alpha$ Grad 1 haben.

2) Wäre $\mathbb{C} \subset L$ vom Grad 2, so wäre wie vorher $L = \mathbb{C}(\alpha)$ und $m_\alpha = x^2 + px + q \in \mathbb{C}[X]$. Dann hat m_α also die Nullstellen $X = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q} \in \mathbb{C}$ und zerfällt in Linearfaktoren ↯.

5.1.2 Lemma

Sei $K \subset L$ eine Galoiserweiterung und $p^k \mid [L:K]$ für eine Primzahl p, dann $\exists$ Zwischenkörper $K \subset N \subset L$ mit $[L:N] = p^k$.

Beweis: Nach dem Hauptsatz der Galoistheorie gilt $[L:K] = |\mathrm{Aut}_K(L)|$ also $p^k \mid |\mathrm{Aut}_K(L)|$.

Nach Satz 1.5.4 $\exists$ Untergruppe

$H \subset \mathrm{Aut}_K(L)$ mit $|H| = p^k$, und nach dem Hauptsatz der Galoistheorie damit $N = \mathrm{Fix}(H)$ mit $K \subset N \subset L$ und $[L:N] = |\mathrm{Aut}_N(L)| = |H| = p^k$. □

5.1.3 Satz (Fundamentalsatz der Algebra)

Der Körper $\mathbb{C}$ ist algebraisch abgeschlossen.

Beweis:

Sei $f \in \mathbb{C}[X]$ ein nicht konstantes Polynom und sei L der Zerfällungskörper von f.

Es gilt $\mathbb{R} \subset \mathbb{C} \subset L$, und $\mathbb{R} \subset L$ ist endlich, separabel (4.5.10) und daher einfach (4.7.1, Satz vom primitiven Element).

$\Rightarrow L = \mathbb{R}(\alpha)$ für ein $\alpha \in L$.

Sei m_α das Minimalpolynom von α über $\mathbb{R}$ und M der Zerfällungs-

körper von M_2.

$\mathbb{R} \subset M$ ist endlich, normal (4.5.3) und separabel (4.5.10), also eine Galoiserweiterung.

$$\mathbb{R} \subset \mathbb{C} \subset L = \mathbb{R}(\alpha) \subset M$$

$$\Rightarrow \quad 2 = [\mathbb{C} : \mathbb{R}] \mid [M : \mathbb{R}]$$

Hauptsatz der Galoistheorie

$$\Rightarrow \quad 2 \mid |\mathrm{Aut}_{\mathbb{R}}(M)|$$

Nach Satz 1.5.4 $\exists$ 2-Sylow untergruppe $H \subset \mathrm{Aut}_{\mathbb{R}}(M)$ und nach dem Hauptsatz der Galoistheorie $N = \mathrm{Fix}(H)$ mit $\mathrm{Aut}_N(M) = H$ und $[M : N] = |\mathrm{Aut}_N(M)| = |H|$.

Da $\mathbb{R} \subset N \subset M$ folgt

$$[N : \mathbb{R}] \cdot [M : N] = [M : \mathbb{R}] \Rightarrow$$

$$[N : \mathbb{R}] \cdot |H| = [M : \mathbb{R}] = |\mathrm{Aut}_{\mathbb{R}}(M)|$$

Da H 2-Sylowgruppe in $\mathrm{Aut}_{\mathbb{R}}(M)$ folgt $[N : \mathbb{R}]$ ist ungrade.

Mit Lemma 5.1.2 1) folgt dann

$N = \mathbb{R}$.

$$\Rightarrow [M:\mathbb{R}] = |H| = 2^k$$

$$\Rightarrow [M:\mathbb{C}] = \frac{[M:\mathbb{R}]}{[\mathbb{C}:\mathbb{R}]} = 2^{k-1}$$

Wäre $k \geq 2$, so wäre $\mathbb{C} \subset M$ endlich, separabel und normal (4.5.5), also Galoiserweiterung. Mit Lemma 5.1.2 $\exists$ dann Zwischenkörper $\mathbb{C} \subset N' \subset M$ mit $[N':\mathbb{C}] = 2$

↯ zu Lemma 5.1.1 1) $\Rightarrow p = 1$

$\Rightarrow M = \mathbb{C}$, da $\mathbb{R} \subset \mathbb{C} \subset L \subset M$

auch $L = \mathbb{C}$.

Damit zerfällt f also schon über $\mathbb{C}$ in Linearfaktoren und $\mathbb{C}$ ist algebraisch abgeschlossen. □

5.2 Auflösbarkeit polynomialer Gleichungen

Sei $f = x^n + a_{n-1}x^{n-1} + \dots + a_0$ ein Polynom in $\mathbb{C}[x]$.

Wir möchten die Nullstellen von f durch die Koeffizienten ausdrücken.

5.2.1 Bsp

1) $n=1$, $f = x + a_0$, $-a_0$ ist Nullstelle.

2) $n=2$ $f = x^2 + px + q$,

Nullstellen sind $-\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}$.

3) $n=3$, die Formeln von Cardano:

Setze $g = f\left(x - \frac{a_2}{3}\right) = x^3 + px + q$

mit $p = a_1 - \frac{a_2^2}{3}$, $q = a_0 - \frac{a_1 a_2}{3} + \frac{2a_2^3}{27}$.

Ist $p = 0$, so sind die 3. Wurzeln aus q die Nullstellen.

Ist $p \neq 0$, setze $x = u + v$ mit $u \neq 0$ und $v = -\frac{p}{3u}$.

Aus $g(x)=0$ wird

$$u^3+v^3+3uv(u+v)+p(u+v)+q=0$$

$$\Rightarrow \quad u^3+v^3+q=0$$

$$\Rightarrow \quad u^3+q-\frac{p^3}{27u^3}=0 \quad \Rightarrow$$

$$u^6+qu^3-\frac{p^3}{27}=0 \quad \Rightarrow$$

$$u^3=-\frac{q}{2}\pm\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}\,.$$

Sei $u \in \mathbb{C}$ eine dritte Wurzel aus der rechten Seite, so gilt mit $v=-\frac{p}{3u}$, daß $u+v$ eine Lösung von $g(x)=0$ ist.

4) $n=4$ so ähnlich.

5.2.2 Def

1) Eine Körpererweiterung $K \subset L$ heißt Radikalerweiterung, wenn $L=K(\alpha_1,\dots,\alpha_n)$ und $\alpha_i^{k_i} \in K(\alpha_1,\dots,\alpha_{i-1})$ für ein $k_i \geq 2$.

2) Eine Radikalerweiterung heißt <u>abelsch</u>, wenn $K(\alpha_1, \dots, \alpha_{i-1}) \subset K(\alpha_1, \dots, \alpha_i)$ eine Galois-erweiterung mit abelscher Galoisgruppe ist $\forall\, i = 2, \dots, n$.

3) $f \in K[x]$ heißt <u>durch Radikale auflösbar</u> über K, wenn es eine Radikal-erweiterung $K \subset L$ gibt, so daß f über L in Linearfaktoren zerfällt.

<u>Bemerkung</u>:
Sei $f = a_n x^n + \dots + a_0 \in \mathbb{C}[x]$,
$K = \mathbb{Q}(a_0, \dots, a_n)$.
Genau dann, wenn $f \in K[x]$ über K durch Radikale auflösbar ist, können wir wie in Bsp. 5.2.1 die Nullstellen von f durch Wurzeln von rationalen Funktionen der Koeffizienten ausdrücken.

5.2.3 Satz

Sei $f \in K[x]$, $\operatorname{char}(K) = 0$, L der Zerfällungskörper von f. Dann:
f ist über K durch Radikale auflösbar
$\Leftrightarrow$ $\operatorname{Aut}_K(L)$ ist auflösbar

5.2.4 Lemma

Sei $\text{char}(K)=0$, $\zeta_n = e^{\frac{2\pi i}{n}} \in K$.

1) Ist $L = K(\alpha)$ mit $\alpha^n \in K$, dann ist L der Zerfällungskörper von $x^n - \alpha^n$, $K \subset L$ ist Galoiserweiterung und $\text{Aut}_K(L)$ ist zyklisch mit $|\text{Aut}_K(L)| \mid n$.

2) Ist $K \subset L$ Galoiserweiterung mit $\text{Aut}_K(L) \cong \mathbb{Z}_n$ und n prim, dann ist $L = K(\alpha)$ mit $\alpha^n \in K$.

Beweis:

1) $x^n - \alpha^n = (x - \zeta_n^0 \alpha) \cdot (x - \zeta_n \alpha) \cdot \ldots \cdot (x - \zeta_n^{n-1} \alpha)$

Da $\zeta_n \in K \Rightarrow \zeta_n^i \in K \Rightarrow \alpha \zeta_n^i \in L$

$\Rightarrow L = K(\alpha) = K(\zeta_n^0 \alpha, \zeta_n \alpha, \ldots, \zeta_n^{n-1} \alpha)$

ist der Zerfällungskörper von $x^n - \alpha^n$

$x^n - \alpha^n$ ist separabel

$\overset{4.7.11}{\Rightarrow}$ $K \subset L$ ist Galoiserweiterung

Wir setzen $\Pi: \text{Aut}_K(L) \longrightarrow \mathbb{Z}_n$:

$$\sigma_k \longmapsto k$$

wobei $\sigma_k(\alpha) = \zeta_n^k \alpha$.

Da $\sigma_k \circ \sigma_\ell = \sigma_{k+\ell}$ ist Π ein Gruppenhomomorphismus. Π ist auch injektiv.

$\Rightarrow$ $\mathrm{Aut}_K(L)$ ist eine Untergruppe von $\mathbb{Z}_n$ und damit selbst zyklisch mit einer Ordnung, die n teilt.

2) $\mathrm{Aut}_K(L) = \langle \sigma \rangle$, $\mathrm{ord}(\sigma) = n$.

Betrachte σ als K-Vektorraumendomorphismus $\sigma : L \to L$.

Da $\sigma^n = \mathrm{id}$ muß das Minimalpolynom μ_σ $x^n - 1$ teilen.

$x^n - 1$ zerfällt über K in die Linearfaktoren $(x - \zeta_n^0) \cdots (x - \zeta_n^{n-1})$.

Da das Minimalpolynom paarweise verschiedene Linearfaktoren hat, ist σ diagonalisierbar.

Alle Eigenwerte sind n-te Einheitswurzeln.

Wäre 1 der einzige Eigenwert $\Rightarrow \sigma = \mathrm{id}$

$\Rightarrow n = 1 \not\equiv$ zu n prim

Sei $0 \neq \alpha \in L$ Eigenvektor zum Eigenwert $\zeta \in K$, also $\sigma(\alpha) = \zeta\alpha$

$\Rightarrow \sigma(\alpha^n) = \sigma(\alpha)^n = \zeta^n \alpha^n = \alpha^n$

$\Rightarrow \alpha^n \in \mathrm{Fix}(\mathrm{Aut}_K(L)) = K$

da $K \subset L$ Galoiserweiterung

Beh: $L = K(\alpha)$

„$\supseteq$" klar

„$\subseteq$" Da $[L : K(\alpha)] \cdot [K(\alpha) : K] = [L : K]$

$= |\mathrm{Aut}_K(L)| = n$ und prim

folgt $[K(\alpha) : K] \in \{1, n\}$.

Wäre $[K(\alpha) : K] = 1 \Rightarrow \alpha \in K \Rightarrow$

$\delta(\alpha) = \alpha$ ↯ zu $\delta(\alpha) = \zeta\alpha$

mit Eigenwert $\zeta \neq 1$

$\Rightarrow [K(\alpha) : K] = n \Rightarrow [L : K(\alpha)] = 1$

$\Rightarrow L = K(\alpha)$.

□

5.2.5 Korollar:

Sei L Zwischenkörper einer Radikalerweiterung mit $\mathrm{char}(L) = 0$. Dann ist L Zwischenkörper einer abelschen Radikalerweiterung.

Beweis: Sei $K \subset L \subset M$,

$M = K(\alpha_1, \dots, \alpha_m)$, $\alpha_i^{k_i} \in K(\alpha_1, \dots, \alpha_{i-1})$.

Sei $K_i = K(\alpha_1, \dots, \alpha_i)$,

Sei $n = k_1 \cdot \ldots \cdot k_m$

Sei $\zeta_n = e^{\frac{2\pi i}{n}} \in \mathbb{C}$.

Betrachte

$K = K_0 \subset K_0(\zeta_n) \subset K_1(\zeta_n) \subset \ldots \subset K_m(\zeta_n) = M(\zeta_n)$

Da mit ζ_n auch die k_i-ten Einheitswurzeln in $K_0(\zeta_n)$ enthalten sind, gilt mit S. 2.4 1) angewendet auf $K_{i-1}(\zeta_n)$ und $K_i(\zeta_n) = K_{i-1}(\zeta_n)(\alpha_i)$ mit $\alpha_i^{k_i} \in K_{i-1}(\zeta_n)$

$K_{i-1}(\zeta_n) \subset K_i(\zeta_n)$ ist Galoiserweiterung mit zyklischer, damit abelscher, Galoisgruppe.

Auch $K_0 \subset K_0(\zeta_n)$ ist Galoiserweiterung, da $K_0(\zeta_n)$ Zerfällungskörper von $x^n - 1$ ist, und die Galoisgruppe ist $\mathbb{Z}_n^*$, da für $b_k(\zeta_n) = \zeta_n^k$ (wegen $b_{ke} = b_k \circ b_e$)

$$\begin{aligned} \mathrm{Aut}_{K_0}(K_0(\zeta_n)) &\xrightarrow{\sim} \mathbb{Z}_n^* \\ b_k &\longmapsto k \end{aligned}$$

Die Einheitengruppe $\mathbb{Z}_n^*$ ist abelsch.

Da $\zeta_n^n = 1$ ist $K \subset M(\zeta_n) = K(\alpha_1, \ldots, \alpha_m, \zeta_n)$ eine abelsche Radikalerweiterung, die L als Zwischenkörper enthält. □

5.2.6 Prop (Translationssatz)

Sei $K \subset M$ eine Erweiterung, N, L Zwischenkörper, $K \subset N$ Galoiserweiterung. Dann sind auch $L \cap N \subset N$ und $L \subset L(N)$ Galoiserweiterungen mit

$$\mathrm{Aut}_{L \cap N}(N) \cong \mathrm{Aut}_L(L(N)).$$

Beweis:

$L \cap N$ ist Zwischenkörper der Galois-erweiterung $K \subset N$, damit ist $L \cap N \subset N$ auch Galoiserweiterung wegen des Hauptsatzes der Galoistheorie 4.7.9.

Wegen 4.7.11 ist N Zerfällungskörper eines separablen Polynoms $f \in K[X]$.

Seien $\alpha_1, \dots, \alpha_n$ die Nullstellen von f

$\Rightarrow N = K(\alpha_1, \dots, \alpha_n)$

$\Rightarrow L(N) = L(\alpha_1, \dots, \alpha_n)$ ist der Zerfällungskörper von f über L und damit ist $L \subset L(N)$ Galoiserweiterung wegen 4.7.11.

Sei $\sigma \in Aut_L(L(N))$, dann hält σ insbesondere K fest, und da $K \subset N$ normal ist folgt mit 4.7.6 $\sigma|_N : N \to L(N)$ ist schon in $Aut_K(N)$.

$\Rightarrow \pi : Aut_L(L(N)) \longrightarrow Aut_K(N)$

$\sigma \longmapsto \sigma|_N$

ist wohldefinierter Gruppenhomomorphismus.

Da σ durch die Bilder der α_i festgelegt ist und $\alpha_i \in N \ \forall i$ folgt π ist injektiv $\Rightarrow$

$Aut_L(L(N)) \cong U$ Untergruppe von $Aut_K(N)$

Dann gilt $Fix(U) = \{ \alpha \in N \mid \sigma(\alpha) = \alpha \ \forall \sigma \in Aut_L(L(N)) \} =$

$N \cap \{\alpha \in L(N) \mid \sigma(\alpha) = \alpha \text{ für } \sigma \in Aut_L(L(N))\}$

$= N \cap Fix(Aut_L(L(N)))$

$= N \cap L$, da $L \subset L(N)$ Galois-erweiterung ist

$\Rightarrow U = Aut_{N \cap L}(N)$ wegen des Hauptsatzes der Galoistheorie. □

Beweis von 5.2.3:

Erinnerung: 5.2.3 Satz

Sei $f \in K[X]$, $char(K) = 0$, L der Zerfällungskörper von f. Dann:

f ist über K durch Radikale auflösbar

$\Leftrightarrow Aut_K(L)$ ist auflösbar

Beweis:

„$\Rightarrow$" nach Def ∃ Radikalerweiterung $K \subset M$, so daß f über M in Linearfaktoren zerfällt. Da L der Zerfällungskörper von f ist, ist $K \subset L \subset M$ Zwischenkörper. Da $char(L) = char(K) = 0$

folgt mit 5.2.5, daß L Zwischenkörper einer abelschen Radikalerweiterung $M' = K(\alpha_1, \dots, \alpha_m)$ ist mit $\alpha_i^{k_i} \in K(\alpha_1, \dots, \alpha_{i-1})$.

Setze $K_i = K(\alpha_1, \dots, \alpha_i)$.

Wir zeigen per Induktion über m, daß $\mathrm{Aut}_K(L)$ auflösbar ist.

Für $m=0$ gilt $K = L = M'$ und $\mathrm{Aut}_K(L) = \{e\}$.

Sei $m>0$. $L(K_1)$ ist der Zerfällungskörper von $f \in K_1[X]$ und ist Zwischenkörper der abelschen Radikalerweiterung $K_1 \subset M'$. Per Induktion können wir annehmen, daß $\mathrm{Aut}_{K_1}(L(K_1))$ auflösbar ist. Es gilt

$$\mathrm{Aut}_{K_1}(L(K_1)) \overset{\text{Translations-satz 5.26}}{\cong} \mathrm{Aut}_{K_1}(K_1(L)) = \mathrm{Aut}_{K_1 \cap L}(L),$$

(da $K \subset L$ Galois-erweiterung ist, da f separabel wegen $\mathrm{char}(K) = 0$, 4.5.11.)

$\Rightarrow \mathrm{Aut}_{K_1 \cap L}(L)$ ist auflösbar. (*)

Da $K \subset M$ abelsche Radikalerweiterung ist, ist $K \subset K_1$ Galoiserweiterung und $\mathrm{Aut}_K(K_1)$ abelsch.

Da $K \subset L \cap K_1 \subset K_1$ Zwischenkörper ist $\mathrm{Aut}_{L \cap K_1}(K_1)$ Untergruppe von $\mathrm{Aut}_K(K_1)$, damit Normalteiler, und aus dem Hauptsatz der Galoistheorie 4.7.9 folgt $K \subset K_1 \cap L$ ist Galoiserweiterung und

$$\frac{\mathrm{Aut}_K(K_1)}{\mathrm{Aut}_{K_1 \cap L}(K_1)} \cong \mathrm{Aut}_K(K_1 \cap L),$$

wobei letztere als Faktorgruppe einer abelschen Gruppe auch abelsch ist.

Da $K \subset L \cap K_1 \subset L$ Zwischenkörper ist und $K \subset L \cap K_1$ Galoiserweiterung folgt wieder mit dem Hauptsatz

4.7.9 $\mathrm{Aut}_{L \cap K_1}(L)$ Normalteiler in $\mathrm{Aut}_K(L)$ und

$$\frac{\mathrm{Aut}_K(L)}{\mathrm{Aut}_{L \cap K_1}(L)} \cong \mathrm{Aut}_K(L \cap K_1)$$

und diese Gruppe ist abelsch und damit auflösbar.

$\Rightarrow$ Der Normalteiler $\mathrm{Aut}_{L \cap K_1}(L)$ ist auflösbar (*), die Faktorgruppe $\mathrm{Aut}_K(L) / \mathrm{Aut}_{L \cap K_1}(L)$ ist auflösbar

1.6.5 $\Rightarrow$ $\mathrm{Aut}_K(L)$ ist auflösbar.

"$\Leftarrow$" Sei $\mathrm{Aut}_K(L)$ auflösbar.

Sei $n = [L : K]$.

1. Fall: Sei $\zeta_n \in K$.

Da $\mathrm{Aut}_K(L)$ auflösbar, $\exists$ nach Satz 1.6.9 eine Kompositionsreihe, i.e.

$\{e\} = G_m \subset G_{m-1} \subset \cdots \subset G_0 = \mathrm{Aut}_K(L)$,

so daß $G_i \subset G_{i-1}$ Normalteiler und

G_{i-1}/G_i zyklisch von Primzahlordnung p_i.

Betrachte die Zwischenkörper

$$K \subset K_i := \mathrm{Fix}(G_i) \subset L.$$

Da $K \subset L$ Galoiserweiterung (f separabel, 4.5.11 und 4.7.11) ist auch

$K_{i-1} \subset L$ Galoiserweiterung mit

$$\mathrm{Aut}_{K_{i-1}}(L) = \mathrm{Aut}_{\mathrm{Fix}(G_{i-1})}(L) = G_{i-1}$$

nach dem Hauptsatz der Galoistheorie 4.7.9.

Da G_i in G_{i-1} Normalteiler ist, gilt

$$G_{i-1}/G_i = \frac{\mathrm{Aut}_{K_{i-1}}(L)}{\mathrm{Aut}_{K_i}(L)} \cong \mathrm{Aut}_{K_{i-1}}(K_i)$$

und $K_{i-1} \subset K_i$ ist Galoiserweiterung mit zyklischer Galoisgruppe G_{i-1}/G_i.

Da $K = K_0 \subset K_1 \subset \cdots \subset K_m = L$ und

$[L:K] = [K_m : K_{m-1}] \cdot \ldots [K_i : K_{i-1}] \cdot \ldots [K_1 : K_0]$

und $[K_i : K_{i-1}] = |\mathrm{Aut}_{K_{i-1}}(K_i)|$

$= |G_{i-1}/G_i| = p_i$ folgt

$p_i \mid n$.

Damit ist auch $\zeta_{p_i} = e^{\frac{2\pi i}{p_i}} = e^{\frac{2\pi i}{n} \cdot \frac{n}{p_i}}$

$= \zeta_n^{\frac{n}{p_i}} \in K$.

Damit können wir S. 2.4 2) anwenden und erhalten $K_i = K_{i-1}(\alpha_i)$ mit

$\alpha_i^{p_i} \in K_{i-1}$.

Damit ist $L = K(\alpha_1, \ldots, \alpha_m)$ eine Radikalerweiterung.

2. Fall $\zeta_n \notin K$.

Verwende den Translationssatz S. 2.6 für $K \subset L(\zeta_n)$, Zwischenkörper L, $K(\zeta_n)$ mit $K \subset L$ Galoiserweiterung, dann ist $L \cap K(\zeta_n) \subset L$ und

$K(\zeta_n) \subset L(\zeta_n)$ Galoiserweiterung

mit $\mathrm{Aut}_{K(\zeta_n)}(L(\zeta_n)) \cong \mathrm{Aut}_{L \cap K(\zeta_n)}(L)$.

Dann ist $k := [L(\zeta_n) : K(\zeta_n)] = |\mathrm{Aut}_{K(\zeta_n)}(L(\zeta_n))| = |\mathrm{Aut}_{L \cap K(\zeta_n)}(L)|$

$= [L : L \cap K(\zeta_n)] \mid [L : K] = n$

$\Rightarrow \zeta_k = \zeta_n^{\frac{n}{k}} \in K(\zeta_n)$

Da $\mathrm{Aut}_K(L)$ auflösbar ist auch die Untergruppe $\mathrm{Aut}_{L \cap K(\zeta_n)}(L)$ auflösbar, also $\mathrm{Aut}_{K(\zeta_n)}(L(\zeta_n))$ auflösbar.

Damit erfüllt $K(\zeta_n) \subset L(\zeta_n)$ die Voraussetzungen von Fall 1.

Der Zerfällungskörper $L(\zeta_n)$ von f über $K(\zeta_n)[X]$ ist wegen Fall 1 eine Radikalerweiterung

$L(\zeta_n) = K(\zeta_n)(\alpha_1, \dots, \alpha_m)$ mit $\alpha_i^{k_i} \in K(\zeta_n)(\alpha_1, \dots, \alpha_{i-1})$. Da $\zeta_n^n = 1 \in K$ ist auch $K \subset L(\zeta_n)$

Radikalerweiterung, über der f zerfällt
$\Rightarrow$ f ist durch Radikale auflösbar. □

5.2.7 Korollar

Sei $f \in K[X]$ vom Grad höchstens 4, K ein Teilkörper von $\mathbb{C}$, L der Zerfällungskörper von f.
Wegen 4.4.8 ist $Aut_K(L) \subset S_4$ Untergruppe und wegen Bsp 2) nach 1.6.4 ist S_4 auflösbar $\Rightarrow$ f ist durch Radikale auflösbar (wußten wir schon wegen der Formeln von Cardano 5.2.1 3)).

5.2.8 Bsp Sei $f = X^5 + X^4 - 4X^3 - 3X^2 + 3X + 1 \in \mathbb{Q}[X]$.
Man kann zeigen, daß f das Minimalpolynom von $\alpha = \zeta_{11} + \zeta_{11}^{-1}$ ist.
Dann ist $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\zeta_{11})$
und $Aut_{\mathbb{Q}}(\mathbb{Q}(\zeta_{11})) = \mathbb{Z}_{11}^*$ (siehe Beweis von 5.2.5), $\mathbb{Z}_{11}^* \cong \mathbb{Z}_{10}$

ist zyklisch, daher ist jede Untergruppe ein Normalteiler und damit $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ Galoiserweiterung.

$$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha)) \cong \frac{\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_{11}))}{\mathrm{Aut}_{\mathbb{Q}(\alpha)}(\mathbb{Q}(\zeta_{11}))}$$

ist Faktorgruppe einer zyklischen Gruppe und damit selbst zyklisch.

Da $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$ folgt

$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha)) = \mathbb{Z}_5$.

Insbesondere ist $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$ auflösbar, und da f über $\mathbb{Q}(\alpha)$ schon zerfällt, gilt f ist durch Radikale auflösbar.

Die Radikalausdrücke für die Nullstellen von f kennen wir dadurch aber nicht.

5.2.9 Prop Sei p eine Primzahl, $\tau \in S_p$ eine Transposition und σ ein p-Zykel, dann gilt

$S_p = \langle \tau, \sigma \rangle$.

Beweis: OE $\tau = (12)$.

Ist $\beta = (123 \cdots p)$, so gilt

$(i \; i+1) = (\beta^{i-1}(1) \; \beta^{i-1}(2)) =$

$\beta^{i-1} \circ (12) \; \beta^{-(i-1)} \in \langle \tau, \beta \rangle$

$\forall \; i = 1, \ldots, p-1$. Da S_p von Nachbartranspositionen erzeugt wird, folgt die Behauptung.

Ist β ein beliebiger p-Zykel, so sind seine Potenzen auch p-Zykel (da p prim) und wir können eine Potenz wählen, so daß

$\beta^i = (1 2 a_3 \cdots a_p)$

Für $\beta' = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & p \\ 1 & 2 & a_3 & a_4 & \cdots & a_p \end{pmatrix}$ gilt

$\beta'^{-1} \circ \beta^i \circ \beta' = (1 \cdots p)$ und

$\beta'^{-1} \circ (12) \circ \beta' = (12)$, so daß

für $U = \langle \tau, \beta \rangle$ gilt

$S_p = \langle \tau, (1 \cdots p) \rangle \subset \beta'^{-1} U \beta' \subset S_p$

$$\Rightarrow \quad b'^{-1} U b' = \mathfrak{S}_p \quad \Rightarrow$$

$$U = b' \mathfrak{S}_p b'^{-1} = \mathfrak{S}_p \qquad \square$$

5.2.10 Satz (Abel-Ruffini)

Sei $f \in \mathbb{Q}[x]$ irreduzibel vom ungeraden Primzahlgrad p mit genau 2 nicht-reellen Nullstellen, sei L der Zerfällungskörper von f, dann gilt $\mathrm{Aut}_{\mathbb{Q}}(L) \cong \mathfrak{S}_p$.

Beweis: Sei $\lambda \in \mathbb{C}$ eine Nullstelle von f, so gilt $f(\bar{\lambda}) = \overline{f(\lambda)} = \bar{0} = 0$

$\Rightarrow$ die komplexe Konjugation $j: \mathbb{C} \to \mathbb{C}$ permutiert die Nullstellen von f

$\Rightarrow j|_L : L \to L \subset \mathrm{Aut}_{\mathbb{Q}}(L)$

Da f genau $p-2$ reelle Nullstellen hat, ist $j|_{\text{Nullstellen}}$ eine Transposition.

Sei α eine Nullstelle von f,

dann gilt

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

da $\mathbb{Q} \subset L$ Galoiserweiterung wegen 4.7.11 und 4.5.11 (char $\mathbb{Q} = 0$, also f separabel).

Damit enthält $\mathrm{Aut}_{\mathbb{Q}}(L)$ p-Sylowgruppen der Ordnung p, also einen p-Zykel.

Mit 5.2.9 folgt $\mathrm{Aut}_{\mathbb{Q}}(L) \cong S_p$. □

5.2.11 Korollar

$f = x^5 - 4x + 2 \in \mathbb{Q}[x]$

ist über $\mathbb{Q}$ nicht durch Radikale auflösbar.

Beweis:

Wegen des Eisensteinkriteriums 4.3.9 ist f irreduzibel über $\mathbb{Z}$ und wegen 4.3.10 auch über $\mathbb{Q}$.

Es gilt für $t \in \mathbb{R}$:

t	-2	-1	1	2
$f(t)$	-22	5	-1	26

Aus dem Zwischenwertsatz folgt dann, daß f mindestens 3 reelle Nullstellen besitzt.

$f' = 5x^4 - 4$

besitzt zwei reelle Nullstellen

$x = \pm \sqrt[4]{\frac{4}{5}}$, daher gibt es nur 2 lokale Extrema und daher höchstens 3 reelle Nullstellen.

Damit hat f genau zwei nicht-reelle Nullstellen.

Aus Abel-Ruffini 5.2.10 folgt, daß für den Zerfällungskörper L von f gilt $\mathrm{Aut}_{\mathbb{Q}}(L) \cong S_5$.

Wegen 1.6.6 ist $\mathrm{Aut}_{\mathbb{Q}}(L)$ nicht auflösbar. Wegen 5.2.3 ist f nicht durch Radikale auflösbar.

Bemerkung:

Daraus folgt, daß es für Polynome

vom Grad ≥ 5 keine allgemeinen Formeln für die Nullstellen wie die Cardano-Formeln geben kann.
Auch wenn für einzelne Polynome (siehe 5.2.6) solche Formeln gibt, so gibt es aber auch welche, für die es keine gibt (5.2.11), so daß es keine allgemeingültigen geben kann.

Notizen zoom-meeting 24.7.

zu Gruppen:

1. Operationen $G \times M \to M$

2. Konjugation $G \times G \to G : (g,h) \mapsto ghg^{-1}$

3. Konjugation M = Menge (aller) Untergruppen von G

$G \times M \to M : (g,U) \mapsto gUg^{-1}$

2. + 3. sind Spezialfälle von 1.

Operation	Stabilisator	Bahn
2. Konjugation	Zentralisator	Konjugationsklasse
3. "	Normalisator	"

$$\text{Zentrum} = \{g \mid hg = gh \ \forall h \in G\}$$

Bsp: $G = S_3$ 2. Konjugationsklasse von $(12) = \{(12),(23),(13)\}$

3. $A_3 = \{id, (123), (132)\}$ Konjugationsklasse von $A_3 =$

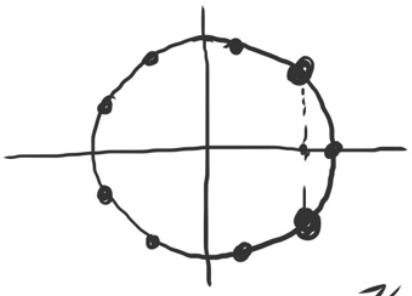
$\{A_3\}$

zu Körpern:

K Zfkp von $x^9 - 1 / \mathbb{Q}$.

$\mathbb{Q} \subset K$ Galoiserweiterung

$K = \mathbb{Q}(\zeta) \qquad \zeta = e^{\frac{2\pi i}{9}}$



$\varphi_k : \zeta \mapsto \zeta^k$ invertierbar $\Leftrightarrow$ k Einheit in $\mathbb{Z}_9$

$\varphi_k \mapsto k$, $\mathrm{Aut}_{\mathbb{Q}}(K) \xrightarrow{\cong} \mathbb{Z}_9^*$

$(\mathbb{Z}_9^*, \cdot) = \{1, 2, 4, 5, 7, 8\} \cong (\mathbb{Z}_6, +) = \langle 1 \rangle$

$(2^2 = 4,\ 2^3 = 8,\ 2^4 = 16 = 7,\ 2^5 = 14 = 5,\ 2^6 = 10 = 1)$

$\langle 2 \rangle$

$2 \cdot 2 = 4$

$2 \cdot 2 \cdot 2 = 8$

1

$2 = 1+1$

$3 = 1+1+1$

$\mathbb{Z}_6$

$\mathbb{Z}_2 \cong \langle 3 \rangle$ $\qquad$ $\mathbb{Z}_3 \cong \langle 2 \rangle$

$\{0\}$

$\mathbb{Z}_6 \cong \mathrm{Aut}_{\mathbb{Q}}(K)$

$\mathbb{Z}_2 \cong \langle \varphi_8 \rangle = U_2$ $\qquad$ $\langle \varphi_4 \rangle \cong \mathbb{Z}_3 = U_1$

$\{id\}$

(*) Minpoly$(a) = x^3 - 3x + 1$ (Nullstellensatz) $\Rightarrow \mathbb{Q}(a) = F_2$

$\mathbb{Q}$

$\mathrm{Fix}(U_2) = F_2$ $\qquad$ $F_1 = \mathrm{Fix}(U_1)$

K

$U_1 = \mathrm{Aut}_{F_1}(K)$

$[K : F_1] = |U_1| = 3 \Rightarrow [K : F_1] \cdot \underbrace{[F_1 : \mathbb{Q}]}_{3} = [K : \mathbb{Q}] = |\mathrm{Aut}_{\mathbb{Q}}(K)| = |\mathbb{Z}_6| = 6$

$\varphi_4(\zeta^3) = (\zeta^3)^4 = \zeta^{12} = \zeta^3 = e^{2\pi i/3}$

$\Rightarrow F_1 = \mathbb{Q}(\zeta^3)$ Minpoly$(\zeta^3) = \frac{x^3 - 1}{x - 1}$

$[F_2 : \mathbb{Q}] = 3.$ $\qquad (\zeta^3)^8 = \zeta^{64} = \zeta$ Sei

$a = \zeta + \zeta^8 \Rightarrow \varphi_8(a) = a \Rightarrow \mathbb{Q}(a) \subset F_2$ (*)