Inhaltsverzeichnis

Kapitel 1

Gruppen

1.1 Definitionen

Definition 1.1.1. Eine Gruppe ist eine Menge G zusammen mit einer Abbildung (Gruppenoperation)

$$\cdot\colon G \times G \to G$$

s.d.

1. Assoz:

$$\forall g, h, k \in G\colon (g \cdot h) \cdot k = g \cdot (h \cdot k)$$

2. Eins:

$$\exists e \in G\colon \forall g \in G\colon e \cdot g = g = g \cdot e$$

3. Inverse:

$$\exists \text{Abb. } ()^{-1}\colon G \to G\colon \forall g \in G\colon g \cdot g^{-1} = e = g^{-1} \cdot g$$

Daraus kann man direkt folgern: e ist eindeutig, $()^{-1}$ ist eindeutig, $()^{-1}$ ist bijektiv, $e^{-1} = e$, $(g \cdot h)^{-1} = h^{-1}g^{-1}$.

Eine abelsche Gruppe ist eine Gruppe G s.d.

$$\forall g, h \in G\colon g \cdot h = h \cdot g$$

Notation: Für abelsche Gruppen schreibt man häufig „+“statt „$\cdot$“.

Beispiel 1.1.2. Für $\mathbb{Z}/3\mathbb{Z}$ können wir die Multiplikation durch eine Tabelle beschreiben. Es gibt die Elemente:

$$\underline{0} = 0 + 3\mathbb{Z}$$
$$\underline{1} = 1 + 3\mathbb{Z}$$
$$\underline{2} = 2 + 3\mathbb{Z}$$

und die Multiplikationstabelle:

$b\backslash a$	$\underline{0}$	$\underline{1}$	$\underline{2}$
$\underline{0}$	$\underline{0}$	$\underline{1}$	$\underline{2}$
$\underline{1}$	$\underline{1}$	$\underline{2}$	$\underline{0}$
$\underline{2}$	$\underline{2}$	$\underline{0}$	$\underline{1}$

Beispiel 1.1.3.

1. k : Körper, V : k-Vektorraum
   - $(V, +)$ ist eine Gruppe
   - $\mathrm{GL}(n, K) = \{$invertierbare lineare Abbildung mit Komposition als Gruppenop.$\}$ ist eine Gruppe
2. $\mathbb{R}^n$ mit Skalarprodukt
$$(x, y) = \sum_{i=1}^{n} x_i y_i$$
und Isometrien, also Abb. $\mathbb{R}^n \to \mathbb{R}^n$ s.d.
$$\forall x, y \in \mathbb{R}^n \colon (f(x), f(y)) = (x, y)$$
Folgerungen*:
   - f ist bijektiv.
   - f ist linear, d.h. es gibt lin. Abb. $A \colon \mathbb{R}^n \to \mathbb{R}^n$, $b \in \mathbb{R}^n$ s.d. $f(x) = Ax + b$.
3. Isometrien von Punktmengen im $\mathbb{R}^n$, z.B.: „Was sind alle Isometrien die ein Quadrat im $\mathbb{R}^2$ fix lassen?“(es gibt 8).
4. Die symmetrische Gruppe S_n also die Bijektionen von $\{1, \ldots, n\}$ auf sich selbst.

Definition 1.1.4. Seien G, H Gruppen. Ein Gruppenhomomorphismus von G nach H ist eine Abbildung $\varphi \colon G \to H$ s.d.
$$\forall x, y \in G \colon \varphi(x \cdot y) = \varphi(x) \cdot y$$
Folgerungen: $\varphi(e) = e$ und $\forall g \in G \colon \varphi(g^{-1}) = \varphi(g)^{-1}$

Beispiel 1.1.5.

- $$\mathbb{Z}/3\mathbb{Z} \to S_{\{0,1,2\}} \qquad a + 3\mathbb{Z} \mapsto (x \mapsto (x + a) \mod 3)$$
  ist Gruppenhomomorphismus. (Warum?)
- $$\psi \colon S_{0,1,2} \to \mathbb{Z}/3\mathbb{Z} \qquad \sigma \mapsto \sigma(0) + 3\mathbb{Z}$$
  erfüllt zwar $\psi \circ \varphi = \mathrm{id}_{\mathbb{Z}/3\mathbb{Z}}$ aber ist kein Gr.hom.

1.2 Isomorphiesätze

Definition. Eine Teilmenge $M \subset G$ heißt Untergruppe, falls:

- $e \in M$ (oder $M \neq \emptyset$)
- $\forall a, b \in M : a \cdot b \in M$
- $\forall a \in M : a^{-1} \in M$

Schreibe $M \leq G$.
Für $\varphi : G \to H$ heißt:

$$\operatorname{im} \varphi = \{\varphi(a) | a \in G\} \subset H \text{ das Bild von } \varphi$$
$$\ker \varphi = \{a \in G | \varphi(a) \in G\} \subset H \text{ das Bild von } \varphi$$

Die Mengen $\operatorname{im} \varphi$ und $\ker \varphi$ sind Untegruppen.

Definition. Eine Untergruppe $M \leq G$ heißt normal, falls:

$$\forall g \in G, m \in M : gmg^{-1} \in M$$

Bemerkung. $\ker \varphi$ ist normal.
Sei $\mathbb{N} \leq G$ normal. Setze für $x, y \in G$:

$$x \sim y :\Leftrightarrow \exists n \in \mathbb{N} : x = yn$$

Sei G/N die Menge der Äquivalenzklassen bzgl. $\sim$. Schreibe aN für die Klasse von $a \in G$.

Satz 1.2.1. *Die Faktorgruppen von G zu N ist*

- *als Menge: G/N*
- *Gruppenoperation.*

$$G/N \times G/N \to G/N \qquad (aN, bN) \mapsto (a \cdot b)N$$

Diese Operation ist wohldefiniert (d.h. unabh. von der Wahl von a und b in aN, bN und ergibt eine Gruppe.

Bew.: Übung
Notation: Seien A, B Teilmengen einer Gruppe G, $x \in G$:

$$xA = \{x \cdot a | a \in A\} \subset G$$
$$AX = \{a \cdot x | a \in A\} \subset G$$
$$AB = \{a \cdot b | a \in A, b \in B\} \subset G$$

Ist $H \leq G$ eine UG und $x \in G$, so heißt xH die x enthaltende Linksnebenklasse und Hx die x enthaltende Rechtsnebenklasse.
Beh: Sei G eine Gruppe, $H \leq G$. Es sind äquivalent:

1. H ist normal
2. für alle $x \in G$: $xH = Hx$

1)⇒ 2)
Es gilt $xH \subset Hx$, denn:

$$y \in xH \Leftrightarrow \exists h \in H \colon y = xh = \underbrace{(xhx^{-1})}_{\in H} x \in Hx$$

$xH \supset Hx$ genauso.
2)⇒ 1) so ähnlich

Bemerkung.

$$xH \cap yH = \begin{cases} xH & x \in yH \\ \emptyset & \text{sonst} \end{cases}$$

Insb.: $x \sim y :\Leftrightarrow x \in yH$ ist eine Äquivalenzrelation.

Beispiel. Sei V ein k-Vektorraum, dann betrachten wir die Gruppe $(V, +)$ $U \subset V$ ein Unter-VR (insb. Untergruppe)

$$x + U = \{x + u | u \in U\}$$

Bemerkung. Die Faktorgruppe G/N ist als Menge gerade die Menge der Links- oder Rechtsnebenklassen:

$$G/N = \{xN | x \in G\} = \{Nx | x \in G\}$$

Satz 1.2.2. *Seien G, N wie in 1.1.1. Die natürliche Projektion*

$$\pi \colon G \to G/N \qquad x \mapsto xN$$

ist ein Gr.hom.

Bew.:

$$\pi(ab) = (ab)N = (aN) \cdot (bN) = \pi(a)\pi(b)$$

□

Beispiel. Sei V ein k-VR, U ein U-VR, dann ist V/U ein Quotientenraum, Faktorgruppen mit Gr.op. $+$

- $3\mathbb{Z} \subset \mathbb{Z}$ ist normale UG, $Z/3\mathbb{Z}$ ist Faktorgruppe

Die universelle Eigenschaft von G/N:

Satz 1.2.3. *Seien G, H: Gruppen, $N \leq G$ normal. Für alle Gr.hom $\varphi \colon G \to H$ mit $N \subset \ker \varphi$ gibt es genau eine Abb. $\overline{\varphi} \colon G/N \to H$, s.d. $\overline{\varphi} \circ \pi = \varphi$.*

Bew.:

- Eindeutigkeit von $\overline{\varphi}$: klar, da π surjektiv ist, ist $\overline{\varphi}$ auf jedem Element von G/N schon festgelegt.
- Existenz von $\overline{\varphi}$: Wir wollen als Definition nehmen: $\overline{\varphi}(aN) := \varphi(a)$ ist. Dafür ist die Repräsentantenunabhängigkeit von $a \in G$ zu zeigen.
  Beh.: Für $a, b \in G$ mit $aN = bN$ gilt $\varphi(a) = \varphi(b)$.
  ⌜

$$aN = bN \Leftrightarrow \pi(a) = \pi(b) \Leftrightarrow \pi(ab^{-1}) = e \Leftrightarrow ab^{-1} \in \ker \pi = N$$
$$\Rightarrow ab^{-1} \in \ker \varphi \Leftrightarrow \varphi(a) = \varphi(b)$$

  ⌟

- $\overline{\varphi}$ ist ein Gr.hom.:

$$\overline{\varphi}(aN \cdot bN) \overset{Def.\ \pi}{=} \overline{\varphi}(\pi(a)\pi(b)) = \overline{\varphi(\pi(ab))} = \varphi(ab) = \varphi(a)\varphi(b)$$
$$= \overline{\varphi}(\pi(a))\overline{\varphi}(\pi(b)) = \overline{\varphi}(aN)\overline{\varphi}(bN)$$

□

Satz 1.2.4. *(Erster Isomorphiesatz) Sei $\varphi\colon G \to H$ ein Gr.hom.. Dann ist*

$$\overline{\varphi}\colon G/\ker \varphi \to \operatorname{im} \varphi$$

ein Gruppeniso.

Bew.:

- $\overline{\varphi}$ existiert nach 1.2.3 mit $N = \ker \varphi$
- surj., da φ surj. auf $\operatorname{im} \varphi$
- **Beh.:** ψ inj. $\Leftrightarrow \ker \psi = \{e\}$
  Setze $N = \ker \varphi$

  $$\overline{\varphi}(xN) = e \Leftrightarrow \varphi(x) = e \Leftrightarrow x \in \ker \varphi\,(= N) \Leftrightarrow xN = N\,(= eN)$$

  Also $\ker \overline{\varphi} = \{eN\}$. Nach Beh. ist $\overline{\varphi}$ injektiv.

□

Beispiel.

$$G = \mathbb{Z} \times \mathbb{Z} \qquad N = \{a(1,2) + b(2,1) | a, b \in \mathbb{Z}\}$$

Betrachte

$$\varphi\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \qquad (m,n) \mapsto m + n$$
$$\psi\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \qquad (m,n) \mapsto m + n + 3\mathbb{Z}$$

Gibt es $\overline{\varphi}$ bzw. $\overline{\psi}$?
Da $\varphi((1,2)) = 3 \neq 0 \in \mathbb{Z}$, gibt es kein $\overline{\varphi}$ wie vorher. Es gilt aber

$$\psi(a(1,2) + b(2,1)) = a\psi((1,2)) + b\psi((2,1)) = a \cdot 3 + b \cdot 3 + 3\mathbb{Z} = 0 + 3\mathbb{Z}$$

also $N \subset \ker \psi$ und es gibt

$$\overline{\varphi} \colon G/N \to \mathbb{Z}/3\mathbb{Z} \qquad \overline{\varphi}((m,n) + N) = m + n + 3\mathbb{Z}$$

Weiter: $\overline{\varphi}$ ist surjektiv ($\operatorname{im} \psi = \mathbb{Z}/3\mathbb{Z}$) dann folgt mit 1.2.4

$$\tilde{\psi}\mathbb{Z} \times \mathbb{Z}/\ker \psi \to \operatorname{im} \psi = Z/3\mathbb{Z}$$

ist ein Gr. iso.. Man kann überlegen: $\ker \psi = N$, dazu der Tipp:

$$N = \{a(3,0) + b(1,2) | a, b \in \mathbb{Z}\}$$
$$\mathbb{Z} \times \mathbb{Z} = \{a = (1,0) + b(1,2) | a, b \in \mathbb{Z}\}$$

Insgesamt folgt $\overline{\psi} \colon G/N \to \mathbb{Z}/3\mathbb{Z}$ ist Gr.isom.

1.3 Produkte und Erweiterungen

Definition. Sei Λ eine Menge, $(G_\lambda)_{\lambda \in \Lambda}$ eine Familie von Gruppen. Das äußere direkte Produkt ist das Produkt

$$\prod_{\lambda \in \Lambda} G_\lambda$$

der unterliegenden Mengen mit Gruppenoperation:

Definition:

$$(g_\lambda)_{\lambda \in \Lambda} \cdot (h_\lambda)_{\lambda \in \Lambda} := (g_\lambda \cdot h_\lambda)_{\lambda \in \Lambda}$$

Eins:

$$(e \in G_\lambda)_{\lambda \in \Lambda}$$

Inv.:

$$((g_\lambda)_{\lambda \in \Lambda})^{-1} = (g_\lambda^{-1})_{\lambda \in \Lambda}$$

Bemerkung. Dies definiert eine Gruppe

Notation: Für $\Lambda = \{1, 2, \ldots, n\}$ schreibe

$$\prod_{\lambda \in \Lambda} G_\lambda = G_1 \times G_2 \times \cdots \times G_n$$

Bemerkung. Es gibt Gr.hom.

$$i_\mu \colon G_\mu \to \prod_{\lambda \in \Lambda} G_\lambda \qquad g \mapsto (h_\lambda)_{\lambda \in \Lambda} \qquad h_\lambda = \begin{cases} g; & \lambda = \mu \\ e; & \lambda \neq \mu \end{cases}$$

$$i_\mu \colon \prod_{\lambda \in \Lambda} G_\lambda \to G_\mu \qquad (h_\lambda)_{\lambda \in \Lambda} \mapsto h_\mu$$

und im i_μ ist eine normale UG von $\prod_{\lambda\in\Lambda} G_\lambda$.

Notation: G Gruppe, $S \subset G$ Teilmenge

$$\langle S\rangle = \bigcap\{H \leq G | S \subset H\}$$

Dies ist die kleinste UG, die S enthält (z.B. $\langle\emptyset\rangle = \{e\}$. Explizit:

$$\langle S\rangle = \{s_1^{\varepsilon_1}\cdots s_n^{\varepsilon_n} | n \geq 0, e_i \in \{\pm 1\}, s_i \in S\}$$

$\langle S\rangle$ heißt die von S erzeugte Untergruppe von G

Es gilt:

$$i_\mu(G_\mu) \cap \langle \bigcup_{\lambda\neq\mu} i_\lambda(G_\lambda)\rangle = \{e\}$$

und falls Λ endlich:

$$\prod_{\lambda\in\Lambda} G_\lambda = \left\langle \bigcup_{\lambda\in\Lambda} i_\lambda(G_\lambda)\right\rangle$$

Warnung: Dies ist falsch für Λ unendlich.

Definition. Sei H eine Gruppe und $(H_\lambda)_{\lambda\in\Lambda}$ normale UG von H und Λ endlich. Gilt

$$\left\langle \bigcup_\lambda H_\lambda\right\rangle = H \qquad \wedge \qquad H_\mu \cap \left\langle \bigcup_{\lambda\neq\mu} H_\lambda\right\rangle = \{e\}$$

so heißt H das innere direkte Produkt der H_λ.

Folgerungen:

a) Für $\lambda \neq \mu$ gilt:

$$\forall l \in H_\lambda m \in H_\mu \colon lm = ml$$

denn:

$$l\underbrace{(ml^{-1}m^{-1})}_{\in H_\lambda} \in H_\lambda \qquad \underbrace{(lml^{-1})}_{H_\mu} m \in H_\mu \Rightarrow lml^{-1}m^{-1} = e$$

b) Die Abbildung

$$\prod_{\lambda\in\Lambda} H_\lambda \to H \qquad (h_\lambda)_{\lambda\in\Lambda} \mapsto \prod_{\lambda\in\Lambda} h_\lambda$$

Wobei $\prod_{\lambda\in\Lambda} h_\lambda$ für das Produkt in irgendeiner Reihenfolge steht, die nach *a)* egal ist. ist ein Gr.iso., denn

Hom.: wegen a)

Sur.: da

$$\langle \bigcup_{\lambda\in\Lambda} H_\lambda \rangle = H$$

Inj.: da

$$\prod_\lambda h_\lambda = e \Leftrightarrow \forall \mu \in \Lambda \colon h_\mu^{-1} = \prod_{\lambda\neq\mu} h_\lambda \in \langle \bigcup_{\lambda\neq\mu} H_\lambda \rangle \cap H_\mu$$

also ist $h_\mu = e$ für jedes $\mu \in \Lambda$.

Satz 1.3.1. *Sei G eine Gruppe und $H_\lambda \leq G$ mit $\lambda \in \Lambda$, Λ endlich. Dann sind äquivalent:*

1. *Die H_λ sind normal und G ist ~~inneres~~ direktes Produkt der H_λ*
2. *Es gilt:*

   i)

   $$\forall \lambda \neq \mu, l \in H_\lambda, m \in H_\mu \colon lm = ml$$

   ii)

   $$\forall g \in G \colon \exists! (g_\lambda)_{\lambda\in\Lambda} \colon g = \prod_{\lambda\in\Lambda} g_\lambda$$

   Wobei nach i) die Reihenfolge egal ist.

Bew.: 1) $\Rightarrow$ 2)

i) Folg. a)

ii) Folg. b) Bijektivität

2) $\Rightarrow$ 1) Damit H_μ normal ist, ist z.z.:

$$\forall g \in G \colon h \in H_\mu \colon ghg^{-1} \in H_\mu$$

Nach ii) $g = \prod_\lambda g_\lambda$, also:

$$ghg^{-1} \overset{i)}{=} g_\mu h g_\mu^{-1} \in H_\mu$$

$$\left\langle \bigcup_{\lambda\in\Lambda} H_\lambda \right\rangle = G$$

klar nach ii) Existenz.

$$H_\mu \cap \left\langle \bigcup_{\lambda\neq\mu} H_\lambda \right\rangle = \{e\}$$

klar nach ii) Eindeutigkeit. □

Definition. Sei $N \leq G$ normal und $H \leq G$ mit

$$NH = G$$

es gilt $NH = HN$ (Warum?)

$$N \cap H = \{e\}$$

in diesem Fall heißt G das innere semidirekte Produkt von N und H, schreibe $N \rtimes H$.

Bemerkung.

- Jedes $g \in G$ lässt sich eindeutig als $g = nh$ schreiben $n \in N, h \in H$.

  Sei auch $g = n'h'$. Dann $N \cap H = \{e\}$

  $$nh = n'h' \Rightarrow {n'}^{-1}n = h'h^{-1} \Rightarrow {n'}^{-1}n = e = h'h^{-1}$$

Notation: Ein Gruppeniso. $G \to G$ heißt Automorphismus von G. Die Menge der Automorphismen nennt man $\mathrm{Aut}G = \{\varphi\colon G \to G | \varphi \text{Autom.}\}$ ist selber eine Gruppe mit Gr.op. Komposition von Abbildungen.

Beispiele:

$$\mathrm{Aut}((\mathbb{Z}, +)) = \{\mathrm{id}, -\mathrm{id}\} \simeq \mathbb{Z}/2\mathbb{Z}$$
$$\mathrm{Aut}((\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)) \simeq S_3 \mathrm{Aut}((\mathbb{Z}/N\mathbb{Z}, +)) = ?$$

- Jedes $h \in H$ gibt einen Autom. von N:

  $$\gamma_h : \begin{array}{l} N \to N \\ n \mapsto hnh^{-1} \end{array}$$

  Dies ergibt einen Gruppenhom. $\begin{array}{ll} H & \to \mathrm{Aut}N \\ h & \mapsto \gamma_h \end{array}$ Es gilt

  $$(nh)(n'h') = nhn'h' = n(hn'h^{-1})hh' = n\gamma_h(n')hh'$$

- Falls $nh = hn \quad \forall n \in N, h \in H$ so $\gamma_h = \mathrm{id}$ und $N \rtimes H$ ist gleich dem direkten Produkt $N \times H$ (Satz 1.) Ferner $hn = nh \Leftrightarrow \gamma_h(n) = n$

- Umgekehrt: Gegeben Gruppen N, H (nicht notw. UG einer vorgegeb. Gruppe) und ein Gr. Hom., $\gamma : H \to \mathrm{Aut}(N)$, so definieren wir das (äußere) semidirekte Produkt $N \rtimes_\gamma H$ als

  - Menge $N \times H$
  - Verknüpfung $(n, h) * (n', h') := (n\gamma_h(n'), hh')$

  Dies ist eine Gruppe (Warum, was ist das Inverse?)

- Äußeres und inneres semidirektes Produkt sind isom. via:

$$N \rtimes_\gamma H \to N \rtimes H \qquad (n,h) \mapsto n \cdot h$$

$H, N \leq G$, N normal, $NH = G$, $N \cap H = \{e\}$

Definition. Sei $\mathbf{1}$ die Gruppe mit einem Element. Seien A_i Gruppen und $(i \in \mathbb{Z})$

$$\ldots \to A_{i-1} \xrightarrow{\varphi_{i-1}} A_i \xrightarrow{\varphi_i} A_{i+1} \xrightarrow{\varphi_{i+1}} \ldots$$

φ_i Gr. Hom Dies nennt man eine **Sequenz von Gruppen**, falls für jedes i in

$$\operatorname{im} \varphi_{i-1} \subset \ker \varphi_i \quad (*)$$

Die Sequenz heißt exakt in A_i, falls $(*)$ mit „=“. Die Sequenz heißt insgesamt exakt, falls sie exakt in allen A_i ist.

Eine kurze exakte Sequenz (von Gruppen) ist eine ex. Seq. der Form

$$\mathbf{1} \to A \xrightarrow{\iota} B \xrightarrow{\pi} C \to \mathbf{1} \quad (**)$$

Das heißt:

- exakt in A $\quad \Leftrightarrow \iota$ injektiv
- exakt in C $\quad \Leftrightarrow \pi$ surjektiv
- exakt in B $\quad \Leftrightarrow \operatorname{im} \iota = \ker \pi$

Nach Satz 1.2.2: $\underbrace{\operatorname{im} \pi}_{=C} \cong B / \underbrace{\ker \pi}_{\iota(A)}$

Also $C = B/\iota(A)$

Man nennt B in $(**)$ auch eine Gruppenerweiterung von A durch C.

Bemerkung.
Für $G = N \rtimes H$ ist

$$\begin{array}{ccccc} 1 \to N & \longrightarrow & N \rtimes H & \longrightarrow & H \to 1 \\ n \mapsto (n,e) & & (n,h) \mapsto h & & \end{array}$$

eine kurze exakte Seq. Wir sagen ein kurze exakte Seq. spaltet, falls es einen Gruppenhom. $\sigma\colon C \to B$ gibt, s.d. $[C \xrightarrow{\sigma} B \xrightarrow{\pi} C] = [C \xrightarrow{\mathrm{id}} C]$, d.h. $\pi\sigma = \mathrm{id}$. Schematisch:

$$(1) \qquad 1 \to A \xrightarrow{\iota} B \underset{\pi}{\overset{\sigma}{\leftrightarrows}} C \to 1$$

Satz 1.3.2. *Ist*

$$1 \to A \xrightarrow{\iota} B \underset{\pi}{\overset{\sigma}{\leftrightarrows}} C \to 1$$

eine kurze exakte Sequenz, die durch σ spaltet, so gilt

$$B \simeq A \rtimes_\gamma C$$

mit $\gamma\colon C \to \mathrm{Aut}(A)$ definiert via $(a \in A, c \in C)$

$$\underbrace{\iota(\gamma_c(a))}_{\in A} = \underbrace{\sigma(c)\iota(a)\sigma(c)^{-1}}_{\in \operatorname{im} \iota}$$

Bew.:
γ ist ein Gr. hom..
Setze $\begin{array}{rccc} \varphi\colon & A \rtimes_\gamma C & \to & B \\ & (a,c) & \mapsto & \iota(a)\sigma(c) \end{array}$
Dies ist ein Gr. Hom. (warum?)

Injektiv: Sei $\varphi(a,c) = e$. Dann

$$\pi(\varphi(a,c)) = \pi(\iota(a)\sigma(c)) = \overbrace{\pi(\iota(a))}^{=e}\underbrace{\pi(\sigma(c))}_{=c} = c$$

Aber nach $\pi(\varphi(a,c)) = \pi(e) = e$, also $c = e$
Dann auch $a = e$, da ι injektiv. Insgesamt: $(a,c) = e$

Surjektiv: Sei $b \in B$ beliebig
Beh.: $b\sigma(\pi(b^{-1})) \in \ker \pi$
⌜

$$\pi(b\sigma(\pi(b^{-1}))) = \pi(b)\underbrace{\pi(\sigma}_{\mathrm{id}_c}(\pi(b^{-1}))) = \pi(b)\pi(b^{-1}) = e$$

⌟

Da Seq. exakt in B ist, gibt es $a \in A$, s. d. $\iota(a) = b\sigma(\underbrace{\pi(b^{-1})}_{\in C})$
Also

$$b = \iota(a)\sigma(\pi(b)) = \varphi(a, \pi(b))$$

□

Beispiel. 1. Die verallgemeinerte Diedergruppe. Sei A eine abelsche Gruppe, setze

$$D_A = \{(a,\varepsilon) | a \in A, \varepsilon \in \{\pm 1\}\}$$

mit Verknüpfung

$$(a,\varepsilon) * (b,\nu) = (ab^\varepsilon, \varepsilon\nu)$$

Dann ist

$$\begin{array}{ccc} \mathbf{1} \to A \xrightarrow{\iota} & & D_A \xrightarrow{\pi} \{\pm 1\} \to \mathbf{1} \\ a \mapsto (a,1) & & (a,\varepsilon) \mapsto \varepsilon \end{array}$$

Also

- D_A ist Erweiterung von A durch $\{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z}$
- Seq. spaltet, also $D_A \simeq A \rtimes_\gamma \{\pm 1\}$

Die DIedergruppe ist $D_{2k} = D_{\mathbb{Z}/k\mathbb{Z}}$ und beschreibt Sym. des regelmäßigen k-Ecks im $\mathbb{R}^2$. $\mathbb{Z}/k\mathbb{Z}$: Rotationen, $\{\pm 1\}$ Spiegelungen an der x-Achse.

2. GL_n **und** SL_n

   - k: Körper
   - $\mathrm{GL}_n(k)$: inv. lin. Abb. $k^n \to k^n$
   - $\mathrm{SL}_n(k)$: inv. lin. Abb. $k^n \to k^n$ mit $\det 1$

   Schreibe $k^* := k \setminus \{0\}$ Die Sequenz

   $$1 \to \mathrm{SL}_n(k) \to \mathrm{GL}_n(k) \xrightarrow{\det} k^* \to 1$$
   $$M \mapsto M$$

   ist exakt (warum?)

   $$\sigma\colon k^* \to \mathcal{R}_n(k)$$
   $$\lambda \mapsto \begin{pmatrix} \lambda & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$$

   ist Gr. Hom. mit $\det(\sigma(\lambda)) = \lambda$

   Somit $\mathrm{GL}_n(k) = \mathrm{SL}_n(k) \rtimes_\gamma k^*$

1.4 Die symmetrische Gruppe

Definition. Sei $M \neq \emptyset$ eine Menge. Die symmetrische Gruppe in M ist

$$S_M := \{ \text{ bijektive Abbildungen von } M \text{ nach } M \ \}$$

Speziell für $M = \{1, 2, \ldots, n\}$ schreibt man $S_n := S_M$.

Satz 1.4.1. *Jede Gruppe ist zu einer Untergruppe einer symmetrischen Gruppe isomorph.*

Bew.: Betrachte zu einer beliebigen Gruppe G die Linkswirkung auf sich selbst:

$$\begin{array}{rcll} \rho\colon G & \to & \mathrm{Map}(G,G) & \\ g & \mapsto & \rho_g & \text{mit } \rho_g(h) = gh \end{array}$$

Es gilt

$$\rho_g \circ \rho_h = \rho_{gh} \qquad \rho_e = \mathrm{id}_G$$

Somit:

$$\rho_{g^{-1}} \circ \rho_g = \rho_e = \mathrm{id}_G = \rho_g \circ \rho_{g^{-1}}$$

also sogar $\rho_g \in S_G \subset \mathrm{Map}(G,G)$ und ρ ist ein Gruppenhomomorphismus.
Beh.: ρ ist injektiv.

$$\ker \rho = \{g \in G | \rho_g = \mathrm{id}\}$$
$$\rho_g = \mathrm{id} \Leftrightarrow \forall x \in G\colon gx = x \Leftrightarrow g = e$$

⌟

Somit ist $\rho\colon G \to \mathrm{im}\,\rho$ ein Isom. □

Definition. Sei G eine Gruppe. Die Ordnung von G ist die Anzahl der Elemente in G, schreibe $|G|$, z.B. $|S_n| = n!$ Sei $g \in G$. Die UG $\langle\{g\}\rangle$ (schreibe $\langle g\rangle$) heißt die von g erzeugte zyklische Untergruppe. Die Ordnung von g ist die Ordnung von $\langle g\rangle$

$$\mathrm{ord} g = |\langle g\rangle|$$

Es gilt, für $\mathrm{ord} g = m < \infty$:

$$\mathrm{ord} g = \min\{m \in \mathbb{N} | g^m = e\}$$

G heißt zyklisch, falls es $g \in G$ gibt, mit

$$G = \langle g\rangle$$

(z.B. ist $\mathbb{Z}/4\mathbb{Z}$ zyklisch, da $\langle 1\rangle = \mathbb{Z}/4\mathbb{Z}$)

Definition. Sei $\pi \in S_n$. Der Träger („support“) von π ist

$$\mathrm{supp}(\pi) = \{m \in \{1, \ldots, n\} | \pi(m) \neq m\}$$

zum Beispiel:

$$\mathrm{supp} \begin{pmatrix} 1 & \mathbf{2} & 3 & \mathbf{4} \\ 1 & \mathbf{4} & 3 & \mathbf{2} \end{pmatrix} = \{2, 4\} \in S_4$$

Definition. Gilt $|\mathrm{supp}\,\pi| = k$ und gibt es $m_1, \ldots, m_k \in \{1, \ldots, n\}$, so dass

- $\mathrm{supp}\,\pi = \{m_1, \ldots, m_k\}$
- $\pi(m_i) = m_{i+1} \quad (i < k) \quad , \ \pi(m_k) = m_1$

so heißt π Zyklus der Länge k. Man schreibt

$$\pi = (m_1, \ldots, m_k)$$

Beispiel.

- $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = (1\ 3\ 4) = (3\ 4\ 1) = (4\ 1\ 3)$ ist Zyklus der Länge 3.
- $\pi' = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ ist kein Zyklus, obwohl $\mathrm{supp}\,\pi' = \{1, 2, 3, 4\}$

Ein Zyklus der Länge 2 heißt Transposition, z.B.

$$\pi = \begin{pmatrix} 1 & \mathbf{2} & 3 & \mathbf{4} \\ 1 & \mathbf{4} & 3 & \mathbf{2} \end{pmatrix}$$

Bemerkung. Sind τ, π Permutationen von $\{1, \ldots, n\}$ (also $\tau, \pi \in S_n$) mit disjunkten Trägern, so gilt $\pi \circ \tau = \tau \circ \pi$. (Warum?)

Satz 1.4.2. *Jedes $\pi \in S_n$ kann als Produkt von Zykeln τ_i mit Länge ≥ 2 und disjunkten Trägern geschrieben werden*

$$\pi = \tau_1 \ldots \tau_n$$

Die Zykel τ_i sind bis auf Reihenfolge eindeutig.

Bew.: Sei $\pi \in S_n$ gegeben.

- **Existenz:** Sei $M = \{1, \ldots, n\}$ und betrachte zykl. UG $\langle \pi \rangle \subset S_n$ Wir definieren nun eine Äquivalenzrelation auf M:

  $$m \sim m' \Leftrightarrow \exists \varphi \in \langle \pi \rangle : \varphi(m) = m'$$

  M zerfällt in Äquivalenzklassen $Z_\lambda, \lambda \in \Lambda$:

  $$Z_\lambda \cap Z_\mu = \emptyset \qquad \bigcup_\lambda Z_\lambda = M$$

  Für jedes Z_λ gilt : Sei $m \in Z_\lambda$ bel., dann

  $$Z_\lambda = \{\underset{= m_1}{m}, \underset{= m_2}{\pi(m)}, \ldots, \underset{= m_N}{\pi^{N-1}(m)}\}$$

  Setze $\tau_\lambda = (m_1, \ldots, m_N)$. Es gilt (per Konstruktion)

  - $\pi\big|_{Z_\lambda} = \tau_\lambda\big|_{Z_\lambda}$
  - $\operatorname{supp} \tau_\lambda = Z_\lambda$
  - $\forall \lambda \neq \mu$: $\tau_\lambda\big|_{Z_\mu} = \mathrm{id}_{Z_\mu}$

  (somit $\tau_\lambda \tau_\mu = \tau_\mu \tau_\lambda$ nach Bem.)

  Schreibe

  $$\prod_{\lambda \in \Lambda} \tau_\lambda \quad \text{(Produkt über alle } \tau_\lambda \text{ unabhängig von Reihenfolge)}$$

  Dann gilt für alle $\mu \in \Lambda$

  $$\left(\prod_\lambda \tau_\lambda\right)\Big|_{Z_\mu} = \tau_\mu\big|_{Z_\mu} = \pi\big|_{Z_\mu}$$

  Da $\bigcup Z_\lambda = M$ folgt $\pi = \prod\limits_{\lambda \in \Lambda} \tau_\lambda$

  Da $\tau_\lambda = \mathrm{id}$ falls $|Z_\lambda| = M$ gilt auch

  $$\pi = \prod_{\substack{\lambda \in \Lambda \\ |Z_\lambda| \geq 2}} \tau_\lambda$$

- **Eindeutigkeit:**
  Sei $\pi = \nu_1 \dots \nu_k$ andere Zerlegung. Setze $\Lambda' = \{\lambda \in \Lambda || z_\lambda | > 1\}$. Es gilt

$$\operatorname{supp} \pi = \bigcup_{\lambda \in \Lambda'} Z_\lambda$$

  Auf $\operatorname{supp} \nu_i$ gilt $\pi_{|_{\operatorname{supp} \nu_i}} = \nu_{i|_{\operatorname{supp} \nu_i}}$. Damit ist $\operatorname{supp} \nu_i = Z_{\lambda_i}$ für ein $\lambda_i \in \Lambda'$ und $\nu_i = \tau_{\lambda_i}$.
  Da auch $\operatorname{supp} \pi = \bigcup \operatorname{supp} \nu_i$, definiert $i \mapsto \lambda_i$ Bijektion $\{1, \dots, k\} \to \Lambda'$

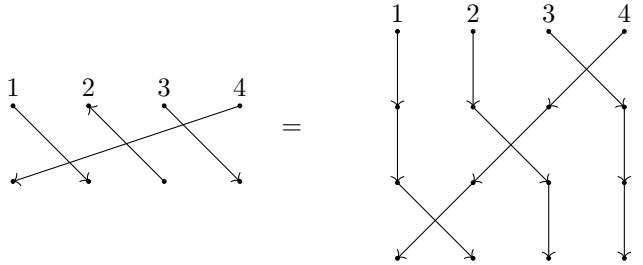
□

Satz 1.4.3. *Die symmetrische Gruppe S_n wird von Transpositionen erzeugt.*

Bew.: Nach 1.4.2 ist es genug, dies Aussage für Zykel zu zeigen. Für Zyklen gilt:

$$(m_1 \ \dots \ m_k) = (m_1 \ m_2)(m_2 \ m_3) \dots (m_{k-1} \ m_k)$$

Beispiel. $(1\ 2\ 3\ 4) = (1\ 2)(2\ 3)(3\ 4)$



Man braucht nicht alle $(i\ j)$ um S_n zu erzeugen:

$$(*) \qquad \langle (1\ 2), (1,3), \dots, (1,n) \rangle = S_n$$

Folgt aus $(i\ j) = (\mathbf{1}\ i)(1\ j)(1\ i)$

$(*)$ $\langle (1\ 2), (2,3), \dots, (n-1,n) \rangle = S_n$

Definition. Das Signum einer Permutation $\pi \in S_n$ ist

$$\operatorname{sgn} \pi = \prod_{\substack{n \geq i \\ j \geq 1}} \frac{\pi(i) - \pi(j)}{i - j}$$

Bemerkung. Sei

$$M = \{(i,j) | i > j \text{ und } \pi(i) < \pi(j)\}$$

Dann $\operatorname{sgn} \pi = (-1)^{|M|}$
⌜

Die Menge $\{\{i,j\} | i > j\}$ enthält jedes ungeordnete Paar $\{i,j\}$ mit $i \neq j$. Das gleiche gilt für

$$\{\{\pi(i), \pi(j)\} | i > j\}$$

Also

$$\prod_{i>j} |\pi(i) - \pi(j)| = \prod_{i>j} |i - j| = \pi(i - j)$$

und damit

$$\operatorname{sgn}(\pi) = \prod_{i>j} \frac{\pi(i) - \pi(j)}{|\pi(i) - \pi(j)|} \overset{(\star)}{=} (-1)^{|M|}$$

$(\star)$ wobei $M := \{i > j | \pi(i) < \pi(j)\}$

⌟

Satz 1.4.4. *a)* $\operatorname{sgn} : S_n \to \{\pm 1\}$ *ist Gr. Hom.*

b) Für jede Transposition τ *gilt:* $\operatorname{sgn}(\tau) = -1$

Bew.:

a) Z.z.: $\operatorname{sgn}(\pi\sigma) = \operatorname{sgn}(\pi)\operatorname{sgn}(\sigma)$

$$\operatorname{sgn}\pi\sigma = \prod_{i>j} \frac{\pi\sigma(i) - \pi\sigma(j)}{i - j} = \prod_{i>j} \frac{\pi\sigma(i) - \pi\sigma(j)}{\sigma(i) - \sigma(j)} \overbrace{\prod_{i>j} \frac{\sigma(i) - \sigma(j)}{i - j}}^{\operatorname{sgn}\sigma}$$

Es gilt

$$\frac{\pi\sigma(i) - \pi\sigma(j)}{\sigma(i) - \sigma(j)} = \frac{\pi\sigma(j) - \pi\sigma(i)}{\sigma(j) - \sigma(i)}$$

Damit

$$\begin{aligned} \prod_{i>j} \frac{\pi\sigma(i) - \pi\sigma(j)}{\sigma(i) - \sigma(j)} &= \prod_{(\star)} \frac{\pi\sigma(i) - \pi\sigma(j)}{\sigma(i) - \sigma(j)} \\ &= \prod_{k>l} \frac{\pi(k) - \pi(l)}{k - l} = \operatorname{sgn}(\pi) \end{aligned}$$

$(\star)$ $\{i, j\} \in$ Menge, die jedes (ungeordnete) Paar $\{i, j\} (i \neq j)$ enthält, wir schreiben $\{\{\sigma^{-1}k, \sigma^{-1}l | k > l\}$.

b)

$$\begin{aligned} \text{Folgt aus} \quad & \operatorname{sgn}(12) = -1 \quad \text{(Warum?)} \\ \text{und} \quad & (ij) = \pi(12)\pi^{-1} \end{aligned}$$

für ein geeignetes $\pi \in S_n$. Denn dann

$$\operatorname{sgn}(ij) = \operatorname{sgn}(\pi(12)\pi^{-1}) \overset{\text{a)}}{=} \operatorname{sgn}(\pi)\operatorname{sgn}(12)\operatorname{sgn}(\pi)^{-1} \quad (\{\pm 1\} \text{ ist abelsch})$$

□

Definition. Die alternierende Gruppe A_n ist der Kern

$$\begin{aligned} A_n &:= \ker(S^n \xrightarrow{\operatorname{sgn}} \{\pm 1\}) \subset S \\ \text{Also} \quad A_n &= \{\pi \in S_n | \operatorname{sgn}(\pi) = 1\} \end{aligned}$$

Bemerkung.

$$\mathbf{1} \to A_n \xrightarrow{\iota} S_n \xrightarrow{\text{sgn}} \{\pm 1\} \to \mathbf{1}$$

ist exakt und spaltet (Wie?)

$$S_n = A_n \rtimes_\gamma \{\pm 1\} \qquad \text{(Welches } \gamma\text{?)}$$

1.5 Operationen auf Mengen

Definition. Eine Operation (oder Wirkung) einer Gruppe G auf einer Menge X ist eine Abb.

$$\cdot : G \times X \to X \qquad (g, x) \mapsto g.x$$

s.d. für alle $x \in X, g, h \in G$:

- $e.x = x$
- $g.(h.x) = (gh).x$

Man nennt dann X auch eine G-Menge

Bemerkung. Äquivalent zur Definition der Wirkung gebe Gruppenhomomorphismus $G \to S_X$ an, via $g \mapsto \rho_g, \quad \rho_g(x) = g.x$ (Warum?)

Beispiel. $\mathbb{R}^2$ und Gruppe der Rotation um $\varphi \in \mathbb{R}$ ($SO(2)$)

Definition. Für $x \in X$ heißt

$$Gx = \{g.x | g \in G\}$$

die Bahn (oder der Orbit) von x unter der Operation von G.

Bemerkung 1.5.1. X ist die disjunkte Vereinigung der Bahnen

$$X = \dot{\bigcup}_{B \text{ Bahnen unter } G} B$$

da $B \cap B' \neq \emptyset \Rightarrow B = B'$ denn

Sei $B = G.x$ und $B' = G.y$ und sei $B \cap B' \neq \emptyset$. Wähle $m \in B \cap B'$. Dann $m = g.x$ und $m = g'.y$ für $g, g' \in G$ geeignet. Somit $y = (g')^{-1}g.x$ und $G.x = G.y$

Definition. Eine Operation von G auf X heißt

- **transitiv**, falls X eine Bahn unter G ist
- **treu**, falls aus $g.x = h.x$ für alle $x \in X$ folgt $g = h$.

(Äquivalent zu treu: Gr. Hom. $G \to S_x$ ist injektiv) (Warum?)

Beispiel.

a) S_n wirkt auf $\{1,\dots,n\}$:

$$\begin{aligned} S_n \times \{1,\dots,n\} &\to \{1,\dots,n\} \\ (\pi, k) &\mapsto \pi(k) \end{aligned}$$

(Wirkung? Transitiv? Treu?)

b) $\mathrm{SO}(n)$ wirkt auf $\mathbb{R}^n$

$$\mathrm{SO}(n) \times \mathbb{R}^n \to \mathbb{R}^n \qquad (M, v) \mapsto Mv$$

c) Eine Gruppe G operiert auf sich

- von **links**:

$$G \times G \to G \qquad (g, x) \mapsto gx$$

- von **rechts**:

$$G \times G \to G \qquad (g, x) \mapsto xg^{-1}$$

(Warum g^{-1} und nicht g?)

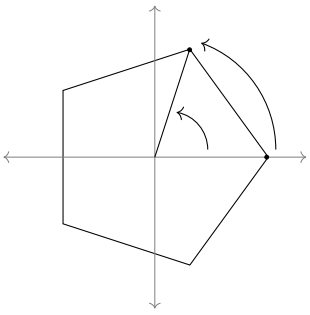
- durch **Konjugation**:

$$G \times G \to G \qquad (g, x) \mapsto gxg^{-1}$$

Die Bahnen unter Konjugation heißen Konjugationsklassen von G.

d) $\mathrm{GL}(V)$ wirkt auf V

D_{2k} wirkt durch Isometrien auf $\mathbb{R}^2$ die ein regelm. k-Eck invariant lassen



e) $H \leq G$ UG. hatten

$$G/H = \{xH | x \in G\}$$

dies ist die Menge der Bahnen unter der Rechtswirkung von H auf G. (**Warnung:** Linksnebenklassen). G operiert auf G/H von links:

$$G \times G/H \to G/H \qquad (g, xH) \mapsto gxH$$

(Warum wohldef.? Warum Wirkung? Transitiv? Treu?)
Genauso

$$H\backslash G = \{Hx | x \in G\}$$

G operiert von rechts auf $H\backslash G$.
Falls H normal ist gilt $H\backslash G = G/H$ (Warum? Gilt die Umkehrung?) .

Satz 1.5.2. *(Satz von Lagrange) Sei $H \leq G$, dann*

$$|G| = |H| \cdot |G/H|$$

wobei $|\cdot| \in \mathbb{N} \cup \{\infty\}$

Bew.: Folgt aus

$$G \overset{1.5.1}{=} \bigcup \{xH | x \in G\} \tag{1.1}$$

disjunkt und $\forall x, y \in G$

$$yx^{-1}.(\cdot)\colon xH \xrightarrow{\sim} yH \text{ ist Bijektion} \tag{1.2}$$

also $|xH| = |yH|$

$$|G| = \sum_{B \in G/H} \overbrace{|B|}^{=|H| \text{ für alle } B} = |H| \cdot |G/H|$$

□

Insbesondere teilt die Ordnung einer Untergruppe die Gruppenordnung.

Definition. Man nennt für $H \leq G$

$$[G : H] := |G/H|$$

den Index von H in G (Es gilt $|G/H| = |H\backslash G|$ Warum?)

Satz 1.5.3. *Für $M \leq N \leq G$, gilt*

$$[G : M] = [G : N][N : M]$$

Bew.: Sei

$$\begin{aligned} \pi\colon G/M &\to G/N \qquad \text{„fein} \to \text{grob“} \\ xM &\mapsto xN \end{aligned}$$

Wohldefiniert? (Warum?)
Es gilt

$$G/M = \dot{\bigcup_{\alpha \in G/N}} \pi^{-1}(\{\alpha\}) \quad \text{disjunkt.}$$

Also

$$|G/M| = \sum_{\alpha \in G/N} |\pi^{-1}(\{\alpha\})|$$

Es gilt $\pi^{-1}(\{N\}) = N/M$. Nach Bsp. e) gibt G Operation auf G/M via:

$$L_x\colon G \times G/M \to G/M \qquad (g, \alpha) \mapsto g\alpha$$

Satz folgt nun aus **Beh.:**

$$L_x\colon N/M \to \pi^{-1}(\{xN\})$$

ist bijektiv.

⌜

Sei $n \in N$. Wir wollen zeigen:

$$L_x(nM) \in \pi^{-1}(\{xN\})$$

Wir haben:

$$\pi(L_x(nM)) = \pi(xnM) = x \underbrace{nN}_{=N} = xN$$

Somit

$$L_x(N/M) \subset \pi^{-1}(\{xN\})$$

Betrachte $L_{x^{-1}}$. Wir wollen zeigen: Für $zM \in \pi^{-1}(\{xN\})$ gilt:

$$L_{x^{-1}}(zM) \in N/M = \pi^{-1}(\{N\})$$
$$\pi(L_{x^{-1}}(zM)) = \pi(x^{-1}zM) = x^{-1}zM = x^{-1}zM = x^{-1}xN = N$$

wegen $\pi(zM) = xN \Rightarrow zN = xN$.
Somit $L_{x^{-1}} \colon \pi^{-1}(\{xN\}) \to N/M$ und da L_x eine Wirkung ist, gilt:

$$L_x \circ L_{x^{-1}} = L_{xx^{-1}} = L_e = \mathrm{id} \qquad L_{x^{-1}} \circ L_X = \mathrm{id}$$

Also $|\pi^{-1}(\{\alpha\})| = |N/M|$ für alle $\alpha \in G/N$. □

Definition. Sei X eine G-Menge und $x \in X$. Der Stabilisator von x ist

$$G_x = \{g \in G | g.x = x\}$$

G_x ist eine UG. (Warum?) Normal?

Satz 1.5.4. *(**Bahnformel**) Sei X eine G-Menge und $x \in X$, dann gilt:*

$$|G.x| = [G : G_x]$$

Bew.: Betrachte die Abbildung

$$f \colon G \to G.x \subset X \qquad g \mapsto g.x$$

Beh.: Gilt $gG_x = hG_x$, so folgt $f(g) = f(h)$

Falls $gs = h$ $(s \in G_x)$, so gilt

$$f(h) = h.x = (gs).x = g.(s.x) = g.x = f(g)$$

Wir bekommen

$$\overline{f} \colon G/G_x \to G.x \qquad gG_x \mapsto g.x$$

$\overline{f}$ ist:

- **surjektiv:** klar, da f surjektiv

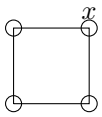
- **injektiv:**

$$\overline{f}(gG_x) = \overline{f}(hG_x) \Leftrightarrow g.x = h.x \Leftrightarrow (h^{-1}g).x = x \Leftrightarrow h^{-1}g \in G_x \Leftrightarrow gG_x = hG_x$$

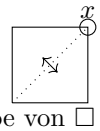
□

Korollar. $|G.x| \cdot |G_x| = |G|$ *also (Länge des Orbits von x)·(Ordnung des Stabilisators von x)=(Ordnung der Gruppe)*

Anwendung: Ordnung von Symmetriegruppen z.B.

1. **Quadrat** im $\mathbb{R}^2$ 

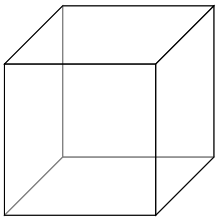
X : Menge der Ecken
$|G.x| = 4$

Stabilisator G_x 

$|G_x| = 2$

Symmetriegruppe von □ : $|G| = 4 \cdot 8 = 8 \to D_8$ Diedergruppe

2. **Würfel**



Variante I)

Operation auf Menge der Ecken.

$$|G_x| = 8$$

Stab. G_x von x ausrechnen: Iterationen des Verfahrens G_x op. auf angrenzenden Kanten Wähle Kante K:

$$\left.\begin{array}{rl} |G_xK| & = 3 \\ |G_K| & = 2 \end{array}\right\} |G_x| = 6$$

$|G| = 8 \cdot 6 = 48$

Variante II) Betrachte Op. der Sym. ?? auf der Menge der Seiten. Wähle Seite S.

$$|G.S| = 6$$
$$|G_S| = \#\text{ Sym von Quadrat } = 8$$

$|G| = 48$

Variante 3 Wähle Kante K (selber überlegen)

Bemerkung 1.5.5. X sei G-Menge Sei $(x_i)_{i\in I}$ Repräsentantensystem für die Bahnen der G Wirkung auf X. (d.h. $X = \bigcup_{i\in I} G_{x_i}$ und für $i \neq j : G_{x_i} \cap G_{x_j} = \emptyset$)
Es gilt

$$|X| = \sum_{i\in I} |G.x_i| \overset{\text{Satz 4}}{=} \sum_{i\in I} [G : G_{x_i}] \tag{1.3}$$

Wir nennen

$$X^G = \{x \in X | gx = x \ \forall g \in G\}$$

die Fixpunkte der G-Operation auf X. Also $x \in X^G \Leftrightarrow G_x = G$. Aus (1.3) wird also

$$|X| = |X^G| + \sum_{\substack{i\in I \\ x_i \notin X^G}} [G : G_{x_i}]$$

Satz 1.5.6. *(Satz von Cauchy) Sei G eine endliche Gruppe, mit $p||G|$ für eine Primzahl p. Dann enthält G ein Element der Ordnung p.*

Bew.: Sei

$$M = \{(g_1, \ldots, g_p) \in G^p | g_1 \cdot g_2 \cdots g_p = e\}$$

Für $g \neq e$ gilt:

$$\text{ord}(g) = p \underset{\text{prim}}{\Leftrightarrow} g^p = e \Leftrightarrow (g, \ldots, g) \in M$$

Es gilt $|M| = |G|^{p-1}$ (Warum?) .
Beh.: $(g_1, \ldots, g_p) \in M \Rightarrow (g_{1+k}, \ldots, g_{p+k}) \in M$ für $k \in \mathbb{Z}/p\mathbb{Z}$, wobei die Einträge als Restklassen bzgl. p zu betrachten sind.
⌜

Es reicht die Behauptung für $k = 1$ zu zeigen, es gilt:

$$\begin{aligned}(g_2, g_3, \ldots, g_p, g_1) \in M &\Leftrightarrow g_2 \cdots g_p \cdot g_1 = e \\ &\Leftrightarrow g_1^{-1} \cdot g_1 \cdot g_2 \cdots g_p \cdot g_1 = e\end{aligned}$$

⌟

Erhalte Wirkung der zyklischen Gruppe $\mathbb{Z}/p\mathbb{Z}$ auf M

$$\mathbb{Z}/p\mathbb{Z} \times M \to M \qquad (k + p\mathbb{Z}, (g_1, \ldots, g_p)) \mapsto (g_{1+k}, \ldots, g_{p+k})$$

Die einzigen UG von $\mathbb{Z}/p\mathbb{Z}$ sind $\{0\}$ und $\mathbb{Z}/p\mathbb{Z}$ nach 1.5.2. Nach der Bahnformel 1.5.4 haben die Orbits der $\mathbb{Z}/p\mathbb{Z}$ Wirkung die Länge 1 oder p. Da $p||G|$ gilt auch $p||M|$. Mit 1.5.5 ($X = M, G = \mathbb{Z}/p\mathbb{Z}$):

$$|M| \equiv |M^{\mathbb{Z}/p\mathbb{Z}}| + \sum_{\substack{i\in I \\ x_i \notin M^{\mathbb{Z}/p\mathbb{Z}}}} \underbrace{|\mathbb{Z}/p\mathbb{Z}.x_i|}_{=p\equiv 0} \pmod p$$

$$|M^{\mathbb{Z}/p\mathbb{Z}}| \equiv 0 \pmod p$$

Es gilt $|M^{\mathbb{Z}/p\mathbb{Z}}| \neq 0$, da $(e, e, \ldots, e) \in M^{\mathbb{Z}/p\mathbb{Z}}$. (es gilt $(g_1, \ldots, g_p) \in M^{\mathbb{Z}/p\mathbb{Z}} \Leftrightarrow g_1 = g_2 = \ldots = g_p$)
Somit enthält $M^{\mathbb{Z}/p\mathbb{Z}}$ min. $p - 1$ Elemente der Form $(g, g, \ldots, g)$ mit $g \neq e$. □

Definition. Sei G Gruppe, $S \subset G$ Teilmenge.
Der Zentralisator von S in G ist

$$C_G(S) = \{g \in G | \forall s \in S : gs = sg\}$$

Schreibe für $x \in G : C_G(x)$ statt $C_G(\{x\})$.

Das Zentrum von G ist $Z(G) = C_G(G)$.
$C_G(s)$ ist Untergruppe von G (Warum?) . $Z(G)$ normal in G (Warum?)

Satz 1.5.7. *(Klassengleichung) Sei G eine Gruppe, $(x_i)_{i\in I}$ Repräsentanten der Konjugationsklassen von G. Es gilt*

$$|G| = |Z(G)| + \sum_{\substack{i\in I \\ x_i \notin Z(G)}} [G : C_G(x_i)]$$

Bew.: Betrachte Wirkung von G auf $X = G$ durch Konjugation $(g, x) \mapsto gxg^{-1}$. Dann $G_{x_i} = C_G(x_i)$ und $X^G = Z(G)$ (Warum?) . Dann folgt die Behauptung aus 1.5.5. □

1.6 Sylowsätze

Definition. Sei p ein Primzahl. Eine endliche Gruppe G heißt p-Gruppe, falls für alle $g \in G$ gilt $\operatorname{ord} g = p^k$ mit $k \geq 0$.

Bemerkung. $G = \{e\}$ ist p-Gruppe für jedes p.

Satz 1.6.1. *Für eine endliche p-Gruppe G sind äquivalent:*

1) $|G| = p^k$ für $k \geq 0$

2) G ist eine p-Gruppe

Bew.: 1) $\Rightarrow$ 2) ist klar, da $\operatorname{ord} g \big| |G|$.
2) $\Rightarrow$ 1) Zeige $\neg 1) \Rightarrow \neg 2)$. Sei $q \neq p$ eine Primzahl mit $q \big| |G|$. Nach 1.5.6 hat G ein Element der Ordnung q. Also ist G keine p-Gruppe. □

Satz 1.6.2. *Sei G eine endliche p-Gruppe und X eine G-Menge. Dann*

$$|X| \equiv |X^G| \mod p$$

Bew.: Aus 1.5.5 wissen wir:

$$|X| = |X^G| + \sum_{\substack{i\in I \\ x_i \notin X^G}} [G : G_{x_i}]$$

Aus 1.5.2:

$$|G| = [G : H] \cdot |H| \Rightarrow [G : G_{x_i}] \big| |G| = p^k \Rightarrow [G : G_{x_i}] = p^l \qquad \text{mit } 0 \leq l \leq k$$

Aber $[G : G_{x_i}] = 1$ bedeutet $G_{x_i} = G$ also $x_i \in X^G$. Somit gilt für $x_i \notin X^G$ gilt $p \big| [G : G_{x_i}]$ □

Korollar 1.6.3. *Sei G eine endliche p-Gruppe mit $G \neq \{e\}$, dann $Z(G) \neq \{e\}$.*

Bew.: G wirke auf G durch Konjugation, dann $G^G = Z(G)$ siehe 1.5.7. und nach 1.6.2

$$\underbrace{0 \mod p \equiv |G|}_{|G|=p^k} \equiv |Z(G)| \mod p \tag{1.4}$$

Da $e \in Z(G)$ folgt $|Z(G)| > 0$ und mit (**??**) auch $|Z(G)| \geq p$. □

Definition. Sei G eine endliche Gruppe und p eine Primzahl.
Schreibe $|G| = p^m q$ mit $m \geq 0$ und $\mathrm{ggT}(p, q) = 1$
Eine UG $S \leq G$ heißt p-Sylowuntergruppe falls $|S| = p^m$.

Bemerkung. Es gibt keine UG H von G mit $|H| = p^l$ und $l > m$. (Warum?)

Satz 1.6.4. *(Sylowsätze) Sei G eine endliche Gruppe, p prim und $|G| = p^m q$ mit $\mathrm{ggT}(p, q) = 1$. Es gilt:*

1) Für alle $0 \leq k \leq n$ gibt es eine UG von G der Ordnung p^k.

2) Für jede p-Untergruppe H (d.h. UG, die auch p-Gruppe ist, d.h. von Ordnung p^k) und jede p-Sylow-UG S gilt:

$$\exists g \in G \colon gHg^{-1} \subset S$$

3) Sei $X = \{S \leq G | S$ ist p-Sylow-UG $\}$ die Menge aller p-Sylow-UG von G. Dann

$$|X| \big| q \wedge |X| \equiv 1 \mod p$$

Für den Beweis brauchen wir:

Satz 1.6.5. *(2. Isomorphiesatz) Sei G eine Gruppe und $N, H \leq G$ UG, N dabei normal, dann*

- *HN ist UG von G*
- *$H \cap N$ ist normal in H. und*

$$\begin{array}{ccc} H/H \cap N & \to & HN/N \\ h(H \cap N) & \mapsto & hN \end{array}$$

ist wohldefiniert und ein Gruppenisomorphismus.

Bew.:

- **Abgeschlossenheit HN:** Seien $hm, in \in HN$, dann ist $hmin = (hi)(i^{-1}min) \in HN$
- **Neutrales Element HN:** $e \in H, N \Rightarrow ee = e \in HN$
- **Inverses Element HN:** Wegen $HN = NH$ ist $(nh)^{-1} = h^{-1}n^{-1} \in HN$.
- **$H \cap N$ normal:** Sei $g \in H \cap N$, dann ist $hgh^{-1} \in H$ wegen der Abgeschlossenheit von H und $hgh^{-1} \in N$ wegen der Normalität von N.

$$H \hookrightarrow HN \twoheadrightarrow HN/N$$

mit $h \mapsto h$, $x \mapsto xN$ sind Gr.hom., also ist $\psi\colon H \to HN/N$, $\psi(h) = hN$ als Verkettung ein Gr.hom.. Ferner:

- ψ ist surjektiv (Warum?)
- $\ker\psi = \{h \in H | \psi(h) = e\} = H \cap N$

Aus dem 1. Isomorphiesatz folgt damit $\overline{\psi}\colon H/\ker\psi \to HN/N$ ist ein Gr. iso..□

Bew. von 1.6.4:

1) Induktion über $|G|$, sei P prim fix. Die Induktionsaussage ist:

   Beh. 1) gilt für alle G mit $|G| = p^m q \leq N$.

   A(1) ist $|G| = 1 : \checkmark (m = 0 \Rightarrow k = 0 \quad H = \{e\})$ Voraussetzung: Beh. sei wahr für $|G| < N = p^m q$. Wenn $m = 0$ ist, dann ist die Beh. wahr. Sei also $m > 0$. $k = 0$ ist auch klar, sei also $k > 0$. Betrachte Wirkung von G auf G durch Konjugation. Dann wiisen wir aus 1.5.7

$$|G| = |Z(G)| + \sum_{\substack{x_i \text{ Rep. der Konj.kl} \\ x_i \notin Z(G)}} [G : C_G(x_i)] \tag{1.5}$$

   Fall 1 $p \big| |Z(G)|$.

   - Nach 1.5.6 gibt es $z \in Z(G)$ mit $\operatorname{ord} z = p$
   - $\langle Z \rangle$ ist normal in G (Warum?) und $G/\langle Z \rangle$ hat Ordnung $p^{m-1}q$.
   - Nach I.V. : Es gibt $\tilde{H} \leq G/\langle Z \rangle$ mit $(\tilde{H}) = p^{k-1}$ Sei

     $$\pi\colon G \to G/\langle Z \rangle$$

     die kanonische Projektion, setze $H = \pi^{-1}(\tilde{H})$.
     Dann $H \leq G, |H| = p^k$ (Warum?)

   Fall 2 $p \not| |Z(G)|$. Wegen (1.5) und $p \big| |G|$ gibt es $x_i \notin Z(G)$ mit

   $$p \not| [G : C_G(x_i)]$$

   Da

   $$|G| = [G : C_G(x_i)] \cdot |C_G(x_i)|$$

   folgt $p^m \big| |C_G(x_i)|$, also $|C_G(x_i)| = p^m \cdot q'$ mit $\operatorname{ggT}(p, q') = 1$. Ferner gilt $C_g(x_i) \lneq G$ (da $x_i \notin Z(G)$). Nach IV gibt es $H \leq C_G(x_i)$ mit $|H| = p^k$.

2) Für $m = 0$ ist dies klar. Sei Also $m > 0$. H operiert auf $G/S =: y$
   Idee: Fixpunkt von H-Wirkung auf y suchen
   ⌜

   Denn: Sei $gS \in y^H$. Dann gilt

   $$\forall h \in H\colon hgS = gS$$

   Also $(e \in S)$ $hg = gs$ für ein $s \in S$ d.h. $g^{-1}hg \in S$

Nach 1.6.2 (H: p-Gruppe, H wirkt auf y) gilt

$$|y| \equiv |y^H| \mod p$$

Nun gilt $|y| = |G/S| = \frac{|G|}{|S|} = q$ und $p \nmid q$ folgt $|y| \not\equiv 0 \mod p$, somit auch $|y^H| \neq 0$.

3) Der Fall $m = 0$ ist klar denn dann ist nur $\{e\}$ eine p-Sylow Gruppe. Sei also $m > 0$. Nach 1) ist $X \neq \emptyset$. G operiert auf X durch Konjugation (Warum?) . Nach 2) ist die Operation transitiv. Nach der Bahnformel (1.5.4) ist für ($S \in X$ beliebig):

$$\underbrace{|G.S|}_{=|X|} = [G : G_S]$$

Da $S \leq G_S$ und $G_s \leq G$ folgt (1.5.3)

$$\underbrace{[G : S]}_{=q} = \underbrace{[G : G_S]}_{=|X|} \cdot [G_S : S]$$

Also $|X| \big| q$.

Betrachte Wirkung von S auf X durch Konjugation. Aus 1.6.4 wissen wir:

$$|X| \equiv |X^S| \mod p$$

Mit der folgenden Behauptung folgt 3)
Beh.: $X^S = \{S\}$

Sei $T \in X^S$, d.h.

$$sts^{-1} \in T \ \forall s \in S, t \in T$$

G Gruppe, $H \leq G$ UG Der Normalisator von H in G ist

$$N_G(H) = \{g \in G \big| gHg^{-1} = H\}$$

$N_G(H)$ ist UG in G und H ist normal in $N_G(H)$ und $N_G(H)$ ist die kleinste Untergruppe in der H normal ist (Warum?) . Also $T \in X^S \Leftrightarrow S \subset N_G(T)$. Dann ist auch $ST \leq N_G(T)$ (Warum UG?) , also $T \leq ST \leq G$. Nach 1.5.3 gilt

$$[G : T] = [G : ST] \cdot [ST : T]$$

ST ist eine p-Gruppe (zeigen wir gleich), somit ist $|ST| = p^k$. Da $p \nmid q$ muss $[ST : T] = 1$ sein. Dann ist aber $S \subset T$ (Warum?) . Wegen $|S| = |T|$ ist folgt $T = S$.

Beh.: ST ist eine p-Gruppe.

T ist normal in ST. Nach 1.6.4 ist:

$$S/S \cap T \xrightarrow{\sim} ST/T$$

Aber

$$\underbrace{|S|}_{=p^m} = \underbrace{|S/S \cap T|}_{=p^a} \cdot \underbrace{|S \cap T|}_{=p^b}$$

und

$$|S/S \cap T| = |ST/T| = \frac{|ST|}{|T|}$$

Genauso: $|ST| = p^k$.

□

Satz 1.6.6. *Sei G eine Gruppe und $|G| = pq$ mit p, q prim und $p < q$ und $p \nmid q-1$. Dann ist G zyklisch, also $G \simeq \mathbb{Z}/pq\mathbb{Z}$. (z.B. $p = 3$, $q = 5$ passt, aber $p = 3, q = 7$ geht nicht).*

Bew.: Sei P eine p-Sylow Gruppe von G und n_p die Anzahl der p-Sylow-Gruppen von G. Entsprechend Q und n_q. Es gilt $P \cap Q = \{e\}$, nach 1.6.4 Teil 3 gilt:

$$n_p \mid q \qquad n_p \equiv 1 \mod p \tag{1.6}$$

$$n_q \mid p \Rightarrow n_q = 1$$
$$n_q \equiv 1 \mod q \Rightarrow Q \text{ normal}$$

Wäre $n_p = q$, dann gilt nach (1.6)

$$q \equiv 1 \mod p$$

was ein Widerspruch dazu ist, dass $p \nmid q-1$. Also ist $n_p = 1$ und P normal. Ferner ist $G = \langle P \cup Q \rangle$ (Warum?) , also gibt es Gr.hom. $P \times Q \to G$ und P, Q sind zyklisch (Warum?) . Sei $P = \langle x \rangle$, $Q = \langle y \rangle$, dann hat xy die Ordnung pq (Warum?) 1663. Somit ist $G = \langle xy \rangle$. □

1.7 Auflösbare Gruppen

Definition. Eine Gruppe G heißt einfach, falls $\{e\}$ und G die einzigen normalen UG von G sind.

Bemerkung. 1. Warum definiert man nicht

$\{e\}$ und G einzige UG von G

Was sind alle endl. die dann einfach wären?

2. Seien G, H Gruppen und H einfach. Für jeden Gr. hom. $f\colon G \to H$ gilt: f ist inj. oder $f(G) = \{e\}$.

3. Einfach Gruppen kann man nicht „kleiner machen“, d.h. die einzigen Faktorgruppen sind $G/\{e\} \simeq G$ und $G/G \simeq \{e\}$

4. Endliche einfache Gruppen sind klassifiziert! Es gibt 18 unendliche Serien und 26 Ausnahmen.

5. Alle **abelschen** endlichen einfachen Gruppen sind $\mathbb{Z}/p\mathbb{Z}$ mit p (Warum?) .

Definition. Sei G eine Gruppe. Eine Normalreihe ist eine endliche Folge von UG G_i von G s.d.

$$\{e\} = G_0 \leq G_1 \leq G_2 \leq \ldots \leq G_n = G$$

wobei G_i normal in G_{i+1}. Warnung: I.A. muss G_k nicht normal in G sei.

Beispiel. Sei $G = S_4$. Setze $K = \{e, (12)(34), (13)(24), (14)(23)\}$. Dann ist

$$\{e\} \leq K \leq A_4 \leq S_4$$

eine Normalreihe (Warum?)

Satz 1.7.1. *A_n ist genau dann einfach, wenn $n \neq 4$.*

Bew.: Für $n = 1, 2, 3$ kann man dies nachrechnen. Sei $n \geq 5$ Nach Zettel 4 A1 wird A_n von 3-Zykeln erzeugt.
Beh.: Alle 3-Zykel sind in A_n konjugiert ($n \geq 5$)
⌜

$$\exists \tau \in S_n\colon \tau(123)\tau^{-1} = (ijk)$$

$\operatorname{sgn}\tau = 1$ ist klar
Für $\operatorname{sgn}\tau = -1$ setze $\sigma = \tau(45)$, dies erfüllt $\sigma(123)\sigma^{-1} = (ijk)$.
⌟

Wir werden zeigen: Sei $N \leq A_n$ normal und $\{e\}$. Dann enthält N einen 3-Zykel. Sei $\sigma \in N$, $\sigma \neq e$. Fallunterscheidung nach Zykeltyp $k_1 \geq k_2 \geq \ldots \geq k_L$ von σ:

a) $(r, \ldots)$ mit $r \geq 4$

b) $(3, 3, \ldots)$

c) $(3, 2, 2, \ldots, 2)$

d) $(2, 2, \ldots, 2)$

Schreibe o.B.d.A. $(12\ldots r)$ statt $(a_1 a_2 \ldots a_r)$. Wir basteln nun die Fälle durch:

a) $\sigma = (12\ldots r)\tau$ für $r \geq 4$. Mit $\delta = (123)$ gilt $\sigma^{-1}(\delta^{-1}\sigma\delta) = (23r)$.

b) $\sigma = (123)(456)\tau$ Mit $\delta = (124)$ gilt $\sigma^{-1}\delta^{-1}\sigma\delta = (12436)$, damit sind wir wieder im Fall a).

c) $\sigma = (123)\tau$ mit $\tau^2 = \mathrm{id}$. Damit ist $\sigma^2 = (132)$.

d) $\sigma = (12)(34)\tau$. Mit $\delta_1 = (123)$ gilt $\sigma^{-1}\delta^{-1}\sigma\delta = (14)(23) =: \alpha$ und $\delta_2 = (125)$ gilt $\delta_2^{-1}\alpha\delta_2 = (13)(45) =: \beta$ und $\alpha\beta = (12345)$, dann Fall a).

Definition. Eine Gruppe G heitßt auflösbar, falls G eine Normalreihe $(G_i)_{i=0,\dots,n}$ besitzt, s.d. G_{i+1}/G_i abelsch ist. Eine solche N.R. heißt abelsche Normalreihe.

Beispiel. 1) Jede abelsche Gruppe ist auflösbar.

2) $\{e\} \leq K \leq A_4 \leq S_4$ ist eine ab. Normalreihe. Aber S_n ist für $n \geq 5$ nicht auflösbar, da $A_n \leq S_n$ einfach und nicht abelsch ist, also nicht auflösbar nach 1.7.2.

3) Sei k ein Körper

$$T = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| a, c \in k^*, b \in k \right\}$$

ist eine UG von $GL_2(k)$ und T ist nicht ablesch. (Warum?)

$$\delta \colon T^* \to k^* \times k^* \qquad \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto (a, c)$$

ist ein Gr.hom. mit

$$\ker \delta = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \right\} \leq T$$

Also ist

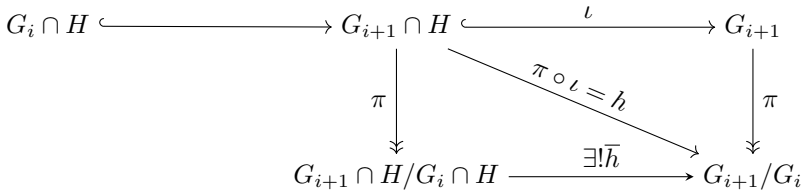
$$\{e\} \leq \ker \delta \leq T$$

eine abelsche N.R., denn $\ker \delta$ ist abelsch und $T/\ker \delta \simeq k^* \times k^*$ ist abelsch. Also ist T auflösbar.

Lemma 1.7.2. *Untergruppen von auflösbaren Gruppen sind auflösbar.*

Bew.: Sei $H \subset G$ eine UG, $(G_i)_{i=0,\dots,n}$ eine abelsche NR in G.
Beh.: $H_i = G_i \cap H$ ist ab. NR in H.
⌜

- $H_i \leq H_{i+1}$ ist normal (Warum?)
- H_{i+1}/H_i ist abelsch.



Wegen $G_i \cap H \subset \ker h$ gibt es genau ein $\overline{h}$ wie oben mit

$$\overline{h}(\pi(y)) = h(y)$$

somit

$$\overline{h}(\pi(y)) = e \Leftrightarrow h(y) = e \Leftrightarrow y \in G_i \cap H \Leftrightarrow \pi(y) = e$$

Also ist $\overline{h}$ injektiv, also H_{i+1}/H_i abelsch.

□

Satz 1.7.3. *Sei*

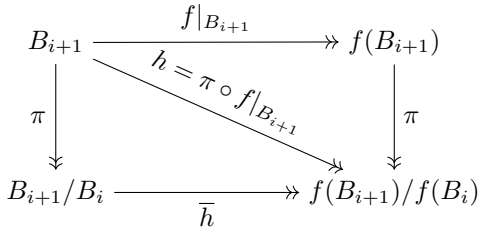
$$1 \to A \xrightarrow{g} B \xrightarrow{f} C \to 1$$

eine kurze exakte Sequenz, dann sind äquivalent:

1. *B ist auflösbar*
2. *A und C sind auflösbar*

Bew.: 1) ⇒ 2): Sei $(B_i)_{i=0,\dots,n}$ ab. NR für B.

- A **ist auflösbar:** $g\colon A \to \operatorname{im} g \leq B$ ist Gr.isom. und $\operatorname{im} g$ ist auflösbar nach 1.7.2.
- C **ist auflösbar:** Setze $C_i = f(B_i)$ für $i = 0, \dots, n$.
  - $C_i \leq C_{i+1}$ ist normal (Warum?)
  - $C_0 = f(B_0) = \{e\}$, $C_n = f(B_n) = C$
  - Wir haben



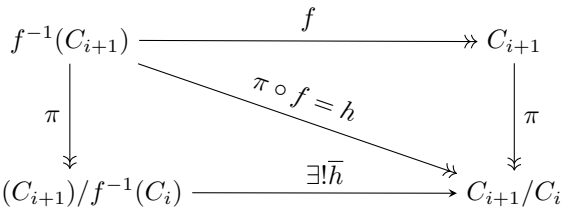
    Setze $h = \pi \circ f|_{B_{i+1}}$, dann ist $B_i \subset \ker h$, da $\pi(f(B_i)) = \{e\}$, also gibt es wieder ein eindeutiges $\overline{h}$ wie oben, dieses ist surjektiv, weil $f|_{B_{i+1}}$ und π surjektiv sind. Da B_{i+1}/B_i abelsch ist und $\overline{h}$ surj. ist, ist auch $f(B_{i+1})/f(B_i)$ abelsch.

2) ⇒ 1) Seien $(A_i)_{i=0,\dots,m}$ und $(C_j)_{j=0,\dots,n}$ abelsche NR für A und C. **Beh.:**

$$\begin{aligned}\{e\} = g(A_0) \leq g(A_1) \leq \ldots \leq g(A_m) = g(A) = \ker f = f^{-1}(\{e\}) \\ = f^{-1}(C_0) = f^{-1}(C_1) \leq \ldots \leq f^{-1}(C_n) = B\end{aligned}$$

ist ab. NR für B.

$g(A_i) \leq g(A_{i+1})$ und $f^{-1}(C_i) \leq f^{-1}(C_{i+1})$ sind jeweils normal (Warum?) und $g(A_{i+1})/g(A_i)$ ist abelsch (Warum?)



Sei $h = \pi \circ f$, dann $f^{-1}(C_i) \subset \ker h$, da

$$\pi(f(f^{-1}(C_i))) \subset \pi(C_i) = \{e\}$$

Also gibt es $\overline{h}$ wie in der Abbildung und $\overline{h}$ ist injektiv, denn

$$\overline{h}(\pi(y)) = e \Leftrightarrow h(y) = e \Leftrightarrow f(y) \in C_i \Leftrightarrow y \in f^{-1}(C_i)$$

Somit ist $f^{-1}(C_{i+1})/f^{-1}(C_i)$ abelsch.

⌟

□

1.8 Abelsche Gruppen

Definition. Sei $(A_\alpha)_{\alpha \in I}$ eine Familie von abelschen Gruppen. Die (äußere) direkte Summe der A_α ist

$$\bigoplus_{\alpha \in I} A_\alpha = \left\{ (a_\alpha)_{\alpha \in I} \subseteq \prod_{\alpha \in I} A_\alpha \mid a_\alpha \neq e \text{ nur für endlich viele } \alpha \in I \right\}$$

Bemerkung. Seien die $A_\alpha \subset A$, A eine abelsche Gruppe. A ist die innere direkte Summe der A_α, falls

$$\bigoplus_{\alpha \in I} A_\alpha \to A, \ (a_\alpha)_{\alpha \in I} \mapsto \sum_{\alpha \in I} a_\alpha$$

ein Gr. isom. ist.
Warnung: Hier sind anders als in Kapitel 1.3 unendliche I erlaubt. Für unendliche U gilt

$$\prod_{\alpha \in I} A_\alpha \supsetneq \bigoplus_{\alpha \in I} A_\alpha$$

Definition. Eine abelsche Gruppe heißt frei, falls es eine Teilmenge $X \subset A$ gibt, s.d.

$$A = \bigoplus_{x \in X} \langle x \rangle$$

und $\langle x \rangle$ unendliche Ordnung hat für jedes $x \in X$. Also: eine freie abelsche Gruppe ist die direkte Summe unendlicher zyklischer Gruppen, also

$$A \simeq \bigoplus_{x \in X} \mathbb{Z}$$

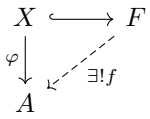
X heißt dann eine Basis von A.

Bemerkung. Sei X Basis von A. Für alle $a \in A$ gibt es $\lambda_x \in \mathbb{Z}$ sodass $a = \sum_{x \in X} \lambda_x x$ und

- λ_x eindeutig bestimmt
- nur endlich viele $\lambda_x \neq 0$

(Warum?)

Satz 1.8.1. *Sei F eine freie abelsche Gruppe und A eine abelsche Gruppe. Für jede Abbildung $\varphi\colon X \to A$ gibt es einen eindeutigen Gruppenhomomorphismus $f\colon F \to A$ sodass $\forall x \in X\colon f(x) = \varphi(x)$*



Bew.:

- **Existenz:** Sei $g \in F$, schreibe $g = \sum_x \lambda_x x$. Da λ_x eindeutig, ist die Abbildung
$$\overline{\varphi}\colon g \mapsto \sum_x \lambda_x \varphi(x)$$
wohldefiniert.
- **Gr.hom.:** klar (Warum?)
- Sei $f\colon F \to A$ ein weiterer solcher Gr.hom., dann sei $g \in F$ beliebig. Dann ist $g = \sum_{x\in X} \lambda_x x$ und
$$f(g) = f\left(\sum_x \lambda_x x\right) = \sum_x \lambda_x f(x) = \sum_x \lambda_x \overline{\varphi}(x) = \ldots = \overline{\varphi}(g)$$

□

Definition. Sei G eine Gruppe. G heißt endlich erzeugt, falls es eine endliche Teilmenge $E \subset G$, so dass $\langle E\rangle = G$. Ab hier betrachten wir (fast) nur noch endlich erzeugte abelsche Gruppen (ee aG).

Bemerkung. (Üb) Sei F eine freie abelsche Gruppe. Es sind äquivalent:

1. F ist endlich erzeugt
2. Jede Basis von F hat nur endlich viele Elemente.

Satz 1.8.2. *Seien A, B freie ee aG mit Basen $X \subset A$ und $Y \subset B$. Es sind äquivalent:*

1. *$A \cong B$ als Gruppen.*
2. *$|X| = |Y|$*

Bemerkung. Gilt auch ohne ee

Bew.: 2) $\Rightarrow$ 1) Wähle Bij. $\varphi\colon X \to Y$ mit Inversem $\varphi^{-1}\colon Y \to X$ (schreibe ψ statt φ^{-1}). Nach 1.8.1 gibt es einen Gr. Hom. $\tilde{\varphi}$ als Fortsetzung von φ auf A und ebenso $\overline{\psi}$. Dann $\overline{\varphi} \circ \overline{\psi} = \mathrm{id}_B$ und $\overline{\psi} \circ \overline{\varphi} = \mathrm{id}_A$.

1) $\Rightarrow$ 2) Es genügt zu zeigen, dass je zwei Basen Y, Y' von B gleichmächtig sind (Warum?) . Sei $2B = \{2b \mid b \in B\} \leq B$

$$b = \sum_{y \in Y} \lambda_y y \qquad 2b = \sum_{y \in Y} 2\lambda_y y$$

In jeder Nebenklasse von $B/2B$ haben wir genau ein Element der Form

$$\sum_{y \in Y} \lambda_y Y \qquad \lambda_y \in \{0, 1\}$$

Also ist

$$|B/2B| = 2^{|Y|}$$

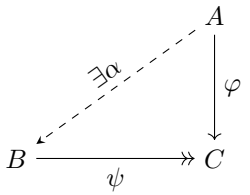
Für eine andere Basis Y' von B ist ebenfalls $|B/2B| = 2|Y'|$, also $|Y| = |Y'|$. $\square$

Definition. Die Mächtigkeit der Basis Y einer Gruppe B wird als Rang von B ($\mathrm{Rang}(B)$) bezeichnet.

Definition. Sei A eine abelsche Gruppe, A heißt projektiv, falls für alle Gr.hom.

$$\varphi\colon A \to C \qquad \psi\colon B \to C \text{ surj.}$$

ein $\alpha\colon A \to B$ existiert, s.d. $\psi \circ \alpha = \phi$.



Bemerkung. α ist normalerweise nicht eindeutig.

Satz 1.8.3. *Sei A eine eeaG, dann gilt: A frei $\Leftrightarrow$ A projetkiv*

Bew.: „$\Rightarrow$ “: Sei A frei mit Basis X und seien $\varphi\colon A \to C$ und $\psi\colon B \to C$ surj. Gr.hom..

$$\forall x \in X\colon \varphi(x) \in C$$

Da ψ surj. ist, gibt es ein b_x in B mit $\psi(b_x) = \varphi(x)$. Wir definieren eine Funktion $f\colon X \to B$ durch $f(x) = b_x$ (bei Uneindeutigkeit von b_x kann willkürlich ausgewählt werden). Es existiert nun genau ein Gr.hom. α s.d. $\alpha(x) = b_x$, nämlich

$$\alpha\left(\sum_{x \in X} \lambda_x x\right) = \sum_{x \in X} \lambda_x b_x$$

Für diesen sieht man nun:

$$\psi \circ \alpha \left(\sum_{x \in X} \lambda_x x \right) = \psi \left(\sum_{x \in X} \lambda_x b_x \right) = \sum_{x \in X} \lambda_x \psi(b_x) = \sum_{x \in X} \lambda_x \varphi(x) = \varphi \left(\sum_{x \in X} \lambda_x x \right)$$

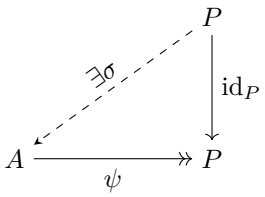
Für „$\Leftarrow$“ brauchen wir noch etwas Vorbereitung.

Satz 1.8.4. *Sei P eine proj. abelsche Gruppe, A ein abelsche Gruppe und $\psi\colon A \to P$ surj. Die Sequenz:*

$$1 \to \ker \psi \to A \xrightarrow{\psi} P \to 1$$

spaltet und $A \simeq P \oplus \ker \psi$

Bew.: Wir betrachten:



Da P projektiv ist, gibt es ein σ s.d. $\phi \circ \sigma = \mathrm{id}_P$, also spaltet die Sequenz durch σ. Also ist nach 1.3.2 A isomorph zu $P \rtimes \ker \psi = P \oplus \ker \psi$.

Satz 1.8.5. *Sei A eine freie abelsche Gruppe und $B \leq A$ eine UG. B ist dann auch frei und* $\mathrm{Rang}(B) \leq \mathrm{Rang}(A)$

Bew.: Wir induzieren nach $\mathrm{Rang}(A) = n$. Für $n = 1$ ist $A \simeq \mathbb{Z}$. Die UG von $\mathbb{Z}$ sind $\{0\}$ und $m\mathbb{Z}$, erstere ist frei mit Rang 0, zweitere mit Rang 1. Für $n > 1$ hat eine Basis

$$X = \{x_1, \ldots, x_n\}$$

Wir definieren:

$$p\colon A \to \mathbb{Z} \qquad \sum_{i=1}^{n} \lambda_i x_i \mapsto \lambda_n$$

Es ist

$$\ker p = \langle x_1, \ldots, x_{n-1} \rangle$$

$\ker p$ ist frei mit Basis $\{x_1, \ldots, x_{n-1}\}$. Betrachte nun $p|_B\colon B \to \mathbb{Z}$ und unterscheide für $\mathrm{im}\, p|_B$:

- **Fall 1:** $\mathrm{im}\, p|_B = \{0\}$, dann ist $B \subset \ker p$ und $\ker p$ war eine freie abelsche Gruppe mit Rang $n-1$. Per Induktion ist B frei und $\mathrm{Rang}(B) \leq n-1 \leq n$.
- **Fall 2:** Sei $\mathrm{im}\, p|_B = m\mathbb{Z} \simeq \mathbb{Z}$ für $m \neq 0$. Dann

  $$1 \to \ker p|_B \to B \xrightarrow{p} m\mathbb{Z} \to 1 \tag{1.7}$$

  Da $m\mathbb{Z}$ frei ist, ist es auch projektiv und darum spaltet (1.7) und

  $$B \simeq m\mathbb{Z} \oplus \ker p|_B$$

  und da $\mathrm{Rang}(m\mathbb{Z}) = 1$ ist $\mathrm{Rang}(B) \leq n$

□

Korollar. *Sei A eine eeaG und $B \leq A$, dann ist B auch ee.*

Bew.: Sei $E = (e_i)_{i\in I}$ der endliche Erzeuger von A (also $|I| = n$), dann setzen wir $F = \mathbb{Z}^n$ und definieren mit 1.8.1 ein Gr. hom. $\phi\colon F \to A$ via

$$\phi((k_i)_{i\in I}) = \sum_{i\in I} k_i e_i$$

. Das Urbild $\varphi^{-1}(B)$ ist eine UG von F, also ebenfalls frei mit Basis X und somit wird B von $\phi(X)$ erzeugt, da ϕ surj. ist. □

Bew. Fort. von 1.8.3: Sei P eine proj. eeaG, dann existieren wie im Korollar eine freie ab. Gruppe F und eine Surjektion $\varphi\colon F \to P$, woraus mit 1.8.4 folgt:

$$F \simeq P \oplus \ker\varphi$$

Also ist P zu einer UG von F isomorph und da UG von freien aG frei sind, ist P frei.

Satz 1.8.6. *(Klassifikationssatz) Sei A eine eeaG. Es gibt $r \in \mathbb{Z}_{>0}$ und $q_1, \ldots, q_n$ Primzahlpotenzen s.d.*

$$A \simeq \mathbb{Z}^r \oplus \bigoplus_{i=1}^{n} (\mathbb{Z}/q_i\mathbb{Z})$$

wobei r eindeutig ist und $q_1, \ldots, q_n$ eindeutig bis auf ihre Reihenfolge sind.

Beweisplan.:

1) $A = \mathbb{Z}^r \oplus$ end. r eindeutig

2) A endlich $A \simeq \bigoplus_{p\ prim} A_p$ und $|A_p| p^{b_p}$.

3) $A_p \simeq \bigoplus_{i=1}^{m} \mathbb{Z}/p^{a_i}\mathbb{Z}$ + Eindeutigkeit

Definition. Sei A eine eeaG und

$$T(A) = \{a \in A | \exists n \in \mathbb{N}\colon na = 0\}$$

Also alle Element von endlicher Ordnung in A. $T(A)$ ist eine UG, wir nennen sie die Torsionsuntergruppe von A. Da $T(A)$ eine UG der eeaG A ist, ist auch $T(A)$ ee.

Satz 1.8.7. *$T(A)$ ist endlich*

Bew.: Sei $X = \{x_1, \ldots, x_l\}$ ein EZS von $T(A)$, wir schreiben

$$\mathrm{ord}(x_i) = c_i$$

Wir können nun jedes $a \in T(A)$ darstellen als:

$$a = \sum_{i=1}^{l} \lambda_i x_i \qquad \lambda_i \in \mathbb{Z}$$

o.B.d.A. ist $\lambda_i \in \{0, 1, \ldots, c_i - 1\}$, dann ist aber:

$$|T(A)| \leq c_1 \cdot c_2 \cdots c_l \leq \infty$$

Satz 1.8.8. *Sei A eine eeaG, wenn $T(A) = 0$, so ist A frei.*

Bew.: Wir haben ein EZS X von A und wählen $M \subset X$ s.d.

1) Die Elemente von M unabhängig sind, d.h.

$$\sum_{m \in M} \lambda_m m = 0 \Rightarrow \forall m \in M \colon \lambda_m = 0$$

2) M mit der Eigenschaft 1) maximal ist.

Dann ist $\langle M \rangle = B$ frei mit Basis M. Es gilt für alle i, dass $x_i \cup M$ abh. sind, also ist

$$\lambda_i x_i + \sum \lambda_{i,m} m = 0$$

für geeignete $\lambda_i, \lambda_{i,m}$ also ist $\lambda_i x_i \in B$. Die Abbildung:

$$\psi \colon A \to A \qquad a \mapsto \lambda_1 \lambda_2 \cdots \lambda_n a$$

ist ein ein Gr. hom. und

$$\ker \psi = \{a \in A | \lambda_1 \cdots \lambda_n a = 0\} \subset T(A) = \{0\}$$

Es ist $\psi(x_i) = \lambda_1 \cdots \lambda_i \cdots \lambda_n x_i \in B$, da $\lambda_i x_i \in B$ ist. Da X ein EZS von A ist, gilt demnach auch $\psi(A) \subset B$

$$a = \sum \mu_i x_i$$
$$\psi(a) = \sum \mu_i \psi(x_i) \in B$$

$\psi \colon A \to \psi(A) \subset B$. $A \simeq \psi(A)$, B frei. $\psi(A) \leq B \Rightarrow \psi(A)$ ist frei $\Rightarrow A$ ist frei. □

Satz 1.8.9. *Sei A eine eeaG und $T(A/T(A)) = \{0\}$, dann ist $A/T(A)$ frei.*

Bew.: Sei $a + T(A)$ ein Element von Ordnung n und $na + T(A) = T(A)$, dann ist $na \in T(A)$, also existiert ein $m \neq 0$ mit $m(na) = 0 = (mn)a$, also ist $a \in T(A)$ und $a + T(A) = T(A)$. □

Satz 1.8.10. *Sei A eine eeaG dann ist $A \simeq T(A) \oplus A/T(A)$*

Bew.: $T(A) \subset A$

$$1 \to T(A) \to A \to A/T(A) \to 1$$

$A/T(A)$ ist frei, also projektiv, demnach spaltet die Sequenz

$$A \simeq T(A) \oplus A/T(A) \simeq T(A) \oplus \mathbb{Z}^r$$

mit $r = \text{Rang}(A/T(A))$.

1. $T(A) = 0 \Rightarrow A$ frei
2. $T(A/T(A)) = 0 \Rightarrow A/T(A)$ ist frei.

Definition. Sei A eine endliche abelsche Gruppe und p eine Primzahl mit $p\big||A|$ wir schreiben:

$$A_p = \{a \in A | \exists n \in \mathbb{N}\colon p^n a = 0\}$$

A_p ist eine UG von A (Warum?) .

Satz 1.8.11. *Wir definieren:*

$$\phi\colon \bigoplus_{p\big||A|} A_p \to A \qquad (a_p)_{p\big||A|} \mapsto \sum_{p\big||A|} a_p$$

ϕ ist ein Gruppenisomorphismus.

Bew.: Zur Vereinfachung der Notation definieren wir:

$$P := \{p \in \mathbb{N}\colon p\big||A|, p \text{ Primzahl}\}$$

Wir zeigen zunächst, dass ϕ ein Gr.hom. ist.

$$\begin{aligned}\phi((a_p)_{p\in P} + (b_p)_{p\in P}) = \phi((a_p + b_p)_{p\in P} &= \sum_{p\in P}(a_p + b_p)\\ &= \sum_{p\in P} a_p + \sum_{p\in P} b_p = \phi((a_p)_{p\in P}) + \phi((b_p)_{p\in P})\end{aligned}$$

Beh.: A_p ist eine - weil A abelsch ist, die einzige - p-Sylowgruppe von A.

A_p ist eine p-Gruppe, denn die Ordnung jedes Elementes ist eine Potenz von P. Sei S eine Sylowgruppe von A, dann hat $s \in S$ die Ordnung p^n für ein $n \geq 0$, also ist $S \subset A_p$, also $S = A_p$, da S und A_p gleich viele Elemente haben müssen.

Wir schreiben

$$|A| = p_1^{a_1} p_2^{a_2} \cdots p_l^{a_l}$$

Da die A_p jeweils Sylowgruppe sind, ist $A_{p_i} = p_i^{a_i}$. Es gilt:

$$\left|\bigoplus_{p\in P} A_p\right| = \prod_{i=1}^{l} |A_{p_i}| p_1^{a_1} p_2^{a_2} \cdots p_l^{a_l}$$

Da Definitions- und Wertebereich die gleiche endliche Mächtigkeit besitzen, reicht es also zu zeigen, dass ϕ injektiv ist, um zu wissen, das ϕ bijektiv ist. Sei dazu $(t_p)_{p\in P} \in \ker\phi$ jeweils mit $t_p \in A_p$ für jedes $p \in P$. Wir nummerieren P als $P = \{p_1, \ldots, p_l\}$ und schreiben statt t_{p_i} nun t_i. Es ist:

$$\phi((t_i)_{p_i\in P}) = t_1 + t_2 + \ldots + t_l = 0$$

Wir schreiben für ein beliebiges fixiertes $i \in \{1, \ldots, l\}$:

$$n = p_1^{a_1} \cdots p_{i+1}^{a_{i+1}} p_{i+1}^{a_{i+1}} \cdots p_l^{a_l} = \frac{|A|}{p_i^{a_i}}$$

Wegen $p_j^{a_j} \big| n$ für $j \neq i$ ist $nt_j = 0$ und wir sehen:

$$\begin{aligned} t_1 + \ldots + t_l = 0 \Rightarrow n(t_1 + \ldots + t_l) = 0 \Rightarrow nt_1 + \ldots + nt_l = 0 \\ \Rightarrow 0 + \ldots + 0 + nt_i + 0 + \ldots + 0 = 0 \Rightarrow nt_i = 0 \end{aligned}$$

Es muss also gelten $\mathrm{ord}(t_i) \big| n$ aber gleichzeitig ist $\mathrm{ggT}(n, p_i^{a_i}) = 1$, deshalb muss $\mathrm{ord}(t_i) = 1$ sein, also $t_i = 0$. Da i beliebig wahr, ist jedes $t_i = 0$ und somit ϕ injektiv, nach vorausgegangener Bemerkung sogar bijektiv. □
Nun wollen wir zeigen, dass A_p die direkte Summe von zyklischen Gruppen ist.

Satz 1.8.12. *Sei p eine Primzahl und A eine endliche abelsche p-Gruppe. Sei $x \in A$ mit maximaler Ordnung $\mathrm{ord}(x) = p^n$ (d.h. $\forall y \in A\colon \mathrm{ord}(y) \big| p^n$), dann ist $\langle x \rangle$ ein direkter Summand in A. Es gibt also eine UG $B \leq A$ s.d. $A = B \oplus \langle x \rangle$.*

Bemerkung. Ohne die Maximalität ist die Aussage nicht wahr: Sei z.B. $A = \mathbb{Z}/p^2\mathbb{Z}$ und $x = p + p^2\mathbb{Z}$, dann hat x die Ordnung p, aber es gibt keine UG von A, die eine direkte Summe mit $\langle x \rangle$ bilden.

Bew. Satz: Wir verwenden eine Induktion nach l für $|A| = p^l$. Für $l = 0$ haben wir $A = \{0\}$ und somit erfüllen $x = 0$ und $B = \{0\}$ die Aussage $A = B \oplus \langle x \rangle$, damit ist der I.A. gezeigt.

Für $l > 0$ ist $A/\langle x \rangle$ eine p-Gruppe, also existiert ein Element $a + \langle x \rangle \in A/\langle x \rangle$ von Ordnung p (wenn $A = \langle x \rangle$ existiert so ein Element nicht, dann kann aber $B = \{0\}$ gewählt werden). Da $pa \in \langle x \rangle$ ist, gibt es $\lambda \in \mathbb{Z}$ s.d. $pa = \lambda x$. Wegen $\mathrm{ord}(x) = p^n$ gilt dann:

$$0 = p^n a = p^{n-1} pa = p^{n-1} \lambda x \Rightarrow p^n \big| p^{n-1} \lambda \Rightarrow p \big| \lambda$$

wir schreiben deswegen $\lambda = pr$ für $r \in \mathbb{Z}$. Wir setzen$b = a - rx$ und erhalten

$$pb = pa - prx = \lambda x - \lambda x = 0$$

also ist $\mathrm{ord}(b) = p$.

Wir betrachten nun $A/\langle b \rangle$, wobei wir wissen, dass $|A|\langle b \rangle = p^{l-1}$. **Beh.:** $\mathrm{ord}(x + \langle b \rangle) = p^n$.
⌜

> Es gilt $\langle x \rangle \cap \langle b \rangle = \{0\}$, denn sonst wäre $\langle b \rangle \subset \langle x \rangle$, also insbesondere $b \in \langle x \rangle$ aber wegen $b + \langle x \rangle = a + \langle x \rangle$ ist $\mathrm{ord}(b + \langle x \rangle) = p$. Dann folgt nun:
>
> $$p^c x + \langle b \rangle = \langle b \rangle \Rightarrow p^c x \in \langle b \rangle \Rightarrow p^c x = 0 \Rightarrow p^n \big| p^c \Rightarrow \mathrm{ord}(x + \langle b \rangle) = p^n$$

⌟

p^n ist als Ordnung maximal in $A/\langle b \rangle$, denn $\mathrm{ord}(y + \langle b \rangle) \big| \mathrm{ord}(y) \big| p^n$. Nach I.V. ist

$$A/\langle b \rangle = \langle x + \langle b \rangle \rangle \oplus \tilde{B}$$

für eine UG $\tilde{B} \leq A/\langle b \rangle$. Wir bezeichnen mit $\pi\colon A \to A/\langle b \rangle$ die Projektion und setzen

$$B = \pi^{-1}(\tilde{B}) = \{y \in A | \pi(y) \in \tilde{B}\}$$

B ist eine UG von A (Warum?) .
Beh.:

$$\forall y \in A \colon \exists! y_x \in \langle x \rangle, y_B \in \langle b \rangle \colon y = y_x + y_B$$

also $A = \langle x \rangle \oplus B$.
⌜

- **Existenz:** Betrachte $\pi(y) \in A/\langle b \rangle$, es gibt eindeutige $\tilde{y_x} \in \langle x + \langle b \rangle \rangle, x_B \in \tilde{B}$ s.d. $\pi(y) = \tilde{y_x} + y_{\tilde{B}}$. Es ist $\tilde{y_x} = \lambda x + \langle b \rangle$ für ein $\lambda \in \mathbb{Z}$ und $y_{\tilde{B}} = \pi(d)$ für ein $d \in B$. daraus folgt:

  $$\pi(y) = \pi(\lambda x + d) \Rightarrow \underbrace{y - \lambda x - d}_{:=f} \in \ker \pi = \langle b \rangle \subset B \Rightarrow y = \lambda x + d + f$$

- **Eindeutigkeit:** Sei $y = \lambda_1 x + z_1 = \lambda_2 x + z_2$, dann gilt

  $$\begin{aligned} \pi(y) &= \pi(\lambda_1 x + z_1) = \lambda_1 x + \langle b \rangle + z_1 + \langle b \rangle \\ &= \pi(\lambda_2 x + z_2) = \lambda_2 x + \langle b \rangle + z_2 + \langle b \rangle \end{aligned}$$

  wobei der jeweils erste Summand aus $\langle x + \langle b \rangle \rangle$, der zweite aus $\tilde{B}$ kommt. Aufgrund der Eindeutigkeit der Zerlegung in der I.V. gilt nun:

  $$\begin{aligned} \lambda_1 x + \langle b \rangle = \lambda_2 x \langle b \rangle &\Rightarrow (\lambda_1 - \lambda_2)(x + \langle b \rangle) = \langle b \rangle \\ &\Rightarrow \operatorname{ord}(x) = \operatorname{ord}(x + \langle b \rangle) \big| \lambda_1 - \lambda_2 \\ &\Rightarrow \lambda_1 x = \lambda_2 x \end{aligned}$$

  Daraus folgt schon die Eindeutigkeit auch des anderen Summanden:

  $$\lambda_1 x + z_1 = \lambda_1 x + z_2 \Rightarrow z_1 = z_2$$

⌟

□

Satz 1.8.13. *Sei A eine eea p-Gruppe, dann ist A zu einer direkten Summe von zyklischen Gruppen isomorph.*

Bew.: Wir induzieren wieder über l für $|A| = p^l$. Im Fall $l = 0$ haben wir die leere Summe, im Fall $l = 1$ ist A isomorph zu $\mathbb{Z}/p\mathbb{Z}$, damit ist der I.A. klar. Sei nun $l > 1$. Wir wählen $s \in A$ von maximaler Ordnung. Nach 1.8.12 gibt es $B \leq A$ s.d. $A = \langle x \rangle \oplus B$ und wegen $|B| \leq |A|$ können wir die I.V. anwenden:

$$B = \bigoplus_{i=1}^{r} \langle b_i \rangle \Rightarrow A = \langle x \rangle \oplus \bigoplus_{i=1}^{r} \langle b_i \rangle$$

□

Wir wollen nun noch die Eindeutigkeit dieser Zerlegung zeigen.

Satz 1.8.14. *Sei A eine abelsche Gruppe und darstellbar durch zwei Zerlegungen in zyklische Gruppen:*

$$A = Z_1 \oplus Z_2 \oplus \ldots \oplus Z_m = Y_1 \oplus Y_2 \oplus \ldots \oplus Y_l$$

Dann sind die Zerlegungen gleich bis auf Reihenfolge. Genauer: Aus $\nu_i = |Z_i|, \mu_i = |Y_i|$ und $\nu_1 \leq \ldots \leq \nu_m, \mu_1 \leq \ldots \leq \mu_l$ folgt $m = l$ und $\nu_1 = \mu_1, \ldots, \nu_m = \mu_m$.

Bew.: Wir schreiben $Y_i = \langle y_i \rangle, Z_i = \langle z_i \rangle$. Nun nehmen wir eine Induktion über l vor mit $|A| = p^l$. Für $l = 0$ ist die Aussage klar, für $l > 0$ setzen wir

$$N = \{a \in A | pa = 0\}$$

N ist eine UG von A (Warum?) . **Beh.:** $|N| = p^m$.

Für jedes $a \in A$, es gibt eine Darstellung $a = (\lambda_1 z_1, \ldots, \lambda_m z_m)$, wobei die $\lambda_i < p^{\nu_i}$ gewählt seien.

$$\begin{aligned} a \in N &\Leftrightarrow 0 = pa = (p\lambda_1 z_1, \ldots, p\lambda_m z_m) \\ &\Leftrightarrow p^{\nu_1} \big| p\lambda_1, \ldots, p^{nu_m} \big| p\lambda_m \\ &\Leftrightarrow p^{\nu_1 - 1} \big| \lambda_1, \ldots p^{\nu_m - 1} \big| \lambda_m \\ &\Leftrightarrow \forall 1 \leq i \leq n \colon \lambda_i \in \{p^{\nu_i - 1}, 2 \cdot p^{\nu_i - 1}, \ldots, (p-1)p^{\nu_i - 1}\} \end{aligned}$$

Also gilt:

$$N = \{(\alpha_1 p^{\nu_1 - 1} z_1, \ldots, \alpha_m p^{\nu_m - 1} z_m) \in A | \alpha_i \in [p-1]\}$$

Also ist $|N| = p^m$.

Nach gleicher Argumentation muss $|A| = p^l$ sein, also ist $l = m$. Es gilt nun

$$Z_1/\langle p^{\nu_1 - 1} z_1 \rangle \oplus \ldots \oplus Z_m/\langle p^{\nu_m - 1} z_m \rangle \simeq A/N \simeq Y_1/\langle p^{\mu_1 - 1} y_1 \rangle \oplus \ldots \oplus Y_m/\langle p^{\mu_m - 1} y_m \rangle$$

(Warum?)
Nach der Induktionsvoraussetzung ist dann aber $\nu_1 - 1 = \mu_1 - 1, \ldots, \nu_m - 1 = \mu_m - 1$, also $\nu_1 = \mu_1, \ldots, \nu_m = \mu_m$. □

Kapitel 2

Ringe

2.1 Definition von Ringen, Idealen und Homomorphismen

Definition. Ein Ring R (**assoziativ und mit 1**) ist eine abelsche Gruppe $(R, +)$ mit neutralem Element 0, zusammen mit einer Multiplikation

$$\cdot : R \times R \to R$$

sodass gilt

- **Assoziativität** $a(bc) = (ab)c \quad \forall a, b, c \in R$
- **Distributivität** $a(b + c) = ab + ac, \quad (b + c)a = ba + ca$
- **Existenz einer 1** es gibt $1_R \in R$, s.d. $a \cdot 1_R = a = 1_R a$.

Beispiel. Sei M eine abelsche Gruppe, dann ist die Menge der Endomorphismen auf M

$$\mathrm{End}(M)\{\varphi : M \to M | \varphi \text{ Gr. hom. } \}$$

ein Ring bezüglich $(\varphi + \psi)(x) = \varphi(x) + \psi(x)$ und $(\varphi \cdot \psi)(x) = \varphi(\psi(x))$. (Warum Ring? Warum M abelsch?)

Bemerkung.

1. R heißt kommutativ, falls $ab = ba \ \forall a, b \in R$.
2. Gilt $1 = 0$, so ist $R = \{0\}$ (Warum?)
3. Sei $(R_i)_{i \in I}$ Familie von Ringen, dann ist

$$\prod_{i \in I} R_i$$

mit elementweiser Mult. und Add. ein Ring. Ist $|I| = \infty$ und $R_i \neq \{0\}$, so ist $\bigoplus_{i \in I} R_i$ kein Ring, da $1 = (1_{R_i})_{i \in I} \notin \bigoplus R_i$.

Definition. Seien R, S Ringe, ein (einserhaltender) Ringhomomorphismus von R nach S ist ein Gruppenhomomorphismus $\varphi\colon (R,+) \to (S,+)$, so dass

- $\forall a, b \in R : \varphi(ab) = \varphi(a)\varphi(b)$
- $\varphi(1_R) = 1_S$

Definition.

- Ein Unterring U von R ist eine Teilmenge U von R, sodass
  - U ist ein Ring
  - Einbettung $U \hookrightarrow R$ ist ein Ringhomomorphismus, also U abgeschlossen bezüglich Multiplikation und Addition und $1_R \in U$.
- Sei $R \to S$ ein Ringhomomorphismus, so ist

$$\ker \varphi = \{r \in R \mid \varphi(r) = 0\}$$
$$\operatorname{im} \varphi = \{\varphi(a) | a \in R\}$$

(Sind Kern und Bild Unterringe?)

Definition. Sei R ein Ring. Eine Untergruppe $I \leq (R,+)$ heißt

$$\left\{\begin{array}{l}\text{Rechts-}\\ \text{Links-}\\ \text{beidseitiges}\end{array}\right. \textbf{Ideal}, \text{ falls } \left\{\begin{array}{ll}\forall a \in R,\ i \in I: & a \cdot i \in I\\ & i \cdot a \in I\\ & i \cdot a \in I \text{ und } a \cdot i \in I\end{array}\right.$$

Bemerkung.

- „Ideal“steht für beidseitiges Ideal Kern eines Ringhomomorphismus ist Ideal.
- Der Kern eines Ringhom. ist ein beidseitiges Ideal
- Für ein bereits rechts / links / beidseitiges Ideal gilt:

$$1_R \in I \implies I = R$$

(Warum?)

Definition. Sei R ein Ring und $I \subset R$ Ideal. Da $I \leq (R,+)$, ist R/I abelsche Gruppe. R/I wird ein Ring via

$$1_{R/I} := 1_R + I$$
$$(r+I)\cdot(s+I) := r \cdot s + I \tag{2.1}$$

(2.1) ist wohldefiniert, da für $a, b \in I$:

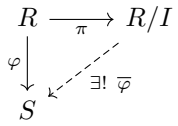
$$(r+a)\cdot(s+b) + I = rs + \underbrace{rb + as + ab}_{\in I} + I = rs + I$$

R/I heißt Quotientenring (oder Faktorring, Restklassenring). Die kanonische Projektion

$$\pi\colon R \to R/I \qquad r \mapsto r + I$$

ist ein Ringhom. (Warum?)

Satz 2.1.1. *Seien R, S Ringe und $\varphi\colon R \to S$ Ringhom., $I \subset R$ ein Ideal. Falls $I \subset \ker\varphi$, so gibt es eine eindeutige Abbildung $\overline{\varphi}\colon R/I \to S$ so dass das folgende Diagramm kommutiert:*



$\overline{\varphi}$ ist Ring. Hom

Bew.: Die Ex. und Eind. eines solchen **Gruppenhomorphismus'** folgen aus 1.2.3. (Ringhom. nachrechnen) . □

Korollar 2.1.2. *Seien R, S, φ wie in 2.1.1. Die Abbildung*

$$\overline{\varphi}\colon R/\ker\varphi \to \operatorname{im}\varphi \subset S$$

ist dann ein Ringisomorphismus.

Bew.: Benutze den Isomorphiesatz für Gruppen, nach diesem ist $\overline{\varphi}$ bijektiv und $\overline{\varphi}$ ist ein Ringhom. nach 2.1.1. □

Definition. Ein Element $r \in R$ heißt Einheit, falls es ein $s \in R$ gibt, sodass $s \cdot r = 1_R = r \cdot s$

Bemerkung.

- Bei Existenz ist s eindeutig, schreibe $r = s^{-1}$.
- Die Menge der Einheiten

$$R^* = \{r \in R \mid r \text{ ist Einheit}\}$$

ist eine Gruppe (Warum?) . Wir nennen sie Einheitengruppe von R.

Beispiel.

$$\mathbb{Z}^* = \{\pm 1\}$$
$$\operatorname{Mat}(n,k)^* = \operatorname{GL}(n,k)$$

wobei k ein Körper ist.

Bemerkung. Ist $R^* = R \setminus \{0\}$ (also $R \neq \{0\}$), so heißt R Schiefkörper oder Divisionsring. Ein kommutativer Divisionsring ist ein Körper.

(Fakt (ohne Bew.)) Jeder Divisionsring mit endlich vielen Elementen ist ein Körper.

2.2 Kommutative Ringe

Bemerkung. Für kommutative Ringe gilt Links- = Rechts- = beidseitiges Ideal.

Definition. Sei A ein komm. Ring. $M \subset A$ Teilmenge, dann ist

$$AM = \left\{ \sum_{m \in M} a_m m \mid a_m \in A, \text{ nur endlich viele } \neq 0 \right\}$$

das von M erzeugte Ideal.

Bemerkung.

- Es gilt

$$AM = \bigcap_{I \subset A \text{ Ideal mit } M \subset I} I$$

- Falls $M = \{m_1, \ldots, m_n\}$ endlich, so schreibt man auch

$$AM = (m_1, \ldots, m_n)$$

Definition. Sei A ein komm. Ring. Wie in der linearen Algebra definieren wir:

- Ein Nullteiler ist ein $n \in A$, s.d. $na = 0$ für $a \in A, a \neq 0$ ($n = 0$ ist immer Nullteiler.)
- Ein Integritätsbereich ist ein komm. Ring mit $1 \neq 0$, in dem 0 der einzige Nullteiler ist, z.B. $\mathbb{Z}$ und $\mathbb{Z}/p\mathbb{Z}$ mit p prim, aber nicht $\mathbb{Z} \oplus \mathbb{Z}$ oder $\mathbb{Z}/m\mathbb{Z}$ für m nicht prim.
- Ein Hauptideal ist ein Ideal $I \subset A$ der Form (a) für ein $a \in A$.
- Ein Hauptidealring ist ein Integritätsbereich, in dem jedes Ideal ein Hauptideal ist.

	$\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z}$	Körper K	$K[X]$	$K[X,Y]$
Int. ber.	✓	×	✓	✓	✓
HIR	✓	×	✓	✓	×

Definition. Sei A ein komm. Ring. Ein Ideal I heißt

- Primideal, falls $I \neq A$ und falls aus $a \cdot b \in I$ folgt, dass $a \in I$ oder $b \in I$.
- maximal, falls $I \neq A$ und falls es kein Ideal J mit $I \subsetneq J \subsetneq A$ gibt.

Bemerkung 2.2.1.

1. I prim $\Leftrightarrow$ A/I Int. ber.
2. I maximal $\Leftrightarrow$ A/I Körper
3. I maximal $\Rightarrow$ I prim.

Beispiel. In $\mathbb{Z}$ gilt:

- $\{0\}$ ist prim, aber nicht maximal
- $n\mathbb{Z}$ für $n > 0$ ist prim und maximal, wenn n prim ist (Warum?) .

Quotientenkörper

Definition. Sei A ein Integritätsbereich, betrachte auf $A\times(A\setminus\{0\}$ die Äquiv.rel. $(a,b) \sim (a',b') \Leftrightarrow ab' = ba'$ (Warum Äquivalenzrelation?) . Setze $Q(A) = A \times (A \setminus \{0\})/\sim$. Schreibe $\frac{a}{b}$ für die Klasse von (a,b) bzgl. $\sim$. (Sinnvoll, da für $c \neq 0$ gilt $\frac{ca}{cb} = \frac{a}{b}$). Definiere nun

$$\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd} \qquad \frac{a}{c} \cdot \frac{c}{d} = \frac{ac}{bd}$$

(Warum repräsentantenunabhängig?) Dann ist $Q(A)$ ein Körper (Warum? Was ist Inverses?) , der Quotientenkörper von A.

Bemerkung. Die Abb.

$$\iota\colon A \to Q(A) \qquad a \mapsto \frac{a}{1}$$

ist ein inj. Ringhom., denn:

$$\frac{a}{1} = 0 \Leftrightarrow (a,1) \sim (0,1) \Leftrightarrow a \cdot 1 = 1 \cdot 0 \Leftrightarrow a = 0$$

Beispiel.

1. $Q(\mathbb{Z}) = \mathbb{Q}$
2. Wenn K ein Körper ist $K \xrightarrow{\iota} Q(K)$, ist ein Isomorphismus.

2.3 Teilbarkeit

In diesem Kapitel ist A immer ein Integritätsbereich.

Definition. Seien $a, b \in A$, wir sagen

- a teilt b (schreibe $a\big|b$) falls eine der äquivalenten Bedingungen
  - $\exists x \in A : xa = b$
  - $(a) \supset (b)$

  gilt (Warum äquivalent?) .
- a ist assoziiert zu b (schreibe $a \sim b$) falls eine der äquivalenten Bedingungen
  - $\exists c \in A^* : ac = b$
  - $(a) = (b)$

  gilt (Warum äquivalent?) . Dies ist eine Äquivalenzrelation, dies macht die zweite Bedingung deutlich. Die Äquivalenzklassen sind Orbits der A^*-Wirkung auf A.
- a ist prim (oder Primelement) falls eine der äquivalenten Bedingungen
  - $a \neq 0, a \notin A^*$ und $\forall u, v \in A : a\big|uv \Rightarrow a\big|u \vee a\big|v$
  - (a) ist ein Primideal

gilt (Warum äquivalent?) .

- a ist unzerlegbar (oder irreduzibel) falls eine der äquivalenten Bedingungen
  - $a \neq 0, a \notin A^*$ und es gilt:
    $$a = uv \ (u, v \in A) \Rightarrow u \in A^* \vee v \in A^*$$
  - $\{0\} \neq (a) \neq A$ und
    $$(\exists v \in A \colon (a) \subset (v)) \Rightarrow (a) = (v) \vee (v) = A$$

  gilt (Warum äquivalent?) .

Bemerkung 2.3.1. 1) Für $a \in A$ gilt a prim $\Rightarrow$ a unzerlegbar.

Sei $a = uv$ also $a \mid uv$ und weil a prim ist, gilt $a \mid u$ oder $a \mid v$. O.B.d.A. gilt $ax = u$ für ein $x \in A$. Damit ist $a = axv$, also $a(1 - xv) = 0$. Weil A ein Int.ber. ist, ist $1 = xv$, also $v \in A^*$.

2) Sei A nun ein Hauptidealring.

- Sei $I \subset A$ ein Ideal, s.d. $I \neq \{0\}$, dann gilt I prim $\Leftrightarrow$ I maximal.

  „$\Leftarrow$ “: 2.2.1
  „$\Rightarrow$ “: A ist ein HIR, also $I = (a)$ mit a prim nach äquivalenter Charakterisierung eines Primideals. Nach Teil 1) ist a unzerlegbar. Nach Definition und da A ein HIR ist, ist (a) dann auch maximal.

- für $a \in A$ gilt a prim $\Leftrightarrow$ a unzerlegbar.

  „$\Rightarrow$ “: Teil 1, „$\Leftarrow$“: (a) max. $\Rightarrow$ (a) prim $\Rightarrow$ a prim.

Satz 2.3.2. *Betrachte die Aussagen:*

1. *Jedes $a \in A$ mit $a \neq 0, a \notin A^*$ lässt sich als Produkt $a = u_1, \ldots, u_n$ von unzerlegbaren Elementen $u_i \in A$ schreiben.*
2. *Die u_i in 1) sind eindeutig bis auf Reihenfolge und Einheiten. D.h. falls $a = v_1, \ldots, v_m$, dann $m = n$ und $u_i \sim v_{\sigma i}$ mit geeigneter Permutation σ*
3. *Jedes unzerlegbare El. ist prim.*

Es gilt $1) \wedge 2) \Leftrightarrow 1) \wedge 3)$.

Definition. Ein Int. ber. A der eine äquivalente Bedingung in 2.3.2 erfüllt, heißt faktorieller Ring.

Beispiel. Es sind

- Z
- $k[X_1, \ldots, X_n]$

faktorielle Ringe.

Beweis von 2.3.2: „$\Rightarrow$“: Sei u unzerlegbar.
Beh.:

$$\forall a, b \in A \colon u \big| ab \Rightarrow u \big| a \vee u \big| b$$

⌜

Es gilt $xu = ab$. Man kann annehmen, dass $a, b \neq 0$ (Warum?) . Falls $a \in A^*$ oder $b \in B^*$, sind wir fertig (Warum?) . Seien also $a, b \notin A^*$ und $a, b \neq 0$. Dann ist auch $x \neq 0, x \neq x \notin A^*$. Somit können wir schreiben:

$$\begin{aligned} x &= x_1 \cdots x_r \\ a &= a_1 \cdots a_s \\ b &= b_1 \cdots b_t \end{aligned}$$

wobei x_i, a_i, b_i alle unzerlegbar sind. Dann ist $x_1 \cdots x_r \cdot u = a_1 \cdots a_s b_1 \cdots b_t$, da die Zerlegung der Produkte eindeutig ist und u unzerlegbar ist, muss $u = a_i$ oder $u = b_i$ sein, also $u \big| a \vee u \big| b$.

⌟

„$\Leftarrow$“: Sei eine Zerlegung $a = u_1 \cdots u_n$ aus unzerlegbaren u_i von a gegeben, $a = v_1 \cdots v_m$ eine weitere Zerlegung. Da $u_1 \big| a$ folgt $u_1 \big| v_1 \cdot (v_2 \cdots v_m)$ und weil u prim ist (da irreduzibel), gilt $u_1 \big| v_1$ oder $u_1 \big| v_2 \cdot (v_3 \cdots v_m)$. (Da v_j unzerlegbar ist, folgt $u_1 \big| v_j \Rightarrow u_1 \sim v_j$). Es gibt also ein $j \in \{1, \ldots, m\}$ s.d. $u_1 \sim v_j$. Also $u_2 \cdots u_n = v_1 \cdots \hat{v_j} \cdots v_m$. Induktiv sieht man $m = n$ und $u_i \sim v_{\sigma i}$ für eine Permutation σ. □

Satz 2.3.3. *Jeder Hauptidealring ist faktoriell*

Bew.: Aus LA ⇝ PDF auf der Website □

Definition. Sei A ein Int. ber. und $a, b \in A$.

1) $d \in A$ heißt größter gemeinsamer Teiler von a und b $\mathrm{ggT}(a, b)$, falls

- $d \big| a$ und $d \big| b$
- $$\forall u \in A \colon u \big| a \wedge u \big| b \Rightarrow u \big| d$$

2) $d \in A$ heißt kleinstes gemeinsames Vielfaches von a und b $\mathrm{kgV}(a, b)$, falls

- $a \mid a$ und $b \mid d$
- $$\forall u \in A \colon a \mid u \wedge b \mid u \Rightarrow d \mid u$$

Bemerkung. 1) *ggT* sind eindeutig bis auf Einheiten, falls sie existieren.

2) In fakt. Ringen (insb. in HIR) existieren ggT und kgV.

Sei A ein fakt. Ring. Sei $\mathcal{P}$ ein Repräsentantensystem der Äquivalenzklassen bzgl. $\sim$ von unzerlegbaren Elementen (=Repr. der A^*-Orbits von unz. Einheiten). Jedes $a \in A, a \neq 0$ kann eind. als

$$a = e \prod_{p \in P} p^{\nu(a)_p}$$

mit $\nu(a)_p \in \mathbb{Z}_{\geq 0}, e \in A^*$ geschrieben werden. Das Produkt ist endlich. Wir können wählen:

$$\mathrm{ggT}(a,b) = \prod_{p \in P} p^{\min(\nu(a)_p, \nu_(b)_p}$$
$$\mathrm{kgV}(a,b) = \prod_{p \in P} p^{\max(\nu(a)_p, \nu_(b)_p}$$

(Warum?)

3) Sei A ein HIR, dann gilt:

$$(\mathrm{ggT}(a,b)) = (a) + (b) = (a,b)(\mathrm{kgV}(a,b)) = (a) \cap (b)$$

2.4 Polynomringe

Definition. Sei A ein komm. Ring. Ein Polynom in einer Unbekannten X mit Koeff. in A ist ein Ausdruck der Form

$$p = \sum_{k=1}^{n} a_k X^k$$

wobei $n \geq 0, a_k \in A$. Die Menge solcher Polynome nennen wir $A[X]$. Formal definiert man:

$$A[X] := \{p \colon \mathbb{Z}_{\geq 0} \to A || \{j \in \mathbb{Z}_{\geq 0} | p(j) \neq 0\}| \in \mathbb{N}_0\}$$

$A[X]$ ist mit Mult. und Add. von Polynomen ist ein kommutativer Ring mit 1.

$A[X_1, \ldots, X_n]$ sind die Polynome in n unbekannten $X_1, \ldots, X_n$ mit Koeffizienten in A, wir schreiben diese als:

$$p = \sum_{j_1, \ldots, j_n \in Z_{\geq 0}} a_{j_1 \ldots j_n} X_1^{j_1} \cdots X_n^{j_n}$$

mit endlich vielen $a_{j_1 \dots j_n} \neq 0$. Formal definiert man:

$$A[X_1, \dots, X_n] := \{p \colon (\mathbb{Z}_{\geq 0})^n \to A || \{u \in (\mathbb{Z}_{\geq 0})^n | p(u) \neq 0\}| \in \mathbb{N}_0\}$$

Noch allgemeiner definieren wir für eine beliebige Menge I die Menge $A[(X_i)_{i \in I}]$ als Polynomring mit Unbekannten X_i für $i \in I$. Wir schreiben

$$p = \sum_{\alpha \in J} a_\alpha \prod_{i \in I} X_i^{\alpha_i}$$

wobei

- $J \subset \prod_{i \in I} \mathbb{Z}_{\geq 0}$ endl. Teilmenge und $\alpha \in J$ hat nur endlich viele $\alpha_i \neq 0$
- $a_\alpha \in A$ $(\alpha \in J)$.

Formal:

$$A[(X_i)_{i \in I}] = \left\{ p \colon \prod_{i \in I} \mathbb{Z}_{\geq 0} \to A \,\middle|\, p \neq 0 \text{nur für endliche viele } u \in \prod_{i \in I} \mathbb{Z}_{\geq 0} \text{ und nur für } u \text{ mit endlich vielen } u_i \neq 0 \right\}$$

$A[(X_i)_{i \in I}]$ ist komm. Ring.

Bemerkung. Ein Polynom ist in diesem Rahmen etwas anderes als eine Funktion wie aus der Analysis. Sei z.B. $A = \mathbb{Z}/2\mathbb{Z}$ und $p = X^2 + X$, bzw.

$$p \colon \mathbb{Z}_{\geq 0} \to \mathbb{Z}/2\mathbb{Z} \qquad \begin{array}{ccc|ccc} 0 & \mapsto & 0 + 2\mathbb{Z} & 1 & \mapsto & 1 + 2\mathbb{Z} \\ 2 & \mapsto & 1 + 2\mathbb{Z} & \geq 3 & \mapsto & 0 + 2\mathbb{Z} \end{array}$$

Ersetze $X \rightsquigarrow 0 + 2\mathbb{Z}$, dann $X^2 + X = 0 + 2\mathbb{Z}$ genauso für $X \rightsquigarrow 1 + 2\mathbb{Z}$. Also ist die FUnktion $x \mapsto x^2 + x$ identisch 0 auf $\mathbb{Z}/2\mathbb{Z}$.

Satz 2.4.1. *Seien A, B kommutative Ringe und $\varphi \colon A \to B$ ein Ringhom.. Für jede Wahl $(b_i)_{i \in I}$ mit $b_i \in B$, gibt es genau einen Ringhom.*

$$\tilde{\varphi} \colon A[(X_i)_{i \in I}] \to B$$

mit $\tilde{\varphi}(X_i) = b_i$ für $i \in I$ und $\tilde{\varphi}(a) = \varphi(a)$.

Bew.:

- **Existenz:** Setze für $J \subset \prod_I \mathbb{Z}_{\geq 0}$ endlich:

$$\tilde{\varphi}\left(\sum_{u \in J} a_u \prod_{i \in I} X_i^{u_i} \right) := \sum_{u \in J} \varphi(a_u) \cdot \prod_{i \in I} b_i^{u_i} \tag{2.2}$$

  (Prüfe Ringhom.)

- **Eindeutigkeit:** Die Ringhom. Eigenschaft erzwingt (2.4.1).

□

Bemerkung. Für $A = B$ und $\varphi = \mathrm{id}_A$ heißt die Abb. $A[(X_i)_{i \in I}] \to A$ aus 2.4.1 Einsetzhomomorphismus. Schreibe für $I = \{1, \dots, n\}$ z.B. $p(b_1, \dots, b_n)$ statt $\tilde{\varphi}(p)$.

2.4.1 Polynome in einer Unbekannten

In diesem Abschnitt ist A ein kommutativer Ring.

Bemerkung. $A[X,Y] \simeq (A[X])[Y]$ etc.

Definition. Der Grad von p ist

$$\operatorname{grad} p = \begin{cases} \max\{i \mid a_i \neq 0\} & \text{für } p \neq 0 \\ -\infty & \text{für } p = 0 \end{cases}$$

Bemerkung 2.4.2. Seien $f, g \in A[X]$, dann

- $\operatorname{grad}(f+g) \leq \max\{\operatorname{grad} f, \operatorname{grad} g\}$
- $\operatorname{grad}(f \cdot g) \leq \operatorname{grad} f + \operatorname{grad} g$ und falls A ein Integritätsbereich ist, gilt sogar Gleichheit. (Warum? Gegenbeispiel wenn kein Int.ber.?)

Bemerkung 2.4.3.

1) Es gilt A Int. ber. $\Leftrightarrow$ $A[X]$ Int. ber. (Warum?) . Da $A[X_1, \ldots, X_n] \simeq (A[X_1, \ldots, X_{n-1}][X_n])$ folgt induktiv A Int. ber. $\Leftrightarrow$ $A[X_1, \ldots, X_n]$ Int. ber.. Damit auch A Int. ber. $\Leftrightarrow$ $A[(X_i)_{i\in I}]$ Int. ber.. (Warum?) . Hinweis: In $ab = 0$ haben a und b nur endlich viele Unbekannte.

2) Ist A ein Int.ber. so gilt

$$A^* = (A[X])^* = (A[(X_i)_{i\in I}])^*$$

(Warum?)

Satz 2.4.4. *Sei A ein komm. Ring, dann gilt $A[X]$ Hauptidealring $\Leftrightarrow$ A Körper.*

Lemma 2.4.5. *Sei A ein komm. Ring. Für $g \in A[X]$ ist $g = g_n X^n +$ (niedrigere X-Potenzen) mit $g_n \in A^*$. Für jedes $f \in A[X]$ gibt es eindeutige $q, r \in A[X]$ mit $\operatorname{grad} r < \operatorname{grad} g$ s.d. $f = gq + r$*

2.5 Nullstellen von Polynomen

In diesem Abschnitt ist A stets ein kommutativer Ring.

Definition. Ein $a \in A$ heißt Nullstelle von $f \in A[X]$, falls $f(a) = 0$

Satz 2.5.1. *Sei $f \in A[X], f \neq 0$. Man kann f schreiben als*

$$f = g \cdot (x - a_1) \cdots (x - a_n)$$

für ein $n \geq 0$ und $a_i \in A$, so dass g keine Nullstelle in A besitzt. Es gilt $n \leq \operatorname{grad} f$.

Bew.: Sei a ein Nullstelle von f nach 2.4.5 gilt: $f = q \cdot (x - a) + r$, wobei $\operatorname{grad} r < 1$, d.h. $r \in A$. Da a Nullstelle ist:

$$0 = f(a) = q(a - a) + r \quad \text{also } r = 0$$

Rekursiv erhalten wir so mit $f = f_1$. Ist a_i Nullstelle von f_i, so setze f_{i+1}, so dass $f_i = f_{i+1} \cdot (x - a_i)$ Diese Rekursion bricht nach spätestens $\operatorname{grad} f$ Schritten ab, denn für $g \cdot (x - a_1) \cdots (x - a_n)$ gilt Gradformel mit „=“ (Warum?) . □

Definition. Falls $g \in A$ in der Darstellung von Satz 1, so sagen wir f zerfällt in Linearfaktoren.

Satz 2.5.2. *Ist A Int.ber. und $f \in A[X], f \neq 0$, so bestitzt f höchstens* $\operatorname{grad} f$ *Nullstellen.*

Bew.: Schreibe

$$f = g \cdot (X - a_1) \cdots (X - a_n) \qquad \text{wie in Satz 1}$$

Angenommen $f(b) = 0$ für ein $b \neq a_i, \forall i \in \{1, \ldots, n\}$ Dann

$$0 = f(b) = \underbrace{g(b)}_{\neq 0 \text{ nach Konstr.}} \underbrace{(b - a_1)}_{\neq 0 (*)} \cdots \underbrace{(b - a_n)}_{\neq 0 (*)} \underset{(**)}{\neq} 0$$

$(*)$ da $b \neq a_i, \forall i$. $(**)$ da A Int.ber.. Dies ist ein Widerspruch. □

Korollar 2.5.3. *A unendlicher Int.ber.. Seien $f, g \in A[X], f \neq g$ Dann gibt es $a \in A$, so dass $f(a) \neq g(a)$*

Bew.: $f - g$ hat nur endlich viele Nullstellen (nach 2.5.2). □

Beispiel.

1. $\mathbb{Z}, \mathbb{Z}^* = \{\pm 1\}$
2. $\mathbb{C}, \mathbb{C}^* = \mathbb{C} \setminus \{0\}$ unendlich daher nicht zyklisch
3. $\mathbb{R}, \mathbb{R}^* = \mathbb{R} \setminus \{0\}$ unendlich daher nicht zyklisch
4. $\{e^{2\pi i \frac{n}{N}} \mid n \in \mathbb{Z}\}$ für ein $N \in \mathbb{Z}_{>0}$ ist endlich und zyklisch
5. K endlicher Körper (z.B. $K = \mathbb{Z}/p/Z, p$ prim)
   - mult $\to K^* = K \setminus \{0\}$ ist zyklische Gruppe
   - add $\to \mathbb{Z}^s/n\mathbb{Z}$ mit $n = |K| - 1$

Satz 2.5.4. *Jede endliche Untergruppe der Einheitengruppe eines Int. ber. ist zyklisch.*

Bew.: Sei $G \leq A^*$ endlich (G ist abelsch=

$$\underset{??}{\Rightarrow} G = \bigoplus_{p \text{ prim}} \overbrace{A_p}^{p \text{ prim Komponente}}$$

Beh.: $A_p \neq \{0\}$ ist zyklisch

Angenommen A_p sei nicht zyklisch. Sei $|A_p| = p^n$ für eine $n > 0$ und $x \in A_p$ von maximaler Ordnung. Dann $\operatorname{ord} x = p^l$ mit $l < n$ (sonst $\langle x \rangle = A_p$). Betrachte das Polynom $f = X^{p^l} - 1 \in A[X]$. Nach 2.5.2 hat f, da A ein Integritätsbereich ist, maximal p^l Nullstellen. Aber für alle $a \in A_p$ gilt $\operatorname{ord} a = p^k$ und $k \leq l$, da p^l max. Ordnung. Daraus folgern wir $a^{p^l} = 1$, also $f(a) = 0$ für alle $a \in A_p$ aber $|A_p| = p^n > p^l$, was nicht sein darf, da wir dann zu viele Nullstellen gefunden hätten, dies ist ein Widerspruch.

⌟

Somit gibt es paarweise verschiedene Primzahlen $p_1, \ldots, p_m \in \mathbb{N}$ und $n_1, \ldots, n_m \in \mathbb{N}$ so dass gilt

$$G = \bigoplus_{i=1}^{m} A_{p_i} \simeq \bigoplus_{i=1}^{m} \mathbb{Z}/p_i^{n_i}\mathbb{Z}$$
$$\underset{(*)}{=} \mathbb{Z}/(p_1^{n_1} \cdots p_m^{m_n})$$

mit $|A_{p_i}| = p_i^{n_i}$. $(*)$ gilt nach dem chinesischem Restsatz, da die $p_i^{m_i}$ teilerfremd sind. □

2.6 Polynomringe über faktoriellen Ringen

Ziel: Sei A ein komm. Ring, dann gilt:
A faktoriell $\Leftrightarrow$ $A[X]$ faktoriell
Bew.: „$\Leftarrow$ “ist klar und „$\Rightarrow$ “braucht Vorbereitung.

Für den Rest des Kapitels soll gelten, dass A ein faktorieller Ring ist und $\mathcal{P}$ Repräsentanten der Äquivalenzklassen der unzerlegbaren (=prim) Elemente bzgl. Assozierheit „$\sim$ “.

Wir haben bereits gelernt: Jedes $a \neq 0$ lässt sich **eindeutig** als

$$a = (\text{Einheit}) \prod_{p \in \mathcal{P}} p^{\nu_p(a)} \quad \text{mit } \nu_p(a) \in \mathbb{Z}_{\geq 0}$$

schreiben. Dies definiert Funktionen $\nu_p \colon A \setminus \{0\} \to \mathbb{N}$. Es gilt für $a, b \neq 0$:

$$a \sim b \Leftrightarrow \forall p \in \mathcal{P} \colon \nu_p(a) = \nu_p(b)$$

Erweitere auf $Q(A)^*$:

Definition. Sei $q = \frac{a}{b}$ Setze

$$\nu_p(q) = \nu_p(a) - \nu_p(b) \in \mathbb{Z}$$

(Warum unabh. von Wahl von a, b?) . Dies definiert wieder Funktionen $\nu_p \colon Q(A)^* \to \mathbb{Z}$.

Für $q \in Q(A)^*$ gilt

$$q = (\text{Einheit aus } A) \prod_{p \in \mathcal{P}} p^{\nu_p(q)}$$

mit eindeutigen $\nu_p(q)$. (Warum eindeutig) .
Für $f \in Q(A)[X], f \neq 0$ setze mit $f = \sum_{k=1}^{n} a_k X^i$

$$\nu_p(f) = \min\{\nu_p(a_k) \mid k = 0, \ldots, n \text{ und } a_i \neq 0\}$$

Definition. Der Inhalt $c(f)$ von $f \in Q(A)[X], f \neq 0$, ist

$$c(f) = \prod_{p \in \mathcal{P}} p^{\nu_p(f)} \in Q(A)^*$$

Bemerkung. Für $q \in Q(A)^*$ und $f \in Q(A)[X], f \neq 0$ gilt

$$c(qf) \underset{(*)}{\sim} q\ c(f)$$

$(*)$ Auch für $x, y \in Q(A)$ soll $x \sim y$ (sind assoziiert) heißen, dass $x = ay$ für ein $a \in A^*$.

Lemma 2.6.1. *Sei $f \in Q(A)[X], f \neq 0$.*

1) Es gibt $a, b \in A, f_0 \in A[X]$ s.d.

- $f = \frac{a}{b} f_0$
- $c(f_0) = 1$ *und* $\mathrm{ggT}(a, b) \sim 1$

und a, b, f_0 sind bis auf Einheiten eindeutig.

2) Für $f \in A[X]$ ist $b \sim 1$ und $a \sim c(f)$.

Bew.:

1) • **Existenz Beh.:**

$$\frac{1}{c(f)} f \in A[X]$$

Sei

$$f = \sum_{k=0}^{n} q_k X^k$$

Es gilt

$$\frac{q_k}{c(f)} = (\text{Einheit von } A) \cdot \prod_{p \in \mathcal{P}} p^{\underbrace{\nu_q(q_k) - \min\{\nu_p(q_l) | l = 0, \ldots, n, q_l \neq 0\}}_{\geq 0}}$$

Setze $f_0 := \frac{1}{c(f)} f$. Dann

$$c(f_0) = c\left(\frac{1}{c(f)} f\right) \sim \frac{1}{c(f)} \cdot c(f) = 1$$

Dann ist $c(f_0) = 1$ (Warum?) . Damit haben wir:

$$c(f) = \underbrace{\prod_{\substack{p \in \mathcal{P} \\ \nu_p(f) > 0}} p^{\nu_p(f)}}_{:= a} \underbrace{\prod_{\substack{p \in \mathcal{P} \\ \nu_p(f) < 0}} p^{\nu_p(f)}}_{:= \frac{1}{b}}$$

Dann $a, b \in A$ und $\mathrm{ggT}(a, b) \sim 1$ (Warum?) .

- **Eindeutigkeit:** Seien $f = \frac{a}{b} f_0 = \frac{a'}{b'} f_0$ Zerlegungen wie in 1). Dann

$$ab' f_0 = a' b f_0' \tag{2.3}$$

$$(2.3) \Rightarrow \underbrace{c(ab' f_0)}_{\sim ab' c(f_0)} = \underbrace{c(a' b f_0')}_{\sim a' b c(f_0')}$$

Somit $ab' \sim a'b$. Insb.: $a \mid a'b$ und da $\mathrm{ggT}(a,b) = 1$ folgt weiter $a \mid a'$ (Warum?) . Genauso gilt $a' \mid a, b \mid b', b' \mid b$, also $a \sim a', b \sim b'$

2) Aus $f = \frac{a}{b} f_0$ wie in 1) folgt

$$c(f) \sim \frac{a}{b} c(f_0) \overset{c(f_0)=1}{\Rightarrow} bc(f) \sim a$$

Also $b \mid a$, aber $\mathrm{ggT}(a,b) \sim 1$ und somit $b \sim 1$, dann auch $c(f) \sim a$.

□

Lemma 2.6.2. *Seien A, B komm. Ringe und $\varphi \colon A \to B$ Ringhomomorphismen. Dann ist*

$$\varphi_* \colon A[X] \to B[X] \qquad \sum a_i X^i \mapsto \sum \varphi(a_i) X^i$$

ein Ringhomomorphismus.

Bew.:

$$A \xrightarrow{\varphi} B \hookrightarrow B[X]$$

und $\psi = \iota \circ \varphi$. Nach 2.4.1 gibt es einen eind. Ringhom. $A[X] \xrightarrow{\varphi_*} B[X]$ s.d. $\varphi_*|_A = \psi$ und $\varphi_*(X) = x$. □

Definition. Ist $I \subset A$ ein Ideal und $\pi \colon A \to A/I, a \mapsto a + I$ die kanonische Projektion, so bekommt man die Reduktion der Koeffizienten nach I als:

$$\pi_* \colon A[X] \to A/I[X] \qquad \sum a_i X^i \mapsto \sum (a_i + I) X^i$$

Lemma 2.6.3. *Sei A ein komm. Ring und I ein Ideal in A. Dann gilt: I prim in $A \Leftrightarrow I[X]$ prim in $A[X]$.*

Bew.: Sei π_* wie in der vorigen Definition. Dann

$$\ker \pi_* = I[X] \qquad \wedge \qquad \pi_* \text{ surj.}$$

Also gilt die Ringisomorphie:

$$A[X]/I[X] \simeq A/I[X] \tag{2.4}$$

und somit

$$I[X] \text{ prim in } A[X] \underset{2.2.1}{\Leftrightarrow} A[X]/I[X] \text{ Int. ber.} \underset{(2.4)}{\Leftrightarrow} A/I\,[X] \text{ Int. ber.}$$
$$\underset{2.4.3}{\Leftrightarrow} A/I \text{ Int. ber.} \Leftrightarrow I \text{ prim in } A$$

□

Satz 2.6.4. *Sei A ein fakt. Ring. Für $f, g \in Q(A)[X]$ mit $f, g \neq 0$ gilt $c(fg) = c(f)c(g)$.*

Bew.: Nach 2.6.1 ist $f = \frac{a}{b} f_0, g = \frac{c}{d} g_0$. Dann $c(f) \sim \frac{a}{b}, c(g) \sim \frac{c}{d}$ und

$$c(fg) \sim \frac{ac}{bd} c(f_0 g_0) \sim c(f)c(g)c(f_0 g_0)$$

Beh.: $c(f_0 g_0) \sim 1$

⌜

Angenommen $c(f_0 g_0) \not\sim 1$, dann gibt es ein $p \in \mathcal{P}$ mit $p \mid c(f_0 g0)$.
Betrachte

$$\pi_* \colon A[X] \to A/(p)[X]$$

p unz. $\underset{A\text{fakt.}}{\Rightarrow}$ p prim $\Rightarrow (p)$ prim $\Rightarrow A/(p)$ Int. ber. $\Rightarrow A/(p)\,[X]$ Int. ber.

Nun $\pi_*(f_0) \neq 0$ und $\pi_*(g_0) \neq 0$, da $c(f_0) = 1 = c(g_0)$. Aber

$$0 = \pi_*(f_0 g_0) = \pi_*(f_0)\pi_*(g_0) \neq 0$$

wobei letztere Ungleichung gilt, da $A/(p)\,[X]$ ein Int. ber. ist, dies ist ein Widerspruch.

⌟

Damit $c(fg) \sim c(f)c(g)$, also auch $c(fg) = c(f)c(g)$ (Warum?) .

Bemerkung. Sei A ein fakt. Ring, $f \in Q(A)[X]$. Dann gilt

$$f \in A[X] \Leftrightarrow c(f) \in A$$

Denn „$\Rightarrow$“ ist klar. „$\Leftarrow$“ folgt mit 2.6.1 denn $f = \frac{a}{b} f_0 \Rightarrow c(f) \sim \frac{a}{b} \in A$.

Lemma 2.6.5. *Sei A ein faktorieller Ring. $f \in A[X]$ erfülle: $f \neq 0$ und*

$$\begin{cases} \operatorname{grad} f = 0: & f \text{ unzerlegbar in } A \\ \operatorname{grad} f > 0: & f \text{ unzerlegbar in } Q(A)[X] \text{ und } c(f) = 1 \end{cases}$$

Dann ist f prim (in $A[X]$).

Bew.:

- $\operatorname{grad} f = 0$: $f \in A$ unz. $\overset{A \text{ fakt}}{\Rightarrow}$ f prim in A $\overset{\text{Def.}}{\Longrightarrow}$ Af prim in A $\overset{\text{Lemma 3}}{\Rightarrow}$ $\underbrace{(Af)[X]}_{=A[X]f}$ prim in $A[X]$ $\overset{\text{Def}}{\Rightarrow}$ f prim in $A[X]$
- $\operatorname{grad} f > 0$: $R = Q(A)[X]$ ist HIR (2.4.4). Also gilt für $r \in R$ nach 2.3.1

  $$r \text{ prim } \Leftrightarrow r \text{ unz.}$$

  Also ist f prim und Rf ist Primideal. Es folgt, dass $Rf \cap A[X]$ in $A[X]$ prim ist (Warum?) .
  Beh.: $Rf \cap A[X] = A[X]f$

  ⌜

$A[X]f \subset Rf$ ✓Sei umgekehrt $r \cdot f \in A[X]$ mit $(r \in R, r \neq 0)$.
Dann ist nach 2.6.4

$$c(rf) = c(r) \cdot c(f) = c(r) \Rightarrow c(r) \in A \Rightarrow r \in A[X]$$

Nun sind wir fertig, da deswegen f prim in $A[X]$ ist.

□

Satz 2.6.6. *Sei A ein faktorieller Ring. Dann*

a) $A[X]$ faktoriell

b) $f \in A[X]$ unzerlegbar genau dann, wenn f die Bedingung an 2.6.5 erfüllt

Sei $g \in A[X], g \neq 0, g \notin A[X]^*$
Beh. 1: $g = f_1 \cdots f_n$, wobei f_i wie in 2.6.5.

- $\operatorname{grad} g = 0$: Dann $g \in A$ und $g = u_1 \cdots u_m$, u_i unz. in A, da A faktoriell ✓
- $\operatorname{grad} g > 0$: $Q(A)[X]$ ist ein HIR nach 2.4.4.
  $\overset{2.3.3}{\Rightarrow} Q(A)[X]$ ist faktoriell
  $\overset{\text{Def}}{\Longrightarrow} g = u_1 \cdots u_m$ wobei u_i unz. in $Q(A)[X]$
  Nach 2.6.1 ist $u_i = \frac{a_i}{b_i} u_{i,0}$ wobei $u_{i,0} \in A[X], c(u_{i,0}) = 1$ und unz. in $Q(A)[X]$. Also

$$g = \underbrace{\frac{a_1 \cdots a_n}{b_1 \cdots b_n}}_{(*)} u_{1,0} \cdots u_{m,0}$$

  entweder ist $(*)$ in A^* (dann $u_{1,0} \rightsquigarrow \frac{a_1 \cdots a_n}{b_1 \cdots b_n} u_{1,0}$) oder $(*)$ ist ein Produkt unzerlegbarer Elemente in A.

Beh. 2: g unz. in $A[X] \Leftrightarrow g$ prim in $A[X]$

„⇐“: ist klar, da $A[X]$ Integritätsbereich (2.3, Bem 1) „⇒“: $g = f_1 \cdots f_m$ wie in Beh 1. Da g unz. ist, gilt $m = 1$ also $g = f_1$, also g prim nach Lemma 5.

a) Nach Beh 1 & Beh 2 können alle $g \in A[X], g \neq 0, g \notin A[X]^*$ als Prod. von unz. El. geschrieben werden. Nach Beh. 2 ist prim äquiv. zu unzerlegbar, also ist $A[X]$ nach 2.3.2 faktoriell.

b) „⇐“: f ist wie in 2.6.5 bedeutet f prim. deshalb ist f unz. in $A[X]$.

„⇒“: f ist unz. in $A[X]$. Wie in Beh. 2 gilt $f = f_1 \cdots f_m$ mit $m = 1$.

□

Korollar 2.6.7. *Ist A ein fakt. Ring, so sind $A[X_1, \ldots, X_n]$ und $A[(X_i)_{i \in I}]$ fakt.*

2.6.1 Zwei Unzerlegbarkeitskriterien

Satz 2.6.8. *Sei A ein fakt. Ring, $p \in A$ unzerlegbar. Sei*

$$f = \sum_{i=0}^{n} f_i X^i \in A[X]$$

s.d.

- $f_n \neq 0$ *also* $\operatorname{grad} f = n > 0$.
- $p \nmid f_n$
- $p \mid f_i$ $(i = 0, \ldots, n-1)$
- $p^2 \mid f_0$

Dann ist f in $Q(A)[X]$ unzerlegbar.

Beispiel. Sei $A = \mathbb{Z}$, $p = 3$ und

$$f = 2X^7 + 18X^5 + 6X + 30$$

dann ist f unz. in $Q[X]$ aber zerl. in $\mathbb{Z}[X]$ als $2 \cdot (\ldots)$.

Bew.: Angenommen $f = gh$ für $g, h \in Q(A)[X]$ und $\operatorname{grad} g, \operatorname{grad} h < n$ (dies ist gleichbedeutend damit, dass $g, h \notin Q(A)[X]^*$). Nach 2.6.1 und 2.6.4 können wir $g, h \in A[X]$ wählen (Warum?) . Betrachte

$$\pi_* \colon A[X] \to A/(p)[X]$$

Wir schließen:

$$p\text{unz.} \Rightarrow p \text{ prim} \Rightarrow (p) \text{ prim} \Rightarrow A/(p) \text{ Int. ber.} \Rightarrow A/(p)\,[X] \text{ Int. ber.}$$

Es gilt $\pi_*(gh) = \pi_*(g)\pi_*(h)$. $\pi(f_i) = 0$ für $i = 0, \ldots, n-1$, deshalb ist $\pi_* = \pi(f_n)X^n$. Sei $L = Q(A/(p))$. Dann gilt auch in $L[X]$:

$$0 \neq \pi(f_n)X^n = \pi_*(g)\pi_*(h)$$

Da $L[X]$ nach 2.4.4 ein HIR ist, ist $L[X]$ auch faktoriell, es folgt

$$X \mid \pi_*(g) \qquad \wedge \qquad X \mid \pi_*(h)$$

denn da X unz. in $L[X]$ ist und der Faktor X^n auch in $\pi_*(g)\pi_*(h)$ auftauchen muss (nach Eind. der Zerl. in unz. El), aber $\pi_*(g)$ und $\pi_*(h)$ einen Grad kleiner n haben.

ALso $\pi($ kleinster Term von g oder $h) = 0$. Aber aus $g = \ldots + g_0$ und $h = \ldots + h_0$ mit $p \mid g_0$ und $p \mid h_0$ folgt

$$f = gh = \underbrace{\ldots}_{\text{höher}} + g_0 h_0$$

mit $p^2 \mid f_0$, was den Voraussetzungen widerspricht. □

Satz 2.6.9 (Reduktionskriterium)**.** *Sei A ein fakt. Ring $I \subset A$ ein Primideal in A. Schreibe*

$$\pi\colon A \to A/I \qquad \pi_*\colon A[X] \to A/I[X]$$

Sei

$$f = \sum_{i=0}^{n} f_i X^i \in A[X]$$

mit $\pi(f_n) \neq 0$ und $n > 0$. Ist $\pi_*(f)$ unz. in $A/I[X]$ oder in $Q(A/I)[X]$, so ist f unz. in $Q(A)[X]$.

Bew.: Wir nehmen an, dass f in $Q(A)[X]$ zerlegbar ist, also wie in 2.6.8. Sei ferner $f = gh$ mit $\operatorname{grad} g, \operatorname{grad} h < n$ und $g, h \in A[X]$. Dann $\pi_*(f) \neq 0$ und keine Einheit (da $\operatorname{grad} f > 0$) und $\pi_*(f) = \pi_*(g)\pi_*(h)$ in $(A/I)[X]$ wobei $\pi_*(g), \pi_*(h)$ keine Einheiten in $A/I[X]$ oder $Q(A/I)[X]$ sind (Warum?) . Dies ist ein Widerspruch zu $\pi_*(f)$ unzerlegbar. □

Bemerkung 2.6.10. Nochmal Satz 6b. Sei A ein fakt. Ring mit $f \in A[X]$, $f \neq 0, \operatorname{grad} f > 0$. Es gilt

$$f\text{unz. in } A[X] \Leftrightarrow f\text{unz. in } Q(A)[X] \quad \text{und } c(f) = 1$$

Beispiel. Wir betrachten die unz. in $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$.
Die unzerlegbaren Polynome vom Grad 1 sind X und $X+1$, vom Grad 2 ist nur X^2+X+1 unzerlegbar. Betrachte nun $7X^2+11X+3 \in \mathbb{Z}[X]$ mod 2 ergibt dies X^2+X+1 und da dies unzerlegbar ist, ist $7X^2+11X+3 \in \mathbb{Z}[X]$ unzerlegbar in $\mathbb{Q}[X]$.

Kapitel 3

Körper

3.1 Körpererweiterungen

Definition. Sei L ein Körper. $K \subset L$ heißt Teilkörper, falls K ein Körper und ein Unterring von L und

$$k \in K, k \neq 0 \Rightarrow k^{-1} \in K$$

gilt. L heißt Erweiterungskörper von K und man sagt L/K ([1]) ist eine Körpererweiterung. Sei $M \subset L$ Teilmenge. Der von M erzeugte Teilkörper ist der kleinste Teilkörper von L, der M enthält. Ist L/K Körpererweiterung, so bezeichnet $K(M)$ den von $K \cup M$ erzeugten Teilkörper von L.

Definition. Sei K wieder ein Körper. Der Primkörper P von K ist der kleinste Teilkörper von K, also der von $\{0, 1\}$ erzeugte Teilkörper.

Satz 3.1.1. *Der Primkörper eines Körpers ist isomorph zu $\mathbb{F}_p$ für eine geeignete Primzahl p, oder zu $\mathbb{Q}$.*

Bew.: Betrachte den Ringhomomorphismus $\varphi\colon \mathbb{Z} \to K$, $n \mapsto n \cdot 1$. Da $\operatorname{im}\varphi$ keine Nullteiler enthält, ist $\ker\varphi$ prim, also folgt aus

- $\operatorname{im}\varphi \subset P$
- $\ker\varphi = p\mathbb{Z}$ für (p prim) oder $\ker\varphi = \{0\}$ nach Z7/A6
- $\mathbb{Z}/\ker\varphi$ ist Int. ber. und $\overline{\varphi}\colon \mathbb{Z}/\ker\varphi \to K$ ist injektiv.
- K enthält $Q(\mathbb{Z}/\ker\varphi)$ nach Z8/A4

□

Definition. Sei $\varphi\colon \mathbb{Z} \to K$ wie im Beweis. Wir sagen K hat Charakteristik

$$\operatorname{char}(K) = \begin{cases} 0 & \text{falls } \varphi \text{ injektiv, also } P \cong \mathbb{Q} \\ p & \text{falls } \varphi \text{ nicht injektiv und } |P| = p \end{cases}$$

Bemerkung 3.1.2. 1) Sei L/K eine Körpererweiterung, dann ist L ein K-VR (Warum?)

[1] Dies ist nur eine Notation, bedeutet nicht Quotient

2) Sei L/K eine Körpererweiterung mit $|L| < \infty$. Dann ist $\operatorname{char} L = p$ mit p prim und L endl. dim. K Vektorraum und $|L| = p^n$ für ein $n > 0$ (Warum?) . Später werden wir zeigen: Für alle p prim und $n > 0$ gibt es bis auf Isomorphie genau einen Körper mit p^n Elementen.

Definition. Sei L/K eine Körpererweiterung. $\dim_K L$ heißt der Grad von L über K, schreibe

$$[L : K] := \dim_K L \in \mathbb{N}_0 \cup \{\infty\}$$

Satz 3.1.3. *Sind L/K und M/L Körpererweiterungen, so gilt*

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

Bew.: Ist $(e_i)_{i\in I}$ eine K-Basis von L und $(f_j)_{j\in J}$ eine L-Basis von M, so ist $(e_i f_j)_{I\times J}$ eine K-Basis von M (Warum?) . □

Definition. Sei L/K eine Körpererweiterung und $a \in L$

$$\exists! \iota_a \colon K[X] \to L$$

Ringhomomorphismus mit $\iota(X) = a$ und $\iota(k) = k$ für $k \in K$. Wir nennen $a \in L$ transzendent über K, falls ι_a injektiv ist und sonst algebraisch über K.

Bemerkung. Für a sind äquivalent:

$$a\text{trans}_K \Leftrightarrow \nexists f \in K[X] \setminus \{0\} \colon f(a) = 0$$
$$a\text{alg}_K \Leftrightarrow \exists f \in K[X] \setminus \{0\} \colon f(a) = 0$$

Schreibe $K[a] := \operatorname{im} \iota_a$ das Bild von ι_a.

Satz 3.1.4. *Sei L/K eine Körpererweiterung und $a \in L$. Dann sind äquivalent:*

a) a ist algebraisch über K

b) $K[a] = K(a)$

c) $\dim_K K(a) < \infty$

Bew.: a) ⇒ b): Nach 2.4.1 ist $K[X]$ ein HIR. also ist $\ker \iota_a = (f)$ für ein $f \in K[X]$. Per Ann. ist $f \neq 0$. $\operatorname{im} \iota_a$ ist ein Int. ber., da es der Unterring eine Körpers ist, also folgt:

$$\operatorname{im} \iota_a \simeq K[X]/\ker \iota_a \Rightarrow (f) \text{ prim } \Rightarrow (f) \text{ max. } \Rightarrow K[X]/\ker \iota_a \text{ Körper}$$

somit ist auch $\operatorname{im} \iota_a = K[a]$ ein Körper, also ist $K(a) \subset K[a]$. Andererseits ist für jedes Polynom $f \in K[X]$ auch

$$f(a) = \sum_{k=0}^{n} f_k a^k \in K(a)$$

also ist auch $K[a] \subset K(a)$.
b) ⇒ c): Sei $a \neq 0$, denn für $a = 0$ ist nichts zu zeigen, dann wäre nämlich $K(a) = K$. Betrachte a^{-1}. Da $K[a] = K(a)$ gibt es $h \in K[X]$ s.d. $h(a) = a^{-1}$, wobei $h(a) = a^n + t.l.o.$ Dann ist $a \cdot h(a) - 1 = 0$ also $a^{n+1} = \sum_{k=0}^{n} c_k a^k$ für

$c_k \in K$. Somit wird der K-VR $K[a]$ von den Elementen $1, a, \ldots, a^n$ erzeugt. Somit

$$\dim_K K(a) = \dim_K K[a] < \infty$$

c) $\Rightarrow$ a): Wenn a nicht algebraisch über K ist, dann ist die Funktion ι_a injektiv, also ist ι_a ein Vektorraumisomorphismus über K von $K[X]$ nach $K[a] \subset K(a)$. Dann muss aber $K(a)$ eine höhere Dimension als $K[X]$ haben. $K[X]$ hat die Basis $1, X, X^2, \ldots$ und ist somit unendlich-dimensional, also ist dann auch $\dim_K K(a) = \infty$.

Definition. Ein Polynom $f \in K[X]$, $f \neq 0$ heißt normiert, falls

$$f = 1 \cdot X^n + t.l.o.$$

für ein $n \geq 0$.

Satz 3.1.5. *Sei K ein Körper, $I \subset K[X]$ ein Ideal.*

1) $K[X]/I$ Körper $\Leftrightarrow$ $I = (f)$ mit f unzerlegbar ($\Leftrightarrow$ f prim)

2) Sei L/K eine Körpererweiterung $a \in L$ algebraisch. Es existiert ein eind. normiertes Polynom $m_{a,K} \in K[X]$ s.d.

$$\overline{\iota_a} \colon K[X]/(m_{a,K}) \to K(a)$$

ein Körperisomorphismus ist.

Bew.:

1) $K[X]$ ist ein HIR nach 2.4.4. Also gilt:

$$K[X]/I \text{ist Körper} \Leftrightarrow I \text{ max.} \Leftrightarrow I \text{ prim}$$

2) Sei $\ker \iota_a = (f) = (g)$. Dann ex. $u \in K^*$ s.d. $f = ug$ (Warum?) . Somit existiert ein normiertes Polynom mit $\ker \iota_a = (m_a, K)$ und

$$\overline{\iota_a} \colon K[X]/(m_a, K) \to K[a] = K(a)$$

□

Definition. $m_{a,K}$ heißt Minimalpolynom von a über K.

Bemerkung. In der linearen Algebra war das Minimalpolynom der Erzeuger des Kerns von:

$$K[X] \to \mathrm{End}_K(V) \qquad p \mapsto p(A)$$

Satz 3.1.6. *Sei K ein Körper, $f \in K[X]$ unz. $L = K[X]/(f)$. Dann ist $[L : K] = \operatorname{grad} f$ und*

$$\{1 + (f), X + (f), \ldots, X^{n-1} + (f)\}$$

ist eine K-Basis von L

Bew.: Schreibe $a := X + (f)$. Da $(f) = 0$ in L ist, folgt $a^n + t.l.o. = 0$ in L. Also

$$L = \text{span}_K\{1, a, \ldots, a^{n-1}\}$$

Angenommen, es gibt $c_k \in K$ für $k \in \{0, \ldots, n-1\}$ nicht alle 0 mit

$$\sum_{k=0}^{n-1} c_k a^k = 0$$

Dann

$$\sum_{k=0}^{n-1} c_k X^k \in (f)$$

was nicht sein kann, da das Polynom ungleich 0 in $K[X]$ ist und Grad kleiner n hat, in (f) aber nur Polynome vom Grad mindestens n und das Nullpolynom enthalten sind. □

Korollar 3.1.7. *Sei L/K eine Körpererweiterung und $a \in L$ algebraisch, $n = \text{grad}\, m_{a,K}$. Dann $[K(a) : K] = n$ und $\{1, a, \ldots, a^{n-1}\}$ ist K-Basis von $K(a)$.*

Beispiel. Betrachte $\mathbb{R}/\mathbb{Q}$ und $a = \sqrt{q}$ für ein $q \in Q$ mit $q > 0$.

$$\iota_a \colon \mathbb{Q}[X] \to \mathbb{R}$$

hat Kern $(m_a, \mathbb{Q})$. Klar ist $X^2 - q \in \ker \iota_a$. Also entweder $\text{grad}\, m_{a,\mathbb{Q}} = 2$, (dann $m_{a,\mathbb{Q}} = X^2 - q$ (Warum?)) oder $\text{grad}\, m_{a,\mathbb{Q}} = 1$ (dann $m_{a,\mathbb{Q}} = X - \sqrt{q}$ also $\sqrt{q} \in \mathbb{Q}$. Mit $\nu_p \colon \mathbb{Q} \to \mathbb{Z}$ gilt $\sqrt{q} \in \mathbb{Q} \Leftrightarrow \nu_p(q) \in 2\mathbb{Z}$ für alle p prim.

Also gilt für $q = \frac{c}{d}$ mit $\text{ggT}(c, d) = 1$ und $c$oder d keine Quadrat, dass $[Q(\sqrt{q}) : \mathbb{Q}] = 2$ und $\{1, \sqrt{q}\}$ sind $\mathbb{Q}$-Basis von $\mathbb{Q}(\sqrt{q})$.

Definition. Eine Körpererweiterung L/K heißt

- endlich, falls $[L : K] < \infty$
- endlich erzeugbar, falls $L = K(a_1, \ldots, a_n)$ für geeignete $a_i \in L$.
- algebraisch, falls **alle** $a \in L$ algebraisch über K sind.

Beispiel.

$Q(K[X])/K$ ist endlich erzeugbar (Durch was?) aber nicht endlich, da $1, X, X^2, \ldots$ linear unabhängig über K (da $K[X] \hookrightarrow Q(K[X])$ Einbettung)

Satz 3.1.8. *a) L/K endlich $\Rightarrow$ L/K alg.*

b) L/K alg. und endlich erzeugt $\Rightarrow$ L/K endlich

c) L/K und M/L alg. $\Rightarrow$ M/K alg.

Beispiel. Betrachte $\mathbb{C} \setminus \mathbb{Q}$ Sei

$$L = \{a \in \mathbb{C} | a \text{ alg}_\mathbb{Q}\}$$

L ist $\text{alg}_\mathbb{Q}$ per Konstruktion.
Beh.: L ist nicht endlich erzeugbar.
⌜

Nach Satz 8 reicht es zu zeigen, dass $L/\mathbb{Q}$ nicht endlich ist. Sei p prim, dann ist $X^n - p$ unzerlegbar in $\mathbb{Q}[X]$ (Warum?) . Also ist $X^n - p$ min. Polynom $m_{\sqrt[n]{p}}$. Da $\mathbb{Q}(\sqrt[n]{p}) \subset L$ und

$$[\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}] = \operatorname{grad} X^n - p = n$$

Somit ist L unendlich-dim. über $\mathbb{Q}$.

⌟

Bemerkung. Wir beurteilen die Richtigkeit der Umkehrungen der Aussagen von 3.1.8

- a) $\not\Leftarrow$ nach Beispiel
- b) $\Leftarrow$ ✓
- c) $\Leftarrow$ ✓
- L/K alg. $\not\Rightarrow$ L/K endlich erzeugt (Bsp 2)

Bew. von 3.1.8:

a) Sei $n := [L : K] < \infty$. Sei $a \in L$ beliebig. Dann sind $1, a, a^2, \ldots, a^n$ lin. abhängig über K da $\dim_K L = n$.

b) $L = K(a_1, \ldots, a_n)$ mit $a_i \in L$. Es ist $K(a_1)_K$ endlich, da a_1 alg_K ist (3.1.4). Da a_2 alg_K ist, ist auch a_2 $\operatorname{alg}_{K(a_1)}$ und somit ist $K = (a_1, a_2) = (K(a_1))(a_2)$ endlich über $K(a_1)$. Induktiv erhalten wir nach diesem Vorgehen die Erkenntnis, dass $K(a_1, \ldots, a_i)$ endlich über $K(a_1, \ldots, a_{i-1})$ ist. Nach 3.1.3 gilt dann

$$\begin{aligned}[K(a_1, \ldots, a_n) : K] &= [K(a_1, \ldots, a_n) : K(a_1, \ldots, a_{n-1})] \cdot [K(a_1, \ldots, a_{n-1}) : K] \\ &= \ldots = \prod_{i=0}^{n-1} [K(a_1, \ldots, a_{i+1}) : K(a_1, \ldots, a_i)] < \infty\end{aligned}$$

c) Sei $a \in M$ beliebig. **Beh.:** $K(a)/K$ ist endlich

⌜

$$a \operatorname{alg}_L \Rightarrow \exists f \in L[X] \colon f(a) = 0$$

Sei $f = \sum_{k=0}^{n} f_k X^k$ Dann $f \in K(f_0, \ldots, f_n)[X] \subset L[X]$ somit

$$a \operatorname{alg}_{K(f_0,\ldots,f_n)} \Rightarrow [K(f_0, \ldots, f_n, a) : K(f_0, \ldots, f_n)] < \infty$$

Ferner $K(f_0, \ldots, f_n)$

- endl. erz. über K
- algebraisch über K, da $K(f_0, \ldots, f_n) \subset L$ und L/K algebraisch.

Nach Teil b) ist $[K(f_0, \ldots, f_n) : K] < \infty$. Dann

$$[K(a) : K] \leq [K(a, f_0, \ldots, f_n) : K]$$

⌟

□

3.2 Algebraischer Abschluss

Satz 3.2.1. *Sei K ein Körper. Es sind äquivalent*

1. *Jedes $f \in K[X], f \notin K$ besitzt Nullstellen in K*
2. *Jedes $f \in K[X], f \notin K$ ist von der Form*

$$f = c(X - a_1) \cdots (X - a_n) \quad c, a_i \in K, n \geq 1$$

3. *Die Menge der normierten unzerlegbaren Polynome ist $\{X - a \mid a \in K\}$*
4. *Ist L/K algebraisch, so gilt $L = K$*

Bew: Übungen.

Definition. Erfüllt K eine der Bedingungen aus Satz 1, so heißt K algebraisch abgeschlossen.

Bemerkung. $\mathbb{C}$ ist abgeschlossen. Dies darf in den Übungen und in Bsp. ohne Beweis verwendet werden, in Beweisen werden wir aber ohne diese Aussage auskommen.

Satz 3.2.2. *Far jeden Körper K gibt es eine Körpererw. $L \supset K$ mit L alg. abgeschlossen.*

Lemma 3.2.3. *Sei K ein Körper $f \in K[X]$ $\operatorname{grad} f \geq 1$. Es gibt eine Körpererweiterung $L \supset K$ mit $[L : K] \leq \operatorname{grad} f$ s.d. f in L eine Nullstelle hat.*

Bew.: Schreibe $f = g \cdot h$ mit g unzerlegbar in $K[X]$, dies ist möglich, da $K[X]$ faktoriell ist. Setze $L = K[X]/(g)$. Dies ist ein Körper nach 3.1.5. Üb.: L erfüllt Bed. in Lemma 3.

Lemma 3.2.4. *Sei A ein komm. Ring. Sei $I \subsetneq A$ ein Ideal. Dann existiert ein maximales Ideal $M \subsetneq A$ mit*

$$I \subset M \subsetneq A$$

Bew.: via Lemma von Zorn auf Website.

Bew. von Satz 2: Wir werden die Bedingung 1 von 3.1.3 zeigen:
Jedes $f \in L[X]$ hat eine Nullst. in L $\quad (*)$
Die Idee ist, einen „Turm von Körpern“zu bauen

$$K \subset L_1 \subset L_2 \subset L_3 \subset \ldots$$

so dass:
Jedes $f \in K[X]$ hat Nullstelle in L_1
Jedes $f \in L_1[X]$ hat Nullstelle in L_2
Jedes $f \in L_2[X]$ hat Nullstelle in L_3
...
Beh.: Dann erfüllt

$$L = \bigcup_{i=1}^{\infty} L_i$$

die Bedingung $(*)$

Sei $f \in L[X] \setminus L$ beliebig, dann auch $f \in L_k[X]$ für ein k (Warum?) . Somit hat f Nullstellen in $L_{k+1} \subset L$.

Konstruktion von L_1: Setze $I = K[X] \setminus K$ und betrachte den Polynomring in unendlich vielen Variablen

$$A := K[(X_f)_{f \in I}]$$

Betrachte

$$N = \langle f(X_f) \mid f \in I \rangle$$

(Bem: In A/N hat jedes $f \in K[X] \setminus K$ eine Nullstelle, nämlich $X_f + N$)
Beh: $N \neq A$

Wir nehmen an $1 \in N$. Dann gibt es $a_1, \ldots, a_n \in A$ und $f_1, \ldots, f_n \in I$, so dass

$$1 = \sum_{k=1}^{n} a_k f_k(X_{f_k})$$

Rekursives anwenden von Lemma 3 ergibt Körpererweiterung M/K, so dass jedes $f_i (i = 1, \ldots, n)$ eine Nullstelle in M hat, sagen wir s_i. Setze $J = I \setminus \{f_0, f_1, \ldots, f_n\}$. Betrachte Ringhomomorphismus (existiert nach 2.4.1):

$$\begin{aligned} \varphi \colon K[(X_f)_{f \in I}] &\to M[(X_f)_{f \in J}] \\ k \in K &\mapsto k \in M \\ X_{f_i} (i = 1, \ldots, n) &\mapsto s_i \\ X_g (g \in J) &\mapsto X_g \end{aligned}$$

Dann

$$1 = \varphi(1) = \sum_{k=1}^{n} \varphi(a_k) \cdot \underbrace{f_k(s_k)}_{=0} = 0$$

Dies ist ein Widerspruch.

In A/N gilt $f(X_f) = 0$, also hat jedes $f \in K[X]$ eine Nullstelle in A/N. Sei M maximales Ideal mit $N \subset M \subsetneq A$. Setze A/M. Der Ringhom.:

$$K \hookrightarrow K[(X_f)_{f \in I}] \to A \to A/M$$

ist nicht 0 und somit injektiv. Somit ist L_{1K} eine Körpererw. s.d. jedes $f \in K[X]$ eine Nullstelle in L_1 hat. Iteriere Konstruktion, erhalte Turm $K \subset L_1 \subset L_2 \subset \ldots$ von Körpererw. wie gewünscht. □

Satz 3.2.5. *Sei K ein Körper. Es gibt eine Körpererw. $\overline{K}/K$ s.d.*

- *$\overline{K}$ ist alg. abg.*
- *$\overline{K}/K$ ist algebraisch.*

Definition. Ein $\overline{K}/K$ mit den Eigenschaften aus Satz 5 heißt ein algebraischer Abschluss von K.

Bew. von Satz 5: Betrachte eine Körpererw. L/K alg. abg. (eine solche ex. nach 3.2.2). Setze

$$\overline{K} = \{a \in L | a \text{ ist algebraisch über } K\}$$

- $\overline{K}$ ist ein Teilkörper von L (Warum? Wie in Kapitel 3.1)
- $\overline{K}/K$ ist alg. per Konstruktion.
- $\overline{K}$ ist algebraisch abgeschlossen.

Sei $f \in \overline{K}[X] \setminus \overline{K}$. Dann hat f eine Nullst. $s \in L$. Also hat f auch eine Nullstelle in $\overline{K}(s)$. Nun sind $\overline{K}(s)/\overline{K}$ und $\overline{K}/K$ algebraisch. Nach 3.1.7 ist $\overline{K}(s)/K$ algebraisch, also ist s algebraisch über K somit ist $s \in \overline{K}$.

Satz 3.2.6. *Seien K, K' Körper und $\sigma\colon K \to K'$ sowie $\sigma_*\colon K[X] \to K'[X]$ Homomorphismen, außerdem $L/K, L'/K'$ Körpererweiterungen. Seien $a \in L, a' \in L'$ s.d. $m_{a',K'} = \sigma_*(m_{a,K})$, so folgt*

$$\exists! \varphi\colon K(a) \to K'(a')$$

mit φ ist Hom. und $\varphi|_K = \sigma$ und $\varphi(a) = a'$. Ist σ ein Isom. so ist auch φ ein Isomorphismus.

Bew.:

- **Eindeutig**: klar, da φ auf K und a festgelegt ist und K und a $K(a)$ als Körper erzeugen.
- textbfExistenz:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & (m_{a,K}) & \hookrightarrow & K[X] & \xrightarrow{\iota_a} & K(a) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \sigma_*} & & \downarrow{\scriptstyle \sigma_*} & \searrow^{\psi} & \vdots{\scriptstyle \exists\varphi} & & \\ 0 & \longrightarrow & (m_{a',K'}) & \hookrightarrow & K'[X] & \xrightarrow{\iota_{a'}} & K'(a') & \longrightarrow & 0 \end{array}$$

(warum kommutiert das erste Diagramm?)

also gib es ein (eindeutiges) φ so dass $\varphi \circ \iota_a = \psi$ (Warum gilt $\varphi(a) = a'$)

- **Bijektivität**: Ist σ bijektiv, so ist φ surjektiv (denn dann liegen K' und a' im Bild von φ) und φ ist sowieso injektiv.

□

Satz 3.2.7. *Wir setzen K, K', σ, L, L' wie in 3.2.6. Sei σ ein Isomorphismus. Dann*

$$\#\{\textit{Hom. } \varphi\colon K(A) \to L' \textit{ mit } \varphi|_K = \sigma\} = \#\{\textit{Nullst. von } \sigma_*(m_{a,K}) \textit{ in } L'\}$$

Bew.: Konstruiere zueinander inverse Abbildungen

$$\{\text{Hom. } \ldots\} \xrightarrow{A} \{\text{Nullst. } \ldots\}$$
$$\{\text{Hom. } \ldots\} \xleftarrow{B} \{\text{Nullst. } \ldots\}$$

- **A: Beh.:** Sei $f \in K[X]$, dann

$$b \in K(a) \text{ ist Nullst. von } f \Leftrightarrow \varphi(b) \in L' \text{ ist Nullst. von } \sigma_*(f)$$

$$f(b) = 0 \Leftrightarrow \varphi(f(b)) = 0 \Leftrightarrow \sum_k \varphi(f_k)(\varphi(b))^k = 0 \Leftrightarrow (\sigma_*(f))(\varphi(b)) = 0$$

Also ist $\varphi(a)$ eine Nullstelle von $\sigma_*(m_{a,K})$. Setze $A(\varphi) := \varphi(a)$.

- **B:** Sei $a' \in L$ eine Nullst. von $\sigma_*(m_{a,K})$. Dann $m_{a',K'} = \sigma_*(m_{a,K})$ (Warum?) . Nach 3.2.6 gibt es genau ein $\varphi\colon K(a) \to K'(a')$ mit $\varphi|_K = \sigma$ und $\varphi(a) = a'$. Setze $B(a') := \varphi$. A und B sind invers zueinander (Warum?) .

□

Satz 3.2.8. *Seien K, M Körper M alg. abg. und $\sigma\colon K \to M$ ein Homomorphismus. Für jede **algebraische** Körpererw. L/K gibt es eine Fortsetzung von σ auf L, d.h.*

$$\exists \tilde{\sigma}\colon L \to M \qquad \tilde{\sigma}|_K = \sigma$$

Bew.: siehe Website

Satz 3.2.9. *Seien K, k' Körper, $\overline{K}$ ein alg. Abschluss von K und $\overline{K'}$ von K'. Jeder Iso $K \to K'$ lässt sich zu einem Iso $\overline{K} \to \overline{K'}$ fortsetzen.*

Für den Beweis brauchen wir:

Lemma 3.2.10. *Seien $K, K', \overline{K}, \overline{K'}$ wie in 3.2.9. Jeder Hom. $\varphi\colon \overline{K} \to \overline{K'}$ mit $K' \subset \operatorname{im}\varphi$ ist ein Isomorphismus.*

Bew.: φ ist klarerweise injektiv, wir zeigen, dass φ surjektiv ist. Sei $M = \operatorname{im}\varphi \subset \overline{K'}$, dann

- M ist alg. abg. (Warum?)
- $K' \subset M \subset \overline{K'}$ per Annahme
- $\overline{K'}/M$ ist alg. da $\overline{K'}/K'$ algebraisch ist.

□**Bew. von Satz 9:** Sei $\sigma\colon K \to K'$ ein Isomorphismus. Außerdem $\overline{K}/K$ alg. per Definition und $\overline{K'}$ ist alg. abg. Nach 3.2.8 gibt es

$$\varphi\colon \overline{K} \to \overline{K'} \qquad \text{mit } \varphi|_K = \sigma$$

nach 3.2.10 ist φ ein Isom. □

Definition. Seien L/K und L'/K Körpererweiterungen. Ein Homomorphismus $\sigma\colon L \to L'$ heißt K-Homomorphismus falls $\sigma|_K = \mathrm{id}_K$. Ferner definieren wir:

- K-Isomorphismus σ ist K-Hom. und bijektiv.
- K-Automorphismus σ ist K-Iso. und $L = L'$

Beispiel. $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \{\mathrm{id}, \text{Konj.}\}$, aber $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{C})$ hat unendliche viele Elemente

Korollar 3.2.11. *Sei L/K eine Körpererw. und $a, b \in L$ algebraisch. Falls $m_{a,K} = m_{b,K}$, so gibt es genau einen K-Isom. $K(a) \to K(b)$ der a auf b abbildet.*

Beispiel. Betrachte $\mathbb{C}/\mathbb{Q}$. Sei $d \in \mathbb{Z}$ und $d \geq 2$ enthält Primfaktor p aber nicht p^2 für ein p . Dann ist $X^n - d$ unz. in $\mathbb{Q}[X]$ (Eisenstein) .

- $n = 2$ es sind $\sqrt{d}, -\sqrt{d}\mathbb{R} \subset \mathbb{C}$ sind ide Nullstellen von $X^2 - d$ und $X^2 - d$ ist Mininmalpolynom von $\sqrt{d}$ und $-\sqrt{d}$. Also gibt es nach 3.2.11 einen $\mathbb{Q}$-Iso.

  $$\varphi\colon \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(-\sqrt{d})$$

  mit $\varphi(a + b\sqrt{d}) = a - b\sqrt{d}$ für $a, b \in \mathbb{Q}$. Hier ist sogar $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(-\sqrt{d})$.

- $n = 3$ Setze $r = \sqrt[3]{d} \in \mathbb{R}$. Dann ist über $\mathbb{C}$:

  $$X^3 - d = (X - r)(X - re^{\frac{2\pi i}{3}})(X - re^{-\frac{2\pi i}{3}})$$

  und $r, re^{\frac{2\pi i}{3}}, re^{-\frac{2\pi i}{3}}$ haben das Minimalpolynom $X^3 - d$ über $\mathbb{Q}$. Also gibt es einen $\mathbb{Q}$-Isom

  $$\mathbb{Q}(r) \to \mathbb{Q}(re^{\frac{2\pi i}{3}}) \not\subset \mathbb{R}$$

Korollar 3.2.12. *Sei K ein Körper. Zwischen je zwei alg. Abschlüssen von K gibt es einen Körperisomorphismus. Deswegen sagen wir **der** alg. Abschluss statt **ein** alg. Abschluss.*

3.3 Zerfällungskörper

Definition. Sei K ein Körper, $f \in K[X], \operatorname{grad} f \geq 1$. Ein Erweiterungskörper L heißt Zerfällungskörper von f über K, falls

- f zerfällt in $L[X]$ in Linearfaktoren
- L wird von den Nullstellen von f über K erzeugt.

In Formeln

- $$f = c \prod_{i=0}^{\operatorname{grad} f} (X - a_i) \quad c, a_i \in L$$
- $$L = K(a_1, \ldots, a_{\operatorname{grad} f})$$

Bemerkung 3.3.1. 1) a) Setze $f_0 := f$. Nach 2.5.1 kann man f_0 schreiben als $f_0 = g(X - a_1) \cdots (X - a_l)$ für $g \in K[X], a_i \in K$ so dass $l \geq 0$ und g keine Nullstellen in K hat. Wenn $g \in K^*$ ist, sind wir fertig. Wenn $g \notin K^*$ ist, dann sei u ein beliebiger unz. Faktor von g. Dann $\operatorname{grad} u \geq 2$ (Warum?) und u (also auch g) hat eine Nullstelle b_1 in $L_1 = K[X]/(u)$. Also $b_1 = X + (g)$. Setze $L_1 = K(b_1)$. Wiederhole diesen Schritt mit mit $f_1 = g \in L_1[X]$ etc. bis das Verfahren abbricht. Das letzte L_m ist ein Zerfällungskörper von f über K, da

$$L = L_m = ((K(b_1))(B_2)\ldots) = K(b_1, \ldots, b_m)$$

b) Betrachte algebraischen Abschluss $\overline{K}$ von K. In $\overline{K}$ gilt

$$f = c \prod_{i=0}^{n} (X - d_i) \quad (n = \operatorname{grad} f)$$

Also gilt: Ein Zerfällungskörper L von f ist $L = K(d_1, \ldots, d_n)$

2) Ist L ein Zerfk. von $f \in K[X] \setminus K$, dann

$$[L : K] \leq (\operatorname{grad} f)!$$

(Warum?)

Satz 3.3.2. *Sei K ein Körper und $f \in K[X] \setminus K$.*

1) Je zwei Zerfällungskörper von f sind K-isom.

2) Sind L, L' Zerfällungskörper von f, so bildet jeder K-Iso. $L \to L'$ sie Nullstellen von f in L (bij.) auf die Nullstellen von f in L' ab.

Bew.: Wir brauchen **Beh.:** Seien $M/K, M'/K$ Körpererweiterungen, so dass f in $M[X]$ und $M'[X]$ in Linearfaktoren zerfällt. Sei $\varphi\colon M \to M'$ ein K-Isomorphismus. Dann gilt: a Nullstelle von f in $M \Leftrightarrow \varphi(a)$ Nullstelle von f in M'.

In $M[X]$ gilt mit $\operatorname{grad} f = n$, dass

$$f = c\prod_{i=1}^{n}(X - a_i)$$

Also in $M'[X]$

$$\varphi_*(f) = \varphi_*(c\prod(X - a_i)) = c\prod(X - \varphi(a_i))$$

und $\varphi_*(f) = f$, da $f \in K[X]$. Also sind $\varphi(a_i)$ genau die Nullstellen von f in M', da f nach 2.5.2 $\leq n$ Nullstellen hat.

⌟

1. Seien L, L' zwei Zerfällungskörper von f über K und $\overline{L}/L$ der algebraische Abschluss von L. Da $\overline{L}/L$ alg. und L/K alg. ist $\overline{L}$ auch ein algebraischer Abschluss von K. Genauso folgt, dass $\overline{L'}/K$ ein algebraischer Abschluss von K ist. Mit 3.2.12 existiert K-Iso. $\psi\colon \overline{L} \to \overline{L'}$ Aus der Beh. folgt (mit $M = \overline{L}, M' = \overline{L'}, \varphi = \psi$), dass

$$\underset{a_i' \text{ Nullst. von } f \text{ in } \overline{L'}}{\{a_1', \ldots, a_n'\}} = \underset{a_i \text{ Nullst. von } f \text{ in } \overline{L}}{\{\psi(a_1), \ldots, \psi(a_n)\}}$$

   Also

$$L' = K(a_1', ldots, a_n') = K(\psi(a_1), \psi(a_n)) = \psi(K(a_1, \ldots, a_n)) = \psi(L)$$

   Somit ist $\psi|_L$ surjektiv (sowieso injektiv).

2. Beh. mit $M = L, M' = L'$.

□

Bemerkung. Wegen **??** sagt man auch **der** Zerfällungskörper (statt **ein**).

3.3.1 Klassifikation endlicher Körper.

Sei K ein Körper mit $|K| = q < \infty$. Dann

- $\operatorname{char} K = p$ für ein p prim.
- $q = p^n$ für $n \geq 1$.
- Primkörper $P \subset K$ ist isom. zu $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Satz 3.3.3. *Sei $q = p^n$ wobei p prim ist, mit $n \geq 1$.*

1) Es gibt einen Körper mit q Elementen.

2) Je zwei Körper mit q Elementen sind isomorph.

Für den Beweis brauchen wir:

Lemma 3.3.4 (Frobenius Automorphismus)**.** *Sei K ein endl. Körper mit* $\operatorname{char} K = p$ *wobei p prim ist. Dann ist*

$$\mathrm{Fr}\colon K \to K \qquad a \mapsto a^p$$

ein Automorphismus von K

Bew.:

- Z7/A6: Fr ist Hom.
- Fr ist injektiv
- K endl. $\Rightarrow$ Fr ist surjektiv.

□

Definition. Sei R ein Ring. Eine Derivation auf R ist eine Abb. s.d. gilt

- D ist Hom. der an. Gr. $(R, +)$.
- Leibniz-Regel $D(ab) = aD(b) + D(a)b$

Lemma Sei A ein komm. Ring. Auf $A[X]$ definiert die Abbildung

$$D(a) = 0 \qquad D(X^n) = nX^{n-1}$$

eine Derivation (Warum?)

Definition. Wir sagen, $a \in A$ ist mehrfache Nullstelle von $f \in A[X]$ für $f \neq 0$, falls

$$f = (X - a)^m g \qquad \text{für ein } m \geq 2$$

Schreibe $f' := D(f)$.

Lemma 3.3.5. *Sei A ein komm. Ring mit $f \in A[X], f \neq 0$. Es sind äquivalent:*

1) a ist mehrfache Nullstelle von f

2) $f(a) = 0$ und $f'(a) = 0$

Bew.: Sei $f \in A[X] \setminus \{0\}$, $a \in A$ mit $f(a) = 0$. Dann gilt nach 2.5.1, dass $f = (X - a)g$.
Z. z.: $f'(a) = 0 \Leftrightarrow g(a) = 0$. Es gilt $f'g + (X - a)g'$ also $f'(a) = g(a)$. □

Bew. von 3.3.3:

1) Sei $f = X^q - X \in \mathbb{F}_p[X]$. Sei $L \subset \overline{\mathbb{F}_p}$ der Zerfällungskörper von f über $\mathbb{F}_p$. Mit

$$f = \prod_{i=1}^{q} (X - a_i) \qquad a_i \in \overline{\mathbb{F}_p}$$

gilt

$$L = \mathbb{F}_p(a_1, \ldots, a_q) \subset \overline{\mathbb{F}_p}$$

Beh.: $L = \{a_1, \ldots, a_1\}$ und $|L| = q$.

Es reicht zu zeigen, dass

a) f keine mehrfachen Nullstellen hat
b) $M = \{a_1, \ldots, a_q\} \subset \overline{\mathbb{F}_p}$ bereits ein Körper ist

(a) Es gilt

$$f' = qX^{q-1} - 1 = -1$$

Nach **??** hat f keine mehrfachen Nullstellen.

(b)
- $a, b \in M \Rightarrow a + b \in M$:

$$(a+b)^q = (a+b)^{p^n} = \left(\left((a+b)^p\right)^{\ddots}\right)^p$$
$$= (\mathrm{Fr} \circ \cdots \mathrm{Fr})(a+b) = (\mathrm{Fr} \circ \cdots \circ \mathrm{Fr})(a) + (\mathrm{Fr} \circ \cdots \circ \mathrm{Fr})(b)$$
$$= a^q + b^q = a + b$$

- $a \in M \Rightarrow -a \in M$: Für $p = 2$ ist $a = -a$. Für $p > 2$ ist p ungerade.

$$(-a)^p = -a^p \Rightarrow (-a)^q = -a^q = -a$$

- $a, b \in M \Rightarrow a \cdot b \in M$

$$(ab)^q = a^q b^q = ab$$

- $a \in M, a \neq 0 \Rightarrow a^{-1} \in M$

$$(a^{-1})^q = (a^q)^{-1} = a^{-1}$$

⌟

also besteht L genau aus den Nullstellen von f und wegen $|L| = q$ zeigt die Behauptung Teil 1.

2) Seien L, L' Körper mit $|L| = q = |L'|$. Dann $\operatorname{char} L = p = \operatorname{char} L'$. D.h. $P \subset L, P' \subset L'$. $P \simeq \mathbb{Z}/p\mathbb{Z} \simeq P'$. Identifiziere P mit $\mathbb{Z}/p\mathbb{Z}$, d.h. $\mathbb{Z}/p\mathbb{Z} \subset L$ und $\mathbb{Z}/p\mathbb{Z} \subset L'$.
Betrachte $f = X^q - X \in \mathbb{F}_p[X]$.
Beh.: $\forall a \in L\colon f(a) = 0$
⌜

Für $a = 0$ gilt $f(0) = 0$. Für $a \neq 0$ gilt L^* ist Gruppe mit $|L| = q - 1$.

$$a^{q-1} = a^{\operatorname{ord}(a) \cdot \frac{|L^*|}{\operatorname{ord} a}} = 1^{\frac{|L^*|}{\operatorname{ord} a}} = 1 \Rightarrow a^q = a$$

⌟

Also ist L Zerfällungskörper von f (Warum?) . Genauso für L'. Nach **??** ist $L \simeq L'$.
□

3.4 Konstruktion mit Zirkel und Lineal

Satz 3.4.1. *Siehe Folien*

Satz 3.4.2. *Sei $M \subset \mathbb{C}$ mit $0, 1 \in M$. Dann ist AM quadratisch abgeschlossen.*

Bew.: Betrachte

$$f = X^2 + pX + q$$

In $\mathbb{C}$ gilt $f = (X + \alpha_+)(X + \alpha_-)$ und

$$\alpha_\pm = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}$$

Es ist zu zeigen, dass $\pm\alpha \in AM$. Dies folgt aus **Beh.:** $z \in AM \Rightarrow \sqrt{z} \in AM$.

1. $z \in AM \Rightarrow |z| \in AM$ (Warum?)
2. $e^{i\varphi} \in AM \Rightarrow e^{i\frac{\varphi}{2}} \in AM$ (Warum?)
   Schreibe $z = re^{i\varphi}$. Nach 1) ist $r = |z| \in AM$, also auch $e^{i\varphi} \in AM$. Dann

$$\sqrt{z} \in \{\pm\sqrt{r}e^{i\frac{\varphi}{2}}$$

es beliebt zu zeigen, dass $r \in R \cap AM \Rightarrow \sqrt{r} \in AM$.

□

Bemerkung. Sei $M \subset \mathbb{C}$ mit $0, 1 \in M$ und $K = \mathbb{Q}(M \cup \overline{M})$. Es gilt $K \subset AM$ und $AK = AM$.

Satz 3.4.3. *Für $z \in \mathbb{C}$ sind äquivalent.*

1) $z \in AM$

2) Es gibt eine Kette

$$K = K_0 \subset K_1 \subset \ldots \subset K_m = L$$

von Teilkörpern in $\mathbb{C}$ s.d. $z \in L$ und $K_{i+1} = K_i(a_i)$ mit $\operatorname{grad} m_{a_i,K_i} = 2$.

Bew.: 2) $\Rightarrow$ 1): Wir machen eine Induktion nach i. Für $i = 0$ ist nach **??** $K \subset AM$. Zeige nun $i \rightsquigarrow i + 1$. Angenommen, $K_i \subset AM$. Da $\operatorname{grad} m_{a_i,K_i} = 2$ und $m_{a_i,K_i} \in AM[X]$. Nach 3.4.2 ist $a_i \in AM$. Damit ist $K_{i+1} = K_i(a_i) \subset AM$. Also $L = K_m \subset AM$, also $z \in AM$.

1) $\Rightarrow$ 2): Sei $z \in AM$ beliebig. z entsteht aus $P_0 := M$ durch eine endliche Anzahl von Schritten der Form $P_{i+1} = P_i \cup \{w_i\}$ wobei w_i der Schnittpunkt von

a) $\lambda, \lambda' \in \mathrm{Gr}(P_i), \lambda \neq \lambda'$

b) $\lambda \in \mathrm{Gr}(P_i), \kappa \in \mathrm{Kr}(P_i$

c) $\kappa, \kappa' \in \mathrm{Kr}(P_i), \lambda \neq \lambda'$

ist. D.h. es gibt n mit $z \in P_n$. Setze $\tilde{K_0} = \mathbb{Q}(M \cup \overline{M})$ und $\tilde{K_{i+1}} := \tilde{K_i}(w_i)$. Dann gilt $P_i \subset \tilde{K_i}$ (Warum?) , also auch $z \in \tilde{K_n}$.
Beh.: Es gilt $\operatorname{grad} m_{w_i, \tilde{K_i}} \in \{1, 2\}$.
⌜

Siehe Website

⌟

Wenn $\operatorname{grad} m_{w_i, \tilde{K_i}} = 1$, dann ist $\tilde{K_{i+1}} = \tilde{K_i}$. Wenn $\operatorname{grad} m_{w_i, \tilde{K_i}} = 2$, dann haben wir die Situation wie im Satz. Lasse aus $\tilde{K_0} \subset \tilde{K_1} \subset \ldots \subset \tilde{K_n}$ alle $\tilde{K_i}$ mit $\tilde{K_i} = \tilde{K_{i+1}}$ weg. □

Korollar 3.4.4. *Sei $\{0, 1\} \subset M \subset \mathbb{C}$, $K = \mathbb{Q}(M \cup \overline{M})$. Sei $z \in AM$. Dann*

- *z ist algebraisch über K*
- *$[K(z) : K] = 2^k$ für ein $k \geq 0$.*

Bemerkung. Die Umkehrung von 3.4.4 gilt nicht.

Bew.:

$$[L : K] = [K_m : K_{m-1}] \cdots [K_1 : K_0] = 2^m$$

Es gilt $K(z) \subset L$

1) z ist alg. über K nach 3.1.4

2)

$$[L : K] = [L : K(z)][K(z) : K]$$

Somit muss $[K(z) : K]$ auch $[L : K] = 2^m$ teilen. Also $[K(z) : K] = 2^k$ mit $k \leq m$. □

Beispiel. Sei nun $M = \{0, 1\}$

1. $\sqrt[n]{2}$: $\sqrt{2}, \sqrt[4]{2} \in A(\{0, 1\})$. Für allgemeines n hat $\sqrt[n]{2}$ das Minimalpolynom:

   $$m_{\sqrt[n]{2}, \mathbb{Q}} = X^n - 2$$

   Dies ist unzerlegbar nach Eisenstein. Also ist $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$. Nach 3.4.4: Für $n \neq 2^k$ ist $\sqrt[n]{2} \notin A(\{0, 1\})$.

2. π ist transzedent.

3. p prim $\zeta = e^{\frac{2\pi i}{p}} \in A(\{0, 1\})$. ζ ist Nullst. von $X^p - 1$

   $$X^p - 1 = (X - 1)(X^{p-1} + X^{p-2} + \ldots + X + 1)$$

   $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$ also $p - 1 \neq 2^k \Rightarrow \zeta \notin A(\{0, 1\})$.

Kapitel 4

Galoistheorie

4.1 Normale und seperable Körpererweiterungen

Definition. Eine algebraische Körpererw. L/K heißt normal, falls für jedes **irreduzible** $f \in K[X]$ gilt: Hat f eine Nullstelle in L, so zerfällt f über L in Linearfaktoren.

Beispiel.

1. $\mathbb{Q}(\sqrt{2})$ ist normal über $\mathbb{Q}$. Zum Beispiel:

$$m_{\sqrt{2},\mathbb{Q}} = X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$$

   Sei $f \in \mathbb{Q}[X]$ bel. und irred. mit Nullstelle $a \in \mathbb{Q}(\sqrt{2})$. Warum zerfällt f in Linearfaktoren $\rightsquigarrow$ 4.1.1

2. $\mathbb{Q}(\sqrt[3]{2})$ ist nicht normal über $\mathbb{Q}$: Betrachte $m_{\sqrt[3]{2},\mathbb{Q}} = X^3 - 2$, dieses Polynom ist irreduzibel, hat aber die Nullstellen:

$$\sqrt[3]{2} \qquad \sqrt[3]{2}e^{\pm\frac{2\pi i}{3}}$$

Satz 4.1.1. *Sei K ein Körper, $K \subset L \subset \overline{K}$. Es sind äquivalent:*

1) L/K normal

2) Es gibt eine Teilmenge $F \subset K[X] \setminus K$ s.d. L der kleinste Teilkörper $K \subset L \subset \overline{K}$ ist, s.d. jedes $f \in F$ über L in Linearfaktoren zerfällt.

3) Für jeden K-Hom. $\varphi\colon L \to \overline{K}$ gilt $\varphi(L) = L$.

Beispiel. Für das Beispiel 1) von eben können wir Kriterium 2 mit $F = \{X^2 - 2\}$ anwenden, daraus erkennen wir, dass $L = \mathbb{Q}(\sqrt{2})$ normal ist.

Bew. von 4.1.1: 1) $\Rightarrow$ 2): Wähle

$$F = \{m_{a,K} | a \in L\}$$

Beh. 1: Jedes $f \in F$ zerfällt über L in Linearfaktoren.

Sei $f = m_{a,K}$ für ein $a \in L$. Dann haben wir $f(a) = 0$, woraus folgt, dass f über L in Linearfaktoren zerfällt, da L/K normal ist. ⌟

Beh. 2: L ist minimal mit der Eigenschaft aus Beh. 1.
⌜

Sei $K \subset M \subset \overline{K}$ zwischen, s.d. die Eigenschaft aus Beh. 1 gilt. Für jedes $a \in L$ enthält M alle Nullstellen von $m_{a,K}$ (da $m_{a,K}$ über M in Linearfaktoren zerfällt. Insbesondere $a \in L \Rightarrow a \in M$. ⌟

2) $\Rightarrow$ 3): Sei $N \subset \overline{K}$ gegeben durch:

$$N = \{a \in \overline{K} | a \text{ ist Nullstelle eines } f \in F\}$$

Per Annahme gilt $L = K(N)$ (Warum?) . Sei $\varphi\colon L \to \overline{K}$ ein K-Homomorphismus.
Beh.: $\varphi(N) = N$
⌜

Sei $f \in F$ mit Nullstellen $\{a_1, \ldots, a_n\}$. Wie in der Beh. im Beweis von **??** gilt:

$$\varphi \text{ permutiert die Menge } \{a_1, \ldots, a_n\} \tag{4.1}$$

Wir können damit folgern: Sei $a \in N$, dann gibt es ein f mit $f(a) = 0$, also ist nach (4.1) auch $\varphi(a)$ eine Nullstelle von f, demnach ist $\varphi(a) \in N$, also ist $\varphi(N) \subset N$.
Wir müssen noch zeigen, dass φ von N nach N surjektiv ist. Sei $n \in N$, dann gibt es $f \in F$ mit $f(n) = 0$. Wegen (4.1) gibt es $m \in N$ mit $\varphi(m) = n$. ⌟

3) $\Rightarrow$ 1): Sei $f \in K[X]$ unzerlegbar mit und $a \in L$ eine Nullstelle von f. O.B.d.A. ist $f = m_{a,K}$ (Warum?) . Sei $b \in \overline{K}$ eine beliebige Nullstelle von f.
Beh.: $b \in L$
⌜

Nach 3.2.6 gibt es einen K-Isom. $\varphi\colon K(a) \to K(b)$. Nach 3.2.8 lässt sich φ zu $\tilde{\varphi}\colon L \to K$ ausdehnen. Es gilt $\tilde{\varphi}(a) = b$. Per Annahme gilt $\tilde{\varphi}(L) = L$. Also $b \in L$. ⌟

Da b eine beliebige Nullstelle war, zerfällt f über L in Linearfaktoren.

Satz 4.1.2. *Sei L/K normal und $a, b \in L$. Es sind äquivalent.*

1) $\exists \sigma \in \mathrm{Aut}_K(L)$ *und* $\sigma(a) = b$

2) $m_{a,K} = m_{b,K}$

Bew.: 1) $\Rightarrow$ 2) (braucht nicht normal). Wir im Beweis von 3.2.6 ist

$$\sigma_*(m_{a,K}) = m_{a,K} \qquad \sigma_*(m_{a,K})(b) = 0$$

2) $\Rightarrow$ 1)

$$m_{a,K} = m_{b,K} \overset{3.2.11}{\Rightarrow} \exists K\text{-Iso.}\varphi\colon K(a) \to K(b) \qquad \text{mit } \varphi(a) = b$$

Wegen $K \subset K(a) \subset \overline{K}$ und $K \subset K(b) \subset \overline{K}$ lässt sich nach 3.2.9 φ zu einem K-Isom. $\tilde{\varphi}\colon \overline{K} \to \overline{K}$ ausdehnen. Setze

$$\sigma = \tilde{\varphi}|_L \colon L \to \overline{K}$$

Da L/K normal ist, ist $\sigma(L) = L$. Daher gilt $\tilde{\varphi}|_K = \mathrm{id}_K$ und $\sigma(a) = \tilde{\varphi}(a) = \varphi(a) = b$. □

Bemerkung 4.1.3. Seien $K \subset M \subset L$ Körpererweiterungen. Ist L/K normal, so auch L/M (aber nicht unbedingt $M/K \rightsquigarrow$ Üb.). Denn nach 4.1.1 gibt es $F \subset K[X]$ s.d. $L = K(N)$ mit N Nullstellenmenge aller $f \in F$. Da $K(N) = M(N)$ folgt L/M normal aus 4.1.1 mit $F \subset K[X] \subset M[X]$.

Definition. Sei K ein Körper.

1) $a \in \overline{K}$ heißt seperabel über K, falls $m_{a,K}$ nur einfache Nullstellen in $\overline{K}$ hat.

2) Eine algebraische Körperweiterung L/K heißt seperabel über K, falls jedes $a \in L$ seperabel ist.

Lemma 4.1.4. *Ein $a \in \overline{K}$ ist seperabel über K g.d.w. $D(m_{a,K}) \neq 0$.*

Bew.: a seperabel $\Rightarrow D(m_{a,K}) \neq 0$: Per Definition hat $m_{a,K}$ keine mehrfachen Nullstellen. Aus Kapitel 3 wissen wir, dass $D(m_{a,K})(a) \neq 0$ ist, also ist $D(m_{a,K}) \neq 0$.

a seperabel $\Leftarrow D(m_{a,K}) \neq 0$: Sei $D(m_{a,K}) \neq 0$. Angenommen $m_{a,K}$ hätte eine mehrfache Nullstelle b. Dann ist $m_{a,K} = m_{b,K}$ (Warum?) und wegen $(D(m_{a,K}))(b) = 0$ folgt

$$D(m_{a,K}) \in (m_{b,K}) = (m_{a,K})$$

Aber $\operatorname{grad} D(m_{a,K}) < \operatorname{grad} m_{a,K}$ also $D(m_{a,K}) = 0$. Dies ist ein Widerspruch. □

Korollar 4.1.5. *Sei* $\operatorname{char} K = 0$. *Dann ist jede alg. Erw. L/K separabel.*

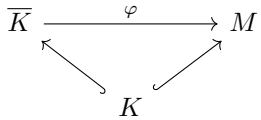
Definition. Sei L/K algebraisch. Der Separabilitätsgrad von L über K ist

$$[L : K]_S = |\mathrm{Hom}_K(L, \overline{K})$$

Bemerkung 4.1.6. 1) Sei L/K algebraisch. Ist M/K Körpererweiterung mit M algebraisch abgeschlossen, so gilt

$$[L : K]_S = |\mathrm{Hom}_K(L, M)|$$

denn betrachte

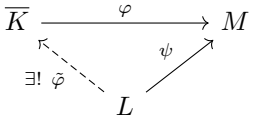


φ gibt es nach 3.2.8 Dann (Warum jeweils?)

- $\varphi(\overline{K}) \subset M$ ist ein algebraischer Abschluss von $K \subset M$
- Für jedes $\psi \in \mathrm{Hom}_K(L, M)$ gilt $\psi(L) \subset \varphi(\overline{K})$

- Für jedes $\psi \in \mathrm{Hom}_K(L, M)$ gilt:

$$\exists!\ \underset{K\text{-Hom}}{\tilde{\varphi}} : L \to \overline{K} :$$



kommutiert.

2) L/K normal $\Rightarrow [L:K]_S = |\mathrm{Aut}_K(L)|$, denn für jedes $\psi \in \mathrm{Hom}_K(L, \overline{K})$ gilt nach **??**: $\psi(L) = L$.

Satz 4.1.7. *1) Sind $K \subset L \subset M$ algebraische Erweiterungen, so gilt*

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

2) Falls L/K endlich, so gilt $[L:K]_S \leq [L:K]$.

Bew.:

1) Wegen $K \subset L \subset M \subset \overline{K}$ gilt $\overline{L} = \overline{K}$. Sei $\sigma \in \mathrm{Hom}_K(L, \overline{K})$, wende 3.2.9 auf

$$\sigma\colon L \to \sigma(L) \subset \overline{K}$$

an: es gibt einen K-Iso. $\varphi_\sigma\colon \overline{K} \to \overline{K}$ mit $\varphi_\sigma|_L = \sigma$. Für jedes $\sigma \in \mathrm{Hom}_K(L, \overline{K})$, wähle $\varphi_\sigma \in \mathrm{Aut}(\overline{K}, \overline{K})$ wie eben. Betrachte die Abbildung:

$$\mathrm{Hom}_K(L, \overline{K}) \times \mathrm{Hom}_L(M, \overline{K}) \to \mathrm{Hom}_K(M, \overline{K}) \qquad (\sigma, \psi) \mapsto \varphi_\sigma \circ \psi$$

Injektiv:

$$\varphi_\sigma \circ \psi = \varphi_{\sigma'} \circ \psi' \tag{4.2}$$

$$(4.1.7) \Rightarrow \varphi_\sigma \circ \underbrace{\psi|_L}_{=\mathrm{id}_L} = \varphi_{\sigma'} \circ \underbrace{\psi'|_L}_{=\mathrm{id}_L} \Rightarrow \underbrace{\varphi_\sigma|_L}_{=\sigma} = \underbrace{\varphi_{\sigma'}|_L}_{=\sigma'}$$

Also auch $\varphi_{\sigma'} \circ \psi = \varphi_\sigma \circ \psi'$ und da φ_σ invertierbar: $\psi = \psi'$.

Surjektiv: Sei $\alpha \in \mathrm{Hom}_K(M, \overline{K})$ beliebig. Setze $\sigma := \alpha|_L \in \mathrm{Hom}_K(L, \overline{K})$ und

$$\psi := \varphi_\sigma^{-1} \circ \alpha \in \mathrm{Hom}_K(M, \overline{K})$$

(Warum in Hom_K?) Dann $\alpha = \varphi_\sigma \circ \psi$

2) **Beh-:** $[K(a):K]_S \leq [K(a):K]$

$$\left|\mathrm{Hom}_K(K(a), \overline{K})\right| \underset{\text{3.2, Satz 5}}{=} \left|\text{Nullstellen von } m_{a,K} \text{ in } \overline{K}\right| \leq \mathrm{grad}\, m_{a,K}$$

$$\mathrm{grad}\, m_{a,K} \underset{\text{3.1, Satz 6}}{=} [K(a):K]$$

Da L/K endlich, gibt es $a_1, \ldots, a_n \in L$, so dass $L = K(a_1, \ldots, a_n)$. Also

$$\begin{aligned}
[L:K]_S &\underset{\text{Teil 1}}{=} [K(a_1,\ldots,a_n) : K(a_1,\ldots,a_{n-1}]_S \\
&\quad \cdot [K(a_1,\ldots,a_{n-1}) : K(a_1,\ldots,a_{n-2}]_S \\
&\quad \vdots \\
&\quad \cdot [K(a_1) : K]_S \\
&\underset{\text{Beh}}{\leq} [K(a_1,\ldots,a_n) : K(a_1,\ldots,a_{n-1}] \cdots [K(a_1) : K] \\
&\underset{\text{3.1, Satz 6}}{=} [L:K]
\end{aligned}$$

Satz 4.1.8. *Sei L/K endlich. Es sind äquivalent.:*

1) L/K ist separabel

2) Es gibt $a_1, \ldots, a_n \in L$ separabel mit $L = K(a_1, \ldots, a_n)$

3) $[L:K]_S = [L:K]$

Bew.: 1)⇒ 2) ist klar.
2) ⇒ 3) Setze $L_i = K(a_1, \ldots, a_i)$.
Beh.: $[L_{i+1} : L_i] = [L_{i+1} : L_i]$

$$\begin{aligned}
[L_{i+1} : L_i]_S &= \left|\mathrm{Hom}_{L_i}(L_{i+1}, \overline{K})\right| \\
&= \left|\text{Nullst. von } m_{a_{i+1},L_i} \text{ in } \overline{K}\right| = (*)
\end{aligned}$$

Es gilt

$$m_{a_{i+1},L_i} \big| m_{a_{i+1},K}$$

(Warum?) . Da $m_{a_{i+1},K}$ keine mehrfachen Nullstellen hat (da a_{i+1} sep. über K) hat auch m_{a_{i+1},L_i} keine mehrfachen Nullstellen. Also

$$(*) = \operatorname{grad} m_{a_{i+1},L_i} = [L_{i+1} : L]$$

Damit folgt 3) wie in 4.1.7.
3)⇒ 1): Sei $a \in L$ beliebig. Wir wissen:

$m_{a,K}$ hat nur einfache Nullstellen $\Leftrightarrow \operatorname{grad} m_{a,K} =$ Anzahl Nullstellen in $\overline{K}$

aber

$$\operatorname{grad} m_{a,K} = [K(a):K] \overset{(*)}{=} [K(a):K]_S = \left|\mathrm{Hom}_K(K(a), \overline{K})\right| = \left| \text{ Anzahl Nullstellen von } m_{a,K} \text{ in } \overline{K}\right|$$

Die Gleichheit bei $(*)$ folgt aus 3) (Warum?) . □

Satz 4.1.9 (Satz vom primitiven Element)**.** *Sei L/K endlich und separabel. Dann gilt: $\exists \lambda \in L\colon L = K(\lambda)$.*

Bew.:

Fall 1 - K endlich: Dann ist auch L endlich. L^* ist endlich, also zyklisch 2.5.4. Wähle λ als einen Erzeuger von L^*.

Fall 2 - K unendlich: Website

4.2 Galoiserweiterungen

Definition. Eine algebraische Erweiterung L/K heißt galois'sch (oder Galoiserweiterung), falls sie normal und separabel ist. Die Gruppe der K-Automorphismen wir dann Galoisgruppe von L über K genannt. $G(L/K) := \mathrm{Aut}_K(L)$. **Notation:** L/K K.erw. $G \subset \mathrm{Aut}_K(L)$. Setze

$$L^G = \{l \in L | \forall g \in G \colon g(l) = l\}$$

Dann ist L^G ein Körper (Warum?) , der Fixkörper von G. Es gilt $K \subset L^G \subset L$.

Satz 4.2.1. *Sei L/K Galoiserw. Dann*

$$L^{G(L/K)} = K$$

Bew.: Schreibe $G = G(L/K)$. Per Definition ist $K \subset L^G$. Sei nun $a \in L \setminus K$.
Beh.: $\exists \varphi \in G \colon \varphi(a) = a$.
⌜

Es gilt $\operatorname{grad} m_{a,K} \geq 2$. Da L/K sep. ist, hat $m_{a,K}$ eine weitere Nullstelle $b \in \overline{K}$, $b \neq a$. Also

$$m_{a,K}(b) = 0 \tag{4.3}$$

Da L/K normal und a eine Nullstelle von $m_{a,K}$, ist $b \in L$. Wegen (4.3) gilt $m_{a,K} = m_{b,K}$. Nach 4.1.2 gilt:

$$\exists \varphi \in \mathrm{Aut}_K(L) \qquad \text{mit } \varphi(a) = b$$

⌟

Damit sind wir fertig. □

Satz 4.2.2. *Sei L ein Körper, $H \subset \mathrm{Aut}(L)$ mit H **endlich**. Setze $K = L^H$. Dann gilt*

- *L/K ist Galoiserweiterung*
- $\mathrm{Aut}_K L = H$
- $[L : K] = |H|$

Bew.:

L/K ist Galoiserw.: L/K ist algebraisch, normal und separabel: Sei $a \in L$ beliebig. Sei $O = H.a$ der Orbit von a unter H. Setze

$$f = \prod_{u \in O} (X - u) \in L[X]$$

Da $\varphi_* f = f$ für alle $\varphi \in H$ (Warum?) ist sogar $f \in K[X]$. Somit:

- Jedes $a \in L$ ist Nullstelle eines Polynoms in $K[X]$, also ist L/K algebraisch.
- Da $f(a) = 0$ mit f wie oben $m_{a,K} | f$. Da f keine mehrfachen Nullstellen hat, hat auch $m_{a,K}$ keine mehrfache Nullstellen, also ist L/K separabel.
- Da f über L in Linearfaktoren zerfällt, zerfällt auch $m_{a,K}$ über L in Linearfaktoren, also ist L/K normal (Warum?) .

$\mathrm{Aut}_K(L) = H$ Klar ist, dass $H \subset \mathrm{Aut}_K(L)$, diese Erkenntnis bezeichnen wir mit $(*)$.
Beh. 1: Sei $K \subset M \subset L$ Zwischenkörper mit M/K endlich und separabel. Dann

$$[M : K] \leq |H|$$

⌜

Aus 4.1.9 wissen wir $M = K(a)$ für ein geeignetes $a \in M$.
Sei $O = H.a \subset L$

$f = \prod u \in O(X - u) \in K[X]$ *toleads* nicht L nach erstem Teil

Da $f(a) = 0$ folgt $m_{a,K} | f$, also

$$\operatorname{grad} m_{a,K} \leq \operatorname{grad} f \leq |H|$$

und

$$[M : K] = [K(a) : K] \underset{3.1.7}{=} \operatorname{grad} m_{a,K} \leq |H|$$

⌟

Beh. 2: L/K ist endlich

⌜

Angenommen L/K ist nicht endlich, dann gibt es $a_1, a_2 \notin M_1, a_3 \notin M_2, \ldots$ s.d.

$$M_1 = K(a_1) \subsetneq M_2 = M_1(a_2) \subsetneq M_3 = M_2(a_3) \subsetneq \ldots$$

Also $\dim M_{i+1} > \dim M_i$, dies ist ein Widersprich zu $\dim M_i \leq |H|$ nach Beh. 1. $M_i = K(a_1, \ldots, a_i)$ ist separabel, da L/K separabel ist, also ist jedes $a_i \in L$ sep. über K. Nach 4.1.8 ist M_i separabel.

⌟

Aus Beh. 1 mit $M = L$ (nach Beh. 2 ist dies erlaubt) wissen wir:

$$[L : K] \leq |H|$$

Insgesamt:

$$|H| \underset{(*)}{\leq} |\mathrm{Aut}_K(L)| \underset{4.1.6}{=} [L : K]_s \underset{4.1.8}{=} [L : K] \leq |H|$$

Also ist $|H| = |\mathrm{Aut}_K(L)|$ und da $H \subset \mathrm{Aut}_K(L)$ und H endlich ist $H = \mathrm{Aut}_K(L)$. Aus der obigen Ungleichungskette folgt außerdem $[L : K] = |H|$.

□

Korollar 4.2.3. *Seien L, H, K wie in 4.2.2. Sei $a \in L$ beliebig und $O = H.a$. Dann*

$$m_{a,K} = \prod_{u \in O} (X - u)$$

Bew.: Setze

$$f = \prod_{u \in O} (X - u)$$

Da $f(a) = 0$ gilt $m_{a,K} \big| f$. Aber $m_{a,K}(\varphi(a)) = 0$ für $\varphi \in H$ (Warum?) . Also ist jedes $u \in O$ eine Nullstelle von $m_{a,K}$, also $f \big| m_{a,K}$. □

Bemerkung 4.2.4. 1) Sei L/K gal. und endlich, dann folgt

$$|G(L/K)| \underset{4.1.6}{=} [L : K]_s \underset{4.1.8}{=} [L : K]$$

2) Ist für $K \subset M \subset L$ die Erw. L/K gal. so auch L/M. Nach 4.1.3 ist L/M normal. Sei $a \in L$ gegeben, wegen $m_{a,M} \big| m_{a,K}$ und a sep. über K folgt: $m_{a,K}$ hat keine mehrfachen Nullstellen, somit hat auch $m_{a,M}$ keine mehrfachen Nullstellen und a ist sep. über M.

Satz 4.2.5. *Sei L/K eine endliche Galoiserweiterung. Setze $G := G(L/K)$ Die Zuordnungen:*

$$\{K \subset M \subset L Zwischenkörper\} \xrightarrow{M \mapsto G(L/M)} \{H \leq G\}$$

$$\{K \subset M \subset L Zwischenkörper\} \xleftarrow{H \mapsto L^H} \{H \leq G\}$$

Bew.: Wir nennen die Abbildungen γ und ρ, also $\gamma(M) = G(L/M)$ und $\rho(H) = L^H$. G ist endlich, da $[L : K] > \infty$. Wir zeigen nun $\rho \circ \gamma = \mathrm{id}$. Sei $K \subset M \subset L$ gegeben, dann ist L/M gal. nach 4.2.4. Sei $H = \gamma(M)$. Dann

$$L^H = L^{G(L/M)} \underset{4.2.1}{M}$$

Also ist $\rho(\gamma(M)) = M$. Wir kommen zu $\gamma \circ \rho = \mathrm{id}$. Sei $H \leq G$ eine Untergruppe. Setze $M = L^H$. Nach 4.2.2 ist L/M gal. und $G(L/M) = H$. Also $\gamma(\rho(H)) = H$.
□

Bemerkung 4.2.6. 1) „Enthaltensein“wird unter den Bijektionen umgedreht:

$$M_1 \subset M_2 \overset{M_i = L^{H_i}}{\Leftrightarrow} H_1 \supset H_2$$

2) Für $H \leq G(L/K)$ und $\varphi \in G(L/K)$ gilt

$$\varphi(L^H) = L^{\phi H \phi^{-1}}$$

⌜

$$\begin{aligned} a \in \varphi(L^H) &\Leftrightarrow \exists b \in L\colon \varphi(b) = a \wedge \forall \psi \in H\colon \psi(b) = b \\ &\Leftrightarrow \forall \psi \in H\colon \psi(\varphi^{-1}(a)) = \varphi^{-1}(a) \\ &\Leftrightarrow \forall \psi \in H\colon \varphi\psi\varphi^{-1}(a) = a \\ &\Leftrightarrow a \in L^{\varphi H \varphi^{-1}} \end{aligned}$$

⌟

Satz 4.2.7. *Sei L/K eine endliche Galoiserweiterung und $K \subset M \subset L$ Zwischenkörper. Es sind äquivalent:*

1) M/K ist normal

2) $G(L/M) \leq G(L/K)$ ist eine normale UG

In diesem Fall ist

$$\mathbf{1} \to G(L/M) \xrightarrow{\psi \mapsto \psi} G(L/K) \xrightarrow{\varphi \mapsto \varphi|_M} G(M/K) \to \mathbf{1}$$

eine kurze exakte Sequenz.

Bew.: Sei $G = G(L/K)$, $H = G(L/M)$.
1) $\Rightarrow$ 2): Zu zeigen:

$$\forall \varphi \in G, \tau \in H\colon \varphi\tau\varphi^{-1} \in H$$

Es gilt

$$L^H = M = \varphi(M) \underset{4.1.1}{=} \varphi(L^H) = L^{\varphi H \varphi^{-1}} \qquad (*)$$

Aus 4.2.5 folgt, dass die Abbildung $H \mapsto L^H$ injektiv ist. Somit folgt aus $(*)$: $H = \varphi H \varphi^{-1}$.

2) $\Rightarrow$ 1): Wir zeigen, dass M/K eine Galoiserweiterung ist. G wirkt auf M:
⌜

Sei $\varphi \in G$ und $m \in M$. Dann ist für $\tau \in H$:

$$\tau(\varphi(m)) = \varphi\varphi^{-1}\tau\varphi(m) = \varphi\tau'(m) = \varphi(m)$$

Da $m \in M = L^H$ ist auch $\varphi(m) \in L^H$.

⌟

Bekomme

$$G \xrightarrow{\varphi \mapsto \varphi|_M} \mathrm{Aut}_K(M)$$

Sei $\tilde{G}$ das Bild dieser Abbildung. Dann $M^{\tilde{G}} = K$ (Warum?) . Also ist nach 4.2.2 M/K gal. und $\mathrm{Aut}_K(M) = \tilde{G}$ $(*)$.

Wir zeigen noch die exakte Sequenz, bisher wissen wir, dass

$$G(L/K) \xrightarrow{\varphi \mapsto \varphi|_M} G(M/K) \to \mathbf{1}$$

exakt ist, die erste Abbildung also surjektiv. Wir haben noch zu zeigen, dass $\varphi|_M = \mathrm{id}_M \Leftrightarrow \varphi \in G(L/M)$ per Definition. □