Vorlesung aus dem Wintersemester 2010/11

Algebra

Priv.-Doz. Dr. Peter Schuster

geTEXt von Viktor Kleen & Florian Stecker

Inhaltsverzeichnis

1 Gruppen

1.1 Untergruppen

Definition. Eine *Gruppe* ist ein Tripel (G, m, e) mit

i) G Menge

ii) e Element von G

iii) $m\colon G \times G \to G, (x, y) \mapsto xy$ Abbildung mit

1) $x(yz) = (xy)z$ für alle $x, y, z \in G$

2) $xe = x = ex$ für alle $x \in G$

3) $\forall x \in G \exists y \in G(xy = e = yx)$

Definition. Sind $(G, m, e), (G', m', e')$ Gruppen, so heißt eine Abbildung $f\colon G \to G'$ ein *Gruppenhomomorphismus*, wenn $f(xy) = f(x)f(y)$ ist für alle $x, y \in G$.

- Ist f auch injektiv, so heißt f ein *Gruppenmonomorphismus.*
- Ist f auch surjektiv, so heißt f ein *Gruppenepimorphismus.*
- Ist f auch bijektiv, so heißt f ein *Gruppenisomorphismus.*

Beobachtung (Kürzungseigenschaft). Aus $xa = xb$ oder $ax = bx$ folgt $a = b$.

Beweis. Ist z.B. $xa = xb$ und y zu x wie in 3), ist $a = ea = (xy)a = y(xa) = y(xb) = (yx)b = eb = b$. □

Bemerkung.

a) Durch 2) wird e eindeutig bestimmt; e heißt *neutrales Element* von G.

b) Zu $x \in G$ ist $y \in G$ wie in 3) eindeutig bestimmt; y heißt das *Inverse* von x, in Zeichen $y = x^{-1}$.

c) Für $x \in G$ und $n \in \mathbb{N}$ definiert man $x^n \in G$ rekursiv durch $x^0 = e$ und $x^{n+1} = x^n x$; man setzt $x^{-n} = (x^n)^{-1}$; damit: $x^{n+m} = x^n x^m$ und $x^{nm} = (x^n)^m$

d) Für jeden Gruppenhomomorphismus $f\colon G \to G'$ gelten automatisch $f(e) = e'$ und $f(x^{-1}) = f(x)^{-1}$; ferner gilt: Ist f ein Isomorphismus, so ist auch f^{-1} ein Isomorphismus.

Beweis.

a) Ist auch $x\tilde{e} = x = \tilde{e}x$ für alle $x \in G$, so ist $e = \tilde{e}e$ wegen $x = \tilde{e}x$ und $\tilde{e} = \tilde{e}e$ wegen $x = xe$, also $e = \tilde{e}$.

b) Ist auch $xz = e = zx$, so ist $y = ye = y(xz) = (yx)z = ez = z$. Aus $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}b = e$ und $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = e$ folgt $(ab)^{-1} = b^{-1}a^{-1}$ wegen der oben gezeigten Eindeutigkeit des Inversen.

c) Übung.

d) Wegen $f(e)^2 = f(e)f(e) = f(ee) = f(e)$ ist $f(e) = e'$. Aus $f(x)f(x^{-1}) = f(xx^{-1}) = f(e) = e'$ und $f(x^{-1})f(x) = \cdots = f(e) = e'$ folgt $f(x^{-1}) = f(x)^{-1}$ mit b). Nun sei f ein Isomorphismus. Setze $f' = f^{-1}$. Für $x', y' \in G'$ sei $x = f'(x')$ und $y = f'(y')$, d.h. $f(x) = x'$ und $f(y) = y'$. Also $f'(x'y') = f'(f(x)f(y)) = f(f(xy)) = xy = f'(x')f'(y')$. □

Definition. Eine Gruppe G heißt (*kommutativ* oder) *abelsch*, wenn $xy = yx$ für alle $x, y \in G$. Dann schreibt man G oft *additiv*, d.h. $x + y$ statt xy, 0 statt e und $-x$ statt x^{-1}.

Beispiel.

0) $(\mathbb{N}, +, 0)$ ist *keine* Gruppe.

1) $(\mathbb{Z}, +, 0)$, $(\mathbb{Q}, +, 0)$, $(\mathbb{R}, +, 0)$, $(\mathbb{C}, +, 0)$ sind Gruppen, alle abelsch.

2) Für jeden Körper K ist $GL(n, K)$, die Menge der invertierbaren $n \times n$-Matrizen über K, eine Gruppe mit Matrizenmultiplikation und Einheitsmatrix. Sie ist genau dann abelsch, wenn $n = 1$ ist.

3) Sind $G_1, \ldots, G_n$ Gruppen, $n \geq 2$, so ist $G = G_1 \times \cdots \times G_n$ eine Gruppe mit $(x_1, \ldots, x_n)(y_1, \ldots, y_n) = (x_1y_1, \ldots, x_ny_n)$ und $e = (e_1, \ldots, e_n)$, wobei e_i neutrales Element von G_i ist; dieses G heißt *direktes Produkt* von $G_1, \ldots, G_n$. Für $1 \leq i \leq n$ ist $p_i \colon G \to G_i, (x_1, \ldots, x_n) \mapsto x_i$ ein Gruppenhomomorphismus.

4) $(\mathbb{R}, +, 0) \to (\mathbb{R}_{>0}, \cdot, 1), x \mapsto e^x$ ist ein Gruppenisomorphismus.

5) Für jede Gruppe G und $a \in G$ ist $k_a \colon G \to G, x \mapsto axa^{-1}$ ein Gruppenisomorphismus mit $k_a^{-1} = k_{a^{-1}}$. k_a heißt *Konjugation* mit a.

Definition. Es sei (G, m, e) eine Gruppe. Eine Teilmenge H von G heißt *Untergruppe*, wenn

i) $e \in H$

ii) $x, y \in H \Longrightarrow xy \in H$

iii) $x \in H \Longrightarrow x^{-1} \in H$

Dann ist H mit der von m induzierten Multiplikation eine Gruppe, und die Inklusion $H \hookrightarrow G, x \mapsto x$ ist ein Gruppenmonomorphismus.

Beispiel.

0) $\{e\}$ und G sind Untergruppen von G, die sogenannten *trivialen Untergruppen.*

1) Das *Zentrum* $Z(G) = \{x \in G \colon \forall y \in G(xy = yx)\}$ ist eine *Untergruppe* von G. Es gilt: $Z(G) = G \Longleftrightarrow G$ abelsch.

2) Es sei $f\colon G \to G'$ ein Gruppenhomomorphismus.

   a) Ist H' Untergruppe von G', so ist $f^{-1}(H') = \{x \in G\colon f(x) \in H'\}$ Untergruppe von G; speziell ist $\mathrm{Ker}(f) = \{x \in G\colon f(x) = e'\}$ eine Untergruppe von G, der sog. *Kern* von f.

   b) Ist H Untergruppe von G, so ist $f(H) = \{f(x)\colon x \in H\}$ Untergruppe von G'; speziell ist $\mathrm{Im}(f) = f(G)$ eine Untergruppe von G', das sog. *Bild* von f.

3) Für jede Teilmenge $S \neq \varnothing$ von G ist

$$\langle S\rangle = \{s_1^{\varepsilon_1} \dots s_k^{\varepsilon_k}\colon k \geq 0; s_1, \dots, s_k \in S; \varepsilon_1, \dots, \varepsilon_k \in \{\pm 1\}\}$$

   eine Untergruppe von G. Man nennt $\langle S\rangle$ die *von S erzeugte Untergruppe* von G. Es gilt

$$\langle S\rangle = \bigcap\{H \subseteq G\colon H \text{ Untergruppe von } G, S \subseteq H\}$$

   $\supseteq$ Folgt aus: $\langle S\rangle$ ist eines der H auf der rechten Seite.

   $\subseteq$ Ist $x \in \langle S\rangle$, so ist $x = s_1^{\varepsilon_1} \dots s_n^{\varepsilon_n}$, $s_1, \dots, s_n \in S$, $\varepsilon_1, \dots, \varepsilon_m \in \{\pm 1\}$ und ist $H \subseteq G$ eine Untergruppe von G mit $S \subseteq H$, so sind $s_1, \dots, s_n \in H$, also $s_1^{\varepsilon_1}, \dots, s_n^{\varepsilon_n} \in H$ und damit $x = s_1^{\varepsilon_1} \dots s_n^{\varepsilon_n} \in H$.

   Speziell: $\langle S\rangle$ ist die kleinste Untergruppe von G, welche ganz S enthält, d.h. ist H eine Untergruppe von G mit $S \subseteq H$, so ist $\langle S\rangle \subseteq H$, und $\langle S\rangle$ ist eine Untergruppe von G mit $S \subseteq \langle S\rangle$.

4) Ist $G = \langle S\rangle$ für eine endliche Teilmenge S, so heißt G *endlich erzeugt* (e.e.). Ist sogar $G = \langle a\rangle$, d.h. $G = \langle\{a\}\rangle$, so heißt G *zyklisch*. Beachte $\langle e\rangle = \{e\}$.

5) Man nennt $|G|$ bzw. $\mathrm{ord}(x) = |\langle x\rangle|$ die *Ordnung* der Gruppe G bzw. die *Ordnung* von $x \in G$. Es gilt $\langle e\rangle = \{e\} \Longrightarrow \mathrm{ord}(e) = 1$

Lemma. *Jede Untergruppe H einer zyklischen Gruppe $G = \langle a\rangle$ ist wieder zyklisch. Genauer: Ist $H \neq \{e\}$, so ist $H = \langle a^{m_0}\rangle$ mit $m_0 = \min\{m \geq 1\colon a^m \in H\}$.*

Beweis. Es sei $H \neq \{e\}$. Damit ist $\{m \geq 1\colon a^m \in H\} \neq \varnothing$ (denn sonst $H = \{e\}$). Wir zeigen $H = \langle a^{m_0}\rangle$.

$\supseteq$ folgt aus $a^{m_0} \in H$ und $\langle a^{m_0}\rangle = \{a^{m_0 k}\colon k \in \mathbb{Z}\}$

$\subseteq$ Ist $x \in H$, so ist $x = a^n$, $n \in \mathbb{Z}$. Schreibe $n = m_0 q + r$ mit $0 \leq r < m_0$, dann folgt $x = a^n = (a^{m_0})^q a^r$, also $a^r = (a^{m_0})^{-q} x \in H$ und $r = 0$ (wäre $r \geq 1$, so wäre $m_0 \leq r < m_0$, was unmöglich ist). Schließlich gilt $x = (a^{m_0})^q \in \langle a^{m_0}\rangle$. □

Lemma. $\mathrm{ord}(x) < \infty \iff \exists m \geq 1 (x^m = e)$. *In diesem Fall:* $\mathrm{ord}(x) = \min\{m \geq 1\colon x^m = e\}$. *Sogar* $x^m = e \Longrightarrow \mathrm{ord}(x) \mid m$ *(auch für $m = 0$).*

Beweis. Wir zeigen zuerst $\Longrightarrow$: Ist $\langle x\rangle = \{x^n\colon n \in \mathbb{Z}\}$ endlich, so gibt es $0 \leq k < l$ mit $x^k = x^l$, also $x^{l-k} = e$ mit $l - k \geq 1$. Nun zu $\Longleftarrow$: Es sei $m_0 = \min\{m \geq 1\colon x^m = e\}$. Für $0 \leq i < j < m_0$ ist $x^{j-i} \neq e$, d.h. $x^i \neq x^j$. Es gilt $\{e, x, x^2, \dots, x^{m_0-1}\} = \langle x\rangle$,

denn $\{e, x, x^2, \ldots, x^{m_0-1}\} \subseteq \langle x\rangle$ und außerdem: Sei $y \in \langle x\rangle \Longrightarrow y = x^n, n \in \mathbb{Z}$. Schreibe $n = m_0 q + r$, $0 \leq r < m_0$, dann $y = (x^{m_0})^q x^r = x^r$, d.h. $y \in \{e, x, x^2, \ldots, x^{m_0-1}\}$. Speziell $|\langle x\rangle| = m_0$. Ist $x^m = e$, so schreibe $m = m_0 s + t$ mit $0 \leq t < m_0$, wofür $e = x^m = (x^{m_0})^s x^t = x^t$, also $t \not\geq 1$, d.h. $t = 0$, d.h. $m_0 \mid m$. □

Konvention. Im folgenden sei H eine Untergruppe der Gruppe G.

Definition. Für $x \in G$ heißt $xH = \{xh \colon h \in H\}$ die *Linksnebenklasse modulo H von x*. Es gilt $x = xe$, also $x \in xH$.

Bemerkung.

a) Folgende Aussagen sind äquivalent:

$$\text{i)}\, xH = yH \quad \text{ii)}\, xH \subseteq yH \quad \text{iii)}\, x \in yH \quad \text{iv)}\, y^{-1}x \in H \quad \text{v)}\, xH \cap yH \neq \varnothing$$

b) Die Abbildung $H \to xH, h \mapsto xh$ ist bijektiv, speziell gilt $|xH| = |H|$.

Beweis.

a) Klar sind: i) $\Longrightarrow$ ii) $\Longleftrightarrow$ iii) $\Longrightarrow$ iv)

iv $\Rightarrow$ v Ist $y^{-1}x \in H$, so ist $x = y(y^{-1}x) \in yH$, aber auch $x \in xH$.

v $\Rightarrow$ i Ist $xh_1 = yh_2$ mit $h_1, h_2 \in H$, so ist $x = y(h_2 h_1^{-1}) \in yH$, also $xH \subseteq yH$, ebenso zeigt man $y \in xH$ und damit $yH \subseteq xH$.

b) Inverse Abbildung: $xH \to H, z \mapsto x^{-1}z$ □

Definition. Man nennt $G/H = \{xH \colon x \in G\}$ die *Faktormenge von G modulo H* und $[G : H] = |G/H|$ den *Index von H in G*. Es gilt $G = \bigsqcup G/H$.

Satz (Lagrange)**.** *Ist G endlich, so gilt $|G| = [G : H] \cdot |H|$.*

Beweis. Schreibe $G/H = \{x_1 H, \ldots, x_m H\}$ mit $m = [G : H]$. Für $i \neq j$ ist $x_i H \neq x_j H$, also $x_i H \cap x_j H = \varnothing$. Aus $G = x_1 H \sqcup \cdots \sqcup x_m H$ und $|x_k H| = |H|$ folgt $|G| = m \cdot |H|$. □

Korollar. *G endlich, $x \in G \Longrightarrow \operatorname{ord}(x) \mid |G|$, $x^{|G|} = e$.*

Beweis. Satz für $H = \langle x\rangle$: $|G| = [G : H] \cdot \operatorname{ord}(x)$, $x^{|G|} = (x^{\operatorname{ord}(x)})^{[G:H]} = e$ □

Korollar. *$|G| = p$, p Primzahl $\Longrightarrow$ G zyklisch. Genauer: $G = \langle a\rangle$ für jedes $a \in G \setminus \{e\}$.*

Beweis. Für $a \in G$ mit $\operatorname{ord}(a) = |G|$ ist $G = \langle a\rangle$. $|G| = p$ prim $\overset{\text{Kor. } 1}{\Longrightarrow} \operatorname{ord}(a) \in \{1, p\} \overset{a \neq e}{\Longrightarrow} \operatorname{ord}(a) = p = |G|$. □

1.2 Faktorgruppen

Definition. Wieder sei G eine Gruppe. Für $A, B \subseteq G$ sei $AB = \{ab\colon a \in A, b \in B\}$. Man schreibt aB bzw. Ab, falls $A = \{a\}$ bzw. $B = \{b\}$. Eine Untergruppe H von G heißt *Normalteiler* von G, in Zeichen $H \lhd G$, wenn $xHx^{-1} = H$, d.h. $k_x(H) = H$ für alle $x \in G$. Man sagt auch H *ist normal in* G.

Bemerkung. Es sei $H \subseteq G$ eine Untergruppe und $x \in G$.

a) $xHx^{-1} = H \iff xH = Hx \iff H = x^{-1}Hx$.

b) $H \lhd G$ folgt schon aus $xHx^{-1} \subseteq H$ für alle $x \in G$.

c) $H \lhd G \iff \forall x \in G(k_x(H) \subseteq H)$

d) Ist $H \lhd G$ und U Untergruppe von G, so ist UH eine Untergruppe von G und es gilt $UH = HU$.

Beweis. a) % b) Ist $xHx^{-1} \subseteq H$ für alle x, so auch für x^{-1}, d.h. $x^{-1}Hx \subseteq H$, also $H \subseteq xHx^{-1}$. Mit $xHx^{-1} \subseteq H$ folgt $xHx^{-1} = H$. c) % d) $e = ee \in UH$ und $u_1, u_2 \in U; h_1, h_2 \in H \implies (u_1h_1)(u_2h_2) = u_1u_2(u_2^{-1}h_1u_2)h_2 \in UH$ (weil $u_2^{-1}h_1u_2 \in H$) und $u \in U, h \in H \implies (uh)^{-1} = h^{-1}u^{-1} = u^{-1}(uhu^{-1}) \in UH$. $u \in U, h \in H \implies uh = (uhu^{-1})u \in HU \wedge hu = u(u^{-1}hu) \in UH$. □

Beispiel.

0) $H \lhd G$, U Untergruppe von G, $H \subseteq U \implies H \lhd U$.

1) Ist G abelsch, so ist jede Untergruppe von G schon Normalteiler. Allgemeiner: Ist H Untergruppe von $Z(G)$, so ist $H \lhd G$.

2) Ist H Untergruppe von G mit $[G : H] = 2$, so ist $H \lhd G$.

3) S_3 hat vier nichttriviale Untergruppen, wovon nur eine Normalteiler ist.

4) Ist $f\colon G \to G'$ ein Homomorphismus, so gilt $H' \lhd G' \Rightarrow f^{-1}(H') \lhd G$. Insbesondere: $\mathrm{Ker}(f) \lhd G$.

5) Für jede Untergruppe H von G ist der *Normalisator* $N_G(H) = \{x \in G\colon xH = Hx\}$ von H in G die größte Untergruppe von G, in der H normal ist.

Beweis.

1) $H \subseteq Z(G), x \in G, h \in H \implies xh = hx \implies xhx^{-1} = h$, also $xHx^{-1} = H$, d.h. $H \lhd G$.

2) $G/H = \{H, aH\}$ mit $H \neq aH$, d.h. $H \cap aH = \varnothing$; für jedes $x \in G$ ist $x^2 \in H$, denn $x \in H$ oder $x \notin H \Rightarrow x \in aH$ und $x^{-1} \notin H \Rightarrow x^{-1} \in aH$, also $xH = aH = x^{-1}H \Rightarrow x^2H = H \Rightarrow x^2 \in H$. Es folgt $y \in G, h \in H \Rightarrow yhy^{-1} = y(hyhh^{-1}y^{-1})y^{-1} = (yh)^2h^{-1}y^{-2} \in H$.

3) Sei $H \subseteq S_3$ eine Untergruppe und $\{\mathrm{id}\} \neq H \neq S_3$, so ist $|H| \in \{2,3\}$ nach Lagrange, also ist H zyklisch und damit $H \in \{H_1, H_2, H_3, H_4\}$, wobei $H_1 = \{\mathrm{id}, \left(\begin{smallmatrix}1&2&3\\2&1&3\end{smallmatrix}\right)\}$, $H_2 = \{\mathrm{id}, \left(\begin{smallmatrix}1&2&3\\3&2&1\end{smallmatrix}\right)\}$, $H_3 = \{\mathrm{id}, \left(\begin{smallmatrix}1&2&3\\1&3&2\end{smallmatrix}\right)\}$, $H_4 = \{\mathrm{id}, \left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2&3\\3&1&2\end{smallmatrix}\right)\}$. Nun ist $[S_3 : H_4] = 2$ nach Lagrange, also $H_4 \lhd S_3$, jedoch nicht $H_i \lhd S_3$ $(i = 1, 2, 3)$.

4) $f^{-1}(H')$ ist eine Untergruppe von G. Sei $x \in G, h \in f^{-1}(H')$, d.h. $f(h) \in H'$, dann $f(xhx^{-1}) = f(x)f(h)f(x)^{-1} \in H'$, d.h. $xhx^{-1} \in f^{-1}(H')$, also $f^{-1}(H') \lhd G$.

5) Wir zeigen zuerst, dass $N_G(H)$ eine Untergruppe ist: $e \in N_G(H)$, $x, y \in N_G(H) \Rightarrow (xy)H = x(yH) = x(Hy) = (xH)y = H(xy)$, d.h. $xy \in N_G(H)$, $x \in N_G(H) \Rightarrow Hx^{-1} = x^{-1}(xH)x^{-1} = x^{-1}(Hx)x^{-1} = x^{-1}H$, d.h. $x^{-1} \in N_G(H)$. Es gilt $H \lhd N_G(H)$, weil $x \in N_G(H) \Leftrightarrow xH = Hx$. $N_G(H)$ ist die „größte“ solche Untergruppe, denn ist $H \lhd U$ und U Untergruppe von G, so ist $xH = Hx$ für alle $x \in U$, also $U \subseteq N_G(H)$. □

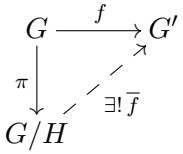
Satz (Faktorgruppe)**.** *Es sei stets $H \lhd G$.*

a) Die Abbildung $G/H \times G/H \to G/H, (xH, yH) \mapsto (xy)H$ ist wohldefiniert und macht G/H zu einer Gruppe mit neutralem Element H und $x^{-1}H$ als Inversem von xH.

b) Die kanonische Abbildung $\pi\colon G \to G/H, x \mapsto xH = \overline{x}$ ist ein Epimorphismus mit $\mathrm{Ker}(\pi) = H$.

c) Die Untergruppen von G/H sind von der Form U/H mit U Untergruppe von G und $H \subseteq U$.

d) Ist $f\colon G \to G'$ ein Homomorphismus mit $f(H) \subseteq \{e'\}$, so gibt es genau einen Homomorphismus $\overline{f}\colon G/H \to G'$ mit $\overline{f} \circ \pi = f$.



Beweis.

a) Sind $xH = x'H$, $yH = y'H$, so ist $xyH = xy'H \overset{H \lhd G}{=} xHy' = x'Hy' \overset{H \lhd G}{=} x'y'H$. Mit $\overline{x} = xH$ ist $\overline{x}\,\overline{y} = \overline{xy}$, $\overline{e} = H$, $(\overline{x}\,\overline{y})\overline{z} = \overline{xy}\,\overline{z} = \overline{(xy)z} = \overline{xyz} = \overline{x}\,\overline{yz} = \overline{x}(\overline{y}\,\overline{z})$, $\overline{e}\,\overline{x} = \overline{ex} = \overline{x} = \overline{xe} = \overline{x}\,\overline{e}$ und $\overline{x}\,\overline{x^{-1}} = \overline{xx^{-1}} = \overline{e}$

b) π ist surjektiv. π ist ein Homomorphismus, denn $\pi(xy) = \overline{xy} = \overline{x}\,\overline{y} = \pi(x)\pi(y)$ und $x \in \mathrm{Ker}(\pi) \Leftrightarrow \pi(x) = \overline{e} \Leftrightarrow xH = H \Leftrightarrow x \in H (x \in G)$.

c) Ist U eine Untergruppe von G mit $U \supseteq H$, so ist U/H eine Untergruppe von G/H, denn: $H = eH \in U/H$, $x, y \in U \Rightarrow xy \in U \Rightarrow \overline{x}\,\overline{y} = \overline{xy} \in U/H$, x^{-1} analog. Ist A eine Untergruppe von G/H, so ist $U = \pi^{-1}(A)$ eine Untergruppe von G mit $\mathrm{Ker}(\pi) = \pi^{-1}(\{\overline{e}\}) \subseteq U$ und $\pi(U) = \pi\pi^{-1}(A) \overset{\pi \text{ surj.}}{=} A$, mit anderen Worten: $H \subseteq U$ und $A = \{\overline{x}\colon x \in U\} = U/H$.

d) $\overline{f}\colon G/H \to G', xH \mapsto f(x)$ ist wohldefiniert, denn aus $xH = yH$, d.h. $x^{-1}y \in H$, folgt $e' = f(x^{-1}y) = f(x)^{-1}f(y)$, d.h. $f(x) = f(y)$. $\overline{f}$ ist ein Homomorphismus, denn $\overline{f}(\overline{x}\,\overline{y}) = \overline{f}(\overline{xy}) = f(xy) = f(x)f(y) = \overline{f}(\overline{x})\overline{f}(\overline{y})$. $\overline{f} \circ \pi = f$ ist klar. Und zur Eindeutigkeit: Ist auch $\tilde{f}\colon G/H \to G'$ ein Homomorphismus mit $\tilde{f} \circ \pi = f$, so ist $\tilde{f}(\overline{x}) = \tilde{f}(\pi(x)) = f(x) = \overline{f}(\pi(x)) = \overline{f}(\overline{x})$ für alle $\overline{x} \in G/H$, also $\tilde{f} = \overline{f}$. □

Korollar (Homomorphiesatz)**.** *Für jeden Homomorphismus $f\colon G \to G'$ ist $G/\operatorname{Ker}(f) \cong \operatorname{Im}(f)$.*

Beweis. Es gilt $\operatorname{Ker}(f) \lhd G$, wir zeigen, dass $\overline{f}\colon G/\operatorname{Ker}(f) \to G', \overline{x} \to f(x)$ injektiv ist (denn $\operatorname{Im}(\overline{f}) = \operatorname{Im}(f)$): $\overline{x} \in \operatorname{Ker}(\overline{f}) \Leftrightarrow \overline{f}(\overline{x}) = e' \Leftrightarrow f(x) = e' \Leftrightarrow x \in \operatorname{Ker}(f)$. □

Korollar (1. Isomorphiesatz)**.** *Ist $H \lhd G$ und U eine Untergruppe von G, so ist $U \cap H \lhd U$, $H \lhd UH$ und $U/(U \cap H) \cong UH/H$.*

Beweis. $H \lhd UH$ ist klar, beachte, dass UH eine Untergruppe ist wegen $H \lhd G$. Zu $U \cap H \lhd U$: Für $x \in U$ ist $x(U \cap H)x^{-1} \subseteq U \cap H$, denn für $y \in U \cap H$ ist $xyx^{-1} \in U$, $xyx^{-1} \in H$ [$H \lhd G$, $y \in H$], also $xyx^{-1} \in U \cap H$. Schließlich ist $U \hookrightarrow UH \xrightarrow{\text{kan.}} UH/H$ ein Homomorphismus, surjektiv [$u \in U, h \in H \Rightarrow uhH = uH$] mit Kern $U \cap H$. Daraus folgt die Behauptung mit dem ersten Korollar. □

Korollar (2. Isomorphiesatz)**.** *Es sei $H \lhd G$. Ist auch $U \lhd G$ mit $H \subseteq U$, so ist $U/H \lhd G/H$ und $(G/H)/(U/H) \cong G/U$. Speziell gilt $[G/H : U/H] = [G : U]$.*

Beweis. Wegen $H \subseteq U$ induziert der Epimorphismus $G \xrightarrow{\text{kan.}} G/U$ einen Homomorphismus $G/H \to G/U$, der wieder surjektiv ist und Kern U/H hat. Die Behauptung folgt mit dem ersten Korollar. $[G/H : U/H] = [G : U]$ lässt sich auch mit Lagrange zeigen, falls G endlich. □

Beispiel (Unter-/Faktorgruppen von $\mathbb{Z}$)**.** Es sei $G = (\mathbb{Z}, 0, +)$. Ist $\{0\} \neq H \subseteq G$ eine Untergruppe von G, so ist G/H endlich: Da $G = \langle 1\rangle = \langle -1\rangle$ zyklisch ist, ist H zyklisch, $H = \langle n\rangle$, $n \geq 1$, $G/H = \mathbb{Z}/\langle n\rangle = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$, denn: Schreibe $x \in \mathbb{Z}$ als $x = qn + r$ mit $0 \leq r \leq n-1$, wofür $\overline{x} = \overline{r}$, da $x - r = qn \in \langle n\rangle$. Ferner ist $\overline{l} \neq \overline{k}$ für $0 \leq k, l \leq n-1$ mit $l \neq k$, etwa $k < l$, denn: $l - k \notin \langle n\rangle$. Also ist $|\mathbb{Z}/\langle n\rangle| = n$ und $\mathbb{Z}/\langle n\rangle$ zyklisch.

Jede Untergruppe von $\mathbb{Z}/\langle n\rangle$ mit $n > 1$ ist von der Form $\langle k\rangle/\langle n\rangle$ mit $\langle k\rangle \supseteq \langle n\rangle$, d.h. $\langle k\rangle \ni n$, d.h. $k \mid n$. Wegen $[\mathbb{Z}/\langle n\rangle : \langle k\rangle/\langle n\rangle] = [\mathbb{Z} : \langle k\rangle] = k$ und $[\mathbb{Z} : \langle n\rangle] = n$ ist $[\langle k\rangle : \langle n\rangle] = n/k$. Zu jedem $d \mid n$ mit $n > 1$ gibt es also genau eine Untergruppe U von $\mathbb{Z}/\langle n\rangle$ mit $|U| = d$, nämlich $U = \langle k\rangle/\langle n\rangle$ mit $k = n/d$, d.h. $d = n/k$.

Satz (Beschreibung der zyklischen Gruppen)**.**

a) Jede unendliche zyklische Gruppe ist isomorph zu $\mathbb{Z}$.

b) Jede endliche zyklische Gruppe ist isomorph zu $\mathbb{Z}/\langle n\rangle$ für ein geeignetes $n \geq 1$, zu jedem $d \mid n$, $d \geq 1$ gibt es genau eine Untergruppe der Ordnung d.

Beweis. Es sei (G, e, m) zyklisch, $G = \langle a\rangle$, d.h. $f\colon \mathbb{Z} \to G, z \mapsto a^z$ ist ein Epimorphismus, also gilt $\mathbb{Z}/\operatorname{Ker}(f) \cong G$. Nun ist $\operatorname{Ker}(f) = \langle n\rangle$, also $\mathbb{Z}/\langle n\rangle \cong G$ für ein $n \geq 0$. $n = 0 \Rightarrow \mathbb{Z} \cong G \Rightarrow G$ unendlich. $n \geq 1 \Rightarrow \mathbb{Z}/\langle n\rangle \cong G \Rightarrow G$ endlich, $|G| = n$. □

Korollar. *Es sei G eine Gruppe.*

a) $|G| = p$, *p Primzahl* $\Rightarrow G \cong \mathbb{Z}/\langle p \rangle$

b) Ist $G \neq \{e\}$ und hat G keine Untergruppen außer $\{e\}$ und G, so ist $G \cong \mathbb{Z}/\langle p \rangle$ für eine Primzahl p.

1.3 Permutationsgruppen

Definition. Eine *Operation* einer Gruppe G auf einer Menge $V \neq \varnothing$ ist eine Abbildung $G \times V \to V, (x, v) \mapsto x.v$ mit

1) $x.y.v = xy.v$ für alle $x, y \in G$, $v \in V$

2) $e.v = v$ für alle $v \in V$.

Man nennt $B(v) = \{x.v \colon x \in G\}$ die *Bahn* von v und $|B(v)|$ ihre *Länge*. Auch heißt $S(v) = \{x \in G \colon x.v = v\}$ der *Stabilisator* von v. Er ist eine Untergruppe von G.

Bemerkung. $|B(v)| = [G : S(v)]$, denn $G/S(v) \to B(v), \overline{x} \mapsto x.v$ ist wohldefiniert und injektiv: $\overline{x} = \overline{y} \Leftrightarrow y^{-1}x \in S(v) \Leftrightarrow y^{-1}x.v = v \Leftrightarrow x.v = y.v$. Sie ist auch surjektiv, also bijektiv.

Folgerung. G endlich $\Rightarrow |B(v)| \mid |G|$, genauer $|S(v)| \cdot |B(v)| = |G|$. Die Bahnen bilden eine *Partition* von V, d.h. $V = \bigcup_{v \in V} B(v)$ und $B(v) \cap B(w) \neq \varnothing \Rightarrow B(v) = B(w)$, denn mit $x.v = y.w$ folgt $B(v) \subseteq B(w)$: $z.v \in B(v) \Rightarrow z.v = zx^{-1}y.w \in B(w)$.

Definition. Die Operation heißt *transitiv*, wenn $B(v) = V$ für alle $v \in V$, d.h. wenn es nur eine Bahn gibt. Ein $v_0 \in V$ mit $S(v_0) = G$, d.h. mit $x.v_0 = v_0$ für alle $x \in G$, heißt *Fixpunkt* der Operation.

Bemerkung. Eine transitive Operation hat keinen Fixpunkt, außer wenn $G = \{e\}$ oder allgemeiner $|V| = 1$.

Beispiel.

1) Es sei V ein K-Vektorraum, K ein Körper mit $|K| \geq 3$, $G = K^*$. Dann hat die Operation $G \times V \to V, (\lambda, v) \mapsto \lambda v$ nur $0 \in V$ als Fixpunkt, und für $v \in V \setminus \{0\}$ ist $S(v) = \{1\}$. (Es gilt: $|K| \geq 3 \Leftrightarrow |K^*| \geq 2 \Leftrightarrow G \neq \{1\}$)

2) Ist G eine Gruppe, $H \subsetneq G$ eine Untergruppe, $V = G/H$, so ist die Operation $G \times V \to V, (x, aH) \mapsto xaH$ transitiv, insbesondere hat sie keinen Fixpunkt. Genauer: $S(aH) = aHa^{-1}$, speziell $S(H) = H$.

3) Ist V die Menge aller Untergruppen einer Gruppe G und die Operation $G \times V \mapsto V$ durch $(x, H) \mapsto xHx^{-1}$ definiert, so besteht $B(H)$ aus den zu H *konjugierten* Untergruppen der Form xHx^{-1} mit $x \in G$, und es gilt $S(H) = N_G(H)$. Die Fixpunkte sind also die H mit $H \lhd G$; nach Bemerkung ist $[G : N_G(H)]$ die Anzahl der zu H konjugierten Untergruppen.

Beweis.

1) $\lambda v = v \Leftrightarrow (\lambda - 1)v = 0 \Leftrightarrow \lambda = 1 \vee v = 0$.

2) Für $a, b \in G$ ist $bH = xaH$ mit $x = ba^{-1} \in G$; für $x \in G$ gilt: $x \in S(aH) \Leftrightarrow xaH = aH \Leftrightarrow xa \in aH \Leftrightarrow \exists h \in H(xa = ah) \Leftrightarrow x \in aHa^{-1}$. □

Definition. Nun sei $n \geq 1$ und $V = \{1, \ldots, n\}$. Die Menge S_n der bijektiven Abbildungen von V nach V ist eine Gruppe mit id als neutralem Element und $f \circ g$ als Produkt von f und g aus S_n. f^{-1} ist die Umkehrabbildung von $f \in S_n$. S_n nennt man die *symmetrische Gruppe* von Grad n. Ein $\pi \in S_n$ heißt *Permutation* der Zahlen $1, \ldots, n$; man schreibt π als

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \pi(1) & \pi(2) & \pi(3) & \ldots & \pi(n) \end{pmatrix}$$

Bemerkung. Die Operation $S_n \times V \to V, (\pi, v) \mapsto \pi(v)$ ist transitiv.

Beweis. Für $v, w \in V$ ist $\pi(v) = w$ mit $\pi(u) = \begin{cases} v & \text{falls } u = w \\ w & \text{falls } u = v \\ u & \text{falls } u \neq \{v, w\} \end{cases}$ □

Folgerung. $|S_n| = n!$

Beweis. Induktion nach n: $n = 1$ ist klar. Für $n > 1$ gilt: $|B(n)| = n \Rightarrow [S_n : S(n)] = n$; $S(n) \cong S_{n-1} \overset{\text{Ind.}}{\Rightarrow} |S(n)| = (n-1)! \Rightarrow |S_n| = n(n-1)! = n!$ □

Definition. Man nennt $\pi, \sigma \in S_n$ *disjunkt*, wenn für kein $v \in V$ sowohl $\pi(v) \neq v$ als auch $\sigma(v) \neq v$.

Bemerkung. Für disjunkte $\pi, \sigma \in S_n$ gilt $\pi\sigma = \sigma\pi$.

Beweis. Für $v \in V$ zeige $\pi\sigma(v) = \sigma\pi(v)$. Der Fall $\pi(v) = v \wedge \sigma(v) = v$ ist klar. Im Fall $\pi(v) \neq v$ gilt $\sigma(v) = v$, denn σ, π disjunkt, also $\pi\sigma(v) = \pi(v)$. Ferner gilt $\pi\pi(v) \neq \pi(v)$, da π eine Bijektion ist, also $\sigma\pi(v) = \pi(v)$, da π, σ disjunkt. Also $\pi\sigma(v) = \sigma\pi(v)$. Der Fall $\sigma(v) \neq v$ ist analog zu beweisen. □

Definition. Ein $\pi \in S_n$ heißt *Zyklus*, wenn die Operation $\langle \pi \rangle \times V \to V, (\pi^k, v) \mapsto \pi^k(v)$ nur eine Bahn mit mehr als einem Element hat. Die Länge r dieser Bahn heißt dann *Länge* von π. Damit ist diese Bahn von der Form $\{v, \pi(v), \ldots, \pi^{r-1}(v)\}$. Man schreibt dann $\pi = (v\ \pi(v)\ \cdots\ \pi^{r-1}(v))$. Mit anderen Worten: $\pi = (v_1\ \cdots\ v_r)$ mit $v_1 = v$, $v_{i+1} = \pi(v_i)$.

Beispiel.

1) $\pi = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 2 & 4 & 1 & 6 \end{smallmatrix}\right) \in S_6$ ist ein Zyklus: $B(1) = \{1, 3, 2, 5\}$, $B(4) = \{4\}$, $B(6) = \{6\}$, also $\pi = (1\ 3\ 2\ 5)$

2) $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 4 & 2 & 6 \end{smallmatrix}\right) \in S_6$ ist kein Zyklus: $B(1) = \{1, 3\}$, $B(2) = \{2, 5\}$, aber $\sigma = (1\ 3)(2\ 5)$.

Bemerkung. Für jeden Zyklus $\pi = (v_1 \ \cdots \ v_r)$ der Länge r gilt:

a) $\mathrm{ord}(\pi) = r$

b) Für jedes $\sigma \in S_n$ ist auch $\sigma\pi\sigma^{-1}$ ein Zyklus der Länge r, genauer:

$$\sigma\pi\sigma^{-1} = \big(\sigma(v_1) \ \cdots \ \sigma(v_r)\big)$$

Beweis.

a) Wegen $\pi^r(v_i) = v_i$ für $1 \le i \le r$ und $\pi(v) = v$ für $v \in V \setminus \{v_1, \ldots, v_r\}$ ist $\pi^r = \mathrm{id}$; für $1 \le s < r$ ist $\pi^s(v_1) = v_{s+1} \neq v_1$, also $\pi^s \neq \mathrm{id}$.

b) Neben $\sigma\pi\sigma^{-1}(\sigma(v_i)) = \sigma\pi(v_i) = \sigma(v_{i+1})$ für $1 \le i < r$ und $\sigma\pi\sigma^{-1}(\sigma(v_r)) = \sigma\pi(v_r) = \sigma(v_1)$ gilt $\pi\sigma^{-1}(v) = \sigma^{-1}(v)$, d.h. $\sigma\pi\sigma^{-1}(v) = v$ für $\sigma^{-1}(v) \in V \setminus \{v_1, \ldots, v_r\}$, d.h. $v \in V \setminus \{\sigma(v_1), \ldots, \sigma(v_r)\}$ □

Satz.

a) Zu jedem $\pi \in S_n$ gibt es paarweise disjunkte Zyklen $\sigma_1, \ldots, \sigma_k \in S_n$, so dass $\pi = \sigma_k \ldots \sigma_1$ ($k \ge 0$); und die Darstellung $\pi = \sigma_k \ldots \sigma_1$ ist bis auf die Reihenfolge eindeutig.

b) $n \ge 2 \Rightarrow S_n = \langle (1\ 2), (1\ 3), \ldots, (1\ n) \rangle$.

c) $n \ge 3 \Rightarrow S_n = \langle (1\ 2), (1\ 2\ 3\ \cdots\ n) \rangle$.

Beweis.

a) Es seien $B_1, \ldots, B_k$ die Bahnen der induzierten Operation $\langle \pi \rangle \times V \to V$, welche mehr als ein Element haben. Für $1 \le i \le k$ ist $\sigma_i \in S_n$, definiert durch $\sigma_i(v) = \begin{cases} \sigma(v) & v \in B_i \\ v & v \notin B_i \end{cases}$, ein Zyklus, und die $\sigma_1, \ldots, \sigma_k$ sind paarweise disjunkt, und $\pi = \sigma_k \cdots \sigma_1$. Ist auch $\pi = \rho_l \ldots \rho_1$ mit paarweise disjunkten Zyklen $\rho_1, \ldots, \rho_l$, so gibt es $u \in V$ mit $\sigma_1(u) \neq u$ und dazu ein j mit $\rho_j(u) \neq u$. [aus $\sigma_1(u) \neq u$ folgt $\pi(u) \neq u$ wegen $\sigma_1, \ldots, \sigma_k$ disjunkt]. Es reicht zu zeigen: $\sigma_1 = \rho_j$ [Die Behauptung folgt nach Kürzen mit Induktion]. Für $1 \le v \le n$ zeigen wir $\sigma_1(v) = \rho_j(v)$. Der Fall $\sigma_1(v) = v$ und $\rho_j(v) = v$ ist klar. Im Fall $\sigma_1(v) \neq v$ gilt: da $u, v \in B_1$, d.h. $\pi^m(u) = v$ mit $m \ge 0$, gilt $\sigma_1(v) = \sigma_1(\pi^m(u)) = \pi^{m+1}(u)$ und $\rho_j(v) = \rho_j(\pi^m(u)) = \pi^{m+1}(u)$, also $\sigma_1(v) = \rho_j(v)$. Der Fall $\rho_j(v) \neq v$ geht analog.

b) folgt aus a: $(v_1 \ \cdots \ v_r) = (v_1\ v_2)(v_2\ v_3) \cdots (v_{r-1}\ v_r)$, für $2 \le u, v \le n$ mit $u \neq v$ ist $(u\ v) = (1\ u)(1\ v)(1\ u)$.

c) folgt aus b: $(1\ 3) = (1\ 2)(2\ 3)(1\ 2)$, $(1\ 4) = (1\ 3)(3\ 4)(1\ 3)$ etc. Mit $\sigma = (1\ 2\ 3\ \cdots\ n)$ ist $(2\ 3) = \sigma(1\ 2)\sigma^{-1}$, $(3\ 4) = \sigma(2\ 3)\sigma^{-1}$ etc. □

Definition. Ein $\pi \in S_n \setminus \{\mathrm{id}\}$ heißt *gerade* (bzw. *ungerade*), wenn in der Zyklendarstellung von π (das ist die bis auf Reihenfolge eindeutige Zerlegung in Produkte von paarweise disjunkten Zyklen) die Anzahl der Zyklen gerader Länge gerade (bzw. ungerade) ist. Auch id heißt gerade.

Beispiel. (1 2)(3 4) und (1 2 3) sind gerade. Transpositionen sind ungerade.

$$\left(\begin{smallmatrix}1&2&3&4&5&6&7&8&9\\6&4&7&2&5&1&8&9&3\end{smallmatrix}\right) = (1\ 6)(2\ 4)(3\ 7\ 8\ 9)$$

ist ungerade.

Lemma. *Für jedes $\pi \in S_n$ und jede Transposition $\tau \in S_n$ gilt: Ist π gerade (bzw. ungerade), so ist $\tau\pi$ ungerade (bzw. gerade).*

Beweis. 1. Fall: τ, π sind disjunkt, d.h. τ kommt in der Zyklendarstellung von π nicht vor, jedoch in der von $\tau\pi$. 2. Fall: τ,π treffen sich in nur einem Punkt, d.h. $\tau = (v_1\ u)$, $\pi = \underbrace{(v_1\ \cdots\ v_r)\sigma}_{\text{disjunkt}}$, $u \notin \{v_1, \ldots, v_r\}$, $\sigma(u) = u$, dann $\tau\pi = \underbrace{(v_1\ \cdots\ v_r\ u)\sigma}_{\text{disjunkt}}$. Unterscheide r gerade bzw. ungerade. 3. Fall: τ und π treffen sich in zwei Punkten, d.h. a) $\tau = (v_1\ v_j)$, $\pi = \underbrace{(v_1\ \cdots\ v_j\ \cdots\ v_r)\sigma}_{\text{disjunkt}}$ oder b) $\tau = (v_1\ u_1)$, $\pi = \underbrace{(v_1\ \cdots\ v_r)(u_1\ \cdots\ u_s)\sigma}_{\text{disjunkt}}$. In a) gilt $\tau\pi = \underbrace{(v_1\ \cdots\ v_{j-1})(v_j\ \cdots\ v_r)\sigma}_{\text{disjunkt}}$ und in b) $\tau\pi = \underbrace{(v_1\ \cdots\ v_r\ u_1\ \cdots\ u_s)\sigma}_{\text{disjunkt}}$. □

Definition. $A_n = \{\pi \in S_n \colon \pi \text{ gerade}\}$ ist eine Untergruppe der S_n, die *alternierende Gruppe* von Grad n.

Satz. *Für $n \geq 2$ ist* $\operatorname{sign}\colon S_n \to \{+1, -1\} = \mathbb{Z}^\times, \pi \mapsto \begin{cases} +1 & \pi \text{ gerade} \\ -1 & \pi \text{ ungerade} \end{cases}$ *ein Epimorphismus mit Kern A_n. Genauer: Ist $\pi = \tau_k \ldots \tau_1$ mit Transpositionen $\tau_1, \ldots, \tau_k$, so ist* $\operatorname{sign}(\pi) = (-1)^k$.

Beweis. Ist $\pi = \tau_k \ldots \tau_1$ wie oben, so ist τ_1 ungerade, $\tau_2\tau_1$ gerade, $\tau_3\tau_2\tau_1$ ungerade etc., also $\operatorname{sign}(\pi) = (-1)^k$. Ist auch $\sigma = \rho_l \ldots \rho_1$ mit Transpositionen $\rho_1, \ldots, \rho_l$, so ist $\pi\sigma = \tau_k \ldots \tau_1\rho_l \ldots \rho_1$, also $\operatorname{sign}(\pi\sigma) = (-1)^{k+l} = (-1)^k(-1)^l = \operatorname{sign}(\pi)\operatorname{sign}(\sigma)$, mit anderen Worten: sign ist ein Homomorphismus. Klar ist: $\operatorname{Ker}(\operatorname{sign}) = A_n$. sign ist surjektiv, da $\operatorname{sign}(\mathrm{id}) = +1$, $\operatorname{sign}((1\ 2)) = -1$. □

Korollar. $A_n \lhd S_n$, $[S_n : A_n] = 2$, $|A_n| = n!/2$

Beweis. sign induziert einen Isomorphismus $S_n/A_n \to \mathbb{Z}^\times$. □

Satz.

(a) $n \geq 3 \Longrightarrow A_n = \langle (1\ 2\ 3), (1\ 2\ 4), \ldots, (1\ 2\ n) \rangle$

(b) $n \geq 5 \Longrightarrow$ in A_n sind alle Zyklen der Länge 3 zueinander konjugiert.

Beweis.

(a) Es sei $\pi \in S_n$. Wir wissen: $\pi = (1\ v_k) \ldots (1\ v_1)$, $v_i \geq 2$. Ist $\pi \in A_n$, so ist k gerade. Für $i, j \geq 2$ mit $i \neq j$ ist $(1\ i)(1\ j) = (1\ j\ i)$. Der Fall $j = 2$ ist klar. Ist $i = 2$, dann $(1\ j\ 2) = (1\ 2\ j)(1\ 2\ j)$. Ist $i, j \geq 3$, dann $(1\ j\ i) = (1\ 2\ i)(1\ 2\ i)(1\ 2\ j)(1\ 2\ i)$.

(b) Sind $\pi = (v_1\ v_2\ v_3)$, $\rho = (w_1\ w_2\ w_3)$, so ist $\sigma\pi\sigma^{-1} = \rho$ für jedes $\sigma \in S_n$ mit $\sigma(v_i) = w_i$ $(1 \leq i \leq 3)$. Der Fall $\sigma \in A_n$ ist klar. Sei also $\sigma \notin A_n$: Wegen $n \geq 5$ gibt es $k, l \in \{1, \ldots, n\} \setminus \{v_1, v_2, v_3\}$ mit $k \neq l$. Setze $\tau = (k\ l)$, also $\sigma\tau \in A_n$ nach „Lemma“, sowie τ, π disjunkt, also $\tau\pi = \pi\tau$ und damit $(\sigma\tau)\pi(\sigma\tau)^{-1} = \sigma(\pi\tau)\tau^{-1}\sigma^{-1} = \sigma\pi\sigma^{-1} = \rho$. □

Beobachtung. Nicht verwendet wurde, dass $\sigma, \rho \in A_n$ sind. Wir haben also gezeigt: Sind $\pi, \rho \in S_n$ 3-Zyklen, dann gilt $\exists\sigma \in A_n(\sigma\pi\sigma^{-1} = \rho)$.

Beispiel (Kleinsche Vierergruppe)**.** $G = \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \in A_4$. G ist abelsch, aber nicht zyklisch, da jedes $\pi \in G \setminus \{\mathrm{id}\}$ Ordnung 2 hat. zudem ist $G \lhd A_4$, sogar $G \lhd S_4$, denn: für jedes $\pi \in S_4$ und $\{i, j, k, l\} = \{1, 2, 3, 4\}$ ist $\pi(i\ j)(k\ l)\pi^{-1} = (\pi(i)\ \pi(j))(\pi(k)\ \pi(l))$.

Definition. Hat eine Gruppe G nur die Normalteiler $\{e\}$ und G und ist $G \neq \{e\}$, so heißt G *einfach*. Weder A_4 noch S_4 sind einfach (Kleinsche Vierergruppe).

Bemerkung. Eine abelsche Gruppe ist genau dann einfach, wenn sie isomorph zu $\mathbb{Z}/\langle p\rangle$ ist für eine Primzahl p.

Satz. *Für $n \geq 5$ ist A_n einfach.*

Beweis. Sei $\{e\} \neq H \lhd A_n$, zu zeigen ist: $H = A_n$. Da für $n \geq 5$ alle 3-Zykel konjugiert sind und $A_n = \langle\{(1\ 2\ i) \colon i \geq 3\}\rangle$ für $n \geq 3$ genügt es zu zeigen, dass H einen 3-Zyklus enthält. Wähle $\pi \in H \setminus \{e\}$. Wir unterscheiden 3 Fälle:

1. Fall π enthält einen Zyklus von Länge ≥ 4, das heißt $\pi = (v_1\ v_2\ v_3\ v_4\ \ldots\ v_r)\pi'$ (disjunkt) mit $\pi' \in S_n$. Sei $\sigma := (v_1\ v_2\ v_3) \in A_n$. Dann $H \ni \pi(\sigma\pi^{-1}\sigma^{-1}) = (\pi\sigma\pi^{-1})\sigma^{-1} = (v_2\ v_3\ v_4)(v_1\ v_3\ v_2) = (v_1\ v_4\ v_2)$.

2. Fall π enthält zwar keinen Zyklus von Länge ≥ 4, aber mindestens einen 3-Zyklus. Falls $\pi = (v_1\ v_2\ v_3)$ sind wir fertig. Falls $\pi = (v_1\ v_2\ v_3)(v_4\ \ldots\ v_r)\pi'$ mit $\pi' \in S_n$, sei $\sigma := (v_1\ v_2\ v_4) \in A_n$. Dann $H \ni (\pi\sigma\pi^{-1})\sigma^{-1} = (v_2\ v_3\ v_5)(v_1\ v_4\ v_2) = (v_1\ v_4\ v_3\ v_5\ v_2)$, also ist nach Fall 1 $(v_1\ v_5\ v_4) \in H$.

3. Fall π enthält nur 2-Zykel (also 2,4,6,… Stück davon). Falls $\pi = (v_1\ v_2)(v_3\ v_4)$ wähle $v_5 \in \{1, \ldots, n\} \setminus \{v_1, v_2, v_3, v_4\}$ (verwende $n \geq 5$) und setze $\sigma := (v_1\ v_3\ v_5) \in A_n$. Dann $H \ni (\pi\sigma\pi^{-1})\sigma^{-1} = (v_2\ v_4\ v_5)(v_1\ v_5\ v_3) = (v_1\ v_2\ v_4\ v_5\ v_3)$, also ist gemäß Fall 1 $(v_1\ v_5\ v_2) \in H$. Falls $\pi = (v_1\ v_2)(v_3\ v_4)(v_5\ v_6)(v_7\ v_8)\pi'$ mit $\pi' \in S_n$, setze $\sigma := (v_1\ v_3\ v_5) \in A_n$. Dann $H \ni (\pi\sigma\pi^{-1})\sigma^{-1} = (v_2\ v_4\ v_6)(v_1\ v_5\ v_3)$, also nach Fall 2 $(v_2\ v_5\ v_1) \in H$. □

Korollar. *Für $n \geq 5$ hat S_n nur die Normalteiler $\{e\}$, A_n und S_n.*

Beweis. Sei $H \lhd S_n$ mit $n \geq 5$. Dann ist $H \cap A_n$ normal in S_n, also auch normal in A_n. Da A_n einfach ist, gibt es bloß 2 Fälle:

1. Fall $H \cap A_n = A_n$, d.h. $A_n \subseteq H \subseteq S_n$. DA $[S_n : A_n] = 2$, folgt mit Lagrange $A_n = H$ oder $H = S_n$.

2. Fall $H \cap A_n = \{e\}$. Sei $h \in H$ beliebig. Dann erhalten wir $ghg^{-1}h^{-1} \in H \cap A_n = \{e\}$ für alle $g \in G$. $(\operatorname{sign}(ghg^{-1}h^{-1}) = \operatorname{sign}(g)\operatorname{sign}(h)(\operatorname{sign}(g))^{-1}(\operatorname{sign}(h))^{-1} = 1)$. Das heißt $h \in Z(S_n) \underset{n\geq 3}{=} \{e\}$. Es folgt $H = \{e\}$. □

1.4 Auflösbare Gruppen

Ziel Analyse der Struktur von Gruppen G.

Methode Zerlege G in „Bestandteile“ N, G/N. Zerlege diese Bestandteile weiter in noch kleinere Bestandteile etc. Ist G endlich, so stoppt dieser Prozess. Die kleinsten Bestandteile sind die einfachen Gruppen. Auflösbar $\Longleftrightarrow$ die kleinsten Bestandteile sind von der Form $\mathbb{Z}/p\mathbb{Z}$ mit p Primzahl.

Problem Wie ist G aus Bestandteilen zusammengesetzt? G ist durch N und G/N nicht eindeutig bestimmt, z.B. $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $S_3 = \mathbb{Z}/3\mathbb{Z} \rtimes_\phi \mathbb{Z}/2\mathbb{Z} \longrightarrow$ semidirekte Produkte, Gruppenkohomologie.

Definition. Zu $a, b \in G$ (G Gruppe) heißt $[a, b] := aba^{-1}b^{-1}$ der *Kommutator* von a und b. Es gilt $ab = [a, b]ba$. Insbesondere kommutieren a und b genau dann, wenn $[a, b] = e$. Außerdem $[a, b]^{-1} = [b, a]$. Man nennt die von allen Kommuatatoren erzeugte Untergruppe $K(G) := \langle\{[a, b] \colon a, b \in G\}\rangle$ von G die *Kommutator-Untergruppe* von G.

Achtung. $\{[a, b] \colon a, b \in G\}$ ist im Allgemeinen keine Untergruppe.

Bemerkung. $K(G) = \{e\} \Longleftrightarrow G$ abelsch.

Lemma. *Sei $f \colon G \to G'$ ein Gruppenhomomorphismus.*

(a) Es gilt $f(K(G)) \subseteq K(G')$

(b) f surjektiv $\Longrightarrow f(K(G)) = K(G')$

(c) Ist $f \in \operatorname{Aut}(G)$, so ist $f(K(G)) = K(G)$. Insbesondere ist $K(G)$ Normalteiler von G.

Beweis.

(a) Jedes Element von $K(G)$ hat die Form $x = [a_1, b_1] \cdots [a_n, b_n]$ mit $a_i, b_i \in G$. Es ist $f(x) = [f(a_1), f(b_1)] \cdots [f(a_n), f(b_n)] \in K(G')$. Also $f(K(G)) \subseteq K(G')$.

(b) Sei nun f surjektiv und $y = [c_1, d_1] \cdots [c_n, d_n]$ ein beliebiges Element von $K(G')$ (also $c_i, d_i \in G'$). Seien $a_i, b_i \in G$ mit $c_i = f(a_i)$ und $d_i = f(b_i)$. Dann ist $y = f([a_1, b_1] \cdots [a_n, b_n]) \in f(K(G))$. Es folgt $f(K(G)) = K(G')$

(c) folgt aus b) und $K(G) \lhd G$ folgt mit $f = k_x$, $x \in G$. □

Lemma. *$K(G)$ ist der kleinste Normalteiler von G mit $G/K(G)$ abelsch.*

Beweis.

(1) $K(G)$ ist normal (siehe oben) und $G/K(G)$ ist abelsch, denn seien $a, b \in G$ und $\overline{a}, \overline{b}$ ihre Bilder in $G/K(G)$, dann $[\overline{a}, \overline{b}] = \overline{[a, b]} = e$, d.h. $\overline{a}$ und $\overline{b}$ kommutieren.

(2) Sei $H \lhd G$ mit G/H abelsch. Seien $a, b \in G$ und seien $\tilde{a}, \tilde{b}$ die Bilder in G/H. Dann ist $e = [\tilde{a}, \tilde{b}] = \widetilde{[a, b]}$, d.h. $[a, b] \in H$. Es folgt $H \supseteq K(G)$. □

Definition. Die Faktorgruppe $G_{ab} = G/K(G)$ heißt *Abelianisierung* von G. G_{ab} ist die größte abelsche Faktorgruppe von G.

Lemma.

(a) $K(S_n) = A_n$ *für alle* $n \geq 1$.

(b) $K(A_1)$,$K(A_2)$,$K(A_3)$ *sind trivial,* $K(A_4) = V$ *(Kleinsche Vierergruppe)*

(c) $K(A_n) = A_n$ *für alle* $n \geq 5$.

Beweis.

(a) S_n/A_n ist abelsch (wegen $|S_n/A_n| \in \{1, 2\}$), also $K(S_n) \subseteq A_n$. Für $n = 1, 2$ ist A_n trivial, also $A_n \subseteq K(S_n)$. Für $n \geq 3$ gilt $A_n = \langle \{(1\ 2\ i) \colon i \geq 3\} \rangle$ und wegen $(1\ 2\ i) = [(1\ i), (2\ i)]$ ist auch hier $A_n \subseteq K(S_n)$

(b) A_1,A_2,A_3 sind abelsch, $A_4/V \cong \mathbb{Z}/3\mathbb{Z}$ ist abelsch, es folgt $K(A_4) \subseteq V$. Zudem gilt $[(i\ j\ k), (i\ j\ l)] = (i\ j\ k)(i\ j\ l)(i\ k\ j)(i\ l\ j) = (i\ j)(k\ l)$. Also gilt $K(A_4) = V$.

(c) Für $n \geq 5$ ist $\{\mathrm{id}\} \neq K(A_n) \lhd A_n$. Da A_n einfach ist, folgt $K(A_n) = A_n$. □

Definition. Zu jeder Gruppe G definiert man eine absteigende Folge von Untergruppen $G = K_0(G) \supseteq K_1(G) \supseteq K_2(G) \supseteq \ldots$ durch $K_0(G) := G$, $K_1(G) := K(G)$ und $K_i(G) := K(K_{i-1}(G))$ für $i \geq 2$. $K_i(G)$ heißt *i-te Kommutatorgruppe von* G.

Bemerkung. Mittels Induktion zeigt man für einen Gruppenhomomorphismus $f \colon G \to G'$:

- $f(K^i(G)) \subseteq K^i(G')$
- ist f surjektiv, so gilt $f(K^i(G)) = K^i(G')$

Insbesondere sind alle $K^i(G)$ Normalteiler von G (mit $f = k_x$, $x \in G$).

Definition. Eine Gruppe G heißt *auflösbar*, falls $m \geq 1$ existiert mit $K^m(G) = \{e\}$.

Beispiel.

1) Abelsche Gruppen sind auflösbar

2) S_n und A_n sind für $n \leq 4$ auflösbar, für $n \geq 5$ hingegen nicht.

3) Jede Untergruppe und jede Faktorgruppe einer auflösbaren Gruppe ist auflösbar.

4) Ist $H \lhd G$ mit H und G/H auflösbar, so ist G auch auflösbar.

Beweis.

1) folgt aus $K^1(G) = \{e\}$ für G abelsch.

2) S_1, S_2, A_1, A_2, A_3 sind abelsch, also auflösbar. $K^1(S_3) = A_3 \Rightarrow K^2(S_3) = \{e\}$. $K^1(S_4) = A_4 \Rightarrow K^3(S_4) = K^2(A_4) = K^1(V) = \{e\}$. Ist $n \geq 5$, so ist $K^1(S_n) = A_n = K^1(A_n)$ und somit ist $K^m(S_n) = A_n = K^m(A_n)$ für alle $m \geq 1$.

3) $K^m(G) = \{e\}$ und $H \subseteq G$ ist eine Untergruppe. Dann ist $K^m(H) \subseteq K^m(G) = \{e\}$, also $K^m(H) = \{e\}$ und H ist somit auflösbar. Sei nun $H \lhd G$ und $\pi\colon G \to G/H$ der kanonische Epimorphismus. Dann ist wegen π surjektiv $K^m(G/H) = \pi(K^m(G)) = \pi(\{e\}) = \{e\}$, also ist G/H auflösbar.

4) Seien $m, n \geq 1$ mit $K^m(H) = \{e\}$ und $K^n(G/H) = \{e\}$. Dann ist $\pi(K^n(G)) = K^n(G/H) = \{e\}$, also $K^n(G) \subseteq \mathrm{Ker}(\pi) = H$. Also $K^{m+n}(G) = K^m(K^n(G)) \subseteq K^m(H) = \{e\}$. Also ist G auflösbar. □

Bemerkung. Man weiß folgendes

- Jede Gruppe von Ordnung kleiner als $60 = |A_5|$ ist auflösbar.
- Jede Gruppe der Ordnung $p^r q^s$ für Primzahlen p, q und $r, s \geq 0$ ist auflösbar. (Burnside → Darstellungstheorie)
- Jede Gruppe von ungerader Ordnung ist auflösbar. (Feit-Thompson, 1963, 255 Seiten langes Paper)

Definition. Eine *Subnormalreihe* ist eine Folge von Untergruppen $G \supseteq G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{e\}$, so dass für jedes i G_{i+1} normal in G_i ist. Die Gruppen G_i/G_{i+1} heißen *Faktoren* der Subnormalreihe. Sind alle G_{i+1} normal in G, so nennt man eine solche Folge *Normalreihe*.

Bemerkung. $G_{i+1} \lhd G \Longrightarrow G_{i+1} \lhd G_i$.

Beispiel.

- $S_4 \supseteq A_4 \supseteq V \supseteq \{e\}$ ist eine Normalreihe von S_4
- $S_4 \supseteq A_4 \supseteq V \supseteq \langle (1\ 2)(3\ 4) \rangle \supseteq \{e\}$ ist eine Subnormalreihe von S_4, aber keine Normalreihe.

Proposition. *Eine Gruppe ist genau dann auflösbar, wenn sie eine Normalreihe besitzt, deren Faktoren alle abelsch sind.*

Beweis. „⇒“: Sei G auflösbar und $m \geq 1$ mit $K^m(G) = \{e\}$. Dann ist $G \supseteq K^1(G) \supseteq \cdots \supseteq K^m(G) = \{e\}$ Normalreihe mit Faktoren $K^i(G)/K^{i+1}(G) = K^i(G)/K(K^i(G))$, die abelsch sind. „⇐“: Sei $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{e\}$ eine Normalreihe mit abelschen Faktoren. Es folgt $G_i \supseteq K^i(G)$ für alle i und damit $K^m(G) \subseteq G_m = \{e\}$. Also ist G auflösbar. □

Lemma. *Sei $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{e\}$ eine Subnormalreihe von G und seien $G_i/G_{i+1} =: G_{i,0} \supseteq G_{i,1} \supseteq \cdots \supseteq G_{i,r_i} = \{e\}$ Subnormalreihen der Faktoren $G_0/G_1, \ldots, G_{n-1}/G_n$. Seien $\pi_i \colon G_i \to G_i/G_{i+1}$ die kanonischen Epimorphismen. Dann gilt $\pi_i^{-1}(G_{i,0}) = G_i$ und $\pi_i^{-1}(G_{i,r_i}) = G_{i+1}$ und die Folge*

$$\begin{array}{ccccccccc} G = G_0 & \supseteq & \pi_0^{-1}(G_{0,1}) & \supseteq & \ldots & \supseteq & \pi_0^{-1}(G_{0,r_0-1}) & \supseteq & G_1 \\ & \supseteq & \pi_1^{-1}(G_{1,1}) & \supseteq & \ldots & \supseteq & \pi_1^{-1}(G_{1,r_1-1}) & \supseteq & G_2 \\ & & \vdots & & & & \vdots & & \vdots \\ & \supseteq & \pi_{n-1}^{-1}(G_{n-1,1}) & \supseteq & \ldots & \supseteq & \pi_{n-1}^{-1}(G_{n-1,r_{n-1}-1}) & \supseteq & G_n = \{e\} \end{array}$$

ist eine Subnormalreihe mit den Faktoren $\pi_i^{-1}(G_{i,j})/\pi_i^{-1}(G_{i,j+1}) \cong G_{i,j}/G_{i,j+1}$.

Beweis. Klar ist $\pi_i^{-1}(G_{i,0}) = \pi_i^{-1}(G_i/G_{i+1}) = G_i$ und $\pi_i^{-1}(G_{i,r_i}) = \pi_i^{-1}(\{e\}) = G_{i+1}$. Es bleibt zu zeigen, dass $\pi_i^{-1}(G_{i,j+1})$ normal in $\pi_i^{-1}(G_{i,j})$ und $\pi_i^{-1}(G_{i,j})/\pi_i^{-1}(G_{i,j+1}) \cong G_{i,j}/G_{i,j+1}$ ist. Betrachte die Komposition $\pi_i^{-1}(G_{i,j}) \xrightarrow{\pi_i} G_{i,j} \longrightarrow G_{i,j}/G_{i,j+1}$. Jene ist surjektiv und hat den Kern $\pi_i^{-1}(G_{i,j+1})$. Damit folgt die Aussage. □

Korollar. *Eine endliche Gruppe ist genau dann auflösbar, wenn sie eine Subnormalreihe hat, deren Faktoren alle (zyklisch) von Primzahlordnung sind.*

Beweis. Übung.

Bemerkung.

- Das Korollar gilt nicht für unendliche Gruppen. Jede Gruppe, welche eine Subnormalreihe mit endlichen Faktoren hat, ist automatisch endlich. Durch Induktion zeigt man (mit Hilfe von Lagrange) $|G| = \prod_{i=0}^{n-1} [G_i : G_{i+1}]$ für eine Subnormalreihe $G = G_0 \supseteq \cdots \supseteq G_n = \{e\}$. Hingegen ist jede abelsche Gruppe (z.B. $\mathbb{Z}$) auflösbar.
- Eine Subnormalreihe heißt *Kompositionsreihe*, falls alle Faktoren nichttrivial und einfach sind. Es gilt: Die Faktoren einer Kompositionsreihe einer Gruppe G sind eindeutig bis auf Isomorphie und bis auf Reihenfolge. (Satz von Jordan-Hölder)
- Die endlichen einfachen Gruppen sind vollständig klassifiziert. Der Beweis umfasst ca. 15000 Seiten und wurde im Jahr 2004 vollendet.

1.5 p-Gruppen

p ist stets eine Primzahl.

Definition. Eine Gruppe G heißt *p-Gruppe*, falls $|G| = p^a$ für ein $a \geq 0$ (Diese Definition wird später noch revidiert).

Beispiel.

- $\mathbb{Z}/p\mathbb{Z}$ ist eine p-Gruppe.
- D_4 ist eine 2-Gruppe.

- Untergruppen und Faktorgruppen von p-Gruppen sind p-Gruppen.

Lemma. *Ist G eine p-Gruppe und ist $\{e\} \neq N \lhd G$, so ist $N \cap Z(G) \neq \{e\}$. Insbesondere ist $Z(G) \neq \{e\}$, sofern $G \neq \{e\}$.*

Beweis. G operiert auf N durch Konjugation $G \times N \to N, (g, n) \mapsto gng^{-1}$. Es gilt

$$|N| = \sum_{K \subseteq N \text{ Konj. Kl.}} |K|$$

Allgemein ist $|K| = 1 \Leftrightarrow K = \{g\}$ für ein $g \in Z(G) \cap N$ und $|K| = [G : Z]$, wobei Z der Zentralisator eines Elements $g \in K$ ist. Hier gilt $[G : Z]$ teilt $|G| = p^a$, also ist entweder $|K| = 1$ oder $p \mid |K|$. Also ist $|Z(G) \cap N|$ durch p teilbar, insbesondere $Z(G) \cap N \neq \{e\}$. □

Korollar. *p-Gruppen sind auflösbar.*

Beweis. Durch Induktion nach $|G| = p^a$. $|G| = 1$ ist klar. Sonst gilt $\{e\} \neq Z(G) \lhd G$ und $G/Z(G)$ ist auflösbar, weil es eine p-Gruppe mit kleinerer Ordnung ist. Also ist G auflösbar. □

2 Ringe

2.1 Ringe und Moduln

Definition. Eine Menge H mit einer Abbildung $m\colon H \times H \to H, (x, y) \mapsto xy$ und einem Element $e \in H$ heißt *Halbgruppe*, wenn $x(yz) = (xy)z$ für alle $x, y, z \in H$ und $xe = x = ex$ für alle $x \in H$. Zum Beispiel sind $(\mathbb{N}, +, 0)$,$(\mathbb{Z}, \bullet, 1)$ Halbgruppen, aber keine Gruppen.

Ein *Ring* ist eine Menge R mit zwei Abbildungen $+\colon R \times R \to R, (x, y) \mapsto x + y$ und $\bullet\colon R \times R \to R, (x, y) \mapsto xy$ sowie Elementen $0, 1 \in R$, so dass folgende Eingeschaften erfüllt sind

1) $(R, +, 0)$ ist eine abelsche Gruppe

2) $(R, \bullet, 1)$ ist eine Halbgruppe

3) $x(y + z) = xy + xz$ und $(x + y)z = xz + yz$ für alle $x, y, z \in R$.

Beobachtung.

a) $x0 = 0 = 0x$ für alle $x \in R$.

b) Ist $0 = 1$ in R, so ist $R = \{0\}$, denn $x \in R \Rightarrow x = 1x = 0x = 0$

Definition. Ein Ring heißt *kommutativ*, wenn $xy = yx$ für alle $x, y \in R$. Eine Teilmenge A eines Rings R nennt man *Unterring*, wenn A eine Untergruppe von $(R, +, 0)$ und $xy \in A$ für alle $x, y \in A$ sowie $1 \in A$ ist. Im Folgenden sei R stets ein Ring.

Definition. Man nennt $x \in R$ *invertierbar* oder eine *Einheit*, wenn es ein $y \in R$ gibt mit $xy = 1 = yx$. Die Menge $R^\times$ aller Einheiten von R ist mit der Multiplikation eine Gruppe, die *Einheitengruppe* von R. Ist R ein kommutativer Ring, so ist $R^\times$ eine abelsche Gruppe. Es gilt $R = \{0\} \iff R^\times = R$

Beispiel.

1) $\mathbb{Z}$ ist ein Ring. Es gilt $\mathbb{Z}^\times = \{-1, 1\}$. Der einzige Unterring von $\mathbb{Z}$ ist $\mathbb{Z}$. (siehe Übung)

2) Ist V ein K-Vektorraum, so ist $\mathrm{End}(V)$ ein Ring mit $(f, g) \mapsto f \circ g$ als Multiplikation, $1 = \mathrm{id}_v$ und $\mathrm{End}(V)^\times = \mathrm{Aut}(V)$. Ist speziell $V = K^n$ ist $\mathrm{End}(V) = K^{n\times n}$,$\mathrm{Aut}(V) = \mathrm{GL}(n, K)$.

Definition. Eine Abbildung $f\colon R \to R'$ zwischen Ringen heißt *Ringhomomorphismus*, wenn folgende Eigenschaften erfüllt sind

1) $f(x + y) = f(x) + f(y)$ für alle $x, y \in R$.

2) $f(xy) = f(x)f(y)$ für alle $x, y \in R$.

3) $f(1) = 1$

Bemerkung. Für einen Ringhomomorphismus $f\colon R \to R'$ gilt $f(R^\times) \subseteq (R')^\times$ (Übung), speziell: $R^\times \to (R')^\times, x \mapsto f(x)$ ist ein Gruppenhomomorphismus.

Definition. Ein *Ideal* I von R ist eine Untergruppe von $(R, +, 0)$, so dass $ar \in I \ni ra$ für alle $a \in I$ und $r \in R$.

Definition. Auf der Faktorgruppe R/I ist die Abbildung $R/I \times R/I \to R/I$, $(\overline{x}, \overline{y}) \mapsto \overline{xy}$ wohldefiniert und macht R/I zu einem Ring mit Eins $\overline{1}$, dem sogenannten *Faktorring* von R modulo I.

Beweis der Wohldefiniertheit. $(\overline{x}, \overline{y}) = (\overline{u}, \overline{v}) \Leftrightarrow (\overline{x} = \overline{u} \wedge \overline{y} = \overline{v}) \Leftrightarrow (x - u \in I \wedge y - v \in I) \Rightarrow (xy - uy \in I \wedge uy - uv \in I) \Rightarrow xy - uv \in I \Leftrightarrow \overline{xy} = \overline{uv}$ □

Bemerkung. Die kanonische Abbildung $R \to R/I, x \mapsto \overline{x}$ ist ein surjektiver Ringhomomorphismus.

Beispiel. Jede Untergruppe U von $\mathbb{Z}$ als abelscher Gruppe ist ein Ideal von $\mathbb{Z}$ als Ring.

Beweis. Wir wissen: $U = \langle n\rangle, n \geq 0$. Dann: $a \in U \Leftrightarrow n \mid a \Rightarrow (n \mid ra \wedge n \mid ar) \Leftrightarrow (ra \in U \wedge ar \in U)$ für alle $r \in \mathbb{Z}$. □

Bemerkung. Also ist $\mathbb{Z}/\langle n\rangle = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ ein Ring mit $\overline{x}\,\overline{y} = \overline{xy}$, wobei $n \geq 1$.

Bemerkung. Es sei $n \in \mathbb{Z}, n \geq 1$. Für jedes $x \in \mathbb{Z}$ sind äquivalent:

i) $\overline{x}$ ist eine Einheit des Ringes $\mathbb{Z}/\langle n\rangle$.

ii) $\overline{x}$ ist ein Erzeugendes der Gruppe $\mathbb{Z}/\langle n\rangle$.

iii) x und n sind teilerfremd, d.h. $\mathrm{ggT}(x, n) = 1$.

Beweis.

i $\Rightarrow$ **ii** $\overline{1} = \overline{x}\,\overline{y} = \overline{xy} = \underbrace{\overline{x + \cdots + x}}_{y\text{-mal}} = \underbrace{\overline{x} + \cdots + \overline{x}}_{y\text{-mal}} = y\overline{x}$, also $\overline{1} \in \langle\overline{x}\rangle$ und damit $\mathbb{Z}/\langle n\rangle = \langle\overline{x}\rangle$, da ja $\mathbb{Z}/\langle n\rangle = \langle\overline{1}\rangle$.

ii $\Rightarrow$ **iii** Mit $\overline{1} \in \langle\overline{x}\rangle$ ist $\overline{1} = y\overline{x}$ für ein $y \in \mathbb{Z}$, d.h. $\overline{1} = \overline{yx}$ wie oben, mit anderen Worten $1 - yx \in \langle n\rangle$, d.h. $1 - yx = zn$ für ein $z \in \mathbb{Z}$, d.h. $1 = yx + zn$, d.h. $\mathrm{ggT}(x, n) = 1$.

iii $\Rightarrow$ **i** Da jede Untergruppe der zyklischen Gruppe $\mathbb{Z}$ wieder zyklisch ist, gibt es $u \in \mathbb{Z}$ mit $u \geq 0$ und $\langle u\rangle = \langle x, n\rangle$, also $u \geq 1$. Da $u \mid x \wedge u \mid n$, ist nach Vorraussetzung $u = 1$. Es ergibt sich $1 \in \langle x, n\rangle$, d.h. $1 = ax + bn$ für geeignete $a, b \in \mathbb{Z}$, wofür $\overline{1} = \overline{a}\,\overline{x} + \overline{b}\,\overline{n} = \overline{a}\,\overline{x}$ wegen $\overline{n} = 0$. Es folgt $\overline{x} = (\mathbb{Z}/\langle n\rangle)^\times$ mit $\overline{x}^{-1} = \overline{a}$. □

Folgerung.

$$\left|(\mathbb{Z}/\langle n\rangle)^\times\right| = \left|\{x \in \{1, \ldots, n\} \colon \mathrm{ggT}(x, n) = 1\}\right|$$

Diese Zahl $\varphi(n) = |(\mathbb{Z}/\langle n\rangle)^\times|$ heißt *Eulersche φ-Funktion* von n.

Beispiel. $\varphi(1) = 1$, da $\mathbb{Z}/\langle 1\rangle = \{0\}$. $\varphi(2) = 1$, da $\mathbb{Z}/\langle 2\rangle = \{\overline{0}, \overline{1}\}$,$(\mathbb{Z}/\langle 2\rangle)^\times = \{1\}$. $\varphi(3) = 2$, da $\mathbb{Z}/\langle 3\rangle = \{\overline{0}, \overline{1}, \overline{2}\}$,$(\mathbb{Z}/\langle 4\rangle)^\times = \{\overline{1}, \overline{2}\}$. Allgemeiner: $\varphi(p) = p - 1$, falls p Primzahl, sogar: $\varphi(p^k) = p^k - p^{k-1}$, falls p Primzahl.

Beweis. Für $1 \leq x \leq p^k$ gilt: $\mathrm{ggT}(x, p^k) \neq 1 \Leftrightarrow p \mid x \Leftrightarrow \exists y \in \{1, \ldots, p^{k-1}\} \colon x = py$. Es gibt p^{k-1} solche y. Also $\varphi(p^k) = |\mathbb{Z}/\langle p^k\rangle| - p^{k-1} = p^k - p^{k-1}$ □

Beispiel. $\varphi(4) = \varphi(2^2) = 2^2 - 2^1 = 4 - 2 = 2$, allgemeiner $\varphi(2^k) = 2^{k-1}$. Oft sieht man: $\varphi(p^k) = p^k(1 - \frac{1}{p}) = p^k\frac{p-1}{p} = p^{k-1}(p-1)$. Später: $\varphi(m \cdot n) = \varphi(m)\varphi(n)$ falls $\mathrm{ggT}(m, n) = 1$. Damit: $n = p_1^{k_1} \ldots p_r^{k_r}$ mit paarweise verschiedenen Primzahlen $p_1, \ldots, p_r$, so ist $\varphi(n) = \prod_{i=1}^r p_i^{k_i - 1}(p_i - 1)$.

Definition. Sei R ein Ring. Mit $R^{\mathbb{N}}$ bezeichnet man die Menge der unendlichen Folgen $(a_n)_{n\in\mathbb{N}}$ aus Elementen von R. Mit $R^{(\mathbb{N})}$ die Menge der $(a_n)_{n\in\mathbb{N}} \in R^{\mathbb{N}}$, für welche $a_n = 0$ für fast alle $n \in \mathbb{N}$. Diese Menge $R^{(\mathbb{N})}$ wird zu einem Ring, wenn man $(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} = (a_n + b_n)_{n\in\mathbb{N}}$ und $(a_n)_{n\in\mathbb{N}}(b_n)_{n\in\mathbb{N}} = (c_n)_{n\in\mathbb{N}}$ mit $c_n = \sum_{i+j=n} a_i b_j = a_0 b_n + \cdots + a_n b_0$ setzt, sowie Null $(0, 0, \ldots)$ und Eins $(1, 0, 0, \ldots)$. Für $X = (0, 1, 0, 0, \ldots)$ und $f \in R^{(\mathbb{N})}$ mit $f = (a_0, a_1, \ldots, a_n, 0, 0, \ldots)$ ist $Xf = (0, a_0, a_1, \ldots, a_n, 0, 0, \ldots) = fX$ und $(*)$ $f = \sum_{i=0}^n (a_i, 0, 0, \ldots)X^i$. Identifiziert man jedes $a \in R$ mit $(a, 0, 0, \ldots) \in R^{(\mathbb{N})}$, so wird $(*)$ zu $f = \sum_{i=0}^n a_i X^i$, d.h. f ist ein *Polynom* in X mit den Koeffizienten $a_0, \ldots, a_n \in R$. Deshalb heißt $R^{(\mathbb{N})}$ der *Polynomring* über R, kurz $R[X]$. Mit obiger Identifizierung ist R ein Unterring von $R[X]$. Die Elemente von R heißen *konstante Polynome*.

Definition. Ist $f = \sum_{i=0}^n a_i X^i \in R[X]$ mit $a_n \neq 0$, so heißt a_n der *Leitkoeffizient* und n der *Grad* $\deg(f)$ von f. Wir setzen $\deg(0) = -1$ (oft sieht man auch $\deg(0) = -\infty$). Für $f \in R[X]$ gilt: $f \in R \Leftrightarrow \deg(f) \leq 0$.

Beobachtung. Für $f, g \in R[X]$ mit $f, g \neq 0$ gilt:

a) $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$

b) $\deg(fg) \leq \deg(f) + \deg(g)$

Definition. Für $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ und $t \in R$ setzt man $f(t) = \sum_{i=0}^{n} a_i t^i$. Die *Auswertungsabbildung* $\varepsilon_t \colon R[X] \to R, f \mapsto f(t)$ ist ein surjektiver Ringhomomorphismus, wenn t im Zentrum von R liegt (also insbesondere wenn R kommutativ ist). Ist $f(t) = 0$, d.h. $f \in \mathrm{Ker}(\varepsilon_t)$, so heißt t *Nullstelle* von f.

Definition. Ein Ring R heißt *Integritätsring*, wenn R kommutativ ist, $1 \neq 0$ in R und für alle $a, b \in R$ gilt: $a \neq 0 \wedge b \neq 0 \Rightarrow ab \neq 0$, d.h. $ab = 0 \Rightarrow a = 0 \vee b = 0$.

Beispiel.

1) $\mathbb{Z}$ ist ein Integritätsring

2) Jeder Körper ist ein Integritätsring

3) Für $n \geq 1$ gilt: $\mathbb{Z}/\langle n \rangle$ Integritätsring $\iff n$ Primzahl.

Beweis. Sei zuerst $\mathbb{Z}/\langle n \rangle$ ein Integritätsring. Wegen $\mathbb{Z}/\langle 1 \rangle = \{0\}$ ist $n \geq 2$. Ferner gilt $n \mid xy \iff \overline{x}\,\overline{y} = 0 \underset{\text{Int.Ring}}{\iff} \overline{x} = 0 \vee \overline{y} = 0 \iff n \mid xy \underset{\text{Primzahl}}{\iff} n \mid x \vee n \mid y$, d.h. $\overline{x} = 0 \vee \overline{y} = 0$. □

Bemerkung. Es gilt: R ist genau dann kommutativ, wenn $R[X]$ kommutativ ist und $1 \neq 0$ in R genau dann, wenn $1 \neq 0$ in $R[X]$.

Bemerkung. Für jeden Integritätsring R gilt:

a) $R[X]$ ist ein Integritätsring

b) $\deg(fg) = \deg(f) + \deg(g)$ für $f, g \in R[X]$ mit $f, g \neq 0$

c) $(R[X])^\times = R^\times$

Beweis. Es seien $f, g \in R[X]$. Für $f = \sum_{i=0}^{n} a_i X^i$ und $g = \sum_{j=0}^{m} b_j X^j$ ist $fg = \sum_{k=0}^{m+n} c_k X^k$ mit $c_k = \sum_{i+j=k} a_i b_j$, speziell $c_{n+m} = a_n b_m$. Ist $a_n \neq 0$ und $b_m \neq 0$, so ist $c_{n+m} \neq 0$. Es folgen a) und b). Noch zu c): Ist $fg = 1$, so $f, g \neq 0$ nach a): $1 \neq 0$ in $R[X]$. Es folgt mit b): $0 \leq \deg(f) + \deg(g) = \deg(fg) = \deg(1) = 0$, also $\deg(f) = 0 = \deg(g)$, also $f, g \in R$, sogar $fg = 1$. □

Definition. Ein Polynom mit Leitkoeffizient 1 heißt *normiert* oder *unitär*.

Satz. *Es sei R ein kommutativer Ring und $g \in R[X]$ normiert.*

a) Zu jedem $f \in R[X]$ gibt es eindeutig bestimmte $q, r \in R[X]$, so dass $f = qg + r$ und $\deg(r) < \deg(g)$ (enthält den Fall $r = 0$)

b) Zu jedem $f \in R[X]$ und zu jedem $a \in R$ gibt es genau ein $q \in R[X]$ mit $f = (X - a)q + f(a)$. Insbesondere gilt (Fall $f(a) = 0$): Genau dann ist $a \in R$ eine Nullstelle von $f \in R[X]$, wenn es ein $q \in R[X]$ gibt mit $f = (X - a)q$. Dieses q ist eindeutig bestimmt.

Beweis.

a) Ist $\deg(f) < \deg(g)$, so setze $q = 0$ und $r = f$ (enthält den Fall $f = 0$). Nun sei $\deg(f) \geq \deg(g)$. Induktion nach $\deg(f) = n$. Mit $m = \deg(g)$ ist $n \geq m \geq 0$. Ist $n = 0$, so ist $m = 0$, also $g = 1$. Setze $q = f$ und $r = 0$. Ist $n \geq 1$ und a_n der Leitkoeffizient von f, so hat $f' = f - a_n X^{n-m} g$ einen Grad kleiner n. Nach Induktion gibt es $q', r' \in R[X]$ mit $f' = q'g + r'$ und $\deg(r') < \deg(g)$. Dafür ist $f = f' + a_n X^{n-m} g = (q' + a_n X^{n-m})g + r'$ wie verlangt. Noch zur Eindeutigkeit: Da $g \in R[X]$ normiert ist und $qg+r = q_1 g+r_1$ mit $\deg(r) < \deg(g)$ und $\deg(r_1) < \deg(g)$, gilt $q = q_1$, also auch $r = r_1$, denn es gilt$(q - q_1)g = r_1 - r$ und wäre $q \neq q_1$, d.h. $q-q_1 \neq 0$, so wäre $\deg(q-q_1) \geq 0$ und $\deg(g) > \max\{\deg(r), \deg(r_1)\} \geq \deg(r_1-r) = \deg((q-q_1)g) \overset{(*)}{=} \deg(q-q_1) + \deg(g) \geq \deg(g)$, was unmöglich ist. Noch zu $(*)$: $\leq$ gilt immer und $\geq$ gilt hier da g normiert ist.

b) Schreibe $f = q(X-a)+r$ wie in a), also $\deg(r) \leq 0$, d.h. $r \in R$. Also $r = q(a)\cdot 0 + r = f(a)$. □

Korollar. *Es sei R ein Integritätsring.*

a) Jedes $f \in R[X]$ mit $f \neq 0$ und $\deg(f) = n$ hat höchstens n verschiedene Nullstellen

b) Für $g \in R[X]$ ist $g = h$ schon dann, wenn $g(a) = h(a)$ für unendlich viele verschiedene $a \in R$.

Beweis. b) folgt aus a), angewandt auf $f = g - h$. Zu a): Sind $a_1, \ldots, a_k$ Nullstellen von f, paarweise verschieden, so ist $f = (X - a_1)q_1$ gemäß Satz b), wofür $0 = f(a_2) = (a_2 - a_1)q_1(a_2)$, also $q_1(a_2) = 0$ (R ist ein Integritätsring), also wieder $q_1 = (X - a_2)q_2$ etc., schleißlich $f = (X - a_1) \cdots (X - a_k)q_k$, worin $q_k \neq 0$ (da $f \neq 0$), also $n = \deg(f) = k + \deg(q_k) \geq k$. □

Beobachtung. In b) reicht es, dass $g(a) = h(a)$ für mehr als $\max\{\deg(g), \deg(h)\}$ verschiedene a.

Satz. *Für jede endliche Gruppe G mit $|G| = n$ sind äquivalent:*

i) G ist zyklisch.

ii) Für jedes $d \mid n$ hat G genau eine Untergruppe der Ordnung d.

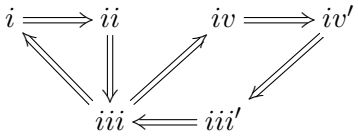
iii) Für jedes $d \mid n$ hat G genau $\varphi(d)$ Elemente der Ordnung d.

iv) Für jedes $d \mid n$ hat G genau d Elemente x mit $x^d = e$

iii') Für jedes $d \mid n$ hat G höchstens $\phi(d)$ Elemente der Ordnung d.

iv') Für jedes $d \mid n$ hat G höchstens d Elemente x mit $x^d = e$

Beweis. Wir gehen nach folgendem Plan vor:



i $\Rightarrow$ **ii** früher gezeigt.

iv $\Rightarrow$ **iv'** %

***** Für $d \mid n$ sei $P_d = \{x \in G \colon x^d = e\}$, $Q_d = \{x \in G \colon \operatorname{ord}(x) = d\}$. Damit $Q_d \subseteq P_d$. Ferner sei $\psi_G(d) = |Q_d|$. Wegen $G = P_n$ und $P_n = \bigsqcup_{d|n} Q_d$ ist $n = \sum_{d|n} \psi_G(d)$.

ii $\Rightarrow$ **iii** Bezeichnet H_d die einzige Untergruppe von G der Ordnung d, so ist $Q_d = \{x \in H_d \colon \langle x \rangle = H_d\}$, also $\psi_G(d) = \varphi(d)$. Mit $(*)$ folgt $n = \sum_{d|n} \varphi(d)$. $(+)$

iii $\Rightarrow$ **i** $d = n$: $\psi_G(n) = \varphi(n) > 0$, also $Q_n \neq \varnothing$.

iii $\Rightarrow$ **iv** Analog zu $(*)$ bzw. $(+)$ gelten $|P_d| = \sum_{k|d} \psi_G(k)$ und $\sum_{k|d} \varphi(k) = d$.

iv' $\Rightarrow$ **iii'** Genauer gilt für $d \mid n$: Aus $\psi_G(d) > 0$, d.h. $Q_d \neq \varnothing$ folgt $\psi_G(d) = \varphi(d)$. Nun sei $\psi_G(d) > 0$; nehme $x \in Q_d$; setze $U = \langle x \rangle$. Wegen $|U| = d$ ist $U \subseteq P_d$; mit $|P_d| \leq d$ sogar $U = P_d$, also $Q_d \subseteq U$, d.h. $Q_d = Q_d \cap U$ und damit $\psi_G(d) = |Q_d \cap U| = \psi_U(d)$. Da U zklisch ist, ist $\psi_U(d) = \varphi(d)$ wie oben gezeigt.

iii' $\Rightarrow$ **iii** $n \overset{(*)}{=} \sum_{d|n} \psi_G(d) \overset{iii'}{\leq} \sum_{d|n} \varphi(d) \overset{(+)}{=} n \overset{iii'}{\Longrightarrow}$ in jedem $\psi_G(d) \leq \varphi(d)$ gilt „=“. □

Lemma. *Es sei G eine Gruppe mit $|G| = n \geq 1$. Ist $|\{x \in G \colon x^d = e\}| \leq d$ für jedes $d \geq 1$ mit $d \mid n$, dann ist G zyklisch.*

Beweis. Folgt aus dem vorhergehenden Lemma. □

Korollar. *Jede endliche Untergruppe von $R^\times$ ist zyklisch, falls R ein Integritätsring ist. Speziell: Für jeden endlichen Körper K ist $K^\times$ zyklisch.*

Beweis. Folgt aus obigem Lemma, denn: Betrachte die Untergruppe $G \subseteq R^\times$ mit R Integritätsring. Es gilt $|G| = n \geq 1$. Ist $d \geq 1$ mit $d \mid n$, so ist $\{x \in G \colon x^d = 1\} \subseteq \{x \in R \colon f(x) = 0\}$ für $f = X^d - 1$. Nun hat die rechte Menge nach dem ersten Korollar höchstens d Elemente. □

Bemerkung. Jeder endliche Integritätsring ist schon ein Körper.

Beweis. Sei R ein Integritätsring, d.h. für alle $a \in R \setminus \{0\}$ ist die Abbildung $\mu_a \colon R \to R, b \mapsto ab$ injektiv, denn $ab = ab' \Leftrightarrow a(b - b') = 0 \Rightarrow b - b' = 0 \Leftrightarrow b = b'$. Ist R endlich, so ist μ_a surjektiv, speziell gibt es $b \in R$ mit $\mu_a(b) = 1$, d.h. $ab = 1$, also $a \in R^\times$. Es folgt: R ist ein Körper. □

Definition. Ein *euklidischer Ring* ist ein Paar (R, δ) aus einem Integritätsring R und einer Abbildung $\delta\colon R \setminus \{0\} \to \mathbb{N}$, so dass mit $\delta(0) = -1$ gilt: Zu $x, y \in R$ mit $y \neq 0$ gibt es $u, v \in R$ mit $x = uy + v$ und $\delta(v) < \delta(y)$. (enthält den Fall $v = 0$)

Beispiel.

1) $(\mathbb{Z}, |\cdot|)$ ist ein euklidischer Ring.

2) Ist K ein Körper, dann ist $(K[X], \deg)$ ein euklidischer Ring, denn sind $f, g \in K[X]$ mit $g \neq 0$ und hat g den Leitkoeffizienten $b \in K$, dann ist $b \neq 0$, also $b \in K^\times$, und $b^{-1}g$ ist unitär. Also $f = q(b^{-1}g) + r = (b^{-1}q)g + r$ mit $\deg(r) < \deg(b^{-1}g) = \deg(g)$.

Definition. Es sei R ein beliebiger Ring. Ein *R-Modul* ${}_RM$ ist eine (additive) abelsche Gruppe M mit einer Abbildung $R \times M \to M, (r, x) \mapsto rx$, so dass für alle $r, s \in R$ und $x, y \in M$ gilt

$$r(sx) = (rs)x \qquad 1x = x \qquad r(x + y) = rx + ry \qquad (r + s)x = rx + sx$$

Ist M' ein R-Modul, so heißt eine Abbildung $f\colon M \to M'$ ein *Modulhomomorphismus*, wenn für $r \in R$ und $x, y \in M$ gilt:

$$f(x + y) = f(x) + f(y) \quad f(rx) = rf(x)$$

Ein *Untermodul* eines R-Moduls M ist eine Untergruppe U von $(M, +, 0)$ mit $rx \in U$ für alle $r \in R$ und $x \in U$. Für jedes $x \in M$ ist $Rx = \{rx\colon r \in R\}$ ein Untermodul von M. Für Untermoduln U, V ist $U + V = \{x + y\colon x \in U, y \in V\}$ ein Untermodul. $U + V$ ist der kleinste Untermodul, der U und V umfasst. Speziell ist $Rx_1 + \cdots + R_xn = \{r_1x_1 + \cdots + r_nx_n\colon r_1, \ldots, r_n \in R\}$ ein Untermodul von M für $x_1, \ldots, x_n \in M$. $\{0\}$ und M sind Untermoduln von M, die *trivialen Untermoduln*.

Beispiel.

1) Ist R ein Körper, so sind die R-Moduln genau die R-Vektorräume, die Untermoduln sind genau die Untervektorräume und die Modulhomomorphismen sind genau die R-linearen Abbildungen.

2) Jeder Ring R wird durch $R \times R \to R, (r, x) \mapsto rx$ zu einem R-Modul. Seine Untermoduln heißen *Linksideale* von R.

3) Jede abelsche Gruppe G wird durch $\mathbb{Z} \times G \to G, (z, x) \mapsto zx$ zu einem $\mathbb{Z}$-Modul. Die Untermoduln sind genau die Untergruppen von $(G, +, 0)$.

4) Für jede Teilmenge S eines R-Moduls M ist die Menge $(S) = \{\sum_{i=1}^n r_ix_i\colon n \geq 1; r_1, \ldots, r_n \in R, x_1, \ldots, x_n \in S\}$ aller *Linearkombinationen* von Elementen aus S ein Untermodul von M, der *von S erzeugte Untermodul*. Ist $S \neq \varnothing$, so ist $(S) = \bigcap\{U \subseteq M\colon U \text{ Untermodul}, S \subseteq U\}$ der kleinste Untermodul von M, der S umfasst (Beweise wie für Gruppen). Speziell gilt $(x) = Rx$ und $(x_1, \ldots, x_n) = Rx_1 + \cdots + Rx_n$, $U + V = (U \cup V)$, allgemeiner $\sum_{i \in I} U_i = (\bigcup_{i \in I} U_i)$.

5) Es sei U ein Untermodul des R-Moduls M. Die Faktorgruppe M/U wird durch $R \times M/U \to M/U, (r, \overline{x}) \mapsto \overline{rx}$ zu einem R-Modul, dem *Faktormodul* von M modulo U. Das ist wohldefiniert, denn $\overline{x} = \overline{y} \Leftrightarrow x - y \in U \Rightarrow rx - ry \in U \Leftrightarrow \overline{rx} = \overline{ry}$. Die kanonische Abbildung $M \to M/U, x \mapsto \overline{x}$ ist ein Modulepimorphismus mit den analogen Eigenschaften wie bei Gruppen. Insbesondere gilt für jeden Modulhomomorphismus $f\colon M \to M'$, dass $M/\operatorname{Ker}(f) \cong \operatorname{Im}(f)$. Die Untermoduln von M/U sind genau die V/U mit V Untermodul von M mit $V \supseteq U$, wofür $(M/U)/(V/U) \cong M/V$. Für Untermoduln U, W von M gilt $(U + W)/U \cong W/(U \cap W)$.

2.2 Kettenbedingungen

Definition. Sei R ein Ring. Ein R-Modul M heißt *zyklisch*, wenn $M = (x)$ für ein $x \in M$, bzw. *endlich erzeugt*, wenn $M = (x_1, \ldots, x_n)$ für geeignete $x_1, \ldots, x_n \in M$. Im Allgemeinen sind die Untermoduln eines zyklischen Moduls nicht alle zyklisch.

Definition. Zyklische Ideale heißen auch *Hauptideale*. Sind alle Ideale eines Integritätsrings R Hauptideale, so nennt man den R einen *Hauptidealring (HIR)*.

Beispiel. ${}_RR = (1)$ ist zyklisch für einen beliebigen Ring R, aber in $R = \mathbb{Z}[X]$ ist das Ideal $I = (2, X)$ nicht zyklisch, denn wäre $I = (f)$, d.h. $2 = g_1 f$, $X = g_2 f$, $f = 2h_1 + Xh_2$, so wäre $\deg(f) = 0$, $f = \pm 1$, $f(0) = 2h_1(0)$, was unmöglich ist, da $f \in \{\pm 1\}$. Also ist $\mathbb{Z}[X]$ kein Hauptidealring. Jedoch ist $\mathbb{Z}$ ein Hauptidealring und $K[X]$ ist ein Hauptidealring, falls K ein Körper ist, zum Beispiel $K = \mathbb{Q}$.

Bemerkung. Ist (R, δ) ein euklidischer Ring, so ist R ein Hauptidealring.

Beweis. Es sei I ein Ideal von R mit $I \neq \{0\}$. Es existiert $n_0 = \min\{\delta(a)\colon a \in I \setminus \{0\}\}$ und dazu $a_0 \in I \setminus \{0\}$ mit $\delta(a_0) = n_0$. Dafür ist $I = (a_0)$, denn „$\supseteq$“ ist trivial und für „$\subseteq$“: Es sei $x \in I$. Es gibt $y, z \in R$ mit $x = ya_0 + z$ und $\delta(z) < \delta(a_0) = n_0$, also $z = 0$, d.h. $x = ya_0 \in (a_0)$, oder $z \neq 0$, dann aber $z = x - ya_0 \in I$, was unmöglich ist. □

Folgerung. $\mathbb{Z}$ und $K[X]$ mit K Körper sind Hauptidealringe. Hingegen ist $\mathbb{Z}[X]$ kein Hauptidealring, da z.B. $(2, X)$ nicht zyklisch ist.

Definition. Es sei R ein Ring. Ein R-Modul M heißt *noethersch*, wenn jeder Untermodul von M endlich erzeugt ist. Insbesondere ist M selbst endlich erzeugt. Der Ring R heißt *linksnoethersch*, wenn ${}_RR$ ein noetherscher R-Modul ist. Ist R kommutativ, heißt R auch *noethersch*.

Satz. *Es sei R ein Ring. Für jeden R-Modul M sind äquivalent:*

i) M ist noethersch.

ii) Jede Folge $U_0 \subseteq U_1 \subseteq U_2 \subseteq \ldots$ von Untermoduln von M wird stationär*, d.h. es gibt $N \in \mathbb{N}$ mit $U_N = U_{N+1} = U_{N+2} = \ldots$*

iii) Jede nichtleere Menge $\mathfrak{U}$ von Untermoduln von M hat ein maximales Element*, das ist ein $U \in \mathfrak{U}$ derart, dass für alle $V \in \mathfrak{U}$ gilt: aus $U \subseteq V$ folgt $U = V$.*

Beweis. Wir verwenden:

ii') Es gibt keine Folge $U_0 \subsetneq U_1 \subsetneq U_2 \subsetneq \dots$ von Untermoduln von M.

iii') Hat eine Menge $\mathfrak{U}$ von Untermoduln von M kein maximales Element, d.h. $\forall U \in \mathfrak{U} \exists V \in \mathfrak{U}\colon U \subsetneq V$, so ist $\mathfrak{U} = \varnothing$.

Klar ist ii) $\Leftrightarrow$ ii') und iii) $\Leftrightarrow$ iii').

i $\Rightarrow$ **ii** Der Untermodul (!) $U = \bigcup_{n\in\mathbb{N}} U_n$ ist nach i endlich erzeugt, etwa $U = (x_1, \dots, x_k)$. Mit $x_i \in U_{n_i}$ $(1 \le i \le k)$ und $N = \max_{1\le i\le k} n_i$ gilt $U \subseteq U_N$, d.h. $U_N = U_{N+1} = \dots$

ii' $\Rightarrow$ **iii'** Wäre $\mathfrak{U} \neq \varnothing$, etwa $U_0 \in \mathfrak{U}$, so gäbe es ein $U_1 \in \mathfrak{U}$ mit $U_0 \subsetneq U_1$. Zu $U_1 \in \mathfrak{U}$ gäbe es ein $U_2 \in \mathfrak{U}$ mit $U_1 \subsetneq U_2$ und so weiter. Wir erhielten eine Folge $U_0 \subsetneq U_1 \subsetneq U_2 \subsetneq \dots$, was nach ii') unmöglich ist.

iii $\Rightarrow$ **i** Es sei U ein Untermodul von M. Betrachte $\mathfrak{U} = \{V \subseteq U\colon V \subseteq M \text{ e.e. UM}\}$ (die endlich erzeugten Untermoduln). Wegen $\{0\} \in \mathfrak{U}$ hat $\mathfrak{U}$ nach iii) ein maximales Element V_0. In $V_0 \subseteq U$ gilt „=“, denn ist $x \in U$, so ist $V_0 \subseteq V_0 + (x) \in \mathfrak{U}$, also $V_0 = V_0 + (x)$, d.h. $x \in V_0$. Also ist $U = V_0$ endlich erzeugt und somit M noethersch. □

Lemma. *Es sei U ein Untermodul des R-Moduls M.*

a) Aus $M = (x_1, \dots, x_k)$ folgt $M/U = (\overline{x_1}, \dots, \overline{x_k})$.

b) Aus $U = (y_1, \dots, y_m)$ und $M/U = (\overline{z_1}, \dots, \overline{z_n})$ folgt $M = (y_1, \dots, y_m, z_1, \dots, z_n)$.

Beweis. a) % b) $x \in M \Rightarrow \overline{x} = \sum_{i=1}^n r_i\overline{z_i} = \sum \overline{r_iz_i} = \overline{\sum r_iz_i} \Leftrightarrow x - \sum r_iz_i \in U \Rightarrow x - \sum_{i=1}^n r_iz_i = \sum_{j=1}^m s_jy_j \Leftrightarrow x = \sum_{i=1}^n r_iz_i + \sum_{j=1}^m s_jy_j$. □

Satz. *Für Untermoduln A, B eines R-Moduls M gilt:*

a) M noethersch $\Longleftrightarrow$ A noethersch und M/A noethersch

b) A und B noethersch $\Longrightarrow$ $A + B$ noethersch

Beweis. b) folgt aus a), denn sei B noethersch und $(A+B)/B \cong A/(A\cap B)$ noethersch als Faktormodul des noetherschen Moduls A, dann folgt mit a), dass $A+B$ noethersch. zu a): „$\Rightarrow$“ A ist noethersch, denn jeder Untermodul von A ist Untermodul von M. M/A ist noethersch, denn jeder Untermodul von M/A ist von der Form U/A für einen Untermodul U von M mit $U \supseteq A$ (verwende Lemma a). „$\Leftarrow$“: Ist U ein Untermodul von M, so ist $U \cap A$ endlich erzeugt (A ist noethersch) und $U/(U\cap A) \cong (U+A)/A$ endlich erzeugt (M/A noethersch), also U endlich erzeugt (Lemma b). □

Folgerung. ${}_RR$ noethersch und ${}_RM$ endlich erzeugt $\Longrightarrow$ ${}_RM$ noethersch.

Beweis. Es sei $M = Rx_1 + \cdots + Rx_n$. Für $1 \leq i \leq n$ ist $f\colon R \to Rx_i, r \mapsto rx_i$ ein Modulepimorphismus, also $R/\operatorname{Ker}(f) \cong Rx_i$ und damit Rx_i noethersch (R noethersch $\overset{\text{Satz a)}}{\Longrightarrow} R/\operatorname{Ker}(f)$ noethersch). Es folgt $M = Rx_1 + \cdots + Rx_n$ noethersch (Satz b, Induktion nach n). □

Satz. *Für jeden Ring R und jedes $k \geq 1$ sind äquivalent:*

i) Jedes Linksideal von R wird von k Elementen erzeugt.

ii) Wird ein R-Modul M von m Elementen erzeugt, so wird jeder Untermodul U von M von km Elementen erzeugt.

Beweis. **ii** ⇒ **i** $M = R \Rightarrow m = 1 \Rightarrow km = k$.

i ⇒ **ii** Induktion nach m. $m = 1$: $M = Rx$, also $M \cong R/\operatorname{Ker}(f)$ mit $f\colon R \to Rx, r \mapsto rx$ (verwende Lemma a). $m > 1$: Ist $M = (x_1, \ldots, x_m)$, so setze $V = (x_1, \ldots, x_{m-1})$. Dann $M/V = (\overline{x_m})$. Nach Fall $m = 1$ wird $U/(U \cap V) \cong (U+V)/V$ als Untermodul von M/V von $k \cdot 1 = k$ Elementen erzeugt. Nach Induktionsvoraussetzung wird $U \cap V \subseteq V$ von $k(m-1)$ Elementen erzeugt. mit Lemma b) wird U von $k + k(m-1) = km$ Elementen erzeugt □

Beispiel. Ist R ein Hauptidealring, dann $k = 1$, also $km = m$. Ist $R = \mathbb{Z}$: G ist eine abelsche Gruppe, durch m Elemente erzeugt ⇒ jede Untergruppe von G wird durch m Elemente erzeugt.

Satz (Hilbertscher Basissatz)**.** *Es sei R ein kommutativer Ring. Ist R noethersch, so ist $R[X]$ noethersch.*

Beweis. Für $f \in \sum_{i=0}^{n} a_i X^i \in R[X]$ bezeichnen wir mit $l(f)$ den Leitkoeffizienten a_n von f ($a_n \neq 0$). Es sei J ein Ideal von $R[X]$. Für $n \geq 0$ ist $I_n = \{l(f)\colon f \in J \wedge \deg(f) \leq n\}$ ein Ideal von R (!). Es gilt $J \cap R = I_0 \subseteq I_1 \subseteq I_2 \subseteq \ldots$, speziell ist $I = \bigcup_{n \geq 0} I_n$ ein Ideal von R (!). Nach Voraussetzung ist I endlich erzeugt und jedes I_n ist endlich erzeugt. Nehme $F \subseteq J$ mit F endlich und $I = (\{l(f)\colon f \in F\})$. Setze $N = \max\{\deg(f)\colon f \in F\}$. Für $0 \leq n \leq N-1$ nehme $F_n \subseteq J$ mit F_n endlich und $I_n = (\{l(f)\colon f \in F_n\})$, sowie $\deg(f) \leq n$ für alle $f \in F_n$. Wir zeigen im folgenden: $J = (F \cup \bigcup_{n=0}^{N-1} F_n)$. Darin ist „$\supseteq$“ klar wegen $F \subseteq J$, $F_n \subseteq J$. Zu „$\subseteq$“ Für $h \in J$ zeigen wir $h \in (F \cup \bigcup_{n=0}^{N-1} F_n)$ durch Induktion nach $n = \deg(h)$. Für $n \geq N$: $l(h) = \sum_{f \in F} r_f l(f)$, also $\deg\left(h - \sum_{f \in F} r_f X^{n-\deg(f)} f\right) < n$. Für $0 \leq n \leq N-1$: $l(h) = \sum_{f \in F_n} r_f l(f)$, also $\deg\left(h - \sum_{f \in F_n} r_f X^{n-\deg(f)} f\right) < n$. Für $n < 0$: $h = 0$. □

Definition. Es sei R ein kommutativer Ring. Für $n \in \mathbb{N}$ definiert man rekursiv den Polynomring $R[X_1, \ldots, X_n]$ in n Unbestimmten $X_1, \ldots, X_n$ wie folgt: Für $n = 0$: $R[\,,\,] = R$ und für $n > 0$: $R[X_1, \ldots, X_{n-1}][X]$, $X_n = X$. Zum Beispiel $R[X_1, X_2] = R[X_1][X_2]$.

Korollar. *Ist R kommutativ und noethersch, dann ist $R[X_1, \ldots, X_n]$ kommutativ und noethersch. ($n \in \mathbb{N}$). Speziell: Ist K ein Körper, dann ist $K[X_1, \ldots, X_n]$ noethersch.*

Definition. Eine Relation $\leq$ zwischen den Elementen einer Menge Ω heißt *partielle Ordnung*, wenn für alle $\alpha, \beta, \gamma \in \Omega$ gilt:

1) $\alpha \leq \alpha$ (Reflexivität)

2) $\alpha \leq \beta \wedge \beta \leq \gamma \Longrightarrow \alpha \leq \gamma$ (Transitivität)

3) $\alpha \leq \beta \wedge \beta \leq \alpha \Longrightarrow \alpha = \beta$ (Antisymmetrie)

Eine partielle Ordnung heißt *totale Ordnung*, wenn zusätzlich gilt:

4) Für $\alpha, \beta \in \Omega$ ist $\alpha \leq \beta$ oder $\beta \leq \alpha$.

Beispiel. Auf $\Omega \subseteq \mathcal{P}(S)$ ist $\subseteq$ eine partielle Ordnung (S Menge).

Definition. Sei $(\Omega, \leq)$ eine partiell geordnete Menge. Eine *Kette* in Ω ist eine total geordnete Teilmenge $T \subseteq \Omega$ mit $T \neq \varnothing$. Man nennt Ω *induktiv geordnet*, wenn $\Omega \neq \varnothing$ und jede Kette T in Ω eine *obere Schranke* in Ω hat, das ist ein $y \in \Omega$ mit $x \leq y$ für alle $x \in T$. Ein $x \in \Omega$ heißt *maximales Element* von Ω, wenn für alle $y \in \Omega$ aus $x \leq y$ schon $x = y$ folgt. Ein *größtes Element* von Ω ist ein $z \in \Omega$ mit $x \leq z$ für alle $x \in \Omega$. Jedes größte Element ist maximal, aber im allgemeinen nicht umgekehrt, zum Beispiel hat $\mathcal{P}(\{1,2\}) \setminus \{1,2\}$ mit $\subseteq$ zwei maximale Elemente, nämlich $\{1\}, \{2\}$, aber kein größtes Element.

Zornsches Lemma. *Jede induktiv geordnete Menge Ω hat ein maximales Element. Dies ist ein Äquivalent des Auswahlaxioms der Mengenlehre.*

Definition. Revision: Eine Gruppe G heißt *p-Gruppe*, wenn es zu jedem $x \in G$ ein $k \geq 1$ gibt mit $\operatorname{ord}(x) = p^k$. Dabei ist p eine Primzahl.

Satz (ZL). *Jede p-Untergruppe H einer beliebigen Gruppe G liegt in einer maximalen p-Untergruppe von G.*

Beweis. $\Omega = \{U \subseteq G\colon U$ p-Untergruppe von G mit $U \supseteq H\}$ mit $\subseteq$ ist induktiv geordnet, denn wegen $H \in \Omega$ ist $\Omega \neq \varnothing$, und für jede Kette T in Ω gehört $V = \bigcup T$ zu Ω (!), dieses V ist natürlich eine obere Schranke von T. Zu (!): a) V ist eine Untergruppe von G, denn: wegen $T \neq \varnothing$, etwa $U \in T$, ist $e \in U$ und damit $e \in V$. Für $x, y \in V$, etwa $x \in U \in T$, $y \in W \in T$, so sind U, W vergleichbar (da T Kette), etwa $U \subseteq W$, also $x, y \in W$ und damit $xy \in W$, also $xy \in V$. Für $x \in V$, etwa $x \in U \in T$, ist $x^{-1} \in U$, also $x^{-1} \in V$. b) V ist eine p-Gruppe: für $x \in V$, etwa $x \in U \in T$, ist $U \in \Omega$, also U eine p-Gruppe und damit $\operatorname{ord}(x) = p^k$ für ein $k \geq 1$. c) $V \supseteq H$, denn mit $T \neq \varnothing$, etwa $U \in T$, ist $V \supseteq U \supseteq H$. Nach dem Zornschen Lemma hat Ω ein maximales Element, dies ist eine maximale p-Untergruppe von G, die H umfasst. □

Definition. Es sei M ein R-Modul. Eine Teilmenge S von M heißt *linear unabhängig*, wenn für paarweise verschiedene $s_1, \ldots, s_n \in S$ gilt: Sind $r_1, \ldots, r_n \in R$ mit $\sum_{i=1}^{n} r_i s_i = 0$, so gilt $r_1 = r_2 = \cdots = r_n = 0$, dabei $n \in \mathbb{N}$. Zum Beispiel ist $\varnothing$ linear unabhängig, da nur $n = 0$ möglich ist. Eine *Basis* von M ist ein linear unabhängiges $S \subseteq M$ mit $(S) = M$. Hat M eine Basis, so heißt M ein *freier R-Modul*.

Beispiel. Es sei R ein Ring $\neq \{0\}$.

1) $M = R^n$ ist ein freier R-Modul mit Basis $\{e_1, \dots, e_n\}$ mit $e_i = (0, \dots, 0, 1, 0, \dots, 0)$.

2) $R[X]$ ist ein freier R-Modul mit Basis $\{1, X, X^2, X^3, \dots\}$.

3) Ist R kommutativ, $g \in R[X]$ unitär und $\deg(g) = n \geq 0$, dann ist $R[X]/(g)$ ein freier R-Modul mit Basis $\{\overline{1}, \overline{X}, \overline{X}^2, \dots, \overline{X}^{n-1}\}$.

Satz (ZL). *Jede linear unabhängige Teilmenge S eines R-Moduls M liegt in einer maximalen linear unabhängigen Teilmenge von M.*

Beweis. $\Omega = \{U \subseteq M : U \text{ linear unabhängig}, U \supseteq S\}$ mit $\subseteq$ ist induktiv geordnet, denn wegen $S \in \Omega$ ist $\Omega \neq \varnothing$, und für jede Kette T in Ω gehört $\bigcup T$ zu Ω (!) und ist obere Schranke von T. Gemäß ZL hat Ω ein maximales Element U_0, das heißt eine maximale linear unabhängige Teilmenge von M mit $U_0 \supseteq S$. Noch zu (!): $\bigcup T$ ist linear unabhängig, denn ist $\sum_{i=1}^n r_i x_i = 0$ mit $r_1, \dots, r_n \in R$ und $x_1, \dots, x_n \in \bigcup T$ paarweise verschieden, also $x_i \in U_i \in T$ für $1 \leq i \leq n$, so gibt es $i_0 \in \{1, \dots, n\}$ mit $U_i \subseteq U_{i_0}$ für $1 \leq i \leq n$, also $x_1, \dots, x_n \in U_{i_0}$, woraus $r_1 = r_2 = \dots = r_n$ folgt, da U_{i_0} linear unabhängig ist. Und es gilt $\bigcup T \supseteq S$ [wie bei p-Untergruppen, Satz vorher]. □

Korollar (ZL). *Sei K ein Körper. Jeder K-Vektorraum hat eine Basis.*

Beweis. Nach Satz hat V eine maximale linear unabhängige Teilmenge T (mit $T \supseteq \varnothing$). Dafür gilt $(T) = V$, denn: Wäre $(T) \neq V$, etwa $x \in V \setminus (T)$, so wäre $T \sqcup \{x\}$ linear unabhängig [aus $\sum_{i=1}^n r_i x_i + rx = 0$ mit $r_1, \dots, r_n, r \in K$ und $x_1, \dots, x_n \in T$ folgt $r = 0$, denn für $r \neq 0$ wäre $x = -r^{-1} \sum_{i=1}^n r_i x_i \in (T)$, was unmöglich ist, und dann $\sum_{i=1}^n r_i x_i = 0$, also $r_1, \dots, r_n = 0$], aber T ist eine maximale linear unabhängige Teilmenge, also $T = T \sqcup \{x\}$, was wegen $x \notin T$ unmöglich ist. □

Definition. Ein *maximaler Untermodul* eines R-Moduls M ist ein Untermodul U von M mit $U \neq M$, so dass für alle Untermoduln V von M mit $V \neq M$ gilt: aus $U \subseteq V$ folgt $U = V$.

Satz (ZL). *Ist der R-Modul M endlich erzeugt, so liegt jeder Untermodul H von M mit mit $H \neq M$ in einem maximalen Untermodul von M.*

Beweis. $\Omega = \{U \subseteq M : U \text{ Untermodul}, H \subseteq U \neq M\}$ mit $\subseteq$ ist induktiv geordnet, denn wegen $H \in \Omega$ ist $\Omega \neq \varnothing$, und für jede Kette T in Ω gehört $\bigcup T$ zu Ω (!) und ist obere Schranke von T. Gemäß ZL hat Ω ein maximales Element U_0, das ist ein maximaler Untermodul von M mit $U_0 \supseteq H$. Noch zu (!): Da T eine Kette ist, gilt wie für die p-Untergruppen (vorvoriger Satz): $\bigcup T$ ist ein Untermodul mit $\bigcup T \supseteq H$. Zu zeigen bleibt: $\bigcup T \neq M$. Dazu sei $M = (x_1, \dots, x_n)$. Wäre $\bigcup T = M$, das heißt $x_1, \dots, x_n \in \bigcup T$, etwa $x_i \in U_i \in T$ für $1 \leq i \leq n$, so gäbe es — da T eine Kette ist — ein $i_0 \in \{1, \dots, n\}$ mit $U_i \subseteq U_{i_0}$ für $1 \leq i \leq n$, also $x_1, \dots, x_n \in U_{i_0}$ und damit $U_{i_0} = M$, was wegen $U_{i_0} \in \Omega$ unmöglich ist. □

Bemerkung. ZL ist unnötig, wenn ${}_R M$ noethersch ist, zum Beispiel wenn M endlich erzeugt und ${}_R R$ noethersch ist.

Definition. Sei R ein kommutativer Ring. Einen maximalen Untermodul von R nennt man auch *maximales Ideal* von R, das ist ein Ideal I von R mit $I \neq R$, so dass für alle Ideale J von R gilt: aus $I \subsetneq J$ folgt $J = R$.

Korollar (ZL). *Jedes Ideal $\neq R$ eines kommutativen Ringes R liegt in einem maximalen Ideal von R. [R ist endlich erzeugt, etwa $R = (1)$] Speziell: Jeder kommutative Ring R mit $1 \neq 0$ hat ein maximales Ideal. [nach Korollar für Ideal (0) und $1 \neq 0 \Leftrightarrow (0) \neq R$]*

Bemerkung. Falls R noethersch ist, so ist ZL nicht erforderlich.

Definition. Ein Ideal P eines kommutativen Rings R heißt *Primideal*, wenn $P \neq R$ ist und wenn für alle $a, b \in R$ gilt: aus $ab \in P$ folgt $a \in P$ oder $b \in P$.

Satz. *Es sei I ein Ideal des kommutativen Rings R.*

a) I ist ein maximales Ideal von R genau dann, wenn R/I ein Körper ist.

b) I ist ein Primideal von R genau dann, wenn R/I ein Integritätsring ist.

Beweis. $I \neq R \Leftrightarrow 1 \notin I \Leftrightarrow \overline{1} \neq \overline{0}$ in R/I.

a) „$\Rightarrow$“ Ist $r \in R$ mit $\overline{r} \neq \overline{0}$ in R/I, d.h. $r \notin I$, so ist $I \subsetneq I+(r)$, also nach Voraussetzung $I + (r) = R$, d.h. $1 = x + rs$ mit $x \in I$, $s \in R$, wofür $\overline{1} = \overline{x} + \overline{rs} = \overline{0} + \overline{rs} = \overline{r}\,\overline{s}$ in R/I, also $\overline{r} \in (R/I)^\times$.

„$\Leftarrow$“ Ist J ein Ideal von R mit $I \subsetneq J$, etwa $y \in J \setminus I$, so ist $\overline{y} \neq \overline{0}$ in R/I, also nach Voraussetzung $\overline{y} \in (R/I)^\times$, etwa $\overline{1} = \overline{y}\,\overline{z}$ für einen $z \in R$, wofür $1 - yz \in I \subseteq J$, also $1 \in J$, d.h. $J = R$.

b) $\forall a, b \in R$: $(ab \in I \Rightarrow a \in I \vee b \in I)$ ist äquivalent zu $\forall a, b \in R (\overline{a}\,\overline{b} = 0 \Rightarrow \overline{a} = 0 \vee \overline{b} = 0)$ in R/I. □

Korollar. *Jedes maximale Ideal ist ein Primideal.*

Bemerkung. Ein kommutativer Ring ist genau dann ein Integritätsring, wenn (0) ein Primideal ist.

Beispiel.

1) Die Primideale von $\mathbb{Z}$ sind (0) und alle (p) mit p Primzahl.

2) Für jeden kommutativen Ring R und $r \in R$ ist $(X - r)$ genau dann ein Primideal bzw. ein maximales Ideal von $R[X]$, wenn R ein Integritätsring bzw. ein Körper ist.

Beweis.

1) $\mathbb{Z}$ Integritätsring $\Longrightarrow$ (0) Primideal. Ist p eine Primzahl und $(p) \subsetneq (n)$ mit $n \geq 1$, so ist $n \mid p$, also $n = 1$, d.h. $(n) = \mathbb{Z}$, oder $n = p$, was unmöglich ist. Es ergibt sich sogar: (p) ist ein maximales Ideal.

2) Die Auswertungsabbildung $\varepsilon_r\colon R[X] \to R, f \mapsto f(r)$ ist ein surjektiver Ringhomomorphismus mit $\mathrm{Ker}(\varepsilon_r) = (X - r)$ [Division mit Rest], also $R[X]/(X - r) \cong R$. Andersherum: Ist (n) ein Primideal $\neq (0)$, so ist n eine Primzahl, denn: o.B.d.A. ist $n \geq 2$. Aus $k \mid n$ mit $k \geq 1$, also $kl = n$ folgt — da (n) ein Primideal ist —, dass $k \in (n)$ oder $l \in (n)$. Fall $k \in (n)$: Hier ist $k = k'n$, also $k'l = 1$, d.h. $k' = l = 1$, also $k = n$. Fall $l \in (n)$: Hier ist $l = l'n$, also $kl' = 1$, d.h. $k = l' = 1$, speziell $k = 1$. □

Bemerkung. Es seien P, Q Primideale und I ein beliebiges Ideal des kommutativen Rings R. Sind Q, I Hauptideale und gilt $P \subsetneq Q \subsetneq I$, so ist $I = R$.

Beweis. Mit $Q = (a)$, $I = (b)$ ist $a \in I$, d.h. $a = bx$ und $b \notin Q$, also $x \in Q$, d.h. $x = ay$. Es folgt $a(1 - by) = 0 \in P$, und mit $a \notin P$ ist $1 - by \in P \subseteq I$, woraus $1 \in I$ folgt, da $b \in I$. □

Folgerung. In einem Hauptidealring ist jedes Primideal ungleich 0 bereits ein maximales Ideal.

Beweis. Ist $(0) \subsetneq Q \subsetneq I$ mit Q Primideal, so ist $I = R$ nach Bemerkung, also Q maximales Ideal. □

Folgerung. Ist R ein Integritätsring, so ist kein Ideal I von $R[X]$ mit $(X) \subsetneq I \subsetneq R[X]$ ein Hauptideal.

Beweis. (0) und nach Beispiel 2 ist auch (X) ein Primideal. Wende die Bemerkung an auf $(0) \subsetneq (X) \subsetneq I \subsetneq R[X]$. □

Definition. Sind M, N R-Moduln, R ein Ring, so wird $M \times N = \{(x, y)\colon x \in M, y \in N\}$ zu einem R-Modul, wenn man $(x, y) + (x', y') = (x + x', y + y')$ und $r(x, y) = (rx, ry)$ definiert, sowie $0 = (0, 0)$ setzt. Man nennt dies das *direkte Produkt von Moduln.*

2.2.1 Exkurs: Noethersche Induktion

Definition. Es sei Γ eine Menge von Untermoduln eines R-Moduls M, wobei R ein Ring ist. Eine Teilmenge A von Γ heißt *hereditär* (oft auch *progressiv*), wenn für jedes $U \in \Gamma$ gilt: Ist $V \in A$ für jedes $V \in \Gamma$ mit $U \subsetneq V$, so ist $U \in A$.

Satz. *Für jede Menge* Γ *wie oben sind äquivalent:*

i) Aufsteigende Kettenbedingung *für* Γ*: Jede aufsteigende Folge* $U_0 \subseteq U_1 \subseteq U_2 \subseteq \ldots$ *von Elementen von* Γ *wird stationär.*

ii) Jedes $B \subseteq \Gamma$ *mit* $B \neq \varnothing$ *hat ein maximales Element.*

iii) Noethersche Induktion (NI) *für* Γ*: Für jedes hereditäre* $A \subseteq \Gamma$ *ist* $A = \Gamma$.

Beweis. **i) ⇔ ii)** wie für $\Gamma = \{$alle Untermoduln von $M\}$.

ii) ⇔ iii) Für $\Gamma = A \sqcup B$ gilt: $A = \Gamma \Leftrightarrow B = \varnothing$. Dann ist A hereditär genau dann, wenn B kein maximales Element hat. Verwende ii'): Hat $B \subseteq \Gamma$ kein maximales Element, so ist $B = \varnothing$. □

Korollar. *In einem* noetherschen *R-Modul M gilt NI für* jede *Menge Γ von Untermoduln von M.*

2.3 Faktorielle Ringe

Definition. Zu jedem Integritätsring R konstruiert man den *Quotientenkörper* $Q(R) = K$ wie folgt: Mit $S = R \setminus \{0\}$ wird auf $R \times S$ durch $(x, s) \sim (y, t) \Leftrightarrow xt = ys$ eine Äquivalenzrelation definiert (!). Schreibt man $\frac{x}{s}$ für die Äquivalenzklasse von (x, s) bezüglich $\sim$, und K für die Menge $(R \times S)/\sim$ aller Äquivalenzklassen von $\sim$, so sind

$$+ : K \times K \to K, \frac{x}{s} + \frac{y}{t} = \frac{xt + ys}{st}$$
$$\bullet : K \times K \to K, \frac{x}{s} \bullet \frac{y}{t} = \frac{xy}{st}$$

wohldefiniert (!) und machen K zu einem kommutativen Ring mit Eins $\frac{1}{1}$ und Null $\frac{0}{1}$. Wegen $1 \neq 0$ in R ist $1 \neq 0$ in K, d.h. $\frac{1}{1} \neq \frac{0}{1}$ [$(1, 1) \not\sim (0, 1)$, weil $1 \cdot 1 \neq 0 \cdot 1$, wegen $1 \neq 0$ in R.] Es ist $\frac{x}{s} = \frac{y}{t} \Leftrightarrow xt = ys$, speziell $\frac{x}{s} = 0 \Leftrightarrow x = 0$. Für $\frac{x}{s} \in K$ mit $\frac{x}{s} \neq 0$, d.h. $x \neq 0$, d.h. $x \in S$ ist $\frac{x}{s} \cdot \frac{s}{x} = 1$, also $\frac{x}{s} \in K^\times$ mit $\left(\frac{x}{s}\right)^{-1} = \frac{s}{x}$. Insgesamt: K ist ein Körper. Ferner ist $R \to K, x \mapsto \frac{x}{1}$ ein injektiver Ringhomomorphismus. Identifiziert man jedes $x \in R$ mit $\frac{x}{1} \in K$, so wird R zu einem Unterring von K.

Beispiel.

1) $Q(\mathbb{Z}) = \mathbb{Q}$

2) Für jeden Körper k heißt $k(X) = Q(k[X])$ der *Körper der rationalen Funktionen* in der *Variablen X* mit *Koeffizienten* aus k.

Definition. Wieder sei R ein Integritätsring. Man sagt, dass $x \in R$ ein *Teiler* von $y \in R$ (oder y ein *Vielfaches* von x) ist, in Zeichen $x \mid y$, wenn es ein $z \in R$ gibt mit $xz = y$. Gilt $x \mid y$ und $y \mid x$, d.h. es gibt $z \in R^\times$ mit $xz = y$, so heißen x und y *assoziiert*, in Zeichen $x \sim y$. Es gilt: $x \mid y \Leftrightarrow (x) \supseteq (y)$ und $x \sim y \Leftrightarrow (x) = (y)$. Ein $x \in R$ mit $x \neq 0$ und $x \notin R^\times$ heißt

- *Primelement* von R, wenn für alle $a, b \in R$ aus $x \mid ab$ folgt $x \mid a$ oder $x \mid b$.
- *irreduzibel* in R, wenn für alle $a, b \in R$ aus $x = ab$ folgt $a \in R^\times$ oder $b \in R^\times$ (also $x \sim b$ bzw. $x \sim a$).

Bemerkung. Jedes Primelement ist irreduzibel.

Beweis. $x \in R$, $0 \neq x \notin R^\times$, x Primelement, $x = ab$, so ist $x \mid ab$, also $x \mid a$ oder $x \mid b$, d.h. $xc = a$ bzw. $xd = b$, also $x = xcb$ bzw. $x = xda$ und damit $1 = cb$ bzw. $1 = da$, d.h. $b \in R^\times$ bzw. $a \in R^\times$. □

Bemerkung. Für jedes $x \in R$ gilt

a) x Primelement $\Leftrightarrow (x) \neq (0) \wedge (x)$ ist ein Primideal.

b) x irreduzibel $\iff (x) \neq (0)$ und (x) ist maximal unter den Hauptidealen $\neq R$, d.h. $(x) \neq R$ und für $a \in R$ gilt, dass aus $(x) \subsetneq (a)$ folgt $(a) = R$.

Folgerung. Ist R ein Hauptidealring, so ist jedes irreduzible Element von R schon ein Primelement. [Nach Bemerkung b) ist (x) schon ein maximales Ideal]

Beispiel.

0) Die Primelemente von $\mathbb{Z}$ sind genau die Primzahlen p und deren Negative $-p$.

1) Für jeden Körper k ist $R = \{\sum_{i=0}^{n} a_i X^i \in k[X] \colon a_1 = 0\}$ ein Unterring von $k[X]$. Speziell ist R ein Integritätsring und $R^\times = k^\times$. Wegen $\deg(f) \neq 1$ für alle $f \in R$ sind X^2, X^3 in R zwar irreduzibel, jedoch keine Primelemente. [zu X^2, X^3 irreduzibel: aus $fg = X^2$ bzw. $= X^3$ folgt $\deg(f) + \deg(g) = 2$ bzw. $= 3$. Zu X^2, X^3 Primelement: $X^2 \mid X^3X^3$ mit $X^2 \nmid X^3$. $X^3 \mid X^2X^4$ mit $X^3 \nmid X^2$, $X^3 \nmid X^4$]. Insbesondere ist R kein Hauptidealring.

2) $R = \{x + \sqrt{-5}y \in \mathbb{C} \colon x, y \in \mathbb{Z}\}$ ist ein Unterring von $\mathbb{C}$, speziell ist R ein Integritätsring. Für die „*Norm*“ $N \colon R \to \mathbb{N}, x + \sqrt{-5}y \mapsto x^2 + 5y^2$ gilt $N(uv) = N(u)N(v)$ und $N(1) = 1$. Genauer gilt: $N(z) = |z|^2$ für $z \in R$. Für $z \in R$ folgt: $z \in R^\times \Leftrightarrow N(z) = 1 \Leftrightarrow z = \pm 1$. Mit $N(z) \notin \{2, 3\}$ für alle $z \in R$ folgt, dass $2, 3, 1 \pm \sqrt{-5} \in R$ mit den Normen $4, 9, 6$ in R zwar irreduzibel, jedoch keine Primelemente sind: $2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Dieser Ring wird auch mit $\mathbb{Z}[-5]$ bezeichnet.

Bemerkung. Es sei R ein Integritätsring, $x, y \in R \setminus (\{0\} \cup R^\times)$ mit $x \sim y$:

a) $x \left\{\begin{matrix}\text{irreduzibel}\\ \text{Primelement}\end{matrix}\right\} \iff y \left\{\begin{matrix}\text{irreduzibel}\\ \text{Primelement}\end{matrix}\right\}$

b) x ist Produkt von $\left\{\begin{matrix}\text{irreduz. Elem.}\\ \text{Primelementen}\end{matrix}\right\} \iff y$ ist Produkt von $\left\{\begin{matrix}\text{irreduz. Elem.}\\ \text{Primelementen}\end{matrix}\right\}$.

Lemma 1. *Genügt ein Integritätsring R der aufsteigenden Kettenbedingung für Hauptideale, so ist jedes $x \in R \setminus (\{0\} \cup R^\times)$ Produkt von irreduziblen Elementen.*

Beweis. Mit noetherscher Induktion (NI) für $\Gamma = \{(x) \colon x \in R \setminus (\{0\} \cup R^\times)\}$. Zu zeigen: $A = \Gamma$ für $A = \{(x) \in \Gamma \colon x$ Produkt von irreduziblen Elementen$\}$. Gemäß NI reicht es zu zeigen, dass A hereditär ist. Dazu sei $(x) \in \Gamma$, so dass $J \in A$ für alle $J \in \Gamma$ mit $J \supsetneq (x)$. Zu zeigen: $(x) \in A$. Fall 1: x ist irreduzibel. Dann $(x) \in A$. Fall 2: x ist reduzibel, d.h. $x = ab$ mit $a, b \in R \setminus R^\times$, sogar $a, b \neq 0$. Dann: $(x) \subsetneq (a)$ und $(x) \subsetneq (b)$, da $a, b \notin R^\times$, also $(a), (b) \in A$ (Induktion) und damit $(x) = (ab) \in A$. □

Folgerung. In einem noetherschen Integritätsring R ist jedes $x \in R \setminus (\{0\} \cup R^\times)$ Produkt von irreduziblen Elementen.

Bemerkung. Ist R ein Integritätsring, $p \in R \setminus R^\times$ und $q \in R$ irreduzibel, so folgt $p \sim q$ schon aus $p \mid q$. [$pr = q \overset{q \text{ irred.}}{\Longrightarrow} r \in R^\times$ oder $p \in R^\times$]

Lemma 2. *Es sei R ein Integritätsring und $x \in R$. Hat x zwei Primfaktorzerlegungen $x = p_1 \cdots p_n$ und $x = q_1 \cdots q_m$ (d.h. p_i, q_j Primelemente), so ist $n = m$ und es gibt $\sigma \in S_n$ mit $p_{\sigma(i)} \sim q_i$ für $1 \leq i \leq n$.*

Beweis. Induktion nach n. $n = 1$: aus $p_1 = x = q_1 \cdots q_m$ folgt $m = 1$, $p_1 = q_1$ [p_1 irreduzibel]. $n > 1$: aus $p_n \mid q_1 \cdots q_m$ folgt etwa $p_n \mid q_m$, also $p_n \sim q_m$ nach Bemerkung, d.h. $rp_n = q_m$ mit $r \in R^\times$, und damit $p_1 \cdots p_{n-1} = q_1 \cdots (q_{m-1}r)$ also nach Induktion $n - 1 = m - 1$ und es gibt $\sigma' \in S_{n-1}$ mit $p_{\sigma'(i)} \sim q_i$ für $1 \leq i \leq n-1$. Es folgt $n = m$. Man setze σ' fort zu $\sigma \in S_n$ mit $\sigma(n) = n$. □

Beispiel. In $R = \{\sum_{i=0}^{n} a_i X^i \colon a_1 = 0\} \subseteq k[X]$ mit k Körper gilt $X^6 = X^2 \cdot X^2 \cdot X^2$, $X^6 = X^3 \cdot X^3$ mit X^2, X^3 irreduzibel. Eine Zerlegung in *irreduzible* Faktoren ist also im allgemeinen nicht eindeutig.

Lemma 3. *Es sei R ein Integritätsring und $x \in R$. Ist $x = p_1^{k_1} \cdots p_n^{k_n}$ mit $k_1, \cdots, k_n \geq 1$ und paarweise nicht assoziierten Primelementen $p_1, \ldots, p_n$, so hat jeder Teiler y von x die Form $y = u \cdot p_1^{b_1} \cdots p_n^{b_n}$ mit $u \in R^\times$, $0 \leq b_i \leq k_i$.*

Beweis. Es sei $ry = x$. Man hat $r = r'p_1^{a_1}$, $y = y'p_1^{b_1}$ mit $a_1 + b_1 = k_1$. Induktion nach n. $n = 1$: $r'y'p_1^{k_1} = ry = x = p_1^{k_1} \Rightarrow r'y' = 1$, speziell $y' \in R^\times$. $n > 1$: $r'y'p_1^{k_1} = ry = x = p_1^{k_1} \cdots p_n^{k_n} \Rightarrow r'y' = p_2^{k_2} \cdots p_n^{k_n} \Rightarrow y' = up_2^{b_2} \cdots p_n^{b_n}$ mit $u \in R^\times$, $0 \leq b_i \leq k_i \Rightarrow y = up_1^{b_1}p_2^{b_2} \cdots p_n^{b_n}$. □

Folgerung. Es sei R ein Integritätsring und $x \in R \setminus (\{0\} \cup R^\times)$. Hat x eine Primfaktorzerlegung, so gibt es nur endlich viele Ideale $(y) \subseteq R$ mit $(x) \subseteq (y)$, d.h. $y \mid x$. Speziell wird jede Folge $(x) \subseteq (x_1) \subseteq (x_2) \subseteq \ldots$ stationär.

Lemma 4. *Es sei R ein Integritätsring. Haben $x, y \in R \setminus (\{0\} \cup R^\times)$ beide eine Primfaktorzerlegung, so ist $(x) \cap (y)$ ein Hauptideal. Genauer gilt: Ist $x = p_1^{k_1} \cdots p_n^{k_n}$, $y = p_1^{l_1} \cdots p_n^{l_n}$ mit $k_1, l_i \geq 0$ und $n \geq 1$, sowie $p_1, \cdots, p_n$ paarweise nicht assoziierte Primelemente, so gilt $(x) \cap (y) \overset{(*)}{=} (z)$ mit $z = p_1^{m_1} \cdots p_n^{m_n}$ wobei $m_i = \max\{k_i, l_i\}$.*

Beweis von $(*)$. „$\supseteq$“ % „$\subseteq$“: Es sei $a \in (x) \cap (y)$, d.h. $a = rx$ und $a = sy$. Aus $rp_1^{k_1} \cdots p_n^{k_n} = a = sp_1^{l_1} \cdots p_n^{l_n}$ folgt $a = r_1 p_1^{m_1} p_2^{k_2} \cdots p_n^{k_n}$ für geeignetes $r_1 \in R$. [Fall $k_1 \geq l_1$, d.h. $m_1 = k_1$: Setze $r_1 = r$. Fall $k_1 < l_1$, d.h. $m_1 = l_1$: Durch Kürzen von $p_1^{k_1}$ erhält man $p_1^{l_1 - k_1} \mid rp_2^{k_2} \cdots p_n^{k_n}$, also $p_1^{l_1-k_1} \mid r$, d.h. $r_1 p_1^{l_1-k_1} = r$ für ein $r_1 \in R$] Ebenso erhält man $a = r_2 p_1^{m_1} p_2^{m_2} p_3^{k_3} \cdots p_n^{k_n}$ usw., bis man bei $a = r_n z$ angelangt ist. □

Definition. Ein Integritätsring R heißt *faktoriell*, wenn jedes $x \in R \setminus (\{0\} \cup R^\times)$ eine Primfaktorzerlegung hat.

Satz. *Für jeden Integritätsring R sind äquivalent:*

i) R ist faktoriell.

ii) Jedes $x \in R \setminus (\{0\} \cup R^\times)$ ist Produkt von irreduziblen Elementen und jedes irreduzible Element von R ist schon ein Primelement.

iii) *R genügt der aufsteigenden Kettenbedingung für Hauptideale, und der Durchschnitt zweier Hauptideale ist wieder ein Hauptideal.*

Beweis. i) $\Leftrightarrow$ ii) % i) $\Rightarrow$ iii) Lemma 4 und Folgerung zu Lemma 3. iii) $\Rightarrow$ ii): „Produkt“ mit Lemma 1. Noch zu „irreduzibel $\Rightarrow$ prim“: Es sei $x \in R$ irreduzibel und $x \mid ab$. Zu zeigen: $x \mid a \vee x \mid b$. Nach Voraussetzung ist $(x) \cap (a) = (c)$, also $xa = rc$, da $xa \in (x) \cap (a)$, und $sx = c = ta$, woraus folgt $xa = rsx$ und $xa = rta$, d.h. $a = rs$ und $x = rt$, da $a \neq 0$. Wegen x irreduzibel ist $r \in R^\times$ oder $t \in R^\times$. Fall $r \in R^\times$: $xa \sim c$, also $(x) \cap (a) = (xa)$: wegen $x \mid ab$ ist $ab \in (x) \cap (a) = (xa)$, also $xa \mid ab$, d.h. $x \mid b$. Fall $t \in R^\times$: $x \sim r$, d.h. $r \mid a \Rightarrow x \mid a$. □

Korollar. *Für jeden noetherschen Integritätsring R sind äquivalent:*

i) *R ist faktoriell.*

ii) *Jedes irreduzible Element von R ist schon ein Primelement.*

iii) *Der Durchschnitt zweier Hauptideale von R ist wieder ein Hauptideal.*

Speziell ist jeder Hauptidealring ein faktorieller Ring, z.B. $k[X]$ (k Körper)

Beweis. Da R noethersch ist, genügt er der aufsteigenden Kettenbedingung (für Hauptideale), weshalb jedes $x \in R \setminus (\{0\} \cup R^\times)$ Produkt von irreduziblen Elementen ist (siehe Lemma 1). Verwende Satz. □

Beispiel.

1) Noethersch (!!), aber nicht faktoriell sind $k[X^2, X^3] = \{\sum_{i=0}^{n} a_i X^i \in k[X] \colon a_1 = 0\} \subseteq k[X]$, k Körper, und $\mathbb{Z}[\sqrt{-5}] = \{x + \sqrt{-5}y \in \mathbb{C} \colon x, y \in \mathbb{Z}\} \subseteq \mathbb{C}$. Beide sind Integritätsringe.

2) $\mathbb{Z}[X]$ ist faktoriell (!!), aber kein Hauptidealring.

Wir werden (!!) jeweils später sehen (vielleicht in der Übung).

Bemerkung. Mit „$\mathbb{Z}$ ist faktoriell“ haben wir den Hauptsatz der elementaren Zahlentheorie gezeigt.

Präzisierung. Hat ein Element x ein Integritätsrings eine *Primfaktorzerlegung*, d.h. $x = q_1 \cdots q_m$ für Primelemente $q_1, \ldots, q_m$ und $m \geq 1$, so kann man erreichen, dass $x = u p_1^{k_1} \cdots p_n^{k_n}$ mit $u \in R^\times$, $n \geq 1$, alle $k_i \geq 1$ und paarweise nicht assoziierten Primelementen $p_1, \ldots, p_n$.

Beweis. Induktion nach m, Übung. □

Beispiel. In $\mathbb{Z}$ ist $-4 = (-1)2^2 = (-1)(-2)^2$.

Definition. Sei R ein Integritätsring. Man nennt $v \in R$ (bzw. $d \in R$) ein *kleinstes gemeinsames Vielfaches* (bzw. einen *größten gemeinsamen Teiler*), kurz kgV (bzw. ggT) von $a_1, \ldots, a_n \in R$, wenn $a_i \mid v$ und aus $a_i \mid v'$ für alle i folgt, dass $v \mid v'$ (bzw. $d \mid a_i$ für alle i und aus $d' \mid a_i$ für alle i folgt $d' \mid d$.

Beobachtung.

a) Ist v ein kgV (bzw. d ein ggT) von $a_1, \ldots, a_n$, so ist w (bzw. e) genau dann auch ein kgV (bzw. ein ggT) von $a_1, \ldots, a_n$, wenn $v \sim w$ (bzw. $d \sim e$) ist.

b) $x \mid y \Longrightarrow y$ ist ein kgV, x ist ein ggT (von x, y). Speziell: 0 ist ein kgV und x ein ggT von $0, x$.

Definition. Man nennt $a_1, \ldots, a_n \in R$ *teilerfremd*, wenn 1 ein ggT von $a_1, \ldots, a_n$ ist, d.h. jede Einheit ist ein ggT von $a_1, \ldots, a_n$.

Bemerkung 1. Ist d ein ggT von $a_1, \ldots, a_n$ und $r \mid a_i$ für alle i mit $r \neq 0$, so ist $\frac{d}{r}$ ein ggT von $\frac{a_1}{r}, \ldots, \frac{a_n}{r}$. [Mit $ra_i' = a_i$ für alle i und $rd' = d$ gilt: $\forall i(x \mid a_i') \Leftrightarrow \forall i(rx \mid a_i) \Leftrightarrow rx \mid d \Leftrightarrow x \mid d'$.] Spezialfall $d = r$: Ist d ein ggT von $a_1, \ldots, a_n$, ein $a_i \neq 0$, d.h. $d \neq 0$, so sind $\frac{a_1}{d}, \ldots, \frac{a_n}{d}$ teilerfremd.

Bemerkung 2.

a) Genau dann ist $v \in R$ ein kgV von $a_1, \ldots, a_n \in R$, wenn $(v) = (a_1) \cap \cdots \cap (a_n)$.

b) Ist $(d) = (a_1, \ldots, a_n)$, so ist d ein ggT von $a_1, \ldots, a_n$.

c) Ist $(a_1, \ldots, a_n)$ ein Hauptideal, so ist $(d) = (a_1, \ldots, a_n)$ genau dann, wenn d ein ggT von $a_1, \ldots, a_n$ ist.

Speziell: Ist R ein Hauptidealring, so haben $a_1, \ldots, a_n \in R$ stets ein kgV und einen ggT.

Beispiel. In $\mathbb{Z}[X]$ sind $2, X$ teilerfremd, aber $(2, X) \neq (1)$. In b) gilt die Umkehrung also im Allgemeinen nicht.

Lemma. *Haben $a, b \neq 0$ ein kgV v, so haben sie auch einen ggT d mit $dv = ab$.*

Beweis. Sei v ein kgV. Wegen $a, b \mid ab$ ist $v \mid ab$, etwa $dv = ab$ für (genau) ein d, welches ein ggT von a, b ist, denn: Wegen $a \mid v$ und $b \mid v$, sowie $dv = ab$ gilt $da \mid ab$ und $db \mid ab$, d.h. $d \mid b$ und $d \mid a$. Aus $d' \mid a$ und $d' \mid b$, etwa $rd' = a$ und $sd' = b$ folgt $sa = rb =: v'$, wofür $a \mid v'$ und $b \mid v'$, also $v \mid v'$, etwa $vt = v'$, also $rd'tb = atb = dvt = dv' = drb$ und damit $d't = d$, also $d' \mid d$. □

Satz. *Es sei R ein faktorieller Ring.*

a) Alle $a_1, \ldots, a_n \in R$ haben ein kgV und einen ggT.

b) Ist $d \in R$ ein ggT von $a_1, \ldots, a_n \in R$ und $r \in R$, so ist rd ein ggT von $ra_1, \ldots, ra_n$.

c) Sind $x, a \in R$ teilerfremd und $x \mid ab$, so ist $x \mid b$.

d) Sind $x, y \in R$ teilerfremd und $x \mid a$ und $y \mid a$, so ist $xy \mid a$.

e) Für $a, b \in R \setminus \{0\}$ mit $a = up_1^{k_1} \cdots p_n^{k_n}$, $b = wp_1^{l_1} \cdots p_n^{l_n}$, $u, w \in R^\times$, $n \geq 1$, alle $k_i, l_i \geq 0$ und $p_1, \ldots, p_n$ paarweise nicht assoziierte Primelemente ist $d = p_1^{\nu_1} \cdots p_n^{\nu_n}$ ein ggT von a, b und $v = p_1^{\mu_1} \cdots p_n^{\mu_n}$ ein kgV von a, b, falls $\nu_i = \min\{k_i, l_i\}$ und $\mu_i = \max\{k_i, l_i\}$ für alle i.

Beweis.

a) Gemäß vorigem Satz ist $(a_1) \cap \cdots \cap (a_n) = (v)$ für ein $v \in R$, was nach Bemerkung 2a) ein kgV ist. Zur Existenz eines ggT: Induktion nach n. $n = 2$: Lemma. $n > 2$: Nach Induktion gibt es einen ggT d' von $a_1, \ldots, a_{n-1}$. Nach Lemma gibt es einen ggT d von d', a_n. Dieses d ist ein ggT von $a_1, \ldots, a_n$.

b) O.B.d.A. $r, d \neq 0$. Nach a) gibt es einen ggT e von $ra_1, \ldots, ra_n$. Wir zeigen $rd \sim e$: Aus $rd \mid ra_i$ für alle i folgt $rd \mid e$, etwa $rds = e$; aus $e \mid ra_i$, also $ds \mid a_i$ für alle i folgt $ds \mid d$, etwa $dst = d$, d.h. $st = 1$, also $s \in R^\times$, also $rd \sim e$.

c) 1 ist ein ggT von $x, a \overset{b)}{\Longrightarrow} b$ ist ein ggT von $bx, ab \overset{x|ab}{\Longrightarrow} x \mid b$.

d) 1 ist ein ggT von $x, y \overset{b)}{\Longrightarrow} a$ ist ein ggT von ax, ay und $x \mid a \wedge y \mid a \Rightarrow xy \mid ay \wedge xy \mid ax$, also $xy \mid a$.

e) Nach Lemma 4 zum vorigen Satz ist $(a) \cap (b) = (v)$, d.h. gemäß Bemerkung 2a): v ist ein kgV von a, b. Nach obigem Lemma ist $\frac{ab}{v}$ ein ggT von a, b. Wir zeigen, dass $\frac{ab}{v} \sim d$. Reicht zu zeigen: $k_i + l_i = \nu_i + \mu_i$ für alle i, denn dann $ab \sim vd$. Aber allgemein gilt: $k + l = \min\{k, l\} + \max\{k, l\}$ für $k, l \in \mathbb{Z}$. □

Korollar. *Es sei R ein faktorieller Ring und $K = Q(R)$ sein Quotientenkörper.*

a) Zu jedem $x \in K$ gibt es teilerfremde $p, q \in R$ mit $q \neq 0$ und $x = \frac{p}{q}$.

b) Ist $x \in K$ Nullstelle eines unitären $f \in R[X]$ mit $\deg(f) \geq 1$, so ist $x \in R$.

Beweis.

a) Es sei d ein ggT von r, s mit $x = \frac{r}{s}$, sowie $dp = r$, $dq = s$. Nach Bemerkung 1 sind p, q teilerfremd, $x = \frac{p}{q}$.

b) Nach a) ist $x = \frac{p}{q}$ mit p, q teilerfremd, $q \neq 0$. Es sei $f = X^n + \sum_{i=0}^{n-1} r_i X^i$ mit $r_i \in R$. Aus $f(x) = 0$ folgt $p^n + r_{n-1}p^{n-1}q + \cdots + r_1 pq^{n-1} + r_0 pq^n = 0$, d.h. $p^n = -q(r_{n-1}p^{n-1} + \cdots + r_1 pq^{n-2} + r_0 q^{n-1})$. Jeder Primteiler von q teilt also p, also hat q keinen Primteiler, d.h. $q \in R^\times$, also $x = pq^{-1} \in R$. □

2.4 Irreduzible Polynome

Konvention. R bezeichne im Folgenden stets einen Integritätsring.

Beispiel. Ist k ein Körper, $f \in k[X]$ irreduzibel, so ist f ein Primelement, sogar (f) ein maximales Ideal, d.h $K = k[X]/(f)$ ein Körper. Ist zudem $\deg(f) = n$, so ist $\overline{1}, \overline{X}, \ldots, \overline{X}^{n-1}$ eine Basis von K als k-Vektorraum. Ist ferner $k = \mathbb{Z}/(p)$ mit einer Primzahl p, so ist $|K| = |k|^n = p^n$. Später: Zu jedem $n \geq 1$ gibt es ein irreduzibles $f \in k[X]$ mit $\deg(f) = n$, je zwei Körper mit p^n Elementen sind isomorph.

Beobachtung. Sei R ein Integritätsring. Für $a, b \in R$ hat $aX + b \in R[X]$ genau dann eine Nullstelle in R, wenn $a \mid b$, zum Beispiel dann, wenn $a \in R^\times$. Die Nullstelle ist eindeutig bestimmt und gleich $-\frac{b}{a}$. In $\mathbb{Z}[X]$ hat $2X + 4$ die Nullstelle -2, aber $2 \notin \mathbb{Z}^\times$.

Bemerkung. Sei R ein Integritätsring, $f \in R[X]$ normiert, $\deg(f) \in \{2, 3\}$. Genau dann ist f (ir)reduzibel, wenn f (k)eine Nullstelle in R hat.

Beweis. Wir zeigen: f ist reduzibel genau dann, wenn f eine Nullstelle hat. „$\Rightarrow$“ $f = gh$ mit $g, h \notin R^\times \Rightarrow \deg(f) = \deg(g) + \deg(h)$ mit $\deg(g), \deg(h) \geq 1 \Rightarrow \deg(g) = 1$ oder $\deg(h) = 1 \Rightarrow g$ oder h hat eine Nullstelle [die Leitkoeffizienten von g, h sind Einheiten, da f normiert ist]. „$\Leftarrow$“ $f(r) = 0, r \in R \Rightarrow f = (X - r)f'$ mit $X - r \notin R[X]^\times = R^\times$ und $\deg(f') \in \{1, 2\}$, also $f' \notin R[X]^\times$. □

Beispiel.

0) $X^4 + 4 \in \mathbb{Z}[X]$ hat keine Nullstelle, ist aber reduzibel, da z.B. $X^4 + 4 = (X^2 - 2X + 2)(X^2 + 2X + 2)$.

1) $X^2 - 2$ ist irreduzibel in $\mathbb{Q}[X]$, aber reduzibel in $\mathbb{R}[X]$

2) $X^2 + 1$ ist irreduzibel in $\mathbb{R}[X]$, aber reduzibel in $\mathbb{C}[X]$

3) Ist A ein Integritätsring und $n \geq 1$ ungerade, so ist $f = X^2 - Y^n \in A[X, Y]$ irreduzibel. Dazu sei $R = A[Y]$, also $f \in R[X]$. Dann $\deg_X(f) = 2$ und f hat keine Nullstelle in R, denn: aus $f(g) = 0$, d.h. $g^2 = Y^n$, $g \in R$ folgt $2 \deg(g) = n$, also n gerade, was ausgeschlossen ist.

Definition. Man nennt $f \in R[X]$ *primitiv*, wenn $f \neq 0$ und die Koeffizienten von f teilerfremd sind, d.h. jeder ihrer gemeinsamen Teiler ist eine Einheit. Dies ist z.B. dann der Fall, wenn ein Koeffizient 1 ist, etwa wenn f unitär ist.

Bemerkung. Jedes nicht konstante irreduzible $f \in R[X]$ ist primitiv. [Teilt $r \in R$ alle Koeffizienten von f, so ist r ein Teiler von f]

Satz (Reduktionskriterium)**.** *Sei R ein Integritätsring, $f \in R[X]$ nichtkonstant und primitiv mit $f = \sum_{i=0}^{n} a_i X^i$. Gibt es ein Primideal P, so dass $a_n \notin P$ und ist die Reduktion $\overline{f}$ von $f \mod P$ irreduzibel ist in $(R/P)[X]$, so ist f irreduzibel in $R[X]$.*

Beweis. Wegen f nicht konstant ist f weder Null noch eine Einheit. Aus $f = gh$ in $R[X]$ folgt $\overline{f} = \overline{g}\,\overline{h}$ in $(R/P)[X]$. Da $\overline{f}$ irreduzibel ist, etwa $\overline{g} \in (R/P)[X]^\times$, insbesondere $\deg(\overline{g}) = 0$, also $\deg(f) \geq \deg(h) \geq \deg(\overline{h}) + \deg(\overline{g}) = \deg(\overline{f}) = \deg(f)$, also $\deg(h) = \deg(f)$, d.h. $\deg(g) = 0$, also $g \in R^\times$, da f primitiv ist. □

Beispiel. $f = X^5 - X^2 + 1$ ist irreduzibel in $\mathbb{Z}[X]$. Dazu: Reduktion modulo (2). In $\mathbb{Z}/(2)$ hat $\overline{f} = X^5 + X^2 + 1$ keine Nullstelle. Als echte Teiler von f kommen also nur die Polynome von Grad 2 oder 3 in Frage, die selber keine Nullstelle haben. Das sind $X^2 + X + 1$, $X^3 + X^2 + 1$, $X^3 + X + 1$, aber daraus kann man f nicht bilden: $(X^2 + X + 1)(X^3 + X^2 + 1) \neq f \neq (X^2 + X + 1)(X^3 + X + 1)$.

Lemma. *Es sei R ein Integritätsring, $f \in R[X]$. Aus $f \mid rX^n$ mit $r \in R \setminus \{0\}$, $n \geq 1$ folgt $f = sX^m$ mit $s \mid r$, $m \leq n$. [$fg = rX^n \Rightarrow f = f'X^a, g = g'X^b$ mit $a + b = n$ $\Rightarrow f'g' = r \Rightarrow f', g' \in R$]*

Satz (Kriterium von Eisenstein)**.** *Es sei R ein Integritätsring, $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ nichtkonstant und primitiv. Hat R ein Primelement p mit $p \nmid a_n, p \mid a_{n-1}, p \mid a_{n-2}, \ldots, p \mid a_1, p \mid a_0, p^2 \nmid a_0$, so ist f in $R[X]$ irreduzibel.*

Beweis. Wieder ist f weder Null noch eine Einheit. Aus $f = gh$ folgt $\overline{f} = \overline{g}\,\overline{h}$ in $(R/(p))[X]$. Nach Voraussetzung ist $\overline{f} = \overline{a_n}X^n$ mit $\overline{a_n} \neq 0$. Gemäß Lemma ist $\overline{g} = \overline{r}X^k$, $\overline{h} = \overline{s}X^l$, $k+l = n$. Wegen $p^2 \nmid a_0$ ist $k = 0$ oder $l = 0$ [aus $k, l \geq 1$ folgt $\overline{g}(0) = 0 = \overline{h}(0)$, d.h. $p \mid g(0)$, $p \mid h(0)$, also $p^2 \mid g(0)h(0) = f(0) = a_0$, ausgeschlossen], etwa $k = 0$, d.h. $\deg(\overline{g}) = 0$, woraus man wie beim Beweis des Reduktionskriteriums auf $g \in R^\times$ schließen kann. □

Beispiel.

1) Hat a einen Primfaktor p mit $p^2 \nmid a$, so ist $X^n - a$ irreduzibel in $\mathbb{Z}[X]$ für alle $n \geq 1$. Z.B. ist $X^2 - p$ irreduzibel in $\mathbb{Z}[X]$ für Primzahlen p.

2) Für jede Primzahl p ist $f = X^{p-1} + X^{p-2} + \cdots + X + 1$ irreduzibel in $\mathbb{Z}[X]$. [Man hat den Ringautomorphismus $\sigma\colon \mathbb{Z}[X] \to \mathbb{Z}[X]$ mit $\sigma(g) = g(X+1)$, $\sigma^{-1}(h) = h(X-1)$. Reicht zu zeigen: $\sigma(f)$ ist irreduzibel in $\mathbb{Z}[X]$. Dazu: $X \cdot \sigma(f) = \sigma(X-1) \cdot \sigma(f) = \sigma((X-1)f) = \sigma(X^p - 1) = (X+1)^p - 1$ und $(X+1)^p = X^p + \binom{p}{1}X^{p-1} + \cdots + \binom{p}{p-1}X + 1$, also $\sigma(f) = X^{p-1} + pX^{p-2} + \binom{p}{2}X^{p-3} + \cdots + \binom{p}{p-2}X + p$. Also erfüllt $\sigma(f)$die Voraussetzungen des Kriteriums von Eisenstein, denn für $1 \leq i \leq p-1$ gilt $p \mid \binom{p}{i}$, da $p! = i!(p-i)!\binom{p}{i}$ und $p \mid p!$, aber $i!(p-i)! \notin (p)$]

3) $n \geq 4$ gerade $\Rightarrow X^{n-1} + X^{n-2} + \cdots + X + 1 \in \mathbb{Z}[X]$ ist reduzibel.

Beobachtung. Sei R faktoriell. Für $a, b \in R \setminus \{0\}$ gilt $a \mid b$ genau dann, wenn jeder Primfaktor (mit Vielfachheit) von a auch Teiler von b ist. Speziell ($b = 1$): $a \in R^\times$ genau dann, wenn a keine Primfaktoren hat. Ferner sind $a_1, \ldots, a_n \in R \setminus \{0\}$ teilerfremd, wenn sie keine gemeinsamen Primfaktoren haben.

Definition. Es sei R ein kommutativer Ring. Für jedes Ideal I von R ist der Ringhomomorphismus $R[X] \to (R/I)[X], f \mapsto \overline{f}$ (mit $\overline{f} = \sum_{i=0}^{n} \overline{a_i}X^i$ für $f = \sum_{i=0}^{n} a_i X^i$) surjektiv und hat den Kern $\{\sum_{i=0}^{n} a_i X^i \colon n \geq 0, a_0, \ldots, a_n \in I\}$. Speziell ist diese Menge ein Ideal, das von I in $R[X]$ erzeugte Ideal, kurz $IR[X]$. Es gilt $R[X]/IR[X] \cong (R/I)[X]$.

Bemerkung. I Primideal von $R \Leftrightarrow IR[X]$ Primideal von $R[X]$. [R/I Integritätsring $\Leftrightarrow$ $(R/I)[X]$ Integritätsring]. Speziell gilt für R Integritätsring und $r \in R$: r Primelement von $R \Leftrightarrow r$ Primelement von $R[X]$. Übrigens gilt auch: r irreduzibel in $R \Leftrightarrow r$ irreduzibel in $R[X]$.

Lemma (Gauß)**.** *Für jeden faktoriellen Ring R gilt: Sind $f, g \in R[X]$ beide primitiv, so ist auch $f \cdot g$ primitiv.*

Beweis. Primitiv heißt, dass die Koeffizienten keinen gemeinsamen Primfaktor haben. Ist also p ein Primfaktor aller Koeffizienten von $f \cdot g$, d.h. $f \cdot g \in (p)R[X]$, also $f \in (p)R[X]$ oder $g \in (p)R[X]$, d.h. p teilt alle Koeffizienten von f bzw. von g. □

Konvention. Im folgenden sei R immer ein faktorieller Ring.

Lemma. *Sei R faktoriell, $K = Q(R)$. Zu jedem $h \in K[X] \setminus \{0\}$ gibt es $u \in K^\times$ mit $uh \in R[X]$ primitiv.*

Beweis. $h = \sum_{i=0}^{n} \frac{r_i}{s} X^i$; $r_n, s \in R \setminus \{0\}$; d ein ggT von $r_0, \ldots, r_n$; $d \neq 0$; $dr_i' = r_i$ $(1 \leq i \leq n) \Rightarrow h' = \sum_{i=0}^{n} r_i' X^i \in R[X]$ primitiv, $dh' = sh$, also $h' = uh$ mit $u = s/d \in K^\times$.] □

Lemma. *Sei R faktoriell, $K = Q(R)$. Ist $f \in R[X]$ primitiv und $h \in K[X]$ mit $f \cdot h \in R[X]$, so ist schon $h \in R[X]$.*

Beweis. O.B.d.A. $h \neq 0$. Nehme $u \in K^\times$ wie im vorigen Lemma mit $h' = uh \in R[X]$ primitiv. Schreibe $u = a/b$. Es gilt $a \mid b$ in R (!), etwa $ac = b$ mit $c \in R$, wofür $u = 1/c$, also $h = \frac{1}{u} h' = ch' \in R[X]$. Noch zu (!): Nach dem Lemma von Gauß ist $fh' \in R[X]$ primitiv. Ist p Primfaktor von a, so teilt p alle Koeffizienten von $afh = bfh'$, also $p \mid b$. □

Folgerung. Ist R faktoriell, $K = Q(R)$ und $f \in R[X] \setminus R$ primitiv, so gilt: f irreduzibel in $R[X] \Leftrightarrow f$ irreduzibel in $K[X]$.

Beweis. $\Leftarrow$ gilt ohnehin. Aus $f \notin R$ folgt $f \notin \{0\} \cup R^\times$. Nun sei $f = gh \in K[X]$. Nehme wie vorletzten Lemma ein $u \in K^\times$ mit $h' = uh$ primitiv, $\in R[X]$. In $f = (\frac{1}{u} g)h'$ ist $\frac{1}{u} g \in R[X]$ gemäß Lemma, also nach Voraussetzung $\frac{1}{u} g \in R^\times$ oder $h' \in R^\times$ und damit $g \in K^\times$ oder $h \in K^\times$. □

Bemerkung. Sei R ein Integritätsring. Genügt R der aufsteigenden Kettenbedingung für Hauptideale, so tut dies auch $R[X]$.

Beweis. Aus $(f_0) \subseteq (f_1) \subseteq \ldots$ in $R[X]$ mit o.B.d.A. $f_0 \neq 0$ folgt $\deg(f_0) \geq \deg(f_1) \geq \ldots$, also gibt es $n \in \mathbb{N}$ mit $\deg(f_n) = \deg(f_{n+1}) = \ldots$. Für $k \geq n$ ist damit $f_k = r_k f_{k+1}$ sogar mit $r_k \in R$, also $c_k = r_k c_{k+1}$ in R für die Leitkoeffizienten c_k der f_k, woraus folgt $(c_n) \subseteq (c_{n+1}) \subseteq \ldots$ und damit nach Voraussetzung $(c_m) = (c_{m+1}) = \ldots$ für ein $m \geq n$, wofür $c_k \sim c_{k+1}$, d.h. $r_k \in R^\times$ für $k \geq m$, also auch $(f_m) = (f_{m+1}) = \ldots$ □

Satz (Gauß)**.** *Ist R faktoriell, so ist auch $R[X]$ faktoriell.*

Beweis. Nach Bemerkung ist jedes $f \in R[X] \setminus (\{0\} \cup R^\times)$ Produkt von irreduziblen Elementen (siehe Lemma am Anfang des Abschnitts über faktorielle Ringe). Noch zu zeigen: Jedes irreduzible $f \in R[X]$ ist schon Primelement. Fall 1: f konstant, d.h. $f = r$, $r \in R$. Ist r irreduzibel in $R[X]$, so ist r irreduzibel in R, also nach Voraussetzung r Primelement von R und damit r Primelement von $R[X]$. [(r) Primideal von $R \Rightarrow (r)$ Primideal von $R[X]$.] Fall 2: f nicht konstant. Nach Folgerung ist f irreduzibel in $K[X]$ mit $K = Q(R)$. Aus $f \mid gh$ in $R[X]$, also $f \mid gh$ auch in $K[X]$, folgt, da f sogar Primelement des Hauptidealrings $K[X]$ ist, dass $f \mid g$ oder $f \mid h$ in $K[X]$, womit nach

Lemma auch $f \mid g$ oder $f \mid h$ in $R[X]$. Beachte, dass f primitiv ist. [Etwa $f \mid g$ in $K[X]$, $fg' = g$, $g' \in K[X]$, $g \in R[X] \underset{\text{Lemma}}{\Longrightarrow} g' \in R[X]$.] □

Beispiel. $\mathbb{Z}[X]$ ist faktoriell, aber kein Hauptidealring.

Korollar. *R faktoriell $\Longrightarrow$ $R[X_1, \ldots, X_n]$ faktoriell, $n \geq 1$. Speziell: k Körper $\Longrightarrow$ $k[X_1, \ldots, X_n]$ faktoriell, $n \geq 1$. Aber: R faktoriell, $n \geq 2 \Longrightarrow R[X_1, \ldots, X_n]$ kein Hauptidealring.*

Beweis. Die ersten beiden Aussagen sind klar. O.b.d.A. $n = 2$, $R[X, Y] = R[X_1, X_2]$. Da (X), (Y) Primideale sind [etwa $R[X, Y]/(Y) \cong R[X]$], sind X, Y Primelemente mit $X \neq Y$, insbesondere sind X, Y teilerfremd (!). Wäre (X, Y) ein Hauptideal, so wäre $(X, Y) = (1)$, d.h. $1 = fX + gY$, also $1 = 0$, was ausgeschlossen ist. □

Bemerkung. Es gilt auch die Umkehrung des Satzes von Gauß. (Übung) Aber $K = Q(R)$, R Integritätsring, dann ist $K[X]$ ein Hauptidealring, aber z.B. $R = \mathbb{Z}[X]$ kein Hauptidealring.

2.5 Ganze und algebraische Elemente

Definition. Es sei $R \subseteq A$ eine *Ringerweiterung*, wenn A ein kommutativer Ring und R ein Unterring ist. Für jedes $S \subseteq A$ heißt $R[S] = \{f(a_1, \ldots, a_n) \colon a_1, \ldots a_n \in S, f \in R[X_1, \ldots, X_n], n \in \mathbb{N}\}$ die *Ringadjunktion* von S an R.

Bemerkung. Es gilt $R[S] = \bigcap\{B \in A \colon B \text{ Unterring von } A \text{ mit } R \cup S \subseteq B\}$, d.h. $R[S]$ ist der kleinste Unterring von A, der $R \cup S$ umfasst. Speziell ist $R[S]$ ein Ring, der natürlich kommutativ ist. Ist $S = \{a_1, \ldots, a_n\}$, so schreibt man $R[a_1, \ldots, a_n]$ anstelle $R[S]$ und $R[a_1, \ldots, a_n] = \{f(a_1, \ldots, a_n) \colon f \in R[X_1, \ldots, X_n]\}$. Speziell $R[a] = \{f(a) \colon f \in R[X]\}$, d.h. $R[a] = \{\sum_{i=0}^{m} r_i a^i \colon r_0, \ldots, r_m \in R, m \in \mathbb{N}\}$. Für den Einsetzungshomomorphismus $\varepsilon \colon R[X_1, \ldots, X_n] \to A, X_i \mapsto a_i$ gilt $\operatorname{Im}(\varepsilon) = R[a_1, \ldots, a_n]$, also $R[X_1, \ldots, X_n]/\operatorname{Ker}(\varepsilon) \cong R[a_1, \ldots, a_n]$. Speziell: R noethersch $\Rightarrow$ $R[a_1, \ldots, a_n]$ noethersch (Hilbertscher Basissatz).

Beispiel.

a) $\mathbb{Z}[\sqrt{d}]$ in $\mathbb{Z} \subseteq \mathbb{C}$ mit $d \in \mathbb{Z}$ (z.B. $\mathbb{Z}[\sqrt{-5}]$) ist noethersch. $\mathbb{Z}[\sqrt{d}] \overset{(!)}{=} \{x + \sqrt{d}y \colon x, y \in \mathbb{Z}\}$.

b) $R[X^2, X^3]$ in $R \subseteq R[X]$ ist noethersch.

Definition. Eine Ringerweiterung $R \subseteq A$ heißt *endlich*, oder kurz A endlich über R, wenn A als R-Modul endlich erzeugt ist, d.h. es gibt $a_1, \ldots, a_n \in A$ mit $Ra_1 + \cdots + Ra_n = A$.

Beispiel.

1) $\mathbb{Z}[\sqrt{d}]$ ist endlich über $\mathbb{Z}$, da $\mathbb{Z}[\sqrt{d}] = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \sqrt{d}$

2) $R[X^2, X^3]$ ist nicht endlich über $R \neq \{0\}$.

3) $\mathbb{C} = \mathbb{R} \cdot 1 + \mathbb{R} \cdot \sqrt{-1}$ ist endlich über $\mathbb{R}$.

4) $\mathbb{Z} \subseteq \mathbb{Q}$ ist nicht endlich. Allgemeiner: Für jeden Integritätsring R ist $K = Q(R)$ nur dann endlich über R, wenn R ein Körper, d.h. $R = K$ ist.

5) Es sei R ein kommutativer Ring, $f \in R[X]$, f normiert, $n = \deg(f) \geq 1$, sowie $A = R[X]/(f)$. Der Ringhomomorphismus $R \hookrightarrow R[X] \overset{\text{kan.}}{\to} A$ ist injektiv. [ist $r \in R$ mit $\overline{r} = 0$ in A, d.h. $r = fg$ in $R[X]$, so muss $g = 0$ sein wegen $\deg(f) \geq 1$, also $r = 0$ in R.] Man kann R also als Unterring von A auffassen: Identifiziere $r \in R$ mit $\overline{r} \in A$. Für $x = \overline{X}$ gilt $A = R[x]$ und $f(x) = 0$. [mit $f = \sum_{i=0}^{n} r_i X^i$ ist $f(x) = \sum_{i=0}^{n} r_i x^i = \sum_{i=0}^{n} \overline{r_i}\,\overline{X}^i = \overline{\sum_{i=0}^{n} r_i X^i} = \overline{f} = 0$ in A.] Ferner ist A endlich über R, sogar als R-Modul frei mit der Basis $1, x, x^2, x^3, \ldots, x^{n-1}$.

Beispiel. Beispiele zu Beispiel 5:

1) $\mathbb{Z}[\sqrt{d}] \cong \mathbb{Z}[X]/(X^2 - d)$

2) $\mathbb{C} \cong \mathbb{R}[X]/(X^2 + 1)$

Bemerkung (Transitivität der Endlichkeit). Sind $R \subseteq B$ und $B \subseteq A$ endliche Ringerweiterungen, so ist auch $R \subseteq A$ endlich. Genauer: $\sum_{j=1}^{m} Rb_j = B \wedge \sum_{i=1}^{n} Ba_i = A \Rightarrow \sum_{i,j=1}^{n,m} R(a_i b_j) = A$. [$a = \sum_{i=1}^{n} c_i b_i$; $c_i = \sum_{j=1}^{m} r_{ij} b_j$ $(1 \leq i \leq n) \Rightarrow a = \sum r_{ij} a_i b_j$].

Lemma. *Es sei R ein kommutativer Ring. Zu jedem normierten $f \in R[X]$ mit $n = \deg(f) \geq 1$ gibt es eine endliche Ringerweiterung $R \subseteq A$ und $a_1, ..., a_n \in A$ mit $f = (X - a_1) \cdots (X - a_n)$ in $A[X]$.*

Beweis. Induktion nach n. $n = 1$: $f = X - r$, $R = A$, $r = a_1$. $n \geq 2$: Nach Beispiel 5 gibt es eine endliche Ringerweiterung $R \subseteq A_1$ und $a_1 \in A_1$ mit $f(a_1) = 0$ in A_1, d.h. $f = (X - a_1) f_1$ in $A_1[X]$, wofür $\deg(F) = n - 1 \geq 1$. Nach Induktionsvoraussetzung gibt es eine endliche Ringerweiterung $A_1 \subseteq A$ und $a_2, \ldots, a_n \in A$ mit $f = (X - a_1) \cdots (X - a_n)$. Dann ist $R \subseteq A$ endlich nach Bemerkung. □

Definition. Es sei $R \subseteq A$ eine Ringerweiterung. Ein $a \in A$ heißt *ganz* über R, wenn es ein normiertes $f \in R[X]$ gibt mit $f(a) = 0$ in A, d.h. es gibt eine Ganzheitsgleichung $a^n + \sum_{i=0}^{n-1} r_i a^i = 0$ für a mit $r_0, \ldots, r_{n-1} \in R$. Ist jedes $a \in A$ ganz über R, so heißt $R \subseteq A$ eine *ganze Ringerweiterung*, oder kurz A *ganz* über R.

Beispiel.

1) R ist ganz über R. [$f = X - r$]

2) Ist $a \in A$ *nilpotent* (d.h. $a^n = 0$ für ein $n \in \mathbb{N}$) oder idempotent (d.h. $a^2 = a$), so ist a ganz über R [$f = X^n$ bzw. $f = X^2 - X$].

3) $\mathbb{Z}[\sqrt{d}]$ ist ganz über $\mathbb{Z}$. [für $a = x + \sqrt{d}y$ mit $x, y \in \mathbb{Z}$ ist $f(a) = 0$ für $f = X^2 - 2x - X + x^2 - dy^2$. Beachte $f \in \mathbb{Z}[X]$.]

4) In $R \subseteq R[X]$ ist X nur dann ganz über R, wenn $R = \{0\}$ ist. [$f \in R[X]$ normiert, $0 = f(X) = f \Rightarrow 0 = 1$ in R]

Satz. *Jede endliche Ringerweiterung ist ganz.*

Beweis. Es sei $R \subseteq A$ eine endliche Ringerweiterung, $A = Ra_1 + \cdots + Ra_n$, sowie $a \in A$. Für $1 \leq i \leq n$ gibt es $r_{i1}, \ldots, r_{in} \in R$ mit $aa_i = \sum_{j=1}^{n} r_{ij} a_j$. Mit $N = (r_{ij}) \in R^{n \times n}$ ist also $a(a_1 \cdots a_n)^T = N(a_1 \cdots a_n)^T$, d.h. $M(a_1 \cdots a_n)^T = 0$ für $M = aI_n - N \in A^{n \times n}$. Für das charakteristische Polynom $\chi_N \in R[X]$ von N ist also $\det M = \chi_N(a)$ und χ_N unitär. Es genügt zu zeigen: $\det M = 0$. Für die Komplementärmatrix $\tilde{M}$ von M ist $\tilde{M}M = \det(M) \cdot I_n$, also $0 = \tilde{M}M(a_1 \cdots a_n)^T = \det(M)(a_1 \cdots a_n)^T$, d.h. $\det(M)a_i = 0$ $(1 \leq i \leq n)$. Mit $1 = \sum_{i=1}^{n} s_i a_i$ folgt $\det M = 0$. □

Konvention. Im folgenden sei $R \subseteq A$ stets eine Ringerweiterung.

Korollar 1. *Für jedes $a \in A$ sind äquivalent:*

i) a ist ganz über R.

ii) Es gibt ein $m \geq 1$ mit $R[a] \overset{(*)}{=} R + Ra + \cdots + Ra^{m-1}$.

iii) $R[a]$ ist endlich über R.

Beweis.

ii ⇒ iii %

iii ⇒ i Satz.

i ⇒ ii Ist $a^m + \sum_{i=0}^{m-1} r_i a^i = 0$ mit $r_0, \ldots, r_{m-1} \in R$, so ist m wie verlangt in ii), denn: in $(*)$ ist „$\supseteq$“ klar, und mit $a^m = -\sum_{i=0}^{m-1} r_i a^i$ liegen auch $a^{m+1} = aa^m$, $a^{m+2} = a^2 a^m$ usw. in $R + Ra + \ldots Ra^{m-1}$. □

Korollar 2. *Es sind äquivalent*

i) A ist endlich über R.

ii) Es gibt ganze $b_1, \ldots, b_m \in A$ mit $A = Rb_1 + \cdots + Rb_m$.

iii) Es gibt ganze $a_1, \ldots, a_n \in A$ mit $A = R[a_1, \ldots, a_n]$.

Beweis. **i ⇒ ii** Satz.

ii ⇒ iii man verwende $Rb_1 + \cdots + Rb_m \subseteq R[b_1, \ldots, b_m] \subseteq A$; dann: $n = m$, $a_1 = b_1$ für alle $i \leq n$.

iii ⇒ i Induktion nach n. $n = 1$: Korollar 1. $n \geq 2$: nach Induktion ist $B = R[a_1, \ldots, a_n]$ endlich über R. Da a_n ganz über R ist, also auch über B, ist $A = B[a_n]$ endlich über B (Korollar 1). Es folgt A endlich über R. (Bemerkung). □

Bemerkung. Speziell gilt für $a_1, \ldots, a_n \in A$: $R[a_1, \ldots, a_n]$ endlich über $R \Leftrightarrow R[a_1, \ldots, a_n]$ ganz über R.

Definition. Man nennt $\overline{R} = \{a \in A \colon a \text{ ganz über } R\}$ den *ganzen Abschluß* von R in A. Es gilt $R \subseteq \overline{R} \subseteq A$. Im Falle $R = \overline{R}$ heißt R *ganz abgeschlossen* in A.

Beispiel. R faktoriell $\Rightarrow$ R ganz abgeschlossen in $K = Q(R)$.

Korollar 3.

a) $\overline{R}$ *ist Unterring von* A.

b) $\overline{R}$ *ist ganz abgeschlossen in* A, *d.h.* $\overline{\overline{R}} = \overline{R}$, *mit anderen Worten: Ist* $a \in A$ *ganz über* $\overline{R}$ *so ist* a *ganz über* R.

Beweis.

a) Sind $x, y \in \overline{R}$, so ist $R[x, y]$ endlich über R (Korollar 2), also $R[x, y] \subseteq \overline{R}$ (Satz), speziell $x \pm y, x \cdot y \in \overline{R}$.

b) Es sei $a^n + \sum_{i=0}^{n-1} b_i a^i = 0$, $b_i \in \overline{R}$. Für $B = R[b_0, \ldots, b_{n-1}]$ gilt $a \in \overline{B}$, also ist $B[a]$ endlich über B (Korollar 1), sowie B endlich über R (Korollar 2). Es folgt: $B[a]$ ist endlich über R (Bemerkung), also $B[a] \subseteq \overline{R}$ (Satz), speziell $a \in \overline{R}$. □

Korollar 4 (Transitivität der Ganzheit)**.** *Sind* $R \subseteq B$ *und* $B \subseteq A$ *ganze Ringerweiterungen, so ist auch* A *ganz über* R.

Beweis.

$$\left.\begin{array}{c} A \subseteq \overline{B} \\ B \subseteq \overline{R} \Rightarrow \overline{B} \subseteq \overline{\overline{R}} \end{array}\right\} \Rightarrow A \subseteq \overline{\overline{R}} = \overline{R} \qquad \square$$

Definition. Eine *Körpererweiterung* ist eine Ringerweiterung $k \subseteq K$, in der k, K beide Körper sind. Ist eine Körpererweiterung $k \subseteq K$ endlich, d.h. $\dim_k(K) < \infty$, so heißt $[K : k] = \dim_k(K)$ der *Grad* von $k \subseteq K$. Statt $k \subseteq K$ schreibt man auch K/k, d.h. „K über k“.

Bemerkung. Es seien k, L, K Körper mit $k \subseteq L \subseteq K$. Genau dann ist K/k endlich wenn K/L und L/k beide endlich sind, dann gilt: $[K : k] = [K : L] \cdot [L : k]$.

Beweis. „$\Leftarrow$“ schon für Ringe bewiesen. „$\Rightarrow$“ %. Noch zu den Graden: Aus $kb_1 \oplus \cdots \oplus kb_m = L$ und $La_1 \oplus \cdots \oplus La_n = K$ folgt wie früher $\sum_{i,j} k(a_i b_j) = K$, und die $a_i b_j$ $(1 \leq i \leq n,\ 1 \leq j \leq m)$ sind linear unabhängig, denn: $0 = \sum_{i,j} \lambda_{ij}(a_i b_j) = \sum_i (\sum_j \lambda_{ij} b_j) a_i \Rightarrow \sum_j \lambda_{ij} b_j = 0$ $(1 \leq i \leq n) \Rightarrow \lambda_{ij} = 0$ $(1 \leq i \leq n,\ 1 \leq j \leq n)$ $\underset{\in k}{}$ □

Folgerung. Hat eine Körpererweiterung K/k Primzahlgrad, so gibt es keinen Körper L mit $k \subsetneq L \subsetneq K$.

Beispiel. $\mathbb{R} \subseteq \mathbb{C}$, $[\mathbb{C} : \mathbb{R}] = 2$.

Lemma (Kronecker)**.** *Es sei* k *ein Körper. Zu jedem* $f \in k[X]$ *mit* $n = \deg(f) \geq 1$ *(speziell* $f \neq 0$*) gibt es eine endliche Körpererweiterung* K/k *mit* $[K : k] \leq n!$ *und dazu* $a_1, \ldots, a_n \in K$ *mit* $f = c \cdot (X - a_1) \cdots (X - a_n)$ *für ein* $c \in k$.

Beweis. Induktion nach n. $n = 1$: wie für Ringe gilt $f = \underset{\neq 0}{c} X + b = c(X - \underset{=a_1}{(-b/c)})$, $K = k$. $n \geq 2$: Da $k[X]$ ein Hauptidealring ist, gibt es ein Primelement $g \in k[X]$ mit $g \mid f$, wofür $1 \leq \deg(g) \leq n$, und (g) ist maximales Ideal von $k[X]$, d.h. $K_1 = k[X]/(g)$ ist ein Körper. O.B.d.A. ist g unitär. Der Ringhomomorphismus $k \hookrightarrow k[X] \underset{\text{kan.}}{\to} K_1$ ist injektiv. [k Körper], also kann man k als Unterkörper von K_1 auffassen mit $[K_1 : k] = \deg(g) \leq n$. Wie im Beispiel ist $a_1 = \overline{X}$ Nullstelle von g in K_1, also auch $f(a_1) = 0$, d.h. $f = (X - a_1) \cdot f_1$ für ein $f_1 \in K_1[X]$ mit $1 \leq \deg(f_1) \leq n - 1$. Nach Induktion gibt es eine Körpererweiterung K/K_1 mit $[K : K_1] \leq (n-1)!$ und $f_1 = c \cdot (X - a_2) \cdots (X - a_n)$ mit $a_2, \ldots, a_n \in K$ und $c \in k$. Nach Bemerkung ist $[K : k] = [K : K_1] \cdot [K_1 : k] \leq n!$. □

Definition. Es sei $k \subseteq K$ eine Körpererweiterung. Man nennt $a \in K$ *algebraisch* über k, wenn es ein $f \in k[X]$ gibt mit $f \neq 0$ und $f(a) = 0$; sonst heißt a *transzendent* über k. Sind alle $a \in K$ algebraisch über k, so heißt die Körpererweiterung $k \subseteq K$ *algebraisch* oder kurz K *algebraisch* über k.

Beobachtung. $a \in K$ (bzw. K) algebraisch über k. $\iff$ a (bzw. K) ist ganz über k.

Satz. *Jede endliche Körpererweiterung ist algebraisch*

Beweis. Mit dem entsprechenden Satz über Ringerweiterungen, oder direkt: Es sei $n = [K : k]$. Für $a \in K$ sind $1, a, a^2, \ldots, a^n$ k-linear abhängig, d.h. es gibt $\lambda_0, \ldots, \lambda_n \in k$ mit $\sum_{i=0}^n \lambda_i a^i = 0$ und $\lambda_i \neq 0$ für ein i. Für $f = \sum_{i=0}^n \lambda_i X^i \in k[X]$ ist $f \neq 0$ und $f(a) = 0$. □

Definition. $\overline{k} = \{a \in K \colon a \text{ algebraisch über } k\}$ den *algebraischen Abschluss* von k in K. Wie früher ist $\overline{k}$ ein Unterring von K, sogar ein Körper: Für $a \in \overline{k}$ mit $a \neq 0$ nehme man $r_0, \ldots, r_n \in k$ mit $\sum_{i=0}^n r_i a^i = 0$ und $r_i \neq 0$ für ein i. Dafür ist $0 = \frac{1}{a^n} \sum_{i=0}^n r_i a^i = \sum_{i=0}^n r_i (\frac{1}{a})^{n-i}$, also $\frac{1}{a} \in \overline{k}$.

Definition. Für $S \subseteq K$ gilt $k[S] \subseteq K$. Die *Körperadjunktion* von $S \subseteq K$ an k ist $k(S) = \{a \in K \colon \text{es gibt } x, y \in k[S] \text{ mit } y \neq 0 \text{ und } a = \frac{x}{y}\}$. Es gilt $k[S] \subseteq k(S) \subseteq K$ und $k(S)$ ist ein Körper. Genauer: $k(S) = \bigcap\{L \subseteq K \colon L \text{ Unterkörper von } K, k \cup S \subseteq L\}$, d.h. $k(S)$ ist der kleinste Unterkörper von K, der $k \cup S$ umfasst. Für $S = \{a_1, \ldots, a_n\}$ schreibt man $k(a_1, \ldots, a_n)$ anstelle $k(S)$. Es gilt

$$k(a_1, \ldots, a_n) = \left\{ \frac{f(a_1, \ldots, a_n)}{g(a_1, \ldots, a_n)} \colon f, g \in k[X_1, \ldots, X_n], g(a_1, \ldots, a_n) \neq 0 \right\}$$

Lemma. *Es sei $k \subseteq K$ eine Körpererweiterung. Sind $a_1, \ldots, a_n \in K$ algebraisch über k, so ist $k[a_1, \ldots, a_n] = k(a_1, \ldots, a_n)$.*

Beweis. Für $B = k[a_1, \ldots, a_n]$ ist zu zeigen: B ist ein Körper. Als Unterring von K ist B ein Integriätsring. Nach Korollar 2 ist B endlich über k, d.h. $\dim_k(B) < \infty$. Für $b \in B \setminus \{0\}$ ist $\mu_b \colon B \to B, x \mapsto xb$ k-linear [sogar B-linear] und injektiv [B Integritätsring, $b \neq 0$], also biektiv. Speziell ist $1 \in \mathrm{Im}(\mu_b)$, d.h. $b \in B^\times$. □

Bemerkung. Beachte jedoch, dass z.B. $k[X] \subsetneq k(X)$.

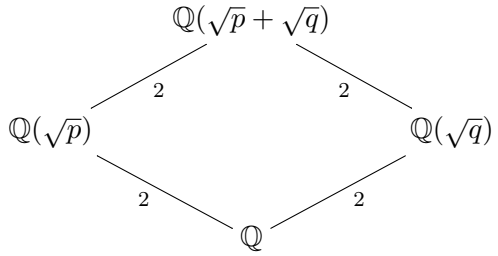
Satz (Definition und Eigenschaften des Minimalpolynoms)**.** *Es sei $k \subseteq K$ eine Körpererweiterung. Ist $a \in K$ algebraisch über k, so gibt es genau ein irreduzibles und normiertes $f \in k[X]$ mit $f(a) = 0$, das* Minimalpolynom *von a über k. Weiterhin gilt für jedes $g \in k[X]$: $g(a) = 0 \Leftrightarrow f \mid g$. Und mit $n = \deg(f)$ ist $1, a, a^2, \ldots, a^{n-1}$ eine k-Basis von $k(a)$.*

Beweis. Für $\varepsilon_a \colon k[X] \to K, g \mapsto g(a)$ ist $\operatorname{Ker}(\varepsilon_a) \neq \{0\}$ [a ist algebraisch über k], also $\operatorname{Ker}(\varepsilon_a) = (f)$ für ein normiertes $f \in k[X]$, und $\operatorname{Im}(\varepsilon_a) = k[a] = k(a)$ ist ein Körper, also (f) ein maximales Ideal von $k[X]$ [verwende $k[X]/\operatorname{Ker}(\varepsilon_a) \cong \operatorname{Im}(\varepsilon_a)$], also ist f irreduzibel. Für $g \in k[X]$ gilt: $g(a) = 0 \Leftrightarrow f \mid g$. Ist $f' \in k[X]$ irreduzibel und normiert mit $f'(a) = 0$, d.h. $f' = fh$ für ein $h \in k[X]$, so ist $h \in k^\times$ [f' irreduzibel], sogar $h = 1$ [f', f normiert], d.h. $f' = f$. Aus $k[X]/(f) = k1 \oplus kX \oplus \cdots \oplus kX^{n-1}$ folgt längs $k[X]/(f) \cong k(a)$, dass $k(a) = k1 \oplus ka \oplus \cdots \oplus ka^{n-1}$. Beachte $\varepsilon_a(X) = a$. □

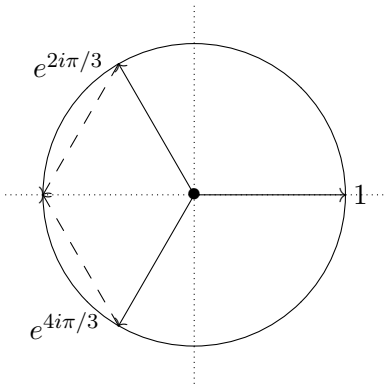
Beispiel.

1) Für $n \geq 1$ und eine Primzahl p ist $X^n - p$ das Minimalpolynom von $\sqrt[n]{p} \in \mathbb{R}$ über $\mathbb{Q}$, speziell ist $[\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}] = n$. Damit ist der algebraische Abschluss $\overline{\mathbb{Q}}$ von $\mathbb{Q}$ in $\mathbb{C}$ nicht endlich über $\mathbb{Q}$. Natürlich ist $\overline{\mathbb{Q}}$ algebraisch über $\mathbb{Q}$.

2) Für Primzahlen p, q mit $p \neq q$ ist $f = X^4 - 2(p+q)X^2 + (p-q)^2$ das Minimalpolynom von $a = \sqrt{p} + \sqrt{q}$ über $\mathbb{Q}$. Denn $a^2 = p + q + 2\sqrt{pq} \Rightarrow (a^2 - (p+q))^2 = 4pq \Rightarrow a$ ist Nullstelle von $(X^2 - (p+q))^2 - 4pq = X^4 - 2(p+q)X^2 + (p+q)^2 - 4pq = f$. Speziell gilt $[\mathbb{Q}(a) : \mathbb{Q}] \leq 4$. Wegen $q = (a - \sqrt{p})^2 = a^2 + p - 2a\sqrt{p}$ und $a \neq 0$ ist $\mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(a)$, jedoch ist $a \notin \mathbb{Q}(\sqrt{p})$ (!), d.h. $\mathbb{Q}(\sqrt{p}) \subsetneq \mathbb{Q}(a)$, woraus mit $[\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = 2$ folgt: $[\mathbb{Q}(a) : \mathbb{Q}] = 4$ [Gradgründe]. Für das Minimalpolynom f_0 von a über $\mathbb{Q}$ ist $\deg(f_0) = 4$, sowie $f_0 \mid f$, also $f_0 = f$ [f ist unitär, $\deg(f) = 4$]. Noch zu (!): Wäre $a \in \mathbb{Q}(\sqrt{p})$, so wäre $a = r + s\sqrt{p}$ mit $r, s \in \mathbb{Q}$, also $\sqrt{q} = r + (s-1)\sqrt{p}$, worin $s \neq 1$ [sonst $\sqrt{q} \in \mathbb{Q}$] und $r \neq 0$ [sonst $\sqrt{pq} = (s-1)p \in \mathbb{Q}$, was wegen $p \neq q$ unmöglich ist], sowie $q = \underbrace{r^2 + (s-1)^2 p}_{\in \mathbb{Q}} + 2\underbrace{r(s-1)}_{\neq 0}\sqrt{p}$, also $\sqrt{p} \in \mathbb{Q}$, was unmöglich ist.



3) Für jede Primzahl p ist $f = X^{p-1} + X^{p-2} + \cdots + X + 1$ das Minimalpolynom von $a = e^{2\pi i/p} \in \mathbb{C}$ über $\mathbb{Q}$, denn f ist irreduzibel und $(a-1)f(a) = a^p - 1 = 0 \Rightarrow f(a) = 0$ und f ist normiert. Im Fall $p = 3$ ist $a = e^{2\pi i/3}$, $f = X^2 + X + 1$:



Bemerkung. Es sei $k \subseteq K$ eine Körpererweiterung, $f \in k[X]$ normiert und $a \in K$ mit $f(a) = 0$. Dann ist f das Minimalpolynom von a über k genau dann, wenn $\deg(f) = [k(a) : k]$ ist. In diesem Falle ist f irreduzibel. Zum Beispiel ist für $a \in K \setminus k$ jedes $f \in k[X]$ mit $\deg(f) = 2$ und $f(a) = 0$ schon das Minimalpolynom von a über k.

Lemma. *Es sei R ein Integritätsring mit Quotientenkörper K, $K \subseteq L$ eine Körpererweiterung, $a \in L$. Genau dann ist a ganz über R, wenn a algebraisch über K ist und die Koeffizienten des Minimalpolynoms von a über K alle ganz über R sind.*

Beweis. O.B.d.A. ist a algebraisch über K. Es sei f das Minimalpolynom von a über K, und $\overline{R}^L$ der algebraische Abschluss von R in L.

„⇐“ $f \in \overline{R}^L[X] \Rightarrow a$ ist ganz über $\overline{R}^L \Rightarrow a$ ist ganz über R.

„⇒“ Nehme $g \in R[X]$ normiert mit $g(a) = 0$. Es gibt eine Körpererweiterung $L \subseteq M$ und $b_1, \ldots, b_m \in M$ mit $f = (X - b_1) \cdots (X - b_m)$. Wegen $f \mid g$ ist $g(b_i) = 0$, also $b_i \in \overline{R}^M$ (= algebraischer Abschluss von R in M) für alle i. Es folgt $f \in \overline{R}^M[X]$ [Die Koeffizienten von f sind Polynome in $b_1, \ldots, b_m$] und damit $f \in \overline{R}^L[X]$, da $f \in K[X] \subseteq L[X]$ und $\overline{R}^M \cap L = \overline{R}^L$ (!). □

$$\begin{array}{ccccc} \overline{R}^M & \subseteq & M & & \\ \cup\!| & & \cup\!| & & \\ \overline{R}^L & \subseteq & L & \ni & a \\ \cup\!| & & \cup\!| & & \\ R & \subseteq & K & = Q(R) & \end{array}$$

Satz. *Ist $d \in \mathbb{Z} \setminus \{0, 1\}$* quadratfrei, *d.h. $p^2 \nmid d$ für alle Primzahlen p, so gilt für den algebraischen Abschlus $\overline{\mathbb{Z}}$ von $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$ (dabei gilt $m \equiv n \bmod k \Leftrightarrow k \mid m - n$):*

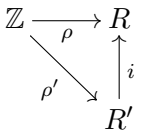
$$\overline{\mathbb{Z}} = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{falls } d \not\equiv 1 \pmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{falls } d \equiv 1 \pmod 4 \end{cases}$$

Beweis. Da $X^2 - d$ nach Voraussetzung keine Nullstelle in $\mathbb{Z}$ hat, ist $X^2 - d$ in $\mathbb{Z}[X]$, also auch in $\mathbb{Q}[X]$ irreduzibel und damit das Minimalpolynom von $\sqrt{d}$ über $\mathbb{Q}$. Speziell: $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = 2$, $\mathbb{Q}(\sqrt{d}) = \mathbb{Q} \cdot 1 \oplus \mathbb{Q}(\sqrt{d})$. Fall $d \not\equiv 1 \bmod 4$: „$\supseteq$“ $\mathbb{Z}[\sqrt{d}]$ ist endich über $\mathbb{Z}$, also ganz über $\mathbb{Z}$. „$\subseteq$“ Es sei $a \in \overline{\mathbb{Z}}$, $a = x + y\sqrt{d}$ mit $x, y \in \mathbb{Q}$. Ist $y = 0$, so ist $a = x \in \mathbb{Q}$, also $a \in \overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$. Ist $y \neq 0$, speziell $a \notin \mathbb{Q}$, so ist $f = X^2 - 2xX + (x^2 - dy^2)$ nach Bemerkung das Minimalpolynom von a über $\mathbb{Q}$, da $f(a) = 0$. Gemäß Lemma ist $2x \in \mathbb{Z}$ und $x^2 - dy^2 \in \mathbb{Z}$, also $4x^2 \in \mathbb{Z}$ und $4dy^2 \in \mathbb{Z}$. Da d quadratfrei ist, ist auch $2y \in \mathbb{Z}$ [$2y = \frac{r}{3}$, $r, s \in \mathbb{Z} \Rightarrow (4dy^2)s^2 = dr^2$, d.h. $zs^2 = dr^2$ für $z = 4dy^2 \in \mathbb{Z} \Rightarrow$ aus $p \mid s$ folgt $p \mid r$, p prim $\Rightarrow s \mid r$]. Mit $u = 2x \in \mathbb{Z}$, $v = 2y \in \mathbb{Z}$ ist $u^2 - dv^2 = 4\underbrace{(x^2 - dy^2)}_{\in\mathbb{Z}}$, d.h. $u^2 \equiv dv^2 \bmod 4$. Fall 1: v gerade $\Rightarrow u$ gerade $\Rightarrow x, \in \mathbb{Z}$. Fall 2: v ungerade $\Rightarrow v^2 \equiv 1 \bmod 4 \Rightarrow u^2 \equiv d \bmod 4 \Rightarrow u$ ungerade $\Rightarrow u^2 \equiv 1 \bmod 4 \Rightarrow d \equiv 1 \bmod 4$, was ausgeschlossen ist. Der Fall $d \equiv 1 \bmod 4$ ist ähnlich zu beweisen. □

3 Körper

3.1 Galoiserweiterungen

Definition. Für jeden Ring R ist $\rho\colon \mathbb{Z} \to R, z \mapsto z \cdot 1$ ein Ringhomomorphismus, also $\operatorname{Ker}(\rho) = (n)$ für genau ein $n \geq 0$. Dieses n nennt man die *Charakteristik* von R, kurz $\operatorname{char}(R) = n$. Für jeden Unterring R' von R ist $\operatorname{Im}(\rho) \subseteq R'$, also $\rho = i \circ \rho'$ für $i\colon R' \hookrightarrow R$, $\rho'\colon \mathbb{Z} \to R', z \mapsto z \cdot 1$, d.h. folgendes Diagramm kommutiert:



Es folgt $\operatorname{Ker}(\rho) = \operatorname{Ker}(\rho')$ und damit $\operatorname{char}(R) = \operatorname{char}(R')$. Ist R ein Integritätsring, so ist auch $\operatorname{Im}(\rho) \cong \mathbb{Z}/\operatorname{Ker}(\rho)$ ein Integritätsring, d.h. $\operatorname{Ker}(\rho) = (\operatorname{char}(R))$ ist ein Primideal, d.h. $\operatorname{char}(R) = 0$ oder $\operatorname{char}(R) = p$ für eine Primzahl p.

Definition. Für jeden Körper K definieren wir den *Primkörper* K_0 von K durch $K_0 = \operatorname{Im}(\rho)$, falls $\operatorname{char}(K) = p$ mit einer Primzahl p bzw. $K_0 = \operatorname{Im}(\tilde{\rho})$, falls $\operatorname{char}(K) = 0$, wobei $\tilde{\rho}\colon \mathbb{Q} \to K, \frac{r}{s} \mapsto \frac{\rho(r)}{\rho(s)}$ der *von ρ induzierte Ringhomomorphismus* sei, welcher injektiv ist. [hier: ρ injektiv].

Bemerkung. In jedem Fall ist K_0 ein Körper, genauer gilt

$$K_0 \cong \begin{cases} \mathbb{Q} & \text{falls } \operatorname{char}(K) = 0 \\ \mathbb{Z}/(p) & \text{falls } \operatorname{char}(K) = p \end{cases}$$

Es gilt sogar $K_o \overset{(!)}{=} \bigcap\{L \subseteq K\colon L \text{ Unterkörper von } K\}$. Speziell ist K_0 der kleinste Unterkörper von K. Noch zu (!): „$\subseteq$“ Für alle L wie oben ist $\operatorname{Im}(\rho) \subseteq L$. Fall $\operatorname{char}(K) = p$: $K_0 = \operatorname{Im}(\rho)$. Fall $\operatorname{char}(K) = 0$: Sogar $\operatorname{Im}(\tilde{\rho}) \subseteq L$ für alle L wie oben [für $\frac{r}{s} \in \mathbb{Q}$ sind $\rho(r), \rho(s) \in L$, also $\frac{\rho(r)}{\rho(s)} \in L$, da L ein Körper ist]. Es ist $K_0 = \operatorname{Im}(\tilde{\rho})$.

Bemerkung.

a) Ist K ein eindlicher Körper, so ist $\mathrm{char}(K) = p$ und $|K| = p^n$ für eine Primzahl p.

b) Ist R ein kommutativer Ring mit $\mathrm{char}(R) = p$ für eine Primzahl p, so ist $F\colon R \to R, x \mapsto x^p$ ein Ringhomomorphismus, der sogenannte *Frobeniushomomorphismus* von R.

Beweis.

a) Wegen $K_0 \subseteq K$ ist $K_0 \ncong \mathbb{Q}$, also $K_0 \cong \mathbb{Z}/(p)$ für eine Primzahl p. Ferner $n = [K : K_0] < \infty$ und $K \cong K_0^n$, also $|K| = p^n$.

b) Für $0 < k < p$ ist $p \mid \binom{p}{k}$, d.h. $\binom{p}{k} = 0$ in $\mathbb{Z}/(p)$ und damit auch in R, da ja $\mathbb{Z}/(p) \underset{\rho}{\to} R$ ein Ringhomomorphismus ist. Es folgt

$$F(x+y) = (x+y)^p = x^p + \underbrace{\sum_{k=1}^{p-1} \binom{p}{k} x^k y^{p-k}}_{0} + y^p = x^p + y^p = F(x) + F(y)$$

Ohnehin gilt $F(1) = 1^p = 1$, $F(xy) = (xy)^p = x^p y^p = F(x)F(y)$. □

Definition. Es sei K ein Körper. Man nennt

$$\mathrm{Aut}(K) = \{\sigma\colon K \to K\colon \sigma \text{ bijektiver Ringhomomorphismus}\}$$

die *Automorphismengruppe* von K. Für jeden Unterkörper k von K ist $\mathrm{Gal}(K/k) = \{\sigma \in \mathrm{Aut}(K)\colon \sigma|_k = \mathrm{id}_k\}$ eine Untergruppe von $\mathrm{Aut}(K)$, die *Galoisgruppe* von K über k.

Beispiel.

0) $\mathrm{Gal}(K/K) = \{\mathrm{id}_K\}$ und $\mathrm{Gal}(K/K_0) = \mathrm{Aut}(K)$ [für $z \in \mathbb{Z}$ und $\sigma \in \mathrm{Aut}(K)$ ist $\sigma(z \cdot 1) = \sigma(1 + \cdots + 1) = \sigma(1) + \cdots + \sigma(1) = z\sigma(1) = z \cdot 1$ bzw, wenn $\mathrm{char}(K) = 0$, dann $K_0 = \{\frac{r1}{s1}\colon \frac{r}{s} \in \mathbb{Q}\}$ und $\sigma(\frac{r1}{s1}) = \frac{\sigma(r1)}{\sigma(s1)} = \frac{r1}{s1}$]

1) Es sei $d \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei, $K = \mathbb{Q}(\sqrt{d})$. Mit $K = \mathbb{Q}1 \oplus \mathbb{Q}\sqrt{d}$ sei $\tau\colon K \to K$ mit $\tau(x + y\sqrt{d}) = x - y\sqrt{d}$. Nun ist $\tau \in \mathrm{Aut}(K)$, und für jedes $\sigma \in \mathrm{Aut}(K)$ ist $\sigma(\sqrt{d})^2 = \sigma(\sqrt{d}^2) = \sigma(d) = d$, d.h. $\sigma(\sqrt{d}) = \pm\sqrt{d}$, d.h. $\sigma = \mathrm{id}_K$ oder $\sigma = \tau$. Es folgt $\mathrm{Aut}(K) = \{\mathrm{id}, \tau\}$.

2) Es sei p eine Primzahl, $K = \mathbb{Q}(\sqrt[3]{p})$ mit $a = \sqrt[3]{p}$ ist $K = \mathbb{Q}1 \oplus \mathbb{Q}a \oplus \mathbb{Q}a^2$. Für jedes $\sigma \in \mathrm{Aut}(K)$ ist $\sigma(a)^3 = \sigma(a^3) = \sigma(p) = p$, also $\sigma(a) = a$, da $\sigma(a) \in \mathbb{R}$ und damit $\sigma(a^2) = \sigma(a)^2 = a^2$, also $\sigma = \mathrm{id}$ und $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{p})) = \{\mathrm{id}\}$.

3) Es seien $p \neq q$ Primzahlen, $K = \mathbb{Q}(a)$ mit $a = \sqrt{p} + \sqrt{q}$. Wegen $a^2 = p + q + 2\sqrt{pq}$, $a^3 = (p + 3q)\sqrt{p} + (3p + q)\sqrt{q}$ ist auch $K = \mathbb{Q}1 \oplus \mathbb{Q}\sqrt{p} \oplus \mathbb{Q}\sqrt{q} \oplus \mathbb{Q}\sqrt{pq}$. Für $\sigma \in \mathrm{Aut}(K)$ ist wie oben $\sigma(\sqrt{p}) = \pm\sqrt{p}$, $\sigma(\sqrt{q}) = \pm\sqrt{q}$ und damit $\sigma(\sqrt{pq}) = \pm\sqrt{pq}$. Als Elemente von $\mathrm{Aut}(K)$ kommen also nur die folgenden $\mathbb{Q}$-linearen Isomorphismen $\sigma_1, \sigma_2, \sigma_3, \sigma_4\colon K \to K$ in Frage:

	1	$\sqrt{p}$	$\sqrt{q}$	$\sqrt{pq}$
σ_1	1	$\sqrt{p}$	$\sqrt{q}$	$\sqrt{pq}$
σ_2	1	$-\sqrt{p}$	$\sqrt{q}$	$-\sqrt{pq}$
σ_3	1	$\sqrt{p}$	$-\sqrt{q}$	$-\sqrt{pq}$
σ_4	1	$-\sqrt{p}$	$-\sqrt{q}$	$\sqrt{pq}$

Nun sind $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ alle Ringhomomorphismen (!) und damit $\mathrm{Aut}(K) = \{\sigma_1 = \mathrm{id}, \sigma_2, \sigma_3, \sigma_4\}$. Also ist $\mathrm{Aut}(K) \cong \mathbb{Z}/(4)$ oder $\mathrm{Aut}(K) \cong V$ mit der Kleinschen Vierergruppe V. Wegen $\sigma_i^2 = \mathrm{id}$ für $i = 1, \ldots, 4$ ist $\mathrm{Aut}(K) \ncong \mathbb{Z}/(4)$, also $\mathrm{Aut}(K) \cong V$.

Lemma (Dedekind)**.** *Es seien K, K' Körper, $n \geq 1$. Für paarweise verschiedene Ringhomomorphismen $\varphi_1, \ldots, \varphi_n \colon K \to K'$ gilt:*

a) Für $y_1, \ldots, y_n \in K'$ gilt: Ist $\sum_{i=1}^n y_i \varphi_i(x) = 0$ für alle $x \in K$, so ist $y_1 = y_2 = \cdots = y_n = 0$.

b) $L = \{x \in K \colon \varphi_1(x) = \cdots = \varphi_n(x)\}$ ist ein Unterkörper von K mit $[K : L] \geq n$. Das gilt auch für $[K : L] \not< \infty$.

Beweis.

a) Induktion nach n. $n = 1$: Aus $0 = y_1\varphi_1(1) = y_1 1 = y_1$ „folgt“ $y_1 = 0$. $n \geq 2$: Für $y \in K'$ und $\varphi \colon K \to K'$ sei $y\varphi \colon K \to K', x \mapsto y\varphi(x)$ (damit wird $(K')^K$ zu einem K'-Vektorraum). Speziell gilt: $\sum y_i\varphi_i = 0 \Leftrightarrow \forall x \in K(\sum y_i\varphi_i(x) = 0)$. Annahme: $\exists i(y_i \neq 0)$. O.B.d.A. $i = 1$, $y_1 = -1$, d.h. $\varphi_1 = \sum_{i=2}^n y_i\varphi_i$. Es folgt: $\sum_{i=2}^n y_i\varphi_i(a)\varphi_i(x) = \sum_{i=2}^n y_i\varphi_i(ax) = \varphi_1(ax) = \varphi_1(a)\varphi_1(x) = \varphi_1(a)\sum_{i=2}^n y_i\varphi_i(x)$ für alle $a, x \in K$, also $\sum_{i=2}^n \underbrace{y_i(\varphi_i(a) - \varphi_1(a))}_{\in K'}\varphi_i = 0$ für alle $a \in K$. Nach Induktion ist $y_i(\varphi_i(a) - \varphi_1(a)) = 0$ für alle $a \in K$ und $i \geq 2$. Für jedes $i \geq 2$ gibt es $a \in K$ mit $\varphi_i(a) \neq \varphi_1(a)$, womit $y_i = 0$ folgt, also $y_1\varphi_1 = 0$ und damit $(n = 1)$: $y_1 = 0$, also Widerspruch.

b) $L = \{x \in K \colon \varphi_1(x) = \cdots = \varphi_n(x)\}$ ist ein Unterkörper von K. (!) Noch zu zeigen: $[L : K] \geq n$. Dafür ist zu zeigen, dass aus $K = \sum_{j=1}^r La_j$ folgt, dass $r \geq n$. Dazu: Für $M = (\varphi_i(a_j))_{i,j}^T \in (K')^{r \times n}$ ist $\mu \colon (K')^n \to (K')^r, s \mapsto Ms$ K'-linear. Es reicht zu zeigen: μ ist injektiv. Dazu sei $s = (y_1, \ldots, y_n)^T \in (K')^n$ mit $Ms = 0$. Für jedes $x \in K$ mit $x = \sum_{j=1}^r \lambda_j a_j$ $(\lambda_j \in L)$ folgt

$$\sum_{i=1}^n y_i\varphi_i(x) = \sum_{i,j} y_i \underbrace{\varphi_i(\lambda_j)}_{\varphi_1(\lambda_j)} \varphi_i(a_j) = \sum_j \varphi_1(\lambda_j) \underbrace{\sum_i \varphi_i(a_j)y_i}_{(M_s)_j = 0} = 0$$

Nach a) ist $y_1 = y_2 = \cdots = y_n = 0$, d.h. $s = 0$. □

Folgerung. Für jede *endliche* Körpererweiterung $k \subseteq K$ ist $|\mathrm{Gal}(K/k)| \leq [K : k]$. Insbesondere ist $\mathrm{Gal}(K/k)$ eine *endliche* Untergruppe von $\mathrm{Aut}(K)$.

Beweis. Für $n \geq 1$ paarweise verschiedene $\sigma_1, \ldots, \sigma_n \in \mathrm{Gal}(K/k)$ ist $k \subseteq L \subseteq K$ für $L = \{x \in K \colon \varphi_1(x) = \cdots = \varphi_n(x)\}$ und nach Lemma b) ist L ein Körper mit $[K : L] \geq n$, also $[k : k] = [K : L] \cdot [L : k] \geq n$. □

Definition. Eine endliche Körpererweiterung $k \leq K$ heißt *galoissch* oder *Galoiserweiterung*, wenn in obiger Folgerung „=“ gilt, d.h. $|\mathrm{Gal}(K/k)| = [K : k]$.

Beispiel. $\mathbb{Q}(\sqrt{d})$ und $\mathbb{Q}(\sqrt{p}+\sqrt{q})$ sind galoissch über $\mathbb{Q}$, $\mathbb{Q}(\sqrt[3]{p})$ ist nicht galoissch über $\mathbb{Q}$.

Bemerkung. Jeder endliche Körper K ist über seinem Primkörper K_0 galoissch. Genauer: Mit $K_0 \cong \mathbb{Z}/(p)$ ist $|K| = p^n$ für $n = [K : K_0]$. Speziell ist $|K^\times| = p^n - 1$, also $a^{p^n-1} = 1$ für alle $a \in K^\times$, d.h. $a^{p^n} = a$ für alle $a \in K$, d.h. $F^n = \mathrm{id}$ für den Frobeniushomomorphismus $F \colon K \to K, x \mapsto x^p$. Es gilt sogar: $\mathrm{ord}(F) = n$, denn ist $F^r = \mathrm{id}$, d.h. $X^{p^r} - X$ hat *alle* $a \in K$ als Nullstellen, so ist $p^n \leq p^r$, d.h. $n \leq r$. Es folgt: $\mathrm{Gal}(K/K_0) = \mathrm{Aut}(K)$ ist gleich $\langle F \rangle$ eine zyklische Gruppe der Ordnung $n = [K : K_0]$. Beachte $|\mathrm{Gal}(K/K_0)| \leq n$. Spezialfall $n = 1$: In $\mathbb{Z}/(p)$ ist $F = \mathrm{id}$, d.h. für alle $x \in \mathbb{Z}$ ist $x^p \equiv x \bmod p$ (Kleiner Satz von Fermat).

Definition. Ist K ein Körper und G eine Untergruppe von $\mathrm{Aut}(K)$, so ist $\mathrm{Fix}_K(G) = \{x \in K \colon \sigma(x) = x \text{ für alle } \sigma \in G\}$ ein Körper, der *Fixkörper* von G in K. Ist G zudem endlich, so hat man $\mathrm{Tr} \colon K \to K, x \mapsto \sum_{\sigma \in G} \sigma(x)$, die *Spur* von G in K („trace“). Diese ist $\mathrm{Fix}_K(G)$-linear. Nach dem Lemma von Dedekind ist $\mathrm{Tr} \neq 0$, d.h. $\mathrm{Tr}(a) \neq 0$ für ein $a \in K$.

Bemerkung. Für jede endliche Untergruppe G von $\mathrm{Aut}(K)$ ist $\mathrm{Im}(\mathrm{Tr}) = \mathrm{Fix}_K(G)$.

Beweis. „$\subseteq$“: Für $\rho \in G$ ist $\rho G = G$, also für $y = \mathrm{Tr}(x) = \sum_{\sigma \in G} \sigma(x)$:

$$\rho(y) = \sum_{\sigma \in G} \rho\sigma(x) = \sum_{\pi \in \rho G} \pi(x) = \sum_{\pi \in G} \pi(x) = \mathrm{Tr}(x) = y$$

„$\supseteq$“: Nehme $a \in K$ mit $\mathrm{Tr}(a) \neq 0$. Dafür $\mathrm{Tr}(a) \in \mathrm{Fix}_K(G)$ gemäß „$\subseteq$“. Für $y \in \mathrm{Fix}_K(G)$ ist also $x = y/\mathrm{Tr}(a) \in \mathrm{Fix}_K(G)$ mit $y = x\,\mathrm{Tr}(a) = \mathrm{Tr}(xa) \in \mathrm{Im}(\mathrm{Tr})$. □

Lemma (Artin)**.** *Ist K ein Körper, und G eine endliche Untergruppe von* $\mathrm{Aut}(K)$*, so ist K galoissch über $k = \mathrm{Fix}_K(G)$ mit* $\mathrm{Gal}(K/k) = G$*, speziell* $[K : k] = |G|$.

Beweis. Es sei $G = \{\sigma_1, \ldots, \sigma_n\}$, $|G| = n$. Für $[K : k] \leq n$ ist zu zeigen: Sind $a_1, \ldots, a_r \in K$ k-linear unabhängig, so ist $r \leq n$. Reicht zu zeigen: Die k-lineare Abbildung $\mu \colon K^r \to K^n, s \mapsto Ms$ mit $M = (\sigma_i^{-1}(a_j))_{i,j} \in K^{n \times r}$ ist injektiv. Dazu sei $s = (y_1, \ldots, y_r)^T \in K^r$ mit $Ms = 0$. Für die Spur $\mathrm{Tr} = \sum_{i=1}^n \sigma_i$ von G in K und $x \in K$ ist

$$\sum_{j=1}^{r} \mathrm{Tr}(xy_j)a_j = \sum_j \sum_i \sigma_i(xy_j)a_j = \sum_i \sum_j a_j\sigma_i(xy_j) = \sum_i \sigma_i\Bigg(x \underbrace{\sum_j \sigma_i^{-1}(a_j)y_j}_{(Ms)_i = 0}\Bigg) = 0$$

also $\mathrm{Tr}(xy_j) = 0$ für alle j [$a_1, \ldots, a_r$ sind k-linear unabhängig und $\mathrm{Tr}(xy_j) \in \mathrm{Im}(\mathrm{Tr}) = \mathrm{Fix}_K(G) = k$]. Nehme $a \in K$ mit $\mathrm{Tr}(a) \neq 0$. Wäre $y_j \neq 0$ für ein j, so wäre $x = a/y_j \in K$ mit $xy_j = a$, also $\mathrm{Tr}(xy_j) \neq 0$ für dieses j, was unmöglich ist. Damit ist $y_1 = \cdots = y_r = 0$, d.h. $s = 0$. Also $[K : k] \leq n$. Mit $G \subseteq \mathrm{Gal}(K/k)$ folgt aus $[K : k] \leq n$, dass $n = |G| \leq |\mathrm{Gal}(K/k)| \leq [K : k] \leq n$, also $G = \mathrm{Gal}(K/k)$ und $|\mathrm{Gal}(K/k)| = [K : k]$, speziell ist K/k galoissch. □

Satz (Erste Charakterisierung der Galoiserweiterungen)**.** *Für jede Körpererweiterung $k \subseteq K$ sind folgende Aussagen äquivalent:*

i) K/k ist galoissch.

ii) K/k ist endlich und $\mathrm{Fix}_K(\mathrm{Gal}(K/k)) = k$.

iii) Es gibt eine endliche Untergruppe G von $\mathrm{Aut}(K)$ mit $\mathrm{Fix}_K(G) = k$.

Bemerkung. $\mathrm{Fix}_K(\mathrm{Gal}(K/k)) = k$ bedeutet, dass $\forall x \in K \setminus k\ \exists \sigma \in \mathrm{Gal}(K/k)\ (\sigma(x) \neq x)$.

Beweis.

i ⇒ ii K/k ist endlich. Nach der Folgerung zum Lemma von Dedekind ist $G = \mathrm{Gal}(K/k)$ endlich. Nach dem Lemma von Artin ist also K galoissch über $\widetilde{k} = \mathrm{Fix}_K(G)$. In $K \subseteq \widetilde{k} \subseteq K$ gilt $[K : \widetilde{k}] = |G| \underset{i}{=} [K : k]$, also $[\widetilde{k} : k] = 1$, d.h. $k = \widetilde{k}$.

ii ⇒ iii Wie oben ist $G = \mathrm{Gal}(K/k)$ endlich.

iii ⇒ i Lemma von Artin. □

Bemerkung. Für G wie in iii) muss $G = \mathrm{Gal}(K/k)$ sein [Lemma von Artin].

Anwendung. Ein Körper K ist genau dann galoissch über seinem Primkörper K_0, wenn K/K_0 endlich und $\mathrm{Fix}_K(\mathrm{Aut}(K)) = K_0$ ist. Dies ist zum Beispiel dann der Fall, wenn K endlich ist, auch für $K = \mathbb{Q}(\sqrt{d})$ und $K = \mathbb{Q}(\sqrt{p} + \sqrt{q})$, jedoch nicht für $K = \mathbb{Q}(\sqrt[3]{p})$.

Korollar. *Für jede endliche Körpererweiterung $k \subseteq K$ ist $|\mathrm{Gal}(K/k)|$ ein Teiler von $[K : k]$ und $\mathrm{Fix}_K(\mathrm{Gal}(K/k))$ ist der kleinste Zwischenkörper von $k \subseteq K$, über dem K galoissch ist.*

Beweis. Mit $G = \mathrm{Gal}(K/k)$, $\widetilde{k} = \mathrm{Fix}_K(G)$ ist G endlich (Folgerung zum Lemma von Dedekind), also $K/\widetilde{k}$ galoissch mit $\mathrm{Gal}(K/\widetilde{k}) = G$ (Lemma von Artin). Speziell: $|G| \mid [K : k]$, genauer: $[K : k] = [K : \widetilde{k}] \cdot [\widetilde{k} : k] = |G| \cdot [\widetilde{k} : k]$. Ist L ein Zwischenkörper mit K/L galoissch, so gilt $\widetilde{k} \subseteq \mathrm{Fix}_K(\mathrm{Gal}(K/L)) = L$ [$G \supseteq \mathrm{Gal}(K/L)$, K/L galoissch, Satz]. □

Satz. *Für Körper $k \subseteq L \subseteq K$ gilt: Ist K/k galoissch, so ist auch K/L galoissch. (Für L/k siehe unten!)*

Beweis. Für $G = \mathrm{Gal}(K/k)$, $H = \mathrm{Gal}(K/L)$ ist $|H| \leq [K : L]$ (Folgerung zum Lemma von Dedekind). Ist $G/H = \{\sigma_1, \ldots, \sigma_r\}$ mit $[G : H] = r$, so sind auch die Ringhomomorphismen $\sigma_i|_L \colon L \to K, x \mapsto \sigma_i(X)$ mit $1 \leq i \leq r$ paarweise verschieden, denn: $\sigma_i|_L = \sigma_j|_L \Leftrightarrow \sigma_j^{-1}\sigma_i \in H \Leftrightarrow \sigma_i H = \sigma_j H$ (beachte $H = \mathrm{Gal}(K/L)$!). Für $L_0 = \{x \in L \colon \sigma_1(X) = \cdots = \sigma_r(x)\}$ ist also $[L : L_0] \geq r$ (Lemma von Dedekind), woraus folgt: $|H| \cdot r = |G| = [K : k] = [K : L] \cdot [L : L_0] \cdot [L_0 : k] \geq [K : L] \cdot r$ [Lagrange, K/k galoissch], d.h. $|H| \geq [K : L]$. □

Satz (Hauptsatz der Galoistheorie)**.** *Es sei $k \subseteq K$ galoissch, $G = \mathrm{Gal}(K/k)$.*

a) Mit $\mathcal{L} = \{L \colon L$ Zwischenkörper von $K/k\}$ und $\mathcal{H} = \{H \colon H$ Untergruppe von $G\}$ sind die Abbildungen

$$\mathcal{L} \to \mathcal{H}, L \mapsto \mathrm{Gal}(K/L) \qquad \mathcal{H} \to \mathcal{L}, H \mapsto \mathrm{Fix}_K(H)$$

zueinander inverse, ordnungsumkehrende Bijektionen. Hier: $\subseteq$ als partielle Ordnung.

b) Für $L \in \mathcal{L}$ mit $H = \mathrm{Gal}(K/L)$:

1) $[K : L] = |H|$ und $[L : k] = [G : H]$.

2) $\forall \sigma \in G \colon (\sigma(L) \subseteq L \Leftrightarrow \sigma \in N_G(H))$.

3) L/k galoissch $\Leftrightarrow H \lhd G$. In diesem Fall ist $\mathrm{Gal}(L/k) \cong G/H$.

Beweis.

a) $L_1 \subseteq L_2 \Rightarrow \mathrm{Gal}(K/L_1) \supseteq \mathrm{Gal}(K/L_2)$; $H_1 \subseteq H_2 \Rightarrow \mathrm{Fix}_K(H_1) \supseteq \mathrm{Fix}_K(H_2)$. Gemäß Lemma von Artin ist $\mathrm{Gal}(K/\mathrm{Fix}_K(H)) = H$ für jedes $H \in \mathcal{H}$. Für jedes $L \in \mathcal{L}$ ist K/L galoissch (voriger Satz), also $\mathrm{Fix}_K(\mathrm{Gal}(K/L)) = L$ (vorvoriger Satz).

b) 1) Wegen K/L galoissch ist $[K : L] = |H|$, also $|H| \cdot [L : k] = [K : k] = |G| = |H| \cdot [G : H]$ [K/k galoissch, Lagrange], d.h. $[L : k] = [G : H]$.

2) Für jedes $\sigma \in G$ gilt $\mathrm{Gal}(K/\sigma(L)) = \sigma H \sigma^{-1}$, denn: Für jedes $\sigma \in G$ gilt $\rho \in \mathrm{Gal}(K/\sigma(L)) \Leftrightarrow \rho\sigma|_L = \sigma|_L \Leftrightarrow \sigma^{-1}\rho\sigma \in H \Leftrightarrow \rho \in \sigma H \sigma^{-1}$. Mit a) folgt für $\sigma \in G$: $\sigma(L) \subseteq L \Leftrightarrow \sigma H \sigma^{-1} \supseteq H \Leftrightarrow \sigma H \sigma^{-1} = H \Leftrightarrow \sigma \in N_G(H)$. Speziell: $\forall \sigma \in G \colon (\sigma(L) \subseteq L) \Leftrightarrow G = N_G(H) \Leftrightarrow H \lhd G$.

3) „⇒“ Es sei $\mathrm{Gal}(L/k) = \{\sigma_1, \ldots, \sigma_r\}$ mit $|\mathrm{Gal}(L/k)| = r$. Wäre $\sigma(L) \not\subseteq L$ für ein $\sigma \in G$, so wäre $L \hookrightarrow K \xrightarrow{\sigma} K$ von jedem $L \hookrightarrow K \xrightarrow{\sigma_i} K$ verschieden. Für $L_0 = \{x \in L \colon \sigma(x) = \sigma_1(x) = \cdots = \sigma_r(x)\}$ wäre dann $[L : L_0] \geq r + 1$ (Lemma von Dedekind), also $[L : k] \geq r + 1$, aber da L/k galoissch nach Voraussetzung ist, ist $[L : k] = r$, was unmöglich ist.

„⇐“ Da $\sigma(L) \subseteq L$ für alle $\sigma \in G$, hat man $\rho \colon G \to \mathrm{Gal}(L/k), \sigma \mapsto \sigma|_L$. Dieses ρ ist ein Gruppenhomomorphismus mit $\mathrm{Ker}(\rho) = H$. Also ist $G/H \cong \mathrm{Im}(\rho) \subseteq \mathrm{Gal}(L/k)$. Es folgt

$$[L : k] \underset{1)}{=} [G : H] = |\,\mathrm{Im}(\rho)| \leq |\,\mathrm{Gal}(L/k)| \leq [L : k]$$

und damit ist L/k galoissch, $\mathrm{Im}(\rho) = \mathrm{Gal}(L/k)$, also $G/H \cong \mathrm{Gal}(L/k)$. □

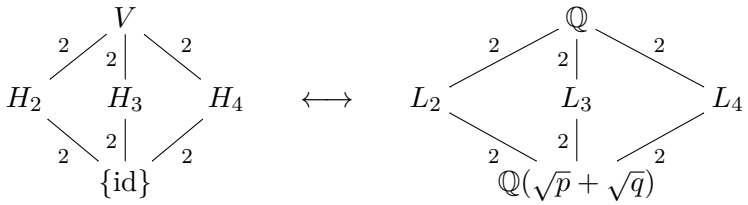
Korollar 1 (Bestimmung des primitiven Elements)**.** *Zu jeder Galoiserweiterung $k \subseteq K$ gibt es ein $a \in K$ mit $K = k(a)$.*

Beweis. Ist k endlich, so ist auch K endlich, also $K^\times$ zyklisch. Aus $K^\times = \langle a \rangle$ folgt $K = k(a)$. Nun sei k unendlich. Im Hauptsatz ist $\mathcal{H}$, also auch $\mathcal{L}$ endlich (dies genügt, zusammen mit k unendlich, für's Folgende). Also: $\{k(a)\colon a \in K\} \subseteq \mathcal{L}$ hat ein bzgl. „$\subseteq$“ maximales Element, etwa $k(a_0)$, wofür $K = k(a_0)$, denn: Für $b \in K$ zeige $b \in k(a_0)$ wie folgt. Die Abbildung $k \to \mathcal{L}, x \mapsto k(a_0 + bx)$ kann nicht injektiv sein. [k ist unendlich, $\mathcal{L}$ aber endlich], also $k(a_0 + bx) = k(a_0 + by)$ für ein $x \neq y$ aus k. Mit $L = k(a_0 + bx)$ ist $L \in \mathcal{L}$ und $b(x - y) = a_0 + bx - (a_0 + by) \in L$, also $b \in L$ und damit $a_0 \in L$, d.h. $k(a_0) \subseteq L$. Also ist $k(a_0) = L$. Speziell ist $b \in k(a_0)$. □

Korollar 2 (Bestimmung des Minimalpolynoms)**.** *Es sei $k \subseteq K$ eine Galoiserweiterung, $[K : k] = n$, $G = \mathrm{Gal}(K/k)$. Für das Minimalpolynom f eines beliebigen $a \in K$ über k gilt $f = \prod_{i=1}^{s}(X - a_i)$, wobei $\{a_1, \ldots, a_s\} = \{\sigma(a)\colon \sigma \in G\}$ mit $a_i \neq a_j$ für $i \neq j$. Insbesondere zerfällt f in $K[X]$ in paarweise verschiedene Linearfaktoren.*

Beweis. G operiert auf K durch $G \times K \to K, (\sigma, x) \mapsto \sigma(x)$. Aus $S(a) = \{\sigma \in G\colon \sigma(a) = a\} = \mathrm{Gal}(K/k(a))$ folgt mit b.1) des Hauptsatzes: $[k(a) : k] = [G : S(a)]$, d.h. $\deg(f) = |B(a)| = s$ wegen $B(a) = \{\sigma(a)\colon \sigma \in G\} = \{a_1, \ldots, a_s\}$. Wegen $f \in k[X]$ ist $f(\sigma(a)) = \sigma(f(a))$ für jedes $\sigma \in G$. Mit $f(a) = 0$ folgt $f(a_i) = 0$ für alle i. Also ist $f = g \cdot \prod_{i=1}^{s}(X - a_i)$ in $K[X]$, worin $g = 1$ wegen $\deg(f) = s$ und f normiert. □

Beispiel. $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{p} + \sqrt{q})$ wie in Beispiel 3). Wir wissen $G = \mathrm{Gal}(\mathbb{Q}(\sqrt{p} + \sqrt{q})/\mathbb{Q}) = \{\mathrm{id}, \sigma_2, \sigma_3, \sigma_4\} \cong V$. V hat die drei nichttrivialen Untergrupppen $H_i = \{\mathrm{id}, \sigma_i\}$ mit $i \in \{2, 3, 4\}$. Diese entsprechen den Zwischenkörpern $L_2 = \mathbb{Q}(\sqrt{q})$, $L_3 = \mathbb{Q}(\sqrt{p})$, $L_4 = \mathbb{Q}(\sqrt{pq})$.



Das Minimalpolynom von $a = \sqrt{p} + \sqrt{q}$:

über $\mathbb{Q}$:	$(X - a)(X - \sigma_2(a))(X - \sigma_3(a))(X - \sigma_4(a)) =$ $= X^4 - 2(p + q)X^2 + (p - q)^2$
über $L_2 = \mathbb{Q}(\sqrt{q})$:	$(X - a)(X - \sigma_2(a)) = X^2 - 2\sqrt{q}X + q - p$
über $L_3 = \mathbb{Q}(\sqrt{p})$:	$(X - a)(X - \sigma_3(a)) = X^2 - 2\sqrt{p}X + p - q$
über $L_4 = \mathbb{Q}(\sqrt{pq})$:	$(X - a)(X - \sigma_4(a)) = X^2 - p + q + 2\sqrt{pq}$
über $\mathbb{Q}(\sqrt{p} + \sqrt{q})$:	$X - a = X - (\sqrt{p} + \sqrt{q})$

Korollar 3 (Bestimmung des Fixkörpers)**.** *Sei K/k eine Galoiserweiterung und sei H eine Untergruppe von* $\mathrm{Gal}(K/k)$*. Sei $K = k(a)$ und $\prod_{\sigma \in H}(X - \sigma(a)) = X^m + c_{m-1}X^{m-1} + \cdots + c_0 \in K[X]$. Dann ist* $\mathrm{Fix}_K(H) = k(c_0, \ldots, c_{m-1})$*.*

Beweis. Aus $K = k(a)$ folgt $\sigma(a) \neq \tau(a)$ für $\sigma \neq \tau \in \mathrm{Gal}(K/k)$. Weil K über $L := \mathrm{Fix}_K(H)$ galoissch ist mit $\mathrm{Gal}(K/L) = H$ ist nach Korollar 2 $g := \prod_{\sigma \in H}(X - \sigma(a))$ das Minimalpolynom von a über L. Insbesondere liegen die Koeffizienten $c_0, \ldots, c_{m-1}$ von g in L, also $L' := k(c_0, \ldots, c_{m-1}) \subseteq L$. Andererseits ist $g \in L'[X]$ auch das Minimalpolynom von a über L' [da immer noch normiert, a ist Nullstelle, irreduzibel]. Also $[K : L] = \deg g = [K : L'] \Rightarrow L' = L$. □

3.2 Zerfällungskörper

Definition. Sei K/k eine Körpererweiterung und $f \in k[X]$ nichtkonstant. K heißt *Zerfällungskörper* von f über k, falls f über K in Linearfaktoren zerfällt und f über keinem echten Zwischenkörper $k \subseteq L \subsetneq K$ in Linearfaktoren zerfällt.

Beispiel. $\mathbb{C}$ ist ein Zerfällungskörper von $X^2 + 1$ über $\mathbb{R}$.

Bemerkung. Zu jedem nichtkonstanten $f \in k[X]$ existiert ein Zerfällungskörper von f über k.

Beweis. Wählt man nach dem Lemma von Kronecker (Abschnitt 2.5) eine Körpererweiterung E/k mit $f = c(X - a_1) \cdots (X - a_n)$ mit $a_1, \ldots, a_n \in E$ und $c \in k$, so leistet $K := k(a_1, \ldots, a_n)$ das Gewünschte [denn ist $k \subseteq L \subseteq K$ und $a_1', \ldots, a_n' \in L$ mit $f = c(X - a_1') \cdots (X - a_n')$, so ist $a_i \in \{a_1', \ldots, a_n'\} \subseteq L$ für alle i. Also folgt $K = k(a_1, \ldots, a_n) \subseteq L$, also $K = L$.] □

Bemerkung. K Zerfällungskörper von f über k, $n = \deg f \geq 1$. Dann gilt $[K : k] \mid n!$.

Beweis. Durch Induktion nach n. $n = 1$: Klar ($1 \mid 1!$). $n > 1$: Wir nehmen an, dass die Aussage für alle Polynome g (über beliebigen Körpern) von Grad kleiner als n gilt. Sei α eine Nullstelle von f in $K \setminus k$ (o.B.d.A., da $1 \mid n!\ \forall n$). Fall 1: $[k(\alpha) : k] = n$. Schreibe $f = (X - \alpha)g$ mit $g \in k(\alpha)[X]$. Also ist K ein Zerfällungskörper von g über $k(\alpha)$. Nach Induktionsvoraussetzung gilt $[K : k(\alpha)] \mid (n-1)!$, also $[K : k] = [K : k(\alpha)] \cdot [k(\alpha) : k] = [K : k(\alpha)] \cdot n \mid n!$. Fall 2: $[k(\alpha) : k] < n$: Sei g das Minimalpolynom von α über k. $1 \leq \deg g = [k(\alpha) : k] < n$. Sei L der Zerfällungskörper von g über k. Dann $[L : k] \mid (\deg g)!$ nach Induktionsvoraussetzung. Wegen $f(\alpha) = 0$ existiert $h \in k[X]$ mit $f = gh$. K ist der Zerfällungskörper von h über L. Mit $\deg h < n$ und der Induktionsvoraussetzung folgt nun $[K : L] \mid (\deg h)!$, also $[K : k] = [K : L] \cdot [L : k] \mid (\deg h)!(\deg g)! \mid n!$. Also $[K : k] \mid n!$. □

Beispiel.

1) $\mathbb{C}$ ist Zerfällungskörper von $X^2 + 1$ über $\mathbb{R}$.

2) $f = X^3 - p$ (p Primzahl) hat in $\mathbb{C}$ die 3 Nullstellen $\sqrt[3]{p} \in \mathbb{R}$, $\zeta\sqrt[3]{p}$, $\zeta^2\sqrt[3]{p}$ mit $\zeta = e^{2\pi i/3} = \frac{-1+\sqrt{-3}}{2}$. Damit ist der Zerfällungskörper von f über $\mathbb{Q}$ gleich $\mathbb{Q}(\sqrt[3]{p}, \zeta\sqrt[3]{p}, \zeta^2\sqrt[3]{p}) = \mathbb{Q}(\sqrt[3]{p}, \zeta)$. Wegen $[\mathbb{Q}(\sqrt[3]{p} : \mathbb{Q}] = 3$ [f ist irreduzibel wegen Eisenstein] und $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$ [$X^2 + X + 1$ ist das Minimalpolynom] ist $[\mathbb{Q}(\sqrt[3]{p}, \zeta) : \mathbb{Q}] = 2 \cdot 3 = 6$ [2, 3 sind teilerfremd].

3) Sei K der Zerfällungskörper von $f = X^3 - 3X - 1$ über $\mathbb{Q}$. Dann ist $[K : \mathbb{Q}] = 3$ [Beweis: Übungsblatt 13].

Definition. Für einen Ringhomomorphismus $\varphi\colon R \to S$ und $g \in R[X]$, $g = \sum_{i=0}^{n} r_i X^i$, $r_i \in R$ definiere ${}^{\varphi}g := \sum_{i=0}^{n} \varphi(r_i) X^i$. Damit ist $R[X] \to S[X], g \mapsto {}^{\varphi}g$ ein Ringhomomorphismus (vgl. Reduktion mod p) und für Ringhomomorphismen $R \xrightarrow{\varphi} S \xrightarrow{\psi} T$, $g \in R[X]$ gilt ${}^{\psi}({}^{\varphi}g) = {}^{(\psi\circ\varphi)}g$.

Bemerkung. Insbesondere erhält man für eine Körpererweiterung K/k eine Operation der Gruppe $\mathrm{Gal}(K/k)$ auf $K[X]$ und die Fixpunkte dieser Operation sind gerade die Elemente von $k[X]$, sofern K/k galoissch ist (vgl. Übungsblatt 11).

Lemma. *Sei $\varphi\colon k \to k'$ ein Homomorphismus von Körpern und K/k eine* endliche *Körpererweiterung. Dann gibt es eine endliche Körperweiterung K'/k' und einen Körperhomomorphismus $\psi\colon K \to K'$mit $\psi(x) = \varphi(x)$ für alle $x \in k$, d.h. das folgende Diagramm kommutiert:*

$$\begin{array}{ccc} k & \hookrightarrow & K \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\psi} \\ k' & \longrightarrow & K' \end{array}$$

Beweis. Sei $K = k(a_1, \ldots, a_n)$ und sei f das Minimalpolynom von a_1 über k. Sei $\alpha\colon k[X]/(f) \to k(a_1), \overline{p} \mapsto p(a_1)$ der Isomorphismus aus Abschnitt 2.5 und sei g ein irreduzibler teiler von ${}^{\varphi}f \in k'[X]$. Dann erhalten wir aus $k[X] \to k'[X]/(g), p \mapsto \overline{{}^{\varphi}p}$ einen Körperhomomorphismus $k[X]/(f) \to k'[X]/(g) =: E_1$, also mit

$$\varphi_1 := \beta \circ \alpha^{-1}\colon k(a_1) \xrightarrow{\alpha^{-1}} k[X]/(f) \xrightarrow{\beta} k'[X]/(g) = E_1$$

das kommutative Diagramm

$$\begin{array}{ccc} k & \hookrightarrow & k(a_1) \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi_1} \\ k' & \longrightarrow & E_1 \end{array}$$

Durch Iteration dieses Verfahrens erhalten wir schließlich

$$\begin{array}{ccccccccc} k & \hookrightarrow & k(a_1) & \hookrightarrow & k(a_1,a_2) & \hookrightarrow & \ldots & \hookrightarrow & k(a_1,\ldots,a_n) = K \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi_1} & & \downarrow{\scriptstyle\varphi_2} & & & & \downarrow{\scriptstyle\psi:=\varphi_n} \\ k' & \longrightarrow & E_1 & \longrightarrow & E_2 & \longrightarrow & \ldots & \longrightarrow & E_n =: K' \end{array}$$

was der Aussage zum obigen geforderten Diagramm entspricht. □

Definition. Ein Körper k heißt *algebraisch abgeschlossen*, falls jedes nicht-konstante $f \in k[X]$ in Linearfaktoren zerfällt.

Beispiel. $k = \mathbb{C}$ ist algebraisch abgeschlossen.

Bemerkung. Für einen algebraisch abgeschlossenen Körper k gilt für jede algebraische Körpererweiterung K/k, dass $K = k$ ist, denn das Minimalpolynom von $a \in K$ über k hat Grad 1, also $a \in k$.

Korollar 1. *Sei $\varphi\colon k \to k'$ ein Homomorphismus von Körpern, k' algebraisch abgeschlossen und K/k eine endliche Körpererweiterung. Dann gibt es einen Homomorphismus $\psi\colon K \to k'$ mit $\psi|_k = \varphi$.*

Beweis. Im Lemma ist $K' = k'$, also kommutiert

$$\begin{array}{ccc} k & \hookrightarrow & K \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\psi} \\ k' & = & K' \end{array}$$

d.h. $\psi|_k = \varphi$. □

Bemerkung. Mit $k' = \mathbb{C}$ folgt, dass jede endliche Körpererweiterung k von $\mathbb{Q}$ isomorph zu einem Unterkörper von $\mathbb{C}$ ist.

Beweis. Wähle $\varphi\colon \mathbb{Q} \hookrightarrow \mathbb{C}$ die Inklusion. Dann kommutiert

$$\begin{array}{ccc} \mathbb{Q} & \hookrightarrow & K \\ {\scriptstyle\varphi}\downarrow & \swarrow{\scriptstyle\psi} & \\ \mathbb{C} & & \end{array}$$

Also ist $K \cong \psi(K) \subseteq \mathbb{C}$ eine Unterkörper. □

Bemerkung. Ohne "algebraisch abgeschlossen" stimmt Korollar 1 nicht. Zum Beispiel

$$\begin{array}{ccc} \mathbb{R} & \hookrightarrow & \mathbb{C} \\ \| & \swarrow{\scriptstyle\neg\exists\psi} & \\ \mathbb{R} & & \end{array}$$

denn sonst wäre $0 = \psi(i^2 + 1) = \psi(i)^2 + 1 > 0$.

Korollar 2. *Sei $f \in k[X]$ nicht-konstant, K ein Zerfällungskörper von f über k und $\varphi\colon k \xrightarrow{\sim} k'$ ein Körperisomorphismus und sei K' ein Zerfällungskörper von ${}^{\varphi}f$ über k'. Dann gibt es einen Isomorphismus $\psi\colon K \xrightarrow{\sim} K'$ mit $\psi(x) = \varphi(x)$ für alle $x \in k$, d.h.*

$$\begin{array}{ccc} k & \hookrightarrow & K \\ {\scriptstyle\varphi}\downarrow{\scriptstyle\sim} & & {\scriptstyle\sim}\downarrow{\scriptstyle\psi} \\ k' & \hookrightarrow & K' \end{array}$$

Beweis. Nach dem Lemma existiert ein kommutatives Diagram

$$\begin{array}{ccc} k & \hookrightarrow & K \\ {\scriptstyle\varphi}\downarrow{\scriptstyle\sim} & & \\ k' & & \downarrow{\scriptstyle\psi} \\ \downarrow & & \\ K' & \hookrightarrow & E \end{array}$$

mit einer endlichen Körpererweiterung E/K'. Es genügt zu zeigen, dass $\psi(K) = K'$. Schreibe $f = c \cdot (X - a_1) \dots (X - a_n)$ mit $c \in k$ und $a_1, \dots, a_n \in K$. Dann ist $K = k(a_1, \dots, a_n)$. Sei nun $b_i = \psi(a_i) \in E$ für $i = 1, \dots, n$. Dann ist $\psi(K) = k'(b_1, \dots, b_n)$. Aus ${}^{\varphi}f = {}^{\psi}f = \varphi(c)(X - b_1) \dots (X - b_n)$ folgt, dass alle b_i Nullstellen von ${}^{\varphi}f$ sind, also $b_i \in K'$ für alle i, also $\psi(K) = k'(b_1, \dots, b_n) \subseteq K'$. Umgekehrt ist $k' = \varphi(k) \subseteq \psi(K)$ und, da ${}^{\varphi}f$ in Linearfaktoren über $\psi(K)$ zerfällt, $\psi(K) \supseteq K'$. □

Bemerkung. Speziell folgt mit $\varphi = \mathrm{id}$: Sind K_1 und K_2 Zerfällungskörper von f über k, so sind K_1 und K_2 isomorph.

Satz (Beschreibung der endlichen Körper)**.** *Sei p eine Primzahl, $n \geq 1$ und K ein Zerfällungskörper von $f = X^{p^n} - X$ über $\mathbb{Z}/p\mathbb{Z} =: \mathbb{F}_p$. Dann gilt:*

1) K besitzt p^n Elemente.

2) Jeder Körper mit p^n Elementen ist isomorph zu K.

3) Ist L ein Unterkörper von K, $|L| = p^m$, so ist $m \mid n$.

4) Umgekehrt gibt es zu jedem Teiler m von n genau einen Unterkörper L von K mit p^m Elementen, nämlich $L = \{x \in K \colon x^{p^m} = x\}$.

Beweis. Die Nullstellen von $f = X^{p^n} - X$ in K bilden einen Körper, nämlich $\{x \in K \colon f(x) = 0\} = \mathrm{Fix}_K(\langle F^n \rangle)$, wobei $F \colon K \to K, x \mapsto x^p$ der Frobeniushomomorphismus ist. Da K Zerfällungskörper von f über $\mathbb{F}_p$ ist, folgt $K = \{x \in K \colon f(x) = 0\} = \{a_1, \dots, a_d\}$ mit $f = c \cdot (X - a_1) \dots (X - a_d)$, $a_i \in K$, $d = p^n$. Die a_i sind paarweise verschieden, denn wäre $f = (X - a)^2 g$, $g \in K[X]$, so wäre $-1 = p^n X^{p^n} - 1 = f' = (X - a)h$ für ein $h \in K[X]$. Es folgt $|K| = d = p^n$.

Sei E ein Körper mit p^n Elementen und sei E_0 sein Primkörper. Dann ist $E_0 \cong \mathbb{F}_p$ und alle $y \in E$ sind Nullstellen von f, denn $E^\times$ ist zyklisch von Ordnung $p^n - 1$. Also ist E ein Zerfällungskörper von f über $E_0 \cong \mathbb{F}_p$. Also folgt mit Korollar 2 $K \cong E$.

Nach der Gradformel ist $m = [L : K_0]$ ein Teiler von $n = [K : K_0]$, d.h. $m \mid n$.

$$\begin{array}{ccc} \langle F \rangle & & K_0 \\ {\scriptstyle m}\big| & & \big|{\scriptstyle m} \\ \langle F^m \rangle & \longleftrightarrow & L \\ {\scriptstyle \frac{n}{m}}\big| & & \big|{\scriptstyle \frac{n}{m}} \\ \{e\} & & K \end{array}$$

In Abschnitt 3.1 wurde gezeigt, dass K/K_0 galoissch ist mit $\mathrm{Gal}(K/K_0) = \langle F \rangle \cong \mathbb{Z}/n\mathbb{Z}$. Da $\langle F \rangle \cong \mathbb{Z}/n\mathbb{Z}$ für $m \mid n$ genau eine Untergruppe von Index m hat, nämlich $\langle F^m \rangle$, gibt es genau einen Zwischenkörper $K_0 \subseteq L \subseteq K$ von Grad m über K_0, nämlich $L = \mathrm{Fix}_K(\langle F^m \rangle) = \{x \in K \colon x^{p^m} = x\}$. □

Korollar 1. *Sei K ein endlicher Körper der Charakteristik p und sei $F \colon K \to K, x \mapsto x^p$ der Frobeniushomomorphismus.*

a) Ist L Unterkörper von K mit $|L| = p^m$, so folgt, dass K/L eine Galoiserweiterung ist mit $\mathrm{Gal}(K/L) = \langle F^m \rangle$.

b) Sind L_1, L_2 Unterkörper von K mit $|L_i| = p^{m_i}$ für $i = 1, 2$, so gilt $L_1 \subseteq L_2 \Leftrightarrow m_1 | m_2$.

Beweis. $L = \mathrm{Fix}_K(\langle F^m \rangle)$, also ist K/L galoissch und $\mathrm{Gal}(K/L) = \langle F^m \rangle$. In b) folgt "⇒" aus 3). Sei umgekehrt $m_1 \mid m_2$. Ist dann $x^{p^{m_1}} = x$, so auch $x^{p^{m_2}} = x$, d.h. mit 4) ist $L_1 \subseteq L_2$. □

Beobachtung. Es sei p eine Primzahl. Zu jedem $n \geq 1$ gibt es bis auf Isomorphie genau einen Körper mit p^n Elementen. Dieser heißt *Galoisfeld* der Ordnung p^n und wird mit $\mathbb{F}_{p^n}$ bezeichnet. Für Primzahlen p, q und $n, m \geq 1$ gibt es genau dann einen Ringhomomorphismus $\mathbb{F}_{q^m} \to \mathbb{F}_{p^n}$, wenn $p = q$ und $m \mid n$ ist. In diesem Fall kann man $\mathbb{F}_{p^m}$ als Unterkörper von $\mathbb{F}_{p^n}$ auffassen. Damit ist $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$ galoissch mit $[\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] = n/m$, $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}) = \langle F^m \rangle$, wobei F der Frobeniushomomorphismus auf $\mathbb{F}_{p^n}$.

Korollar 2. *Ist k ein endlicher Körper, so gibt es zu jedem $l \geq 1$ ein irreduzibles $f \in k[X]$ mit* $\deg f = l$. *Speziell ist* kein *endlicher Körper algebraisch abgeschlossen.*

Beweis. Übung.

Definition. Eine algebraische Körpererweiterung $k \subseteq K$ heißt *normal*, wenn für jedes $a \in K$ das Minimalpolynom $f \in k[X]$ von a über k in $K[X]$ in Linearfaktoren zerfällt.

Bemerkung.

a) Jede Galoiserweiterung K/k ist normal.

b) Ist $k \subseteq K$ eine normale Körpererweiterung und L ein Zwischenkörper, so ist auch $L \subseteq K$ normal.

Beweis.

a) Es sei $a \in K$ und f das Minimalpolynom von a über k. Nach Korollar 2 zum Hauptsatz ist $f = \prod_{i=1}^{s}(X - a_i)$ mit $a_1, \ldots, a_s$ paarweise verschieden, $\{a_1, \ldots, a_s\} = \{\sigma(a) \colon \sigma \in \mathrm{Gal}(K/k)\}$.

b) Es sei $a \in K$. Für die Minimalpolynome f und g von a über k bzw. über L gilt $g \mid f$ in $L[X]$. Aus $f = \prod_{i=1}^{s}(X - a_i)$ in $K[X]$ folgt $g = \prod_{i=1}^{r}(X - a_i)$ mit $r \leq s$. □

Beispiel.

1) Jede Körpererweiterung K/k vom Grad 2 ist normal. [Für jedes $a \in K \setminus k$ ist $k(a) = K$, also $\deg(f) = 2$ für das Minimalpolynom f von a über k, d.h. in $f = (X-a)h$ mit $h \in K[X]$ hat h Grad 1.]

2) $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{p})$ ist nicht normal. [Das Minimalpolynom $X^3 - p$ von $\sqrt[3]{p}$ über $\mathbb{Q}$ hat $\sqrt[3]{p}$ als einzige reelle Nullstelle, zerfällt nicht in $\mathbb{Q}(\sqrt[3]{p})$.]

3) $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{p})$ und $\mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(\sqrt[4]{p})$ sind beide normal [Grad 2], aber $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{p})$ ist nicht normal. [Das Minimalpolynom von $a = \sqrt[4]{p}$ über $\mathbb{Q}$ ist $X^4 - p = X^4 - a^4 = (X^2 - a^2)(X^2 + a^2) = (X+a)(X-a)(X^2+a^2)$, aber $X^2 + a^2 = X^2 + \sqrt{p}$ hat keine reellen Nullstellen, ist also in $\mathbb{Q}(\sqrt[4]{p})$ irreduzibel.]

Lemma. *Es sei $k \subseteq K$ eine Körpererweiterung. Für jedes $f \in k[X] \setminus k$ ist K genau dann ein Zerfällungskörper von f über k, wenn es $b_1, \ldots, b_m \in K$ gibt, sodass $f = c \cdot \prod_{j=1}^{m}(X - b_j)$ für ein $c \in k^\times$ und $K = k(b_1, \ldots, b_m)$.*

Beweis. Übung.

Folgerung 1. Ist K ein Zerfällungskörper von $f \in k[X]$ über k, so ist K auch ein Zerfällungskörper von f über jedem Zwischenkörper L von $k \subseteq K$. [Im Lemma kann man k durch L ersetzen.]

Folgerung 2. Es sei $k \subseteq K$ eine Körpererweiterung, $K = k(a_1, \ldots, a_n)$, $f \in k[X]$. Zerfällt f in $K[X]$ und sind $a_1, \ldots, a_n$ Nullstellen von f, so ist K ein Zerfällungskörper von f über k. [Mit $b_1, \ldots, b_m$ wie im Lemma ist $\{a_1, \ldots, a_n\} \subseteq \{b_1, \ldots, b_m\}$, also $K = k(b_1, \ldots, b_n)$.]

Satz. *Eine Körpererweiterung $k \subseteq K$ ist genau dann endlich und normal, wenn K ein Zerfällungskörper eines $f \in K[X] \setminus k$ ist.*

Beweis. $\Rightarrow$ Da K/k endlich ist, ist $K = k(a_1, \ldots, a_n)$ mit $a_1, \ldots, a_n$ algebraisch über k. Da K/k normal ist, zerfällt das Minimalpolynom $f_i \in k[X]$ von a_i in $K[X]$ für $1 \leq i \leq n$, also zerfällt auch $f = \prod_{i=1}^{s} f_i$ in $K[X]$. Nach Folgerung 2 ist K ein Zerfällungskörper von f über k.

$\Leftarrow$ Es sei $g \in k[X]$ das Minimalpolynom eines beliebigen $a \in K$, und E der Zerfällungskörper von g über K (!). Für jedes $b \in E$ mit $g(b) = 0$ ist g auch das Minimalpolynom von b über k. Man hat also bijektive Ringhomomorphismen $\varphi\colon k(a) \underset{\cong}{\to} k[X]/(g) \underset{\cong}{\to} k(b)$, $a \leftarrow\!\shortmid \overline{X} \mapsto b$. Nach Folgerung 1 ist K ein Zerfällungskörper von f über $k(a)$ und $K(b)$ ein Zerfällungskörper von f über $k(b)$. Man hat also das kommutative Diagramm

$$\begin{array}{ccccc} k & \hookrightarrow & k(a) & \hookrightarrow & K \\ \| & & \downarrow{\scriptstyle \varphi \mid \cong} & & \downarrow{\scriptstyle \psi \mid \cong} \\ k & \hookrightarrow & k(b) & \hookrightarrow & K(b) \end{array}$$

und weiß dann $[K : k] = [K(b) : k]$, weshalb „=“ in $K \subseteq K(b)$, d.h. $b \in K$. $\square$

Korollar 3. *Zu jeder endlichen Körpererweiterung $k \subseteq K$ gibt es eine Körpererweiterung $K \subseteq E$, sodass $k \subseteq E$ endlich und normal ist.*

Beweis. Es sei $K = k(a_1, \ldots, a_n)$ und f_i das Minimalpolynom von a_i über k. $(1 \leq i \leq n)$, sowie $f = \prod_{i=1}^{n} f_i$. Jeder Zerfällungskörper E von f über K (!) ist wie verlangt, denn: Nach Lemma ist $E = K(b_1, \ldots, b_m)$ mit $f = \prod_{j=1}^{m}(X - b_j)$ in $E[X]$. Wegen $\{a_1, \ldots, a_n\} \subseteq \{b_1, \ldots, b_m\}$ ist sogar $E = k(b_1, \ldots, b_m)$, d.h. nach Lemma: E ist ein Zerfällungskörper von f über k (!), also E/k endlich, normal (Satz). □

Korollar 4. *Ist K/k endlich (und normal), so haben $a, b \in K$ (genau) dann dasselbe Minimalpolynom, wenn $\sigma(a) = b$ ist für ein $\sigma \in \mathrm{Gal}(K/k)$.*

Beweis.

„dann“ Für das Minimalpolynom g von a über k ist $g(b) = g(\sigma(a)) = {}^{\sigma}g(\sigma(a)) = \sigma(g(a)) = \sigma(0) = 0$, also g auch das Minimalpolynom von b über k.

„genau dann“ Ist $g \in k[X]$ das Minimalpolynom von a und b, so hat man $\varphi\colon k(a) \xrightarrow[\cong]{} k[X]/(g) \xrightarrow[\cong]{} k(b), a \leftarrow\!\shortmid \overline{X} \mapsto b$, speziell $\varphi(a) = b$. Nach Satz 1 ist K ein Zerfällungskörper über k eines $f \in k[X] \setminus k$. Nach Folgerung 1 ist K dies auch über $k(a)$ und $k(b)$. Man hat also ein kommutatives Diagramm

$$\begin{array}{ccccc} k & \hookrightarrow & k(a) & \hookrightarrow & K \\ \| & & \varphi \downarrow \cong & & \sigma \mid \cong \\ \| & & & & \downarrow \\ k & \hookrightarrow & k(b) & \hookrightarrow & K \end{array}$$

worin $\sigma \in \mathrm{Gal}(K/k)$ und $\sigma(a) = \varphi(a) = b$.

□

Definition. Es sei $k \subseteq K$ eine Körpererweiterung, $f \in k[X]$, $n \geq 1$. Man nennt $a \in K$ eine *n-fache Nullstelle* von f in K, wenn $(X - a)^n \mid f$ und $(X - a)^{n+1} \nmid f$ in $K[X]$. Ist dies für irgendein $n \geq 2$ der Fall, so heißt *a mehrfache Nullstelle* von f in K.

Lemma. *Es sei $k \subseteq K$ eine Körpererweiterung, $f \in k[X] \setminus k$. Genau dann hat f in K eine mehrfache Nullstelle, wenn f und f' (formale Ableitung) in K eine gemeinsame Nullstelle haben.*

Beweis. Übung.

Satz. *Für jedes $f \in k[X] \setminus k$ sind äquivalent*

i) f hat in keiner Erweiterung K/k eine mehrfache Nullstelle.

ii) Es gibt eine Erweiterung K/k, sodass $f = c \cdot \prod_{i=1}^{m}(X - b_i)$ mit $c \in k^{\times}$, $b_1, \ldots, b_m \in K$ paarweise verschieden.

iii) f und f' sind teilerfremd in $k[X]$.

Aus i), ii) oder iii) folgt

iv) $f' \neq 0$

Ist f irreduzibel, so ist iv) äquivalent zu i), ii) und iii).

Beweis. **i** $\Rightarrow$ **ii** Nehme für K einen Zerfällungskörper von f.

ii $\Rightarrow$ **iii** Mit $f_j = c \cdot \prod_{i \neq j}(X - b_i)$ für $1 \leq j \leq m$ ist $f = (X - b_j)f_j$, also $f' = f_j + (X - b_j)f_j'$, also $f'(b_j) = f_j(b_j) \neq 0$. Nun sei g ein gemeinsamer von f, f' in $k[X]$. Klar: $g \neq 0$. Wäre $g \notin k^\times$, also $g \in k[X] \setminus k$, so hätte g eine Nullstelle a in einer Erweiterung K_1/k, wofür $f(a) = 0$, d.h. $a = b_j$ für ein j, und $f'(a) = 0$, aber $f'(a) = f'(b_j) \neq 0$, unmöglich. Also muss $g \in k^\times$ sein.

iii $\Rightarrow$ **iv** Da $k[X]$ ein Hauptidealring ist, hat man $1 = fh + f'h_1$ in $k[X]$, woraus folgt $f' \neq 0$ $[f' = 0 \Rightarrow f \in k^\times]$.

iii $\Rightarrow$ **i** Wie oben hat man $1 = fh + f'h_1$ in $k[X]$. Gäbe es $K \supseteq k$, $a \in K$ mit $f(a) = 0 = f'(0)$, so folgt $1 = 0$, was unmöglich ist.

iv $\Rightarrow$ **iii** für f irreduzibel: Es sei g ein gemeinsamer Teiler von f, f' in $k[X]$. Klar(wie oben): $g \neq 0$. Wegen $\deg(g) \leq \deg(f') < \deg(f)$ ist $g \not\sim f$, also $g \in k^\times$. □

Definition. Ein Polynom $f \in k[X] \setminus k$ heißt *separabel*, wenn für jeden irreduziblen Teiler g von f gilt: g hat in keiner Erweiterung $K \supseteq k$ eine mehrfache Nullstelle.

Beispiel.

1) $f = (X - r)^n$ ist seperabel ($r \in k$, $n \geq 1$).

2) $f = X^{p^n} - X \in \mathbb{F}_p[X]$ ist sperabel ($n \geq 1$), denn: $f' = -1$, also f, f' teilerfremd.

Korollar 1. *Ein irreduzibles Polynom $f \in k[X]$ ist genau dann separabel, wenn $f' \neq 0$ ist.*

Korollar 2. *Ist a) k algebraisch abgeschlossen oder b)* $\mathrm{char}(k) = 0$*, so ist jedes $f \in k[X] \setminus k$ separabel.*

Beweis. O.B.d.A. ist f irreduzibel. a) $\deg(f) = 1$. b) $f = \sum_{i=0}^{n} r_i X^i$ mit $r_i \in k$, $n \geq 1$, $r_n \neq 0 \Longrightarrow f' = nr_n X^{n-1} + \ldots$ mit $nr_n \neq 0$. □

Bemerkung.

a) Genau dann sind $f_1, \ldots, f_m \in k[X] \setminus k$ alle separabel, wenn $f = f_1 \cdots f_m \in k[X]$ separabel ist.

b) Ist $f \in k[X] \setminus k$ separabel und $K \supseteq k$ eine Erweiterung, so ist f auch in $K[X]$ separabel.

Beweis.

a) Die irreduziblen Teiler von f sind genau die irreduziblen Teiler der $f_1, \ldots, f_m$.

b) Schreibe $f = f_1 \cdots f_m$ mit $f_1, \ldots, f_m$ irreduzibel. Ist $g \in K[X]$ irreduzibel und $g \mid f$ in $K[X]$, d.h. $f \mid f_i$ in $K[X]$ für ein i, so kann g in keiner Erweiterung $E \supseteq K$ eine mehrfache Nullstelle haben, denn sonst hätte f_i eine solche in $E \supseteq k$, was unmöglich ist. □

Definition. Eine algebraische Körpererweiterung $k \subseteq K$ heißt *separabel*, wenn für jedes $a \in K$ das Minimalpolynom f von a über k in $K[X]$ separabel ist (d.h. $f' \neq 0$).

Folgerung. Ist $k \subseteq K$ eine separable Körpererweiterung, und L ein Zwischenkörper, so sind auch $k \subseteq L$ und $L \subseteq K$ separabel.

Beweis. Übung.

Satz (Zweite Charakterisierung von Galoiserweiterungen)**.** *Für jede Körpererweiterung $k \subseteq K$ sind äquivalent:*

i) K/k ist eine Galoiserweiterung

ii) K/k ist endlich, normal und separabel.

iii) K ist Zerfällungskörper eines separablen $f \in k[X]$.

Beweis. **i** ⇒ **ii** Endlich und normal ist klar. Sei $f \in k[X]$ das Minimalpolynom eines $a \in K$. Nach Korollar 2 zum Hauptsatz ist $f = \prod_{i=1}^{s}(X - a_i)$ mit $a_1, \ldots, a_s$ paarweise verschieden. Nach Satz ist f separabel.

ii ⇒ **iii** Es sei $K = k(a_1, \ldots, a_n)$ und f_i das Minimalpolynom von a_i über k. Nach Beweis des vorvorigen Satzes ist K Zerfällungskörper von $f = f_1 \cdots f_n$ über k. Nach Voraussetzung sind $f_1, \ldots, f_n$ alle separabel, also ist auch f separabel gemäß Bemerkung a).

iii ⇒ **i** Induktion nach $m = |\{a \in K \setminus k \colon f(a) = 0\}|$. $m = 0$: $K = k$. $m > 0$: Nehme $a \in K \setminus k$ mit $f(a) = 0$, betrachte $L = k(a)$. Nach Induktion ist K/L galoissch, denn: K ist auch Zerfällungskörper von f über L, und f ist auch separabel in $L[X]$; ferner $|\{b \in K \setminus L \colon f(b) = 0\}| < m$. Für „$K/k$ galoissch“ ist nach der 1. Charakterisierung von Galoiserweiterungen zu zeigen: $\mathrm{Fix}_K(G) = k$ für $G = \mathrm{Gal}(K/k)$. DArin ist nur „$\subseteq$“ zu zeigen. Es sei g das Minimalpolynom von a über k, $n = \deg(g)$. Ist $x \in \mathrm{Fix}_K(G)$, so ist $x \in \mathrm{Fix}_K(\mathrm{Gal}(K/L)) = L$, denn K/L galoissch, d.h. $x = \sum_{i=0}^{n-1} r_i a^i$ mit $r_i \in k$. Da K/k normal ist, hat man $g = \prod_{j=1}^{n}(X - b_j)$ mit $b_1, \ldots, b_n \in K$. Da f separabel, $g \mid f$, g irreduzibel, ist $|\{b_1, \ldots, b_n\}| = n$. Betrachte $h = (r_0 - x) + \sum_{i=1}^{n-1} r_i X^i$. Es gilt $\deg(h) \leq n - 1$.

Behauptung: $h(b_j) = 0$ für alle j. Dann $h = 0$, speziell $x = r_0 \in k$. Noch zur Behauptung: Für jedes j ist g auch Minimalpolynom von b_j über k, also $b_j = \sigma(a)$ für ein $\sigma \in G$ [K/k normal], wofür $x = \sigma(x)$ [da $x \in \mathrm{Fix}_K(G)$], also $x = \sum_{i=0}^{n-1} r_i b_j^i$, d.h. $0 = h(b_j)$. □

Korollar 1. *Es sei K/k galoissch und L ein Zwischenkörper. Genau dann ist L/k galoissch, wenn L/k normal ist. [L/k ist ohnehin endlich und separabel.]*

Korollar 2. *Zu jeder endlichen und separablen Körpererweiterung $k \subseteq K$ gibt es eine Erweiterung $K \subseteq E$, sodass $k \subseteq E$ eine Galoiserweiterung ist.*

Beweis. Es sei $K = k(a_1, \ldots, a_n)$ und f_i das Minimalpolynom von a_i über k $(1 \leq i \leq n)$. Nehme einen Zerfällungskörper von $f = f_1 \cdots f_n$ über K. Wegen $f(a_i) = 0$ für alle i ist E auch Zerfällungskörper von f über k [wie früher]. Da alle $f_i \in k[X]$ separabel sind, ist auch f separabel. □

Korollar 3 (Satz vom primitiven Element)**.** *Zu jeder endlichen und separablen Körpererweiterung $k \subseteq K$ gibt es ein $a \in K$ mit $K = k(a)$.*

Beweis. Mit E wie in Korollar 2 hat E/k nur endlich viele Zwischenkörper, also auch K/k. Die Behauptung folgt wie für Korollar 1 des Hauptsatzes. □