Algebra I

Manuel Kauers
nach einer Vorlesung von
Dr. W. Trinks

21. Oktober 2000

Inhaltsverzeichnis

1 Gruppen und Monoide

Def. 1 Sei M eine Menge. Eine (partielle) Abbildung

$$v : M \times M \to M, \qquad (x, y) \mapsto v(x, y)$$

heißt *Verknüpfung*. Statt $v(x, y)$ schreibt man auch $x + y$, $x \cdot y$, xy, ...

Def. 2 Sei M eine Menge mit einer Verknüpfung $\cdot$. Dann können folgende Regeln erfüllt sein:

1. *Assoziativgesetz*

$$\forall \quad x, y, z \in M : \qquad (x \cdot y) \cdot z = x \cdot (y \cdot z)$$

2. Existenz eines *neutralen Elements*

$$\exists \quad e \in M \quad \forall \quad m \in M : \qquad e \cdot m = m = m \cdot e$$

3. Existenz eines *Inversen*

$$\forall \quad x \in M \quad \exists \quad y \in M : \qquad x \cdot y = y \cdot x = e$$

4. *Kommutativgesetz*

$$\forall \quad x, y \in M : \qquad x \cdot y = y \cdot x$$

Das System $(M, \cdot)$ heißt *Halbgruppe*, falls (1) gilt, es heißt *Monoid*, falls (1) und (2) gelten. Es heißt *Gruppe*, falls (1), (2) und (3) gelten. Es heißt *kommutative Gruppe* (oder ABEL*sche Gruppe*), falls (1), (2), (3) und (4) gelten.

Bsp.

- $(\mathbb{N}, +)$ ist Halbgruppe,
- $(\mathbb{N}_0, +)$, $(\mathbb{N}, \cdot)$ sind Monoide,
- $(S_3, \circ)$ ist Gruppe, aber nicht ABELsch,
- $(\mathbb{Z}, +)$ ist ABELsche Gruppe.

Bem.

- In einem Monoid ist das neutrale Element e eindeutig bestimmt. Man schreibt auch 1_M für das neutrale Element in M.
- In einer Gruppe ist zu jedem x das Inverse Element y eindeutig bestimmt. Man schreibt x^{-1} für das Inverse von x.

Def. 3 Sei $(M, \cdot)$ Halbgruppe [Monoid, Gruppe] und $N \subseteq M$. $(N, \cdot|_{N \times N})$ heißt *Unterhalbgruppe* [*Untermonoid*, *Untergruppe*], falls $(N, \cdot|_{N \times N})$ Halbgruppe [Monoid, Gruppe] ist. Schreibweise: $(N, \cdot|_{N \times N}) \leq (M, \cdot)$

Satz 1 Es seien U_i $(i \in I)$ Unterhalbgruppen [Untermonoide, Untergruppen] von M. Dann ist

$$D := \bigcap_{i \in I} U_i$$

ebenfalls Unterhalbgruppe [Untermonoid, Untergruppe] von M.

Bem. Zu jedem $X \subseteq M$ kann man daher

$$D := \bigcap_{\substack{X \subseteq U, \\ U \text{ ist UG [UM] von } M}} U$$

bilden. D heißt *von X erzeugte(s)* Untergruppe [Untermonoid], Schreibweise: $D = \langle X \rangle$

Def. 4 Seien $(G, \cdot)$ und $(H, *)$ Gruppen. Eine Abbildung $f : G \to H$ heißt *(Homo-)Morphismus*, falls gilt:

$$\forall \quad x, y \in G : \qquad f(x \cdot y) = f(x) * f(y)$$

Bem. Sind G, H, K Gruppen und $f : G \to H$, $g : H \to K$ Morphismen, so ist auch $f \circ g : G \to K$ ein Morphismus. Ist f bijektiv, dann ist auch $f^{-1} : H \to G$ ein Morphismus.

Def. 5 Sei G eine Gruppe und $K \leq G$. K heißt *Normalteiler* von G, falls gilt

$$\forall \quad x \in G : \qquad x^{-1}Kx = K$$

Schreibweise in diesem Fall: $K \trianglelefteq G$.

Satz 2 Seien G, H Gruppen und $f : G \to H$ ein Morphismus. Dann gilt:

- $f(1_G) = 1_H$
- $f(G)$ ist Untergruppe von H
- $f(x^{-1}) = (f(x))^{-1}$ $(x \in G)$
- $K := f^{-1}(\{1_H\})$ ist Normalteiler von G

Def. 6 Sei $(G, \cdot)$ eine Gruppe und M eine Menge. Eine Verknüpfung $*$ der Art

$$* : G \times M \to M, \qquad (x, m) \mapsto x * m$$

heißt *Operation von links* von G auf M, falls gilt:

- $\forall \quad m \in M : \qquad 1_G * m = m$
- $\forall \quad x, y \in G \quad \forall \quad m \in M : \qquad (x \cdot y) * m = x * (y * m)$

(Operation von rechts analog)

Def. 7 M operiere von links auf G.

1. $m \in M$ heißt *Fixpunkt* von $x \in G$, falls $xm = m$ gilt.

2. $G_m := \{x \in G : xm = m\}$ heißt *Fixgruppe* (oder *Stabilisator*) von $m \in M$.

3. $G\cdot m := \{xm : \; x \in G\}$ heißt *Bahn* (oder *Transitivitätsgebiet*) von m unter G.

4. Schreibweise für die Menge aller Bahnen:

$$G\backslash M := \{G \cdot m : \; m \in M\}$$

(Analog M/G für Operationen von rechts)

5. Falls $|\, G\backslash M \,| = 1$, so heißt die Operation von M auf G *transitiv.*

Bem. Die Fixgruppe G_m ist eine Gruppe.

Satz 3 Zwei Bahnen Gm, Gn sind entweder gleich oder disjunkt.

Bsp. Schreibweise für Permutationen $\sigma \in S_m$: S_m operiert nach Definition auf $M := \{1, 2, \ldots, m\}$. Dann erst recht auch die von σ erzeugte Untergruppe $H := \{1, \sigma, \sigma^2, \ldots, \sigma^{k-1}\}$. Seien $B_1, B_2, \ldots, B_l$ die Bahnen von M unter H, $B_i := \{b_{i1}, b_{i2}, \ldots, b_{i,k_i}\}$. Die Operation von H auf B_i ist transitiv, etwa $\sigma(b_{ij}) = b_{i,j+1}$ (Index j modulo k).

Betrachte z.B. die S_4 und

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \in S_4.$$

Hier ist $l = 1$, $k_1 = 4$ und demnach $\sigma = (1\ 2\ 3\ 4)$. Für

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \in S_4$$

gilt $l = 2$, $k_1 = k_2 = 2$ und demnach $\tau = (1\ 2)(3\ 4)$.

Zyklen der Länge $k_i = 1$ sind Fixpunkte und werden nicht mitgeschrieben.

Satz 4 (Satz von Lagrange) G sei eine endliche Gruppe.

1. Ist $H \leq G$, so $|H|$ ein Teiler von $|G|$.

2. Die Ordnung eines Elements $x \in G$ ist Teiler von G.

Def. 8 G sei Gruppe, $H \leq G$. Die Bahnen Hg $(g \in G)$ heißen *Rechtsrestklassen* von G modulo H. (Linksrestklassen analog)

Satz 5 Sei $H \subseteq G$ und

$$f : G\backslash H \to H/G, \qquad xH \mapsto Hx^{-1}.$$

f ist (wohldefiniert und) bijektiv.

Def. 9 Sei $H \subseteq G$.

$$(G : H) := |\, H\backslash G \,| = |\, G/H \,|$$

heißt *Index* von H in G.

Bem. Im endlichen Fall gilt $(G : H) = \frac{|G|}{|H|}$.

Bsp. Die Abbildung

$$G \times G \to G, \qquad (g, h) \mapsto ghg^{-1} =: g * h$$

ist eine Operation, denn es gilt

- $1 * h = 1h1^{-1} = h$,
- $(g_1 g_2) * h = g_1 * (g_2 * h)$.

Diese Operation heißt *Konjugation* (mit $g \in G$). Die Fixpunkte dieser Konjugation sind die $h \in G$, die mit g vertauschbar sind.

Def. 10 Sei G eine Gruppe. Die Menge

$$\mathcal{Z}(G) := \{h \in G : \quad \forall\, g \in G : \quad gh = hg\}$$

heißt *Zentrum* von G.

Bem. Es gilt $\mathcal{Z}(G) \trianglelefteq G$.

Satz 6 G operiere auf M. Die Abbildung

$$f_m := {}^{G}\!/_{G_m} \to Gm, \qquad xG_m \mapsto xm$$

ist eine Bijektion und es gilt $(G : G_m) = |Gm|$.

Def. 11 Ein System $V \subseteq M$ heißt *Vertretersystem* der Bahnen, falls $|V \cap B| = 1$ für jede Bahn B gilt.

Bem. M ist demnach in Bahnen „zerlegt“:

$$M = \dot{\bigcup_{v \in V}} G \cdot v$$

Im endlichen Fall gilt überdies die *Bahnbilanz*:

$$|M| = \sum_{v \in V} |G \cdot v| = \sum_{v \in V} (G : G_v)$$

Bsp. Es sei p eine Primzahl und G eine Gruppe mit $|G| = p^n$.
Beh.: Dann gilt $\mathcal{Z}(G) > \{1\}$.
Bew.: Betrachte die Operation von G auf G durch Konjugation und die zugehörigte Bahnbilanz:

$$|G| = p^m = \sum_{v \in V} (G : G_v)$$

Alle $(G : G_v)$ teilen p^n. Für mindestens ein $v \in V$ gilt $(G : G_v) = 1$, nämlich $(G : G_1)$. Wegen $p \mid \sum_{v \in V} (G : G_v)$ müssen noch weitere Summanden 1 vorkommen. Diese gehören zu den Bahnen der Länge 1, also zu Elementen von $\mathcal{Z}(G)$. ∎

2 Ringe

Def. 12 Eine algebraische Struktur $(R, +, \cdot)$ heißt *Ring (mit 1)*, falls gilt:

1. $(R, +)$ ist ABELsche Gruppe
2. $\exists \quad 1 \in R: \qquad (R, \cdot)$ ist Monoid
3. *Distributivgesetze*:

$$\begin{aligned} x \cdot (y + z) &= x \cdot y + x \cdot z \\ (x + y) \cdot z &= x \cdot z + y \cdot z \end{aligned}$$

   $(x, y, z \in R)$

Ein Ring R heißt *kommutativ*, falls das Monoid $(R, \cdot)$ kommutativ ist.

Bsp.

- $\mathbb{Z}$ ist kommutativer Ring mit 1.
- Ist V ein Vektorraum mit $\dim V > 1$, so ist $\operatorname{End} V$ ein nicht kommutativer Ring.
- Ist R ein Ring, dann ist auch $R^{n \times n}$ ein Ring
- Der *Restklassenring*: Es ist

$$m\mathbb{Z} := \{n \cdot m : \; n \in \mathbb{Z}\} \leq \mathbb{Z}.$$

  Die Menge $\mathbb{Z}/_{m\mathbb{Z}}$ wird mit den Verknüpfungen

$$\begin{aligned} (x + m\mathbb{Z}) + (y + m\mathbb{Z}) &:= (x + y) + m\mathbb{Z} \\ (x \cdot m\mathbb{Z}) + (y \cdot m\mathbb{Z}) &:= (x \cdot y) + m\mathbb{Z} \end{aligned}$$

  ein Ring.

Def. 13 Sei R ein Ring. Dann heißt

$$R^{\times} := \{e \in \mathbb{R} : \quad \exists \; y \in R : \quad ey = ye = 1\}$$

die *Einheitengruppe* von R.

Bem. $R^{\times}$ ist eine Gruppe.

Bsp.

- $\mathbb{Z}^{\times} = \{-1, 1\}$
- Sei V ein Vektorraum. Dann ist $(\operatorname{End} V)^{\times} = \operatorname{Aut} V$.
- $\left(\mathbb{Z}/_{12\mathbb{Z}}\right)^{\times} = \{1, 5, 7, 11\}$

Def. 14 Es sei R ein Ring. Ein Element $u \in \mathbb{R}$ mit

$$\exists \quad v \in R \setminus \{0\} : \qquad uv = 0$$

heißt *Nullteiler*. Ein Ring heißt *integer*, wenn er kommutativ ist und 0 der einzige Nullteiler ist.

Bsp.

- $\mathbb{Z}$ ist integer.
- ${\mathbb{Z}}/{m\mathbb{Z}}$ ist genau dann integer, wenn m eine Primzahl ist.

Satz 7 Es sei $R \neq \{0\}$ ein endlicher, integrer Ring. Dann ist R ein Körper.

Def. 15 R sei ein integrer Ring und $x, y \in R$.

1. $x \mid y \quad :\Longleftrightarrow \quad \exists\, z \in R: \quad xz = y$. Sprechweise: „$x$ *teilt* y“.
2. x, y heißen *teilergleich*, wenn gilt $x \mid y \ \wedge\ y \mid x$. Schreibweise in diesem Fall: $x \approx y$.
3. $\tilde{x} := \{y \in R: \quad y \mid x \ \wedge\ x \mid y\}$ heißt *Teilbarkeitsklasse* von x.

Bem.

- Die Relation $\mid$ ist transitiv
- $\tilde{1} = R^\times$.

Def. 16 Sei R ein Ring und $x \in R \setminus (R^\times \cup \{0\})$

1. x heißt *unzerlegbar*, falls gilt

$$\forall \quad u, v \in R: \qquad x = uv \quad \Longrightarrow \quad u \in R^\times \ \vee\ v \in R^\times.$$

2. x heißt *prim*, falls gilt

$$\forall \quad u, v \in R: \qquad x \mid (uv) \quad \Longrightarrow \quad x \mid u \ \vee\ x \mid v.$$

Bsp. Betrachte

$$R := \mathbb{Z}[\sqrt{-6}] := \{a + b\sqrt{-6}: \ a, b \in \mathbb{Z}\} \subseteq \mathbb{C}.$$

$x = \sqrt{-6}$ ist unzerlegbar, aber nicht prim, denn $x \mid (2 \cdot 3)$, aber $x \nmid 2$, $x \nmid 3$.

Def. 17 Ein integrer Ring R heißt *faktoriell*, wenn jedes $x \in R \setminus (R^\times \cup \{0\})$ eine Primfaktorzerlegung besitzt.

Bsp. $\mathbb{Z}$ ist faktoriell, $\mathbb{Z}[\sqrt{-6}]$ nicht.

Def. 18 Sei R ein kommutativer Ring. Das System $R^{\mathbb{N}} = \mathrm{Abb}(\mathbb{N} \to R)$ wird ein Ring, wenn die Verknüpfungen $+, \cdot$ folgendermaßen definiert: Seien

$$f = (f_0, f_1, \ldots), g = (g_0, g_1, \ldots) \in R^{\mathbb{N}}.$$

Dann sei

$$\begin{aligned} f + g &:= (f_0 + g_0, f_1 + g_1, \ldots) \\ (f \cdot g)_k &:= \sum_{i+j=k} f_i g_j. \end{aligned}$$

$R^{\mathbb{N}} =: R[[x]]$ heißt *Ring der formalen Potenzreihen* in einer Variablen. Dabei sind

$$x = (0, 1, 0, 0, \ldots), \qquad x^n = (\underset{\substack{0\text{-te}\\ \text{Stelle}}}{0}, 0, \ldots, 0, \underset{\substack{n\text{-te}\\ \text{Stelle}}}{1}, 0, 0, \ldots).$$

Mit den selben Verknüpfungen ist

$$R[x] := R^{\mathbb{N}}_{fin} = \{f = (f_0, f_1, \ldots) \in R^{\mathbb{N}} : \ f_i = 0 \text{ für fast alle } i\}$$

ein Unterring von $R[[x]]$. $R[x]$ heißt *Polynomring* über R in einer Variablen.

Für $f \in R[x]$ heißt

$$\partial f := \max\{i \in \mathbb{N}_0 : \ f_i \neq 0\}$$

der *Grad* von f.

Bem.

- Seien $f, g \in R[x]$. Dann gilt:

$$\begin{aligned} \partial(f+g) &\leq \max\{\partial f, \partial g\} \\ \partial(f \cdot g) &\leq \partial f + \partial g \end{aligned}$$

- Ist R integer, dann ist auch $R[x]$ integer.

Def. 19 Sei R ein integrer Ring, $a, b \in R$. $c \in R$ heißt ein ggT von a und b, falls gilt

1. $c \mid a, \ c \mid b$
2. Für $d \in R$ mit $d \mid a, \ d \mid b$ gilt $d \mid c$.

Schreibweise: $c = \mathrm{ggT}(a, b)$

Def. 20 Sei R ein integrer Ring und $\varphi : R \to \mathbb{N}$ eine Abbildung. R heißt EUKLID*isch* (mit Größenfunktion φ), falls gilt:

$$\forall \ a, b \in R, \ b \neq 0 \ \exists \ q, r \in R : \quad a = q \cdot b + r \ \wedge \ (r = 0 \ \vee \ \varphi(r) < \varphi(b)).$$

Bsp.

- $\mathbb{Z}$ ist mit $\varphi(z) = |z|$ EUKLIDisch.
- Ist K ein Körper, so ist $K[x]$ mit $\varphi(f) = \partial f + 1$ EUKLIDisch.
- $\mathbb{Z}[\sqrt{-1}]$ ist mit $\varphi(z) = z \cdot \overline{z}$ EUKLIDisch.

Satz 8 Sei R ein EUKLIDischer Ring mit Größenfuktion φ, $a, b \in R$. Dann existiert ein $c = \mathrm{ggT}(a, b)$. Außerdem gibt es $x, y \in R$ mit $c = x \cdot a + y \cdot b$.

Def. 21 R sei kommutativer Ring. Eine Untergruppe $\mathfrak{a}$ von $(R, +)$ heißt *Ideal*, falls gilt

$$\forall \quad x \in R : \qquad x \cdot \mathfrak{a} \subseteq \mathfrak{a}.$$

Schreibweise in diesem Fall: $\mathfrak{a} \trianglelefteq R$,

Bem. In einem EUKLIDischen Ring haben alle Ideale die Form $\mathfrak{a} = x \cdot R$ ($x \in R$). Allgemein heißen Ideale dieser Form *Hauptideal.*

Satz 9 Sei R ein EUKLIDischer Ring und $u \in R \setminus (R^\times \cup \{0\})$. Dann gilt: Ist u unzerlegbar, dann ist u prim.

Satz 10

1. In einem EUKLIDischen Ring R hat jedes Element $x \in R \setminus (R^\times \cup \{0\})$ eine Darstellung $x = p_1 \cdot p_2 \cdot \dots \cdot p_n$ mit primen p_i.

2. Wenn in einem integren Ring ein Element x Produkt von Primelementen ist, dann ist diese Darstellung im Wesentlichen eindeutig, d.h. ist

$$x = p_1 \cdot p_2 \cdot \dots \cdot p_m = q_1 \cdot q_2 \cdot \dots \cdot q_n$$

mit primen p_i, q_i, so ist $m = n$ und es gibt eine Permutation $\sigma \in S_m$ mit $p_i = q_{\sigma(i)}$ ($i = 1, \dots, m$).

Def. 22 Sei R ein faktorieller Ring. Mit $\mathbb{P} := \mathbb{P}_R$ sei ein Vertretersystem der Teilbarkeitsklassen $\tilde{p}$ der Primelemente bezeichnet.

Bsp. $\mathbb{P}_\mathbb{Z}$ ist die Menge aller positiven Primzahlen.

Bem. Damit ist jedes $x \in R \setminus \{0\}$ in der Form

$$x = e \cdot \prod_{p \in \mathbb{P}_R} p^{v_p}$$

zu schreiben, wobei $e \in R^\times$, $v_p \in \mathbb{N}_0$ und nur endlich viele $v_p > 0$ sind. Ist

$$y = e' \cdot \prod_{p \in \mathbb{P}_R} p^{w_p},$$

dann ist

$$\mathrm{ggT}(x, y) \approx \prod_{p \in \mathbb{P}_R} p^{\min\{v_p, w_p\}}, \qquad \mathrm{kgV}(x, y) \approx \prod_{p \in \mathbb{P}_R} p^{\max\{v_p, w_p\}}$$

Satz 11 Sei K ein Körper, $R = K[x]$, $f, g \in R$, $g \neq 0$.

1. Dividiere f durch g mit Rest r, $f = q \cdot q + r$. Wenn $\lambda \in K$ eine Nullstelle von g ist, dann gilt $f(\lambda) = r(\lambda)$.

2. $f \neq 0$ hat in K höchstens ∂f Nullstellen.

3 Der Quotientenring

In diesem Kapitel sei R ein kommutativer Ring, S ein Untermonoid von $(R, +)$.

Def. 23 Auf der Menge $R \times S$ wird eine Relation $\sim$ definiert durch

$$[r, s] \sim [r', s'] \iff \exists\, t \in S:\ trs' = tr's$$

Die Äquivalenzklasse $[r, x]$ wird $\frac{r}{s}$ geschrieben.

Def. 24 Seien R, R' Ringe. Eine Abbildung $f : R \to R'$ heißt *Ringhomomorphismus*, falls gilt:

1. $\forall \quad x, y \in R : \qquad f(x+y) = f(x) + f(y)$
2. $\forall \quad x, y \in R : \qquad f(x \cdot y) = f(x) \cdot f(y)$
3. $f(1_R) = 1_{R'}$

Bem. Sind R, R', R'' Ringe und $f : R \to R'$, $f' : R' \to R''$ Ringhomomorphismen, so ist $f \circ f' : R \to R''$ ebenfalls ein Ringhomomorphismus.

Satz 12 $S^{-1}R$ wird ein Ring mit folgenden Verknüpfungen:

$$\frac{r}{s} + \frac{r'}{s'} := \frac{rs' + sr'}{ss'}, \qquad \frac{r}{s} \cdot \frac{r'}{s'} := \frac{rr'}{ss'}.$$

Die Abbildung $f : R \to S^{-1}R$, $f(r) := \frac{r}{1}$ ist ein Ringhomomorphismus. f ist injektiv, falls es in S keine Nullteiler gibt.

Bem. $S^{-1}R$ heißt der *Quotientenring von* R *mit Nennermenge* S.

Def. 25 Sei R ein integrer Ring und $f = f_0 + f_1x + \cdots + f_nx^n \in R[x]$. Dann heißt

$$i(f) := \mathrm{ggT}(f_0, f_1, \ldots, f_n)$$

der *Inhalt* von f. Ist $i(f) = 1$, so heißt f *primitiv*.

Satz 13 (Lemma von Gauss) Sei R ein integrer Ring und $f, g \in R[x]$. Dann gilt

$$i(f \cdot g) = i(f) \cdot i(g).$$

Satz 14 Ist R ein faktorieller Ring, dann ist auch $R[x]$ faktoriell.

Bem. Mittels Induktion ist dann auch $R[x_1, x_2, \ldots, x_n]$ faktoriell.

4 Homomorphiesätze

Satz 15 Die Quotientenmenge ${}^{G}/_{K} = \overline{G}$ wird durch folgende wohldefinierte Verknüpfung zu einer Gruppe:

$$xK \cdot yK := (xy)K, \qquad \overline{x} \cdot \overline{y} := \overline{xy}.$$

Die Abbildung $p : x \mapsto \overline{x} = xK$ ist ein surjektiver Homomorphismus mit $\mathrm{Kern}\, p = K$.

Bem.

- $\overline{G}$ heißt *Faktorgruppe*.

- Schematische Darstellung: Sei $f: G \to H$ ein Homomorphismus und $K = \operatorname{Kern} f$. Dann kann man f durch folgendes Diagramm charakterisieren:

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ {\scriptstyle p}\downarrow & & \uparrow{\scriptstyle i} \\ G/K & \xrightarrow[\overline{f}]{} & f(G) \end{array}$$

  (p surjektiv, i injektiv, $\overline{f}$ Isomorphismus).

Bsp.

- Die Signatur $\operatorname{sgn}: S_n \to \mathbb{Z}^\times = \{-1, 1\}$ ist Homomorphismus mit Kern A_n
- Sei R ein kommutativer Ring, $S = R^{n \times n}$. Dann ist

$$S^\times = GL_n(R) = \{A \in S : \det A \in R^\times\}$$

  und die Abbildung $\det : GL_n(R) \to \mathbb{R}^\times$ ist ein Homomorphismus mit

$$\operatorname{Kern} \det = SL_n(R) = \{A \in S : \det A = 1\}.$$

  Es gilt ${GL_n(R)}/{SL_n(R)} \cong R^\times$, denn det ist surjektiv ($n \geq 1$).

Satz 16 Sei R ein EUKLIDischer Ring und $\mathfrak{a}$ ein Ideal von R. Dann wird die Faktorgruppe $\overline{R} := R/\mathfrak{a}$ ein Ring, wenn man definiert

$$\overline{x} \cdot \overline{y} := \overline{x \cdot y}, \qquad (x, y \in R).$$

Bem. Dann heißt $\overline{R}$ *Faktorring.*

Bsp. Betrachte $R = \mathbb{Z}, \mathfrak{a} := m\mathbb{Z}$. Dann ist $\overline{R} = \mathbb{Z}/\mathfrak{a} =: \mathbb{Z}/(m) =: Z_m$.

Def. 26 Sei R ein kommutativer Ring. Zwei Ideale $\mathfrak{a}, \mathfrak{b}$ heißen *komaximal*, falls gilt $R = \mathfrak{a} + \mathfrak{b}$.

Bem. Es gilt $R = \mathfrak{a} + \mathfrak{b} \iff 1 \in \mathfrak{a} + \mathfrak{b}$.

Def. 27 Das Produkt zweier Ideale $\mathfrak{a}, \mathfrak{b}$ sei definiert durch

$$\mathfrak{a} \cdot \mathfrak{b} := \left\{ \sum_i a_i \cdot b_i,\ a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \right\}.$$

Bem.

- Sind $\mathfrak{a}, \mathfrak{b}$ und $\mathfrak{a}, \mathfrak{c}$ jeweils komaximale Ideale, dann sind auch $\mathfrak{a}, \mathfrak{b} \cdot \mathfrak{c}$ komaximal.
- Für $x + \mathfrak{a} = y + \mathfrak{a}$ schreibt man auch $x \equiv y\,(\mathfrak{a})$.

Satz 17 (Hauptsatz über simultane Kongruenzen, chinesischer Restsatz) R sei ein kommutativer Ring. $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_k$ seien paarweise komaximale Ideale. Dann ist die Abbildung

$$f: R/\prod_{i=1}^{k} \mathfrak{a}_i \to \prod_{i=1}^{k} R/\mathfrak{a}_i\,, \qquad x + \prod_{i=1}^{k} \mathfrak{a}_i \mapsto (x + \mathfrak{a}_i, x + \mathfrak{a}_2, \ldots, x + \mathfrak{a}_k)$$

wohldefiniert und ein Ringisomorphismus.

Bem. D.h. zu vorgegebenen Restklassen $x_i \bmod \mathfrak{a}_i$ gibt es eine Restklasse $x \bmod \mathfrak{a} = \prod_i \mathfrak{a}_i$ so, daß gilt $x \equiv x_i\,(\mathfrak{a})$.

Bsp.

- $R = \mathbb{Z}$, $\mathfrak{a}_i = m_i\mathbb{Z}$. Es gilt

  $$\mathfrak{a}_i \text{ komaximal} \iff \forall\, i, j: \ \mathrm{ggT}(m_i, m_j) = 1$$

  Rechnen mit großen Zahlen: Sei $A \in \mathbb{Z}^{n\times n}$ (n groß), gesucht ist $\det A$. Finde $N \in \mathbb{Z}$ mit $|\det A| < \frac{1}{2}N$, z.B. durch die LEIBNITZ-Formel:

  $$|\det((\alpha_{ij}))| \leq n!(\max_{i,j} \alpha_{ij})^n$$

  Wähle teilerfremde Zahlen m_i mit $\prod_{i=1}^{k} m_i > N$. Berechne $\det(\alpha_{ij}) \bmod m_l$ $(l = 1, \ldots, k)$ durch Rechnen im Körper $\mathbb{F}_{m_l}$. Resultat: Ist $x_i = \det A\,(m_l)$ $(l = 1, \ldots, k)$, das gesuchte x ist dann wegen

  $$|x| < \frac{1}{2}N < m_1 \cdot \cdots \cdot m_l.$$

  x ist $\mathrm{mod} m_1 \cdot m_2 \cdot \cdots \cdot m_l$ eindeutig bestimmt und muß im Intervall $[-\frac{1}{2}m_1 m_l, \frac{1}{2}m_1 m_l]$ liegen.

- u. v. m.

5 Moduln

Def. 28 Sei R ein Ring und $(M, +)$ eine ABELsche Gruppe. M heißt ein R-*Linksmodul*, wenn eine Operation $R \times M \to M$, $(r, m) \mapsto r \cdot m$ gegeben ist, die folgenden Bedingungen genügt:

1. $\forall \quad m \in M: \qquad 1 \cdot m = m$
2. $\forall \quad m \in M, r, s \in R: \qquad (r + x)m = rm + sm$
3. $\forall \quad m, n \in M, r \in R: \qquad r(m + n) = rm + rn$
4. $\forall \quad m \in M, r, s \in R: \qquad (rs)m = r(sm)$

Bem. Ein Modul über einem Ring entspricht formal einem Vektorraum über einem Körper.

Bsp.

- Ist R ein Ring, dann sind $M = R^n, R^{n\times n}$ mit den bekannten Matrix- und Vektoroperationen als Verknüpfungen Moduln über R.
- Ist $R = \mathbb{Z}$ und M eine beliebige ABELsche Gruppe. M wird zu einem $\mathbb{Z}$-Linksmodul, wenn man definiert

$$z \cdot m := \begin{cases} \sum\limits_{i=1}^{z} m & (z \geq 0) \\ \sum\limits_{i=1}^{n} -m & (z < 0) \end{cases}$$

  Also sind $\mathbb{Z}$-Moduln und ABELsche Gruppen im Wesentlichen dasselbe.
- Sei K ein Körper, $R = K[x]$ und $A \in K^{n\times n}$ fest. Der Vektorraum $V = K^n$ wird zu einem R-Modul, wenn man für $f = \alpha_0 + \alpha_1 x + \cdots + \alpha_m x^m \in R$ und $v \in V$ definiert

$$f \cdot v := (\alpha_0 I + \alpha_1 A + \alpha_2 A^2 + \cdots + \alpha_m A^m) \cdot v.$$

Satz 18 (Elementarteilersatz) Es sei R ein EUKLIDischer Ring und $A \in R^{m\times n}$. Dann gibt es ein $P \in GL_m(R)$, $Q \in GL_n(R)$ so, daß

$$D = PAQ =: \operatorname{diag}(d_1, d_2, \ldots)$$

eine Diagonalmatrix ist und gilt $d_1 \mid d_2 \mid \ldots$ Dabei sind die $d_i R^\times = \tilde{d_i}$ eindeutig bestimmt.

Satz 19 Zu $e, f \in R$, $g = \operatorname{ggT}(e, f)$, $f = \frac{ef}{g}$ (bzw. $h = 0$, falls $g = 0$) gibt es

1. $a, b, c, d \in R$ mit $ad - bc = 1$ und

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e \\ f \end{pmatrix} = \begin{pmatrix} g \\ 0 \end{pmatrix}$$

2. $a, b, c, d, a', b', c', d' \in R$ mit $ad - bc = 1 = a'd' - b'c'$ und

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & 0 \\ 0 & f \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} g & 0 \\ 0 & h \end{pmatrix}$$

Def. 29 Sei M ein Modul über einem Ring R. N sei eine Untergruppe von M. Gilt $RN \subseteq N$, so heißt N *Untermodul* von M.

Seien M, N zwei R-Moduln. $f : M \to N$ sei ein Gruppenhomomorphismus. f heißt *R-Modul-Morphismus*, falls

$$\forall \quad r, m \in M : \qquad f(r \cdot m) = r \cdot f(m)$$

Bem. Sei M ein R-Modul, N ein Untermodul von M, dann wird die Faktorgruppe ${}^{M}/_{N}$ zu einem R-Modul, wenn man die Operation von R auf $\overline{M}$ definiert durch

$$r \cdot (m + N) := r \cdot m + N$$

Satz 20 Sei $f : M \to N$ R-Modul-Morphismus. Dann gilt:

1. $\operatorname{Bild} f \leq N$, $\operatorname{Kern} f \leq N$.
2. Durch $\overline{f} : {}^{M}\!/_{\operatorname{Kern} f} \to \operatorname{Bild} f$, $m + \operatorname{Kern} f \mapsto f(m)$ wird ein Isomorphismus ${}^{M}\!/_{\operatorname{Kern} f} \xrightarrow{\sim} \operatorname{Bild} f$ gegeben.
3. Dabei entsteht eine Bijektion von $M \geq \operatorname{Kern} f$ auf $\operatorname{Bild} f \geq N$

Bem. Schematische Darstellung:

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "p"'] & N \\ {}^{M}\!/_{K} \arrow[r, "\sim", "\overline{f}"'] & B \arrow[u, "i"'] \end{tikzcd}$$

p surjektiv, i injektiv, $\overline{f}$ Isomorphismus.

Def. 30 Der R-Modul M heißt *endlich erzeugt*, falls es $x_1, x_2, \ldots, x_m \in M$ gibt mit

$$M = Rx_1 + \cdots + Rx_m \qquad (m \in \mathbb{N})$$

Satz 21 (Struktursatz für endlich erzeugte ABELsche Gruppen) Jede ABELsche Gruppe ist isomorph zu

$$Z_{d_1} \times \cdots \times Z_{d_r} \times \mathbb{Z}^s$$

mit $d_i > 1$ und $d_1 \mid d_2 \mid \cdots \mid d_r$.

Falls $d = d_1 \cdot d_2$ mit $\operatorname{ggT}(d_1, d_2) = 1$, so gilt weiterhin

$${}^{R}\!/_{dR} \cong {}^{R}\!/_{d_1R} \times {}^{R}\!/_{d_2R}.$$

Ist $d = p_1^{e_1} \cdot \cdots \cdot p_m^{e_m}$ (p_i prim, paarweise nicht teilergleich), so hat man eine „Primärzerlegung"

$${}^{R}\!/_{dR} \cong {}^{R}\!/_{p_1^{e_1}} \times \cdots \times {}^{R}\!/_{p_m^{e_m}}$$

Satz 22 Sei R ein euklidischer Ring, M ein endlich erzeugter Modul. Dann existieren $d_1, d_2, \ldots, d_r \in R$ so, daß $d_1 \mid d_2 \mid \cdots \mid d_r$, $d_1 \notin R^\times$, $d_r \neq 0$ und

$$M \cong {}^{R}\!/_{d_1R} \times \cdots \times {}^{R}\!/_{d_rR} \times R^s.$$

Dabei sind r, s, d_iR durch M eindeutig bestimmt.

Bem. Ein Modul heißt *zyklisch*, wenn er (als R-Modul) von einem Element erzeugt ist. Insbesondere ist ${}^{R}\!/_{dR}$ erzeugt von $\overline{1} = 1 + dR$.

Satz 23 Sei K ein Körper, E eine endliche Untergruppe von $K^\times$. Dann ist E zyklisch.

Bem. (Kleiner Satz von FERMAT) $\mathbb{F}_p^x$ ist zyklisch. Es gibt eine „Primitivwurzel" w modulo p so, daß $\langle \overline{w} \rangle_{mult} = \mathbb{F}_p^x$.

Satz 24 (Struktur von $\left(\mathbb{Z}/p^m\mathbb{Z}\right)^\times$, p prim) Ist $p = 2$, so gilt

$$\left(\mathbb{Z}/2^n\mathbb{Z}\right)^\times \cong Z_2 \times Z_{2^{n-1}}, \qquad (n \geq 2),$$

also nicht zyklisch für $n \geq 3$. Ist $p \neq 2$, so gilt

$$\left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times \cong Z_{p-1} \times Z_{p^{n-1}},$$

also zyklisch wegen $\operatorname{ggT}(p-1, p^{n-1}) = 1$.

Bsp. (Anwendung auf die Kryptographie) Diffie und Hellman (1976) schlugen vor, *Trapdoor-functions* α, β zu wählen mit folgender Eigenschaft: Aus der alleinigen Kenntnis von α kann man man α^{-1} nicht berechnen. Es sei A der „Eigentümer“ von α und B der Eigentümer von β. Beide machen ihre Funktionen öffentlich bekannt, behalten die Umkehrfunktionen jedoch für sich. Verschickt nun A eine Nachricht x an B, so wird dies in der Form

$$\texttt{"An B:"} + \beta(\texttt{"von A:"} + \alpha^{-1}(x)).$$

getan. B kennt β^{-1}, α ist öffentlich, damit kann x nur von B gelesen werden und B ist sicher, daß die Nachricht von A kam.

Das Problem ist nun die Konstruktion solcher Funktionen α, β. Sie *Sicherheit* dieser Funktionen beruht darauf, daß man große $N \in \mathbb{N}$ leicht als nichtprim nachweisen, aber die Primfaktorzerlegung i. a. nur schwer bestimmen kann. Wähle große Primzahlen p, q (z.B. $p, q > 10^{200}$). Es sei $N := p \cdot q$. Betrachte nun

$$\alpha : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, \qquad (x \bmod N) \mapsto x^e \bmod N$$

mit einem gewissen e. α wird eine Bijektion, wenn gilt $\operatorname{ggT}(e, (p-1)(q-1)) = 1$.

Sei M nun das Alphabet, aus dessen Zeichen Nachrichten verschlüsselt werden sollen. Eine Verschlüsselung ist eine Permutation $\sigma \in S_M$, die die oben beschriebenen Eigenschaften einer Trapdoor-function erfüllt. $|M| = N \Longrightarrow |S_M| = N!$, also ist $\sigma^{N!} = \mathrm{id}$ und $\sigma^{-1} = \sigma^{N!-1}$. Wegen der Größe von $N!$ kann aber niemand kann aber niemand $\sigma^{N!-1}$ berechnen.

Konkret: Der *RSA-Algorithmus* (Rivest, Shamir, Adleman) verwendet die Tatsache, daß es zwar leicht ist, große Primzahlen zu finden und miteinander zu multiplizieren, man jedoch aus dem Produkt nicht in akzeptabler Zeit auf die Primfaktoren Rückschlüsse ziehen kann. Für das oben eingeführte α gilt

$$\begin{aligned} & \alpha \circ \alpha^{-1} = \mathrm{id} \quad \Longleftrightarrow \quad (x^e)^f = x^{ef} \equiv x\,(N) \\ \Longleftrightarrow \quad & x^{ef} \equiv x \bmod p \quad \wedge \quad x^{ef} \equiv x \bmod q. \end{aligned}$$

Dies aber gilt für $ef \equiv 1 \bmod (p-1)$ und $ef \equiv 1 \bmod (q-1)$. Nach beliebiger Wahl von e kann man damit f mit dem EUKLIDischen Algorithmus berechnen. Es ist keine Methode bekannt, f aus N und e zu berechnen, ohne N zu faktorisieren.

6 Nochmals Gruppen

Satz 25 Sei G eine Gruppe und A, B Untergruppen von G. Dann ist

$$A \cdot B := \{a \cdot b : \quad a \in A, b \in B\}$$

genau dann Untergruppe von G, wenn gilt $A \cdot B = B \cdot A$.

Satz 26 Sei G eine Gruppe, $H, N \trianglelefteq G$. Dann ist $H \cdot N \leq G$ und es gilt

$$H \cdot N/_N \cong H/_{(H \cap N)}$$

Def. 31 Sei G eine Gruppe. Ein Normalteiler $N \lhd G$ heißt *maximal*, falls gilt

$$N \leq \tilde{N} \lhd G \quad \Longrightarrow \quad N = \tilde{N}.$$

Def. 32 Eine Gruppe G heißt *einfach*, falls $\{1\}$ maximaler Normalteiler von G ist.

Bem.

- Die endlichen, einfachen, ABELschen Gruppen sind genau die Z_p mit p prim.
- Seit 1980 sind alle endlichen einfachen Gruppen bekannt.

Def. 33 G sei eine Gruppe. Eine Folge

$$\mathcal{K} = (G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_r = E)$$

heißt *Kompositionsreihe* von G, falls G_{i+1} maximaler Normalteiler von G_i ist. In diesem Fall heißt r die *Länge* der Kompositionsreihe und die $H_i := G_i/_{G_{i+1}}$ heißen *Kompositionsfaktoren.*

Zwei Kompositionsreihen heißen zueinander *äquivalent*, wenn sie die selbe Länge haben und ihre Kompositionsfaktoren (evtl. nach Umordnung) zueinander isomorph sind.

Satz 27 (Satz von JORDAN-HÖHLER) Hat eine Gruppe G eine Kompositionsreihe, so sind alle Kompositionsreihen von G äquivalent.

Bem.

- Ist G endlich, so existiert eine Kompositionsreihe. z.B. $\mathbb{Z}$ hat keine Kompositionsreihe, denn die Folge

  $$\mathbb{Z} \rhd 2\mathbb{Z} \rhd 4\mathbb{Z} \rhd \cdots$$

  bricht nicht ab.
- Der obige Satz sagt für endliche Gruppen nur, daß ihre Primfaktorzerlegung eindeutig bestimmt ist.

Satz 28 Seien H, N Gruppen. $\varphi : H \to \operatorname{Aut} N$ sei ein Homomorphismus. Dann wird $G := H \times N$ zu einer Gruppe, wenn man für $(h_1, n_1), (h_2, n_2) \in G$ eine Verknüpfung $\cdot$ definiert durch

$$(h_1, n_1) \cdot (h_2, n_2) := (h_1 \cdot h_2, (\varphi(h_2^{-1}))(h_1) \cdot n_2)$$

Bem. In diesem Fall heißt G das *semidirekte Produkt* von H mit N (über φ), Schreibweise $G = H \rtimes N$.

Bsp. Betrachte die Permutationen

$$\sigma := (1\,2\,3\,\ldots n), \quad \tau := (1\,n)(2\,n-1)\cdots \in S_n$$

sowie den Homomorphismus $\varphi : \sigma \mapsto \sigma^{-1}$. Dann ist

$$H \rtimes N = D_n := \langle (1\,2\,3\,\ldots n), (1\,n)(2\,n-1)\cdots \rangle$$

Satz 29

- Die Gruppe A_n wird von 3-Zyklen erzeugt.
- Ist $n \geq 5$, so wird A_n von den disjunkten Doppel-2-Zyklen $(a\,b)(c\,d)$ erzeugt.
- Ist $n = 4$, so erzeugen die disjunkten Doppel-2-Zyklen einen Normalteiler der Ordnung 4 in S_4.
- Ist $n \geq 5$, so ist A_n einfach.

7 Die Sylow-Sätze

Satz 30 Es sei G eine endliche Gruppe, $A, B \leq G$. Dann gilt

$$|A \cdot B| = \frac{|A| \cdot |B|}{|A \cap B|}.$$

Satz 31 Es sei G eine Gruppe, $U, V \leq G$. Dann gilt

$$G = \dot{\bigcup_{g \in G}} UgV.$$

Ist G endlich, so gilt außerdem

$$|G| = \sum_{g \in G} \frac{|U| \cdot |V|}{|U^{g_i} \cap V|}.$$

Bem.

- Die Mengen UgV $(g \in G)$ heißen *Doppelrestklassen* von G modulo (U, V).
- Die Schreibweise U^g bezeichnet die Konjugierten.

Def. 34 Sei G eine Gruppe und $U \leq G$. Dann heißt

$$\mathcal{N}_G(U) := \{\gamma \in G : U^\gamma = U\}$$

der *Normalisator* von U in G.

Bem.

- $\mathcal{N}_G(U)$ ist die größte Untergruppe von G, in der U Normalteiler ist.

- Die Anzahl der verschiedenen Konjugierten U^γ, $\gamma \in G$ ist $(G : \mathcal{N}_G(U))$.

Def. 35 Sei G eine endliche Gruppe, $|G| = g = p^a n = p^b m$ mit p prim und $\mathrm{ggT}(p, m) = 1$. Eine Untergruppe H von G heißt SYLOW-*Gruppe*, falls gilt $|H| = p^b$.

Satz 32 (SYLOW-Sätze) Sei G eine endliche Gruppe, $|G| = g = p^a n = p^b m$ mit p prim und $\mathrm{ggT}(p, m) = 1$. $N(p^a)$ sei die Anzahl der $H \leq G$ mit $|H| = p^a$. Dann gilt

1. $N(p^a) \equiv 1 \bmod p$ (Insbesondere gibt es also $H \leq G$ mit $|H| = p^a$.)
2. Sei H eine p-SYLOW-Gruppe und U eine p-Untergruppe von G ($U = p^a$). Dann gibt es ein $\gamma \in G$ mit $U^\gamma \leq H$. (bzw. $U \leq H^\gamma$).
3. Alle p-SYLOW-Gruppen von G sind konjugiert. Also: ist H eine p-SYLOW-Gruppe, so gilt
$$N(p^b) = (G : \mathcal{N}_G(H)).$$

Bsp.

- Sei G eine Gruppe.
Beh.: $|G| = 30 \implies G$ ist nicht einfach.
Bew.: Es gilt
$$\begin{aligned} & 30 = 2 \cdot 3 \cdot 5 \\ \implies \quad & N_2 \in \{1, 3, 5, 15\}, \quad N_3 \in \{1, 10\}, \quad N_5 \in \{1, 6\}. \end{aligned}$$
Im Fall „1“ ist die SYLOW-Gruppe Normalteiler, andernfalls enthält G mindestens
$$\begin{array}{rl} 3 & \text{Elemente der Ordnung 2 in den 2-SYLOW-Gruppen} \\ 20 & \text{Elemente der Ordnung 3 in den 3-SYLOW-Gruppen} \\ \underline{24} & \text{Elemente der Ordnung 5 in den 5-SYLOW-Gruppen} \\ 47 & > 30 \text{ W!} \end{array}$$

- **Beh.:** Sind p, q prim und ist G eine Gruppe der Ordnung $p \cdot q$, so ist G nicht einfach.
Bew.:
  1. Ist $p = q$, so ist G ABELsch und damit nicht einfach.
  2. Ist $p \neq q$, so ist $N_p \in \{1, q\}$ und $N_q \in \{1, p\}$. Falls $N_p \neq 1 = N_q$, so enthielte G
  $$\begin{array}{rl} q \cdot (p-1) & \text{Elemente der Ordnung } p \\ p \cdot (q-1) & \text{Elemente der Ordnung } q \end{array}$$
  Dies sind jedoch viel zu viele.

- Ist G eine einfache Gruppe der Ordnung 60, so ist $G \cong A_5$.

- Zu einem Körper K seien definiert

$$SL(n,K) = \{A \in K^{n\times n} : \det A = 1\}$$

und

$$PSL(n,K) = {}^{SL(n,K)}/_{\mathcal{Z}(SL(n,K))}$$

Es gilt: Die zweitkleinste einfache Gruppe ist

$$PSL(2,\mathbb{F}_7) \cong PSL(3,\mathbb{F}_2).$$

Satz 33

1. (Burnsides p^a-q^b-Satz) Sind p, q prim und ist G eine Gruppe der Ordnung $p^a q^b$, so ist G nicht einfach.
2. Ist G eine Gruppe ungerader Ordnung, so ist G nicht einfach.

8 Produkte und Koprodukte von Gruppen

Satz 34 G_i $(i \in I)$, H seien Gruppen und G das karthesische Produkt

$$G = \prod_{i\in I} G_i.$$

γ_i sei die Projektion von G auf G_i $(i \in I)$. Dann hat G die folgende *universelle Abbildungseigenschaft*: Sind $\eta_i : H \to G_i$ Morphismen, so gibt es genau einen Morphismus $\varphi : H \to G$ mit $\eta_i = \gamma_i\varphi$ $(i \in I)$. Weiter sind die γ_i surjektiv und es gilt

$$\bigcap_{i\in I} \operatorname{Kern} \gamma_i = E$$

Def. 36 Seien G_i $(i \in I)$, H Gruppen. Erfüllt eine Gruppe G die folgende universelle Abbildungseigenschaft, dann heißt G das *Koprodukt* der G_i: Sind $\gamma_i : G_i \to G$ und $\eta_i : G_i \to H$ Morphismen, so gibt es genau einen Morphismus $\varphi : G \to H$ mit $\eta_i = \varphi \circ \gamma_i$ $(i \in I)$

Bem.

- Ist G das Koprodukt von Gruppen G_i $(i \in I)$, so schreibt man

$$G = \coprod_{i\in I} G_i.$$

- Die γ_i aus der Definition sind injektiv. G wird erzeugt von den Mengen $\gamma_i(G)$ $(i \in I)$ und ist bis auf Isomorphie eindeutig bestimmt.
- G wird auch als *freies Produkt* der G_i bezeichnet und man verwendet auch die Schreibweisen

$$G = \mathop{\ast}_{i\in I} G_i \quad \text{bzw.} \quad G = G_1 * G_2 * \cdots$$

- Spezialfall: $G_i \cong \mathbb{Z} =: \langle x_i \rangle$, $G_i = \{x_i^n : \ n \in \mathbb{Z}\}$. Dann heißt $G := \coprod_{i \in I} \langle x_i \rangle$ die *freie Gruppe* auf $|I|$ Elementen.
- Ist H eine Gruppe mit Erzeugendensystem $\{y_i : \ i \in I\}$, so durch

$$\varphi : \coprod_{i \in I} \langle x_i \rangle \to H, \qquad \varphi(x_i) := y_i$$

ein surjektiver Homomorphismus definiert. Ist

$$K := \operatorname{Kern} \varphi \trianglelefteq \coprod_{i \in I} \langle x_i \rangle ,$$

dann ist K die Menge der Relatoren, denen die y_i genügen.

Bsp.

- $H := \langle y \rangle$ sei zyklisch von der Ordnung m. Dann ist

$$K = \{x^{k \cdot m} : \quad k \in \mathbb{Z}\}.$$

- Betrachte

$$D_m := \left\langle \{\sigma, \tau : \quad \sigma^m = \tau^2 = 1, \tau^{-1} \sigma \tau = \sigma^{-1}\} \right\rangle .$$

Dann ist K als Normalteiler „erzeugt von den Relatoren“:

$$K = \bigcap_{\substack{N \trianglelefteq \coprod_{i \in I} \langle x_i \rangle \\ \text{alle Relatoren } \in N}} N.$$

- S_n wird erzeugt von $x_1, \ldots, x_{n-1}$ mit den Relatoren

$$\begin{aligned} x_i^2 &= 1 \quad (1 \le i \le n-1), \\ (x_i \, x_{i+1})^3 &= 1 \quad (1 \le n-2), \\ x_i x_j &= 1 \quad (j < i-1). \end{aligned}$$

Die Transpositionen $\pi_i := (i, i{+}1)$ erfüllen gerade diese Relationen. Damit ist also $\varphi : x_i \mapsto \pi_i$.

Bem. (Navikow, 1957) Wenn G mit endlich vielen Erzeugern und Relatoren repräsentiert ist, also

$$G = \coprod_i \langle x_i \rangle / K ,$$

und $a, b \in \coprod_i \langle x_i \rangle$ sind, so ist i. a. nicht algorithmisch entscheidbar, ob gilt

$$a \bmod K = b \bmod K.$$

9 Symmetrie-Gruppen

Def. 37 Sei $M \subseteq \mathbb{R}^n$. Eine isometrische Abbildung $\varphi : \mathbb{R}^n \to \mathbb{R}^n$ mit $\varphi(M) = M$ heißt *Symmetrie* von M.

Bem. Jede Symmetrie φ hat die Form $\varphi(x) = Ax + b$ für ein $b \in \mathbb{R}^n$ und eine Matrix

$$A \in O(n, \mathbb{R}) := \{M \in \mathbb{R}^{n \times n} : \quad M^\top M = I\}.$$

Die Menge

$$O_+(n, \mathbb{R}) := \{M \in O(n, \mathbb{R}) : \quad \det M = +1\}$$

heißt die Menge der *eigentlichen orthogonalen Abbildungen.*

Ist speziell $n = 3$, so kann zu jeder Isometrie φ durch Basiswechel angenommen werden, daß die zugehörige Matrix A von der Form

$$A = \begin{pmatrix} \cos\alpha & -\sin\alpha & 0 \\ \sin\alpha & \cos\alpha & 0 \\ 0 & 0 & \pm 1 \end{pmatrix}$$

ist ($\alpha \in [0, 2\pi]$).

Satz 35 Sei $M \subseteq \mathbb{R}^n$ endlich und

$$\mathrm{Sym}(M) := \{\varphi : \mathbb{R}^n \to \mathbb{R}^n | \quad \varphi \text{ ist Symmetrie von } M\}.$$

Falls es in M $n+1$ Punkte in allgemeiner Lage gibt, ist $\mathrm{Sym}(M)$ endlich. Dabei heißen $n + 1$ Punkte $P_0, \ldots, P_n \in \mathbb{R}^n$ *in allgemeiner Lage*, falls die Menge

$$\{P_1 - P_0, P_2 - P_0, \ldots, P_n - P_0\} \subseteq \mathbb{R}^n$$

linear unabhängig ist.

Bem. Wir untersuchen die Symmetriegruppen von regelmäßigen Körpern. Im Folgenden sei also

$$\begin{aligned} T &:= \mathrm{Sym}(\text{„Tetraeder“}) \\ W &:= \mathrm{Sym}(\text{„Würfel“}) = \mathrm{Sym}(\text{„Oktaeder“}) \\ I &:= \mathrm{Sym}(\text{„Ikosaeder“}) = \mathrm{Sym}(\text{„Dodekaeder“}). \end{aligned}$$

Die Eckenmenge aller dieser Körper enthält vier Punkte in allgemeiner Lage, also sind T, W und I endlich.

Def. 38 Sei $\mathrm{id} \neq \Phi \in O_+(3, \mathbb{R})$ von endlicher Ordnung und $k := |\langle\Phi\rangle|$ (d.h. Φ ist Drehung um den Winkel $\alpha = \frac{2\pi}{k}$). D sei die Drehachse von Φ. Die Punkte

$$P_1, P_2 \in D \cap \{x \in \mathbb{R}^n : \ ||x|| = 1\}$$

heißen *Pole* von Φ.

Bem.

- Sei G eine Symmetriegruppe, $\mathrm{id} \neq \varphi \in G$, P ein Pol von Φ. Dann ist die Fixgrupe G_P zyklisch. Gilt $|G_P| = k$, so heißt G_P *k-zählig*.
- Für T, W und I gelten folgende speziellen Eigenschaften. Jeweils seien P die Menge aller Pole, k die Anzahl der Bahnen von G auf P.

G	Name	$\|G\|$	$\|P\|$	k
Z_m	zyklische Gruppe	m	2	2
D_m	Diedergruppe	$2m$	$2m+2$	3
$A_4 \cong T$	Tetraedergruppe	12	14	3
$S_4 \cong W$	Würfelgruppe	24	26	3
$A_5 \cong I$	Ikosaedergruppe	60	62	3

Satz 36 Jede endliche Untergruppe $G < O_+(3, \mathbb{R})$ ist eine der Gruppen aus obiger Tabelle.

10 Algebraische Körpererweiterungen

Def. 39 R sei ein kommutativer Ring. Ein Ideal $\mathfrak{a} \lhd R$ heißt

1. *Primideal*, falls gilt

$$\forall \quad x, y \in R: \qquad xy \in \mathfrak{a} \quad \Longrightarrow \quad x \in \mathfrak{a} \ \vee \ y \in \mathfrak{a}.$$

2. *maximales Ideal*, falls für jedes Ideal $\mathfrak{b}$ mit $\mathfrak{a} \leq \mathfrak{b} \lhd R$ gilt $\mathfrak{a} = \mathfrak{b}$.

Bem.

- Ist $\mathfrak{a} \unlhd R$, so gelten folgende Äquivalenzen:

$$\begin{aligned} \mathfrak{a} \text{ ist Primideal} \quad &\Longleftrightarrow \quad R/\mathfrak{a} \text{ ist integer} \\ \mathfrak{a} \text{ ist maximal} \quad &\Longleftrightarrow \quad R/\mathfrak{a} \text{ ist Körper.} \end{aligned}$$

- Sei k ein Körper, $R = k[x]$ und $f \in R$ prim. Dann ist $\mathfrak{a} := R \cdot f$ ein maximales Primideal und somit $K := R/\mathfrak{a}$ ein Körper. In K hat f die Nullstelle $\overline{x}$, denn $f(\overline{x}) = \overline{f(x)} = \overline{0}$.

Def. 40 Ist k ein Körper und $f \in k[x]$ prim, dann heißt

$$K := k[x]/k[x] \cdot f$$

Stammkörper zu f über k.

Bem.

- Wegen $\alpha \mapsto \alpha \bmod \mathfrak{a}$ gilt $k \hookrightarrow K$.
- Sind $g, h \in R$, so gilt

$$\overline{h} \cdot \overline{g} = \overline{h \cdot g}, \quad \overline{h} + \overline{g} = \overline{h + g}, \quad \overline{h} - \overline{g} = \overline{h - g}.$$

- Induktiv erhält man einen Erweiterungköper $L \geq K$ derart, daß $f \in L[x]$ in Linearfaktoren zerfällt, also eine Darstellung

$$f(x) = \gamma \cdot \prod_{i=1}^{\partial f} (x - \alpha_i), \qquad (\gamma, \alpha_i \in L)$$

hat. Dieser Körper heißt *Zerfällungskörper* von f.

Def. 41 Sei L/k eine Körpererweiterung. $\alpha \in L$ heißt *algebraisch* über k, falls es ein $0 \neq f \in k[x]$ gibt mit $f(\alpha) = 0$.

Bem. Wenn (wie beim Stamm- und Zerfällungskörper) L/k eine endlichdimensionale Vektorraum-Erweiterung ist, dann ist jedes $\alpha \in L$ algebraisch über k, denn $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$ ist für hinreichend großes n linear abhängig über k. Damit existieren β_i mit

$$\beta_0 + \beta_1 \alpha + \cdots + \beta_n \alpha^n = 0,$$

somit ist α Nullstelle von $f(x) := \sum_{i=1}^{n} \beta_i x^i$.

Def. 42 Sei $(M, \leq)$ eine teilgeordnete Menge. Eine Untermenge $K \leq M$ heißt *Kette*, falls $(K, \leq|_K)$ total geordnet ist. Ein Element $s \in M$ heißt *obere Schranke* von $N \subseteq M$, falls gilt

$$\forall \quad x \in N: \qquad s \geq x.$$

s heißt *maximal*, falls aus $x \in N$ und $x \geq s$ stets folgt $x = s$.

Axiom 1 (Lemma von ZORN) Sei $(M, \leq)$ eine teilgeordnete Menge. Jede Kette in M habe eine obere Schranke. Dann gibt es in M maximale Elemente.

Bem. Dies ist ein Axiom, unabhängig von den anderen Axiomen der Mengelehre. Das ZORNsche Lemma ist äquivalent zum *Auswahlaxiom*:
Sind M_i $(i \in I)$ nichtleere Mengen, dann gilt $\prod_{i \in I} M_i \neq \emptyset$.

Satz 37 Sei R ein kommutativer Ring, $\mathfrak{a} \lhd R$. dann ex. ein maximales Ideal $\mathfrak{m}$ mit $\mathfrak{a} \leq \mathfrak{m} \lhd R$.

11 Der algebraische Abschluß eines Körpers

Def. 43 Ein Körper K heißt *algebraisch abgeschlossen*, falls jedes $f \in K[x]$ mit $\partial f \geq 1$ eine Nullstelle in K hat.

Bsp. $\mathbb{C}$

Satz 38

1. (Fundamentalsatz der Algebra) Im Körper $\mathbb{C}$ hat jedes $f \in \mathbb{C}[x]$ mit $\partial f \geq 1$ eine Nullstelle und damit (über Induktion) auch eine Darstellung

$$f(x) = \gamma \prod_{i=1}^{\partial f} (x - \alpha_i)$$

mit $\alpha_i \in \mathbb{C}$.

2. Sei k ein Körper. Dann existiert eine Erweiterung K/k so, daß K algebraisch abgeschlossen ist (d.h. in $K[x]$ zerfällt jedes Polynom in Linearfaktoren).

Satz 39 (Eindeutigkeit des algebraischen Abschlusses) Seien k, k' Körper, $\sigma : k \to k'$ ein Körperisomorphismus, $L' \geq k'$ eine algebraisch abgeschlossene Erweiterung und $\overline{K}$ der algebraische Abschluß von k. Dann existiert ein Körperisomorphismus $\tau : \overline{K} \to L'$ mit $\tau|_k = \sigma$. Ist L' algebraisch abgeschlossen über k', so gilt weiter $\tau(\overline{K}) = L'$.

12 Endliche Körper

Bem. Sei $\mathbb{F}$ ein Körper mit $|\mathbb{F}| = q < \infty$. Dann ist die Abbildung

$$\mathbb{Z} \to \mathbb{F}, \qquad z \mapsto \sum_{i=1}^{z} 1_{\mathbb{F}}$$

ein Ringhomomorphismus, etwa mit $\mathbb{Z}_p$ (p prim) als Kern. p heißt *Charaktekteristik* von $\mathbb{F}$, Schreibweise $\operatorname{char} \mathbb{F} = p$. Also ist $\mathbb{F}_p \leq \mathbb{F}$ und $\mathbb{F}$ ein endlichdimensionaler Vektorraum über $\mathbb{F}_p$, etwa mit $\dim_{\mathbb{F}_p} \mathbb{F} = n$. Somit gilt $|\mathbb{F}| = q = p^n$.

Satz 40 K sei ein Körper, $f \in K[x]$ sei in $K[x]$ als Produkt von Linearfaktoren darstellbar. Dann gilt:

$$\exists \ \ \xi \in K : \qquad (x - \xi)^2 \mid f \quad \Longleftrightarrow \quad \operatorname{ggT}(f, f') \neq 1$$

Bem. Mit f' ist in obiger Definition die formale Ableitung von f gemeint.

Def. 44 $\mathbb{F}$ sei endlicher Körper der Charakteristik p. Die Abbildung

$$F : \mathbb{F} \to \mathbb{F}, \qquad F(x) := x^p$$

heißt FROBENIUS-*Automorphismus.*

Bem. F ist ein Automorphismus und die Abbildungen

$$F^i : \mathbb{F} \to \mathbb{F}, \qquad F^i(x) := x^{(p^i)}$$

sind ebenfalls Automorphismen.

Satz 41 Sei K ein Körper und G eine Menge von Automorphismen in K. Dann ist die Menge

$$K^G := \{x \in K : \quad \forall\ \sigma \in G : \ \sigma(x) = x\}$$

ein Unterkörper von K.

Satz 42 Sei K ein Körper, $\sigma \in \operatorname{Aut} K$ und $f \in K[x]$ so daß σ alle Koeffizienten von f festhält (d.h. $f \in K^{\langle\sigma\rangle}[x]$). Weiter sei $\varphi \in K$ Nullstelle von f. Dann ist auch $\sigma(\varphi)$ eine Nullstelle von f.

Satz 43 (Hauptsatz der GALOIS-Theorie für endliche Körper)

1. Ein endlicher Körper $\mathbb{F}$ der Charakteristik p (p prim) hat $q = p^n$ Elemente. Umgekehrt gibt es zu $q = p^n$ genau einen Körper $\mathbb{F}$ mit $|\mathbb{F}| = q$ Elementen (bis auf Isomorphie).

2. Die Gruppe $G = \operatorname{Aut} \mathbb{F}$ wird erzeugt von $F = (x \mapsto x^p)$ und ist zyklisch von der Ordnung n.

3. Ist $m \mid n$ und $H = \langle F^m \rangle$, dann ist
$$\mathbb{F}^H := \{x \in \mathbb{F} : \quad \forall\, \sigma \in H : \sigma(x) = x\}$$
der einzige Unterkörper von H der Ordnung p^m.

4. Ist $K \leq \mathbb{F}$ ein Unterkörper mit $|K| = p^m$, dann ist
$$\operatorname{Aut}(\mathbb{F}/K) = \{\sigma \in G : \quad \forall\, x \in K : \sigma(x) = x\}$$
die von F^m erzeugte Untergruppe von G.

Bsp. Der ZECH-Algorithmus Wegen $\mathbb{F}_q^\times = \langle w \rangle$ läßt sich jedes $x \in \mathbb{F}_q^\times$ auf genau eine Weise schreiben als $x = w^i$ $(0 \leq i < q-1)$. Dafür schreiben wir $i = \log_w x$ und definieren $* := \log_w 0$.

Sind nun $i = \log_w x, j = \log_w y$, so gilt
$$x = w^i, y = w^j \implies x \cdot y = w^{i+j} \implies \log_w(x \cdot y) = i + j \bmod (q-1).$$
Analog folgt $\log_w \frac{x}{y} = i - j \bmod (q-1)$. Zur Addition geht man wie folgt vor: Es gilt (o.B.d.A. $i \leq j$)
$$x + y = w^i + w^j = w^i \cdot (1 + w^{j-i}).$$
Man legt eine Tabelle aller $\log_w(1 + w^k)$ $(0 \leq k < q-1)$ an („ZECH-Tabelle"). Durch diese Tabelle ist die Addition auf die Multiplikation reduziert. Die Subtraktion ist auf Addition und Multiplikation mit -1 reduzierbar.

Sei z.B. $K = \mathbb{F}_{16} = \mathbb{F}_2[x]/(f)$ mit $f(x) = x^4 + x + 1$. In diesem Fall ist die Primitivwurzel w die Restklasse von x. $\alpha \in \mathbb{F}_{16}$ ist darstellbar als
$$\alpha_0 + \alpha_1 w + \alpha_2 w^2 + \alpha_3 w^3 \qquad (\alpha_i \in \mathbb{F}_2).$$
Jedes solche Polynom wird mit einer Nummer N codiert mit
$$N := \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \alpha_3 p^3 \quad (\alpha_i \in \mathbb{F}_2 \subseteq \{0,1\} \subseteq \mathbb{N}).$$
Dann trägt man in die Tabelle ein: $A[i] := N(w^i)$, $B[i]$ das Inverse von $A[i]$ und $Z[i] = \log_w(1 + w^i)$. Im Beispiel:

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$A[i]$	1	2	4	8	3	6	12	11	5	10	7	14	15	13	9	0
$B[i]$	15	0	1	4	2	8	5	10	3	14	9	7	6	13	11	12
$Z[i]$	15	4	8	14	1	10	13	9	2	7	5	12	11	6	3	0

Ist zum Beispiel $y = 1 + w$ und $z = w + w^2$, dann ist $N(y) = 3, N(z) = 6$ und damit

$$\begin{aligned} & \log_w(y) = B[3] = 4, \ \log_w(z) = B[6] = 5 \\ \Longrightarrow \quad & \log_w(y \cdot z) = 4 + 5 = 9. \end{aligned}$$

Die Decodierung liefert

$$N(y \cdot z) = A[9] = 10 = 2 + 8 \quad \Longrightarrow \quad y \cdot z = w + w^3.$$

Bem.

- Sei $f \in \mathbb{F}_q^\times$ gegeben. Falls f in einem Erweiterungskörper $K \geq \mathbb{F}_q$ einen quadratischen Faktor $(x-\alpha)^2$ hat, dann gilt $(x-\alpha) \mid \mathrm{ggT}(f, f')$.
- Man kann $\mathrm{ggT}(f, x^{(q^i)} - x)$ schnell berechnen unter Verwendung der Methode zum binären Potenzieren.

Satz 44

1. k, k' seien Körper und $\sigma : k \to k'$. $f \in k[x]$ sei prim, ϑ sei Nullstelle von f, $K := k(\vartheta)$. Dann ist auch $\sigma(f) \in k'[x]$ prim. Sei $K' = k(\vartheta')$, wobei ϑ' Nullstelle von $\sigma(f)$ ist. Dann existiert genau eine Fortsetzung $\tau : K \to K'$ von σ mit $\tau|_K = \sigma$ und $\tau(\vartheta) = \vartheta'$.
2. Sei $f \in k[x]$ beliebig und $\vartheta_1, \vartheta_2, \ldots, \vartheta_m$ seien Nullstellen von f. Weiter seien $K = k(\vartheta_1, \vartheta_2, \ldots, \vartheta_m)$, $\sigma : k \to k'$, $\vartheta'_1, \vartheta'_2, \ldots, \vartheta'_m$ die Nullstellen von $\sigma(f)$ und $K' = k'(\vartheta'_1, \vartheta'_2, \ldots, \vartheta'_m)$. Dann existiert (mindestens) eine Fortsetzung τ von σ mit $\tau(\vartheta_i) = \vartheta'_i$ $(i = 1, \ldots, m)$.
3. $\mathrm{Aut}(K/k)$ läßt sich auffassen als Untergruppe von S_m vermöge der Permutationen der Nullstellen von φ_i.

Bem. Das kommutative Diagramm zu (1):

$$\begin{array}{ccc} K & \xrightarrow{\tau} & K' \\ \| & & \| \\ k & \xrightarrow{\sigma} & k' \end{array}$$

Def. 45 Sei K/k eine Körpererweiterung.

1. K/k heißt *endlich*, falls $K = k(\vartheta_1, \ldots, \vartheta_n)$.
2. $\vartheta \in K$ heißt *algebraisch* über k, falls gilt $\dim_k k(\vartheta) < \infty$, sonst *transzendent*.
3. K/k heißt *algebraisch*, falls alle $\vartheta \in K$ algebraisch sind.
4. K/k heißt *einfach*, falls es ein ϑ gibt mit $K = k(\vartheta)$.

Bem. Ist K/k eine Körpererweiterung, dann schreibt man auch (K/k) statt $\dim_k K$ und nennt diese Zahl den *Körpergrad*.

Satz 45 (Gradschachtelungsformel) Für $K \leq L \leq M$ gilt

$$(M/K) = (M/L) \cdot (M/K).$$

Def. 46 Sei $L = K(\vartheta)$ eine einfache algebraische Erweiterung. Mit f_φ sei das Minimalpolynom von φ bezeichnet, also das normierte Polynom kleinsten Grades in $K[x]$ mit $f_\vartheta(\vartheta) = 0$. Für $\alpha \in L$ sei

$$M_\alpha : L \to L, \qquad M(\beta) := \alpha \cdot \beta.$$

$D_B(M_\alpha)$ sei eine Darstellungsmatrix von M_α bezüglich einer K-Basis von L. Das charakteristische Polynom von M_α wird mit $g_\alpha := g_{L/K,\alpha}$ bezeichnet und heißt *Hauptpolynom* von α.

$$S_{L/K}(\alpha) := \mathrm{Spur}(M_\alpha) := \mathrm{Spur}(D_B(M_\alpha))$$

heißt die *Spur* und $N_{L/K} := \det M_\alpha$ heißt die *Norm* von M_α.

Bem.

- In der Situation $K \leq L \leq M$ gilt:

$$\begin{aligned} N_{M/K}(\vartheta) &= \left(N_{L/K}(\vartheta)\right)^{(M/L)}, \\ S_{M/K}(\vartheta) &= (M/L) \cdot S_{L/K}(\vartheta). \end{aligned}$$

- Falls überdies $L = K(\vartheta)$ gilt und $f_{L/K,\vartheta}$ das Minimalpolynom ist, so gilt

$$g_{M/K,\vartheta} = \left(f_{L/K,\vartheta}\right)^{(M/L)}$$

13 Resultanten und Diskriminante

Def. 47 Sei K ein Körper und $f, g \in K[x]$ mit $\partial f = m$, $\partial g = n$,

$$f(x) = f_0 + f_1 x + \cdots + f_m x^m, \quad g(x) = g_0 + g_1 x + \cdots + g_n x^n.$$

Dann heißt die Determinante der Matrix

$$A := \begin{pmatrix} f_0 & 0 & \cdots & 0 & g_0 & 0 & \cdots & 0 \\ f_1 & \ddots & \ddots & \vdots & g_1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & \ddots & \ddots & 0 \\ f_m & & \ddots & f_0 & \vdots & & \ddots & g_0 \\ 0 & \ddots & & f_1 & g_n & & & g_1 \\ \vdots & \ddots & \ddots & \vdots & 0 & \ddots & & \vdots \\ \vdots & & \ddots & f_m & \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 & 0 & \cdots & 0 & g_n \end{pmatrix}$$

die *Resultante* von f und g, Schreibweise: $\mathrm{Res}(f, g) := \det A$.

Bem.

- Zu $f \in K[x]$ heißt $\operatorname{Dis} f := \operatorname{Res}(f, f')$ die *Diskriminante*.
- Für $u = (u_0, \ldots, u_{m-1}), v = (v_0, \ldots, v_{n-1}) \in K[x]$ ist die Gleichung $h = fu + gv$ genau dann lösbar, wenn das lineare Gleichungssystem

$$\begin{pmatrix} f_0 & 0 & \cdots & 0 & g_0 & 0 & \cdots & 0 \\ f_1 & \ddots & \ddots & \vdots & g_1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & \ddots & \ddots & 0 \\ f_m & & \ddots & f_0 & \vdots & & \ddots & g_0 \\ 0 & \ddots & & f_1 & g_n & & & g_1 \\ \vdots & \ddots & \ddots & \vdots & 0 & \ddots & & \vdots \\ \vdots & & \ddots & f_m & \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 & 0 & \cdots & 0 & g_n \end{pmatrix} \begin{pmatrix} u_0 \\ \vdots \\ u_{m-1} \\ v_0 \\ \vdots \\ v_{n-1} \end{pmatrix} = \begin{pmatrix} h_0 \\ h_1 \\ \vdots \\ \vdots \\ \vdots \\ h_{m+n-1} \end{pmatrix}$$

  lösbar ist. Dies aber ist genau dann der Fall, wenn $\operatorname{Res}(f, g) \neq 0$.

Satz 46 Ein Polynom f hat in einem Erweiterungskörper genau dann mehrfache Nullstellen, wenn seine Diskriminante verschwindet.

Def. 48

1. Ein Polynom f heißt *separabel*, wenn gilt $\operatorname{Dis} f \neq 0$.
2. Sei K/k eine Körpererweiterung. $\varphi \in K$ heißt *separabel*, wenn $f_{K/k,\varphi}$ separabel ist.

Bsp. Betrachte $k = \mathbb{F}_p(y) := \operatorname{Quot}(\mathbb{F}_p[y])$. In $k[x, y]$ ist $f(x) := x^p - y$ ein Primpolynom. Nach dem Lemma von Gauss ist f dann auch irreduzibel in $\mathbb{F}_p(y)[x]$. Es gilt $f'(x) = px^{p-1} = 0$ und damit $\operatorname{ggT}(f, f') \neq 1$. Damit ist f nicht separabel.

Satz 47 (Satz vom primitiven Element) Sei $K = k(\alpha_1, \ldots, \alpha_n)$ (α_i algebraisch über k). Sind $\alpha_2, \ldots, \alpha_n$ separabel, so existiert ein $\varphi \in K$ mit $K = k(\varphi)$.

Bem. Im Folgenden seien alle Körpererweiterungen endlich algebraisch. Alternative Formulierung des obigen Satzen: Eine einfache separable Erweiterung L/k einer einfachen Erweiterung K/k ist wieder eine einfache Erweiterung K/k. Zu K/k definieren wir

$$\mathcal{L} := \{L \text{ Körper}: \quad k \leq L \leq K\}$$

Satz 48 Genau dann ist K/k eine einfache Erweiterung, wenn $\mathcal{L}_{K/k}$ endlich ist.

Def. 49 Sei $\overline{K}$ der algebraische Abschluß von K. L/K sei eine endliche algebraische Erweiterung. Dann heißt

$$(L/K)_{sep} := |\operatorname{Hom}_K(L, \overline{K})|$$

der *Separabilitätsgrad* von L/K.

Satz 49 Sei $M \geq L \geq K$. Dann gilt

$$(M/K)_{sep} = (M/L)_{sep} \cdot (L/K)_{sep}.$$

Bem. $|\mathrm{Hom}_k(L, \overline{K})|$ ist die Anzahl der verschiedenen Nullstellen des Minimalpolynoms f_α in $\overline{K}$ für $L = K(\alpha)$. Daher gilt:

$$L/K \text{ ist separabel} \quad \Longleftrightarrow \quad (L/K)_{sep} = (L/K).$$

Satz 50 Sei K ein Körper der Charakteristik $p > 0$ und $f \in K[x]$ irreduzibel. Dann gilt:

1. f Es gibt ein $d \geq 0$ und ein irreduzibles und separables Polynom $g \in K[x]$ mit $f(x) = g(x^{p^d})$.
2. Jede Nullstelle von f in $\overline{K}$ hat die Vielfachheit p^d.

Bem. Sei L/K endlich algebraisch. Dann sind folgende Aussagen äquivalent:

- L/K ist separabel.
- Jedes $\alpha \in L$ ist separabel über K.
- Es gibt über K separable $\alpha_1, \ldots, \alpha_n \in L$ mit $L = K(\alpha_1, \ldots, \alpha_n)$.

Weiter gilt: Sind M/L und L/K separabel, so ist auch M/K separabel.

Def. 50 Zu L/K heißt

$$(L/K)_i := \frac{(L/K)}{(L/K)_{sep}}$$

der *Inseparabilitätsgrad.*

Bem. Auch hier gilt für $M \geq L \geq K$ die Gradschachtelungsformel

$$(M/K)_i = (M/L)_i \cdot (L/K)_i.$$

Weiter gilt $(L/K)_i = p^d$.

Def. 51 L/K heißt *rein inseparabel,* falls gilt $(L/K) = (L/K)_i$. Ist speziell $L = K(\alpha)$, so heißt auch α rein inseparabel.

Bem. α ist genau dann rein inseparabel, wenn $f_{\alpha,K}$ die Form $f_{\alpha,K}(x) = x^{p^m} - c$ für ein $c \in K$ hat.

Satz 51 L/K sei eine endliche algebraische Erweiterung. Dann existiert ein eindeutig bestimmter Zwischenkörper $L \geq K_s \geq K$, so daß K_s/K separabel und L/K_s rein inseparabel ist.

Bem. K_s heißt der *separable Abschluß* von K in L.

14 Allgemeine GALOIS-Theorie endlicher algebraischer Körper

Satz 52 (Satz von DEDEKIND) K, K' seien Körper, $\sigma_i : K \to K'$ seien paarweise verschiedene Körperisomorphismen ($1 \le i \le n$). Dann ist die Menge

$$\{\sigma_1, \ldots, \sigma_n\} \subseteq \mathrm{Abb}(K \to K')$$

linear unabhängig.

Satz 53 (Satz von ARTIN)

1. $S := \{\sigma_1, \ldots, \sigma_n\}$ sei ein endliches System paarweise verschiedener Monomorphismen $K \to K'$ und

   $$K^S := \{\alpha \in K : \quad \sigma_1(\alpha) = \sigma_2(\alpha) = \cdots = \sigma_n(\alpha)\}.$$

   Dann gilt $(K : K^S) = |S|$.

2. Ist speziell $K = K'$ und $S = G$ eine Gruppe von Automorphismen in K, so gilt $(K : K^G) = |G|$.

3. Ferner gilt dann $G = \mathrm{Aut}({}^{K}\!/_{K^G})$.

Def. 52 Eine endliche Erweiterung K/k heißt GALOISsch mit GALOIS-Gruppe $G = \mathrm{Aut}(K/k)$, wenn gilt $k = K^G$. In diesem Fall schreibt man auch $G = \mathrm{Gal}(K/k)$.

Bsp. Sei $k = \mathbb{Q}$ und $f(x) = x^3 - 2$. f ist irreduzibel. Sei $\vartheta \in \mathbb{R}$ eine Nullstelle von f und $K = k(\vartheta)$. Dann gilt $(K : k) = 3$ und $\mathrm{Aut}(K/k) = \{\mathrm{id}\}$, weil $\sigma(\varphi)$ Nullstelle von f sein muß. Damit ist $K^G = K$ nicht GALOISsch.

Satz 54 Sei $f \in k[x]$ irreduzibel mit $\partial f = n$ und φ eine Nullstelle von f. $K := k(\vartheta)$ sei ein Stammkörper von f. Wenn f in K n verschiedene Nullstellen hat, dann ist K/k GALOISsch.

Satz 55 (Hauptsatz der GALOIS-Theorie) K/k sei eine endliche GALOISsche Erweiterung, $G = \mathrm{Gal}(K/k)$. Weiter seien:

$$\begin{aligned}
&\mathcal{L} = \mathcal{L}_{K/k} = \{L : \ k \le L \le K\},\\
&\mathcal{H} = \mathcal{H}_G = \{H : \ H \le G\},\\
&\varphi : \mathcal{L} \to \mathcal{H}, \quad \varphi(L) = \mathrm{Aut}(K/L) \le G,\\
&\psi : \mathcal{H} \to \mathcal{L}, \quad \psi(H) = K^H.
\end{aligned}$$

$$\begin{array}{ccc}
K & & E \\
\| & \xrightarrow{\ \varphi\ } & \| \\
L & & H \\
\| & \xleftarrow{\ \psi\ } & \| \\
k & & G \\
\mathcal{L} & & \mathcal{H}
\end{array}$$

Dann gilt

1. Die Abbildungen φ und ψ sind zueinander invers.

2. Aus $\varphi(L) = H$ folgt $(K : L) = |H|$ und $(L : K) = (G : H)$.

3. Aus $\varphi(L) = H$ folgt: Die Körperisomorphismen $\tilde{\sigma} : L \to K$ stehen in Bijektion zu den Restklasssen $\sigma H \in {}^{G}\!/_{H}$.

4. L und L' sind als Körper genau dann zueinander adjungiert, wenn $\varphi(L)$ und $\varphi(L')$ als Gruppen zueinander adjungiert sind.

5. L/k ist genau dann GALOISsch, wenn $H = \varphi(L)$ Normalteiler in G ist. In diesem Fall ist
$$f : G \to \mathrm{Gal}(L/k), \qquad f(\sigma) := \sigma|_L$$
ein Homomorphismus mit Kern $f = H$ und $\mathrm{Gal}(L/k) \cong {}^{G}\!/_{H}$.

6. φ und ψ sind Verbandsantiisomorphismen.

Bem. Ist K/k eine endliche algebraische Erweiterung, so ist $\mathcal{L}_{K/k}$ endlich. Also gibt es ein $\vartheta \in K$ mit $K = k(\vartheta)$. Das Minimalpolynom f_ϑ von ϑ ist irreduzibel in $k[x]$. Für $\sigma \in G$ gilt
$$\sigma(f(\vartheta)) = f(\sigma(\vartheta)) = 0 \quad\Longrightarrow\quad f_\vartheta(x) = \prod_{\sigma \in G} (x - \sigma(\vartheta)).$$
σ ist also durch $\sigma(\vartheta)$ festgelegt. Die $\sigma(\vartheta)$ sind damit paarweise verschieden. Daraus folgt, daß f_ϑ separabel ist. Jede GALOISsche Erweiterung ist somit separabel.

Def. 53 G sei eine Gruppe und K sei ein Körper. Ein Homomorphismus $\sigma : G \to K^\times$ heißt ein *Charakter* von G mit Werten in K.

Satz 56 Seien $\sigma_1, \ldots, \sigma_n$ paarweise verschiedene Charaktere von $G \leq K$. Dann sind diese linear unabhängig als Elemente des K-Vektorraums $\mathrm{Abb}(G \to K)$.

15 Normale Erweiterungen

Es bezeichne $S(K/k) := \mathrm{Hom}_k(K, \overline{K})$. (Damit ist also $S(K/k) \supseteq \mathrm{Aut}(K/k)$).

Satz 57 Ist K/k algebraisch, so ist jedes $\sigma \in S(K/k)$ mit $\sigma(k) \subseteq K$ auch surjektiv.

Satz 58 K/k sei eine algebraische Erweiterung. Dann sind folgende Aussagen äquivalent:

1. $S(K/k) = \mathrm{Aut}(K/k)$

2. Ist $f \in k[x]$ irreduzibel und hat f in k eine Nullstelle, so zerfällt f in $K[x]$ in Linearfaktoren.

Bem. Eine Erweiterung K/k, die die Eigenschaft des obigen Satzes erfüllt, heißt *normal*.

Satz 59 K/k sei eine endliche algebraische Erweiterung. Dann gilt: K/k ist genau dann normal, wenn K der Zerfällungskörper eines Polynoms $f \in k[x]$ ist.

Bem.

- $\overline{K}/k$ ist normal.
- Ist K/k GALOISsch, dann ist K/k auch normal.
- Ist L/k eine endliche algebraische Erweiterung, dann existiert ein K/L derart, daß K/k normal ist.

Satz 60 K/k sei endliche algebraische Erweiterung. Dann gilt: K/k ist genau dann GALOISsch, wenn K der Zerfällungskörper eines separablen Polynoms $f \in k[x]$ ist.

16 Bestimmung der GALOIS-Gruppe

Def. 54 Es sei $\mathbb{P} := \{2, 3, 5, \ldots\}$ die Menge aller natürlichen Primzahlen. Zu $M \subseteq \mathbb{P}$ heißt

$$\delta(M) := \lim_{x \to \infty} \frac{|\{p \in M :\ p \leq x\}|}{|\{p \in \mathbb{P} :\ p \leq x\}|}$$

die *Dichte* von M in $\mathbb{P}$, falls dieser Grenzwert existiert.

Bsp. Ist $M = \{p \in P :\ p \equiv 1\,(4)\}$, dann ist $\delta(M) = \frac{1}{2}$.

Bem. Sei $f \in \mathbb{Z}[x]$ normiert, $p \in P$ und $\overline{f} := f \bmod p \in \mathbb{F}_p[x]$. Es gilt

$$f \text{ separabel} \quad \Longleftrightarrow \quad \operatorname{Dis} f \neq 0$$

und

$$\overline{f} \text{ separabel} \quad \Longleftrightarrow \quad p \nmid \operatorname{Dis} f.$$

Im Folgenden sei stets $p \nmid \operatorname{Dis} f$.

Def. 55 $f \bmod p$ hat den *Zerlegungstyp* $(n_1, n_2, \ldots, n_k)$, falls $\overline{f} = f \bmod p$ in $\mathbb{F}_p[x]$ Primfaktoren der Grade $n_1, n_2, \ldots, n_k$ hat.

Bem. Die GALOIS-Gruppe $G := \operatorname{Gal} f \leq S_{\partial f}$ ist bestimmt durch die Operation auf den Nullstellen von f.

Def. 56 $\sigma \in G$ hat den *Zerlegungstyp* $(n_1, n_2, \ldots, n_k)$, falls $\sigma = \zeta_1 \zeta_2 \ldots \zeta_k$ mit elementweise disjunkten Zyklen ζ_i ist.

Def. 57 Eine *Konjugiertenklasse* $C \subseteq G$ ist die Bahn eines $\sigma \in G$ unter der Operation

$$G \times G \to G, \qquad (\tau, \sigma) \mapsto \tau\sigma\tau^{-1}.$$

Satz 61 (Satz von TSCHEBOTARÖW) Sei $f \in \mathbb{Z}[x]$ normiert und separabel mit $\partial f =: n$. $G \leq S_n$ sei die GALOIS-Gruppe des Zerfällungskörpers von f über $\mathbb{Q}$. Weiter seien $(n_1, n_2, \ldots, n_k)$ mit $\sum_{i=1}^{k} n_i = n$. Dann existiert $\delta(M)$, wobei

$$M = \{p \in \mathbb{P} : \text{ der Zerlegungstyp von } f \bmod p \text{ ist } (n_1, \ldots, n_k)\}$$

und es gilt

$$\delta(M) = \frac{|\{\sigma \in G : \text{ der Zerlegungstyp von } \sigma \text{ ist } (n_1, \ldots, n_k)\}|}{|G|}.$$

Bsp. Sei $n = 4$ und $G \leq S_4$. Es gilt

$$f \text{ ist irreduzibel} \iff G \text{ ist transitiv auf } \{1, 2, 3, 4\}.$$

G	Zyklen	Anzahl
S_4	1111	1
	211	6
	22	3
	31	8
	4	6
A_4	1111	1
	22	3
	31	8
D_4	1111	1
	211	2
	22	3
	4	2
V_4	1111	1
	22	3
Z_4	1111	1
	22	1
	4	2

Daraus ergibt sich für das spezielle $f(x) = x^4 - 4x^3 - 4x + 13$

Typ	211	22	4
mod$p$	11.23	7.19	5.17

also kommen nur $G = D_4$ und $G = S_4$ in Frage.

Bem. In den meisten Fällen kann man die GALOIS-Gruppe auf diese Weise erraten. Es gibt jedoch Ausnahmen: Die beiden Gruppen G_1, G_2 der Ordnung $3 \cdot 7 \cdot 13$ sind Untergruppen von S_{91} und anhand ihrer Zyklentypen nicht unterscheidbar.

Meistens verbleibt ein Restproblem der Form $H \leq G \leq S_n$, wobei $\mathrm{Gal} f \leq G$ bekannt ist. In diesem Fall ist man daran interessiert, ob auch $\mathrm{Gal} f \leq H$ gilt.

Def. 58 Sei k_0 ein Körper und a_i seien die elementar-symmetrischen Funktionen in $x_1, \ldots, x_n$. Weiter seien $K := k_0(x_1, \ldots, x_n)$, $f \in k_0[a_0, \ldots, a_{n-1}, x]$ und $k = k_0(a_0, \ldots, a_{n-1})$. Weiter gelte $H \leq G \leq S_n$. Ein primitives Element

$\varphi_{G/H}(x_1,\ldots,x_n)$ von K^H/K^G heißt *primitive Invariante* von H bezüglich G. In diesem Fall schreibt man

$$F_{G/H}(x_1,\ldots,x_n,x) = \prod_{\sigma\in G/H} (x - \sigma(\varphi_{G/H}))$$

für das Minimalpolynom von $\varphi_{G/H}$ in K^H/K^G.

Satz 62 f_0 in $k_0[x]$ sei ein normiertes, separables Polynom mit den Nullstellen $\xi_1,\ldots,\xi_n \in \overline{k}_0$. Es gelte $H \leq G \leq S_n$ und $\mathrm{Gal}\, f_0 \leq G$. Bei der Spezialisierung $x_i \mapsto \xi_i$ bleibe $F_{G/H}(\xi_1,\ldots,\xi_n,x)$ separabel. Dann gibt es ein $\sigma\in G$ mit

$$\mathrm{Gal}\, f_0 \leq H^\sigma \quad\iff\quad F_{G/H}(\xi_1,\ldots,\xi_n,x) \text{ hat Nullstellen in } k_0.$$

Bsp. Betrachte das TRINKS-*Polynom*

$$f(x) = x^7 - 7x + 3.$$

Es gilt $\mathrm{Dis}\, f = 3^8 - 7^8$ und damit $\mathrm{Gal}\, f \leq A_7$. Prüft man die Zerlegungstypen mod p für $p \leq 10\,000$, so drängt sich die Vermutung auf, daß $\mathrm{Gal}\, f$ die einfache Gruppe der Ordnung 168, G_{168}, ist. Es gilt

$$G_{168} = \langle (1\,2\,3\,4\,5\,6\,7), (2\,3\,5)(4\,7\,6), (2\,4)(3\,5\,7\,6)\rangle \cong PGL(3,\mathbb{F}_2) \cong PSL(2,\mathbb{F}_7).$$

Setze $\vartheta_{A_7/G_{168}} = x_1x_2x_4 + x_2x_3x_5 + \cdots$ und numeriere die Nullstellen von f in $\mathbb{C}$ wie folgt:

$$\begin{aligned}
\xi_1 &:= 1.44\ldots\\
\xi_2 &:= 0.42\ldots\\
\xi_4 &:= 1.29\ldots\\
\xi_{3/5} &:= 0.61\cdots \pm 1.21\ldots \mathrm{i}\\
\xi_{6/7} &:= -0.75\cdots \pm 1.20\ldots \mathrm{i}.
\end{aligned}$$

Dann hat das Polynom

$$F_{A_7/G_{168}}(\xi_1,\ldots,\xi_7,x) = x^{15} - 147x^{13} + 4116x^{11} + 120050x^9 + \cdots$$

die Nullstelle -7. Damit ist $\mathrm{Gal}\, f = G_{168}$.

17 Die „Auflösung von Gleichungen" durch Radikalausdrücke

Satz 63 Sei k ein Körper der Charakteristik 0 und $f(x) = x^n - 1 \in k[x]$. Dann gilt:

1. $\mathrm{Gal}\, f$ ist ABELsch.
2. Zerfällt f in $k[x]$ in Linearfaktoren, so gilt:

$$\forall \quad a\in k: \qquad \mathrm{Gal}(x^n - a) \leq Z_n$$

Satz 64 Sei k ein Körper, p prim. k enthalte p verschiedene p-te Einheitswurzeln. K/k sei eine GALOISsche Erweiterung mit zyklischer GALOIS-Gruppe Z_p. Dann ist K von der Form $K = k(b)$ für ein b mit $b^p \in k$.

Satz 65 (Verschiebungssatz) Sei $f \in k[x]$ und $L \geq K$. Dann gilt $\mathrm{Gal}(f/K) \leq \mathrm{Gal}(f/k)$.

Def. 59 Eine Folge $k_0 \leq k_1 \leq \cdots$ von Körpererweiterungen heißt *Wurzelturm*, falls gilt $k_i = k_{i-1}(\vartheta_i)$ mit $\vartheta_i^{n_i} \in k_{i-1}$.

Bem. Nach Satz 64 wird k_i GALOISsch mit zyklischer GALOIS-Gruppe, falls die n_i-ten Einheitswurzeln in k_{i-1} enthalten sind und $\operatorname{char} k_0 = 0$ ist.

Satz 66 Sei $k = k_0 \leq k_1 \leq k_2 \leq \cdots$ ein Wurzelturm. Dann exsitiert eine GALOISsche Erweiterung L/k, die ebenfalls in einem Wurzelturm enthalten ist.

Satz 67 (Hauptsatz von GALOIS über die Auflösbarkeit von Gleichungen) Sei k ein Körper der Charakteristik 0 und $f \in k[x]$ durch Radikale auflösbar. Dann ist nach Adjunktion von Einheitswurzeln an den Grundkörper k jede Stufe k_{i+1}/k_i des Wurzelturms zyklisch (GALOISsch), also die zugehörige Gruppe $H_{i+1} \trianglelefteq H_i$ mit H_i/H_{i+1} zyklisch.

Umkehrung: Ist $G = \mathrm{Gal}(K/k)$ auflösbar (d.h. G hat eine Kompositionsreihe mit zyklischen Kompositionsfaktoren), so ist nach Adjunktion von Einheitswurzeln an k der Körper K in einem Wurzelturm enthalten.

Bem. Da es nicht auflösbare Gruppen gibt (z.B. A_n für $n \geq 5$), ist die allgemeine Gleichung n-ten Grades nicht durch Wurzeln darstellbar.

Satz 68

1. (Satz von VAN DER WARDEN)

$$\lim_{n\to\infty} \frac{|\{f = \sum_{i=0}^{n} a_i x^i : \ |a_i| \leq x, \ \ \mathrm{Gal}\, f = S_n\}|}{|\{f = \sum_{i=0}^{n} a_i x^i : \ |a_i| \leq x\}|} = 1$$

   D.h. Polynome f mit $\mathrm{Gal}\, f \neq S_n$ sind sehr selten.

2. (Satz von ŠAFAREVIČ) Für jede auflösbare Gruppe G gibt es ein Polynom f mit $\mathrm{Gal}\, f = G$.

18 NOETHERsche Ringe und Moduln

In diesem Abschnitt sei R stets ein kommutativer Ring. Statt „M ist R-Modul“ schreiben wir „$M \in {}_R\mathcal{M}$“. Damit soll aber nicht gesagt sein, daß ${}_R\mathcal{M}$ eine Menge ist.

Def. 60 Sei $M \in {}_R\mathcal{M}$. M heißt NOETHERsch, falls gilt: Jede aufsteigende Kette $N_1 \leq N_2 \leq \cdots$ von R-Untermoduln von M wird stationär.

Bem. Folgende Aussagen sind äquivalent:

- M ist NOETHERsch.
- Jeder R-Untermodul $N \leq M$ ist endlich erzeugt.
- Jede Menge $\mathcal{N} \neq \emptyset$ von R-Untermoduln von M hat ein maximales Element.

Def. 61 R heißt NOETHER*sch*, falls $R = R^1$ als R-Modul NOETHERsch ist.

Bem. Da ein R-Untermodul von R ein Ideal ist, sind äquivalent:

- R ist NOETHERsch.
- Jede Idealkette $\mathfrak{a}_1 \leq \mathfrak{a}_2 \leq \cdots$ wird stationär.
- Jedes Ideal ist endlich erzeugt.
- Jede nichtleere Menge von Idealen hat ein maximales Element.

Def. 62 Eine Folge von Gruppenhomomorphismen der Art

$$M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \xrightarrow{f_3} \cdots$$

heißt *exakt* bei M_2, falls gilt Bild $f_1 =$ Kern f_2. Eine Folge heißt insgesamt *exakt*, wenn sie an jeder Stelle exakt ist.

Bem.

- Seien $M_i \in {}_R\mathcal{M}$ und

  $$0 \longrightarrow M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \longrightarrow 0$$

  exakt. Dann gilt $M_3 \cong {}^{M_2}/_{M_1}$.
- Wenn R NOETHERsch ist, dann sind auch NOETHERsch: R^n, ${}^R/_{\mathfrak{a}}$ ($\mathfrak{a}$ Ideal von R), und $S^{-1}R$ (S Untermonoid von $(R, \cdot)$).
- Jeder endlich erzeugte Modul M eines NOETHERschen Rings R ist wieder NOETHERsch, denn

  $$0 \longrightarrow \text{Kern}\,\varphi \longrightarrow R^n \longrightarrow M \longrightarrow 0$$

  ist exakt, wenn man $\varphi(e_i) := x_i$ setzt ($i = 1, \ldots, n$, e_i i-ter Standardbasisvektor in R^n).

Satz 69 (Basissatz von HILBERT) R sei ein kommutativer NOETHERscher Ring. Dann auch $R[x]$ NOETHERsch.

19 Maximale Ideale, Primideale und Primärzerlegungen

Def. 63 Ein Ideal $\mathfrak{m} \trianglelefteq R$ heißt *maximal*, wenn es kein Ideal $\mathfrak{a}$ mit $\mathfrak{m} < \mathfrak{a} < R$ gibt. Ein Ideal $\mathfrak{p}$ heißt *prim*, falls $R/\mathfrak{p}$ ein integrer Ring ist. Weiter definieren wir das *Spektrum* von R durch

$$\operatorname{Spec} R := \{\mathfrak{p} \trianglelefteq R : \ \mathfrak{p} \text{ prim}\}$$

Bsp.

- $\{0\}$ ist genau dann prim, wenn R integer ist
- Es ist $\operatorname{Spec} \mathbb{Z} = \{0\} \cup \{p\mathbb{Z} : \ p \text{ prim}\}$

Def. 64 Sei $M \in {}_R\mathcal{M}$ und $a \in R$. Der Endomorphismus a_M sei definiert durch

$$a_M : M \to M, \qquad a_M(x) = ax.$$

Def. 65

1. Ein $a \in R$ heißt *nilpotent*, falls gilt:
$$\exists \quad n \in \mathbb{N} : \qquad a^n = 0.$$
2. Ein Ideal $\mathfrak{p} \trianglelefteq R$ heißt *primär*, falls jeder Nullteiler von $R/\mathfrak{p}$ nilpotent ist.
3. Sei $M \in {}_R\mathcal{M}$, $N < M$. N heißt *primär* in M, falls für jedes $A \in R$ der Endomorphismus $a_{M/N}$ entweder injektiv oder nilpotent ist.

Satz 70 Sei Q primär in $M \in {}_R\mathcal{M}$. Dann ist die Menge

$$\mathfrak{p} := \{a \in R : \ a_{M/Q} \text{ ist nilpotent}\}$$

ein Primideal.

Bem.

- $\mathfrak{p}$ heißt das zu $Q < M$ *gehörige* Primideal.
- Speziell für $M = R$ und $Q = \mathfrak{q}$ schreibt man $\mathfrak{p} := \sqrt{\mathfrak{q}}$. (*Radikal* von $\mathfrak{q}$).

Satz 71 Seien $Q_1, Q_2, \ldots, Q_t < M$ primär zum selben Primideal $\mathfrak{p}$. Dann ist auch

$$Q := \bigcup_{i=1}^{t} Q_i$$

primär zu $\mathfrak{p}$.

Def. 66 Seien $M, N \in {}_R\mathcal{M}$, $N < M$. Eine Relation

$$N = Q_1 \cup Q_2 \cup \cdots \cup Q_t,$$

wobei alle Q_i in M primär zu $\mathfrak{p}_i$ seien, heißt *Primärzerlegung* von N in M.

Bem. Gibt es eine Primärzerlegung, so kann man eine Primärzerlegung finden, bei der die Ideale $\mathfrak{p}_i$ paarweise verschieden sind.

Satz 72 (Primidealvermeidungslemma) Es seien $\mathfrak{b}, \mathfrak{a}_1, \mathfrak{a}_2, \dots, \mathfrak{a}_n \trianglelefteq R$. Von den Idealen $\mathfrak{a}_i$ seien höchstens zwei nicht prim. Dann folgt aus

$$\mathfrak{b} \subseteq \mathfrak{a}_1 \cup \mathfrak{a}_2 \cup \dots \cup \mathfrak{a}_n$$

die Existenz eines i mit $\mathfrak{b} \subseteq \mathfrak{a}_i$.

Satz 73 (Satz von Laskar) $M \in {}_R\mathcal{M}$ sei NOETHERsch und $N < M$. Dann gibt es eine Primärzerlegung von N in M.

Bem. Ist R ein Hauptidealring, so sind die primären Ideale genau die $p^n R$, wobei p Primelement ist.

Satz 74 Seien $M, N \in {}_R\mathcal{M}$, $N > M$ und

$$N = \bigcap_{i=1}^{s} Q_i = \bigcap_{j=1}^{t} Q'_j$$

zwei Primärzerlegungen, $\mathfrak{p}_i$ sei das zu Q_i und $\mathfrak{p}'_j$ das zu Q'_j gehörige Primideal. Dann gilt $s = t$ und

$$\{\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_s\} = \{\mathfrak{p}'_1, \mathfrak{p}'_2 \dots, \mathfrak{p}'_r\}.$$

Ist $\mathfrak{p}_i = \mathfrak{p}'_j$ ein minimales Element dieser Menge, so gilt $Q_i = Q'_j$.

Def. 67 Seien $N, M \in {}_R\mathcal{M}$, $N \leq M$ und $e \in R$. Dann sei

$$N \underset{M}{:} e := \{x \in M : \ ex \in N\}$$

Satz 75 Seien $N, M \in {}_R\mathcal{M}$ NOETHERsch, $N < M$. N sei nicht primär in M. Dann ist zum minimalen j mit $N \underset{M}{:} e^j = N \underset{M}{:} e^{j+1}$

$$N = (N \underset{M}{:} e^j) \cap (N + e^j M)$$

eine echte Zerlegung von M.

Bsp.

- Seien $\mathfrak{m} \trianglelefteq R$ maximal, $k \in \mathbb{N}$ und $\mathfrak{m} \geq \mathfrak{q} \geq \mathfrak{m}^k$. Dann ist $\mathfrak{q}$ primär mit zugehörigem Primideal $\mathfrak{m}$.
- Sei k ein Körper mit $\operatorname{char} k \neq 2$, $R = k[x]$, $\mathfrak{q} = \langle x \rangle = xR$, $\mathfrak{q}_a = \langle y - ax, x^2 \rangle$. $\mathfrak{q}_a$ ist prim und daher primär zu $\mathfrak{q}$. $\mathfrak{p} := \langle x, y \rangle$ ist maximal.

  $$\mathfrak{p} > \mathfrak{q}_a > \mathfrak{p}^2 = \langle x^2, xy, y^2 \rangle .$$

  Nach dem vorherigen Beispiel ist $\mathfrak{q}_a$ primär zu $\mathfrak{p}$ und für $\mathfrak{a} = \langle x^2, xy \rangle$ ist $\mathfrak{a} = \mathfrak{q} \cap \mathfrak{q}_a$ eine reduzierte Primärzerlegung nicht eindeutig bestimmt.

20 Annullatoren und assoziierte Primideale

Def. 68 Sei $M \in {}_R\mathcal{M}$ und $x \in M$. Das Ideal

$$\operatorname{Ann} x := \{a \in R : \ ax = 0\}$$

heißt *Annullator* von x.

Bem. Ist $\operatorname{Ann} x = \mathfrak{a}$, so enthält M einen zu $R/\mathfrak{a}$ isomorphen Untermodul, nämlich Rx.

Def. 69 Sei $M \in {}_R\mathcal{M}$. Das Primideal $\mathfrak{p} \lhd R$ heißt *assoziiert* zu M, es ein $x \in M$ gibt mit $\mathfrak{p} = \operatorname{Ann}(x)$. $\operatorname{Ass}(M)$ bezeichne die Menge aller zu M assoziierten Primideale:

$$\operatorname{Ass} M := \operatorname{Spec} R \cap \{\operatorname{Ann} x : \ x \in M\}.$$

Satz 76

1. Seien $\mathfrak{p} \in \operatorname{Spec} R$ und $M \neq 0$ ein Untermodul von $R/\mathfrak{p}$. Dann gilt $\operatorname{Ass} M = \mathfrak{p}$.
2. Seien $M \in {}_R\mathcal{M}$ und
$$\mathcal{A} := \{\operatorname{Ann} x : \ 0 \neq x \in M\}.$$
Dann ist jedes maximale Element von $\mathcal{A}$ in $\operatorname{Ass}(M)$ enthalten.
3. Ist R NOETHERsch und $M \neq \emptyset$, so ist $\operatorname{Ass} M \neq \emptyset$.
4. Für $r \in R$, $M \in {}_R\mathcal{M}$ gilt:
$$r_M \text{ ist injektiv} \quad \Longleftrightarrow \quad \forall\, \mathfrak{a} \in \operatorname{Ass} M : \ r \notin \mathfrak{p}.$$
5. Ist R NOETHERsch, so ist
$$\bigcup_{\mathfrak{p} \in \operatorname{Ass} R} \mathfrak{p}$$
die Mengel der Nullteiler von R.
6. Seien $M \in {}_R\mathcal{M}$, $N \leq M$. Dann gilt
$$\operatorname{Ass} N \subseteq \operatorname{Ass} M \subseteq \operatorname{Ass} N \cup \operatorname{Ass}(M/N).$$
7. Für $M = \bigoplus\limits_{i \in I} M_i$ gilt
$$\operatorname{Ass} M = \bigcup_{i \in I} \operatorname{Ass} M_i.$$
8. Seien $M \in {}_R\mathcal{M}$ und $Q_i < M$ $(1 \leq i \leq n)$ und $\bigcap\limits_{i=1}^{n} Q_i = 0$. Dann gilt
$$\operatorname{Ass} M \subseteq \bigcup_{i=1}^{n} \operatorname{Ass}(M/Q_i).$$

9. Seien $M \in {}_R\mathcal{M}$, $B \subseteq \operatorname{Ass} M$. Dann existiert ein Untermodul $N \leq M$ mit $\operatorname{Ass} N = \operatorname{Ass} M \setminus B$ und $\operatorname{Ass}(M/_N) = B$.

Satz 77 Sei R ein kommutativer Ring und $(S, \cdot)$ ein Untermonoid von $(R, \cdot)$. Weiter sei

$$M := R \times S = \{(r, s) : r \in R, s \in S\}.$$

Dann wird auf M eine Äquivalenzrelation definiert durch

$$(r_1, s_1) \sim (r_2, r_2) \qquad :\Longleftrightarrow \qquad \exists \quad t \in S: \quad t(r_1 s_2 - r_2 s_1) = 0.$$

Die Äquivalenzklasse $[(r, s)]_\sim$ wird $\frac{r}{s}$ geschrieben. $S^{-1}R := M/_\sim$ wird ein Ring durch

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} := \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}, \qquad \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} := \frac{r_1 \cdot r_2}{s_1 \cdot s_2}.$$

Bem.

- Ist $M \in {}_R\mathcal{M}$ und S wie im obigen Satz, dann wird $N := M \times S$ mit den analogen Verknüpfungen zu einem $S^{-1}R$-Modul, der als $S^{-1}M$ bezeichnet wird.
- Die maximal mögliche Menge S, bei der die Abbildung $r \mapsto \frac{r}{1}$ injektiv bleibt, ist die Menge aller Nicht-Nullteiler von R. Der damit gebildete Ring $S^{-1}R$ heißt der *totale Quotientenring.* Ist R integer und $S = R \setminus \{0\}$, so ist $S^{-1}R = \operatorname{Quot} R$ der Quotientenkörper.
- Die Abbildung $i_s : R \to S^{-1}R$, $i_s(r) := \frac{r}{1}$ ist ein Ringhomomorphismus, der $S^{-1}R$ zu einer R-Algebra macht. Zu jedem Ringhomomorphismus $f : R \to \tilde{R}$ mit $f(S) \subseteq \tilde{R}^\times$ gibt es genau einen Morphismus $g : S^{-1}R \to \tilde{R}$ mit $f = g \circ i_s$. Entsprechendes gilt für Moduln.
- Es gibt eine Bijektion zwischen den $S^{-1}R$-Moduln und den R-Moduln, auf denen die Elemente von S bijektiv operieren.

Def. 70 Es sei $M \in {}_R\mathcal{M}$ und $D : R \to M$ Homomorphismus zwischen den ABELschen Gruppen $(R, +)$, $(M, +)$ mit

$$\forall \quad x, y \in R: \qquad D(xy) = xD(y) + yD(x).$$

Dann heißt D *Derivation.*

Bem. Es gibt genau eine Derivation $D_s : S^{-1}R \to S^{-1}M$ mit

$$D_s(\frac{r}{1}) = \frac{D_s(r)}{1} \qquad (r \in R).$$

Def. 71 Seien $(S, \cdot)$ ein Untermonoid von $(R, \cdot)$, $N, M \in {}_R\mathcal{M}$, $N \leq M$. N heißt in M *S-saturiert*, falls gilt:

$$\forall \quad m \in M, s \in S: \qquad (sm \in N \quad \Longrightarrow \quad m \in N).$$

Bem. Für beliebiges $N \leq M$ ist

$$\mathrm{Sat}_S^M(N) = j_S^{-1}(S^{-1}N)$$

der kleinste in M S-saturierte, N enthaltende Modul. Dabei ist $j_S : M \to S^{-1}M$ definiert durch $j_S(m) := \frac{m}{1}$. Man erhält

$$\mathrm{Sat}_S^M(N) = \{m \in M : \quad \exists\, s \in S : \ sm \in N\}.$$

Satz 78 Es sei R integer und $N \leq M =: R^n$ ein Untermodul vom Rang r. A sei die aus den Erzeugenden von N gebildete Matrix und $d \neq 0$ eine nicht verschwindende $r \times r$-Unterdeterminante von A. Dann gilt

$$\mathrm{Sat}_S^{R^n}(N) = N \underset{M}{:} d.$$

Index

L

M

N

O

P

Q

R