Einführung in die Algebra , TUD WS 6

1 Ganzzahlige Arithmetik

1.1 Natürliche Zahlen

Die Arithmetik gründet auf das Prinzip des "Weiterzählens" und erscheint eng mit der Zeitvorstellung verbunden. Die Reihe $\mathbb{N}$ der *natürlichen Zahlen* $0, 1, 2, 3, \ldots$ nehmen wir als gegeben. Die relevante Struktur ist das ausgezeichnete Element 0 und die "Nachfolgeroperation" $n \mapsto n+1$. Sie wird charakterisiert durch die folgenden Eigenschaften

- 0 ist kein Nachfolger, d.h. $0 \neq n+1$ für alle n
- Aus $n+1 = m+1$ folgt $n = m$
- Induktionsprinzip: Ist $A(x)$ ein Aussage so, dass $A(0)$ gilt (Verankerung) und $A(n+1)$ stets aus $A(n)$ folgt (Induktionsschritt), so gilt $A(n)$ für alle n

Hinzu kommt das (beweisbare) Prinzip der rekursiven Definition. Dieses erlaubt z.B. das n-fache $n\vec{a}$ eines Vektors $\vec{a}$ durch folgende Angaben zu definieren

$$0\vec{a} = \vec{0}, \quad (n+1)\vec{a} = n\vec{a} + \vec{a}$$

Weitere Beispiele sind die Definitionen

$$m + 0 = m, \; m + (n+1) = (m+n) + 1 \quad \text{(Addition)}$$

$$m \cdot 0 = 0, \; m \cdot (n+1) = m \cdot n + m \quad \text{(Multiplikation)}$$

$$m \not< 0, \quad m < n+1 \text{ genau dann, wenn } m < n \text{ oder } m = n \quad \text{(Anordnung)}$$

$$0! = 1, \quad (n+1)! = n! \cdot (n+1) \quad \text{(Fakulät)}$$

Dass dann die Ihnen wohlbekannten Gesetze der Arithmetik gelten, kann man (meist durch Induktion) beweisen.

1.2 Ganze Zahlen

Die Zahl $a - b$ ist dadurch charakterisiert, dass $(a-b) + b = a$. Innerhalb der natürlichen Zahlen existiert sie genau dann, wenn $b \leq a$. Will man diese Einschränkung aufheben (und dafür gibt es viele praktische Gründe), so kommt man zu den *ganzen Zahlen*: diese haben eine eindeutige Darstellung der Form

$$n \text{ mit } n \in \mathbb{N} \;\text{ bzw. }\; -n \text{ mit } n \in \mathbb{N}, n \neq 0$$

Wir rechnen mit Zahlen aus $\mathbb{N}$ wie vorher und setzen

$$n + (-m) = (-m) + n = \begin{cases} n - m & \text{falls } m \leq n \\ -(m-n) & \text{falls } n < m \end{cases} \qquad (-n) + (-m) = -(n+m)$$

$$(-n) \cdot m = m \cdot -(n) = -(nm), \quad (-n) \cdot (-m) = nm$$

$$-n < m, \quad -n < -m \text{ genau dann, wenn } m < n$$

Wir können nun die Umkehrung und die Subtraktion für beliebige ganze Zahlen definieren

$$-(-n) = n, \quad a - b = a + (-b)$$

Wieder ergibt sich die Aufgabe, alle Gesetze der Arithmetik nachzuweisen.

1.3 Rekursive Definition

Wir haben die Ordung `[order]`, Addition und Multiplikation auf $\mathbb{N}$ "rekursiv" definiert, ohne genau zu sagen, was wir damit meinen, oder zu beweisen, dass das auch funktioniert. Das wollen wir nachholen.

Prinzip 1.1 *(*Rekursion*) Seien g und h Funktionen auf $\mathbb{N}$ in m bzw. $m+2$ Variablen. Dann gibt es eine Funktion f auf $\mathbb{N}$ in $m+1$ Variablen derart, dass für alle natürlichen Zahlen $x_1, \ldots x_n, y$ gilt*

$$\begin{aligned} f(x_1, \ldots, x_m, 0) &= g(x_1, \ldots, x_m) \\ f(x_1, \ldots, x_m, \sigma(y)) &= h(x_1, \ldots, x_m, y, f(x_1, \ldots, x_m, y)) \end{aligned}$$

Der Werteverlauf dieser Funktion ist eindeutig bestimmt.

Definition 1.2 *Wir sagen, f sei die* rekursiv definierte Funktion *zu dem durch g und h gegebenen* Rekursionsschema *bzw.* Rekursionsvorschrift `[recursion scheme]`.

Zum Beispiel definieren wir $f(y) = y!$ durch das Schema $g = 1,\ h(y,z) = (y+1)\cdot z$

$$0! = 1, \quad (n+1)! = n! \cdot (n+1)$$

1.4 Ordnungsinduktion

Prinzip 1.3 *(*Minimalbedingung `[minimal condition]`*) Sei $C(x:\mathbb{N})$ eine Formel so, dass $\exists x:\mathbb{N}.\ C(x)$. Dann gibt es ein* minimales *m in $\mathbb{N}$ mit $C(m)$ - d.h. es gilt $C(m)$ und $\forall y:\mathbb{N}.\ y < m \Rightarrow \neg C(y)$.*

Beweis. Sei die Formel $B(x)$ gegeben als

$$\exists y{:}\mathbb{N}.\ (y \leq x \wedge C(y)) \Rightarrow \exists u{:}\mathbb{N}.\ u \leq x \wedge C(u) \wedge \forall z{:}\mathbb{N}.\ z < u \Rightarrow \neg C(z)$$

Wir benutzen das Induktionsprinzip um $\forall x{:}\mathbb{N}.\ B(x)$ zu beweisen. Gilt $\exists y{:}\mathbb{N}.\ (y \leq 0 \wedge C(y))$ so ist 0 selbst das gesuchte minimale Element; andernfalls ist nichts zu zeigen. Sei nun $B(n)$ vorausgesetzt. Gilt $\exists y:\mathbb{N}.\ (y \leq n \wedge C(y))$, so haben wir wegen $B(n)$ auch das gesuchte minimale Element. Andernfalls gilt entweder $C(\sigma n)$ und σn ist das minimale Element; oder $\neg C(\sigma n)$ und damit $\neg\exists y:\mathbb{N}.\ (y \leq \sigma n \wedge C(y))$ und es ist wieder nichts zu zeigen. Damit ist $\forall x{:}\mathbb{N}.\ B(x)$ bewiesen. Gibt es nun ein n mit $C(n)$, so gilt auch $\exists y{:}\mathbb{N}.\ (y \leq n \wedge C(y))$ (wähle $y = n$) und es folgt die Existenz eines minimalen $m(\leq n)$ mit $C(m)$. □ Es folgt sofort das folgende (indem man $C(x) := \neg A(x)$ setzt)

Prinzip 1.4 *(*des kleinsten Verbrechers*). Hat man die Annahme, dass m minimal ist mit $\neg A(m)$, zum Widerspruch geführt, so hat man $\forall x{:}\mathbb{N}.\ A(x)$ bewiesen.*

Satz 1.5 *Jede natürliche Zahl $n > 1$ ist ein Produkt von unzerlegbaren* `[irreducible]` *Zahlen.*

Beweis. Sei n der kleinste Verbrecher, insbesondere selbst zerlegbar. Also $n = a \cdot b$ mit $1 < a, b < n$. Da a kein Verbrecher ist, ist es ein Produkt $a = p_1 \cdot \ldots \cdot p_k$ von unzerlegbaren Zahlen und $b = q_1 \cdot \ldots \cdot q_l$ ebenfalls. Also ist $n = p_1 \cdot \ldots \cdot p_k \cdot q_1 \cdot \ldots \cdot q_l$ auch ein Produkt von unzerlegbaren Zahlen. Widerspruch `[contradiction]` □

Für Leute, die das Direkte lieben, können wir unser Prinzip auch so formulieren

Prinzip 1.6 *(*Ordungsinduktion*). Sei $A(x:\mathbb{N})$ eine Formel. Es sei die folgende Aussage nachgeprüft:*

$$\forall x{:}\mathbb{N}.\ (\forall y{:}\mathbb{N}.\ y < x \Rightarrow A(y)) \Rightarrow A(x)$$

Dann gilt: $\forall x{:}\mathbb{N}.\ A(x)$

$\forall y:\mathbb{N}.\ y < n \Rightarrow A(y)$ heisst *Induktionsvoraussetzung* oder *Induktionsannahme* `[inductive hypothesis]` für n. Im Induktionschritt `[inductive step]` haben wir von allen $m < n$ auf n zu schliessen (was ggf. leichter ist, als allein von $n-1$ auf n schliessen zu müssen). Der Induktionsanfang `[basis of induction]` ist formal mit darin enthalten: für $n = 0$ gibt es halt kein $m < n$. Oft ist es besser, das auch als gesonderten Fall zu behandeln.

1.5 Teilbarkeit

In $\mathbb{Z}$ definieren wir

$$x|y := \exists z{:}\mathbb{Z}.\ xz = y \quad \text{lies } x \text{ teilt } \texttt{[divides]} y.$$

Lemma 1.7

$$a|0,\ \ 0|a \Rightarrow a = 0,\ \ |a| = |b| \ \approx\!\!>\ a|b \ \approx\!\!>\ |a| \le |b|,\ \ a|1 \Rightarrow |a| = 1.$$

$$a|b \wedge b|c \Rightarrow a|c,\ \ a|b \wedge b|a \Rightarrow |a| = |b|,\quad a|b \Rightarrow (ac)|(bc),\ \ a|b \wedge a|c \Rightarrow a|(b+c)$$

Algorithmus 1.8 *(*Division mit Rest `[division with remainder]`*). In $\mathbb{Z}$ gibt es zu allen a und $b \neq 0$ eindeutig bestimmte Zahlen $r = R(a,b)$ und $q = Q(a,b)$ mit*

$$a = bq + r,\ 0 \le r \le |b|.$$

Für $a \ge b > 0$ ergeben sich diese rekursiv mit jeweils geignetem $m \ge 1$

$$R(a,b) = \begin{cases} a - mb & \text{falls } 0 \le a - mb < b \\ R(a-mb,b) & \text{falls } a - mb \ge b \end{cases}$$

$$Q(a,b) = \begin{cases} 1 & \text{falls } a = b \\ m & \text{falls } a - mb < b \\ Q(a-mb,b)+1 & \text{falls } a - mb \ge b \end{cases}$$

Beweis. Die Existenz ergibt sich sofort aus der Formulierung des Algorithmus. Ist nun $a = bq + r = bq' + r'$ und z.B. $r' \ge r$, so folgt $b(q-q') = r' - r$. Also $q - q' = 0$, da sonst $|b| \le |r' - r| < |b|$. Und es folgt $r = r'$. □

t ist ein *gemeinsamer Teiler* von a und b, falls $t|a$ und $t|b$. Ein gemeinsamer Teiler d von a und b ist ein *grösster gemeinsamer Teiler* oder *GGT* `[greastest common divisor, GCD]`, falls jeder andere gemeinsame Teiler t von a, b auch Teiler von d ist. Es folgt, das es zu a, b bis aufs Vorzeichen `[sign]` höchstens einen *GGT* d gibt, wir schreiben $GGT(a,b) = d$ mit $d \ge 0$, falls es einen gibt, andernfalls $GGT(a,b) = \emptyset$.

Lemma 1.9

$$GGT(a,b) = GGT(a-qb,b) = GGT(b,a) = GGT(|a|,|b|),\quad a|b \Leftrightarrow GGT(a,b) = |a|$$

Beweis. Aus $t|a \wedge t|b$ folgt $t|(qb)$ und $t|(a-qb)$. Dasselbe Argument mit $-q$ erlaubt den Rückschluss. □

Algorithmus 1.10 *(*Euklid+Bezout*). Zu je zwei ganzen Zahlen gibt es den $GGT(a,b)$ und ganze Zahlen x und y mit*

$$GGT(a,b) = ax + by.$$

Den GGT und geeignete Zahlen x, y kann man so bestimmen. Gegeben a, b setze

$$d' := a,\ x' := 1,\ y' := 0;\ d := b,\ x := 0,\ y := 1$$

Bestimme

$$d' = dq + r \text{ mit } |r| < |d| \text{ oder } r = 0$$

$$\text{solange } r \neq 0 \text{ tu } (d', d) := (d, r),\ (x', x) := (x, x' - xq),\ (y', y) := (y, y' - yq)$$

$$\text{falls } r = 0 \text{ halt ein } :\ d = ax + by =: GGT(a,b).$$

Beweis. Mit den Lemma und Induktion ist die Existenz eines GGT sofort klar. Da $\mathbb{N}$ wohlgeordnet ist, muss der Algorithmus zum Halten kommen. Korrektheit des Algorithmus: Für alle Iterationsschritte gilt:

$$d = ax + by,\ d' = ax' + by' \text{ und } GGT(a,b) = GGT(d,d').$$

Nämlich

$$a(x' - xq) + b(y' - yq) = ax' + by' - (ax + by)q = d' - dq = r$$

$$GGT(r,d) = GGT(d,d') = GGT(a,b).$$

Ist $r = 0$, so folgt $d|d'$, also $d = GGT(a,b)$. □

Korollar 1.11 $a|(bc) \wedge GGT(ab) = 1 \ \Rightarrow\ a|c$

Beweis. $1 = ax + by$, also $a|(axc + bcy) = c$.

Ein Teiler d von a ist *echt*, falls $|d| \neq 1$ und $|d| \neq |a|$. Eine Zahl a mit $|a| > 1$ ist *unzerlegbar*, falls sie keine echten Teiler besitzt. Eine Zahl p mit $|p| > 1$ ist eine *Primzahl*, falls

$$\forall x{:}\mathbb{Z}.\forall y{:}\mathbb{Z}.\ p|(x \cdot y) \Rightarrow p|x \vee p|y.$$

Mit Induktion folgt

$$p \text{ prim } \wedge p|\prod_{i\in I} a_i \Rightarrow \exists i \in I.\ p|a_i.$$

Satz 1.12 *In $\mathbb{Z}$ sind die unzerlegbaren Zahlen genau die Primzahlen.*

Beweis. Sei p prim und $p = a \cdot b$, so o.B.d.A. $p|a$, also $|p| \leq |a|$. Andererseits $|a| \leq |p|$, also $|a| = |p|$. Mit der Kürzungsregel folgt $|b| = 1$.

Sei umgekehrt p unzerlegbar und $p|(ab)$. Ist p kein Teiler von a, so $\mathrm{GGT}(p,a) = 1$, also $1 + ax + by$ und $b = abx + bpy$ und es folgt $p|b$. □

Satz 1.13 *Jede ganze Zahl a mit $|a| > 1$ hat eine Zerlegung*

$$a = p_1 \cdot \ldots \cdot p_n \text{ in Primfaktoren } p_1, \ldots, p_n,\ n \geq 1.$$

Die p_i sind bis auf Vorzeichen `[sgn]` *und Reihenfolge* `[order]` *eindeutig bestimmt* `[uniquely determined]`.

Beweis. Die Existenz haben wir schon gezeigt 1.5. Die Eindeutigkeit folgt ebenso mit Induktion: Ist $a = \prod_{i=1}^{n} p_i = \prod_{j=1}^{m} q_j$ so teilt p_n eines der q_j nach Umsortieren etwa q_m. Es folgt $|p_n| = |q_m|$ und durch Kürzen `[cancellation]` $\prod_{i=1}^{n-1} |p_i| = \prod_{j=1}^{m-1} |q_j|$. Mit Induktion folgt $n = m$ und der Rest der Behauptung. □

1.6 Diophantische Gleichungen

Satz 1.14 *(Diophant) Es gibt zu gegebenen $a, b, c \in \mathbb{Z}$ genau dann (mindestens) eine ganzzahlige Lösung der Gleichung*

$$ax + by = c \quad wenn \;\; d := GGT(a, b) | c.$$

Hat man eine Lösung x_0, y_0, so ist die Lösungsgesamtheit gegeben durch

$$x = x_0 + qb',\; y = y_0 - qa',\;\; q \in \mathbb{Z}, \quad wobei\; a = a'd,\; b = b'd.$$

Beweis. Die Äquivalenz folgt leicht mit dem Satz von Bezout. Bemerke $GGT(a', b') = 1$, da für einen gemeinsamer Teiler t von a', b' gälte: $td|a, b$. Dass x, y der angegebenen Gestalt Lösung ist, ist klar. Sei umgekehrt eine Lösung x, y gegeben. Durch Herauskürzen von d folgt $xa' + yb' = x_0a' + y_0b'$, also $a'(x - x_0) = b'(y_0 - y)$. Mit dem Korollar 1.11 folgt $a'|(y_0 - y)$, d.h. $x - x_0 = qb'$ für ein $q \in \mathbb{Z}$. Es folgt $a'qb' = b'(y - y_0)$ und durch Kürzen $y - y_0 = qa'$.

2 Algebraische Strukturen

2.1 Monoide

Eine *algebraische Struktur* `[algebraic structure]` vom Typ (Signatur) `[type (signature)]` der Monoide `[monoid]` kann angegeben werden durch `[can be presented by]` eine (Grund)-Menge `[base set]` A (für Pedanten: U_A wie "unterliegende Menge"), eine zweistellige Operation `[binary operation]` $(x, y) \mapsto x \cdot y$ auf A, und eine Konstante `[constant]` e in A. Notfalls dekorieren wir auch die Operationen: $\cdot_A$ und e_A. Es handelt sich um ein *Monoid* (auch *Halbgruppe mit Eins*) `[semigroup with unit]`, wenn die Axiome (G1-2) gelten:

$$(G1) \quad \text{für alle } x, y, z \text{ in } G \text{ gilt } x \cdot (y \cdot z) = (x \cdot y) \cdot z$$

$$(G2) \quad \text{für alle } x \text{ in } G \text{ gilt } e \cdot x = x = x \cdot e$$

Die zweistellige Operation heisst auch die Multiplikation des Monoids und man schreibt auch $xy = x \cdot y$. Das Element e ist *neutral* und durch (G2) eindeutig bestimmt `[uniquely determined]` - gilt $ee' = e$ so $e = ee' = e'$ - man muss es also nicht immer ausdrücklich angeben. *Beispiele.* `[examples]`

- $\mathbb{N}$ bzgl. `[with respect to]` $+$ und 0
- $\mathbb{N}_{>0}$ bzgl. $\cdot$ und 1
- $K^{n \times n}$ mit der Matrizenmultiplikation `[matrix multiplication]`
- Für eine Menge `[set]` M das Monoid aller Selbstabbildungen `[selfmaps]`

  $$M^M = \{f \mid f : M \to M \text{ Abbildung}\}$$

  mit der Hintereinanderausführung `[composition]` $\circ$ als Multiplikation und der identischen Abbildung `[identity map]` id als neutralem Element.

- Ist eine Menge (Alphabet) Σ gegeben, so erhält man das *Wortmonoid* `[word monoid]` als die Menge Σ^* aller endlichen Listen `[finite lists]`

$$a_1, \ldots, a_n, \quad a_i \in \Sigma$$

mit der leeren `[empty]` Liste ϵ als neutralem Element und der Verkettung concatenation als Multiplikation

$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = a_1, \ldots, a_n, b_1, \ldots, b_m$$

Man kann die Kommata weglassen `[omit]` - dann hat man *Wörter*. Oder Klammern drummachen `[put brackets]` - dann hat man "Tupel". v ist *Präfix* von w, wenn es u gibt mit $vu = w$ - und u ist dann eindeutig bestimmt.

In jeder algebraischen Struktur A von Typ der Monoide definieren wir rekursiv zu gegebenen b bzw. $b_1, b_2, \ldots$ in A

$$b^0 = e_A, \quad b^{n+1} = b^n \cdot_A b$$

$$\prod_{i=1}^{0} b_i = e_A, \quad \prod_{i=1}^{m+1} b_i = (\prod_{i-1}^{m} b_i) \cdot_A b_{m+1}$$

Wir schreiben auch anschaulicher `[more intuitively]` $b_1 \cdot \ldots \cdot b_m$ statt $\prod_{i=1}^{m} b_i$.

2.2 Terme

Der Begriff `[concept]` "Term" ist seit früher Schulzeit wohlbekannt. Für algebraische Strukturen vom Typ der Monoide, kann man *Terme in den paarweise veschiedenen Variablen* `[pairwise distinct variables]` $x_1, \ldots, x_n$ so einführen

- Jedes x_i ist ein Term
- e ist ein Term
- Sind s und t Terme, so auch $(s \cdot t)$
- Das ist alles `[that's all]`: nur was so entsteht ist ein Term

Wir haben also die Menge der Terme über $x_1, \ldots, x_n$ als Teilmenge `[subset]` der Wortmonoids mit Alphabet $\{x_1, \ldots, x_n, e, \cdot, (,)\}$ eingeführt und vorausgesetzt, dass die "Symbole" $e, \cdot, (,)$ unter den "Variablen" x_i nicht vorkommen. Wir schreiben auch $t(x_1, \ldots, x_n)$ um auf die Auflistung der Variablen hinzuweisen.

Der Zweck der Terme (vom Typ der Monoide) ist, dass sie bei Vorgabe einer algebraischen Struktur A vom Typ der Monoide und einer Liste $a_1, \ldots, a_n$ von Elementen von A auf eindeutige Weise ausgewertet werden `[evaluated]` können

$$t(x_1, \ldots, x_n) \mapsto t^A(a_1, \ldots, a_n) \in A$$

so, dass

(1) $x_i^A(a_1, \ldots, a_n) = a_i$

(2) $e^A(a_1, \ldots, a_n) = e_A$

(3) $(s \cdot t)^A(a_1, \ldots, a_n) = s^A(a_1, \ldots, a_n) \cdot_A t^A(a_1, \ldots, a_n)$

Wir nehmen das hier als Erfahrungstatsache, ein Beweis folgt spaeter.

2.3 Allgemeines Assoziativgesetz

Wir können nun das allgemeine Assoziativgesetz `[general associative law]` für Monoide formulieren und beweisen

> Die Auswertung `[value]` eins Terms in einem Monoid ändert sich nicht, wenn man die Klammern umstellt `[rearrange]`

Anders ausgedrückt: Beschreibt die Liste $y_1, \ldots, y_m$ das Vorkommen `[occurence]` der Variablen im Term $t = t(x_1, \ldots, x_n)$ (mit jeder Wiederholung) `[repetition]`, so erhält man den linkgeklammerten `[left bracketed]` Term zu t als

$$\lambda(t) = \prod_{i=1}^{m} y_i$$

und für jedes Monoid A und $a_1, \ldots, a_n$ in A gilt

$$t^A(a_1, \ldots, a_n) = \lambda(t)^A(a_1, \ldots, a_n) = \prod_{i=1}^{m} b_i \text{ wobei } b_i = a_j \text{ falls } y_i = x_j$$

Insbesondere gilt in jedem Monoid

$$\prod_{i=1}^{n} \prod_{j=1}^{n_i} b_{ij} = \prod_{k=1}^{m} c_k \quad \text{mit } m = \sum_{i=1}^{n} n_i \text{ und } b_{ij} = c_k \text{ wo } k = j + \sum_{l=1}^{i-1} n_l$$

$$b^{n+m} = b^n \cdot b^m, \quad (b^n)^m = b^{nm}$$

Beweis. Wir zeigen die Behauptung durch Ordnungs-Induktion `[order induction]` über die Wortlänge `[word length]`. Der Einfachheit halber schreiben wir $\phi(t) =$
$= t^A(a_1, \ldots, a_n)$. Ist $t = x_j$ oder $t = e$, so ists klar. Wir haben nun $\phi(s \cdot t) = \phi(\lambda(s \cdot t))$ zu zeigen unter der Annahme, dass $\phi(u) = \phi(\lambda(u))$ für alle Terme u von Wortlänge kleiner als der von $(s \cdot t)$.

Ist t eine Variable, so $t = y_m$ und $\lambda(s \cdot y_m) = \lambda(s) \cdot y_m$, also $\phi(s \cdot y_m) = \phi(s) \cdot_A \phi(y_m) = \phi(\lambda(s)) \cdot_A \phi(y)_m = \phi(\lambda(s) \cdot \lambda(y_m)) = \phi(\lambda(s \cdot y_m)$.

Ist $t = e$ eine Variable, so $\lambda(s \cdot e) = \lambda(s)$, also $\phi(s \cdot e) = \phi(s) \cdot_A \phi(e) = \phi(\lambda(s)) \cdot_A e_A = \phi(\lambda(s)) = \phi(\lambda(s \cdot e))$.

Andernfalls gilt $\lambda(t) = \lambda(u) \cdot y_m$ und $\lambda(s \cdot t) = \lambda(\lambda(s) \cdot \lambda(u)) \cdot y_m$. Es folgt $\phi(s \cdot t) = \phi(s) \cdot_A \phi(t) = \phi(\lambda(s)) \cdot_A \phi(\lambda(t)) = \phi(\lambda(s)) \cdot_A \phi(\lambda(u) \cdot y_m) = \phi(\lambda(s)) \cdot_A (\phi(\lambda(u)) \cdot_A \phi(y_m)) = (\phi(\lambda(s)) \cdot_A \phi(\lambda(u))) \cdot_A \phi(y_m) = \phi(\lambda(s) \cdot \lambda(u)) \cdot_A \phi(y_m) = \phi(\lambda(\lambda(s) \cdot \lambda(u)) \cdot_A \phi(y_m) = \phi(\lambda(\lambda(s) \cdot \lambda(u)) \cdot y_m) = \phi(\lambda(s \cdot t))$ □

Seien $s(x_1, \ldots, x_n)$ und $t(x_1, \ldots, x_n)$ Terme vom Monoid-Typ. Wir sagen, dass die *Gleichung* $s \approx t$ für Monoide *gilt*, falls sie in allen Monoiden genauso ausgewertet werden, d.h.

$$s^A(a_1, \ldots, a_n) = t^A(a_1, \ldots, a_n) \quad \text{für alle Monoide } A \text{ und } a_1, \ldots, a_n \text{ in } A$$

Ein Term ist in *Monoid-Normalform* `[monoid normal form]`, wenn er linksgeklammertes (ggf. `[possibly]` leeres) Produkt von Variablen ist.

Korollar 2.1 *Zu jedem Term t vom Monoid-Typ gibt es einen Term t' in Monoid-Normalform so, dass $t \approx t'$ für Monoide gilt.*

t' ist sogar eindeutig bestimmt (*Übung).

2.4 Kommutative Monoide

Ein Monoid heißt *kommutativ*, wenn

$$(G4) \qquad \text{für alle } x, y \text{ in } G \text{ gilt } xy = yx\,.$$

Ein Beispiel ist das System aller Teilmengen bzw. endlichen *Multi-Teilmengen* `[bags]` einer Menge M mit der Vereinigungsbildung `[formation of unions]` als Multiplikation und der leeren Menge als neutralen Element. Multimengen kann man auffassen als Listen, bei denen es auf die Reihenfolge `[order]` nicht ankommt, wohl aber auf Wiederholung `[repetition]` (z.B. wenn sich Leute in eine Liste für Kaffeeverbrauch eintragen). Alternativ kann man eine Multi-Teilmenge von M als Abbildung $\alpha : M \to \mathbb{N}$ ansehen, wobei $\alpha(x)$ angibt, wie oft x drin ist; Multiplikation und Neutralelement sind dann gegeben durch

$$(\alpha \cdot \beta)(x) = \alpha(x) + \beta(x), \quad \varepsilon(x) = 0$$

In einem kommutativen Monoid gilt das allgemeine Kommutativ-Assoziativ-Gesetz `[general commutative-associative law]`

> In einem kommutativen Monoid hängt die Auswertung eines Terms nur von der Häufigkeit `[frequency]`, nicht von der Reihenfolge des Auftretens `[occurence]` der Variablen ab

Anders ausgedrückt: zu jedem Term $t(x_1, \ldots, x_n)$ sei

$$\mu(t) = \prod_{i=1}^{n} x_i^{k_i}$$

die zugehörige *kommutative Monoid-Normalform*. wobei k_i die Häufigkeit des Auftretens von x_i in t ist. Dann gilt für alle $a_1, \ldots, a_n$ in einem kommutativen Monoid A

$$t^A(a_1, \ldots, a_n) = \mu(t)^A(a_1, \ldots, a_n) = \prod_{i=1}^{n} a_i^{k_i}$$

insbesondere

$$\prod_{i=1}^{n} a_i^{k_i} \prod_{i=1}^{n} a_i^{l_i} = \prod_{i=1}^{n} a_i^{k_i+l_i}. \quad (a \cdot b)^n = a^n \cdot b^n$$

Die erste dieser beiden Gleichungen beweist man leicht durch Induktion über n. Dann folgt das allgemeine Gesetz durch Induktion über den Termaufbau (Übung!). □.

Für eine endliche Indexmenge `[set of indices]` I und a_i $(i \in I)$ in einem kommutativen Monoid können wir also definieren

$$\prod_{i \in I} a_i = \prod_{k=1}^{n} a_{f(k)} \quad \text{wobei } f : \{1, \ldots, n\} \to I \text{ bijektiv}$$

und das hängt nicht `[does not depend]` von f ab.

2.5 Gruppen

Eine *algebraische Struktur* G vom Typ der Gruppen kann angegeben werden durch eine (Grund)Menge G, eine zweistellige Operation $(x, y) \mapsto x \cdot y = xy$ auf G, eine einstellige Operation $x \mapsto x^{-1}$ auf G und eine Konstante e in G. Es handelt sich um eine *Gruppe* `[group]`, wenn gilt

$$\begin{array}{lll} (G1) & \text{für alle } x, y, z \text{ in } G \text{ gilt} & x(yz) = (xy)z \\ (G2) & \text{für alle } x \text{ in } G \text{ gilt} & ex = x = xe \\ (G3) & \text{für alle } x \text{ in } G \text{ gilt} & xx^{-1} = e = x^{-1}x \end{array}$$

Man nennt dann $\cdot$ die *Multiplikation* der Gruppe, $^{-1}$ die *Inversion* und e das neutrale Element.

Zum Begriff der Gruppe gehören also vier Daten: Die Grundmenge und die drei Operationen. Wir notieren das, wenn nötig, als $(G; \cdot, ^{-1}, e)$ - wobei wir natürlich auch andere geeignete Zeichen `[symbols]` benutzen dürfen, etwa $(A, +, -, 0)$, d.h. Grundmenge A, 'Multiplikation' (oder besser *Addition*) $(x, y) \mapsto x + y$, Inversion $x \mapsto -x$ und neutrales Element 0. Wennn klar ist, welche Operationen wir meinen, sprechen wir einfach von der Gruppe G bzw. A.

Neutrales Element und Inversion einer Gruppe sind schon eindeutig durch Grundmenge und Multiplikation bzw. Addition bestimmt (s. Lemma), man muss also in Beispielen nur letztere angeben. Dies rechtfertigt auch die folgende alternative Definition: Eine Gruppe kann angegeben werden durch eine (Grund)Menge G und eine zweistellige Operation $(x, y) \mapsto xy$ auf G derart, dass (G1) und

$$\begin{array}{ll} (G2+3) & \text{es gibt ein Element } e \text{ von } G \text{ mit} \\ & (a) \quad \text{für alle } x \text{ in } G \text{ gilt } ex = x = xe \\ & (b) \quad \text{für alle } x \text{ in } G \text{ gibt es ein } y \text{ in } G \text{ mit } xy = e = yx \end{array}$$

Dass die Angabe aller drei Operationen die sinvollere Sicht ist, wird beim Begriff der Untergruppe klar werden.

Beispiele:

- Die ganzen Zahlen `[integers]` bilden eine Gruppe $(\mathbb{Z}; +, -, 0)$ bzgl. der üblichen Addition
- Die Vektoren des Raumes `[space]` bilden eine Gruppe $(\mathcal{V}; +, -, \vec{0})$ bzgl. der Addition von Vektoren
- Die rationalen Zahlen `[rational numbers]` $\neq 0$ bilden eine Gruppe $(\mathbb{Q}_{\neq 0}; \cdot, ^{-1}, 1)$ bzgl. der üblichen Multiplikation
- Die reellen Zahlen `[real numbers]` > 0 bilden eine Gruppe $(\mathbb{R}_{>0}; \cdot, ^{-1}, 1)$ bzgl. der üblichen Multiplikation
- Die invertierbaren `[invertible]` Matrizen in $K^{n \times n}$ bilden die (*allgemeine lineare*) Gruppe $\mathsf{GL}(n, K)$ bzgl. der Matrizenmultiplikation
- Die bijektiven Abbildungen `[bijective maps]` einer Menge M in sich bilden bzgl. der Komposition $\circ$, der Inversion $^{-1}$, und dem neutralen Element id_M eine Gruppe S_M, die *symmetrische Gruppe* `[symmetric group]` auf M.

- Endliche Gruppen können wir durch eine Tafel `[table]` für die Multiplikation angeben, z.B.

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Lemma 2.2 *In einer Gruppe gelten*

(1)	$ab = a$	$\Lsh\!\!\Rsh$	$b = e$	$\Lsh\!\!\Rsh$	$ba = a$
(2)	$b = a^{-1}$	$\Lsh\!\!\Rsh$	$ab = e$	$\Lsh\!\!\Rsh$	$ba = e$
(3)	$(a^{-1})^{-1} = a$				(4) $(ab)^{-1} = b^{-1}a^{-1}$

Beweis. (1). Aus $ab = a$ folgt durch Multiplikation mit a^{-1} von links, dass $a^-1(ab) = a^{-1}a$. Nun ist aber nach (G1-3) $a^{-1}(ab) = (aa^{-1})b = eb = b$ und $a^{-1}a = e$, also $b = e$. Ebenso geht der Schluss von $ba = a$ auf $b = e$ durch Multiplikation mit a^{-1} von rechts. Die Umkehrungen sind trivial.

(2). Gilt $ab = e$ so folgt durch Multiplikation mit a^{-1} von links, dass $a^{-1}(ab) = a^{-1}e$. Nun ist aber wie eben $a^{-1}(ab) = b$ und $a^{-1}e = a^{-1}$, also $b = a^{-1}$. Ebenso geht der Schluss von $ba = e$ auf $b = a^{-1}$ durch Multiplikation mit a^{-1} von rechts. Die Umkehrungen sind trivial.

(3) folgt sofort aus (2) mit $b = a^{-1}$. In (4) hat man wegen (2) nur $(b^{-1}a^{-1})(ab) = e$ zu zeigen. Das geht so: $(b^{-1}a^{-1})(ab) = (b^{-1}(a^{-1}a))b = (b^{-1}e)b = b^{-1}b = e$. (4) heisst auch die *Socke-Schuh-Regel*. □ Die Verallgemeinerung folgt nun leicht durch Induktion

$$(a_1 \cdot \ldots \cdot a_n)^{-1} = a_n^{-1} \cdot \ldots \cdot a_1^{-1}$$

Wir definieren für a in G

$$a^{-n} = (a^n)^{-1} \text{ für } n \in \mathbb{N}$$

Ist G eine Gruppe, so gilt (Übung!)

$$a^z \cdot a^w = a^{z+w},\ (a^z)^w = a^{zw} \quad \text{für alle } z, w \in \mathbb{Z}$$

Wenn wir über Terme reden wollen, ist die Notation t^{-1} unhandlich. Wir verstehen sie einfach als traditionelle Schreibweise für ιt. Also kommt bei der Termerzeugung die folgende Regel hinzu

- Ist t ein Term vom Typ der Gruppe, so auch ιt

Ein Gruppenterm ist in *Gruppen-Normalform*, falls er folgende Gestalt hat

$$\prod_{i=1}^{m} y_i^{z_i} \quad \text{mit } z_i \in Z \text{ und } y_i \neq y_{i+1} \text{ für alle } i < m$$

und man zeigt, dass es zu jedem t ein t' in Normalform (in denselben Variablen) gibt so, dass t und t' in jeder Gruppe gleich ausgewertet werden. Übung!

2.6 Kommutative Gruppen

Die Gruppe G ist abelsch `[abelian]` oder kommutativ `commutative` , falls

$$(G4) \quad \text{für alle } x, y \text{ in } G \text{ gilt } xy = yx$$

Beispiele: Abelsche Gruppen sind $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ jeweils mit Addition, Subtraktion und Null bzw. $\mathbb{Q} \setminus \{0\}$ und $\mathbb{R} \setminus \{0\}$. jeweils mit Multiplikation, Inversion und Eins.

Man benutzt meist die additive Schreibweise und bezeichnet Operationen als Addition, Umkehrung bzw. Inversion und Nullelement bzw. neutrales Element. Statt $a + (-b)$ schreiben wir auch $a - b$. Statt $\prod_i a_i$ haben wir $\sum_i a_i$, statt a^z haben wir za und es gilt für $z, w \in \mathbb{Z}$

$$0a = 0,\ (-1)a = -a,\ (z + w)a = za + wa,\ z(wa) = (zw)a,\ z(a + b) = za + zb$$

Indem man mithilfe der Kommutativiät die Vielfachen derselben Variablen zusammenfasst, erhält man nun aus der Gruppen-Normalform eines Term $t(x_1, \ldots x_n)$ eine *kommutative Gruppen-Normalform*

$$\sum_{i=1}^{n} z_i x_i \quad z_i \in \mathbb{Z},\ x_i \neq x_j \text{ für } i \neq j$$

die in jeder kommutativen Gruppe genauso wie t ausgewertet wird. Es folgt

In einer kommutativen Gruppe gelten alle Gleichungen von $\mathbb{Z}$

Indem man die eine Seite der Gleichung von der anderen abzieht, erhält man nämlich eine äquivalente Gleichung der Form $\sum_i z_i x_i \approx 0$. Ist z.B. $z_{i_0} \neq 0$, so setze $x_{i_0} = 1$ und $x_i = 0$ für $i \neq i_0$ um eine Auswertung mit Wert $\neq 0$ zu erhalten. Alos gilt die Gleichung genau dann in $\mathbb{Z}$, wenn alle $z_i = 0$ sind. Dann gilt sie aber in jeder kommutativen Gruppe.

2.7 Ringe

Eine *algebraische Struktur* R von Typ der Ringe besteht aus einer additiv geschriebenen Struktur von Typ der Gruppen une einer multiplikativ geschriebenen Struktur vom Typ der Monoide (meist mit 1 anstelle von e) auf derselben Grundmenge. Es handelt sich um einen *Ring* `[ring]`, wenn $(R, +, -, 0)$ eine abelsche Gruppe ist (auch als (R1-4) notiert), $(R, \cdot, 1)$ ein Monoid (R5-6), und wenn die *Distributivgesetze* `[distributive laws]` gelten

$(R7)$ für alle x, y, z in R gilt $\quad x(y + z) = xy + xz$
$(R8)$ für alle x, y, z in R gilt $\quad (y + z)x = yx + zx$

R ist kommutativ, wenn
$(R9)$ für alle x, y in R gilt $\quad xy = yx$

Einen endlichen Ring können wir durch zwei Tafeln, für $+$ und $\cdot$ je eine, angeben. Bei unendlichen Ringen können wir uns das zumindest denken. Beispiele kommutativer Ringe sind $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$ mit den üblichen Operationen. Beispiele nichtkommutativer Ringe sind die Matrizenrinmge $K^{n \times n}$ (dabei kann K irgendein Ring sein). In jedem Ring gelten

$$0_R r = 0_R = r 0_R,\ \ (-1_R)r = -r,\ \ (z1_R) = zr = r(z1_R) \text{ für } z \in \mathbb{Z}$$

und das allgemeine Distributivgesetz

$$\prod_{i=1}^{n}(\sum_{j\in J_i} a_{ij}) = \sum_{f\in\mathcal{A}}\prod_{i=1}^{n} a_{if(i)}$$

wobei

$$\mathcal{A} = \{f \mid f : \{1,\ldots,n\} \to \bigcup_{i=1}^{n} J_i,\ f(i) \in J_i\}$$

die Menge der *Auswahlfunktionen* `[choice functions]` ist. Der Beweis beruht auf der Erfahrung, dass man systematisch 'ausmultiplizieren' kann. Man kann auch die anderen üblichen Gesetze der Buchstabenrechnung leicht aus (R1-9) herleiten. Sogar (wie wir später zeigen werden)

In einem kommutativen Ring gelten alle Gleichungen von $\mathbb{Z}$

Unserer Notation für die Operationen entsprechen die folgenden Erzeugungsregeln für Terme vom Typ der Ringe

- Variable, 0 und 1 sind Terme
- Sind s, t Terme, so auch $(s + t), -s, (s \cdot t)$

Zur Klammerersparnis benutzen wir auf der Mittteilungebene die bekannte Konvention 'Punkt vor Strich' und ungeklammerte Smmen bzw. Produkte verstehen wir als linksgeklammert. Im Prinzip denken wir die Terme aber nach wie vor komplett geklammert. Andernfalls müssten wir etwas mehr Sorgfalt aufwenden, um die eindeutige Lesbarkeit und damit die Funktionalität der Auswertung zu beweisen.

2.8 Integritätsbereiche

Ein *Integritätsbereich* `[integral domain]` ist ein kommutativer Ring ohne *Nullteiler* `[divisors of zero]`, d.h. aus $ab = 0$ folgt stets, dass $a = 0$ oder $b = 0$. Gleichbedeutend `[eqivalent]` ist die *Kürzungsregel* `[cancellation law]`

- Aus $ax = ay$ und $a \neq 0$ folgt $x = y$

Bespiele $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

2.9 Körper

Definition. Ein Schiefkörper `[skew field]` oder Divisonsring `[divsion ring]` kann angegeben werden als ein Ring K mit $1 \neq 0$ derart, dass

$$\forall x.\ x \neq 0 \Rightarrow \exists y.\ xy = 1$$

d.h. die $x \neq 0$ bilden eine Gruppe unter der Multiplikation. Also ist y durch x eindeutig bestimmt (vgl. Lemma 2.2) und wir schreiben $y = x^{-1}$. In einem Schiefkörper K gilt $ab = 0 \Rightarrow a = 0 \vee b = 0$ und somit die Kürzungsregel

$$c \neq 0 \wedge ac = bc \Rightarrow a = b$$

Zu $a \neq 0$ und b, c hat man eine eindeutige Lösung der Gleichung

$$ax + b = c \quad \text{nämlich } x = a^{-1}(c - b)$$

Aus $b \neq 0$ folgt nämilch $a = a1 = a(bb^{-1}) = (ab)b^{-1} = 0b^{-1} = 0$.

Eine in vieler Hinsicht angemessenere Sicht ist, die Inversion $x \mapsto x^{-1}$ als partielle. nur für $x \neq 0$ definierte, Operation zu verstehen.

Ist die Maltiplikation kommutativ, so spricht man von einem *Körper* `[field]`. Beispiele von Körpern sind $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Jeder Körper ist ein Integriätsbereich.

2.10 Moduln

Sei K ein Ring . Eine *algebraische Struktur* V (auch ${}_KV$) vom Typ der K-Moduln ist eine additiv geschriebene Struktur vom Typ der Gruppen mit zusätzlich zu jedem $r \in K$ einer einstelligen Operation r_V notiert als $x \mapsto rx$. Es handelt sich um einen *K-Modul* `[module]`, wenn $(V, +, -, 0)$ kommutative Gruppe ist (V1-4) und

$$(V5) \quad \text{für alle } r \text{ in } K \text{ und } \vec{v}, \vec{w} \text{ in } V \text{ gilt } r(\vec{v} + \vec{w}) = r\vec{v} + r\vec{w}$$

$$(V6) \quad \text{für alle } \vec{v} \text{ in } V \text{ gilt } 1\vec{v} = \vec{v}$$

$$(V7) \quad \text{für alle } r, s \text{ in } K \text{ und } \vec{v} \text{ in } V \text{ gilt } (r + s)\vec{v} = r\vec{v} + s\vec{v}$$

$$(V5) \quad \text{für alle } r, s \text{ in } K \text{ und } \vec{v} \text{ in } V \text{ gilt } r(s\vec{v}) = (rs)\vec{v}\,.$$

Ist dabei K ein Körper, so sprechen wir von einem *K-Vektorraum*. Der Ring K ist integraler Bestandteil des Begriffs, seine Elemente heissen Skalare. Beispiele

1. Die Vektoren des Raumes bzw. einer Ebenen bilden einen $\mathbb{R}$-Vektorraum
2. Jeder abelsche Gruppe ist ein $\mathbb{Z}$-Modul mit (rekursiv definiert)
$$0a = 0. \;\; (n + 1)a = na + a, \;\; (-n)a = -(na)$$
3. Ist I eine Menge und K ein Ring, so bilden die Abbildungen $f : I \to K$ einen K-Modul bzgl. des komponentenweisen Rechnens
$$(f + g)(i) = f(i) + g(i), \;\; (rf)(i) = r(f(i)) \quad \text{alle } i \in I$$
Insbesondere ist $R = R^1$ ein R-Modul.
4. R^n wird zum $R^{n\times n}$-Modul mit der Multiplikation "Matrix mal Spalte".

Es folgt das allgemeine Assoziativ-Kommutativgesetz für die Addition, und die Distributivgesetze (Beweis als Übung)

$$r(\sum_{i=1}^{n} v_i) = \sum_{i=1}^{n} rv_i, \quad [\sum_{i=1}^{n} r_i]v = \sum_{i=1}^{n} r_i v$$

$$0\vec{v} = r\vec{0} = \vec{0}, \; (-r)\vec{v} = -(r\vec{v}).$$

Alternativ kann man die Multiplikation mit Skalaren als Abbildung $(r, v) \mapsto rv$ verstehen. Das erfordert dann den Begriff der "mehrsortigen algebraischen Struktur" `multi-sorted`. Obige Auffassung passt jedoch für unsere Zwecke besser. Für Terme haben wir die Erzeugungsregeln

- Jede Variable x_i und 0 sind ein Term
- Sind s, t Terme, so auch $(s + t)$, $-t$, rt (alle $r \in K$)

Werden mehrere Skalare verküpft, so benutzen wir die Klammern $[,]$, z.B. $[2 + 3 \cdot 4]x_1$. Mit den genannten Gesetzen erhält man sofort zu jedem Term $t(x_1, \ldots, x_n)$ eine *K-Modul-Normalform*

$$NF(t) = \sum_{i=1}^{n} r_i x_i$$

die in jedem K-Modul genaus wie t ausgewertet wird (in diesem Kontext mitgeteilt durch $t \approx NF(t)$). Man spricht auch von einer *Linearkombination* `[linear combination]` der $x_1, \ldots, x_n$. Übung!

2.11 Algebren

Sei K ein. Eine *algebraische Struktur* A von Typ der K-Algebra besteht aus einer algebraischen Struktur vom Typ des K-Moduls und einer von Tp des Rings mit derselben additiven Struktur. Es handelt sich um eine *K-Algebra* `algebra` , wenn es sich hierbei um einen K-Modul und einen Ring handelt und gilt

$$(A) \quad r(a \cdot b) = (ra) \cdot b = a \cdot (rb) \quad \text{für alle } a, b \in A,\ r \in K$$

A is *kommutativ*, wenn es als Ring kommutativ ist. Beispiel

1. Die Matrix-Algebren $K^{n \times n}$ sind nicht kommutativ für $n > 1$.
2. Jeder Ring ist eine $\mathbb{Z}$-Algebra.
3. Der Polynomring $K[x_1, \ldots, x_n]$ ist eine kommutative K-Algebra.
4. $\mathbb{C}$ ist eine $\mathbb{R}$-Algebra.

2.12 Algebraische Strukturen

Das gemeinsame Prinzip bei diesen algebraischen Strukturen scheint zu sein, dass sie aus einer Menge mit einem System von *fundamentalen* Operationen bestehen. Man denke dabei an formales Objekte oder *Operationssymbole* f mit fester Stelligkeit `[arity]` (abhängig von der betrachteten Strukturklasse, *Typ* oder *Signatur*), die dann in der jeweiligen Struktur A (aus dieser Klasse) als n-stellige Operation f^A implementiert sind, d.h. als Abbildung f^A, die jedem n-Tupel $(a_1, \ldots, a_n)$ von Elementen aus A einen Wert $f(a_1, \ldots, a_n)$ in A zuordnet. Eine Ausnahme gibts hier nur bei den Körpern, wo 0^{-1} nicht definiert ist.

GgF. kann eine Teilmenge der Operationssymbole selbst wieder eine algebraische Struktur tragen, wie bei den Moduln. Bei Moduln macht es aber auch Sinn, zwei Mengen, d.h. zwei Sorten von Elementen, Vektoren und Skalaren, zu sehen. Wollte man die Matrizen beliebigen Formats über einem Ring als algebraische Struktur (*Ringoid*) auffassen so hätte man zu jedem Format $n \times m$ ein 'Sorte' und könnte nur Matrizen gleicher Sorte addieren, 'passender' Sorten multiplizieren. Entsprechend bilden die bijektiven Abbildungen $f : M \to N$, mit M, N in einem gegebenen System von Mengen, ein *Gruppoid*.

3 Grundlegende algebraische Begriffe

3.1 Unterstrukturen

Eine *Unterstruktur* `[substructure]` B einer algebraischen Struktur A wird bestimmt durch eine Teilmenge B von A, die unter den Operationen von A abgeschlossen ist, d.h.

- $a, b \in B \Rightarrow a \cdot b \in B$; $e \in B$ für Monoidtyp
- $a, b \in B \Rightarrow a \cdot b \in B$; $e \in B$; $a \in B \Rightarrow a^{-1} \in B$ für Gruppentyp
- $a, b \in B \Rightarrow a + b$, $a \cdot b \in B$; $0, 1 \in B$; $a \in B \Rightarrow -a \in B$ für Ringtyp
- $a, b \in B \Rightarrow a + b \in B$; $0 \in B$; $a \in B \Rightarrow ra \in B$ $(r \in K)$ für K-Modultyp
- $a, b \in B \Rightarrow a + b$, $a \cdot b \in B$; $0, 1 \in B$; $a \in B \Rightarrow -a$, $ra \in B$ $(r \in K)$ für K-Algebratyp

Das Gemeisame lässt sich so fassen: B ist *Unterstruktur* von A, wenn $B \subseteq A$ und

$$f^A(b_1, \ldots, b_n) \in B \quad \text{für jede fundamentale Operation } f \text{ und alle } b_1, \ldots, b_n \in B$$

sofern $f^A(b_1, \ldots, b_n)$ erklärt ist. Insbesondre $c^A \in B$ für jede fundamentale Konstante. B ist dann auf natürliche Weise eine algebraische Struktur desselben Typs - mit der Einschränkung der Operationen von A.

Prinzip 3.1 *Sei α eine Ausssage der Form $\forall x_1 \ldots \forall x_n.\ \beta(x_1, \ldots, x_n)$, wobei β keine weiteren Quantoren enthält. Gilt α in A, so auch in jeder Unterstruktur B.*

Korollar 3.2 *Unterstrukturen von (kommutativen) Monoiden, (kommutativen) Gruppen, (kommutativen) Ringen, K-Moduln bzw. K-Algebren sind wieder solche.*

Man spricht dann auch von *Untermoniden*, *Untergruppen Umterringen*, *K-Untermolduln* bzw. *K-Unteralgebren*. K ist ein *Unterkörper* von L, wenn's ein Unterring ist und

$$r^{-1} \in L \text{ für alle } r \neq 0 \text{ in } K.$$

Dann ist K auch ein Körper. Beispiele:

- $\mathbb{N}$ ist additiv wie multiplikativ Untermonoid von $\mathbb{Z}$
- $\mathbb{Z}$ ist Unterring von $\mathbb{Q}$
- $\mathbb{Q}$ ist Unterkörper von $\mathbb{R}$ und $\mathbb{R}$ von $\mathbb{C}$
- Vektorielle Ebenen und Geraden im vektoriellen Raum sind $\mathbb{R}$-Untervektorräume
- Die Lösungsmenge eines homogenen linearen Gleichungssystems in n Variablen mit Koeffizienten aus K bildet einen K-Untervektorraum von K^n.
- Ist A Unterstruktur von B und B von C, so ist A Unterstruktur von C.
- Sind alle B_i $(i \in I)$ Unterstrukturen von A, so ist auch $\bigcap_{i \in I} B_i$ Unterstruktur von A.

- Jede Untergruppe ist Untermonoid
- Jeder Unterring ist additiv Untergruppe und multiplikativ Untermonoid
- Jeder K-Untermodul ist Untergruppe
- Jede K-Unteralgebra ist K-Untermodul und Unterring
- Jeder Unterring eines Körpers ist ein Intergritätsbereich
- Ist K Unterköper von L, so ist L eine K-Algebra mit K-Unteralgebra K
- $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ ist $\mathbb{Q}$-Unteralgebra von $\mathbb{R}$.
- Die invertierbaren Elemente a eines Monoids M (d.h. es gibt $x, y \in M$ mit $ax = e = ya$) bilden ein Untermonoid $M^\times$, das eine Gruppe ist, die *Einheitengruppe* `[group of units]` von M. Ist $M = K^{n\times n}$, so ist das die allgemeine lineare Gruppe `[general linear group]` $\mathsf{GL}(n, K)$ - und der Beweis geht im allgemeien Fall wie da. Ein Ring R ist Schiefkörper ganau dann, wenn `[if and only if]` $R^\times = R \setminus \{0\}$.
- $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ ist Untergruppe von $\mathbb{C}^\times$.
- $\{z \in \mathbb{C} \mid z^n = 1\}$ ist Untergruppe von S^1
- $\{f \in S_M \mid f(N) = N\}$ und $\{f \in S_M \mid f(x) = x \text{ für alle } x \in N\}$ sind Untergruppen der symmetrischen Gruppe S_M für jedes $N \subseteq M$.

Lemma 3.3 *In einer endlichen Gruppe G gibt es zu jedem $g \in G$ ein $m \in \mathbb{N}$ mit $g^{-1} = g^m$. Insbesondere ist jede nichtleere, unter Multiplikation abgeschlossene Teilmenge eine Untergruppe.*

Beweis. Die Elemente g^k können nicht alle voneinander verschieden sein. Also gibt es $k < l$ mit $g^k = g^l$. Es folgt $e = (g^k)^{-1}g^l = g^{l-k}$. □

3.2 Erzeugnis

Für eine algebraische Struktur A und Teilmenge E von A bestehe das *Erzeugnis* `[span]` $\mathsf{Spann}\, E$ von E aus den $t^A(a_1, \ldots, a_n)$ mit $a_1, \ldots, a_n$ in E und beliebigen Termen $t(x_1, \ldots, x_n)$. Hat man für A eine Normalform etabliert, so braucht man nur t in Normalform.

Lemma 3.4 $\mathsf{Spann}\, E$ *ist eine Unterstruktur von A. Für Unterstukturen B von A gilt* $\mathsf{Spann}\, E \subseteq B$ *genau dann, wenn $E \subseteq B$.*

Man sagt auch, $\mathsf{Spann}\, E$ sei die kleinste E enthaltende Unterstruktur von A. Beweis: $\mathsf{Spann}\, E$ ist Unterstruktur. Z.B. abgeschlossen unter Multiplikation: hat man $c_i \in \mathsf{Spann}\, E$, d.h. $c_i = t_i^A(a_{i1}, \ldots, a_{in_i})$ mit passenden $t_i(x_{i1}, \ldots, x_{in_i})$ und $a_{ij} \in E$, so bringe man die Variablen in die Reihenfolge $x_{11}, \ldots, x_{1n_1}, x_{21}, \ldots, x_{2n_2}$ und wähle $t = (t_1 \cdot t_2)$ und $c_1 \cdot_A c_2 = t(a_{11}, \ldots, a_{2n_2})$ zu erhalten.

Sei andererseits B Unterstruktur mit $E \subseteq B$. Induktion über den Termaufbau liefert $t^A(a_1, \ldots, a_n) \in B$ für $a_i \in E$. Z.B. für $t = (t_1 \cdot t_2)$ hat man als Induktionannahme $t_i^A(a_1, \ldots, a_n)$ also auch $t^A(a_1, \ldots, a_n) = t_1^A(a_1, \ldots, a_n) \cdot_A t_2^A(a_1, \ldots, a_n)$ in B. □ Es folgt

- $E \subseteq \mathsf{Spann}\, E$
- $E \subseteq F \Rightarrow \mathsf{Spann}\, E \subseteq \mathsf{Spann}_{\vdash} F$
- $\mathsf{Spann}\, \mathsf{Spann}\, E = \mathsf{Spann}\, E$

Klasse	Struktur	Erzeugendenmenge
Monoid	$(\mathbb{N}, +, 0)$	$\{1\}$
Monoid	$(\mathbb{N}_{>0}, \cdot, 1)$	$\{p \mid p \text{ prim}\}$
Gruppe	$(\mathbb{Z}, +, 0, -)$	$\{1\}$
Gruppe	$(\mathbb{Q}, +, 0, -)$	$\{\frac{1}{p^n} \mid n > 27,\ p \text{ prim}\}$
Gruppe	$(\mathbb{Q}_{>0}, \cdot, 1, ^{-1})$	$\{p \mid p \text{ prim}\}$
Gruppe	$(\mathbb{Q}_{\neq 0}, \cdot, 1, ^{-1})$	$\{-1\} \cup \{p \mid p \text{ prim}\}$
Gruppe	$\mathsf{GL}(n, K)$	$\{S \mid S\ n \times n\text{-Elementarmatrix}\}$
Gruppe	$\mathsf{SL}(n, K)$	$\{S \mid S\ n \times n\text{-Scherungsmatrix}\}$
Gruppe	S_n	$\{\tau \mid \tau \text{ Vertauschung } i \leftrightarrow j\}$
Gruppe	D_n	$\{\rho, \sigma\},\ \rho\ n\text{-zählige Drehung}, \sigma \text{ Spiegelung}$
Ring	$(\mathbb{Z}, +, 0, -, \cdot, 1)$	$\emptyset$
Ring	$(\mathbb{Q}, +, 0, -, \cdot, 1)$	$\{\frac{1}{p} \mid p \text{ prim }\}$
Körper	$(\mathbb{Q}, +, 0, -, \cdot, 1, ^{-1})$	$\emptyset$
K-Modul	K^n	$\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\}$
$\mathbb{R}$-Modul	$\mathbb{C}$	$\{1, i\}$
R-Algebra	$R[x_1, \ldots, x_n]$	$\{x_1, \ldots, x_n\}$
$\mathbb{R}$-Algebra	$\mathbb{C}$	$\{i\}$

Korollar 3.5 *Für ein kommutatives Monoid M gilt*

$$\mathsf{Spann}\, E = \{\prod_{i=1}^{n} v_i^{n_i} \mid n_i \in \mathbb{N}\} \quad \textit{falls } E = \{v_1, \ldots, v_n\}$$

Korollar 3.6 *Für einen K-Modul V gilt*

$$\mathsf{Spann}\, E = \{\sum_{i=1}^{n} r_i v_i \mid r_i \in K\} \quad \textit{falls } E = \{v_1, \ldots, v_n\}$$

$$\mathsf{Spann}\, E = \{\sum_{i=1}^{n} r_i v_i \mid n \in \mathbb{N},\ v_i \in E,\ r_i \in K\}$$

Korollar 3.7 *Für eine kommutative K-Algebra A gilt für $E = \{v_1, \ldots, v_n\}$*

$$\mathsf{Spann}\, E = \{\sum_{n_1, \ldots, n_k} r_{n_1, \ldots n_k} \prod_{i=1}^{k} v_i^{n_i} \mid k \in \mathbb{N},\ (n_1, \ldots, n_k) \in \mathbb{N}^k,\ r_{n_1, \ldots n_k} \in K\}$$

3.3 Isomorphismen

Der Begriff der algebraischen und sonstigen mathematischen Strukturen ergibt sich zwangsläufig, wenn man Mathematik nicht nur als Rechnung oder Herleitung von Aussagen verstehen will, sondern auch Objekte denken will, auf die sich diese Rechnungen und Aussagen beziehen. Zudem erhält man die Möglichkeit, aus schon bekannten Objekten neue zu konstruieren. Man hat dann aber zu akzeptieren, dass es z.B. 'den' Körper $\mathbb{Q}$ der rationalen Zahlen nur 'bis auf Isomorphie' gibt, d.h dass die gedachte Realisierung (z.B. als Quotienten ganzer Zahlen oder als periodische Dezimalzahlen) nicht mit erfasst ist. Will man das doch, so hat man den Strukturbegriff entsprechend zu erweitern, aber auch dann hat mans letzlich nur bis auf Isomorphie. Man sollte dies aber eher als Vorteil sehen, da die Aufmerksamkeit auf die jeweils relevanten Fragen gerichtet wird. Jedenfalls wollen wir uns das Denken in Strukturen nicht vermiesen lassen. Dass die Umsetzung für den Schulunterricht eine diffizile Aufgabe ist, steht auf einem anderen Blatt.

Ein *Isomorphimsus* zwischen zwei algebraischen Strukturen A und B desselben Typs wird angeben durch eine bijektive Abbildung $\phi : A \to B$ derart, dass für jede fundamentale Operation f gilt:

$$\text{für alle } a_1, \ldots, a_n, a \in A.\ \ f^A(a_1, \ldots, a_n) = a \ \Leftrightarrow\ f^B(\phi a_1, \ldots, \phi a_n) = \phi a$$

Man sagt auch ϕ ist ein Isomorphismus von A auf B bzw. $\phi : A \to B$ ist ein Isomorphismus. Dass ϕ ein Isomorphismus des Rings R auf S ist, bedeutet demnach

$$\phi(a +_R b) = \phi a +_S \phi b,\ \phi 0_R = 0_S,\ \phi -_R a = -_S \phi a,\ \phi(a \cdot_R b) = \phi a \cdot_S \phi b,\ \phi 1_R = 1_s$$

Bei R-Moduln bzw. -Algebren hat man insbesondere bzgl. der skalaren Multiplikation in A bzw. B die Bedingungen $\phi(ra) = r\phi a$ für jeden Skalar $r \in R$, d.h. eine lineare Abbildung.
Beispiel. Der Witz des Rechnens mit Blockmatrizen ist z.B. der natürliche Isomorphismus von R_n auf $(R_m)_k$ wobei $n = mk$

$$\begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \vdots & \\ a_{n1} & \ldots & a_{nn} \end{pmatrix} \mapsto \begin{pmatrix} A_{11} & \ldots & A_{1k} \\ \vdots & & \vdots \\ A_{k1} & \ldots & A_{kk} \end{pmatrix},\ \ A_{ij} = \begin{pmatrix} a_{im+1,jm+1} & \ldots & a_{im+1,jm+m} \\ \vdots & & \vdots \\ a_{im+m,jm+1} & \ldots & a_{im+m,jm+m} \end{pmatrix}$$

Lemma 3.8 *Ist ϕ Isomorphismus von A auf B so ist die Umkehrabbildung ϕ^{-1} ein Isomorphismus von B auf A. Ist zudem ψ Isomorphismus von B auf C, so ist die Hintereianderausführung $\psi \circ \phi$ Isomorphismus von A auf C.*

Beweis als Übung. Gibt es einen Isomorphismus von A auf B, so heissen A und B (zueinander) *isomorph* und man schreibt $A \cong B$. Nach dem Lemma gilt

$$A \cong A, \quad A \cong B \Rightarrow B \cong A, \quad A \cong B \cong C \Rightarrow A \cong B$$

Prinzip 3.9 *Sind A und B isomorph, so gelten für A und B dieselben Aussagen.*

Ein Isomorphismus ϕ von A auf A heisst ein *Automorphismus* von A. *Beispiele.*

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{R}, \quad \phi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2}),\ \ \phi(a + b\sqrt{2}) = a + b(-\sqrt{2})$$

$$\phi : \mathbb{C} \to \mathbb{C}, \quad \phi(a + bi) = a + b(-i)$$

D.h. man kann $\sqrt{2}$ und $-\sqrt{2}$ nicht unterscheiden, wen man in $\mathbb{Q}(\sqrt{2})$ sitzt. Ebenso mit i und $-i$ in $\mathbb{C}$. In ersten Fall kann man sich noch retten, wenn man die Ordnung $<$ als weiteren Strukturbestandteil hinzunimmt. Bei $\mathbb{C}$ hilft nicht einmal Didaktik: auch wenn man glaubt, es gebe 'die' reellen Zahlen, die komplexen hat man nur bis auf diesen Automorphismus. Die Geometrie hilft auch nicht weiter, da 'die Ebene' keine inherente Orientierung hat. Es bleibt also nur im Bourbaki-Stil zu sagen: Sei i ein ausgezeichnetes Element von $\mathbb{C}$ mit $i^2 = -1$. Ein Unglück ist das nicht.

3.4 Automorphismengruppen.

Hat man auf A und B zusätzlich (oder nur) eine binäre Relation notiert z.B. als $<_A$ und $<_B$ so muss man von einem Isomorphismus $\phi : A \to B$ für diese (neben der Bijektiviät und den Bedingungen für die Operationen) verlangen

$$a <_A b \;\Leftrightarrow\; \phi(a) <_B \phi(b)$$

Ist $A = B$ so spricht man von *Automorphismen.*

Korollar 3.10 *Die Automorphismen einer Struktur A bilden eine Untergruppe $\mathsf{Aut}(A)$ der Gruppe S_A aller Permutationen von A.*

Eine Menge A mit binärer Relation $<$ heisst auch ein *gerichteter Graph*, die Elemente *Ecken.* Die Kanten sind die Paare (a, b) mit $a < b$. Der Graph ist ungerichtet, falls $a < b \Leftrightarrow b < a$. In diesem Fall kann man die Kanten als Mengen $\{a, b\}$ auffassen.

3.5 Homomorphismen

Ein *Homomorphismus* $\phi : A \to B$ einer algebraischen Struktur A in eine Struktur B gleichen Typs wird angegeben durch eine Abbildung $\phi : A \to B$, die mit den Operationen *vertäglich* `[comparible]` ist

$$\phi(f^A(a_1, \ldots, a_n)) = f^B(\phi a_1, \ldots, \phi a_n) \qquad \begin{array}{l}\text{für jede fundamentale Operation } f \\ \text{und alle } a_1, \ldots, a_n \in A\end{array}$$

sofern $f^A(a_1, \ldots, a_n)$ erklärt ist. Insbesondre $\phi c_A = c_B$ für jede fundamentale Konstante c. ϕ ist *Endomorphismus* von A, falls $A = B$ (als Strukturen). Im Falle der R-Moduln spricht man auch von (R)*linearen Abbildungen.*

Beispiele. Alle Isomorphismen.

$$(\mathbb{R}, +, 0, -) \to (\mathbb{C}_{\neq 0}, \cdot, 1, ^{-1}), \quad x \mapsto e^{xi} = \cos x + i \sin x$$

Die Abbildung det von $\mathsf{GL}(n, K)$ in die Gruppe $K_{\neq 0}$.

Lemma 3.11 *Sind $\phi : A \to B$ und $\psi : B \to C$ Homomorphismen, so auch $\psi \circ \phi : A \to C$. Ein Homomorphismus $\phi : A \to B$ ist genau dann ein Isomorphismus, wenn es einen Homomorphismus $\psi : B \to A$ gibt mit $\psi \circ \phi = \mathsf{id}_A$ und $\phi \circ \psi = \mathsf{id}_B$, d.h. wenn ϕ bijektiv ist und $\phi^{-1} : B \to A$ auch Homomorphismus ist.*

Beweis. Hintereinanderausführung als Übung. Ist ϕ^{-1} Homomorphismus, so folgt aus $\phi a = f^B(\phi a_1, \ldots, \phi a_n)$, dass $a = \phi^{-1}\phi a = \phi^{-1} f^B(\phi a_1, \ldots, \phi a_n) =$
$= f^A(\phi^{-1}\phi a_1, \ldots, \phi^{-1}\phi a_n) = f^A(a_1, \ldots, a_n)$. □ Gibt es einen surjektiven Homomorphismus von A auf B, so sagt man.B sei *homomorphes Bild* von A. Im allgemeinen ist $\mathsf{Bild}\phi = \{\phi a \mid a \in A\}$ eine Unterstruktur von B.

Prinzip 3.12 *Alle Aussagen, die als logische Zeichen nur $\wedge, \vee, \exists, \forall$ benutzen, übertragen sich von A auf jedes homomorphe Bild von A.*

Setzt man voraus, dass A und B schon zu einer der uns interessierenden Klassen gehören, kann man aus einem Teil der Verträglichkeitsbedingungen die restlichen beweisen

Klasse $\mathcal{C}$	Verträglichkeitsbedingung (V)	(N)
Monoide	$\phi(a \cdot b) = \phi a \cdot \phi b$	$\phi e = e$
Gruppen	$\phi(a \cdot b) = \phi a \cdot \phi b$	
Ringe	$\phi(a + b) = \phi a + \phi b, \quad \phi(a \cdot b) = \phi a \cdot \phi b$	$\phi 1 = 1$
Körper	$\phi(a + b) = \phi a + \phi b, \quad \phi(a \cdot b) = \phi a \cdot \phi b$	
R-Moduln	$\phi(a + b) = \phi a + \phi b, \quad \phi(ra) = r\phi a \, (r \in R)$	
R-Algebren	$\phi(a + b) = \phi a + \phi b, \quad \phi(ra) = r\phi a \, (r \in R), \quad \phi(a \cdot b) = \phi a \cdot \phi b$	$\phi 1 = 1$

Proposition 3.13 *Sei $\mathcal{C}$ wie in der Tabelle und $A \in \mathcal{C}$.*

$B \in \mathcal{C}, \quad \phi : A \to B$	*mit* $(V) + (N)$	*dann* $\phi : A \to B$ *Homomorphismus*
$B \in \mathcal{C}, \quad \phi : A \to B$ *surjektiv*	*mit* (V)	*dann* $\phi : A \to B$ *Homomorphismus*
$B \in \mathcal{C}, \quad \phi : A \to B$ *bijektiv*	*mit* (V)	*dann* $\phi : A \to B$ *Isomorphismus*

Ist $\phi : A \to B$ ein surjektiver Homomorphismus, so $B \in \mathcal{C}$. Ist $\phi : A \to B$ eine surjektive Abbildung, die (V) erfüllt, so kann man die restlichen Operationen auf B auf genau eine Weise so definieren, dass $\phi : A \to B$ ein Homomorphismus wird oder $B \in \mathcal{C}$ (und dann gilt beides).

Beweis. Wir betrachten nur den Fall der Gruppen (Rest als Übung) und erinnern uns, dass in einer Gruppe das neutrale Element e eindeutig bestimmt ist durch $e \cdot e = e$ und das Inverse x^{-1} durch $xx^{-1} = e$. Damit ist klar, dass (V) als Homomorphiebedingung ausreicht. Ist ϕ bijektiv, so ergibt $\phi^{-1}\phi a \cdot \phi^{-1}\phi b = a \cdot b = \phi^{-1}\phi(a \cdot b) = \phi^{-1}(\phi a \cdot \phi b)$ die Bedingung (V) für ϕ^{-1} und wir können das Lemma anwenden. Dass sich die Gruppeneigenschaft auf homomorphe Bilder überträgt, liegt daran, dass sie durch Gleichungen definiert ist. Hat man in B zunächst nur eine Multiplikation, aber eine surjektive Abbildung ϕ von A auf B mit (V), so erhält man mit $e_B := \phi e_A$ und $(\phi a)^{-1} := \phi(a^{-1})$ neutrales Element und Inverse. □

Lemma 3.14 *Wird A von E erzeugt und sind $\phi, \psi : A \to B$ Homomorphismen, so gilt*

$$\phi|E = \psi|E \;\Rightarrow\; \phi = \psi$$

Beweis. $U = \{a \in A \mid \phi a = \psi a\}$ ist eine Unterstruktur von A und $U \supseteq E$, also $U = A$. Nämlich für $a_i \in U$

$$\phi f^A(a_1, \ldots, a_n) = f^B(\phi a_1, \ldots, \phi_a n) = f^B(\psi a_1, \ldots, \psi a_n) = \psi f^A(a_1, \ldots, a_n) \;\square$$

Korollar 3.15 *Wird A von $\emptyset$ erzeugt, so gibt es zu jedem B höchstens einen Homomorphimsus $\phi : A \to B$. Insbesondre gibt es zu jedem Ring R höchstens einen Homomorphismus $\phi : \mathbb{Z} \to R$.*

Ein injektiver Homomorphismus $\phi : A \to B$ heisst auch eine *Einbettung* von A in B. Dann ist $\mathsf{Bild}(\phi)$ eine zu A isomorphe Unterstruktur von B.

3.6 Äquivalenzrerl;ationen

Eine binäre Relation $\sim$ auf einer Menge M heisst eine *Äquivalenzrelation*, wenn für alle $x, y, z \in M$ gilt

$(E1)$	$x \sim x$	Reflexivität
$(E2)$	$x \sim y \Rightarrow y \sim x$	Symmetrie
$(E3)$	($x \sim y$ und $y \sim z$ $\Rightarrow x \sim z$	Transitivität

Beispiele: 1. Zwei Brüche bedeuten die gleiche rationale Zahl

$$\frac{a}{b} \sim \frac{c}{d} \;\Leftrightarrow\; ad = bc.$$

2. Zwei rationale Cauchyfolgen bedeuten die gleiche reelle Zahl

$$(a_n)_{n\in N} \sim (b_n)_{n\in N} \;\Leftrightarrow\; (a_n - b_n)_{n\in N} \text{ ist Nullfolge}$$

3. Zwei Quotienten reeller Polynome bedeuten die gleiche rationale Funktion

$$\frac{p(x)}{q(x)} \sim \frac{r(x)}{s(x)} \;\Leftrightarrow\; p(x)s(x) \equiv r(x)(q(x)$$

4. Zwei Pfeile im Anschauungsraum bedeuten den gleichen Vektor

$$\begin{aligned}(P,Q) \sim (P',Q') \quad &\Leftrightarrow\; P,Q,Q',P' \text{ ist Parallelogramm}\\ &\Leftrightarrow\; (P,Q) \text{ und } (P',Q') \text{ haben dieselbe Länge und Richtung}\end{aligned}$$

5. Zwei Tupel stimmen in gewissen Komponenten überein

$$(a_i \mid i \in I) \sim_J (b_i \mid i \in I) \;\Leftrightarrow\; \text{ für alle } j \in J.\ a_j = b_j$$

6. Zwei ganze Zahlen haben den gleichen Rest modulo n

$$a \sim_n b \;\Leftrightarrow\; a \equiv b \bmod n \;\Leftrightarrow\; n \text{ teilt } a - b$$

7. Zwei algebraische Strukturen sind isomorph

$$A \sim B \;\Leftrightarrow\; A \cong B$$

8. Für eine Abbildung $\phi : M \to .$ der *Kern* `[kernel]` $\sim_\phi$

$$x \sim_\phi y \;\Leftrightarrow\; \phi(x) = \phi(y).$$

9. Sind $\sim_1, \ldots, \sim_n$ Äquivalenzrelationen auf M, so auch der *Durchschnitt* mit

$$a \sim b \;\Leftrightarrow\; a \sim_1 b \text{ und } \ldots \text{ und } a \sim_n b$$

3.7 Klasseneinteilung

Sei $\sim$ eine Äquivalenzrelation auf M. Wir definieren

$$\tilde{a} := a[\mathsf{mod}\sim] = [a] = \{x \in M | \, x \sim a\} \text{ die (Äquivalenz)Klasse von } a \text{ nach/modulo } \sim .$$

Lemma 3.16 *$a \in \tilde{a}$ und $a \sim b \Leftrightarrow \tilde{a} = \tilde{b} \Leftrightarrow \tilde{a} \cap \tilde{b} \neq \emptyset$.*

Beweis. $a \in \tilde{a}$ nach (E1). Sei $a \sim b$. Aus $x \sim a$ folgt dann mit (E3), dass $x \sim b$, also $\tilde{a} \subseteq \tilde{b}$. Wegen (E2) haben wir auch $b \sim a$ und $\tilde{b} \subseteq \tilde{a}$. Also haben $\tilde{a}$ und $\tilde{b}$ dieselben Elemente, weshalb $\tilde{a} = \tilde{b}$. Dann natürlich $\tilde{a} \cap \tilde{b} \neq$ *emptyset*.

Gelte umgekehrt $\tilde{a} \cap \tilde{b} \neq \emptyset$, d.h. es gibt $x \in \tilde{a} \cap \tilde{b}$, Dann $x \sim a$ und $x \sim b$, mit (E2) $a \sim x$ und mit (E3) $a \sim b$. □

Eine *Partition* oder *Klasseneinteilung* von M ist ein System Π von Teilmengen von M derart, dass

$(P1)$ $P \neq \emptyset$ für alle $P \in \Pi$
$(P2)$ Zu jedem $x \in M$ gibt es $P \in \Pi$ mit $x \in P$
$(P3)$ Für alle $P, Q \in \Pi$ gilt $P = Q$ oder $P \cap Q = \emptyset$

Lemma 3.17 *Zwischen Äquivalenzrelationen und Partitionen auf einer Menge M besteht eine bijektive Entsprechung vermöge*

$$\Pi_\sim = \{\tilde{a} \mid a \in M\}, \quad a \sim_\Pi b \Leftrightarrow \text{ es gibt } A \in \Pi \text{ mit } a, b \in A.$$

Partitionen taugen insbesondre als bildliche Vorstellung von Äquivalenzrelationen. Beweis. Dass zu eine Äquivalemnzrelation eine Partition gehört, folgt sofort aus den vorangehenden Lemma. Ist die Partition gegeben, so gilt (E1) wegen (P2) und (E2) ist trivial. Hat man $a \sim_\Pi b \sim_\Pi c$, so $a, b \in A$ und $b, c \in B$ mit $A, B \in \Pi$, also $b \in A \cap B$ und $A = B$ nach (P3), also $a \sim_\Pi c$.

Wir müssen aber auch noch zeigen, dass wir durch zweimaligen Seitenwechsel zum Ausgangspunkt zurückkommen, d.h.

$$a \sim_{\Pi_\sim} b \Leftrightarrow a \sim b \quad \text{und} \quad \Pi_{\sim_\Pi} = \Pi$$

Dazu: $a \sim_{\Pi_\sim} b$ bedeutet $a, b \in \tilde{c}$ für ein c, also $a \sim c \sim b$ und somit $a \sim b$. Andererseits gibt es nach (P2) zu jedem $a \in M$ ein $P \in \Pi$ mit $a \in P$ und nach (P1) zu jedem $P \in \Pi$ ein $a \in P$. Es ist also zu zeigen

$$\tilde{a}^\Pi = P \text{ falls } a \in P$$

Nun

$$\tilde{a}^\Pi = \{x \in M \mid \text{ es gibt } Q \in \Pi \text{ mit } x, a \in Q\} = \{x \in M \mid x, a \in P\} = P$$

weil hier stets $Q = P$ nach (P3). □.

3.8 Repräsentanten

Sei $\sim$ eine Äquivalenzrelation auf M. Ein Element a von M heisst *Repräsentant* der Klasse A, wenn $a \in A$. Also

$$a, b \text{ repräsentieren dieselbe Klasse, nämlich } \tilde{a} = \tilde{b}, \Leftrightarrow a \sim b.$$

Eine Teilmenge S von M, die aus jeder Klasse genau einen Repräsentanten enthält, heisst ein *Repräsentantensystem*.

Prinzip 3.18 *Jede Äquivalenzrelation hat mindestens ein Repräsentantensystem*

Hat man eine Aufzählung von M gegeben, so kann man als Repräsentant jeweil das erste Element eine Klasse nehmen. Im allgemeinen ist das Prinzip zum Auswahlaxiom gleichwertig. Die Angabe eines konkreten Repräsentantensytems ist meist eine nichttriviale, im Prinzip eine unlösbare Aufgabe. Für obige Beispiele hat man z.B. folgende Repräsentantensysteme

1	$\frac{a}{b}$	a, b teilerfremd, $b > 0$
2	$(a_n)_{n\in\mathbb{N}}$	$a_0 \in \mathbb{Z},\ \forall n > 0.\ (a_n - a_{n-1})10^n \in \{0, \ldots, 9\},\ \forall m.\exists n.\ (a_n - a_{n-1})10^n \neq 9$
3	$\frac{p(x)}{q(x)}$	$p(x), q(x)$ teilerfremd, $q(x)$ normiert
4	(O, Q)	mit festem Punkt O
5	$(a_i \mid i \in I)$	$a_j = 0_j$ für alle $j \in J$ mit ausgezeichnetem $0_j \in A_j$
6	a	$a \in \mathbb{Z},\ 0 \leq a < n$

3.9 Kongruenzrelationen

Von Leibniz haben wir gelernt, dass wir, wenn wir in einer algebraischen Struktur A einen erweiterten Gleichheitsbegriff einführen wollen, wir eine Äquivalenzrelation $\sim$ benutzen sollen, die mit der Struktur *verträglich* `[compatible]` ist

$$a_1 \sim b_1 \wedge \ldots \wedge a_n \sim b_n \quad \Rightarrow f^A(a_1, \ldots, a_n) \sim f^A(b_1, \ldots, b_n)$$
für jede fundamentale Operation f
und alle $a_1, b_1, \ldots, a_n, b_n \in A$

wobei wir voraussetzen, dass $f^A(a_1, \ldots, a_n)$ und $f^A(b_1, \ldots, b_n)$ beide erklärt sind. Dann heisst $\sim$ auch eine *Kongruenzrelation* `[congruence relation]` der Struktur A. Die Äquivalenzklassen von $\sim$ heissen dann auch *Kongruenzklassen.*

Korollar 3.19 *Ist $\phi : A \to B$ ein Homomoprhismus, so ist die folgende* Kern(relation) *eine Konrguenzrelation auf A*

$$a \sim_\phi b \ \Leftrightarrow\ a \,\mathsf{Ker}\phi\, b \ \Leftrightarrow\ \ \phi a = \phi b$$

Lemma 3.20 *Eine Äquivalenzrelation auf einer algebraischen Struktur A ist schon dann Kongruenzrelation , wenn jede fundamentale Operation die Verträglichkeiysbedingung erfüllt, wobei jeweisl nur ein Argument variabel ist, d.h. für jedes $k \leq n$ und alle $a_1, \ldots, a_n, b_k \in A$*

$$a_k \sim b_k \ \Rightarrow\ f^A(a_1, \ldots, a_{k-1}, a_k, a_{k+1}, \ldots, a_n) \sim f^A(a_1, \ldots, a_{k-1}, b_k, a_{k+1}, \ldots, a_n)$$

Beweis. Hat man $a_i \sim b_i$ für alle $i \leq n$, so $f^A(a_1, a_2 \ldots, a_n) \sim f^A(b_1, a_2, a_3, \ldots, a_n) \sim f^A(b_1, b_2, a_3, \ldots, a_n) \sim \ldots \sim f^A(b_1, \ldots, b_n)$. Mit der Transitivität folgt die Behauptung. □

Lemma 3.21 *Ist θ Konrguenzrelation auf A und U Unterstruktur von A so ist die Einschränkung $\theta|U$ (d.h. $x(\theta|U)y \Leftrightarrow x\theta y$ für $x, y \in U$) Kongruenzrelation auf U.*

Beweis: klar, □. Setzt man voraus, dass A Monoid, Gruppe, Ringe, R-Modul oder R-Algebra ist, kann man aus einem Teil der Verträglichkeitsbedingungen die restlichen beweisen

Klasse $\mathcal{C}$	Verträglichkeitsbedingung (V)
Monoide, Gruppen	$a \sim b \Rightarrow\ \ a \cdot c \sim b \cdot c$ und $c \cdot a \sim c \cdot b$
Ringe	$a \sim b \Rightarrow\ \ a + c \sim b + c, \quad a \sim b \Rightarrow a \cdot c \sim b \cdot c$ und $c \cdot a \sim c \cdot b$
R-Moduln	$a \sim b \Rightarrow\ \ a + c \sim b + c$ und $ra \sim rb$
R-Algebren	$a \sim b \Rightarrow\ \ a + c \sim b + c$ und $ra \sim rb$ und $a \cdot c \sim b \cdot c$ und $c \cdot a \sim c \cdot b$

Proposition 3.22 *Sei $\mathcal{C}$ wie in der Tabelle und $A \in \mathcal{C}$. Dann ist eine Äquivalenzrelation auf A genau dann Kongruenzrelation, wenn sie (V) erfüllt.*

Beweis als Übung. □ Später können wir uns mit den Begriff der Faktorstruktur die meiste Arbeit sparen, z. B. für Gruppen: Nach Lemma 3.20 haben wir Veträglichkeit mit der Multiplikation. Dann ist aber die Faktorstruktur bzgl. der Multiplikation gemäss 3.12 und 3.13 eine Gruppe und die Projektion ein Homomorphismus. Also ist $\sim$ nach Satz ?? eine Gruppenkongruenz.

3.10 Beispiele von Kongruenzen

Lemma 3.23 *Ist R ein kommutativer Ring und p ein festes Element von R, so wird eine Kongruenz auf R definiert durch*

$$a \equiv b\,(\mathsf{mod} p) \;\Leftrightarrow\; p \text{ teilt } a-b \;\Leftrightarrow\; \exists z \in R.\ a-b = pz$$

Beweis als leichte Übung. □ Das kennen wir für $\mathbb{Z}$ bzw. $K[x]$.

Die Kongruenzen des Ringes $\mathbb{Z}$ sind auch Kongruenzen der Gruppe bzw. des Monoids $\mathbb{Z}$ und Einschränkung erhalten wir Kongruenzen des Monoids $\mathbb{N}$ (bzgl. $=, 0$). Auf $\mathbb{N}$ können wir aber allgemeinere Kongruenzen definieren

$$a \sim_{k,p} b \;\Leftrightarrow\; a = b \text{ oder } a, b \geq k \text{ und } p \text{ teilt } a-b$$

Wegen Lemma 3.20 genügt es zu zeigen: $a \sim_{k,p} b \Rightarrow a + c \sim_{k,p} b + c$. Die Klasseneinteilung ist wie in der Skizze.
Jede Kongruenz von $(\mathbb{N}, +, 0)$ hat diese Form. Ist $\sim$ gegeben, so sei k minimal so, dass es $b \neq k$ gibt mit $k \sim b$ (also $k \not\sim b$ für alle $b < k$), und dann p minimal mit $k \sim k + p$. Dann $np + k \sim k$ mit Induktion: $(n+1)p + k = p + np + k \sim p + k \sim k$, also $a \sim_{k,p} b \Rightarrow a \sim b$. Sei umgekehrt $a \sim b$ und $a \neq b$. Dann $k \leq a$ und $a = k + r + qp$ mit $0 \leq k < p$ und $a \sim_{k,p} k + r$. Ebenso $b \sim_{k,p} k + s$ und $0 \leq s < p$. Es folgt $k + r \sim k + s$. Sei z.B. $s > r$. Dann $k + p + (s - r) = k + r + p - s \sim k + s + p - s = k + p \sim k$ also $s - r = 0$ wegen der Minimalität p. Es folgt $a \sim_{k,p} b$. □

Fasst man Befehle als Buchstaben eines Alphabets und Wörter als Befehlsfolgen auf, so erhält man eine Kongruenz auf dem Wortmonoid, indem man (in einem gegebenen Zusammenhang) für zwei Wörter $a_1 \ldots a_n \sim b_1 \ldots b_m$ setzt, wenn die Befehlsfolgen $a_1, \ldots, a_n$ und $b_1, \ldots, b_m$ bei gleicher Ausgangslage stets zum gleichen Ergebnis führen. Z.B. vier Stühle $1, 2, 3, 4$ und vier Personen A, B, C, D und die Platzwechseloperationen s, d

$$d : 1 \mapsto 2 \mapsto 3 \mapsto 4 \mapsto 1, \quad s : 1 \leftrightarrow 3, 2 \mapsto 2, 4 \mapsto 4$$

Beim leeren Wort e passiert nichts. Dann gilt in $\{s, d\}^*$ z.B.

$$dddd \sim e,\ ss \sim e,\ ds = sddd,\ ds \not\sim sd,\ dd \not\sim e$$

3.11 Normalteiler, Ideale, Untermoduln beschreiben Kongruenzen

Eine Untergruppe N einer Gruppe G heisse ein *Normalteiler* `[normal subgroup]` von G, falls $gag^{-1} \in N$ für alle $g \in G$ und $a \in N$. Eine Untergruppe I der additiven Gruppe eines Rings R heisse ein *Ideal* von R, falls $ra \in I$ und $ar \in I$ für alle $r \in R$ und $a \in I$.

Satz 3.24 *Für Gruppen bzw. Ringe bzw. R-Moduln gibt es eine bijektive Entsprechung zwischen Kongruenzrelationen $\sim$ und Normalteilern N bzw. Idealen I bzw. Untermoduln U gegeben durch*

$$a \sim b \;\Leftrightarrow\; \begin{cases} ab^{-1} \in N & N = \{x \mid x \sim e\} \\ a - b \in I & I = \{x \mid x \sim 0\} \\ a - b \in U & U = \{x \mid x \sim 0\} \end{cases}$$

Beweis. Wir zeigen, dass zu einem Normalteiler N eine Gruppenkongruenz $\sim$ gehört. Reflexivität ist trivial. Symmetrie, da N under $^{-1}$ abgeschlossen. Transitivität, das N unter Multiplikation abgeschlossen. Sei $b \sim c$. Dann $ba(ca)^{-1} = bc^{-1} \in N$ und $ab((ac)^{-1} = abc^{-1}a^{-1}$ in N, da N normal. Also $ab \sim ac$ und $ba \sim ca$. Rest als Übung - insbeosndere dass man durch zweimaligen Wechsel zurückkommt. □

Entspricht der Normalteiler N der Kongruenz $\sim$ auf der Gruppe G, so haben die Kongruenzklassen die Gestalt

$$\tilde{a} = aN = Na = \{an \mid n \in N\}$$

und heissen deshalb auch *Nebenklassen* (hier ist links und rechts noch dasselbe). In der Tat, $a \sim b \Leftrightarrow e = a^{-1}a \sim a^{-1}b \Leftrightarrow a^{-1}b \in N \Leftrightarrow b \in aN$ und genauso auf der anderen Seite. Für den Untermodul bzw. Ideal U haben wir

$$\tilde{a} = U + a = \{u + a \mid u \in U\}$$

Ist R ein kommutativer Ring und $p \in R$, so ist

$$(p) = \{rp \mid r \in R\} = pR$$

das zur Kongruenz aus Lemma ?? gehörige Ideal und die Kongruenzklassen von der Form

$$a + (p) = \{a + rp \mid r \in R\}$$

Das Beispiel $(p) = p\mathbb{Z} \subseteq \mathbb{Z}$ motiviert die Bezeichnung als *Restklassen*.

Ist A Gruppe, Ring bzw. Modul, so entspricht die Kongruenz $\mathsf{Ker}(\phi)$ dem Normalteiler, Ideal bzw. Untermodul

$$\mathsf{Kern}(\phi) = \{x \in A \mid \phi(x) = e \text{ bzw. } = 0\}$$

- ϕ ist injektiv genau dann, wenn $\mathsf{Kern}(\phi) = \{e\}$ bzw. $= \{0\}$.

3.12 Direktes Produkt endlich vieler Faktoren

In der Linearen Algebra kommt man zwangsläufig dazu, die Menge K^n der n-Tupel von Elementen aus einem Körper K als Vektorraum zu verstehen. Und die Lineare Algebra ist so halbeinfach, weil jeder endlichdimensionale K-Vektorraum isomorph zu einem K^n ist.

Wir verallgemeinern im Rahmen der uns interessierenden algebraischen Strukturen. Sind $A_1, \ldots, A_n$ Mengen, so ist

$$A_1 \times \ldots \times A_n = \{ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \mid a_1 \in A_1 \text{ und } \ldots \text{ und } a_n \in A_n \}$$

die Menge der n-Tupel mit i-ter *Komponente* $a_i \in A_i$, das *direkte Produkt* der (Familie von) Mengen $A_1, \ldots, A_n$. Man kann statt Spalten auch Zeilen denken oder schreiben, wichtig ist nur

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \Leftrightarrow a_1 = b_1 \text{ und } \ldots \text{ und } a_n = b_n$$

Sind die A_i R-Moduln so ist das direkte Produkt `[direct product]` eine algebraische Struktur mit

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ \vdots \\ a_n + b_n \end{pmatrix}, \quad 0 = \begin{pmatrix} 0_1 \\ \vdots \\ 0_n \end{pmatrix}, \quad - \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} -a_1 \\ \vdots \\ -a_n \end{pmatrix}, \quad r \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} ra_1 \\ \vdots \\ ra_n \end{pmatrix}$$

für die wir ungeniert auch $A_1 \times \ldots \times A_n$ schreiben. Entsprechend für die anderen Typen von Strukuren. Man sagt

Die Operationen auf dem direkten Produkt sind komponentenweise erklärt

Gilt $A_i = A$ fúr a;;e i, so schreiben wir A^n und sprechen von *direkter Potenz*. Wie man leicht nachrechnet, ist das direkte Produkt von Monoiden/ Gruppen/ Ringen/ R-Moduln/ R-Algebren wieder ein solches und auch Kommutativität bleibt erhalten. Dagegen hapert es bei Integritätsbereichen und (Schief)körpern.

Zur Veranschaulichung von Produkten mit vielen oder gar unendlich vielen Faktoren A_i denke man sich die A_i als Halme `[stalks]` auf dem Indexfeld und die Elemente von $\prod_{i \in I} A_i$ als Schnitte `[section]` durch diese Halme: $(a_i \mid i \in I)$ schneidet aus dem Halm A_i gerade a_i heraus.

Prinzip 3.25 *Eine Aussage, die in allen A_i gilt, gilt auch in $\prod_{i \in I} A_i$, wenn sie folgende Form hat*

$$\forall x_1. \ldots . \forall x_n.\ s_1 = t_1 \wedge \ldots \wedge s_n = t_n \ \Rightarrow s = t \quad \textit{mit Termen } s_t, t_i, s, t$$

Beispiele sind (G1-4), (R5-9), (M5-8), (A) und die *Kürzungsregeln* `[cancellation rules]`

$$\forall x. \forall y. \forall z.\ xz = yz \Rightarrow x = y, \quad \forall x. \forall y. \forall z.\ zx = zy \Rightarrow x = y$$

Für jedes direkte Produkt $\prod_{i \in I} A_i$ und $J \subseteq I$ hat man einen Homomorphismus, *Projektion*

$$\pi_J : \prod_{i \in I} A_i \to \prod_{i \in J} A_i, \quad (a_i \mid i \in I) \mapsto (a_i \mid i \in J)$$

$\pi_j = \pi_{\{j\}} : \prod_{i \in I} A_i \to A_j$ heisst auch *kanonische Projektion*.

Lemma 3.26 *Sind $\phi_i : M \to M_i$ Homomorphismen, so erhält man einen (eindeutig bestimmten) Homomorphismus*

$$\phi : M \to \prod_{i \in I} M_i, \quad \textit{mit } \phi a = (\phi_i a \mid i \in I)$$

Beweis als leichte Übung. □.

4 Gruppen und Wirkungen

4.1 Definition

Die Symmetriegruppe G des Quadrats 'wirkt' auf der Menge M der Diagonalen: jede Symmetrie lässt entweder die Diagonalen fest oder vertauscht sie. Es können aber verschiedene Symmetrien dieselbe Wirkung haben, d.h. man kann G nicht immer als Untergruppe von S_M auffassen. Wir definieren daher: Eine *Wirkung* oder *Operation* einer Gruppe G auf einer Menge M ordnet jedem Element $g \in G$ und $x \in M$ ein Element $g(x) \in M$ zu so, dass gilt

$$e(x) = x, \quad (hg)(x) = h(g(x)) \qquad \text{für alle } g, h \in G,\ x \in M$$

Man darf auch $gx = g(x)$ schreiben.

Satz 4.1 *Die Wirkungen einer Gruppe G auf einer Menge M entsprechen bijektiv den Homomorphismen $\phi : G \to S_M$ vermöge*

$$\phi(g)(x) = g(x) \qquad \textit{für } g \in G,\ x \in M$$

Beweis. Sei eine Wirkung gegeben. Es ist zu zeigen, dass jedes $\phi(g) : M \to M$ bijektiv ist. Nun gibt es aber in G das inverse Element g^{-1} und wir haben $\phi(g^{-1})(\phi(g)(x)) = g^{-1}(g(x)) = (g^{-1}g)(x) = e(x) = e$ und $\phi(g)(\phi(g^{-1})(x)) = g(g^{-1}(x)) = (gg^{-1})(x) = e(x) = x$. Das besagt aber gerade, dass $\phi(g^{-1})$ die Umkehrabbildung von $\phi(g)$ ist und somit beide bijektiv. Die Homomorphiebedingung $\phi(hg) = \phi(h) \circ \phi(g)$ ist gleichbedeutend zu $(hg)(x) = h(g(x))$ (für alle $x \in M$), da $\phi(hg)(x) = (hg)(x)$ und $h(g(x)) = \phi(h)(\phi(g)(x)) = (\phi(h) \circ \phi(g))(x)$. Und $\phi(e) = \mathsf{id}_M$ bedeutet gerade, dass $\phi(e)(x) = x$ für alle x. □

4.2 Beispiele

- S_M wirkt kanonisch auf M als Gruppe von Abbildungen.
- Wirkt G auf M, so auch jede Untergruppe U von G - mit $g(x)$ wie vorher, aber nur für $g \in U$.
- Jede Untergruppe G von $\mathsf{Aut}(A)$ wirkt auf A, wobei A eine algebraische bzw. relationale Struktur.
- $\mathsf{GK}(n, k)$ wirkt auf K^n vermöge $(A, \boldsymbol{x}) \mapsto A\boldsymbol{x}$.

- Sei G eine Wirkung auf M und N eine Teilmenge von M so, dass

$$g(x) \in N \text{ für alle } g \in G,\ x \in N$$

d.h. dass N *invariant* ist unter G. Definiere die Wirkung von G auf N durch die *Einschränkung* auf N

$$(g, x) \mapsto g(x) \text{ für } x \in N, g \in G$$

Z.B wirkt so die Symmetriegrupe des Quadrats auf der Eckenmenge des Quadrats.

- Sei eine Wirkung von G auf M gegeben. Setze $g(X) = \{g(x) \mid x \in X\}$. Sei $\mathcal{X}$ eine Menge von Teilmengen X von M so, dass

$$\{g(X) \mid X \in \mathcal{X}\} \subseteq \mathcal{X}$$

Dann wird durch

$$(g, X) \mapsto g(X) \text{ für } X \in \mathcal{X},\ g \in G$$

eine Wirkung von G auf $\mathcal{X}$ definiert - die Symmetriegruppe des Quadrats wirkt auf der Menge der Diagonalen. Zum Beweis betrachte zunächst den Fall, dass $\mathcal{X}$ aus allen Teilmengen von M besteht. Danach wende Einschränkung an

- Ist V ein K-Vektorraum und $K^\times$ die Gruppe $K \setminus \{0\}$ mit der Multiplikation, so wird eine Wirkung gegeben durch

$$r(v) = rv \text{ für } r \in K^\times,\ v \in V.$$

- Die Gruppe der Vektoren der (Anschauungs)Raumes wirkt auf der Punktmenge - man spricht vom *affinen Raum*

- Die Untergruppe der $n \times n$-Permutationsmatrizen in $\mathsf{GL}(n, K)$ wirkt auf jeder Basis (als Menge aufgefasst) eines n-dimensionalen K-Vektorraums

4.3 Bahnen

Sei eine Wirkung der Gruppe G auf der Menge M gegeben. Die *Bahn* oder *Orbit* eines Elements a von M ist definiert als

$$G(a) = \{g(a) \,|\, g \in G\} \subseteq M.$$

Hat man nur die eine Bahn M, so spricht man von *transitiver* Wirkung. Ein *Repräsentantesystem* für eine Wirkung ist eine Teilmenge von M, die genau ein Element aus jeder Bahn enthält.

Lemma 4.2 *Die Bahnen der Wirkung einer Gruppe auf M sind die Klassen einer Äquivalenzrelation auf M*

$$x \sim y \quad \Leftrightarrow \quad \text{es gibt } g \in G \text{ mit } g(x) = y$$

Inbsondere gehört jedes Element von M zu genau einer Bahn - und das ist dann seine Bahn.

Beweis. Zunächst ist zu zeigen, dass $\sim$ Äquivalenzrelation ist. Wegen $e(x) = x$ haben wir $x \sim x$. Ist $x \sim y$, also $g(x) = y$ für ein $g \in G$, so $g^{-1}(y) = x$ und somit $y \sim x$. Haben wir $x \sim y \sim z$, so $y = g(x)$ und $h(y) = z$ für passende $g, h \in G$ und $(hg)(x) = h(g(x)) = h(y) = z$, woraus $x \sim z$. Die Klasse zum Element $a \in M$ ist $\{y \in M \mid a \sim y\} = \{y \in M \mid \exists g \in G.\ g(a) = y\}$ also gerade die Bahn $G(a)$ von a. Ist a auch in der Bahn $G(b)$ von b, so gilt folgt $b \sim a$. Also für jedes $x \in G(a)$ auch $b \sim a \sim x$ und somit $G(a) \subseteq G(b)$. Andererseits aber für jedes $y \in G(b)$ auch $a \sim b \sim y$ und somit $G(b) \subseteq G(a)$ und es folgt $G(b) = G(a)$. □

Beispiele.

- Die Wirkung von D_4 auf der Eckenmenge des Quadrats ist transitiv.
- Macht man aus zwei regelmässigen Tetraedern eine Doppelpyramide, so hat man bei der Wirkung der Symmetriegruppe auf der Eckenmenge 2 Bahnen: Die eine mit den Ecken des 'Grunddreiecks', die andere mit den beiden 'Spitzen'.
- Ist σ eine Permutation von M, so wirkt die Gruppe $\mathbb{Z}$ der ganzen Zahlen (mit Addition) auf M vermöge
$$(z, x) \mapsto \sigma^z(x) \text{ für } z \in \mathbb{Z},\ x \in M$$

4.4 Zykelzerlegung

Sei eine Permutation $\sigma \in S_n$ gegeben. Dann hat man eine Wirkung von $\mathbb{Z}$ auf $\{1, \ldots, n\}$ gegeben durch
$$za = \sigma^z(a)$$
σ ist ein *Zyklus* der Länge $l > 0$, wenn es genau 1 nichttriviale Bahn B gibt und $|B| = l$. Anders ausgedrückt, wenn es b und l gibt mit
$$B = \{(b, \sigma(b), \sigma^2(b), \ldots, \sigma^{l-1}(b)\} \text{ mit } l = |B| \text{ und } \sigma(x) = x \text{ für } x \notin B$$
Dann kann man σ in *Zykelschreibweise* (ausnahmseise von links nach rechts!) schreiben als
$$\sigma = [b \mapsto \sigma(b) \mapsto \sigma^2(b) \mapsto \ldots \mapsto \sigma^{l-1}(b) \mapsto b] = (b\, \sigma(b)\, \sigma^2(b) \ldots \sigma^{l_i-1}(b))$$
Die Identität ist Zyklus der Länge 0.

Proposition 4.3 *Für $\sigma \in S_n$ liefern die Bahnen $B_1, \ldots, B_m$ der Wirkung $\sigma \mapsto \sigma^z$ von Z die* Zykelzerlegung *von σ*
$$\sigma = \sigma_m \circ \ldots \circ \sigma_1 \text{ mit dem Zykeln } \sigma_i(x) = \begin{cases} \sigma(x) & \text{falls } x \in B_i \\ x & \text{sonst} \end{cases}$$
Dabei kommt es auf die Reihenfolge nicht an. Triviale Bahnen, d.h. $|B_i| = 1$, können weggelassen werden.

Beweis der Zerlegung ist trivial. Die Vertauschungsaussage folgt aus dem trivialen Lemma.

Lemma 4.4 *Ist $M = M_1 \cup M_2$ und $\sigma_i \in S_M$ mit $\sigma_i(M_i) = M_i$ und $\sigma_i | M_j = \mathsf{id}_{M_j}$ für $j \neq i$, so gilt $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$.*

Beweis: $(\sigma_1 \circ \sigma_2)(x) = (\sigma_2 \circ \sigma_1)(x) = \sigma_1(x)$ falls $x \in M_1$ und $= \sigma_2(x)$ falls $x \in M_2$. □

4.5 Symmetrische Gruppe

Für $\sigma \in S_n$ definieren wir das *Vorzeichen* oder *Signum* dorch

$$\mathsf{sign}\sigma = \prod_{i=1}^{m} -1^{l_i+1}$$

wobei die $l_1, \ldots, l_m$ die Längen der Bahnen $B_1, \ldots, B_m$ unter der Wirkung $\sigma \mapsto \sigma^z$ von $\mathbb{Z}$ sind. σ heisst *gerade*, falls $\mathsf{sign}\sigma = 1$, andernfalls *ungerade*. Eine *Transposition* ist eine Permutation τ mit

$$\tau = (ij) \text{ wobei } \tau(i) = j \neq \tau(j) = i,\ \tau(k) = k \text{ sonst}$$

und ihre eigene inverse. Es gilt $\mathsf{sign}\tau = -1$.

Proposition 4.5 sign *ist ein Homomorphismus von S_n auf die Gruppe $\{1, -1\}$. Jede Permutation lässt sich als Produkt von Transpositionen schreiben. Dabei ist die Anzahl dieser Transpositionen modulo 2 eindeutig bestimmt, und zwar gerade genau dann, wenn* $\mathsf{sign}\sigma = 1$.

Der Kern von sign ist eine Untergruppe von S_n, die *alternierende Gruppe* A_n der geraden Permutationen. Die Gruppe $\{1, -1\}$ kann als Untergruppe von $K^\times$ aufgefasst werden, wobei K ein beliebiger Körper mit $1 + 1 \neq 0$ ist. Zum Beweis folgendes Lemma:

Lemma 4.6 *Seien G und H Gruppen, G erzeugt von E , wobei $b^{-1} \in E$ für alle $b \in E$. Eine Abbildung $\phi : G \to H$ ist genau dann ein Homomorphismus, wenn $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$ für alle $a \in G$ und $b \in E$.*

Beweis: Jedes $b \in G$ lässt sich als $b = \prod i = 1^n b_i$ mit $b_i \in E$ schreiben. Durch Induktion über k folgt für alle $a \in G$: $\phi(a \cdot \prod_{i=1}^{k} b_i) = \phi((a \cdot \prod_{i=1}^{k-1} b_i) \cdot b_k) = \phi(a \cdot \prod_{i=1}^{k-1} b_i) \cdot \phi(b_k) = \phi(a) \cdot \phi(\prod_{i=1}^{k-1} b_i) \cdot \phi(b_k) = \phi(a) \cdot \phi(\prod_{i=1}^{k} b_i)$. $\square$.

Beweis der Prop. Zyklen können wir wie folgt als Produkte von Transpositionen darstellen

$$(b_0 b_1 \ldots b_l) = (b_0 b_l) \circ \ldots \circ (b_0 b_2) \circ (b_0 b_1)$$

Also können wir nach der Zykelzerlegung jede Permutation als Produkt von Transpositionen schreiben und nun das Lemma anwenden: Ist σ und eine Transposition τ gegeben, so haben wir zu zeigen

$$\mathsf{sign}\,(\tau \circ \sigma) = \mathsf{sign}\,(\tau) \cdot \mathsf{sign}\,(\sigma) = -\mathsf{sign}\,(\sigma)$$

Sei also $\sigma = \sigma_m \circ \ldots \circ \sigma_1$ eine Zerlegung in Zykeln mit den Bahnen $B_1, \ldots B_m$ mit $|B_i| > 1$ und τ Transposition mit Bahn $B = \{a, b\}/$ Nur die folgenden 4 Fälle können auftreten, In jedem wird das Sihnim von σ umgekehrt: durch Hinzufügen einer disjunkten Transpositioo, Zerlegung eines Zyjkus in zwei oder Vereining von zwei in einen, schliessloch durch Hinzugügen eines Elemets in einem Zyklus.
Fall 1: $B \cap B_i = \emptyset$ fur alle i. Zerlegung $\tau \circ \sigma = \tau \circ \sigma_m \circ \ldots \circ \sigma_1$
Fall 2: $B \subseteq B_i$. i ist eindeutig bestimmt. Sei $\sigma_i = (b_0 \ldots b_l)$ und $a = b_h, b = b_k$, $h < k$. Die Zerlgung von $\tau \circ \sigma$ erhält man durch Ersetzen von σ_i durch

$$\tau \circ \sigma_i = \mathsf{sign}\,(b_h \ldots b_{k-1}) \circ (b_0 \ldots b_{h-1} b_k \ldots b_l)$$

Fall 3: $|B \cap B_i| = 1$ fir genau ein i. Sei $a = b_h \in B_i$. Wir ersetzen σ_i durch

$$\tau \circ \sigma_i = (b_0 \dots b_{h-1} b b_h \dots b_l)$$

Fall 4: $|B \cap B_i| = 1 = |B \cap B_j|$ für eindeutig bestimmte $i < j$, o.B.d.AS. $a = b_h$, $\sigma_j = (c_r \dots c_0)$, $b = c_k$. Wir ersetzen $\sigma_j \circ \sigma_i$ durch

$$\tau \circ \sigma_j \circ \sigma_i = (b_0 \dots b_{h-1} c_k \dots c_r \dots c_{k-1} b_h \dots b_l) \quad \square$$

Die Gruppe S_n wird in $\mathsf{GL}(n, K)$ eingebettet durch

$$\sigma \mapsto P_\sigma \quad \text{wobei } P_\sigma = (p_{ij}) \text{ mit } p_{ij} = \begin{cases} 1 & \text{falls } i = \sigma(j) \\ 0 & \text{sonst} \end{cases}$$

d.h. in AP_σ ist die j-te Spalte von A durch die $\sigma(j)$-te ersetzt worden. Die Homomorphiebedingung $P_{\sigma\circ\tau} = P_\sigma \cdot P_\tau$ ist netterweise erfüllt, weil in $AP_\sigma P_\tau$ erst die $k = \tau(j)$-te Spalte durch die $\sigma(k) = \sigma(\tau(j))$-te und dann die j-te Spalte durch die $k = \tau(j)$-Spalte ersetzt wurde, insgesamt also die j-te Spalte durch die $\sigma(\tau(j))$-te ersetzt wurde - was gerade $AP_{\sigma\circ\tau}$ entspricht. Das Bild von S_n unter dieser Einbettung ist dann die Gruppe der *Permutationsmatrizen*. Den elementaren Vertauschungsmatrizen $P_\tau = [Si \leftrightarrow Sj]$ entsprechen dabei die *Transpositionen* τ. Die Gruppe der Permutationsmatrizen wirkt treu auf der Menge der Basisvektoren und ist zu S_n isomorph. Es folgt, dass jede Permutationsmatrix P_σ ein Produkt von Vertauschungsmatrizen ist und somit $\mathsf{sign}(\sigma) := \det P_\sigma = \pm 1$ falls $1 + 1 \neq 0$.

4.6 Reguläre Wirkung

Satz 4.7 *Jede Untergruppe U einer Gruppe G wirkt auf der Menge G vermöge der* Linksmultiplikation

$$(g, x) \mapsto g \times x \quad g \in U,\ x \in G$$

Die zugehörige Aëquivalenzrelation ist gegeben durch

$$a \sim_U b \ \Leftrightarrow \ \ b \cdot a^{-1} \in U \quad \textit{mit Klassen } U(a) = Ua := \{ua \mid u \in U\}$$

U wird bijektiv auf Ua abgebildet durch $u \mapsto ua$.

Man spricht von einer *reguläre* Wirkung von U auf G, im Falle $U = G$: *der. Beispiel:* affiner Raum

Beweis. Die Wirkungsgsetze ergeben sich sofort aus Assoziativität und Neutralität. Nun $a \sim b$ genau dann, wenn $b = ua$ für ein $u \in U$, d.h. $ba^{-1} = u$. Die Surjektivität der Abbildung von U auf Ua ist trivial, die Injektiviät folgt aus der Kürzungsregel: aus $ua = va$ folgt $u = v$. $\square$

Die Klassen Ua heissen auch *Rechtsnebenklassen* von U. Die Elementanzahl $|G|$ einer Gruppe heisst auch *Ordung*, die Anzahl $[G : U]$ der Rechtsnebenklassen einer Untergrupppe U der *Index* $[G : U]$.

Korollar 4.8 Lagrange. *Für jede Untergruppe U einer endlichen Gruppe G gilt:*

$$|G| = |U| \cdot [G : U]$$

Ganz analog kann man eine Äquivalenzrelation $a_U \sim b \Leftrightarrow a^{-1} \cdot b \in U$ und die zugehörige Zerlegung in *Linksnebenklassen* $a \cdot U$ definieren (dem entspricht eine Rechtswirkung von U auf G). Ihre Anzahl ist dann auch $[G : U]$.

Bei kommutativen Gruppen gibt es zu jedem Teiler der Ordnung von G auch mindestens eine Untergruppe dieser Ordnung. In nicht-kommutativen gibt es immer noch zu jeder Primzahlpotenz p^k so, dass p^k nicht jedoch p^{k+1} die Gruppenordnung $|G|$ teilt, eine *p-Sylow-Untergruppe* dieser Ordnung.

Korollar 4.9 *Ist $\phi : G \to H$ ein Homomorphismus und $|\phi(G)| = 2$, so sind $\mathsf{Kern}(\phi)$ und seine Nebenklasse $G \setminus \mathsf{Kern}(\phi)$ gleich gross.*

Beispiel. In jeder Symmetriegruppe, die eine Drehspiegelung enthält, gibt es genausoviel Drehungen wie Drehspiegelungen - benutze det. A_n hat halbsoviel Elemente wie S_n.

Die *Ordnung* eines Elements ist die Ordnung der von ihm erzeugten Untergruppe.

Korollar 4.10 *Die Ordnung eines Elements a teilt die Gruppenordnung und ist das kleinste $n > 0$ mit $a^n = 1$.*

4.7 Bahnformel

Die *Standuntergruppe* oder *Stabilisator* eines Elements a von M besteht aus den $g \in G$, die a festlassen

$$G_a = \{g \in G \,|\, g(a) = a\} \subseteq G.$$

Satz 4.11 ***Bahnformel.*** $|G| = |G_a| \cdot |G(a)|$.

Beweis. Sei $a \in M$ fest. Definiere für den Moment

$$\Phi(b) = \{g \in G \,|\, g(a) = b\} \text{ für } b \in G(a).$$

Die Mengen $\Phi(b)$ sind offenbar alle voneinander verschieden und jedes $g \in G$ gehört zu genau einem $\Phi(b)$. Und $\Phi(e) = G_a$. Es ist also zu zeigen, dass $|\Phi(b)| = |G_a|$ für alle $b \in G(a)$. Wir zeigen genauer

$$h \mapsto g_0 h\,, \quad h \in G_a$$

ist für festes $g_0 \in \Phi(b)$ Bijektion von G_a auf $\Phi(b)$. Injektivität: aus $g_0 h = g_0 k$ folgt $h = g_0^{-1} g_0 h = g_0^{-1} g_0 k = k$. Surjektivität: Sei $g \in \Phi(b)$. Dann $g_0^{-1} g(a) = g_0^{-1}(b) = a$, also $h = g_0^{-1} g \in G_a$ und $g = g_0 h$. □

Beispiele: Für das Quadrat gilt $|G(a)| = 4$, $|G_a| = 2$, also $|D_4| = 8$. Für das Tetraeder $|G(a)| = 4$, $|G_a| = 6$ also $|G| = 24$. Für die Doppelpyramide z.B. mit a eine Spitze: $|G(a)| = 2$, $|G_a| = |S_3| = 6$, also $|G| = 12$.

Will man die Bahnformel für die bestimmung größerer Gruppen benuzten, so hilft oft folgender Trick,

$$|G_a| = |G_{a,b}| \cdot |G_a(b)| \text{ wobei } G_{a,b} = G_a \cap G_b$$

d.h. man wendet die Bahnformel erstmal auf die Wirkung von G_a auf$M$ an. Den Trick kann man auch iterieren

$$|G_{a,b}| = |G_{a,b,c}| \cdot G_{a,b}(c) \text{ wobei } G_{a,b,c} = G_a \cap G_b \cap G_c$$

Für den Graphen mit Eckenmenge $V = \{1, \ldots, 10\}$ und Kantenmenge $E =$

$$\{\{i\, i+5\} \mid i = 1, \ldots, 5\} \cup \{i\, i+1\} \mid i = 1, 2, 3, 4\} \cup \{\{1\,5\}, \{6\,8\}, \{8\,10\}, \{10\,7\}, \{7\,9\}, \{9\,6\}\}$$

hat man

$$G_{1,2,5} = \{\mathsf{id}, (3\,7)(4\,10)(8\,9)\}$$

$$|G_{1,2}| = |G_{1,2,5}| \cdot 2,\ |G_1| = |G_{12}| \cdot 3,\ |G| = |G_1| \cdot 10 = 120$$

4.8 Treue

Eine Wirkung einer Gruppe G auf einer Menge M heisse *treu* , wenn

$$\text{zu allen Paaren } g \neq h \in G \text{ ein } x \in M \text{ existiert mit } g(x) \neq h(x).$$

Anders ausgedrückt: der Homomorphismus $\phi : G \to S_M$ mit $\phi(g)(x) = g(x)$ ist injektiv.
Beispiele: Ist G eine Untergruppe der Gruppe S_M aller Permutationen von M, so ist ihre natürliche Wirkung auf M treu. Die Symmetriegruppe des Quadrats wirkt nicht treu auf der Menge der Diagonalen. Bei der Wirkung des Körpers auf dem Vektorraum wird die Treue zum Exzess getrieben: $r = 1$ wenn nur $rv = v$ für ein einziges $v \neq 0$. Nur der Null ist alles wurscht.

Lemma 4.12 *Die Wirkung einer Gruppe G auf einer Menge M ist genau dann treu, wenn nur dann $g(x) = x$ für alle $x \in M$ gilt, wenn $g = e$ neutrales Element von G:*

$$\phi(g) = id_M \ \Rightarrow\ g = e.$$

Dann ist G auf natürliche Weise isomorph zu einer Untergruppe der Gruppe S_M.

Beweis. Es geht darum, dass der Homomorphismus $\phi : G \to s_M$ Kern $\{e\}$ hat. Im Fall der Treue besteht die zu G isomorph zu seinem Bild in S_M □

Korollar 4.13 Cayley *Die reguläre Wirkung einer Untergruppe auf einer Gruppe ist treu.*

Beweis. Die Treue folgt, indem man $x = e$ einsetzt: aus $g = ge = g(e) = h(e) = he = h$ folgt $g = h$. □ Es folgt (mit $U = G$), dass man jede Gruppe in eine symmetrische Gruppe einbetten kann.

Beispiele: Die Gruppe G der Symmetrien des Tetraeders wirkt treu auf der Menge $M = \{1, 2, 3, 4\}$ der Ecken (weil die ein Koordinatensystem liefern), also ist sie wegen $|G| = 24 = |S_4|$ zu S_4 isomorph.
Tüftleraufgabe: Finde möglichst kleines n so, dass die Drehgruppe des Dodekaeders zu einer Untergruppe von S_n isomorph ist, und gib diese Untergruppe an.

4.9 Cayley-Graphen

Sei G eine Gruppe mit ausgezeichneter Teilmenge A. Der zugehörige *Cayley-Graph* hat die Eckenmenge G und die mit a beschriftete Kante von x nach y falls $xa = y$. Anders ausgedrückt: es handelt sich um die Menge G mit den 2-stelligen Relationen

$$\Gamma_a = \{(x, y) \mid ga = h\}$$

Da a, sofern vorhanden, durch x, y eindeutig bestimmt ist, können wir

$$\alpha : \Gamma_A = \bigcup_{a \in A} \Gamma_a \to A \text{ definieren durch } \alpha(x,y) = a \Leftrightarrow xa = y$$

und somit aus Γ_a und α die Γ_a zurückgewinnen.

Lemma 4.14 *Die Gruppe G wirkt durch Linksmultiplikation als Untergruppe der Automorphismengruppe jedes ihrer Cayley-Graphen. D.h. wir haben einen injektiven Homomorphismus*

$$\phi : G \to \mathsf{Aut}(G, \Gamma_a(a \in A)), \quad \textit{mit } \phi(g)(x) = gx$$

Beweis. Dass G auf G treu wirkt, wurde schon gezeigt. Dass $\phi(g)$ ein Automorphimsus ist, heisst

$$(x,y) \in \Gamma_a \Leftrightarrow xa = y \Leftrightarrow gxa = gy \Leftrightarrow (gx, gy) \in \Gamma_a$$

Gilt a^2, so ist Γ_a symmetrisch, und man kann zwei gegegenläufige gerichtete Kanten durch eine ungerichtete ersetzen, d.h. $\Gamma_a = \{\{x,y\} \mid xa = y\}$.

Dem Weg $x_0, x_1, x_2, \ldots x_n$ im ungerichteten Graph G mit Kantenmenge $\{\{x,y\} \mid (x,y) \in \Gamma_A\}$ entspricht das Wort

$$w = a_1^{\varepsilon_1} \ldots a_n^{\varepsilon_n}, \quad \text{mit } x_{i_1} a^{\varepsilon_i} = x_i,\ a_i \in A$$

Setzen wir $x_0 = e$, so wird diese Entsprechung eindeutig,

Korollar 4.15 *G wird von A erzeugt genau dann, wenn der ungerichtete Graph zusammenhängend ist. Die Relationen der Form $w = e$ entsprechen dann genau den Wegen von e nach e.*

4.10 Innere Automorphismen und Konjugation

Ein Isomorphismus $\phi : A \to A$ heisst ein *Automorphismus.*

Lemma 4.16 *Sei G eine Gruppe und $g \in G$ fest. Dann erhält man einen (*inneren*) Automorphismus von G durch*

$$x \mapsto gxg^{-1}$$

Beweis. Die inverse Abbildung ist $y \mapsto g^{-1}yg$. Die Homomorphiebedingung folgt so: $gxg^{-1}gyg^{-1} = gxeyg^{-1} = gxyg^{-1}$. □

Lemma 4.17 *Jede Gruppe G wirkt auf der Menge G bzw. auf der Menge der Untergruppen von G durch* Konjugation

$$(g,x) \mapsto gxg^{-1}, \quad U \mapsto gUg^{-1} = \{gug^{-1} \mid u \in U\}$$

Beweis. $exe^{-1} = xe = e$ und $(hg)x(hg)^{-1} = h(gxg^{-1})h^{-1}$ und gUg^{-1} ist Untergruppe als Bild der Untergruppe U unter dem Homomorphismus $x \mapsto gxg^{-1}$. □

Zwei Elemente x, y bzw. Untergruppen U, V von G heissen zueinander *konjugiert*, wenn es $g \in G$ gibt, mit $y = gxg^{-1}$ bzw. $gUg^{-1} = V$, d.h. wenn sie in derselben Bahn liegen. Konjugiertheit ist somit eine Äquivalenzrelation auf G bzw. der Menge der Untergruppen von G - ihre Klassen heissen *Konjugiertenklassen.* Konjugierte Elemente bzw. Untergruppen sind 'abstrakt' nicht unterscheidbar - insbesondere sind konjugierte Untergruppen zueinander isomorph.

Lemma 4.18 *Bei der Wirkung einer Gruppe G sind Standgruppen zu Elementen derselben Bahn zueinander konjugiert.*

Beweis. Sei $b = g(a)$. Dann gilt für alle $h \in G_a$ dass $(ghg^{-1})(b) = g(h(g^{-1}(b))) = g(h(a)) = g(a) = b$, also $gG(a)g^{-1} \subseteq G_b$. Da $a = g^{-1}(b)$ folgt ebenso $g^{-1}G_bg \subseteq G_a$, also $G_b \subseteq gg^{-1}G_bgg^{-1} \subseteq gG_ag^{-1}$ und somit $G_b = gG_ag^{-1}$. □

Beispiele:

- In einer kommutativen Gruppe ist nix konjugiert.
- In D_4 sind jeweils die beiden Spiegelungen an den Diagonalen und die an den Mittelsenkrecchten zueinander konjugiert - veröge der 90^o- und 270^o-Drehung. Die 90^o- und 270^o-Drehung sind vermöge jeder Spiegelung konjugiert
- Bei der Drehgruppe des Tetraeders sind alle 120^o- und 240^o-Grad Drehungen konjugiert, und alle 180^o-Drehungen.

4.11 Normalteiler

Für Teilmengen A, B einer Gruppe ist das *Komplexprodukt* definiert als

$$AB = A \cdot B = \{a \cdot b \mid a \in A,\ b \in B\}$$

$$A^{-1} = \{a^{-1} \mid a \in A\},\ cA = \{c\}A,\ Ac = A\{c\}$$

Es gilt

$$eA = A = Ae,\ A(BC) = (AB)C,\ (AB)^{-1} = B^{-1}A^{-1}$$

$$e \in A,\ AA = A \text{ und } A^{-1} = A \text{ genau dann, wenn } A \text{ Untergruppe}$$

Lemma 4.19 *Für eine Untergruppe U $(= \overline{F})$ einer Gruppe G $(= \overline{E})$ sind die folgenden Aussagen äquivalent*

(1)	$a \cdot U = U \cdot a$	*für alle* $a \in G$
(2)	$a \cdot u \cdot a^{-1} \in U$	*für alle* $a \in G,\ u \in U$
(3)	$gUg^{-1} = U$	*für alle* $g \in G$
(4)	$gug^{-1} \in U$ *und* $g^{-1}ug \in U$	*für alle* $g \in E, u \in F$

Ein solches U ist nur zu sich selbst konjugiert und heisst ein *Normalteiler* von G.

Beweis. Gilt (1), so gibt es zu jedem $u \in U$ ein $v \in U$ mit $a \cdot u \cdot a^{-1} = v \cdot a \cdot a^{-1} = v \in U$. Gilt (2), so $aUa^{-1} \subseteq U$ für alle a, insbesondere $a = g$ und $a = g^{-1}$. Also auch $U \subseteq gg^{-1}U(g^{-1})^{-1}g^{-1} \subseteq gUg^{-1}$ und somit $U = gUg^{-1}$. Gilt (3) so mit $g = a^{-1}$ auch $aU = aa^{-1}Ua = Ua$. (4) folgt sofort aus (3). Gelte (4). Wir zeigen $aua^{-1} \in U$ für alle $u \in U$ und $a \in E$ oder $a^{-1} \in E$. Nämlich $u = \prod u_j$ mit $u_j \in F$ oder $u_j^{-1} \in F$ und daher $au_ja^{-1} \in U$, also $aua^{-1} = \prod_j (au_ja^{-1}) \in U$. Für solche a_i und $a = \prod_{i=1}^n a_i$ folgt nun mit Induktion $aua^{-1} = a_1 \dots a_n u a_n^{-1} \dots a_1^{-1} \in U$. Also (2) □

Beispiele:

- Jede Untergruppe vom Index 2 ist Normalteiler, z.B. die Untergruppe der Drehsymmetrien einer Symmetriegruppe oder die alternierende Gruppe A_n in der symmetrischen Gruppe S_n
- Der Kern eines Homomorphismus ist Normalteiler

4.12 Bestimmung von Konjugiertenklassen

Satz 4.20 *Für $\sigma, \tau \in S_n$ sind äquivalent*

- *σ und τ sind in S_n zueinander konjugiert*
- *σ und τ haben die gleiche Zyklenstruktur*
- *Die Wirkung von τ ergibt sich aus der Wirkung von σ durch Umbenennung der Elemente von $M = \{1, \ldots, n\}$*

M zerfällt in disjunkte Zyklen bzgl, σ und σ ist durch seine Einschränkungen auf diese eindeutig bestimmt. Gilt $\tau = \gamma^{-1} \circ \sigma \circ \gamma$, so erhält man aus B einen Zyklus von τ:

$\gamma^{-1}(B) =$
$\{\gamma^{-1}(x), \gamma^{-1} \circ \sigma \circ \gamma \circ \gamma^{-1}(x) = \tau(\gamma^{-1}(x)), \gamma^{-1} \circ \sigma \circ \gamma \circ \gamma^{-1} \circ \sigma \circ \gamma \circ \gamma^{-1}(x) = \tau^2(\gamma^{-1}(x)), \ldots\}$

Hat man umgekehrt eine 1-1-Entsprechung zwischen den Zyklen B_i von σ und C_i von τ, so definiere man eine Bijektion $\gamma_i : B_i \to C_i$, indem man $x \in B_i$ und $y \in C_i$ beliebig auswählt und dann setzt

$$\gamma_i(\sigma^l(x)) = \tau^l(y)$$

Es folgt $\tau|C_i = \gamma_i^{-1} \circ \sigma|B_i \circ \gamma_i$ und somit $\tau = \gamma^{-1} \circ \sigma \circ \gamma$, wenn man γ als Vereinigung der γ_i wählt (d.h. $\gamma(x) = \gamma_i(x)$ wobei i eindeutig bestimmt mit $x \in B_i$.

Weniger formal geht's so: Eine Permutation σ von M kann man auch so verstehen, dass mit den Nummern $1, \ldots, n$ nummerierte Dinge ihre Plätze tauschen sollen: Das Ding mit Nummer i soll den Platz des Dinges mit Nr. $\sigma(i)$ einnehmen. Die Konjugation mit γ^{-1} kann man dann als Umnummerierung verstehen

> Das Ding mit der neuen Nummer i hat die alte Nummer $\gamma(i)$

Dann gibt $\tau = \gamma^{-1} \circ \sigma \circ \gamma$ an, wie man für ein und dieselbe Permutation von Dingen die Beschreibung vom alten Nummernsystem ins neue umrechnet. □
Aus der Klassifikation orthogonaler Matrizen folgen

Korollar 4.21 *$A, B \in \mathsf{O}(2)$ sind genau dann konjugiert, wenn $A = \pm B$ oder $\det A = \det B = -1$*

Korollar 4.22 *$A, B \in \mathsf{O}(3, \mathbb{R})$ sind genau dann konjugiert, wenn $\det A = \det B$ und $\mathsf{Spur}(A) = \mathsf{Spur}(B)$, d.h. wenn es sich um Dreh(spiegel)ungen mit demselben nicht orientierten Winkel handelt.*

Korollar 4.23 *Sei G Untergruppe der Symmetriegruppe eines Polyeders. Notwendig dafür, dass die Dreh(spiegel)ungen ϕ und ψ in G konjugiert sind, ist*

- $\det(\phi) = \det(\psi)$, *d.h. ist* ϕ *Drehung so auch* ψ *und umgekehrt*
- *beide haben denselben nicht orientierten Winkel*
- *die Achse von* ϕ *kann durch einen Symmetrie aus* G *in die von* ψ *überführt werden*

Das ist hinreichend, falls zu G *eine Spiegelung an einer die Achse von* ϕ *(oder* ψ*) enthaltenden Ebene gehört.*

4.13 Klassengleichung

Korollar 4.24 *Eine Untergruppe ist Normalteiler genau dann, wenn sie Vereinigung von Konjugiertenklassen ist*

Das *Zentrum* $Z(G)$ einer Gruppe ist definiert als

$$Z(G) = \{x \in G \mid xg = gx \text{ für alle } g \in G\}$$

Lemma 4.25 *Das Zentrum ist ein Normalteiler und es gilt* $x \in Z(G)$ *genau dann, wenn* $\{x\}$ *Konjugiertenklasse ist. In einer abelschen Gruppe sind alle Konjugiertenklassen einelementig.*

Beweis. Sind $x, y \in Z(G)$ so $gxy = xgy = xyg$ und $gx^{-1} = (xg^{-1})^{-1} = (g^{-1}x)^{-1} = x^{-1}g$. Rest klar. □ Die folgende Aussage ist ganz simpel, verdient ihren schönen Namen aber wegen enormer Nützlichkeit, Der Beweis folgt sofort aus der Bahnformel.

Satz 4.26 Klassengleichung. *Jede Gruppe ist disjunkte Vereinigunng ihres Zentrums und der nichttrivialen Konjugiertenklassen* K_i*, Ist* G *endlich, so ist jedes* K_i *ein echter Teiler von* $|G|$*.*

$$|G| = |ZG) + |K_1| + \ldots + |K_r|, \;\; |G| = n_i|K_i| \text{ mit } 1 < n_i < |G|$$

Korollar 4.27 *Sei* $|G| = p^k$ *mit* p *prim. Dann ist* p *ein Teiler von* $|Z(G)|$*. Ist* $k \leq 2$*, so ist* G *abelsch.*

Beweis. Nach der Klassengleichung teilt p die $|K_i|$ also auch $|Z(G)|$. Sei nun $k = 2$ und $Z(G) \neq G$ angenommen, Wähle $g \in Z(G)$ und $h \notin Z(G)$. Dann hat $\mathsf{Spann}\{g, h\}$ Ordnung $> p$, also $= p^2$ nach Lagrange und ist somit $= G$. Wegen $gh = gh$ ist G abelsch (vgl. U2H2). □

4.14 Dodekaeder und Konjugierte in der Drehgruppe

Lemma 4.28 *Konjugation in* $\mathsf{SO}(2)$ *bedeutet Gleichheit. In einer Untergruppe* G *von* $\mathsf{SO}(3)$ *sind* ϕ *und* χ *genau dann konjugiert, wenn es zu einer/jeder gerichteten Achse* a *von* ϕ *ein* $\psi \in G$ *gibt so, dass* $b = \psi(a)$ *eine Achse von* χ *ist und die orientierten Drehwinkel von* ϕ *bzgl.* a *und von* χ *bzgl.* b *übereinstimmen.*

Beweis, $\mathsf{SO}(2) \cong \{z \in \mathbb{C} \mid |z| = 1\}$ also abelsch und damit alles klar. Nun sei $G \subseteq \mathsf{SO}(3)$ Sei $\chi = \psi \circ \phi \circ \psi^{-1}$. Dann $\mathsf{Spur}(\chi) = \mathsf{Spur}(\phi)$ d.h. es stimmen die unorietierten Drehwinkel überein. Sei nun a gerichtete Achse für ϕ und $b = \psi(a)$, Dann

$$\chi(b) = \psi\phi\psi^{-1}\psi(a) = \psi\phi(a) = \psi(a) = b$$

also bestimmt b eine Achse. Weil ψ Längen und Orientierung erhält gilt

$$\det(b, y, \psi(y)) = \det(a, x, \phi(x)) \quad \text{für alle } y = \psi(x)$$

d.h. es stimmen auch die orientierten Drehwinkel überein. Ist umgekehrt $\psi \in G$ wie verlangt gegeben, so folgt $\chi = \psi\phi\psi^{-1}$ da, wie gerade gezeigt, ψ mit χ in gerichteter Achse und orientiertem Winkel übereinstimmt. □

Beispiel: In der Drehgruppe des Tetraeders entsprechen dei Konjugiertenklassen gerade den Drehwinkeln 0^o, 120^o, 180^o, 240^o. Dass die 120^o und die 240^o-Drehung an derselben Achse nicht zueinander konjugiert sind, liegt daran, dass man die Achse nicht durch eine Drehung der Tetraeders umorientieren kann.

Das Dodekader hat 12 Flächen, 20 Ecken und 30 Kanten. Die Bahnformel bei Wirkung auf den Flächen ergibt für die Drehgruppe G die Ordnung $|G| = 5 \cdot 12 = 60$. Die Konjugiertenklassen und ihre Ordnugen ergeben sich so

- 1: id
- 20: $\pm 120^o$-Drehung um Achse durch gegenüberliegende Ecken
- 12 $\pm 72^o$-Drehung um Achse durch Mittelpunkte gegenüberliegender Flächen
- 12 $\pm 144^o$-Drehung um Achse durch Mittelpunkte gegenüberliegender Flächen
- 15: 180^o-Drehung um Achse durch Mittelpunkte gegenüberliegender Kanten

Satz 4.29 *Die Drehgruppe des Dodekaeders besitzt keinen echten Normalteiler und ist zur alternierden Gruppe A_5 isomorph.*

Beweis. Angeommen N ist echter Normalteiler, Dann $|N|$ echter Teiler von 60 und N Vereinigung von Konjugiertenklassen inklusive id, also $|N| > 13$. Damit $|N| \in \{15, 20, 30\}$. Diese Zahlen lassen sich aber nicht in der geforderten Weise als Summen schreiben. Also hat G keinen echten Normalteiler,

G wirkt nichttrivial auf der Menge der 5 eingeschriebenen Würfel des Dodekaeders, also hat man einen Homomorphismus $\phi : G \to S_5$. Da $\mathsf{Kern}(\phi)$ Normalteiler ist, folgt $\mathsf{Kern}(\phi) = \{\mathsf{id}\}$ und damit die Injektivität von ϕ. Wir haben den Homomorphismus $\mathsf{sign} : S_5 \to C_2$. also $\psi = \mathsf{sign} \circ \phi : G \to C_2$. $\mathsf{Kern}(\psi)$ ist Normalteiler, also trivial. Da ψ aus Anzahlgründen nicht injektiv ist, folgt $\mathsf{Kern}(\psi) = G$, also $\phi(G) \subseteq \mathsf{Kern}(\mathsf{sign}) = A_5$. Da $G| = 60 = |A_5|$ ist $\phi : G \to A_5$ Isomorphismus. □

4.15 Burnside-Lemma

Auf wieviele "wesentlich verschiedene" Weisen lässt sich ein Dodekaeder mit 2 Farben färben - mit einfarbigen Flächen?

Wenn wir die Flächen eines fixierten Dodekaeders mit $1, \ldots, 12$ und die Farben mit $0, 1$ nummerieren, kann man eine solche Färbung als Abbildung $\phi : \{1, \ldots, 6\} \to \{0, 1\}$ verstehen, hat als eine 2^{12}-elementige Menge M solcher Färbungen. Zwei Färbungen ψ, ψ sind *äquivalent* unter der Wirkung der Drehgruppe G des Dodekaeders, genau dann, wenn

- es $g \in G$ gibt so, dass $\psi(gi) = \phi(i)$ für alle $i = 1, \ldots, 6$

Das bedeutet: ψ liegt auf der Bahn von ϕ unter der Wirkung von G auf M gegeben durch

$$(g\phi)(i) = \phi(g^{-1}i) \;\; i = 1, \ldots, 6$$

Die Frage ist also nach der Anzahl der Bahnen unter einer Wirkung einer Gruppe G auf einer Menge M. Dazu sei die *Fixpunktmenge* von $g \in G$ definiert als

$$\mathsf{Fix}(g) = \{x \in M \mid gx = x\}$$

Satz 4.30 Burnside-Lemma. *Die Anzahl der Bahnen der Wirkung einer Gruppe G auf einer Menge M ist die "mittlere Anzahl der Fixpunkte"*

$$\frac{1}{|G|} \sum_{g \in G} |\mathsf{Fix}(g)|$$

Nun ist eine Färbung ϕ in $\mathsf{Fix}(g)$ genau dann, wenn die Bahnen auf der Menge der Flächen unter der Wirkung von $\mathsf{Spann}(\{g\}$ einfarbig sind. Jede Bahn kann unabhängig von den anderen gefärbt werden. Also $|\mathsf{Fix}|(g) = 2^{m_g}$ wobei m_g die Anzahl dieser Bahnen. Diese Anzahlen stimmen auf den Konjuiertenklassen überein. Für das Dodekaeder ergibt das

$$\frac{1}{|G|} \sum_{g \in G} |\mathsf{Fix}(g)| = \frac{1}{60}(1 \cdot 2^{12} + 20 \cdot 2^4 + 12 \cdot 2^4 + 12 \cdot 2^4 + 15 \cdot 2^6) = \frac{2^4}{60}(44 + 60 + 256) = 960$$

Beweis:

$$g \in G_x \;\Leftrightarrow\; gx = x \;\Leftrightarrow\; x \in \mathsf{Fix}(g)$$

$$\sum_{x \in M} |G_x| = |\{(g, x) \mid gx = x\}| = \sum_{g \in G} |\mathsf{Fix}(g)|$$

Das nennt man auch das *Prinzip der doppelten Abzählung*. Hat man nur eine Bahn, also $G(x_1) = M$ für ein x_1, so $G_x \cong G_{x_1}$ für alle $x \in M$ (Lemma ??) und mit der Bahnformel folgt die Behauptung

$$\sum_{x \in M} |G_x| = |G_{x_1}| \cdot |M| = |G|$$

Im allgemeinen Fall sei $M = X_1 \uplus \ldots \uplus X_m$ die Zerlegung in Bahnen. Nun wirkt G auch auf X_i mit den Fixpunktmengen $X_i \cap \mathsf{Fix}(g)$ und nach dem schon Gezeigten gilt

$$\sum_{g \in G} |X_i \cap \mathsf{Fix}(g)| = |G|$$

Offenbar

$$\mathsf{Fix}(g) = X_1 \cap \mathsf{Fix}(g) \uplus \ldots \uplus X_m \cap \mathsf{Fix}(g)$$

und es folgt

$$\sum_{g \in G} |\mathsf{Fix}(g)| = \sum_{i=1}^{m} \sum_{g \in G} |X_i \cap \mathsf{Fix}(g)| = m \cdot |G|$$

□

4.16 Rechte Wirkung

Was wir bisher beschrieben haben ist *Linkswirkung* - im Einklang mit der vorherrschenden Schreibweise für Abbildungen. Eine *Rechtswirkung* von G auf M wird gegeben durch

$$(x, g) \mapsto x^g \ (x \in M,\ g \in G) \text{ mit } x^e = x,\ x^{gh} = (x^g)^h$$

und von richtigen Gruppentheoretikern bevorzugt - die sind dann meistens Engländer und schreiben eh' von links nach rechts. Eine Rechtswirkung kann man als Linkwirkung der *entgegengesetzten* Gruppe G^{op} auffassen mit $a \cdot^{op} b = ba$ - und diese ist via $g \mapsto g^{-1}$ zu G isomorph. Insofern darf man hier Lechts und Rinks (mit der gebotenen Vorsicht) velwechsern. Insbesondere erhält man dieselben Bahnen.
Beispiele:

- $\mathsf{GL}(n, K)$ wirkt auf $K^{m\times n}$ durch $(A, S) \mapsto AS$
- $\mathsf{GL}(n, K)$ wirkt auf $K^{n\times n}$ durch $(A, S) \mapsto S^{-1}AS$
- $\mathsf{GL}(n, K)$ wirkt auf $K^{n\times n}$ durch $(A, S) \mapsto S^*AS$ - zu gegebener Involution auf K
- Die Gruppe der $n \times n$-Permutationsmatrizen wirkt auf $K^{m\times n}$ durch Spaltenvertauschung.
- Man kann eine Permutation auf $M = \{1, \ldots, n\}$ auch als Umsortierung einer Reihe aus n verschiedenen Zeichen verstehen: z.B. $abc \rightsquigarrow cab$ steht für den Zyklus (123) - der Inhalt von Platz 1 geht nach Platz 2 usw. Nur sollte man dann als Zeichen besser keine Zahlen benutzen. Das ist eine Rechtswirkung von S_n

4.17 Wirkungen der allgemeinen linearen Gruppen

Aus der LA wissen wir

Satz 4.31 *Für Matrizen $A, B \in K^{m\times n}$ sind äquivalent*

- *A, B haben gleiche Bahn unter der Wiirkung $(U, A) \mapsto UA$ von $\mathsf{GL}(m, K)$*
- *A und B beschreiben dieselbe lineare Abbildung nach Koordinatentransformation im Bildraum*
$$B = {}^{\delta}\phi^{\alpha} = {}_{\delta}T_{\beta}\,{}^{\beta}\phi^{\alpha} = UA$$
zu einer/jeder Basis α bzw. β eines n- bzw. m-dimensionalen K-Vektorraums V bzw. W gibt es eine Basis δ von W so, dass $B = {}^{\delta}\phi^{\alpha}$ die Matrix von ϕ bzgl. α und δ ist, wobei ϕ die durch $A = {}^{\beta}\phi^{\alpha}$ bzgl. α und β definierte lineare Abbildung ist
- *die Spalten von A bzw. B bezeichnen nach Koordinatentransformation dasselbe System von Vektoren*
$$A = (x_1^{\alpha}, \ldots, x_n^{\alpha}),\quad B = (x_1^{\beta}, \ldots, x_n^{\beta})$$
zu einer/jeder Basis α eines m-dimensionalen K-Vektorraums V gibt es eine Basis β von V so, dass die Spalten von A, als Koordinatenspalten bzgl. α betrachet, dieselbe Liste von Vektoren ergeben wie die Spalten von B als Koordinatenspalten bzgl. β

- *Die Zeilen von A erzeugen denselben Untervektorraum von K^{n*} wie die Zeilen von B.*
- *Die Gleichungssysteme $A\boldsymbol{x} = \mathbf{0}$ und $B\boldsymbol{x} = \mathbf{0}$ haben denselben Lösungsraum*

*Ein Repräsentantensystem ist gegeben durch die ausgeräumte obere Stufenform (*Hermite Normalform*)*

Satz 4.32 *Für Matrizen $A, B \in K^{m\times n}$ sind äquivalent*

- *A, B haben gleiche Bahn unter der Rechtswirkung $(A, S) \mapsto AS$ von $\mathsf{GL}(n, K)$*
- *A und B bezeichnen nach Koordinatentransformation im Urbildraum dieselbe lineare Abbildung*

  $$B = {}^{\beta}\phi^{\gamma} = {}^{\beta}\phi^{\alpha}\,{}_{\alpha}T_{\gamma} = AS$$

  zu einer/jeder Basis α bzw. β eines n- bzw. m-dimensionalen K-Vektorraums V bzw. W gibt es eine Basis γ von V so, dass $B = {}^{\beta}\phi^{\gamma}$ die Matrix von ϕ bzgl. γ und β ist, wobei ϕ die durch $A = {}^{\beta}\phi^{\alpha}$ bzgl. α und β definierte lineare Abbildung ist
- *die Spalten von A und B beschreiben denselben erzeugten Untervektorraum*

  $$A = (x_1^{\alpha}, \ldots, x_n^{\alpha}),\quad B = (y_1^{\alpha}, \ldots, y_n^{\alpha}) \;\Rightarrow\; \sum_{j=1}^{n} Kx_j = \sum_{j=1}^{n} Kx_j$$

  zu einer/jeder Basis α eines m-dimensionalen K-Vektorraums V erzeugen die Vektoren mit Koordinatenspalten in A denselben Untervektorraum wie die mit Koordinatenspalten in B
- *Die Spalten von A erzeugen denselben Untervektorraum von K^m wie die Spalten von B*

Ein Repräsentantensystem ist gegeben durch die ausgeräumte untere Stufenform

Satz 4.33 *Für Matrizen $A, B \in K^{n\times n}$ sind äquivalent*

- *A, B haben gleiche Bahn unter der Rechtswirkung $(A, S) \mapsto S^{-1}AS$ von $\mathsf{GL}(n, K)$*
- *A und B sind Matrizen desselben Endomorphimus*

  $$B = \phi^{\beta} = {}_{\beta}T_{\alpha}\,\phi^{\alpha}\,{}_{\alpha}T_{\beta} = S^{-1}AS$$

  zu einer/jeder Basis α eines n-dimensionalen K-Vektorraums gibt es eine Basis β, so dass $B = \phi^{\beta}$ die Matrix von ϕ bzgl. β ist, wobei ϕ die durch A bzgl. α definierte lineare Abbildung ist

Für algebraisch abgeschlossene Körper (z.B. $\mathbb{C}$) ist ein Repräsentantensystem gegeben durch die Jordansche Normalform (wenn man eine bestimmte Reihenfolge der EW einhält). Für $\mathbb{R}$ durch die reelle Jordansche Normalform.

Satz 4.34 *Für hermitesche Matrizen $A, B \in \mathbb{C}^{n\times n}$ sind äquivalent*

- *A, B haben die gleiche Bahn bei der Rechts-Wirkung $(S, A) \mapsto S^*AS$ der Gruppe $\mathsf{GL}(n, \mathbb{C})$*

- *A und B sind Grammatrizen derselben Form*

$$B = \Phi^\beta = {}_\beta T_\alpha^t \, \Phi^\alpha \, {}_\alpha T_\beta = S^* A S$$

zu einer/jeder Basis α eines n-dimensionalen $\mathbb{C}$-Vektorraums gibt es eine Basis β, so dass $B = \Phi^\beta$ die Matrix von Φ bzgl. β ist, wobei Φ die durch A bzgl. α definierte Sesquilinearform ist

- *A und B haben die gleiche Anzahl positiver EW und ebenfalls die gleiche Anzahl negativer EW (und damit denselben Rang)*

Ein Repräsentantensystem ist gegeben durch die $\begin{pmatrix} E_p & O & O \\ O & -E_q & O \\ O & O & O \end{pmatrix}$

Entsprechend für $\mathbb{R}$ (Sylvester).

4.18 Wirkungen der unitären und orthogonalen Gruppen

Die unitären Matrizen in $\mathbb{C}^{n\times n}$ bilden die *unitäre* Gruppe $\mathsf{U}(n)$. Aus LA wissen wir

Satz 4.35 *Für normale Matrizen $A, B \in \mathbb{C}^{n\times n}$ sind äquivalent*

- *A, B haben die gleiche Bahn bei der Rechts-Wirkung $(S, A) \mapsto S^* A S$ der Gruppe $\mathsf{U}(n)$*
- *A und B sind Grammatrizen derselben Sequilinearform bzgl. ON-Basen:*

$$B = \Phi^\beta = {}_\beta T_\alpha^* \, \Phi^\alpha \, {}_\alpha T_\beta = S^t A S \quad \alpha, \beta \text{ ON}, S \in \mathsf{U}(n)$$

zu einer/jeder ON-Basis α eines n-dimensionalen unitären Vektorraums gibt es eine ON-Basis β, so dass $B = \Phi^\beta$ die Matrix von Φ bzgl. β ist, wobei Φ die durch A bzgl. α definierte Sesquilinearform ist

- *A und B beschreiben denselben Endomorphismus bzgl. ON-Basen*

$$B = \phi^\beta = {}_\beta T_\alpha \, \phi^\alpha \, {}_\alpha T_\beta = S^{-1} A S \quad \alpha, \beta \text{ ON}, S \in \mathsf{U}(n)$$

zu einer/jeder ON-Basis α eines n-dimensionalen unitären Vektorraums gibt es eine ON-Basis β, so dass $B = \phi^\beta$ die Matrix von ϕ bzgl. β ist, wobei ϕ die durch A bzgl. α definierte lineare Abbildung ist

- *A und B haben dasselbe System von komplexen Eigenwerten (*Spektrum*)*

Ein Repräsentantensytem bilden die Diagonalmatrizen (wenn man eine bestimmte Reihenfolge der EW einhält).

Korollar 4.36 *Für normale Matrizen $A, B \in \mathbb{R}^{n\times n}$ sind äquivalent*

- *A, B haben die gleiche Bahn bei der Rechts-Wirkung $(S, A) \mapsto S^t A S$ der Gruppe $\mathsf{O}(n)$*
- *A und B sind Grammatrizen derselben Bilinearform bzgl. ON-Basen*

$$B = \Phi^\beta = {}_\beta T_\alpha^t \, \Phi^\alpha \, {}_\alpha T_\beta = S^t A S \quad \alpha, \beta \text{ ON}, S \in \mathsf{O}(n)$$

zu einer/jeder ON-Basis α eines n-dimensionalen euklidischen Vektorraums gibt es eine ON-Basis β, so dass $B = \Phi^\beta$ die Matrix von Φ bzgl. β ist, wobei Φ die durch A bzgl. α definierte Bilinearform ist

- *A und B beschreiben denselben Endomorphismus bzgl. ON-Basen*

$$B = \phi^\beta = {}_\beta T_\alpha \, \phi^\alpha \, {}_\alpha T_\beta = S^{-1} A S \quad \alpha, \beta \text{ ON}, S \in \mathsf{O}(n)$$

zu einer/jeder ON-Basis α eines n-dimensionalen euklidischen Vektorraums gibt es eine ON-Basis β, so dass $B = \phi^\beta$ die Matrix von ϕ bzgl. β ist, wobei ϕ die durch A bzgl. α definierte lineare Abbildung ist

- *A und B haben dasselbe System von komplexen Eigenwerten (Spektrum)*

Ein Repräsentantensystem ist gegeben durch die reellen Normalformen (wenn man eine bestimmte Reihenfolge der EW einhält).

4.19 Beidseitige Wirkung

In vielen Beispielen haben wir eine eine (Links)Wirkung einer Gruppe G_l und gleichzeitig eine Rechtswirkung einer Gruppe G_r auf derselben Menge M so, dass

$$g(x)^h = g(x^h) \quad \text{für alle } g \in G_r,\ h \in G_l$$

Die Links- und Rechtswirkung kann man via $g = e$ bzw. $h = e$ aus folgender Abbildung, der *beidseitigen Wirkung*, zurückerhalten

$$G_l \times M \times G_r \to M \quad \text{mit } (g, x, h) \mapsto g(x)^h = g(x^h)$$

Beispiel. Eine beidseitige Wirkung von $\mathsf{GL}(m, K)$ und $\mathsf{GL}(n, K)$ auf $K^{m \times n}$ ist gegeben durch

$$(U, A, S) \mapsto UAS \quad U \in \mathsf{GL}(m, K),\ A \in K^{m \times n},\ S \in \mathsf{GL}(n, K)$$

Eine beidseitige Wirkung ist offenbar dasselbe wie eine Wirkung der Gruppe $G_l \times G_r^{op}$ vermöge

$$(g, h)(x) = g(x^h)$$

Aus LA wissen wir

Satz 4.37 *Für Matrizen $A, B \in K^{m \times n}$ sind äquivalent*

- *A, B haben gleiche Bahn unter der beidseitigen Wirkung $(U, A, S) \mapsto UAS$ von $\mathsf{GL}(m, K)$ und $\mathsf{GL}(n, K)$*

- *A und B beschreiben nach Koordinatentransformationen im Bild- und Urbildraum dieselbe lineare Abbildung*

$$B = {}^\delta \phi^\gamma = {}_\delta T_\beta \, {}^\beta \phi^\alpha \, {}_\alpha T_\gamma = UAS$$

zu einer/jeder Basis α bzw. β eines n- bzw. m-dimensionalen K-Vektorraums V bzw. W gibt es Basen γ von V und δ von W so, dass $B = {}^\delta \phi^\gamma$ die Matrix von ϕ bzgl. γ und δ ist, wobei ϕ die durch $A = {}^\beta \phi^\alpha$ bzgl. α und β definierte lineare Abbildung ist

- *A und B beschreiben nach Koordinatentransformation denselben erzeugten Untervektorraum*

$$A = (x_1^\alpha, \ldots, x_n^\alpha), \quad B = (y_1^\beta, \ldots, y_n^\beta) \;\Rightarrow\; \sum_{j=1}^{n} Kx_j = \sum_{j=1}^{n} Kx_y$$

  zu einer/jeder Basis α eines m-dimensionalen K-Vektorraums V gibt es Basis β von V so, dass die Vektoren mit den Spalten von A als Koordinatenspalten bzgl. α denselben Untervektorraum von V erzeugen wie die, welche die Spalten von B als Koordinatenspalten bzgl. β haben

- *$Rang(A) = Rang(B)$*

Ein Repräsentantensystem ist gegeben durch die $\begin{pmatrix} E_r & O \\ O & O \end{pmatrix}$

Satz 4.38 *Für Matrizen $A, B \in C^{m\times n}$ sind äquivalent*

- *A, B haben gleiche Bahn unter der beidseitigen Wirkung $(U, A, S) \mapsto UAS$ der unitären Gruppen $\mathsf{U}(m)$ und $\mathsf{U}(n)$*

- *zu einer/jeder ON-Basis α bzw. β eines n- bzw. m-dimensionalen unitären Vektorraums V bzw. W gibt es ON-Basen γ von V und δ von W so, dass $B = {}^\delta\phi^\gamma$ die Matrix von ϕ bzgl. γ und δ ist, wobei ϕ die durch $A = {}^\beta\phi^\alpha$ bzgl. α und β definierte lineare Abbildung ist*

- *zu einer/jeder ON-Basis α bzw. β eines n- bzw. m-dimensionalen unitären Vektorraums V bzw. W gibt es ON-Basen γ von V und δ von W so, dass $B = {}^\delta\Phi^\gamma$ die Matrix von Φ bzgl. γ und δ ist, wobei Φ die durch $A = {}^\beta\Phi^\alpha$ bzgl. α und β definierte Sesquilinearform ist*

- *A und B haben dieselben Singulärwerte*

Ein Repräsentantensystem ist gegeben durch die reellen Diagonalmatrizen mit Diagonaleinträgen $\sigma_1 \geq \sigma_2 \ldots \geq \sigma_k \geq 0$, $k = \min\{m, n\}$. Alles analog für $\mathbb{R}$.

5 Faktorisierung.

5.1 Motivation

Die Umgangssprache bezeichnet häufig Dinge als gleich, wenn sie in gewissen, jeweils relevanten, Merkmalen übereinstimmen. Damit allein kann man aber keine ernsthafte mathematische Begriffsbildung treiben, sondern man muss, in gegebenem Zusammenhang, 'Gleichheit' als eine Relation definieren, etwa auf der Grundlage gegebener Relationen und Operationen. Der Zusammenhang ist dabei wesentlich: Etwa beim Rechnen mit rationalen Zahlen ist 1 gleich $\frac{2}{2}$, jedoch wird man 1 Teller und $\frac{2}{2}$ Teller nicht unbedingt als gleich ansehen.

Nach Leibniz bedeutet Gleichheit zweier Objekte in einem gegebenen Zusammenhang, dass man das eine durch das andere ersetzen kann, ohne dass sich an den relevanten Aussagen und Beziehungen etwas ändert. Die Axiome der Äquivalenzrelationen ergeben sich zwingend daraus: Schreibt man $s \sim t$, falls s gleich t ist, und geht man davon aus, dass jedes Ding sich selbst gleich sei ($s \sim s$), so kann man aus $s \sim t$ auf $t \sim s$ schliessen (ersetze in $t \sim t$ das zweite t durch s) und man kann von $s \sim t$ und $t \sim u$ auf $s \sim u$ schliessen, indem man in $t \sim u$ das t durch s ersetzt.

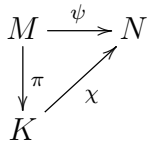
Diese Axiome reichen aus, solange man keine Struktur berücksichtigt. Die Verwendung des Gleichheitszeichens '=' signalisert, dass in dem gegebenen Zusammenhang klar ist, was mit Gleichheit gemeint ist. Kommt Struktur hinzu. so braucht man Verträglichkeit, d.h. Kongruenzrlationen. Mit dieser Verallgemeinerten Gleichheit kann man ganz locker umgehen, wenn man noch nicht durch zu viel Mathematik verunsichert worden ist. Wir wollen jetzt sehen, dass sich der lockere Umgang mathematisch präzisieren und rechtfertigen lässt.

5.2 Ergänzung

Satz 5.1 *Seien M, N, K algebraische Strukturen dessselben Typs. Sei π ein surjektiver Homomorphismus von M auf K und ψ ein Homomorphimsus von M in N. Genau dann gibt es einen Homomorphismsus χ von K in N mit*

$$\psi = \chi \circ \pi \qquad \text{wenn } (*)\ \ x \sim_\pi y \ \Rightarrow\ x \sim_\psi y \ \text{ für alle } x, y \in M$$

Der Homomorphismus χ ist dabei eindeutig bestimmt $\chi(y) = \psi(x)$ falls $y = \pi(x)$.



χ *injektiv* $\Leftrightarrow (**)\ \ x \sim_\pi y \ \Leftrightarrow\ x \sim_\psi y$ *für alle* $x, y \in M$

$\chi : K \to N$ *surjektiv* $\Leftrightarrow \psi : M \to N$ *surjektiv*

Beweis. Zunächst betrchten wir nur den Spezialfall der Mengen (ohne Operationen). Sei χ gegeben und $a \sim_\pi b$. Dann $\pi(a) = \pi(b)$, also $\psi(a) = \chi(\pi(a)) = \chi(\pi(b)) = \psi(b)$ und somit $a \sim_\psi b$. Sei umgekehrt (*) erfüllt. Setze

$$\chi = \{(y, z) |\, y \in K,\ z \in N \text{ und } \exists x \in M : \pi(x) = y \text{ und } \psi(x) = z\}.$$

χ ist in der Tat eine Abbildung: Ist $y \in K$ gegeben, so gibt es wegen der Surjektivität von π ein $x \in M$ mit $\pi(x) = y$ und man hat $(y, z) \in \chi$ für $z = \psi(x)$. Hat man $(y, z) \in \chi$ und $(y, z') \in \chi$, so gibt es nach Definition $x, x' \in M$ mit $\pi(x) = y$, $\psi(x) = z$, $\pi(x') = y$, $\pi(x') = z'$. Es folgt $\pi(x) = \pi(x')$ (da '=' eine Äquivalenzrelation ist), also $x \sim_\pi x'$ und nach

Voraussetzung (*) $x \sim_\psi x'$. Das besagt aber $z = \psi(x) = \psi(x') = z'$.
Beweis des Zusatzes. Sei χ injektiv und $a \sim_\psi b$, d.h $\chi(\pi(a)) = \psi(a) = \psi(b) = \chi(\pi(b)$. Mit der Injektivität folgt $\pi(a) = \pi(b)$, also $a \sim_\pi b$. Gelte umgekehrt (**) und sei $\chi(c) = \chi(d)$. Nach Definition von χ gibt es $a, b \in M$ mit $c = \pi(a)$, $d = \pi(b)$ und $\psi(a) = \chi(c) = \chi(d) = \psi(d)$. Das bedeutet $a \sim_\psi b$, also nach (**) $a \sim_\pi b$ und damit $c = \pi(a) = \pi(b) = d$.

Kommt algebraische Struktur hinzu, ist nur festzustellen, dass eine Abbildung $\chi : K \to N$ mit $\psi = \chi \circ \pi$ automatisch ein Homomorphimsus ist:

$$\text{Mit } b_i = \pi a_i \text{ hat man } \chi b_i = \psi a_i$$

$$\chi f^K(b_1, \ldots, b_n) = \chi f^K(\pi a_1, \ldots, \pi a_n) = \chi \pi f^M(a_1, \ldots, a_n)$$
$$= \psi f^M(a_1, \ldots, a_n) = f^N(\psi a_1, \ldots, \psi a_n) = f^N(\chi b_1, \ldots, \chi b_n) \quad \square$$

5.3 Abstraktion

Proposition 5.2 *Zu jeder Äquivalenzrelation $\sim$ auf einer Menge M gibt es eine Menge K und eine surjektive Abbildung π von M auf K so, dass*

$$x \sim y \Leftrightarrow \pi(x) = \pi(y) \quad \textit{für alle } x, y \in M.$$

Wir sagen dann, dass K eine *Faktormenge* (auch Quotientenmenge) von M nach (oder modulo) $\sim$ ist mit *kanonischer Projektion* π. Kurz: $\pi : M \to K$ ist *Abstraktion* nach $\sim$. Durch einen solchen Übergang kommen wir z.B. von den (konkreten) Brüchen/Cauchyfolgen zu den (abstrakten) rationalen/reellen Zahlen, von den Pfeilen im Anschauungsraum zu den Vektoren.
Beweis. Am besten versteht man das als eine mengentheoretisches Prinyip, das keines Beweises bedarf. Wer sich einen abstrusen, aber sehr beliebten Beweis basteln will, gehe so vor: Wir definieren eine Abbildung π von M in die Menge aller Teilmengen von M durch $\pi(x) = \tilde{x}$. Wenn wir die Surjektivität erzwingen wollen, brauchen wir nur noch zu definieren

$$K = \{\pi(x) |\, x \in M\} = \{\tilde{x} |\, x \in M\} =: M/\sim .$$

Das so definierte $M/\sim$ ist "die" Faktormenge von M nach (modulo) $\sim$. Ihre Elemente sind die Klassen modulo $\sim$. $\square$ Man kann sich K auch auf andere Weise verschaffen, etwa durch Repräsentanten. Ist M gar keine Menge (wie in Beisp. 7), so verbietet es sich von selbst, von 'der Menge der Äquivalenzklassen' zu reden. Ist z.B. M das System aller endlichen Mengen und $X \sim Y$ genau denn, wenn es eine bijektive Abbildung von X auf Y gibt, so kommt man bei solchem Vorgehen schwupp zur Russellschen Antinomie, weil eben nicht einmal die Gesamtheit der einelementigen Mengen eine Menge ist, weshalb Herr Frege sein großes Werk zur Begründung der Mathematik einstampfen lassen musste. Trotzdem kann man durch Abstraktion den Begriff 'Isomorphietyp' bilden und, etwa im Falle der endlichen abelschen Gruppen, die Menge der Isomorphietypen explizit bestimmen. Wir empfehlen daher folgenden Umgang mit 'der Faktormenge' $M/\sim$

- Man arbeite bevorzugt in M mit der 'erweiterten Gleichheitsbeziehung' $\sim$
- Man bezeichne die Elemente von $M/\sim$, wenns denn sein muss, mit $\tilde{a} = \pi(a) = [a]$ und rechne mit

$$\tilde{a} = \pi(a) \;=\; \tilde{b} = \pi(b) \qquad \Leftrightarrow a \sim b$$

5.4 Faktorstruktur

Satz 5.3 *Eine Äquivalenzrelation $\sim$ auf einer algebraischen Struktur A ist genau dann Kongruenzrelation, wenn man für eine/jede Abstraktion $\pi : A \to B$ auf B so eine algebraische Struktur einführen kann, dass $\pi : A \to B$ ein Homomorphismus wird. Die Struktur auf B ist dann eindeutig bestimmt.*

Beweis. Die Wohldefiniertheit des repräsentantenweisen Rechnens in B ist gerade die Verträglichkeit von $\sim$. Wenn π Homomorphismus werden soll, gibt es für die Struktur B keine andere Wahl. □

Wir sagen dann auch $\pi : A \to B$ sei eine *Faktorisierung* `[factorization]` der Struktur A und B *Faktor-* oder *Quotienten-Struktur* mit *kanonischer Projektion* π. Es gilt

$$x \sim y \Leftrightarrow \pi(x) = \pi(y)$$

Nach dem Ergänzungssatz sind B und π bis auf Isomorphie eindeutig bestimmt. Das heisst: Hat man $\pi' : M \to K'$ surjektiv mit $x \sim y \Leftrightarrow \pi'(x) = \pi'(y)$, so gibt es einen eindeutig bestimmten Isomorphismus $\omega : K \to K'$ mit $\pi' = \omega \circ \pi$. Nämlich man definiert wohl $\omega(\pi(x)) := \pi'(x)$.

Kongruenzrelationen sind insofern legitime Gleichheitbegriffe, als wir in B wie in A rechnen, nur eben noch gleicher. Die Homomorphiebedingung besagt

$$f^B(\pi a_1, \ldots, \pi a_n) = \pi f^A(a_1, \ldots a_n)$$

d.h. wenn man a_i als Representant von πa_i bezeichnet, so gilt

In der Faktorstruktur rechnet man repräsentantenweise und unabhängig von der Wahl der Repräsentanten

Schreibt man $\widetilde{a} = \pi a$ so liest's sich etwa für Gruppen so

$$\widetilde{a} \cdot \widetilde{b} = \widetilde{a \cdot b}, \;\; \widetilde{a}^{-1} = \widetilde{a^{-1}}$$

Ist $\phi : M \to N$ ein Homomorphimus, so ist $\phi : M \to \mathsf{Bild}(\phi)$ trivialerweise eine Faktorstruktur von M nach der Kongruenzrelation $x \sim y \Leftrightarrow \phi(x) = \phi(y)$, dem Kern $\mathsf{Kern}(\phi)$ von ϕ.

Eine algebraische Struktur A kann man nach einer Kongruenzrelation $\sim$ faktorisieren

Das folgt daraus, dass man die Grundmenge nach der Äquivalenzrelation faktorisieren kann. Wie man das macht, ist Privatsache und man darf die Aussage dazu verweigern. Wegen der Eindeutigkeit bis auf Isomorphie können wir von "der" *Faktorstruktur* sprechen und sie mit $A/\sim$ bezeichnen.

Sei U der der Konzgruenz $\sim$ des Modulas M entsprechende Untermodul. Man kann dann $M/\sim = M/U$ auch aus dieser Sicht verstehen. Das Rechnen mit Kongrueznzklassen geht dann so

$$(U + a) + (U + b) = U + (a + b), \;\; -(U + a) = U + (-a) = U - a, \;\; U + 0 = U$$

Entsrechend für ein Ideal I in einem Ring hat man R/I und

$$a+I+b+I=a+b+I,\ -(a+I)=-a+I,\ 0+I=I,\ (a+I)\cdot(b+I_{=}ab+I$$

wobei $a+I=I+a=\{a+x \mid x\in I\}$. Die Faktorstruktur $A/\sim$ schrieben wir dann auch als A/I bzw. A/U.

Ist N ein Normalteiler der Gruppe G so gilt $gN=Ng=\pi(g)$ (da $\pi(h)=\phi(g)\Leftrightarrow\pi(g^{-1}h)=e\Leftrightarrow g^{-1}h\in N\Leftrightarrow h\in gN$), d.h. linke und rechte Nebenklassen stimmen überein. Die Faktorgruppe wird dann auch als G/N notiert und man kann so rechnen

$$gNhN=ghN,\ (gN)^{-1}=g^{-1}N,\ eN=N$$

Man kann G/N auch direkt so einführen, ohne über Kongruenzen nachzudenken. Dann verpasst man zwar das allgemeine Prinzip, hat aber einen Kalkül, der insbesondere bei endlichen Gruppen durchaus von Nutzen ist. Bei Moduln gehts analog, bei Ringen gibts aber ein Problem mit dem Produkt von Nebenklassen.

Nach 1.11 bleiben in der Faktorstruktur alle Gesetze erhalten, die nur mit $\wedge,\vee,\forall,\exists$ formuliert sind.

Faktorstrukturen von (kommutativen) Monoiden, Gruppen, Ringen, R-Moduln, R-Algebren sind wieder welche

Den Faktorring nach em Ideal $(p)=\{rp \mid r\in R\}$ und die kanonische Projektion wollen wir so notieren

$$R/(p)=R/Rp,\quad a\mapsto a[\mathsf{mod}p]$$

Im Falle $R=\mathbb{Z}$ ist auch $\mathbb{Z}_p$ populär aber missverständlich. Mit $p=12$ sehen wir, dass das Stundenzählen funktioniert.

Bemerkung 5.4 *In einem Körper K gilt: Ist $0\neq n\in\mathbb{N}$ minimal mit $n1_K=0_K$, so ist n eine Primzahl.*

So ein n brauchts nicht zu geben, z.B. wenn K Unterkörper von $\mathbb{C}$. Sei nun $n=qm$ mit $q,m<n$ und $n1=0$. Dann $(q1)(m1)=n1=0$ also $q1=0$ oder $m1=0$ was der Minimalität widerspricht.

Beispiel 5.5 *$\mathbb{Z}/n\mathbb{Z}$ ist ein Körper genau dann, wenn n eine Primzahl ist.*

Beweis. Für $0<m<n$ ist n kein Teiler von m, also $m\not\sim_n 0$. Ist also $\mathbb{Z}/n\mathbb{Z}$ Körper, so n prim nach der vorangehenden Bemerkung. Sei umgekehrt $n=p$ prim und $\pi(a)\neq\pi(0)$, d.h. p und a teilerfremd. Nach Bezout gibt es ganze Zahlen x,y mit $ax+py=1$, also $ax\sim_n 1$ und $\pi(a)\pi(x)=\pi(ax)=\pi(1)$. Somit ist $\mathbb{Z}/p\mathbb{Z}$ Körper.

Lemma 5.6 *Ist M ein R-Modul, so erhält man eine Kongruenzrelation des Ringes R*

$$r\sim s\quad\Leftrightarrow\quad\forall x\in M.\ rx=sx$$

und M wird auf natürliche Weise zum $R/\sim$-Modul mit $\widetilde{r}a=ra$,

Beweis als Übung. □

6 Erzeugen von Kongruenzrelationen

6.1 Motivation

Faktorisieren unter Berücksichtigung einer Struktur ist eine grundlegende Kulturtechnik. Sie besteht darin, die aus gegebenen Gleichsetzungen folgenden Gleichsetzungen auszuführen, nach der so erhaltenen Äquivalenzrelation zu abstrahieren und das Abstraktum wieder als Struktur zu verstehen.

Beispiel 1. Wir wollen Stunden zählen. Dazu könnten wir alle Stunden seit dem Urknall durchnummerieren und dann weiterzählen. Besser bewährt hat sich jedoch die Methode nach 12 bzw. 24 Stunden wieder von vorn anzufangen, d.h. wir erzwingen

$$12 \stackrel{!}{=} 0$$

Dann müssen wir auch die Konsequenzen akzeptieren, nämlich dass $13 = 1$ usw. Und wir müssen klären, ob nicht etwa die ganze Zeitrechnung zusammenbricht, weil etwa $1 = 0$ folgte. Die Probleme mit $99 + 01 \stackrel{!}{=} 00$ sind ja bekannt.

Beispiel 2. Wir betrachten Gruppen, die von Elementen d und s erzeugt werden, für die wir nur die folgende Informatuion haben: $d^4 = e = s^2$, $sd = d^{-1}s$. Welchen Gruppen sind möglich? Gibt es unter diesen eine 'allgemeinste', d.h. eine im Prinzip eindeutig bestimmte, in der nur das gilt, was aus den Voraussetzungen logisch folgt.

Beispiel 3. Wir sollen mit numerischen (z.B. physikalischen) Grössen rechnen, für die wir aber keine Zahlenwerte gegeben haben. Die Aufgabe besteht darin, aus gegebenen Beziehungen zwischen diesen Grössen rein logisch weitere herzuleiten oder die Unmöglichkeit einer Herleitung einzusehen. Wir führen dazu für jede dieser Grössen einen Buchstaben ein (genauer: eine neue Konstante, die eine feste aber beliebige Zahl bezeichnet) und rechnen mit diesen Buchstaben nach den Gesetzen der Arithmetik etwa

$$(ab)(cd) \stackrel{!}{=} ((ab)c)d$$

(d.h. wir treiben *Buchstabenrechnung*) und nach weiteren speziellen (physikalischen) Gesetzen oder Definitionen etwa

$$K \stackrel{!}{=} mb$$

Beispiel 4. Wie Beispiel 3 aber es gibt noch Buchstaben (Unbekannte) wie $x, y, \ldots$, bei denen wir uns nicht schon wohlbestimmte Zahlen denken, sondern bei denen wir die möglichen (Kombinationen von) Werte(n) in Abhängigkeit von den vorgegebenen Werten der Konstanten ermitteln wollen z.B. $ax + by = c$.

Beispiel 5. Wir betrachten Polyome $a_0 + a_1x + \ldots a_nx^n$ mir Koeffizienten im Körper K. Dann sind die a_i Konstanten im Sinne von Beispiel 3. Der Buchstabe x kann aber einmal eine Variable bedeuten (insbesondere falls $K \subseteq \mathbb{C}$), d.h. wir benutzen das Polynom, um über die Polyomfunktion $x \mapsto \sum_i a_i x^i \, (x \in k)$ zu reden. Andererseits kann es aber auch sein, dass wir die Polynome nur als 'formale Ausdrücke' sehen wollen (insbesondere wenn K endlich ist) und mit diesen im Sinne der Buchstabenrechnung operieren. Es bleibt aber der Apsekt erhalten, dass wir für x Werte aus K einsetzen wollen und können. In diesem Falle schreibt man oft X anstelle von x und spricht von einer Unbestimmten'.c

Es ist noch ein Wort über das wichtigste Hülfsmittel der Algebra, die Buchstabenrechnung, zu sagen. Die Anwendung dieses Hülfsmittels ist so allgemein, dass man bisweilen das Wort Buchstabenrechnung synonym mit Algebra gebraucht. Die Regeln, wie mit solchen Buchstabenausdrücken gerechnet wird, setzen wir als bekannt voraus. Gleichungen zwischen Buchstabenausdrücken können zweierlei Art sein; entweder es sind sogenannte Identitäten, d.h. die zwei einander gleich gesetzten Ausdrücke können durch Anwendung der Rechenregeln so umgeformt werden, dass beide Ausdrücke genau übereinstimmen. Man erhält dann aus solchen Buchstabengleichungen richtige Zahlengleichungen, wenn die Buchstaben durch irgend welche, sei es reelle, sei es complexe Zahlen ersetzt werden, vorausgesetzt, dass dabei nicht die Forderung der Division durch Null auftritt. Die Buchstaben in solchen Gleichungen werden oft auch als Variable bezeichnet, weil man sich vorstellen kann, ohne je zu einem Widerspruch zu gelangen, dass für die Buchstaben nach und nach andere und andere Zahlenwerthe gesetzt werden.

Eine andere Art von Gleichungen zwischen Buchstabenausdrücken haben nicht diesen Charakter der Identität. Sie enthalten vielmehr eine Forderung, die an solche Zahlen gestellt wird, die man, ohne die Gleichungen unwahr zu machen, für die Buchstaben einsetzen darf. Die Algebra hat die Aufgabe, Zahlenwerthe zu ermitteln, die einer solchen Forderung genügen, die Gleichung zu lösen. In diesen Gleichungen werden die Buchstaben auch als 'Unbekannte' bezeichnet. Es kommen sehr häufig in ein und derselben Gleichung Buchstaben von zwei Arten vor, solche, für die beliebige Zahlenwerthe gesetzt werden sollen, und andere, deren Zahlenwerth erst ermittelt werden soll. H.Weber, Lehrbuch der Algebra I-III, 1894

6.2 Erzeugen von Äquivalenzralationen

Hat man Äquivalenzrelationen $\approx$ und $\sim$ auf M mit

$$x \approx y \;\Rightarrow\; x \sim y \quad \text{für alle } x, y \in M$$

so ist $\approx$ *feiner* als $\sim$ und $\sim$ *gröber* als $\approx$. Gleicbbedeutend: Zu den Faktormengen mit kanonischen Projektionen gibt es Ergänzung $\chi : M/\approx \to M/\sim$

Fasst man Äquivalenzrelationen auf M als Teilmengen von $M \times M$ auf, so handelt es sich gerade um die abgeschlossenen Mengen unter dm folgenden Regelsystem

$$\frac{}{(a,a)} \qquad \frac{(a,b)}{(b,a)} \qquad \frac{(a,b),(b,c)}{(a,c)} \qquad (a,b,c \in M)$$

In diesem Sinne kann man von der von einer Menge $R \subseteq M^2$ von Paaren *erzeugten* Äquivalenzrelation $\sim$ auf M sprechen. Schreibt man $R = \{(v_i, w_i) \mid i \in I\}$, so kann man $\sim$ aber auch die durch die *Vorgaben* (traditionell: *Relationen*) $v_i \stackrel{!}{=} w_i$ $(i \in I)$ *erzwungene* Äquivalenzrelation nennen. Nach dem Abschluss-Prinzip ist das die feinste Äquivalenzrelation $\sim$ mit

$$v_i \stackrel{!}{=} w_i \;\Rightarrow\; v_i \sim w_i \quad \text{für alle } i \in I$$

Man bekommt sie, indem man zu den Ausgangspaaren ihre symmetrischen dazunimmt und dann unter Transitivität abschliesst - die Paare (a,a) kann kann man vorher oder nachher dazunehmen. Also

- $a \sim b \Leftrightarrow\; a = b$ oder es gibt $a_0, \ldots, a_n$ mit $a = a_0, a_n = b$
  und für alle i gilt $a_i \stackrel{!}{=} a_{i+1}$ bzw. $a_{i+1} \stackrel{!}{=} a_i$

6.3 Erzeugen von Kongruenzrelationen

Um Kongruenzrelationen auf einer algebraischen Struktur A analog zu Äquivalenzrelationen als abgeschlossene Mengen bzgl. eines Regelsystems zu verstehen, haben wir auch die Verträglichkeitsbedingungen als Regeln aufzufassen

$$\frac{(a_1,b_1),\ldots,(a_n,b_n)}{(f^A(a_1,\ldots,a_n),f^A(b_1,\ldots,b_n))} \qquad (f\in\Omega,\ a_i,b_i\in A \text{ und} f^A(a_1,\ldots,a_n) \text{ definiert})$$

Insbesondere ist dabei auch $f^A(b_1,\ldots,b_n)$ definiert. Nach dem Abschluss-Prinzip folgt

Prinzip 6.1 *Zu jeder algebraischen Struktur A und Gleichsetzungen $v_i \stackrel{!}{=} w_i$, $(i\in I)$, gibt es eine feinste Kongruenzrelation $\sim$, die diese Gleichsetzungen* implementiert*, d.h. mit $v_i\sim w_i$ für $i\in I$.*

Wir sagen auch, $\sim$ sei die durch die Gleichsetzungen $v_i \stackrel{!}{=} w_i$, $(i\in I)$ *erzwungene* bzw. *erzeugte Kongruenz(relation).* Nach den Ergänzungssatz erhalten wir

Korollar 6.2 *Sei $\sim$ sei die durch die Gleichsetzungen $v_i \stackrel{!}{=} w_i$, $(i\in I)$ erzwungene Kongruenzrelation auf A. Für einen Homomorphismus $\psi: A\to B$ gilt $\psi v_i=\psi w_i$ für alle $i\in I$ genau dann, wenn es einen (eindeutig bestimmten) Homomorphismus $\chi: A/\sim \to B$ mit $\psi=\chi\circ\pi$, wobei $\pi: A\to A/\sim$ die kanonische Projektion ist.*

Wir geben das Regelsystem zu den Vorgaben $v_i \stackrel{!}{=} w_i$ nochmal komplett in intuitiverer Form an

$$\frac{v_i \stackrel{!}{=} w_i}{v_i\sim w_i} \qquad \frac{}{a\sim a} \qquad \frac{a\sim b}{b\sim a} \qquad \frac{a\sim b,\ b\sim c}{a\sim c}$$

$$\frac{a_1\sim b_1,\ldots,a_n\sim b_n}{f^A(a_1,\ldots,a_n)\sim f^A(b_1,\ldots,b_n)} \qquad (f\in\Omega,\ a_i,b_i\in A \text{ und } f^A(a_1,\ldots,a_n) \text{ definiert})$$

Zur Beschreibung des Erzeugungsprozesses aus einer Menge ρ von Paaren kann man sich auch rekursiv eine Folge ρ_k von Relationen definieren und $\overline{\rho}$ als Vereinigung von diesen

- $a\,\rho_0\,a \ \Leftrightarrow\ a\,\rho\,b$ oder $a=b$
- $a\,\rho_{k+1}\,b$ falls einer der folgenden Fälle eintritt
  - $b\,\rho_k\,a$
  - $a\,\rho_k\,c\,\rho_k\,b$ für ein c
  - $a=f(a_1,\ldots,a_n),\ b=f(b_1,\ldots,b_n)$ mit $a_1\,\rho_k\,b_1$ und $\ldots$ und $a_n\,\rho_k\,b_n$
- $a\,\overline{\rho}\,b \ \Leftrightarrow$ es gibt k mit $a\,\rho_k\,b$

Mit Induktion folgt

$$a\,\rho_k\,b \ \Rightarrow\ a\,\rho_l\,b \quad \text{für } k\le l$$

Will man nun z.B. eine Verträglichkeitsbedingung nachprüfen, so betrachtet man $a_i\,\overline{\rho}\,b_i$ d.h. $a_i\,\rho_{k_i}\,b_i$ mit einem k_i für $i=1,\ldots,n$. Setzt man $k=\max\{k_1,\ldots,k_n\}$ so gilt $a_i\,\rho_k\,b_i$ für alle i, also nach Definition $f(a_1,\ldots,a_n)\,\rho_{k+1}\,f(b_1,\ldots,b_n)$ und damit auch $f(a_1,\ldots,a_n)\,\overline{\rho}\,f(b_1,\ldots,b_n)$. Ist andererseits θ eine ρ vergröbernde Kongruenzrelation, so folgt induktiv

$$a\,\rho_k\,b\ \Rightarrow a\theta b, \quad \text{also } a\,\overline{\rho}\,b\ \Rightarrow a\theta b \quad \square$$

Für Gruppen, Ringe, Moduln und Algebren kommt man mit einen speziellen Typ Gleichsetzungen aus

$$w_i \stackrel{!}{=} e \quad \text{bzw. } w_i \stackrel{!}{=} 0$$

Durch Multiplikation von rechts mit b bzw. b^{-1} sieht man nämlich, dass für jede Kongruenzrelation $\sim$ gilt

$$a \cdot b^{-1} \sim e \;\Leftrightarrow\; a \sim b$$

Korollar 6.3 *Sei A Gruppe, Modul, Ring oder Algebra und seien die $a_i, b_i\,(i \in I)$ in A. Sei $\sim$ die feinste Kongruensrelation mit $a_i \sim b_i$ für alle $i \in I$. und N der kleinste Normalteiler mit $a_i b_i^{-1} \in N$ bzw Untermodul/ Ideal mit $a_i - b_i \in N$. Dann entsprechen sich $\sim$ und N, d.h. asimb $\Leftrightarrow ab^{-1} \in N$ und $N = \{a \mid a \sim e$ bzw.$0\}$.*

6.4 Termersetzung

Das Erzeugen einer Kongruenzrelation auf einer algebraischen Struktur A wird wesentlich komfortabler durch Hinzunahme der folgenden Regel

$$\frac{a_1 \sim b_1, \ldots, a_m \sim b_m}{t^A(a_1, \ldots, a_m) \sim t^A(b_1, \ldots, b_m)} \qquad \text{Termersetzung}$$

Die Zulässigkeit dieser Regel folgt sofort über den Aufbau des Terms t: Sie ist klar für $t = x_i$ und für $t = f(t_1, \ldots, t_n)$ haben wir nach Induktionsannahme $t_i^A(a_1, \ldots, a_m) \sim t_i^B(b_1, \ldots, b_m)$ also $t^A(a_1, \ldots, a_m) = f^A(t_1^A(a_1, \ldots, a_m), \ldots, t_n^A(a_1, \ldots, a_m))$
$\sim f^A(t_1^A(b_1, \ldots, b_m), \ldots, t_n^A(b_1, \ldots, b_m)) \sim t^A(b_1, \ldots, b_m)$. □ Man kann die Regel etwas lockerer auch so formulieren

$a \sim b$, falls man a und b so durch Terme beschreiben kann, dass die Beschreibung von b aus der von a entsteht, indem man einige der Vorkommen von a_i durch b_i ersetzt sofern $a_i \sim b_i$

6.5 Durchsetzen von Gesetzen

Eine wohlbekannte Anwendung ist der Umgang mit Gesetzen im Rahmen der Buchstabenrechnung. Die Gesetze haben dabei die Form von *Gleichheits-Gesetzen*

$$\forall x_1 \ldots . \forall x_n.\; s(x_1, \ldots, x_n) \stackrel{!}{=} t(x_1, \ldots, x_n) \quad \text{kurz } \forall \mathbf{x}.\; s(\mathbf{x}) \stackrel{!}{=} t(\mathbf{x}))$$

mit Termen s und t. Ein solches Gesetz ist *erfüllt* bzw. *gilt* in der algebraischen Struktur B genau dann, wenn

- $s^B(b_1, \ldots, b_n) = t^B(b_1, \ldots, b_n)$ für jede Wahl der $b_1, \ldots, b_n$ in B

Wir betrachten nun eine Sammlung solcher Gesetze $\forall \mathbf{x}.\; s_i(\mathbf{x}) \stackrel{!}{=} t_i(\mathbf{x})$, $(i \in I)$ und eine algebraische Struktur A, in der sie noch nicht durchgängig erfüllt sind. Um die Gesetze für A *durchzusetzen*, faktorisieren wir A nach der Kongruenzrelation $\sim$, die von folgenden Gleichsetzungen gemeinsam erzwungen wird

$$s_i^A(a_1, \ldots, a_n) \stackrel{!}{=} t_i^A(a_1, \ldots, a_n) \quad \text{mit } i \in I \text{ und } a_1, \ldots, a_n \in A$$

Wir nennen $\sim$ auch die von den Gesetzen $\forall \mathbf{x}.\; s_i(\mathbf{x}) \stackrel{!}{=} t_i(\mathbf{x})$, $i \in I$ *erzwungene* Kongruenz.

Prinzip 6.4 *Ist $\sim_\Gamma$ die von den Gesetzen Γ erzwungene Kongruenz auf A, so gelten in $A/\sim_\Gamma$ alle Gesetze aus Γ. Jede in A dabei vorzunehmende Gleichsetzung $v \stackrel{!}{=} w$ ergibt sich zwingend (nach den Regeln der Logik) aus den Gesetzen Γ und der Struktur von A.*

Korollar 6.5 *Ist $\psi : A \to B$ ein surjektiver Homomorphimus, so gibt es genau dann einen (eindeutig bestimmten) Homomorphismus $\chi : A/\sim_\Gamma \to B$ mit $\psi = \chi \circ \pi$, wenn die Gesetze Γ in B gelten.*

Beweis: Prinzip 3.12 und Homomorphie-Ergänzungssatz. □

7 Freiheit, Gleichheit und Präsentierung

7.1 Buchstabenrechnung

Seien Operationssymbole bestimmten Typs gegeben und sei Γ eine Sammlung von Gleichheits-Gesetzen. Die *Buchstabenrechnung* über dem Alphabet E nach den Gesetzen Γ ist das Rechnen in der Termstuktur $T(E)$ modulo der von Γ erzwungenen Kongruenzrelation $\sim_\Gamma$. D.h. Webers 'bekannte Regeln' sind einerseits die vorausgesetzten Gleichheits-Gesetze Γ und andererseits die Erzeugungsregeln für die Kongruenzrelation $\sim_\Gamma$ (in ihrer stärksten Form) :

- $t \sim_\Gamma t$
- $t \sim_\Gamma s$ falls $s \sim_\Gamma t$
- $s \sim_\Gamma w$ falls $s \sim_\Gamma t \sim_\Gamma w$
- $t(s_1, \ldots, s_n) \sim_\Gamma t(t_1, \ldots, t_n)$ für Term $t(x_1, \ldots, x_n)$ falls $s_1 \sim_\Gamma t_1, \ldots, s_n \sim_\Gamma t_n$
- $w \sim_\Gamma w'$ falls $\forall x_1, \ldots, \forall x_m.\ s(x_1, \ldots, x_m) = t(x_1, \ldots, x_m)$ ein Gesetz in Γ ist, w einen Teilterm $s(t_1, \ldots, t_m)$ hat und w' aus w entsteht, indem ein oder mehrere Vorkommen dieses Teilterm durch $t(t_1, \ldots, t_m)$ ersetzt werden.

Das Ergebnis ist die freie Struktur $F(E) \cong T(E)/\sim$ in der durch die Gleichungen Γ definierten Klasse von Strukturen.

7.2 Termstrukturen und Auswertung

Prinzip 7.1 *Zu jeder Menge E gibt es eine Struktur $T(E) = (T(E), *, e)$ vom Typ der Monoide, die von E erzeugt wird und so, dass gilt*

- *Für jede Struktur M von Typ der Monoide und Abbildung $\gamma : E \to M$ gibt es einen eindeutig bestimmten* Auswertungs=*Homomorphismus $\overline{\gamma} : T(E) \to M$ mit $\overline{\gamma}|E = \gamma$*

Intern ist $T(E)$ durch die folgenden Peano-*Axiome charakterisiiert*

*(P0) $T(E)$ wird von E erzeugt (*Induktionsprinzip*).*

(P1) $x \neq e$, $x \neq s * t$ für alle $x \in E$ und $s, t \in I(E)$

(P2) $e \neq s * t$, $s * t = s' * t' \Rightarrow s = s'$ und $t = t'$ für alle $s, t, s', t' \in T(E)$

$T(E)$ ist bis auf (auf E identischen) Isomorphimus eindeutig bestimmt.

$T(E)$ kann man sich wie in Kap.2 als eine Menge von Zeichenfolgen denken, wobei die Zeichen die Elemente von E, $\cdot$, e, (und) sind. Dann ist $s * t = (s \cdot t)$. Die Klammern werden wegen der Infixnotation benötigt.

Entsprechendes hat man für andere Typen von algebraischen Stukturen. Z.B. beim Typ der Gruppen $e \neq s \cdot t$hat man eine weitere einstellige Operation $^{-1}$ und in den Peanoaxiomen zusätzlich

$$x \neq t^{-1},\ e \neq t^{-1},\ s * t \neq u^{-1},\ \ s^{-1} = t^{-1} \Rightarrow s = t$$

Ist R ein Ring und betrachtet man Stukturen vom Typ der R-Moduln, so kann man jedes $r \in R$ als Symbol für eine einstellige Operation auffassen und hat, wenn man e durch 0, $*$ durch $+$ und $^{-1}$ durch $-$ ersetzt in den Peanoaxiomen zusätzlich

$$r(t) \neq x,\ r(t) \neq e,\ r(t) \neq s + u,\ r(t) \neq -s,\ r(t) = r(s) \Rightarrow t = s$$

Das Grundbeispiel sind jedoch die natürlichen Zahlen als Termstruktur über $E = \emptyset$ mit einer Konstanten 0 und einer einstelligen *Nachfolger*-Operation s, Die Etnprechenden Axiome in Kap.1.1 stammen von Peano.

7.3 Freies Monoid

Prinzip 7.2 *Für ein Monoid M mit ausgezeichneter Teilmenge E sind äquivalent*

(i) M entsteht aus den Monoidtermen über der (Variablen- bzw. Erzeuger-)Menge E, indem man modulo der Monoidgesetze rechnet, d.h. die Termstruktur $T(E)$ nach der Kongruenzrelation $\sim$ faktorisiert, die sich ergibt, wenn man neben den Kongruenzregeln auch noch die folgenden Regeln hat

$$s(tu) \sim (st)u,\ \ et \sim t,\ te \sim t \text{ fúr alle Terme } s, t, u$$

(ii) Fortsetzungs- oder universelle Eigenschaft*: M wird von E erzeugt und zu jedem Monoid A und jeder Abbildung $\gamma : E \to A$ gibt es einen (eindeutig bestimmten) Homomorphismus $\overline{\gamma} : M \to A$ mit $\overline{\gamma}|E = \gamma$*

Gilt eine der beiden Bedingungen, so heisst M ein von E *frei erzeugtes Monoid*. Die Eindeutigkeit von $\overline{\gamma}$ folgt aus Lemma 3.14, da M von E erzeugt wird.

Korollar 7.3 *Zu jeder Menge E gibt es ein bis auf Isomorphie eindeutig bestimmtes von E frei erzeugtes Monoid.*

Lemma 7.4 *Hat M' die universelle Eigenschaft bzgl. E' und ist $\varepsilon : E \to E'$ eine bijektive Abbildung, so hat auch M bzgl. E die universelle Eigenaschaft genau dann, wenn es einen (eindeutig bestimmten) Isomorphismus $\phi : M \to M'$ gibt mit $\phi|E = \varepsilon$.*

Beweis des Lemmas. Sei $\psi : M' \to M$ der Homomorphismus mit $\psi|E' = \varepsilon^{-1}$. Hat auch M bzgl. E die universelle Eigenachaft, so gibt es $\phi : M \to M'$ mit $\phi|M = \varepsilon$. Dann $(\psi \circ \phi)|E = \mathsf{id}_E$, also $\psi \circ \phi = \mathsf{id}_M$ nach Lemma 3.14. Entsprechend $\phi \circ \psi = \mathsf{id}|M'$. Also ist ϕ Isomorphismus.

Ist ϕ gegeben und $\gamma : E \to A$, so sei $\delta : E' \to A$ definiert als $\gamma \circ \varepsilon^{-1}$. Dann gibt es $\overline{\delta} : M' \to A$ mit $\overline{\delta}|E' = \delta$ und wir haben die universelle Eigenschaft mit $\overline{\gamma} = \overline{\delta} \circ \phi$ nachgewiesen. □

Beweis des Prinzips und Korollars. Erfahrungsgemäß kann man mit Termen modulo in Form von Gleichungen gegebener Gesetze rechnen. Damit folgt die Existenz eines Monoids wie in (i).

Sei nun (i) vorausgesetzt und π die kanonische Projektion auf $M = T(E)/\sim$. Könnte man $x \sim y$ für $x \neq y$ in E herleiten, so hätte man einen Beweis, dass jedes Monoid einelementig ist, wozu es reichlich Gegenbeispiele gibt. Also ist $\pi|E$ injektiv und wir dürfen E als Teilmenge von M auffassen mit $\pi(x) = x$ für $x \in E$. Sei nun ein Monoid A und eine Abbildung $\gamma : E \to A$ gegeben. Die Termauswertung

$$\phi(t(x_1, \ldots, x_n)) = t^A(\gamma(x_1), \ldots, \gamma(x_n))$$

ist ein Homomorphismus $\phi : T(E) \to A$ mit $\phi|E = \gamma$. Weil N ein Monoid ist, werden neben den Kongruenzregeln auch die zusätzlichen Regeln für $\sim$ respektiert und es folgt

$$s \sim t \;\Rightarrow \phi(s) = \phi(t) \quad \text{für alle } s, t \in T(E)$$

Dann gibt es nach dem Ergänzungssatz einen Homomorphismus $\overline{\gamma} : M \to A$ mit $\overline{\gamma} \circ \pi = \phi$, also insbesondere $\overline{\gamma}(x) = \overline{\gamma}(\pi(x)) = \phi(x) = \gamma(x)$ für $x \in E$.

Sei nun (ii) vorausgesetzt. Wir wissen schon, dass wir $M' \supseteq E$ nach (i) konstruieren können und haben gerade bewiesen, dass dann für M' auch (ii) gilt. Nach dem Lemma gibt es zu $\varepsilon = \mathsf{id}_E$ einen Isomorphismus $\omega : M \to M'$ mit $\omega|E = \varepsilon$, d.h. M is ebenfalls eine Faktorstruktur $T(E)/\sim$. □

Die obigen Aussagen beweist man ebenso für jede Klasse algebraischer Strukturen, die durch Gleichungen definiert ist und nicht nur aus einelementigen besteht. In einigen Fällen, wie hier bei den Monoiden, kann man die Struktur der freien Strukturen explizit bestimmen.

Satz 7.5 *Für ein Monoid M mit ausgezeichneter Teilmenge E sind äquivalent*

- *M wird von E frei erzeugt,*
- *Die Elemente von M haben eindeutige Darstellung $a = (\ldots((g_1g_2)g_3)\ldots g_{n-1})g_n$ mit $g_i \in E$; insbesondere $n = 0$ für des neutrale Element e*
- *Es gibt einen Isomorphismus ϕ von M auf das Wortmonoid E^* mit $\phi|E = id_E$*

Beweis. Sei F ein von E frei erzeugtes Monoid, M wie in (2) und $\phi : F \to M$ der Homomorphismus mit $\phi|E = \mathsf{id}|E$ - nach Voraussetzung bezeichnen verschiedene g_i aus E auch verschiedene Elemente von M. ϕ ist surjektiv, weil M von E erzeugt wird. Weil F ein von E erzeugtes Monid ist, kann man jedes Element von F in der Form $a = (\ldots((g_1g_2)g_3)\ldots g_{n-1})g_n$ mit $g_i \in E$ darstellen. Also $\phi(a) = (\ldots((g_1g_2)g_3)\ldots g_{n-1})g_n$ wobei das Produkt in M ausgerechnet wird. Die Eindeutigkeit der Darstellung besagt also, dass ϕ injektiv ist. Also ist ϕ ein Isomorphismus und auch M von E frei erzeugt. Dies beweist $2 \Rightarrow 1$.

E^* ist offensichtlich ein Monoid mit eindeutiger Darstellung, also $3 \Rightarrow 2$. Wegen $2 \Rightarrow 1$ ist alos E^* frei von E erzeugt. Mit dem Lemma folgt $1 \Leftrightarrow 3$. □ Hacker rechnen fuer E^* die Fortsetzungseigenschaft (ii) nach und denken, das wär's.

Eine Methode mit deutliche gößerem Anwendungsbereich ist die *Mathode der Normalformen*, die im nächsten Kapitel präzise erläutert wird. Dei Idee ist es, ein Repräsentantensystem N (Normalformen) für $\sim$, d.h. den Kern der kanonsichen Projektion π von der Termalgebra $T(E)$ auf die freie Struktur $F(E)$ anzugeben. Die Existenz bzw. Eindeutigkeit der Darstellung bedeutet dass es mindestene bzw. höchstens 1 Repräsentanten in N aus jeder Klasse gibt.

Der Nachweis erfolgt, indem man auf N ein von E erzeugtes Monoid $(N, *, e')$ definiert und zwar so, dass

$$s * t \sim s \cdot t.\ \ e' \sim e$$

Dann ist nämlich $\pi|N : N \to F(E)$ surjektiv und ein Homomorphismus. Weil N ein Monoid ist, gibt es einen Homomorphismus $\overline{\gamma} : F(E) \to N$ mit $\overline{\gamma}|E = \mathsf{id}_E$. Dann ist $\phi \circ \overline{\gamma}$ ein Endomorphismus von $F(E)$ der auf E die Identität ist, also die Identität auf $F(E)$. Es folgt, dass $\pi|N$ injektiv ist und damit in der Tat N ein Repräsentatnetsystem für $\sim$.

Im Falle der Monoide ist N z.B, die Menge der linksgeklammerten Terme. Wir schreiben $(g_1, \ldots, g_n)$ als Abürzung für $((\ldots(g_1 \cdot g_2) \cdot \ldots) \cdot g_n)$. Mit Induktion über m folgt aus dem Assoziativgesetz $(g_1, \ldots, g_n) \cdot (h_1, \ldots, h_m) \sim (g_1, \ldots, g_n) \cdot ((h_1, \ldots, h_{m-1}) \cdot (h_m)) \sim ((g_1, \ldots, g_n) \cdot (h_1, \ldots, h_{m-1})) \cdot (h_m) \sim (g_1, \ldots, g_n, h_1, \ldots, h_{m-1}) \cdot (h_m) \sim (g_1, \ldots, g_n, h_1, \ldots, h_m) =: (g_1, \ldots, g_n) * (h_1, \ldots, h_m)$. Und mit $e' = e$ aus dem Neutralitätsgesetz: $e * (g_1, \ldots, g_n) = (e, g_1, \ldots, g_n) \sim (g_1, \ldots, g_n) \sim (g_1, \ldots, g_n, e) = (g_1, \ldots, g_n) * e$.

7.4 Freies kommutatives Monoid

Prinzip 7.6 *Für ein kommutatives Monoid M (in additiver Schreibweise) mit ausgezeichneter Teilmenge E sind äquivalent*

(i) M entsteht aus den Monoidtermen úber der (Variablen- bzw. Erzeuger-)Menge E, indem man modulo der Gesetze der kommutativen Monoide rechnet, d.h. die Termstruktur $T(E)$ nach der Kongruenzrelation $\sim$ faktorisiert, die sich ergibt, wenn man neben den Kongruenzregeln auch noch die folgenden Regeln hat

$$s + (t + u) \sim (s + t) + u,\ \ 0 + t \sim t,\ t + 0 \sim t.\ \ s + t \sim t + s \text{ fúr alle Terme } s, t, u$$

(ii) Fortsetzungs- oder universelle Eigenschaft*: M wird von E erzeugt und zu jedem kommutativen Monoid A und jeder Abbildung $\gamma : E \to A$ gibt es einen (eindeutig bestimmten) Homomorphismus $\overline{\gamma} : M \to A$ mit $\overline{\gamma}|E = \gamma$*

Gilt eine der beiden Bedingungen, so heisst M ein von E *frei erzeugtes kommutatives Monoid.* Die Eindeutigkeit von $\overline{\gamma}$ folgt aus Lemma 3.14, da M von E erzeugt wird.

Korollar 7.7 *Zu jeder Menge E gibt es ein bis auf Isomorphie eindeutig bestimmtes von E frei erzeugtes kommutatives Monoid.*

Beweis wörtlich wie oben. □

Für Terme in $+, 0$ definieren wir rekursiv

$$0t = 0,\ \ (k + 1)t = (kt) + t$$

Satz 7.8 *Für ein kommutatives Monoid M mit Teilmenge E sind äquivalent*

- *M ist von E frei erzeugtes kommutatives Monoid*
- *Die Elemente von M haben bis auf Reihenfolge eindeutige Darstellung $a = k_1g_1 + \ldots + k_ng_n$ mit $g_i \in E$, $k_i \in \mathbb{N}_{>0}$*
- *Gibt man eine Anordnung $\prec$ von E vor, so haben die Elemente von M eindeutige Darstellung $a = k_1g_1 + \ldots + k_ng_n$ mit $k_i \in \mathbb{N}_{>0}$, $g_1 \prec g_2 \ldots \prec g_n$*
- *Es gibt einen Isomorphismus $a \mapsto \hat{a}$ von M auf das additive Monoid $\mathbb{N}^{(E)}$ mit $\hat{g}(h) = \begin{cases} 1 & \text{falls } g = h \\ 0 & g \neq h \in E \end{cases}$ für $g \in E$*

Hierbei besteht $\mathbb{N}^{(E)}$ aus allen Abbildungen $f : E \to \mathbb{N}$ mit $f(x) \neq 0$ nur für endlich viele $x \in E$. Ist $E = \mathbb{N}$ oder $E = \{1, \ldots, n\}$, so kann man f als Folge $(f(0), f(1), \ldots)$ bzw. n-Tupel $(f(1), \ldots, f(n))$ verstehen. Gerechnet wird, wie in LA, komponentenweise.

Korollar 7.9 *Für ein kommutatives Monoid M mit n-elementiger Teilmenge $E = \{g_1, \ldots, g_n\}$ sind äquivalent*

- *M ist von E frei erzeugtes kommutatives Monoid*
- *Die Elemente von M haben eindeutige Darstellung $a = k_1g_1 + \ldots + k_ng_n$ mit $k_i \in \mathbb{N}$*
- *Es gibt einen Isomorphismus ϕ von M auf $\mathbb{N}^n$ mit $\phi g_i = (0, \ldots, 1_i, \ldots, 0)$*

Beweis. Die Existenz der Darstellung in einem kommuativen Monoid ist logo -man kann's durch Induktion beweisen. Die Eindeutigkeit bedeutet wieder Injektivität wie oben.

$\mathbb{N}^{(E)}$ ist kommutatives Monoid weil $\mathbb{N}$ eins ist und hat offenbar die Darstellung $(k_g \mid g \in E) = k_1g_1 + \ldots + k_ng_n$ wobei $g_1 \prec \ldots \prec g_n$ und $\{g_1, \ldots, g_n\} \supseteq \{g \in E \mid k_g \neq 0\}$ - und wenn man da '=' verlangt, wird die Darstellung eindeutig. □

Bei der Normalformenmethode können wir statt in der Termalgebra auch im freien Monoid arbeiten (weil wir das schon im Griff habem) und es genügt sich (induktiv über n) zu überlegen, dass $(k_1g_1 + \ldots + k_ng_n) + (l_1g_1 + \ldots + l_ng_n) = k_1g_1 + \ldots + k_{n-1}g_{n-1} + l_1g_1 + \ldots + l_{n-1}g_{n-1} + k_ng_n + l_ng_n = (k_1 + l_1)g_1 + \ldots (k_{n-1} + l_{n-1})g_{n-1} + (k_n + l_n)g_n$ wobei $kg + lg = (k + l)g$ durch Induktion über l beweisen wird.

7.5 Freie abelsche Gruppen

Satz 7.10 *Für eine abelsche Gruppe M mit Teilmenge E sind äquivalent*

- *M ist von E frei erzeugte abelsche Gruppe*
- *Die Elemente von M haben bis auf Reihenfolge eindeutige Darstellung $a = r_1g_1 + \cdot + r_ng_n$ mit $g_i \in E$, $0 \neq r_i \in \mathbb{Z}$*
- *Gibt man eine Anordnung $\prec$ von E vor, so haben die Elemente von M eindeutige Darstellung $a = r_1g_1 + \ldots + r_ng_n$ mit $0 \neq r_i \in \mathbb{Z}$, $g_1 \prec g_2 \ldots \prec g_n$*
- *Es gibt einen Isomorphismus $a \mapsto \hat{a}$ von M auf die Gruppe $\mathbb{Z}^{(E)}$ mit $\hat{g}(h) = \begin{cases} 1 & \text{falls } g = h \\ 0 & g \neq h \in E \end{cases}$ für $g \in E$*

Hierbei besteht $\mathbb{Z}^{(E)}$ aus allen Abbildungen $f : E \to \mathbb{Z}$ mit $f(x) \neq 0$ nur für endlich viele $x \in E$. Ist $E = \mathbb{N}$ oder $E = \{1, \ldots, n\}$, so kann man f als Folge $(f(0), f(1), \ldots)$ bzw. n-Tupel $(f(1), \ldots, f(n))$ verstehen. Gerechnet wird, wie in LA, komponentenweise.

Korollar 7.11 *Für eine abelsche Gruppe M mit n-elementiger Teilmenge $E = \{g_1, \ldots, g_n\}$ sind äquivalent*

- *M ist von E frei erzeugte abelsche Gruppe*
- *Die Elemente von M haben eindeutige Darstellung $a = r_1 g_1 + \ldots + r_n g_n$ mit $r_i \in \mathbb{Z}$*
- *Es gibt einen Isomorphismus ϕ von M auf $\mathbb{Z}^n$ mit $\phi g_i = (0, \ldots, 1_i, \ldots, 0)$*

Beweis. Nach dem Muster von oben. Kennt man aber auch aus LA. □ Normalformenmethode: Für die Addition wie bei kommutativen Monoiden nur mit $k_i, l_i \in R$. Hier ist $kg+lg = (k+l)g$ durch die Modulgesetze garantiert. Das allgemeine Distributivgesetz beweise man als Übung.

Ist S ein Ring, so ist der Gruppenhomomorphismus $z \mapsto z1$ auch ein Ringhomomorphismus, also ist $\mathbb{Z}$ der von $\emptyset$ frei erzeugte (kommutative) Ring.

Freie Gruppen gibt's natürlich auch, aber fúr die Charakterisierung muss man sich ein bisschen mehr anstrengen: man hat eine eindeutige (linksgeklammerte) Darstellung

$$g_1^{z_1} \cdot \ldots \cdot g_n^{z_n}, \quad z_i \in \mathbb{Z},\ g_i \in E,\ g_i \neq g_{i+1}$$

Hier ist die Normalformenmethode der übliche Weg.

7.6 Präsentierung von Monoiden und Gruppen

Unter den Monoiden mit Erzeuger a so, dass die *Relation* $a^k = a^{k+p}$ für gegebene $k, p \in \mathbb{N}$, gibt es ein allgemeinstes, d.h. eines, aus dem sich alle anderen als homomorphe Bilder ergeben. Nämlich $\mathbb{N}/\sim$, wobei $\sim$ die feinste Kongruenzrelation mit $a^k \sim a^{k+p}$ ist vgl. Kap.3.10. Für $k = 0$ erhalten wir $\mathbb{N}/\sim \cong \mathbb{Z}/(p)$.

Allgemeiner sei E eine Menge von Erzeugersymbolen. Ein Monoid M mit *Erzeugersystem* E wird gegeben durch eine Abbildung $\gamma : E \to M$ so, dass M von $\gamma(E)$ erzeugt wird. γ muss nicht injektiv sein, trotzdem dürfen wir die Symbole aus E benutzen, um die entsprechenden Elemente von M zu bezeichnen.

Sind w, v Monoid-Terme bzw. Wörter in Symbolen aus E, so sagen wir, dass die *Relation* $w \stackrel{!}{=} v$ in M mit Erzeugerystem E *erfüllt* is bzw. *gilt*, falls $\overline{\gamma}(w) = \overline{\gamma}(v)$, wobei $\overline{\gamma}$ die Fortsetzung von γ zu einem Homomorphimus der Termstruktur bzw. des freien Monoids über E in das Monoid M ist.

Beispiel. $E = \{d, s\}$, Die Relationen

$$d^4 \stackrel{!}{=} e,\ s^2 \stackrel{!}{=} e,\ sd = d^3 s$$

gelten im Monoid D_4 der Symmetrien des Quadrats, wenn d eine 90^o-Drehung und s eine Spiegelung bezeichnet. Sie gelten auch in $\mathbb{Z}/(2)$, wenn d, s irgendein Erzeugersystem bezeichnen. Die Relation $s^2 \delta e$ gilt nicht in $\mathbb{Z}/(4)$, wenn d, s beide den Erzeuger $\tilde{1}$ bezeichnen. Die Relation $d^4 \stackrel{!}{=} e$ und $s^2 \stackrel{!}{=} e$ nicht aber $sd \stackrel{!}{=} d^3 s$ gelten in $\mathbb{Z}/(4) \times \mathbb{Z}/(2)$, wenn die Erzeuger d, s die Elemente $(\tilde{1}, \tilde{0})$ und $(\tilde{0}, \tilde{1})$ bezeichnen.

Prinzip 7.12 *Sei E eine Menge von Erzeugersymbolen und w_i, v_i $(i \in I)$ Elemente (Wörter) aus dem freien Monoid $f(E) = E^*$ über E. Sei M eine Monoid mit durch E bezeichneter Erezugermenge. Dann sind die folgenden Aussagen äquivalent*

- *M entsteht aus $F(E)$ indem man modulo der Relatioen $w_i \stackrel{!}{=} v_i$ $(i \in I)$ rechnet, d.h. $f(E)$ nach der feinsten Knngruenz $\sim$ mit $w_i \sim v_i$ für alle $i \in I$ faktorisiert.*
- Universelle Eigenschaft. *Zu jedem Monoid A mit durch E bezeichneter Erzeugermeneg derart, dass die Relationen $w_i \stackrel{!}{=} v_i$ $(i \in I)$ gelten, gibt es eonen (eindeutig bettimmten surjektiven) Homomorphismus $\phi : M \to A$ so, dass für alle $a \in E$ das durch a bezeichnete Element von A gerade $\phi(a)$ ist.*

Ein solches M ist bis auf Isomorphie, die die durch E bezeichneten Elemente festlässt, eindeutig bestimmt und heisst von E unter den Relationen $w_i \stackrel{!}{=} v_i$ $(i \in I)$ frei erzeugt bzw. durch die Präsentierung $E,\ w_i \stackrel{!}{=} v_i$ $(i \in I)$ *gegeben.*

Beweis nach demselben Muster wie bei der freien Monoiden. Schlauköpfe bemerken, dass man den Spezialfall einer von der leeren Mange frei erzeugten algebraischen Struktu hatr, wobei die betrachete Klasse die der Monoids mit den Konstanten $a \in E$ ist und den Relationen w_i *deq*v_i als definierenden Gleichungen. □

Beispiele: Das freie Monoid mit Erzeugern E und Relationen $ab = ba\,(a, b \in E)$ ist das freie kommutative Monoid mit Erzeugermenge E. Beweis. Zeige Kommuativität durch Induktion über Wortlänge,
Das Monoid D_4 hat oben angebene Präsentierung. Beweis. Zeige dass zu jedem $w \in \{d, s\}^*$ $k \in \{0, 1, 2, 3\}$ und $l \in \{0, 1\}$ gibt mit $w \sim d^k s^l$. Also hat das durch die Präsentierung gegebene Monoid M höchstens 8 Elemente. Andererseits erfüllt D_4 auf naheliegende Weise die Relationen, also gibt es surjektiven Homomorphismus $\phi : M \to D_4$. Da $|D_4| = 8$, muss ϕ Isomorphismus sein.
Die Gruppe D_n der Symmetrien einesc regelmäßigen n-Ecks ist gegeben durch die Präsentierung

$$\{d, s\},\ \ d^n \stackrel{!}{=} e,\ s^2 \stackrel{!}{=} e,\ sd \stackrel{!}{=} d^{-1}s$$

Interne Charakterisierungen von durch Präsentierungen gegebenen Monoiden oder Gruppen darf man im allgemeinen nicht erwarten: in der Regel gibt es kenien Algorithmus um für Wórter w, v die Gültigkeit von $w \sim v$ zu entscheiden (d.h. das *Wortproblem* zu lösen). Nur für kommutative Monoide ist ein solcher Algorithmus garaniert.

7.7 Äquivalenz von Präsentierungen.

Wir betrachten Präsentierungen in einer nichtttrivialen Klasse algebraischer Strukturen, die durch Gleichungen definiert ist. Dann haben wir zu jeder Menge E eine bis aus Isomorphie eindeutig bestimmte freie Struktur $F(E)$. Eine *Präsentierung* über der Erzeugermenge E wird dann durch eine Menge $R \subseteq F(E) \times F(E)$ von *Relationen* gegeben. Die durch die Präsentierung gegebene Struktur A und der zugehörige kanonische Homomorphismus π sind dann äquivalent durch folgende beiden Eigenschaften charakterisiert

- π ist surjektiv und der Kern von π ist die von R erzeugte Kongruenz von $F(E)$

- zu jeder Struktur B in der Klasse und Abbiildung $\phi : E \to B$ für die R im Kern von ϕ liegt (d.h. die $\phi(v)(v \in E)$ erfüllen die Relationen aus R) gibt es einen Homomorphismus $\overline{\phi} : A \to B$ mit $\overline{\phi}\pi|E = \phi$

A und π sind durch die Präsentierung bis auf Isomorphie eindeutig bestimmt - d.h. hat man auch A', π', so gibt es Isomorphismus $\omega : A \to A'$ mit $\omega\pi = \pi'$.

Zwei Präsentierungen E_i, R_i $(i = 1, 2)$ sind *äquvalent*, wenn die zugehörigen Strukturen A_i isomorph sind. Die folgende Bedingung ist dafür notwendig und hinreichend. Dabei ist $\sim_i$ die von R_i erzeugte Kongruenz von $F(E_i)$.

- Zu allen $(i, j) \in \{(1, 2), (2, 1)\}$ gibt es Abbildugen $\alpha_i : E_j \to E_i$ so, dass gilt (wobei $\overline{\alpha}_i : F(E_j) \to F(E_i)$ die homomorphe Fortsetzung von α_i)

  (1) $\alpha_i v \sim_i \alpha_i w$ für alle $(v, w) \in R_j$

  (2) Zu jedem $v \in E_i$ gibt es Term $t(x_1, \ldots, x_n)$ und $w_1, \ldots, w_n \in E_j$ so, dass $v \sim_i t(\alpha_i w_1, \ldots, \alpha_i w_n)$

  (3) Für alle $v \in E_i$ gilt $v \sim_i \overline{\alpha_i}\alpha_j v$

Mit den kanonischen Projektionen $\pi_i : F(E_i) \to A_i$ liest es sich so

(1) $\pi_i\alpha_i v = \pi_i\alpha_i w$ für alle $(v, w) \in R_j$

(2) $\pi_i v \in \mathsf{Spann}(\pi_i\overline{\alpha}_i(E_j))$ für alle $v \in E_i$

(3) Für alle $v \in E_i$ gilt $\pi_i v = \pi_i\overline{\alpha_i}\alpha_j v$

Beweis. Die Notwendigkeit ist klar. Umgekehrt seien (1)-(3) vorausgesetzt und $\pi : F(E_i) \to A_i$ surjektiv mit Kern $\sim_i$. Nach (1) gilt $\sim_j \subseteq \mathsf{Kern}(\pi_i\alpha_i)$, also gibt es nach dem Ergäznungssatz

$$\beta_i : A_j \to A_i \text{ mit } \beta_j\pi_j = \pi_i\overline{\alpha}_i.$$

Nach (3) gilt für $v \in E_i$

$$\pi_i v = \pi_i\overline{\alpha}_i\alpha_j v$$

also

$$\pi_j\alpha_j v = \beta_j\pi_j v = \beta_j\pi_i\overline{\alpha}_i\alpha_j v = \beta_j\beta_i\pi_j\alpha_j v$$

Da A_j nach (2) von den $\pi_j\alpha_j(v)$ mit $v \in E_i$ erzeugt wird, folgt

$$\beta_j\beta_i = \mathsf{id}_{A_j} \quad \square$$

Beispiel. Die Gruppenpräsentierungen

$$(a) \quad \{d, s\}, d^n = e = s^2,\ sd = d^{-1}s$$

$$(b) \quad \{s_1, s_2\}, s_1^2 = s_2^2 = e = (s_2s_1)^n$$

sind äquivalent mit

$$d \mapsto s_2s_1,\ s \mapsto s_1, \quad s_1 \mapsto s,\ s_2 \mapsto ds$$

Beweis. $s_2s_1,\ s_1$ erfüllen Relationen von (a), weil $s_1(s_2s_1) = s_1^{-1}s_2^{-1}s_1 = (s_2s_1)^{-1}s_1$, und spannen (b) auf, weil $s_2 = (s_2s_1)s_1$.

$ds,\ s$ erfüllen Relationen von (b), weil $(ds)^2 = dsds = dd^{-1}ss = e$ und $((ds)s)^n = d^n = e$, und spannen (a) auf, weil $d = (ds)s$.

(3) gilt, weil $d = (ds)s$ und $s = s$ sowie $s_2 = (s_2s_1)s_1$ und $s_1 = s_1$.

7.8 Freie Gruppen

Lemma 7.13 *Sei M ein Monoid und $E \subseteq M$. Zu jedem $a \in E$ gebe es $a^\ominus \in M$ mit $aa^\ominus = e = a^\ominus a$. Sei M von $E \cup E^\ominus$ erzeugt mit $E^\ominus = \{a^\ominus \mid a \in E\}$ Dann ist M eine Gruppe und von E erzeugt. Weiterhin gilt: Für jede Gruppe G und Monoidhomomorphismus $\phi : M \to G$ ist $\phi : M \to G$ ein Gruppenhomomorphismus mit $\phi(a^\ominus) = \phi(a)^{-1}$ für $a \in E$.*

Beweio. Nach Voraussetzung ist $a^\ominus = a^{-1}$ eindeutig bestimmtes Inverses zu $a \in E$. Also $E \cup E^\ominus \subseteq M^\times$ und somit $M^\times = M$, da die Einheiten ein Untermonoid bilden. Monoidhomomorphismen zwischen Gruppen sind schon Gruppenhomomorphismens $\square$.

Wenn wir nur Monoide betrachten, können wir statt der Terme in TE) Wörter im freien Monoid E^* benuzten.

Satz 7.14 *Gegeben seien Erzeugersymbole $a \in E$ und $a^\ominus$. Für ein Monoid M sind die folgenden Aussagen äquivalent äquivalent*

(1) M ist von E frei erzeugte Gruppe und $a^\ominus = a^{-1}$ für $a \in E$, d,h. M wird von E erzeugt und zu jeder Gruppe A und Abbildung $\gamma : E \to A$ gibt es homomorphe Fortsetzung $\overline{\gamma} : M \to A$.

(2) M hat Präsentierung mit Erzeugern $a, a^\ominus\, (a \in E)$ und Relationen $aa^\ominus = e = a^\ominus a$

(3) Jedes Element von M hat eine eindeutige Darstellung

$$w = a_1^{\varepsilon_1} \cdot \ldots \cdot a_n^{\varepsilon_n} \quad \textit{mit } n \in \mathbb{N},\ a_i \in E,\ \varepsilon_i = 1 \textit{ bzw. } \varepsilon_i = \ominus \textit{ und } a_i = a_{i+1} \Rightarrow \varepsilon_i = \varepsilon_{i+1}$$

Und es gibt zu jedem E ein solche Gruppe M, die freie Gruppe $\mathsf{FG}(E)$. Diese ist bis auf Isomorphie eindeutig bestimmt.

Beweis. $2 \Rightarrow 1$. Sei A eine Gruppe und $\gamma : E \to A$. Setze γ auf $E \cup E^\ominus$ fort mit $\gamma(a^\ominus) = \gamma(a)^{-1}$. Dann sind die Relationen von M für die $\gamma(a)$ und $\gamma(a^\ominus)$ erfúllt. Also gibt es Monoidhomomorphismus $\overline{\gamma} : M \to A$ mit $\overline{\gamma}(\tilde{a}) = \gamma(a)$ und $\overline{\gamma}(\widetilde{a^\ominus}) = \gamma(a^\ominus) = \gamma(a)^{-1}$. Nach dem Lemma ist M Gruppe und $\overline{\gamma}$ Gruppenhomomorphismus.

$2 \Rightarrow 3$ zeigen wir weiter unten mit der Methode der Termersetzung. Es folgt insbesondere

- Es gibt ein Monoid M' mit eindeutiger Darstellung wie in (3) gefordert.

Wegen der Eindeutigkeit der Darstellung dürfen wir E als Teilmenge von M' auffassen, M' ist Gruppe nach dem Lemma.

$1 \Rightarrow 3$ Sei M von E frei erzeugte Gruppe und M' wie gerade beschrieben. Sei $\phi : M \to M'$ der Gruppenhomomorphismus mit $\phi(a) = a \in M'$ für $a \in E$. Da M von E erzeugt ist, hat man da Darstellung in der Form $x = a_1^{\varepsilon_1} \cdot \ldots \cdot a_n^{\varepsilon_n}$ mit $\varepsilon = \pm 1$) und, indem man Teilwörter $a^\varepsilon a^{-\varepsilon}$ in beliebiger Reihenfolge wegstreicht, erhält man eine Darstellung von x mit $a_i = a_{i+1} \Rightarrow \varepsilon_i = \varepsilon_{i+1}$. Da die entsprechende Darstellung von $\phi(x) \in M'$ eindeutig ist, ist ϕ injektiv und auch die Darstellung in M eindeutig.

7.9 Fundierung

Sei P eine Menge und $\to$ eine Relation auf P. Lies $x \to y$ als x *reduziert direkt* zu y. $(P, \to)$ heisst *fundiert, terminierend, artinsch* (auf informatisch auch noethersch) wenn es keine unendlichen Folgen gibt mit

$$a_0 \to a_1 \to a_2 \dots$$

Das Beweisprinzip vom *minimalen Verbecher* bzgl. $(P, \to)$ geht so: Sei $A(x)$ eine Aussage über Elemente x von P. Ein Verbecher ist ein Element x von P, für das $A(x)$ nicht gilt. Er ist *minimal*, wenn $A(y)$ für alle $y \in P$ gilt, zu denen x direkt reduziert, d.h. $x \to y$. Das Beweisprinzip besagt nun

- *Gibt es keine minimalen Verbrecher, so gilt $A(x)$ für alle $x \in P$.*

Prinzip 7.15 *Ist $(P, \to)$ fundiert, so gilt das Prinzip vom minimalen Verbecher.*

Beweis. Angeommen, es gibt keine minimalen Verbecher, aber die Menge V der Verbecher ist nicht leer. Wähle eine Verbrecher v_0, der ist nicht minimal, also kann man einen Vebrecher v_1 mit $v_0 \to v_1$ wählen. U.s.w.: ist der Verbrecher v_n shcon gewähtl, so ist der nicht minimal, also kann man einen Verbecher v_{n+1} mit $v_n \to v_{n+1}$ wählen. Ad infinitum, Widerspruch! □
Hier wurde das Prinzip der bedingten Auswahl benutzt.

Eine *Quasiordung* ist eine reflexive und transitive Relation. Setze $t \leftrightarrow s \Leftrightarrow t \to s$ oder $s \to t$. Wir definieren

$$\begin{aligned} t \xrightarrow{*} s &\quad\Leftrightarrow\quad t = s \text{ oder es gibt } t = t_0 \to t_1 \to \dots \to t_n = s \\ t \overset{*}{\leftrightarrow} s &\quad\Leftrightarrow\quad t = u \text{ oder es gibt } t = t_0 \leftrightarrow t_1 \leftrightarrow \dots \leftrightarrow t_n = s \end{aligned}$$

Offenbar handelt es sich um eine Quasiordnung bzw. Äquivalenzrelation, und zwar die kleinste $\to$ umfassende, die von $\to$ *erzeugte*.

a ist *minimal* oder *Normalform* in $(P, \to)$, falls $a \to b$ für kein $b \in P$.

Lemma 7.16 *Ist $\to$ terminierend, so gibt es zu jedem t mindestens eine Normalform u mit $t \xrightarrow{*} u$*

Beweis. Sei t ein minimaler Verbecher. Dann ist t selbst keine Normalform, also gibt es b mit $a \to b$ und b ist kein Verbrecher. Also gibt es Normalform u mit $b \xrightarrow{*} u$ und dann auch $a \xrightarrow{*} u$. Widerspruch. □.

Wie kann man Termination erreichen? Eine Gewichtung ist eine Abbildung τ in eine geordnete Menge $(M, <)$ mit Minimalbedingung - d.h. jede nichtleere Teilmenge hat ein minimales Element - (z.B. die natürlichen Zahlen mit natürlicher Ordnung) so, dass

$$s \to t \;\Rightarrow\; \tau(t) < \tau(s) \;\text{ für alle } s, t \in P.$$

Lemma 7.17 *Erlaubt $(P, \to)$ eine Gewichtung, so ist es terminierend*

Beweis. Hätte man eine unendliche Folge $a_0 \to a_1 \to \dots$, so hätte $\{\tau(a_n) | \, n \in \mathbb{N}\}$ kein minimales Element. □

7.10 Konfluenz

Wir sagen, dass $\to$ lokal konfluent ist, wenn es zu $t \to t_1$, $t \to t_2$ stets s gibt mit $t_1 \overset{*}{\to} s$ und $t_2 \overset{*}{\to} s$.

Lemma 7.18 Newman, Diamanten. *Ist $\to$ terminierend und lokal konfluent, so gibt es zu jedem t eine eindeutig bestimmte Normalform t' mit $t \overset{*}{\to} t'$.*

Beweis durch Überführung der minimalen Verbrecher. Sei t ein solcher. Dann gibt es mindestens zwei verschiedene Normalformen u_1, u_2 mit $t \overset{*}{\to} u_1$ und $t \overset{*}{\to} u_2$. Nach Definition von $\overset{*}{\to}$ gibt es aber

$$t \to t_1 \overset{*}{\to} u_1 \quad \text{und} \quad t \to t_2 \overset{*}{\to} u_2.$$

Nach der Annahme der lokalen Konfluenz und dem vorangehenden Lemma gibt es aber ein s und dann eine Nromalform u so, dass

$$t_1 \overset{*}{\to} s, \quad t_2 \overset{*}{\to} s \quad \text{und} \quad s \overset{*}{\to} u.$$

Es folgt mit Transitivität

$$t_1 \overset{*}{\to} u \quad \text{und} \quad t_2 \overset{*}{\to} u.$$

Nun sind aber t_1 und t_2 keine Verbrecher (da ja $t \to t_i$), also folgt $u = u_1$ und $u = u_2$. Also $u_1 = u_2$, ein Widerspruch. □

Korollar 7.19 *Ist $\to$ terminierend und lokal-konfluent auf P, so bilden die Normalformen ein Repräsentantensytem der von $\to$ erzeugten Äquivalenzrelation $\overset{*}{\leftrightarrow}$ auf P.*

Beweis. Sei u die eindeutig bestimmte Normalform mit $t \overset{*}{\to} u$. Durch Induktion über n in der Def. von $t \overset{*}{\leftrightarrow} t_n$ zeigen wir: $t_n \overset{*}{\to} u$. Also nach Induktionsannahme $t_{n-1} \overset{*}{\to} u$. Gilt $t_n \to t_{n-1}$ so folgt die Behauptung sofort. Andernfalls $t_{n-1} \to t_n$. Es gibt Normalfrom v mit $t_n \overset{*}{\to} v$, also $t_{n-1} \overset{*}{\to} v$ und somit $v = u$ aus der Eindeutigkeit. □

7.11 Gerichtete Termersetzung

In einem Wortmonoid A^* sei eine Menge R von Paaren (r, r') gegeben, die *Erszetzungsregeln* $r \to_0 r$ Das zugehörige *Termersetzungssystem* ist die folgende Relation $\to$ auf A^*

- $w \to w'$ falls es $r \to_0 r'$ in R gibt so,
  dass r als Teilwort in W vorkommt und w' aus w entsteht,
  indem r durch r' ersetzt wird.

Lemma 7.20 *$\overset{*}{\leftrightarrow}$ ist die von R auf dem Monoid A^* erzeugte Kongruenzrelation.*

Beweis. Es gilt offensichtlich

$$w \to w' \Rightarrow wv \to w'v \text{ und } vw \to vw'$$

Es folgt

$$w \leftrightarrow w' \Rightarrow wv \leftrightarrow w'v \text{ und } vw \leftrightarrow vw'$$

Durch Induktion über die Definition von $\overset{*}{\leftrightarrow}$ folgt

$$w \overset{*}{\leftrightarrow} w' \Rightarrow wv \overset{*}{\leftrightarrow} w'v \text{ und } vw \overset{*}{\leftrightarrow} vw'$$

7.12 Normalformen für Gruppen

Wir betrachten das Monoid mit Erzeugern $a, a^{\ominus}$ $(a \in E)$ und Relationen

$$aa^{\ominus} = e, \;\; a^{\ominus}a = e$$

Die Ersetzungsregeln im Wortmonoid $(E \cup E^{\ominus})^*$ (dabei ist e das leere Wort) sind so gegeben

$$aa^{\ominus} \to e, \;\; a^{\ominus}a \to e$$

Gilt $w \overset{*}{\to} w'$ so ist w' kürzer als w, also ist $\to$ terminierend. Zum Nachweis der lokalen Konfluenz hat man folgende Fälle zu betrachten

$$w = w_1 a^{\varepsilon} a^{-\varepsilon} w_2 b^{\eta} b^{-\eta} w_3, \;\; w \to w' = w_1 w_2 b^{\eta} b^{-\eta} w_3, \; w \overset{*}{\to} w'' = w_1 a^{\varepsilon} a^{-\varepsilon} w_2 w_3$$

$$\text{hier } w' \overset{*}{\to} w_1 w_2 w_3, \; w'' \overset{*}{\to} w_1 w_2 w_3$$

$$a = b, \; w = w_1 a^{\varepsilon} a^{-\varepsilon} b^{\varepsilon}, \;\; w \overset{*}{\to} w_1 b^{\varepsilon} w_2, \; w \overset{*}{\to} w_1 a^{\varepsilon} w_2$$

$$\text{hier } w_1 b^{\varepsilon} w_2 = w_1 a^{\varepsilon} w_2 \;\; \text{weil } a = b$$

Die Äquivalenzrelation $\overset{*}{\leftrightarrow}$ ist nach Lemma ?? gerade die von $aa^{\ominus} \sim e$ und $a^{\ominus}a \sim e$ $(a \in E)$ erzeugte Kongruenzrelation, also $(E \cup E^{\ominus})^*/\sim$ das Monoid aus (2) des Satzes. Nach Kor.?? bilden die Normalformen von $\to$ ein Repräsentantensystem für $\overset{*}{\leftrightarrow}$. Diese sind dadurch charakterisiert, dass sie kein Teilwort der Form $aa^{\ominus}$ bzw. $a^{\ominus}a$ mit $a \in E$ enthalten, also der Anforderung in (3) genügen. Damit ist der Satz über die Charakterisierung der freien Gruppen bewiesen. □

Die durch Erzeugende $a_1, \ldots, a_n$ und Relationen $r = e$ $(r \in R)$ gegebene Gruppe erhalten wir (theoretisch), indem wir in der freien Gruppe $F = \mathsf{FG}(a_1, \ldots, a_n)$ den von R erzeugten Normalteiler N, nämlich

$$\mathsf{Nt}(R) = \{\prod_{i=1}^{n} g_i^{-1} r^{\varepsilon_i} g_i \mid n \in \mathbb{N}, \; r_i \in R, \; g_i \in G\}$$

bilden und dann die Faktorgruppe F/N mit Erzeugern $g_i = Na_i$. Der Homomorphieergänzungssatz liefert uns die geforderte Ergänzungseigenschaft. Aber wie F/N genau aussieht, wissen wir nur ausnahmsweise. Etwa bei der unendlchen Diedergrueppe mit Erzeugern d, s und Relatiionen $s^2 = e, \; sd = d^{-1}s$. Das Termersetzungssystem

$$s^2 \to e, \;\; sd \to d^{-1}s$$

ist lokal knfluent und terminierend und liefert die eindeutige Darstellung $d^z s^l$ mit $z \in \mathbb{Z}, l = 0, 1$.

8 Freie Moduln

8.1 Rechtsmoduln

Will man bei der hierzulande üblichen Notation von Abbildungen in der Form $\phi(x)$ und entsprechend der Beschreibung linearer Abbildunge durch Matrizen in der Form $\boldsymbol{x} \mapsto A\boldsymbol{x}$

bleiben. so muss man entweder voraussetzen, dass man nur R-Moduln über kommutativen Ringen betrachet oder zu *Rechts-R-Moduln* übergehen - man schreibt die Skalare r rechts an die Vektoren v, also vr, und verlangt

$$v1 = v,\ (v+w)r = vr + wr,\ v(r+s) = vr + vs,\ \ v(rs) = (vr)s$$

Ein R-Rechtsmodul wird zum $R^{op}-$Linksmodul, wenn man $rv := vr$ setzt und im *entgegengesetzen Ring* R^{op} so multipliziert: $r * s = s \cdot r$. An der Theorie ändert sich also im Prinzip nichts. Ist R kommutativ, so ist demnach links und rechts gehupft wie gesprungen. Freidenker und Computer schreiben und lesen von links nach rechts, also Vektoren als Zeilen und Abbildungen in der Form $y = xA$.

Achtung. Im Folgenden sind alle Moduln als Rechtsmoduln zu verstehen.

8.2 Basen

Eine Familie $a_i, i \in I$ von Elementen a_i eines R-Moduls V heisse *linear unabhängig* `[linear independent]` , wenn für jede endliche Teilmenge $J \subseteq I$ die Teilfamilie $a_i, i \in J$ die folgende Bedingung erfüllt

$$\text{für alle } r_j \in R \text{ gilt: } \sum_{j\in J} a_j r_j = 0 \ \Rightarrow r_j = 0 \text{ für alle } j \in J$$

Eine linear unabhängige Familie $a_i, i \in I$ ist *Basis* `[basis]` von V, wenn V von der Menge $\{a_i \mid i \in I\}$ erzeugt wird.

8.3 Modulare Philosophie der Freiheit

Sei R ein fester Ring. Wie wir freie R-Moduln auf zwei äquivalente Weisen zu definieren haben und das es sowas gibt, sollte jetzt klar sein. Falls nicht, dann nochmal dies:

Den freien R-Modul mit Erzeugern $v_1, \ldots, v_n$ (bei festen R) kann (und sollte) man auch so verstehen: man bildet die algebraische Struktur T aller Terme, die man aus den $v_1, \ldots, v_n$ mithilfer der Addition, Subtraktion, Konstante 0, und den Moltiplikationen mit Skalaren aus R aufbauen kann, d.h

- $v_1, \ldots, v_n$ und 0 sind Terme
- Sind s, t Terme, so auch $s + i$, $-t$ und tr für $r \in R$.

und rechnet dann modulo ($\sim$) der Gesetze der R-Moduln. Insbsodere findet man zu jedem Term eine äquivalente Linearkombination $\sum_{i=1}^{n} v_i r_i$. Diese Darstellung muss eindeutig sein, weil sie es in dem konkreten Modell R^n ist: Genauer: Man hat Homomorphismus $\phi : T \to R^n$ mit $\phi(v_i) = \boldsymbol{e}_i$ (durch Termauswertung), der Kern von ϕ ist gröber als $\sim$, das R^n ein R-Modul ist. Ist nun $\sum_i v_i r_i \sim \sum_i v_i s_i$ so, $\sum_i \phi(v_i) r_i = \sum_i \phi(v_i) s_i$, also $r_i = s_i$.

Insbesondere gilt: Der R-Modul M ist von E *frei erzeugt*, falls M von E erzeugt wird und zu jedem R-Modul N und Abbildung $\gamma : E \to N$ ein (dann eindeutig bestimmter) Homomorphismus $\overline{\gamma} : M \to N$ existiert mit $\gamma | E = \overline{\gamma}$.

8.4 Freier Modul

Satz 8.1 *Für einen R-Modul M mit Teilmenge E sind äquivalent*

- *M ist von E frei erzeugter R-Modul*
- *Die Elemente von M haben bis auf Reihenfolge eindeutige Darstellung $a = v_1r_1 + \cdot + v_nr_n$ mit verschiedenen $v_i \in E$, $0 \neq r_i \in R$*
- *Gibt man eine Anordnung $\prec$ von E vor, so haben die Elemente von M eindeutige Darstellung $a = v_1r_1 + \ldots + v_nr_n$ mit $0 \neq r_i \in R$, $v_1 \prec v_2 \ldots \prec v_n$ in E*
- *E ist, als Familie aufgefasst, eine Basis von M.*
- *Es gibt einen Isomorphismus $a \mapsto \hat{a}$ von M auf den R-Modul $R^{(E)}$ mit $\hat{g}(h) = \begin{cases} 1 & falls\ g = h \\ 0 & g \neq h \in E \end{cases}$ für $g \in E$*

Hierbei besteht $R^{(E)}$ aus allen Abbildungen $f : E \to R$ mit $f(x) \neq 0$ nur für endlich viele $x \in E$. Ist $E = \mathbb{N}$ oder $E = \{1, \ldots, n\}$, so kann man f als Folge $(f(0), f(1), \ldots)$ bzw. n-Tupel $(f(1), \ldots, f(n))$ verstehen. Gerechnet wird, wie in LA, komponentenweise.

Korollar 8.2 *Für einen R-Modul M mit n-elementiger Teilmenge $E = \{v_1, \ldots, v_n\}$ sind äquivalent*

(1) E ist, als Familie aufgefasst, eine Basis von M.

(2) Die Elemente von M haben eindeutige Darstellung $a = v_1r_1 + \ldots + v_nr_n$ mit $r_i \in R$

(3) Es gibt einen Isomorphismus ϕ von M auf R^n mit $\phi v_i = \boldsymbol{e}_i = (0, \ldots, 1_i, \ldots, 0)^t$

(4) M ist von E frei erzeugter R-Modul

Nochmal ein direkter Beweis. (1) $\Leftrightarrow$ (3): Die Existenz der Darstellung bedeutet Surjektivität der Abbildung, die Eindeutigkeit Injektivität. Die Linearität geht wie in LA. Bei (1) $\Leftrightarrow$ (2) bedeutet die Existenz der Darstellung, dass die v_i erzuegen, die Eindeutigkeit die Unabhängigkeit der v_i. Sei nun M mit 1)-(3) und $\gamma : E \to N$ gegeben. Dann ist

$$\overline{\gamma}(\sum_i v_i r_i) = \sum_i \gamma(v_i) r_i$$

wohldefinert und man rechnet leicht nach, dass es ein Homomorphismus ist. Gilt (4), und setzt man $\gamma(v_i) = \boldsymbol{e}_i$, so hat man $\phi := \overline{\gamma}$. Andererzeits gib es, wei gerade gesehen $\psi : R^n \to M$ mit $\psi(\boldsymbol{e}_i) = v_i$. Also sind ϕ uns ψ nvers zueinander. □ Normalformenmethode: Für die Addition wie bei kommutativen Monoiden nur mit $k_i, l_i \in R$. Hier ist $kg + lg = (k + l)g$ durch die Modulgesetze garantiert. Das allgemeine Distributivgesetz beweise man als Übung. Dann ist klar, wie man die Multiplikation mit Skalaren erklären muss.

Für Vektorräume kennen wir aus der Linearen Algebra die komplette Strukturtheorie. Sie ist dadurch gekennzeichnet, dass jeder Vektorraum frei erzeugt ist, dass alle Varianten des Begriffs Basis äquivalent sind und dass Basen gleich groß sind. R-Moduln über beliebigen Ringen sind nicht mehr so langweilig,

Ist R ein Integriätsbereich und M ein freier R-Modul, so gibt es einen Vektorraum V über dem Quotientenkörper Q von R, so dass M Untergruppe von V ist, die Multiplikation von Skalaren aus R in V wie in M ausgeführt wird und V von M erzeugt wird. Denkt man $M = R^n$ so wähle man $V = Q^n$. Es folgt, dass jede Basis von M eine Basis von V ist (weil aus $\sum_i e_i \frac{r_i}{s_i} = 0$ nach Durchmultiplizieren mit $s = \prod_i s_i$ folgt $\sum_i e_i \frac{sr_i}{s_i} = 0$, also $sr_i = 0$ und $r_i = 0$). Also sind alle Basen von M gleich groß. Die Elemenetanzahl n heisst der *Rang* des freien Moduls, Aber: weder minimale Erzeugendensysteme noch maximal unabhängige Mengen müssen Basen sein, auch wenn es eine Basis gibt. Z.B. ist in $\mathbb{Z}$ (mit Basis $\{1\}$) die Menge $\{2, 3\}$ minimal erzeugend und $\{2\}$ maximal unabhängig, aber keine eine Basis. Dageben besitzt der $\mathbb{Z}$-Modul $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ überhaupt keine Basis.

8.5 Umformungen

Wir betrachten folgende *Umformungen* für Familien $a_i, i \in I$ von Elementen eines R-Moduls M:

- Simultane Addition von Vielfachen eines Erzeugers zu anderen:
  Für $i_0 \in I$, $i_0 \notin J \subset I$ und $r_j \in R$ setze $b_i := \begin{cases} a_i + a_{i_0} r_i & i \in J \\ a_i & i \notin J \end{cases}$
- Multiplikation eines Erzeugers mit einer Einheit:
  Für $i_0 \in I$ und $r \in R^*$ setze $b_i := \begin{cases} a_{i_0} r & i = i_0 \\ a_i & i \neq i_0 \end{cases}$
- Vertauschen: Für eine Permutation σ von I setze $b_i := a_{\sigma(i)}$, $i \in I$
- Weglassen von $a_i = 0$

Lemma 8.3 *Die Umformungen ändern nichts am Erzeugnis. Sie überführen Basen in Basen*

Beweis nach Art des Gausses. Es ist klar, dass jedes b_i im Erzeugnis der a_i ist. Umgekehrt gewinnt man die a_i aus den b_i zurück: bei der ersten Umformung $a_i = b_i - b_{i_0} r$ da $b_{i_0} = a_{i_0}$, bei der zweiten $a_{i_0} = b_{i_0} r^{-1}$. Sei nun $a_i, i \in I$ eine Basis und $\sum b_i s_i = 0$. Bei der ersten Umformung bedeutet das

$$0 = \sum_{i \notin J} a_i s_i + \sum_{i \in J} (a_i s_i + a_{i_0} s_i r_i) = \sum_{i \neq i_0} a_i s_i + a_{i_0} t \text{ mit } t = s_{i_0} + \sum_{i \in J} s_i r_i$$

also $s_i = 0$ für $i \neq i_0$ und $t = 0$, da die a_i eine Basis bilden. Es folgt auch $s_{i_0} = 0$. Bei der zweiten Umformung haben wir $0 = a_{i_0} s_{i_0} r + \sum_{i \neq i_0} a_i s_i$, also $s_i = 0$ und $s_{i_0} r = 0$ und somit auch $s_{i_0} = 0 r^{-1} = 0$. Für die dritte Umformung ist's klar, die vierte kann nicht vorkommen, da 0 nie zu einer Basis gehört. □

8.6 Koordinaten

Sei nun F freier R-Modul mit Basis $\alpha : e_1, \ldots, e_n$. Dann können wir die Elemente von F durch ihre Koordinatenspalten beschreiben

$$a^\alpha = \begin{pmatrix} a_1^\alpha \\ \vdots \\ a_n^\alpha \end{pmatrix} \Leftrightarrow a = \sum_i e_i a_i^\alpha.$$

Ist F gar R^n, so isst a seine eigene Koordinatenspalte. Im allgemeinen darf man in der jeweiligen Situtation so tun als ob - so sieht man manches leichter. Dann muss man aber wieder auf koordinatenfreies Denken umschalten: Tupelei, d.h. Festklammern an einer einfürallemal gültigen 'Standardbasis' ist ein uralter Hut, der alles wieder unnötig verkompliziert.

Hat man eine Familie von $a_j \in F$, $j \in I$ und formt die um, so bedeutet das, dass man die Koordinatenspalten $(a_j)^\alpha$ ganz entsprechend umzuformen hat (durch komponentenweises Rechnen). Man kann sich die Koordinatenspalten $(a_j)^\alpha$ als Spalten einer Matrix $\mathcal{A}$ denken, besonders dann wenn $I = 1, 2, \ldots$

$$(a_j)^\alpha = \begin{pmatrix} (a_j)^\alpha_1 \\ \vdots \\ (a_j)^\alpha_n \end{pmatrix} = \begin{pmatrix} a^\alpha_{1j} \\ \vdots \\ a^\alpha_{nj} \end{pmatrix}, \quad \mathcal{A} = \begin{pmatrix} a^\alpha_{11} & a^\alpha_{12} & a^\alpha_{13} & \ldots \\ a^\alpha_{21} & a^\alpha_{22} & a^\alpha_{23} & \ldots \\ \vdots & & & \\ a^\alpha_{n1} & a^\alpha_{n2} & a^\alpha_{n3} & \ldots \end{pmatrix}.$$

Die Matrix $\mathcal{B}$ der Koordinatenspalten $(b_j)^\alpha$ erhält man dann durch Multiplikation mit der entsprechenden *Umformungsmatrix* $\mathcal{T}$:

$$\mathcal{B} = \mathcal{A}\mathcal{T}.$$

Ist z.B. $i_0 = 1$, $J = \{2\}$, $\sigma = (12)$ so hat man als $\mathcal{T}$ jeweils

$$\begin{pmatrix} 1 & r & 0 & \ldots \\ 0 & 1 & 0 & \ldots \\ 0 & 0 & 1 & \ldots \\ \vdots & & & \ddots \end{pmatrix}, \quad \begin{pmatrix} r & 0 & 0 & \ldots \\ 0 & 1 & 0 & \ldots \\ 0 & 0 & 1 & \ldots \\ \vdots & & & \ddots \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 0 & \ldots \\ 1 & 0 & 0 & \ldots \\ 0 & 0 & 1 & \ldots \\ \vdots & & & \ddots \end{pmatrix}.$$

Die entsprechenden Spaltenumformungen notieren wir auch mit

$$S2 := S2 + (S1)r, \quad S1 := (S1)r, \quad S1 \leftrightarrow S2.$$

8.7 Koordinatentransformation

Oft ist es angesagt, von der alten Basis $\alpha : e_1, \ldots e_n$ eines freien R-Moduls F zu einer neuen Basis $\beta : f_1, \ldots, f_n$ überzugehen, z.B. durch Anwendung der elementaren Umformungen. Dann können wir die Transformationsmatrix $\mathcal{S}$ als $n \times n$-Matrix wählen und es gilt

Die Spalten von $\mathcal{S}$ sind die Koordinaten der neuen Basis β bgl. der alten α

Welche Beziehung besteht nun zwischen den neuen Koordinaten a^β und den alten Koordinaten a^α eines 'Vektors' $a \in F$? Durch Einsetzen der Linearkombinationen der f_j aus den e_j erhält man sofort

$$\boxed{a^\alpha = \mathcal{S}a^\beta.}$$

Bei obigen Beispielen haben wir für $a = \sum_i f_i a^\beta_i$

$$a = e_1(a^\beta_1 + ra^\beta_2) + \sum_{i \neq 1} e_i a^\beta_i \text{ da } f_2 = e_2 + e_1 r,\ f_i = e_i, i \neq 2$$

$$a = e_1 r a_1^\beta + \sum_{i\neq 1} e_i a_i^\beta \text{ da } f_1 = e_1 r,\ e_i = f_i, i \neq 1$$

$$a = e_1 a_2^\beta + e_2 a_1^\beta + \sum_{i\neq 1,2} e_i a_i^\beta \text{ da } f_1 = e_2,\ f_2 = e_1,\ e_i = f_i, i \neq 1,2.$$

Netterweise sind die Matrizen $\mathcal{S}$ invertierbar mit Inversen

$$\begin{pmatrix} 1 & -r & 0 & \dots \\ 0 & 1 & 0 & \dots \\ 0 & 0 & 1 & \dots \\ \vdots & & & \ddots \end{pmatrix}, \quad \begin{pmatrix} r^{-1} & 0 & 0 & \dots \\ 0 & 1 & 0 & \dots \\ 0 & 0 & 1 & \dots \\ \vdots & & & \ddots \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 0 & \dots \\ 1 & 0 & 0 & \dots \\ 0 & 0 & 1 & \dots \\ \vdots & & & \ddots \end{pmatrix}$$

also können wir auch die neuen Koordinaten durch die alten ausdrücken

$$\boxed{a^\beta = \mathcal{S}^{-1} a^\alpha.}$$

In den Beispielen entstehen also die neuen Koordinaten aus den alten durch die Zeilenumformungen

$$Z1 := Z1 - rZ2, \quad Z1 := r^{-1}Z1, \quad Z1 \leftrightarrow Z2.$$

Allgemeiner haben wir folgende Entsprechung zwischen *Basistransformation* (d.h. Abänderung der Basis), ausgedrückt durch die zugehörigen *Spaltenumformungen* nach 5.3 einerseits, und *Zeilenumformungen* der Koordinatenspalten andererseits

$Si := Si - (Sh)r$	entspricht	$Zh := Zh + rZi$
$Si := (Si)r$	entspricht	$Zi := r^{-1}Zi$
$Sh \leftrightarrow Si$	entspricht	$Zi \leftrightarrow Zh$

Haben wir einen ganzen Haufen $a_j, j \in I$ von Vektoren mit Koordinatenspaltenmatrix $\mathcal{A}$ bzgl. α, so entsteht die neue Koordinatenspaltenmatrix $\mathcal{A}'$ (desselben Haufens!) durch Zeilenumformung

$$\mathcal{A}' = \mathcal{S}^{-1}\mathcal{A}.$$

Man kann die Einführung von Koordinaten bzgl. α auch als Isomorphismus $a \mapsto a^\alpha$ von R auf R^n verstehen, und den Übergang $a^\beta \mapsto a^\alpha$ von den neuen auf die alten Koordinaten als lineare Abbildung $a^\beta \mapsto a \mapsto a^\alpha$ von R^n in sich. Dann gilt für die Einheitstupel $\boldsymbol{e}_j \mapsto f_j \mapsto (f_j)^\alpha$, d.h. $\mathcal{S}$ ist die Matrix dieser linearen Abbildung.

8.8 Präsentierung von Moduln

Der R-Modul M sei durch die Erzeugern $e_1, \dots, e_n$ und die Relationen $a_i \stackrel{!}{=} b_i\, (i \in I)$ (bzw. gleichwertig $w_i = a_i - b_i \stackrel{!}{=} 0$) gegeben, d.h. man rechnet mit R-Modul-Termen in den $e_1, \dots, e_n$ modulo der R-Modulgesetze (was die Operationstafeln von R einschliesst) und der Gleichheiten $w_i = 0$. Da die Modulgesetze erlauben, alles auf Linearkombinationen $\sum_i e_i r_i$ zu reduzieren, können wir annehmen, dass auch die w_i von dieser Form sind. Haben wir keine Relationen gegeben, so rechnen wir nur modulo der R-Modulgesetze und erhalten gerade den freien R-Modul mit Erzeugern $e_1, \dots, e_n$. Es folgt

1 Jede Präsentierung eines R-Moduls mit Erzeugermenge $E = \{e_1, \ldots, e_n\}$ lässt sich äquivalent umformen auf die Gestalt

$$\sum_{i=1}^{n} e_i r_{ij},\ j = 1, 2, 3, \ldots, \quad \mathcal{A} = \begin{pmatrix} r_{11} & r_{12} & r_{13} & \ldots \\ \vdots & & & \\ r_{n1} & r_{n2} & r_{n3} \ldots & \end{pmatrix} \in R^{n \times m}$$

2 Die Matrix $\mathcal{A}$ heisst auch die *Präsentierungsmatrix*

3 Man erhält den zugehörigen Modul M als R^n/U, U erzeugt von den Spalten von $\mathcal{A}$

4 Für invertierbare $\mathcal{S}, \mathcal{T}$ ist $\mathcal{S}^{-1}\mathcal{A}\mathcal{T}$ eine Präsentierung von M bzgl. der Basis $f_1, \ldots, f_n$ deren Koordinatenspalten bzgl. $e_1, \ldots, e_n$ gerade die Spalten von $\mathcal{S}$ sind.

5 Ist $n = 1$ und $\mathcal{A} = (d_1)$, so ist M isomorph zu R/dR wobei $dR = \{dr \mid r \in R\}$

6 Ist die Präsentierungsmatrix eine Diagonalmatrix mit Diagonaleinträgen $d_1, \ldots, d_n$, so ist M isomorph zu

$$R/d_1R \times \ldots \times R/d_nR$$

Zu 6: Sei U der von den $e_1d_1, \ldots, e_nd_n$ erzeugte Untermodul von R^n und $\pi : R^n \to R^n/U$ und $\pi_i : R \to R/d_iR$ die kanonischen Projektionen und

$$\psi : R^n \to R/d_1R \times \ldots \times R/d_nR \text{ mit } \psi \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} = \begin{pmatrix} r_1[\mathsf{mod\ d_1R}] \\ \vdots \\ r_n[\mathsf{mod\ d_nR}] \end{pmatrix}$$

Dann ist ψ offensichtlich ein surjektiver Homomorphismus. Ausserdem

$$\begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} \in \mathsf{Kern}(\pi) \Leftrightarrow \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} = \sum e_i d_i s_i = \begin{pmatrix} d_1 s_1 \\ \vdots \\ d_n s_n \end{pmatrix} \Leftrightarrow$$

$$\Leftrightarrow r_1 \in d_1R, \ldots, r_n \in d_nR \Leftrightarrow \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} \in Kern\psi$$

Also hat man einen Isomorphismus $\chi : R^n/U \to R/d_1R \times \ldots \times R/d_nR$ nach dem Homomorphiesatz.

Wir werden zeigen, dass für euklidische Ringe R ein Präsentierung immer in eine wie in 6. umformem kann und somit das Wortproblem lösen.

8.9 Tensorprodukt

Analog kann man Präsentierungen mit beliebiger Erzeugendenzahl betrachten. Ein Beispiel ist das *Tensorprodukt* $A \otimes B$ zweier R-Moduln A, B. Schreiben wir sugestiver $a \otimes b = (a, b)$ für Paare, so ist das der R-Modul mit Präsentation

$$E = \{a \otimes b \,|\, a \in A, b \in B\}$$

$$(a + a') \otimes b \stackrel{!}{=} a \otimes b \stackrel{!}{=} a' \otimes b,\ a \otimes (b + b') \stackrel{!}{=} a \otimes b + a \otimes b',\ (ar) \otimes b \stackrel{!}{=} (a \otimes b)r \stackrel{!}{=} a \otimes br)$$

d.h. man will mit $\otimes$ bilinear rechnen.

0 Für alle, die es genauer wissen wollen

Nocheinmal Termstrukturen (zunächst am Beispiel der Monide), Gleichungsaxiome und freie Strukturen sowie Deatils zum Erzeugen von Kongruenzen.

0.1 Terme

Für algebraische Strukturen vom Typ der Monoide, kann man *Terme in den paarweise veschiedenen Variablen* `[pairwise distinct variables]`

- Jedes x_i ist ein Term
- e ist ein Term
- Sind s und t Terme, so auch $(s \cdot t)$
- Das ist alles `[that's all]`: nur was so entsteht ist ein Term

Wir haben also die Menge der Terme über $x_1, \ldots, x_n$ als Teilmenge `[subset]` der Wortmonoids mit Alphabet $\{x_1, \ldots, x_n, e, \cdot, (,)\}$ eingeführt und vorausgesetzt, dass die "Symbole" $e, \cdot, (,)$ unter den "Variablen" x_i nicht vorkommen. Wir schreiben auch $t(x_1, \ldots, x_n)$ um auf die Auflistung der Variablen hinzuweisen. Die Terme bilden eine algebraische Struktur vom Typ der Monoide mit Konstante e und Multiplikation $(s, t) \mapsto (s \cdot t)$.

Dass ein Wort w ein Term ist, weist man dadurch nach, dass man einen *Herleitungsbaum* `[derivation tree]` für w angibt. Ein solcher Herleitungsbaum ist insbesondere ein *beschrifteter gerichteter Wurzel-Graf* `[rooted graph]`, d.h. eine Menge V von "Knoten' `[vertices]` ', einer Menge $P \subseteq V \times V$ von "Pfeilen" `[arrows]` , einem ausgezeichneten Knoten, der "Wurzel" `[root]` und einer Abbildung σ, die jedem Knoten ein Wort zuordnet `[attaches]`. Was ein Herleitungsbaum für einen Term ist, ergibt sich nach folgenden Regeln

- Eine isolierte `[isolated]` mit x_i bzw. e beschriftete `[labeled]` Wurzel (ohne Pfeil) ist ein Herleitungsbaum von Tiefe `[depth]` 0 für x_i bzw. e und ihr einziges Blatt.
- Sind B_s bzw. B_t Herleitungsbäume für s bzw. t von Tiefe m_s bzw. m_t und sind ihre Knotenmengen disjunkt `[disjoint]` , so erhält man einen Herleitungsbaum für $(s \cdot t)$ von Tiefe $\max\{m_s.m_t\} + 1$, indem man B_s und B_t vereinigt (inklusive Pfeilen und Beschriftung), eine neue Wurzel w hinzufügt, diese mit $(s \cdot t)$ beschriftet und Pfeile (w, w_s) und (w, w_t) zu den (ehemaligen) Wurzeln von B_s bzw. B_t hinzufügt. Die Menge der Blätter `[leaves]` ergibt sich als Vereinigung `union` der Blattmengen von B_s und B_t.

0.2 Induktion

Will man etwas über Terme beweisen, so bedient man sich am besten des folgenden Prinzips der *Induktion über den Termaufbau* `[induction on term complexity]`, das als eine Präzisierung von "Das ist alles" verstanden werden kann.

Prinzip 0.1 *Sei $A(t)$ eine Aussage* `[statement]` *über Terme t und gelte*

- *$A(x_i)$ für jede Variable x_i sowie $A(e)$ (Verankerung* `[basis]` *)*

- *Für alle Wörter s, t gilt: Wenn $A(s)$ und $A(t)$ gelten (Induktionsannahme* `[inductive assumption/ hyothesis]`*, so gilt auch $A((s \cdot t))$ (Induktions-Schritt* `[inductive step]`*).*

Dann gilt $A(t)$ für alle Terme t.

Lemma 0.2

- *Jeder Term ist von der Form x_i, e oder $(s \cdot t)$ mit passenden* `[suitable]` *Termen s, t*
- *Ist der Term s Präfix des Terms t oder umgekehrt* `[or conversely]` *, so $s = t$.*

Beweis. Die erste Behauptung `[claim]` folgt trivial mit Induktion. Die zweite zeigen wir durch Induktion über den Aufbau von s. Die Verankerung mit $s = x_i$ bzw. $s = e$ ist offensichtlich `[obviously]`. Sei nun $s = (s_1 \cdot s_2)$ und die Behauptung für s_1 und s_2 angenommen `[assumed]`. Ist `[if is]` s Präfix von t oder umgekehrt, so muss t von der Form $t = (t_1 \cdot t_2)$ sein und daher s_1 Präfix von t_1 sein oder umgekehrt. Also $s_1 = t_1$. Es folgt, dass s_2 Präfix von t_2 oder umgekehrt. Also $s_2 = t_2$ und damit $s = t$. □

0.3 Termauswertung

Der Zweck der Terme (vom Typ der Monoide) ist, dass sie bei Vorgabe einer algebraischen Struktur A vom Typ der Monoide und einer Liste $a_1, \ldots, a_n$ von Elementen von Elementen von A auf eindeutige Weise ausgewertet werden `[evaluated]` können

$$t(x_1, \ldots, x_n) \mapsto t^A(a_1, \ldots, a_n) \in A$$

so, dass

(1) $x_i^A(a_1, \ldots, a_n) = a_i$

(2) $e^A(a_1, \ldots, a_n) = e_A$

(3) $(s \cdot t)^A(a_1, \ldots, a_n) = s^A(a_1, \ldots, a_n) \cdot_A t^A(a_1, \ldots, a_n)$

Dass es höchstens eine `[at most one]` solche Abbildung ϕ geben kann, folgt leicht mit Induktion. Angenommen, ψ sei auch eine. Dann $\psi(x_i) = a_i = \phi(x_i)$ und $\psi(e) = e_A = \phi(e)$ nach (1-2). Im Induktionsschritt sei $\psi(s) = \phi(s)$ und $\psi(t) = \phi(t)$ angenommen. Es folgt mit (3): $\psi((s \cdot t)) = \psi(s) \cdot_A \psi(t) = \phi(s) \cdot_A \phi(t) = \phi(s \cdot t)$.

Um die Existenz einer solchen Abbildung zu beweisen, muss man sich mehr anstrengen. Das folgende, leider auch in anderen Zusammenhängen sehr beliebte "Argument" `[reasoning]` tuts jedenfalls nicht. "Wir machen Ordnungs-Induktion `[order induction]` über die (Wort) Länge `[length]` der Terme. Induktionsverankerung: Bei Länge 1. haben wir einen Term der Form x_i bzw. e und den eindeutig bestimmten Wert a_i bzw. e_A. Induktionsschritt: Sei $n > 1$ und gelte die Behauptung für alle Terme von Länge $< n$. Ein Term der Länge $n > 1$ ist von der Form $(s \cdot t)$ und s, t habe Länge $< n$. Also sind die Werte von s und t eindeutig bestimmt, also auch der von $(s \cdot t)$.

Die Klammern kommen in diesem "Argument" nicht vor, das "Argument" müssste also auch für ungeklammerte "Terme" gelten. Als Gegenbeispiel `[counterexample]` nehmen wir $x_1 \cdot x_2 \cdot x_3$ und versuchen, das in $\mathbb{Z}$ mit der Subtraktion auszuwerten für $a_1 = 0, a_2 = a_3 = 1$. Wir erhalten die zwei Auswertungen $(0-1)-1 = -2$ und $0-(1-1) = 0$. Mit viel gutem Willen

kann man allenfalls herauslesen, dass es, wie oben gezeigt, höchstens eine Abbildung mit (1-3) gibt bzw. dass es eine für alle Terme definierte "mehrwertige Abbildung" `[multivalued map]` (d.h. Relation ρ zwischen Termen und Elementen von A) gibt. Diese Relation ist durch einen Erzeugungsprozess `[generation process]` induktiv definiert:

(4) $x_i \,\rho\, a_i$,

(5) $e \,\rho\, e_A$

(6) Aus $s \,\rho\, a$ und $t \,\rho\, b$ ergibt sich $(s \cdot t) \,\rho\, a \cdot_A b$

Das Problem liegt bei der Wohldefiniertheit `[well definedness]` der gesuchten Abbildung. Diese erfordert i.A. die Eindeutigkeit `[uniqueness]` der Herleitungen im Erzeugungsprozess. Diese drückt sich hier so aus

Lemma 0.3 *(Peano)*

(P1) $x_i \neq e$, $x_i \neq (s \cdot t)$, $e \neq (s \cdot t)$ *für alle* i *und Terme* s, t

(P2) $(s \cdot t) = (s' \cdot t') \Rightarrow\ s = s'$, $t = t'$ *für alle Terme* s, t, s', t'

Beweis. (P1) ist klar. (P2) folgt aus Lemma ??. □ Nun können wir die Auswertung `[evaluation]` problemlos durch (1-3) "rekursiv" defineren, d.h. wir können induktiv beweisen, dass die induktiv definierte Relation in der Tat eine wohldefinierte `[well defined]` Abbildung ist. Wir zeigen durch Induktion über den Herleitungsprozess für $s \,\rho\, a$

$$\text{aus } s \,\rho\, a \text{ und } s \,\rho\, a' \text{ folgt } a = a'$$

Entsteht $s \,\rho\, a$ nach (4), so $s = x_i$ für ein i und $a = a_i$. Wegen (P1) kann dann auch $x_i \,\rho\, a'$ nur nach (4) entstanden sein und weil die x_j paarweise verschieden sind, haben wir $a' = a_i$.

Entsteht $s \,\rho\, a$ nach (5), so $s = e$ und $a = e_A$. Wegen (P1) kann dann auch $e \,\rho\, a'$ nur nach (5) entstanden sein und wir haben $a' = e_A$.

Entstehe nun $(s \cdot t) \,\rho\, c$ nach (6). d.h. $c = a \cdot_A b$ mit $s \,\rho\, a$ und $t \,\rho\, b$ und für letztere gelte schon die Behauptung. Wegen (P1) kann auch $(s \cdot t) \,\rho\, c'$ nur nach (6) entstanden sein, d.h. $(s \cdot t) = (s' \cdot t')$ mit $c' = a' \cdot_A b'$, $s' \,\rho\, a'$ und $t' \,\rho\, b'$. Wegen (P2) gilt $s = s'$ und $t = t'$. Mit der Induktionsannahme folgt $a = a'$ und $b = b'$. Also $c = c'$. □

Korollar 0.4 *Es gibt eine Abbildung* τ *von der Menge der Terme in die Menge* $\mathbb{N}$ *so. dass jeder Herleitungsbaum des Terms* t *Tiefe* $\tau(t)$ *hat.*

Beweis. $\tau(t(x_1, \ldots, x_n)) = t^{\mathbb{N}}(0, \ldots, 0)$ wobei $\mathbb{N}$ mit $(a, b) \mapsto \max\{a.b\}$ und Konstante 0. □

Wenn wir Strukturen vom Typ der Gruppen betrachten, kommt bei der Termerzeugung die folgende Regel hinzu, entsprechend für die Herleitunsbäume und bei den Eindeutigkeitsaussagen

- Ist t ein Term vom Typ der Gruppe, so auch ιt
- Ist B_t ein Herleitungsbaum für t, so erhält man einen Herleitungsbaum für ιt, indem man eine neue Wurzel w und Pfeil (w, w_t) hinzufügt und w mit ιt beschriftet.
- (P1) $\iota u \neq x_i$, e , $(s \cdot t)$ und (P2) $\iota u = \iota u' \Rightarrow u = u'$ für alle i und Terme s, t, u

0.4 Termstrukturen

Bis jetzt sind wir, mit gutem Recht, mit Termen naiv umgegangen und haben meist exemplarisch argumentiert. Wenn wir jedoch aus Termen reale mathematische Gegenstände zusammenbasteln wollen, wie etwa die Polynomringe, ist ein wenig mehr Präzision angesagt.

Mit der Buchstabenrechung im Sinn, gehen wir aus von einem Alphabet E von *Erzeugendensymbolen* (wir benuzten als alias g, g_i wie 'Generator', einige dürfen mit richtigem Namen auch $x, y, \ldots$ heissen und später die Rollen von Unbestimmten spielen) und bilden dazu die *Termstruktur* $T(E)$ zu den vorgegebenen fundamentalen Operationssymbolen

- Jedes g aus E ist ein Term in $T(E)$
- Sind $t_1, \ldots, t_n$ Terme in $T(E)$ und ist f ein n-stelliges fundamentales Operationssymbol, so ist auch $f(t_1, \ldots, t_n)$ ein Term in $T(E)$
- Nur was man so erhält ist ein Term in $T(E)$
- Terme sind nur dann gleich, wenn sie formal identisch sind.
- Terme kann man stets auf eindeutige und natürliche Weise auswerten

Wir verschaffen uns also 'symbolische' mathematische Objekte, die zur Beschreibung 'konkreter' mathematischer Objekte taugen sollen. Wer mit diesem 'symbolischen' Geschwätz nichts anfangen kann, denke bei E einfach eine Menge. Und bei den Operationssymbolen ebenfalls an eine Menge Ω zusammen mit einer Abbildung von Ω in $\mathbb{N}$, die für jedes 'Operationsssymbol' $f \in \Omega$ die vorgesehene Stelligkeit angibt, das heisst dann *Signatur* oder *Typ*. Die Konvention $E \cap \Omega = \emptyset$ erweist sich als nützlich.

Die Gesamtheit $T(E)$ der symbolischen Objekte wird zur algebraischen Struktur, passend zu den gegebenen Operationssymbolen, wenn man $(t_1, \ldots, t_n) \mapsto f(t_1, \ldots, t_n)$ als Operation $f^{T(E)}$ auf $T(E)$ auffasst. Damit kann man die ersten drei Bedingungen prägnant so formulieren

$$\boxed{T(E) \text{ wird vom Alphabet } E \text{ erzeugt bzgl. der Operationen } f^{T(E)}}$$

Um der vierten bzw. fünften Bedingung eine präzise Bedeutung zu geben, haben wir drei mögliche Wege:

Implementierung, interne Charakterisierung bzw. externe Charakterisierung.

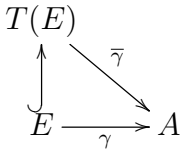
Dem Umstand, dass Charakterisierung nur bis auf Isomorphie möglich ist, entspricht das Vorhandensein verschiedenartiger Implementierungen.

- Implementierungen
  - Wir fassen $T(E)$ als Teilmenge des Wortmonoids auf dem um die Operationssymbole, Klammern und Komma erweiteterten Alphabet. Nämlich als Erzeugnis von E bzgl. der Operationen $f^{T(E)}$ wobei $f^{T(E)}(t_1, \ldots, t_n)$ das Wort $f(t_1, \ldots, t_n)$ ist. Auf Klammern und Kommas kann man auch verzichten, andererseits für ausgewählte 2- bzw. 1-stellige Operationen Infix- bzw. Exponentialschreibweise benutzen
$$(t_1, t_2) \mapsto (t_1 + t_2), \quad t \mapsto (t^{-1})$$

  - Terme als gelabelte Bäume wie in Inf.

- Interne Charakterisierung
  - $T(E)$ ist erzeugt von E
  - $f^{T(E)}(t_1, \ldots, t_n) \notin E$
  - $f^{T(E)}(t_1, \ldots, t_n) = \hat{f}_T(s_1, \ldots, s_{\hat{n}}) \Rightarrow f = \hat{f}$, $n = \hat{n}$, $t_1 = s_1, \ldots, t_n = s_n$ für alle fundamentalen Operationssymbole $f, \hat{f}$ und $t_i, s_i \in T(E)$

- Externe Charakterisierung: Zu jeder algebraischen Struktur A des betrachteten Typs und Abbildung $\gamma : E \to A$ gibt es einen eindeutig bestimmten Homomorphismus $\overline{\gamma} : T(E) \to A$ mit $\overline{\gamma}|E = \gamma$.



- $T(E)$ existiert und ist eindeutig bestimmt bis auf einen E elementweise festlassenden Isomorphismus

Denkt man Terme als konkrete Objekte, so deutet man durch die Schreibweise $t(g_1, \ldots, g_m)$ an, dass alle in t vorkommenden Erzeuger $g \in E$ schon in der Liste $g_1, \ldots, g_m$ enthalten sind. Der Homomorphismus $\overline{\gamma}$ heisst dann auch *Termauswertung* zur Einsetzung bzw. Belegung $g_i \mapsto a_i = \gamma(g_i) \in A$, $g_i \in E$ und wird so geschrieben

$$\overline{\gamma}t = t^A(a_1, \ldots, a_m)$$

und die Homomorphiebedingung liest sich so

$$f(t_1, \ldots, t_n)^A(a_1, \ldots, a_m) = f^A(t_1^A(a_1, \ldots, a_m), \ldots t_n^A(a_1, \ldots, a_m))$$

und gilt sogar für beliebige Terme $s(x_1, \ldots x_n)$ anstelle von $f(x_1, \ldots, x_n)$

$$s(t_1, \ldots, t_n)^A(a_1, \ldots, a_m) = s^A(t_1^A(a_1, \ldots, a_m), \ldots t_n^A(a_1, \ldots, a_m))$$

wie man leicht exemplarisch oder durch Induktion über den Aufbau von s beweist. Das Erzeugnis von $\gamma(E)$ in A kann man nun auch mit einer festen Einsetzung von Elementen aus A in die Terme, nämlich der Abbildung γ, schreiben.

Korollar 0.5

$$\mathsf{Spann}(\gamma(E)) = \{t^A(\gamma g_1, \ldots, \gamma g_n) \mid t \in T(E)\} = \overline{\gamma}(T(E))$$

Ist $\phi : A \to B$ ein surjektiver Homomorphismus und wird A von G erzeugt, so wird B von $\phi(G)$ erzeugt.

Beweis. Das Bild $\overline{\gamma}(T(E))$ ist eine Unterstruktur von A und offensichtlich im Erzeugnis von $\gamma(E)$ enthalten. Für die zweite Behauptung wähle man $\gamma : E \to G$ surjektiv (z.B. $E = G$ und $\gamma = id_E$) und $\gamma_1 = \phi \circ \gamma : E \to B$. Dann gilt $\phi \circ \overline{\gamma} = \overline{\gamma}_1$ wegen der Eindeutigkeit und

$$B = \phi(A) = \phi(\overline{\gamma}(T(E))) = \overline{\gamma}_1(T(E)) = \mathsf{Spann}(\gamma_1(E)) = \mathsf{Spann}(\phi(G)) \quad \square$$

Um die Charakterisierungen von $T(E)$ zu beweisen, stellen wir fest

- Es gibt eine Implementierung, die der internen Charakterisierung genügt
- Erfüllt $T(E)$ die interne Charakterisierung, so auch die externe
- Durch die externe Charakterisierung ist $T(E)$ bis auf Isomorphie bestimmt

1 als Übung. Zu 2: Der Graph von $\overline{\gamma}$ sei die vom Graphen von γ erzeugte Unterstruktur von $T(E)\times A$. Dass $\overline{\gamma}$ dann eine wohldefinierte Abbildung ist, folgt aus der internen Charakterisierung. Die Homomorphie-Eigenschaft ergibt sich aus der Unterstruktur-Eigenschaft. $\overline{\gamma}|E = \gamma$ ist klar und die Eindeutigkeit folgt aus Lemma 3.16 Zu 3: Sei die externe Charakterisierung für $T(E)$ und $T'(E)$ erfüllt. Dann kamm man die identische Abbildung $\gamma = id_E : E \to E$ sowohl zu einem Homomorphismus $\phi : T(E) \to T'(E)$ wie auch einem Homomorphismus $\psi : T'(E) \to T(E)$ fortsetzen. $\psi \circ \phi : T(E) \to T(E)$ ist dann ein Homomorphismus $\overline{\gamma} : T(E) \to T(E)$ mit $\overline{\gamma}|E = \gamma$. Die identische Abbildung $id_{T(E)}$ ist aber auch so einer. Wegen der vorausgesetzten Eindeutigkeit folgt $\psi \circ \phi = id_{T(E)}$. Analog $\phi \circ \psi = id_{T'(E)}$. Also sind ϕ und ψ Isomorphismen nach Lemma 3.13 □

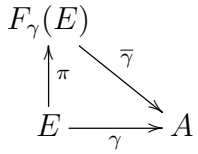
0.5 Buchstabenrechnung

Wollen wir die Buchstabenrechung im Rahmen der 'Strukturmathematik' sehen, so bilden wir durch Abstraktion die kanonische Projektion

$$\pi : T(E) \to F_\Gamma(E) = T(E)/\!\sim_\Gamma, \quad t \mapsto \pi t = t[\mathsf{mod}\ \sim_\Gamma] =: \widetilde{t}$$

auf die Faktorstrukur, die von E unter den Gesetzen Γ *frei erzeugte Struktur*. Besteht Γ aus den Gesetzen für (kommutative) Monoide, R-Moduln, kommutative Ringe bzw. R-Algebren, so sprechen wir auch von freiem (kommutativem) Monoid, freiem R-Modul, freiem kommutativen Ring bzw. R-Algebra.

- $F_\Gamma(E)$ wird erzeugt von der Menge $\widetilde{E} = \{\widetilde{g} \mid g \in E\}$
- $F_\Gamma(E)$ erfüllt Γ
- *Fortsetzungseigenschaft:* Zu jeder Γ erfüllenden algebraischen Struktur A (des gebenenen Typs) und Abbildung $\gamma : E \to A$ gibt es einen eindeutig bestimmten Homomorphismus $\widetilde{\gamma} : F_\Gamma(E) \to A$ mit $\widetilde{\gamma} \circ \pi = \gamma$, d.h. $\forall g \in E.\ \widetilde{\gamma}\widetilde{g} = \gamma g$



- Die freie algebraische Struktur ist durch E und Γ bis auf Isomorphie eindeutig bestimmt: Erfüllt $F'_\Gamma(E')$ die Gesetze Γ und hat man eine Abbildung $\pi' : E' \to F'_\Gamma(E)$ mit der Fortsetzungseigenschaft und eine Bijektion $\varepsilon : E \to E'$, so gibt es einen Isomorphismus

$$\phi : F_\Gamma(E) \to F'_\Gamma(E) \quad \text{mit } \phi \circ \pi = \pi' \circ \varepsilon \text{ d.h. } \forall g \in E.\ \phi\pi g = \pi'\varepsilon g$$

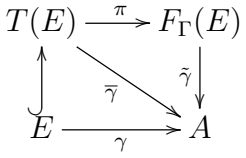
- Haben wir so einen Isomorphismus, so ist auch $F'_\Gamma(E')$ von E unter Γ frei erzeugt.

Beweis. Die erste Beh. gilt nach Kor. ??. Ist $\forall \mathbf{x}.\ s(\mathbf{x}) \stackrel{!}{=} t(\mathbf{x})$ ein Gesetz in Γ, und sind $a_i \in F = F_\Gamma(E)$ so gibt es $t_i \in T(E)$ mit $\pi t_i = a_i$. Nach der Definition von $\sim_\Gamma$ gilt

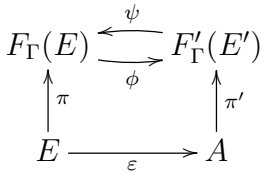
$$s(t_1, \ldots, t_n) \sim_\Gamma t(t_1, \ldots, t_n)$$

$$s^F(a_1, \ldots, a_n) = \pi\, s(t_1, \ldots, t_n) = \pi\, t(t_1, \ldots, t_n) = t^F(a_1, \ldots, a_n)$$

Da Γ in A erfüllt ist, haben wir $\overline{\gamma} s_i(g_1, \ldots, g_n) = s_i^A(\gamma g_1, \ldots, \gamma g_n) = t_i^A(\gamma g_1, \ldots, \gamma g_n) = \overline{\gamma} t_i(g_1, \ldots, g_n)$ d.h. der Kern von $\overline{\gamma}$ ist feiner als die Kongruenz $\sim_\Gamma$. Daher gibt es $\widetilde{\gamma}$ nach dem Homomorphiergänzungsatz, nach Lemma 3.16 ist es eindeutig bestimmt.



Die Fortsetzungseigenscgaft für $F_\Gamma(E)$ garantiert einen Homomorphismus $\phi : F_\Gamma(E) \to F'_\Gamma(E')$ mit $\phi \circ \pi = \pi' \circ \varepsilon$. Umgekehrt garantiert die Fortsetzungseigenschaft für $F'_\Gamma(E')$ einen Homomorphismus $\psi : F'_\Gamma(E') \to F_\Gamma(E)$ mit $\psi \circ \pi' = \pi \circ \varepsilon^{-1}$. Dann ist $\psi \circ \phi$ ein Homomorphismus $\chi : F_\Gamma(E) \to F_\Gamma(E)$ ein Homomorphismus mit $\chi \circ \pi = \pi$. Die identische Abbildung auf $F_\Gamma(E)$ ist auch so einer, also $\psi \circ \phi = id_{F(\Gamma}(E)$. Ebenso $\phi \circ \psi = id_{F'_\Gamma(E')}$. Also ist $\phi : F_\Gamma(E) \to F'_\Gamma(E')$ ein Isomorphismus. □



Freie Strukturen gibt es auch, wenn die Gesetze die folgende allgemeinere Form haben

$$\forall \mathbf{x}.\ (s_1(\mathbf{x}) \stackrel{!}{=} t_1(\mathbf{x}) \text{und } \ldots \text{ und } s_n(\mathbf{x}) \stackrel{!}{=} t_n(\mathbf{x}) \ \Rightarrow s(\mathbf{x}) \stackrel{!}{=} t(\mathbf{x}))$$

und der Beweis ist fast derselbe. Probleme treten dann auf, wenn es Alternativen gibt, z.B bei nullteilerfreien Ringen. Hier ist das Axiom $\forall x \forall y.\ (xy = 0 \Rightarrow x = 0 \text{ oder } y = 0)$. Verlangt man zusätzlich Kommutativität und $6x = 0.$ so müsste der freie Ring mit leerer Erzeugendenmenge homomorphes Bild von $\mathbb{Z}/6\mathbb{Z}$ sein und $\mathbb{Z}/2\mathbb{Z}$ ebenso wie $\mathbb{Z}/3\mathbb{Z}$ als homomorphe Bilder haben. Also müsste es $\mathbb{Z}/6\mathbb{Z}$ sein wo man mit $2 \cdot 3 = 0$ einen Widerspruch zur Nullteilerfreiheit hat.

0.6 Normalformen

Wir haben nun Existenz und Eindeutigkeit der freien algebraischen Struktur $F_\Gamma(E)$ durch triviales algebraisches Geschwätz bewiesen, aber wissen sonst so gut wie nichts über sie. Die Frage aber ist, welche Identitäten denn nun gelten und wie wir sie herleiten können. Die folgenden Aussagen sind äquivalent (wir schreiben $t[a_1, \ldots, a_n]$ statt $t^A(a_1, \ldots, a_n)$ wenn klar ist, in welcher Struktur A ausgewertet wird)

- $s[\widetilde{g}_1, \ldots, \widetilde{g}_n] = t[\widetilde{g}_1, \ldots, \widetilde{g}_n]$ in $F_\Gamma(E)$
- $s(g_1, \ldots, g_n) \sim_\Gamma t(g_1, \ldots, g_n)$

- Das Gleichheits-Gesetz $\forall x_1 \ldots \forall x_n.\ s(x_1, \ldots, x_n) \stackrel{!}{=} t(x_1, \ldots, x_n)$ folgt aus den Gesetzen Γ

Soviel Gleichheit wie nötig, soviel Freiheit wie möglich

Beweis. $3 \Rightarrow 1 \Leftrightarrow 2$ nach Definition. $1 \Rightarrow 3$: Sind $a_i \in A$ gegeben, so setze $\gamma g_i = a_i$. Dann $s[a_1, \ldots, a_n] = \widetilde{\gamma} s[\widetilde{g}_1, \ldots, \widetilde{g}_n] = \widetilde{\gamma} t[\widetilde{g}_1, \ldots, \widetilde{g}_n] = t[a_1, \ldots, a_n]$. □

Lemma 0.6 *Für eine Teilmenge $N_\Gamma(E) \supseteq E$ von $T(E)$ sind äquivalent*

- *$N_\Gamma(E)$ ist Repräsentantensystem von $\sim_\Gamma$*
- *Jedes Element a von $F_\Gamma(E)$ hat eine eindeutige Darstellung $a = t[\widetilde{g}_1, \ldots, \widetilde{g}_m]$ mit $t(g_1, \ldots, g_m) \in N_\Gamma(E)$*
- *Es gibt eine algebraische Struktur A und Abbildung $\gamma : E \to A$, sodass gilt*
  - *A erfüllt Γ*
  - *Jedes a in A hat eindeutige Darstellung $a = t[\gamma g_1, \ldots, \gamma g_m]$ mit $t(g_1, \ldots, g_m) \in N_\Gamma(E)$*
  - *Die Struktur von A ergibt sich aus Γ, d.h. wenn immer $f^A(a_1, \ldots, a_n) = t[\gamma g_1, \ldots, \gamma g_m]$ mit $a_i = t_i[\gamma g_1, \ldots, \gamma g_m]$ und $t_i, t \in N_\Gamma(E)$ liegt's daran, dass $t \sim_\Gamma f(t_1, \ldots, t_n)$*
- *Zu jedem Term $s \in T(E)$ gibt es $t \in N_\Gamma(E)$ mit $s \sim_\Gamma t$ und man kann auf $N_\Gamma(E)$ Operationen f^N so definieren, dass*
  - *man eine algebraische Struktur erhält, die Γ erfüllt und von E erzeugt wird*
  - *$f^N(t_1, \ldots, t_n) \sim_\Gamma f(t_1, \ldots, t_n)$ für $t_i \in N_\Gamma(E)$*

Man nennt dann $N_\Gamma(E)$ auch ein *System von Termen in Normalform modulo* Γ. Beweis. $1 \Leftrightarrow 2 \Rightarrow 3$ ist trivial. $3 \Rightarrow 4$: $\overline{\gamma}|N_\Gamma(E)$ bildet $N_\Gamma(E)$ bijektiv auf A ab und man definiere f^N so, dass es ein Isomorphismus wird. Gilt (4), so ist $\pi|N_\Gamma(E)$ surjektiv und ein Homomorphismus. Ausserdem lässt sich die identische Abbildung $\gamma : E \to N_\gamma(E)$ zu einem surjektiven Homomorphismus $\widetilde{\gamma} : F_\Gamma(E) \to N_\Gamma(E)$ fortsetzen. Dann ist $\pi \circ \widetilde{\gamma}$ ein Homomorphismus von $F_\Gamma(E)$ in sich, der auf E Identiät ist, also insgesamt Identität. Folglich ist $\pi|N_\Gamma(E)$ auch injektiv, also Isomorphismus und es gilt (2). □

Ein Algorithmus, der für jedes vorgelegte Paar von Termen (korrekt) entscheidet, ob $s(g_1, \ldots, g_n) \sim_\Gamma t(g_1, \ldots, g_n)$ gilt, ist ein *Entscheidungsverfahren für die Gleichungstheorie* von Γ bzw. Lösung des *Wortproblems für freie algebraische Strukturen* $F_\Gamma(E)$. Sowas gibt's, wenn wir die Existenz eines Systems von Normalformen beweisen und zu jedem Term t die zugehörige Normalform t^N berechnen können

$$s \sim_\Gamma t \quad \Leftrightarrow \quad s^N = t^N$$

Das ist insbesondre dann der Fall, wenn wir $N_\Gamma(E)$ und die Operationen f^N effektiv angeben können. Wir können dann t^N rekursiv berechnen

$$g^N = g \text{ für } g \in E, \quad f(t_1, \ldots, t_n)^N = f^N(t_1^N, \ldots, t_n^N)$$

Netterweise geht das für die uns interessierenden Strukturen, z.B. durch konkrete Konstruktion eines A wie im Lemma. Die Alternative besteht in einer genaueren Untersuchung der Herleitungsregeln im Rahmen eines 'Termersetzungssystems'.

Gibt es eine mindestens 2-elementige Struktur, die Γ erfüllt, so folgt dass die Abbildung $g \mapsto \widetilde{g} \in F_\gamma(E)$ $(g \in E)$ injektiv ist, wir uns also die lästige Schlange ersparen können.

9 Polynomring und Quotientenkörper

9.1 Polynomring in einer Unbestimmten

Prinzip 9.1 *Sei R ein kommutativer Ring und A eine kommutative R-Algebra und $x \in A$. Dann sind äquivalent*

- *A ist von $\{x\}$ frei erzeugte kommutative R-Algebra*
- *Die Elemente von A haben eindeutige Darstellung $p = p(x) = r_0x^0 + r_1x^1 + r_2x^2 + \ldots + r_nx^n$ mit $r_i \in R$, $r_n \neq 0$*
- *Die Elemente von A haben eindeutige Darstellung $p = p(x) = r_nx^n + r_{n-1}x^{n-1} + \ldots + r_1x^1 + r_0x^0$ mit $r_i \in R$, $r_n \neq 0$*
- *$M = \{x^k \mid k \in \mathbb{N}\}$ ist von x frei erzeugtes kommutatives (multiplikatives) Monoid und A als R-Modul frei von M erzeugt*

Die Multiplikation ist dann eindeutig bestimmt

$$(*)\ \ (\sum_{i=0}^{n} r_ix^i) \cdot (\sum_{j=0}^{m} s_jx^j) = \sum_{k=0}^{m+n} (\sum_{i+j=k} r_is_j)x^k$$

Wir nennen dann A auch *Polynomring in der Unbestimmten x mit Koeffizienten in (über)* R und schreiben $A = R[x]$.

Korollar 9.2 *Die Abbildung $r \mapsto rx^0$ ist ein injektiver Homomorphismus von R in $R[x]$. Ist B eine R-Algebra und $b \in B$ so gibt es einen eindeutig bestimmten Homomorphismus $\phi : R[x] \to B$ mit $\phi(x) = b$.*

Also kann man R als Unterring von $R[x]$ auffassen. Man spricht bei ϕ auch vom *Einsetzungshomomorphismus* und schreibt

$$\phi(p(x)) = p(b) = \sum_i r_ib^i \ \text{ für } p(x) = \sum_i r_ix^i$$

Dass $R[x]$ freie R-Algebra ist, heißt in der Hauptsache folgendes: Man bilde alle Ausdrücken, die man aus x und den Elementen von R mit den Ringoperationen sinnvoll zusammensetzen kann (Terme). Zwei Ausdrücke sind äquivalent ($t \sim s$), wenn die Gleichheit aus den Axiomen der kommutativen R-Algebren, insbesondere den Operationstafeln von R, hergeleitet werden kann. $\sim$ ist eine Kongruenzrelation und die Faktorstruktur eine kommutative R-Algebra, traditionell der *Polynomring* $R[x]$ über R in der Unbestimmten x genannt - oft wird X statt x benutzt. Insbesondere gibt es zu jedem Ausdruck einen äquivalenten in *Normalform*

$$\sum_{i=0}^{n} a_ix^i = a_nx^n + \ldots + a_1x_1 + a_0 \quad \text{mit } a_i \in R$$

wobei Summanden $0x^k$ nicht angegeben werden müssen. Summen und Produkte überführt man leicht wieder in Normalform

$$\sum_{i=0}^{n} a_ix^i \ + \ \sum_{i=0}^{n} b_ix^i = \sum_{i=0}^{n} (a_i + b_i)x^i$$

$$(\sum_{i=0}^{n} a_i x^i) \cdot (\sum_{j=0}^{m} b_j x^j) = \sum_{k=0}^{n+m} (\sum_{i+j=k} a_i b_j) x^k$$

Insbesondere kann man in Polynome $p(x)$ aus $K[x]$ in jeder K-Algebra B auswerten, d.h. b aus B in $p(x)$ einsetzen um $p(b)$ zu erhalten und es gilt

$$p(b) + q(b) = (p+q)(b), \quad p(b) \cdot q(b) = (p \cdot q)(b)$$

Dass die Konstruktion anch diesem Rezept zur Existenz des Einseztunghomomorphismus äquivalent ist, folgt mit demselben Beweis wie fúr Monoide. Also

Polynome über K sind K-Algebra-Terme modulo der von den K-Algebra-Gesetzen erzwungenen Kongruenzrelation.

Schließlich sind verschiedene Normalformen nicht äquivalent, d.h. wir haben den *Koeffizientenvergleich*

$$\sum_{i=0}^{n} a_i x^i \;=\; \sum_{i=0}^{n} b_i x^i \;\;\Rightarrow\;\; a_0 = b_0, \ldots, a_n = b_n$$

und einen injektiven Homomorphismus von R in $R[x]$, der $a \in R$ auf das konstante Polynom a abbildet.

In Analysis und Numerik darf man unbedenklich Polynome als Polynomfunktionen z.B. $x \mapsto \sum_i a_i x^i$ $(x \in \mathbb{R})$ auffassen, wie wir bald sehen werden. Im Allgemeinen ist das nicht erlaubt: über dem 2-elementigen Körper definiert das Polynom $x + x^2$ die Nullfunktion, ist aber offensichtlich nicht das Nullpolynom.

Um die internen Charaktierisierungen zu beweisen, kann man z.B. für die Folgen $(a_9, \ldots, a_n, 0 \ldots)$ Addition und Multiplikation wie bei den Summen definieren und dann zeigen, dass man eine kommutative R-Algebra und Einbettung $a \mapsto (a, 0, \ldots)$ $(a \in R)$ erhält. Genauer ausgeführt wird dies in Satz ??. Der entscheidende Punkt ist aber, dass die beiden Sichtweisen als 'formale Ausdrücke' der Gestalt $a_0 + a_1 x + \ldots + a_n x^n$ bzw. als Folgen $(a_0, \ldots, a_n, 0, \ldots)$ zusammenpassen. Jede für sich greift zu kurz.

9.2 Grad

Ist $p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \in R[x]$ mit $a_i \in R$ und $a_n \neq 0$ so ist $n = \deg p(x)$ der *Grad* von $p(x)$, die a_i *Koeffizienten* von $p(x)$ und a_n der *Leitkoeffizient*. $\deg 0 := -\infty$.

Proposition 9.3 *Ist R ein Intergritätsbereich, so auch $R[x]$ und es gilt*

$$\deg(p(x)q(x)) = \deg p(x) + \deg q(x).$$

Beweis. Angenommen, $\deg p(x) = n \geq 0$ und $\deg q(x) = m \geq 0$. Dann $a_n b_m \neq 0$, also ist $p(x)q(x) = a_n b_m x^{n+m} + \ldots + a_0 b_0$ nicht das Nullpolynom.

9.3 Polynomdivision

Lemma 9.4 *Sind $p(x)$ und $q(x)$ in $R[x]$ Polynome der Grade $n \geq m$ und ist der Leitkoefizient von $q(x)$ eine Einheit in R, so gibt es Polynome $s(x)$ und $r(x)$ von Grad $n - m$ bzw. höchstens $m - 1$ so, dass $p(x) = s(x)q(x) + r(x)$.*

Beweis und Algorithmus. Zur Berechnung geht man wie bei der Division von Dezimalzahlen vor: setze $c_{n-m} = \frac{a_n}{b_m}$ und $r_1(x) = p(x) - c_{n-m}x^{n-m}q(x)$. Dann hat r_1 höchstens Grad $n-1$ und $p(x) = c_{n-m}x^{n-m}q(x) + r_1(x)$. Man setzt nun das Verfahren mit $r_1(x)$ anstelle von $p(x)$ fort und erhält $r_1(x) = c_{n-m-1}x^{n-m-1}q(x) + r_2(x)$ mit $r_2(x)$ von Grad höchstens $n-2$. Schliesslich erhält man $r_{n-m}(x) = c_0q(x) + r_{n-m+1}(x)$ mit $r(x) = r_{n-m+1}(x)$ von Grad höchstens $m-1$. Fasst man zusammen, so ergibt das $p(x) = (c_{n-m}x^{n-m} + \ldots + c_0)q(x) + r(x)$.

9.4 Nullstellen

In folgenden sei A Integritätsbereich mit Unterring R. Ein Element $\alpha \in A$ heisst eine Nullstelle von $p(x) \in R[x]$, falls $p(\alpha) = 0$ in A. Es ist α Nullstelle von $p(x)q(x)$ genau dann, wenn α Nullstelle von $p(x)$ oder/und $q(x)$ ist.

Korollar 9.5 Abspaltung. *Ist $p(x) \in R[x]$ ein Polynom vom Grad $n > 0$ und $\alpha \in A$ eine Nullstelle in A, so gibt es ein (eindeutig bestimmtes) Polynom $s(x) \in A[x]$ vom Grad $n-1$ so, dass $p(x) = s(x)(x-\alpha)$.*

Beweis. Division mit Rest in $A[x]$ ergibt $p(x) = s(x)(x-\alpha) + r(x)$ mit $\deg r(x) < 1$, also $r(x) = c \in A$ und es folgt $0 = p(\alpha) = c$. □

$x - \alpha$ heisst der Linearfaktor zur Nullstelle α. Hat man $p(x) = q(x)(x-\alpha)^k$ mit $q[\alpha] \neq 0$ (und das ist eindeutig bestimmt), so ist α eine k-fache Nullstelle von $p(x)$.

Korollar 9.6 *Sei R ein Integritätsbereich. Ein Polynom aus $R[x]$ von Grad $n \geq 0$ hat höchstens n verschiedene Nullstellen in A*

Korollar 9.7 *Ist R unendlicher Integritätsbereich, so ist ein Polynom schon eindeutig bestimmt durch die zugehörige* Polynomfunktion *auf R*

$$\alpha \mapsto p[\alpha] \in R \text{ für } \alpha \in R.$$

Lemma 9.8 *Sind die $a_i \in \mathbb{Z}$, so ist jede rationale Nullstelle von $f(x) = a_nx + \ldots + a_0$ von der Form rs^{-1} mit ganzen $r|a_0$ und $s|a_n$*

Beweis. Sei $f[\alpha] = 0$. O.B.d.A. $\alpha = rs^{-1}$ mit r, s teilerfremd. Es folgt

$$0 = s^n f[\alpha] = a_n r^n + s a_{n-1} r^{n-1} + \ldots + s^{n-1} a_1 r + s^n a_0$$

also $r|(a_0 s^n)$ und $s|(a_n r^n)$. Wegen wegen $\mathrm{GGT}(s^n, r) = \mathrm{GGT}(s, r^n) = \mathrm{GGT}(s, r) = 1$ folgen $r|a_0$ und $s|a_n$. □

9.5 Hornerschema

Lemma 9.9 *Zu jedem Polynom $p(x)$ vom Grad n und $\alpha \in R$ gibt es ein Polynom $h(x)$ so, dass*

$$p(x) = h(x)(x-\alpha) + p[\alpha]$$

Beweis. Die Idee hierbei ist, dass

$$p(x) = (\dots((a_n x + a_{n-1})x + a_{n-2})\dots + a_1)x + a_0$$

also kann man $p[\alpha]$ mit weniger Multiplikationen so ausrechnen

a_n	a_{n-1}	$\dots$	a_1	a_0
α	$c_{n-1}\alpha$	$\dots$	$c_1\alpha$	$c_0\alpha$
$c_{n-1} = a_n$	$c_{n-2} = c_{n-1}\alpha + a_{n-1}$	$\dots$	$c_0 = c_1\alpha + a_1$	$p[\alpha] = c_0\alpha + a_0$

Setze

$$h(x) = c_{n-1}x^{n-1} + \dots + c_1 x + c_0.$$

Zum Beweis betrachte man

$$q(x) = (\dots(a_n x + a_{n-1})x + a_{n-2})\dots + a_1 \text{ d.h. } p(x) = q(x)x + a_0.$$

Dann hat man bei der Berechnung von $q[\alpha]$ die Horner-Koeffizienten $c_{n-1}, \dots, c_1$ und es gilt $q[\alpha] = c_0$. Und $c_0\alpha + a_0 = p(\alpha)$. Indem wir für $q(x)$ die Behauptung schon als bewiesen annehmen, folgt

$$\begin{aligned} p(x) = q(x)x + a_0 &= ((c_{n-1}x^{n-2} + \dots + a_1)(x - \alpha) + q[\alpha])x + a_0 \\ &= (c_{n-1}x^{n-1} + \dots c_1 x + c_0)(x - \alpha) - c_0 x + c_0\alpha + q[\alpha]x + a_0 \end{aligned}$$

und die letzten vier Summanden ergeben gerade $p[\alpha]$.

9.6 Quotientenkörper

Der Körper Q heisst *Quotientenkörper* des Ringes R, falls R ein Unterring von Q ist und

$$Q = \{ab^{-1} \mid a, b \in R,\ b \neq 0\}$$

Dann ist R notwendigerweise Integriätsbereich. Beispiel: $\mathbb{Q}$ ist Quotientenkörper von $\mathbb{Z}$.

Satz 9.10 *Jeder Integritätsbereich R besitzt einen (bis auf Isomorphie über R eindeutig bestimmten) Quotientenkörper Q. Ist K ein Körper und $\phi : R \to K$ eine Einbettung, so gibt es eine eindeutig bestimmte Einbettung $\overline{\phi} : Q \to K$ mit $\overline{\phi}|R = \phi$.*

Beweis. Wie bei der Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$ definiere auf $Q' = \{(a, b) \mid a, b \in R,\ b \neq 0\}$

$$\begin{aligned} &(a, b) \sim (c, d) \ \Leftrightarrow ad = bc \\ &(a, b) + (c, d) = (ad + bc, bd), \quad (a, b) \cdot (c, d) = (ac, bd) \end{aligned}$$

Das ergibt mit diesen Operationen verträgliche Äquivalenzrelation.. Durch Faktorisieren $\pi : Q' \to Q'/\sim$ erhält man eine algebraische Struktur und sogar einen kommutativen Ring Q - $(Q, \cdot, 1)$ ist ein Monoid als homomorphes Bild von $R \times (R \setminus \{0\})$, ansonsten muss man rechnen. Das Inverse von $\pi(a, b)$ ist $\pi(b, a)$. Die Abbildung $a \mapsto \pi(a, 1)$ ist eine Einbettung von R in Q, und $\pi(a, b) = \pi(a, 1)\pi(1, b)$. Also können wir R als Unterring von Q auffassen und haben dann die gewünschte Darstellung der Elemente von Q. Ist $\pi : R \to K$ gegeben, so definiere

$$\overline{\phi}(ab^{-1}) = \phi(a)\phi(b)^{-1}$$

Das ist wohldefiniert, da aus $ad = bc$ folgt dass $\phi(a)\phi(d) = \phi(b)\phi(c)$, also $\phi(a)\phi(b)^{-1} = \phi(c)\phi(d)^{-1}$. □

Der Quotientenkörper des Polynomrings $K[x]$ über einem Körper heisst auch Körper der *rationalen Funktionen* über K und wird mit $K(x)$ bezeichnet und seine Elemente werden geschrieben als $\frac{f(x)}{g(x)}$

9.7 Polynomringe in mehreren Unbestimmten

Satz 9.11 *Sei R ein kommutativer Ring und A eine kommutative R-Algebra und $\{x_1, \ldots, x_n\}$ n-elementige Teilmenge von A. Dann sind äquivalent*

- *A ist von $\{x_1, \ldots, x_n\}$ frei erzeugte kommutative R-Algebra*
- *Die Elemente von A haben bis auf Reihenfolge der Summanden und Weglassen von Summanden mit Koeffizient $r_{k_1,\ldots,k_n} = 0$ eindeutige Darstellung*

$$p = p(x_1, \ldots, x_n) = \sum r_{k_1,\ldots,k_n} x_1^{k_1} \cdot \ldots \cdot x_n^{k_n} \quad \text{nur endlich viele } r_{k_1,\ldots,k_n} \neq 0$$

- *$M = \{x_1^{k_1} \cdot \ldots \cdot x_n^{k_n} \mid k_i \in \mathbb{N}\}$ ist von $\{x_1, \ldots, x_n\}$ frei erzeugtes kommutatives Monoid und A als R-Modul frei von M erzeugt*

Die Multiplikation ist dann eindeutig bestimmt

$$(**) \quad (\sum_{\mu \in M} r_\mu \mu) \cdot (\sum_{\nu \in M} s_\nu \nu) = \sum_{\lambda \in M} (\sum_{\mu \cdot \nu = \lambda} r_\mu s_\nu) \lambda$$

Wir nennen dann A auch *Polynomring in den Unbestimmten $x_1, \ldots, x_n$ mit Koeffizienten in (über) R* und schreiben $A = R[x_1, \ldots, x_n]$. Seine Elemente sind *Polynome*. Die Elemente μ von M heissen auch *primitive Monome*, die $r_\mu \mu$ mit $r_\mu \in R$ *Monome*. Beweis folgt aus Satz ??. □

Korollar 9.12 $R[x_1, \ldots, x_n] \cong R[x_1, \ldots, x_{n-1}][x_n]$

Beweis. Durch Ausmultiplizieren in $R[x_1, \ldots, x_{n-1}][x_n]$ kann man

$$(*) \quad \sum q_i(x_1, \ldots, x_{n-1}) x_n^i = p(x_1, \ldots x_n)$$

als Summe von Monomen über $x_1, \ldots, x_n$ schreiben. Dabei geht ein primitives Monom μ von q_i über in das primitive Monom μx_n^i von p. Ist λ primitives Monom von q_j und $i \neq j$ oder $i = j$ und $\lambda \neq \mu$, so folgt auf jeden Fall $\mu x^i \neq \lambda x^j$. Also kann p nur dann das Nullpolynom aus $R[x_1, \ldots, x_n]$ sein, wenn alle q_i schon das Nullpolynom aus $R[x_1, \ldots, x_{n-1}]$ waren. Das reicht aus für die Eindeutigkeit der Darstellung $(*)$, d.h. die Isomorphie zu $R[x_1, \ldots, x_n]$. □

Korollar 9.13 *Ist R ein unendlicher Integritätsbereich, so ist ein Polynom $p(x_1, \ldots, x_n)$ genau dann das Nullpolynom, wenn $p[a_1, \ldots, a_n] = 0$ für alle $a_1, \ldots, a_n \in R$.*

Beweis durch Induktion über n. Sei p nach $(*)$ dargestellt. Seien $a_1, \ldots, a_{n-1} \in R$ gegeben.

$$0 = p[a_1, \ldots, a_n] = \sum q_i[a_1, \ldots, a_{n-1}] a_n^i = (\sum q_i[a_1, \ldots, a_{n-1}] x_n^i)[a_n]$$

für alle $a_n \in R$. Nach Kor. 6.6 ist also $\sum q_i[a_1, \ldots, a_{n-1}] x_n^i$ das Nullpolynom in $R[x_n]$, d.h. für alle i ist $q_i[a_1, \ldots, a_{n-1}] = 0$. Das gilt für alle $a_1, \ldots, a_{n-1} \in R$. Also ist nach Induktionsannahme jedes $q_i(x_1, \ldots, x_{n-1})$ das Nullpolynom aus $R[x_1, \ldots, x_{n-1}]$. Also ist $p(x_1, \ldots, x_n)$ das Nullpolynom aus $R[x_1, \ldots, x_n]$. □

Theorem 9.14 *Sei R ein unendlicher Integritätsbereich. Eine R-Algebra-Gleichung gilt genau dann in allen kommutativen R-Algebren, wenn sie in R gilt.*

Beweis. Eine solche Gleichung ist von der Form $\forall \mathbf{x}.\ s(\mathbf{x}) = t(\mathbf{x})$ mit Polynomen $s(\mathbf{x})$ und $t(\mathbf{x})$ über R. Sie gilt nach Lemma ?? genau dann in allen kommutativen R-Algebren, wenn diese Polynome dasselbe Element der freien R-Algebra, d.h. der Polynomalgebra $R[\mathbf{x}]$ sind. Gleichbedeutend: $s(\mathbf{x}) - t(\mathbf{x})$ ist das Nullpolynom. Das ist nach Kor.?? gleichbedeutend damit, dass $(s-t)[\mathbf{a}] = 0$, d.h. $s[\mathbf{a}] = t[\mathbf{a}]$ für jede Wahl von $\mathbf{a}$ aus R. □

Korollar 9.15 *$\mathbb{Z}[x_1, \ldots, x_n]$ ist der freie kommutative Ring in n Erzeugenden $x_1, \ldots, x_n$. Eine Ring-Gleichung gilt genau dann in allen kommutativen Ringen, wenn sie in $\mathbb{Z}$ gilt.*

Die Gleichungen $\det(AB) = \det(A \cdot \det(B)$ und $A \cdot \mathsf{Ad}(A) = \det(A)E$ können wir als Gleichungen zwischen den Koeffizienten der Matrizen auffassen. Wir haben sie insbeondere für Koeffizientin in $\mathbb{Q}$, also auch in $\mathbb{Z}$ bewiesen. Sie gelten also über beliebigen kommutativen Ringen.

9.8 Halbgruppenalgebra

Proposition 9.16 *Die Endomorphismen eines R-Moduls ${}_RM$ bilden eine R Algebra*

$$(\phi + \psi)(x) = \phi(x) + \psi(x),\ (\phi \circ \psi)(x) = \phi(\psi(x)),\ (r\phi)(x) = r(\phi(x))\ \ x \in M$$

Beweis: Routineübung.

Satz 9.17 *Sei H ein Monoid und R ein kommutativer Ring. Auf dem freien R-Modul $R[H]$ mit Basis H gibt es eine eindeutig bestimmte Multiplikation so, dass $R[H]$ zur R-Algebra wird und die Multiplikation auf H mit der gegebenen übereinstimmt und $e \in H$ als Einslement hat. Die Algebra $R[H]$ lässt sich in in die Endomorphismenalgebra des Moduls $R[H]$ einbetten. Ist H kommutativ, so auch $R[H]$.*

Der Polynomring $R[x_1, \ldots, x_n]$ ist der Spezialfall, wo H das freie kommutative Monoid mit Erzeugern $x_1, \ldots, x_n$ ist.

Beweis. Für $a = \sum_{g \in H} r_g g \in R[H]$ (nur endliche viele $r_g \neq 0$) sei $\Phi(a)$ der Endomorphismus des R-Moduls $R[H]$ mit

$$\Phi(a)(h) = \sum_{g \in H} r_g (g \cdot h)$$

Die Abbildung Φ von $R[H]$ in die R-Algebra $\mathsf{End}({}_RR[H])$ ist offenbar R-linear. Ist $\Phi(a) = 0$ die Nullabbildung, so $\Phi(a)(e) = 0$ und daher $r_g = 0$ für alle g in H, weil die $g = g \cdot e\ (g \in H)$ lauter verschiedene Elemente des Basis H sind. Also $a = 0$. D.h. Φ hat Kern 0 und ist injektiv.

Nach Definition von Φ gilt $\Phi(k)(h) = k \cdot h$ für alle $k, h \in H$, da $k = \sum_{g \in h} r_g g$ mit $r_g = 1$ für $g = k$ und $r_g = 0$, sonst. Es folgt $(\Phi(g) \circ \Phi(k))(h) = \Phi(g)(\Phi(k)(h)) = \Phi(g)(k \cdot h) = g \cdot (k \cdot h) = (g \cdot k) \cdot h = \Phi(g \cdot k)(h)$ für alle $g, k, h \in H$ und somit

$$\Phi(g) \circ \Phi(k) = \Phi(g \cdot k)\ \text{ für } k, g \in H$$

Da $\Phi(e)(h) = h \cdot e = h$ ist $\Phi(e) = \mathsf{id}_{R[H]}$. Die $\Phi(a)$ $(a \in R[H])$ bilden eine Unteralgebra A von $\mathsf{End}({}_RR[M])$ - es ist noch der Abschluss unter $\circ$ nachzuprüfen: ist $b = \sum_{k \in h} s_k k$. so

$$\Phi(a) \circ \Phi(b) = (\sum_{g \in h} r_h \Phi(g)) \circ (\sum_{k \in H} s_k \Phi(k)) = \sum_{g,k \in H} r_g s_k \Phi(g) \circ \Phi(k) = \sum_{g,k \in H} r_g s_k \Phi(g \cdot k) \in A$$

Somit definiere man auf $R[H]$ die Multiplikation durch

$$a \cdot b = c \;\Leftrightarrow\; \Phi(a) \circ \Phi(b) = \Phi(c)$$

und erhält so die gesuchte Algebra. Dass die Multiplikation durch die von H eindeutig bestimmt ist, folgt sofort mit den Algebra-Gesetzen durch Ausmultiplizieren. Ist H kommutativ, so folgt die Kommutativität von $R[H]$ ganz einfach durch Ausmultiplizieren

$$(\sum_{g\in H} r_g g) \cdot (\sum_{k\in H} s_k k) = \sum_{g,k\in H} r_g s_k (g \cdot k) = \sum_{g,k\in H} s_k g_g (k \cdot g) = (\sum_{k\in H} s_k k) \cdot (\sum_{g\in H} r_g g) \quad \square$$

10 Euklidische Ringe

10.1 Einheiten

Ein *Monoid* ist eine Menge M mit einer assoziativen Multiplikation mit neutralem Element e. Ein Element u eines Monoids M ist eine *Einheit* oder *invertierbar*, wenn es $x \in M$ gibt mit $xu = ux = 1$.

Lemma 10.1 *Die Einheiten eines Monoids M bilden eine Gruppe M^*.*

Beweis. Das Inverse x ist eindeutig bestimmt, nämlich aus $yu = uy = 1$ folgt $y = y1 = yux = 1x = x$. Wir dürfen also schreiben $x = u^{-1}$ und es ist klar, dass $u^{-1} \in M^*$ und $(u^{-1})^{-1} = u$. Ist v eine weitere Einheit, so $uvv^{-1}u^{-1} = u1u^{-1} = uu^{-1} = 1$ und ebenso $v^{-1}u^{-1} = uv$, also $uv \in M^*$. $\square$

Die *Einheitengruppe* R^* eines Ringes besteht aus den Einheiten des Monoids $(R, \cdot, 1)$. Man sieht leicht (eine Einheit in Polynomring muss Grad 0 haben)

$$\mathbb{Z}^* = \{1, -1\}, \;\; (K[x])^* = K^* \text{ für Körper } K$$

Für das direkte Produkt $R_1 \times R_2$ zweier Ringe mit komponentenweiser Addition und Multiplikation gilt offenbar

$$(R_1 \times R_2)^* = R_1^* \times R_2^*.$$

Im Ring der $n \times n$-Matrizen über einem kommutativen Ring R: definiert man die Determinante nach der expliziten Formel aus LA. Die Formel $(\det A)\mathsf{ad}A = E$ gilt auch in R, weil sie in $\mathbb{Z}$ gilt. falls $\det A \in R^*$ erhält man $A^{-1} = \det(A)^{-1}\mathsf{ad}A$ und somit

$$(R^{n\times n})^* = \{A \mid \det A \in R^*\} \text{ für kommutative } R.$$

10.2 Teilbarkeit

In einem kommutativen Ring definieren wir

$$d|a \;\Leftrightarrow d \text{ teilt } a \;\Leftrightarrow \exists r \in R.\, rd = a.$$

Durch die Teilbarkeit erhalten wir eine 'Quasiordnung' auf R

$$a|a \text{ (reflexiv)}, \;\; a|b \text{ und } b|c \Rightarrow a|c \text{ (transitiv)}$$

mit den Verträglichkeitseigenschaften

$$a|b \Rightarrow ac|bc, \;\; a|b \text{ und } a|c \Rightarrow a|(b \pm c)$$

(Beweis als Übung).

10.3 Hauptideale

In einem kommuativen Ring R ist $(a) = Ra = \{ra \mid r \in\}$ ein Ideal, das von a erzeugte Hauptideal. Es gilt

$$a \mid b \Leftrightarrow Ra \supseteq Rb$$

Ein Integritätsbereich, in dem jedes Ideal ein Hautpideal ist, ist ein *Hauptidealring.*

10.4 Teilbarkeit und Assoziiertheit in Integriätsbereichen

Assoziiertheit in eime Integritätsbereich ist definiert durch

$$a|b \text{ und } b|a \Leftrightarrow \exists r \in R^* : ra = b \Leftrightarrow: a \approx b$$

nämlich aus $ra = b$ und $sb = a$ folgt $rsb = b$ also $rs = 1$ mit der Kürzungsregel. Dass $\approx$ eine Äquivalenzrelation ist, folgt sofort daraus, dass die Einheiten eine Untergruppe bilden.

$$a \approx a' \text{ und } b \approx b' \Rightarrow (a|b \Leftrightarrow a'|b').$$

Es gilt in einem Integritätsbereich

- $a \sim b$ bzgl. der zu (d) gehörigen Kongruenz $\Leftrightarrow a \equiv \mathsf{mod\ d} \Leftrightarrow \mathsf{d}|(\mathsf{a} - \mathsf{b})$
- $a|b \Leftrightarrow (b) \subseteq (a)$
- $a \approx b$ (assoziiert) $\Leftrightarrow (a) = (b)$
- $a \in R^* \Leftrightarrow (a) = (1) = R$

10.5 Euklidische Ringe

Ein Integritätsbereich R heisse ein *euklidischer Ring*, wenn es eine Abbildung gibt

$$\delta : R \setminus \{0\} \to \mathbb{N}$$

$$\begin{array}{ll} \forall a, b \in R \setminus \{0\} : & \delta(ab) \geq \delta(a) \\ \forall a, b \in R \setminus \{0\}\ \exists q, r \in R : & a = bq + r \qquad \text{und } \delta(r) < \delta(b) \text{ oder } r = 0 \end{array} .$$

Will man $\delta(0)$ definieren, so am besten als $-\infty$. Beispiele:

$$\mathbb{Z} \text{ mit } \delta(a) = |a|, \quad K[x] \text{ mit } \delta(f(x)) = \deg f(x),\ K \text{ ein Körper.}$$

Lemma 10.2 *In einem euklidischen Ring gilt*

$$a|b \text{ und } \delta(a) = \delta(b) \Leftrightarrow a \approx b.$$

Beweis. Sei $b = ac$. Wir haben $a = bq + r$ mit $r = 0$ oder $r = a - bq = a = acq = a(1 - cq)$ und $\delta(b) > \delta(r) = \delta(a(1 - cq)) \geq \delta(a)$, da $r = a - bq = a - acq = a(1 - cq)$. Gilt $\delta(a) = \delta(b)$, so entfällt diese Möglichkeit und es gilt auch $b \mid a$, also $a \approx b$. □ Manche Autoren lassen den ersten Teil der Definition weg und können dann das Lemma nicht beweisen.

Satz 10.3 *Jeder euklidische Ring R ist ein Hauptidealring.*

Beweis: Sei $I \neq (0)$. Wähle $0 \neq a \in I$ mit $\delta(a)$ minimal. Dann $(a) \subseteq I$. Sei nun $0 \neq b \in I$. Dann $b = aq + r$ mit $r = 0$ oder $\delta(r) < \delta(a)$. In zweiten Falle auch $r = b - aq \in I$ im Widerpsruch zur Minimalität von $\delta(a)$. Also $r = 0$ und somit $b \in (a)$. □ Viele der folgenden Ergebnisse gelten auch für Hauptidealringe, nur fehlen dann die Algorithmen.

10.6 Satz von Bezout

Wir sagen, d sei ein *grösster gemeinsamer Teiler* von a und b im Integritätsbereich R, bzw.

$$d \approx GGT(a,b) \;\Leftrightarrow\; d|a, d|b \text{ und } \forall c : (c|a \text{ und } c|b) \Rightarrow c|d.$$

Die Schreibweise rechtfertigt sich dadurch, dass d, wenn's überhaupt existiert, bis auf Assoziiertheit eindeutig bestimmt ist. Es gilt

$$\mathrm{GGT}(a,b) \approx \mathrm{GGT}(b, a - qb)$$

weil jeder Teiler von a, b auch einer von $a - qb$ ist und umgekehrt. Wir schreiben fúr das von a, b erzeugte Ideal

$$\{ra + sb \mid r, s \in R\} = (a,b) = (a) + (b)$$

Satz 10.4 *In einem euklidischen Ring existiert der GGT stets und hat eine additive Darstellung*

$$d \approx GGT(a,b) \;\Leftrightarrow\; d|a, d|b \text{ und } \exists r,s : d = ra + sb \;\Leftrightarrow\; (d) = (a) + (b).$$

Beweis. Der erweiterte euklidische Algortihmus liefert d, r, s mit $d|a$, $d|b$, $d = ra + sb$. Dann ist d ein GGT: aus $c|a$ und $c|b$ folgt $c|ra$ und $c|sb$ also $c|(rs + sb)$. Ist umgekehrt d' ein GGT von a, b so $d' \approx d$ wegen der Eindeutigkeit und somit $(d') = (a) + (b)$. □

Algorithmus 10.5 *(*Euklid+Bezout*). Sei R ein euklidischer Ring. Zu je zwei a, b in R gibt es einen $GGT(a,b)$ und x und y in R mit*

$$GGT(a,b) = ax + by.$$

Den GGT und geeignete x, y kann man so bestimmen. Gegeben a, b setze

$$d' := a,\ x' := 1,\ y' := 0;\ d := b,\ x := 0,\ y := 1$$

Bestimme

$$d' = dq + r \text{ mit } 0 \le \delta r < \delta d \text{ oder } r = 0$$

$$\text{solange } r \neq 0 \text{ tu } (d', d) := (d, r),\ (x', x) := (x, x' - xq),\ (y', y) := (y, y' - yq)$$

$$\text{falls } r = 0 \text{ halt ein } :\ d = ax + by =: GGT(a,b).$$

Beweis. Da $\mathbb{N}$ wohlgeordnet ist, muss der Algorithmus zum Halten kommen. Korrektheit des Algorithmus: Für alle Iterationsschritte gilt:

$$d = ax + by,\ d' = ax' + by' \text{ und } GGT(a,b) = GGT(d,d').$$

Nämlich

$$a(x' - xq) + b(y' - yq) = ax' + by' - (ax + by)q = d' - dq = r$$

$$GGT(r,d) = GGT(d,d') = GGT(a,b).$$

Ist $r = 0$, so folgt $d|d'$, also $d = GGT(a,b)$. □

Korollar 10.6 $a|(bc) \wedge GGT(a,b) = 1 \;\Rightarrow\; a|c$

Beweis. $1 = ax + by$, also $a|(axc + bcy) = c$.

Korollar 10.7 *Ist $GGT(a,b) = 1$, so ist $\tilde{b} = b[\mathsf{mod\ a}]$ invertierbar in $R/(a)$*

$$by \equiv 1 \,\mathsf{mod\ a} \quad \textit{falls } 1 = \mathsf{ax} + \mathsf{by}$$

10.7 Summe, Schnitt und Produkte von Idealen

Sind die $I_1, \ldots, I_n$ Ideale von R, so sind

$$I_1 + \ldots + I_n = \{r_1 + \ldots + r_n \mid r_i \in I_i\}$$

$$I_1 \cap \ldots \cap I_n$$

Ideale, das kleinste, das alle I_i umfasst bzw. das größte, das in allen I_i enthalten ist.

$$I_1 \cdot \ldots \cdot I_n = \{\sum_{k=1}^{m} r_{k1} \cdot \ldots \cdot r_{kn} \mid m \in \mathbb{N},\, r_{ki} \in I_i\}$$

ebenfalls ein Ideal, das *Produkt* der $I_1, \ldots, I_n$. Es gilt

$$I_1 \cdot \ldots \cdot I_n \subseteq I_1 \cap \ldots \cap I_n$$

10.8 GGT und KGV

Lemma 10.8 *Sei R ein euklidischer Ring. d ist grösster gemeinsamer Teiler der $k_1, \ldots, k_n$ genau dann, wenn d Teiler der k_i ist und es*

$$a_i \in R \text{ gibt mit } \; d = a_1k_1 + \ldots + a_nk_n$$

Beweis und Algorithmus. Falls $n = 2$ nach Bezout. Für $n > 2$ rekursiv.

- Bestimme c_i mit $d_{n-1} = \mathrm{GGT}(k_1, \ldots, k_{n-1}) = c_1k_1 + \ldots + c_{n-1}k_{n-1}$
- $d = \mathrm{GGT}(d_{n-1}, k_n)$. Bestimme b, a_n mit $d = bd_{n-1} + a_nk_n$
- $a_1 = bc_1, \ldots, a_{k-1} = bc_{k-1}$ $\quad \square$

v ist *kleinstes gemeinsames Vielfaches* (KGV) der $k_1, \ldots, k_n$ falls $k_i \mid v$ für alle i und falls $v \mid w$ für alle w mit $k_i \mid w$ für $i = 1, \ldots n$). Es folgt

- $(\mathsf{GGT}(k_1, \ldots, k_n)) = (k_1) + \ldots + (k_n)$
- $(\mathsf{KGV}(k_1, \ldots, k_n)) = (k_1) \cap \ldots \cap (k_n)$
- $(k_1 \cdot \ldots \cdot k_n) = (k_1) \cdot \ldots \cdot (k_n)$

10.9 Primelemente

Satz 10.9 *Für ein Element $0 \neq a \notin R^*$ eines euklidischen Rings sind äquivalent*

- *a ist* unzerlegbar *oder* irreduzibel*, d.h. $a = bc \Rightarrow b \in R^*$ oder $c \in R^*$*
- *(a) ist ein* maximales Ideal*, d.h. für alle Ideale: $a \in I \Rightarrow (a) = I$ oder $I = R$.*
- *$R/(a)$ ist Körper*
- *a ist* prim*, d.h. $a|bc \Rightarrow a|b$ oder $a|c$*

Beweis. (1) $\Rightarrow$ (2): $I = (b)$ und $a = bc$, also $I = R$ falls $b \in R^*$ bzw. $(a) = I$ falls $c \in R^*$.
(2) $\Rightarrow$ (3): Sei $\tilde{b} \neq 0$ in $R/(a)$, also $b \notin (a)$. Also $(a) \neq (a, b)$ und daher $1 \in R = (a, b)$, d.h. es gibt r, c mit $ar + bc = 1$. Es folgt $\tilde{b} \cdot \tilde{c} = \tilde{1}$, d.h. $\tilde{b}$ ist invertierbar. (3) $\Rightarrow$ (4): Aus $a|bc$ folgt $\tilde{b} \cdot \tilde{c} = \widetilde{bc} = 0$ also $\tilde{b} = 0$ oder $\tilde{c} = 0$, d.h. $b \in (a)$ oder $c \in (a)$.
(4) $\Rightarrow$ (1): Ist $a = bc$ prim, so $a|b$ oder $a|c$. Andererseits $c|a$ und $b|a$, also $b \in R^*$ oder $c \in R^*$. $\square$

Korollar 10.10 *Für a, b in einem euklidischen Ring R ist b[mod a] genau dann in $R/(a)$ invertierbar, wenn $GGT(a, b) \approx 1$.*

10.10 Zerlegung

Lässt sich jede Nichteinheit $a \neq 0$ eines Integritätsbereiches als Produkt

$$a = p_1 \cdot \ldots \cdot p_n$$

von Primelementen schreiben und sind dabei die p_i bis auf Reihenfolge und Assoziiertheit eindeutig bestimmt, so spricht man von einem *faktoriellen* Ring oder ZPE-Ring.

Satz 10.11 *Jeder euklidische Ring ist faktoriell.*

Beweis der Existenz durch Ordnungsinduktion über $\delta(a)$: Ist a nicht schon selbst irreduzibel, so $a = bc$ mit $\delta(a) > \delta(b), \delta(c)$, also nach Induktion $b = \prod_i p_i$ und $c = \prod_j q_j$ sowie $a = \prod_i p_i \cdot \prod_j q_j$ mit irreduziblen p_i und q_j.
Beweis der Eindeutigkeit durch Induktion über die Anzahl der Faktoren. Sei

$$p_1 \cdot \ldots \cdot p_n \approx q_1 \cdot \ldots \cdot q_m.$$

O.B.d.A. $p_1|q_1$, d.h. $q_1 \approx p_1$ da beide prim. Es folgt

$$p_2 \cdot \ldots \cdot p_n \approx q_2 \cdot \ldots \cdot q_m$$

und mit Induktion $n = m$ und nach Umnummerieren und $p_i \approx q_i$. $\square$
Für ganze Zahlen ist das Faktorisieren algorithmisch aufwendig, so aufwendig, dass man schwer zu faktorisierende Produkte zur Grundlage von Public-key-codes gemacht hat. Im Gegensatz dazu gibt es ein recht einfaches Verfahren (GGT mit Testpolynomen) für Polynome über endlichen Körpern (Berlekamp, Algebraic coding theory), ein hinsichtlich der verwendeten Theorie anspruchsvolles aber effektives für Polynome über $\boldsymbol{Q}$ (Lenstra[2],Lovasz, Math.Ann 261) vgl. Lenstra[2]: Algorithms in number theory, Handbook of Theoretical Computer Science A.

Betrachet man die Primfaktorzerlegungen nur für endlich viele Elemente, so gibt es auch nur endlich viele verschiedene Primelemente $p_1, \ldots, p_n$ die darin vorkommen. Dann kann man schreiben

$$a = p_1^{k_1} \cdot \ldots \cdot p_n^{k_n},\ b = p_1^{l_1} \cdot \ldots \cdot p_n^{l_n}$$

$$GGT(a, b) \approx p_1^{\min\{k_1, l_1\}} \cdot \ldots \cdot p_n^{\min\{k_n, l_n\}}$$

$$KGV(a, b) \approx p_1^{\max\{k_1, l_1\}} \cdot \ldots \cdot p_n^{\max\{k_n, l_n\}}, \quad m \approx KGV(a, b) \Leftrightarrow (a) \cap (b) = (m).$$

$$d \approx GGT(a, b) \Rightarrow KGV(a, b) = ab/d$$

11 Invariante Teiler

11.1 Elementarmatrizen

Wir betrachten Matrizen mit Koeffizienten in einem kommutativen Ring R. Addition und Multiplikation sind wie üblich definiert. Die $n \times n$-Matrizen bilden einen (nichtkommuativen Ring $R^{n\times n}$ mit Einheitengruppe bestehend aus den invertierbaren Matrizen (wobei die Koffefizienten der Inversen A^{-1} wieder in R sein müssen).

Hat die $m \times n$ Matrix A die Spalten $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ und ist $T = (t_{jh})_{n\times n}$, so hat die $m \times n$-Matrix $A' = AT$ die Spalten

$$\boldsymbol{a}'_1 = t_{11}\boldsymbol{a}_1 + \ldots + t_{n1}\boldsymbol{a}_n, \ \ldots \ , \boldsymbol{a}'_n = t_{1n}\boldsymbol{a}_1 + \ldots + t_{nn}\boldsymbol{a}_n$$

d.h. wir können das 'Rechtsranmultipizieren' von T so verstehen, dass aus den Spalten von A die Spalten der neuen Matrix $A' = AT$ als 'Linearkombinationen' gebildet werden. Insbesondre haben wir für festes k bzw. $k \neq l$ und Einheiten $r \in R$

Scherung $T = [Sk := Sk + rSl]$	$\boldsymbol{a}'_j = \begin{cases} \boldsymbol{a}_k + r\boldsymbol{a}_l & j = k \\ \boldsymbol{a}_j & j \neq k \end{cases}$	$t_{ij} = \begin{cases} r & i = l, j = k \\ 1 & i = j \\ 0 & \text{sonst} \end{cases}$
Streckung $T = [Sk := rSk]$	$\boldsymbol{a}'_j = \begin{cases} r\boldsymbol{a}_k & j = k \\ \boldsymbol{a}_j & j \neq k \end{cases}$	$t_{ij} = \begin{cases} r & i = j = k \\ 1 & i = j \neq k \quad r \in R^* \\ 0 & \text{sonst} \end{cases}$
Vertauschung $T = [Sk \leftrightarrow Sl]$	$\boldsymbol{a}'_j = \begin{cases} \boldsymbol{a}_l & j = k \\ \boldsymbol{a}_k & j = l \\ \boldsymbol{a}_j & \text{sonst} \end{cases}$	$t_{ij} = \begin{cases} 1 & \{i, j\} = \{k, l\} \\ 1 & i = j \notin \{k, l\} \\ 0 & \text{sonst} \end{cases}$

Matrizen T dieser Gestalt heissen *Elementarmatrizen* und Matrixumformungen $A' = AT$ *elementare (Spalten)Umformungen.*

Elementarmatrizen sind invertierbar und ihre Inversen wieder elementar

$$\begin{aligned} [Sk := Sk + rSl]^{-1} &= [Sk := Sk - rSl] \\ [Sk := rSk]^{-1} &= [Sk := r^{-1}Sk] \\ [Sk \leftrightarrow Sl]^{-1} &= [Sk \leftrightarrow Sl] \end{aligned}$$

Entsprechend bewirkt Multiplikation von links ($A \mapsto SA$) Zeilenumformungen von A, die wir entsprechend notieren. Für die 3 Matrizen T wie oben heisst das (beachte den Rollentausch von k und L im Falle der Scherung)

$$T = [Zl := Zl + rZk], \ \ T = [Zk : rZk], \ \ T = [Sr \leftrightarrow Zl]$$

11.2 Invariantenteilersatz

Theorem 11.1 *Jede $n \times m$-Matrix A mit Einträgen aus einem euklidischen Ring R kann durch elementare Spalten- und Zeilenumformungen überführt werden in eine $n\times m$-Diagonalmatrix, insbesondere existieren invertierbare S in $R^{n\times n}$ und T in $R^{m\times m}$ mit*

$$S^{-1}AT = D = \begin{pmatrix} d_1 & 0 & 0 & \ldots \\ 0 & d_2 & 0 & \\ \vdots & & \ddots & \\ & & \ldots & \end{pmatrix} \quad \textit{mit} \ \ d_i | d_{i+1} \ \textit{für} \ i < \min\{m, n\}.$$

Die $d_1, d_2, \ldots$ bilden ein System *invarianter Teiler* der Matrix A. Später werden wir die Eindeutigkeit bis auf Assozierte zeigen.

Beweis und Algorithmus dymamisch $A \rightsquigarrow A_{\text{neu}} =: A$.

> ein Indexpaar (i,j) heisse *aktiv* in A, falls $a_{ij} \neq 0$ und es in der Zeile oder Spalte noch einen Eintrag $\neq 0$ gibt

Nun gehen wir mit Induktion bzw. Rekursion nach

$$\delta(A) = \begin{cases} \min\{\delta(a_{ij}) \mid (i,j) \text{ aktiv in } A\} \text{ falls nichtleer} \\ -\infty \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{sonst} \end{cases}$$

vor, um A zunächst in eine Diagonalmatrix zu überführen:

- Solange $\delta(A) \geq 0$ mache
  - $[Sk := Sk - qSi]$ mit $\delta(a_{ik} - qa_{ij}) < \delta(a_{ij})$
  - $[Zk := Zk - qZj]$ mit $\delta(a_{ki} - qa_{ij}) < \delta(a_{ij})$
  - sodass $\delta(A_{\text{neu}}) < \delta(A)$
- Wenn $\delta(A) = -\infty$ mache A diagonal durch Vertauschungen

Eine 2×2-Matrix mit $d = GGT(a,b) = ra + sb$ überführen wir so in Normalform mit den Umformungen $[S2 := S2 + rS1]$, $[Z1 := Z1 + sZ2]$, $[S1 := S1 - \frac{a}{d}S2]$, $Z2 := Z2 - \frac{b}{d}Z1]$, $S1 \leftrightarrow S2]$, $S2 := (-1)S2]$

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \rightsquigarrow \begin{pmatrix} a & ra \\ 0 & b \end{pmatrix} \rightsquigarrow \begin{pmatrix} a & d \\ 0 & b \end{pmatrix} \rightsquigarrow \begin{pmatrix} 0 & d \\ -\frac{a}{d}b & b \end{pmatrix}$$

$$\rightsquigarrow \begin{pmatrix} 0 & d \\ -\frac{a}{d}b & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} d & 0 \\ 0 & -\frac{a}{d}b \end{pmatrix} \rightsquigarrow \begin{pmatrix} d & 0 \\ 0 & \frac{a}{d}b \end{pmatrix}$$

Die Umformung einer Diagonalmatrix D geht nun so

- Solange es $i < j$ gibt mit d_i teilt nicht d_j wähle erst i mininal und dann zu diesem i das j minimal und mache die passenden Umformungen für die Untermatrix $\begin{pmatrix} d_i & 0 \\ 0 & d_j \end{pmatrix}$.

Die gesuchten invertierbaren Matrizen S^{-1} und T sind die Produkte der links bzw, rechts für die Umformungen benutzten Elemenarmatrizen, links in der Reihenfolge von lrechts nach links aufmultipliziert, rechts in der Reihenfolge von rechts nach links. □

11.3 Determinanten

Für Matrizen $A \in R^{n \times n}$, R ein Integritätsbereich, haben wir die Determinanten $\det(A)$ zunächst im Quotientenkörper. Induktion über n und Entwickeln zeigen aber sofort, dass $\det(A) \in R$.

Korollar 11.2 *Sei R euklidisch. Für $A \in R^{n \times n}$ sind äquivalent*

- *A ist in $R^{n\times n}$ invertierbar*
- *A ist Produkt in $R^{n\times n}$ invertierbarer Elementarmatrizen, d.h. von Scherungen, Vertauschungen und Streckungen um Einheiten.*
- $\det(A)$ *ist in R invertierbar.*

Beweis. Aus dem Beweis des Satzes über die invarianten Teiler folgt, dass man die invertierbaren Matrizen T und S^{-1} als Produkte von Scherungen und Vertauschungen wählen kann. Diese haben det $= \pm 1$, also $\det D = \pm \det A$. Und eine Diagonalmatrix D ist genau dann invertierbar, wenn ihre Diagonaleinträge invertierbar sind bzw. gleichbedeutend wenn $\det(D) \in R^*$. $1 \Rightarrow 2$: Für invertierbares A hat man die Produktdarstellung $D = SAT^{-1}$ und damit D und $\pm \det D$ invertierbar. $2 \Rightarrow 3$ nach dem Determinanten-Produkt-Satz. $3 \Rightarrow 1$: $\det D$ invertierbar, also D und somit A invertierbar. □

11.4 Eindeutigkeit der invarianten Teiler

Die ergibt sich später viel durchsichtiger über die Strukturtheorie endliche erzeugter Moduln. Wer's lieber ohnen Abtsaktion aber dafür knifflig mag, darf hier diesen Abschnitt lesen. Sei im Folgenden R ein euklidischer Ring. B heisst *äquivalent* zu A in $R^{n\times n}$, wenn es in $R^{n\times n}$ invertierbare S, T gibt mit $B = S^{-1}AT$. Das liefert offenbar eine Äquivalenzrelation auf $R^{n\times n}$ und der Invariantenteilersatz besagt, dass die Diagonalmatrizen mit $d_i | d_{i+1}$ ein Repräsentantensystem bilden. Sei $I(A)$ das von den a_{ij} $(i, j \leq n)$ erzeugte Ideal.

Lemma 11.3 *Für äquvalente Matrizen gilt* $\det(A) \approx \det(B)$ *und* $I(A) = I(B)$

Beweis. Die erste Aussage folgt mit Produktsatz und dem Korollar. Wird nun z.B. das q-fache der k-ten Spalte von der j-ten abgezogen, d.h. $b_{ik} = a_{ik}$, $b_{ij} = a_{ij} - qa_{ik}$ und $b_{il} = a_{il}$ sonst. Somit für die erzeugten Ideale $(a_{ik}, a_{ij}) = (b_{ik}, b_{ij})$ und damit ist alles klar. □

Eine $k \times k$-Untermatrix B einer Matrix A enthält gerade Einträge aus ausgewählten je k Zeilen und Spalten. $\det(B)$ heisst dann ein *k-Minor* von A. Sei $I_k(A)$ das von der Gesamtheit der k-Minoren von A erzeugte Ideal von R.

Lemma 11.4 *Sei $A \in R^{n\times n}$ und T, U invertierbar in $R^{n\times n}$. Dann $I_k(A) = I_k(AT) = I_k(UA)$.*

Beweis der Eindeutigkeit der invarianten Teiler bis auf assoziierte. Der GGT $d_1 \cdot \ldots \cdot d_k$ der k-Minoren von D ist durch A bis auf assoziierte eindeutig bestimmt als Erzeuger Δ_k von $I_k(A)$. Somit

$$d_1 = \Delta_1, \quad d_k = \frac{\Delta_k}{\Delta_{k-1}} \text{ für } k > 1$$

Beweis des Lemmas. Die Spalten von AT sind R-Linearkombinationen der Spalten von A: die j-Spalte ist $t_{1j}\boldsymbol{a}_1 + \ldots + t_{nj}\boldsymbol{a}_n$. Sei nun B eine k-Untermatrix von AT. Jede Spalte von B ist Linearkombination von Spalten der Matrix C, die man aus AT erhält, wenn man nur die ausgwählten k-Zeilen erlaubt, also

$$\det(B) = \det(\sum_{j=1}^{n} r_{1j}\boldsymbol{c}_j, \ldots, \sum_{j=1}^{n} r_{kj}\boldsymbol{c}_j = \sum_{j_1,\ldots,j_k} r_{1j_1} \cdot \ldots \cdot r_{kj_k} \det(\boldsymbol{c}_{j_1}, \ldots, \boldsymbol{c}_{j_k})$$

also in der Tat eine R-Linearkomination von k-Minoren von AT. Also

$$I_k(AT) \subseteq I_k(A)$$

Indem man dasselbe Argument aus AT und T^{-1} anwendet, folgt $I_k(A) = I_k(ATT^{-1}) \subseteq I_k(At)$, also $I_k(A) = I_k(AT)$. Da sich Determinanten beim Transponieren nicht ändern, gilt das auch für die $I_k()$, und wir haben $I_k(UA) = I_k((AU)^t) = I_k(A^tU^t) = I_k(A^t) = I_k(A)$. □

11.5 Elementarteiler

Hat man die invarianten Teiler $d_1, \ldots, d_k$ der Matrix A über dem euklidischen Ring R bestimmt, so sei

- k_1 das maximale i mit $d_i \notin R^\times$
- k_2 das minimale mit $d_i \neq 0$
- $d_{k_2} = p_1^{n_1} \cdot \ldots \cdot p_l^{n_l}$ eine Primfaktorzerlegung von d_{k_2}
- d_i assoziiert zu $p_1^{n_{i1}} \cdot \ldots \cdot p_l^{n_{il}}$
- Sei i_j minimal mit $n_{ij} > 0$

Dann ergibt sich das System der *Elementarteiler* A als Liste bestehend aus $k_1 - 1$ Einsen und $\min\{n, m\} - k_2$ Nullen, sowie zu jedem p_j der Liste aller $p_j^{n_{ij}}$, die $\neq 1$ sind - also ggf. mit Wiederholung. Damits schöner aussieht sortiert man diese Primpotenzen jeweils nach wachsendem Exponenten.

Lemma 11.5 *Die invarianten Teiler sind durch die Elementarteiler eindeutig bestimmt.*

Beweis, Wir können annemhen, dass es keine invarianten Teiler 0 und 1 gibt, also $k_1 = 1$ und $k_2 = \min\{n, m\}$. Es gibt dann ein j mit $n_{1j} \neq 0$. Dividiere alles durch $p^{n_{1j}}$ und berufe Dich auf Induktion. □.

12 Isomorphiesätze

12.1 Zerlegung

Korollar 12.1 Zerlegung eines Homomorphismus *Sei ψ ein Homomorphismsus von M nach N. Dann gibt es eindeutig bestimmte Unterstruktur N' von N und Isomorphismus $\omega : M/\sim_\psi \to N'$ so, dass*

$$\psi = \varepsilon \circ \omega \circ \pi \quad \pi : M \to M/\sim_\psi \text{ kanonische Projektion }, \ \varepsilon : N' \to N \text{ Identität.}$$

Das folgt sofort aus ??. Man kann's noch weiter treiben und χ zerlegen in $\chi = \varepsilon \circ \omega$, wobei ω Bijektion von $M/\sim_\psi$ auf $N' = \text{Bild}(\chi) \subseteq N$ ist (nämlich die hintere Einschränkung von χ auf N' und ε die Inklusion von N' in N, d.h. $\varepsilon(x) = x$ für $x \in N'$.

Beispiel: ψ sei der Homomorphismus $\psi r = e^{2pir}$ von der additiven Gruppe $\mathbb{Q}$ in die multiplikative Gruppe der komplexen Zahlen von Betrag 1. Die zugeörige Kongruenzrelation ist gegeben durch $r \sim s \Leftrightarrow r - s \in \mathbb{Z}$. Die Faktorstruktur $\mathbb{Q}/\mathbb{Z}$ is isomorph zur Untergruppe der Einheitswurzeln `[roots of unity]` in $\mathbb{C}$.

Eine Sequenz

$$\ldots A_i \stackrel{\phi_i}{\to} A_{i+1} \stackrel{\phi_{i+1}}{\to} A_{i+2} \ldots$$

von Gruppen bzw. Ringen bzw. Moduln und Homomorphismen heisst *exakt* `[exact]`, wenn

$$\mathsf{Bild}\phi_i = \mathsf{Kern}\phi_{i+1} \quad \text{für alle } i$$

Eine exakte Sequenz

$$0 \to A \stackrel{\varepsilon}{\to} B \stackrel{\pi}{\to} C \to 0$$

von Moduln heisst eine *kurze exakte Sequenz* `[short exact sequence]`. Gleichbedeutend dazu ist, dass ε injektiv und π kanonische Projektion der Faktorisierung von B nach A ist. Die Zerlegung schreibt sich dann so

$$0 \to \mathsf{Kern}(\phi) \stackrel{\mathsf{id}}{\to} M \stackrel{\phi}{\to} \mathsf{Bild}(\phi) \to 0$$

12.2 Erster Isomorphiesatz

Lemma 12.2 *Sei A eine algebraische Struktur mit Unterstruktur U und Kongruenz θ. Dann is*

$$U\theta = \{a \in G \mid \exists u \in U,\ a\theta u\} = \bigcup_{u \in U} [u]\theta$$

eine Unterstruktur von G. Ist A Gruppe (Ring, Modul) und N der zu θ gehörige Normalteiler (Ideal, Untermodul) so gilt $U\theta = UN$ ($U\theta = U + N$).

Beweis: klar. □.

Satz 12.3 *Unter den Voraussetzungen des Lemmas gilt $U\theta/(\theta|U\theta) \cong U/(\theta|U)$.*

Beweis. Wir dürfen ohne Beschränkung der Allgemeinheit $A = U\theta$ annehmen. Sei $\pi : A \to A/\theta$ die kanonische Projektion. Die Einschränkung $\pi|U$ auf U ist surjektiv: ist $a \in A$, so $a\theta u$ mit $u \in U$, also $\pi(a) = \pi(u)$. Der Kern des Homomorphismus $\pi|U$ ist offensichtlich $\theta|U$ und nach dem Homomorphiesatz haben wir die Behauptung. □

12.3 Vergröberung

Sind $\sim$ und $\approx$ zwei Kongruenzzrelationen auf A, so heisst $\sim$ *gröber* `[coarser]` als $\approx$ und $\approx$ *feiner* `[finer]` als $\sim$, falls

$$a \approx b \quad \Rightarrow a \sim b \quad \text{für alle } a, b \in A$$

Handelt es sich z.B. um die Kongruenzen zu Idealen I und J, so bedeutet das $J \subseteq I$, Nun kann man den Ergänzungssatz so formulieren

Weiteres Abstrahieren/Abbilden bedeutet Vergröbern des Kerns

Satz 12.4 Homomorphie- und 2.Isomorphiesatz. *Sei ϕ ein Homomorphismus von M in K und $\approx$ eine Kongruenzrelation auf K. Dann erhält man eine Kongruenzrelation $\sim$, die Vergröberung des Kerns $\sim_\phi$ ist, durch die Definition*

$$x \sim y \;\Leftrightarrow\; \phi(x) \approx \phi(y).$$

Ist $\phi : M \to K$ surjektiv, so ergibt das eine bijektive Entsprechung zwischen den Kongruenzrelationen auf K und den den Kern $\sim_\phi$ vergröbernden Kongruenzrelationen auf M. Es gilt dann

$$M/\sim \;\cong\; K/\approx$$

$a \in E$ oder $a^{-1} \in E$. Nämlich Beweis. Wir betracten zunächst wieder den Fall der Mengen. $x \sim x$, da $\phi(x) \approx \phi(x)$ nach (E1) für $\approx$. Gilt $x \sim y$, so $\phi(x) \approx \phi(y)$, also $\phi(y) \approx \phi(x)$ nach (E2) für $\approx$, also $y \sim x$. Gelten $x \sim y$ und $y \sim z$, so $\phi(x) \approx \phi(y)$ und $\phi(y) \approx \phi(z)$, also $\phi(x) \approx \phi(z)$ nach (E3) für $\approx$ und somit $x \sim z$. Ist $\phi : M \to K$ surjektiv und $\sim$ Vergröberung von $\sim_\phi$, so gibt es nach dem Ergänzungssatz eine Abbildung χ von K auf $M/\sim$ mit $\chi \circ \phi = \psi$, die kanonische Projektion. Mit $\approx$ als Kern von χ hat man die $\sim$ entsprechende Äquivalenzrelation von K und nach dem Ergänzungssatz die Bijektion von $K/\approx$ auf $M/\sim$. Kommt algebraische Struktur hinzu, ist nur die Veträglichkeit von $\sim$ nachzuweisen. Aus $a_i \sim b_i$ folgt $\phi a_i \approx \phi b_i$ also

$$\phi f^M(a_1, \ldots, a_n) = f^K(\phi a_1, \ldots, \phi a_n) = f^K(\phi b_1, \ldots, \phi b_n) = \phi f^M(b_1, \ldots, b_n)$$

$$f^M(a_1, \ldots, a_n) \sim f^M(b_1, \ldots, b_n) \qquad \square$$

Korollar 12.5 *Für die Ringe bzw. Gruppen $\mathbb{Z}$, $\mathbb{Z}/(n)$ und $\mathbb{Z}/(m)$ sind die folgenden Aussagen sind äquivalent*

(1) Es gibt einen surjektiven Homomorphismus von $\mathbb{Z}/(n)$ auf $\mathbb{Z}/(m)$

(2) Es gibt einen Homomorphimsus $\chi : \mathbb{Z}/(n) \to \mathbb{Z}(m)$ mit $a[\mathsf{mod}m] = \chi(a[\mathsf{mod}n])$

(3) Kongruenz modulo m ist gröber als Kongruenz modulo n:

$$\forall x.\forall y.\;\; x \equiv y\,(\mathsf{mod}n) \;\Rightarrow x \equiv y\,(\mathsf{mod}m)$$

(4) m teilt n. d.h. es gibt $q \in \mathbb{Z}$ mit $n = qm$.

Beispiel: Wenn man die Uhr von 24er-Modus auf 12er-Modus umstellt, verliert man Information, aber das Chaos hält sich in Grenzen. Beweis. (3) $\Leftrightarrow$ (2) $\Rightarrow$ (1) sofort aus dem Satz. (1) $\Rightarrow$ (2) für Ringe folgt daraus, dass es nach Kor. 3.15 höchstens einen Homomorphimsus von $\mathbb{Z}/(n)$ in $\mathbb{Z}/(m)$ gibt. Für Gruppen als Übung. Ist $n = qm$ und n Teiler von $x - y$, so auch m. Sei umgekehrt (3) angenommen. Es gilt $n \equiv 0(\mathsf{mod}n)$, also auch $n \equiv 0(\mathsf{mod}m)$, d.h. m teilt n. $\square$

Korollar 12.6 *Die Kongruenzrelationen auf $\mathbb{Z}/(n)$ entsprechen den $\equiv (\mathsf{mod}n)$ vergröbernden Kongruenzrelationen von $\mathbb{Z}$.*

13 Struktur direkter Produkte und Summen

13.1 Direkte Summen endlich vieler Faktoren

Sei I endlich z.B. $= \{1, \ldots, n\}$. Wir setzen nun voraus, dass die Signatur genau eine Konstante e enthält und dass dass gilt:

$$f(e, \ldots, e) = e \quad \text{für jede fundamentale Operation } f$$

Dann hat man für jedes $i \in I$ eine Unterstruktur der direkten Produkts

$$U_i = \{ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \mid a_i = 0\} \subseteq \prod_i A_i$$

Dann kann man $\bigoplus_{i\in I} A_i := \prod_{i\in I} A_i$ als "direkte Summe" der U_i auffassen. Wir diskutieren das für r-Moduln. Hier hat man $e = 0$. Sei ${}_RV$ ein R-Modul mit Untermoduln U_i, $i \in I$.

$$\sum_{i\in I} U_i = \{\sum_{j\in J} u_j \mid J \subseteq I \text{ endlich }, u_j \in U_j \text{ für alle } j \in J\}$$

ist der von der Vereinigung $\bigcup_{i\in I} U_i$ der Untermoduln U_i erzeugte Untermodul von ${}_RV$, d.h. der kleinste Untermodul, der alle U_i umfasst, und heisst deren *Summe* . Ebenso ist der Schnitt `[intersection]` ein Untermodul

$$\bigcap U_i = \{v \in V \mid v \in U_i \text{ für alle } i \in I\}$$

Satz 13.1 *Für gegebene Untermoduln U_i und U eines Moduls ${}_RV$ sind äquivalent:*

- *(1) $U = \sum_{i\in I} U_i$ und für alle endlichen $J \subseteq I$ folgt aus $\sum_{j\in J} u_j = 0$, $u_j \in U_j$ dass $u_j = 0$ für alle $j \in J$*
- *(2) Für jedes u aus U gibt es (bis auf die Reihenfolge) genau eine Darstellung $u = \sum_{j\in J} u_j$ mit $J \subseteq I$ endlich, $u_j \in U_j$, $u_j \neq 0$ für alle $j \in J$*
- *(3) $U = \sum_{i\in I} U_i$ und $U_i \cap \sum_{j\in J} U_j = 0$ für alle endlichen $J \subseteq I$ und $i \notin J$*
- *(4) Falls $I = \{1, \ldots, m\}$: $U = U_1 + \ldots + U_m$ und $(U_1 + \ldots + U_{k-1}) \cap U_k = 0$ für $1 < k \leq m$.*
- *(5) $(u_i | i \in I) \mapsto \sum u_i$ ist ein Isomorphismus von der direkten Summe $\bigoplus_{i\in I} U_i$ auf U*

Beweis. (1) $\Rightarrow$ (2): Aus $u = \sum u_i = \sum u'_i$ folgt $0 = \sum v_i$ mit $v_i = u_i - u'_i$, dabei braucht man natürlich nur über die $v_i \neq 0$ zu summieren. Gäbe es solche, so hätte man eine nichttriviale Darstellung von 0 in Widerspruch zu (1). (2) $\Rightarrow$ (3): z.B. $i = 1$. Aus $u_1 = 0 + u_2 + \ldots + u_k$ folgt $u_1 = 0$.
(3) $\Rightarrow$ (1): Sei $0 = \sum u_i$ und z.B. $u_k \neq 0$. Dann $-u_k = u_1 + \ldots + u_{k-1}$ in $U_k \cap (U_1 + \ldots + U_{k-1})$, also $u_k = 0$.
(3) $\Rightarrow$ (4) ist trivial, (4) $\Rightarrow$ (1) wie eben. (5) $\Leftrightarrow$ (2) ist klar. $\square$

13.2 Produkte beschrieben durch Kongruenzen: 2 Faktoren

Hier zunäxchst der Fall von nur 2 Faktoren, Sei $A = A_1 \times A_2$. Dann hat man die kanonischen Projektionen

$$\pi_1(x_1, x_2) = x_1, \quad \pi_2(x_1, x_2) = x_2$$

mit den Kern-Kongruenzen θ_i

$$(x_1, x_2)\theta_1(y_1, y_2) \Leftrightarrow x_1 = y_1, \quad (x_1, x_2)\theta_2(y_1, y_2) \Leftrightarrow x_2 = y_2$$

Es gilt

$$\theta_1 \cap \theta_2 = \mathsf{id}_1$$

nämlich

$$(x_1, x_2)\,\theta_1\,(y_1, y_2) \text{ und } (x_1, x_2)\,\theta_2\,(y_1, y_2);\ \Rightarrow x_1 = y_1 \text{ und } x_2 = y_2$$

also $(x_1, x_2) = (y_1, y_2)$. Wir definieren nur für beliebige binäre Relationen θ und τ auf einer Menge M das *Produkt*

$$a(\theta \circ \tau)b \ \Leftrightarrow \ \text{ es gibt } c \text{ mit } a\,\theta\,c\,\tau\,b$$

Dann gilt hier

$$\theta_1 \circ \theta_2 = A \times A$$

d.h. man erhält die totale Relation auf A. In der Tat,

$$(x_1, x_2)\,\theta_1\,(x_1, y_2)\,\theta_2\,(x_2, y_2)$$

Satz 13.2 *$A \cong A_1 \times A_2$ genau dann, wenn es Kongruenzen θ_1 und θ_2 auf A gibt mit*

$$A_i = A/\theta_i, \quad \theta_1 \cap \theta_2 = \mathsf{id}_A, \quad \theta_1 \circ \theta_2 = A^2$$

Die eine Richtung haben wir gerade gezeigt. Für die Umkehrung sei

$$A_i = A/\theta_i \text{ mit kanonischer Projektion } a \mapsto [a]\theta_i$$

Wir definieren

$$\varepsilon : A \to A_1 \times a_2 \text{ mit } \varepsilon(c) = ([c]\theta_1,\ [c]\theta_2)$$

Das ist ein Homomorphismus, weil aus zwei Homomorphismen komponentenweise zusammengesetzt. Für den Kern gilt

$$c\,\mathsf{Ker}(\varepsilon)\,d \Leftrightarrow \ ([c]\theta_1,\ [c]\theta_2) = ([d]\theta_1,\ [d]\theta_2) \ \Leftrightarrow c\,\theta_1\,d \text{ und } c\,\theta_2\,d \ \Leftrightarrow c = d$$

nach Voraussetzung. Also ist ε injektiv. Um die Surjektivität zu zeigen, sei ein Element von $A_1 \times A_2$ gegeben. Das können wir als $([a]\theta_1,\ [b]\theta_2)$ mit passenden $a, b \in A$ schreiben. Gesucht ist also $c \in A$ mit

$$\varepsilon(c) = ([c]\theta_1,\ [c]\theta_2) = ([a]\theta_1,\ [a]\theta_2)$$

Das bedeutet

$$a\,\theta_1\,c \text{ und } c\,\theta_2\,b$$

Ein solches c ist aber durch die Voraussetzung $\theta_1 \circ \theta_2 = A^2$ garantiert. □

Korollar 13.3 *Für einen Ring R gilt $R \cong R_1 \times R_2$ genau dann, wenn es Ideal I_1 und I_2 von R gibt mit*

$$R_i = R/I_i, \;\; I_1 \cap I_2 = 0, \;\; I_1 + I_2 = R$$

Beweis. Ist $R = R_1 \times R_2$ so wähle $I_1 = \{0\} \times R_2$ und $I_2 = R_1 \times \{0\}$. Oder beide Richtungen mit dem Satz: I_i sei das θ_i entsprechende Ideal. Dann entspricht $I_1 \cap I_2$ der Kongruenz $\theta_1 \cap \theta_2$, Also $\theta_1 \cap \theta_2 = \mathsf{id}_R \;\Leftrightarrow I_1 \cap I_2 = 0$. Wir behaupten, dass auch $\theta_1 \circ \theta_2 = R^2 \;\Leftrightarrow I_1 + I_2 = R$. In der einen Richtung haben wir $c \in R$ mit $0\,\theta_1\,c\,\theta_2\,1$, also $c \in I_1$ und $1 - c \in I_2$. In der umgekehrten Richtung haben wir

$$1 = s_1 + s_2 \text{ für passende } s_i \in I_i$$

Gegeben a, b setze

$$c = as_2 + bs_1$$

Dann

$$\begin{aligned} a = a1 = a(s_1 + s_2) = as_1 + as_2 \equiv (\mathsf{mod} I_1)\; bs_1 + as_2 = c \\ b = b1 = b(s_1 + s_2) = bs_1 + bs_2 \equiv (\mathsf{mod} I_2)\, bs_1 + as_2 = c \end{aligned}$$

Noch einmal im Klartext

- Ist $1 = s_1 + s_2$ mit *simultanen Kongruenzen*

$$x \equiv a(\mathsf{mod} I_1), \;\; x \equiv b(\mathsf{mod} I_2)$$

13.3 Produkte beschrieben durch Kongruenzen

Die Äquivalenzrelationen $\theta_1, \ldots, \theta_n$ auf einer Menge M bilden eine *direkte Zerlegung*, wenn

$$\begin{array}{lllll} (*) & \forall a.\forall b. & a\theta_1 b \text{ und } \ldots \text{ und } a\theta_n b & \Rightarrow & a = b \\ (**) & \forall k < n.\forall a.\forall b.\exists c. & a\theta_1 c \text{ und } \ldots \text{ und } a\theta_k c & \text{und} & c\theta_{k+1} b \end{array}$$

Satz 13.4 *Seien $\theta_1, \ldots, \theta_n$ Konrguenzrelationen auf M mit Faktorstrukturen $\pi_i : M \to M_i$. Genau hat man eine direkte Zerlegung, wenn folgende Abbildung ein Isomorphismus ist*

$$\varepsilon : M \to \prod_{i=1}^{n} M_i, \quad \varepsilon a = (\pi_1 a, \ldots, \pi_n a)$$

Beweis. $(*)$ ist äquivalent zur Injektivität von ε, da die Prämisse gerade $\varepsilon a = \varepsilon b$ bedeutet. $(**)$ ist zur Surjektivität von ε gleichwertig ist. Ist nämlich ε surjektiv, so wähle c mit

$$\varepsilon c = (\pi_1 a, \ldots, \pi_k a, \pi_{k+1} b, \ldots, \pi_n b)$$

Umgekehrt zeigen wir durch Induktion über k:

$$\forall a_1 \in M_1 \ldots \forall a_k \in M_k.\; \exists a \in M.\;\; \pi_1 a = a_1 \wedge \ldots \wedge \pi_k a = a_k$$

Sind $a_i \in M_i$, $i = 1, \ldots k+1$ gegeben, so wähle $a \in M$ zu $a_1, \ldots, a_k$ nach Induktionsannahme und und $b \in M$ mit $\pi_{k+1} b = a_{k+1}$. Wähle nun c nach $(**)$. Dann $\pi_i c = a_i$ für $i \leq k = 1$. $\square$.

Satz 13.5 *$A \cong A_1 \times \ldots \times A_n$ genau dann, wenn es Kongruenzen θ_i auf A gibt mit*

$$A_i = A/\theta_i,\ \ \theta_1 \cap \ldots \cap \theta_n = \mathsf{id}_A,\ \ (\theta_1 \cap \ldots \cap \theta_k) \circ \theta_{k+1} = A^2 \text{ für } k = 1, \ldots .n-1$$

Der Isomorphismus ist gegeben durch

$$c \mapsto ([c]\theta_1, \ldots, [c]\theta_n)$$

Die Bedingung besagt, dass die θ_i eine drrekte Zerlegung bilden. Also könen wir den vorangehenden Satz anwenden. Direkter Beweis durch Induktion über k: $c \mapsto \varepsilon_k(c) = ([c]\theta_1, \ldots, [c]\theta_k)$ ist surjektiver Homomorphismus $A \to A_1 \times \ldots \times A_k$ mit Kern $\tau_k = \theta_1 \cap \ldots \cap \theta_k$. Im Schritt von k nach $k+1$ ist nach der Voraussetzung des Satzes und dem Fall $n = 2$ die Abbildung $c \mapsto \eta(c) = ([c]\tau_k, [c]\theta_{k+1})$ ein surjektiver Homomorphimsmus $A \to A/\tau_k \times A_{k+1}$ mit Kern $\tau_k \cap \theta_{k+1} = \tau_{k+1}$. Nach dem Homomorphiesatz und der Induktionsannahme haben wir einen Isomorphismus $\omega : A/\tau_k \to A_1 \times \ldots \times A_k$ mit $\varepsilon_k(c) = \omega([c]\tau_k)$. Mit dem Isomorphismus $(x, y) \mapsto \hat{\omega}(x, y) = (\omega(x), y)$ von $A./\tau_k \times A_{k+1}$ auf $A_1 \times \ldots \times A_k \times A_{k+1}$ (vgl. Lemma ??) erhalten wir $\varepsilon_{k+1}(c) = \hat{\omega}([c]\tau_k, [c]\theta_{k+1})$ und die Behauptung. □

Korollar 13.6 *Für einen Ring R gilt $R \cong R_1 \times \ldots \times R_n$ genau dann, wenn es Ideale I_i auf R gibt mit*

$$R_i = A/I_i,\ \ I_1 \cap \ldots \cap I_n = 0,\ \ I_j + I_k = R \text{ für alle } i \neq j$$

Insbesondere gilt

$$R = I_1' + \ldots + I_n' \quad \text{mit } I_j' = \bigcap_{i \neq j} I_i$$

und man erhält (die eindeutig bestimmte) Lösung c der simultanen Kongruenzen

$$x \equiv b_1 (\mathsf{mod} I_1). \ldots, x \equiv b_n (\mathsf{mod} I_n)$$

durch

$$c = b_1 a_1 m_1' + \ldots + b_n a_n m_n' \ \ \text{falls } 1 = a_1 m_1' + \ldots + a_n m_n'$$

Beweis. Für Ideale I, J, K eines Ringes mit $I + K = R = J + K$ gilt auch $(I \cap J) + K = R$. In der Tat, wegen $I + K = R$ gibt es $a \in I$ und $b \in K$ mit $a + b = 1$ und für $x \in J$ folgt $x = x1 = x(a + b) = xa + xb \in (I \cap J) + (K \cap J)$ da $xa \in I \cap j$ und $xb \in K \cap J$. Also $J \subseteq (I \cap J) + (K \cap J)$ und es gilt Gleichheit, weil $\supseteq$ trivial ist (vgh. H7d). Nun $I \cap J) + K = (I \cap J) + (K \cap J) + K = J + K = R$ nach Voraussetzung.

Mit Induktion folgt nun sofort aus den Voraussetzungen des Korollars: $(I_1 \cap \ldots \cap I_k) + I_{k+1} = R$. Die Aussage über die I_i' folgt sofort mit $k = n - 1$ und Permutation der Indices. Und z.B.

$$b_1 = b_1 1 = b_1 a_1 m_1' + b_1 a_2 m_2' + \ldots \equiv (\mathsf{mod} I_1)\ b_1 a_1 m_1' + b_2 a_2 m_2' + \ldots = c$$

da $m_k' \in I_k' \subseteq I_1$ für $k \neq 1$. □

Wir haben also die direkte Zerlegung von R als R-Modul

$$R = I_1' \oplus \ldots \oplus I_n'$$

Dabei sind die I'_k jedooch keine Unterringe, da sie 1 nicht enthalten. Aus der Isomorphie zu $\prod_i R_i$ folgt jedoch sofort, dass es in I'_i ein Element e_i gibt mit

$$e_i \in I_i, \;\; r \in I_i \Leftrightarrow r = e_i r$$

$$1 = e_1 + \ldots + e_n, \; e_i^2 = e_i, \; e_i e_j = 0 \text{ für } i \neq j, \; re_i = e_i r \text{ für alle } r \in R$$

Nämlich e_i entspricht $(r_1, \ldots, r_n)$ mit $r_i = 1$ und $r_j = 0$ für $j \neq i$. Eine solche Familie heisst auch eine System *orthogonaler zentraler Idempotente* und steht in 1-1-Entsprechug mit den direkten Zerlegungen.

13.4 Chinesischer Restsatz

Satz 13.7 Chinesischer Restsatz. *Sei R ein euklidischer Ring. Für $m_1, \ldots, m_n \in R$ und $m = m_1 \cdot \ldots \cdot m_n$ betrachet man die simultanen Kongruenzen*

$$(*) \quad x \equiv b_1 \,(\mathsf{mod}\ \mathsf{m_1}), \ldots, \mathsf{x} \equiv \mathsf{b_n} \,(\mathsf{mod}\ \mathsf{m_n})$$

und den Ring-Homomorphismus (soagr R-Algebra-Homomorphismus)

$$\phi : R/(m) \to R/(m_1) \times \ldots \times R/(m_n) \;\; \textit{mit } a[\mathsf{mod}\ \mathsf{m}] \mapsto (\mathsf{a}[\mathsf{mod}\ \mathsf{m_1}], \ldots, \mathsf{a}[\mathsf{mod}\ \mathsf{m_n}])$$

Dann sind die folgenden Aussagen äquivalent

(1) ϕ ist bijektiv (und damit Isomorphismus)

(2) Zu allen $b_1, \ldots, b_m \in R$ gibt es Lösung $a \in R$ von (*) eindeutig bis auf Kongruenz modulo m

(3) Die $m_1, \ldots, m_n$ sind paarweise teilerfremd

Zusatz: $a = b_1 a_1 \frac{m}{m_1} + \ldots + b_n a_n \frac{m}{m_n}$ löst $(*)$ falls $1 = a_1 \frac{m}{m_1} + \ldots + a_n \frac{m}{m_n}$.

Beweis. Die angegebene Abbildung ist ein Homomorphimsus von $R/(m)$ in $R/(m_1) \times \ldots \times R/(m_n)$, weil es in jeder Komponente einer ist. Die Lösbarkeit aller simultanen Kongruenzen $(*)$ bedeutet aber gerade die Surjektivität dieser Abbildung, die Eindeutigkeit die Injektiviät. Also sind (1) und (2) äquivalent. (1) $\Leftrightarrow$ (3) nach Kor. ??.

Der Zusatz folgt so

$$b_i a_i \frac{m}{m_i} \equiv 0 \equiv b_1 a_i \frac{m}{m_i} \,(\mathsf{mod}\ \mathsf{m_1}) \qquad \text{für } \mathsf{i} > 1$$

$$a \equiv b_1 a_1 \frac{m}{m_1} + b_1 a_2 \frac{m}{m_2} + \ldots + b_1 a_n \frac{m}{m_n} \equiv b_1 (a_1 \frac{m}{m_1} + \ldots + a_n \frac{m}{m_n}) \equiv b_1 \,(\mathsf{mod}\ \mathsf{m_1})$$

und ebenso für $m_2, \ldots, m_n$. $\square$.

13.5 Chinesischer Restsatz für ganze Zahlen

Lemma 13.8 *Ist d grösster gemeinsamer Teiler der $k_1, \ldots, k_n$, so gibt es*

$$a_i \in \mathbb{Z} \text{ mit } d = a_1k_1 + \ldots + a_nk_n$$

Beweis und Algorithmus. Falls $n = 2$ nach Bezout (erweiterter euklidischer Algorithmus). Für $n > 2$ rekursiv.

- Bestimme c_i mit $d_{n-1} = \text{GGT}(k_1, \ldots, k_{n-1}) = c_1k_1 + \ldots + c_{n-1}k_{n-1}$
- $d = \text{GGT}(d_1, k_n)$. Bestimme b, a_n mit $d = bd_{n-1} + a_nk_n$
- $a_1 = bc_1, \ldots, a_{k-1} = bc_{k-1}$ $\square$

Satz 13.9 Chinesischer Restsatz `[Chinese Remainder Theorem]`. *Für $m_1, \ldots, m_n \in \mathbb{Z}$ und $m = m_1 \cdot \ldots \cdot m_n$ sind die folgenden Aussagen äquivalent*

(1) $\mathbb{Z}/(m) \cong \mathbb{Z}/(m_1) \times \ldots \times \mathbb{Z}/(m_n)$ *(mit* $a[\mathsf{mod}m] \mapsto (a[\mathsf{mod}m_1], \ldots, a[\mathsf{mod}m_n])$*)*

(2) Zu allen $b_1, \ldots, b_m \in \mathbb{Z}$ gibt es (bis auf Kongruenz modulo m eindeutig bestimmte) ganzzahlige Lösung a der simultanen Kongruenzen

$$(*) \quad x \equiv b_1 \,(\mathsf{mod}m_1), \ldots, x \equiv b_n \,(\mathsf{mod}m_n)$$

(3) Die $m_1, \ldots, m_n$ sind paarweise teilerfremd `[pairwise prime]`

$a = b_1a_1\frac{m}{m_1} + \ldots + b_na_n\frac{m}{m_n}$ *löst* $(*)$ *falls* $1 = a_1\frac{m}{m_1} + \ldots + a_n\frac{m}{m_n}$.

Beweis. Die angegebene Abbildung ist nach Kor.3.7 und Lemma 1.15 ein Homomorphimsus von $\mathbb{Z}/(m)$ in $\mathbb{Z}/(m_1) \times \ldots \times \mathbb{Z}/(m_n)$ und nach Kor. 1.14 der einzige. Die Lösbarkeit aller simultanen Kongruenzen $(*)$ bedeutet aber gerade die Surjektivität dieser Abbildung, die Eindeutigkeit die Injektiviät. Da $\mathbb{Z}/(m)$ und $\mathbb{Z}/(m_1) \times \ldots \times \mathbb{Z}/(m_n)$ beide m-elementig sind, ist hier Surjektivität und Injektivität gleichbedeutend, d.h. Existenz- und Eindeutigkeits-Aussage von (2). Der Zusatz folgt so

$$b_ia_i\frac{m}{m_i} \equiv 0 \equiv b_1a_i\frac{m}{m_i} \,(\mathsf{mod}m_1) \quad \text{für } i > 1$$

$$a \equiv b_1a_1\frac{m}{m_1} + b_1a_2\frac{m}{m_2} + \ldots + b_1a_n\frac{m}{m_n} \equiv b_1(a_1\frac{m}{m_1} + \ldots + a_n\frac{m}{m_n}) \equiv b_1 \,(\mathsf{mod}m_1)$$

und ebenso für $m_2, \ldots, m_n$. Also folgt aus (3) die Lösbarkeit simultaner Kongruenzen mit dem Lemma angewandt auf $k_i = \frac{m}{m_i}$. Ist die Eindeutigkeit vorausgesetzt, so betrachte

$$x \equiv 0 \,(\mathsf{mod}m_1), \ldots, x \equiv 0 \,(\mathsf{mod}m_n)$$

Jedes Vielfache des KGV der $m_1, \ldots, m_n$ ist eine Lösung, insbesondre m. Wegen der Eindeutigkeit ist m das KVG, also sind die $m_1, \ldots, m_n$ paarweise teilerfremd. $\square$.

13.6 Partialbruchzerlegung

Satz 13.10 *Jedes Element $\frac{f}{g}$ aus dem Quotientenkörper eines euklidischen Rings kann als $q+$ Summe von* Partialbrüchen $\frac{h}{p^k}$ *geschrieben werden mit irreduziblen $p|g$, $\delta h < \delta p$ und $\delta q < \delta f$.*

Beweis. Sei $g = p_1^{k_1} \cdot \ldots \cdot p_m^{k_m}$ mit primen p_i und

$$q_i = p_1^{k_1} \cdot \ldots \cdot p_{i-1}^{k_{i-1}} \cdot p_{i+1}^{k_{i+1}} \cdot \ldots \cdot p_m^{k_m}$$

Nach dem Chinesischen Restsatz gibt es

$$f = a_1 q_1 + \ldots + a_m q_m, \quad \frac{f}{g} = \frac{a_1}{p_1^{k_1}} + \ldots + \frac{a_m}{p_m^{k_m}}$$

Es bleibt also die Behauptung für Quotienten $\frac{a}{p^k}$ zu zeigen. Das geht mit Induktion über k. Dazu durch Division mit Rest ergibt

$$a = bp + r, \quad \frac{a}{p^k} = \frac{r}{p^k} + \frac{b}{p^{k-1}} \quad \text{mit } \delta r < \delta p \quad \square$$

14 Endlich erzeugte Moduln über euklidischen Ringen

14.1 Untermoduln freier Moduln

Aus dem Invariantenteilersatz erhält man

Korollar 14.1 *Zu jedem R-Untermodul U eines freien R-Moduls F von Rang n über dem euklidischen Ring R gibt es eine Basis $f_1, \ldots, f_n$ von F, $r \leq n$ und $d_i \in R$ mit $d_i | d_{i+1}$, $i < n$ so, dass $d_1 f_1, \ldots, d_r f_r$ Basis von U ist. Insbesondre ist U ein freier R-Modul von Rang r.*

Algorithmus. Ist eine Basis $\alpha : e_1, \ldots, e_n$ von F gegeben und ein Erzeugendensystem a_i von U, so sei $\mathcal{A}$ die Matrix, deren Spalten die Koordinaten der $(a_i)^\alpha$ sind. In $\mathcal{B}$ notieren wir die Koordinaten $(f_j)^\alpha$ der jeweils gültigen Basis $f_1, \ldots, f_n$, d.h. am Anfang ist $\mathcal{B}$ die $n \times n$-Einheitsmatrix. Bei jeder Zeilenumformung von $\mathcal{A}$ führen wir die entsprechende Spaltenumformung von $\mathcal{B}$ aus. Haben wir $\mathcal{A}$ in $\mathcal{D}$ überführt, so hat die gesuchte Basis $\beta : f_1, \ldots, f_n$ als Koordinaten $(f_j)^\alpha$ die Spalten von $\mathcal{B}$. Wir wählen r maximal, mit $d_r \neq 0$.

Beweis. $d_i \neq 0$ für alle $i \leq r$. Dann wird U nach Lemma ?? auch von den Elementen erzeugt, deren Koordinaten bzgl. β die ersten r Spalten von $\mathcal{D}$ sind, d.h. von den $d_1 f_1, \ldots, d_r f_r$. Diese erzeugen U jedoch frei: Aus $\sum_{i=1}^r r_i d_i f_i = 0$ folgt $r_i d_i = 0$ (da die f_j eine Basis von F bilden) und $r_i = 0$ wegen der Nullteilerfreiheit. $\square$ Ist U nicht schon als endlich erzeugt gegeben. muss man beim Invariantenteilersatz nachbesseren und auch unendliche viele Spalten erlauben, darf aber auch passende Vielfache einer Spalte simultan von unendlich vielen anderen Spalten abziehen. Dann sind nach endlicher Zeit alle Spalten bis auch endlich viele zu Nullspalten geworden. Und die Nullspalten darf man einfach weglassen.

14.2 Struktursatz

Theorem 14.2 *Jeder n-erzeugte R-Modul über einem euklidischen Ring R ist isomorph zu einem direkten Produkt $R/Rd_1 \times \ldots \times R/Rd_n$ zyklischer Moduln.*

Dabei heisst ein Modul *zyklisch*, wenn er von einem Element erzeugt wird, also homomorphes Bild von R ist.

Korollar 14.3 *Jede n-erzeugte abelsche Gruppe ist isomorph zu einem direkten Produkt $\mathbb{Z}/(d_1) \times \ldots \times \mathbb{Z}/(d_n)$ zyklischer Gruppen.*

Korollar 14.4 *Für einen euklidischen Ring R ist jeder zyklische R-Modul M von der Form R/Rd d.h. präsentiert durch e_1; $de_1 \stackrel{!}{=} 0$ und d ist durch den Isomorphietyp von M bis aud Assoziiertheit eindeutig bestimmt. Eine zyklische abelsche Gruppe ist von der Form $\mathbb{Z}/(d)$.*

d ist eindeutig dadurch bestimmt, dass $dx = 0$ fúr alle $x \in M$. □

Korollar 14.5 *Jeder endlich erzeugte Modul M über einem euklidischen Ring R ist endlich präsentiert und isomorph zu einem direkten Produkt*

$$M \cong R/(p_1^{k_1}) \times \ldots \times R/(p_s^{k_s}), \quad p_i \text{ prim oder } 0$$

primärer zyklischer Moduln. *Hat man eine Präsentierung gegeben, so erhält man diese Zerlegung auf dem Weg über die Diagonalisierung der Präsentierungmatrix und die zugehörige direkte Zerlegung in zyklische Moduln $R/(d_i)$ mit den Diagonaleinträge d_i, die Primfaktorzerlegung der d_i und den chinesischen Reststatz angewendet auf die $R/(d_i)$. Faktoren $R/(1)$ sind trivial und können wegfallen. M ist zyklisch genau dann, wenn die $p_1, \ldots, p_s$ paarweise teilerfremd sind. In diesem Fall sind $p_i^{k_i}$ durch den Isomorphietyp von M bis auf Assoziiertheit eindeutig bestimmt.*

Beweis. Wir haben $M \cong R^n/U$ mit einem Untermodul U. Als Präsentierungsmatix nehmen wir zunächst die Matrix, deren Spalten gerade die Elemente von U sind. Nach dem Satz über invariante Teiler gibt es eine Basis von R^n bzgl. deren die Präsentierung durch eine Diagonalmatrix gegeben wird. Die Eindeutigkeit im zyklischen Fall folgt aus der eindeutigen Primfaktorzerkegung. □

14.3 Modul zu einer linearen Abbildung

Ist V ein K-Vektorraum und ϕ ein *Endomorphismus*. d.h. K-lineare Abbildung von V in sich, so wird V durch Einsetzen von ϕ zum $K[x]$-Modul ${}_{K[\phi]}V$

$$f(x)v = f(\phi)(v) = r_0 v + r_1\phi(v) + r_2\phi^2(v) + \ldots + r_n\phi^n(v) \text{ für } f(x) = \sum_{i=0}^{m} r_i x^i$$

vgl.Übung. Die Untermoduln sind gerade die *ϕ-invarianten* K-Untervektorräume (d.h. $\phi(u) \in U$ für alle $u \in U$).

Jeder $K[x]$-Modul M ist von dieser Art: Er ist ein K-Vektorraum, da $K[x]$ eine K-Algebra ist und man definiert eine lineare Abbildung ϕ mit $f(\phi)(v) = f(x)v$ durch

$$\phi(v) := xv \in M.$$

Literatur: F.Lorenz, Lineare Algebra II: B.Hartley, T.O.Hawkes. Rings,Modules and Linear Algebra; F.R.Gantmacher, The Theory of Matrices

14.4 Annullator

Ist M ein R-Modul, so ist (wie man leicht sieht)

$$I = Ann_R M = \{r \in R \,|\, \forall v \in M : rv = 0\}$$

ein Ideal von R, der *Annullator*.

$$Ann_R M = \{r \in R \,|\, re_1 = \ldots = re_n = 0\} \text{ falls } M \text{ erzeugt von } e_1, \ldots, e_n.$$

M wird auf natürliche Weise zum $R/Ann_R M$-Modul

$$\tilde{r}v = rv.$$

Da der Ring R euklidisch ist, ist der Annullator ein Hauptideal. Hat man einen $K[x]$-Modul, so wird der Annullator erzeugt von einem Polynom $m(x)$ kleinsten Grades so, dass $m(\phi) = 0$ die Nullabbildung ist: $m(\phi)(v) = 0$ für alle $v \in V$. Ist $m(x) = x^n + r_{n-1}x^{n-1} + \ldots + r_0$ normiert auf Leitkoeffizient 1, so ist's eindeutig bestimmt und heisst das *Minimalpolynom* von ϕ bzw. dessen Matrix A.

14.5 Zyklische Moduln

Ein R-Modul M heisst *zyklisch*, wenn er von einem Element g erzeugt wird: $M = Rg$.

Proposition 14.6 *Die zyklischen R-Moduln $M = Rg$ sind gerade die Moduln mit Präsentation*

$$g;\ mg \stackrel{!}{=} 0$$

Dabei $(m) = Ann_R M$ und $M \cong R/(m)$. Insbesondre M frei genau dann, wenn $m = 0$.

Das ist klar, aber doch noch'n Beweis. Da R von 1 frei erzeugter R-Modul ist, gibt es eine R-lineare Abbildung π von R auf M mit $\pi(1) = g$. Dann ist Kern$\pi = Ann_R M = (m)$, da jedes Ideal eine euklidischen Ringes Hauptideal ist. Nach dem Homomorphiesatz $M \cong R/(m)$, dem Modul mit Präsentation $g;\ mg \stackrel{!}{=} 0$. □

Satz 14.7 *Ein $K[x]$-Modul ${}_{K[\phi]}V$ ist zyklisch mit Erzeugendem v_0 und Minimalpolynom $m = m(x) = \sum r_i x^i$ vom Grad n genau dann, wenn der K-Vektorraum V Dimension n und folgende Basis hat und ϕ bzgl. dieser die* Frobenius-*Matrix A zum Polynom $m(x)$*

$$v_0, \phi(v_0), \phi^2(v_0), \ldots, \phi^{n-1}(v_0), \quad A = \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & -r_0 \\ 1 & 0 & 0 & \ldots & 0 & -r_1 \\ 0 & 1 & 0 & & 0 & -r_2 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & & & 0 & -r_{n-2} \\ 0 & 0 & & \ldots & 1 & -r_{n-1} \end{pmatrix}$$

Und $m(x) = (x - \lambda)^n$ genau dann, wenn ϕ bzgl. folgender Basis als Matrix die transponierte eines Jordanblock $J_{\lambda,n}$

$$v_0, (\phi - \lambda id)(v_0), \ldots, (\phi - \lambda id)^{n-1}(v_0), \quad J_{\lambda,n} = \begin{pmatrix} \lambda & 0 & 0 & \ldots & 0 \\ 1 & \lambda & 0 & & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & & 1 & \lambda & 0 \\ 0 & & \ldots & 1 & \lambda \end{pmatrix}.$$

Will man den Jordanblock selbst haben, so muss man die Basis rückwärts lesen.

Beweis. Ist $R = K[x]$, so $m = m(x)$ von Grad n genau dann, wenn $K[x]/(m(x))$ ein n-dimensionaler K-Vektorraum ist mit Basis $1, x, x^2, \ldots, x^{n-1}$ modulo $(m(x))$. Das überträgt sich dann mit dem Isomorphismus auf V mit $1 + (m(x)) \mapsto v_0$. Dass A die Matrix von ϕ ist ergibt sich aus

$$m(\phi)(v) = 0 \text{ also } \phi^n(v) = -(r_0 + r_1\phi(v) + \ldots + r_{n-1}\phi^{n-1}(v)).$$

Die $(x-\lambda)^k$ erzeugen den K-Vektorraum $K[x]$: man erhält induktiv alle x^k im Erzeugnis, da $(x-\lambda)^k = x^k + p_k(x)$ mit einem Polynom $p_k(x)$ vom Grad $< k$. Folglich erzeugen die $(x-\lambda)^k$, $k < n$, modulo $m(x) = (x-\lambda)^n$ den Vektorraum $K[x]/(m(x))$ und bilden eine Basis (da wir schon dim $= n$ wissen). Dass die Matrix so aussieht, sieht man an

$$x(x-\alpha)^k = (x-\lambda)^k(\lambda + x - \lambda) = \lambda(x-\lambda)^k + (x-\lambda)^{k+1}. \quad \square$$

14.6 Normalformen

Theorem 14.8 *Jeder Endomorphismus eines endlichdimesionalen K-Vektorraums kann bzgl. einer geigeneten Basis beschrieben werden durch eine Matrix, die blockdiagonal zusammengesetzt ist aus Frobeniusmatrizen zu Polynomen $m_i(x) \in K[x]$. Dabei kann man verlangen*

- $m_i(x)|m_{i+1}(x)$ *für alle i,* Frobenius- *oder* rationale Normalform *mit* invarianten Teilern $m_i(x)$
- $m_i(x) = p_i(x)^{k_i}$ *mit primem $p_i(x)$,* Weierstrass-Normalform *mit* Elementarteilern $p_i(x)^{k_i}$
- *Ist K algebraisch abgeschlossen, z.B. $K = \mathbb{C}$, so kann man in der Weierstrass-Normalform die Frobeniusmatrizen durch Jordanblöcke ersetzen und erhält die* Jordan-Normalform

Beweis. Folgt sofort aus den beiden Struktursätzen und der Beschreibung der zyklischen Moduln. $\square$ Auch der Rechenweg ist klar, wenn man einmal eine Präsentierung des $K[x]$-Moduls hat.

14.7 Charakteristische Matrix

Theorem 14.9 *Sei V ein K-Vektorraum mit Basis $\alpha : e_1, \ldots, e_n$ und sei ϕ eine K-lineare Selbstabbildung von V mit Matrix A bzgl. α. Bzgl. der Erzeuger $e_1, \ldots, e_n$ des $K[x]$-Moduls ${}_{K[\phi]}V$ gilt:*

die charakteristische Matrix $A - xE$ *von ϕ ist eine Präsentierungmatrix von* ${}_{K[\phi]}V$.

Beweis: Jeder $K[x]$-Modul mit durch e_i bezeichneten Erzeugern, der die Relationen in $A-xE$ erfüllt, wird schon als K-Modul von disen erzeugt. Und man kennt den durch ϕ bestimmten $K[x]$-Modul ${}_{K[\phi]}V$, wenn man weiss, wie die Basisverktoren abgebildet werden. Diese Information steckt aber gerade in der Matrix A und die Matrix $A-xE$ schreibt's um in Relationen des $K[x]$-Moduls. $\square$. Wir stellen dazu zunächst fest, dass die Erzeuger e_i des Moduls ${}_{K[\phi]}V$ die durch $A - xE$ gegebenen Relationen erfüllen: das ist gerade die Zuordnung von A zu ϕ:

es gilt $\phi(e_j) = \sum_i a_{ij} e_i$. Folglich gibt es eine surjektive $K[x]$-lineare Abbildung $\tilde{\chi}$ vom freien $K[x]$-Modul M mit Präsentierungsmatrix $A - xE$ auf ${}_{K[\phi]}V$ mit $e_i \mapsto e_i$. M wird von den $\tilde{\chi}(e_i)$ als $K[x]$-Modul erzeugt. M ist auch ein K-Vektorraum. Der von den $\tilde{\chi}(e_i)$ erzeugte K-Untervektorraum U von ist aber auch ein $K[x]$-Untermodul, da $x\tilde{\chi}(e_j) = \sum_i a_{ij}\tilde{\chi}(e_i)$ wegen der Präsentierung. Also $U = M$ und somit $\dim_K M \leq n$. $\tilde{\chi}$ ist aber auch K-linear. Da es surjektiv ist und $\dim_K V = n$, muss es auch ein Isomorphismus sein. □

14.8 Mehr zur Zerlegung einer linearen Abbildung

Zusatz 1. Die Basis α des freien $K[x]$-Moduls und die Matrix $A - xE$ kann man nach dem Satz von den invarianten Teilern umformen in eine Basis $f_1, \ldots, f_n$ und Diagonalmatrix mit normierten Diagonaleinträgen $1, \ldots, 1, d_s, \ldots, d_n \in K[x]$, $d_i \not\approx 1$ für $i \geq s$, und erhält so eine direkte Zerlegung in zyklische Untermoduln mit Minimalpolynom d_i

$$V = K[x]f_s \oplus \ldots \oplus K[x]f_n$$

$$\text{wobei } f_j = \sum_{i,k} b_{jik}\phi^k(e_i) \text{ in } V \text{ falls } f_j = \sum_i (\sum_k b_{jik}x^k)e_i \text{ im freien Modul.}$$

Zusatz 2. Der K-Vektorraum V hat Basis

$$f_i, \phi(f_i), \ldots, \phi^{n_i-1}(f_i), \quad i = s, \ldots, n, \ n_i = \deg d_i.$$

Bezüglich dieser Basis hat ϕ eine Matrix A', die blockdiagonal zusammengesetzt ist aus den Frobeniusmatrizen oder Begleitmatrizen zu den Polynomen d_i.
Zusatz 3.$\det(A - xE) \approx d_1 \cdot \ldots \cdot d_n$, $n = \dim_K V = \deg \det(A - xE) = \sum_i \deg d_i$.
Zusatz 4. Man kann so umformen, dass $d_i \mid d_{i+1}$ für $i < n$. Dann sind die d_i die bis auf $\approx$ eindeutig bestimmten invarianten Teiler von ϕ, es ist d_n das Minimalpolynom von ϕ und man spricht von A' als Frobenius- oder rationaler Normalform zu A.
Zusatz 5. (Cayley-Hamilton) Das $KGV(d_1, \ldots, d_n)$ ist assoziiert zum Minimalpolynom $m(x)$ von ϕ und teilt das charakeristische Polynom von ϕ. Und per definitionem gilt $m(\phi) = 0$.
Zusatz 6. Zerlegt man die d_i in Potenzen d_{ij} teilerfremder normierter irreduzibler Polynome, $d_i = d_{i1} \cdot \ldots \cdot d_{im_i}$, so erhält man eine direkte Zerlegung in primäre zyklische Untermoduln mit Minimalpolynom d_{ih}

$$V = K[x]f_{s1} \oplus \cdots \oplus K[x]f_{sm_s} \oplus \ldots \oplus K[x]f_{n1} \oplus \cdots \oplus K[x]f_{nm_n}$$

$$\text{wobei } f_{ih} = (d_i/d_{ih})f_i = (d_{i1}(\phi) \circ \ldots d_{i,h-1}(\phi) \circ d_{i,h+1}(\phi) \circ \ldots \circ d_{im_i}(\phi))(f_i) \text{ in } V$$

Zusatz 7. Der K-Vektorraum V hat Basis

$$f_{ih}, \phi(f_{ih}), \ldots, \phi^{n_{ih}-1}(f_{ih}), \quad i = s, \ldots, n, \ h = 1, \ldots, m_i, \ n_{ih} = \deg d_{ih}.$$

Bezüglich dieser Basis hat ϕ eine Matrix A', die blockdiagonal zusammengesetzt ist aus den Frobeniusmatrizen zu den Polynomen $d_i h$.
Zusatz 8. Die Elementarteiler d_{ih} von ϕ sind eindeutig bestimmt und man spricht von A' als Weierstrass-Normalform zu A.
Zusatz 9. Sind die d_{ih} Potenzen linearer Polynome $d_{ih} = (x - \lambda_{ih})^{n_{ih}}$ so hat der K-Vektorraum V die Jordanbasis

$$(\phi - \lambda_{ih}id)^{n_{ih}-1}(f_{ih}), \ldots, (\phi - \lambda_{ih}id)(f_{ih}), f_{ih}, \quad i = s, \ldots, n, \ h = 1, \ldots, m_i.$$

Bezüglich dieser Basis hat ϕ eine Matrix A' die blockdiagonal zusammengesetzt ist aus $n_{ih} \times n_{ih}$ Jordanblöcken $J_{\lambda_{ih},n_{ih}}$
Zusatz 10. Die Zerlegung ist, wenn sie existiert, eindeutig bis auf die Reihenfolge der Blöcke und A' heisst Jordansche Normalform zu A. Man kann eine Zerlegung stets erreichen, indem man zum algebraischen Abschluss von K übergeht.

Beweis. Zusatz 1 und 2 sind klar. Zusatz 3 folgt sofort daraus, dass $\det(A - xE)$ nach LA Leitkoeffizient $(-1)^n$ hat und daraus, dass die Determinante bei Umformungen bis auf eine Einheit unverändert bleibt. Dazu muss man sich klar machen, dass das ebenso für Determinanten über euklidischen Ringen gilt, z.B. weil die Umformung auf Dreicksform und die LR=Zerlegung nach wie vor möglich sind (vgl. Übung).

Die weitere Umformung in Zusatz 4 folgt aus dem Algorithmus zu den invarianten Teilern, die Eindeutigkeit kommt noch. Dass dann d_n Minimalpolynom ist, ist klar. Zusatz 5 ergibt sich daraus, dass die maximalen auftretenden Primpotenzen in den d_i und damit das KGV der d_i eindeutig bestimmt sind. In der Diagonalmatrix aus Zusatz 4 ist das aber d_n und ein Teiler des charakeristischen Polynoms. Die Zusätze 6-10 folgen sofort aus dem Struktursatz und den noh zu beweisenden Eindeutigkeitsaussagen. □

14.9 Eindeutigkeit

Satz 14.10 *Je zwei Basen eines freien R-Moduls über einem euklidischen Ring haben gleiche Elementanzahl - den* Rang

Bem. Ist M ein R-Modul und I ein Ideal von R, so hat man einen Untermodul

$$IM = \{ra \,|\, r \in I,\, a \in M\}.$$

Beweis des Satzes. Wir brauchen's nur für endliche Basen von M. Sei p ein Primelement von R, also $K = R/(p)$ ein Körper. Sei $V = M/(p)M$. Ist $a_1, \ldots, a_n$ eine Basis, so haben wir $M \cong R^n$ und somit $V \cong K^n$ - wir rechnen mit n-Tupeln modulo (p). Somit ist V ein K-Vektorraum und n eindeutig bestimmt.

Derselbe Beweis geht allgemeiner für kommutative Ringe: man muss mit dem Zornschen Lemma zeigen, dass es ein maximales Ideal I gibt. Dann R/I ein Körper (vgl. Übung). □

Theorem 14.11 *In der Zerlegung eines endlich erzeugten Moduls über einem euklidischen Ring in primäre zyklische Moduln sind diese bis auf die Reihenfolge eindeutig bestimmt.*

Beweis. Wir zeigen zunächst, dass s eindeutig bestimmt ist. Dazu nehmen wir an, dass M direktes Produkt nach Kor.5.19 ist

$$M \cong R/(p_1^{k_1}) \times \ldots \times R/(p_l^{k_l}) \times R^s$$

mit primen p_i und betrachten wir den Untermodul $T = R/(p_1^{k_1}) \times \ldots \times R/(p_l^{k_l}) \times 0^s$. T besteht genau aus den *Torsionselementen*

$$T = \{a \in M \,|\, \exists r \in R : r \neq 0 \text{ und } ra = 0\}.$$

Andererseits $M/T \cong R^s$, also freier Modul vom Rang s. Da T durch eine abstrakte Eigenschaft definiert ist, ist der Isomorphietyp von T unabhängig von der konkreten Produktzerlegung und somit s nach obigem Satz eindeutig bestimmt.

Sei nun p ein Primelement und den Untermodul

$$N_p(M) = \{x \in M \mid px = 0\}$$

Nun ist $N_p(M)$ ein $R/(p)$-Vektorraum und dessen Dimension ist gerade die Anzahl der p-primären zyklischen Summanden, d.h. der $p_i \approx p$.

Bilden wir den Faktormodul $M/N_p(M)$, so wird aus einem Summanden $R/(p^k)$ von M ein Summand $R/(p^{k-1})$ von $M/N_p(M)$. Damit können wir induktiv die Anzahl dieser Summanden bestimmen. Explizit ist die Anzahl der Summanden $R/(p^k)$ gerade

$$\dim M/N_p^{k-1}(M) - \dim M/N_p^k(M)$$

d.h. gerade die, die nach $k-1$-maligem Faktorisieren eindimensionale Vektorräume geworden sind und dann beim nächsten Faktoriseren verschwinden. □

Alternativ können wir mit Untermoduln argumentieren. Natürlich können wir annehmen, dass die p_i entweder gleich oder nicht assoziiert sind. Zu gegebenem Primelelement p fassen wir nun alle Faktoren mit $p_i = p$ zusammen. o.B.d.A. sind das die $p_1, \ldots, p_h$ und es gilt

$$T \cong P \times W \text{ mit } P = R/(p^{k_1}) \times \ldots \times R/(p^{k_h}),\ W = R/(p_{h+1}^{k_{h+1}}) \times \ldots \times R/(p_l^{k_l}) \times R^s.$$

Dann ist P charakterisiert als *p-Primärkomponente*

$$P = \{a \in M \mid \exists k :\ p^k a = 0\}.$$

Wie finden wir nun die k_i? Dazu bemerken wir, dass

$$P = Rg_1 \oplus \ldots \oplus Rg_h \text{ mit } p^{k_i} g_i = 0, p^{k_i - 1} g_i \neq 0.$$

Der Untermodul $P_k = (p^k)P = \{p^k a \mid a \in P\}$ wird also erzeugt von den $p^k g_i$ und es gilt $pP_k = P_{k+1} \subseteq P_k$. Bilden wir nun den Faktormodul P_k/P_{k+1} so ist p im Annullator, d.h. P_k/P_{k+1} ist auf natürliche Weise ein $R/(p)$-Vektorraum und hat eine eindeutig bestimmte Dimension n_k: die Anzahl der i mit $k_i > k$. Die n_k sind schon durch den abstrakten Modul P, also auch durch M eindeutig bestimmt. Aus ihnen lassen sich h und die k_i bestimmen: $h = n_1$. Schreiben wir die Exponenten $k_1, \ldots, k_n$ von p in der Form

$$\underbrace{h_1 = \ldots = h_1}_{m_1} < \underbrace{h_2 \ldots = h_2}_{m_2} < \ldots$$

so gilt $\underbrace{n_1 = \ldots = n_{h_1}}_{m_1} > \underbrace{n_{h_1+1} = \ldots = n_{h_2}}_{m_2} > \ldots, \quad m_1 = n_{h_1} - n_{h_2},\ m_2 = n_{h_2} - n_{h_3}, \ldots.$

Am besten denkt man sich hier wieder die 'Jordanketten'
$g_i \to pg_i \to p^2 g_i \to \ldots \to p^{k_i - 1} g_i \to 0$.

Korollar 14.12 *Die invarianten Teiler (Elementarteiler) einer Matrix über einem euklidischen Ring sind eindeutig bis auf Assoziiertheit (und Reihenfolge).*

Beweis. Wie erhalten wir die Eindeutigkeit der d_i? Wir fassen die Matrix als Präsentierungsmatrix eines Moduls M. Die Anzahl der $d_i = 0$ ist die der freien Summanden $\cong R$, also $s = n - r$. Sind die $d_i \not\approx 1$ in Primpotenzen zerlegt, so treten wegen $d_i | d_r$ zu jedem p die höchsten Potenzen in d_r auf, die zweithöchsten in d_{r-1} usw. Da die Vielfachheit der auftretenden Primpotenzen nach dem Vorangehenden eindeutig bestimmt ist, sind auch die d_i eindeutig bestimmt. □ Das System dieser Primpotenzen heisst auch System von *Elementarteilern* von $\mathcal{A}$. Man kann natürlich auch umgekehrt aus der Eindeutigkeit der invarianten Teiler auf die der Elementarteiler schliessen und daraus auf die Eindeutigkeit der Zerlegung.

14.10 Ähnliche Matrizen

Satz 14.13 *Für zwei $n \times n$-Matrizen A und A' über einem Körper K sind äquivalent*

- *A und A' sind* ähnlich*, d.h. es gibt eine invertierbare Matrix S über K mit $A' = S^{-1}AS$*
- *$A - xE$ und $A' - xE$ sind* äquivalent*, d.h. es gibt invertierbare Matrizen P und Q über $K[x]$ mit $A' - xE = P(A - xE)Q$*
- *Die K-Moduln ${}_{K[A]}K^n$ und ${}_{K[A']}K^n$ sind isomorph*
- *A und A' haben 'dieselben' invarianten Teiler*
- *A und A' haben 'dieselben' Elementarteiler*
- *A und A' haben dieselben Determinantenteiler*

Beweis. $1 \Rightarrow 2$: $S^{-1}(A - xE)S = S^{-}1AS - xE = A' - xE$. $2 \Rightarrow 3$: $A - xE$ und $(A - xE)Q$ erzeugen denselben Untermodul U von $K[x]^n$. Bzgl. der Basis P^{-1} von $K[x]^n$ haben die Spalten von $(A - xE)Q$ die Koordinaten $P(A - xE)Q$. Also präsentieren sowohl $A - xE$ wie auch $A' - xE$ einen zu K^n/U isomorphen Modul. Nun benutze, dass die charakteristische Matrix eine Präsentierungsmatix ist.
$3 \Rightarrow 1$: Der Zusammenhang zwischen dem Modulisomorphismus $\sigma : {}_{K[A']}K^n \to {}_{K[A]}K^n$ und der Matrix S ist $\sigma(\boldsymbol{v}) = S\boldsymbol{v}$. Ist σ gegeben, so ist es auch bijektiv und K-linear und man kann ein solches S finden. Wegen der $K[x]$-Linearität gilt insbesondere für alle $\boldsymbol{v}$ $AS\boldsymbol{v} = A\sigma\boldsymbol{v} = x\sigma\boldsymbol{v}\sigma(x\boldsymbol{v}) = SA'\boldsymbol{v}$. Ist S gegeben und $\omega : {}_{K[A]}K^n \to {}_{K[A']}K^n$ mit $\omega\boldsymbol{v} = S^{-1}\boldsymbol{v}$, so für alle $\boldsymbol{v}$

$$f(x)\omega(\boldsymbol{v}) = \sum_k r_k A'^k \omega(\boldsymbol{v}) = \sum_k r_k (S^{-1}AS)^k S^{-1}\boldsymbol{v} = \sum_k r_k S^{-1}A^k\boldsymbol{v} =$$

$$= S^{-1}\sum_k r_k A^k \boldsymbol{v} = \omega(f(x)\boldsymbol{v}).$$

Dass (3) aus (4) bzw (5) folgt, ist folgt aus der Existenz der Zerlegungen (Zusatz 1 und 6), die Umkehrung aus der Eindeutigkeit. Der k-te *Determinantenteiler* von A ist dabei definiert als der normierte GGT aller $k \times k$-Unterdeterminanten von $A - xE$. Dieser ändert sich bei Unformungen nicht. Aus der Diagonalgestalt liest man aber ab, dass der k-te Determinantenteiler das Produkt der ersten k invarianten Teiler ist. Folglich bestimmen sich diese wechselseitig. □

Beispiel

Sei V ein $\mathbb{Q}$-Vektorraum mit Basis $e_1, \ldots, e_5$ und ϕ der Endomorphimus mit Matrix

$$\begin{pmatrix} 2 & 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 1 & 1 & 0 & 1 & -4 \\ -1 & 0 & 0 & 1 & -2 \end{pmatrix}$$

Die charakteristische Matrix wird diagonalisiert nach dem Satz über die invarianten Teiler

$$E \mid A - xE \quad \rightsquigarrow \quad (f_1, \ldots, f_5) \mid \mathcal{A}'$$

$$\begin{array}{ccccc||ccccc}
1 & 0 & 0 & 0 & 0 & 2-x & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 2-x & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 2-x & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1-x & -4 \\
0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 1 & -2-x
\end{array}$$

$$\boxed{S1 := S1 - (2-x)S2}$$

$$\begin{array}{ccccc||ccccc}
1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & -(2-x)^2 & 2-x & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 2-x & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & -1+x & 1 & 0 & 1-x & -4 \\
0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 1 & -2-x
\end{array}$$

$$\boxed{Z2 := Z2 - (2-x)Z1,\ Z4 := Z4 - Z1,\ S1 \leftrightarrow S2}$$

$$\begin{array}{ccccc||ccccc}
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
2-x & 1 & 0 & 0 & 0 & 0 & -(2-x)^2 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 2-x & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & -1+x & 0 & 1-x & -4 \\
0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 & 1 & -2-x
\end{array}$$

$$\boxed{S2 := S2 + S4,\ S5 := -(S5 + (2+x)S4)}$$

$$\begin{array}{ccccc||ccccc}
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
2-x & 1 & 0 & 0 & 0 & 0 & -(2-x)^2 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 2-x & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1-x & x^2+x+2 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0
\end{array}$$

$$\boxed{Z4 := Z4 - (1-x)Z5}$$

$$\begin{array}{ccccc||ccccc}
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
2-x & 1 & 0 & 0 & 0 & 0 & -(2-x)^2 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 2-x & 0 & 0 \\
1 & 0 & 0 & 1 & 1-x & 0 & 0 & 0 & 0 & x^2+x+2 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0
\end{array}$$

$$\boxed{S4 \leftrightarrow S2,\ Z5 \leftrightarrow Z2,\ Z5 \leftrightarrow Z4,\ S4 := -S4}$$

$$\begin{array}{ccccc||ccccc}
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
2-x & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 2-x & 0 & 0 \\
1 & 1-x & 0 & 0 & 1 & 0 & 0 & 0 & (2-x)^2 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x^2+x+2
\end{array}$$

$$d_1 = d_2 = 1,\ d_3 = 2-x,\ d_4 = (2-x)^2,\ d_5 = x^2+x+2$$

Charakteristisches Polynom	$(x-2)^3(x^2+x+2)$
Minimalpolynom	$(x-2)^2(x^2+x+2)$
Eigenwerte	2 (geom. Vielf. 2, alg. Vielf. 3)
	$-\frac{1}{2} \pm \frac{\sqrt{7}}{2}i$

Daraus erhält man die Zerlegung von V in zyklische Untermoduln: die Erzeuger sind jeweils die Bilder $\tilde{f}_1, \ldots, \tilde{f}_5$ in V der neuen Basisvektoren $f_1, \ldots, f_5$ des freien Moduls $\mathbb{Q}[x]^5$. Die

wo 0 sind, kann man vergessen, hier $\tilde{f_1}$ und $\tilde{f_2}$ weil da an entsprechender Stelle der neuen Präsentierungsmatrix $\mathcal{A}'$ eine 1 steht (lies $1f_1 \stackrel{!}{=} 0$). Wir prüfen mal nach, dass wirklich $\tilde{f_1} = 0$

$$\tilde{f_1} = e_1 + (2-x)e_2 + e_4 = e_1 + 2e_2 - \phi(e_2) + e_4 = e_1 + 2e_2 - (e_1 + 2e_2 + e_4) + e_4 = 0$$

Bleiben (dass sich die so einfach ergeben, ist ein dummer Zufall, im allgemeinen muss man hier wieder die Matrix A anwenden)

$$\tilde{f_3} = e_3,\ \tilde{f_4} = e_2,\ \tilde{f_5} = e_4$$

mit den Relationen

$$(2-x)f_3 \stackrel{!}{=} 0,\ (2-x)^2 f_4 \stackrel{!}{=} 0,\ (x^2+x+2)f_5 \stackrel{!}{=} 0$$

Daraus kann man die Struktur von V als $\mathbb{Q}[x]$-Modul ablesen und passende Basen wählen

$$\begin{array}{rcccccc}
V & \cong & \mathbb{Q}[x]/(2-x) & \times & \mathbb{Q}[x]/(2-x)^2 & \times & \mathbb{Q}[x]/(x^2+x+2) \\
 & & 1 & & 1, x & & 1, x \\
V & = & \mathbb{Q}[x]\tilde{f_3} & \oplus & \mathbb{Q}[x]\tilde{f_4} & \oplus & \mathbb{Q}[x]\tilde{f_5} \\
 & & \tilde{f_3} & & \tilde{f_4}, x\tilde{f_4} & & \tilde{f_5}, x\tilde{f_5} \\
 & & e_3 & & e_2, \phi(e_2) & & e_4, \phi(e_4) \\
 & & \begin{pmatrix}0\\0\\1\\0\\0\end{pmatrix} & & \begin{pmatrix}0\\1\\0\\0\\0\end{pmatrix}, \begin{pmatrix}1\\2\\0\\1\\0\end{pmatrix} & & \begin{pmatrix}0\\0\\0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\0\\1\\1\end{pmatrix}
\end{array}$$

Die zugehörige Matrix von ϕ ist dann

$$A' = \begin{pmatrix}2&0&0&0&0\\0&0&-4&0&0\\0&1&4&0&0\\0&0&0&0&-2\\0&0&0&1&-1\end{pmatrix}$$

Da die zugehörigen Polynome Potenzen irreduzibler sind, ist A' schon Weierstrass-Normalform. Den Erzeuger eines zyklischen Untermodulns kann man auch mit einem modulo des zugeörigen Mimimalpolynoms invertierbaren Polynom multiplizieren und hat dann immer noch einen Erzeuger.

Die Frobenius-Normalform erhält man, indem man soweit wie möglich nach dem chinesischen Restsatz zusammenfasst. Hier geht das mit $(2-x)^2$ und x^2+x+1. Die beiden Erzeuger $\tilde{f_4}$

und $\tilde{f_5}$ addiert man gerade zusammen zu einem Erzeuger $\tilde{f_4}+\tilde{f_5}$ der direkten Summe

$$\begin{array}{rcccc}
V & \cong & \mathbb{Q}[x]/(2-x) & \times & \mathbb{Q}[x]/((2-x)^2(x^2+x+2) \\
 & & 1 & & 1,x,x^2,x^3 \\
V & = & \mathbb{Q}[x]\tilde{f_3} & \oplus & \mathbb{Q}[x](\tilde{f_4}+\tilde{f_5}) \\
 & & \tilde{f_3} & & \tilde{f_4}+\tilde{f_5}, x(\tilde{f_4}+\tilde{f_5}), x^2(\tilde{f_4}+\tilde{f_5}), x^3(\tilde{f_4}+\tilde{f_5}) \\
 & & e_3 & & e_2+e_4, \phi(e_2+e_4), \phi^2(e_2+e_4), \phi^3(e_2+e_4) \\
 & & \begin{pmatrix}0\\0\\1\\0\\0\end{pmatrix} & & \begin{pmatrix}0\\1\\\\1\\0\end{pmatrix}, \begin{pmatrix}1\\2\\0\\2\\1\end{pmatrix}, \begin{pmatrix}4\\4\\0\\1\\-1\end{pmatrix}, \begin{pmatrix}12\\8\\0\\13\\-1\end{pmatrix}
\end{array}$$

mit Matrix in Frobenius-Normalform

$$A'' = \begin{pmatrix}2&0&0&0&0\\0&0&0&0&-8\\0&1&0&0&4\\0&0&1&0&2\\0&0&0&1&3\end{pmatrix}$$

$$\text{da } (2-x)^2(x^2+x+2) = x^4-3x^3-2x^2-4x+8.$$

Natürlich gibt es auch andere Erzeuger von $\mathbb{Q}[x](\tilde{f_4}+\tilde{f_5})$: alle

$$b(x)\tilde{f_4}+a(x)\tilde{f_5}$$

wobei $b(x)$ invertierbar $\mathsf{mod}\ (2-\mathsf{x})^2$, $\mathsf{a(x)}$ invertierbar $\mathsf{mod}\ \mathsf{x}^2+\mathsf{x}+2$

Will man die Jordan-Normalform, so muss man im Prinzip alles über $\mathbb{C}$ angucken. Die Zerlegung in zyklische Untermoduln geht zunächst genauso, nur geht's jetzt noch weiter, da man zerlegen kann

$$x^2+x+2 = (x-\lambda)(x-\overline{\lambda}) \text{ mit } \lambda = \frac{-1}{2}+\frac{\sqrt{7}}{2}i,\ \overline{\lambda} = \frac{-1}{2}-\frac{\sqrt{7}}{2}i$$

$$\begin{array}{rcccccccc}
\mathbb{C}^5 & \cong & \mathbb{C}[x]/(2-x) & times & \mathbb{C}[x]/(2-x)^2 & times & \mathbb{C}[x]/(x-\lambda) & times & \mathbb{C}[x]/(x-\overline{\lambda}) \\
 & & 1 & & x-2,1 & & 2i\Im\lambda & & -2i\Im\lambda \\
\mathbb{C}^5 & = & \mathbb{C}[x]\tilde{f_3} & \oplus & \mathbb{C}[x]\tilde{f_4} & \oplus & \mathbb{C}[x]\tilde{f_{51}} & \oplus & \mathbb{C}[x]\tilde{f_{52}} \\
 & & \tilde{f_3} & & (x-2)\tilde{f_4}, \tilde{f_4} & & (x-\overline{\lambda})\tilde{f_5} & & (x-\lambda)\tilde{f_5} \\
 & & e_3 & & (\phi-2id)(e_2), e_2 & & (\phi-\overline{\lambda}id)e_4 & & (\phi-\lambda id)e_4 \\
 & & \begin{pmatrix}0\\0\\1\\0\\0\end{pmatrix} & & \begin{pmatrix}1\\0\\0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\0\\0\end{pmatrix} & & \begin{pmatrix}0\\0\\0\\\frac{-1}{2}+\frac{\sqrt{7}}{2}i\\1\end{pmatrix} & & \begin{pmatrix}0\\0\\0\\\frac{-1}{2}-\frac{\sqrt{7}}{2}i\\1\end{pmatrix}
\end{array}$$

Jordanmatrix von ϕ

$$\begin{pmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & \frac{-1}{2}+\frac{\sqrt{7}}{2}i & 0 \\ 0 & 0 & 0 & 0 & \frac{-1}{2}-\frac{\sqrt{7}}{2}i \end{pmatrix}$$

Es ist nämlich $x - \overline{\lambda} \equiv 2i\Im\lambda \bmod \mathsf{x} - \lambda$ und $x - \lambda \equiv -2i\Im\lambda \bmod \mathsf{x} - \overline{\lambda}$ da

$$1 = \frac{-1}{2i\Im\lambda}(x-\lambda) + \frac{1}{2i\Im\lambda}(x-\overline{\lambda})$$

Eigenvektoren

$$\tilde{f}_3, (x-2)\tilde{f}_4 \text{ zum } EW2$$

$$\tilde{f}_{51} \text{ zum } EW\ \frac{-1}{2}+\frac{\sqrt{7}}{2}i$$

$$\tilde{f}_{52} \text{ zum } EW\ \frac{-1}{2}-\frac{\sqrt{7}}{2}i$$

Letztere hätte man auch auf die aus LA bekannte Art bekommen. Dass man bei mehrfachem EV nicht ohne weiteres die richtige, d.h. zu Jordanbasis ausbaubare Basis des Eigenraums findet, sehen Sie in der Übung. Darum der Aufwand.

15 Irreduzibilität von Polynomen

15.1 Irreduzibiliät ganzzahliger Polynome

Sei R ein Integritätsbereich, etwa $\mathbb{Z}$.

Lemma 15.1 *Sei $\pi : R[x] \to R'[y]$ Homomorphismus, R, R' Integritätsbereiche, $f = \sum a_i x^i \in R[x]$ mit $\pi(x) \in R^*$ und $\pi f = \sum \pi(a_i) y^i$ irreduzibel in $R'[y]$ und $\deg f = \deg \pi(f)$. Dann ist f irreduzibel in $R[x]$.*

Solche Homomorphismen entstehen z.B. aus Homomorphismen $R \to R'$ mit $x \mapsto y$. Beispiel: $x^5 - x^2 + 1$ ist irreduzibel in $\mathbb{Z}/(2)[x]$ (weil da $x+1$ und x^2+x+1 die einzigen irreduziblen von $\deg \leq 2$ sind, aber keine Teiler unseres Polyoms), also in $\mathbb{Z}[x]$ irreduzibel.
Beweis. Aus $f = gh$ in $R[x]$ folgte also $\pi f = \pi g \pi h$ in $R'[y]$ und damit $\deg \pi g = \deg \pi f$ oder $\deg \pi h = \deg \pi f$, also $\deg g = \deg f$ oder $\deg h = \deg f$. □

Satz 15.2 *(*Eisenstein*) Zu $f = \sum_{i=0}^{n} a_i x^i$ in $R[x]$ gebe es primes $p \in R$ mit*

$$p \nmid a_n,\ p | a_i \text{ für alle } i < n,\ \ p^2 \nmid a_0$$

Dann ist f irreduzibel in $R[x]$.

Beweis. Angenommen $f = gh$ mit $g = \sum_{i=0}^{r} b_i x_i$ und $h = \sum_{i=0}^{s} c_i x^i$. Dann $a_0 = b_0 c_0$, also o.B.d.A. $p | b_0$ und $p \nmid c_0$. Da $a_n = b_r c_s$ folgt $p \nmid b_r$. Sei m minimal mit $p \nmid b_m$. Dann $p \mid a_m = b_m c_0 + b_{m-1} c_1 + \ldots$ und $p | b_{m-1} c_1, \ldots$ also $p | b_m c_0$ ein Widerspruch. □

Beispiel 15.3 *Das* Kreisteilungspolynom $\frac{x^p-1}{x-1} = x^{p-1} + \ldots + x + 1$ *ist irreduzibel, falls* p *prim.*

Beweis mit dem Homomorphismus $x \mapsto y+1$ von $R[x]$ in $R[y]$, Eisenstein und

$$\frac{(y+1)^p = 1}{(y+1)-1} = y^{p-1} + \binom{p}{1} y^{p-2} + \ldots + \binom{p}{p-2} y + \binom{p}{p-1}$$

15.2 Polynomring eines faktoriellen Rings

Satz 15.4 *(*Gauss*) Ist* R *faktorieller Ring, so auch* $R[x]$

Der Beweis braucht Vorbereitung. Sei Quotientenkörper Q von R. Ein Polynom $f = \sum a_i x^i \in R[x]$ ist *primitiv*, falls $\mathrm{GGT}(a_0, \ldots, a_n) = 1$. Gleichbedeutend: es gibt kein Primelement p von R so, dass $p|f$ in $R[x]$. Ist $rf \in R[x]$ für ein $r \in Q^*$, so ist $r \in R$. Sei nämlich $r = ab^{-1}$ mit $a, b \in R$ und $\mathrm{GGT}(a,b) = 1$. Für jedes i gilt $ab^{-1}a_i \in R$, also $b|aa_i$ in R und somit $b|a_i$. Da f primitiv ist, ist b eine Einheit d.h. $b^{-1} \in R$ (wegen Eindeutigkeit des Inversen) und $r = ab^{-1} \in R$.

Zu $f = \sum a_i b_i^{-1} x^i \in Q[x]$ gibt es ein $r \in Q^*$ so, dass $rf \in R[x]$ primitiv ist, nämlich $r = ba^{-1}$ mit $a =$ GGT $(a_0, \ldots, a_n)$ und $b =$ KGV $(b_0, \ldots, b_n)$.

Lemma 15.5 *Ist* p *prim in* R *so auch in* $R[x]$*. Sind* $f, g \in R[x]$ *primitiv, dann auch* fg*.*

Beweis. Der kanonische Homomorphismus $\pi : R \to R/(p) = R/Rp$ bestimmt einen surjektiven Homomorphismus

$$\phi : R[x] \to (R/Rp)[x] \text{ mit } \phi(\sum a_i x^i) = \sum \pi(a_i) x^i$$

mit

$$\mathrm{Kern}\phi = \{\sum a_i x^i \mid \forall i.\ \pi a_i = 0\} = R[x]p.$$

Also ist nach dem Homomorphiesatz

$$R[x]/R[x]p \cong (R/Rp)[x]$$

ein Integritätsbereich. Das bedeutet aber, dass p prim in $R[x]$. Sei nun angenommen, dass $p|fg$ für ein Primelement p von R. Wie oben gezeigt, ist p prim in $R[x]$, also $p|f$ oder $p|g$, Widerspruch. □

Lemma 15.6 *Für alle* $g, h \in Q[x]$ *gilt*

$$gh \in R[x] \Rightarrow \exists r \in Q^*.\ rg \in R[x] \text{ und } r^{-1}h \in R[x]$$

Beweis. O.B.d.A. ist $gh = f$ primitiv in $R[x]$. Wie oben bemerkt gibt es $r, s \in Q^*$ so, dass rg und sh in $R[x]$ primitiv sind. Dann $rsf = rgsh \in R[x]$ und daher $rs \in R$. Nach dem Lemma ist rsf primitiv und somit ist rs Einheit, d.h. es gibt ein $t \in R$ mit $rst = 1$. Es folgt $r^{-1}h = tsh \in R[x]$. □

Korollar 15.7 $g, f \in R[x]$, g *primitiv und* $g|f$ *in* $Q[x] \Rightarrow g|f$ *in* $R[x]$.
f *unzerlegbar in* $R[x] \Leftrightarrow f$ *prim in* $R[x]$
$\Leftrightarrow f \in R$ *prim oder* $f \notin R$ *unzerlegbar in* $Q[x]$ *und primitiv in* $R[x]$.

Beweis. Ist $f = gh$ in $Q[x]$ so gibt es nach dem Lemma $r \in Q^*$ mit rg und $r^{-1}h$ in $R[x]$. Da g primitiv ist, ist $r \in R$ und somit $h = rr^{-1}h \in R[x]$.

Ist $f \notin R$ unzerlegbar in $R[x]$, so f primitiv. Wäre f zerlegbar in $Q[x]$, so auch mit einem primitiven g, also $g|f$ in $R[x]$, Widerspruch. Sei schliesslich f primitiv und unzerlegbar, also prim in $Q[x]$ und $f|gh$ in $R[x]$. Dann $f|g$ oder $f|h$ in $Q[x]$ und somit auch in $R[x]$. □
Beweis des Satzes. Wir zeigen: Jedes f in $R[x]$, das weder Einheit noch 0 ist, hat bis auf Assoziiertheit eindeutige Darstellung

$$f = \prod p_i \prod g_j \text{ mit } p_i \text{ prim in } R, g_j \text{ primitiv in } R[x] \text{ und unzerlegbar in } Q[x]$$

Sei $f \notin R$. Da $Q[x]$ faktoriell ist, haben wir $f = \prod h_j$ mit unzerlegbaren h_j in $Q[x]$ und somit $f = r \prod g_j$ mit g_j assoziert zu h_j in $Q[x]$ und primitiv in $R[x]$. Da nach dem ersten Lemma auch $\prod g_j$ primitiv ist, ist $r \in R$ und entweder Einheit (dann schlage man es zu g_1) oder hat eine Zerlegung $r = \prod p_i$. Die Eindeutigkeit ergibt sich daraus, dass alle p_i und g_j prim in $R[x]$ sind. □

Korollar 15.8 *Sind $f, p \in R[x]$, p prim und $S \supseteq R$ ein Integritätsbereich mit einem $\alpha \in S$ so, dass $f[\alpha] = p[\alpha] = 0$. Dann $p|f$ in $R[x]$.*

Beweis. Sei L Quotientenkörper von S, o.B.d.A. $Q \subseteq L$. Sei $d = \text{GGT}(f, p)$ in $L[x]$, $\deg d \geq 1$ da $(x - \alpha)|d$. Der euklidische Algorithmus liefert sogar eine $d \in Q[x]$. Da p prim, sind p und d assoziiert in $Q[x]$, also $p|f$ in $Q[x]$ und somit in $R[x]$.

15.3 Faktorisierung über $\mathbb{Q}$

Ein simples, nicht effektives Verfahren zur Faktorisierung von Polynomen in $\mathbb{Q}[x]$ stammt von Kronecker. Man kann genausogut das ganzzahlige Polynom zerlegen, dass man durch Durchmultiplizieren mit dem Hauptnenner der Koeffizienten erhält. Nach Kor. ??, ist ein nicht konstantes Polynom $f(x)$ aus $\mathbb{Z}[x]$, das in $\mathbb{Q}[x]$ reduzibel ist auch in $\mathbb{Z}[x]$ reduzibel. Man wähle nun Stützstellen $\alpha_0 \ldots, \alpha_m \in \mathbb{Z}$ mit $m \geq \frac{1}{2} \deg f$. Hat f einen Teiler, so auch einen Teiler g von Grad $\leq m$ und g ist durch die $g(\alpha_i)$ eindeutig bestimmt (hat man noch so ein Polynom h mit $h(\alpha_i) = g(\alpha_i)$ so hat $g - h$ Grad $\leq m$ aber mehr als m viele Nullstellen, ist also nach Horner das Nullpolynom). Aber $g(\alpha_i)|f(\alpha_i)$ (weil Einsetzen ein Homomorphismus ist), d.h. es gibt nur endlich viele mögliche $g(\alpha_i)$. Aus diesen gewinnt man Teiler-Kandidaten g vom Grad $k \leq m$ z.B. durch Interpolation. Man muss dann nur solange f durch Kandidaten g mit Rest dividieren, bis es mal aufgeht und dann mit f/g weitermachen.

$$g(x) = \sum_{i=0}^{k} g(\alpha_i) \prod_{j \neq i} \frac{x - \alpha_j}{\alpha_i - \alpha_j}.$$

16 Körper und Erweiterungen

16.1 Primkörper

Die *Charakteristik* $n = \text{char} R$ eines Ringes R ist die kleinste natürliche Zahl > 0 mit $n \cdot 1_R = 0_R$, falls es das gibt, sonst ist sie 0.

Bemerkung 16.1 *Die Charakteristik von R ist n genau dann, wenn der von $\emptyset$ erzeugte Unterring zu $\mathbb{Z}/(n)$ isomorph ist. Für einen Integritätsbereich ist n stets 0 oder prim. Der kleinste Unterkörper (*Primkörper*) eines Körpers K ist*

- $\cong \mathbb{Z}/(p)$ *falls* $charK = p$ *prim*
- $\cong \mathbb{Q}$ *falls* $charK = 0$.

Beweis. $\mathbb{Z}$ ist freier von $\emptyset$ erzeugter Ring und hat nur die $\mathbb{Z}/(n)$ als homomorphe Bilder. Also bildet $S = \{z1 \mid z \in Z\}$ einen zu $\mathbb{Z}/(n)$ isomorphen Unterring von R. Ist R ein Integritästbereich, so ist n prim und S ein Unterkörper. Ist $n = 0$, so bilden die $\{z1(w1)^{-}1 \mid z, w \in \mathbb{Z}, w \neq 0\}$ einen zu $\mathbb{Q}$ isomorphen Unterkörper.□

16.2 Einfache Körpererweiterung

Ist K ein Unterring von L und beides Körper, so ist K ein *Unterkörper* von L (ist $a \in K$ und $b \in L$ mit $ab = 1$ schon $b \in K$) und es ist L ein K-Vektorraum. Dessen Dimension ist der *Grad* $[L : K]$ der Körpererweiterung.

Sind $K \subseteq M_i \subseteq L$ Unterkörper, so auch $K \subseteq M = \bigcap_{i \in I} M_i \subseteq L$. Insbesondere gibt es also zu $\alpha \in L$ einen kleinsten Unterkörper M mit

$$\alpha \in M, \quad K \subseteq M \subseteq L, \text{ wir schreiben } M = K(\alpha)$$

und sagen, $K(\alpha)$ ist *einfache Erweiterung* von K.

Satz 16.2 *Für einfache Körpererweiterungen $K(\alpha)$ gibt es zwei Fälle*

- $K(\alpha) \cong K(x)$*, dem Körper der rationalen Funktionen, mit* $\alpha \mapsto x$*. Dann heisst* α transzendent *über* K
- *Es gibt ein* $0 \neq f(x) \in K(x)$ *mit* $f[\alpha] = 0$ *in* $K(\alpha)$*, dann heisst* α algebraisch *über* K *und es gibt ein eindeutig bestimmtes normiertes Polynom* $m(x) \in K[x]$ *minimalen Grades mit* $m[\alpha] = 0$ *in K(a), das* Minimalpolynom *von* α *über* K *und es gilt*
  - $K(\alpha) \cong K[x]/(m(x))$ *mit* $\alpha \mapsto \tilde{x}$
  - $n = K(\alpha) : K] = \deg m(x)$ *und* $K(\alpha)$ *hat Basis* $1, \alpha, \ldots \alpha^{n-1}$ *über* K
  - $m(x)$ *ist irreduzibel in* $K[x]$
  - $m(x)|f(x)$ *in* $K[x]$ *für alle* $f(x) \in K[x]$ *mit* $f[\alpha] = 0$

Beweis. Sei $f[\alpha] \neq 0$ für alle $f(x) \neq 0$. Definiere

$$\phi : K[x] \to K(\alpha), \quad \phi(r(x)) = r[\alpha]$$

Das ist gerade der Auswertungshomomorphismus an der Stelle α und, nach Vorraussetzung ist Kern$\phi = 0$, also ϕ injektiv. Nach Satz über Quotientenkörper haben wir die Fortsetzung

$$\overline{\phi} : K(x) \to K(\alpha), \quad \overline{\phi}(\frac{r(x)}{s(x)}) = r[\alpha] \cdot s[\alpha]^{-1}$$

und es ist das Bild $\overline{\phi}(K(x))$ ein Unterkörper von $K(a)$. Da $\overline{\phi}(x) = a$, ist das Bild schon ganz $K(\alpha)$. $K(\alpha)$ wird zum $K[x]$-Modul unter der Wirkung

$$r(x)v = r[\alpha] \cdot v$$

und $\{f(x) \in K[x] \mid f[\alpha] = 0\}$ ist ein Ideal I. Gibt es darin ein $f \neq 0$, so ist $m(x)$ ein Erzeuger dieses Ideals: $I = (m(x))$ und für die Ringe bzw. $K[x]$-Moduln gilt

$$K[x]/(m(x)) \cong K(\alpha) \quad \text{mit } \tilde{x} \mapsto x[\alpha] \cdot 1 = \alpha$$

Die Basis $1, x, \ldots x^{n-1}$ geht also über in $1, \alpha, \ldots, \alpha^{n-1}$. Da $K(\alpha)$ ein Körper ist, ist $m(x)$ nach Satz 5.15 irreduzibel. □

Das Rechnen in einer einfachen algebraischen Erweiterung $K(a)$ mit Minimalpolynom $m(x) = a_0 + a_1 x + \ldots + x^n$ geht so

- Die Elemente von $K(\alpha)$ haben eindeutige Darstellung $\beta = g[\alpha] = b_0 + b_1 a + \ldots + b_{n-1} a^{n-1}$
- Addition koeffizientenweise
- Multiplikation: Ausmultiplizieren und dann Vereinfachen mit
$$\alpha^n = -a_0 - a_1\alpha - \ldots - a_{n-1}\alpha^{n-1}$$
- Inversion: bestimme $1 = h(x)g(x) + r(x)m(x)$ nach Bezout, dann $1 = h[\alpha]g[\alpha]$, also $h[\alpha] = g[\alpha]^{-1}$

Bespiele: $\mathbb{Q}(e)$ und $\mathbb{Q}(\pi)$ sind transzendent, $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(i)$ sind algebraisch von Grad 2.

Korollar 16.3 *Haben $\alpha, \beta \in L$ dasselbe Minimalpolynom über $K \subseteq L$, so $K(\alpha) \cong K(\beta)$*

Es kann $K(\alpha) = K(\beta)$ gelten, muss aber nicht. Z.B. $x^4 - 2$ irreduzibel über $\mathbb{Q}$ nach Eisenstein, $\mathbb{Q}(\sqrt[4]{2}) \cong \mathbb{Q}(i\sqrt[4]{2})$ aber $\mathbb{Q}(\sqrt[4]{2}) \neq \mathbb{Q}(i\sqrt[4]{2})$.

16.3 Gradsatz

Satz 16.4 *Sind $K \subseteq M \subseteq L$ Unterkörper so*

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

Beweis. Sei A Basis von M über K, B Basis von L über M. Dann hat L über K die Basis

$$A \cdot B = (\alpha \cdot \beta \mid \alpha \in A, \beta \in B) \text{ als Liste}$$

Zu v in L hat man

$$v = \sum_{\beta \in B} r_\beta \beta \text{ mit } r_\beta \in M, \quad r_\beta = \sum_{\alpha \in A} s_{\alpha\beta} a \text{ mit } r_{\alpha\beta} \in K$$

$$v = \sum r_\beta \beta = \sum_{\beta \in B} (\sum_{\alpha \in A} s_{\alpha\beta}\alpha)\beta = \sum_{\alpha \in A, \beta \in B} s_{\alpha\beta}\alpha\beta$$

also erzeugt $A \cdot B$ den K-Vektorraum L. Zum Beweis der Unabhängigkeit betrachte

$$0 = \sum_{\alpha \in A, \beta \in B} s_{\alpha\beta}\alpha\beta = \sum r_\beta \beta \quad \text{mit } r_\beta = \sum_{\alpha \in A} s_{\alpha\beta}\alpha \in M$$

Dann $r_\beta = 0$, da B Basis von L über M und dann $s_{\alpha\beta} = 0$, da A Basis von M über K. □

16.4 Algebraische Erweiterungen

Eine Iteration einfacher Erweiterungen heisst *endlich* und wird so geschrieben

$$K(\alpha_1)(\alpha_2)\dots(\alpha_m) = K(\alpha_1,\dots,\alpha_m)$$

Eine Erweiterung $L \supseteq K$ heisst *algebraisch* über K, falls alle $\alpha \in L$ algebraisch über K sind.

Satz 16.5 *Für eine Körpererweiterung $L \supseteq K$ sind äquivalent*

- $[L:K] < \infty$
- $L \supseteq K$ *endliche algebraische Erweiterung*
- *Es gibt m und $\alpha_1,\dots,\alpha_m \in L$ so, dass $K(\alpha_1,\dots,\alpha_k)(\alpha_{k+1})$ algebraisch über $K(\alpha_1,\dots,\alpha_k)$ für $k = 0,1,\dots,m-1$*

Beweis: 1 $\Rightarrow$ 2: $L = K(\beta_1,\dots,\beta_n)$ mit Basis $\beta_1,\dots,\beta_n$ von L über K. 2 $\Rightarrow$ 3: $L = K(\alpha_1,\dots,\alpha_m)$ nach Voraussetzung und die α_i sogar algebraisch über K. 3 $\Rightarrow$ 1: Gradsatz $m-1$-mal anwenden. $\square$ Mit dem Gradsatz folgt sofort

Korollar 16.6 *Sind $L \supseteq M$ und $M \supseteq K$ algebraisch, so auch $L \supseteq K$.*

16.5 Zerfällungskörper

Satz 16.7 *Zu jedem Körper K und Polynom $f(x)$ gibt es bis auf Isomorphie genau einen Körper $L = K(\alpha_1,\dots,\alpha_n)$, in dem $f(x) = \prod_{i=1}^{n}(x-\alpha_i)$, den* Zerfällungskörper *von $f(x)$ über K.*

Beweis durch Induktion über den Grad. Existenz: Wähle irreduziblen Faktor $g(x)$ von $f(x)$ und $M = K[x]/(g(x))$, $\alpha_1 = \tilde{x}$, d.h $M = K(\alpha_1)$. Wir haben nun $f(x) = (x-\alpha_1)h(x)$ in $M[x]$ und nach Induktion einen Zerfällungskörper L von M zu $h(x)$, d.h $L = M(\alpha_2,\dots,\alpha_n)$,$h(x) = (x-\alpha_2)\cdot\ldots\cdot(x-\alpha_n)$ Damit ist L auch Zerfällungskörper von $f(x)$ über K. Zum Beweis der Eindeutigkeit, müssen wir die Behauptung etwas verschärfen: Ist $\phi : K \to K_1$ ein Isomorphismus mit Fortsetzung $\phi : K[x] \to K_1[x]$, $x \mapsto x$, und sind L bzw. L_1 Zerfällungskörper von $f(x)$ über K bzw, $f_1(x) = \phi(f)$ über K_1, so gibt es einen Isomorphismus $\psi : L \to L_1$ mit $\psi|K = \phi$. Sei wieder $g(x)$ wie oben. Wähle aus den $\alpha_i \in L$ so, dass nach Umnummerieren $g[\alpha_1] = 0$. Sei $g_1(x) = \phi(g)$ und nummeriere die Linearfaktoren $x-\beta_i$ von f_1 so, dass $g_1[\beta_1] = 0$. Dann $M = K(\alpha_1) \cong M_1 = K_1(\beta_1)$ mit einem Isomorphismus χ, der ϕ fortsetzt. Da L Zerfällungskörper von $h(x)$ und L_1 von $h_1(x) = \chi(h)$, gibt es nach Induktion Fortsetztung $\psi : L \to L_1$ von χ. $\square$

16.6 Mehrfache Nullstellen

Die *Ableitung* eines Polynoms ist definiert als

$$(\sum a_i x^i)' = \sum_{i\geq 1} i a_i x^{i-1}$$

Es folgt

$$(f+g)' = f' + g', \quad (fg)' - f'g + g'f$$

Lemma 16.8 *Sei R Integritätsbereich, $f \in R[x]$. Ist $\alpha \in R$ k-fache Nullstelle von f, so α l-fache Nullstelle von f' mit $l \geq k-1$. Für charR $\not|$ k gilt $l = k-1$*

Beweis. Nach Kor.6.5 können wir Nullstellen abspalten $f = (x-\alpha)^k g$ mit $g[\alpha] \neq 0$, also

$$f' = k(x-\alpha)^{k-1}g + (x-\alpha)^k g' = (x-\alpha)^{k-1}h \text{ mit } h = kg + (x-\alpha)g'$$

Ist $k \cdot 1 \neq 0$, so $h[\alpha] = kg[\alpha] \neq 0$ □

Ein Polynom in $K[x]$ heisst *separabel*, wenn es in jeder Erweiterung von K nur Nullstellen von Vielfachheit 1 hat.

Lemma 16.9 *Ist $\mathsf{GGT}(f, f') = 1$ in $K[x]$ so ist f separabel. Ein irreduzibles Polynom in $K[x]$, $K \subseteq \mathbb{C}$, ist stets separabel.*

Beweis. Hat f mehrfache Nullstelle α, so haben f und f' gemeinsame Nullstelle α also $d = \mathsf{GGT}(f, f')$ in $K(\alpha)$ mit deg > 0. Also auch in $K[x]$ - euklidischer Algorithmus. Wegen $\deg f' < \deg f$ folgt $d = 1$. Widerspruch. □.

16.7 Primitive Elemente

Satz 16.10 *Jede endliche algebraische Erweiterung $L \supseteq K$ mit $L \subseteq \mathbb{C}$ ist einfach: $L = K(\gamma)$ mit einem* primitiven *Element γ.*

Beweis. Es genügt zu zeigen: für alle $\alpha, \beta \in \mathbb{C}$ gibt es $\gamma \in \mathbb{C}$ mit $K(\alpha, \beta) = K(\gamma)$. Sei $f(x)$ das Minimalpolynom von α und $g(x)$ das von β. In $\mathbb{C}$ haben wir nach dem Fundamentalsatz eine Zerlegung

$$f(x) = (x-\alpha_1)\cdot\ldots\cdot(x-\alpha_n), \quad g(x) = (x-\beta_1)\cdot\ldots\cdot(x-\beta_m) \quad \text{mit } \alpha_1 = \alpha,\ \beta_1 = \beta$$

Da K unendlich ist, kann man $c \in K$ so wählen, dass

$$c \neq \frac{\alpha_i - \alpha}{\beta - \beta_j} \text{ also } \alpha + c\beta \neq \alpha_i + c\beta_j \quad \text{für } 1 \leq i \leq n, 2 \leq j \leq m.$$

Setze

$$\gamma = \alpha + c\beta, \quad h(x) = f(\gamma - cx)$$

Also $K(\gamma) \subseteq K(\alpha, \beta)$ und

$$h(\beta_j) = 0 \Leftrightarrow \gamma - c\beta_j = \alpha_i \text{ für ein } i \Leftrightarrow j = 1$$

Also ist β einzige gemeinsame komplexe Nullstelle von $g(x)$ und $h(x) \in K(\gamma)[x]$, also $x - \beta = \mathrm{GGT}(g(x), h(x))$ in $\mathbb{C}[x]$. Es folgt $x - \beta \in K(\gamma)[x]$ da man den GGT ja mit Euklid in $K(\gamma)[x]$ berechnen kann. Somit $\beta \in K(\gamma)$, also auch $\alpha \in K(\gamma)$. □

16.8 Endliche Untergruppen

Lemma 16.11 *Jede endliche Untergruppe G der multiplikativen Gruppe eines Körpers K ist zyklisch.*

Beweis. Nach dem Strukturstatz für abelsche Gruppen

$$G \cong \mathbb{Z}/(m_1) \times \ldots \times \mathbb{Z}/(m_r), \quad n = |G| = m_1 \cdot \ldots \cdot m_r$$

Angenommen, G ist nicht zyklisch, dann $r > 1$ und wegen des Chinesischen Restsatzes gibt es $\mathrm{GGT}(m_i, m_j) \not\approx 1$. Also $m = KGV(m_1, \ldots, m_r) < n, \quad a^m = 1$ für alle $a \in G$. Also hätte das Polynom $x^m - 1$ mehr als m Nullstellen in K, Widerspruch zu Kor.6.6. □

Lemma 16.12
$$\begin{array}{rcl} d = GGT(n,m) & \Rightarrow & GGT(x^n-1, x^m-1) = x^d - 1 \\ & \textit{und} & GGT(p^n-1, p^m-1) = p^d - 1 \end{array}$$
$$x^{p^m-1} - 1 \mid x^{p^n-1} - 1 \text{ in } K[x] \quad \Leftrightarrow \quad p^m - 1 \mid p^n - 1 \quad \Leftrightarrow \quad m|n$$

16.9 Einheitswurzeln

Korollar 16.13 *Eine endliche Untergruppe G von $\mathbb{C}^*$ besteht gerade aus den $n-$ten Einheitswurzeln*

$$G = C_n = \{e^{2\pi i \frac{k}{n}} \mid k = 0, \ldots, n-1\} = \{\alpha \in \mathbb{C} \mid \alpha^n = 1\}, \quad |G| = n$$

und dies sind genau die n verschiedenen Nullstellen von $x^n - 1$

$$x^n - 1 = \prod_{\alpha \in C_n} (x - \alpha)$$

$C_m \subseteq C_n$ (und damit Untergruppe) genau dann, wenn $m \mid n$. Ist C_n erzeugt von ζ, so ist ζ^k genau dann Erzeuger von C_n wenn $\mathsf{GGT}(k, n) = 1$,

Beweis, $C_m \subseteq C_n \Leftrightarrow x^m - 1 \mid x^n - 1 \Leftrightarrow m \mid n$ nach Lemma ??. Die letzte Behauptung beweist man für die isomorphe Gruppe $\mathbb{Z}/n\mathbb{Z}$: a ist Erzeuger genau dann, wenn es $k \in \mathbb{Z}$ gibt mit $ka = 1$, also genau dann, wenn a Einheit. Und das sind die $\tilde{a}$ mit $\mathsf{GGT}(a, n) = 1$. Ist e eine Einheit, so ist $a = ke$ eine Einheit genau dann, wenn $\tilde{k}$ Einheit ist, also $\mathsf{GGT}(k, n) = 1$. □ Es geht natürlich auch mit dem Sätzchen von Lagrange: ist U Untergruppe der endlichen Gruppe G so, $|U|$ Teiler von $|G|$.

Es folgt: Für $\alpha \in \mathbb{C}$ ist gleichbedeutend:

- $\alpha \in C_n$ und $\alpha \notin C_m$ für alle echten Teiler m von n
- α erzeugt die Gruppe C_n
- α ist *primitive* n-te Einheitswurzel

Ihre Anzahl ist $\phi(n) = |\mathbb{Z}/(n)^*|$, die Anzahl der Erzeuger der (zu C_n isomorphen) Gruppe $\mathbb{Z}/(n)$, d.h. der inverierbaren Elemente des Ringes $\mathbb{Z}/(n)$. Sind $\alpha_1, \ldots, \alpha_{\phi(n)}$ die verschiedenen primitiven Einheitswurzeln, so ist

$$\Phi_n(x) = (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_{\phi(n)}) \text{ das } n\text{-te Kreisteilungspolynom}$$

Es folgt

$$\prod_{d|n} \Phi_d = x^n - 1$$

Mit Induktion und Divisionsalgortihmus folgt

- $\Phi_n \in \mathbb{Z}[x]$ mit Leitkoeffizient 1

Lemma 16.14 *$\Phi_n(x)$ ist Minimalpolynom der primitiven n-ten Einheitswurzeln.*

Beweis. In $\mathbb{Z}[x]$ gibt es eindeutig bestimmte Zerlegung $\Phi_n = \prod_i f_i(x)$ in irreduzible. Sei α primitive Einheitswurzel α, also $\Phi_n(\alpha) = 0$, Dann gibt es ein $f(x) = f_i(x)$ mit $f(\alpha) = 0$, und es folgt mit Kor.11.8 dass $f(x) \mid x^n - 1$ in $\mathbb{Z}[x]$, also $f(x)$ mit Leitkoeffizient 1 und somit das Minimalpolynom von α.

Sei nun $\beta = \alpha^q$, $q \not| n$, eine weitere primitive Einheitswurzel mit Minimalpolynom $g(x)$. Wir behaupten, dass $f(\beta) = 0$. Betrachte das Polynom $g(x^q) \in \mathbb{Z}[x]$. Die Polynome $f(x)$ und $g(x^q)$ haben die gemeinsame Nullstelle α, also nach Kor. 11.8 $f(x) \mid g(x^q)$ in $\mathbb{Z}[x]$ und somit auch in $\mathbb{Z}/(q)[x]$. Hier gilt $(a+b)^q = a^q + b^q$ und somit $g(x^q) \equiv g(x)^q \bmod q$, Also $f(x)$ Teiler von $g(x)^q$ in $(\mathbb{Z}/q\mathbb{Z})x$ und $f(x)$ wie $g(x)$ beide Teiler von $x^n - 1$. Man bilde nun den Zerfällungskörper von $x^n - 1$ über $\mathbb{Z}/(q)$. Dann hat $f(x)$ eine Nullstelle und die ist auch eine von $g(x)$. Da $\mathrm{GGT}(x^n - 1, nx^{n-1}) = 1$ in $\mathbb{Z}/(q)[x]$, hat aber $x^n - 1$ modulo q nur einfache Nullstellen und es kann $f(x) \cdot g(x)$ kein Teiler von $x^n - 1$ in $\mathbb{Z}/(q)[x]$ sein. Dann kann es das auch in $\mathbb{Z}[x]$ nicht sein. Inspektion des Divisionsalgorithmus zeigt, dass es dann auch in $\mathbb{C}[x]$ kein Teiler ist. Da aber $f(x)$ und ebenso $g(x)$ Teiler von $x^n - 1$ ist, müssen $f(x)$ und $g(x)$ (wegen der eindeutigen Zerlegung in Linearfaktoren) eine gemeinsame Nullstelle in $\mathbb{C}$ haben. Wieder mit Kor.11.8 folgt $g(x) \mid f(x)$ in $\mathbb{Z}[x]$ und so $f[\beta] = 0$.

Die primitiven Einheitswurzeln sind aber gerade von der Form α^k mit $GGT(k, n) = 1$, d.h. wir erhalten sie, indem wir den Übergang $\alpha \mapsto \alpha^q$ iterieren. Es folgt $f[\beta] = 0$ für alle primitiven n-ten Einheitswurzeln und damit $\Phi_n(x) \mid f(x)$ und somit $\Phi_n(x) = f(x)$ Minimalpolynom. □

16.10 Radikale

$K(\alpha) \supseteq K$ ist eine *radikale* Erweiterung, wenn α Nullstelle eine *reinen Gleichung* $x^n - a = 0$ mit $a \in K$ ist. Quadratische Polynome löst man durch quadratische Ergänzung, falls $2 \neq 0$

$$\alpha^2 + p\alpha + q = 0 \;\Leftrightarrow\; \alpha = -\frac{p}{2} \pm \beta \;\text{ mit } \beta^2 = \frac{p^2}{4} - q$$

Ein Polynom $y^3 + ay^2 + by + c$ geht, falls $2, 3 \neq 0$, durch die Substitution $x = y + \frac{1}{3}a$ über in

$$x^3 + px + q \in K[x]$$

Die Lösungen sind

$$\alpha_1 = \frac{1}{3}(\beta + \gamma), \;\; \alpha_2 = \frac{1}{3}(\beta\omega^2 + \gamma\omega), \;\; \alpha_3 = \frac{1}{3}(\beta\omega + \gamma\omega^2)$$

wobei

$$\omega \neq 1,\; \omega^3 = 1, \;\; \beta\gamma = -3p, \;\; \beta^3 + \gamma^3 = -27q$$
$$\beta^3 = -\frac{27}{2}q + \frac{3}{2}\varepsilon) \text{ mit } \varepsilon^2 = -3\Delta = 12p^3 + 81q^2$$

Zum Beweis sei $x^3 + px + q = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ und benutze $\omega^2 + \omega + 1 = 0$. Setze

$$\beta = \alpha_1 + \alpha_2\omega + \alpha_3\omega_2 = (\omega - 1)\alpha_2 + (\omega^2 - 1)\alpha_3, \;\; \gamma = \alpha_1 + \alpha_2\omega^2 + \alpha_3\omega = (\omega^2 - 1)\alpha_2 + (\omega - 1)\alpha_3$$

Man erhält die α_i aus β und γ wie angegeben. Koeffizientenvergleich liefert

$$\alpha_1+\alpha_2+\alpha_3=0,\ p=\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3=-(\alpha_2^2+\alpha_2\alpha_3+\alpha_3^2),\ q=-\alpha_1\alpha_2\alpha_3=\alpha_2^2\alpha_3+\alpha_2\alpha_3^2$$

Es bleibt nachzurechnen, dass β und γ obige Bedingungen erfüllen. □ Polynome von Grad 4 kann man sich beim Italiener durch Radikale auflösen lassen, aber z.B. bei $x^5-5x+1\in\mathbb{Q}[x]$ geht's nicht mehr. Die Charakterisierung der auflösbaren Erweiterungen und die Bestimmung der Zwischenkörper $K\subseteq M\subseteq L$ zu gegebenem $K\subseteq L$ ist Gegenstand der *Galoistheorie*. Ein zentrale Rolle spielen dabei die Gruppen und Unterkörper

$$\mathrm{Aut}(M)=\{\phi\mid\phi:L\to L \text{ Automorphismus mit } \phi|M=id_M\}$$

$$\mathrm{Fix}(U)=\{a\in L\mid\phi(a)=a \text{ für alle } \phi\in U\} \text{ mit } U\subseteq\mathrm{Aut}(L)$$

16.11 Zirkel und Lineal

Satz 16.15 *Seien $i\in K\subseteq L\subseteq\mathbb{C}$ und $L\supseteq K$ endliche Erweiterung. Fasst man die Elemente von $\mathbb{C}$ als Punkte der Ebene auf, so sind äquivalent*

- *die Punkte aus L sind mit Zirkel und Lineal aus welchen in K konstruierbar*
- *Es gibt $K=L_0\subseteq L_1\subseteq\ldots\subseteq L_n=L$ mit $[L_{k+1}:L_k]=2$*
- *$[L:K]=2^r$ für ein r.*

Beweis. $1\Leftrightarrow 2$ als Übung: Schneiden von Geraden und Kreisen ist lösen linearer, quadratischer bzw. biquadratischer Gleichungen. $2\Rightarrow 3$ mit Gradsatz. $3\Rightarrow 2$ mit Galoistheorie. □. Mit dem Gradsatz und $[\mathbb{Q}(i):\mathbb{Q}]=2$ folgt

Korollar 16.16 *$\alpha_1,\ldots,\alpha_n\in\mathbb{C}$ konstruierbar $\Leftrightarrow$ $\mathbb{Q}\alpha_1,\ldots,\alpha_n):\mathbb{Q}]=2^r$ für ein r.*

Satz 16.17 (Gauss) *Das regelmässige n-Eck ist genau dann konstruierbar, wenn*

$$n=2^r\cdot p_1\cdot\ldots\cdot p_s \quad \textit{mit verschiedenen} \text{ Fermat'schen Primzahlen } p_i=2^{k_i}+1$$

Die Fermat'schen Primzahlen $<10^{40000}$ sind $2,3,5,17,257,65537$. Beweis. Das regelmässige n-Eck kann man sich gerade als die Gruppe C_n denken. Da nach dem Chinesichen Restsatz $C_{nm}\cong C_n\times C_m$ (konstruktiv) für teilerfremde n,m, genügt es $n=p^r$ zu betrachten. In Falle $n=p$ erhält man aus einer Wurzel $\alpha\neq 1$ alle anderen als Potenzen (da C_p nach Lagrange keine echte Untergruppe hat) und mit Beisp,11.3 gilt $[\mathbb{Q}(\alpha):\mathbb{Q}]=p-1$. Konstruierbarkeit ist demnach gleichbedeutend mit $p-1=2^k$ für ein k. (Dann sogar $k=2^l$). Wäre ein p^r-Eck mit $r>1$ konstruierbar, so auch das p^2-Eck. Sei $\alpha\in C_{p^2}\setminus C_p$. Nach dem Lemma ?? ist α Nullstelle eines irreduziblen Polynoms von Grad p und es gilt $[\mathbb{Q}(\alpha):\mathbb{Q}]=p$. Widerspruch. □

Korollar 16.18 *Die folgenden Konstruktionen gehen nicht mit Zirkel und Lineal*

- *Quadratur des Kreises*
- *Winkeldreiteilung*
- *Verdoppelung des Würfelvolumens (Deli'sches Problem)*

Beweis. π ist transzendent über $\mathbb{Q}$ - das ist nicht trivial. Der 120^o-Winkel lässt sich nicht dreiteilen, sonst könnte man das 9-Eck konstruieren. Das Delische Problem verlangt eine Lösung von $x^3-2=0$, also eine Erweiterung mit $3\mid[L:\mathbb{Q}]$. □

16.12 Endliche Körper

Satz 16.19 *Sei L ein endlicher Körper. Dann*

- *L hat p^n Elemente, p die Charakteristik von L, also prim, $n = [L : \mathbb{Z}/(p)]$.*
- *L^* ist zyklisch und $a^{p^n} = a$ für alle $a \in L$*
- *$a \mapsto a^{p^k}$ ist ein Automorphismus*
- *$U(k) = \{a \in K \mid a^{p^k} = a\} = \{0\} \cup \{a \in K \mid a^{p^k-1} = 1\}$ ist ein Unterkörper*
- *Die Unterkörper von L sind gerade die $U(m)$ mit $m|n$ und haben p^m Elemente*

Die erste Behauptung ist klar, weil L ein $\mathbb{Z}/pZ$-Vektorraum ist. $(ab)^p = a^p \cdot b^p$ ist klar. Nach Binomi $(a+b)^p = a^p + b^p$ da p prim und somit Teiler der Binomialkoeffizienten. Also haben wir einen Endomorphismus $a \mapsto a^p$ und die Hintereinanderausführungen $a \mapsto a^{p^k}$ und die Unterkörper $U(k)$. L^* ist nach ?? zyklisch von Ordnung $p^n - 1$, also gilt $a^{p^n-1} = 1$ für alle $a \neq 0$. Ist m ein Teiler von n, so nach ?? $p^m - 1 \mid p^n - 1$ und somit $U(m)^*$ eine Untergruppe von L^* mit $p^m - 1$ Elementen. Ist M Unterkörper von L, so $|M| = p^m$ für ein m und M^* Untergruppe von L^*, also $p^m - 1 \mid p^n - 1$ also nach ?? $m|n$. Da $M \subseteq U(m)$)nach (2) angewendet für M) folgt $M = U(m)$. □

Satz 16.20 *Zu jedem p^n gibt es bis auf Isomorphie genau einen Körper $GF(p^n)$ mit p^n Elementen.*

Beweis. Schön wäre es, einfach ein irreduzibles Polynom von Grad in $\mathbb{Z}/(p)[x]$ hinzuschreiben. Das ist aber nicht so einfach, also machen wir's wischiwaschi mit dem Zerfällungskörper des Polynoms $x^{p^n} - x$. Dieses hat nämlich Ableitung $p^n x^{p^n-1} - 1 = -1 \neq 0$, also keine mehrfachen Nullstellen. Damit haben wir im Zerfallungskörper L den Unterkörper $U(n)$ hier mit p^n Elementen. Und $U(n) = L$, da alle Nullstellen des Polynoms drin liegen. □

17 Direkte Produkte und Summen mit beliebig vielen Faktoren

17.1 Direkte Produkte mit unendlich vielen Faktoren

Die Ergebnisse zu direkten Produkten übertragen sich auch auf den Fall einer unendlichen Indexmege I anstelle von $\{1, \ldots, n\}$. Das direkte Produkt ist dann

$$\prod_{I \in I} A_i = \{f \mid f : I \to \bigcup_{i \in I} A_i, \ \ \forall i \in I.\ f(i) \in A_i\}$$

die Menge aller *Auswahlfunktionen* `[choice functions]` oder, etwas intuitiver, die Menge aller I-Tupel

$$(a_i \mid i \in I) \quad \text{mit } a_i \in A_i \text{ für alle } i \in I$$

Dass das Produkt nichtleerer Mengen nicht leer ist, wird durch das Auswahlaxiom `[axiom of choice]` garantiert. Sind die A_i algebraische Strukturen gleichen Typs, so wird auch das direkte Produkt zu einer solchen durch komponentenweise Definition der Operationen.

Stimmen die A_i alle überein, $A_i = A$, so schreibt man das direkte Produkt als *direkte Potenz* `[direct power]`

$$A^I = \{f \mid f : I \to A\}$$

Ein *Funktionenraum* `[function space]` ist ein Untervektorraum eines Vektorraums K^I, K ein Körper (und somit ein K-Vektorraum), meist $\mathbb{R}$ oder $\mathbb{C}$.

17.2 Direkte Produkte: universelle Eigenschaft

Das direkte Produkt $A = \prod_{i\in I} A_i$ mit den kanonischen Projektionen $\pi_i \to A_i$ ist durch folgende Eigenchaft charakterisiert:

- Sind die $\phi_i : V \to A_i$ Homomorphismen, so gibt es einen eindeutig bestimmten Homomorphismus $\phi : B \to B$ mit $\pi_i \circ \phi = \phi_i$ für alle $i \in I$

Man hat $\phi(x) = (\phi_i(x) \mid i \in I)$.

Hier sind alle Strukturen des gebenen Tys erlaubt. Die Charakterisierung ist aber auch dann korrekt, wenn man sich nur auf eine unter Produkten abgeschlossene Klasse bezieht.

17.3 Direkte Summen mit unendlich vielen Siummanden

Wir setzen nun voraus, dass die Signatur genau eine Konstante e enthält und dass dass gilt:

$$f(e, \ldots, e) = e \quad \text{für jede fundamentale Operation } f$$

Dann hat man eine Unterstruktur der direkten Produkts

$$\sum_{i\in I} A_i = \{(a_i \mid i \in I) \mid \{i \in I \mid a_i \neq e)\} \text{ ist endlich } \} \subseteq \prod_{i\in I} A_i$$

die aus den I-Tupeln besteht, die nur an endlich vielen Stellen von e verschieden sind. Das ist dann die *direkte Summe* `[direct sum]`. Sind alle A_i gleich, $A_i = A$, so schreibt man $A^{(I)}$. Die Ergebnisse für endliches i wurden schon so formuliert und bewiesen, dass auch jetzt alles passt.

17.4 Basen von Moduln

Eine Familie $a_i, i \in I$ von Elementen a_i eines R-Moduls V heisse *linear unabhängig* `[linear independent]` , wenn für jede endliche Teilmenge $J \subseteq I$ die Teilfamilie $a_i, i \in J$ die folgende Bedingung erfüllt

$$\text{für alle } r_j \in R \text{ gilt: } \sum_{j\in J} r_j a_j = 0 \Rightarrow r_j = 0 \text{ für alle } j \in J$$

Eine linear unabhängige Familie $a_i, i \in I$ ist *Basis* `[basis]` von V, wenn V von der Menge $\{a_i \mid i \in I\}$ erzeugt wird.

Lemma 17.1 *Für einen R-Modul V und Familie $a_i, i \in I$ von Elementen von V sind äquivalent*

(1) $a_i, i \in I$ ist Basis von V

(2) Jedes Element $v \in V$ hat eindeutige Darstellung $v = \sum_{i\in I} r_i a_i$, $r_i \in R$, $r_i \neq 0$ für nur endlich viele i

(3) $(r_i \mid i \in I) \mapsto \sum_{i\in I} r_i a_i$ ist Isomorphismus von $R^{(I)}$ auf V.

Beweis. Beachte dass die Summen wohldefiniert sind, da nur endlich viele Summanden $\neq 0$. Die Existenz der Darstellung bedeutet Surjektivität der Abbildung, die Eindeutigkeit Injektivität. Die Linearität geht wie in LA. Bei (1) $\Leftrightarrow$ (2) bedeutet die Existenz der Darstellung, dass $\{a_i \mid \in I\}$ Erzeugendenmenge ist; die Eindeutigkeit die Unabhängigkeit von $a_i, i \in I$. □

Satz 17.2 *Jeder K-Vektorraum besitzt eine Basis und ist somit isomorph zu einem Funktionenraum.*

Dieser Satz ist mehr ideologischer Art, da bei Funktionenräumen über $\mathbb{R}$ und $\mathbb{C}$ die topologische Struktur, d.h. die Approximation von Funktionen, das eigentliche Interesse ist. Auch gelingt es selten, eine Basis explizit anzugeben. Insofern genügt folgender 'Beweis': Man denke die Elemente von V aufgezählt

$$0 = v_0, v_1, v_2, \ldots, v_\omega, v_{\omega+1}, \ldots, v_{2\omega}, v_{2\omega+1}, \ldots, v_{\omega^2}, v_{\omega^2+1}, \ldots v_{\omega^2+\omega}, v_{\omega^2+\omega+1}, \ldots$$

was wieder wegen des Auswahlaxioms erlaubt ist (wenn man einmal über das erste 'Unendlich', ω, hinausgezählt hat, geht's viel leichter weiter). Dann fange man an, die Basis aufzubauen, indem man setzt $a_1 = v_1$. Sind v_1, v_2 unabhängig, so $a_2 = v_2$ andernfalls kommt v_2 in den Müll. Allgemein: Sind die a_β für alle $\beta < \alpha$ schon definiert, so ist a_α das erste v_γ, bei dessen Hinzunahme zur Familie die Unabhängigkeit erhalten bleibt

$$a_\alpha = v_\gamma, \quad \gamma \text{ minimal mit } a_\beta(\beta < \alpha), v_\gamma \text{ unabhängig}$$

Warnung. Ist R kein Körper, so werden die wenigsten R-Moduln eine Basis besitzen - z.B. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ als $\mathbb{Z}$- oder $\mathbb{Z}/4Z$-Modul. Ist R nicht kommutativ, so kann ein und derselbe R-Modul Basen unterschiedlicher Größe besitzen. Sei dazu V ein Vektorraum mit Bssis $e_1, e_2, \ldots$ und $R = \mathsf{End}V$. Der R-Modul R hat natürlich die Bssis $\{1\}$. Er hat aber auch eine 2-elementige Basis $\{f_1, f_2\}$ wie folgt

$$f_1(e_{2n}) = e_n,\ f_1(e_{2n-1}) = 0,\ \ f_2(e_{2n-1}) = e_n,\ f_2(e_{2n}) = 0$$

Sie ist unabhängig, weil aus $h_1 f_1 + h_2 f_2 = 0$ folgt $0 = (h_1 f_1 + h_2 f_2)(e_{2n}) = (h_1 f_1)(e_{2n}) = h_1(e_n)$ und ebenso $0 = h_2(e_n)$. Sie ist erzeugend, weil sich jedes $g \in R$ als $g = g_1 f_1 + g_2 f_2$ schreiben lässt mit $g_1(e_n) = g(e_{2n})$ und $g_2(e_n) = g(e_{2n-1})$.

17.5 Direkte Summen: Universelle Eigenschaft

Die direkte Summe

$$A = \bigoplus_{i\in} A_i = \{(a_i \mid i \in I) \mid a_i \in A_i, \text{ nur endliche viele } a_i \neq 0\}$$

von R-Moduln, Gruppen oder Monoiden (in additiver Schreibweise) hat die kanonischen Einbettungen

$$\varepsilon_i : A_i \to A \text{ mit } \pi_i(\varepsilon_i(x)) = x,\ \pi_j(\varepsilon(x)) = 0 \text{ für } j \neq i$$

Im kommotativen Falle ist sie durch folgende Eigenchaft charakterisiert:

- Sind die $\phi_i : A_i \to B$ Homomorphismen, so gibt es einen eindeutig bestimmten Homomorphismus $\phi : A \to B$ in einen R-Modul oder kommutatives Monoid mit $\phi \circ \varepsilon = \phi_i$ für alle $i \in I$

Man hat $\phi((a_i \mid i \in I) = \sum_{i \in I} a_i$ was definiert ist, weil nur endliche viele $a_i \neq 0$. Mit der Kommutativität rechnet man sofort nach, dass es ein Homomorphimsus ist.

Achtung; Zum direkte Produkt zweier nichttrivialer Gruppen A_1, A_2 gibt es immer eine Gruppe B so, dass kein ϕ existiert (vgl. H14).

17.6 Minimale Erzeugendenmengen

Eine Erzeugendenmenge E einer alegrbaischen Struktur heisst *minimal*, wenn keine echte Teimenge von E erzeugdend ist. Nach der Charakterisierung als direkte Summen sind die Basen von R-Moduln minimal erzeugend.

Satz 17.3 *Hat eine Struktur A eine endliche Erzeugendenmenge, so auch minimale und die sind sind alle endlich. Hat die Struktur A keine endliche Erzeugendenmenge, so sind alle minimalen Erzeugendenmengen gleich groß.*

Beweis. Ist B eine Teilmenge von A so gilt

$$\mathsf{Spann}\, B = \bigcup_{X \subset B \text{ endlich}} \mathsf{Spann}\, X$$

weil das eine Unterstruktur ist. Seien nun E und B Erzeugendenmengen. Dann gibt es zu jedem $a \in E$ ein endliches $B_a \subseteq B$ so, dass $a \in \mathsf{Spann}\, B_a$ und es gilt

$$A = \mathsf{Spann}\, B' \text{ mit } B' = \bigcup_{a \in E} B_a \subseteq B$$

Ist B minimal erzeugend, so folgt $B = B'$. Ist E endlich, so also auch B. Andernfalls B höchstens die Kardinaliät $|E \times \mathbb{N}| = |E|$. $\square$.

18 Struktur von Gruppen

18.1 Direktes Produkt von Gruppen

Lemma 18.1 *Ist N ein Normalteiler und U eine Untergruppe von G, so ist $N \cdot U = U \cdot N$ die von $N \cup U$ erzeugte Untergruppe von G. Sind N und M Normalteiler der Gruppe G, so ist $N \cap M$ ein Normalteiler und*

$$N \cdot M = \{a \cdot b \,|\, a \in N, b \in M\}$$

der kleinste Normalteiler $\supseteq N \cup M$ von G.

Beweis. $NU = \bigcup_{u \in U} Nu = \bigcup_{u \in U} uN = UN$. $e = ee \in NU$, $NUNU = NNUU = NU$. $(NU)^{-1} = U^{-1}N^{-1} = UN = NU$, also NU Untergruppe. $gNMg^{-1} = gNg^{-1}gMg^{-1} = NM$, also NM Normalteiler und sicher der kleinste $\supseteq N \cup M$. $\square$ Aus der Entsprechung zwischen Normalteilern und Kongruenzen und der Charakterisierung von direkten Produkten durch Kongruenzen folgt

Korollar 18.2 *Hat die Gruppe G ist isomorph zu $G_1 \times G_2$ genau dann, wenn es Normalteiler N_i gibt mit $G_i \cong G/N_i$ und*

$$N_1 \cap N_2 = \{e\}, \quad N_1 \cdot N_2 = G$$

Der Isomorphismus auf $G/N_1 \times G/N_2$ ist dann durch $x \mapsto (xN_1, xN_2)$ gegeben

Andererseits haben wir in $G = G_1 \times G_2$ die Normalteiler

$$N_1 = \{e\} \times G_2 = U_2, \quad N_2 = G_1 \times \{e\} = U_1$$

und

$$G/N_1 \cong G_1 \cong U_2, \quad G/N_2 \cong G_2 \cong U_1$$

und es gilt

$$U_1 \cap U_2 = \{e\}, \quad U_1 \cdot U_2 = G$$

Seien nun U_1, U_2 Untergruppen von G und $\phi : U_1 \times U_2$ definiert durch $\phi(u_1, u_2) = u_1 u_2$. Dann gilt

- ϕ ist injektiv genau dann, wenn $U_1 \cap U_2 = \{e\}$
- ϕ ist surjektiv genau dann, wenn $U_1 \cdot U_2 = G$
- ϕ ist ein Homomorphismus, wenn $u_1 u_2 = u_2 u_1$ für alle $u_i \in U_i$.

Beweis. Ist $u_1 u_2 = v_1 v_2$ so $v_1^{-1} u_1 = v_2 u_2^{-1} \in U_1 \cap U_2$. Und das is genau dann $= e$, wenn $u_1 = v_1$ und $u_2 = v_2$. Die Aussage zur Surjektivität ist klar. Die Homomorphiebedingung und def. des Produkts besagt dass $u_1 v_1 u_2 v_2 = \phi((u_1 v_1, u_2 v_2)) = \phi((u_1, u_2) \cdot (v_1, v_2)) = u_1 u_2 v_1 v_2$ für alle u_i, v_i, insbesondere $u_1 = e = v_2$, also äquivalent zu $u_2 v_2 = v_1 u_2$ für alle $u_1 \in U_1, v_2 \in U_2$. □

Lemma 18.3 *Seien U_1, U_2 Untergruppen von G. Dann sind äquivalent*

- *$(u_1, u_2) \mapsto u_1 u_2$ ist ein Isomorphismus von $U_1 \times U_2$ auf G.*
- *$U_1 \cap U_2 = \{e\}$, G wird von $U_1 \cup U_2$ erzeugt, $u_1 u_2 = u_2 u_1$ für alle u_i in U_i*
- *$U_1 \cap U_2 = \{e\}$, $U_1 \cdot U_2 = G$, U_1 und U_2 sind Normalteiler von G.*

Man sagt: G ist *inneres direktes Produkt* siner Untergruppen U_1 und U_2. Beweis. Die Vorbemerkung beweist, dass 2 aus 1 folgt. Umgekehrt hat man $U_1 U_2 = G$ wenn G von $U_1 \cup U_2$ erzeugt wird und $u_1 u_2 = u_2 u_1$ gilt. Also folgt 1, aber auch 3: U_1 ist normal, weil für $g = u_1 u_2$ gilt $g U_1 g^{-1} = u_1 u_2 U_1 u_2^{-1} u_1^{-1} = u_1 U_1 u_1^{-1} = U_1$ und U_2 ist normal mit $g = u_2 u_1$ und demselben Argument. Setzen wir 3 voraus, so können wir mit $G \cong G/U_1 \times G/U_2$ argumentieren oder direkt: $u_1 u_2 u_1^{-1} u_2^{-1} \in u_1 u_2 U_1 u_2^{-1} = u_1 U_1 = U_1$ und $\in u_1 U_2 u_1^{-1} u_2^{-1} = U_2 u_2^{-1} = U_2$, also nach Voraussetzung $u_1 u_2 u_1^{-1} u_2^{-1} = e$ und $u_1 u_2 = u_2 u_1$. □.

Korollar 18.4 *Enthält eine Untergruppe G von $O(\mathbb{R}^3)$ die Ursprungsspiegelung $-id$, so ist sie direktes Produkt ihrer Dreh-Untergruppe $U_1 = G \cap SO(\mathbb{R}^3)$ und von $U_2 = \{\mathsf{id}, -\mathsf{id}\} \cong C_2$.*

Beweis. U_1 hat Index 2 und Nebenklasse $U_1\mathsf{id}$, also wird G von $U_2 \cup U_2$ erzeugt. $U_1 \cap U_2 = \{\mathsf{id}\}$ wegen det. Und $-\mathsf{id} \circ \phi = -\phi = \phi \circ \mathsf{id}$ für alle linearen ϕ. $\square$
Beispiel. Die Symmetriegruppe eines Körpers mit einer Punktsymmetrie σ (z.B. Dodekaeder) ist inneres direktes Produkt der Untergruppe U_1 der Drehsymmetrien und $U_2 = \{id, \sigma\}$. Legt man nämlich den Koordinatenursprung in den Punkt, an dem σ spiegelt, so wird σ durch die Matrix $-E$ und die Drehungen durch die orthogonalen Matrizen A mit $\det(A) = 1$ beschrieben. Die Symmetrien lassen sich also eindeutig in der Form AE bzw. $A(-E)$ mit $A \in U_1$ darstellen. Und es gilt $A(-E) = -A = (-E)A$.

Lemma 18.5 *Sind U_1, U_2 Gruppen von G mit Erzeugendenmengen E_1, E_2 und gilt $ab = ba$ für alle $a \in E_1$, $b \in E_2$ so folgt $u_1u_2 = u_2u_1$ für allle $u_i \in U_i$.*

Beweis, Ist $a_i \in U_i$, so $a_i = \prod_{i=1}^{n_i} a_{ik}$ mit $a_{ik} \in E_i$ oder $a_{ik}^{-1} \in E_i$. Auf jeden Fall $a_{ik}a_{jl} = a_{jl}a_{ik}$ für $i \neq j$ nach Regel (9). Also durch Induktion über $n_1 + n_2$
$a_1a_2 = a_{11} \dots a_{1\,n_1-1}a_{1\,n_1}a_{21}a_{22} \dots a_{2\,n_2} = a_{11} \dots a_{1\,n_1-1}a_{21}a_{1\,n_1}a_{22} \dots a_{2\,n_2}$
$= a_{21}a_{11} \dots a_{1\,n_1-1}a_{1\,n_1}a_{22} \dots a_{2\,n_2} = a_{21}a_{22} \dots a_{2\,n_2}a_{11} \dots a_{1\,n_1-1}a_{1\,n_1} = a_2a_1$. $\square$ Die U_i müssen keineswegs kommutativ sein!

18.2 Semidirektes Produkt

Sei N Normalteiler von G und U eine Untergruppe so, dass G von $N \cap U$ erzeugt wird und $N \cap U = \{e\}$. Wir sagen, dass G ein *semidirektes Produkt* von N und U ist. Dann gilt:

- $G = NU = UN$ und jedes Element von G hat eine eindeutige Darstellung $g = nu$ mit $n \in N$, $u \in U$.
- U ist ein Repräsentantensystem für die Nebenklassen von N
- $\varepsilon : G/N \to U$ mit $\varepsilon Ng = u \;\Leftrightarrow\; u \in Ng$, ist wohldefiniert und ein Isomorphimus von G/N auf U
- $\pi \circ \varepsilon = \mathsf{id}_{G/N}$ wobei $\pi : G \to G/N$ kanonische Projektion.

Beispiele. 1. Jede Unterguppe G von $\mathsf{O}(n)$, die eine Spiegelung σ enthält ist semidirektes Produkt von $G \cap \mathsf{SO}(n)$ und $\{\mathsf{id}, \sigma\}$.
2. Die *affine Gruppe* $\mathsf{AG}(n, K)$ ist die Untergruppe von $\mathsf{GL}(n+1, K)$ bestehend aus den Matrizen

$$\begin{pmatrix} 1 & \mathbf{0}^t \\ \boldsymbol{t} & A \end{pmatrix} = \begin{pmatrix} 1 & \mathbf{0}^t \\ \boldsymbol{t} & E \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0}^t \\ \mathbf{0} & A \end{pmatrix} = \begin{pmatrix} 1 & \mathbf{0}^t \\ \mathbf{0} & A \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0}^t \\ A^{-1}\boldsymbol{t} & E \end{pmatrix}, \quad \boldsymbol{t} \in K^n,\ A \in \mathsf{GL}(n, K)$$

und hat den Normalteiler N der *Translationen* bestehend aus den Matrizen mit $A = E$ und die Untergruppe U bestehend aus den Matrizen mit $\boldsymbol{t} = \mathbf{0}$. Dabei ist N zu der additiven Gruppe K^n isomorph und U zu $\mathsf{GL}(n, K)$. Ist $G \supseteq N$ eine Untergruppe von $\mathsf{AG}(n, K)$, so ist G semidirektes Produkt von N und $G \cap U$.

Lemma 18.6 *Sind $\pi : G \to H$ und $\varepsilon : H \to G$ Homomorphismen mit $\pi \circ \varepsilon = \mathsf{id}_H$, so ist G semidirektes Produkt von $N = \mathsf{Kern}\,\pi$ und $U = \mathsf{Bild}\,\varepsilon$. Zudem ist π surjektiv und ε injektiv.*

Beispiele: 2. Bei den Untergguppen von $\mathsf{AG}(n,k)$ haben wir

$$\pi \begin{pmatrix} 1 & \mathbf{0}^t \\ \boldsymbol{t} & A \end{pmatrix} = A, \quad \varepsilon A = \begin{pmatrix} 1 & \mathbf{0}^t \\ \mathbf{0} & A \end{pmatrix}$$

Koordinatenfrei sieht es so aus: Sei G eine Gruppe von affinen Abbildungen, die alle Translationen enthält. Wähle Ursprung O und H als die Untergruppe der Abbildungen in G mit Fixpunkt O. Dann

$$\pi : G \to H \text{ mit } \pi(\phi) = \phi_O = \tau^{-1} \circ \phi \text{ wobei } \tau \text{ die Translation mit } \tau O = \phi O;\ \varepsilon = \mathsf{id}_H$$

3. Sei G eine Untergruppe von $\mathsf{GL}(n,K)$. Definiere $\pi(A) = \det A$, $H = \mathsf{Bild}\,\pi$ und setze voraus, dass

$$\varepsilon : H \to G \text{ mit } \varepsilon a = \begin{pmatrix} a & \mathbf{0}^t \\ \mathbf{0} & E_{n-1} \end{pmatrix}$$

$\mathsf{GL}(n.K)$ ist semidirektes Produkt von $\mathsf{SL}(n,K)$ und einer zur $K^\times$ isomorphen Gruppe.

Beweis. Ist $h \in H$ so $h = \pi\varepsilon h$ also π surjektiv. Ist $\varepsilon h = e$, so $h = \pi\varepsilon h = e$, also π injektiv. Sei $g \in N \cap U$. Dann $g = \varepsilon h$ für ein $h \in H$, und $h = \pi\varepsilon h = \pi g = e_H$ da $g \in \mathsf{Kern}\pi$. Es folgt $g = \varepsilon h = e_G$ und somit $N \cap U = \{e\}$. Für alle $g \in G$ gilt $\pi g = \pi\varepsilon\pi g$. Es folgt $\varepsilon\pi g \sim_N g$, also $g \in N\varepsilon\pi g$. Somit $NU = G$. □

Um ein semidirektes Prododukt bis auf Isomorphie eindeutig zu bestimmen, braucht man neben den Faktoren N und U weitere Information:

- U wirkt durch Konjugation auf N. Die Abbildung

  $$u \mapsto \alpha_u, \quad \alpha_u x = uxu^{-1}\ (x \in N)$$

  ist ein Homomorphimsus von U in die Gruppe $\mathsf{Aut}(N)$ der Automorphismen von N.

- Es handelt sich um ein inneres direktes Produkt von N und U genau dann, wenn $\alpha_u = \mathsf{id}_N$ für alle $u \in U$, d.h. $uxu^{-1} = x$ für alle $u \in U$, $x \in N$.

Satz 18.7 *Sind die Gruppen N und U und ein Homomorphismus $\alpha : U \to \mathsf{Aut}(N)$ gegeben, so wird das direkte Produkt $N \times U$ der Mengen zur Gruppe $N \times_\alpha U$ mit*

$$(n,u) \cdot (m,v) := (n \cdot \alpha_u(m),\ u \cdot v)$$

und diese ist semidirektes Produkt ihrer zu N bzw, U isomorphen Untergruppen $N \times \{e\}$ und $\{e\} \times U$. Ist G ein semidirektes Produkt von N und U mit $\alpha_u x = uxu^{-1}$, so ist G auf natürliche Weise zu $N \times_\alpha U$ isomorph.

Beispiel. Sei $U = \mathbb{Z}/n\mathbb{Z}$, $N = (\mathbb{Z}/n\mathbb{Z})^2$ und α definiert durch

$$\alpha_u(x) = \begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix} x$$

Dann ist $(\mathbb{Z}/n\mathbb{Z})^2 \times_\alpha \mathbb{Z}/n\mathbb{Z}$ eine nichtkommutative Gruppe der Ordnung n^3. Sie ist isomorph D_4 für $n = 2$.

Beweis. $(n,u)\cdot((m,v)\cdot(k,w)) = (n,u)\cdot(m\cdot\alpha_v(k),\, vw) = (n\cdot\alpha_u(m\cdot\alpha_v k),\, uvw) = (n\cdot\alpha_u m\cdot\alpha_u\alpha_v k,\, uvw) = (n\cdot\alpha_u m\alpha_{uv}k,\, uvw) = ((n,u)\cdot(v,m))\cdot(k,w)$. Neutralelement ist (e,e) und

$$(n,u)^{-1} = (\alpha_{u^{-1}}(n^{-1}),\, u^{-1})$$

Wegen $\alpha_e = \mathsf{id}$ ist $N\times\{e\}$ eine zu N ismorphe Untergruppe und Normalteiler, weil $(n,u)\cdot(m,e)\cdot(n,u)^{-1}) = (k, uu^{-1} = (k,e)$ für ein $k\in N$. Die Untergruppe $\{e\}\times U$ ergibt sich wie im direkten Produkt weil $\alpha_u e = e$. Ist ein semidirektes Produkt G gegeben, so definiere man

$$\phi : N\times_\alpha U \to G \text{ durch } \phi(n,u) = nu$$

Das ist bijektiv wegen Existenz und Eindeutigkeit der Darstellung und ein Homomorphimus: $\phi((n,u)\cdot(m,v)) = \phi(n\alpha_u m,\, uv) = \phi(numu^{-1},\, uv) = numu^{-1}uv = numv = \phi(n,u)\cdot\phi(m,v)$. □

Seien U,V,N,M Gruppen und $\alpha : U\to \mathsf{Aut}(N)$ und $\beta : V\to\mathsf{Aut}(M)$ Homomorphismen. Dann sind die zugehörigen semidirekten Produkte $N\times_\alpha U$ und $M\times_\beta V$ isomorph, wenn es Isomorphismen gibt mit

$$(*)\ ;\phi_1 : U\to V,\ \phi_2 : N\to M,\ \ \beta(\phi_1(u))(\phi_2(x)) = \phi_2(\alpha(u)(x)) \text{ für alle } u\in U,\, x\in N$$

d.h. $\phi_2^{-1}\circ\beta(\phi_1(u))\circ\phi_2 = \alpha(u)$ für alle $u\in U$. Das ist hireichend, weils der natürliche Begriff von Isomorphie ist - wenn man $\alpha : U\to\mathsf{Aut}(N)$ als 3-sortige Struktur auffasst.

Umgekehrt sei $G = NU = MV$ inneres semidirektes Produkt und $V = gUg^{-1}$. Definiert man $\phi_1(u) - gug^{-1}$ und $\phi_2(x) = gxg^{-1}$, so ist $(*)$ erfüllt.

18.3 Sylowsätze

Satz 18.8 *Sei G endliche Gruppe und $q = p^\alpha$ eine Primzahlpotenz, die $|G|$ teilt. Dann ist die Anzahl der q-elementigen Untergruppen von G kongruent zu 1 modulo p*

$$|\{U \mid U\subseteq G \text{ Untergruppe }, |U| = q\}| \equiv 1 \mathsf{mod\ p}$$

Eine Untergruppe P von G maximaler p-Potenzordnung (p prim), d.h. mit $|P| = p^\alpha$ Teiler von $|G|$ aber $p^{\alpha+1}$ kein Teiler von $|G|$, heisst eine *p-Sylow-Untergruppe* von G.

Satz 18.9 *Jede Untergruppe von p-Potenzordnung ist in einer p-Sylow-Untergruppe enthalten.*

Satz 18.10 *Je zwei p-Sylow Untergruppen sind zueinander konjugiert.*

Satz 18.11 *Ist $|G| = p^\alpha m$ mit $p\not| m$, so ist die Anzahl der p-Sylow-Untergruppne von G ein Teiler von m.*

Lemma 18.12 *Ist V ein Representantensytem der Wirkung von G auf M, so gilt*

$$|M| = \sum_{a\in V} G(a) = \sum_{a\in V}[G : G_a]$$

Ist e das einzige Element von G mit einem Fixpunkt (man sagt: die Wirkung ist fixpunktfrei*), so gilt*

$$G_a = \{e\},\ \ |G(a)| = |G| \text{ für alle } a\in M, \quad \text{also } |M| = |V|\cdot|G|$$

Das folgt sofort aus der Bahnformel und der Zerlegung der Menge M in disjunkte Bahnen.

Beweis des ersten Sylow-Satzes - nach Wielandt. Stehe $A_G(q)$ für die Anzahl der q-elementigen Untergruppen der Gruppe G wobei $q = p^\alpha$ ein Teiler von $n = |G|$ und p prim. Wir zeigen:

$$(0) \quad \binom{n}{q} \equiv A_G(q) \cdot \frac{n}{q} \mathsf{mod} \ \ \frac{\mathsf{pn}}{\mathsf{q}}$$

Nun gilt

$$\binom{n}{q} \equiv \frac{n}{q} \mathsf{mod} \ \ \frac{\mathsf{pn}}{\mathsf{q}}$$

wie man z.B. dadurch herauskriegt, dass man in (0) für G die zyklische Gruppe C_n einsetzt und bemerkt, dass hier $A_G(q) = 1$ ist. Nun folgt wegen der Transitivität von $\equiv$

$$A_G(q) \cdot \frac{n}{q} \equiv \frac{n}{q} \mathsf{mod} \ \ \frac{\mathsf{pn}}{\mathsf{q}}$$

also

$$p\frac{n}{q} \mid (A_G(q) - 1) \cdot \frac{n}{q}, \quad p \mid A_G(q) - 1 \quad QED$$

Um (0) zu beweisen, werden diverse Wirkungen bemüht, um einen Zusammenhang zwischen $\binom{n}{q}$ und der Gruppe G herzustellen. Die nächstliegende besagt, dass $\binom{n}{q}$ die Anzahl der q-elementigen Teilmengen der n-elementigen Menge G ist

$$\binom{n}{q} = |\mathcal{X}| \quad \text{wobei } \mathcal{X} = \mathcal{P}_{=q}(G)$$

Die Gruppe G wirkt auf $\mathcal{X}$ vermöge $\quad (g, X) \mapsto g \cdot X = gX = \{gx \mid x \in X\}$

und diese Wirkung hat ein Repräsentantensystem $\quad \mathcal{V} \quad$ mit $e \in X$ für alle $X \in \mathcal{V}$

(Zu X wähle man $x \in X$ und $g = x^{-1}$ um $e \in gX$ zu bekommen.) Es folgt mit Bahnformel und Lemma

$$(1) \ \ n = |G| = |G_X| \cdot |G(X)|. \quad (2) \ \ \binom{n}{q} = \sum_{X \in \mathcal{V}} [G : G_X]$$

Dabei ist G_X die Standgruppe von $X \in \mathcal{X}$ unter der Wirkung auf $\mathcal{X}$, d.h.

$$G_X = \{g \in G \mid gX = X\}$$

Somit wirkt G_X auf der Menge X vermöge $\quad (g, x) \mapsto gx$
und das fixpunktfrei. Also nach dem Lemma

$$|G_X(a)| = |G_X| \quad \text{für alle } a \in X \text{ und } \quad |G_X| \text{ teilt } |X| = q$$

Da $q = p^\alpha$ mit primem p, hat man wegen (1)

$$|G_X| \neq q \ \ \Leftrightarrow \ \ \frac{pn}{q} \text{ teilt } |G(X)|$$

Rechnet man modulo $\frac{pn}{q}$ so braucht man demnach in der Summe (2) nur die $X \in \mathcal{V}$ mit $|G_X| = q$ d.h. $[G : G_X] = \frac{n}{q}$ zu berücksichtigen: setze

$$\mathcal{V}_0 = \{X \in \mathcal{V} \mid |G_X| = q\}$$

dann

$$(3)\quad \binom{n}{q} \equiv \sum_{X\in\mathcal{V}_0} [G:G_X] = |\mathcal{V}_0| \cdot \frac{n}{q} \mathsf{mod}\ \frac{\mathsf{pn}}{\mathsf{q}}$$

Schliesslich haben wir noch zu zeigen, dass

$$(4)\quad A_G(q) = |\mathcal{V}_0|$$

Dazu behaupten wir ganz frech, dass $\quad X \in \mathcal{V}_0 \ \Leftrightarrow\ X$ Untergruppe und $|X| = q$

Um das zu beweisen, sei zunächst U eine Untergruppe, $|U| = q$. Nach Wahl von $\mathcal{V}$ gibt es ein $g \in G$ mit $gU \in \mathcal{V}$ und insbesondere $e \in gU$. Also $e = gu$ mit einem $u \in U$, daher $g = u^{-1} \in U$ und schliesslich $gU \subseteq U$, da U Untergruppe. Es folgt $U = gU \in \mathcal{V}$. Weil U Untergruppe ist, besteht seine Bahn unter der Wirkung von G gerade aus den Linksnebenklassen gU und $gU = U \Leftrightarrow g \in U$. Daher $G_U = U$ und somit $|G_U| = q$ und $U \in \mathcal{V}_0$.

Sei umgekehrt $X \in \mathcal{V}_0$. Wir wissen $e \in X$. Es folgt $G_X = G_X \cdot e \subseteq X$. Anderserseits $|G_X| = q = |X|$ und daher $G_X = X$. Nun ist aber G_X eine (Stand)-Untergruppe, also X ebenso. □

Zum Beweis der beiden weiteren Sätze sei P eine p-Sylow-Untergruppe von G. Sowas gibts nach dem ersten Satz. Wir zeigen

$$U \text{ Untergruppe }, |U| = p^\alpha \ \Rightarrow\ \text{es gibt } g \in G \text{ mit } U \subseteq gPg^{-1}$$

Beweis. U wirkt auf $\mathcal{X} = \{gP \mid g \in G\}$ vermöge $\quad (u, gP) \mapsto ugP$

Nun ist wegen der Maximalität von $|P|$ die Zahl p kein Teiler von $[G : P] = |\mathcal{X}|$. Für jedes $X \in \mathcal{X}$ ist die Bahnlänge $|U(X)| = [U : U_X]$ ein Teiler der p-Potenz $|U|$ und $|\mathcal{X}|$ ist die Summe dieser Bahnlängen. Daher ist, Cauchy lässt grüssen, mindestens eine Bahn von Länge 1, d.h sie hat das eine Element gP mit $UgP = gP$. Es folgt $UgPg^{-1} = gPg^{-1}$ und daraus $U = Ue \subseteq gPg^{-1}$. □

Beim vierten Satz betrachten wir die Wirkung von G durch Konjugation auf der Menge der Untergruppen. Der Stabilisator $N(H) = \{g \in G \mid gHg^{-1} = H$ einer Untergruppe H heisst dann auch der *Normalisator* von H und ist die größte Untergruppe U von G so, dass H Normalteiler von U ist. Ist H eine p-Sylow-Untergruppe, so besteht die Bahn von H gerade aus allen p-Sylow-Untergruppen und nach der Bahnformel ist die Anzahl $[G : N(H)]$. Wegen $[G : H] = [G : N(H)] \cdot [N(H) : H]$ ist das ein Teiler von $m = [G : H]$. □

Nach Burnside ist bei Gruppen der Ordnung $p^k q^l$ mit primen p, q die p- oder die q-Sylow-Untergruppe normal. Die mit normaler p-Sylowgruppe N sind dann semidirektes Produkt NU, wo U q-Sylowuntergruppe ist, und ihre Isomorphietypen entspechen bijektiv den Isomorphietypen von Homomorphismem $\alpha : U \to \mathsf{Aut}(N)$ wobei $|N| = p^k$ und $|U| = q^l$.

19 Freie Gruppen

19.1 Involutive Monoide

$(M, \cdot, ^{-1}, e)$ ist ein *involutives Monoid*, falls $(M, \cdot, e)$ ein Monoid ist und gilt $(x{\cdot}y)^{-1} = y^{-1}{\cdot}x^{-1}$ und $(x^{-1})^{-1} = x$ für alle $x \in M$. In G 13a wird das Erzeugnis $\mathsf{Spann}\, E$, das kleinste E umfassende Untermonoid wie folgt beschrieben

$$\mathsf{Spann}\, E = \{a_1^{\varepsilon_1} \dots a_k^{\varepsilon_k} \text{ mit } k \in \mathbb{N},\ a_i \in E,\ \varepsilon = \pm 1\}$$

Anders gesagt, die Element von M mit einer Darstellung in der Form

$$(*) \quad a_1^{\varepsilon_1} \dots a_k^{\varepsilon_k} \text{ mit } k \in \mathbb{N},\ a_i \in E,\ \varepsilon = \pm 1$$

bilden gerade den $\mathsf{Spann}\, E$. Sei dazy X die Menge aller Elemente von M mit einer Darstellung $(*)$. Klar ist $X \subseteq \mathsf{Spann}, E$ weil das Unterstruktur ist. Umgekehrt ist zu zeigen, dass Untersturktuktur ist ($X \supseteq E$ ist klar). D.h. dass Produkt und Inverse von Elementen mit einer Darstellung wie in $(*)$ wieder eine solche haben. Für die Inversen ist das nichttrivial, sondern nur wegen der vorausgesetzen Gleichungen der Fall

$$(a_1^{\varepsilon_1} \dots a_k^{\varepsilon_k})^{-1} = a_k^{-\varepsilon_k} \dots a_1^{-\varepsilon_1}$$

Für das Produkt ist es trivial, aber die Formulierung ist das Problem: das zweite Element müssen wir als $(**)$ $b_1^{\eta_1} \dots b_l^{\eta_l}$ mit $b_i \in E$ und $\eta_i = \pm 1$ schreiben. Und dann ist es trivial. Man darf aber auch exemplarisch argumentieren. Das neutrale Element ist gut versteckt: als das leere Produkt ($n = 0$).

Wir wollen nun die freien involutiven Monoide charakterisieren. Ist eine (Erzeuger)Menge E gegeben, so betrachten wir $E^{-1} = \{a^{-1} \mid a \in E\}$ und nehmen an, dass $E \cap E^{-1} = \emptyset$ und $a \mapsto a^{-1}$ bijektiv, Wir betrachten der (freie) Wortmonoid $W = (E \cup E^{-1})^*$. Seine Elemente haben jetzt eine eindeutige Dsrstellung $(*)$ (aber beachte, dass a^{-1} ein neuer Buchstabe ist). Wir definieren nun

$$(a_1^{\varepsilon_1} \dots a_k^{\varepsilon_k})^{\ominus} = a_k^{-\varepsilon_k} \dots a_1^{-\varepsilon_1}$$

In der Übung G 13 b) wird gezeigt, dass $(W, \cdot, ^{\ominus}, e)$ ein involutives Monoid ist und dass $a^{-1} = a^{\ominus}$ für $a \in E$, Alles trivial bis auf $(w^{\ominus})^{\ominus} = w$ und $(wv)^{-\ominus} = v^{-\ominus} w^{\ominus}$. Ist w wie in $(*)$ gegeben, so nach Definition von $^{\ominus}$

$$(w^{\ominus})^{\ominus} = ((a_1^{\varepsilon_1} \dots a_k^{\varepsilon_k})^{\ominus})^{\ominus} = (a_k^{-\varepsilon_k} \dots a_1^{-\varepsilon_1})^{\ominus} = a_1^{\varepsilon_1} \dots a_k^{\varepsilon_k} = w$$

Haben wir noch ein v, so können wir es wie in $(**)$ schreiben und erhalten

$$(wv)^{\ominus} = (a_1^{\varepsilon_1} \dots a_k^{\varepsilon_k} b_1^{\eta_1} \dots b_l^{\eta_l})^{\ominus} = b_l^{-\eta_l} \dots b_1^{-\eta_1} a_k^{-\varepsilon_k} \dots a_1^{-\varepsilon_1} = w^{\ominus} v^{\ominus}$$

Wir dürfen also schreiben

$$w^{-1} := w^{\ominus}$$

Lemma 19.1 *Das involutive Monoid W ist von E frei erzeugt. Ein Monoid M wird von $E \subseteq M$ frei erzeugt genau dann, wenn jedes Element von M eine eindeutige Darstellung $(*)$ hat.*

Beweis. Zur Freiheit siehe G 13c: Zu zeigen ist, dass es zu jedem involutiven Monoid M und Abbildung $\gamma : E \to M$ eine eindeutig bestimmte homomorphe Fortsetzung $\overline{\gamma} : W \to M$ gibt. Das lässt keine Wahl, als so zu definieren

$$\gamma(a^{-1}) = \gamma)a)^{-1} \quad \text{für } a \in E$$

Nun ist W freies Monoid über $E \cup E^{-1}$, also gibt es einen eindeutig bestimmten Monoidhomomorphimus $\overline{\gamma} : W \to M$, mit

$$\overline{\gamma}(a) = \gamma)a)m \ \ \overline{\gamma}(a^{-1}) = \gamma(a)^{-1}$$

nämlich

$$\overline{\gamma}(a_1^{\varepsilon_1} \dots a_k^{\varepsilon_k}) = \gamma(a_1)^{\varepsilon_1} \dots \gamma(a_k)^{\varepsilon_k}$$

Zu zeigen ist noch, dass $\overline{\gamma}$ auch mit der Inversion vertäglich ist - dau brauchen wir die Definition der Inversion in W und die Gesezte in M

$$\overline{\gamma}((a_1^{\varepsilon_1} \dots a_k^{\varepsilon_k})^{-1}) = \overline{\gamma}(a_k^{-\varepsilon_k} \dots a_1^{-\varepsilon_1}\gamma(a)_k^{-\varepsilon_k} \dots \gamma(a)_1^{-\varepsilon_1} =)\gamma(a_1)^{\varepsilon_1} \dots \gamma(a_k)^{\varepsilon_k})^{-1}$$

Die eindeutige Darstellung ist fúr W klar. Also gilt sie für jedes von E frei erzeugte involutive Monoid, weils zu W isomorph ist. □

Lemma 19.2 *Das Monoid M sei von E erzeugt. Zu jedem $a \in E$ gebe es $b \in M$ mit $ab = e = ba$. Dann ist M eine Gruppe.*

Beweio. Jedes $x \in M$ kann man als $a_1 \dots a_n$ mit $a_i \in E$ schreiben. Nach Vorausseztung gibt es $b_i a_i = e = a_i b_i$. Sei $y = b_n \dots b_1$. Dann $yx - e = xy$. □.

19.2 Freie Gruppe

Sei $\sim$ die feinste Kongruenz aif W so dass

$$aa^{-1} \sim e \sim a^{-1}a \text{ für alle } a \in E$$

In $W/\sim$ haben wir nach Definition von $\sim$ dass $\pi(a^{-1})\pi(a) = \pi(a^{-1}a) = \pi(e) = \pi(aa^{-1} = \pi(a)\pi(a^{-1})$ fúr alle $a \in E$ und können das Lemma anwenden, d.h. wir haben eine Gruppe.

Um zu zeigen dass $\pi : E \to W/\sim$ freie Gruppe ist, haben wir zu jeder Gruppe G und Abbildung $\gamma : E \to G$ einen Homomorphismus $\overline{\gamma} : W/\sim \to G$ so anzugeben, dass $\overline{\gamma} \circ \pi = \gamma$. Nun. G ist auch ein involutives Monoid, also haben wir nach G13c einen Homomorphismus (für involutive Monoide) $\phi : w \to F$ mit $\phi|E = \gamma$. Da G eine Gruppe ist, giilt

$$\phi(aa^{-1}) = \phi(a)\phi(a)^{-1} = e = \phi(a)^{-1}\phi(a) = \phi(aa^{-1}) \;\; a \in E$$

Also ist der $\mathsf{Kern}(\phi)$ eine Kongruenz, die alle $a^1 a$ und aa^{-1} mit e idenifiziert - für $a \in E$. $\sim$ ist nach Definition die feinste solche Kongruenz. also in $\mathsf{Kern}(\phi)$ enthalten. Daher gibt es nach dem Homomorphie-Ergänzungssatz einen (eindeutig bestimmten) Homomorphismus $\overline{\gamma} : W/\sim \to G$ mit $\overline{\gamma} \circ \pi = \phi$. Der tuts. □.
Damit haben wir die Existenz der freien Gruppe aber wir müssen noch herausfinden, was bei $\sim$ wirklich passiert. Das Lemma hätten wir und sparen können, wenn wir $\sim$ als die feinste Kongruenz mit

$$w^{-1} \sim e \sim ww^{-1} \quad w \in W$$

definiert hätten. Dann wüssten wir aber noch weninger, Und auch auch die Monoide und involutiven Monoide hätten wir uns sparen können, wenn wir auf der Termalgeba $\mathbb{T}(E)$ zu den Operationen $\cdot, ,^{-1}, e$ die Kongruenz $\sim$ als die feinste definiert hätten mit

$$t(su) \sim (ts)u, \; et \sim t \sim te. \; t^{-1}t \sim e \sim tt^{-1}, \;\; t, s, u \in \mathbb{T}(E)$$

Dan wüssten wir aber überhaupt nichts, ausser dass es die freie Gruppe über E gibt - und dass das genauso für elle durch Gleichungen definierten Klassen algebraischer Strukturen gilt.

Satz 19.3 *Für eine Gruppe F und Teilmenge E von F sind äquivalent*

- *Jedes Element von F hat eine eindeutige Darstellung*

$$w = a_1^{\varepsilon_1} \cdot \ldots \cdot a_n^{\varepsilon_n} \quad \textit{mit } n \in \mathbb{N},\ a_i \in E,\ \varepsilon_i = \pm 1 \textit{ und } \varepsilon_i + \varepsilon_{i+1} \neq 0 \textit{ für alle } i < n$$

- *Jedes Element von F hat eine eindeutige Darstellung*

$$w = b_1^{z_1} \cdot \ldots \cdot b_m^{z_m} \quad \textit{mit } m \in \mathbb{N},\ b_j \in E,\ z_i \in \mathbb{Z} \textit{ und } b_j \neq b_{j+1} \textit{ für alle } j < m$$

- *Zu jeder Gruppe G und Abbildung $\alpha : E \to G$ gibt es einen eindeutig bestimmten Homomorphismus $\overline{\alpha} : F \to G$ mit $\overline{\alpha}|E = \alpha$.*

Und es gibt zu jedem E ein solche Gruppe G, die freie Gruppe $\mathsf{FG}(E)$.

Beweis. Die Äquivalenz der beiden Darstellungen ergibt sich, indem man ein maximales Teilwort $v = a \cdot \ldots \cdot a$ bzw. $v = a^{-1} \cdot \ldots \cdot a^{-1}$ durch $a^{\pm k}$ ersetzt, k die Länge von v. Und umgekehrt.

Die Existenz einer Gruppe mit eindeutiger Darstellung ist zu zeigen. Die Existenz kann durch unterschiedliche Konstruktionen belegt werde. Eine ist die Homotopiegruppe aus H 17. Eine andere als Untergruppe der Automorphismengruppe bestimmter Graphen kann man aus H 18 ableiten: Sei Γ der gerichtete und mit Werten aus E gewichtete zusammenhämgende Graf, bei dem für jeden Knoten v und $a \in E$ genau eine mit a gewichtete Kante hieningeht und genau eine heraus. Kann man sich für $|E| = 2$ hinmalen. Dann gibt es zu jedem $a \in E$ einen eindeutig bestimmten Automorphismus α_a so, dass v und $\alpha_a(v)$ durch eine Kante mit Gewicht a verbunden sind. Sie G die von den $\alpha_a (a \in E)$ erzeugte Untergruppe der Automorphismengruppe. Die eindeutige Darstellung ist dann offensichtlich. Hat amn die Existenz der freiee Gruppe F ber E durch allgemeines Gelaber wie oben eingesehen, so hat mn den Homomorphismus $\overline{\gamma} : F \to G$ mit $\overline{\gamma}(a)\alpha_a$. Wie in G13 mithile von Socke und Schuh gesehen, hat jedes Element eine Darstellung $(*)$. Da die für das Bild unter $\overline{\gamma}$ eindeutig ist, muss sie auch in F eindeutig sein (und $\overline{\gamma}$ ein Isomorphismus). Wegen der durch die Homomorphie-Fortsetzungeigenschaft gegebenen Eindeutigkeit bis auf Isomorphie haben wir dann auch die behaupteten Äquivalenzen. □

Alternativ können wir die freie Gruppe aus formalem Zeugs zusammenbasteln. Wenn wir schlau sind, machen wir die Konstruktion so, dass wir Fortsetzungseigenschaft und eindeutige Darstellung zugleich bekommen und uns die Laber-Konstruktion sparen. Dazu konstruieren wir die Gruppe aus dem freien involutiven Monoid W. In G 14 wird das schon vorbereitet. Wir müssen allerdings die Kongruenz $\sim$ besser in den Griff bekommen, wenn wir die Eindeutigkeit der Darstellung ablesen wollen. Genauer: wir müssen zeigen, dass die Wörter der im Satz erwähnten Form ein Repräsentantentesystem bilden. Auch dazu gibt es wieder zwei Methoden.

Dwer

Methode der Normalformen. Definiere N als die Menge aller Elemente von W, die kein Teilwort aa^{-1} oder $a^{-1}a$ enthalten. Klar: $E \subseteq M$. $e \in N$ und $w^{-1} \in N$ für $w \in N$. Aber: Das Produkt ist im Allgemeinen nicht wieder in N. Also definieren wir eine neues Produkt $w * v$ für $w, v \in N$ und zeigen, dass

- $(N, *, ^{-1}, e)$ eine Gruppe ist und von E erzeugt
- $\phi(w * v) = \phi(w) \cdot \phi(v)$ für jeden Homomorphismus $\phi : W \to G$, G Gruppe

Haben wir nun eine Abbildung $\gamma : E \to G$ gegeben und ist $\phi : W \to G$ der fortsetzende Homomorphismus involutiver Monoide, so ist die Einschränkung $\overline{\gamma}$ auf N ein Homomorphismus. Also ist N von E frei erzeugt. Wählen wir $G = N$ und $\gamma = \mathsf{id}_E$, so ist $\overline{\gamma}$ surjektiv und daher wegen der Eindeutigkeit der faktorstruktur $\mathsf{Kern}(\overline{\gamma}) = \mathsf{Kern}(\pi) = \sim$. Da $\overline{\gamma}(w) = w$ für die Ezeuger $w \in E$ von N. gilt das auch für alle $w \in N$. Also

$$w \sim v \Rightarrow w = v \text{ für } w, v \in N$$

und wir haben somit ein Repräsentantesytem für $\sim$. Und es folgt $w * v = wv$ falls $wv \in N$. Damit haben wir die eindeutige Darstellung wie gewünscht.

Nun ist es aber echt ätzend, $*$ mathematisch korrekt (d.h. rekursiv) zu definieren und dann die Assoziativität nachzuweisen. Bei so simplen Objekten wie den freien Gruppen gehts auch bequemer mit der Methode der Termersetzung (vgl. G14b).

Der Cayley-Graph einer freien Gruppe (bzg. der frien Erzeuger) ist ein Baum. Umgekehrt is jede Gruppe, die auf einem kreisfreien gerichteten Graphen fixpinktfrei wirk, frei erzeugt von passdenen Erzeugern. Es folgt, dass Untergruppen von freien Gruppen frei sind (Bilsen, Schreier).

19.3 Fundierung

Sei P eine Menge und $\to$ eine Relation auf P. Lies $x \to y$ als x *reduziert direkt* zu y. $(P, \to)$ heisst *fundiert, terminierend, artinsch* (auf informatisch auch noethersch) wenn es keine unendlichen Folgen gibt mit

$$a_0 \to a_1 \to a_2 \ldots$$

Das Beweisprinzip vom *minimalen Verbecher* bzgl. $(P, \to)$ geht so: Sei $A(x)$ eine Aussage über Elemente x von P. Ein Verbecher ist ein Element x von P, für dad $A(x)$ nicht gilt. Er ist *minimal*, wenn $A(y)$ für alle $y \in P$ gilt, zu denen x direkt reduziert, d.h. $x \to y$. Das Beweisprinzip besagt nun

- *Gibt es keine minimalen Verbrecher, so gilt $A(x)$ für alle $x \in P$.*

Prinzip 19.4 *Ist $(P, \to)$ fundiert, so gilt das Prinzip vom minimalen Verbecher.*

Beweis. Angeommen, es gibt keine minimalen Verbecher, aber die Menge V der Verbecher ist nicht leer. Wähle eine Verbrecher v_0, der ist nicht minimal, also kann man einen Vebrecher v_1 mit $v_0 \to v_1$ wählen. U.s.w.: ist der Verbrecher v_n shcon gewähtl, so ist der nicht minimal, also kann man einen Verbecher v_{n+1} mit $v_n \to v_{n+1}$ wählen. Ad infinitum, Widerspruch! □
Hier wurde das Prinzip der bedingten Auswahl benutzt.

Eine *Quasiordung* ist eine reflexive und transitive Relation. Setze $t \leftrightarrow s \Leftrightarrow t \to s$ oder $s \to t$. Wir definieren

$$\begin{aligned} t \xrightarrow{*} s &\quad\Leftrightarrow\quad t = s \text{ oder es gibt } t = t_0 \to t_1 \to \ldots \to t_n = s \\ t \overset{*}{\leftrightarrow} s &\quad\Leftrightarrow\quad t = u \text{ oder es gibt } t = t_0 \leftrightarrow t_1 \leftrightarrow \ldots \leftrightarrow t_n = s \end{aligned}$$

Offenbar handelt es sich um eine Quasiordnung bzw. Äquivalenzrelation, und zwar die kleinste $\to$ umfassende, die von $\to$ *erzeugte*.

a ist *minimal* oder *Normalform* in $(P, \to)$, falls $a \to b$ für kein $b \in P$.

Lemma 19.5 *Ist $\to$ terminierend, so gibt es zu jedem t mindestens eine Normalform u mit $t \stackrel{*}{\to} u$*

Beweis. Sei t ein minimaler Verbecher. Dann ist t selbst keine Normalform, also gibt es b mit $a \to b$ und B ist kein Verbrecher. Also gibt es Normalform u mit $b \stackrel{*}{\to} u$ und dann auch $a \stackrel{*}{\to} u$. Widerspruch. □.

Wir sagen, dass $\to$ lokal konfluent ist, wenn es zu $t \to t_1$, $t \to t_2$ stets s gibt mit $t_1 \stackrel{*}{\to} s$ und $t_2 \stackrel{*}{\to} s$.

Lemma 19.6 Newmann, Diamanten *Ist $\to$ terminierend und lokal konfluent, so gibt es zu jedem t eine eindeutig bestimmte Normalform t' mit $t \stackrel{*}{\to} t'$.*

Beweis durch Überführung der minimalen Verbrecher. Sei t ein solcher. Dann gibt es mindestens zwei verschiedene Normalformen u_1, u_2 mit $t \stackrel{*}{\to} u_1$ und $t \stackrel{*}{\to} u_2$. Nach Definition von $\stackrel{*}{\to}$ gibt es aber

$$t \to t_1 \stackrel{*}{\to} u_1 \quad \text{und} \quad t \to t_2 \stackrel{*}{\to} u_2.$$

Nach der Annahme der lokalen Konfluenz und dem vorangehenden Lemma gibt es aber ein s und dann eine Nromalform u so, dass

$$t_1 \stackrel{*}{\to} s, \quad t_2 \stackrel{*}{\to} s \quad \text{und} \quad s \stackrel{*}{\to} u.$$

Es folgt mit Transitivität

$$t_1 \stackrel{*}{\to} u \quad \text{und} \quad t_2 \stackrel{*}{\to} u.$$

Nun sind aber t_1 und t_2 keine Verbrecher (da ja $t \to t_i$), also folgt $u = u_1$ und $u = u_2$. Also $u_1 = u_2$, ein Widerspruch. □

Korollar 19.7 *Ist $\to$ terminierend und lokal-konfluent auf P, so bilden die Normalformen ein Repräsentantensytem der von $\to$ erzeugten Äquivalenzrelation $\stackrel{*}{\leftrightarrow}$ auf P.*

Beweis. Sei u die eindeutig bestimmte Normalform mit $t \stackrel{*}{\to} u$. Durch Induktion über n in der Def. von $t \stackrel{*}{\leftrightarrow} t_n$ zeigen wir: $t_n \stackrel{*}{\to} u$. Also nach Induktionsannahme $t_{n-1} \stackrel{*}{\to} u$. Gilt $t_n \to t_{n-1}$ so folgt die Behauptung sofort. Andernfalls $t_{n-1} \to t_n$. Es gibt Normalfrom v mit $t_n \stackrel{*}{\to} v$, also $t_{n-1} \stackrel{*}{\to} v$ und somit $v = u$ aus der Eindeutigkeit. □

Wie kann man Termination erreichen? Eine Gewichtung ist eine Abbildung τ in eine geordnete Menge $(M, <)$ mit Minimalbedingung - d.h. jede nichtleere Teilmenge hat ein minimales Element - (z.B. die natürlichen Zahlen mit natürlicher Ordnung) so, dass

$$s \to t \;\Rightarrow\; \tau(t) < \tau(s) \;\text{ für alle } s, t \in P.$$

Lemma 19.8 *Erlaubt $(P, \to)$ eine Gewichtung, so ist es terminierend*

Beweis. Hätte man eine unendliche Folge $a_0 \to a_1 \to \ldots$, so hätte $\{\tau(a_n) | \, n \in \mathbb{N}\}$ kein minimales Element. □

19.4 Gerichtete Termersetzung

In einem Wortmonoid A^* sei eine Menge R von Paaren (r, r') gegeben, die *Erszetzungsregeln* $r \to_0 r$ Das zugehörige *Termersetzungssystem* ist die folgende Relation $\to$ auf A^*

- $w \to w'$ falls es $r \to_0 r'$ in R gibt so,
  dass r als Teilwort in W vorkommt und w' aus w entsteht,
  indem r durch r' ersetzt wird.

Lemma 19.9 $\overset{*}{\leftrightarrow}$ *ist die kleinste Kongruenzrelation auf dem Monoid A^*, die R umfasst.*

Beweis. Es gilt offensichtlich

$$w \to w' \Rightarrow wv \to w'v \text{ und } vw \to vw'$$

Es folgt

$$w \leftrightarrow w' \Rightarrow wv \leftrightarrow w'v \text{ und } vw \leftrightarrow vw'$$

Durch Induktion über die Definition von $\overset{*}{\leftrightarrow}$ folgt

$$w \overset{*}{\leftrightarrow} w' \Rightarrow wv \overset{*}{\leftrightarrow} w'v \text{ und } vw \overset{*}{\leftrightarrow} vw'$$

19.5 Normalformen für die freie Gruppe.

Gegeben sei die Erzeugermenge E. Wir wählen für jedes $a \in A$ ein neues Symbol a^{-1} und betrachten nun das (involutive) Wortmonoid W über dem Alphabet $E \cup E^{-1}$ und die Ersetzungsregeln (dabei ist e das leere Wort)

$$aa^{-1} \to e, \quad a^{-1}a \to e$$

Gilt $w \overset{*}{\to} w'$ so ist w' kürzer als w, also ist $\to$ terminierend. Zum Nachweis der lokalen Konfluenz hat man folgende Fälle zu betrachten

$$w = w_1 a^\varepsilon a^{-\varepsilon} w_2 b^\eta b^{-\eta} w_3, \quad w \to w' = w_1 w_2 b^\eta b^{-\eta} w_3, \; w \overset{*}{\to} w'' = w_1 a^\varepsilon a^{-\varepsilon} w_2 w_3$$

$$\text{hier } w' \overset{*}{\to} w_1 w_2 w_3, \; w'' \overset{*}{\to} w_1 w_2 w_3$$

$$a = b, \; w = w_1 a^\varepsilon a^{-\varepsilon} b^\varepsilon, \quad w \overset{*}{\to} w_1 b^\varepsilon w_2, \; w \overset{*}{\to} w_1 a^\varepsilon w_2$$

$$\text{hier } w_1 b^\varepsilon w_2 = w_1 a^\varepsilon w_2 \text{ weil } a = b$$

Die Kongruenz $\overset{*}{\leftrightarrow}$ is gerade die Kongruenz $\sim$ aus G14. Es folgt, dass $W/\overset{*}{\leftrightarrow}$ freie Gruppe über E ist und dass die Normalformen von $\to$ ein Repräsentantensystem für die Kongruenz $\overset{*}{\leftrightarrow}$ bilden. Die Normalformen sind dadurch charakterisiert, dass sie kein Teilwort der Forn aa^{-1} bzw. $a^{-1}a$ mit $a \in A$ enthalten, bilden also genau die Menge N. □ Die Multiplikation auf N kann man dann so erklären

$$w * v = u \Leftrightarrow \; wv \overset{*}{\to} u \in N$$

Und das ist dann doch etwas geschickter.

Lemma 19.10 *Das Monoid M von E erzeugt, d.h. jedes Element von M hat die Form $\prod_i a_i$ mit a_i in E. Gibt es zu jedem Element a von E ein $a' \in M$ mit $aa' = e = aa$, so ist M eine Gruppe.*

Beweis. $a_1 \cdot \ldots \cdot a_n \cdot a'_n \cdot \ldots \cdot a'_1 = e = a'_n \cdot \ldots \cdot a'_1 \cdot a_1 \cdot \ldots \cdot a_n$ □

Die durch Erzeugende $a_1, \ldots, a_n$ und Relationen $r = e$ ($r \in R$) gegebene Gruppe erhalten wird nun, indem wir in der freien Gruppe $F = \mathsf{FG}(a_1, \ldots, a_n)$ den von R erzeugten Normalteiler N bilden und dann die Faktorgruppe F/N mit Erzeugern $g_i = Na_i$. Der Homomorphieergänzungssatz liefert uns die geforderte Ergänzungseigenschaft. □ Aber wie F/N genau aussieht, wissen wir nur ausnahmsweise.

Lemma 19.11 *Sei G Gruppe und $R \subseteq G$, Dann ist*

$$\mathsf{Nt}(R) = \{\prod_{i=1}^{n} g_i^{-1} r^{\varepsilon_i} g_i \mid n \in \mathbb{N},\ r_i \in R,\ g_i \in G\}$$

der kleinste Normalteiler $\supseteq R$, der von R erzeugte.

Beweis: klar.

Wenn man unbedingt will, kann man aus der eindeutigen Darstellung auf die homomorphe Fortsetzung schliesen. Ist die Abbildung $\alpha : E \to G$ gegeben, so definiere man

$$\overline{\alpha}(w) = \alpha(b_1)^{\varepsilon_1} \cdot \ldots \cdot \alpha(b_m)^{\varepsilon_m}$$

Die Homomorphieeigenschaft ergibt sich aus dem nachstehenden Lemma angewendet auf die Erzeugermenge $E \cup E^{-1}$: Sei w wie oben, $a \in E$ und $\varepsilon = \pm 1$. Ist $a \neq b_m$ so folgt mit der Assoziativiät

$$\overline{\alpha}(w \cdot a^{\varepsilon}) = \alpha(b_1)^{\varepsilon_1} \cdot \ldots \cdot \alpha(b_m)^{\varepsilon_m} \alpha(a)^{\varepsilon} = \overline{\alpha}(w) \cdot \overline{\alpha}(a^{\varepsilon})$$

Sei nun $a = b_m$. Dann

$$\overline{\alpha}(w \cdot a^{\varepsilon}) = \overline{\alpha}(b_1^{\varepsilon_1} \cdot \ldots \cdot b_{m-1}^{\varepsilon_{m-1}} b_m^{\varepsilon_m + \varepsilon}) = \alpha(b_1)^{\varepsilon_1} \cdot \ldots \cdot \alpha(b_{m-1}^{\varepsilon_{m-1}}) \cdot \alpha(b_m)^{\varepsilon_m + \varepsilon}$$

$$= \alpha(b_1)^{\varepsilon_1} \cdot \ldots \cdot \alpha(b_m)^{\varepsilon_m} \alpha(a)^{\varepsilon} = \overline{\alpha}(w) \cdot \overline{\alpha}(a^{\varepsilon})$$

Lemma 19.12 *Seien G und H Gruppen, G erzeugt von E , wobei $b^{-1} \in E$ für alle $b \in E$. Eine Abbildung $\phi : G \to H$ ist genau dann ein Homomorphismus, wenn $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$ für alle $a \in G$ und $b \in E$.*

Beweis: Jedes $b \in G$ lässt sich als $b = \prod_{i=1}^{n} b_i$ mit $b_i \in E$ schreiben. Durch Induktion über k folgt für alle $a \in G$: $\phi(a \cdot \prod_{i=1}^{k} b_i) = \phi((a \cdot \prod_{i=1}^{k-1} b_i) \cdot b_k) = \phi(a \cdot \prod_{i=1}^{k-1} b_i) \cdot \phi(b_k) = \phi(a) \cdot \phi(\prod_{i=1}^{k-1} b_i) \cdot \phi(b_k) = \phi(a) \cdot \phi(\prod_{i=1}^{k} b_i)$. □.

Inhaltsverzeichnis