Einführung in die Algebra , TUD SS 10

Inhaltsverzeichnis

Kapitel 1

Allgemeines

1.1 Ganzzahlige Arithmetik

Dieses Kapitel dient nur zur Auffrischung von Stoff aus der Schule und den ersten 3 Semestern

1.1.1 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.

1.1.2 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

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

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

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

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

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

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

1.1.3 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 1.1.1 *(*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*

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

Der Werteverlauf dieser Funktion ist eindeutig bestimmt.

Definition 1.1.2 *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 $g = 1$, $h(y, z) = (y + 1) \cdot z$

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

1.1.4 Ordnungsinduktion

Prinzip 1.1.3 *(*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 1.1.4 *(*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 1.1.5 *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 1.1.6 *(*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.

1.1.5 Teilbarkeit

In $\mathbb{Z}$ definieren wir

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

Lemma 1.1.7

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

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

Algorithmus 1.1.8 *(*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*

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

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

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

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

Beweis. Die Existenz ergibt sich sofort aus der Formulierung des Algorithmus. Ist nun $a = bq + r = bq' + r'$ und z.B. $r' \geq r$, so folgt $b(q - q') = r' - r$. Also $q - q' = 0$, da sonst $|b| \leq |r' - r| < |b|$. 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 $d \geq 0$, falls es einen gibt, andernfalls $GGT(a,b) = \emptyset$.

Lemma 1.1.9

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

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

Algorithmus 1.1.10 *(*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 1.1.11 $a|(bc) \wedge GGT(ab) = 1 \;\Rightarrow\; a|c$

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 1.1.12 *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 1.1.13 *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 1.1.5. 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. □

1.1.6 Diophantische Gleichungen

Satz 1.1.14 *(Diophant) Es gibt zu gegebenen $a, b, c \in \mathbb{Z}$ genau dann (mindestens) eine ganzzahlige Lösung der Gleichung*

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

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

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

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 1.1.11 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 $y - y_0 = qa'$.

1.2 Algebraische Strukturen

1.2.1 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 $\prod_{i=1}^{m} b_i$.

1.2.2 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.

1.2.3 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 1.2.1 *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).

1.2.4 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.

1.2.5 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

$(G1)$	für alle x, y, z in G gilt	$x(yz) = (xy)z$
$(G2)$	für alle x in G gilt	$ex = x = xe$
$(G3)$	für alle x in G gilt	$xx^{-1} = e = x^{-1}x$

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

$(G2+3)$ es gibt ein Element e von G mit
- (a) für alle x in G gilt $ex = x = xe$
- (b) für alle x in G gibt es ein y in G mit $xy = e = yx$

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 1.2.2 *In einer Gruppe gelten*

(1) $ab = a \iff b = e \iff ba = a$
(2) $b = a^{-1} \iff ab = e \iff ba = e$
(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!

1.2.6 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.

1.2.7 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.

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

1.2.9 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 2.1.1) 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.

1.2.10 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 verknüpft, 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!

1.2.11 Algebren

Sei K ein Körper. Eine *algebraische Struktur* A von Typ der K-Algebra besteht aus einer algebraischen Struktur vom Typ des K-Moduls und einer vom Typ 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.

1.2.12 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*.

1.3 Unterstrukturen und Homomorphismen

1.3.1 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 1.3.1 *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 1.3.2 *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 1.3.3 *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 $e = (g^k)^{-1} g^l = g^{l-k}$. □

1.3.2 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 1.3.4 $\mathsf{Spann}\, E$ *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 1.3.5 *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 1.3.6 *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 1.3.7 *Für eine kommutative K-Algebra A gilt für $E = \{v_1, \ldots, v_n\}$*

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

1.3.3 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 $n = mk$

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

Lemma 1.3.8 *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 Hintereinanderausführung $\psi \circ \phi$ 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 1.3.9 *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.

1.3.4 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 1.3.10 *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.

1.3.5 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

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

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 1.3.11 *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 1.3.12 *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	$\phi(a + b) = \phi a + \phi b, \;\; \phi(a \cdot b) = \phi a \cdot \phi b$	$\phi 1 = 1$
Körper	$\phi(a + b) = \phi a + \phi b, \;\; \phi(a \cdot b) = \phi a \cdot \phi b$	
R-Moduln	$\phi(a + b) = \phi a + \phi b, \;\; \phi(ra) = r\phi a \,(r \in R)$	
R-Algebren	$\phi(a + b) = \phi a + \phi b, \;\; \phi(ra) = r\phi a \,(r \in R), \;\; \phi(a \cdot b) = \phi a \cdot \phi b$	$\phi 1 = 1$

Proposition 1.3.13 *Sei $\mathcal{C}$ wie in der Tabelle und $A \in \mathcal{C}$.*

$B \in \mathcal{C}, \;\; \phi : A \to B$	*mit* $(V) + (N)$	*dann* $\phi : A \to B$ *Homomorphismus*
$B \in \mathcal{C}, \;\; \phi : A \to B$ *surjektiv*	*mit* (V)	*dann* $\phi : A \to B$ *Homomorphismus*
$B \in \mathcal{C}, \;\; \phi : A \to B$ *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 1.3.14 *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 1.3.15 *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.

1.4 Kongruenzrelationen und Faktorisierung

1.4.1 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.

1.4.2 Äquivalenzrelationen

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

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

1.4.3 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 1.4.1 *$a \in \tilde{a}$ 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 1.4.2 *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). □.

1.4.4 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 1.4.3 *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	$a \in \mathbb{Z},\ 0 \leq a < n$

1.4.5 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 1.4.4 *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 1.4.5 *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 1.4.6 *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 1.4.7 *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 1.4.5 haben wir Veträglichkeit mit der Multiplikation. Dann ist aber die Faktorstruktur bzgl. der Multiplikation gemäss 1.3.12 und 1.3.13 eine Gruppe und die Projektion ein Homomorphismus. Also ist $\sim$ nach Satz 1.4.12 eine Gruppenkongruenz.

1.4.6 Beispiele von Kongruenzen

Lemma 1.4.8 *Ist R ein kommutativer Ring und p ein festes Element von R, so wird eine Kongruenz auf R definiert durch*

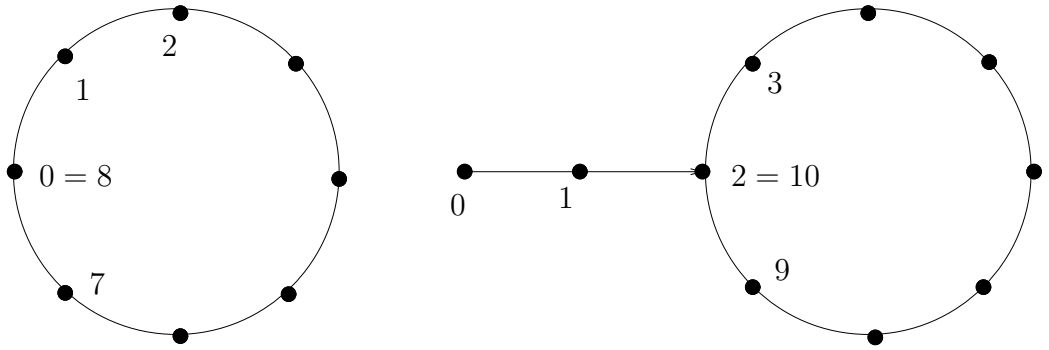
$$a \equiv b\,(\mathsf{mod} p) \;\Leftrightarrow\; p \text{ teilt } a-b \;\Leftrightarrow\; \exists z \in R.\ a-b = pz$$

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 1.4.5 genügt es zu zeigen: $a \sim_{k,p} b \Rightarrow a + c \sim_{k,p} b + c$. Die Klasseneinteilung ist wie in der Skizze.



$\mathbb{N}/\sim_{0,8}$ $\mathbb{N}/\sim_{2,8}$

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 $a \sim_{k,p} b$. □

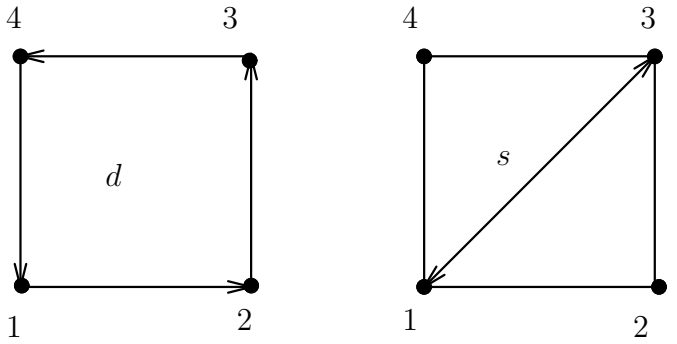
Fasst man Befehle als Buchstaben eines Alphabets und Wörter als Befehlsfolgen auf, so erhält man eine Kongruenz auf dem Wortmonoid, indem man (in einem gegebenen Zusammenhang) für zwei Wörter $a_1 \ldots a_n \sim b_1 \ldots b_m$ setzt, wenn die Befehlsfolgen $a_1, \ldots, a_n$ und $b_1, \ldots, b_m$

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.

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



1.4.7 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 1.4.9 *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*

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

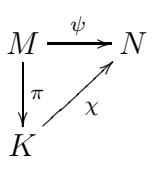
Beweis. Wir zeigen, dass zu einem Normalteiler N eine Gruppenkongruenz $\sim$ gehört. Reflexivität ist trivial. Symmetrie, da N under $^{-1}$ abgeschlossen. Transitivität, da N unter Multiplikation abgeschlossen. Sei $b \sim c$. Dann $ba(ca)^{-1} = bc^{-1} \in N$ und $ab((ac)^{-1} = abc^{-1}a^{-1}$ in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

1.4.8 Ergänzung

Satz 1.4.10 *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

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

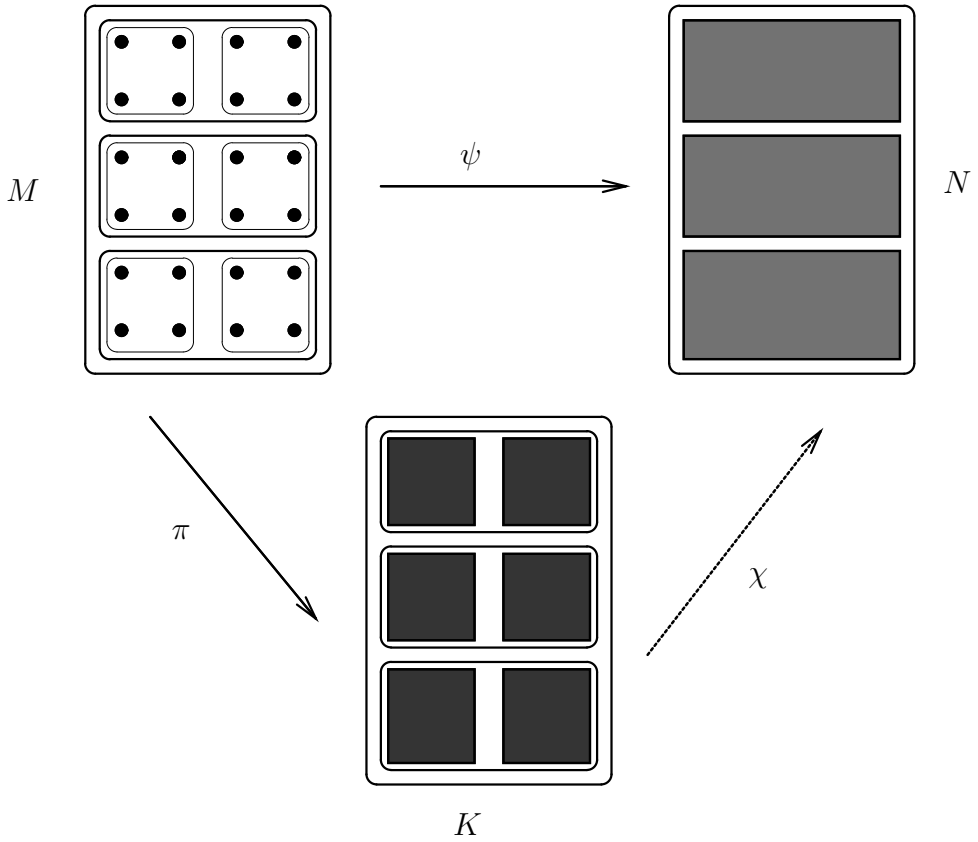
χ ist in der Tat eine Abbildung: Ist $y \in K$ gegeben, so gibt es wegen der Surjektivität von π ein $x \in M$ mit $\pi(x) = y$ und man hat $(y, z) \in \chi$ für $z = \psi(x)$. Hat man $(y, z) \in \chi$ und $(y, z') \in \chi$, so gibt es nach Definition $x, x' \in M$ mit $\pi(x) = y$, $\psi(x) = z$,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

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

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

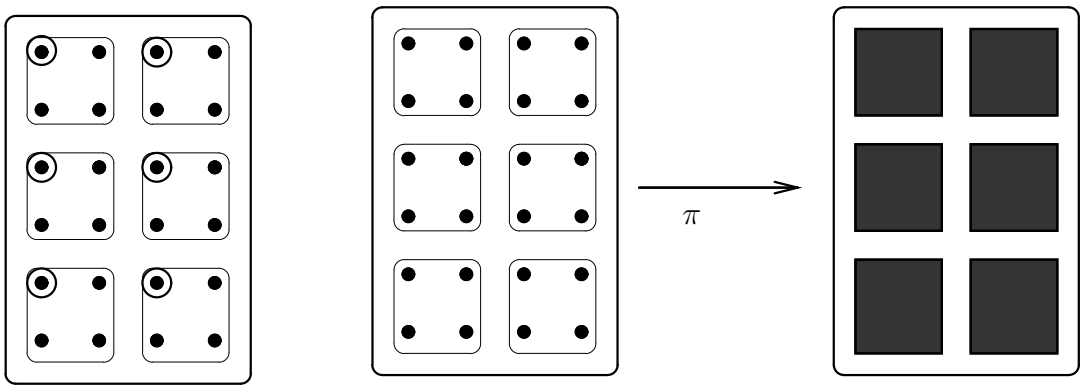
$$= \psi f^M(a_1, \ldots, a_n) = f^N(\psi a_1, \ldots, \psi a_n) = f^N(\chi b_1, \ldots, \chi b_n) \quad \square$$



1.4.9 Abstraktion

Proposition 1.4.11 *Zu jeder Äquivalenzrelation $\sim$ auf einer Menge M gibt es eine Menge K und eine surjektive Abbildung π von M auf K so, dass*

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



Repräsentantensystem M Abstraktion K

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 $\sim$. □ 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

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

1.4.10 Faktorstruktur

Satz 1.4.12 *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

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

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.

Nach 3.11 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

1.4.11 Faktorringe

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 1.4.13 *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 1.4.14 *$\mathbb{Z}/n\mathbb{Z}$ 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 1.4.15 *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. □

1.4.12 Restklassen

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 1.4.8 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. $= \{0\}$.

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.

1.5 Direkte Produkte und Summen

1.5.1 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

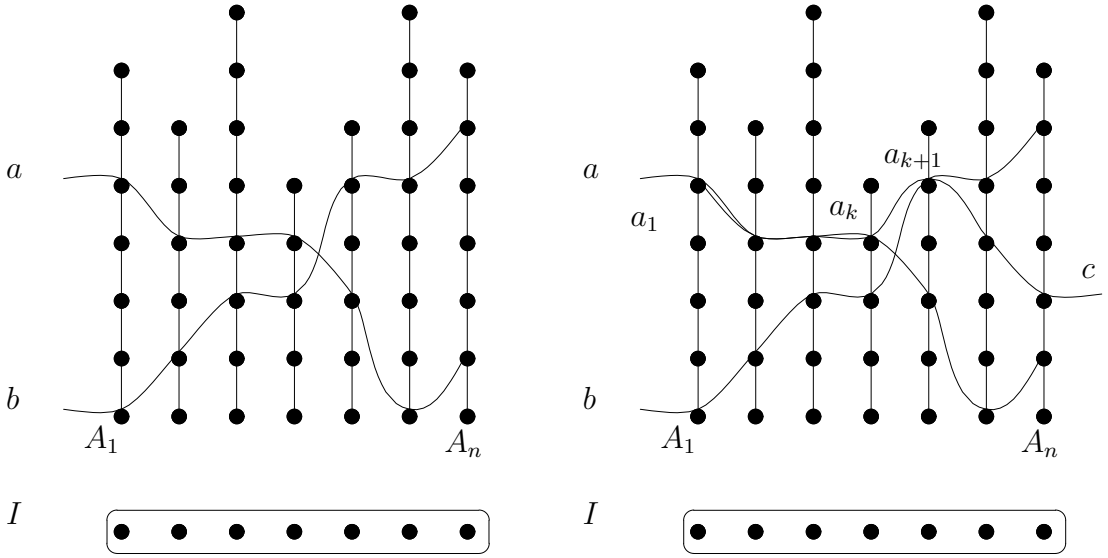
$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ \vdots \\ a_n + b_n \end{pmatrix}, \quad 0 = \begin{pmatrix} 0_1 \\ \vdots \\ 0_n \end{pmatrix}, \quad - \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix}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

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 1.5.1 *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 1.5.2 *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. □.

1.5.2 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 1.5.3 *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) ⇒ (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) ⇒ (3): z.B. $i = 1$. Aus $u_1 = 0 + u_2 + \ldots + u_k$ folgt $u_1 = 0$.
(3) ⇒ (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) ⇒ (4) ist trivial, (4) ⇒ (1) wie eben. (5) ⇔ (2) ist klar. □

1.5.3 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 1.5.4 *$A \cong A_1 \times A_2$ 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 1.5.5 *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*

$$R_i = R/I_i, \quad I_1 \cap I_2 = 0, \quad I_1 + I_2 = R$$

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

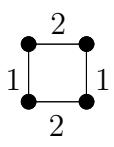
- Ist $1 = s_1 + s_2$ mit *simultanen Kongruenzen*

$$x \equiv a(\mathsf{mod} I_1), \quad x \equiv b(\mathsf{mod} I_2)$$

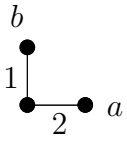
1.5.4 Produkte beschrieben durch Kongruenzen

Die Äquivalenzrelationen $\theta_1, \ldots, \theta_n$ auf einer Menge M bilden eine *direkte Zerlegung*, wenn

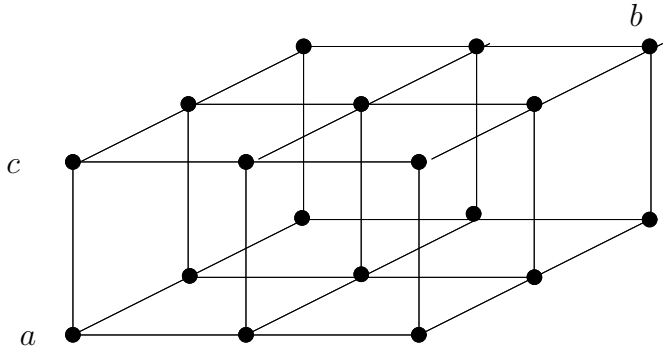
$$\begin{array}{lllll} (*) & \forall a.\forall b. & a\theta_1 b \text{ und } \ldots \text{ und } a\theta_n b & \Rightarrow & a = b \\ (**) & \forall k < n.\forall a.\forall b.\exists c. & a\theta_1 c \text{ und } \ldots \text{ und } a\theta_k c & \text{und} & c\theta_{k+1} b \end{array}$$

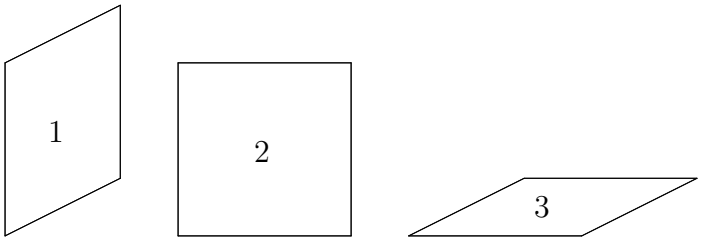


Zerlegung



Keine Zerlegung





Satz 1.5.6 *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 1.5.7 *$A \cong A_1 \times \ldots \times A_n$ 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 1.5.2) erhalten wir $\varepsilon_{k+1}(c) = \hat{\omega}([c]\tau_k, [c]\theta_{k+1})$ und die Behauptung. $\square$

Korollar 1.5.8 *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 $k \neq 1$. $\square$

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

$$e_i \in I_i, \quad r \in I_i \Leftrightarrow r = e_i r$$

$$1 = e_1 + \ldots + e_n,\ e_i^2 = e_i,\ e_i e_j = 0 \text{ für } i \neq j,\ re_i = e_i r \text{ für alle } r \in R$$

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.

Kapitel 2

Groups and actions

2.1 Definitions, examples, and basis facts about groups

2.1.1 Definition

An *algebraic structure* G of group type can be given by a base set G, a binary operation $(x, y) \mapsto x \cdot y = xy$ on G, unary operation $x \mapsto x^{-1}$ on G and a constant e in G. It is a *group* `[Gruppe]`, if the following hold

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

$\cdot$ is the *multiplication* of the group, $^{-1}$ *inversion*, and e the *neutral element*.

Here, the concept of group is based on 4 data: The base set and the 3 operations. If neccessary, we denote this as $(G; \cdot, ^{-1}, e)$. Of course, we may use other symbols, e.g. $(A, +, -, 0)$ with addition $+$. We denote a group shortly e.g. by G if the choice of operations is obvious.

Neutral element and inversion of a group are already unqiuely determined by base set and multiplication resp. addition (cf Lemma). This justifies the

Alternative definition: A group can be given by a base set G and a binary operation $(x, y) \mapsto xy$ on G such that (G1) and

$$\begin{array}{ll} (G2+3) & \text{there is an element } e \text{ of } G \text{ with} \\ & (a) \quad \text{for all } x \text{ in } G \text{ it holds } ex = x = xe \\ & (b) \quad \text{for all } x \text{ in } G \text{ there is } y \text{ in } G \text{ with } xy = e = yx \end{array}$$

That refering to all 3 operations is more adequate will become clear when we discuss subgroups.

2.1.2 Examples

- The integers `[ganzen Zahlen]` form a group $(\mathbb{Z}; +, -, 0)$ w.r.t. the usual addition
- The rational numbers `[rationalen Zahlen]` $\neq 0$ form a group $(\mathbb{Q}_{\neq 0}; \cdot, ^{-1}, 1)$ w.r.t. the usual multiplication
- The real numbers `[reellen Zahlen]` > 0 form a group $(\mathbb{R}_{>0}; \cdot, ^{-1}, 1)$ w.r.t. the usual multiplication

- The bijective maps [bijektive Abbildungen] of a set M into itself from a group S_M w.r.t. the composition [Hintereinanderausführung] $\circ$, the inversion $^{-1}$, and the identity map id_M as neutral element, the *symmetric group* [symmetrische Gruppe] on M. If $M = \{1, 2, \ldots, n\}$ we write $S_n = S_M$.

- Finite groups can be given by a *table* [Tafel] for multiplication, e.g.

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

- $\mathsf{GL}(n, K)$ is the *general linear group* of invertible $n \times n$-matrices over the field K.

- $\mathsf{GL}(V) = \mathsf{Aut}(V)$ is the group of automorphisms (= bijective endomorphisms) of the vector space V

2.1.3 Calculation in a group

Lemma 2.1.1 *In a group*

$$\begin{array}{llllll} (1) & ab = a & \leftrightsquigarrow & b = e & \leftrightsquigarrow & ba = a \\ (2) & b = a^{-1} & \leftrightsquigarrow & ab = e & \leftrightsquigarrow & ba = e \\ (3) & (a^{-1})^{-1} = a & & & & (4)\ (ab)^{-1} = b^{-1}a^{-1} \end{array}$$

Proof. (1). From $ab = a$ it follows by multiplication with a^{-1} from the left $a^{-1}(ab) = a^{-1}a$. Now, by (G1-3) $a^{-1}(ab) = (aa^{-1})b = eb = b$ and $a^{-1}a = e$, whence $b = e$. Similarly, one gets $b = e$ from $ba = a$ by multiplication with a^{-1} on the right. The converses are trivial.

(2). From $ab = e$ it follows by multiplication with a^{-1} from the left that $a^{-1}(ab) = a^{-1}e$. Now, as before $a^{-1}(ab) = b$ and $a^{-1}e = a^{-1}$, whence $b = a^{-1}$. By the same reasoning from $ba = e$ we get $b = a^{-1}$ by multiplication with a^{-1} on the right . The converses are trivial.

(3) follows immediately from (2) with $b = a^{-1}$. In (4), in view of (2), one has to show $(b^{-1}a^{-1})(ab) = e$, only. Indeed: $(b^{-1}a^{-1})(ab) = (b^{-1}(a^{-1}a))b = (b^{-1}e)b = b^{-1}b = e$. (4) is also called the the *rule of sock and boot*. $\square$
The generalization now follows easily by induction

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

We define for a in G

$$a^{n+1} = a^n \cdot a, \quad a^{-n} = (a^n)^{-1} \text{ for } n \in \mathbb{N}$$

If G is a group then (exercise!)

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

2.2 Subgroups and homomorphism

2.2.1 Subgroups

A *subgroup* U of a group G is given by a subset U of G such that

$$e \in U, \quad a, b \in U \Rightarrow a \cdot b \in U, \;\; a \in U \Rightarrow a^{-1} \in U.$$

U is a group, naturally.

Examples

- $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$
- $\mathbb{Q}^\times \subseteq \mathbb{R}^\times \subseteq \mathbb{C}^\times$
- $\mathbb{R}_{>0} = \{x \in \mathbb{R} \mid x > 0\} \subseteq \mathbb{R}$
- $C_n = \{z \in \mathbb{C} \mid z^n = 1\} \subseteq C_m \subseteq S_1 = \{z \in \mathbb{C} \mid |z| = 1|\} \subseteq \mathbb{C}^\times$ for $n \mid m$
- Every vector subspace U of the vector space V is, in particular, a subgroup of V
- $\mathsf{GL}(V)$ is a subgroup of S_V.

2.2.2 Generators

Let E be a subset of the group G and define

$$\begin{aligned} \overline{E} &= \{a_1^{\varepsilon_1} \cdot \ldots \cdot a_n^{\varepsilon_n} \mid n \in \mathbb{N},\, a_i \in E,\, \varepsilon_i = \pm 1\} \\ &= \{b_1^{z_1} \cdot \ldots \cdot b_m^{z_m} \mid m \in \mathbb{N},\, b_i \in E,\, z_i \in \mathbb{Z}\} \end{aligned}$$

Then $\overline{E}$ is a subgroup (since e is the empty product and $(a_1^{\varepsilon_1} \cdot \ldots \cdot a_n^{\varepsilon_n})^{-1} = a_n^{-\varepsilon_n} \cdot \ldots \cdot a_1^{-\varepsilon_1}$) containing E and contained in any subgroyp U of G which contains E. Thus, $\overline{E}$ is the smollest such subgroup and called the subgroup *generated by* E. If $\overline{E} = G$ we say that E is a *set of generators* for G.

- $\mathsf{GL}(n, K)$ is generated by the elementary matrices
- $\mathbb{Z}$ with $+, 0, -$ is generated by 1

2.2.3 Homomorphisms

A *homomorphism* from an algebraic structure A into another, B, both of the typwe of gtoups, is a map $\phi : A \to B$ such that for all $a, b \in A$

$$\phi(a \cdot_A b) = \phi(a) \cdot_B \phi(b), \;\; \phi(a^{-1_A}) = (\phi(a))^{-1_B}, \;\; \phi(e_A) = e_B$$

Example

- $\mathbb{R} \to \mathbb{C}^\times$ with $x \mapsto e^{xi} = \cos x + i \sin x$

Proposition 2.2.1 *Let A be a group and assume that on B there is given a multiplication. Let $\phi : A \to B$ be a map such that $\phi(a \cdot_A b) = \phi(a) \cdot_B \phi(b)$ for all $a, b \in A$. If $\phi : A \to B$ is onto then B is a group.. If B is a group then $\phi : A \to B$ is a homomorphism.*

Proof. Let ϕ be surjective. The associative law carries over to images and $\phi(e)$ is neutral since e.g. $\phi(a)\phi(e) = \phi(ae) = \phi(a)$. Also, $\phi(a^{-1})$ is inverse to $\phi(a)$ (since e.g. $\phi(a^{-1})\phi(a) = \phi(a^{-1}a) = \phi(e)$), so B is a group. Now, assume B is a group. We apply (1) and (2): From $\phi(e_A) \cdot_B \phi(e_a) = \phi(e_A \cdot_A e_A) = \phi(e_A)$ it follows $\phi(e_A) = e_B$ and from $\phi(a^{-1_A}) \cdot_B \phi(a) = \phi(a^{-1_A} \cdot_A a) = \phi(e_A) = e_B$, It follows $\phi(a^{-1_A}) = (\phi(a))^{-1_B}$. □

Define the *kernel*

$$\mathsf{Ker}(\phi) = \{g \in G \mid \phi(g) = e_H\}$$

Lemma 2.2.2 *The kernel of a group-homomorphism $\phi : G \to H$ is a subgroup of G and ϕ injective if and only if $\mathsf{Ker}(\phi) = \{e\}$. The image $\phi(G)$ is a subgroup of H.*

Proog. If $\phi(x) = \phi(y)$ then $\phi(xy^{-1}) = e$ and $xy^{-1} = e$ implies $x = y$. □

Lemma 2.2.3 *Let G and H be groups, G generated by E, where $b^{-1} \in E$ for all $b \in E$. A map $\phi : G \to H$ is a homomorphism, if and only if $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$ for all $a \in G$ and $b \in E$.*

Proof. Each $b \in G$ can be written as $b = \prod_{i=1}^{n} b_i$ with $b_i \in E$. By induction we get for all $a \in G$: $\phi(a \cdot \prod_{i=1}^{k} b_i) = \phi((a \cdot \prod_{i=1}^{k-1} b_i) \cdot b_k) = \phi(a \cdot \prod_{i=1}^{k-1} b_i) \cdot \phi(b_k) = \phi(a) \cdot \phi(\prod_{i=1}^{k-1} b_i) \cdot \phi(b_k) = \phi(a) \cdot \phi(\prod_{i=1}^{k} b_i)$. □.

2.2.4 Isomorphisms

A bijective homomorphism $\phi : A \to B$ is an *isomorphism*. If so, the inverse maps ϕ^{-1} is a homomorphism from B to A. *Example.*

- The logarithm $\ln : (\mathbb{R}_{>0}, \cdot, 1, ^{-1}) \to (\mathbb{R}, +, 0, -)$ with inverse the exponential exp.

2.2.5 Cyclic groups and order of elements

A group with one generator a is a *cyclic group*.

Lemma 2.2.4 *Let G be a group and $a \in G$, Define $\phi(z) = A^z$ for $z \in \mathbb{Z}$, Then ϕ is a sujective homomorphism from $(\mathbb{Z}, +, 0, -)$ onto the subgroup $\overline{\{a\}}$ generated by a. Either, ϕ ia an isomorphism or there is a minimal $n > 0$ such that $a^n = e$. In this case, $\overline{\{a\}}$ is isomorhic to $\mathbb{Z}_n$ and*

$$\overline{\{a\}} = \{e = a^0, a = a^1, \ldots, a^{n-1} = a^{-1}\} \quad \textit{and} \quad a^z = a^w \;\Leftrightarrow\; z \equiv w \mathsf{mod\ n}$$

Proof. If ϕ is not injective, then (since with z also $-z$ belongs to the kernel) there is a minimal $n > 0$ in $\mathsf{Ker}(\phi)$. Now, if $z \neq 0$ is in $\mathsf{Ker}(\phi)$ then by division with remainder $z = qn + r$ where $0 \leq r < n$ and $\phi(r) = \phi(z - qn) = a^z(a^{qn})^{-1} = e \cdot e = e$ whence $r = 0$ by minimality. It follows that $sfKer(\phi)$ consist of the multiples of n. Now, recall that $\phi(z) = \phi(w)$ if and only if $z - w \in \mathsf{Ker}(\phi)$. □

2.3 Group actions and permutations

2.3.1 Group actions

We say that the group G *acts* or *operates* [wirkt] on the set M if with each $g \in G$ and $x \in M$ there is associated a unique element $gx \in M$ such that the following holds

$$ex = x, \quad (h \cdot g)x = h(gx) \text{ for all } x \in M, g, h \in G$$

It follows

$$g^{-1}(gx) = x = g(g^{-1}x) \quad \text{for all } x \in M \text{ and fixed } g \in G$$

which means that the map defined by $\phi_g(x) = gx$ ($x \in M$) is a bijection on M. The axioms of an action can be read as follows: the map $g \mapsto \phi_g$ is a homomorphism from G into S_M.

2.3.2 Examples

- S_M acts on M, canonically.
- $\mathsf{GL}(n, k)$ acts on K^n via $(A, \boldsymbol{x}) \mapsto A\boldsymbol{x}$.
- The group of vectors acts on the affine space.

2.3.3 Orbit

Let G act on M and $a \in M$. The *orbit* of a is defined as

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

Lemma 2.3.1 *The orbits from a partition of M.*

Proof. Let $b \in G(a)$. We have $b = ga$. Thus $hb = hga \in G(a)$ for all $h \in G$ and so $G(b) \subseteq G(a)$. But also $a = g^{-1}b$ whence $G(a) \subseteq G(b)$ and so $G(a) = G(b)$. Now if $c \in G(a) \cap G(b)$ it follows $G(a) = G(c) = G(b)$. □

2.4 Permutations

2.4.1 Cycle decomposition

Given $\sigma \in S_M$ we get an action of $\mathbb{Z}$ on M by

$$za = \sigma^z(a)$$

Assume $M = \{1, \ldots, n\}$ amd let $B_1, \ldots, B_m$ the non-singleton orbits. Observe that by the finiteness of M we have

$$B_i = \{(b, \sigma(b), \sigma^2(b), \ldots, \sigma^{l_i - 1}(b)\} \text{ where } l_i = |B_i|$$

σ is a *cycle* if it has a unique non-singelton orbit. Define

$$\sigma_i(x) = \begin{cases} \sigma(x) & \text{if } x \in B_i \\ x & \text{else} \end{cases}$$

Then we obtain the *cycle decomposition*

$$\sigma = \sigma_m \circ \ldots \circ \sigma_1$$

Here, exeptionally, order does not matter since the B_i's are pairwise disjoint.

Lemma 2.4.1 *Let M be the disjoint union of A and B and $\sigma, \rho \in S_M$ such that*

$$\sigma(A) \subseteq A,\ \sigma|B = \mathsf{id}_B,\ \rho(B) \subseteq B,\ \rho|A = \mathsf{id}_A$$

then $\sigma \circ \rho = \rho \circ \sigma$.

Proof. Let w.l.o.g. $a \in A$. then $\sigma(\rho(a)) = \sigma(a) = \rho(\sigma(a))$ since $\sigma(a) \in A$. □

The σ_i are called the *cycles* of σ and the l_i the *cycle lengths*. We also write

$$\sigma_i = (b\, \sigma(b)\, \sigma^2(b) \ldots \sigma^{l_i - 1}(b))$$

for B_i as above. Of course, this representation is unique up to cyclic permutation.

2.4.2 Sign of a permutation

For $\sigma \in S_M$ we definine the *sign*

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

refering to the cycle decomposition. σ is *even*, if $\mathsf{sign}\, \sigma = 1$, and *odd* if $\mathsf{sign}\, \sigma = -1$. A *transposition* is a permutation τ such that

$$\tau = (ab) \text{ where } \tau(a) = b \neq \tau(b) = a,\ \tau(x) = x \text{ else}$$

and its own inverse. One has $\mathsf{sign}\, \tau = -1$.

Theorem 2.4.2 sign *is a homomorphism from S_n onto the group $\{1, -1\}$. Every permutation is a product of transpositions the number of which is unique modulo 2. It is even iff* $\mathsf{sign}\, \sigma = 1$.

The kernel of sign is a subgroup of S_n, the *alternating group* A_n. The group $\{1, -1\}$ can be considered a subgroup of $K^\times$ where K is a field with $1 + 1 \neq 0$.

Proof. Cycles can be written as transpositions

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

and using cycle decompsition we get any permutation as a product of transpositions. Hence we may apply Lemma 2.2.3 (reverting order of multiplication): given σ and a transposition τ we have to show that

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

Consider the cycle decomposition of σ and let τ have non-trivial orbit $B = \{a, b\}$. Only the following 4 cases may occur in each of which we get a cycle decomposition of $\tau \circ \sigma$. Observe

that each of the following reverts the sign of σ: adding a disjoint transpositioo, decomposing a cycle into two or joining two into one, adding a new element to a cycle.
Case 1: $B \cap B_i = \emptyset$ for all i. Decomopsition $\tau \circ \sigma = \tau \circ \sigma_m \circ \ldots \circ \sigma_1$
Case 2: $B \subseteq B_i$. Here i is unique. Let $\sigma_i = (b_0 \ldots b_l)$ and $a = b_h, b = b_k$, $h < k$. The decomposition of $\tau \circ \sigma$ is obtained replacing σ_i by

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

case 3: $|B \cap B_i| = 1$ for exactly one i, say $a = b_h$. Here, we replace σ_i by

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

Case 4: $|B \cap B_i| = 1 = |B \cap B_j|$ for unique $i < j$, say $a = b_h$, $\sigma_j = (c_r \ldots c_0)$, $b = c_k$. Here, we replace $\sigma_j \circ \sigma_i$ by

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

2.5 Normal subgroups, cosets, order

2.5.1 Congruence relations

Given a structure $(G, \cdot, e, ^{-1})$ of group type, a congruence relation $\sim$ on G is an equivalence relation such that

$$(1) \quad a \sim c \text{ and } b \sim d \Rightarrow a \cdot b \sim c \cdot d$$
$$(2) \quad a \sim c \Rightarrow a^{-1} \sim c^{-1}$$

(1) can be replaced, equivalently, by

$$(1') \quad a \sim c \Rightarrow a \cdot b \sim c \cdot b \quad \text{and } b \sim d \Rightarrow a \cdot b \sim a \cdot d$$

Otherwise, the results of 11.3.1-4 hold, analoguously.

2.5.2 Normal subgroups

A subgroup N of a group G is a *normal subgroup* of G, if $gag^{-1} \in N$ for all $g \in G$ and $a \in N$.

Corollary 2.5.1 *If $\phi : G \to H$ is a group homomorphism then $\mathsf{Ker}\,\phi$ is a normal subgroup of G.*

Proposition 2.5.2 *For groups there is a 1-1-correspondence between congruence relations $\sim$ and normal subgroups N given by*

$$a \sim b \Leftrightarrow ab^{-1} \in N \qquad N = \{x \mid x \sim e\}.$$

Proof. Given a normal subgroup N we show that $\sim$ is a congruence. Reflexivity is trivial. Symmetry since N closed under $^{-1}$. Transitivity since N closed under multiplication. Let $b \sim c$. Then $ba(ca)^{-1} = bc^{-1} \in N$ snd $ab(ac)^{-1} = abc^{-1}a^{-1} \in N$ since N is normal. Thus $ab \sim ac$ and $ba \sim ca$.

If $\sim$ is a congruence then N is the kernel of the canonical projection onto $G/\sim$ whence a normal subgroup.

That $N \mapsto \sim$ and $\sim \mapsto N$ are inverse to each other follows as for vector spaces. $\square$

Corollary 2.5.3 *A subset of G is a congruence class or* a coset *if and only if it has the form*

$$[a] = \{x \in G \mid x \sim a\} = aN = Na = \{an \mid n \in N\}$$

The quotient group $G/\sim = G/N$ may be considered the set of all cosets with group operations

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

Proof. $a \sim b \Leftrightarrow e = a^{-1}a \sim a^{-1}b \Leftrightarrow a^{-1}b \in N \Leftrightarrow b \in aN$ and similarly on the right. □

Corollary 2.5.4 *A subgroup N of G is normal iff $aN = Na$ for all $a \in G$.*

2.5.3 Cosets of subgroups

Given a subgroup H of G define the *right* resp. *left cosets* of H as sets of the form

$$Hg = \{hg \mid h \in H\} \text{ resp. } gH = \{gh \mid h \in H\}$$

Corollary 2.5.5 *The right (resp. left) cosets of H in G form a partition with all classes having size $|H|$.*

Proof. H acts on G by left multiplication:

$$(h, x) \mapsto hx$$

The orbit $H(g)$ of g under this action is the right coset Hg. Thus, we have a partition by Lemma 2.3.1. The map $h \mapsto hg$ from H to Hg has inverse $x \mapsto xg^{-1}$. Thus $|Hg| = |H|$. To deal with left cosets consider right multiplication: $(x, h) \mapsto xh$. This is a "right action" of H i.e. $x(hh') = (xh)h'$ and $xe = x$) and Lemma 2.3.1 holds analoguously. □

2.5.4 Order

The *order* of an group G is its number $|G|$ of elements. The order $\mathsf{ord}(g)$ of an element g of G is the order of the subgroup $\overline{\{g\}}$ generated by g.

Corollary 2.5.6 *Given $n \in \mathbb{N}_{>0}$ and $g \in G$ t.f.a.e.*

(1) $\mathsf{ord}(g) = n$

(2) $\overline{\{g\}} \cong \mathbb{Z}/n\mathbb{Z}$ *for*

(3) $n = \min\{m \in \mathbb{N}_{>0} \mid g^m = e\}$

(4) $g^n = e$ *and for all* $m \in \mathbb{N}_{>0}$*, if* $g^m = e$*, then* n *divides* m*.*

Proof. The equivalence of (1),(2), and (3) follows from Lemma 2.2.4. (4) follows from (2) by inspection of $\mathbb{Z}/n\mathbb{Z}$. The proof of Lemma 2.2.4 also shows that (4) implies (3). □

Corollary 2.5.7 Lagrange. *If G is finite and H a subgroup then $|H|$ divides $|G|$. In particular,* $\mathsf{ord}(g)$ *divides $|G|$ for any $g \in G$.*

Kapitel 3

Gruppen und Wirkungen

3.1 Grundlegendes

3.1.1 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 3.1.1 *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. □

3.1.2 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.

- $\mathsf{GL}(n,k)$ 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

3.1.3 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 3.1.2 *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
$$(z, x) \mapsto \sigma^z(x) \text{ für } z \in \mathbb{Z},\ x \in M$$

3.1.4 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 3.1.3 *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 3.1.4 *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 $x \in M_2$. □

3.1.5 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 3.1.5 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 direkten Beweis folgendes Lemma:

Lemma 3.1.6 *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 Signum von σ umgekehrt: durch Hinzufügen einer disjunkten Transposition, Zerlegung eines Zykus in zwei oder Vereinigung von zwei in einen, schließlich durch Hinzufügen eines Elements 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 $1 + 1 \neq 0$. Das kann man auch als Definition des Signums ansehen und dann die Homomorphieigenschaft aus dem Determinantenproduktsatz folgern.

3.1.6 Reguläre Wirkung

Satz 3.1.7 *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

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

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 3.1.8 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 3.1.9 *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 3.1.10 *Die Ordnung eines Elements a teilt die Gruppenordnung und ist das kleinste $n > 0$ mit $a^n = 1$.*

3.1.7 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 3.1.11 ***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

$$G_{1,2,5} = \{\mathsf{id}, (3\,7)(4\,10)(8\,9)\}$$
$$|G_{1,2}| = |G_{1,2,5}| \cdot 2,\ |G_1| = |G_{12}| \cdot 3,\ |G| = |G_1| \cdot 10 = 120$$

3.1.8 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 3.1.12 *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 ist G isomorph zu seinem Bild in S_M □

Korollar 3.1.13 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.

3.1.9 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 3.1.14 *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 $a^2 = e$, 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 3.1.15 *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.*

3.2 Konjugation

3.2.1 Innere Automorphismen und Konjugation

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

Lemma 3.2.1 *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 3.2.2 *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 3.2.3 *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 bzw. alle 240^o-Grad Drehungen konjugiert, ebenso und alle 180^o-Drehungen.

3.2.2 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 3.2.4 *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

3.2.3 Bestimmung von Konjugiertenklassen

Satz 3.2.5 *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 $M = \{1, \dots, n\}$*

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:

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

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 $1, \dots, n$ 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 3.2.6 *$A, B \in \mathsf{O}(2)$ sind genau dann konjugiert, wenn $A = B^{\pm 1}$ oder $\det A = \det B = -1$*

Korollar 3.2.7 *$A, B \in \mathsf{O}(3, \mathbb{R})$ 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 3.2.8 *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 Ebene orthogonal zu Achse von ϕ (oder ψ) gehört.

3.2.4 Klassengleichung

Korollar 3.2.9 *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 3.2.10 *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 3.2.11 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 $|G|$.*

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

Korollar 3.2.12 *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). □

3.2.5 Dodekaeder und Konjugierte in der Drehgruppe

Lemma 3.2.13 *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

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

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, $\psi\phi\psi^{-1}$ 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 3.2.14 *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. □

3.2.6 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 3.2.15 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

$$\frac{1}{|G|} \sum_{g \in G} |\mathsf{Fix}(g)| = \frac{1}{60}(1 \cdot 2^{12} + 20 \cdot 2^4 + 12 \cdot 2^4 + 12 \cdot 2^4 + 15 \cdot 2^6) = \frac{2^4}{60}(44 + 60 + 256) = 96$$

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 3.2.3) 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

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

□

3.2.7 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

3.3 Lineare Gruppen

3.3.1 Wirkungen der allgemeinen linearen Gruppen

Aus der LA wissen wir

Satz 3.3.1 *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 3.3.2 *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 3.3.3 *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*

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

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 3.3.4 *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).

3.3.2 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 3.3.5 *Für normale Matrizen $A, B \in \mathbb{C}^{n\times n}$ sind äquivalent*

- *A, B haben die gleiche Bahn bei der Rechts-Wirkung $(S, A) \mapsto S^*AS$ 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*

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

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

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

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

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*

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

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).

3.3.3 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 3.3.7 *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 3.3.8 *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 $\mathbb{R}$.

3.4 Struktur von Gruppen

3.4.1 Direktes Produkt von Gruppen

Lemma 3.4.1 *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 3.4.2 *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

$$U_1 = G_1 \times \{e\}, \quad U_2 = \{e\} \times G_2$$

und

$$G/U_1 \cong G_2 \cong U_2, \quad G/U_2 \cong G_1 \cong U_1$$

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 $\phi(u_1, u_2) = u_1u_2$. 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 $u_1u_2 = u_2u_1$ für alle $u_i \in U_i$.

Beweis. Ist $u_1u_2 = v_1v_2$ so $v_1^{-1}u_1 = v_2u_2^{-1} \in U_1 \cap U_2$. 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 $u_1v_1u_2v_2 = \phi((u_1v_1, u_2v_2)) = \phi((u_1, u_2) \cdot (v_1, v_2)) = u_1u_2v_1v_2$ für alle u_i, v_i, insbesondere $u_1 = e = v_2$, also äquivalent zu $u_2v_2 = v_1u_2$ für alle $u_1 \in U_1, v_2 \in U_2$. $\square$

Lemma 3.4.3 *Seien U_1, U_2 Untergruppen von G. Dann sind äquivalent*

- $(u_1, u_2) \mapsto u_1u_2$ *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,* $u_1u_2 = u_2u_1$ *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 $U_1U_2 = G$ wenn G von $U_1 \cup U_2$ erzeugt wird und $u_1u_2 = u_2u_1$ gilt. Also folgt 1, aber auch 3: U_1 ist normal, weil für $g = u_1u_2$ gilt $gU_1g^{-1} = u_1u_2U_1u_2^{-1}u_1^{-1} = u_1U_1u_1^{-1} = U_1$ und U_2 ist normal mit $g = u_2u_1$ und demselben Argument. Setzen wir 3 voraus, so können wir mit $G \cong G/U_1 \times G/U_2$ argumentieren oder direkt: $u_1u_2u_1^{-1}u_2^{-1} \in u_1u_2U_1u_2^{-1} = u_1U_1 = U_1$ und $\in u_1U_2u_1^{-1}u_2^{-1} = U_2u_2^{-1} = U_2$, also nach Voraussetzung $u_1u_2u_1^{-1}u_2^{-1} = e$ und $u_1u_2 = u_2u_1$. □.

Korollar 3.4.4 *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. □
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 3.4.5 *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 $n_1 + n_2$
$a_1a_2 = a_{11} \ldots a_{1\,n_1-1}a_{1\,n_1}a_{21}a_{22} \ldots a_{2\,n_2} = a_{11} \ldots a_{1\,n_1-1}a_{21}a_{1\,n_1}a_{22} \ldots a_{2\,n_2}$
$= a_{21}a_{11} \ldots a_{1\,n_1-1}a_{1\,n_1}a_{22} \ldots a_{2\,n_2} = a_{21}a_{22} \ldots a_{2\,n_2}a_{11} \ldots a_{1\,n_1-1}a_{1\,n_1} = a_2a_1$. □ Die U_i müssen keineswegs kommutativ sein!

3.4.2 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 3.4.6 *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 Unterguppen 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 3.4.7 *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 $G = NU = NV$ inneres semidirektes Produkt und $V = gUg^{-1}$. Definiert man $\phi_1(u) - gug^{-1}$ und $\phi_2(x) = gxg^{-1}$, so ist $(*)$ erfüllt.

3.4.3 Sylowsätze

Satz 3.4.8 *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 3.4.9 *Jede Untergruppe von p-Potenzordnung ist in einer p-Sylow-Untergruppe enthalten.*

Satz 3.4.10 *Je zwei p-Sylow Untergruppen sind zueinander konjugiert.*

Satz 3.4.11 *Ist $|G| = p^\alpha m$ mit $p \not| m$, so ist die Anzahl der p-Sylow-Untergruppen von G ein Teiler von m.*

Lemma 3.4.12 *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:

$$(0) \quad \binom{n}{q} \equiv A_G(q) \cdot \frac{n}{q} \bmod \frac{pn}{q}$$

Nun gilt

$$\binom{n}{q} \equiv \frac{n}{q} \bmod \frac{pn}{q}$$

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 $\equiv$

$$A_G(q) \cdot \frac{n}{q} \equiv \frac{n}{q} \bmod \frac{pn}{q}$$

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

$$(3)\quad \binom{n}{q} \equiv \sum_{X \in \mathcal{V}_0} [G : G_X] = |\mathcal{V}_0| \cdot \frac{n}{q} \bmod \frac{pn}{q}$$

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 $|U| = q^l$.

3.4.4 Isomorphie semidirekter Produkte

Satz 3.4.13 *Seien U und V Gruppen und $\alpha : U \to \mathsf{Aut}(N)$ und $\beta : B \to \mathsf{Aut}(N)$ Homomorphismen.*

(i) Eine hinreichende Bedingung dafür, dass die semidirekten Produkte $N \times_\alpha U$ und $N \times_\beta U$ isomorph sind, ist, dass es $\phi \in \mathsf{Aut}(U)$ und $\psi \in \mathsf{Aut}(N)$ gibt mit

$$\psi^{-1} \circ \beta(\phi(u)) \circ \psi = \alpha(u) \quad \text{für alle } u \in U$$

(ii) Aus der Bedingung in (i) folgt, dass $\mathsf{Bild}(\alpha)$ und $\mathsf{Bild}(\beta) = \mathsf{Bild}(\beta \circ \phi)$ in $\mathsf{Aut}(N)$ konjugiert sind - und gleich, falls $\mathsf{Aut}(N)$ abelsch ist.

(iii) Ist U endlich und entweder zyklisch oder direktes Produkt von Gruppen von Primzahlordnung und sind $\mathsf{Bild}(\alpha)$ und $\mathsf{Bild}(\beta)$ in $\mathsf{Aut}(N)$ konguiert, so gilt $N \times_\alpha U \cong N \times_\beta U$.

(iv) Sei $G = N \times_\alpha U$ so, dass für jede semidirekte Zerlegung $G = MV$ mit $M \cong N$ und $V \cong U$ schon $M = N \times \{e\}$ und V konjugiert zu $\{e\} \times U$ in G ist. Dann gilt $N \times_\alpha U \cong N \times_\beta U$ genau dann, wenn es ϕ und ψ wie in (i) gibt.

Lemma 3.4.14 *Sei G endliche Gruppe unedentweder zyklisch oder direktes Produkt von Gruppen Primzahlordnung. Sind $\alpha : G \to A$ und $\beta : G \to B$ Homomorphismen und gibt es einen Isomorphismus $\omega : \mathsf{Bild}(\beta) \to \mathsf{Bild}(\alpha)$ so gibt es einen Automorphismus ϕ von G so, dass*

$$\alpha = \omega \circ \beta \circ \phi$$

Beweis des Satzes. (i) folgt daraus, dass die angegeben Bedingung gerade die Isomorphie der 3-sortigen Strukturen $\alpha : U \to \mathsf{Aut}(N)$ und $\beta : U \to \mathsf{Aut}(N)$ mit den Sorten U, N und $\mathsf{Aut}(N)$ beschreibt. (ii) ist trivial.

Zu (iii). Sei $\mathsf{Bild}(\alpha) = \psi^{-1} \circ \mathsf{Bild}(\beta) \circ \psi$ für ein $\psi \in \mathsf{Aut}(N)$. Dann gibt es nach Lemma 3.4.14 (mit $G = U$, $A = B = \mathsf{Aut}(N)$ und $\omega(\sigma) = \psi^{-1}\sigma\psi$) einen Automorphismus ϕ von U so, dass (i) gilt.

Zu (iv). Sei $\omega : G' = N \times_\beta U \to G$ Isomorphismus. G' ist semidirekt zerlegt in $N \times \{e\}$) und $\{e\} \times U$. Die Bilder M und V unter ω liefern als eine semidirekte Zerlegung $G = MV$. Nach Voraussetzung $M = N \times \{e\}$ und $V = g(\{e\} \times U)g^{-1}$ für ein g. Wir haben also O.B.d.A. semidirekte Zerlegungen $G = G = NU = NV$ mit $V - gUg^{-1}$. Insbesondre gilt $\alpha_u(x) = uxu^{-1}$ für $u \in U$ und $x \in N$ und $\beta_v(x) = uxu^{-1}$ für $v \in V$ und $x \in N$. Die Bedingung aus (i) ist erfüllt mit

$$\phi(u) = gug^{-1}, \;\; \psi(x) = gxg^{-1}$$

In der Tat

$$\psi^{-1}(\beta(\phi(u))(\psi(x))) = g^{-1}((gug^{-1})(gxg^{-1})(gug^{-1})^{-1})g = uxu^{-1}$$

3.4.5 Endliche zyklische Gruppen

1. Eine endliche Gruppe G ist zyklisch genau dann, wenn $G \cong \mathbb{Z}/(n)$ für ein n, nämlich $n = |G|$

2. Ist U Untergruppe von $\mathbb{Z}/(n)$ und $m > 0$ minimal mit $m \in U$, so ist $m \bmod n$ Erzeuger von U. Insbesondere ist U zyklisch.

3. U ist Untergruppe von $G = \mathbb{Z}/(n)$ genau dann, wenn es Teiler m von n gibt mit
$$U = \{xm \bmod n \mid x \in \mathbb{Z}\} =: mG$$
Dann $G/U \cong \mathbb{Z}(d)$ mit $d = \frac{n}{m}$.

4. Untergruppen U einer endlichen zyklischen Gruppe sind durch ihre Ordnung eindeutig bestimmt.

5. $x \bmod n$ ist Erzeuger von $\mathbb{Z}/(n)$ genau dann, wenn $GGT(x, n) = 1$

6. Chinesischer Restsatz: $\mathbb{Z}/(n) \cong \mathbb{Z}/(m_1) \times \mathbb{Z}/(m_2)$ genau dann wenn $n = m_1 m_2$ und $GGT(m_1, m_2) = 1$. Den Isomorphismus kann man dann wählen als
$$x \bmod n \ \mapsto (x \bmod m_1,\ x \bmod m_2)$$

7. $GGT(m_1, m_2) = 1$ genau dann, wenn es $x_i \in \mathbb{Z}$ gibt mit $x_1 m_1 + x_2 m_2 = 1$

8. Jede endliche zyklische Gruppe ist (isomorph zu einem) direktes Produkt von zyklischen Gruppen von Primzahlpotenzordnung

Beweis. 1. Ist G zyklisch mit Erzeuger g, so wähle $n > 0$ minimal mit $g^n = e$. Dann $g^{-1} = g^{n-1}$ also $G = \{g^k \mid 0 \le k < n\}$. Es folgt für $k > 0$ dass $g^k = e \Leftrightarrow k = dn$ für ein d - wähle d mit $dn \le k < (d+1)n$; dann $k = dn$ weil sonst $g^l = e$ mit $0 < l < n$ im Widerspruch zur Minimalität von n. Nun $g^k = g^l \Leftrightarrow g^{k-l} = e \Leftrightarrow k - l \in n\mathbb{Z}$, also ist $Z/(n) \to G$ mit $(k \bmod n) \mapsto g^k$ Isomorphismus.
2+3+4. Zu $k > 0$ mit $(k \bmod n) \in U$ wähle d mit $dm \le k < (d+1)m$. Wäre $dm < k$ so $m > k - dm \in U$, Widerspruch. Also U zyklisch von Ordnung m und m teilt n nach Lagrange. $d = \frac{m}{n} = [G : U]$ also $G/U \cong \mathbb{Z}/(d)$ da G/U als Bild einer zyklischen Gruppe auch zyklisch ist.
5. O.B.d.A. $0 < x \le n$. Sei d gemeinsamer Teiler von n und x, also $n = rd$ und $x = sd$. Dann
$$rx = rsd = sn = 0 \bmod$$
Aber x Erzeuger heisst $ord(x) = n$ und das bedeutet $r = n$ und somit $d = 1$.
6. Sei $G = \mathbb{Z}/(n)$ und $m_1 m_2 = n$ teilerfremde Zerlegung. Dann hat hat jedes Element x von $m_i G$ eine Ordnung, die $m_j,\ j \ne i$ teilt, da $m_j m_i x = mx = 0$. Also $m_1 G \cap m_2 G = \{0\}$. Andererseits $|m_i G| = m_j$ da $m_i \bmod n$ die Ordnung m_j hat kleiner geht nicht, weil sonst 1 Ordnung kleiner n hätte. Also bilden $m_2 G,\ m_1 G$ eine direkte Zerlegung und somit nach 3.
$$\mathbb{Z}/(n) \cong \mathbb{Z}/m_2 G \times \mathbb{Z}/m_1 G \cong \mathbb{Z}/(m_1) \times \mathbb{Z}/(m_2)$$
Die angegebene Abbildung ist Homomorphismus. Sie ist injektiv, weil aus $n \ge x = 0 \bmod m_i,\ (i = 1, 2)$ dass $n = m_1 m_2$ Teiler von x ist, also $x = n$ oder $x = 0$. Da aber
$$|\mathbb{Z}/(n)| = n = m_1 m_2 = |\mathbb{Z}/(m_1)| \cdot |\mathbb{Z}/(m_2)| = |\mathbb{Z}/(m_1) \times \mathbb{Z}/(m_2)|$$
endlich ist, ist sie auch surjektiv.
7. Hat man für $n = m_1 m_2$ die Zerlegung nach den Chinesischen Restsatz so folgt $1 = x_1 m_1 + x_2 m_2$ aus den inneren direkten Zerlegung. Ist umgekehrt $1 = x_1 m_1 + x_2 m_2$ und d Teiler von m_1 und m_2, so auch von 1.
8. Folgt sofort aus 6 durch Primfaktorzerlegung. □

3.4.6 Endliche abelsche Gruppen

Satz 3.4.15 *Jede endliche abelsche Gruppe ist direktes Produkt von zyklischen Gruppen,*

Diesen Satz beweist man vernünftigerweise im Kontext der Elementarteiler.

Satz 3.4.16 *Ist $G = G_1 \oplus G_2$ eine direkte Zerlegung einer endlichen abelschen Gruppe, und haben $g_1 \in G_1$ und $g_2 \in G_2$ stets teilerfremde Ordnung, so ist jede Untergruppen von G von der Form*

$$U = U_1 \oplus U_2, \quad U_i \text{ Untergruppe von } U_i$$

und dabei $U_i = U \cap G_i$.

Die Umkehrung gilt ohne die Annahme der Teilerfremdheit. Entsprechendes gilt für Normalteiler endlicher Gruppen.

Beweis. Sei $u \in U$. Nach Voraussetzung $u = g_1 + g_2$ mit $g_i \in G_i$ und $ord(g_i) = m_i$ mit teilerfremden m_i. Insbesondere $m_i g_i = 0$. Also

$$u_1 := m_2 u = m_2 g_1 + m_2 g_2 = m_2 g_1 \in U_1. \;\; u_2 := m_1 u \in U_2$$

Nach 3.4.5.7 gibt es $x_i \in \mathbb{Z}$ mit $x_1 m_1 + x_2 m_2 = 1$. Dann

$$u = 1u = x_1 m_1 u + x_2 m_2 u = x_1 u_2 + x_2 u_1 \in U_1 + U_2 \quad \square$$

Beweis des Lemmas 3.4.14. O.B.d.A.

$$\mathsf{Bild}(\alpha) = A, \quad \mathsf{Bild}(\beta) = B$$

und nach dem Ergänzungssatz mit kanonischen Abbildungen

$$\alpha : G \to G/\mathsf{Kern}(\alpha) = A \cong_\omega B = G/\mathsf{Kern}(\beta) \leftarrow G : \beta$$

Sei G zyklisch, o.B.d.A. $G = \mathbb{Z}/(n)$. Dann ist jede Untergruppe durch ihren Isomorphietyp (sogar durch die Ordnung) eindeutig bestimmt, also $\mathsf{Kern}(\alpha) = \mathsf{Kern}(\beta)$ jede solche Kongruenzrelation ist die modulo m mit einem Teiler m von n. Nun wird $B = \mathbb{Z}/(m)$ von $1 \bmod m$ erzeugt und wir haben

$$\omega(1 \bmod m) = a \bmod m \in \mathbb{Z}/(m) = A$$

Nun ist wegen der Isomorphie $a \bmod m$ ein Erzeuger von $\mathbb{Z}/(m)$ also können wir $a \bmod n$ auch als Erzeuger von $\mathbb{Z}/(n)$ wählen - das ist klar falls $n = p^k$ mit Primzahl p, hier sind die Erzeuger in beiden Gruppen die nicht durch p teilbaren a. Für allgemeines n folgt es dann mit dem Chinesischen Restsatz. Definiere nun

$$\phi(a \bmod n) = 1 \bmod n$$

dann setzt sich ϕ zu einem eindeutig bestimmen Automorphismus von $\mathbb{Z}/(n)$ fort und

$$\omega\beta\phi(a \bmod n) = \omega\beta(1 \bmod n) = \omega(1 \bmod m) = a \bmod m$$

Sei nun G direktes Produkt von Gruppen von Primzahlordnung. Fasst man die der gleichen Ordnung p zusammen, so hat man einen $Z/(p)$ Vektorraum V_p, also $G = V_{p_1} \oplus \ldots \oplus V_{p_r}$. Für jede Untergruppe von G gilt dann

$$U = U_1 \oplus \ldots \oplus U_r, \;\; U_i = U \cap V_{p_i}$$

also gibt es W_i mit $V_{p_i} = W_i \oplus U_i$ und Untergruppe $W = W_1 \oplus \ldots \oplus W_r$ mit $G = U \oplus W$. Hat man $U' \cong U$ und entsprechend $G = U' \oplus W'$ so $U' \cap V_{p_i} \cong U \cap V_{p_i}$ also $W' \cap V_{p_i} \cong W \cap V_{p_i}$ und somit $W \cong W'$. Wir haben nun o.B.d.A.

$$\mathsf{Bild}(\alpha) \oplus \mathsf{Kern}(\alpha) = G = \mathsf{Bild}(\beta) \oplus \mathsf{Kern}(\beta)$$

also auch einen Isomorphismus $\rho : \mathsf{Kern}(\beta) \to \mathsf{Kern}(\alpha)$ und setzen $\phi = \omega \oplus \rho$. $\square$.

3.3.8 Supplement

Sei einen (auch mehrsortige) Struktur M gegeben und sei $G = \mathsf{Aut}(M)$ die Automorphismengruppe von M. Wir bertachten Listen $(a_1, \ldots, a_n)$ bzw. $(b_1, \ldots, b_n)$ von Elementen von M so, dass a_i und b_i jeweils von derselben Sorte sind, und Aussagen $\Phi(\xi, x_1, \ldots, x_n)$ über die durch die Wirkung von G auf M gegebene Struktur ${}_GM$

Satz 3.3.17 *(i) Gilt in G $\psi = \omega\phi\omega^{-1}$ und gilt $\omega a_i = b_i$, so gilt*

$$\Phi(\phi, a_1, \ldots, a_n) \Leftrightarrow \Phi(\psi, b_1, \ldots, b_n)$$

(ii) Seien $(a_1, \ldots, a_n)$, $(b_1, \ldots, b_n)$ und Φ gegeben, so dass für alle $\chi \in G$ gilt

$$\chi = \phi \Leftrightarrow \Phi(\chi, a_1, \ldots, a_n), \quad \text{und} \quad \chi = \psi \Leftrightarrow \Phi(\chi, b_1, \ldots, b_n)$$
$$(x_1, \ldots, x_n) = (a_1, \ldots, a_n) \Leftrightarrow \Phi(\phi, x_1, \ldots, x_n)$$
$$(x_1, \ldots, x_n) = (b_1, \ldots, b_n) \Leftrightarrow \Phi(\psi, x_1, \ldots, x_n)$$

Dann $\psi = \omega\phi\omega^{-1}$ genau dann, wenn $\omega(a_i) = b_i$ für $i = 1, \ldots, n$.

Beispiel: Drehgruppe des Dodekaeders. Die Struktur bestehe aus allen Ecken, Flächen, Kanten, den möglichen orientierten Drehachsen, den Vektoren $\overrightarrow{OP}$, O das Zentrum und P eine Ecke sowie der euklidischen Struktur des Raumes und der Determinantenabbildung (d.h. der Orientierung). Die 144^o-Drehung ϕ an der orientierten Achse $\vec{a}$ ist dann eindeutig bestimmt durch die folgende Aussage $\Phi(\phi, \vec{a})$

- $\phi(\vec{x} + O) = \vec{x} + O \;\Leftrightarrow\; \exists r.\, \vec{x} = r\vec{a}$ $\quad$ • $\phi^5 = \mathsf{id}$
- $P\phi(P)$ is ein Kante, wenn P auf zu $\vec{a}$ senkrechtem Pentagon und $\det(\vec{a}, \overrightarrow{OP}, \overrightarrow{O\phi(P)}) = 1$

Da man die orientierten 5-zähligen ortientierten Drehachsen durch Drehungen ineinander überführen kann, folgt mit (ii), dass die 144^o-Drehungen an orientierten Achsen, d.h. die $\pm 144^o$-Drehungen alle zueinander konjugiert saind. Mit (i) folgt, dass sie eine Konjugiertenklasse bilden.
Beweis folgt sofort aus folgendem Lemma und trivialer Logik.

Lemma 3.3.18 *Ist $\omega \in G$ so ist*

$$x \mapsto \omega x \; (x \in M) \quad \phi \mapsto \omega\phi\omega^{-1} \; (\phi \in G)$$

ein Automorphismus der Struktur ${}_GM$.

Beweis.

$$\phi a = b \Rightarrow \; (\omega\phi\omega^{-1})\omega a = \omega\phi a = \omega b$$

3.5 Ergänzungen

3.5.1 Bestimmung von Isomorphietypen

Siehe Vorlesung: Beispiele Ordnung 2p, 12, 20, 30, 55, 60, 75, 147, scan semi.pdf,

3.5.2 Einfacheit der A_n, $b \geq 5$

Siehe Vorlesung und scan An.pdf

3.5.3 Struktur endlicher abelscher Gruppen

Siehe Vorlesung, scan Jordan.pdf und Kap.5.5 und 6.5

3.5.4 Freie abelsche Gruppen

Siehe Vorlesung und Kap.4.

3.5.5 Struktur endlich erzeugter abelscher Gruppen

Siehe Vorlesung und Kap.5.5 und 6.5

3.5.6 Bewegungsgruppe

Siehe Vorlesung und Kap.7