Elementare Algebra und Geometrie
Übersicht über den Stoff

Vorlesung SoSem 2010

PD Dr Dirk Frettlöh
Fakultät Mathematik
Universität Bielefeld

July 20, 2010

Alles Urdenken geschieht in Bildern ARTHUR SCHOPENHAUER

Die Algebra ist nichts anderes als eine symbolische Notierung geometrischer Sachverhalte, die Geometrie ihrerseits — das ist in Figuren verkörperte Algebra

SOPHIE GERMAIN

Vorab: Dies ist eine Zusammenfassung des Stoffes der Vorlesung “Elementare Algebra und Geometrie: Ringe und Symmetriegruppen” im Sommersemester 2010 an der Uni Bielefeld. Die Hörer sind Lehramtsstudenten (Grund-, Haupt- oder Realschule) mit Mathe im Haupt- oder Nebenfach.

Diese Zusammenfassung ersetzt keinesfalls die Mitschrift der Vorlesung, und sie eignet sich nicht als alleinige Lernquelle. Überdies besteht eine große Wahrscheinlichkeit, dass dieser Text Tipp- oder sonstige Fehler enthält. Falls Sie einen finden, bin ich dankbar, wenn Sie mich drauf hinweisen.

Contents

Part I

Gruppen, Ringe, Körper

1 Gruppen, Eigenschaften, Untergruppen

[13.4.2010:]

Definition 1.1. Ein Paar $(G,*)$ mit einer Menge G und einer inneren zweistelligen Verknüpfung $*$: auf G heißt *Gruppe*, wenn folgende Axiome erfüllt sind:

- Abgeschlossenheit: Für alle Gruppenelemente a,b gilt: $a*b \in G$.
- Assoziativität: Für alle Gruppenelemente a,b und c gilt: $(a*b)*c = a*(b*c)$.
- Neutrales Element: Es gibt ein neutrales Element $e \in G$, mit dem für alle Gruppenelemente a gilt: $a*e = e*a = a$.
- Inverses Element: Zu jedem Gruppenelement a existiert ein Element $a^{-1} \in G$ mit $a*a^{-1} = a^{-1}*a = e$.

Eine Gruppe $(G,*)$ heißt *abelsch* oder *kommutativ*, wenn die Verknüpfung * symmetrisch ist, d. h., wenn zusätzlich das folgende Axiom erfüllt ist:

- Kommutativität: Für alle Gruppenelemente a und b gilt $a*b = b*a$.

(Beispiele: s. wikipedia, oder eines der Lehrbücher)

(Einschub: komplexe Zahlen, s. wikipedia, oder eines der Lehrbücher)

[15.4.2010:]

Bemerkung 1.2. Eigenschaften einer Gruppe:

- Das neutrale Element einer Gruppe ist eindeutig bestimmt:
- Es gilt die Kürzungsregel: Aus $a*b = a*c$ oder $b*a = c*a$ mit Gruppenelementen a,b,c folgt jeweils $b = c$.
- Daraus ergibt sich, dass die Verknüpfungstabelle einer Gruppe ein Lateinisches Quadrat ist, bei dem in jeder Zeile und in jeder Spalte jedes Gruppenelement genau einmal vorkommt.
- Die Gleichung $a*x = b$ ist stets eindeutig lösbar und die Lösung ist $x = a^{-1}*b$. Ebenso hat $x*a = b$ die eindeutige Lösung $x = b*a^{-1}$.
- Das zu einem Gruppenelement a inverse Element a^{-1} ist eindeutig bestimmt.
- Es gilt $e^{-1} = e$ und $\left(a^{-1}\right)^{-1} = a$.
- Für alle Elemente gilt $(a*b)^{-1} = b^{-1}*a^{-1}$.

Falls $(G,*)$ eine Gruppe ist und $U \subseteq G$, dann heißt U *Untergruppe* von G, falls $(U,*)$ wieder eine Gruppe ist. Das kann auch so ausgedrückt werden:

Definition 1.3. In der obigen Situation heißt U Untergruppe von G, falls gilt:

- $a,b \in U \Rightarrow a*b \in U$, und
- $a \in U \Rightarrow a^{-1} \in U$

2 Permutationen

Definition 2.1. Eine bijektive Abbildung $f : \{1,2,\ldots,n\} \to \{1,2,\ldots,n\}$ heißt *Permutation*.

Als Wertetabelle, z.B.

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

Kürzer: Notation in Zykelschreibweise:

$$f = (1\ 4)\,(2\ 3)$$

[20.4.:]

Bemerkung: Die Zykeldarstellung ist eindeutig.

Definition 2.2. (und Satz) Die Menge aller Permutationen auf $\{1,2,\ldots,n\}$ bezeichnen wir mit $\mathcal{S}_n$. Mit der Komposition (Hintereinanderausführung) von Funktionen, kurz $\circ$, ist $(\mathcal{S}_n,\circ)$ eine Gruppe.

Bemerkung 2.3. Das Inverse einer Permutation f erhält man durch "Umdrehen" der einzelnen Zykel.

Bsp: $f = (1234)(567)$, dann $f^{-1} = (1432)(576)$.

Bemerkung 2.4. $|\mathcal{S}_n| = n!$

Dabei bezeichnet $|M|$ einfach die Anzahl der Elemente von M.

Bemerkung: $(\mathcal{S}_n,\circ)$ ist nicht kommutativ!

Bemerkung: (Satz von Cayley) Jede endliche Gruppe lässt sich als Untergruppe einer $\mathcal{S}_n$ darstellen.

"Darstellen" heißt hier: "ist isomorph zu". Und isomorph heißt: Gleich bis auf Umbenennung und Umsortierung der Elemente.

Definition 2.5. $|G|$ heißt *Ordnung* von G.

Satz 2.6. (Satz von Lagrange) *Ist U Untergruppe einer Gruppe G, so ist $|U|$ Teiler von $|G|$.*

Definition. $\frac{|G|}{|U|}$ heißt *Index* von U in G.

Folgerung 2.7. *Ist $|G|$ Primzahl, so hat G nur zwei Untergruppen: G selbst und* $\{\mathrm{id}\}$.

Fakt. Jede Permutation lässt sich als Produkt von Zweierzyklen (= Zyklen der Länge 2) schreiben.

Bsp: $(12345) = (12) \circ (23) \circ (34) \circ (45)$

Definition 2.8. Sei $f \in \mathcal{S}_n$. Dann ist das *Signum* von f, kurz: $\operatorname{sgn}(f)$, gleich 1, falls f Produkt von gerade vielen Zweierzyklen ist, und -1 sonst.

Satz 2.9. $\operatorname{sgn}(f) = (-1)^k$, *wobei k die Anzahl der Zyklen von* f *mit gerader Länge ist.*

Satz 2.10. $\mathcal{A}_n = \{f \in \mathcal{S}_n \mid \operatorname{sgn}(f) = 1\}$ *ist Untergruppe von* $\mathcal{S}_n$ *vom Index 2.* $\mathcal{A}_n$ *heißt* alternierende Gruppe.

[22.4.:]

3 Andere wichtige Gruppen

3.1 Die zyklischen Gruppen $\mathcal{C}_n$

Modulorechnen: $b \mod n$ heißt: der ganzzahlige Rest von b geteilt durch n. Z.B. ist 17 durch 5 gleich 3, Rest 2. Also ist 17 mod 5 gleich diesem Rest, also 2. In anderen Worten:

Definition 3.1. $a \equiv b \mod n$, falls $n | b - a$.

Dabei heißt $p|q$: p ist Teiler von q. Im Bsp oben: $5|17-2$, also gilt $17 \equiv 2 \mod 5$.

Definition 3.2. (und Satz) $\mathcal{C}_n := (\{0,1,2,\ldots,n-1\}, + \mod n)$ ist eine Gruppe (mit Addition mod n als Verknüpfung). $\mathcal{C}_n$ heißt *zyklische Gruppe* (der Ordnung n).

$\mathcal{C}_n$ ist endlich, $|\mathcal{C}_n| = n$.

Bemerkung 3.3. $\mathcal{C}_n$ ist kommutativ.

Obiges ist nur eine der Realisierungen der $\mathcal{C}_n$. Man kann sie auch als Untergruppe der $\mathcal{S}_n$ darstellen: Mit $a = (123\ldots n)$ ist die Gruppe $(\{\mathrm{id}, a, a^2, \ldots, a^{n-1}\}, \circ)$ isomorph zur $\mathcal{C}_n$ (also einfach eine andere Darstellung derselben). Dabei heißt $a^2 = a \circ a$, $a^3 = a \circ a \circ a$ usw.

Oder: sie ist auch Symmetriegruppe verschiedener Muster oder Gegenstände.

[Diashow: Wappen, Ornamente, Felgen,... Alle diese Bilder fand ich in der google-Bildersuche, Begriffe: Felgen, Rosette, Ornament; bzw wikipedia: Isle of Man, Füssen]

3.2 Die Diedergruppen $\mathcal{D}_n$

Anschaulich: Die Symmetriegruppe eines regulären n-Ecks enthält n Drehungen (also eine $\mathcal{C}_n$), aber noch mehr: auch noch n Spiegelungen. Diese Symmetriegruppe heißt *Diedergruppe* (sprich: Di-eder).

[27.4.:]

Definition 3.4. (und Satz) Sei $a = (123\ldots n)$ und

$$b = \begin{cases} (1n)(2n-1)\cdots(\frac{n}{2}\ \frac{n+1}{2}) & \text{falls } n \text{ gerade} \\ (2n)(3n-1)\cdots(\frac{n-1}{2}\ \frac{n+1}{2}) & \text{falls } n \text{ ungerade} \end{cases}$$

Dann ist $\mathcal{D}_n = (\{\mathrm{id}, a, a^2, \ldots, a^{n-1}, b, b\circ a, b\circ a^2, \ldots, b\circ a^{n-1}\}, \circ)$ eine Gruppe. Diese heißt *Diedergruppe* (der Ordnung $2n$).

Bemerkung 3.5. $\mathcal{D}_n$ ist nicht kommutativ (für $n > 2$).

Bemerkung 3.6. Als Gruppen sind $\mathcal{C}_2$ und $\mathcal{D}_1$ isomorph (also i.Wes. gleich). Vereinbarung: Wann immer wir von Symmetriegruppen reden, wollen wir $\mathcal{C}_2$ und $\mathcal{D}_1$ unterscheiden: Erstere enthält id und eine 180-Grad-Drehung, zweitere id und eine Spiegelung.

$\mathcal{D}_2$ enthält id, eine 180-Grad-Drehung und zwei Spiegelungen. Damit ist $\mathcal{D}_2$ die Symmetriegruppe eines Rechtecks, oder auch einer Raute $\diamondsuit$.

3.3 Die Tetraedergruppe $\mathcal{T}$

Nummerieren wir die 4 Ecken eines regulären Tetraeders und betrachten alle Symmetrien, so erhalten wir:

Bemerkung 3.7. Es bezeichne $\mathcal{T}$ die Symmetriegruppe eines regulären Tetraeders. $\mathcal{T}$ ist isomorph zu $\mathcal{S}_4$. Falls wir Spiegelungen ausschließen, so erhalten wir die $\mathcal{A}_4$.

[29.4.: Bastelstunde mit zometool]

[4.5.:]

4 Ringe (und Körper)

Definition 4.1. Ein Ring ist eine Menge R mit zwei inneren binären Verknüpfungen "+" und "$\cdot$", so dass gilt

1. $(R, +)$ ist eine kommutative Gruppe,
2. $(R, \cdot)$ ist abgeschlossen
3. $(R, \cdot)$ ist assoziativ
4. Es gelten die Distributivgesetze:

$$a\cdot(b+c) = a\cdot b + a\cdot c \quad \text{und} \quad (a+b)\cdot c = a\cdot c + b\cdot c \quad \text{für alle } a,b,c \in R.$$

So ein Objekt $(R, \cdot)$ (abgeschlossen und assoziativ) heißt auch *Halbgruppe*.

Das neutrale Element von $(R, +)$ heißt *Nullelement* von R und wird einfach mit 0 bezeichnet.

Ein Ring heißt kommutativ, falls er bezüglich der Multiplikation kommutativ ist.

Ab jetzt schreiben wir für die Verknüpfungen in einem Ring immer $+$ und $\cdot$. Das inverse Element von a bzgl Addition bezeichnen wir als $-a$, das inverse Element bzgl Multiplikation als a^{-1}.

Definition 4.2. Eine nichtleere Untermenge U eines Ringes R heißt *Unterring* von R, wenn U zusammen mit den beiden auf U eingeschränkten Verknüpfungen von R wieder ein Ring ist.
Ein Ring S heißt *Oberring* (oder Erweiterung) eines Ringes R, wenn R ein Unterring von S ist.

Besitzt ein Ring ein neutrales Element bezüglich der Multiplikation, so nennt man dieses die Eins (oder das Einselement) des Ringes. Dieses Element wird mit 1 bezeichnet und hat die Eigenschaft

$$1 \cdot a = a \cdot 1 = a \quad \text{für alle } a \in R.$$

Ein Ring mit Einselement wird auch unitärer Ring genannt.

Definition 4.3. Sei R ein unitärer Ring. Gelten die folgenden zusätzlichen Eigenschaften, so heißt $(R, +, \cdot)$ *Körper*.

1. $(R \setminus \{0\}, \cdot)$ ist kommutative Gruppe.
2. $(R, \cdot)$ ist *nullteilerfrei*, d.h. es gibt keine Elemente $a, b \in R$ mit $a \cdot b = 0$.

Insbesondere gilt in einem Körper: es gibt zu jedem $a \in R$ ein inverses Element bzgl der Multiplikation. D.h., für jedes $a \in R$ existiert $a^{-1} \in R$, so dass $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Bsp für Ring: $(\mathbb{Z}, +, \cdot)$. Bsp für Körper: $(\mathbb{R}, +, \cdot)$ und $(\mathbb{Q}, +, \cdot)$. (Jeder Körper ist natürlich automatisch ein Ring.)

Bsp für einen nicht unitären Ring: $(2\mathbb{Z}, +)$.

Definition 4.4. (und Satz) Sei R ein unitärer Ring. Ein Element $a \in R$ heißt *Einheit*, falls es ein Inverses bzgl Multiplikation besitzt (falls es also $b \in R$ gibt mit $a \cdot b = 1$).
Alle Einheiten eines Rings bilden die *Einheitengruppe* $(R^\times, \cdot)$.

5 Endliche Ringe

[6.5.: Fällt ausnahmsweise aus.]

[11.5.:]

Satz 5.1. $(\mathcal{C}_n, + \mod n, \cdot \mod n)$ *ist unitärer kommutativer Ring für* $n \geq 2$.

Satz 5.2. *Ein Element a von* $(\mathcal{C}_n, + \mod n, \cdot \mod n)$ *ist Einheit genau dann, wenn* $\mathrm{ggT}(a, n) = 1$.

Folgerung 5.3. $(\mathcal{C}_n, + \mod n, \cdot \mod n)$ *ist Körper genau dann, wenn n prim ist.*

5.1 Teilbarkeit und Primzahlen

Definition 5.4. Eine Zahl $m \in \mathbb{N}$ heißt *Teiler* einer Zahl $n \in \mathbb{Z}$, falls es ein k gibt, so dass $m \cdot k = n$. (Also falls $n/m = k \in \mathbb{Z}$.)

Definition 5.5. Eine Zahl $n \in \mathbb{Z}$ heißt *Primzahl*, falls 1 und n die einzigen Teiler von n sind.

Definition 5.6. Der *größte gemeinsame Teiler* von m und n (kurz: $\mathrm{ggT}(m, n)$) ist $\max\{q \mid q|n \text{ und } q|m\}$.

Man könnte den ggT von n und m über die Primfaktorzerlegung von n und m zu finden. Das ist aber i.Allg. knifflig (siehe [WIK], Stichwort RSA Factoring Challenge). Daher:

(Erweiterter) Euklidischer Algorithmus

Gegeben $k > m > 0$. Frage: $ggt(k,m) = ?$

Schritt 0: $a_1 := k,\ a_2 := m,\ n := 2; \quad (c_1 := 1, c_2 := 0, d_1 := 0, d_2 := 1)$

Schritt 1: $q_n := \max\{r \in \mathbb{N} \mid a_{n-1} - r a_n \geq 0\},\ a_{n+1} := a_{n-1} - q_n a_n,$
$(c_{n+1} := c_{n-1} - q_n c_n, \quad d_{n+1} := d_{n-1} - q_n d_n)$

Schritt 2: Falls $a_{n+1} = 0$: STOP, sonst $n := n+1$, weiter bei Schritt 1.

Beim Abbruch ($a_{n+1} = 0$) ist $a_n = \mathrm{ggT}(k,m)$ (und $\mathrm{ggT}(k,m) = c_n k - d_n m$).

Der liefert auch Lösung zu folgender Frage:

Satz 5.7. *Gegeben $n \in \mathbb{N}$ und $a, b \in \{0,1,\ldots,n-1\}$. Die Gleichung $a \cdot x \equiv b \mod n$ hat eine Lösung (in x) genau dann, wenn $\mathrm{ggT}(a,n) | b$. Es gibt dann genau $\mathrm{ggT}(a,n)$ Lösungen.*

[13.5.: Feiertag]

[18.5.:]

Wie genau finden wir die Lösungen von $ax \equiv b \mod n$, falls es sie gibt:

Bemerkung 5.8. Berechne mit dem erweiterten Euklidischen Algorithmus eine Lösung p, q von $g := \mathrm{ggT}(a,n) = pa + qn$.

- Falls $g \not| b$: Es gibt keine Lösung.

- Falls $g | b$: Die Lösungen sind $x = \frac{pb}{g} + \frac{kn}{g}$, wobei $k = 0, 1, \ldots, g-1$.

Mit Satz 5.7 beweist man nun Satz 5.2, denn: Ein $a \in \mathcal{C}_n$ ist ja laut Definition Einheit, wenn es $x \in \mathcal{C}_n$ gibt mit $a \cdot x \equiv 1 \mod n$.

Mehr Interessantes über endliche Ringe in [WIK], unter "Ring_(mathematics)".

6 Der Ring $\mathbb{Z}[i]$ der Gaußschen Zahlen

$\mathbb{C} := \{a + bi \mid a, b \in \mathbb{R}\}$ ist die Menge der *komplexen Zahlen*. Dabei ist i die *imaginäre Einheit*: Die (bzw eine) Zahl mit der Eigenschaft $i^2 = -1$. Die natürliche Weise, komplexe Zahlen zu addieren ist

$$(a+bi) + (c+di) = (a+c) + (b+d)i$$

und die Multiplikation ist

$$(a+bi) \cdot (c+di) = (ac - bd) + (ad + bc)i.$$

Nun sei $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$.

Satz 6.1. *$(\mathbb{Z}[i], +, \cdot)$ ist ein kommutativer unitärer Ring. (Und $(\mathbb{C}, +, \cdot)$ ist ein Körper.)*

Wichtig:

Definition 6.2. Zu einem Element $x = a + bi$ in $\mathbb{C}$ heißt $\overline{x} = a - bi$ das *komplex konjugierte (Element)*.

Dabei ist $x\overline{x}$ immer reell:

$$x\overline{x} = (a+bi)(a-bi) = (a^2 - (-b^2)) + (ab - ab)i = a^2 + b^2$$

Daher definiere einen Größenbegriff, die *komplexe Norm* (von x):

$$N(x) = N(a+bi) := a^2 + b^2$$

Lemma 6.3. *Seien $x, y \in \mathbb{Z}[i]$. Es gilt:*

(a) $N(x) \in \mathbb{Z}$

(b) $N(xy) = N(x)N(y)$.

Satz 6.4. *Die Einheitengruppe $\mathbb{Z}[i]^\times$ ist $(\{1, -1, i, -i\}, \cdot)$.*

[20.5.:]

Motivation: Wie kann Algebra genutzt werden, um eine zahlentheoretische Frage zu beantworten. Hier: Welche (Prim-)Zahlen kann ich als Summe von zwei Quadratzahlen schreiben? Dazu: Die entsprechung von Primzahlen in $\mathbb{Z}$ sind Primelemente in $\mathbb{Z}[i]$:

Bezeichnung: Ein $x \in \mathbb{Z}[i]$, für dass gilt: aus $y|x$ folgt $y = \pm 1$; $\pm i$ $\pm x$; $\pm ix$ heißt *Primelement*.

Wie sehen die aus?

Lemma 6.5. *(a)* $\forall x \in \mathbb{Z}[i] : x|N(x)$.
(b) $\forall x, y \in \mathbb{Z}[i] : x|y \Rightarrow N(x)|N(y)$.

[25.5.:]

Also: Um Teiler von x zu finden, finde erst die Teiler $n_1, n_2, \ldots, n_k$ von $N(x)$. Finde dann $y_j \in \mathbb{Z}[i]$ mit $N(y_j) = n_j \quad (j = 1, \ldots, k)$. Das sind mögliche Teiler von x.

Dabei wollen wir Elemente in $\mathbb{Z}[x]$ als "gleich" auffassen (zumindest bzgl ihrer Teilereigenschaften), falls sie durch Multiplikation mit einer Einheit auseinander hervorgehen.

Definition 6.6. Falls $x = \pm y$ oder $x = \pm iy$, so heißen x und y *assoziiert (zueinander)*.

Z.B. $2 + i$ und $1 - 2i$ sind assoziiert zueinander, denn $-i(2+i) = 1 - 2i$).

Lemma 6.7. *Ist $N(x)$ prim in $\mathbb{Z}$, so ist x Primelement in $\mathbb{Z}[i]$.*

Damit können wir für Elemente in $\mathbb{Z}[i]$ eine Primfaktorzerlegung durchführen.

Bemerkung 6.8. Die Primfaktorzerlegung in $\mathbb{Z}[i]$ ist eindeutig (bis auf assoziierte Zahlen).

Dabei heißt "eindeutig", dass die Faktoren eindeutig sind, bis auf zu ihnen assoziierte Zahlen. ($5 = (2+i)(2-i) = (1-2i)(1+2i)$, aber $2+i$ ist assoziiert zu $1-2i$ usw.)

[27.5.:]

(Erweiterter) Euklidischer Algorithmus in $\mathbb{Z}[i]$

Genau wie oben (s. S. 9), nur in Schritt 1:

Finde q_n so dass $a_{n+1} = a_{n-1} - q_n a_n$, wobei $N(a_{n+1}) < N(a_n) < N(a_{n-1})$, und zwar so:

Berechne a_{n-1}/a_n und runde das auf ganze Zahlen. Sonst alles wie gehabt. (Beim runden kann man Pech haben, z.B. $1/2+i$ kann man auf i runden, oder auf $1+i$. Dann: ausprobieren, was klappt.)

Wie sehen Primelemente in $\mathbb{Z}[i]$ aus? Dazu

Lemma 6.9. *Seien $a,b \in \mathbb{Z}$. Dann gilt $a^2+b^2 \equiv 0 \mod 4$, oder $a^2+b^2 \equiv 1 \mod 4$, oder $a^2+b^2 \equiv 2 \mod 4$.*

Satz 6.10. *Die Primelemente in $\mathbb{Z}[i]$ sind*

(a) $1+i$.

(b) Primzahlen in $\mathbb{Z}$ der Form $p \equiv 3 \mod 4$.

(c) Die Zahlen $a+bi$ und $a-bi$, falls a^2+b^2 Primzahl in $\mathbb{Z}$ ist.

Nun kann damit ein zahlentheoretisches Resultat bewiesen werden.

Satz 6.11. *Eine Primzahl ungleich 2 ist Summe zweier Quadratzahlen genau dann, wenn $p \equiv 1 \mod 4$.*

7 Die Polynomringe $\mathbb{Z}[x]$ und $\mathbb{Q}[x]$

Notation: $\mathbb{Z}[a]$ ist der kleinste Ring, der a und $\mathbb{Z}$ enthält. Bsp: $\mathbb{Z}[i]$, siehe letztes Kapitel. Analog für $\mathbb{Q}[a]$. Ist x eine Element ohne bestimmte Eigenschaften (also weder $x+x+\cdots+x \in \mathbb{Z}$, noch $x^n \in \mathbb{Z}$) so führt das zu:

Definition 7.1. Die *Polynomringe* $\mathbb{Z}[x]$ und $\mathbb{Q}[x]$ sind definiert durch:

$$\mathbb{Z}[x] := \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \,|\, n \in \mathbb{N}_0,\ a_k \in \mathbb{Z}\ (0 \le k \le n)\}$$

$$\mathbb{Q}[x] := \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \,|\, n \in \mathbb{N}_0,\ a_k \in \mathbb{Q}\ (0 \le k \le n)\}$$

Die Elemente davon heißen *Polynome*.

Statt immer $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ zu schreiben, schreiben wir auch kurz a.

Rechenregeln:

$$a+b: \quad \left(\sum_{k=0}^{n} a_k x^k\right) + \left(\sum_{k=0}^{n} b_k x^k\right) = \sum_{k=0}^{n} (a_k + b_k) x^k$$

$$a \cdot b: \quad \left(\sum_{k=0}^{n} a_k x^k\right) \cdot \left(\sum_{j=0}^{m} b_j x^j\right) = \sum_{k=0}^{m+n} \left(\sum_{k+j=k} a_k b_j\right) x^k.$$

Satz 7.2. *$(\mathbb{Z}[x],+,\cdot)$ und $(\mathbb{Q}[x],+,\cdot)$ sind kommutative, unitäre Ringe.*

Definition 7.3. Der *Grad* eines Polynoms a ist die höchste auftretende Potenz von x in a.

Definition 7.4. Ein Polynom $a \in \mathbb{Z}[x]$ heißt *Teiler* (in $\mathbb{Z}[x]$ [bzw in $\mathbb{Q}[x]$]) von $b \in \mathbb{Z}[x]$, falls es $c \in \mathbb{Z}[x]$ [bzw $c \in \mathbb{Q}[x]$] gibt, so dass $a \cdot c = b$.

Ob a Teiler von b ist, ermittelt man durch Polynomdivision (s. [WIK]). Falls die ohne Rest aufgeht, ist a Teiler von b.

Satz 7.5. *Seien $a, b, \in \mathbb{Q}[x]$, Grad(a)≥Grad(b). Dann existiert genau ein Paar $r, q \in \mathbb{Q}[x]$, so dass gilt: $a = qb + r$ und Grad(r)¡Grad(b).*

Damit:

(Erweiterter) Euklidischer Algorithmus in $\mathbb{Z}[x]$

Alles wie gehabt (s. S. 9), außer: "Größe" heißt hier: Sortieren bzgl Grad; und q_n wird bestimmt aus a_{n-1} und a_n durch Polynomdivision: a_{n-1}/a_n.

[8.6.:]

Bemerkung 7.6. Beim Bestimmen des ggT g wie oben erhält man den ggT in $\mathbb{Q}[x]$ von a und b. Falls $a, b \in \mathbb{Z}[x]$, und man möchte wissen ob g auch Teiler in $\mathbb{Z}[x]$ ist, muss getestet werden, ob (a) $g \in \mathbb{Z}[x]$, und (b) ob g auch Teiler in $\mathbb{Z}[x]$ von a und von b (zwei weitere Polynomdivisionen).
Evtl wird aus g ein Teiler in $\mathbb{Z}[x]$ erst, nachdem man g durch den ggT (in $\mathbb{Z}$) seiner Koeffizienten geteilt hat.

Bemerkung 7.7. Ist p Teiler von q in $\mathbb{Z}[x]$, $p = p_m x^m + \cdots + p_1 x + p_0$, $q = q_n x^n + \cdots + q_1 x + q_0$, $n > m \geq 1$, so gilt: $p_m | q_n$ und $p_0 | q_0$.

Damit kann man manchmal Faktoren von Polynomen raten. Soviel zu Teil I. Zum Abschluss eine kurze Zusammenfassung der algebraischen Objekte, die wir bisher kennengelernt haben:

Gruppen	Ringe	(← ist Körper?)
$(\mathbb{R}, +)$	$(\mathbb{R}, +, \cdot)$	ja
$(\mathbb{Q}, +)$	$(\mathbb{Q}, +, \cdot)$	ja
$(\mathbb{Z}, +)$	$(\mathbb{Z}, +, \cdot)$	nein
$(\mathcal{C}_n, + \mod n)$	$(\mathcal{C}_n, + \mod n, \cdot \mod n)$	nur für n prim
$(\mathcal{D}_n, \circ)$	$(\mathbb{Z}[i], +, \cdot)$	nein
$(\mathcal{S}_n, \circ)$	$(\mathbb{Z}[x], +, \cdot)$	nein
$(\mathcal{A}_n, \circ)$	$(\mathbb{Q}[x], +, \cdot)$	nein

Die in den ersten vier Zeilen der Tabelle entsprechen einander offenbar, die Ringe sind Erweiterungen der jeweiligen Gruppen. In den Zeilen 5 bis 7 gibt es keine solche Entsprechung, die sind nur aus Platzgründen nebeneinander aufgeführt.

Part II

Symmetriegruppen

8 Präsentationen von Gruppen

[10.6.:]

Wir möchten Gruppen nun beschreiben durch einige Elemente ("Erzeuger") und Beziehungen zwischen denen ("Relationen").

Definition 8.1. Ein *Alphabet A* ist eine Menge von Buchstaben, z.B. $\{a,b,c,\dots\}$. Ein *Wort* (über A) ist eine endliche Sequenz der Buchstaben in A mit Exponenten in $\mathbb{Z}$.

Exponenten in $\mathbb{Z}$, weil mit a auch sein Inverses a^{-1} in der Gruppe liegt, sowie deren Potenzen (z.B. $a^5 = aaaaa$ oder $a^{-3} = a^{-1}a^{-1}a^{-1}$. Dabei ist $a^0 = e$ das neutrale Element.

Definition 8.2. **(a)** Ein Wort heißt *reduziert*, falls es keine Paare $aa^{-1}, a^{-1}a, bb^{-1}$ usw enthält.
(b) Zwei Worte stellen dasselbe Gruppenelement dar, falls sie sich durch Ausnutzen der Relationen (und den daraus folgenden Gleichungen) ineinander überführen lassen.

Bsp: $\mathcal{D}_3 = \langle a,b \,|\, a^3 = b^2 = (ab)^2 = e\rangle$, und darin ist z.B. $aba = b$, denn: $(ab)^2 = abab = e \Leftrightarrow ababb = eb = b \Leftrightarrow aba = b$.

Definition 8.3. Eine Darstellung $\langle A\,|\,R\rangle$ einer Gruppe durch ein Alphabet A (*Erzeuger*) und einer Menge R von Gleichungen aus Worten über diesem Alphabet (*Relationen*) heißt *Präsentation* einer Gruppe.

Bemerkung 8.4. Eine Gruppe kann viele verschiedene Präsentationen haben.

[15.6.:]

Definition 8.5. Sei $A = \{a,b,\dots\}$ (n Buchstaben) so heißt $F_n = \langle A\,|\,\ \rangle$ (keine Relationen) die *freie Gruppe* vom Rang n.

Notation: Ein beliebiges Wort bezeichnen wir mit w, seine Buchstaben mit $w_1, w_2, \dots, w_m$. Also $w = w_1 w_2 \cdots w_m$.

Lemma 8.6. *Ist $w = w_1 w_2 \cdots w_n$ ein Wort, so ist sein Inverses $w^{-1} = w_n^{-1} w_{n-1}^{-1} \cdots w_2^{-1} w_1^{-1}$*

Definition 8.7. Ein *gerichteter Graph C* ist ein Paar (V,E), wobei $V = \{1,2,\dots\}$ die *Knotenmenge* von C und $E = \{(j,k)\,|\,j,k \in V\}$ die *Kantenmenge*.
Ein *ungerichteter Graph C* ist ein Paar (V,E), wobei $V = \{1,2,\dots\}$ und $E = \{j,k\,|\,j,k \in V\}$.

Zur Anschauung von Graphen und mehr siehe [WIK].

Definition 8.8. Der *Cayleygraph* $C(G)$ einer Gruppe $G = \langle A\,|\,R\rangle$ ist gegeben durch die Knotenmenge V, die die Elemente von G enthält, sowie die Kantenmenge

$$E = \{(g,h)\,|\,\exists x \in A :\ gx = h\}$$

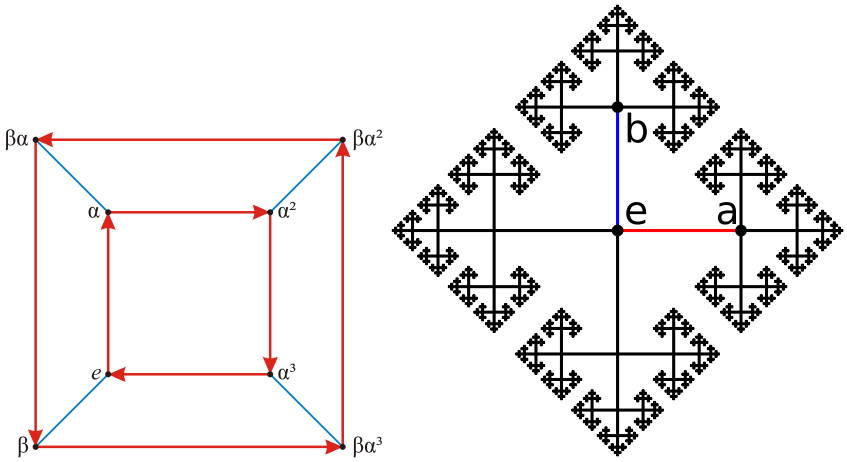

Figure 1: Cayleygraphen von $\mathcal{D}_4$ (links, endlicher Graph) und von F_2 (rechts, unendlicher Graph).

Die gerichteten Kanten markieren wir mit Pfeilen, von g nach h. Falls wir eine Doppelkante sehen ($g \to h$ und $h \to g$) so ersetzen wir sie durch eine ungerichtete Kante (ohne Pfeil).

Bsp: Siehe Fig. 1, Seite 14.

Definition 8.9. Die *freie abelsche Gruppe* (vom Rang n) ist

$$K_n := \langle a_1, a_2 \ldots, a_n \,|\, a_k a_m = a_m a_k \,(1 \le k < m \le n) \rangle.$$

Bemerkung 8.10. $\mathcal{D}_n = \langle a, b \,|\, a^n = b^2 = (ab)^2 = e \rangle$

[17.6.:]

9 Isometrien und Symmetrien

Definition 9.1. Eine *Isometrie* ist eine bijektive längenerhaltende Abbildung von $\mathbb{R}^2 \to \mathbb{R}^2$ (bzw von $\mathbb{R}^d \to \mathbb{R}^d$).
Die Menge aller Isometrien von $\mathbb{R}^2$ (bzw $\mathbb{R}^d$) ist eine Gruppe, die *euklidische Gruppe* $E(2)$ (bzw $E(d)$), mit Hintereinanderausführung als Verknüpfung.

Dabei ist $\mathbb{R}^d$ einfach der d-dimensionale Raum, mit dem üblichen Abstands- bzw Längenbegriff. "Längenerhaltend" heißt genau das, was man sich darunter vorstellt: f ist längenerhaltend, falls für alle $x, y \in \mathbb{R}^2$ gilt: Abstand(x,y) = Abstand $(f(x), f(y))$.

Definition 9.2. Ist f Isometrie, so heißt jeder Punkt P mit $f(P) = P$ *Fixpunkt* von f.

Drehungen, Spiegelungen und Verschiebungen ("Translationen") sind Isometrien. Wir sehen gleich, dass das fast alle sind: Außerdem gibt's noch Gleitspiegelungen.

Die Identität ist natürlich auch eine Isometrie, sie kann als Verschiebung (um 0), oder Drehung (um 0, oder um 360 Grad) interpretiert werden.

Offenbar gibt es zwei Sorten: entweder eine Isometrie bildet Rechtshänder auf Rechtshänder ab, oder auf Linkshänder. Die erste Sorte heißt *orientierungserhaltend* (o.-e.), die zweite *orientierungsumkehrend* (o.-u.).

Satz 9.3. *Eine Isometrie der Ebene $\mathbb{R}^2$ mit Fixpunkt ist eine Drehung, falls sie o.-e. ist, ansonsten eine Spiegelung.*
Eine Isometrie der Ebene ohne Fixpunkt ist eine Translation, falls sie o.-e. ist, ansonsten eine Gleitspiegelung.

Drei Punkte in der ebene heißen *kollinear*, falls sie auf einer Geraden liegen.

Satz 9.4. *Jede Isometrie der Ebene mit drei nicht-kollinearen Fixpunkten ist die Identität.*

Korollar 9.5. *Eine Isometrie der Ebene ist eindeutig bestimmt durch das Bild dreier nicht-kollinearer Punkte.*

Satz 9.6. *Das Produkt zweier Spiegelungen entlang paralleler Spiegelachsen ist eine Translation senkrecht zu diesen Spegelachsen, um das doppelte des Abstands der Spegelachsen.*
Das Produkt zweier Spiegelungen an zwei nicht-parallelen Spiegelachsen ist eine Drehung um den Schnittpunkt dieser Achsen, um das doppelte des Winkels zwischen diesen.

Bemerkung 9.7. Also lässt sich jede Isometrie in $E(2)$ als Kombination von maximal drei Spiegelungen darstellen:

(a) Spiegelungen: 1 Spieg.
(b) Drehung: 2 Spieg.
(c) Translation: 2 Spieg.
(d) Gleitspiegelung: 3 Spieg.

Definition 9.8. Sei M ein Muster in der Ebene $\mathbb{R}^2$. Ist f eine Isometrie mit $f(M) = M$, so heißt f *Symmetrie* von M. Die Menge aller Symmetrien von M ist die *Symmetriegruppe* von M, kurz: $\mathrm{Sym}(M)$.

Sei $G_{4,4}$ die Symmetriegruppe von "unendlichem Karopapier", also von der Zerlegung der Ebene in gleichgroße Quadrate, so dass an jeder Ecke 4 Quadrate aneinanderliegen.

Allgemein: Sei $G_{p,q}$ die Symmetriegruppe der Zerlegung der Ebene in reguläre p-Ecke, so dass an jeder Ecke q Stück aneinanderliegen.

Wir haben geometrisch hergeleitet, unter Benutzung von Korollar 9.6:

$$G_{4,4} = \langle a,b,c \,|\, a^2 = b^2 = c^2 = (ab)^4 = (ac)^2 = (bc)^4 = e \rangle, \quad \text{und (in den Übungen)}$$

$$G_{6,3} = G_{3,6} = \langle a,b,c \,|\, a^2 = b^2 = c^2 = (ab)^6 = (ac)^2 = (bc)^3 = e \rangle.$$

[22.6.:]

Definition 9.9. Eine *Spiegelungsgruppe* ist eine Symmetriegruppe eines Musters in $\mathbb{R}^d$, die von Spiegelungen erzeugt wird.
Eine *Coxetergruppe* ist eine Gruppe mit Präsentation

$$\langle s_1, \ldots, s_n \,|\, (s_j s_k)^{m_{jk}} = e \rangle,$$

mit $m_{jj} = 1$, $m_{jk} = m_{kj}$ und $m_{jk} \geq 2$ für $j \neq k$.

Klar ist: Jede Spiegelungsgruppe ist eine Coxetergruppe. Beispiele für Spiegelungsgruppen (und somit Coxetergruppen) sind $G_{4,4}$, $G_{6,3}$ sowie die Diedergruppen $\mathcal{D}_n$.

Ziel: Alle Symmetriegruppen (und somit erst recht alle Spiegelungsgruppen) ebener Muster zu bestimmen. Dazu:

[24.6.:]

10 Orbifold-Notation

Ein sehr gutes System zur Notation von Symmetriegruppen: Die Orbifold-Notation. Zu einem gegebenen Muster M geht man so vor wie im folgenden beschrieben.

1. Drehzentren P finden.
   (a) Falls durch P eine Spiegelachse läuft: P rot markieren, und eine rote Zahl n dranschreiben, wenn n ein n-zähliges Drehzentrum ist. Falls P auf keiner schon berücksichtigten Spiegelachse liegt (insbesondere, wenn P das erste rote Symbol bekommt) ein rotes $*$ dranschreiben.
   (b) Sonst (P liegt auf keiner Spiegelachse): P blau markieren, und eine blaue Zahl n dranschreiben, wenn n ein n-zähliges Drehzentrum ist.
2. Danach: Gibt es Spiegelachsen, die kein Drehzentrum enthalten? Diese (rot) einzeichnen. Falls diese Spiegelachse noch nicht berücksichtigt wurde (durch keinen bereits markierten Punkt läuft): ein rotes $*$ dranschreiben.
3. Danach: Gibt es ein *Mirakel*? D.h., kann ich von einem Teil des Musters zu seinem Spiegelbild gelangen, ohne eine Spiegelachse zu kreuzen? Einen solchen Pfad in rot markieren, ein rotes $\times$ dranschreiben.
4. Falls nichts von den obigen: gibt es ein *Wunder*? D.h., es gibt zwei unabhängige Translationen (d.h., in verschiedene Richtungen), die M auf sich abbilden: Einen blauen $\circ$ hinschreiben.

Wichtig: Immer nur verschiedene Punkte markieren. Zwei Punkte sind verschieden, wenn sie nicht durch eine Symmetrie des Musters aufeinander abgebildet werden können.

Nachdem dies getan ist: Alle Symbole sammeln, d.h. alle Zahlen, alle $*$, $\times$ und $\circ$. Diese hintereinander schreiben, und zwar so: Blaue Symbole nach links. Alle Zahlen absteigend ordnen. Rote Symbole nach rechts, Sterne $*$ zuerst, dann Zahlen, dann $\times$e. Die so erhaltene Zeichenkette heißt *Signatur* des Musters.

In der Signatur brauchen wir die Farben nicht mehr: Alle $*$ und $\times$ sind rot, alle Zahlen rechts eines $*$s auch, Zahlen links des $*$s blau. Falls kein $*$ vorkommt, sind alle Zahlen blau.

Wir ordnen den Symbolen Kosten zu:

Blau:

Symbol	$\circ$	2	3	4	5	6	$\cdots$	N	$\cdots$	∞
Euro	2	$\frac{1}{2}$	$\frac{2}{3}$	$\frac{3}{4}$	$\frac{4}{5}$	$\frac{5}{6}$	$\cdots$	$\frac{N-1}{N}$	$\cdots$	1

Rot:

Symbol	$\times$	$*$	2	3	4	5	6	$\cdots$	N	$\cdots$	∞
Euro	1	1	$\frac{1}{4}$	$\frac{1}{3}$	$\frac{3}{8}$	$\frac{4}{10}$	$\frac{5}{12}$	$\cdots$	$\frac{N-1}{2N}$	$\cdots$	$\frac{1}{2}$

Satz 10.1. *(Magisches Theorem für 2-periodische ebene Muster).*
Die möglichen Signaturen eines 2-periodischen ebenen Musters sind genau die, die insgesamt 2 Euro kosten und kein ∞ enthalten.

Bsp: $*632$ kostet $1+5/12+1/3+1/4=2$ Euro. Damit können wir herleiten:

Bemerkung 10.2. Es gibt genau 17 Symmetriegruppen 2-periodischer ebener Muster. Das sind genau die mit folgenden Signaturen:

$$*632,\ *442,\ *333,\ *2222,\ **,\ *\times,\ \times\times,\quad 632,\ 442,\ 333,\ 2222,\ \circ,\quad 4*2,\ 3*3,\ 2*22,\ 22*,22\times.$$

Dass dies alle möglichen Signaturen sind, leitet man aus Satz 10.1 und der Tabelle darüber ab: es gibt genau 17 Signaturen, die exakt 2 Euro kosten. Dass die auch alle auftreten, dazu sahen wir 17 Beispiele in der Vorlesung und in den Übungen.

[29.6.:]

11 Symmetriegruppen sphärischer Muster

Betrachten wir nun Muster auf einer Kugel, z.B. auf einem Fußball. Diesen können wir genau wie ebenen Mustern ihre Signatur zuordnen, nach demselben Rezept wie im letzten Kapitel.

Satz 11.1. *(Magisches Theorem für sphärische Muster).*
Die möglichen Signaturen eines sphärischen Musters sind genau die, die insgesamt $2-\frac{2}{g}$ Euro kosten und kein ∞ enthalten. Dabei ist g die Zahl der Symmetrien des Musters. (Also $g=|\mathrm{Sym}(M)|$)

Damit können wir herleiten:

Satz 11.2. *Die Symmetriegruppen sphärischer Muster sind die mit den Signaturen*

$$332,\ 432,\ 532,\ 22N, NN,\quad *332,\ *432,\ *532,\ *22N,\ *NN,\quad 3*2,\ 2*N,\ N*,\ N\times,$$

wobei $N\in\mathbb{N}$, $N\geq 2$.

Dass dies alle möglichen Signaturen sind, leitet man zunächst aus der Kostentabelle oben her. Damit erhalten wir allerdings zusätzlich die Möglichkeiten MN und $*MN$. Für $M\neq N$ gibt es aber kein sphärisches Muster mit dieser Signatur.

Dass die anderen Signaturen alle vorkommen, davon überzeugt man sich wieder mittels konkreten Beispielen für jede einzelne Möglichkeit (s. Vorlesung und Übungsblatt 12).

[1.7.:]

Friesgruppen

Sei M ein Muster in der Ebene $\mathbb{R}^2$, das nur eine unabhängige Translation enthält. Solche Muster heißen *Friesmuster*, deren Symmetriegruppen *Friesgruppen*.

Bsp.

$$\cdots \mathsf{pdpdpdpdpdpdpdpdpdp} \cdots$$

$$\cdots \mathsf{xxxxxxxxxxxxxxxxxxxxx} \cdots$$

$\cdots$EEEEEEEEEEEEEEEEEEEE$\cdots$

Solche Muster können wir um den Äquator einer Kugel wickeln, so dass sich die Bausteine nur endlich oft, sagen wir, N mal, wiederholen. N können wir dazu beliebig groß wählen. So erhalten wir ein sphärisches Muster, dessen Signatur (mindestens) ein N enthält. Davon gibt es genau sieben (s.o.). Also gibt es maximal sieben Friesgruppen.

Satz 11.3. *Es gibt genau sieben verschiedene Signaturen für Friesgruppen:*

$$22\infty,\ \infty\infty,\ \infty\times,\ \infty *,\ 2*\infty,\ *22\infty \text{ und } *\infty\infty$$

Nach den obigen Überlegungen brauchen wir zum Beweis des Satzes nur noch zu zeigen, dass alle sieben Möglichkeiten auch wirklich vorkommen (s. Übungsblatt 13). Damit erhalten wir auch:

Satz 11.4. *(Magisches Theorem für Friesmuster).*
Die möglichen Signaturen eines Friesmusters sind genau die, die insgesamt 2 Euro kosten und mindestens ein ∞ enthalten.

Nun gibt es noch ebene Muster, die *keine* Translation als Symmetrie haben. Dazu brauchen wir zunächst:

Satz 11.5. *Sei M ein Muster in $\mathbb{R}^2$, $\mathrm{Sym}(M)$ enthalte keine Translation. Dann gilt entweder*
(a) *Alle $f \in \mathrm{Sym}(M)$ haben einen gemeinsamen Fixpunkt. D.h., es gibt einen Punkt P, so dass für alle $f \in \mathrm{Sym}(M)$ gilt: $f(P) = P$. Oder*
(b) *$\mathrm{Sym}(M)$ enthält unendlich viele Drehungen, und die Menge derer Drehzentren ist unendlich ausgedehnt.*

Zum Beweis dieses Satzes brauchen wir wiederum:

Lemma 11.6. *Seien f, g, h drei Spiegelungen.*
(a) *Haben f, g, h einen gemeinsamen Fixpunkt (d.h., es gibt P mit $f(P) = P = g(P) = h(P)$), dann ist fgh eine Spiegelung an einer Geraden durch P.*
(b) *Sonst ist fgh Gleitspiegelung.*

Damit folgen fast direkt zwei Resultate:

Korollar 11.7. *Jede Symmetriegruppe eines endlichen Musters in $\mathbb{R}^2$ hat einen gemeinsamen Fixpunkt.*

Satz 11.8. *Ist die Symmetriegruppe eines endlichen Musters in $\mathbb{R}^2$ endlich, so ist es eine zyklische Gruppe $\mathcal{C}_n$ oder eine Diedergruppe $\mathcal{D}_n$.*

Insbesondere können die folgenden Fälle eintreten: Keine Symmetrie (außer der Identität): $\mathcal{C}_1 = \{e\}$; nur eine Spiegelung als Symmetrie (außer der Identität): $\mathcal{D}_1$.

Die Forderung nach einer endlichen Symmetriegruppe ist notwendig, denn betrachte etwa einen (perfekten) Kreisring als Muster. Der hat unendlich viele Symmetrien, nämlich etwa jede Spiegelung an Geraden durch den Kreismittelpunkt. Dessen Symmetriegruppe ist nicht "endlich erzeugt", d.h., sie hat keine Darstellung als Präsentation mit endlich vielen Erzeugern.

[6.7.:]

12 Von Signaturen zu Präsentationen

Wir können nun ebenen und sphärischen Mustern (falls sie nicht zu exotisch sind) ihre Signatur zuordnen. Das legt die Symmetriegruppe fest. Wie aber können wir diese "klassisch" hinschreiben? Viele Mathematiker kennen die Orbifold-Notation gar nicht! Aber praktisch jeder Mathematiker kennt Präsentationen von Gruppen. Die erhält man so:

1. Für jede blaue Zahl A notieren wir einen Erzeuger mit einem griechischen Buchstaben: α ($\beta, \gamma, \ldots$), und eine Relation: $\alpha^A = e$.

2. Für jede Gruppe roter Symbole der Form $*AB\cdots N$ mit n Zahlen notieren wir: $n+1$ Erzeuger mit lateinischen Buchstaben: $P, Q, R, \ldots, W$, sowie einen weiteren Erzeuger mit einem griechischen Buchstaben: λ, sowie Relationen

   $$P^2 = (PQ)^A = Q^2 = (QR)^B = R^2 = \cdots = (VW)^N = W^2 = e; \quad \lambda^{-1} P \lambda = W$$

   (Falls nur ein $*$ ohne rote Zahl: zwei Erzeuger λ, P; Relationen $P^2 = e$; $\lambda^{-1} P \lambda = P$).

3. Für ein (blaues) $\circ$ ("Wunder") zwei Erzeuger S, T, sowie eine Relation $STS^{-1}T^{-1} = e$.

4. Für ein (rotes) $\times$: Zwei Erzeuger Z, δ, sowie eine Relation $Z^2 = \delta$.

5. Zum Schluss eine weitere Relation ("globale Relation"): Produkt aller vorkommenden griechischen Buchstaben $\alpha\beta\gamma\cdots\lambda\cdots\delta = e$.

Es ist praktisch, die Erzeuger an die Signatur zu schreiben, nach folgendem Schema:

Bsp. Signatur $*632$ liefert: ${}^{\lambda}*^{P}6^{Q}3^{R}2^{S}$. Daran liest man ab:

$$P^2 = (PQ)^6 = Q^2 = (QR)^3 = R^2 = (RS)^2 = S^2 = e; \quad \lambda^{-1} P \lambda = S; \quad \lambda = e$$

Wegen $\lambda = e$ ist $P = S$, also können wir die Präsentation vereinfachen zu:

$$G_{6,3} = \langle P, Q, R \,|\, P^2 = Q^2 = R^2 = (PQ)^6 = (QR)^3 = (RP)^2 = e \rangle.$$

Bsp. Signatur $3*3$: liefert: ${}^{\alpha}3^{\lambda}*^{P}3^{Q}$. Daran lesen wir ab:

$$\alpha^3 = e = P^2 = (PQ)^3 = Q^2; \quad \lambda^{-1} P \lambda = Q; \quad \alpha\lambda = e.$$

Also ist $\lambda = \alpha^{-1}$, somit $Q = \alpha P \alpha^{-1}$. Wir können daher die Erzeuger λ und Q durch α und P darstellen, das spart uns zwei Erzeuger. Wir erhalten die Präsentation

$$\langle \alpha, P \,|\, \alpha^3 = e = P^2 = (P\alpha P \alpha^{-1})^3 \rangle.$$

(Die Relation $Q^2 = e$ scheint weggefallen zu sein. Die dürfen wir weglassen, weil sie aus den anderen folgt: Es ist ja $Q^2 = (\alpha P \alpha^{-1})^2 = \alpha P \alpha^{-1} \alpha P \alpha^{-1} = \alpha P P \alpha^{-1} = \alpha P^2 \alpha^{-1} = \alpha\alpha^{-1} = e$.)

[8.7.:]

13 Eulerscher Polyedersatz

Definition 13.1. Ein ungerichteter Graph G (vgl. Def 8.7) heißt *zusammenhängend*, falls für alle Paare von Knoten x, y in G ein Kantenzug von x nach y führt.
G heißt planar, falls er so gezeichnet werden kann, dass die Kanten sich nicht kreuzen.

Satz 13.2. *Sei G ein zusammenhängender planarer Graph mit v Knoten, e Kanten und f Flächen. Dann gilt: $v - e + f = 2$.*

[13.7.:]

Damit konnten wir die Sätze 10.1 und 11.1 beweisen (langer Beweis, siehe Vorlesungsmitschrift oder [CBG]).

[15.7.:]

14 Reguläre Polytope (Platonische Körper)

Definition 14.1. Ein *Polygon* ist ein geschlossener Kantenzug in der Ebene. Ein Polygon P heißt *konvex*, falls (a) seine Kanten sich nicht schneiden und (b) für je zwei Punkte x, y des Polygons (im Innern oder auf dem Rand) die Strecke $\overline{xy}$ ganz in P liegt.
Ein Polygon heißt *regulär*, falls es konvex ist, alle seine Kanten gleich lang sind und alle Innenwinkel gleich groß.

Reguläre Polygone sind genau diese: n-Ecke mit gleichlangen Kanten und Innenwinkel $\frac{n-2}{n}180^\circ$, wobei $n \geq 3$. Insbesondere gibt es unendlich viele verschiedene reguläre Polygone.

Definition 14.2. Ein *Polytop* ist ein endlicher Teil des Raumes $\mathbb{R}^3$, dessen Rand aus endlich vielen Polygonen besteht.
Ein Polytop P heißt *regulär*, falls (a) P konvex ist, (b) seine Flächen alles gleiche (kongruuente) reguläre Polygone sind, und (c) an jeder Ecke gleichviele Flächen zusammenstoßen.

Satz 14.3. *Es gibt genau fünf verschiedene reguläre Polytope: Tetraeder, Würfel, Oktaeder, Dodekaeder und Ikosaeder.*

Eigentlich müsste es heißen “reguläres Tetraeder” usw., denn es gibt auch “schiefe” (nichtreguläre) Tetraeder. Das “regulär” lassen wir aber im folgenden weg.

Für Polytope gilt auch (oder gerade) der Eulersche Polyedersatz: Falls v die Zahl der Ecken ist, e die der Kanten und f die der Fächen, gilt für konvexe Polytope immer $v - e + f = 2$.

Ein anderer Name für reguläre Polytope ist “Platonische Körper”. Mehr zu denen unter “Platonische Körper” in [WIK].

Definition 14.4. Sei P ein konvexes Polytop. Das *duale* Polytop zu P ist das, das die Flächenmittelpunkte von P als Ecken hat.

Man überzeugt sich, dass das duale Polytop des Tetraeders wieder das Tetraeder ist, das des Würfels das Oktaeder, und das des Dodekaeders das Ikosaeder. (Und umgekehrt: Das duale des dualen ist eine verkleinerte Kopie des ursprünglichen Polytops.)

Die Symmetriegruppe des Tetraeders ist $*332$, die des Würfels und des Oktaeders ist $*432$ und die des Dodekaeders und des Ikosaeders ist $*532$.

Definition 14.5. Ein Polytop P heißt *eckentransitiv* (oder vertex-transitiv), falls zu je zwei Ecken x, y von P immer ein $f \in \mathrm{Sym}(P)$ existiert, so dass $f(x) = y$.
Analog definiert man *kantentransitiv* und *flächentransitiv*.

Reguläre Polytope sind alles: ecken-, kanten- und flächentransitiv.

[20.7.:]

Wenn wir weniger von dem Polytop verlangen bekommen wir:

15 Archimedische und Catalanische Körper

Definition 15.1. Ein ecken-transitives Polytop heißt *semiregulär*. Ist es außerdem kantentransitiv, heißt es *quasiregulär*.

Insbesondere gilt, dass alle Ecken eines semiregulären Polytops gleich aussehen. D.h., es treffen sich dort immer die gleiche Konstellation von Flächen. Daher benutzen wir folgende Notation: Ist die Ecke im Uhrzeigersinn umgeben von einem n-Eck, einem m-Eck, einem ℓ-Eck..., dann notieren wir das Polytop als $(n.m.\ell\ldots)$.

Es gibt zwei unendliche Serien von semiregulären Polytopen: Prismen und Antiprismen. Daneben sind die fünf regulären Polytope auch semiregulär. Außer diesen gibt es exakt 13 weitere semireguläre Polytope. Diese heißen *archimedische Körper*.

(Bilder unter [WIK], “semiregular polytopes”).

Die Symmetriegruppen der semiregulären Polytope sind: $*22N$ (Prismen), $2*N$ (Antiprismen), sowie die der regulären Polytope: $*332$, $*432$ und $*532$. Mit zwei Ausnahmen: Das $(3.3.3.3.4)$ hat Symmetriegruppe 432, das $(3.3.3.3.5)$ hat 532.

Unter den archimedischen Körpern gibt es zwei, die auch kantentransitiv sind: $(3.4.3.4)$ und $(3.5.3.5)$.

Die flächentransitiven Polytope gehen aus den semiregulären durch Bildung des dualen Polytops hervor. Die dualen der archimedischen Körper heißen *catalanische* Körper (nach dem Mathematiker Catalan). Benannt werden sie nach ihren dualen Polytopen, den archimedischen Körpern, nur mit eckigen Klammern: Das duale zu $(3.4.3.4)$ (auch Kubooktaeder) ist $[3.4.3.4]$, das Rhombendodekaeder.

Ich kenne kein Buch, das genau den Inhalt dieser Vorlesung umfasst.

Den Teil I — Gruppen, Ringe und Körper — findet man in fast jedem Algebrabuch. Z.B. im Bibliothekskatalog suchen: “Einführung Algebra” liefert viele Treffer. Obacht: “Lineare” Algebra (Vektoren, Matrizen,...) behandeln wir hier nicht. Online verfügbar sind — vom Netz der Uni aus — [S-P] und [KRA].

Der Anfang von Teil II (Kap 8 und 9) findet sich z.B. in [R]. Der Rest von Teil II steht dagegen so nur in einer Quelle, nämlich [CBG].

References

[A] M. Artin: *Algebra*, Birkhäuser (versch. Auflagen)

[CCS] A.M. Cohen, H. Cuypers, H. Sterk: Algebra interactive, Springer (1999)

[CBG] J.H. Conway, H. Burgiel, C. Goodman-Strauss: *Symmetries of Things* Peters (2008)

[C] H.S.M. Coxeter: *Regular Polytopes*, Metheun & Co. Ltd., London (versch. Auflagen)

[H] J.E. Humphreys: *Reflection Groups and Coxeter Groups*, Cambridge University Press (1990)

[KRA] J. Kramer: *Zahlen für Einsteiger: Elemente der Algebra und Aufbau der Zahlbereiche* Vieweg (2008)

[R] S. Rosebrock: *Geometrische Gruppentheorie* Vieweg (2004)

[S-P] R. Schulze-Pillot: *Einführung in Algebra und Zahlentheorie*, Springer (2008)

[VDW] B. van der Waerden: *Algebra*, Springer (versch. Auflagen)

[WIK] Online: `http://en.wikipedia.org`