1 Gruppentheorie

1.1 Halbgruppen, Monoide, Gruppen

Definition (Halbgruppe)**.** $(H, \cdot)$ mit einer inneren Verknüfung $\cdot : H \times H \to H$ heißt *Halbgruppe*, falls $\forall a, b, c \in H$ das Assoziativgesetz gilt:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

Definition (Neutrale Elemente)**.** $(H, \cdot)$ Halbgruppe, $e \in H$.

1. e heißt *linksneutral*, falls $\forall a \in H : e \cdot a = a$.
2. e heißt *rechtsneutral*, falls $\forall a \in H : a \cdot e = a$.
3. e heißt *neutral*, falls e links- und rechtsneutral ist.

Bemerkung. In jeder Halbgruppe kann es höchstens ein neutrales Element geben.

Definition (Monoid)**.** Eine Halbgruppe mit neutralem Element e heißt *Monoid*, $(H, \cdot, e)$.

Definition (Inverse)**.** $(M, \cdot, e)$ Monoid, $a, b \in M$.

1. b heißt *linksinvers* zu a, falls $b \cdot a = e$.
2. b heißt *rechtsinvers* zu a, falls $a \cdot b = e$.
3. b heißt *invers* zu a, falls b zu a links- und rechtsinvers ist.

Bemerkung. Zu jedem Element eines Monoids gibt es höchstens ein inverses Element.

Definition (Einheitengruppe)**.** $(M, \cdot, e)$ Monoid. Setze

$$\mathcal{E}(M) \equiv M^x := \{a \in M \mid a \text{ besitzt ein Inverses}\}.$$

Für $a \in M$ bezeichne das eindeutig bestimmte Element mit a^{-1}.

Definition (Gruppe)**.** Ein Monoid $(M, \cdot, e)$ heißt *Gruppe*, falls $\mathcal{E}(M) = M$, d.h. jedes Element invertierbar ist.

Satz 1.1. Sei $(M, \cdot, e)$ ein Monoid. Dann ist $\mathcal{E}(M), \cdot, e)$ eine Gruppe.

Korollar. $(M, \cdot, e)$ Monoid, $a, b \in \mathcal{E}(M)$.

- $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$
- $(a^{-1})^{-1} = a$

Bemerkung. G Gruppe, $a, b \in G$. Dann sind die Gleichungen

$$a \cdot x = b \qquad\qquad y \cdot a = b$$

eindeutig lösbar.

Bemerkung. Sei $(H, \cdot)$ eine Halbgruppe, in der es ein linksneutrales und zu jedem Element ein linksinverses Element gibt.
Dann ist H eine Gruppe.

Satz 1.2 (Komplexprodukte)**.** $(H, \cdot)$ Halbgruppe. Setze

$$\mathcal{C}(H) := \mathcal{P}(H) \setminus \{\emptyset\}$$

und für $A, B \in \mathcal{C}(H)$ (d.h. $A, B \subseteq H$, $A \neq \emptyset$, $B \neq \emptyset$) setze

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

Dann ist $(\mathcal{C}, \cdot)$ eine Halbgruppe.

Notationen. Schreibe

- $\{a\} \cdot B = a \cdot B$
- $B \cdot \{a\} = B \cdot a$

Definition. $(H, \cdot)$ Halbgruppe, $a \in H, m \in \mathbb{Z}$.

1. Falls $m > 0$: $a^m = \underbrace{a \cdot a \cdots a}_{m \text{ mal}}$.
2. Falls H ein Monoid: $a^0 = e$.
3. Falls H ein Monoid, $a \in \mathcal{E}(H), m < 0$, setze $a^m := (a^{-1})^{|m|}$.

Proposition. Es gilt

1. $a^{m+n} = a^m \cdot a^n$
2. $(a^m)^n = a^{m \cdot n}$
3. $(a \cdot b)^m = a^m \cdot b^m$, falls $a \cdot b = b \cdot a$

1.2 Untergruppen und Erzeugendensysteme

Definition (Untergruppe)**.** G Gruppe, $H \subseteq G$, sodass $H \cdot H \subseteq H$ (d.h. $\forall a, b \in H : a \cdot b \in H$, „$H$ ist abgeschlossen bzgl. Multiplikation“) und H eine Gruppe ist. Dann heißt H eine *Untergruppe* von G, $H \leq G$.

Proposition. $H \leq G \Rightarrow e_G = e_H$

Satz 1.3 (Charakterisierung von Untergruppen)**.** G Gruppe, $H \subseteq G$. Äquivalente Aussagen:

1. $H \leq G$
2. $H \neq \emptyset$ und $\forall a, b \in H : a \cdot b \in H$ und $\forall a \in H : a^{-1} \in H$
3. $H \neq \emptyset$ und $\forall a, b \in H : a \cdot b^{-1} \in H$

Beispiele. Untergruppen:

- $(k\mathbb{Z}, +) \leq (\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +) \leq (\text{Quaternionen}, +)$
- $(SL_n(K), \cdot) \leq (GL_n(K), \cdot)$, wobei

$$SL_n(K) := \{M \in GL_n(K) \mid \det M = 1\}$$

- $(\underbrace{SO_n(\mathbb{R}), \cdot)}_{\text{unitär}} \leq \underbrace{(O_n(\mathbb{R}), \cdot)}_{\text{Drehungen}}$

Definition (Erzeugte Untergruppe)**.** G Gruppe, $A \subseteq G$.

$$\langle A \rangle := \bigcap_{H \leq G, A \subseteq H} H$$

heißt die von A *erzeugte Untergruppe* von G.

Satz 1.4. G Gruppe, $A \subseteq G$.

$\langle A \rangle = \{a_1 \cdot a_2 \cdots a_n \mid n \in \mathbb{N}_0, a_j \in A \text{ oder } a_j^{-1} \in A\}$.

Notation. $a \in G$. Schreibe

$$\langle a \rangle := \langle \{a\} \rangle .$$

Definition (Erzeugendensystem)**.** G Gruppe, $H \leq G$ und $A \subseteq G$. A heißt *Erzeugendensystem* von H, falls

$$\langle A \rangle = H.$$

G heißt *endlich erzeugt*, falls es eine endliche Menge A mit $\langle A \rangle = G$ gibt.

1.3 Nebenklassen, Normalteiler und Faktorgruppen

Definition. G Gruppe, $H \leq G$.

- $a \, \lambda_H \, b \Leftrightarrow a^{-1}b \in H$
- $a \, \rho_H \, b \Leftrightarrow ab^{-1} \in H$

Satz 1.5. Es gilt:

1. λ_H ist Äquivalenzrelation auf G. Äquivalenzklasse von a ist aH („Linksnebenklasse“), d.h.

$$a \, \lambda_H \, b \Leftrightarrow b \in aH \Leftrightarrow bH = aH.$$

2. ρ_H ist Äquivalenzrelation auf G. Äquivalenzklasse von a ist Ha („Rechtsnebenklasse“), d.h.

$$a \, \rho_H \, b \Leftrightarrow b \in Ha \Leftrightarrow Hb = Ha.$$

Satz 1.6 (Mächtigkeit von Nebenklassen)**.** G Gruppe, $H \leq G$.

1. Für jedes $a \in G$ gilt

$$|aH| = |H| = |Ha| ,$$

insbesondere haben alle Nebenklassen bzgl. H dieselbe Kardinalität.

2.

$$|G/\lambda_H| = |G/\rho_H| ,$$

„Anzahl der Linksnebenklassen ist gleich der Anzahl der Rechtsnebenklassen.“

Definition (Ordnung)**.** $|G|$: Ordnung von G, $|a| := |\langle a \rangle|$: Ordnung von a.

Satz 1.7 (Ordnung von Elementen)**.** G Gruppe, $a \in G$. Dann gilt *genau eine* der folgenden Aussagen:

1. $|a| = |\mathbb{N}|$, also $\langle a \rangle$ ist abzählbar unendlich, die Abbildung $n \mapsto a^n$ von $\mathbb{Z}$ nach $\langle a \rangle$ ist bijektiv.
2. $|a|$ ist endlich, es gilt

$$|a| = \min\{n \in \mathbb{N} \mid a^n = e\}$$

und

$$a^n = a^m \Leftrightarrow n - m \text{ ist Vielfaches von } |a| .$$

Definition. Gruppe G heißt *zyklisch*, wenn es ein $a \in G$ mit $G = \langle a \rangle$ gibt.

Definition (Index)**.** G Gruppe, $H \leq G$. Die Anzahl der Linksnebenklassen (= Anzahl der Rechtsnebenklassen) von G bzgl. H heißt der *Index* von H in G,

$$[G : H] := |G/\lambda_H| = |G/\rho_H| .$$

Satz 1.8 (Indexmultiplikationsformel)**.** G Gruppe, $H \leq G$, $K \leq H$ („tower of groups“). Dann gilt

$$[G : K] = [G : H] \cdot [H : K].$$

Korollar (Satz von Lagrange)*.* G Gruppe, $H \leq G$. Dann gilt

$$|G| = [G : H] \cdot |H| .$$

Korollar (Satz von Fermat)*.* G endliche Gruppe, $a \in G$. Dann gilt

$$a^{|G|} = e.$$

Korollar (Kleiner Satz von Fermat)*.* p Primzahl, $a \in \mathbb{Z}$ mit $p \nmid a$. Dann gilt

$$a^{p-1} \equiv 1 \mod p.$$

Definition. $(G, \cdot)$ Gruppe. Eine Äquivalenzrelation $\equiv$ mit

$$\forall a, b, c, d \in G : a \equiv b \vee c \equiv d \to a \cdot c \equiv b \cdot d$$

heißt *Kongruenzrelation* („mit der Gruppenstruktur verträgliche Äquivalenzrelationen“).

Definition (Normalteiler)**.** $H \leq G$ Gruppe. H heißt *Normalteiler* von G, $H \trianglelefteq G$, wenn

$$\forall a \in G : a^{-1}Ha \subseteq H.$$

Satz 1.9 (Charakterisierung von Normalteilern)**.** G Gruppe, $H \leq G$. Äquivalente Aussagen:

1. λ_H ist eine Kongruenzrelation.
2. ρ_H ist eine Kongruenzrelation.
3. $\lambda_H = \rho_H$
4. H ist ein Normalteiler von G.
5. $\forall a \in G : a^{-1}Ha = H$
6. $\forall a \in G : aH = Ha$
7. $\forall a \in G : aH \subseteq Ha$
8. $\{aH \mid a \in G\}$ ist eine Gruppe bzgl. Komplexprodukt.
9. Es gibt einen Gruppenhomomorphismus $f : G \to K$ mit $\operatorname{Ker} f = H$.

Korollar. G Gruppe, $N \trianglelefteq G$. Dann ist

$$G/N := G/\lambda_N = \{aN \mid a \in G\}$$

mit $aN \cdot bN = abN$, neutr. Element N und

$$(aN)^{-1} = a^{-1}N$$

eine Gruppe („Faktorgruppe“ G nach N).

Proposition. G Gruppe, $H \leq G$.

1. Falls $H = \{e\}$ oder $H = G$, so ist $H \trianglelefteq G$.
2. Falls $[G : H] = 2$, so ist $H \trianglelefteq G$.
3. Falls G kommutativ ist, so ist $H \trianglelefteq G$.

1.4 Homomorphismen, Isomorphiesätze

Definition (Gruppenhomomorphismen & Co.)**.** Seien G, H Gruppen, $f : G \to H$.

1. f heißt *Gruppenhomomorphismus*, falls
$$\forall a, b \in G : f(a \cdot b) = f(a) \cdot f(b).$$
2. Gruppenepimorphismus: surjektiv
3. Gruppenmonomorphismus: injektiv
4. Gruppenisomorphismus: bijektiv
5. Gruppenendomorphismus: $G = H$
6. Gruppenautomorphismus: bijektiver Endomorphismus
7. $\operatorname{Ker} f = f^{-1}(e_H) = \{a \in G \mid f(a) = e_H\}$
8. $\operatorname{Im} f = f(G) = \{f(a) \mid a \in G\}$
9. H heißt *homomorphes Bild* von G, falls es einen Gruppenepimorphismus $f : G \to H$ gibt.
10. Zwei Gruppen G und H heißen *isomorph*, falls es einen Gruppenisomorphismus $f : G \to H$ gibt.

Satz 1.10 (Eigenschaften von Gruppenhomomorphismen)**.** G, H Gruppen, $f : G \to H$ Homomorphismus.

1. $\forall K \leq G : f(K) \leq H$
2. $\forall K \trianglelefteq G : f(K) \trianglelefteq \operatorname{Im} f$
3. $\forall L \leq H : f^{-1}(L) \leq G$

4. $\forall L \trianglelefteq H : f^{-1}(L) \trianglelefteq G$
5. $\operatorname{Ker} f \trianglelefteq G$
6. $\operatorname{Im} f \leq H$
7. $f(e_G) = e_H$
8. $\forall a \in G : f(a^{-1}) = (f(a))^{-1}$
9. f Epimorphismus $\Leftrightarrow \operatorname{Im} f = H$
10. f Monomorphismus $\Leftrightarrow \operatorname{Ker} f = \{e_G\}$

Satz 1.11 (Kanonische Projektion und kanonische Einbettung)**.** G Gruppe.

1. Sei $H \leq G$. Dann ist

   $$\iota : H \to G; h \mapsto h$$

   ein Gruppenmonomorphismus („kanonische Einbettung“).

2. Sei $H \trianglelefteq G$. Dann ist

   $$\pi_H : G \to G/H; a \mapsto aH$$

   ein Gruppenepimorphismus („kanonische Projektion“) mit $\operatorname{Ker} \pi_H = H$.

Satz 1.12 (Homomorphiesatz, 1. Isomorphiesatz)**.** Seien G, H Gruppen, $f : G \to H$ ein Homomorphismus, $N \trianglelefteq G$ mit $N \subseteq \operatorname{Ker} f$. Dann gibt es genau einen Homomorphismus

$$\overline{f} : G/N \to H,$$

sodass

$$f = \overline{f} \circ \pi_N,$$

nämlich

$$\overline{f}(aN) = f(a).$$

Falls f ein Epimorphismus und $N = \operatorname{Ker} f$, so ist $\overline{f}$ ein Isomorphismus.

Beispiel.

$$f : (\mathbb{R}, +) \to (S^1 = \{z \in \mathbb{C} \mid |z| = 1\}, \cdot)$$

mit $f(\alpha) = e^{i\alpha}$ ist ein Homomorphismus. f ist surjektiv, $\operatorname{Ker} f = 2\pi\mathbb{Z}$. Dann folgt $\mathbb{R}/2\pi\mathbb{Z}$ (Winkel) ist isomorph zu S^1 (Einheitskreis).

Satz 1.13 (3. Isomorphiesatz, Transfersatz)**.** Seien G, H Gruppen, $f : G \to H$ ein Epimorphismus, $K := \operatorname{Ker} f$. Setze

$$\begin{aligned}
&\mathcal{U}(G) := \{L \leq G \mid K \subseteq L\} \\
&\mathcal{U}(H) = \{M \leq H\} \\
&\mathcal{N}(G) := \{N \trianglelefteq G \mid K \subseteq N\} \\
&\mathcal{N}(H) = \{P \trianglelefteq H\}.
\end{aligned}$$

Dann ist

$$\Phi : \mathcal{U}_K(G) \to \mathcal{U}(H)$$

mit

$$\Phi(L) = f(L) = \{f(x) \mid x \in L\}$$

eine Bijektion.

Die Einschränkung von Φ auf $\mathcal{N}_K(G)$ ist eine Bijektion auf $\mathcal{N}(H)$.

Satz 1.14 (3. Isomorphiesatz, Kürzungssatz)**.** Sei G eine Gruppe, $K \trianglelefteq G, N \trianglelefteq G$ mit $K \subseteq N \subseteq G$. Dann ist $K \trianglelefteq N$ und $N/K \trianglelefteq G/K$ und es gilt

$$(G/K)/(N/K) \text{ ist isomorph zu } G/N.$$

Satz 1.15. G, H, K Gruppen, $f : G \to H$ und $g : H \to K$ Homomorphismen.

1. $g \circ f : G \to K$ ist Gruppenhomomorphismus.
2. Falls f ein Isomorphismus, so ist auch f^{-1} ein Isomorphismus.
3. $(\operatorname{End}(G), \circ)$ ist ein Monoid.
4. $(\operatorname{Aut}(G), \circ)$ ist eine Gruppe.

1.5 „Berühmte“ Gruppen

1.5.1 Zyklische Gruppen

G heißt zyklisch, falls

$$\exists a \in G \text{ mit } G = \langle a \rangle,$$

wobei

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}.$$

Satz 1.16 (Charakterisierung zyklischer Gruppen)**.** G Gruppe. Äquivalente Aussagen:

1. G ist zyklisch.
2. G ist homomorphes Bild von $(\mathbb{Z}, +)$.

3. Es gibt ein $m \in \mathbb{N}_0$, sodass G isomorph zu $\mathbb{Z}/m\mathbb{Z}$ ist.

Satz 1.17 (Eigenschaften zyklischer Gruppen)**.** Es gilt:

1. Zyklische Gruppen sind abelsch.
2. Homomorphe Bilder zyklischer Gruppen sind zyklisch.
3. Untergruppen zyklischer Gruppen sind zyklisch.
4. Faktorgruppen zyklischer Gruppen sind zyklisch, d.h. G zyklische Gruppe, $N \trianglelefteq G \Rightarrow G/N$ ist zyklisch.

1.5.2 Symmetrische Gruppe

Definition. Sei $n \in \mathbb{N}_0$. Dann ist

$$S_n = \{\pi : \{1, \dots, n\} \to \{1, \dots, n\}, \pi \text{ ist bijektiv}\}$$

die *symmetrische Gruppe* auf n Elementen („Permutationen“).

Bemerkung. S_n ist Gruppe bzgl. $\circ$.

Notationen. Schreibe:

1. Für $n \in \mathbb{N}$ setze $\underline{n} := \{1, 2, \dots, n\}$.
2. Permutationen schreibt man gerne als

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

Definition. $n \in \mathbb{N}, k \leq n, \{a_1, \dots, a_n\}$ eine k-elementige Teilmenge von $\underline{n}$. Definiere Permutation π durch

$$\begin{aligned} \pi(a_j) &= a_{j+1} && \text{für } 1 \leq j \leq k-1 \\ \pi(a_k) &= a_1 \\ \pi(l) &= l && \text{für } l \notin \{a_1, \dots, a_k\}. \end{aligned}$$

Schreiben $\pi = \begin{pmatrix} a_1 & a_2 & \dots & a_k \end{pmatrix}$ („Zyklus“).

$\{a_1, \dots, a_k\}$ heißt *Träger* von π. Zwei Zyklen heißen *disjunkt*, wenn ihre Träger disjunkt sind.

Satz 1.18 (Zyklendarstellung von Permutationen)**.** Jede Permutation $\pi \in S_n$ kann als Produkt disjunkter Zyklen geschrieben werden. Je zwei disjunkte Zyklen σ, π kommutieren ($\sigma \circ \pi = \pi \circ \sigma$).

Definition. Ein $k \in \underline{n}$ mit $\pi(k) = k$ heißt *Fixpunkt* von π.

Ein Zyklus der Länge 2 heißt *Transposition* (vertauscht nur 2 Elemente).

Proposition. Jeder Zyklus der Länge $l > 2$ kann als Produkt von $l - 1$ Transpositionen geschrieben werden.

Definition. Sei π eine Permutation. Dann ist

$$\begin{aligned} \operatorname{sign} \pi &= (-1)^{\#\text{ Fehlstände von } n} \\ &= (-1)^{|\{(i,j) | i<j \wedge \pi(i) > \pi(j)\}|}. \end{aligned}$$

Bemerkung. Es gilt

$$\operatorname{sign}(\sigma \circ \pi) = \operatorname{sign}(\sigma) \cdot \operatorname{sign}(\pi).$$

Satz 1.19. Die Abbildung sign ist ein Gruppenepimorphismus von S_n nach $(\{\pm 1\}, \cdot)$.

Korollar. Sei $\begin{pmatrix} a_1 & \dots & a_l \end{pmatrix}$ ein l-Zyklus. Dann gilt

$$\operatorname{sign} \begin{pmatrix} a_1 & \dots & a_l \end{pmatrix} = (-1)^{l-1}.$$

Definition.

$$A_n := \operatorname{Ker} \operatorname{sign} \trianglelefteq S_n$$

heißt alternierende Gruppe auf n Elementen.

Proposition. $[S_n : A_n] = 2$.

Satz 1.20. Es gilt:

1. $|S_n| = n!$
2. $|A_n| = \frac{n!}{2}$
3. Es gibt Untergruppen der S_n, die zu S_{n-1} isomorph sind.

1.5.3 Die Diedergruppe

Definition. Sei $n \geq 3$. Dann ist

$$D_n := \{M \in O_2(\mathbb{R}) \mid M(P_n) = P_n\},$$

wobei

$$P_n = \left\{ e^{\frac{2\pi i}{n} \cdot k} \mid k \in \{0, 1, \dots, n-1\} \right\}$$

(regelmäßiges n-Eck).

Satz 1.21 (Struktur der D_n)**.** Sei $n \geq 3$. Dann hat D_n $2n$ Elemente.

D_n ist isomorph zur Untergruppe von S_n, die von

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \end{pmatrix}$$

und

$$\begin{pmatrix} 1 & n-1 \end{pmatrix} \begin{pmatrix} 2 & n-2 \end{pmatrix} \cdots \begin{pmatrix} \lfloor \frac{n}{2} \rfloor & \lceil \frac{n}{2} \rceil \end{pmatrix}$$

erzeugt wird.

1.5.4 Kleinsche Vierergrupppe

Definition.

$$V_4 = \{\mathrm{id}, \begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}, \begin{pmatrix}1 & 3\end{pmatrix}\begin{pmatrix}2 & 4\end{pmatrix}, \begin{pmatrix}1 & 4\end{pmatrix}\begin{pmatrix}2 & 3\end{pmatrix}\}$$

heißt *Kleinsche Vierergruppe*.

1.6 Gruppenwirkungen

Definition. G Gruppe, M Menge. Eine Abbildung $F : G \times M \to M$ heißt *Gruppenwirkung*, falls

1. $\forall x \in M : F(e_G, x) = x$,
2. $\forall g, h \in G \, \forall x \in M : F(h, F(g, x)) = F(h \cdot g, x)$.

Falls F aus dem Kontext klar ist, schreiben wir für $F(g, x)$ auch gx.

Satz 1.22 (Charakterisierung von Gruppenwirkungen)**.** G Gruppe, M Menge und $F : G \times M \to M$. Weiters sei

$$S(M) := \{f : M \to M \mid f \text{ bijektiv}\}.$$

Dann ist F genau dann eine Gruppenwirkung, wenn die Abbildung $\Phi : G \to S(M)$ mit $\Phi(g)(x) = F(g, x)$ wohldefiniert ist und ein Gruppenhomomorphismus ist.

Bemerkung. Sei G endlich. Dann ist $S(G) \simeq S_n$ für $n = |G|$.

Satz von Cayley: G ist isomorph zu einer Untergruppe von S_n.

Definition (Orbit und Stabilisator)**.** Die Gruppe G wirke auf M.

1. Zwei Elemente $x, y \in M$ heißen *äquivalent* unter G, $x \sim_G y$, falls es ein $g \in G$ mit $gx = y$ gibt.
2. Die Menge
$$x^G := \{y \in M \mid x \sim_G y\} = \{gx \mid g \in G\}$$
heißt der *Orbit* von $x \in M$ unter G.
3. Für $x \in M$ heißt
$$G_x := \{g \in G \mid gx = x\}$$
der *Stabilisator* von x unter G.

Proposition. G wirke auf M.

1. $\sim_G$ ist Äquivalenzrelation,
2. $\forall x \in M : x^G = [x]_\sim$ die Äquivalenzklasse.
3. $\forall x \in M : G_x \leq G$

Satz 1.23. Gruppe G wirke auf M, $x \in M, g \in G$.

1. $\left| x^G \right| = [G : Gx]$ („Kardinalität des Orbits ist Index des Stabilisators.“)
2. $G_{gx} = gGxg^{-1}$

Bemerkung. (2) besagt, dass bei Wanderung durch einen Orbit der Stabilisator eine Konjugiertenklasse (Orbit unter Konjugation) durchläuft.

Korollar (Bahnengleichung)*.* G wirke auf M, M sei endlich, $x^1, \ldots, x^N$ ein Repräsentantensystem der Orbits. Dann gilt

$$|M| = \sum_{j=1}^{N} [G : G_{x^j}].$$

Definition. Eine Gruppenwirkung von G auf M heißt *transitiv*, falls

$$\forall x, y \in M \, \exists g \in G : g = gx.$$

Bemerkung. Wirkung transitiv $\Rightarrow$ Es gibt nur einen Orbit.

Korollar. G wirke transitiv auf M. Dann gibt es eine Bijektion zwischen M und den Linksnebenklassen von Gx bezüglich eines $x \in M$.

Satz 1.24 (Lemma von Burnside)**.** G wirke auf M, M sei endlich, G sei endlich. Dann gilt

$$|M/{\sim_G}| = \frac{1}{|G|} \sum_{g \in G} |\{x \in M \mid gx = x\}| .$$

(„Anzahl der Orbits = Mittlere Anzahl der Fixpunkte der Gruppenelemente.“)

Bemerkung. G wirke auf M. Dann wirkt G auch auf $\mathcal{P}(M)$ (Potenzmenge).

Für $N \subseteq M, g \in G$: $gN = \{gn \mid n \in \mathbb{N}\}$. Damit ist auch G_N (Stabilisator von $N \subseteq M$) definiert.

Beispiel. O_n wirkt auf $\mathbb{R}$, damit auch auf Teilmenge $N \subseteq R$.

1.7 Direkte Produkte und direkte Summen

Definition. Sei $G_j, j \in J$, ein System von Gruppen. Auf

$$\prod_{j\in J} G_j = \{(g_j)_{j\in J} \mid g_j \in G_j\}$$

definiere eine Verknüfung $\cdot$ durch

$$(g_j)_{j\in J} \cdot (h_j)_{j\in J} := (g_j \cdot h_j)_{j\in J}.$$

Weiters sei für $k \in J$

$$\pi_k : \prod_{j\in J} G_j \to G_k; (g_j)_{j\in J} \mapsto g_k$$

die k-te *Projektion* auf G_k.

Satz 1.25. Seien $G_j, j \in J$, Gruppen. Dann ist $\prod_{j\in J} G_j$ eine Gruppe, die π_k sind Gruppenepimorphismen. Das Produkt erfüllt die universelle Eigenschaft eines Produkts in der Kategorie der Gruppen, d.h.:

Falls H eine Gruppe ist, $f_j : H \to G_j$, $j \in J$, Gruppenhomomorphismus, dann gibt es einen eindeutig besimmten Homomorphismus $f : H \to \prod_{j\in J} G_j$, sodass das nebenstehende Diagramm $\forall j \in J$ kommutiert.

Bemerkung. Die „universelle Eigenschaft“ charakterisiert das Produkt bis auf Isomorphie eindeutig.

Definition. Seien G_j, $j \in J$, Gruppen. Dann definiere

$$\prod_{j\in J}^{w} G_j := \{(g_j)_{j\in J} \in \prod_{j\in J} G_j \mid g_i \neq e_{G_j} \text{ für nur endlich viele } j \in J\}$$

als das *schwache innere Produkt*.

Falls alle G_j abelsch sind, nennt man es *direkte Summe*

$$\sum_{j\in J} G_j.$$

Die Abbildungen

$$\varepsilon_k : G_k \to \prod_{j\in J}^{w} G_j$$

mit $g_k \mapsto (g_j)_{j\in J}$, wobei

$$g_j = \begin{cases} g_k & j = k \\ e_{G_j} & j \neq k \end{cases}$$

heißen *kanonische Einbettungen*.

Satz 1.26. Seien $G_j, j \in J$, Gruppen. Dann ist

$$\prod_{j\in J}^{w} G_j \trianglelefteq \prod_{j\in J} G_j,$$

also insbesondere wieder eine Gruppe.

Die $\varepsilon_k, k \in J$, sind Gruppenmonomorphismen.

Falls alle G_j abelsch sind, so erfüllt $\sum_{j\in J} G_j$ die universelle Eigenschaft eines Coprodukts in der Kategorie der abelschen Gruppen, d.h. für alle abelschen Gruppen H, Homomorphismen $f_j, j \in J, f_j : G_j \to J$, gibt es genau einen Homomorphismus

$$f : \sum_{j\in J} G_j \to H,$$

sodass das Diagramm kommutiert.

Bemerkung. Die universelle Eigenschaft charakterisiert das Produkt eindeutig.

Satz 1.27. Sei G eine Gruppe, $K \trianglelefteq G, N \trianglelefteq G$, sodass

$$K \cap N = \{e\} \text{ und } K \cdot N = G.$$

Dann ist G isomorph zu $K \times N$. („G ist inneres direktes Produkt von K und N.)

Beispiel. Seien m und n teilerfremde positive ganze Zahlen. Dann gilt

$$\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

(dem Inhalt nach: Chinesischer Restsatz).

2 Graphentheorie

2.1 Definitionen

Definition. Ein *Graph* G ist ein Paar (V, E), wobei V eine Menge ist und

$$E \subseteq \{\{i, j\} \mid i, j \in V, i \neq j\}.$$

- V heißt Menge der Knoten/Ecken/Nodes/Vertices,
- E heißt Menge der Kanten/Edges.
- $|V|$ heißt *Ordnung* des Graphen.

Definition.

1. G heißt *endlich*, wenn V endlich ist.
2. Zwei Knoten $i, j \in V$ heißen *adjazent*, falls $\{i, j\} \in E$.
3. Zwei Kanten $e, f \in E$ heißen *adjazent*, falls $e \cap f \neq \emptyset$.
4. Ein Knoten i und eine Kante e heißen *inzident*, falls $i \in e$.
5. Falls $e \in E$ mit $e = \{i, j\}$, so heißen i und j die *Endpunkte* von e.

Definition (unabhängige Menge)**.** Sei $G = (V, E)$ ein Graph. Eine Teilmenge $W \subseteq V$ heißt *unabhängig*, falls je zwei Knoten aus W nicht adjazent sind.

Definition (Clique)**.** Sei $G = (V, E)$ ein Graph. Eine Teilmenge $W \subseteq V$ heißt *Clique*, wenn je zwei Knoten aus W adjazent sind.

Definition (Teilgraph)**.** Sei $G = (V, E)$ ein Graph, $W \subseteq V, F \subseteq E$ mit $\forall f \in F : f \subseteq W$. Dann heißt (W, F) ein *Teilgraph* von G.

Definition. Sei $G = (V, E)$ ein Graph, $e \in E$. Dann setze

$$G - e := (V, E \setminus \{e\}).$$

Definition (induzierter Teilgraph)**.** Sei $G = (V, E)$ ein Graph, $W \subseteq V$. Dann heißt

$$G[W] = (W, \{\{i, j\} \in E \mid i, j \in W\})$$

der durch W induzierte Teilgraph von G.

Definition (aufspannender Teilbaum)**.** Sei G ein Graph, G' ein Teilgraph. Dann heißt G' ein *aufspannender* Teilgraph von G, falls V(G') = V(G).

Definition (isomorphe Graphen)**.** Seien G_1, G_2 zwei Graphen, $\phi : V(G_1) \to V(G_2)R$. Dann heißt ϕ *Graphenepimorphismus*, wenn ϕ bijektiv ist und

$$E(G_2) = \{\{\phi(i), \phi(j)\} \mid \{i, j\} \in E(G_1)\}.$$

In diesem Fall heißen G_1 und G_2 *isomorph*.

Definition (Gerichteter Graph)**.** Sei V eine Menge und A eine Menge,

$$head, tail : A \to V.$$

Dann heißt $D = (V, A)$ ein *gerichteter* Graph oder *Digraph*.

Die Elemente von A heißen Bögen/arcs/gerichtete Kanten.

Ein Loop (Schleife) ist ein Bogen a mit $head(a) = tail(a)$.

Definition (Multigraph)**.** Ein *Multigraph* ist ein $G = (V, E)$, wobei V eine Menge ist und

$$\phi : E \to V \cup \{\{i, j\} \mid i, j \in V, i \neq j\},$$

also ein gerichteter Graph, dessen Orientierungen entfernt wurden oder ein Graph, bei dem Schleifen und Mehrfachkanten erlaubt sind.

Definition (orientierter Graph)**.** Sei $G = (V, E)$ ein Graph. Eine *Orientierung* von G ist ein Paar von Funktionen $head, tail : E \to V$.

Bemerkung. Jede Kante bekommt eine Richtung, aber keine Rückwärtskanten udgl.

Definition (zugrundeliegender ungerichteter Graph)**.** Sei $D = (V, A)$ ein Digraph ohne Loops und Mehrfachkanten. Dann heißt

$$(V, \{head(a), tail(a) \mid a \in A\})$$

der *zugrundeliegende ungerichtete Graph*.

Definition (Hypergraph)**.** Sei V eine Menge und E eine Menge von Teilmengen von V. Dann heißt (V, E) ein *Hypergraph*.

2.2 Grad, Vollständigkeit

Definition (Grad)**.** $G = (V, E)$ Graph, $v \in V$. Dann heißt

$$d(v) = |\{w \in V \mid vw \in E\}|$$

der *Grad* von v, die Menge

$$N(v) = \{w \in V \mid vw \in E\}$$

heißt die Menge der *Nachbarn* von v.

Lemma (Handschlaglemma)**.** Sei $G = (V, E)$ ein endlicher Graph. Dann gilt

$$\sum_{v \in V} d(v) = 2 \cdot |E| .$$

Korollar. Sei $G = (V, E)$. Dann ist die Anzahl der Knoten mit ungeradem Grad gerade.

Definition (reguläre Graphen)**.** Sei $G = (V, E)$ ein Graph und $k \in \mathbb{N}_0$. Dann heißt G *k-regulär*, falls

$$\forall v \in V : d(v) = k.$$

Ein 3-regulärer Graph heißt auch *kubischer Graph.*

Definition (vollständiger Graph)**.** $n \in \mathbb{N}_0$. Ein $(n-1)$-regulärer Graph der Ordnung n heißt *vollständiger Graph* der Ordnung n und wird als K_n bezeichnet.

2.3 Wege, Kreise, Zusammenhang

Definition (Wege, Wanderungen, Kreise)**.** Sei $G = (V, E)$ ein Graph (evtl. gerichtet).

1. Eine *Wanderung* in G ist eine alternierende Folge inzidenter Knoten und Kanten der Gestalt

   $$x_0, x_0x_1, x_1, x_1x_2, \ldots, x_{n-1}x_n, x_n,$$

   wobei die $x_j \in V$ und für $0 \leq j < n$ auch $x_jx_{j+1} \in E$.

   x_0: Startknoten, x_n: Endknoten, n: Länge der Wanderung

2. Wanderung heißt *Weg*, wenn die x_j paarweise verschieden sind.

3. Wanderung heißt *geschlossen* (circuit), falls Start- und Endknoten übereinstimmen.

4. Eine geschlossene Wanderung heißt *Kreis*, falls $x_0, x_1, \ldots, x_{n-1}$ paarweise verschieden sind, und auch Kanten $x_0x_1, x_1x_2, \ldots, x_{n-1}x_n$ paarweise verschieden (schließt Kreise der Länge ≤ 2 aus).

2.4 Wälder und Bäume

Definition. G Graph.

1. G heißt *Wald*, wenn G azyklisch ist, d.h. keinen Kreis enthält.

2. Ein zusammenhängender Wald heißt *Baum.*

Satz 2.1 (Charakterisierung von Bäumen)**.** G Graph. Äquivalente Aussagen:

1. G ist ein Baum.

2. $\forall x, y \in V(G)$ gibt es genau einen Weg von x nach y in G.

3. G ist minimal zusammenhängend, d.h. jeder echte aufspannende Teilgraph ist unzusammenhängend.

4. G ist maximal azyklisch, d.h. jeder echte „Obergraph“ auf derselben Knotenmenge enthält einen Kreis.

Satz 2.2. G Baum, G endlich. Dann gilt

$$|E(G)| = |V(G)| - 1.$$

Definition. Definiere:

1. Ein *Blatt* eines Baumes ist ein Knoten vom Grad 1.

2. Ein Teilgraph T eines Graphen heißt *Spannbaum*, falls $V(G) = V(T)$ und T ein Baum ist.

Proposition. Jeder Baum hat mindestens 2 Blätter, sofern er Ordnung ≥ 2 hat und endlich ist.

2.5 (Bi)partite Graphen

Definition. Sei $G = (V, E)$ ein Graph, $k \geq 2$ eine ganze Zahl. G heißt *k-partit*, falls es eine Partition $V_1, \ldots, V_n$ von V gibt (also $V = V_1 \cup V_2 \cup \ldots \cup V_k$, V_j paarweise disjunkt), sodass

$$\forall \{x, y\} \in E \; \exists i \neq j : x \in V_i \wedge y \in V_j.$$

Ein 2-partiter Graph heißt *bipartit.*

Satz 2.3 (Charakterisierung bipartiter Graphen)**.** Sei G ein Graph. Dann ist G genau dann bipartit, wenn G keinen ungeraden Kreis (d.h. keinen Kreis ungerader Länge) enthält.

2.6 Eulersche Kreise

Definition. Sei G ein Graph. Ein *Eulerkreis* in G ist ein geschlossene Wanderung, die jede Kante von G genau einmal benutzt.

G heißt *eulersch*, wenn es einen Eulerkreis gibt.

Satz 2.4 (Charakterisierung eulerscher Graphen)**.** Sei G ein (Multi)graph. Dann ist G genau dann eulersch, wenn alle Knotengrade gerade sind und G zusammenhängend ist.

2.7 Hamiltonsche Kreise

Definition. Sei G ein Graph. Ein *Hamilton-Kreis* in G ist ein Kreis, der jeden Knoten genau einmal besucht.

Ein Graph G heißt *hamiltonsch*, wenn G einen Hamilton-Kreis besitzt.

Satz 2.5 (Dirac)**.** Sei G ein Graph mit n Knoten, wo jeer Knoten Grad $\geq \frac{n}{n}$ besitzt. Dann ist G hamiltonsch.

2.8 Matchings

Definition (Matching)**.** Sei $G = (V, E)$ ein Graph, $M \subseteq E$. Dann heißt M *Matching*,, falls jeder Knoten $v \in V$ zu höchstens einer Kante aus M inzident ist.

Ein *vollständiges Matching* ist ein Matching, in dem jeder Knoten $v \in V$ zu genau einer Kante aus M inzident ist.

Definition (k-Faktor)**.** Sei $G = (V, E)$ ein Graph, H ein Teilgraph von G und $k \in \mathbb{N}$. Dann heißt H ein k-Faktor von G, falls H aufspannender Teilgraph ist und k-regulär ist.

Bemerkung. Sei $M \subseteq E$. Dann gilt

M vollständiges Matching $\Leftrightarrow$ (V, M) ist ein 1-Faktor von G.

2.8.1 Matchings von bipartiten Graphen

$G = (A \cup B, E)$ ein bipartiter Graph mit Knotenklassen A und B.

Definition. Eine Knotenüberdeckung von G ist eine Teilmenge $C \subseteq A \cup B$, sodass jede Kante $e \in E$ zu mindestens einem Knoten aus C inzident ist. („Jede Kante wird überdeckt.“)

Satz 2.6 (Satz von König)**.** Sei G ein bipartiter Graph. Dann ist die maximale Kardinalität eines Matchings gleich der minimalen Kardinalität einer Knotenüberdeckung von G.

Satz 2.7 (Satz von Hall, „Heiratssatz“)**.** Sei $G = (A \cup B, E)$ bipartit. Dann enthält G genau dann ein Matching, in dem jeder Knoten von A gematcht wird, wenn

$$\forall S \subseteq A : |\{b \in B \mid \exists a \in S : ab \in E\}| \geq |S|\,.$$

Korollar. Falls $|A| = |B|$, dann ist die Hall-Bedingung gleichwertig mit der Existenz eines vollständigen Matchings.

Korollar. Sei G regulär und bipartit. Dann enthält G ein vollständiges Matching.

Korollar (Satz von Petersen). Sei G ein beliebiger (also nicht notwendig bipartiter) $2k$-regulärer Graph ($k \in \mathbb{N}$). Dann enthält G einen 2-Faktor.

2.9 Planare Graphen

Definition (Ebener Graph)**.** Ein *ebener* Graph $G = (V, E)$ ist ein Paar zweier Mengen V und E, wobei V eine endliche Teilmenge des $\mathbb{R}^2$ und jedes Element $e \in E$ eine einfache Kurve im $\mathbb{R}^2$ zwischen zwei verschiedenen Knoten v und $w \in V$ ist (d.h. $e : [0, 1] \to \mathbb{R}^2$ stetig mit $e(0) = v$ und $e(1) = w$), sodass

- das Innere jedes $e \in E$ keine Punkte aus V enthält und
- für je 2 Kanten $e, f \in E$

  $$e([0, 1]) \cap f([0, 1]) \subseteq V$$

  („Durchschnitt höchstens einelementig“) gilt.

Definition (Planarer Graph)**.** Ein „abstrakter“ Graph heißt *planar*, wenn es einen dazu als Graphen isomorphen ebenen Graphen gibt.

Definition (Fläche)**.** $G = (V, E)$ ebener Graph. Dann heißen die topologischen Zusammenhangskomponenten von $\mathbb{R}^2 \setminus \{V \cup E\}$ die *Flächen* $F(G)$ von G.

Satz 2.8 (Eulersche Polyederformel)**.** Sei G ein zusammenhängender ebener Graph. Dann gilt

$$|V(G)| - |E(G)| + |F(G)| = 2.$$

Korollar. Sei G ein zusammenhängender ebener Graph. Dann gilt

$$|E(G)| \leq 3 \cdot (|V(G)| - 2).$$

Korollar. K_5 ist nicht planar.

Korollar. Sei G ein ebener bipartiter Graph. Dann gilt

$$|E(G)| \leq 2 \cdot (|V(G)| - 2).$$

Korollar. $K_{3,3}$ ist nicht planar.

Definition (topologischer Minor)**.** Seien G, K zwei Graphen. Dann heißt K ein *topologischer Minor* von G, falls es einen Teilgraphen H von G gibt, der aus K durch Unterteilen von Kanten (d.h. „ersetze Kanten durch unabhängige Wege“) entsteht.

Satz 2.9 (Kuratowski)**.**] Sei G ein Graph. Dann gilt:

G planar $\Leftrightarrow$ G hat weder einen $K_{3,3}$ noch einen K_5 als topologischen Minor.

2.10 Färbbarkeit von Graphen

Definition (Chromatische Zahl)**.** Sei G ein Graph. Die chromatische Zahl $\chi(G)$ ist die kleinset natürliche Zahl, sodass es eine „Färbung“ der Knoten von G mit $\chi(G)$ Farben gibt, sodass adjazente Knoten verschiedene Farben haben.

Satz 2.10. Sei G ein planerer Graph. Dann gilt

$$\chi(G) \leq 5.$$

2.11 Graphen und Lineare Algebra

Definition (Adjazenzmatrix)**.** Sei G ein (eventuell gerichteter) Graph mit n Knoten. Dann definiere die *Adjazenzmatrix* A von G durch

$$A = (a_{ij})_{1 \leq i \leq n, 1 \leq j \leq j},$$

wobei a_{ij} = Anzahl der Kanten von i nach j.

Bemerkung. Falls G ungerichtet ist, so ist A eine symmetrische 0-1-Matrix.

Satz 2.11. Sei G ein eventuell gerichteter Graph mit n Knoten. Dann ist die Anzahl der Wanderungen der Länge k von i nach j im Graphen G durch $(A^k)_{ij}$ gegeben.

Definition (Inzidenzmatrix)**.** Sei G ein ungerichteter Graph mit $V(G) = \{1, \ldots, n\}$ und $E(G) = \{e_1, \ldots, e_m\}$. Die *Inzidenzmatrix* B von G ist die $m \times n$ Matrix (b_{ij}) mit

$$b_{ij} = [j \in e_i].$$

Proposition. G Graph. Es gilt

$$B^t \cdot B = A + D,$$

wobei $D = \operatorname{diag}(d(1), d(2), \ldots, d(n))$.

Definition (Orientierte Inzidenzmatrix)**.** G orientierter Graph. Die *orientierte Inzidenzmatrix* ist die Matrix $C = (c_{ij})$ mit

$$c_{ij} = \begin{cases} -1 & j = t(e_i) \\ 1 & j = h(e_i) \\ 0 & \text{sonst} \end{cases}.$$

Satz 2.12. Sei G ein ungerichteter Graph, C die orientierte Inzidenzmatrix bzgl. irgendeiner Orientierung und $n = |V(G)|$. Dann gilt

$$\operatorname{rg}(C) = n - \#\{\text{Zh.-Komponenten von } G\}.$$

Definition.

$$L := D - A$$

heißt *Laplace-Matrix* eines Graphen.

Proposition.

$$C^t C = L$$

3 Partialgeordnete Mengen und Verbände

Definition (Partialordnung)**.** Relation $\leq$ heißt *Partialordnung*, wenn

- reflexiv: $\forall x : x \leq x$
- transitiv: $\forall x, y, z : x \leq y \wedge y \leq z \to x \leq z$
- antisymmetrisch: $\forall x, y : x \leq y \wedge y \leq x \to x = y$

3.1 Satz von Dilworth

Definition. Sei $(X, \leq)$ partialgeordnet.

1. Eine Teilmenge $A \subseteq X$ heißt *Kette*, falls
$$\forall x, y \in A : x \leq y \text{ oder } y \leq x.$$
2. Eine Teilmenge $A \subseteq X$ heißt *Antikette*, falls
$$\forall x, y \in A : x \text{ und } y \text{ sind nicht vergleichbar,}$$
d.h. $\neg(x \leq y) \wedge \neg(y \leq x)$.
3. Sei X endlich und nicht leer. Die *Kettenzahl* $k(X)$ ist die kleinste positive ganze Zahl m, sodass es eine Zerlegung von X in m disjunkte Ketten gibt.
4. Sei X endlich und nicht leer. Die *Dilworth-Zahl* $d(X)$ ist die größte Kardinalität einer Antikette.

Satz 3.1 (Dilworth)**.** Sei X eine endliche partialgeordnete Menge. Dann gilt
$$d(x) = k(X).$$

3.2 Bemerkungen zum Hasse-Diagramm

Definition. Sei $(X, \leq)$ endliche partialgeordnete Menge. y heißt *direkter Vorgänger* von x, falls
$$y \leq x \text{ und } \nexists z \in X : y \leq z \leq x.$$

Definition (Hasse-Diagramm)**.** Das *Hasse-Diagramm* zu einer endl. partialgeordneten Menge X ist der gerichtete Graph
$$(X, \{(y, x) \mid y \text{ ist Vorgänger von } x\}),$$
wobei man die Bögen meist nicht durch Pfeile zeichnet sondern die Orientierung „von unten nach oben“ festlegt.

Definition. Sei R eine Relation auf X. Dann ist die *transitive Hülle* von R durch
$$\bigcap_{R \subseteq T, T \text{ transitive Relation auf } X}$$
definiert.

Bemerkung. $\leq$ ist die transitive Hülle von „ist der Vorgänger von“.

3.3 Verbände

Definition (Verband)**.** Ein Verband ist ein Tupel $(X, \sqcup, \sqcap)$ aus einer Menge X und zwei inneren Verknüpfungen $\sqcup$ und $\sqcap$, sodass $\forall x, y, z \in X$

1. $(x \sqcup y) \sqcup z = x \sqcup (y \sqcup z)$ und $(x \sqcap y) \sqcap z = x \sqcap (y \sqcap z)$ („assoziativ“)
2. $x \sqcup y = y \sqcup x$ und $x \sqcap y = y \sqcap x$ („kommutativ“)
3. $x \sqcup (x \sqcap y) = x$ und $x \sqcap (x \sqcup y) = x$ („Absorptionsgesetzte“).

Bemerkung (Dualitätsprinzip)*.* Hat man irgendeine Aussage aus den Verbandsaxiomen hergeleitet, so gilt sie auch nach Vertauschen von $\sqcup$ und $\sqcap$.

4 Kombinatorik

- $A = A_1 \cup A_2 \cup \ldots \cup A_n$ (A_i endliche Mengen, paarweise disjunkt)

$$\Rightarrow |A| = |A_1| + |A_2| + \cdots + |A_n|$$

- $A = A_1 \times A_2 \times \ldots \times A_n$ (A_i endliche Mengen)

$$\Rightarrow |A| = |A_1| \cdot |A_2| \cdots |A_n|$$

Beispiel.

$$|\{f : X \to Y\}| = \left| Y^{|X|} \right| = |Y|^{|X|}$$

4.1 Inklusions-Exklusions-Prinzip

Satz 4.1. Seien $A_1, \ldots, A_n$ endliche Mengen. Dann gilt

$$\left| \bigcup_{j=1}^{n} A_j \right| = \sum_{J \subseteq \{1,\ldots,n\}, J \neq \emptyset} (-1)^{|J|+1} \left| \bigcap_{j \in J} A_j \right|.$$

Korollar.

$$\begin{aligned} |A \cup B \cup C| = {} & |A| + |B| + |C| \\ & - |A \cap B| - |A \cap C| - |B \cap C| \\ & + |A \cap B \cap C| \end{aligned}$$

4.2 Zählen mit Binomialkoeffizienten und seinen Freunden

Bemerkung.

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!} = \frac{n!}{k!(n-k)!}$$

ist die Anzahl der k-elementigen Teilmengen einer n-elementigen Menge. („Kombinationen ohne Wiederholung“)

Satz 4.2. Anzahl der Mandatsverteilungen in einem Parlament mit n Sitzen und k Parteien, oder

Anzahl der Kollektion von n Elementen aus k-elementiger Menge, wobei Elemente öfter gewählt werden dürfen und die Reihenfolge unerheblich ist:

$$\binom{n+k-1}{k-1}$$

(„Kombinationen mit Wiederholung“)

Definition. Für $z \in \mathbb{R}$ und $n \in \mathbb{N}_0$ schreibe

$$z^{\underline{n}} := \underbrace{z(z-1)\cdots(z-n+1)}_{n}$$

(„fallende Faktorielle“) und

$$z^{\overline{n}} := \underbrace{z(z+1)\cdots(z+n-1)}_{n}$$

(„steigende Faktorielle“).

Proposition. Rechenregeln für Binomialkoeffizienten:

1. $\binom{x}{k} = \frac{x}{k} \cdot \binom{x-1}{k-1}$ ($k \neq 0$ und ganz)
2. $\binom{x}{k} = \binom{x-1}{k-.1} + \binom{x-1}{k}$ (k ganz)
3. $\sum_{m=0}^{n} \binom{m}{k} = \binom{m+1}{k+1}$ ($k, n \geq 0$)
4. $\sum_{k=0}^{n} \binom{x+k}{k} = \binom{x+n+1}{n}$ (n ganz)

Satz 4.3 (Vandermonde-Identität)**.**

$$\sum_{k=0}^{n} \binom{x}{k}\binom{y}{n-k} = \binom{x+y}{n},$$

wobei n ganzzahlig.

4.2.1 Catalan-Zahlen

Beispiel. Wie viele Möglichkeiten für die Torabfolge bei einem Fußballspiel gibt es, in dem insgesamt $2n$ Tore fallen, die Partie unentschieden endet und Mannschaft B nie im Rückstand ist?

Definition. Die n-te *Catalan-Zahl* ist

$$C_n := \frac{1}{n+1}\binom{2n}{n}.$$

Bemerkung. C_n erfüllt

$$C_n = \binom{2n}{n} - \binom{2n}{n+1}$$

und ist somit eine ganze Zahl.

4.3 Stirling-Zahlen

Definition (Stirling-Zahl 2. Art)**.** Seien $n, k \in \mathbb{N}_0$. Die *Stirling-Zahl 2. Art* von n und k wird mit

$$\left\{ n \atop k \right\}$$

bezeichnet und gibt die Anzahl der Partitionen einer n-elementigen Menge in k nichtleere Mengen an.

Proposition.

$$\begin{Bmatrix} n \\ 0 \end{Bmatrix} = [n = 0]$$
$$\begin{Bmatrix} n \\ 1 \end{Bmatrix} = 1$$
$$\begin{Bmatrix} n \\ n \end{Bmatrix} = 1$$
$$\begin{Bmatrix} n \\ n-1 \end{Bmatrix} = \binom{n}{2}$$

Satz 4.4 (Rekursion für Stirling-Zahlen 2. Art)**.**

$$\begin{Bmatrix} n \\ k \end{Bmatrix} = \begin{Bmatrix} n-1 \\ k-1 \end{Bmatrix} + k \cdot \begin{Bmatrix} n-1 \\ k \end{Bmatrix}$$

Definition (Stirling-Zahl 1. Art)**.** Seien $n, k \in \mathbb{N}$. Die *Stirling-Zahl 1. Art* ist die Anzahl der Permutationen aus S_n, die aus k Zyklen bestehen.

Proposition.

$$\begin{bmatrix} n \\ 0 \end{bmatrix} = [n = 0]$$
$$\begin{bmatrix} n \\ 1 \end{bmatrix} = (n-1)!$$
$$\begin{bmatrix} n \\ n \end{bmatrix} = \begin{Bmatrix} n \\ n \end{Bmatrix} = 1$$
$$\begin{bmatrix} n \\ n-1 \end{bmatrix} = \begin{Bmatrix} n \\ n-1 \end{Bmatrix} = \binom{n}{2}$$

Satz 4.5 (Rekursion für Stirling-Zahlen 1. Art)**.**

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} + (n-1) \cdot \begin{bmatrix} n-1 \\ k \end{bmatrix}$$

Proposition.

$$\sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} = n!$$

Satz 4.6 (Übergang zwischen Potenzen, steigenden und fallenden Faktoriellen)**.** Es gilt:

1. $x^n = \sum_{k=0}^{n} \begin{Bmatrix} n \\ k \end{Bmatrix} x^{\underline{k}}$
2. $x^{\overline{n}} = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} x^k$
3. $x^n = \sum_{k=0}^{n} \begin{Bmatrix} n \\ k \end{Bmatrix} (-1)^{n-k} x^{\overline{k}}$
4. $x^{\underline{n}} = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} (-1)^{n-k} x^k$

4.4 Einführung in erzeugende Funktionen

Definition. Sei R ein Ring mit 1. Dann ist der *Ring der formalen Potenzreihen* in Z über R, $R[[Z]]$, definiert als

$$R[[Z]] = \{(a_n)_{n \in \mathbb{N}_0} \mid a_n \in R\},$$

wobei diese Folgen als formale Summe

$$\sum_{n=0}^{\infty} a_n Z^n$$

geschrieben werden.

Addition auf $R[[Z]]$ ist komponentenweise definiert, also

$$\sum_{n \geq 0} a_n Z^n + \sum_{n \geq 0} b_n Z^n := \sum_{n \geq 0} (a_n + b_n) Z^n.$$

Multiplikation auf $R[[Z]]$ ist als Faltung definiert, d.h.

$$\left(\sum_{n \geq 0} a_n Z^n \right) \cdot \left(\sum_{n \geq 0} b_n Z^n \right) := \sum_{n \geq 0} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) Z^n.$$

Satz 4.7. Sei R ein Ring mit 1 und $R[[Z]]$ der „Ring“ der formalen Potenzreihen. Dann ist $R[[Z]]$ ein Ring mit

$$-\left(\sum_{n \geq 0} a_n Z^n \right) = \sum_{n \geq 0} (-a_n) Z^n.$$

Neutrales Element bzgl. Addition:

$$\sum_{n \geq 0} 0 \cdot Z^n.$$

Neutrales Element bzgl. Multiplikation

$$\sum_{n \geq 0} [n = 0] \cdot Z^n.$$

Satz 4.8 (Standard-Manipulationen für erzeugende Funktionen)**.** Seien g_n, h_n Folgen, $G(Z) = \sum_{n \geq 0} g_n z^n$ und $H(Z) = \sum_{n \geq 0} h_n z^n$ ihre erzeugenden Funktionen. Dann gelten die Beziehungen in Tabelle 1.

Proposition.

$$\sum_{n \geq 0} n^k a_n Z^n = \sum_{l=0}^{k} \begin{Bmatrix} k \\ l \end{Bmatrix} l! \frac{(aZ)^l}{(1 - aZ)^{l+1}}$$

für k positiv ganz.

„Folgen-Welt“	„GF-Welt“
$g_n + h_n$	$G(Z) + H(Z)$
Faltung $(\sum_{k=0}^{n} g_k h_{n-k})_n$	$G(Z) \cdot H(Z)$
$\alpha \cdot g_n$	$\alpha \cdot G(Z)$
$(\underbrace{0, \ldots, 0}_{m}, g_0, g_1, \ldots)$	$Z^m G(Z)$
$(g_m, g_{m+1}, \ldots)$	$\frac{G(Z) - \sum_{k=0}^{m-1} g_k Z^k}{Z^m}$
$(0g_0, 1g_1, 2g_2, 3g_3, \ldots)$	$ZG'(Z)$
$(0, \frac{g_1}{1}, \frac{g_2}{2}, \frac{g_3}{3}, \ldots)$	$\int_{t=0}^{Z} \frac{G(t) - g_0}{t} dt$
$(g_0, g_0 + g_1, g_0 + g_1 + g_2, \ldots)$	$\frac{1}{1-Z} G(Z)$

Tabelle 1: Standard-Manipulationen für erzeugende Funktionen

4.5 Lineare Rekursionen über erzeugende Funktionen

Satz 4.9 (Lineare Rekursionen)**.** Die Folge f_n genüge der Rekursion

$$f_n = \sum_{j=1}^{d} a_j f_{n-j} + \sum_{j=1}^{k} P_j(n) \beta_j^n,$$

wobei d positiv ganz, $a_1, \ldots, a_d$ Konstanten, $P_j(n)$ ein Polynom vom Grad d_j, und es seien Startwerte $f_0, \ldots, f_{d-1}$ gegeben.

Seien $\alpha_1, \ldots, \alpha_r$ die verschiedenen Nullstellen des „charakteristischen Polynoms“

$$Z^d - \sum_{j=1}^{d} a_j Z^{d-j}$$

und $\mu(a_j)$ die Vielfachheiten von a_j als Nullstelle des char. Polynoms sowie $\mu(\gamma) = 0$, falls γ keine Nullstelle des char. Polynoms ist.

Dann gibt es Polynome

$$Q_1(n), \ldots, Q_r(n)$$

der Grade $\leq \mu(\alpha_1) - 1, \ldots, \mu(\alpha_r) - 1$ sowie Polynome

$$R_1(n), \ldots, R_k(n)$$

der Grade $d_1, \ldots, d_{k_r}$, sodass

$$f_n = \sum_{j=1}^{r} Q_j(n) \cdot \alpha_j^n + \sum_{j=1}^{k} n^{\mu(\beta_j)} R_j(n) \beta_j^n$$

für $n \geq 0$.

4.6 Weitere Beispiele zu erzeugenden Funktionen

4.7 Exponentiell-erzeugende Funktionen

Definition. Sei a_n, $n \in \mathbb{N}_0$, eine Folge. Dann definiere ihre *exponentiell-erzeugende Funktion* durch

$$\tilde{G}(Z) := \sum_{n \geq 0} a_n \frac{Z^n}{n!}.$$

Bemerkung. Die exponentiell-erzeugende Funktion von a_n ist also die gewöhnliche erzeugende Funktion von $\frac{a_n}{n!}$.

Bemerkung. Exponentiell-erzeugende Funktionen sind besonders nützlich, wenn in der Kombinatorik Reihenfolge durch Division durch Fakultäten „gekillt“ wird.