Kapitel 2 Grundlagen der Gruppentheorie

Gliederung wurde verändert:

2.1 Mengen und Abbildungen

2.1.1 Eine *Menge* X ist eine Gesamtheit von Objekten, welche Elemente von X genannt werden. Man schreibt $x \in X$.
Angabe von X durch Auflisten oder durch Eigenschaften der Elemente, z.b. sind die geraden Zahlen

$$X = \{\cdots - 4, -2, 0, 2, 4, \cdots\} = \{x \in \mathbb{Z};\ \ 2|x\}.$$

Beispiele: Zahlbereiche und Matrizen darüber.

Grundoperationen für Mengen:
Inklusion: $X \subset Y$ oder $X \subseteq Y$, z.B. $\mathbb{Z} \subset \mathbb{Q}$, $\mathbb{Q}^{m\times n} \subset \mathbb{R}^{m\times n}$. Die Relation $\subseteq$ definiert eine partielle Ordnung.
Vereinigung: $X \cup Y$ besteht aus den Elementen, welche in X oder in Y liegen.
Durchschnitt: $X \cap Y$ besteht aus den Elementen , welche in X und in Y liegen.
Differenz: $X - Y$ besteht aus den Elementen, welche in X, aber nicht in Y liegen.
Die *leere Menge* $\emptyset$ hat kein Element.
X und Y heißen *disjunkt*, falls $X \cap Y = \emptyset$.

Eine *endliche Menge* X ist eine Menge mit endlich vielen Elementen. In diesem Fall bezeichnet $|X|$ oder $\sharp X$ die Anzahl der Elemente.
Mengentheoretische Identitäten Übungsaufgabe
Die Potenzmenge $\mathfrak{P}(M)$ einer endlichen Menge M hat $2^{|M|}$ Elemente.

2.1.2 Eine *Abbildung* $f : X \to Y$ zwischen zwei Mengen ist eine eindeutige Zuordnung

$$x \in X \mapsto f(x) \quad (\mapsto \text{ „geht über in“}).$$

Jedem $x \in X$ wird eindeutig sein Bild $f(x) \in Y$ zugeordnet. *Abbildungsvorschrift*. X heißt *Definitionsbereich* von f und Y *Bildbereich* von f.

Die *identische Abbildung* ist: $Id_X : X \to X$
$$x \mapsto x \;\; \forall x \in X.$$

Beispiel: Jede Funktion welche einem Objekt ein bestimmtes Datum zuordnet kann man als Abbildung Objektmenge$\to$ Datenmenge interpretieren , z.B. Alter eines Einwohners, Temperatur eines Körpers, Höhe eines Berges.

Gegenbeispiel: $x \in I\!R_{>0} \mapsto \sqrt{x} \in I\!R$ ist keine Abbildung weil die Quadratwurzel nicht eindeutig bestimmt ist. Um hieraus eine Abbildung zu machen müsste man in jedem Fall präzisieren, ob man die positive oder die negative Wurzel meint. Oder man ändert den Bildbereich ab: Man nimmt als Bildbereich nicht $I\!R$ sondern die Menge aller ungeordneten Paare $\{x, -x\}$.

2.1.3 Hintereinanderausführungen von Abbildungen:
$f : X \to Y;\; g : Y \to Z$. Dann ist $g \circ f : X \to Z$ definiert durch:

$$(g \circ f)(x) = g(f(x)).$$

Man schreibt $g \circ f$ und sagt „g angewendet auf f“.

2.1.4 Bemerkung: Sei $f : X \to Y$ eine Abbildung. Dann ist $f \circ Id_X = f, \quad Id_Y \circ f = f$. Sind $f : X \to Y,\; g : Y \to Z,\; h : Z \to W$ drei Abbildungen, dann gilt das Assoziativgesetz:

$$h \circ (g \circ f) = (h \circ g) \circ f$$

2.1.5 Spezielle Eigenschaften von Abbildungen:

	$f : X \to Y$
injektiv	$x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$
surjektiv	zu jedem $y \in Y$ *ex.* $x \in X$, sodass $f(x) = y$
bijektiv	= injektiv + surjektiv

Man spricht auch von *Injektion, Surjektion, Bijektion.*
Eine Injektion ist eine charakterisierende Abbildung, dh. das Bild eines Elementes reicht aus um den Ursprung zu identifizieren. Beispiel: der ID eines Einwohners, Gegenbeispiel: das Geburtsdatum eines Einwohners.

Weitere Terminologie:

Bild $(f) = Im(f) = \{y \in Y; y = f(x)\}$.
Zu $f : X \to Y$ gehört eine Äquivalenzrelation auf X nämlich $x_1 \sim_f x_2$ falls $f(x_1) = f(x_2)$.
Die Quotientenmenge $X/\sim_f$ hat als Elemente die Fasern der Abbildung (eine *Faser* für f besteht aus allen Elementen von X, welche unter f dasselbe Bild in Y haben).

$f^{-1}(y)$ bezeichnet die Faser aller x mit $f(x) = y$. Möglich ist $f^{-1}(y) = \emptyset$, nämlich dann, wenn $y \notin Bild(f)$.
Jede Abbildung f läßt sich zerlegen in eine Surjektion, Bijektion und eine Injektion

$$X \xrightarrow{\pi} X/\sim_f \xrightarrow{f_*} \text{Bild}(f) \xrightarrow{\iota} Y.$$

$f = \iota \circ f_* \circ \pi$.

Die Abbildung π ordnet jedem x die Faser zu, in der x liegt. π ist surjektiv.
Die Abbildung f_* ordnet jeder Faser ihr Bild zu. f_* ist bijektiv.
Die Abbildung ι bettet Bild (f) in Y ein. ι ist injektiv.

Folgerung: Sei X endliche Menge und $f : X \to X$ eine Selbstabbildung. Wenn f injektiv ist dann muss es auch surjektiv sein, und wenn es surjektiv ist dann muss es auch injektiv sein.
Beweis: X ist die disjunkte Vereinigung der Fasern von f. Die Abbildung ist injektiv genau dann, wenn alle Fasern aus einem Element bestehen.
Für unendliche Mengen Gegenbeispiele: $n \mapsto n+1$ auf der Menge der natürlichen Zahlen ist injektiv aber nicht surjektiv. $x \mapsto x^2$ auf der Menge der komplexen Zahlen ist surjektiv aber nicht injektiv.
Übung: $\mathbb{Q}$:= rationale Zahlen. Man diskutiere die Zerlegung von $f : \mathbb{Q} \to \mathbb{Q}, x \mapsto x^2$.

2.1.6 Wenn $f : X \to Y$ bijektiv ist, dann gibt es zu jedem $y \in Y$ genau ein $x \in X$, sodass $f(x) = y$. Wir nennen $x =: f^{-1}(y)$. Damit ist eine Abbildung $f^{-1} : Y \to X$ erklärt, sodass $f^{-1} \circ f = Id_X, \quad f \circ f^{-1} = Id_Y$.

Umgekehrt, wenn zu $f : X \to Y$ eine Abbildung $g : Y \to X$ existiert mit $g \circ f = Id_X, f \circ g = Id_Y$, dann ist f bijektiv und $g = f^{-1}$.

Wir nennen f^{-1} die zu f *inverse Abbildung* oder die *Umkehrabbildung*. Natürlich ist dann auch f^{-1} bijektiv und $(f^{-1})^{-1} = f$.

Beispiel: $A \in \mathbb{R}^{n\times n}$ invertierbare Matrix. Dann ist $X \in \mathbb{R}^{n\times 1} \mapsto AX \in \mathbb{R}^{n\times 1}$ invertierbare Abbildung. Die inverse Abbildung ist $X \mapsto A^{-1}X$.

2.1.7 Kardinalzahlen
Übung: Es seien $f : X \to Y$ und $g : Y \to Z$ zwei Bijektionen. Dann ist $g \circ f$ eine Bijektion und $(g \circ f)^{-1} = (f^{-1}) \circ (g^{-1})$.
Wir nennen zwei Mengen X und Y *gleichmächtig* wenn sich zwischen ihnen eine Bijektion herstellen lässt. Die Gleichmächtigkeit von Mengen ist offensichtlich eine Äquivalenzrelation. Die Äquivalenzklassen bezüglich dieser Relation bezeichnet man als **Kardinalzahlen**.
Man schreibt $|X|$ für die Äquivalenzklasse der zu X gleichmächtigen Mengen.

Definition: $|X| \leq |Y|$ falls es eine Injektion von X in Y gibt. Diese Definition ist repräsentantenunabhängig.
Satz von Schröder und Bernstein: Wenn $|X| \leq |Y|$ und $|Y| \leq |X|$, dann folgt $|X| = |Y|$. Zu je zwei Mengen X, Y gilt: $|X| \leq |Y|$ oder $|Y| \leq |X|$. Somit ist $\leq$ eine Totalordnung auf der Menge der Kardinalzahlen.
Die kleinste unendliche Kardinalzahl ist $|\mathbb{N}|$.
Satz von G.Cantor:$|\mathfrak{P}(M)| > |M|$.
Kontinuumshypothese: Die Kardinalzahl des Kontinuums $|\mathbb{R}| = 2^{|\mathbb{N}|} = |\mathfrak{P}(\mathbb{N})|$ ist die nächste auf $|\mathbb{N}|$ folgende Kardinalzahl. Allgemeiner:Für unendliche Kardinalzahlen ist $|\mathfrak{P}(M)|$ die nächste auf $|M|$ folgende Kardinalzahl.
Satz von Paul Cohen (1963): Die Kontinuumshypothese ist im Rahmen der Mengenlehre nicht entscheidbar. Man kann also eine Mengenlehre mit oder ohne K.hypothese entwickeln genau so wie eine Geometrie mit oder ohne Parallelenaxiom.

2.1.8 Produktmenge.
X, Y zwei Mengen. $X \times Y = \{(x, y); x \in X, y \in Y\}$ Menge der geordneten Paare (x, y), wobei an der 1. Stelle Element von X, an der 2. Stelle Element von Y.
Spezialfall: $X \times X$
Iteration: $X_1 \times X_2 \cdots \times X_n$.

Beispiel: $\mathbb{R} \times \mathbb{R}$ ist die Ebene, deren Punkte durch 2 reelle Koordinaten definiert sind.
Graph einer Abbildung $f : X \to Y$: $\Gamma(f) = \{(x, f(x));\ x \in X\} \subset X \times Y$.

2.1.9 Bemerkung: Die Assoziativität 2.1.4, die Existenz des Inversen 2.1.6 und die Identität Id_X machen aus der Menge aller Bijektionen von X auf sich eine Gruppe mit der Operation „Hintereinanderausführung von Abbildungen“ (vgl. nächster Abschnitt).

2.2 Gruppen, Definition und Beispiele

2.2.1 Defintion:Eine Gruppe G ist eine Menge versehen mit einer Operation $(x, y) \mapsto x \cdot y$ für alle $x, y \in G$ welche folgende Eigenschaften hat: Assoziativität, Einselement, Existenz des Linksinversen (oder äquivalent dazu, Existenz des Rechtsinversen). (Begriff der kommutativen Gruppe.)

2.2.2 Satz: *e und g^{-1} eindeutig, $(gh)^{-1} = h^{-1}g^{-1}$, $axb = c \Rightarrow x = a^{-1}cb^{-1}$ eindeutig, $(g^{-1})^{-1} = g$.*

2.2.3 Beispiele: $S(X)$ Gruppe aller Bijektionen von X auf sich, Spezialfall, wenn X nur endlich viele $(= n)$ Elemente hat. Dann ist $S(X) = S_n$. Die allgemeine lineare Gruppe $\mathrm{GL}_n(\mathbb{R})$und die Einbettung

$\mathrm{GL}_n(\mathbb{R}) \subset S(\mathbb{R}^{n\times 1})$. Die Matrix A ist aus der Abbildung $X \mapsto AX$ rekonstruierbar.

2.2.4 Multiplikationstafel. Beispiel, die Symmetriegruppe eines Rechtecks, welches kein Quadrat ist. $G = \{e, s_x, s_y, r_\pi\}$ Spiegelungen an der x-Achse, der y-Achse und Drehungen um 180°.
In jeder Zeile und jeder Spalte der Multiplikationstafel von G kommt jedes Element von G genau einmal vor.

2.2.5 Definition der Potenzen und der Ordnung eines Elementes.
Mit $|g|$ bezeichnen wir die Ordnung des Elementes g in der Gruppe G.
Vorsicht: $(gh)^n \neq g^n h^n$ wenn G nicht kommutativ.

2.2.6 Satz: *$g \in G$ habe die Ordnung $n \geq 1$.*
Dann gilt für $r, s \in \mathbb{Z}$: (i) $g^r = g^s$ gdw. $n|(r-s)$
(ii) $g^k = e (= g^0)$ gdw. $n|k$.
(ii) ist Spezialfall von (i).
Man beweist zuerst (ii) wobei die Division mit Rest für ganze Zahlen benötigt wird. Aus (ii) folgt dann (i).

2.3 Zyklische Gruppen und Diedergruppen.

2.3.1 Zyklische Gruppen, Definition und Schreibweise $G =< g >$. Z.B. die Rotationen um Vielfache von $\frac{2\pi}{n}$.

2.3.2 Sei $G =< g >$ eine endliche zyklische Gruppe. Dann ist $|G| = |g|$.

2.3.3 Jede unendliche zyklische Gruppe ist isomorph zu $(\mathbb{Z}, +)$. Jede endliche zyklische Gruppe ist isomorph zu $(\mathbb{Z}/n\mathbb{Z}, +)$.

2.3.4 Definition der Untergruppe. Als Untergruppe einer Gruppe G bezeichnet man eine nichtleere Teilmenge H, sodass die Einschränkung der Gruppenoperation von G auf H aus der Menge H eine Gruppe macht.
Die Untergruppe H hat dann dasselbe Einselement wie die Gruppe G. Demzufolge ist auch das Inverse eines Elementes aus H dasselbe wie sein Inverses in G.
Beweis: Nach Definition ist das Produkt von zwei Elementen aus H dasselbe wie ihr Produkt in G. Seien e_1, e die Einselemente von H bzw. G. Mit e_1' bezeichnen wir das Inverse von e_1 in der Gruppe G. Wir benutzen $e_1 e_1' = e$ sowie $e_1 e_1 = e_1$ innerhalb von H. Dann folgt:

$$e_1 = e_1 \cdot e = e_1(e_1 e_1') = (e_1 e_1) \cdot e_1' = e_1 e_1' = e.$$

2.3.5 Gruppentheorie und elementare Zahlentheorie - Übung

Es sei $n \in \mathbb{Z}$ und $n\mathbb{Z}$ die Menge der Vielfachen von n. Dann gilt:
(i) $(n\mathbb{Z}, +)$ ist Untergruppe von $(\mathbb{Z}, +)$.
(ii) Ist m eine weitere ganze Zahl, dann $m\mathbb{Z} \subseteq n\mathbb{Z}$ genau dann, wenn $n|m$.
(iii) Ist $U \subseteq (\mathbb{Z}, +)$ eine beliebige Untergruppe dann hat U stets die Form $U = n\mathbb{Z}$, wobei $|n|$ eindeutig bestimmt ist. Entweder ist $U = \{0\}$ oder $n \in U$ hat unter den Zahlen aus U kleinstmöglichen Absolutbetrag $\neq 0$.
Der Beweis benutzt Division mit Rest, ähnlich wie 2.2.6.
(iv) Seien $m,\ n \in \mathbb{Z}$ und sei $U = m\mathbb{Z} + n\mathbb{Z}$ die Menge aller Linearkombinationen von m und n. Dann ist U eine Untergruppe, also nach (iii) gilt: $U = d\mathbb{Z}$. Weiter folgt dann: d ist der, dem Betrag nach, grösste gemeinsame Teiler von m und n, und ausserdem ist d Linearkombination von m und n.

2.3.6 Die Anzahl der Erzeugenden einer zyklischen Gruppe Es sei $G =< g >$ endliche zyklische Gruppe der Ordnung n, es sei $k \in \{0, \dots, n-1\}$ und es sei $< g^k >$ die zyklische Untergruppe der Potenzen von g^k. Dann gilt $< g^k >=< g^d >$ wobei $d = ggT(k, n)$. Es folgt:
(i) $| < g^k > | = n/ggT(k, n)$. Insbesondere $< g^k >= G$ genau dann wenn $ggT(k, n) = 1$.
(ii) Die Anzahl der Erzeugenden einer zyklischen Gruppe der Ordnung n ist gleich der Anzahl aller $k \in \{0, \dots, n-1\}$ mit $ggT(k, n) = 1$. Man bezeichnet diese Zahl mit $\varphi(n) =$ Eulersche Funktion.
Beispiel: Rotationen um Vielfache von $2\pi/6 = \pi/3$.

2.3.7 Jede Untergruppe U einer zyklischen Gruppe G ist ebenfalls zyklisch. Wenn $G =< g >$ die Ordnung n hat dann hat jede Untergruppe U die Form $U =< g^m >$ mit $m|n$, und $\frac{n}{m}$ ist dann die Ordnung von U. Insbesondere gibt es zu jedem Teiler $d|n$ genau eine Untergruppe der Ordnung d.

2.3.8 Beispiel: Die **Diedergruppen**. Die stetige Diedergruppe O_2 ist definiert als die Gruppe aller Drehungen r_α und Spiegelungen s_g der Ebene $\mathbb{R}^2$ welche den Nullpunkt fixieren. Dabei bezeichnet r_α die Drehung um den Winkel α entgegen dem Uhrzeigersinn, und s_g bezeichnet die Spieglung an der Geraden g durch den Nullpunkt. Man beweist die Relationen
$r_\alpha \cdot r_\beta = r_{\alpha+\beta}$,
$s_g \cdot r_\alpha \cdot s_g = r_{-\alpha}$,
$r_\alpha \cdot s_g = s_{r_{\alpha/2}(g)}$,
$s_{g_1} \cdot s_{g_2} = r_{2\alpha}$, wobei α der Drehwinkel von g_2 nach g_1 ist, dh. $g_1 = r_\alpha(g_2)$.
Die **endlichen Diedergruppen** $D_n,\ n \geq 3$, sind definiert als die Symmetriegruppen regelmässiger n-Ecke. Wenn man ein solches regelmässiges n-Eck einem Kreis um den Nullpunkt einbeschreibt dann wird D_n Un-

tergruppe der stetigen Diedergruppe O_2 welche aus n Drehungen und n Spiegelungen besteht. Sie wird erzeugt durch zwei Spiegelungen s_{g_1} und s_{g_2} an Geraden die miteinander den Winkel π/n bilden. Dann gilt nämlich $s_{g_1} s_{g_2} = r_{2\pi/n}$.

2.3.9 Realisierung von O_2 als Matrizengruppe.
Drehungen und Spiegelungen mit Fixpunkt 0 sind lineare Selbstabbildungen des $I\!R^2$. Somit kann man sie durch 2×2-Matrizen realisieren.

2.3.7 Additiv geschriebene Gruppen (z.B Vektoren). Manchmal wird das Gruppengesetz auf G auch als Addition geschrieben $(g, h) \mapsto g + h$. Dies ist nur erlaubt, wenn die Gruppe kommutativ ist. Anstelle von e, g^n, g^{-1} hat man dann $0, ng, -g$.
Die *Ordnung* von g ist das kleinste $n \geq 1$ mit $ng = 0$.

2.4 Aktion einer Gruppe auf einer Menge

Die Elemente einer Gruppe interpretieren sich oftmals als Operatoren auf einer Menge

2.4.1 Def. Aktion einer Gruppe G auf einer Menge X, ist eine Abbildung $(g, x) \in G \times X \mapsto g \circ x \in X$ (g angewendet auf x).
Die Elemente von G werden hier als Operatoren auf der Menge X betrachtet. Dabei soll folgendes gelten:
(i) $(g_1 \cdot g_2) \circ x = g_1 \circ (g_2 \circ x)$
(ii) $e \circ x = x \qquad \forall x \in X$.

2.4.2 Beispiele: $\mathrm{GL}_m(I\!R) \times I\!R^{m\times n} \to I\!R^{m\times n}$. Aktion durch Multiplikation von links.
Die Gruppe S_n der Vertauschungen von n Elementen operiert auf $X = \{x_1, \cdots, x_n\}$, $\pi \circ x_i = x_{\pi(i)}$.
$I\!R/2\pi\mathbb{Z}$ operiert auf der Ebene $I\!R^2$ als Gruppe der Drehungen. Ist $[\alpha]$ eine Restklasse und p ein Punkt der Ebene, dann sei $[\alpha] \circ x = r_\alpha(x)$, wobei r_α die Linksdrehung um den Winkel α bezeichnet.

2.4.3 Satz: *Eine Operation von G auf X induziert immer eine Äquivalenzrelation auf X, nämlich: $x \sim y$, falls ein $g \in G$ existiert, sodass $y = g \circ x$.*
Die Äquivalenzklassen heißen die *Bahnen* von G auf X.

2.4.4 Beispiel: X = Einheitskreis. G = Rotationen um Vielfache von $\frac{\pi}{2}$. Jede Bahn besteht aus 4 Punkten auf dem Einheitskreis.

2.4.5 Beispiel der Zeilenäquivalenz. $\mathrm{GL}_m(I\!R) \times I\!R^{m\times n} \to I\!R^{m\times n}$. Bahnen unter der Aktion von $\mathrm{GL}_m(I\!R)$ auf $I\!R^{m\times n}$ durch Multiplikation von links sind die Klassen zeilenäquivalenter Matrizen.(vgl.1.5.5)

2.4.6 $(\mathbb{Z}, +)$ mit Untergruppe $(n\mathbb{Z}, +)$. Aktion $n\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, (a, b) \mapsto a + b$ hat als Bahnen die Restklassen modulo n.

2.4.7 Unser **Hauptbeispiel** ist die Aktion der symmetrischen Gruppe S_n auf der Menge $X = \{1, ..., n\}$ der ersten n Zahlen. Die Gruppe operiert dabei durch Vertauschungen der Zahlen, und die Gruppenoperation ist die Hintereinander ausführung von Vertauschungen. In diesem Fall gibt es nur eine Bahn. Man sagt dass die Gruppe S_n auf X **transitiv** operiert. Sei $\pi \in S_n$ ein einzelnes Element und $< \pi >$ die davon erzeugte zyklische Gruppe. Dann gibt es bei Aktion von $< \pi >$ auf X i.a. viele Bahnen. Das führt auf die Zykelzerlegung der Permutation π.

2.5 Untergruppen und Nebenklassen

2.5.2 Beispiele: G Gruppe, $g \in G, < g > =$ die von g erzeugte zyklische Untergruppe.
G operiert auf X. Als **Stabilisator** eines Punktes $x \in X$ bezeichnet man die Menge $\text{Stab}_G(x) = \{g \in G; g \circ x = x\}$. Dies ist eine Untergruppe von G.
$G = \{e, s_x, s_y, r_\pi\}$ die Symmetriegruppe des Rechtecks operiert auf $X = \mathbb{R}^2$. $P \in \mathbb{R}^2$ in allg. Lage, dann ist $\text{Stab}_G(x) = \{e\}$, P auf einer der Achsen, dann ist $\text{Stab}_G(x) = \{1, s\}, P = 0$ dann ist $\text{Stab}_G(P) = G$.

2.5.3 Notationen und Bemerkungen

M, N Teilmengen in einer Gruppe G. Dann kann man M^{-1}, gM, Mg, $M \cdot N$ bilden. $(gM)^{-1} = M^{-1}g^{-1}$. Ist $M = H$ eine Untergruppe, dann gilt: $gH = H$ genau dann, wenn $g \in H$.
Ausserdem folgt: $H^{-1} = H$, $H = Hg$ genau dann, wenn $g \in H$, $H \cdot H = H$.
Im allgemeinen nennt man gH eine *Linksnebenklasse*, Hg eine *Rechtsnebenklasse*.

2.5.4 Satz: *Gruppe $G \supset H$ = Untergruppe.*

(i) *Die H-Linksnebenklassen sind die Äquivalenzklassen bezüglich der Relation $g_1 \sim g_2$, falls $g_1^{-1}g_2 \in H$. Die entsprechende Quotientenmenge schreibt man G/H.*

(ii) *Entsprechend sind die H-Rechtsnebenklassen die Äquivalenzklassen für $g_1 \sim g_2$, falls $g_1 g_2^{-1} \in H$. Die Quotientenmenge schreibt man $H \backslash G$.*

2.5.5 Das ergibt zwei Partitionen von G:

$$G = \bigcup_{gH \in G/H} gH, \quad G = \bigcup_{Hg \in H \backslash G} Hg.$$

Vermittels $gH \in G/H \mapsto (gH)^{-1} = Hg^{-1} \in H\backslash G$ erhält man eine Bijektion zwischen G/H und $H\backslash G$. Wenn es nur endlich viele solcher Nebenklassen gibt, dann nennt man ihre Anzahl $(G:H)$ = *Index* von H in G, und sagt: H hat endlichen Index in G.

2.5.6 Satz von Lagrange : *Es sei G endliche Gruppe, und $H \subset G$ eine Untergruppe. Dann gilt:*
$|G| = |H| \cdot (G:H)$.
Beweis: H operiert auf G fixpunktfrei. Alle Bahnen haben dieselbe Ordnung $= |H|$. Anders ausgedrückt: alle Äquivalenzklassen aus den Partitionen 2.5.5 haben dieselbe Ordnung wie die Gruppe H. Also sind in den unter 2.5.5 angegebenen Partitionen von G alle Teilmengen gleich gross.

2.5.7 Es sei G endlich und $g \in G$. Dann ist die Ordnung von g Teiler der Gruppenordnung.
Beweis: Man wendet den Satz von Lagrange an im Fall $H =< g >$ und benutzt $\#g = \# < g >$.

2.5.8 Satz: *G operiere auf X und es sei B eine Bahn, $b \in B, H = \mathrm{Stab}_G(b)$. Dann induziert die Abbildung $g \in G \mapsto g \circ b \in B$ eine Bijektion $G/H \longleftrightarrow B$, denn die Abbildung ist surjektiv und ihre Fasern sind genau die Linksnebenklassen gH.*

2.5.9 G endlich, operiere auf X. Für jede Bahn B ist dann $|B|$ Teiler von $|G|$. (Nach 2.5.8 ist $|B| = (G:H)$ und nach 2.5.6 ist dies ein Teiler von $|G|$.)

2.5.10 S_n = Gruppe der Vertauschungen von $\{x_1, \cdots, x_n\} = X$. S_n operiert auf X. Ganz X ist eine Bahn. Also:

$$n = |X| = (S_n : \mathrm{Stab}\,(x_n)) = (S_n : S_{n-1})$$
$$|S_n| = (S_n : S_{n-1})|S_{n-1}| = n|S_{n-1}|;$$

daraus folgt induktiv: $|S_n| = n!$.

2.5.11 Satz: *G = Gruppe von Primzahlpotenzordnung $|G| = p^f$ (=: eine p-Gruppe). Dann existiert ein Element $h \neq e$ in G, sodass $gh = hg \ \ \forall g \in G$.*

Der Beweis benutzt die Operation $G \times G \to G, \quad g \circ h := ghg^{-1}$. Nach 2.5.9 müssen alle Bahnen p-Potenzordnung haben. Also mindestens 2 Bahnen habe die Ordnung 1.

2.5.12 Beispiel: $G = \{r_0 = e, r_1, r_2, r_3; s_1, s_2, s_3, s_4\}$ die Symmetriegruppe des Quadrates, 4 Rotationen und 4 Spiegelungen. $|G| = 2^3$. Bezüglich der Operation $g \circ h = ghg^{-1}$ ergeben sich 5 Bahnen $\{e\}, \{r_1, r_3\}, \{r_2\}, \{s_1, s_3\}, \{s_2, s_4\}$.
Also: r_2 = Drehung um π ist mit allen anderen Elementen vertauschbar.

2.6 Normalteiler und Faktorgruppen

2.6.1 Definition und Satz über Normalteiler.

Für eine Untergruppe H von G sind folgende Eigenschaften äquivalent:

(i) $H\backslash G = G/H$, dh. jede Rechtsnebenklasse ist auch Linksnebenklasse und umgekehrt.

(ii) $gH = Hg \ \ \forall g \in G$,

(iii) $gHg^{-1} = H \ \ \forall g \in G$.

Wenn diese Eigenschaften erfüllt sind, dann nennt man H einen Normalteiler von G.

2.6.2 Wenn $H \subseteq G$ ein Normalteiler ist, dann kann man auf $H\backslash G = G/H$ eine Multiplikation einführen:

$$(g_1H) \cdot (g_2H) := g_1g_2H$$

Man nennt dann G/H mit der angegebenen Multiplikation die Faktorgruppe von G nach H.

Bemerkung: Wenn H kein Normalteiler in G ist, dann ist das Produkt von zwei Nebenklassen nicht eindeutig bestimmt. Als Beispiel betrachten wir die Diedergruppe $G = D_4$ aller Symmetrien des Quadrates und darin die Untergruppe welche aus der Identität und einer Spiegelung besteht. $G = \{r_0, \cdots, r_3, s_1, \cdots, s_4\}, \quad H = \{r_0, s_1\}$. Die Untergruppe H ist kein Normalteiler, weil $r_1Hr_1^{-1} = \{r_0, \ s_3\} \neq H$. Das Produkt der Linksnebenklassen r_1H, r_2H hat 4 Elemente: $r_1H \cdot r_3H = H \cup r_2H$, weil einerseits $r_1 \cdot r_3 = r_0 \in H$, und andererseits $(r_1s_1)r_3 = r_1(s_1r_3) = r_1(r_1s_1) = r_2s_1 \in r_2H$.

Wäre G/H tatsächlich eine Gruppe dann müssten die Klassen r_1H und r_3H zueinander invers sein, dh. es müsste $r_1H \cdot r_3H = H$ gelten.

2.6.3 Beispiel, In kommutativen Gruppen ist jede Untergruppe ein Normalteiler und man kann immer die Faktorgruppe bilden.

2.6.4 Beispiel, Im Fall der kommutativen Gruppe $(\mathbb{Z}, +)$ ergeben sich als Faktorgruppen die endlichen zyklischen Gruppen $(\mathbb{Z}/n\mathbb{Z}, +)$.

2.7 Permutationen

Wir betrachten die Gruppe S_n aller Vertauschungen der ersten n Zahlen. $S_n = S(X)$ für $X = \{1, \cdots, n\}, \pi = \begin{pmatrix} 1 & \ldots & n \\ \pi(1) & & \pi(n) \end{pmatrix}$. Die Multiplikation geschieht durch Hintereinanderausführung der Vertauschungen: $\pi \cdot \pi' := \pi \circ \pi'$. Man muss also das Produkt von rechts nach links lesen. Zuerst wird die Vertauschung π' ausgeführt und danach die Vertauschung π.

Das Inverse von π erhält man indem man die obere und untere Zeile vertauscht und die Spalten umordnet sodass in der ersten Zeile wieder die richtige Reihenfolge hergestellt wird.

2.7.1 Satz: *Die Anzahl der Vertauschungen ist $|S_n| = n!$.*

Beweis: $\pi(1) \in \{1, \cdots, n\}$ ist frei wählbar. Danach bleiben für $\pi(2) \neq \pi(1)$ noch $n-1$ Möglichkeiten. Entsprechend bleiben dann für $\pi(3)$ noch $n-2$ Möglichkeiten usw.
z.B. hat S_3 genau 6 Elemente.

2.7.2 Definition: $\varphi \in S(X)$ heißt *Zyklus*, falls es eine endliche Teilmenge $T = \{a_1, \cdots, a_k\} \subset X$ gibt, sodass die Abbildung φ wie folgt wirkt:

$$a_1 \mapsto a_2 \mapsto \cdots \mapsto a_n \mapsto a_1, \quad \varphi = (a_1, \cdots, a_n).$$

Die Teilmenge T nennen wir den *Träger* des Zyklus.
Bemerkungen: Nicht bewegte Elemente werden weggelassen, Schreibweise eines Zyklus ist nicht eindeutig, die Ordnung eines Zyklus ist gleich der Ordnung des Trägers.

Zwei Zyklen heißen *disjunkt*, wenn ihre Träger disjunkt sind.

2.7.3 Satz: *Seien π_1, π_2 disjunkte Zyklen. Dann gilt $\pi_1 \cdot \pi_2 = \pi_2 \cdot \pi_1$.*
Beweis Das Nachprüfen einer Gleichheit von Permutationen geschieht durch Anwenden beider Seiten auf Elemente $x \in X = \{1, \ldots, n\}$.

2.7.4 Satz: *Jede Permutation $\pi \in S_n, \pi \neq e$ ist ein Produkt von eindeutig bestimmten disjunkten Zyklen. Sie ergeben sich als die Bahnen der Aktion der zyklischen Gruppe $< \pi >$ auf X. Dabei sind die Bahnen der Länge 1 die Fixpunkte von π. Sie finden keine Berücksichtigung.*

2.7.5 Definition der zu $\pi \in S_n$ gehörigen Partition von n. Eine Partition von n ist eine Aufteilung in natürliche Zahlen mit der Summe n. Dabei werden die Summanden der Grösse nach geordnet oder man gibt an, mit welcher Vielfachheit k_i die einzelnen Summanden i (welche natürlich zwischen 1 und n liegen müssen) auftreten.

$$p = (n_1 \geq n_2 \geq \cdots \geq n_r) = (1^{k_1}, 2^{k_2} \cdot \cdots, n^{k_n}),$$

sodass $n = n_1 + \cdots + n_r = k_1 \cdot 1 + k_2 \cdot 2 + \cdot + k_n \cdot n$.
Jedem $\pi \in S_n$ wird nach 2.7.4 eine Partition $p(\pi)$ von n zugeordnet. $\pi \in S_n \mapsto p(\pi) \in \mathrm{Part}(n)$. Sie besteht aus den Zykellängen.
Zahl der Einsen in $p(\pi)$ = Zahl der Fixpunkte von π.

2.7.6 Das Young Diagramm einer Partition. Ist $p = (n_1 \geq n_2 \geq \cdots \geq n_r)$ eine Partition von n dann bildet man dazu ein Diagramm aus n Kreuzchen (oder Kästchen) welche in Zeilen linksbündig angeordnet werden. Dabei stehen in der i-ten Zeile n_i Kreuzchen (oder Kästchen), dh. die Länge der Zeilen nimmt nach unten hin ab und die Gesamtzahl der Kreuzchen ist gleich n.

2.7.7 Definition: Elemente in einer Gruppe G heißen *konjugiert*, $g_1 \sim g_2$, falls ein $g \in G$ existiert, sodass $g_2 = g g_1 g^{-1}$. Dies ist eine Äquivalenzrelation auf G. Die Äquivalenzklassen bezeichnet man als Konjugationsklassen.

2.7.8 Sei $\pi = (a_1, \cdots, a_k) \in S_n$ ein Zyklus, und sei $\sigma \in S_n$ eine beliebige Permutation. Dann gilt stets:

$$\sigma(a_1, \cdots, a_k)\sigma^{-1} = (\sigma(a_1), \cdots, \sigma(a_k)).$$

2.7.9 Hauptsatz: *Zwei Permutationen $\pi_1, \pi_2 \in S_n$ sind konjugierte Elemente der Gruppe S_n gdw. zu ihnen dieselbe Partition von n gehört, d.h.* $p(\pi_1) = p(\pi_2)$ im Sinne von 2.7.5.

Anwendungen des Hauptsatzes:
Wir wollen Eigenschaften E von Permutationen, sodass $E(\pi) = E(\sigma\pi\sigma^{-1})$ bereits aus der zu π gehörigen Partition ablesen. Ein Beispiel gibt der folgende Satz.

2.7.10 Satz:

(i) : In G (= Gruppe) haben konjugierte Elemente stets dieselbe Ordnung.

Der Fall $G = S_n$:

(ii) Zu $\pi \in S_n$ gehöre die Partition $p(\pi) = (n_1, \cdots, n_r)$. Dann gilt $|\pi| = \mathrm{kgV}\ (n_1, \cdots, n_r)$.

2.7.11 Definition:

$\pi \in S_n \mapsto l(\pi) :=$ Zahl der *Fehlstände* = Zahl der Paare $i < j$ mit $\pi(i) > \pi(j)$.

π heißt *primitiv*, falls $\pi = (i, i+1)$ zwei benachbarte Zahlen vertauscht.

2.7.12 Sei $\sigma = (i, i+1)$ primitiv, $\pi \in S_n$ beliebig. Dann gilt:

$$\begin{aligned} l(\pi\sigma) &= l(\pi) + 1 \quad \text{falls} \quad \pi(i) < \pi(i+1) \\ & l(\pi) - 1 \quad \text{falls} \quad \pi(i) > \pi(i+1). \end{aligned}$$

2.7.13 Hilfssatz: *$\pi \in S_n$ lässt sich schreiben als Produkt von $l(\pi)$ primitiven Permutationen. Insbesondere folgt aus $l(\pi) = 1$, dass $\pi = \sigma$ primitiv ist.* Beweis durch Induktion über $l(\pi)$. Benutze 2.7.12. Mit weniger primitiven Faktoren geht es nicht, sonst wäre die Zahl der Fehlstände zu klein.

2.7.14 Satz: *Seien $\pi_1, \pi_2 \in S_n$. Dann ist*

$$l(\pi_1\pi_2) \equiv l(\pi_1) + l(\pi_2) \bmod 2.$$

2.7.15 Definition und Satz. *Das Vorzeichen einer Permutation $sgn(\pi) = (-1)^{l(\pi)}$ hat die Eigenschaft $sgn(\pi_1\pi_2) = sgn(\pi_1) \cdot sgn(\pi_2)$.*

2.7.16 *(i) Konjugierte Permutationen haben dasselbe Vorzeichen.*

(ii) Ist $\pi = (a_1, \cdots, a_k)$ Zyklus der Länge k, dann ist $sgn(\pi) = (-1)^{k-1}$.
Zyklen der Länge 2 heißen Transpositionen. Sie haben das Vorzeichen -1.

(iii) Sei $\pi \in S_n$ und sei r die Anzahl der Bahnen bei der Aktion von $< \pi >$ auf $\{1, \cdots, n\}$. Dann ist $sgn(\pi) = (-1)^{n-r}$.

Zusatz: Andere Interpretationen von r sind:
r = Zahl der Zyklen von π + Zahl der Fixpunkte
(= Zyklen der Länge 1).
r = Anzahl der Zeilen im Young Diagramm zu π.

2.7.17 Satz: *Die Permutationen $\pi \in S_n$ mit $sgn(\pi) = 1$, d.h. $l(\pi)$ gerade, bilden eine Untergruppe A_n vom Index 2. Diese Untergruppe heißt alternierende Gruppe. Für jedes $\sigma \in S_n$ mit $sgn(\sigma) = -1$ gilt: $S_n = A_n \dot{\bigcup} A_n\sigma$.*

2.7.18 Satz: *Für $p = (1^{v_1}, 2^{v_2}, \cdots, n^{v_n})$, $\sum_{s=1}^{n} s \cdot v_s = n$ hat die Konjugationsklasse $K_p = \{\pi \in S_n | p(\pi) = p\}$ die Ordnung*

$$|K_p| = n!/(v_1! 1^{v_1})(v_2! 2^{v_2}) \cdots (v_n! n^{v_n}).$$

Insgesamt können wir aus p leicht $|K_p|$ sowie die Ordnung aller $\pi \in K_p$ und $sgn(\pi)$ ablesen.

2.8 Homomorphismen von Gruppen

2.8.1 Definition: Eine Abbildung $f : G \to H$ zwischen zwei Gruppen heißt *Homomorphismus* , falls $f(g_1 \cdot g_2) = f(g_1) \cdot f(g_2)$, d.h. f ist verträglich mit den Gruppengesetzen.

2.8.2 Satz: *Für jeden Homomorphismus $f : G \to H$ gilt:*
(i) $f(e_G) = e_H$, (ii) $f(g^{-1}) = f(g)^{-1}$.

2.8.3 Definition/Satz: Als *Kern* eines Homomorphismus $f : G \to H$ bezeichnet man

$$\mathrm{Ker}(f) = \{g \in G; f(g) = e_H\},$$

das ist die Faser von f über e_H.
Der Kern ist ein Normalteiler in G und die Fasern von f sind genau die Nebenklassen $G/\mathrm{Ker}(f)$. Der Homomorphismus f ist injektiv gdw. $\mathrm{Ker}(f) = \{e_G\}$.
Da alle Fasern eines Homomorphismus gleich gross sind, genügt zum Überprüfen der Injektivität die Betrachtung einer einzigen Faser.

2.8.4 Satz: *Sei $f : G \to H$ ein Gruppenhomomorphismus. Dann ist das Bild von f eine Untergruppe von H. Ist f bijektiv, dann ist die Umkehrabbildung f^{-1} ebenfalls ein Gruppenhomomorphismus.*

2.8.5 Definition: Bijektive Gruppenhomomorphismen $f : G \to H$ heißen *Isomorphismen*. Man schreibt dann $G \cong H$ bzw. $f : G \xrightarrow{\sim} H$.
Die Isomorphie ist eine Äquivalenzrelation, welche die Menge aller Gruppen in Isomorphieklassen teilt.

2.8.6 Beispiel für einen Isomorphismus. Die Würfelgruppe:
Sei W die Gruppe der Rotationen des $\mathbb{R}^3$, welche den Würfel mit Schwerpunkt im Koordinatenursprung in sich überführen. Alle Drehachsen gehen durch den 0-Punkt und verbinden gegenüberliegende Seitenmittelpunkte, Kantenmittelpunkte bzw. Eckpunkte miteinander. Man hat die natürliche Abbildung

$$r \in W \longmapsto \pi(r) \in S_4 = S(g_1, g_2, g_3, g_4),$$

welche einer Drehung r die Permutation der vier Raumdiagonalen zuordnet, die durch Ausführung von r verursacht wird.
$r \mapsto \pi(r)$ ist injektiv und ergibt einen Isomorphismus $W \cong S_4$.
Also gibt es 24 Drehungen des Würfels, welche den 24 Permutationen der vier Raumdiagonalen entsprechen.

2.8.7 Der Homomorphiesatz: *Sei $f : G \to H$ ein Gruppenhomomorphismus. Dann bildet die Menge der Fasern eine Gruppe $G/\mathrm{Ker}(f)$ und die Abbildung f induziert einen Isomorphismus*

$$f_* : G/\mathrm{Ker}(f) \xrightarrow{\sim} \mathrm{Bild}(f).$$

Der Beweis geht aus von der Zerlegung der Abbildung f in eine Kombination aus Surjektion, Bijektion, Injektion. Dies hatten wir ganz allgemein in 2.1.5 bemerkt.

2.8.8 Beispiel: $\exp_g : (\mathbb{Z}, +) \to < g > \subset G$.
Wenn g die Ordnung n hat, dann folgt aus 2.8.7

$$\exp_{g*} : \mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} < g > .$$

Wenn g unendliche Ordnung hat, dann:

$$\exp_g : \mathbb{Z} \xrightarrow{\sim} < g > .$$

Das Vorzeichen einer Permutation ergibt

$$sgn_* : S_n/A_n \xrightarrow{\sim} \{\pm 1\}.$$

2.8.9 Gruppenaktionen und Homomorphismen.
Seien G eine Gruppe, X eine Menge, $S(X)$ die Gruppe der Permutationen von X (d.h. Bijektionen von X auf sich). Dann erhält man Bijektionen zwischen den möglichen Operationen von G auf X und den möglichen Homomorphismen $G \to S(X)$.

Kapitel 3 Determinanten

Wir wollen in diesem Kapitel jeder quadratischen Matrix A eine Zahl $\det(A)$ zuordnen.
Der Wert dieser Bildung besteht in folgenden Ergebnissen:

(i) Eine $n \times n$ Matrix A ist invertierbar genau dann, wenn $\det(A) \neq 0$ ist.

(ii) Ein neues Verfahren zur Berechnung von A^{-1} und damit zum Lösen von LGS. (Die adjunkte Matrix)

3.1 Die Definition der Determinante

3.1.1 Begriff des Elementarproduktes für eine $n \times n$ Matrix $A = (a_{ij})$.

3.1.2 Die Leibniz'sche Definition der Determinante einer $n \times n$ Matrix A. Spezialfälle $n = 2, n = 3$. (Formel von Sarrus im Fall n=3.)

$$\det(A) = \sum_{\pi \in S_n} sgn(\pi) a_{1\pi(1)} \cdots a_{n\pi(n)}.$$

3.2 Berechnung der Determinanten durch Zeilenreduktion

3.2.1 Wenn in A eine Zeile verschwindet, dann ist $\det A = 0$.

3.2.2 Definition der oberen und unteren Dreiecksmatrizen.

3.2.3 Satz:

(i) Sei A eine obere oder untere Dreiecksmatrix, dann ist $\det(A) = a_{11} \cdots a_{nn}$ *das Produkt über die Einträge der Hauptdiagonale.*

(ii) Insbesondere gilt $\det(I_n) = 1$.

3.2.4 Satz: *Wenn in der Matrix A dieselbe Zeile zweimal auftritt, dann ist* $\det(A) = 0$.

3.2.5 Satz: *Wir betrachten eine Matrix A, wo sämtliche Einträge einer fixierten Zeile i aus 2 Summanden zusammengesetzt sind:*

$$a_{ij} = b_{ij} + c_{ij} \quad \forall j = 1, \cdots, n.$$

Wir bilden aus A die Matrizen A' bzw. A'', welche sich von A nur in der i-ten Zeile unterscheiden, nämlich:
i-te Zeile $(A') = (b_{i1}, \cdots, b_{in})$, *$i$-te Zeile* $(A'') = (c_{i1}, \cdots, c_{in})$.
Dann ist $\det(A) = \det(A') + \det(A'')$.

3.2.6 Hauptsatz: *Es sei A eine $n \times n$ Matrix.*

(i) *A' entstehe aus A durch Multiplikation einer Zeile mit einer Konstanten c. Dann ist* $\det A' = c \cdot \det A$ *(Enthält 3.2.1).*

(ii) *A' entstehe aus A durch Vertauschen von 2 Zeilen. Dann ist* $\det A' = -\det A$.

(iii) *A' entstehe aus A durch die Zeilenoperation*

$$z_{i_0}(A') = z_{i_0}(A) + c \cdot z_{j_0}(A),$$

für fixierte $i_0 \neq j_0$. Dann ist $\det A' = \det A$.

3.2.7 Als Grundeigenschaften der Determinante bezeichnen wir die Eigenschaften:

$D1$	=	3.2.6(i)	homogen in den Zeilen
Aus D 1 folgt auch 3.2.1			
$D2$	=	3.2.4	alternierend in den Zeilen
$D3$	=	3.2.5	additiv in den Zeilen.

Die Eigenschaften 3.2.6 (ii), (iii) folgen aus D_1 bis D_3.

3.2.8 Folgerung:

(i) *Es sei E eine elementare Zeilenoperation. Dann gilt* $\det(E \cdot A) = \lambda(E) \cdot \det(A)$ *mit einem Faktor $\lambda(E) \neq 0$, der nur von E, aber nicht von A, abhängt.*
Folgt aus dem Hauptsatz.

(ii) $\det(A)$ *kann mit Hilfe des Gauß Algorithmus, d.h. durch Reduktion auf Zeilenstufenform berechnet werden. Sei nämlich $E_1, \cdots, E_r$ eine Folge elementarer Zeilenop-s, sodass $A' = E_r \circ \cdots \circ E_1(A)$ Zeilenstufenform hat. Dann gilt:*

$$\det(A) = \frac{1}{\lambda(E_1) \cdot \ldots \cdot \lambda(E_r)} \cdot \det(A'),$$

und $\det(A')$ *ist das Produkt über die Hauptdiagonale, weil A' = obere Dreiecksmatrix.*

(iii) *Die Determinantenfunktion ist durch die Eigenschaften $D1, D2, D3$ und durch $D4 : \det(I_n) = 1$ vollständig bestimmt.*
Insbesondere ist $\det(A) \neq 0$ *gdw $A \sim I_n$ zeilenäquivalent zur Einheitsmatrix.*

Beweis von (iii). Aus $D1 - D3$ ergeben sich die Formeln (i), (ii). Man kann solange weitermachen, bis A' reduzierte Zeilenstufenform hat. Da A' quadratisch ist, gibt es bei reduzierter Zeilenstufenform nur zwei Alternativen
a) A' hat am Ende eine Nullzeile. Dann ist $\det A = 0$.

b) $A' = I_n$. Dann ist $\det A' = \det I_n = 1$, und aus 3.2.8(ii) folgt: $\det(A) = \dfrac{1}{\lambda(E_1)\cdot\ldots\cdot\lambda(E_r)}$.

Bemerkung: Die Existenz einer Determinantenfunktion mit den Eigenschaften $D1-D4$ ist durch die Leibniz'sche Definition gesichert. 3.2.8 (iii) besagt, dass dies die einzige derartige Funktion ist. Lässt man D4 weg, dann ist die Funktion nur eindeutig bis auf einen Proportionalitätsfaktor.

3.3 Multiplikativität

3.3.1 Hauptsatz: *Für zwei $n\times n$ Matrizen A, B gilt* $\det(AB) = \det(A)\cdot\det(B)$.

3.3.2 *A ist invertierbar genau dann, wenn* $\det(A) \neq 0$.

3.3.3 Folgerung: *Es sei $GL_n(\mathbb{R})$ die Gruppe der invertierbaren $n \times n$ Matrizen mit reellen Einträgen und $\mathbb{R}^\times$ die multiplikative Gruppe der von 0 verschiedenen reellen Zahlen. Dann ist* $\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times$ *ein Gruppenhomomorphismus. Insbesondere ist* $\det(A^{-1}) = \det(A)^{-1}$.

3.3.4 Satz: $\det(A^t) = \det(A)$.

3.3.5 Die Determinante verhält sich bei elementaren Spaltenoperationen ebenso wie bei elementaren Zeilenoperationen. Das beruht auf der Identität $[s(A)]^t = z(A^t)$ falls sich die Spaltenoperation s und die Zeilenoperation z entsprechen.

3.4 Kofaktorentwicklung, Cramersche Regel

3.4.1 Satz: *Es sei $n = n_1 + \ldots + n_r$, $A = (A^{ij})$ eine Blockmatrix mit Blöcken A^{ij} vom Format $n_i\times n_j$. A heißt obere Block-Dreiecksmatrix, falls $A^{ij} \equiv 0$ für die Blöcke mit $i > j$, und in diesem Fall gilt:*

$$\det A = \det(A^{11}) \cdot \ldots \cdot \det(A^{rr}).$$

3.4.2 Definition: $A = n\times n$ Matrix. Die *Minormatrix* $MM_{ij}(A)$ entsteht durch Wegstreichen der i-ten Zeile und der j-ten Spalte. Der i, j *Minor* ist: $M_{ij}(A) := \det(\,MM_{ij}(A))$.
Der i, j *Kofaktor* ist $C_{ij}(A) := (-1)^{i+j}M_{ij}(A)$.
Für die Determinante hat man auch die Schreibweise $\det(A) = |A|$.

3.4.3 Lemma: *Für den i, j Kofaktor von A gilt:*

$$C_{ij} = |S_1(A), \cdots, e_i, S_{j+1}(A), \cdots| \,,$$

d.h. man ersetzt die Spalte $S_j(A)$ durch den Einheitsvektor

$$e_i = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \leftarrow i - te \ \underline{Zeile} \ .$$

3.4.4 Satz: *Für A sei $C := (C_{ij})$ die Kofaktormatrix und $A^\sharp := C^t$ die Adjunkte oder komplementäre Matrix: Dann gilt:*

$$A^\sharp \cdot A = A \cdot A^\sharp = \det(A) \cdot I_n.$$

Der Beweis von $A^\sharp A = \det(A) I_n$ benutzt 3.4.3 und die Tatsache, dass die Determinante homogen und additiv in den Spalten ist. (Die Eigenschaften $D1$ bis $D3$ der Determinante gelten auch für Spalten.)
Danach beweist man $A \cdot A^\sharp = \det(A) I_n$ mit Hilfe von:

3.4.5 Lemma: *Es gilt $(A^\sharp)^t = (A^t)^\sharp$.*
Weil $A^\sharp = C(A)^t$, so bedeutet dies:

$$C(A) = (A^t)^\sharp = [C(A^t)]^t, \ d.h. \ C_{ik}(A) = C_{ki}(A^t).$$

3.4.6 Folgerung: *Wenn A invertierbar, dann ist $A^{-1} = \dfrac{1}{\det(A)} \cdot A^\sharp$.*
Ansonsten ist $A \cdot A^\# = A^\# \cdot A$ die Nullmatrix.

3.4.7 Entwicklungssatz von Laplace:

$$\det(A) = \sum\nolimits_k a_{kj} C_{kj} = \sum_k a_{ik} C_{ik}.$$

Die 1. Formel nennt man die Entwicklung nach der j-ten Spalte und die 2. Formel die Entwicklung nach der i-ten Zeile.

3.4.8 Die Cramersche Regel: Sei $AX = B$ ein LGS von n Gleichungen mit n Unbekannten und sei $\det(A) \neq 0$. Dann gilt:

$$x_i = \frac{\det(A_i)}{\det(A)} \ \text{für} \ \ i = 1, \cdots, n,$$

wobei A_i aus A entsteht, indem man die i-te Spalte durch B ersetzt.

2.9 Normalteiler, Faktorgruppen und Homomorphismen

2.10 Einige Matrizengruppen

2.10.1 Es seien G eine Gruppe und N, S zwei Untergruppen von G. Dann heisst G das *semidirekte Produkt* von N und S, falls
(i) N ist Normalteiler von G.
(ii) S ist ein Schnitt für G/N.

2.10.2 Es sei G eine Gruppe und $\omega : G \to G$ ein Homomorphismus von G in sich (=wird als Endomorphismus bezeichnet). Dann heisst ω ein Projektor, falls $\omega \circ \omega = \omega$. Kurzschreibweise: $\omega^2 = \omega$.

2.10.3 Satz: Ist G das semidirekte Produkt von N und S. Dann ist jedes $g \in G$ eindeutig darstellbar in der Form: $g = n_g \cdot s_g$, und die Abbildung $g \mapsto s_g$ ist ein Projektor von G mit dem Bild $S \subset G$.
Umgekehrt sei $\omega : G \to G$ ein Projektor mit $N := Ker(\omega)$ und $S := Bild(\omega)$. Dann ist G semidirektes Produkt von N und S.

2.10.4 Beispiel: Es seien $G \subset GL_n(\mathbb{R})$ die Gruppe der oberen Dreiecksmatrizen, $N \subset G$ der Normalteiler der oberen unipotenten Matrizen und $S \subset G$ die Untergruppe der Diagonalmatrizen. Dann ist die Vergissabbildung $\omega : G \to S \subset G$ welche alle Einträge ausserhalb der Hauptdiagonale durch 0 ersetzt, ein Projektor, also G ist das semidirekte Produkt aus N und S.

2.10.5 Beispiel: Es sei $G \subset GL_n(\mathbb{R})$ die Untergruppe der Monomialmatrizen, dh. in jeder Zeile und Spalte gibt es genau einen von Null verschiedenen Eintrag. Weiter seien $N \subset G$ der Normalteiler aller Diagonalmatrizen und $S \subset G$ die Untergruppe der Permutationsmatrizen. Dann ist die Vergissabbildung $G \to S \subset G$ welche jeden von Null verschiedenen Eintrag durch 1 ersetzt ein Projektor mit dem Kern N, und daher ist G das semidirekte Produkt von N und S.