Kapitel 1
Allgemeine lineare Gruppen

Gruppe:

Zunächst einmal ganz allgemein über Gruppen. X und Y seien Mengen, dann ist XxY das cartesische Produkt, die Menge aller geordneten Paare (x,y) mit x aus X und y aus Y. Man schreibt:

X x Y = {(x,y)|x aus X und y ausY}.

Unter einer binären Operation f auf einer Gruppe S versteht man eine Funktion :

f: S x S→S, d.h. für ein geordnetes Paar (s1, s2) mit Elementen aus S weist f ein weiteres Element aus S zu, f(s1,s2). Beispielsweise gibt es in N zwei wohlbekannte binäre Operationen: die Addition weist einem geordneten Paar (a,b) aus N den Wert a+b zu, die Multiplikation weist ein geordnetes Paar (a,b) zu ab.

DEFINITION: Eine Menge G zusammen mit einer binären Operation f:G x G →G heißt Gruppe, wenn die folgenden Bedingungen erfüllt sind:

Assoziativität: (ab)c = a(bc) (Kurzschreibweise statt f(a,b))

Es ex. eine neutrales Element e aus G, so dass für alle g aus G gilt: ea = ae = a

Es ex. ein Inverses: zu jedem a aus G gibt es ein a^{-1} aus G, so dass gilt: $aa^{-1} = a^{-1}a = e$

PROPOSITION 1: Jede Gruppe hat genau ein neutrales Element und jedes a aus G hat genau ein Inverses.

Beweis: Seien e und f neutrale Elemente: fe = e wegen f neutrales Element, fe = f wegen e neutrales Element ⇒ f=e, also genau ein neutrales Element.

Seien b und c Inverse von a: b = eb = (ca)b = c(ab) = ce = c

BEISPIELE:

- Z ist eine Gruppe bezüglich der Addition, 0 ist das neutrale Element, -a das Inverse. Keine Gruppe bezüglich der Multiplikation, da kein Inverses zu jedem z aus Z existiert
- Q\{0} ist eine Gruppe bezüglich der Multiplikation, Q bezüglich der Addition
- R bezüglich der Addition
- R^n, die Menge aller angeordneten n-Tupeln reeller Zahlen ist eine Gruppe bezüglich folgender Verknüpfung: wenn

$x = (x_1, x_2, \ldots, x_n)$ und $y = (y_1, y_2, \ldots, y_n)$, dann gilt:

$x + y = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$

Identität: 0 = (0, 0, ..., 0) und das Inverse von $x = (-x_1, -x_2, ..., -x_n)$

- S = (a, b, c). G sei die Menge aller Abbildungen f: S→S, zum Beispiel:

f(a) = b, f(b) = c, f(c) = a ist ein Element aus G. Wir definieren die Verknüpfung auf G wie folgt: wenn f und g aus G sind, so sei:

$f \circ g : S \to S$ definiert als $(f \circ g)(a) = f(g(a))$, $(f \circ g)(b) = f(g(b))$, $(f \circ g)(c) = f(g(c))$

i: S→S sei die Identität, also i(a) = a, i(b) = b, i(c) = c

Ebenso existiert ein $f^{-1} \Rightarrow$ G ist eine Gruppe, eine sogenannte symmetrische Gruppe.

Definition: Eine Gruppe heißt abelsch, wenn stets gilt ab = ba für a, b aus G. Z, R, Q und auch R^n sind abelsch.
Die symmetrische Gruppe ist nicht abelsch.

Definition: G und H seien Gruppen. Eine Funktion f: G→H heißt Homomorphismus, wenn für alle a, b aus G gilt:
f(ab) = f(a)f(b). Das bedeutet, es ist egal, ob wir beispielsweise erst a mal b rechnen und dann mit Hilfe von f abbilden, oder ob wir erst a und b in H abbilden und dann multiplizieren. Das Ergebnis ist das gleiche.

PROPOSITION 2: Ein Homomorphismus f: G→H bildet das neutrale Element auf das neutrale Element ab und Inverse auf Inverse.
Beweis: Seien e, e' die Identitäten in G und H. Es gilt:
f(e) = f(ee) = f(e)f(e) und f(e) hat ein Inverses h in H. Also:
e' = hf(e) = hf(e)f(e) = f(e). (das neutrale Element wird auf das neutrale Element abgebildet)
Für a aus G gilt:
$(f(a))^{-1}(f(a)) = e' = f(e) = f(a^{-1})f(a)$
das zeigt, dass $f(a^{-1}) = (f(a))^{-1}$
Ein Homomorphismus ist surjektiv, wenn f(G) = H. Beispielsweise wäre f: R → R² mit f(x) = (x, x) nicht surjektiv, weil f(R) nur eine diagonale Linie im R² wäre.
Aber f:R²→R mit f(x, y) = x ist ein surjektiver Homomorphismus.
Ein Homomorphismus f: G→H heißt injektiv, wenn aus f(a) = f(b) immer folgt, dass a = b ist. (Es werden nie zwei Elemente aus G auf ein und dasselbe Element aus H abgebildet).
Somit ist unser Beispiel f: R→R² injektiv!
Ein Homomorphismus, der sowohl injektiv als auch surjektiv ist, heißt Isomorphismus.

Völlig abstrakt gesehen sind zwei Gruppen, die zueinander isomorph sind, gleich.
R sei die additive Menge aller reellen Zahlen, R^+ die multiplikative Menge aller positiven reellen Zahlen. a>1 aus R. f: $R \rightarrow R^+$ definiert als: $f(x) = a^x$.
Dann ist f ein Homomorphismus, weil:
$f(x+y) = a^{x+y} = a^x a^y = f(a)f(b)$.
f ist injektiv: Sei f (x) = f (y).(Daraus müsste ja jetzt x = y folgen)
Also $a^x = a^y \Rightarrow a^{-y}a^x = a^{-y}a^y = 1$ (Inverses!) $\Rightarrow a^{x-y} = 1 \Rightarrow x-y = 0 \Rightarrow x = y$.
f ist surjektiv: y sei eine eine positive reelle Zahl, $x = \log_a y \Rightarrow a^x = y$, mit anderen Worten, jesdes y hat eine Darstellung als $a^x \Rightarrow$ f ist surjektiv!
Das heißt also, dass diese beiden Gruppen isomorph sind.

Körper, Quaternionen

Ein Körper ist eine Menge K, auf der die Multiplikation und die Addition erklärt ist und folgende Bedingungen erfüllt sind:

- „Punkt vor Strichrechnung“ a (b+c) = ab + ac
- K ist eine abelsche Gruppe, mit neutralem Element 0 bezüglich der Addition.
- K\(0) ist abelsch bezüglich der Multiplikation , mit neutralem Element 1

BEISPIELE:
Q und R sind Körper. Wir können R^2 wie folgt als einen Körper C (die komplexen Zahlen) verstehen:
(x_1, x_2) und (y_1, y_2) seien geordnete Paare reeller Zahlen, es sei:
$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2)$. Wie wir schon gesehen haben, ist somit R^2 abelsch.
Für die Multiplikation probieren wir:
$(x_1, x_2)(y_1, y_2) = (x_1y_1, x_2y_2)$ (wäre das naheliegenste). Dann wäre:
(1, 0)(0, 1) = (0, 0) Jetzt hätten wir zwei Elemente ungleich Null, deren Produkt aber gleich 0 ist. Das kann keinen Körper ergeben wegen:
PROPOSITION 3: In einem Körper K gilt stets:
Wenn a und b ungleich 0 sind, so ist auch ab ungleich 0.
Beweis: Sei a ungleich 0. Es ex. also ein a^{-1} so $a^{-1}a = 1$. Sei nun ab = 0. Also:
$a^{-1}(ab) = (a^{-1})(0) = 0$, aber ebenso:
$a^{-1}(ab) = (a^{-1}a)b = 1b = 0 \Rightarrow b = 0$.
Wie können wir jetzt aber R^2 in einen Körper verwandeln, nachdem der erste naive Versuch fehlgeschlagen ist?

Die Lösung ist, die Multiplikation wie folgt zu definieren:
(a, b)(c, d) = (ac – bd, ad + bc).
Das Nachrechen von (i) ersparen wir uns: Buchstabensalat.
Nun prüfen wir nach, dass (a, b) ungleich (0, 0) ein multiplikatives Inverses hat:
(a, b) ungleich (0, 0) $\Leftrightarrow$ $a^2 + b^2$ ungleich 0.
Die Identität ist trivialerweise (1, 0) und somit gilt:
(a, b) * $(a/(a^2+b^2), -b/(a^2+b^2)) = (1, 0)$.
Somit ist R^2 zu einem Körper geworden , welchen wir von nun an C nennen, die komplexen Zahlen. Andere Schreibweise: (a, b) = a + ib, wobei $i^2 = -1$:
$(a + ib)(c + id) = ac + aid + ibc + i^2bd = (ac-bd) + i(ad + bc)$.
Wir können R als ein Unterkörper von C ansehen, mit x aus R: x+i0.
Wir wollen die Addition und Multiplikation kurz nachrechnen:
x+y=x+i0+y+i0=(x+y)+i0
xy=(x+i0)(y+i0)=(xy)+i0

Wir haben also aus dem Körper R den Körper R^2=C gemacht und es stellt sich unweigerlich die Frage, ob wir nicht auch aus dem R^2 einen Körper R^3 machen können. Das geht nicht:
PROPOSITION 4: Die Rechenoperationen in C können nicht so ausgeweitet werden, dass R^3 zu einem Körper wird, weil:
1, i, j seien Basisvektoren, so dass jedes Element des R^3 eine eindeutige Darstellung als a+ib+jc, mit a,b,c aus R. Wenn wir die Multiplikation aus c ausweiten, müsste gelten:
ij = a+ib+jc, aber auch: $i(ij) = ia + i^2b+ijc$
$\Rightarrow$ $-j = ia-b+ijc$ $\quad -j = ia-b+(a+ib+jc)c$ $\quad -j = ia-b+ac+cib+jc^2$
Das schließt ein, dass $c^2 = -1$, aber c war ja aus R, also wird R^3 kein Feld.
Das Hauptproblem ist, dass wenn wir behaupten, dass ij im R^3 liegt, dass das nicht gut geht.

Erstaunlich ist nun aber, dass es im R^4 wieder funktioniert, allerdings nur, wenn wir unsere dritte Bedingung ändern: K ist eine Gruppe bezüglich der Multiplikation, aber sie ist nicht abelsch: wir werden noch sehen, wie das möglich ist.
Wir nehmen eine Basis 1, i, j, k für den R4 und definieren:

	1	i	j	k
1	1	i	j	k
i	i	-1	k	-j
j	j	-k	-1	i
k	k	j	-i	-1

Also ist 1 die Identität, ij=k usw…

Multiplizieren geschieht, wie man das gewohnt ist: jedes Glied der einen Klammer mal jedem Glied der anderen Klammer, zusammengefasst und z. T. ausmultipliziert und ausgeklammert gibt das dann:

(a+ib+jc+kd)(x+iy+jz+kw) = (ax-by-cz-dw) + i(ay+bx+cw-dz) + j(az+cx+dy-bw) + k (aw+bx+bz-cy).

R^4 mit dieser Multiplikation wird Schiefkörper der Quaternionen genannt (Quaternion =ein „Vierergebilde“).

Man kann leicht zeigen, dass die Multiplikation aus C hervorgeht, indem man c=0=d und z=0=w setzt.

Damit sind die veränderten Körperaxiome erfüllt, es muss nur noch gezeigt werden, dass jedes Quaternion ungleich 0 ein Inverses hat. Wenn q=a+ib+jc+kd ungleich 0 $\Rightarrow$ $a^2+b^2+c^2+d^2$ ungleich 0.

Wir setzen $q^{-1}=(a-ib-jc-kd) / (a^2+b^2+c^2+d^2)$.

Wer sich jetzt die Mühe macht, das nachzurechnen wird erhalten:

$qq^{-1} = 1 = q^{-1}q$.

Die Menge der Quaternionen wird mit H bezeichnet.

Vektoren und Matrizen

Für k aus {R, C, H} sei k^n die Menge aller geordneten n-Tupel der Elemente aus k.

Addition:

$x = (x_1,\ldots,x_n)$, $y = (y_1,\ldots,y_n)$, $x+y = (x_1+y_1,\ldots,x_n+y_n)$.

Das macht den k^n zu einer abelschen Gruppe mit der Identität $0 = (0,\ldots,0)$.

Für c aus k gelte außerdem: $cx = (cx_1,\ldots,cx_n)$.

Das macht k^n zu einem Vektorraum über k.

Eine Abbildung $f: k^n \rightarrow k^n$ ist linear, wenn sie Linearkombinationen zulässt, d.h.:

Falls c, d aus k und x, y aus k^n, dann:

f(cx + dy) = cf(x) + df(y). (*)

Speziell also: f(x + y) = f(x) + f(y), also ist eine lineare Abbildung ein Homomorphismus bezüglich der Addition im k^n.

Es gilt auch: $f(cx) = cf(x)$.
Diese beiden Bedingungen zusammen ergeben die gleiche Aussage wie (*).

PROPOSITION 5: Wenn f und g definiert als $k^n \to k^n \to k^n$ linear sind, so auch $g \circ f$.
Beweis: $(g \circ f)(cx + dy) = g(cf(x) + df(y)) = c(g \circ f)(x) + d(g \circ f)(x)$.
Definition: $M_n(k)$ ist die Menge aller nxn Matrizen mit Elementen aus k.
Wenn M so eine Matrix ist, $M=(m_{ij})$aus k, können wir eine lineare Abbildung f(M) definieren durch: $f(M)(x_1,\ldots,x_n) = (x_1,\ldots,x_n)(m_{ij})$
wobei die Matrix rechts steht, d.h. also, wir multiplizieren eine 1xn Matrix mit einer nxn Matrix und erhalten eine 1xn Matrix. Das ist linear:
Beweis: $f(M)(cx+dy) = (cx+dy)(m_{ij}) = c(x1,\ldots,xn)(m_{ij}) + d(y_1,\ldots,y_n)(m_{ij})$.
Wir nehmen Zeilenvektoren und keine Spaltenvektoren. Wir machen den H^n zu einem Vektorraum, indem wir die Skalarmultiplikation linksseitig definieren:
$c(x_1,\ldots,x_n) = (cx_1,\ldots,cx_n)$, und das ist i.A. nicht $= (x_1c,\ldots,x_nc)$.
Wenn wir Spaltenvektoren nähmen und die Matrixmultiplikation rechtsseitig definieren würden, so bekämen wir nicht immer lineare Abbildungen.
Für q, c, d aus H und x, y aus H^n schauen wir uns das Beispiel auf Seite 14 an.

Eine lineare Abbildung f ist isomorph, wenn sie injekitiv und surjektiv ist, also die gleiche Definition wie bei den Gruppen-Homomorphismen. f^{-1} ist ebenso ein linearer Isomorphismus und $f \circ f^{-1}$ = identische Abbildung = $f^{-1} \circ f$. Für die entsprechende Matrix heißt das, dass $M(f^{-1})M(f) = I = M(f)M(f^{-1})$, also ist $M(f^{-1})$ ein beidseitiges Inverses für M(f). Das bedeutet, wenn A^{-1} ein linksseitiges Inverses zu A ist, so ist es auch gleichzeitig ein rechtsseitiges Inverses.

Wir machen $M_n(k)$ in einen Vektorraum:
(I) Wenn $A = (a_{ij})$ und $B = (b_{ij})$, dann gilt:
$A+B = (a_{ij}+b_{ij})$:
(II) Wenn $A = (a_{ij})$ und c aus k, dann gilt:
$cA = (ca_{ij})$.
Das ist identisch zu dem Weg, mit dem wir den k^n zu einem Vektorraum gemacht haben, jedoch haben wir es jetzt mit n^2-tupeln zu tun.
Aber Mn(k) ist nicht nur ein Vektorraum. Ebenso gilt:
$A(B + C) = AB + AC$ und $(B + C)A = BA + CA$.

Ein solches System nennt sich Algebra. Im folgenden ist immer eine Algebra gemeint, mit einer beidseitigen Identität bezüglich der Multiplikation, bezüglich $M_n(k)$ ist das die Einheitsmatrix I.

Allgemeine lineare Gruppen

DEFINITION: A sei eine Algebra, x aus A heißt Einheit, wenn es ein y aus A gibt, so dass xy = 1 = yx, d.h., wenn ein multiplikatives Inverses existiert.

PROPOSITION 6: Wenn A eine Algebra mit einer assoziativen Multiplikation ist und U⊂A die Menge von Einheiten aus A, dann ist U eine Gruppe bezüglich der Multiplikation.

Beweis: Die Operation ist assoziativ, es existiert eine Identität und jedes Element hat ein Inverses (alles per Definition…)

DEFINITION: Die Gruppe der Einheiten der Algebra in $M_n(R)$ wird als $GL(n,R)$ bezeichnet, in $M_n(C)$ als $GL(n,C)$ und in $M_n(H)$ als $GL(n,H)$.
Diese Gruppen heißen allgemeine lineare Gruppen.

Bemerkung: A aus $M_n(k) \Leftrightarrow$ A wird repräsentiert einen Isomorphismus des k^n.

DEFINITION: G sei eine Gruppe, H eine Teilmenge von G, dann ist H eine Untergruppe von G, wenn die Rechenoperation auf G H in eine Gruppe verwandelt.

PROPOSITION 7: H ist eine Untergruppe von G, wenn H<G und:

1. x, y aus H $\Rightarrow$xy aus H
2. Identitätselement ist in H
3. x aus H $\Rightarrow x^{-1}$ aus H.

Hierbei sei kurz erwähnt, dass das das Thema dieses Kurses ist. Im weiteren Verlauf werden wir die Untergruppen dieser allgemeinen linearen Gruppen untersuchen.
Eine 1x1-Matrix über k ist lediglich ein Element von k und die Matrizenmultiplikation ist die Multiplikation in k. Somit ist:
$GL(1,R) = R\backslash\{0\}$ $GL(1,C) = C\backslash\{0\}$ $GL(1,H) = H\backslash\{0\}$
weil alle Elemente ungleich 0 Einheiten sind.
$GL(2,R)$ ist die Menge aller Einheiten im Vektorraum $M_2(R)$.
$GL(2,R) = \{(a\ b$
$c\ d)|$ a,b,c,d aus R,ad - bc ungleich 0}

Erklärung: Ist ad – bc = 0, so sind die Zeilen linear abhängig, dann gäbe es kein Inverses mehr (siehe Formel für Inverses für 2x2-Matrix: 1/(ad-bc) mal [d –b, –c a])
Für R und C gibt es Determinanten, die auf $M_n(R)$ und $M_n(C)$ definiert sind, von der linearen Algebra wissen wir:
GL(n,R) = {A aus $M_n(R)$| det A ungleich 0}
GL(n,C) = {A aus $M_n(C)$| det A ungleich 0}
Bemerkung: det A = ad-bc, falls n = 2
Angenommen, wir würden jetzt eine Determinante des $M_2(H)$ definieren durch:
det (a b
a b)= ad-bc.
Dann wäre
det (i j
i j)= k - (-k) = 2k ungleich 0.
Diese Matrix kann keine Einheit sein, denn die zugehörige lineare Abbildung würde keinen Isomorphismus darstellen, weil sie nicht injektiv ist:
(j, -j)(i j
i j) = (0, 0) Hier wird (j, -j) auf (0,0) abgebildet, bei einem Isomorphismus wird aber nur das neutrale Element auf das neutrale Element abgebildet, kein weiteres Element, aus f(x)=f(y) folgt nicht x=y!

PROPOSITION 8: f: G→H sei ein Homomorphismus von Gruppen. Dann ist f (G) eine Untergruppe von H.

Beweis: f(id) = id (siehe PROP. 2), also enthält G das Identitätselement von H.
Wenn x, y aus f(G) sind, so gibt es a, b aus G, so dass f(a)=x, f(b)=y. Dann:
xy = f(a)f(b) = f(ab) aus G (Homomorphismus)
Und zuletzt: x aus f(G), dann x = f(a), und somit $x^{-1} = f(a^{-1})$ aus f(G).
⇒ f(G) ist eine Untergruppe von H.

Wenn f: G→H ein injektiver Homomorphismus ist, so ist f ein Isomorphismus von G bezüglich der Untergruppe f(G) von H, also können wir auch G als eine Untergruppe von H ansehen. Wir konstruieren einen injektiven Homomorphismus:
f: GL(n,H)→GL(2n,C).
und dann werden wir A aus GL(n,H) die Determinante von f(A) zuweisen.
Wir beginnen mit g: H→$M_2(C)$ sei gegeben durch:
g(x+iy+jz+kd) = (x+iy -z-iw
z-iw x-iy)

LEMMA 9:

(i) $g(a+b) = g(a) + g(b)$

(ii) $g(ab) = g(a)g(b)$

(iii) g ist injektiv

Die Beweise dazu lassen wir aus Zeitgründen weg; sie sind aber nicht so schwer.

Nun sei A aus $M_n(H)$ und es sei $f(A) = (g(a_{ij}))$, d.h. f(A) ist die komplexe 2n x 2n Matrix, dessen 2 x 2 Block in der ij Position $g(a_{ij})$ ist.

LEMMA 10:

$f(AB) = f(A)f(B)$.

Beweis: Sei A = (auv), B = (buv). Dann gilt:

$(AB)ij = a_{i1}b_{1j}+\ldots+a_{in}b_{nj}$. Wegen Lemma 9 gilt weiter: (ii)

$(f(AB)ij) = g(a_{i1})g(b_{1j})+\ldots+g(a_{in})g(b_{nj})$

und das ist ja genau der ij-te Eintrag in f(A)f(B).

Nun sei A aus GL(n,H), also gibt es ein A^{-1} aus GL(n,H) mit $AA^{-1} = I = A^{-1}A$. Dann hat f(A) ein $f(A^{-1}) = (f(A))^{-1}$, so dass f(A) nicht singulär ist, d.h. det f(A) ungleich 0.

regulär: Rang A = n, andernfalls singulär!

Umgekehrt, det f(A) ungleich 0. Dann existiert $(f(A))^{-1}$ und da f(GL(n,H)) eine Untergruppe von GL(2n,C) ist (PROP. 8), bekommen wir heraus, dass $(f(A))^{-1}$ aus f (GL(n,H)).

Also gibt es ein A^{-1} aus GL(n,H), für das gilt $f(A^{-1}) = (f(A))^{-1}$. Dann:

$f(AA^{-1}) = I$ und f ist injektiv, folglich $AA^{-1} = I$. Also ist A nicht singulär.