Einführung in die Algebra
2. Übung
Lösungsvorschlag

Gruppenübung

G 5 (Normalteiler und Homomorphiesatz für Gruppen)

Es sei $f : G \to H$ ein Homomorphismus und N ein Normalteiler von G, der in $\ker f$ enthalten ist. Die Quotientenabbildung $G \to G/N$ sei mit π bezeichnet.

Zeige, dass es eine eindeutig bestimmte Abbildung $\overline{f} : G/N \to H$ gibt, so dass $f = \overline{f} \circ \pi$. Weiterhin zeige, dass folgende Aussagen richtig sind:

1. $\overline{f}$ ist ein Gruppenhomomorphismus.
2. Seien $\sim_\pi$ und $\sim_f$ die den obigen Faktorstrukturen zugeordneten Kongruenzrelationen. Dann gilt $N \subset ker\, f$ genau dann, wenn $a \sim_\pi b \Rightarrow a \sim_f b$.
3. $\overline{f}$ ist injektiv genau dann wenn $N = \ker f$.

Wir betrachten die konforme Gruppe $G = CO(n, \mathbb{R})$ bestehend aus Paaren (A, b), $A \in GL_n(\mathbb{R})$, $AA^T = I$, $b \in \mathbb{R}^n$, welche durch Operation auf $\mathbb{R}^n$ definiert ist:

$$\begin{array}{rcl} (A,b) : \mathbb{R}^n & \to & \mathbb{R}^n \\ v & \mapsto & Av + b. \end{array}$$

Sei $f : G \to \mathbb{R}\backslash\{0\}$ der Homomorphismus $f : (A, b) \mapsto \det(A)$ und $N = \{(I, b) \in G \mid b \in \mathbb{R}^n\}$.

1. Identifiziere die Quotientenabbildung $\pi : G \to G/N$.
2. Konstruiere $\overline{f}$ wie oben definiert.
3. Was sind die geometrischen Bedeutungen dieser Definitionen?

- *Zunächst definieren wir eine Abbildung $\overline{f}$ und zeigen dann, dass sie die geforderten Eigenschaften hat:*

$$\begin{array}{rccc} \overline{f} : & G/N & \longrightarrow & H \\ & gN & \longmapsto & f(g) \end{array}$$

Die Abbildung ist wohldefiniert, d.h. das Bild von gN ist unabhägig von dem gewählten Element der Restklasse:
Für beliebiges $n \in N$ gilt $f(gn) = f(g)f(n) = f(g) \cdot e = f(g)$ wegen $N \subseteq \ker f$.
Weiterhin gilt $\overline{f} \circ \pi(g) = \overline{f}(gN) = f(g)$ für alle $g \in G$, also $\overline{f} \circ \pi = f$.

1. *Nun zeigen wir, dass $\overline{f}$ ein Homomorphismus ist:*

$$\overline{f}(gN \cdot hN) = \overline{f}(ghNh^{-1} \cdot hN) = \overline{f}(ghN) = f(gh) = f(g)f(h) = \overline{f}(gN)\overline{f}(hN).$$

2. *$N \subset ker\, f$ bedeutet $x \in N \Rightarrow f(x) = 1$ was äquivalent ist zu $x \in yN \Rightarrow f(x) = f(y)$ für jedes $y \in G$. Die Quotientenabbildung ist aber gerade $\pi : x \mapsto xN$. Also $a \sim_\pi b \Rightarrow a \sim_f b$.*
3. *Die Abbildung $\overline{f}$ ist injektiv genau dann, wenn N die einzige Restklasse ist, die auf 1 abgebildet wird. Wegen $1 = \overline{f}(gN) = f(g)$ ist dies genau dann der Fall, wenn alle $g \in \ker f$ auch Elemente von N sind, also $N = \ker f$.*

- *Zunächst müssen wir einsehen, dass $CO(n)$ eine Gruppe ist. Die Multiplikation ist wegen der Gruppenwirkung gegeben durch*

$$(A, b)(B, c) = (AB, Ac + b)$$

Das Inverse $(A, b)^{-1}$ ist gegeben durch $(A^{-1}, -A^{-1}c)$.

1. *π vermittelt $x \mapsto xN$, also $(A, b) \mapsto \{(A, Ac + b) \mid c \in \mathbb{R}^n\} = \{(A, c) \mid c \in \mathbb{R}^n\}$ da A eine Bijektion vermittelt, also insbesondere surjektiv ist.*
2. *Damit ist $\overline{f} : G/N \to H$ gegeben durch $\{(A, c) \mid c \in \mathbb{R}^n\} \mapsto \det A$*
3. *$kerf$ sind die Drehungen und Translationen und N nur die Translationen.*

G 6 (Rechnen mit Kongruenzen)

1. Bestimmen Sie $0 \leq x < 7$, sodass

$$x \equiv (10^{27} + 666) \cdot 27^{10} \pmod 7.$$

2.* Es seien p und q zwei verschiedene Primzahlen. Zeige, dass für ganze Zahlen m und n stets gilt

$$m \equiv n \mod p \quad \text{und} \quad m \equiv n \mod q \qquad \Longleftrightarrow \qquad m \equiv n \mod pq.$$

Was bleibt von dieser Aussage richtig, wenn p und q beliebige natürliche Zahlen sein dürfen?

-

$$10^{27} \equiv 3^{27} = 3^{3 \cdot 9} = (3^3)^9 \equiv (-1)^9 = -1$$

$$666 = 777 - 111 \equiv -111 \equiv -41 \equiv 1$$

$$27^{10} \equiv (-1)^{10} = 1$$

$$(10^{27} + 666)27^{10} \equiv (-1 + 1)1 = 0$$

- *Die Richtung "$\Rightarrow$" ist trivial, denn*

$$m \equiv n \mod pq \quad \Longrightarrow \quad pq \,|\, m - n \quad \Longrightarrow \quad p \,|\, m - n \;\; \text{und} \;\; q \,|\, m - n.$$

Dass die Umkehrung für zwei verschiedene Primzahlen p und q richtig ist, sehen wir folgendermaßen:

$$m \equiv n \mod p \quad \Longrightarrow \quad p \,|\, m - n \quad \Longrightarrow \quad (\exists k \in \mathbb{Z})\, m - n = pk.$$

Aus $q \neq p$ folgt wegen der Primzahleigenschaft $q \not| p$. Zusammen mit $q \,|\, m - n = pk$ impliziert, dass $q \,|\, k$ und somit $k = ql$ mit einer geeigneten Zahl $l \in \mathbb{Z}$. Damit erhalten wir nun

$$m - n = pql \quad \Longrightarrow \quad pq \,|\, m - n \quad \Longrightarrow \quad m \equiv n \mod pq.,$$

Die Umkehrung gilt nicht für beliebige natürliche (Prim-)Zahlen p und q:

$$\begin{array}{llllll} 17 \equiv 5 \mod 4 & \textit{und} & 17 \equiv 5 \mod 6, & \textit{aber} & 17 \not\equiv 5 \mod 24. \\ 12 \equiv 2 \mod 5 & \textit{und} & 12 \equiv 2 \mod 5, & \textit{aber} & 12 \not\equiv 2 \mod 25. \end{array}$$

G 7 (Polynomdivision über Restklassenringen)

Wir rechnen mit Koeffizienten in $\mathbb{Z}/2\mathbb{Z}$.
Ist $x^2 + x + 1$ ein Teiler von $x^6 + 1$?

Ja!

G 8 (Ideale in Polynomringen)

Sei ϕ ein Endomorphismus des Vektorraumes V. Zeige das $I(\phi) := \{p \in F[x] : p(\phi) = 0\}$ ein Ideal in $\mathbb{F}[x]$ ist.

$I(\phi) \neq 0$ as $0 \in I(\phi)$, and $I(\phi)$ is closed under addition, $p, q \in I(\phi)$ then $p(\phi) + q(\phi) = 0$ and so $p + q \in I(\phi)$, and is closed under multiplication with arbitrary $r \in \mathbb{F}[x]$, $p \in I(\phi), r \in \mathbb{F}[x]$ then $qr(\phi) = q(\phi)r(\phi) = 0r(\phi) = 0$ and so $qr \in I(\phi)$.

Hausübung

H 5 (Eigenschaften endlicher Gruppen)

Es sei G eine Gruppe der Ordnung $2q$, wobei q eine ungerade Zahl ist. Zeige, dass G ein Element der Ordnung 2, d.h. ein Element $a \neq 0$, für das $a^2 = 1$ gilt, besitzt. Betrachte dazu die Abbildung $G \to G$, die jedem Element sein Inverses zuordnet.

Die Abbildung $\iota : G \to G$, $g \mapsto g^{-1}$, ist eine Permutation der Menge G, denn $\iota^2 = \iota \circ \iota$ ist die identische Abbildung auf G und somit ist ι invertierbar. Damit ist ι ein Element von S_G der Ordnung zwei, und enthält eine Darstellung von ι als Produkt elementfremder Zyklen nur Zyklen der Längen eins und zwei. Schreibt man dabei auch alle einelementigen Zyklen auf, so muss jedes der $2q$ Gruppenelemente genau einmal in einem der Zyklen vorkommen. Da das Einselement e unter ι auf sich selbst abgebildet wird, steht e als einelementiger Zyklus (e) da. Die anderen $2q-1$ Elemente können nicht alle in Transpositionen unterkommen, denn wegen der ungeraden Anzahl bleibt mindestens ein Element g in einem weiteren einelementigen Zyklus (g) übrig. Nach Definition von ι bedeutet das aber gerade $g = \iota(g) = g^{-1}$ bzw. $g^2 = e$, also ist g das gesuchte Element der Ordnung zwei.

H 6 (Rechnenregeln für Normalteiler)

Es seien N_1 und N_2 Normalteiler von G. Zeige:

1. $N_1 \cap N_2$ ist ein Normalteiler von G.
2. $N_1 N_2$ ist ein Normalteiler von G.
3. Ist U eine Untergruppe von G, so ist $NU = \{nu \mid n \in N, u \in U\}$ eine Untergruppe von G.

1. *Wir müssen zegen, dass für jedes Element n aus $N_1 \cap N_2$ und jedes Element g aus G auch $g^{-1}ng$ in $N_1 \cap N_2$ liegt.*
   Dies folgt daraus, dass n ein Element aus N_1 und N_2 ist und damit $g^{-1}ng$ wieder in N_1 und N_2 liegt.
2. *N_1N_2 ist die Menge $\{n_1n_2 \mid n_1 \in N_1, n_2 \in N_2\}$. Wie zeigen zunächst, dass N_1N_2 eine Untergruppe ist.*
   Um die Abgeschlossenheit bezüglich der Multiplikation zu zeigen, seien $x_1, x_2 \in N_1$ und $y_1, y_2 \in N_2$. Dann ist $y_1x_2y_1^{-1}$ wieder ein Element aus N_1, weil N_1 Normalteiler ist. Damit erhalten wir:

   $$x_1y_1 \cdot x_2y_2 = x_1 \underbrace{y_1x_2y_1^{-1}}_{\in N_1} \cdot \underbrace{y_1y_2}_{\in N_2} \in N_1N_2.$$

   Es seien $x \in N_1$ und $y \in N_2$. Dann ist auch $y^{-1}x^{-1}y \in N_1$, weil N_1 Normalteiler ist. Damit folgt

   $$(xy)^{-1} = y^{-1}x^{-1} = \underbrace{y^{-1}x^{-1}y}_{\in N_1} \cdot y^{-1} \in N_1N_2.$$

   Dies zeigt, dass zu jedem Element xy auch sein Inverses in N_1N_2 liegt.
   Beachte, dass wir bisher nur benutzt haben, dass N_1 ein Normalteiler ist und N_2 eine Untergruppe.
   Nun ist noch zu zeigen, dass mit xy aus N_1N_2 und $g \in G$ auch $g^{-1}(xy)g = g^{-1}xg \cdot g^{-1}yg$ ein Element von N_1N_2 ist. Dies ist jedoch offenbar, da N_1 und N_2 Normalteiler sind und daher $g^{-1}xg \in N_1$ und $g^{-1}yg \in N_2$.

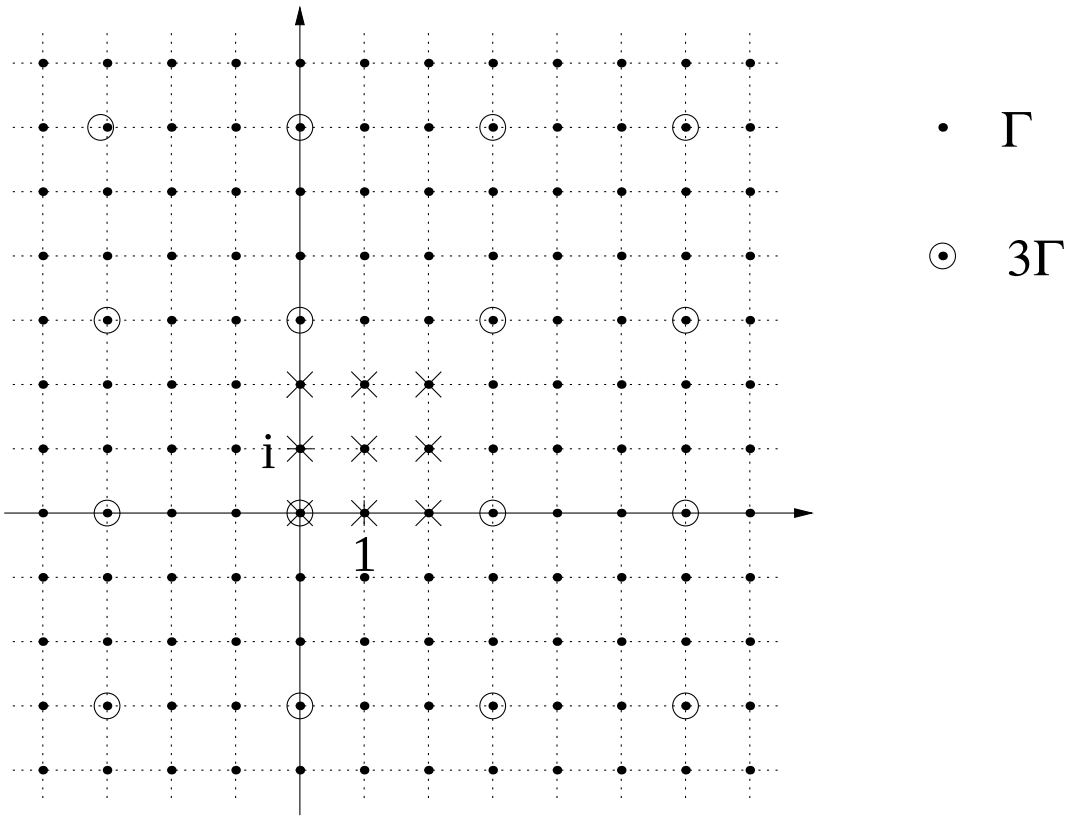
3. Die folgt mir $N = N_1$ und $U = N_2$ aus dem ersten Teil der Rechnung unter b).

H 7 (Gauß'sche Zahlen)

Es sei Γ der Ring der ganzen Gauß'schen Zahlen und $3\Gamma = \{3(a+bi) \mid a, b \in \mathbb{Z}\}$.

1. Skizziere Γ und 3Γ in der komplexen Zahlenebene. Zeige, dass 3Γ ein Ideal von Γ ist.
2. Gib die Kongruenzklassen der durch 3Γ definierten Kongruenzrelation an.
3. Beschreibe die Elemente des Faktorrings $\Gamma/3\Gamma$ und erstelle Verknüpfungstafeln für die Addition und die Multiplikation.
4. Ist $\Gamma/3\Gamma$ ein Körper?

1. Wir skizzieren Γ und 3Γ:



Die Teilmenge 3Γ ist eine Untergruppe von Γ bezüglich der Addition wegen

- $0 = 3 \cdot 0 \in 3\Gamma$,
- *für* $3(u+iv), 3(x+iy) \in 3\Gamma$ *gilt* $3(u+iv) + 3(x+iy) = 3(u+x+i(v+y)) \in 3\Gamma$,
- *und für* $3(u+iv) \in 3\Gamma$ *gilt* $-3(u+iv) = 3(-u-iv) \in 3\Gamma$.

Es handelt sich sogar um ein Ideal, da für alle $(u+iv) \in \Gamma$ und $3(x+iy) \in 3\Gamma$ gilt:

$$(u+iv) \cdot 3(x+iy) = 3ux - 3vy + i(3uy + 3vx) = 3(ux - vy + i(uy + vx)) \in 3\Gamma.$$

2. Die Kongruenzklassen sind von der Form

$$x + iy + 3\Gamma = \{u + iv \in \Gamma : u \equiv x, v \equiv y \,(\mathrm{mod}\ 3)\},$$

wobei wir alle neun verschiedenen bekommen z.B. für $x, y \in \{0, 1, 2\}$. In der Skizze oben entspricht das den durch Kreuzen gekennzeichneten Repräsentanten für die verschiedenen Klassen.

3. *$\Gamma/3\Gamma$ besteht aus den neun Kongruenzklassen, die wir in b) beschrieben haben. Wir rechnen in $\Gamma/3\Gamma$, indem wir Repräsentanten einer Klasse in Γ addieren bzw. multiplizieren und das Ergebnis modulo 3Γ wieder auf einen unserer Repräsentanten reduzieren. In den folgenden Tabellen für die Addition und Multiplikation schreiben wir nur die Repräsentanten, obwohl wir eigentlich die Klassen aufführen müssten:*

$+$	0	i	$2i$	1	$1+i$	$1+2i$	2	$2+i$	$2+2i$
0	0	i	$2i$	1	$1+i$	$1+2i$	2	$2+i$	$2+2i$
i	i	$2i$	0	$1+i$	$1+2i$	1	$2+i$	$2+2i$	2
$2i$	$2i$	0	i	$1+2i$	1	$1+i$	$2+2i$	2	$2+i$
1	1	$1+i$	$1+2i$	2	$2+i$	$2+2i$	0	i	$2i$
$1+i$	$1+i$	$1+2i$	1	$2+i$	$2+2i$	2	i	$2i$	0
$1+2i$	$1+2i$	1	$1+i$	$2+2i$	2	$2+i$	$2i$	0	i
2	2	$2+i$	$2+2i$	0	i	$2i$	1	$1+i$	$1+2i$
$2+i$	$2+i$	$2+2i$	2	i	$2i$	0	$1+i$	$1+2i$	1
$2+2i$	$2+2i$	2	$2+i$	$2i$	0	i	$1+2i$	1	$1+i$

$\cdot$	0	i	$2i$	1	$1+i$	$1+2i$	2	$2+i$	$2+2i$
0	0	0	0	0	0	0	0	0	0
i	0	2	1	i	$2+i$	$1+i$	$2i$	$2+2i$	$1+2i$
$2i$	0	1	2	$2i$	$1+2i$	$2+2i$	i	$1+i$	$2+i$
1	0	i	$2i$	1	$1+i$	$1+2i$	2	$2+i$	$2+2i$
$1+i$	0	$2+i$	$1+2i$	$1+i$	$2i$	2	$2+2i$	1	i
$1+2i$	0	$1+i$	$2+2i$	$1+2i$	2	i	$2+i$	$2i$	1
2	0	$2i$	i	2	$2+2i$	$2+i$	1	$1+2i$	$1+i$
$2+i$	0	$2+2i$	$1+i$	$2+i$	1	$2i$	$1+2i$	i	2
$2+2i$	0	$1+2i$	$2+i$	$2+2i$	i	1	$1+i$	2	$2i$

4. *Da 3Γ ein Ideal von Γ ist, ist der Quotient $\Gamma/3\Gamma$ ein kommutativer Ring mit den in c) explizit ausgeschriebenen Additions- und Multiplikationstafeln. An der Tafel für die Multiplikation lesen wir ab, dass jedes von Null verschiedene Element invertierbar ist, denn in jeder Zeile bzw. Spalte der von Null verschiedenen Elemente findet sich eine 1. Damit ist $\Gamma/3\Gamma$ ein Körper, und zwar einer mit neun Elementen. So einen hatten wir bislang nicht gesehen.*

H 8 (Ideale in Matrizenringen)

Beweise, dass der Ring $R := M(n \times n, \mathbb{K})$ der $n \times n$-Matrizen mit Einträgen in einem Körper $\mathbb{K}$ nur die trivialen Ideale $\{0\}$ und R enthält. Ist der Matrizenring R ein Körper?

Hinweis: Aufgabe H4

- *Seien E_{ij} und $P_{ki} = E - E_{kk} - E_{ii} + E_{ki} + E_{ik}$ wie in Aufgabe H4. Dann ist $E_{ij}E_{kl} = \delta_{jk}E_{il}$. Damit ist:*

$$\begin{aligned} E_{ii}AE_{jj} &= E_{ii}\left(\sum_{k,l} a_{kl}E_{kl}\right)E_{jj} = \sum_{k,l} a_{kl}E_{ii}E_{kl}E_{jj} = \sum_{k,l} a_{kl}\delta_{ik}E_{il}E_{jj} \\ &= \sum_{k,l} a_{kl}\delta_{ik}\delta_{jl}E_{ij} = a_{ij}E_{ij} \end{aligned}$$

und weiter

$$\begin{aligned} P_{ki}E_{ij}P_{jl} &= (E - E_{kk} - E_{ii} + E_{ki} + E_{ik})E_{ij}(E - E_{jj} - E_{ll} + E_{jl} + E_{lj}) \\ &= (E_{ij} - \delta_{ki}E_{kj} - E_{ij} + E_{kj} + \delta_{ki}E_{ij})(E - E_{jj} - E_{ll} + E_{jl} + E_{lj}) \\ &= E_{kj}(E - E_{jj} - E_{ll} + E_{jl} + E_{lj}) \\ &= E_{kj} - E_{kj} - \delta_{jl}E_{kl} + E_{kl} + \delta_{jl}E_{kj}) \\ &= E_{kl}. \end{aligned}$$

Anschaulich vertauscht Linksmultiplikation mit P_{ki} gerade die i-te und k-te Zeile, macht also aus E_{ij} mit der Eins an Position (i,j) gerade E_{kj} mit der Eins an Position (k,j). Rechtsmultiplikation mit P_{jl} vertauscht die j-te und l-te Spalte, liefert also E_{kl}.

- *Linksmultiplikation mit $S(x)$ multipliziert alle Einträge der Matrix mit x.*
- *Ist $A = (a_{ij})_{i,j} \neq 0$ Element eines Ideals I von R, so gibt es insbesondere eine Position (i,j) mit $a_{ij} \neq 0$. Dann sind auch $E_{ii}AE_{jj} = a_{ij}E_{ij}$, $S(a_{ij}^{-1})(a_{ij}E_{ij}) = E_{ij}$ und $P_{ki}E_{ij}P_{jl} = E_{kl}$ für alle k,l Elemente des Ideals I, weil I bezüglich Linksmultiplikation und Rechtsmultiplikation mit beliebigen Matrizen aus R abgeschlossen ist.*

  Ist nun $B = (b_{kl})_{k,l}$ eine beliebige Matrix, so zeigt

  $$B = \sum_{k,l} b_{kl}E_{kl} = \sum_{k,l} S(b_{kl})E_{kl}$$

  sogar $B \in I$, weil die Elementarmatrizen E_{kl} alle in I liegen, damit auch die Produkte $S(b_{kl})E_{kl}$ und deren Summe. Das zeigt $I = R$.

Der Matrizenring $M(n \times n, \mathbb{K})$ ist genau dann ein Körper, wenn $n = 1$ ist. Andernfalls existieren nilpotente Elemente, wie z.B. E_{1n}, d.h. $E_{1n}^2 = 0$.

Abgabe der Hausübungen: Am 11./12. Mai und 18./19. Mai 2010 zu Beginn der Übung.