Übungsblatt 7: Gruppen und Normalformen

1. ABELSCHE GRUPPEN

1.1. Sei $\nu(n)$ die Anzahl der Isomorphieklassen abelscher Gruppen der Ordnung n.

(a) ν ist multiplikativ, d.h. $\nu(nm) = \nu(n)\nu(m)$ für $\mathrm{ggT}(n,m) = 1$.

(b) Sei $p(k) = \#\{(a_1,\dots,a_m) : m \in \mathbb{N}, 1 \le a_1 \le \dots \le a_m, \sum_{i=1}^m a_i = k\}$ die Anzahl der Partitionen von $k \in \mathbb{N}$. Für Primzahlen q gilt $\nu(q^k) = p(k)$.

(c) Bestimmen Sie die Anzahl der Isomorphieklassen abelscher Gruppen der Ordnung n, für alle $n \le 60$.

(d) Man bestimme alle abelschen Gruppen der Ordnung 8000 bis auf Isomorphie.

Lösungshinweise: —

(a) *Nach dem Elementarteilersatz kann man jede abelsche Gruppe G der Ordnung nm mit $ggT(n,m) = 1$ eindeutig in zwei Gruppen $G = G_n \times G_m$ der Ordnungen n und m zerlegen. Die Anzahl solcher Gruppen G ist also das Produkt der Anzahlen für G_n und G_m, was zu zeigen ist.*

(b) *Die Potenz q^k kann auf verschiedene Weisen in $q^k = q^{k_1} q^{k_2} \cdots q^{k_m}$ zerlegt werden. Fordert man, dass die k_i der Größe nach geordnet sind, so ist die Zerlegung eindeutig durch die Zahlen k_i festgelegt und die Anzahl solcher Zerlegungen ist gerade $p(k)$. Andererseits hat eine abelsche Gruppe der Ordnung q^k nach Lagrange nur Elemente der Ordnung q^i und somit eine Darstellung der Form $\mathbb{Z}/q^{j_1} \times \mathbb{Z}/q^{j_2} \times \cdots \times \mathbb{Z}/q^{j_r}$. Die Ordnung dieser Gruppe ist $q^{j_1+\dots+j_r} = q^k$. Also muss $(j_1, j_2, \dots, j_r)$ auch eine Partition von k sein, wenn man die j_i der Größe nach anordnet (dies ist möglich, da $G \times H \cong H \times G$ gilt). Alle so entstehenden Gruppen sind nach dem Elementarteilersatz unterschiedlich, also ist $\nu(q^k) = p(q^k)$.*

(c) *Da die Primfaktoren der Zahlen bis 60 maximal Exponent 5 haben $(32 = 2^5)$, reicht es $p(1) = 1, p(2) = 2, p(3) = 3, p(4) = 5$ und $p(5) = 7$ zu kennen. Damit und mit den Teilen (a) und (b) kann man die ganze Liste schnell erstellen.*

(d) *Es ist $8000 = 2^6 \cdot 5^3$. Die Gruppen der Ordnung 64 sind: $\mathbb{Z}/64, \mathbb{Z}/2 \times \mathbb{Z}/32, \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/16, (\mathbb{Z}/2)^3 \times \mathbb{Z}/8, (\mathbb{Z}/2)^4 \times \mathbb{Z}/4, (\mathbb{Z}/2)^6, (\mathbb{Z}/2)^2 \times (\mathbb{Z}/4)^2, \mathbb{Z}/2 \times \mathbb{Z}/4 \times \mathbb{Z}/8, (\mathbb{Z}/4)^3, \mathbb{Z}/4 \times \mathbb{Z}/16$ und $\mathbb{Z}/8 \times \mathbb{Z}/8$, entsprechend den Partitionen $6 = 1+5 = 1+1+4 = 1+1+1+3 = 1+1+1+1+2 = 1+1+1+1+1+1 = 1+1+2+2 = 1+2+3 = 2+2+2 = 2+4 = 3+3$.*
Die Gruppen der Ordnung 125 sind $\mathbb{Z}/5 \times \mathbb{Z}/5 \times \mathbb{Z}/5, \mathbb{Z}/2 \times \mathbb{Z}/25$ und $\mathbb{Z}/125$, entsprechend den Zerlegungen $1+1+1 = 1+2 = 3$. Alle Gruppen der Ordnung 8000 ergeben sich durch Kombination aller Möglichkeiten aus den beiden Listen. Also insgesamt $11 \cdot 3 = 33$ Gruppen.

—

1.2. Man formuliere und beweise, in welchem Sinne die Zerlegung in unzerlegbare abelsche Gruppen maximal ist. Man formuliere und beweise, in welchem Sinne die Zerlegung in Elementarteilerform minimal ist.

Lösungshinweise: — *Eine Gruppe der Form $\mathbb{Z}/p^k$ kann nicht mehr in der Form $G \times H$ für nichttriviale Gruppen G, H geschrieben werden. Denn nach Lagrange hätten diese die Ordnungen p^i und p^j mit $i + j = k$. In $G \times H$ hätte dann jedes Element höchstens die Ordnung $\max\{p^i, p^j\} < p^k$. In $\mathbb{Z}/p^k$ hat aber die 1 Ordnung p^k, so dass $\mathbb{Z}/p^k$ nicht zu $G \times H$ isomorph sein kann. Also ist die Zerlegung in Gruppen der Form $\mathbb{Z}/p^k$ maximal in dem Sinne, dass man nicht mehr Faktoren haben kann.*
Die Elementarteilerform ist eine der Formen mit minimaler Faktorenzahl, da für $d_1 \mid \cdots \mid d_m$ alle Zahlen einen gemeinsamen Primteiler p besitzen und somit enthält $\mathbb{Z}/d_i$ stets eine Untergruppe, die zu $\mathbb{Z}/p^{e_i}$ isomorph ist. Diese können nach obigen Überlegungen nicht weiter zusammengefasst werden, so dass man nicht mit weniger als m Faktoren auskommt. —

1.3. Die Gruppen $\mathbb{Z}/_5^\times$ und $\mathbb{Z}/_8^\times$ und $\mathbb{Z}/_{12}^\times$ sind alle der Ordnung 4. Man finde ihre Darstellung in Normalteilerform bzw. ihre Zerlegung in unzerlegbare Gruppen.

Lösungshinweise: — *Es gibt nur die beiden Möglichkeiten $\mathbb{Z}/_4$ und $\mathbb{Z}/_2 \times \mathbb{Z}/_2$.*
$\mathbb{Z}/_5^\times \cong \mathbb{Z}/_4$, weil das Element 2 Ordnung 4 hat.
$\mathbb{Z}/_8^\times \cong \mathbb{Z}/_2 \times \mathbb{Z}/_2$, weil jedes Element Ordnung 2 hat.
$\mathbb{Z}/_{12}^\times \cong \mathbb{Z}/_2 \times \mathbb{Z}/_2$, weil jedes Element Ordnung 2 hat —

S 1.4. (2 Punkte) Zeigen Sie, dass die folgenden Aussagen äquivalent sind:
(a) Die Gruppe G ist abelsch.
(b) Für alle $n \in \mathbb{Z}$ ist $\varphi_n : G \to G, g \mapsto g^n$ ein Gruppenhomomorphismus.
(c) Die Abbildung $\varphi_{-1} : G \to G, g \mapsto g^{-1}$ ist ein Gruppenhomomorphismus.
(d) Die Abbildung $\varphi_2 : G \to G, g \mapsto g^2$ ist ein Gruppenhomomorphismus.

Lösungshinweise: — *$(a) \Rightarrow (b)$: Wegen der Kommutativität gilt $\varphi_n(gh) = (gh)^n = g^n h^n = \varphi_n(g)\varphi_n(h)$.*
$(b) \Rightarrow (c)$ und $(b) \Rightarrow (d)$: klar.
$(c) \Rightarrow (a)$: Es gilt $(gh)^{-1} = g^{-1}h^{-1}$ für alle $g,h \in G$ nach Voraussetzung. Ausrechnen liefert (a).
$(d) \Rightarrow (a)$: Es gilt $(gh)^2 = g^2h^2$. Ausrechnen und Kürzen ergibt wieder (a). —

2. Untergruppen und Normalteiler

Seien im Folgenden G, H Gruppen und $U, V < G$ Untergruppen.

2.1. Wenn $U \cup V$ eine Untergruppe ist, dann gilt schon $U \subset V$ oder $V \subset U$.

Lösungshinweise: — *Angenommen es gilt nicht $U \subset V$, dann gibt es ein $u \in U \backslash V$. Für alle $v \in V$ folgt dann $uv \in U \cup V$, da $U \cup V$ eine Untergruppe ist. Also $uv \in U$ oder $uv \in V$. Die zweite Gleichung ist nicht möglich, da sonst $u \in Vv^{-1} = V$ wäre. Also ist $v \in u^{-1}U = U$, was zu zeigen war.* —

S 2.2. (2 Punkte) Jede Untergruppe vom Index zwei ist normal.
Jede normale Untergruppe von Ordnung zwei ist zentral (d.h. in $Z(G)$ enthalten).

Lösungshinweise: — *Sei $|G:U| = 2$. Die Linksnebenklassen gU sind gleich oder disjunkt, bilden eine Partition von G und es ist $gU = U$ genau dann, wenn $g \in U$. Für $g \in G \backslash U$ gilt also $G = U \cup gU$. Ebenso ist für Rechtsnebenklassen $G = U \cup Ug$ falls $g \in G \backslash U$. Damit folgt aber $gU = Ug$, also ist U normal.*
Sei $U \lhd G$ mit $|U| = 2$, also $U = \{1, u\}$. Da die 1 bei der Konjugation stets auf sich selbst geht, muss also das Element u ebenfalls immer auf sich selbst konjugiert werden, wenn $gUg^{-1} = U$ gelten soll. Dann folgt aber $gug^{-1} = u$, oder $gu = ug$. Damit ist $U \subset Z(G)$. —

2.3. (a) Sei $G \times H$ das Produkt der Gruppen G und H. Dann sind $N = G \times \{1\}$ und $M = \{1\} \times H$ Normalteiler mit $N \cap M = \{1\}$ und $MN = G \times H$.
(b) Seien nun $N, M \lhd G$ Normalteiler mit $N \cap M = \{1\}$ und $NM = G$. Konstruieren Sie einen Isomorphismus $G \cong N \times M$.

Lösungshinweise: —
(a) *Es sind alles einfache Rechnungen.*
(b) *Batrachte die Abbildung $\varphi : N \times M \to G : (n,m) \mapsto nm$. Die Abbildung ist nach Voraussetzung surjektiv und für $nm = 1$ folgt $n = m^{-1} \in N \cap M$, also $n = m = 1$. Damit ist φ auch injektiv. Es ist also noch zu zeigen, dass es ein Gruppenhomomorphismus ist. Dazu betrachten wir zuerst $nmn^{-1}m^{-1}$. Durch die Klammerung $n(mn^{-1}m^{-1})$ sieht man, dass das Element in N liegt, weil N normal ist. Genauso folgt aus der Klammerung $(nmn^{-1})m^{-1}$, dass es in M liegt. Deswegen ist also $nmn^{-1}m^{-1} = 1$, bzw. $nm = mn$ für alle $n \in N, m \in M$. Damit ist dann*
$\varphi((n_1,n_2)\cdot(m_1,m_2)) = \varphi(n_1n_2, m_1m_2) = n_1n_2m_1m_2 = n_1m_1n_2m_2 = \varphi(n_1,n_2)\varphi(m_1,m_2)$.

—

V 2.4. Eine Untergruppe $U < G$ heißt *charakteristisch* in G, wenn für alle Automorphismen $f : G \to G$ gilt, dass $f(U) = U$.

(a) Zeigen Sie, dass jede charakteristische Untergruppe U normal ist.
(b) Finden Sie eine normale Untergruppe, die nicht charakteristisch ist.
(c) Zeigen Sie, dass das Zentrum $Z(G)$ charakteristisch in G ist.
(d) Zeigen Sie, dass die Kommutatoruntergruppe $[G,G]$ charakteristisch in G ist.
(e) Sei K charakteristisch in H und H charakteristisch in G. Ist dann K charakteristisch in G?
(f) Sei K normal in H und H normal in G. Ist dann K normal in G?

Lösungshinweise: —

(a) *Konjugationen sind spezielle Automorphismen. Wenn also eine Untergruppe unter allen Automorphismen invariant ist, dann auch unter allen Konjugationen. Dann ist sie aber normal.*
(b) *Die Untergruppe $\mathbb{Z}/2 \times \{0\} \subset \mathbb{Z}/2 \times \mathbb{Z}/2$ ist normal (jede Untergruppe einer abelschen Gruppe ist normal, bzw. siehe Aufgabe 2.3), aber nicht charakteristisch, denn die Abbildung $(g,h) \mapsto (h,g)$ ist ein Automorphismus, der $\mathbb{Z}/2 \times \{0\}$ auf $\{0\} \times \mathbb{Z}/2$, also nicht auf sich selbst abbildet.*
(c) *Es sei $z \in Z(G)$ und $\varphi \in \mathrm{Aut}(G)$ gegeben. Dann existiert zu jedem $g \in G$ ein $h \in G$ mit $g = \varphi(h)$. Es ist $\varphi(z)g = \varphi(z)\varphi(h) = \varphi(zh) = \varphi(hz) = \varphi(h)\varphi(z) = g\varphi(z)$, also $\varphi(z) \in Z(G)$. Damit ist $\varphi(Z(G)) \subset Z(G)$ gezeigt. Die andere Inklusion folgt aber ebenso, da φ^{-1} auch ein Automorphismus ist.*
(d) *Sei $[g,h] = ghg^{-1}h^{-1}$ ein Kommutator. Dann ist $\varphi([g,h]) = \varphi(ghg^{-1}h^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1}\varphi(h)^{-1}$ $= [\varphi(g),\varphi(h)]$ wieder ein Kommutator. Die Gruppe $[G,G]$ wird nun von Produkten aus Kommutatoren der Form $[g,h]$ erzeugt und φ vertauscht mit Produktbildung. Also sind Bilder unter φ wieder Produkte aus Kommutatoren. Damit folgt $\varphi([G,G]) \subset [G,G]$. Die andere Inklusion folgt wieder, da φ^{-1} auch ein Automorphismus ist.*
(e) *Sei $\varphi \in \mathrm{Aut}(G)$ ein Automorphismus. Dann gilt $\varphi(H) = H$. Damit ist die Einschränkung $\varphi|_H \in \mathrm{Aut}(H)$ ein Automorphismus von H. Dieser lässt nun nach Voraussetzung K invariant, also ist K charakteristisch in G. Die Eigenschaft "charakteristisch zu sein" ist also transitiv auf dem Untergruppenverband.*
(f) *Betrachte $\{id,(12)(34)\} \lhd \{id,(12)(34),(13)(24),(14)(23)\} \lhd S_4$. Es ist aber $\{id,(12)(34)\}$ kein Normalteiler in S_4, da z.B. $(123)(12)(34)(123)^{-1} = (14)(23)$.*

—

3. Elementarteilersatz und Jordan–Normalform

Sei K ein Körper und sei $P = X^n + p_{n-1}X^{n-1} + \cdots + p_0$ ein Polynom in $K[X]$. Den $K[X]$-Modul $U = K[X]/(P)$ können wir vermöge $K \subset K[X]$ als K-Vektorraum auffassen. Die Multiplikation mit X definiert eine K-lineare Abbildung $\varphi\colon U \to U$.

V 3.1. Man zeige $\dim_K(U) = n$. Man zeige, dass sich φ bezüglich der Basis $(1,X,\ldots,X^{n-1})$ darstellt als die Matrix

$$B = \begin{pmatrix} 0 & \cdots & 0 & -p_0 \\ 1 & \ddots & \vdots & -p_1 \\ 0 & \ddots & 0 & \vdots \\ 0 & 0 & 1 & -p_{n-1} \end{pmatrix}.$$

Eine solche Matrix heißt *Begleitmatrix* von P oder *rationale Normalform* von φ.
Man bestimme das charakteristische Polynom $\det(X1_{n\times n} - B)$ der Matrix B.

Lösungshinweise: — *Es ist $P(X)=0$ in U und somit kann jedes Polynom S durch Polynomdivision als $S=PQ+R=R$ mit $\deg(R)<n$ geschrieben werden.*
Diese Darstellung ist eindeutig, da man sonst eine Gleichung der Form $R=QP$ in $K[X]$ hätte, was aus Gradgründen nicht sein kann. Also ist $\dim_K(U)=n$.
Offenbar bildet die Multiplikation mit X das Element X^i auf X^{i+1} ab. Damit ergibt sich schon die gewünschte Matrix, wenn man noch beachtet, dass $X^n=-p_{n-1}X^{n-1}-\cdots-p_0$ gilt.
Das charakteristische Polynom berechnet man am Besten durch Entwicklen nach der ersten Spalte und Induktion. Es ergibt sich (natürlich) $P(X)$. —

S 3.2. (2 Punkte) Sei nun speziell $P=(X-a)^n$. Man bestimme eine Basis von U über K, bezüglich der sich φ darstellt als die Matrix

$$J=\begin{pmatrix} a & 0 & \ddots & 0 \\ 1 & \ddots & \ddots & 0 \\ 0 & \ddots & \ddots & 0 \\ 0 & 0 & 1 & a \end{pmatrix}$$

Eine solche Matrix heißt *Jordanblock* oder *Jordan–Normalform* von φ.

Lösungshinweise: — *Man wählt die Basis $(1,X-a,(X-a)^2,\ldots,(X-a)^{n-1})$. Dann gilt $X\cdot(X-a)^i=(X-a)^{i+1}+a(X-a)^i$ und damit die gewünschte Matrix, wenn man noch $(X-a)^n=0$ beachtet.* —

Sei nun V ein K-Vektorraum mit $\dim_K(V)<\infty$. Gegeben sei eine K-lineare Abbildung $\varphi\in\mathrm{End}_K(V)$. Hierdurch wird V zu einem $K[X]$-Modul mit der Operation $K[X]\times V\to V$ gegeben durch $(P,v)\mapsto P(\varphi)(v)$.

Der Elementarteilersatz beschert uns nun einen $K[X]$-Modulisomorphismus

$$V\cong K[X]/(P_1)\times\cdots\times K[X]/(P_m) \tag{1}$$

wobei $P_1,\ldots,P_m$ normierte Polynome in $K[X]$ sind mit $P_1\mid\cdots\mid P_m$.

V 3.3. Folgern Sie hieraus, dass es eine K-Basis von V gibt, bezüglich der sich φ darstellt als eine Blockdiagonalmatrix

$$\begin{pmatrix} B_1 & & \\ & \ddots & \\ & & B_m \end{pmatrix}$$

wobei die Matrizen $B_1,\ldots,B_m$ in rationaler Normalform sind.

Man bestimme das charakterische Polynom von φ.

Lösungshinweise: — *Wähle eine Basis von V, indem man zuerst Basen $(b_1^{(i)},\ldots,b_{n_i}^{(i)})$ in $K[X]/(P_i)$ nach Aufgabe 3.1 wählt. Dann ist die Menge $(0,\ldots,0,b_k^{(i)},0,\ldots,0)$, $i=1,\ldots,m$ und $k=1,\ldots,n_i$ eine Basis des Kreuzproduktes, welche durch den Isomorphismus auf eine Basis von V abgebildet werden kann. (Bemerkung: Im Auffinden dieses Isomorphismus steckt die eigentliche Arbeit bei der Bestimmung der Normalform...).*
Die einzelnen Faktoren $K[X]/(P_i)$ sind φ-invariant, und somit hat die Darstellungsmatrix die Form, wie sie in der Aufgabe angegeben ist. Weiter sind die einzelnen Basen so gewählt, dass die Matrizen B_i gerade die Form aus Aufgabe 3.1 haben. —

Mittels des chinesischen Restsatzes erhalten wir aus (1) einen $K[X]$-Modulisomorphismus $V\cong K[X]/(Q_1)\times\cdots\times K[X]/(Q_s)$, wobei jedes Q_i Potenz eines normierten irreduziblen Polynoms in K[X] ist. Dabei ist $Q_1\cdots Q_s$ das charakteristische Polynom von φ.

S 3.4. (2 Punkte) Nehmen wir an, dass das charakteristische Polynom von φ über K in Linearfaktoren zerfällt. (Zum Beispiel ist dies immer der Fall für $K = \mathbb{C}$.) Zeigen Sie, dass es eine K-Basis von V gibt, bezüglich der sich φ darstellt als eine Blockdiagonalmatrix

$$\begin{pmatrix} J_1 & & \\ & \ddots & \\ & & J_s \end{pmatrix}$$

wobei die Matrizen $J_1, \dots, J_s$ Jordanblöcke sind.

Lösungshinweise: — *Da φ auf dem $K[X]$-Modul gerade die Multiplikation mit X darstellt, sind die einzelnen Faktoren $K[X]/(Q_i)$ φ-invariant. Wir wählen also, ähnlich wie in Aufgabe 3.3, eine Basis von V, indem wir jeweils Basen der einzelnen Vektorräume $K[X]/(Q_i)$ aufsuchen und diese mit dem Isomorphismus zurück nach V abbilden. Dabei ist $Q_i = (X - a_i)^{n_i}$, da wir angenommen haben, dass alle irreduziblen Polynome linear sind. Also können wir nach Aufgabe 3.2 eine Basis wählen, bezüglich derer wir einen Jordanblock J_i erhalten.*
Alles zusammen liefert die gewünschte Matrixdarstellung. —

3.5. Sei R ein Ring und M ein R-Linksmodul. Zeigen Sie, dass der Annihilator

$$\operatorname{ann}_R(M) := \{\, r \in R : rm = 0 \text{ für alle } m \in M \,\}$$

ein Linksideal in R ist. Bestimmen Sie zum Beispiel $\operatorname{ann}_{\mathbb{Z}}(\mathbb{Z}/3 \times \mathbb{Z}/6)$.

Lösungshinweise: — *Aus $rm = 0$ und $sm = 0$ für alle $m \in M$, folgt auch $(r+s)m = 0$ und $trm = 0$ für alle $r, s \in \operatorname{ann}_R(M)$, $t \in R$. Also ist $\operatorname{ann}_R(M)$ ein Linksideal in R. Es ist $\operatorname{ann}_{\mathbb{Z}}(\mathbb{Z}/3 \times \mathbb{Z}/6) = 6\mathbb{Z}$.* —

S 3.6. (2 Punkte) Zeigen Sie, dass in (1) $\operatorname{ann}_{K[X]}(V) = (P_m)$ gilt.
Damit ist P_m das Minimalpolynom von φ.

Lösungshinweise: — *Da $P_1 \mid \cdots \mid P_m$ gilt, führt die Multiplikation mit P_m im Modul* (1) *dazu, dass jeder Eintrag* 0 *wird. Also ist $(P_m) \subset \operatorname{ann}_{K[X]}(V)$.*
Ist andererseits S ein Polynom in $\operatorname{ann}_{K[X]}(V)$, so teile man mit Rest $S = QP_m + R$. Dann ist auch $R \in \operatorname{ann}_{K[X]}(V)$ mit $\deg(R) < \deg(P_m)$. Bei Multiplikation mit R, wird in $K[X]/(P_m)$ nur dann jedes Element annihiliert, wenn $R = 0$ gilt, also ist $S = P_m Q$, bzw. $\operatorname{ann}_{K[X]}(V) \subset (P_m)$.
Das Minimalpolynom von φ ist das normierte Polynom minimalen Grades Q, so dass $Q(\varphi)(v) = 0$ für alle $v \in V$. Das heißt aber $Q \in \operatorname{ann}_{K[X]}(V) = (P_m)$. Also wegen Minimalität und Normiertheit $Q = P_m$ —