Übung zur Vorlesung Einführung in die Algebra

Prof. Dr. J. H. Bruinier
Stephan Ehlen

TECHNISCHE UNIVERSITÄT DARMSTADT

Sommersemester 2009
Lösungshinweise zu Übungsblatt 7

Aufgabe G7.1 Perlenketten und Gruppenoperationen

Wir wollen herausfinden, wie viele verschiedene Perlenketten mit n Perlen es gibt, wobei wir uns aus einem Vorrat von m Sorten von Perlen bedienen.

(a) Es gibt 4 verschiedene Ketten aus 3 schwarzen oder weißen Perlen.

(b) Wir modellieren das Problem folgendermaßen: Die Symmetriegruppe $G(R_n)$ des regulären n-Ecks operiert auf der Menge X der Verteilungsfunktionen indem man $(g.F)(x) := F(g^{-1}(x))$ setzt, wobei $x \in E(R_n)$ eine Ecke und $F \in X$ eine Verteilungsfunktion ist. (Rechnen Sie nach, dass dies eine Gruppenoperation ist!) Zwei verschiedene Verteilungsfunktionen stehen für die gleiche Kette genau dann, wenn Sie unter der Operation von $G(R_n)$ äquivalent sind. Damit ergibt sich, dass die Anzahl der verschiedenen Perlenketten gleich der Anzahl der Bahnen dieser Gruppenoperation ist.

(c) Nach dem Satz von Burnside gilt für die Anzahl $A(n,m)$ der verschiedenen Perlenketten der Länge n (die aus m verschiedenen Perlen bestehen):

$$A(n,m) = \frac{1}{|G(R_n)|} \sum_{g \in G(R_n)} \left| Fix(g) \right|.$$

(d) Wir wissen, dass die Symmetriegruppe des regulären n-Ecks aus Drehungen und Spiegelungen besteht (es ist die Gruppe D_n).

Da 7 eine Primzahl ist, erhält man über eine Drehung nur dann wieder die gleiche Verteilungsfunktion, wenn alle Perlen von der gleichen Sorte sind. Damit ergibt sich für eine nicht-triviale Drehung g, dass $\left|Fix(g)\right| = m = 2$ ist. Für eine Spiegelung gilt: Es wird immer eine Ecke festgehalten und die restlichen $n-1=4$ Ecken werden in Paaren miteinander identifiziert. Damit ist für eine Spiegelung $|Fix(g)| = 2^{\frac{n+1}{2}} = 16$.

Für die Identität gilt natürlich, dass alle ausgerichteten Ketten festgehalten werden. Davon gibt es $m^n = 2^7$.

Insgesamt erhalten wir also, dass die Anzahl der verschiedenen Perlenketten der Länge 7 aus 2 verschiedenen Perlensorten

$$A(7,2) = \frac{1}{14}\left(2^7 + 6 \cdot 2 + 7 \cdot 16\right) = \frac{252}{14} = 18$$

ist.

Aufgabe G7.2 Konjugationsklassen in der symmetrischen Gruppe S_n

Zu Vorbereitung auf diese Aufgabe, wiederholen Sie die Zykelschreibweise für Permutationen. Es sei $n \geq 3$ und $\pi \in S_n$, dann lässt sich π in Zykelschreibweise zerlegen:

$$\pi = (k_{1,1}\ k_{1,2}\ \ldots\ k_{1,m_1}) \cdots (k_{n,1}\ k_{n,2}\ \ldots\ k_{n,m_n}),$$

wobei alle $k_{i,j} \in \{1,\ldots,n\}$ und paarweise verschieden sind. Hierbei ist ein einzelner Zykel $(k_1\ k_2\ \ldots\ k_m) \in S_n$ die Abbildung, die k_1 auf k_2, k_2 auf k_3, $\ldots$, k_{m-1} auf k_m und k_m auf k_1 abbildet. Beispielsweise ist die Transposition der Elemente 1 und 2 durch den Zykel (1 2) gegeben und die Permutation der Menge $\{1,\ldots,5\}$ die 1 und 2 sowie 4 und 5 vertauscht, aber 3 festlässt durch (1 2)(4 5).

(a) (1 2 3)(4 5)

(b) Setze $g := \pi \circ (1\ 2\ 3) \circ \pi^{-1}$. Wir berechnen

$$g(\pi(1)) = \pi((1\ 2\ 3)(1)) = \pi(2)\,,$$

$$g(\pi(2)) = \pi((1\ 2\ 3)(2)) = \pi(3)\,,$$

$$g(\pi(3)) = \pi((1\ 2\ 3)(3)) = \pi(1)$$

sowie für $k \in \{1,\dots,n\} \setminus \{1,2,3\}$

$$g(\pi(k)) = \pi((1\ 2\ 3)(k)) = \pi(k)\,.$$

Die gleichen Werte erhält man für den 3-Zyklus $(\pi(1)\ \pi(2)\ \pi(3))$. Also $g = (\pi(1)\ \pi(2)\ \pi(3))$.

(c) Wir definieren $g := \pi \circ \sigma \circ \pi^{-1}$. Für $i \in \{1,\dots,m-1\}$ ist

$$g(\pi(k_i)) = \pi(\sigma(k_i)) = \pi(k_{i+1})$$

und weiter

$$g(\pi(k_m)) = \pi(\sigma(k_m)) = \pi(k_1)\,.$$

Also ist $\{\pi(k_1),\dots,\pi(k_m)\}$ eine m-elementige Bahn von g, deren Elemente in der angegebenen Reihenfolge durchlaufen werden. Der Zyklus $(\pi(k_1)\ \pi(k_2)\ \cdots\ \pi(k_m))$ kommt daher in der Zykelzerlegung von g vor.

(d) Wir schreiben die Zykelzerlegung von σ als

$$\sigma = z_{x_1} \circ \cdots \circ z_{x_r}\,.$$

Es ist dann

$$\pi \circ \sigma \circ \pi^{-1} = (\pi \circ z_{x^1} \circ \pi^{-1}) \circ (\pi \circ z_{x^2} \circ \pi^{-1}) \circ \cdots \circ (\pi \circ z_{x^r} \circ \pi^{-1})$$

die Zykelzerlegung von $\pi \circ \sigma \circ \pi^{-1}$, da $\pi \circ z_{x^i} \circ \pi^{-1}$ als Konsequenz von Teil (c) paarweise verschiedene Zykel von $\pi \circ \sigma \circ \pi^{-1}$ sind.

(e) Sind σ und τ konjugiert, so haben sie nach (d) den gleichen Zykeltyp.

Umgekehrt sei nun angenommen, dass σ und τ den gleichen Zykeltyp haben. Schreiben wir die Zykelzerlegungen mit Zykeln monoton fallender Länge hin, so gilt dann also

$$\sigma = z_{x_1} \cdots z_{x_r} \qquad \text{und} \qquad \tau = \zeta_{y_1} \cdots \zeta_{y_r}\,,$$

wobei z_{x_j} ein Zykel von σ ist von derselben Länge m_j wie der Zykel ζ_{y_j} von τ, für jedes $j \in \{1,\dots,r\}$. Die Elemente $x_j, y_j \in \{1,\dots,n\}$ sind die Elemente, and denen jeweils ein Zykel beginnt von σ bzw. τ beginnt. Die Zykeln sind also genauer gegeben als

$$z_{x_j} = (x_j\ \sigma(x_j)\ \cdots\ \sigma^{m_j-1}(x_j)) \in S_n$$

und

$$\zeta_{y_j} = (y_j\ \tau(y_j)\ \cdots\ \tau^{m_j-1}(y_j)) \in S_n\,.$$

Wir definieren nun $\pi : \{1,\dots,n\} \to \{1,\dots,n\}$ indem wir setzen: $\pi(\sigma^i(x^j)) := \tau^i(y^j)$ für alle $j \in \{1,\dots,r\}$ und $i \in \{0,\dots,m_j-1\}$. Dabei wird π wirklich für alle $x \in \{1,\dots,n\}$ definiert, denn die Werte $\sigma^i(x_j)$ sind nach Definition der Zykelzerlegung ja alle verschieden.

Dann ist also $\pi \in S_n$ wirklich eine Permutation und

$$\pi \circ \sigma \circ \pi^{-1} = (\pi \circ z_{x_1} \circ \pi^{-1}) \circ \cdots \circ (\pi \circ z_{x-r} \circ \pi^{-1}) = \zeta_{y_1} \circ \cdots \zeta_{y_r} = \tau\,,$$

nach Teil (c). Also sind σ und τ konjugiert.

(f) S_3 hat nur 3 verschiedene Zykeltypen, repräsentiert durch (1), (1 2) und (1 2 3). In S_5 gibt es fünf verschiedene Zykeltypen, repräsentiert durch (1), (1 2), (1 2 3), (1 2 3 4) und (12)(34).

Aufgabe G7.3 Einige Anwendungen des Satzes von Sylow

(a) Wir bezeichnen im Folgenden mit s_p die Anzahl der p-Sylow-Untergruppen von G. Der Satz von Sylow ergibt, dass

$$\begin{aligned} s_3 &\equiv 1 \mod 3 \text{ und } & s_3 \mid 5 \\ s_5 &\equiv 1 \mod 5 \text{ und } & s_5 \mid 3. \end{aligned}$$

Daraus folgt direkt, dass $s_3 = s_5 = 1$ gilt. Da jedes Element der Ordnung p eine Untergruppe der Ordnung p erzeugt und umgekehrt auch jedes Element einer Untergruppe der Ordnung p die ordnung p haben muss oder die 1 ist, sieht man, dass es in G genau 2 Elemente der Ordnung 3 und genau 4 Elemente der Ordnung 5 geben muss. Außerdem gibt es natürlich genau ein Element der Ordnung 1. Das macht zusammen 7 Elemente mit Ordnung ≤ 5. Nach dem Satz von Lagrange kann G aber nur Elemente der Ordnung $1, 3, 5$ und 15 haben. Die Übrigen 8 Elemente haben also Ordnung 8 und somit ist jede Gruppe der Ordnung 15 zyklisch. Sie ist also isomorph zu $\mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

(b) Es ist $s_q \equiv 1 (\mod q)$ und gleichzeitig $s_q \mid p$. Da $p < q$ folgt, dass $s_q = 1$. Es gibt also genau eine q-Sylow-Untergruppe Q. Da aber für jedes $g \in G$ auch $g \in G$ auch gQg^{-1} eine q-Sylow-Untergruppe ist, folgt $gQg^{-1} = Q$ für alle $g \in G$; also ist Q normal.

(c) Dies folgt, da Q normal ist und für irgendeine p-Sylow-Untergruppe P von G die Multiplikationsabbildung $P \times Q \to G$ bijektiv ist, da p und Q trivialen Schnitt haben.

Aufgabe H7.1 Gruppen der Ordnung pq

Wir wissen aus Aufgabe G7.3 (c) nun, dass G isomorph zum semidirekten Produkt $\mathbb{Z}/q\mathbb{Z} \rtimes_\alpha \mathbb{Z}/p\mathbb{Z}$ ist, wobei $\alpha : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ ein Homomorphismus ist. Nun ist aber $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/(q-1)\mathbb{Z}$, denn ein solcher Automorphismus ist eindeutig durch das Bild der 1 bestimmt. Also ist $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ zyklisch von Ordnung $q-1$. Nun ist aber $\mathrm{id} = \alpha(0) = \alpha(p \cdot 1) = \alpha(1)^p$. Damit kann die Ordnung von $\alpha(1)$ nur 1 oder p sein und da p teilerfremd zu $q-1$ ist, muss $\alpha(1)$ die Identität sein. Damit ist dann aber α bereits trivial und G ist isomorph zum direkten Produkt.

Alternativ hätte man wie in Aufgabe G7.3 (a) durch abzählen argumentieren können, dass es auch einen Normalteiler der Ordnung P geben muss und damit folgt nach dem Satz über die direkten Produkte die Isomorphie.

Aufgabe H7.2 Alle Gruppen der Ordnung ...

(a) Es liegt mit $10 = 2 \cdot 5$ natürlich der Fall pq vor, aber 2 teilt hier $5 - 1 = 4$. Damit muss man noch bestimmen, welche Möglichkeiten es für den Homomorphismus α im semidirekten produkt geben kann. Dies muss dann ein Homomorphismus von $\mathbb{Z}/2\mathbb{Z}$ nach $\mathbb{Z}/4\mathbb{Z}$ sein. Es gibt nur zwei Möglichkeiten, die gegeben sind durch den trivialen Homomorphismus und $\alpha(1) = 2 \in \mathbb{Z}/4\mathbb{Z}$. Im ersten Fall erhält man die abelsche Gruppe $\mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ und im zweiten Fall die nicht-abelsche Diedergruppe D_5 der Ordnung 10.

(b) Alle drei Fälle sind von der Form pq, wobei p nicht $q-1$ teilt und somit gibt es jeweils nur die zyklische Gruppe $\mathbb{Z}/(pq)\mathbb{Z}$.

Aufgabe H7.3 Die multiplikative Gruppe eines endlichen Körpers

Es sei $\mathbb{F}$ ein endlicher Körper. Da die multiplikative Gruppe $\mathbb{F}^\times$ endlich ist, ist sie endlich erzeugt und somit nach dem Satz über endlich erzeugte abelsche Gruppen

$$\mathbb{F}^\times \cong C_{p_1^{k_1}} \times \cdots \times C_{p_r^{k_r}} =: G$$

für ein $r \in \mathbb{N}$, Primzahlen $p_1, \ldots, p_r$ und positive natürliche Zahlen $k_1, \ldots, k_r$ (da $\mathbb{F}^\times$ endlich ist, können keine Faktoren der Gestalt $\mathbb{Z}$ auftauchen). Wäre $\mathbb{F}^\times$ nicht zyklisch, so gäbe es $i \neq j$ mit $p_i = p_j =: p$ (andernfalls wäre $\mathbb{F}^\times$ ja zyklisch!). Dann sind

$$A' := \{(x_1, \ldots, x_n) \in G : x_i \in C_p \text{ und } x_k = 1 \text{ für alle } k \neq i\} \qquad \text{und}$$

$$B' := \{(x_1, \ldots, x_n) \in G : x_j \in C_p \text{ und } x_k = 1 \text{ für alle } k \neq j\}$$

Untergruppen der Ordnung p von G mit $A' \cap B' = \{1\}$. Ist also $\phi : \mathbb{F}^\times \to G$ ein Isomorphismus, so sind $A := \phi^{-1}(A')$ und $B := \phi^{-1}(B')$ Untergruppen der Ordnung p von $\mathbb{F}^\times$ mit $A \cap B = \{1\}$. Dann ist $AB \cong A \times B$ (vgl. den Satz über die direkten

Produkte) eine Untergruppe der Ordnung p^2 von $\mathbb{F}^\times$ derart, dass jedes von 1 verschiedene Element $x \in AB$ die Ordnung p hat. Es gäbe in $\mathbb{F}$ also $\geq p^2 - 1 = (p+1)(p-1) > p$ Elemente x, welche die Gleichung

$$x^p - 1 = 0$$

erfüllen. Wie im Reellen und Komplexen hat aber auch über einem beliebigen Körper ein Polynom der Ordnung p höchstens p verschiedene Nullstellen, Widerspruch!

Beispiel: Ist p eine Primzahl, so ist $\mathbb{Z}/p\mathbb{Z}$ ein endlicher Körper mit p Elementen, nach dem Vorigen also $(\mathbb{Z}/pZ)^\times$ eine zyklische Gruppe der Ordnung $p-1$ und somit $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$. Es ist also $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$. Ist p ungerade, so ist $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ nach dem Vorigen eine zyklische Gruppe gerader Ordnung. Eine solche enthält genau eine Untergruppe der Ordnung 2 und daher genau ein Element der Ordnung 2.