Gruppentheorie

FSU Jena - SS 2009

Übungsserie 01 - Lösungen

Stilianos Louca

9. Juli 2009

Aufgabe 01

(i)
- Es seien $a, b, c \in \mathbb{N}$ und
$$h := \mathrm{ggT}(\mathrm{ggT}(a,b), c)$$
Dann teilt h per Konstruktion $\mathrm{ggT}(a,b)$ und c, und somit auch a und b. Somit teilt h auch $\mathrm{ggT}(b,c)$ [1], das heißt definitionsgemäß
$$h \leq \mathrm{ggT}(a, \mathrm{ggT}(b,c))$$
Da ggT kommutativ ist, folgt
$$\mathrm{ggT}(a, \mathrm{ggT}(b,c)) = \mathrm{ggT}(\mathrm{ggT}(c,b), a) \leq \mathrm{ggT}(c, \mathrm{ggT}(b,a)) = \mathrm{ggT}(\mathrm{ggT}(a,b), c) = h$$
das heißt
$$\mathrm{ggT}(\mathrm{ggT}(a,b), c) = \mathrm{ggT}(a, \mathrm{ggT}(b,c))$$
Somit ist $(\mathbb{N}, \mathrm{ggT})$ eine Halbgruppe. Allerdings gelte für ein neutrales Element n_0:
$$n_0 = \mathrm{ggT}(2n_0, n_0) \overset{n_0 \text{ neutral}}{=} 2n_0$$
was für $n_0 \in \mathbb{N}$ unmöglich ist, das heißt $(\mathbb{N}, \mathrm{ggT})$ ist **kein** Monoid.
- Für $a, b, c \in \mathbb{N}$ sei
$$h := \mathrm{kgV}(\mathrm{kgV}(a,b), c)$$
Dann ist h ein Vielfaches von $\mathrm{kgV}(a,b)$ und c und somit auch von a, b. Analog zu vorhin ist dann h auch ein Vielfaches von $\mathrm{kgV}(b,c)$ und somit definitionsgemäß
$$h \geq \mathrm{kgV}(a, \mathrm{kgV}(b,c))$$
Analog zu vorhin folgt hieraus die Assoziativität von kgV. Das neutrale Element ist hier die 1, weshalb $(\mathbb{N}, \mathrm{kgV})$ ein Monoid ist.

(ii) **Gegenbeispiel:** Für Primzahlen $p \neq q \in \mathbb{P}$ ist
$$f(\mathrm{kgV}(p, qp)) = f(qp) = 2 \neq 3 = f(p) + f(qp)$$

Aufgabe 02

(i) Betrachten die Halbgruppe $(G, \cdot) \subset (\mathbb{R}^{2\times 2}, \cdot)$ definiert durch
$$G := \left\{ \begin{pmatrix} 1 & \lambda \\ 0 & 0 \end{pmatrix} | \lambda \in \mathbb{R} \right\}$$
Tatsächlich ist $\cdot : G \times G \to G$ und $|G| = \infty$. Ferner ist jedes Element aus G linksneutral.

[1] Dies kann man sich z.B. durch eine Primfaktorzerlegung von h, b, c und $\mathrm{ggT}(b,c)$ klarmachen.

(ii) Es sei $\mathbb{R}_+ := [0, \infty)$ und

$$G := \mathbb{R}_+^{\mathbb{R}_+} := \{f \mid f : \mathbb{R}_+ \to \mathbb{R}_+\}$$

Dann ist G zusammen mit der Verkettung $\circ$ ein Monoid mit neutralem Element Id. Das Element $f \in G$ definiert durch

$$f(x) := 1 + x$$

besitzt unendlich viele links-inverse, denn für beliebiges $\lambda \geq 0$ ist $g_\lambda \in G$ definiert durch

$$g_\lambda(y) := \begin{cases} y - 1 & y \geq 1 \\ \lambda & : \text{sonst} \end{cases}$$

linksinvers zu f.

Aufgabe 03

(i) f ist tatsächlich ein Homomorphismus, denn für $A, B \in \mathscr{P}(X)$:

$$f(A \cup B) = (A \cup B)^c = A^c \cap B^c = f(A) \cap f(B)$$

Da $f \circ f = \text{Id}$ ist f auch bijektiv.

(ii) Für $\varphi : X \to X$ setzen

$$F(\varphi) := f \circ \varphi \circ f^{-1}$$

Dann ist F ein Homomorphismus, denn

$$F(\varphi \circ \vartheta) = f \circ \varphi \circ \vartheta \circ f^{-1} = f \circ \varphi \circ f^{-1} \circ f \circ \vartheta \circ f^{-1} = F(\varphi) \circ F(\vartheta)$$

und bijektiv, mit

$$F^{-1}(\gamma) = f^{-1} \circ \gamma \circ f$$

Aufgabe 04

(i)

- Es sei S eine Gruppe der Ordnung 4. Dann hat S entweder die Form

$$S = \left\{e, q, q^2, q^3\right\} \tag{1}$$

also insbesondere $q^4 = e$, oder

$$S = \{e, q, p, pq\} \quad \text{mit} \quad q = q^{-1},\ p = p^{-1},\ pq = qp \tag{2}$$

Beweis: Es sei $S = \{e, q, p, r\}$ für irgendwelche paarweise verschiedenen q, p, r. Ist $p = q^{-1}$ (*) dann $rq \neq e$ (sonst $r = p$), $rq \neq q$ (sonst $r = e$) und $rq \neq r$ (sonst $q = e$), somit $rq = q^{-1}$, also $r = q^{-2}$:

$$S = \left\{e, q, q^{-1}, q^{-2}\right\}$$

Demnach

$$q^2 = qq \notin \{\underbrace{eq}_{q}, \underbrace{q^{-1}q}_{e}\}$$

und

$$q^3 = qq^2 \notin \{\underbrace{eq^2}_{q^2}, \underbrace{q^{-1}q^2}_{q}, \underbrace{q^{-2}q^2}_{e}\}$$

Analog folgt auch $q^4 \notin \left\{q^3, q^2, q\right\}$ also $\underbrace{q^4}_{\in S} = e$.

Alternativ zu (*), wäre $q = q^{-1}, p = p^{-1}, r = r^{-1}$. Somit $pq \neq e$ (sonst $p = q^{-1} = q$), $pq \neq p$ (sonst $q = e$) und $pq \neq q$ (sonst $p = e$), also $pq = r$. Per Symmetrie analog $qp = r$.
□

- Form 1 ist sogar hinreichend, das heißt für $q, q^2, q^3 \neq e$ und $q^4 = e$ ist $\left\{e, q, q^2, q^3\right\}$ eine Untergruppe.
- Form 2 ist ebenfalls hinreichend, das heißt für $q, p \neq e, q \neq p, q = q^{-1}, p = p^{-1}, pq = qp$ ist $\{e, q, p, pq\}$ eine Untergruppe.

- Es genügt also die Suche auf Untergruppen der obigen Form zu beschränken (bemerke dass sich die beiden Formen gegenseitig ausschließen). Bei der ersten Form muss außerdem darauf geachtet werden dass q und q^3 die gleiche Gruppe generieren. Ähnlich ist auch bei der zweiten Form $\langle x, y\rangle = \langle x, xy\rangle$. Der Code

```
G := SymmetricGroup(9);
C := Filtered(G, x->Order(x)=4); #Cyclic subgroups of order 4

N := Filtered(G, x->Order(x)=2);
countN := 0;
for q in N do
  for p in N do
    if (q*p = p*q) and (q <> p) then
      #Creates subgroup of type {e,q,p,pq}
      countN := countN + 1;

    fi;
  od;
od;
countN := countN/6; #Every group counted 6-times: <x,y> <x,xy> <y,x> <y,xy> <xy,x>

Print("Cyclic ", Size(C)/2, ", Involutions ", countN, ", Total ", Size(C)/2 +countN
```

ergibt

$$|\{S : S \leq \mathrm{Sym}(9) \ \wedge \ |S| = 4\}| = 56\ 007$$

(ii) Der Code

```
G := DirectProduct(CyclicGroup(12), CyclicGroup(15));
LoadPackage("sonata");
Print("Subgroup count ", Size(Subgroups(G)), "\n");
```

ergibt 36 Untergruppen von $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$.

(iii) Die Permutationen α, β, γ sind jeweils gegeben durch

$$\alpha = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & \infty \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 0 & \infty \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix}$$

$$\beta = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & \infty \\ 0 & 2 & 4 & 6 & 8 & 10 & 1 & 3 & 5 & 7 & 9 & \infty \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 & 8 & 5 & 10 & 9 & 7 & 3 & 6 \end{pmatrix}$$

$$\gamma = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & \infty \\ \infty & 10 & 5 & 7 & 8 & 2 & 9 & 3 & 4 & 6 & 1 & 0 \end{pmatrix} = (0 \quad \infty)\,(1 \quad 10)\,(2 \quad 5)\,(3 \quad 7)\,(4 \quad 8)\,(6 \quad 9)$$

GAP liefert

$$|\langle \alpha, \beta, \gamma\rangle| = 1\ 320$$