ETH Zürich, D-INFK
HS 2024, 8. November 2024

Prof. Ueli Maurer
Giovanni Deligios, Dr. Karen Klein

Diskrete Mathematik

Exercise 8

Exercise 8.5 gives bonus points, which can increase the final grade. The solution to this exercise must be your own work. You may not share your solutions with anyone else. See also the note on dishonest behavior on the course website: `https://crypto.ethz.ch/teaching/DM24/`.

8.1 Algebras ($\star$)

For each of the following algebras, decide whether it is a monoid, a group or neither. In case it is a monoid or a group, decide whether it is abelian. Justify your answers.

a) $\langle \mathbb{Z}; \star \rangle$, where $\star$ is defined by $a \star b \stackrel{\text{def}}{=} a^2 + b^2$ for any $a, b \in \mathbb{Z}$.

b) $\langle \mathcal{P}(X); \cup \rangle$, where X is a non-empty finite set.

c) $\langle S; * \rangle$, where $S = (\mathbb{Q} \setminus \{0\}) \times \mathbb{Q}$ and

$$(a, b) * (c, d) \stackrel{\text{def}}{=} (ac, ad + b).$$

8.2 Facts About Groups ($\star\,\star$)

In this exercise you are **not** allowed to use lemmas from the lecture notes (especially, Lemma 5.3). Let $\langle G; *, \widehat{\ }, e \rangle$ be a group.

a) Prove that the group axiom **G2** can be simplified (see also Section 5.2.4 of the lecture notes). That is, show that **G2** follows from the axioms **G1**, **G2′** and **G3**, where

G2′ e is a right neutral element: $a * e = a$ for all $a \in G$.

b) Prove that $\widehat{a * b} = \widehat{b} * \widehat{a}$ for all $a, b \in G$.

c) Prove that $a * b = a * c \implies b = c$ for all $a, b, c \in G$.

8.3 Group Structure Induced by Bijections ($\star\,\star$)

Let $\langle G, *, \widehat{\ }, e \rangle$ be a group, and let S be a set. Assume that $f : G \to S$ is a bijection, and consider

- the binary operation $\star$ on S given by $s \star s' \stackrel{\text{def}}{=} f\left(f^{-1}(s) * f^{-1}(s')\right)$,
- the unary operation $\widetilde{\ }$ on S given by $\widetilde{s} \stackrel{\text{def}}{=} f\left(\widehat{f^{-1}(s)}\right)$.

Prove the following statements.

a) Axiom **G1** holds for $\langle S,\ \star\ , \tilde{}, f(e)\rangle$.

b) Axioms **G2** and **G3** hold for $\langle S,\ \star\ , \tilde{}, f(e)\rangle$.

c) $f : G \to S$ is a group isomorphism.

d) For all non-empty countable sets A, there exists a group with A as carrier.

8.4 Structure of Groups ($\star\,\star$)

a) List all subgroups of $\langle \mathbb{Z}_4; \oplus\rangle \times \langle \mathbb{Z}_5; \oplus\rangle$.

b) Let $\langle G; *, \hat{}, e\rangle$ be a group, such that $a * a = e$ for all $a \in G$. Prove that G is abelian.

c) Prove that $\langle \mathbb{Z}_{15}^*, \odot_{15}\rangle \simeq \langle \mathbb{Z}_{16}^*, \odot_{16}\rangle$.

8.5 Inner Direct Products ($\star$) *(8 Points)*

a) Let $\langle G;\ *\,,\ \hat{},\ e\rangle$ be a commutative group. Let H and K be subgroups of G such that

i. $G = \{h * k \mid h \in H, k \in K\}$,

ii. $H \cap K = \{e\}$.

Prove that G is isomorphic to the direct product $H \times K$. In this case, G is called the *inner* direct product of H and K.

b) Use the previous subtask to prove that $\langle \mathbb{Z}_{15}^*, \odot_{15}\rangle \simeq \mathbb{Z}_2 \times \mathbb{Z}_4$. You can use the subtask even if you have not proven it. **Do not** prove the isomorphism directly.

8.6 A Binary Operation From a Group Homomorphism ($\star\,\star$)

Let $\langle G; *, \hat{}, e\rangle$ be a group, and let $\psi : G \to G$ be a group homomorphism. Consider the algebra $\langle G; \cdot\rangle$ with

$$x \cdot y \stackrel{\text{def}}{=} \psi(x) * \psi(y) \quad \text{for any } x \in G \text{ and } y \in G.$$

We say that a function $f : X \to X$ is *idempotent* if $f(x) = f(f(x))$ for all $x \in X$.
Prove that

The binary operation $\cdot$ is associative if and only if ψ is idempotent.

8.7 Isomorphisms Map Generators to Generators ($\star\,\star$)

Let ψ be a group isomorphism from $\langle G; *, \hat{}, e\rangle$ to $\langle H; \star, \tilde{}, e'\rangle$. Prove that if G is cyclic and g is a generator of G then $\psi(g)$ is a generator of H.

8.8 Rotations of a Cube ($\star$)

Consider a sofa in the shape of a cube with corners labeled $0, 1, \ldots, 7$, standing in the corner of a room.

a) In how many ways can the sofa be placed in the corner?

Now one can take the sofa from the corner, rotate it in an arbitrary way and place it back in the corner. We distinguish two rotations b_1 and b_2 if the position of the sofa is different after the rotation b_1 and after b_2. Let R denote the set of such different rotations.

b) Determine $|R|$. Is it possible to describe each element of R as a rotation around a single axis? (For different elements the axes can be different.)

c) Let $b_2 \circ b_1$ denote applying to the sofa first the rotation b_1 and then the rotation b_2. Is $\langle R; \circ \rangle$ a group?

d) Is $\circ$ commutative?

Due by 14. November 2024.
Exercise 8.5 is graded.