ETH Zürich, D-INFK
HS 2020, 16. October 2020

Prof. Ueli Maurer
David Lanzenberger

Diskrete Mathematik

Exercise 6

Exercise 6.3 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/DM20/`.

6.1 An Equivalence Relation (⋆ ⋆)

The relation $\sim$ on $\mathbb{R}^2 \setminus \{(0,0)\}$ is defined as follows:

$$(x_1, y_1) \sim (x_2, y_2) \quad \overset{\text{def}}{\iff} \quad \exists \lambda > 0 \ (x_1, y_1) = (\lambda x_2, \lambda y_2)$$

a) Prove that $\sim$ is an equivalence relation.

b) Describe geometrically the equivalence classes $[(x, y)]$.

6.2 Composition of Equivalence Relations (⋆ ⋆)

Let ρ and σ be equivalence relations on a set A. Prove that if $\rho \circ \sigma = \sigma \circ \rho$, then $\rho \circ \sigma$ is an equivalence relation.

6.3 Lifting an Operation to Equivalence Classes (⋆ ⋆) *(8 Points)*

In the lecture (and in Section 3.3.3 of the lecture notes), we have considered the following equivalence relation $\sim$ on the set $A \overset{\text{def}}{=} \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$:

$$(a, b) \sim (c, d) \overset{\text{def}}{\iff} ad = bc.$$

We then defined the rational numbers $\mathbb{Q} \overset{\text{def}}{=} A/{\sim}$, capturing the fact that each rational number has different *representations* as fractions.

The goal of this exercise is to understand how to define an operation on equivalence classes (e.g., the sum of two rational numbers) by lifting an operation defined at the level of the *elements* of the equivalence classes (e.g., the fractional representations A of the rationals).

Consider an equivalence relation θ on some set B and a function $f : B^2 \to B$. We want to lift f to the set of equivalence classes B/θ, i.e., we want to define a function $F : (B/\theta)^2 \to (B/\theta)$ canonically in terms of f. For this to be meaningful, f has to be *θ-consistent*. That is, if f is applied to a pair $(b_1, b_2) \in B^2$, the equivalence class $[f(b_1, b_2)]_\theta$ may only depend on the *equivalence classes* $[b_1]_\theta$ and $[b_2]_\theta$ (irrespective of which concrete elements both b_1 and b_2 are within their equivalence classes).

a) Define the sum of two fractional representations of rational numbers as a function $\mathsf{sum} : A^2 \to A$ (for $A = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ as defined above), using standard addition and multiplication in the integers.

b) Express formally what it means for a function $f : B^2 \to B$ to be θ-consistent for an equivalence relation θ on B.

Hint: For example, the function sum defined in Subtask a) being $\sim$-consistent captures the fact that when adding two rational numbers x and y, we can add two *arbitrary* fractional representations of x and y from the set A (by applying sum), and the rational number obtained does not depend on which representation of x and y was used.

c) Prove that the function $\mathsf{sum} : A^2 \to A$ defined in Subtask a) is $\sim$-consistent.

6.4 Partial Order Relations ($\star$)

a) Consider the poset $(\mathbb{N} \setminus \{0\};\ |\ )$. Which of the following pairs are comparable?

i) $11, 12$ **ii)** $4, 6$ **iii)** $5, 15$ **iv)** $42, 42$

b) Consider the set $A := (\mathbb{N} \setminus \{0\}) \times (\mathbb{N} \setminus \{0\})$ with the lexicographic order $\leq_{\mathsf{lex}}$ defined by the divisability relation $|$. Determine all elements $a \in A$, such that $a \leq_{\mathsf{lex}} (2, 5)$.

c) Prove or disprove: $(\{1, 3, 6, 9, 12\},\ |\ )$ is a lattice.

d) Prove or disprove: If $(A; \preceq)$ is a poset, then $(A; \widehat{\preceq})$ is also a poset.

6.5 Hasse Diagrams ($\star$)

For each of the two posets: $(\{1, 2, 3\}; \leq)$ and $(\{1, 2, 3, 5, 6, 9\};\ |\ )$, draw the Hasse diagram and determine all least, greatest, minimal and maximal elements.

6.6 The Lexicographic Order ($\star\ \star$)

Prove Theorem 3.11 from the lecture notes.

6.7 Inverses of Functions ($\star\ \star$)

For a set A, the identity function id is defined by $\mathrm{id}(a) = a$ for all $a \in A$. Consider a function $f : A \to A$. Prove that there exists a function $g : A \to A$ such that $g \circ f = \mathrm{id}$ if and only if f is injective.

Such g is called a *left inverse* of f.

Due on 27. October 2020.
Exercise 6.3 is graded.