Cryptography

Dr. Patrick Mehlitz, M.Sc. Ameen Naif

Exercise Sheet 2
Version 23.04.2020

Exercise 1.

Decide for each of the following pairs of sets X and binary operations $*\colon X \times X \to X$ whether $(X, *)$ is a (commutative) semigroup, monoid, or group.

i) $X := \mathbb{Q}$, $a * b := \frac{1}{2}(a + b)$ for all $a, b \in \mathbb{Q}$

ii) $X := \mathbb{Z}$, $a * b := a + b - 1$ for all $a, b \in \mathbb{Z}$

iii) $X := \mathbb{N}$, $a * b := \max(a, b)$ for all $a, b \in \mathbb{N}$

Exercise 2.

Let us consider the functions $f_1, f_2, f_3, f_4\colon \mathbb{R} \setminus \{0\} \to \mathbb{R} \setminus \{0\}$ given by

$$\forall x \in \mathbb{R} \setminus \{0\}\colon \quad f_1(x) := x \quad f_2(x) := -x \quad f_3(x) := \frac{1}{x} \quad f_4(x) := -\frac{1}{x}.$$

Show with the aid of a Cayley-table that $(\{f_1, f_2, f_3, f_4\}, \circ)$ is an abelian group and determine all its subgroups.

Exercise 3.

We consider the special monoid of transformations $(\mathcal{T}_{\mathbb{R}}, \circ)$. Furthermore, we set

$$\mathcal{A}_{\mathbb{R}} := \{f \in \mathcal{T}_{\mathbb{R}} \,|\, \exists a \in \mathbb{R} \setminus \{0\}\, \exists b \in \mathbb{R}\colon\ f(x) = ax + b\, \forall x \in \mathbb{R}\},$$

i.e., the set of all affine functions in $\mathcal{T}_{\mathbb{R}}$ which are not constant. Show that $(\mathcal{A}_{\mathbb{R}}, \circ)$ is a subgroup of $(\mathcal{T}_{\mathbb{R}}, \circ)$.

Exercise 4.

Prove Lemma 2.29 or the lecture. Show with the aid of an example that the intersection of subgroupoids of a given groupoid can be empty.

Exercise 5.

Let $n \in \mathbb{N}$ be fixed.

(a) Prove that $(\mathcal{S}_n, \circ)$ is a group.

(b) Is $(\mathcal{S}_n, \circ)$ an abelian group? Why?

(c) Give one nontrivial subgroup of $(\mathcal{S}_3, \circ)$.