Cryptography

Dr. Patrick Mehlitz, M.Sc. Ameen Naif

Exercise Sheet 3
Version 30.04.2020

Exercise 1.

For a set $S := \{e, u, v, x, y, z\}$, we consider the group $(S, *)$ which is given by the following Cayley-table.

$*$	e	u	v	x	y	z
e	e	u	v	x	y	z
u	u	v	e	y	z	x
v	v	e	u	z	x	y
x	x	z	y	e	v	u
y	y	x	z	u	e	v
z	z	y	x	v	u	e

Determine the order of all its elements and deduce that $(S, *)$ is not cyclic. Verify the relation $\langle\{u, x\}\rangle = S$.

Exercise 2.

We consider the group $(\mathbb{Z} \times \mathbb{Z}, +)$ of all pairs of integers equipped with the componentwise addition, i.e.,

$$\forall (k, \ell), (u, v) \in \mathbb{Z} \times \mathbb{Z}: \quad (k, \ell) + (u, v) := (k + u, \ell + v).$$

Show that $(\mathbb{Z} \times \mathbb{Z}, +)$ is not cyclic. Verify the relation $\langle\{(2, 1), (1, 1)\}\rangle = \mathbb{Z} \times \mathbb{Z}$.

Exercise 3.

Let $(G, \cdot)$ be a cyclic group generated by $a \in G$ and $n := ord(a)$. Prove that $\langle\{a^m\}\rangle = \langle\{a^d\}\rangle$, for any $m \in \mathbb{N}$ and $d := gcd(m, n)$.

Exercise 4.

a) We set $\mathbb{Z} + \sqrt{3}\mathbb{Z} := \{k + \sqrt{3}\ell \,|\, k, \ell \in \mathbb{Z}\}$ and equip this set with the standard addition $+$ and multiplication $\cdot$. Show that $\mathbb{Z} + \sqrt{3}\mathbb{Z}$ is closed under $+$ and $\cdot$. Observing that $(\mathbb{R}, +, \cdot)$ is a ring, deduce that $(\mathbb{Z} + \sqrt{3}\mathbb{Z}, +, \cdot)$ is a ring, too. Is it a field?

b) We set $\mathbb{Q} + \sqrt{3}\mathbb{Q} := \{r + \sqrt{3}s \,|\, r, s \in \mathbb{Q}\}$ and equip this set with the standard addition $+$ and multiplication $\cdot$. Show that $(\mathbb{Q} + \sqrt{3}\mathbb{Q}, +, \cdot)$ is a field.