Martin Schlichenmaier
Université du Luxembourg

Basic Algebraic Structures

Exercise sheet 1

1. Let $(G, \cdot)$ be a group. Show the following
(a) For $a, b, c \in G$ the relation $a \cdot b = a \cdot c$ implies $b = c$.
(b) For $a, b \in G$ we habe $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

2. a) Let $Mat(2 \times 2, \mathbb{R})$ be the set of 2×2 matrices with real entries. Take as operation the multiplication of matrices. Show by exhibiting a counter example that in this case $A \cdot B = A \cdot C$ does not necessarily imply $B = C$ (even if $A \neq 0$).
b) Consider the subset of matrices A with $\det A \neq 0$. Show that this subset is a group. Hence for such matrices $A \cdot B = A \cdot C$ implies $B = C$.

3. Let S_3 be the group of bijective maps from $\{1, 2, 3\}$ to $\{1, 2, 3\}$. Give all elements of this group. Calculate the order of the elements and find all subgroups of S_3. Is this group abelian?

4. Let $(G_1, \cdot_1)$ and $(G_2, \cdot_2)$ be two groups. Define for the Cartesian product $G_1 \times G_2$ the multiplication: $a_1, b_1 \in G_1$, $a_2, b_2 \in G_2$

$$(a_1, a_2) \cdot (b_1, b_2) := (a_1 \cdot b_1, a_2 \cdot b_2).$$

Show that this defines a group structure.

5. Determine up to isomorphy all groups of order less or equal 5. Are these groups abelian?

6. Let G be a group and U, V subgroups of G.
a) Show that $U \cap V$ is also a subgroup of G.
b) Assume that U and V are finite groups such that $\gcd(\#U, \#V) = 1$ (gcd = greatest common divisor). Show that then $U \cap V = \{e\}$, the trivial group.

7. Let G_1 and G_2 be cyclic groups, $\#G_1 = n_1$, $\#G_2 = n_2$.
a) Assume that $\gcd(n_1, n_2) = 1$. Show that $G_1 \times G_2$ is also a cyclic

group and that its order is $n_1 \cdot n_2$.
b) Is the same also true if $\gcd(n_1, n_2) \neq 1$? (Look at $C_2 \times C_2$. Is this a cyclic group? What are the orders of its elements?)

8. Let G be a cyclic group and H a subgroup of G. Show that H is also a cyclic group.

---

9. (a) Let $a = a_n a_{n-1} \dots a_1 a_0$ be the presentation of a natural number a by a decimal expansion. Show (using residue calculus) that $3|a$ if and only if $3|(\sum_{i=1}^{n} a_i)$.
(b) Find a corresponding rule for the divisibility by 9, resp. by 11.

10. Let $\varphi(n)$ be Euler's phi-function which is defined as the number of elements in $\mathbb{Z}_n^*$, the group of units in the ring $\mathbb{Z}_n$. Show that for p and q prime, one has

$$\varphi(p) = (p-1), \qquad \varphi(p \cdot q) = (p-1)(q-1).$$

11. Let $\mathbb{F}_{23}$ be the finite field with 23 elements. For $\bar{5} = 5 \bmod 23$ calculate its inverse element with respect to the multiplication by using Euclid's algorithm (e.g. via expressing the $gcd(n, m)$ as integer combination of n and m).

12. Calculate the inverse elements of the following elements, if they exist.

$$\overline{5} \bmod 3, \quad \overline{5} \bmod 9, \quad \overline{5} \bmod 11,$$
$$\overline{27} \bmod 11, \quad \overline{27} \bmod 64, \quad \overline{27} \bmod 81, \quad \overline{27} \bmod 101.$$

13.
a) As it is known from the lecture, $\mathbb{F}_7^*$ is a cyclic group. Determine all generators.
b) An element a of a field $\mathbb{K}$ is called a square if there exists b in $\mathbb{K}$ such that $b^2 = a$. Determine all squares in $\mathbb{F}_7^*$.

The web-page of the course:
`http://math.uni.lu/schlichenmaier/cours/mics`