INTRODUCTORY NOTES 3. GROUPS AND FIELDS

Please treat every proposition in this text as an exercise.

1. Groups

Definition 1.1. Consider a non-empty set G with a map mult : $G \times G \to G$. Such a map is called a binary operation. In this case, we will denote mult(a, b) by ab. The pair $(G, mult)$ is called a monoid if the following conditions hold:

(1) $a(bc) = (ab)c, \quad \forall a, b, c \in G$;
(2) $\exists e \in G$ such that $ae = ea = a, \quad \forall a \in G$ (e is called the identity element).

Exercise 1.2. Show that the identity element e in a monoid is unique.

Definition 1.3. A monoid G is called a group if $\forall a \in G \, \exists b \in G$ such that

$$ab = ba = e. \tag{1.1}$$

An element b is called the inverse element of a and is denoted by a^{-1}.

Exercise 1.4. Show that for every group element, its inverse element is unique.

Exercise 1.5. Suppose that G is a group, $a, b \in G$ and $ab = e$. Is it always true that $ba = e$?

Proposition 1.6. *Let G be a group. Then for all $a, b \in G$ the equation*

$$ax = b \tag{1.2}$$

has a unique solution.

Definition 1.7. A group G is called cyclic if $\exists a \in G$ such that every $g \in G$ can be written as

$$g = a^m \tag{1.3}$$

for some $m \in \mathbb{Z}$

Definition 1.8. A group G such that

$$ab = ba \, \forall a, b \tag{1.4}$$

is called abelian. In an abelian group, the group operation is usually denoted by $+$, and the inverse element of an element a is denoted by $-a$.

Exercise 1.9. Does there exist a non-abelian group?

Definition 1.10. Let G be a group. A non-empty subset H of the set G is called a subgroup of G if $\forall a, b \in H$ we have that $ab \in H$ and $a^{-1} \in H$.

Proposition 1.11. *Let H be a subgroup of G. Then H is a group with respect to the operation of multiplication inherited from G.*

Proposition 1.12. *Suppose that G is a group and $a \in G$. Among the subgroups of G containing a, there exists a unique minimal subgroup and it is cyclic.*

Definition 1.13. For two groups G and H a map $f : G \to H$ is called a homomorphism of groups if

$$f(ab) = f(a)f(b), \quad \forall a, b \in G. \tag{1.5}$$

If a homomorphism is also a bijection, then it is called an isomorphism of the groups. An isomorphism of a group to itself is called an automorphism of this group.

Note that the multiplications involved in the LHS and the RHS of the equality (1.5) are different: in the LHS, we multiply a and b in the group G, and, in the RHS, we multiply their images in the group H.

Exercise 1.14. For a homomorphism f of groups G and H show that:

(a)
$$f(e_G) = e_H; \tag{1.6}$$

(b)
$$(f(a))^{-1} = f(a^{-1}), \quad \forall a \in G. \tag{1.7}$$

Exercise 1.15. Show that being isomorphic is an equivalence relation on the collection of groups.

Proposition 1.16. *Let G be a group. The set of its automorphisms is a group with respect to the operation of composition of maps.*

Proposition 1.17. *Suppose that G is a group and $a \in G$. Define the map $\psi_a : G \to G$ by*

$$\psi_a(x) := axa^{-1}. \tag{1.8}$$

The map ψ_a is an automorphism of the group G. It is called an inner automorphism of the group G. The set of inner automorphisms is a subgroup of the automorphism group of G.

2. Fields

Definition 2.1. A set $\mathbb{F}$ with binary operations of multiplication and addition is called a field if the following conditions hold:

(1) $(\mathbb{F}, +)$ is an abelian group. We denote its identity element by 0 or by $0_{\mathbb{F}}$.
(2) $(\mathbb{F} \setminus \{0\}, \cdot)$ is an abelian group. We denote its identity element by 1 or by $1_{\mathbb{F}}$. Every group is a non-empty set, hence, $1 \neq 0$
(3) $a(b + c) = ab + ac$, $(a + b)c = ac + bc$, $\quad \forall a, b, c \in \mathbb{F}$.

Exercise 2.2. For a field $\mathbb{F}$ show that $a \cdot 0 = 0$, $\forall a \in \mathbb{F}$.

Exercise 2.3. For a field $\mathbb{F}$ show that $a \cdot (-1) = -a$, $\forall a \in \mathbb{F}$.

Exercise 2.4. Which of the following sets are fields with respect to standard operations:

$$\emptyset, \quad \{0\}, \quad \mathbb{Z}, \quad \mathbb{Q}, \quad \mathbb{R}_+, \quad \mathbb{R} \quad ?$$

Proposition 2.5. *Define the operations of addition and multiplication on the set* $\mathbb{R} \times \mathbb{R}$ *by the following equalities:*

$$(a, b) + (c, d) := (a + c, b + d); \tag{2.1}$$

$$(a, b) \cdot (c, d) := (ac - bd, ad + bc). \tag{2.2}$$

The set $\mathbb{R} \times \mathbb{R}$ *is a field with respect to these operations. It is called the complex field and is denoted by* $\mathbb{C}$*. One usually writes* $a + bi$ *instead of a pair* (a, b)*.*

Definition 2.6. A non-empty subset E of a field $\mathbb{F}$ is called a subfield if E is a field with respect to the operations of addition and multiplication in $\mathbb{F}$.

Proposition 2.7. $\mathbb{R}$ *is a subfield of the field* $\mathbb{C}$*.*

Proposition 2.8. *Let* p *be a prime number. The set* $\mathbb{Z}_p$ *of integers modulo* p *with addition and multiplication modulo* p *is a field.*