Chapter 2: Real numbers

1 Groups

Definition 1 (Group)**.** *Let G be a non-empty set and $\circ : G \times G \to G$ be a binary operator. Then $(G, \circ)$ is a group iff all of the following hold:*

1. *Associativity: $a \circ (b \circ c) = (a \circ b) \circ c$ for all $a, b, c \in G$.*
2. *Identity exists: $\exists e \in G$ such that $\forall a \in G$, $e \circ a = a \circ e = a$. Such an e is called an* identity *of $(G, \circ)$. We can prove that the identity is unique.*
3. *Inverses exist: Let e be an identity of $(G, \circ)$. Then $\forall a \in G$, $(\exists \ell \in G, \ell \circ a = e)$ and $(\exists r \in G, a \circ r = e)$. ℓ is called a* left inverse *of a. r is called a* right inverse *of a.*

$(G, \circ)$ is called symmetric, commutative, *or* abelian *iff $\forall a \in G$, $\forall b \in G$, $a \circ b = b \circ a$.*

Lemma 1. *In a group $(G, \circ)$, the identity is unique and each element has a unique inverse.*

Proof. Let e_1 and e_2 be identities of $(G, \circ)$. Then $e_1 \circ e_2 = e_1$, since e_2 is an identity, and $e_2 \circ e_1 = e_2$, since e_1 is an identity. Hence, $e_1 = e_2$.

Let ℓ be a left inverse and r be a right inverse of $a \in G$. Then

$$\ell = \ell \circ e = \ell \circ (a \circ r) = (\ell \circ a) \circ r = e \circ r = r.$$

Hence, every left inverse equals every right inverse. Hence, they are all equal. $\square$

If we use $+$ as a group operator, we denote identity as 0 and inverse of g as $-g$. If we use $\times$ as a group operator, we denote identity as 1 and inverse of g as g^{-1}.

Definition 2. *Let $(G, \times)$ be a group. Then for any $n \in \mathbb{Z}$ and any $g \in G$, define*

$$g^n = \begin{cases} g \times g \times \ldots \times g \ (n \text{ times}) & \text{if } n > 0 \\ 1 & \text{if } n = 0 \\ g^{-1} \times g^{-1} \times \ldots \times g^{-1} \ (-n \text{ times}) & \text{if } n < 0 \end{cases}.$$

Lemma 2 (Basic properties)**.** *Let $(G, \cdot)$ be a group. Let $a, b \in G$ and $m, n \in \mathbb{Z}$.*

1. *$(ab)^{-1} = b^{-1}a^{-1}$.*
2. *$(a^{-1})^{-1} = a$.*
3. *$a^m a^n = a^{m+n}$.*
4. *$(a^m)^n = a^{mn}$.*
5. *If G is symmetric, $(ab)^n = a^n b^n$.*

2 Fields

Definition 3 (Field)**.** *$(F, +, \times)$ is a field iff it satisfies all of the following:*

1. *$(F, +)$ is a symmetric group. It's identity is denoted as 0.*
2. *$(F - \{0\}, \times)$ is a symmetric group. It's identity is denoted as 1.*
3. *Distributivity: $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.*

Lemma 3 (Basic properties)**.** *Let $(F, +, \times)$ be a field. Let $a, b \in F$.*

1. *$a0 = 0a = 0$.*
2. *$a(-b) = (-a)b = -(ab)$.*
3. *$(-a)(-b) = ab$.*
4. *$ab = 0 \iff (a = 0$ or $b = 0)$.*
5. *$(-a)^{-1} = -a^{-1}$.*

Proof sketches.

1. $a0 = a(0 + 0) = a0 + a0$.
2. $0 = a0 = a(b + (-b)) = ab + a(-b)$.
3. $(-a)(-b) = a(-(-b)) = ab$.
4. Suppose $a \neq 0$. Then $ab = 0 \implies b = a^{-1}0 = 0$.
5. $(-1)(-1) = 1$, so $(-1)^{-1} = -1$. $(-a)^{-1} = ((-1)a)^{-1} = (-1)^{-1}a^{-1} = -a^{-1}$.

□