

Chapter 2: Real numbers

1 Groups

Definition 1 (Group). Let G be a non-empty set and $\circ : G \times G \rightarrow G$ 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

Definition 2 (Standard operators). 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} . $a - b := a + (-b)$. $a/b := ab^{-1}$.

Definition 3. Let (G, \times) be a group. Then for any $n \in \mathbb{Z}$ and any $g \in G$, define

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

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

1. $(F, +)$ is a symmetric group. Its identity is denoted as 0.
2. $(F - \{0\}, \times)$ is a symmetric group. Its 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. $ab = 0 \iff (a = 0 \text{ or } b = 0)$.
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 $(-1)^{-1} = -1$. $(-a)^{-1} = ((-1)a)^{-1} = (-1)^{-1}a^{-1} = -a^{-1}$.

□

3 Partial Orders

Definition 5 (Partial and total orders). Let L be a set and let \leq be a binary predicate over $L \times L$. Then (L, \leq) is called a partial order (aka poset) iff all of the following hold:

1. Reflexivity: $\forall a \in L, a \leq a$.
2. Anti-symmetry: $a \leq b \text{ and } b \leq a \implies a = b$.
3. Transitivity: $a \leq b \text{ and } b \leq c \implies a \leq c$.

Additionally, if $\forall a, b \in L$, we have $a \leq b$ or $b \leq a$, then (L, \leq) is called a total order.

$$a < b :\iff (a \leq b \text{ and } a \neq b). \quad a \geq b :\iff b \leq a. \quad a > b :\iff b < a.$$

Definition 6 (Upper bound). Let (L, \leq) be a poset. Let $S \subseteq L$.

1. $u \in L$ is an upper bound for S iff $s \leq u$ for all $s \in S$. S is called upper-bounded iff an upper bound exists for S .

2. $u \in L$ is a least upper bound or supremum for S (denoted $\sup(S)$) iff u is an upper bound for S and for every upper bound v of S , we have $u \leq v$.

Definition 7 (Lower bound). Let (L, \leq) be a poset. Let $S \subseteq L$.

1. $u \in L$ is a lower bound for S iff $u \leq s$ for all $s \in S$. S is called lower-bounded iff a lower bound exists for S .
2. $u \in L$ is a greatest lower bound or infimum for S (denoted $\inf(S)$) iff u is a lower bound for S and for every lower bound v of S , we have $v \leq u$.

Lemma 4. $\sup(S)$, if it exists, is unique. $\inf(S)$, if it exists, is unique.

4 Ordered Field

Definition 8 (Ordered field). Let $(F, +, \times)$ be a field. $(F, +, \times, \leq)$ is an ordered field iff all of the following hold:

1. (F, \leq) is a total order.
2. $a \leq b \implies (\forall c \in F, a + c \leq b + c)$.
3. $a \geq 0$ and $b \geq 0 \implies ab \geq 0$.

Lemma 5 (Strict inequalities). Let $(F, +, \times, \leq)$ be an ordered field. Then

1. $a < b$ and $b < c \implies a < c$.
2. $a < b \implies (\forall c \in F, a + c < b + c)$.
3. $a > 0$ and $b > 0 \implies ab > 0$.

Definition 9 (Field with positives (non-standard terminology)). Let $(F, +, \times)$ be a field. Let $P \subseteq F$. $(F, +, \times, P)$ is called a field with positives iff

1. $a, b \in P \implies a + b \in P$.
2. $a, b \in P \implies ab \in P$.
3. $\forall a \in F$, exactly one of these is true: $a = 0$, $a \in P$, $-a \in P$.

The following two results state that either of Definitions 8 and 9 could be used to define the other.

Lemma 6. Let $(F, +, \times, P)$ be a field with positives. Let $a \leq b :\iff (b - a \in P \text{ or } b = a)$. Then $(F, +, \times, \leq)$ is an ordered field.

Lemma 7. Let $(F, +, \times, \leq)$ be an ordered field. Let $P := \{x \in F : x > 0\}$. Then $(F, +, \times, P)$ is a field with positives.

Lemma 8. Let $(F, +, \times, \leq)$ be an ordered field.

1. $a_1 \leq b_1$ and $a_2 \leq b_2 \implies a_1 + a_2 \leq b_1 + b_2$.

2. $a^2 \geq 0$ and $(a^2 = 0 \iff a = 0)$.
3. $1 > 0$.
4. $ab > 0 \implies (a > 0 \text{ and } b > 0) \text{ or } (a < 0 \text{ and } b < 0)$.
5. $a > 0 \implies a^{-1} > 0$.

Lemma 9. $(\forall \epsilon > 0, a \leq \epsilon) \implies a \leq 0$.

Definition 10. $|a| := \begin{cases} a & \text{if } a \geq 0 \\ -a & \text{if } a < 0 \end{cases}$.

Lemma 10. Let $(F, +, \times, \leq)$ be an ordered field.

1. $|a| \geq 0$ and $(|a| = 0 \iff a = 0)$.
2. $|-a| = |a|$.
3. $|a| \geq a$ and $|a| \geq -a$.
4. Let $c \geq 0$. Then $|a| \leq c \iff -c \leq a \leq c$.
5. $-|a| \leq a \leq |a|$.
6. $|ab| = |a||b|$.
7. For $a \neq 0$, $|a^{-1}| = |a|^{-1}$.

Lemma 11 (Triangle inequalities). $||a| - |b|| \leq |a + b| \leq |a| + |b|$.

Proof. $-|a| \leq a \leq |a|$ and $-|b| \leq b \leq |b|$. Add these to get $-(|a| + |b|) \leq a + b \leq |a| + |b|$. By Lemma 10.4, we get $|a + b| \leq |a| + |b|$.

By previous result, $|a| = |(a + b) + (-b)| \leq |a + b| + |b|$, so $|a| - |b| \leq |a + b|$. Also, $|b| = |(a + b) + (-a)| \leq |a + b| + |a|$, so $-|a + b| \leq |a| - |b|$. Hence, $-|a + b| \leq |a| - |b| \leq |a + b|$. By Lemma 10.4, we get $||a| - |b|| \leq |a + b|$. \square

5 Real Numbers

Definition 11. The set of real numbers is an ordered field $(\mathbb{R}, +, \times, \leq)$ in which every set with an upper bound has a supremum.