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. □

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*

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

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 4 (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 $(-1)^{-1} = -1$. $(-a)^{-1} = ((-1)a)^{-1} = (-1)^{-1}a^{-1} = -a^{-1}$.

□

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: $a \leq b$ and $b \leq a \implies a = b$.*
3. *Transitivity: $a \leq b$ 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*.*

$a < b \;:\iff (a \leq b$ and $a \neq b)$. $a \geq b \;:\iff b \leq a$. $a > b \;:\iff b < a$.

Definition 6 (Upper and lower 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 $u \leq v$.*

3. *$u \in L$ 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.*

4. *$u \in L$ 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 $v \leq u$.*

5. *S is called* bounded *iff it has a lower bound and an upper bound.*

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

4 Ordered Field

Definition 7 (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 8 (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 7 and 8 could be used to define the other.

Lemma 6. *Let $(F, +, \times, P)$ be a field with positives. Let $a \leq b :\iff (b - a \in P$ 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. $ab > 0 \implies (a > 0$ *and* $b > 0)$ *or* $(a < 0$ *and* $b < 0)$.

5. $a > 0 \implies a^{-1} > 0$.

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

Definition 9. $|a| := \begin{cases} a & \text{if } a \geq 0 \\ -a & \text{if } a < 0 \end{cases}$.

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 $||a| - |b|| \leq |a + b|$. □

Definition 10. *Define* max *and* min *as*

$$\max(x, y) := \begin{cases} x & \text{if } x \geq y \\ y & \text{if } y > x \end{cases}. \qquad \min(x, y) := \begin{cases} y & \text{if } x \geq y \\ x & \text{if } y > x \end{cases}.$$

Lemma 12. max *and* min *are symmetric and associative, i.e.,* $\max(a, b) = \max(b, a)$, $\max(\max(a, b), c) = \max(a, \max(b, c))$. $\min(a, b) = \min(b, a)$, *and* $\min(\min(a, b), c) = \min(a, \min(b, c))$.

5 Supremum, Infimum, and 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. (In fact, such an ordered field is unique, but proving that is beyond the scope of the course/book.)*

Lemma 13. *Let* $S \subseteq \mathbb{R}$ *and* $S' = \{-x : x \in S\}$. *Then* $\inf(S) = -\sup(S')$ *and* $\sup(S) = -\inf(S')$.

Lemma 14. *Let* $S \subseteq \mathbb{R}$. *Then for any* $\alpha \in \mathbb{R}$, $(\forall x \in S, x \leq \alpha) \iff \sup(S) \leq \alpha$, *and* $(\forall x \in S, x \geq \alpha) \iff \inf(S) \geq \alpha$.

Lemma 15. *Let* $A, B \subseteq \mathbb{R}$. *Then*

1. $\sup(A \cup B) = \max(\sup(A), \sup(B))$ *and* $\inf(A \cup B) = \min(\inf(A), \inf(B))$.

2. $A \subseteq B \implies \inf(B) \leq \inf(A) \leq \sup(A) \leq \sup(B)$.

Definition 12. *Let* $f : D \to \mathbb{R}$. *Then* $\sup_{x \in D} f(x) := \sup(f(D))$.

Lemma 16 (Archimedian Properties, floor, and ceil)**.** *Let* $x \in \mathbb{R}_{>0}$. *Then*

1. $\exists n \in \mathbb{N}$ *such that* $x < n$.

2. $\exists n \in \mathbb{N}$ *such that* $1/n < x$.

3. *There is a unique* $n \in \mathbb{N} \cup \{0\}$ *such that* $n \leq x < n + 1$. *(We denote* n *as* $\lfloor x \rfloor$.*)*

4. *There is a unique* $n \in \mathbb{N}$ *such that* $n - 1 < x \leq n$. *(We denote* n *as* $\lceil x \rceil$.*)*

Proof.

1. Suppose this is not true. Then x is an upper-bound of $\mathbb{N}$. By completeness property of $\mathbb{R}$, $u := \sup(\mathbb{N})$ exists. Hence, $u - 1$ is not an upper-bound of $\mathbb{N}$, and so $\exists m \in \mathbb{N}$ such that $u - 1 < m$. Hence, $u \leq m + 1$. This is a contradiction, since $m + 1 \in \mathbb{N}$.

2. $\exists n \in \mathbb{N}$ such that $n > 1/x$. Hence, $1/n < x$.

3. Let $T := \{m \in \mathbb{N} : x < m\}$. By part 1, $T \neq \emptyset$. By well-ordering of $\mathbb{N}$, T has a least element t. Then $t - 1 \notin T$, so $t - 1 \leq x$. Hence, $t - 1 \leq x < t$. Set $n = t - 1$.

4. Let $T := \{m \in \mathbb{N} : x \leq m\}$. By part 1, $T \neq \emptyset$. By well-ordering of $\mathbb{N}$, T has a least element n. Then $n - 1 \notin T$, so $n - 1 < x$.

□

Lemma 17 ($\mathbb{Q}$ is dense in $\mathbb{R}$)**.** *Let* $x, y \in \mathbb{R}$ *and* $x < y$. *Then* $\exists z \in \mathbb{Q}$ *such that* $x < z < y$.

Proof. By Archimedian property, $\exists n \in \mathbb{N}$ such that $1/n < y - x$. Then $nx + 1 < y$. Let $k := \lfloor nx \rfloor + 1$. Then $nx < \lfloor nx \rfloor + 1 \leq nx + 1 < ny$. Hence, $x < k/n < y$. □

Lemma 18 (Principle of iterated suprema)**.** *Let* X *and* Y *be non-empty sets and* $f : X \times Y \to \mathbb{R}$ *be upper-bounded. Then*

$$\sup_{(x,y) \in X \times Y} f(x, y) = \sup_{x \in X} \sup_{y \in Y} f(x, y) = \sup_{y \in Y} \sup_{x \in X} f(x, y).$$

Proof. We will prove the first equality, since the second's proof is similar. Let

$$g(x) := \sup_{y\in Y} f(x,y) \qquad \alpha := \sup_{x\in X} g(x) \qquad \beta := \sup_{(x,y)\in X\times Y} f(x,y)$$

We need to show that $\alpha = \beta$. For any $z \in \mathbb{R}$,

$$\begin{aligned} &\beta \le z \\ \iff &\forall (x,y) \in X \times Y, f(x,y) \le z \\ \iff &\forall x \in X, \forall y \in Y, f(x,y) \le z \\ \iff &\forall x \in X, g(x) \le z \\ \iff &\alpha \le z. \end{aligned}$$

□

Lemma 19. *Let X and Y be non-empty sets and $f : X \times Y \to \mathbb{R}$ be bounded. Then $\alpha \le \beta$, where*

$$\alpha := \sup_{x\in X} \inf_{y\in Y} f(x,y), \qquad \beta := \inf_{x\in X} \sup_{y\in Y} f(x,y).$$

(Hint: Consider the special case where X and Y are finite, and then generalize.)

Proof. Pick any $\epsilon > 0$. Then $\exists x^* \in X$ such that $\inf_{y\in Y} f(x^*,y) \ge \alpha - \epsilon$, and $\exists y^* \in Y$ such that $\sup_{x\in X} f(x,y*) \le \beta + \epsilon$. Hence,

$$\alpha - \epsilon \le \inf_{y\in Y} f(x^*,y) \le f(x^*,y^*) \le \sup_{x\in X} f(x,y^*) \le \beta + \epsilon.$$

Hence, $\forall \epsilon > 0$, we get $\alpha - \beta \le 2\epsilon$. Hence, $\alpha - \beta \le 0$. □

6 Intervals

Definition 13 (Interval)**.** *Let $a, b \in \mathbb{R}$, such that $a \le b$.*
The following are called closed intervals*:*

1. $[a,b] := \{x \in \mathbb{R} : a \le x \le b\}$.
2. $[a,\infty) := \{x \in \mathbb{R} : a \le x\}$.
3. $(-\infty,b] := \{x \in \mathbb{R} : x \le b\}$.

The following are called open intervals*:*

1. $(a,b) := \{x \in \mathbb{R} : a < x < b\}$.
2. $(a,\infty) := \{x \in \mathbb{R} : a < x\}$.
3. $(-\infty,b) := \{x \in \mathbb{R} : x < b\}$.

The following are called half-open intervals*:*

1. $[a,b) := \{x \in \mathbb{R} : a \le x < b\}$.
2. $(a,b] := \{x \in \mathbb{R} : a < x \le b\}$.

$(-\infty, \infty) := \mathbb{R}$ *is both an open and closed interval.*

Lemma 20. *Let $S \subseteq \mathbb{R}$ be a non-empty set. Then S is an interval iff $\forall x \in S, \forall y \in S, (x < y \implies [x, y] \subseteq S)$.*

Proof sketch. Let $a := \inf(S)$ and $b := \sup(S)$. (Let $a := -\infty$ if S is not lower bounded, and $b := \infty$ if S is not upper bounded.)

Pick any $z \in (a, b)$. Since z is not a lower or upper bound of S, $\exists x \in S$ such that $x < z$, and $\exists y \in S$ such that $y < z$. Then $z \in [x, y]$ and $[x, y] \subseteq S$, so $z \in S$. Hence, $(a, b) \subseteq S$. Also, $S \subseteq [a, b]$ (where $[a, \infty] := [a, \infty)$ and $[-\infty, b] := (-\infty, b]$). □

Lemma 21. *Let $[a_i]_{i\in\mathbb{N}}$ and $[b_i]_{i\in\mathbb{N}}$ be infinite sequences and $I_n := [a_n, b_n]$ for all $n \in \mathbb{N}$. Then*

6.1 Nested Intervals

Let $[a_n]_{n\in\mathbb{N}}$ and $[b_n]_{n\in\mathbb{N}}$ be two sequences of real numbers such that $a_i \le a_{i+1} \le b_{i+1} \le b_i$ for all $i \in \mathbb{N}$. Let $I_n := [a_n, b_n]$ for $n \in \mathbb{N}$. Let $I := \cap_{n\in\mathbb{N}} I_n$.

$\forall n \in \mathbb{N}$, $a_1 \le a_n \le b_n \le b_1$. Hence, sequences $[a_n]_{n\in\mathbb{N}}$ and $[b_n]_{n\in\mathbb{N}}$ are bounded. Let $a := \sup_{n\in\mathbb{N}} a_n$ and $b := \inf_{n\in\mathbb{N}} b_n$. Let $\ell := \inf_{n\in\mathbb{N}}(b_n - a_n)$ ($\ell \ge 0$, since $b_n - a_n \ge 0$ for all $n \in \mathbb{N}$).

Lemma 22. $I = [a, b]$.

Proof. Let $z \in \mathbb{R}$.

$$\begin{aligned}
& z \in [a, b] \\
\iff & (\forall n \in \mathbb{N}, a_n \le z) \text{ and } (\forall n \in \mathbb{N}, b_n \le z) \\
\iff & (\forall n \in \mathbb{N}, a_n \le z \le b_n) \\
\iff & (\forall n \in \mathbb{N}, z \in I_n) \\
\iff & z \in I.
\end{aligned}$$

□

Lemma 23. $\ell := b - a$.

Proof.

$$\begin{aligned}
& (\forall n \in \mathbb{N}, a_n \le a) \text{ and } (\forall n \in \mathbb{N}, b \le b_n) \\
\implies & (\forall n \in \mathbb{N}, a_n \le a \text{ and } b \le b_n) \\
\implies & (\forall n \in \mathbb{N}, b - a \le b_n - a_n) \\
\implies & b - a \le \inf_{n\in\mathbb{N}} (b_n - a_n) = \ell.
\end{aligned}$$

Let $\epsilon > 0$. Then $\exists p \in \mathbb{N}$ such that $a_p \ge a - \epsilon$, and $\exists q \in \mathbb{N}$ such that $b_q \le b + \epsilon$. Let $r := \max(p, q)$. Then

$$a - \epsilon \le a_p \le a_r \le b_r \le b_q \le b + \epsilon.$$

Hence,

$$\ell \le b_r - a_r \le (b + \epsilon) - (a - \epsilon) = (b - a) + 2\epsilon.$$

Since this is true for all $\epsilon > 0$, we get $\ell \le b - a$. □