Analysis

Gaotang Li

July 24, 2022

Contents

Part I

Foundations

Chapter 1

Groups and Homomorphism

1.1 Basics

Definition 1.1.1 (Group). A pair $(G, \odot)$ consisting of a nonempty set G and an operation $\odot$ is called a **group** if the following holds:

- G is closed under the operation $\odot$
- $\odot$ is associative
- $\odot$ has an identity element e
- Each $g \in G$ has an **inverse** $h \in G$ such that $g \odot h = h \odot g = e$

Definition 1.1.2 (Abelian group). A group $G, \odot$ is called **commutative** or **Abelian** if $\odot$ is a commutative operation on G.

Remark. Let $G = (G, \odot)$

(a) the identity element e is unique

(b) Each $g \in G$ has a unique inverse which we denote by g^b. In particular $e^b = e$.

(c) For each $g \in G$, we have $\left(g^b\right)^b = g$.

(d) For arbitrary group elements g and h, $(g \odot h)^b = h^b \odot g^b$

Example. (a) Let $G := \{e\}$ be a one element set. Then $\{G, \odot\}$ is an Abelian group, the **trivial group**, with the (only possible) operation $e \odot e = e$.

(b) Let X be a nonempty set, and S_X be the set of all bijections from X to itself. Then $S_X := (S_X, \circ)$ is a group with identity element id_X when $\circ$ denotes the composition of functions. Further, the inverse function f^{-1} is the inverse of $f \in S_X$ in the group. When X is finite, the element of S_X are called permutations and S_X is called the **permutation group** of X.

(c) Let X be a nonempty set and $G, \odot$ a group. With the induced operation $\odot$, $\left(G^X, \odot\right)$ is a group. The inverse of $f \in G^X$ is the function

$$f^b \colon X \to G, \quad x \mapsto (f(x))^b$$

(d) Let $G_1, \ldots, G_m$ be groups. Then $G_1 \times \cdots \times G_m$ with the operation defined analogously to (d) is a group called the **direct product** of $G_1, \ldots, G_m$.

1.2 Subgroup

Definition 1.2.1 (Subgroup). Let $G = (G, \odot)$ be a group and H a nonempty subset of G, if

- $H \odot H \subseteq H$
- $h^b \in H$ for all $h \in H$

then $H := (H, \odot)$ is itself a group and is called a **subgroup** of G.

Remark. Here we use the same symbol $\odot$ for the restriction of the operation to H. Since H is nonempty, there is some $h \in H$ and so, from the two axioms above, $e = h^b \odot h$ is also in H.

Example. Let $G = (G, \odot)$ be a group.

(a) The trivial subgroup $\{e\}$ and G itself are subgroups of G, the smallest and largest subgroups with respect to inclusion

(b) If H_α, $\alpha \in A$ are subgroups of G, then $\bigcap_\alpha H_\alpha$ is also a subgroup of G.

1.3 Cosets

Definition 1.3.1 (Coset). Let N be a subgroup of G and $g \in G$. Then $g \odot N$ is the **left coset** and $N \odot g$ is the **right coset** of $g \in G$ with respect to N.

Remark. The definition of coset is related to the particular element.

Note. If we define

$$g \sim h \Leftrightarrow g \in h \odot N \tag{1.1}$$

Then $\sim$ is an equivalence on G.

Proof. $\sim$ is reflexive because $e \in N$
Let $g \in h \odot N$ and $h \in k \odot N$, then

$$g \in (k \odot N) \odot N = k \odot (N \odot N) = k \odot N$$

Let $g \in h \odot N$, then there is some $n \in N$ with $g = h \odot n$. Then it follows that $h = g \odot n^b \in N$. ∎

Here 1.1 defines an equivalence relation on G. For the equivalence classes $[\cdot]$ with respect to $\sim$, we have

$$[g] = g \odot N, \quad g \in G. \tag{1.2}$$

For this reason, we denote $G/\sim$ by G/N, and call G/N the **set of left cosets** of G **modulo** N. Particularly, we have subgroups N such that

$$g \odot N = N \odot g, \quad g \in G. \tag{1.3}$$

Such a subgroup 1.3 is called a **normal subgroup** of G. We call $g \odot N$ the **coset of** g **modulo** N since each left coset is a right coset and vice versa. We have a well-defined operation on G/N where N is the normal subgroup of G, induced from $\odot$, such that

$$(G/N) \times (G/N) \to G/N, \quad (g \odot N, h \odot N) \mapsto (g \odot h) \odot N \tag{1.4}$$

Proposition 1.3.1. Let G be a group and N a normal subgroup of G. Then G/N with the induced operation is a group, the **quotient group of G modulo** N.

Proof. It is easy to check that the operation is associative. Since $(e \odot N) \odot (g \odot N) = (e \odot g) \odot N = g \odot N$, the identity element of G/N is $N = e \odot N$. Also

$$\left(g^b \odot N\right) \odot (g \odot N) = \left(g^b \odot g\right) \odot N = N$$

■

Remark. (a) In notion of 1.1, $[e] = N$ is the identity element of G/N and $[g]^b = [g^b]$ is the inverse of $[g] \in G/N$. We also have $[g] \odot h = [g \odot h]$, $g, h \in G$.

(b) Any subgroup N of an Abelian group G is normal and so G/N is a group. Meanwhile, G/N is Abelian.

1.4 Homomorphisms

Definition 1.4.1 (Homomorphism). Let $G = (G, \odot)$ and $G' = (G', \circledast)$ be groups... A function $\varphi\colon G \to G'$ is called a **(group) homomorphism** if

$$\varphi(g \odot h) = \varphi(g) \circledast \varphi(h), \quad g, h \in G$$

Definition 1.4.2 (Endomorphism). A homomorphism from G to itself

Remark. (a) Let e and e' be the identity elements of G and G' respectively, and let $\varphi\colon G \to G'$ be a homomorphism. Then

$$\varphi(e) = e' \quad \text{and} \quad (\varphi(g))^b = \varphi(g^b), \quad g \in G$$

Proof. $e' \circledast \varphi(e) = \varphi(e) = \varphi(e \odot e) = \varphi(e) \circledast \varphi(e)$
$e' = \varphi(e) = \varphi\left(g^b \odot g\right) = \varphi\left(g^b\right) \circledast \varphi(g)$ ■

(b) Let $\varphi\colon G \to G'$ be a homomorphism. The **kernel** of φ, $\ker(\varphi)$, defined by

$$\ker(\varphi) \coloneqq \varphi^{-1}(e') = \{g \in G\,;\ \varphi(g) = e'\}$$

is a normal subgroup of G.

Proof. First, try to prove $\ker(\varphi)$ is a subgroup of G. For all $g, h \in G$,

- $\varphi(g \odot h) = \varphi(g) \circledast \varphi(h) = e' \circledast e' = e'$
- $\varphi\left(g^b\right) = (\varphi(g))^b = (e')^b = e'$

Second, try to prove it is a normal subgroup. Let $h \in g \odot \ker(\varphi)$. Then we there is some $n \in G$ such that $\varphi(n) = e'$ and $h = g \odot n$. For $m \coloneqq g \odot n \odot g^b$, we have

$$\varphi(m) = \varphi(g) \circledast \varphi(n) \circledast \varphi(g^b) = \varphi(g) \circledast \varphi(g^b) = e'$$

and hence $m \in \ker(\varphi)$. Since $m \odot g = g \odot m = h$, this implies that $h \in \ker(\varphi) \odot g$. So $\ker(\varphi) \odot g \subseteq g \odot \ker(\varphi)$. Similarly one can show $g \odot \ker(\varphi) \subset \ker(\varphi) \odot g$. ■

(c) Let $\varphi\colon G \to G'$ be a homomorphism and $N \coloneqq \ker(\varphi)$. Then

$$g \odot N = \varphi^{-1}(\varphi(g)), \quad g \in G,$$

and so

$$g \sim h \Leftrightarrow \varphi(g) = \varphi(h), \quad g, h \in G,$$

where $\sim$ denotes the equivalence relation 1.1.

(d) A homomorphism is injective if and only if its kernel is trivial, that is, $\ker(\varphi) = \{e\}$

(e) The image $\mathrm{im}(\varphi)$ of a homomorphism $\varphi\colon G \to G'$ is a subgroup of G'.

Example. (a) The constant function $G \to G'$, $g \mapsto e'$ is a homorphism, the **trivial** homomorphism.

(b) The identity function $\mathrm{id}_G\colon G \to G$ is an endomorphism.

(c) Compositions of homomorphisms (endomorphisms) are homomorphisms (endomorphisms).

(d) If $\varphi\colon G \to G'$ is a bijective homomorphism, then so is $\varphi^{-1}\colon G \to G'$

Definition 1.4.3 (Isomorphism)**.** A homomorphism $\varphi\colon G \to G'$ is called a (**group**) **isomorphism** from G to G' if φ is bijective.
In this circumstance, we say that the groups G and G' are **isomorphic** and write $G \cong G'$.

Definition 1.4.4 (Automorphism)**.** An isomorphism from G to itself.

Chapter 2

Rings, Fields and Polynomials

2.1 Rings

Definition 2.1.1 (Ring). A triple $(R, +, \cdot)$ consisting of a nonempty set R and operations, **addition** $+$ and **multiplication** $\cdot$, is called a **ring** if

- $(R, +)$ is an Abelian group
- Multiplication is associative
- The **distributive law** holds:

$$(a + b) \cdot c = a \cdot c + b \cdot, \quad c \cdot (a + b) = c \cdot a + c \cdot b, \quad a, b, c \in R$$

Note. A ring is called **commutative** if multiplication is commutative.
If there is an identity element with respect to multiplication, then it is written as 1_R or simply 1, and is called the **unity** (or **multiplicative identity**) of R, and we say $(R, +, \cdot)$ is a **ring with unity**.
When the addition and multiplication operations are clear from context, we write simply R instead of $(R, +, \cdot)$.

Example. (a) The **trivial ring** has exactly one element 0 and is itself denoted by 0. A ring with more than one element is **nontrivial**. If R is a ring with unity, then it follows from $1_R \cdot a = a$ for each $a \in R$, that R is trivial if and only if $1_R == 0_R$.

(b) Suppose R is a ring and S is a nonempty subset of R that satisfies the following:

- S is a subgroup of $(R, +)$.
- $S \cdot S \subseteq S$

Then S itself is a ring, a **subring** of R, and R is called an **overring** of S. If R is commutative then so is S, but the converse is not true in general.

(c) Intersections of subrings are subrings.

Definition 2.1.2 (Ring Homomorphism). Let R and R' be rings. A (**ring**) **homomorphism** is a function $\varphi\colon R \to R'$ which is compatible with the ring operations, that is,

$$\varphi(a + b) = \varphi(a) + \varphi(b), \quad \varphi(ab) = \varphi(a)\varphi(b), \; a, b \in R \tag{2.1}$$

Note. If, in addition, φ is bijective, then φ is called a (**ring**) **isomorphism** and R and R' are **isomorphic**.

A homomorphism φ from R to itself is a **(ring) endomorphism**. If φ is an isomorphism, then it is a **(ring) automorphism**.

Example. (a) A ring homomorphism $\varphi\colon R \to R'$ is, in particular, a group homomorphism from $(R,+)$ to $(R',+)$. The **kernel**, $\ker(\varphi)$, of φ is defined to be the kernel of this group homomorphism, that is,

$$\ker(\varphi) = \{a \in R; \varphi(a) = 0\} = \varphi^{-1}(0)$$

(b) The **zero function** $R \to R'$, $a \mapsto 0_{R'}$ is a homomorphism with $\ker(\varphi) = R$.

(c) Let R and R' be rings with unity and $\varphi\colon R \to R'$ a homomorphism. As (b) shows, it does not necessarily follow that $\varphi(1_R) = 1_{R'}$. This can be seen as a consequence of the fact that, with respect to multiplication, a ring is not a group.

2.2 Consequence of Ring Definitions

Definition 2.2.1 (The Binomial Theorem)**.** Let a and b be two commuting elements ($ab = ba$) of a ring R with unity. Then, for all $n \in \mathbb{N}$,

$$(a+b)^b = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Lemma 2.2.1. For $m \in \mathbb{N}$ with $m \geq 2$, an element $\alpha = (\alpha_1 \ldots \alpha_m) \in \mathbb{N}^m$ is called a **multi-index**. The **length** $|\alpha|$ of a multi-index $\alpha \in \mathbb{N}^m$ is defined by

$$|\alpha| \coloneqq \sum_{j=1}^{m} \alpha_j$$

Set also

$$\alpha! \coloneqq \prod_{j=1}^{m} (\alpha_j)!,$$

and define the **natural (partial) order** on $\mathbb{N}^m$ by

$$\alpha \leq \beta \rightleftarrows (\alpha_j \leq \beta_j,\ \ 1 \leq j \leq m).$$

for $a = (a_1, \ldots, a_m) \in R^m$ and $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{N}^m$

Definition 2.2.2 (The Multinomial Theorem)**.** Let R be a commutative ring with unity. Then for all $m \geq 2$,

$$(\sum_{j=1}^{m} \alpha)^k = \sum_{|\alpha|=k} \frac{k!}{\alpha!} a^\alpha, \quad a = (a_1, \ldots, a_m) \in R^m, \ \ k \in \mathbb{N}.$$

2.3 Field

Definition 2.3.1 (Field)**.** K is a **field** when the following are satisfied:

- K is a commutative ring with unity.
- $0 \neq 1$
- $K^\times \coloneqq K \backslash \{0\}$ is an Abelian group with respect to multiplication.

Note. The Abelian group $K^\times := (K^\times, \cdot)$ is called the **multiplicative group** of K.

Remark. Let K be a field.

(a) For all $a \in K^\times$, $\left(a^{-1}\right)-1 = a$

(b) A field has no zero divisors

(c) Let $a \in K^\times$ and $a \in K^\times$ and $b \in K$. Then there is an unique $x \in K$ with $ax = b$, namely the **quotient** $\frac{b}{a} := b/a := ba^{-1}$

(d) Let K' be a field and $\varphi\colon K \to K'$ a homomorphism with $\varphi \neq 0$. Then

$$\varphi(1_K) = 1_{K'} \quad \text{and} \quad \varphi(a^{-1}) = \varphi(a)^{-1},\ a \in K^\times$$

2.4 Ordered Field

Definition 2.4.1 (Ordered Ring)**.** A ring R with an ordered $\leq$ is called an **ordered ring** if the following holds:

- $(R, \leq)$ is totally ordered.
- $x < y \Rightarrow x + z < y + z, z \in R$
- $x, y > 0 \Rightarrow xy > 0$

Note. This leads to a series of basic arithmetic rules.
We may define absolute value function from $K \mapsto K$.

Proposition 2.4.1. Let K be an ordered field and $x, y, a, \epsilon \in K$ with $\epsilon > 0$.

(i) $x = |x| \operatorname{sign}(x)$, $|x| = x \operatorname{sign}(x)$

(ii) $|x| = |-x|, x \leq |x|$

(iii) $|xy| = |x||y|$

(iv) $|x| \geq 0$ and $(|x| = 0 \Leftrightarrow x = 0)$

(v) $|x - a| < \epsilon \leftrightarrow a - \epsilon < x < a + \epsilon$

(vi) $|x + y| \leq |x| + |y|$ (**triangular inequality**)

Corollary 2.4.1 (reversed triangular inequality)**.** In any ordered field K we have

$$|x - y| \geq ||x| - |y||, \quad x, y \in K.$$

2.5 Formal Power Series

Definition 2.5.1 (formal power series)**.** Let R be a nontrivial ring with unity. On the set $R^{\mathbb{N}} = \operatorname{Funct}(\mathbb{N}, R)$ define addition by

$$(p + q)_n := p_n + q_n, \qquad n \in \mathbb{N},$$

and multiplication by **convolution**,

$$(pq)_n \coloneqq (p \cdot q)_n \coloneqq \sum_{j=0}^{n} p_j q_{n-1} = p_0 q_n + p_1 q_{n-1} + \cdots + p_n q_0$$

for $n \in \mathbb{N}$. Here p_n denotes the value of $p \in R^{\mathbb{N}}$ at $n \in \mathbb{N}$ and is called the n^{th} **coefficient** of p. In this situation an element $p \in R^{\mathbb{N}}$ is called a **formal power series over** R, and we set $R[X] \coloneqq \left(R^{\mathbb{N}}, +, \cdot\right)$

Proposition 2.5.1. $R[X]$ is a ring with unity, the **formal power series ring over** R. If R is commutative, then so is $R[X]$

2.6 Polynomials

Definition 2.6.1 (Polynomial)**.** A **polynomial over** R is a formal power seres $p \in R[X]$ such that $\{n; p_n \neq 0\}$ is finite, in other words, $p_n = 0$ "almost everywhere".

Chapter 3

The Real Numbers

Starting words: we seek an ordered **extension field** of $\mathbb{Q}$ in which the equation $x^2 = a$ is solvable for each $a > 0$.

3.1 Order Completeness

We say a totally ordered set X is **order complete** (or X satisfies the **completeness axiom**) if every nonempty subset of X which is bounded above has a supremum.

Proposition 3.1.1. Let X be a totally ordered set. Then the followings are equivalent:

(i) X is order complete.

(ii) Every nonempty subset of X which is bounded below has an infimum.

(iii) For all nonempty subsets A, B of X such that $a \leq b$ for all $(a, b) \in A \times B$, there is some $c \in X$ such that $a \leq c \leq b$ for all $(a, b) \in A \times B$ (**Dedekind cut property**)

Note. A relation $\leq$ on X is a **partial order** on X if it is reflexive, transitive and **anti-symmetric**, that is,

$$(x \leq y)(y \leq x) \Rightarrow x = y$$

If $\leq$ is a partial order on X, then the pair $(X, \leq)$ is called a **partially ordered set**. If, in addition,

$$\forall x, y \in X : (x \leq y) \vee (y \leq x)$$

then $\leq$ is called a **total order** on X and $(X, \leq)$ is a **totally ordered set**.

Corollary 3.1.1. A totally ordered set is order complete if and only if every nonempty bounded subset has a supremum and an infimum.

Theorem 3.1.1 (Dedekind's Construction of the Real Numbers)**.** There is, up to isomorphism, a unique order complete extension field $\mathbb{R}$ of $\mathbb{Q}$. This extension is called **the field of real numbers**.

Proposition 3.1.2 (A Characterization of Supremum and Infimum)**.** Followed from natural order defined by $\mathbb{R}$.

(i) If $A \subseteq \mathbb{R}$ and $x \in \mathbb{R}$, then

(a) $x < \sup(A) \Leftrightarrow \exists a \in A$ such that $x < a$.

(b) $x < \inf(A) \Leftrightarrow \exists a \in A$ such that $x > a$.

(ii) Every subset A of $\mathbb{R}$ has a supremum and an infimum in $\mathbb{R}$

3.2 The Consequence of Order Completeness

The Archimedean Property

Proposition 3.2.1 (Archimedes). $\mathbb{N}$ is not bounded above in $\mathbb{R}$, that is, for each $x \in \mathbb{R}$ there is some $n \in \mathbb{N}$ such that $n > x$.

Corollary 3.2.1. Equivalent statements as the above proposition

(a) Let $a \in \mathbb{R}$. If $0 \leq a \leq 1/n$ for all $n \in \mathbb{N}^{\times}$.

(b) For each $a \in \mathbb{R}$ with $a > 0$ there is some $n \in \mathbb{N}^{\times}$ such that $1/n < a$.

The Density of the Rational/Irrational Numbers in $\mathbb{R}$

Proposition 3.2.2. For all $a, b \in \mathbb{R}$ such that $a < b$, there is some $r \in \mathbb{Q}$ such that $a < r < b$.

Proposition 3.2.3 (n^{th} Roots). For all $a \in \mathbb{R}^{+}$ and $n \in \mathbb{N}^{\times}$, there is a unique $x \in \mathbb{R}^{+}$ such that $x^n = a$

Proposition 3.2.4. For all $a, b \in \mathbb{R}$ such that $a < b$, there is some $\xi \in \mathbb{R} \backslash \mathbb{Q}$ such that $a < \xi < b$.

Intervals

An **interval** is a subset J of $\mathbb{R}$ such that

$$(x, y \in J, x < y) \Rightarrow (z \in J \text{for} x < z < y)$$

If J is a nonempty interval, then $\inf(J) \in \bar{\mathbb{R}}$ is the **left endpoint** and $\sup(J) \in \bar{\mathbb{R}}$ is the **right endpoint** of J. J is **closed on the left** if $a := \inf(J)$ is in J, and otherwise it is **open on the left**. The same applies to the other side.

An interval is **perfect** if it contains at least two points. It is **bounded** if both endpoints are in $\mathbf{R}$ and is **unbounded** otherwise. If J is a bounded interval, then the nonnegative number $|J| := \sup(J)$ - $\inf(J)$ is called the **length** of J.