

1 Group

1.1 Law of Composition

Definition 1.1 (Composition). *Composition (or Law of composition) on a set S is to combine two element $a, b \in S$, to get another element p in S :*

$$S \times S \rightarrow S.$$

Here, \times means Cartesian product of two sets. We can denote the composition in several ways:

$$p = ab \quad p = a \cdot b \quad p = a \circ b \quad p = a + b.$$

We will often use ab (or $a \cdot b$ when necessary) to denote the composition of a and b in this document.

Example

- In the set \mathbb{N} , operation “add” $+$ is a law of composition. It takes two elements of $a, b \in \mathbb{N}$ and gives an element $a + b \in \mathbb{N}$. e.g. $(2, 3) \mapsto 5$, $(5, 1) \mapsto 6$
- In the set \mathbb{R} , operation “multiply” \cdot is a law of composition. It takes two elements of $a, b \in \mathbb{R}$ and gives an element $a \cdot b \in \mathbb{R}$. e.g. $(-1, 4) \mapsto -4$, $(2, 3.5) \mapsto 7$

Note that the definition of composition naturally brings out the property of closure — the composition of two element of S is still in the same set.

A way of defining composition is using functions. $f: S \times S \rightarrow S$, so for $a, b \in S$, $f(a, b)$ is the composition of a and b .

Definition 1.2 (Associativity). *For element a, b and c , if the composition satisfies $(ab)c = a(bc)$, then the composition is **associative**.*

For multiple element a_1, a_2, \dots, a_n , there’s only one distinct way to define the composition of them:

$$a_1 a_2 \cdots a_n = (a_1 \cdots a_i)(a_i \cdots a_n),$$

where $1 \leq i < n$. For instance,

$$a_1 a_2 a_3 a_4 = a_1(a_2 a_3 a_4) = (a_1 a_2)(a_3 a_4) = (a_1 a_2 a_3)a_4 = a_1(a_2 a_3)a_4.$$

Definition 1.3 (Commutativity). *The composition of two element a and b is called **commutative** if $ab = ba$.*

Example Addition in \mathbb{R} is commutative: $a, b \in \mathbb{R}, a + b = b + a$.

1.2 Special elements

Definition 1.4 (Identity element). *If $\forall s \in S, \exists e \in S$ such that $es = s$, then e is the **left identity** of S . Likewise, e is the **right identity** if $se = s$. If e is both left identity and right identity, then it's called a **two-sided identity** or simply **identity**.*

If we use multiplication to represent composition, then 1 is commonly used as the symbol of identity. And 0 is often identity for addition representation.

Example

- Consider zero in \mathbb{Z} . For all $a \in \mathbb{Z}$, $0 + a = a$, so 0 is the left identity. And by commutativity we also have $a + 0 = a$, so 0 is also the right identity. Therefore, 0 is the identity of addition on \mathbb{Z}
- 1 is the identity of multiplication on \mathbb{R} , because $\forall a \in \mathbb{R}, 1 \cdot a = a \cdot 1 = a$

Definition 1.5 (Inverse). *Let 1 be the identity. If $\forall a \in S, \exists l \in S$ such that $la = 1$, then l is called the **left inverse** of a . Likewise, $ar = 1$ then r is called the **right inverse** of a . If b is both left and right inverse of a , then it's called the **two-sided inverse** or simply **inverse** of a , denoted by a^{-1} .*

Example

- -3 is the additive inverse of 3 in \mathbb{R} , because $(-3) + 3 = 3 + (-3) = 0$ and 0 is the identity of addition.
- $1/2$ is the multiplicative inverse of 2 in \mathbb{R} , because $(1/2) \times 2 = 2 \times (1/2) = 1$ and 1 is the identity of multiplication.

A fraction $\frac{a}{b}$ is exactly the composition of a and b^{-1} . And the notation $\frac{a}{b}$ is not recommended, because sometimes the composition is not commutative, therefore ab^{-1} and $b^{-1}a$ are different.

The notations like a^n or a^{-n} , $n \in \mathbb{N}$ can be recursively defined as below:

$$\begin{aligned}a^{n+1} &:= a^n a, \\a^{-n-1} &= a^{-n} a^{-1}, \\a^0 &= 1.\end{aligned}$$

Proposition 1.1. If inverse of a exists, which means a has left inverse and right inverse, then the left and right inverse are equal, therefore the inverse is unique.

proof. If $a \in G$ has left inverse b and right inverse c . Consider element $bac \in G$, $(ba)c = 1c = c$, and $b(ac) = b1 = b$. By associativity, $(ba)c = b(ac)$, so $c = b$. The inverse is unique. ■

Proposition 1.2. $(ab)^{-1} = b^{-1}a^{-1}$.

proof. $(ab)^{-1}(ab) = 1$ is true, multiply b^{-1} on the right for both sides. $(ab)^{-1}(ab)b^{-1} = 1 \cdot b^{-1}$, which is $(ab)^{-1}a(bb^{-1}) = (ab)^{-1}a \cdot 1 = b^{-1}$. This time multiply a^{-1} on the right for both sides: $(ab)^{-1}aa^{-1} = b^{-1}a^{-1}$, the left-hand side is exactly $(ab)^{-1}$. ■

And this can be easily generalized to n elements (using associativity and induction):

$$(a_1a_2 \dots a_n)^{-1} = a_n^{-1} \dots a_2^{-1}a_1^{-1}.$$

1.3 Group

Definition 1.6. A group (G, \cdot) is a set G equipped with a binary operation \cdot which follows four axioms, namely **closure**, **associativity**, **identity** and **invertibility**.

Remark. If a group is commutative, then it's called **abelian group**.

The four axioms are explained below:

closure For all a, b in G , the result of operation \cdot is still in G . This can be written in the form: $\forall a, b \in G, a \cdot b \in G$.

associativity $\forall a, b, c \in G, (a \cdot b) \cdot c = a \cdot (b \cdot c)$.

identity $\exists e \in G$ such that, $\forall a \in G$, the equation $e \cdot a = a \cdot e = a$ holds. Such an element is unique and is called the **identity element**.

invertibility For each $a \in G$, $\exists b$ in G , commonly denoted a^{-1} , such that $a \cdot b = b \cdot a = e$, where e is the identity element.

We use ordered pair to denote (G, \cdot) a set G equipped with operation \cdot . So the two parts — set and its operation — together forms the algebraic structure. This is critical, because strictly speaking, a set on its own can not be a group. But informally, it's common to say that a set G is a group, if no ambiguity is caused.

Example These are some familiar abelian groups: $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, (\mathbb{R}^+, \times) , $(\mathbb{C}, +)$, (\mathbb{C}, \times) . Take $(\mathbb{R}^+, +)$ for example.

1. Two the addition of positive real numbers a, b is still a real number (closure)
2. $(a + b) + c = a + (b + c)$, which is associativity
3. For any given $a \in \mathbb{R}^+$, $1 \times a = a \times 1 = a$ holds, which indicates that 1 is the multiplicative identity of \mathbb{R}^+
4. For any given $a \in \mathbb{R}^+$, $\exists a^{-1}$ such that $a^{-1} \times a = a \times a^{-1} = 1$ holds, which indicates all $a \in \mathbb{R}^+$ is invertable

Therefore, (\mathbb{R}^+, \times) is a group. Also, for any positive real number a and b , $a \times b = b \times a$. So (\mathbb{R}^+, \times) is also an abelian group.

Remark. Note that (\mathbb{R}, \times) is not a group, because 0 is not invertable: $\nexists r \in \mathbb{R}$ such that $r \times 0 = 0 \times r = 1$.

Proposition 1.3. Left identity e_L and right identity e_R of a group are the same.

proof. $e_L = e_L e_R = e_R$. ■

Proposition 1.4. The (two-sided) identity of G , if exists, must be unique.

proof. Let $e, e' \in G$ identities and $e \neq e'$, i.e. $\forall a \in G$, $e = ei$ as well as $e'a = a$. Hence $e' = e'e = e$. ■

The two propositions above can be concluded with quote below (from Wikipedia):

... it is possible for $(S, *)$ to have several left identities. In fact, every element can be a left identity. In a similar manner, there can be several right identities. But if there is both a right identity and a left identity, then they must be equal, resulting in a single two-sided identity.

Since groups are sets equipped with operations, and we have cardinality to describe how many elements we have in a set, it's natural to have a similar concept to describe the number of elements contained in a group.

Definition 1.7 (Order of a group). *The order of a group describe the number of elements contained in this group. Suppose we have group (G, \cdot) , the order of this group equals the cardinality of G , denoted by $|G|$.*

Example The previous example, abelian group $(\mathbb{Z}, +)$ is an infinite group, because \mathbb{Z} is an infinite set.

Because of invertibility property, a group follows **cancellation law**.

Proposition 1.5. Cancellation law Let a, b, c be elements of a group G :

- if $ac = bc$ or $ca = cb$ then $a = b$
- if $ac = c$ or $ca = c$ then $a = 1$

proof. Proofs of all cases are analogous — by multiplying c^{-1} to both sides. ■

Following corollary is the contrapositive of last proposition which is supported by invertability.

Corollary 1.1. Let a, b, c be elements of a group G :

- if $a \neq b$, then $ca \neq cb$ and $ac \neq bc$
- if $a \neq 1$, then $ca \neq c$ and $ac \neq c$

Concider matrices. Not all matrices are invertable, so we can't just say matrix with multiplication operation is or is not a group.

Definition 1.8 (General linear group). The general linear group of degree n is the set of $n \times n$ invertable matrices:

$$\text{GL}_n := \{n \times n \text{ invertable matrices}\}.$$

And enable to distinguish what kind of elements we are having in the matrices, notations like $\text{GL}_n(\mathbb{R})$ or $\text{GL}_n(\mathbb{C})$ are used.

1.4 半群

半群是弱于群的概念.

Definition 1.9 (半群). (G, \cdot) 被称为半群, 当且仅当 G 对 \cdot 封闭且 \cdot 满足结合律.

如果 (G, \cdot) 中存在 a , 满足 $aa = a$. 则称 a 为 \cdot 运算的幂等元. 借助下面的引理可以证明, 有限的半群中必然存在幂等元.

Lemma 1.1. 如果对于有限半群 G 的元素 a , 存在正整数 $k \geq 2$, 满足 $a^k = a$, 则 G 中存在幂等元.

proof. 对于 $a^k = a$, 若 $k = 2$, a 为幂等元, 引理得证. 若 $k > 2$, 则将等式两边同时乘以 a^{k-2} . 得到 $a^{2(k-1)} = a^{k-1}$. 即 $(a^{k-1})^2 = a^{k-1}$, 而 $a^{k-1} \in G$, 所以 G 中存在幂等元 a^{k-1} . ■

Proposition 1.6. 有限的半群必然包含幂等元, 即若 G 为有限的半群, 则存在 $a \in G$, 使得 $aa = a$.

proof. 对于任意 $a \in G$, 考虑无限序列

$$(a^{2^p})_{p=0}^{\infty} : a, a^2, a^4, a^8, a^{16}, \dots$$

由于封闭性, 序列中每一项都在 G 中, 于是必然存在不同的 s, t 满足 $a^{2^s} = a^{2^t}$. 因为如果不然, 序列中的每一项互不相同, 则 G 不可能有限. 不失一般性地假设 $s > t$, 于是有:

$$a^{2^s} = a^{2^{t+(s-t)}} = a^{2^t 2^{s-t}} = a^{2^t},$$

于是得到 $(a^{2^t})^{2^{s-t}} = a^{2^t}$. 于是我们找到了 $b = a^{2^t} \in G$, 使得存在 $k = 2^{s-t}$, 满足 $b^k = b$, 根据上一个引理, G 中存在幂等元. ■

1.5 子群

Definition 1.10 (子群). (G, \cdot) 为一个群, $H \subseteq G$, 若 H :

- 满足封闭性
- 存在单位元
- 每个元素都可逆

则称 H 为 G 的子群, 记作 $H \leq G$.

每个群 G 都有两个明显的子群, 称为平凡子群, 即单位元构成的集合 $\{1\}$ 以及 G 本身. 若 $H \leq G$, 且 H 不是平凡子群, 则称 H 为 G 的真子群, 记作 $H < G$.

子群只需满足三个条件, 因为结合律自动转移到子集上: $\forall a, b, c \in H, a, b, c \in G$, G 具有结合律, 所以 H 也满足结合律. 换句话说, 群 G 的子集 H 也是一个群, 则 H 为 G 的子群.

1.5.1 整数倍数子群 $\mathbb{Z}a$

定义 $\mathbb{Z}a$ 为 a 的整倍数构成的集合:

$$\mathbb{Z}a := \{ka \mid k \in \mathbb{Z}\}.$$

等价的定义为:

$$\mathbb{Z}a := \{n \mid \exists k \in \mathbb{Z}, n = ka\}.$$

例

$$\mathbb{Z}0 = \{0\},$$

$$\mathbb{Z}1 = \{0, 1, -1, 2, -2, \dots\} = \mathbb{Z},$$

$$\mathbb{Z}2 = \{0, 2, -2, 4, -4, \dots\},$$

$$\mathbb{Z}5 = \{0, 5, -5, 10, -10, \dots\}.$$

可以证明, $\mathbb{Z}a$ 为 $(\mathbb{Z}, +)$ 的子群. $\mathbb{Z}a$ 满足封闭性: $\forall n_1, n_2 \in \mathbb{Z}a, \exists k_1, k_2 \in \mathbb{Z}$ 满足 $n_1 = k_1a, n_2 = k_2a$. 故 $n_1 + n_2 = (k_1 + k_2)a$, 而 $k_1 + k_2 \in \mathbb{Z}$, 所以 $n_1 + n_2 \in \mathbb{Z}a$.

此外, 0 为 $\mathbb{Z}a$ 的单位元; 对于任意 $a \in \mathbb{Z}a$, 都能找到 $-a \in \mathbb{Z}a$, 使得 $a + (-a) = 0$, 即 $\mathbb{Z}a$ 中每个元素可逆.

由于 G 和其子群 H 共享唯一的单位元, 如果 G 的单位元 1 也在 H 中, 那么 1 也一定是 H 的单位元.

$\mathbb{Z}a$ 的重要之处在于下面的命题:

Proposition 1.7. $(\mathbb{Z}, +)$ 的子群一定有 $\mathbb{Z}a$ 的形式.

1.5.2 循环群

下一个重要的抽象子群例子为:

Definition 1.11 (循环群). 群 G 中的元素 x 生成的子群:

$$\langle x \rangle := \{1, x, x^{-1}, x^2, x^{-2}, \dots\}$$

称为 G 循环子群. 如果一个群 H 中任意元素都能写成某一元素 x 的幂次 x^n , 即能由单个元素 x 生成, 则该群被称为循环群.

例 考虑 (\mathbb{R}, \times) 的元素 -1 . -1 的不同幂次得到的元素可能是相同的:

$$\begin{aligned} & \vdots \\ & (-1)^2 = 1 \\ & (-1)^3 = -1 \\ & (-1)^4 = 1 \\ & \vdots \end{aligned}$$

所以实数乘群中, -1 的生成的循环子群为 $\langle -1 \rangle = \{1, -1\}$.

Proposition 1.8. $S = \{n \in \mathbb{Z} \mid x^n = 1\}$ 为 $(\mathbb{Z}, +)$ 的子群.

proof. 封闭性: $\forall n_1, n_2 \in S, x^{n_1} = 1, x^{n_2} = 1, x^{n_1}x^{n_2} = x^{n_1+n_2} = 1$, 所以 $n_1+n_2 \in S$.

单位元: 只需考虑 $(\mathbb{Z}, +)$ 的单位元 0 是否在 S 中即可. 显然, $x^0 = 1, 0 \in S$, 所以 S 存在单位元 0.

逆元: $\forall n \in S, x^n = 1$, 所以 $x^{-n} = x^{-n}x^n = x^0 = 1$. 所以 $-n \in S$. ■

1.5.3 正规子群

Definition 1.12 (正规子群 (Normal subgroup)). 群 G 的子群 N 被称为是正规子群, 当且仅当对任意 $n \in N$, 和任意 $g \in G, gng^{-1} \in N$.

1.6 同态

两个群之间可以存在映射关系, 而满足一定条件的映射称为同态.

Definition 1.13 (同态 (Homomorphism)). 同态 $\varphi: G \rightarrow G'$ 是群 G 到 G' 的映射, 该映射满足:

$$\forall a, b \in G, \quad \varphi(ab) = \varphi(a)\varphi(b).$$

和映射一样, 同态也有像的概念:

$$\varphi(G) := \text{im } \varphi := \{\varphi(x) \mid x \in G\}.$$

Remark. 注意此处 G 和 G' 中的运算都是用乘法表示的, 不代表它们必须是同一种运算. 严格地定义同态应该是下面这样的, $\varphi: (G, \circ) \rightarrow (G', *)$, 其中:

$$\forall a, b \in G, \quad \varphi(a \circ b) = \varphi(a) * \varphi(b).$$

换句话说, 先在 G 中对 a, b 做运算, 然后在映射到 G' 中; 和先映射 a, b 到 G' 中, 然后做 G' 中的运算; 两种路径得到的结果是一样的. 即: G 和 G' 中对应的两组元素, 分别在各自的群内合成, 得到的结果也是满足相同的对应关系. 如: $a' = \varphi(a), b' = \varphi(b)$. 则 $a \circ b = a' * b'$.

例 $\exp: (\mathbb{R}, +) \rightarrow (\mathbb{R}, \times), \exp(x) = e^x$, 为一个同态, 因为 $\exp(x+y) = \exp(x)\exp(y)$. 反过来, 指数函数不是 (\mathbb{R}, \times) 到 $(\mathbb{R}, +)$ 的同态. 对于 $x, y \in \mathbb{R}$, 先合成 xy , 再映射 $\exp(xy)$; 和先映射 $\exp(x), \exp(y)$, 再合成 $\exp(x) + \exp(y)$ 是不同的.

绝对值 $||: (\mathbb{R}, \times) \rightarrow (\mathbb{R}, \times)$ 也是一个同态, $|xy| = |x||y|$.

几个明显的同态 平凡同态: $\varphi: G \rightarrow G'$, 将 G 中的每个元素映射到 G' 中的单位元. 于是 $\forall a, b \in G, \varphi(a) = \varphi(b) = \varphi(ab) = e$. $\varphi(ab) = e = ee = \varphi(a)\varphi(b)$.

对于 $H \leq G$, 存在包含同态: $i: H \rightarrow G, i(x) = x$. H 和 G 的合成法则一致, $\forall x \in H, x \in G, i(x) = x$. 所以 $i(xy) = xy = i(x)i(y)$.

Proposition 1.9. 令 $\varphi: G \rightarrow G'$ 为同态.

1. $a_1, a_2, \dots, a_k \in G, \varphi(a_1 a_2 \cdots a_k) = \varphi(a_1) \varphi(a_2) \cdots \varphi(a_k)$
2. 恒等元映射到恒等元: $\varphi(1_G) = 1_{G'}$
3. 逆元映射为逆元: $\varphi(a^{-1}) = \varphi(a)^{-1}$

proof. (1) 通过归纳法.

(2) $\varphi(a) = \varphi(1_G a) = \varphi(1_G) \varphi(a)$. 两边同时右乘 $\varphi(a)$ 在 G' 中的逆元: $\varphi(a) \varphi(a)^{-1} = \varphi(1_G) \varphi(a) \varphi(a)^{-1}$. 而 $\varphi(a) \varphi(a)^{-1}$ 为 G' 的单位元 $1_{G'}$. 所以 $1_{G'} = \varphi(1_G) 1_{G'} = \varphi(1_G)$.

(3) $aa^{-1} = 1_G$, 同时应用 φ , $\varphi(aa^{-1}) = \varphi(a) \varphi(a^{-1}) = \varphi(1_G) = 1_{G'}$. 两边同时乘以 $\varphi(a)^{-1}$, $\varphi(a)^{-1} \varphi(a) \varphi(a^{-1}) = \varphi(a^{-1}) = \varphi(a)^{-1} 1_{G'} = \varphi(a)^{-1}$. ■

Proposition 1.10. 同态的像为陪域的子群. $\varphi: H \rightarrow G$, 则 $\varphi(H)$ 为 G 的子群.

proof. 封闭性: 对于任意 $x, y \in \varphi(H)$, $\exists a, b \in H, x = \varphi(a), y = \varphi(b)$. $xy = \varphi(a) \varphi(b) = \varphi(ab)$, 由于 $ab \in H, \varphi(ab) \in \varphi(H)$. 所以 $xy \in \varphi(H)$.

单位元: $\forall x \in \varphi(H), \exists a \in H, \varphi(a) = x$. $\varphi(a) = \varphi(ae_H) = \varphi(a) \varphi(e_H)$. 即 $x = x \varphi(e_H)$. 同样地, 从 $\varphi(a) = \varphi(e_H a)$ 可以得到 $x = \varphi(e_H) x$. 所以 $\varphi(e_H)$ 为 $\varphi(H)$ 的单位元.

逆元: $\forall x \in \varphi(H), \exists a \in H, \varphi(a) = x$. $\varphi(aa^{-1}) = \varphi(a) = \varphi(a^{-1}) = x \varphi(a^{-1}) = \varphi(e_H) = e_G$. 同理可以得到, $\varphi(a^{-1}) x = e_G$. 所以 $\varphi(a^{-1})$ 为 x 的逆元. ■

同态的核是定义域中所有映射到陪域单位元的元素集合.

Definition 1.14 (核(kernel)). 设 $\varphi: G \rightarrow G'$ 为同态. 定义同态 φ 的核为:

$$\ker \varphi := \{x \in G \mid \varphi(x) = 1_{G'}\}.$$

容易验证下面的命题.

Proposition 1.11. 同态的核是定义域的子群. 设 $\varphi: G \rightarrow G', \ker \varphi \leq G$.

注意到, $\ker \varphi$ 为 G 的子集, G 的单位元 e_G 也在 $\ker \varphi$ 中, 故 e_G 是 $\ker \varphi$ 的单位元.

Proposition 1.12. 一个同态 $\varphi: G \rightarrow G'$ 的核 $\ker \varphi$ 是一个正规子群.

proof. 要证明 $\forall a \in \ker \varphi, \forall g \in G, gag^{-1} \in \ker \varphi$. 注意到: $gag^{-1} \in G$, 对其应用同态, $\varphi(gag^{-1}) = \varphi(g) \varphi(a) \varphi(g^{-1}) = \varphi(g) e_{G'} \varphi(g^{-1}) = \varphi(g) \varphi(g^{-1}) = e_{G'}$. 所以 $gag^{-1} \in \ker \varphi$. ■

Proposition 1.13. 同态 $\varphi: G \rightarrow G'$ 是单射当且仅当 $\ker \varphi = \{e_G\}$.

proof. 如果 φ 是单射的, 则存在唯一 $a \in G$, 使得 $\varphi(a) = e_{G'}$. 而 $\varphi(e_G) = e_{G'}$, 所以 $a = e_G$. 而对于其余元素, 其像都不为 $e_{G'}$. 故 $\ker \varphi = \{e_G\}$.

若 $\ker \varphi = \{e_G\}$, 对于任意 $a, b \in G$ 满足 $\varphi(a) = \varphi(b)$. $\varphi(a)\varphi(b)^{-1} = \varphi(b)\varphi(b)^{-1} = e_{G'}$. 于是 $ab^{-1} \in \ker \varphi$. 而 $\ker \varphi = \{e_G\}$ 为一个单元素集, 故 $ab^{-1} = e_G$, $a = b$. 说明 φ 为单射. ■

1.7 同构

Definition 1.15 (同构(Isomorphism)). 若同态 $\varphi: G \rightarrow G'$ 是双射的, 则称 G 和 G' 是同构的. 记作 $G \cong G'$.

由此可以看出, 同构是比同态更强的条件.

例 $\exp: (\mathbb{R}, +) \rightarrow (\mathbb{R}, \times)$, $\exp(x) = e^x$, 为一个同态, 也为一个同构, 因为 $\exp: x \mapsto e^x$ 为一个双射.

验证同构的方法 由上一小节的命题, 同态 $\varphi: G \rightarrow G'$ 是单射, 当且仅当 $\ker \varphi = \{e_G\}$. 而 φ 为满射, 当且仅当像 $\varphi(G) = G'$.

Lemma 1.2. 若 $\varphi: G \rightarrow G'$ 为同构, 则其逆映射 $\varphi^{-1}: G' \rightarrow G$ 也是同构.

这说明了, 两个同构的群本质是相同的. 二进制加法群和十进制加法群之间就是一种同构关系, 其结构是完全相同的.

$$1011_2 + 0010_2 = 1101_2,$$

$$11_{10} + 2_{10} = 13_{10}.$$

我们忽略了次要的信息, 而提取出两种代数结构的本质. 两个同构的群, 无论形式上有多么不同, 但其本质都是相同的.