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:*

$$S \times S \to S\,.$$

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 neccessary) 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 natrually 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. $f\colon S \times S \to S$, 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, $\ldots$, 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 $1 \leqslant i < n$. 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 Addtion 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

- Concider 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 $\forall a \in Z$, $1 \cdot a = a \cdot 1 = a$

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:

$$a^{n+1} := a^n a\,,$$

$$a^{-n-1} = a^{-n} a^{-1}\,,$$

$$a^0 = 1\,.$$

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. Concider 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):

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

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 $r \times 0 = 0 \times r = 1$.

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 1.3. 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:*

$$\mathrm{GL}_n \coloneqq \{n \times n \textit{ invertable matrices}\}.$$

And enable to distinguish what kind of elements we are having in the matrices, notations like $\mathrm{GL}_n(\mathbb{R})$ or $\mathrm{GL}_n(\mathbb{C})$ 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 $k \geqslant 2$, 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 $\left(a^{k-1}\right)^2 = a^{k-1}$, 而 $a^{k-1} \in G$, 所以 G 中存在幂等元 a^{k-1}. ■

Proposition 1.4. 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

$$\left(a^{2^p}\right)_{p=0}^{\infty}: \quad a, a^2, a^4, a^8, a^{16}, \ldots$$

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 $\left(a^{2^t}\right)^{2^{s-t}} = a^{2^t}$. 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.

定义 $\mathbb{Z}a$ 为 a 的整倍数构成的集合:

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

等价的定义为:

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

例

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

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

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

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

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 $n_1 = k_1 a$, $n_2 = k_2 a$. 故 $n_1 + n_2 = (k_1 + k_2)a$, 而 $k_1 + k_2 \in Z$, 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.

Proposition 1.5. 群 G 的单位元是唯一的.

proof. 设 $i, i' \in G$ 为单位元, 且 $i \neq i'$, 即 $\forall a \in G$, $a = ai$ 以及 $i'a = a$. 所以 $i' = i'i = i$. ■

这也意味着, 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 1.6. $(\mathbb{Z},+)$ 的子群一定有 $\mathbb{Z}a$ 的形式.

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:*

$$\{1, x, x^{-1}, x^2, x^{-2}, \ldots\}$$

称为循环子群.

Proposition 1.7. $S = \{n \mid x^n = 1\}$ 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 $-n \in S$. ■