目录

1 逻辑前提 **2**
1.1 命题逻辑 . . . 2
1.2 映射 . . . 4
1.3 集合 . . . 6
1.4 其他 . . . 8

2 群论 **9**
2.1 幺半群 . . . 9
2.2 群的基本概念 . . . 12
2.3 常用类型的群 . . . 14
2.4 群的基本结构 . . . 15
2.5 正规子群与商群 . . . 23
2.6 同态与同构 . . . 27
2.7 置换群 . . . 30
2.8 群的直积 . . . 33
2.9 群对集合的作用 . . . 35
2.10 Sylow定理 . . . 37
2.11 有限生成Abel群 . . . 38
2.12 正规群列与可解群 . . . 39
2.13 低阶有限群的结构 . . . 41

3 环论 **41**
3.1 环的基本概念 . . . 41

1 逻辑前提

1.1 命题逻辑

定义 1.1.1 真值 ()
真值（Truth Value）是指命题在逻辑上的真假状态。通常用符号 T 表示真，用符号 F 表示假。

定义 1.1.2 命题 ()
命题（Proposition/statement）是指在逻辑上有真值的陈述句。

定义 1.1.3 蕴含 ()
蕴含（Implication）是指若 P 为真，则 Q 也为真的关系，记作 $P \Rightarrow Q$。

性质 1.1.3.1 等价 ()
蕴含的真值表如下：

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

定义 1.1.4 ()
等价（Equivalence）是指 P 与 Q 有相同的真值，记作 $P \Leftrightarrow Q$。
也指 $P \Rightarrow Q$ 且 $Q \Rightarrow P$。

性质 1.1.4.1 ()
等价的真值表如下：

P	Q	$P \Leftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

定义 1.1.5 否定 ()
否定（Negation）是指 P 为真时，$\neg P$ 为假；P 为假时，$\neg P$ 为真。

性质 1.1.5.1 合取 ()
否定的真值表如下：

P	$\neg P$
T	F
F	T

定义 1.1.6 ()
合取（Conjunction）是指 P 与 Q 同时为真时，$P \wedge Q$ 为真。

性质 1.1.6.1 ()
合取的真值表如下：

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

定义 1.1.7 析取 ()
析取（Disjunction）是指 P 与 Q 至少有一个为真时，$P \vee Q$ 为真。

性质 1.1.7.1 异或 ()
析取的真值表如下：

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

定义 1.1.8 ()
异或（Exclusive Or）是指 P 与 Q 有且仅有一个为真时，$P \oplus Q$ 为真。

性质 1.1.8.1 ()
异或的真值表如下：

P	Q	$P \oplus Q$
T	T	F
T	F	T
F	T	T
F	F	F

1.2 映射

定义 1.2.1 映射 ()
映射（Mapping）是指集合 A 中的每个元素 a 都对应到集合 B 中的唯一元素 b 的关系，记作 $f : A \to B$。A称为定义域，B称为陪域。
我们用

$$x \mapsto f(x)$$

来表示 f 对 A 中元素 x 的作用。
我们用 $f(A)$ 表示所有 $x \in A$ 的 $f(x)$ 的集合，即值域。

定义 1.2.2 单射 ()
设 $f : A \to B$ 是一个映射。如果 $x \neq y$ 蕴含 $f(x) \neq f(y)$，我们称 f 是**单射**的（Injective）。

定义 1.2.3 满射 ()
设 $f : A \to B$ 是一个映射。如果对于任意 $b \in B$，存在 $a \in A$ 使得 $f(a) = b$，我们称 f 是**满射**的（Surjective）。

定义 1.2.4 双射 ()
设 $f : A \to B$ 是一个映射。如果 f 既是单射又是满射，我们称 f 是**双射**的（Bijective）。

定义 1.2.5 恒同映射 ()
恒同映射（Identity Mapping）是指将集合 A 中的每个元素 a 映射到其自身的映射，记作 $\mathrm{id}_A : A \to A$，对于所有 $a \in A$，有 $\mathrm{id}_A(a) = a$。

定义 1.2.6 映射的复合 ()
如果集合 B 的子集 A 满足 $A \neq B$，我们称 A 是 B 的真子集。
设 $f : A \to B$ 是一个映射，A' 是 A 的一个子集。f 在 A' 上的限制是一个从 A' 到 B 的映射，记作 $f|_{A'}$。

定义 1.2.7 ()
映射的复合: 设 $f : A \to B$ 和 $g : B \to C$ 是两个映射，那么我们有一个复合映射 $g \circ f$，使得对于所有 $x \in A$，$(g \circ f)(x) = g(f(x))$。

定义 1.2.8 集合 ()

设 $f : A \to B$ 是一个映射，B' 是 B 的一个子集。$f^{-1}(B')$ 表示 A 的一个子集，包含所有 $x \in A$ 使得 $f(x) \in B'$。我们称其为 B' 的逆像。我们称 $f(A)$ 为 f 的像。

定义 1.2.9 ()
如果图中任意两个对象之间的两条路径的复合映射相等，则称该图为交换图。具体来说，如果存在

两条路径：

$$A_1 \xrightarrow{f_1} A_2 \xrightarrow{f_2} \cdots \xrightarrow{f_{n-1}} A_n$$

和

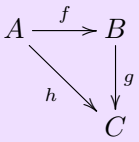
$$A_1 \xrightarrow{g_1} B_2 \xrightarrow{g_2} \cdots \xrightarrow{g_{m-1}} B_m = A_n,$$

则满足

$$f_{n-1} \circ \cdots \circ f_1 = g_{m-1} \circ \cdots \circ g_1,$$

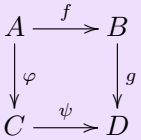
换句话说，复合映射相等。

例 1.2.10 ()
一个图表



被称为交换图，如果满足 $g \circ f = h$。

例 1.2.11 ()
一个图表



被称为交换图，如果满足 $g \circ f = \psi \circ \varphi$。

定理 1.2.12 ()
一个由三角形或正方形组成的图是交换的 $\Leftrightarrow$ 其中的每个三角形和正方形是交换的。

证明:
证明略。

定义 1.2.13 ()
设 A 和 I 为集合。一个由 I 索引的 A 的元素族是指映射 $f : I \to A$。对每个 $i \in I$，存在元素 $f(i) \in A$。尽管族与映射本质相同，我们将其视为 A 中一组对象，记作

$$\{f(i)\}_{i \in I}$$

或

$$\{a_i\}_{i\in I},$$

其中 $a_i = f(i)$。称 I 为索引集。

1.3 集合

定义 1.3.1 ()
集合（Set）是指一组对象的无序集合。

定义 1.3.2 关系 ()
设 A 和 B 是两个集合，A 和 B 的笛卡尔积 $A \times B$ 定义为所有有序对 (a, b) 的集合，其中 $a \in A$ 且 $b \in B$。即：

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

笛卡尔积可以推广到多个集合的情况。例如，对于集合 $A_1, A_2, \ldots, A_n$，其笛卡尔积定义为：

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i, i = 1, 2, \ldots, n\}.$$

定义 1.3.3 ()
设 S 和 T 为两个集合，$S \times T$ 是它们的笛卡尔积。一个**关系** R 是 $S \times T$ 的一个子集，即：

$$R \subseteq S \times T.$$

如果 $(s, t) \in R$，则称 s 与 t 具有关系 R，记作 sRt。

性质 1.3.3.1 自反关系 ()

- **自反关系**：对于所有 $s \in S$，有 sRs。
- **对称关系**：对于所有 $s, t \in S$，如果 sRt，则 tRs。
- **传递关系**：对于所有 $s, t, u \in S$，如果 sRt 且 tRu，则 sRu。
- **反对称关系**：对于所有 $s, t \in S$，如果 sRt 且 tRs，则 $s = t$。

定义 1.3.4 等价关系 ()
等价关系（Equivalence relation）是集合 A 上的一个二元关系，通常记作 $\sim$，满足以下三个性质：
1. **自反性 (Reflexivity)**：对于任意 $a \in A$，有 $a \sim a$。
2. **对称性 (Symmetry)**：对于任意 $a, b \in A$，如果 $a \sim b$，则 $b \sim a$。
3. **传递性 (Transitivity)**：对于任意 $a, b, c \in A$，如果 $a \sim b$ 且 $b \sim c$，则 $a \sim c$。

定义 1.3.5 等价类 ()
等价类（Equivalence class）是指集合 A 上的一个等价关系 $\sim$ 的一个划分，其中每个等价类是 A 的一个子集，满足以下性质：

1. **非空性**：对于任意 $a \in A$，存在一个等价类包含 a。
2. **互斥性**：对于任意 $a, b \in A$，如果 a 和 b 在同一个等价类中，则 $a \sim b$；如果 a 和 b 不在同一个等价类中，则 $a \not\sim b$。

例 1.3.6 商集 ()
假设集合 $A = \{1, 2, 3, 4, 5\}$，并定义等价关系 $\sim$ 为“模 2 同余”，即：

$$x \sim y \iff x \text{ 和 } y \text{ 的奇偶性相同}$$

那么：
- 等价类 $E_1 = \{1, 3, 5\}$（所有奇数）。
- 等价类 $E_2 = \{2, 4\}$（所有偶数）。
这里，E_1 和 E_2 是集合 A 在等价关系 $\sim$ 下的两等价类。

定义 1.3.7 ()
如果 E 是集合 A 的一个等价类，且 $a \in E$，则 E 可表示为：

$$E = [a] = \{x \in A \mid x \sim a\}.$$

这里，$[a]$ 称为 a 的等价类。

要定义类 E 上的映射 f，我们通常采取以下步骤：

1. 选择一个代表元 $x \in E$，并定义 $f(x)$。
2. 证明 $f(x)$ 的值与代表元 x 的选择无关，即对于任意 $y \in E$，若 y 也是 E 的代表元，则 $f(y) = f(x)$。

定义 1.3.8 ()
商集定义为：

$$X/\sim := \{[x] \mid x \in X\},$$

其中等价类 $[x]$ 为：

$$[x] = \{y \in X \mid y \sim x\}.$$

集合 $X/\sim$ 称为 X 关于等价关系 $\sim$ 的商集，即所有等价类构成的集合。

定义 1.3.9 ()
设 $\{A_i\}_{i \in I}$ 是一个集合族，其中 I 是一个索引集。集合族 $\{A_i\}_{i \in I}$ 的乘积定义为所有函数 $f : I \to \bigcup_{i \in I} A_i$ 的集合，满足对于每个 $i \in I$，有 $f(i) \in A_i$。即：

$$\prod_{i \in I} A_i = \left\{ f : I \to \bigcup_{i \in I} A_i \mid \forall i \in I, f(i) \in A_i \right\}.$$

我们使用 $\#(S)$ 表示集合 S 的元素个数，也称为 S 的基数（cardinality）。该符号通常用于 S 是有限集的情况。我们也可以写作 $\#(S) = \mathrm{card}(S)$。

1.4 其他

定义 1.4.1 ()
部分映射是从集合 S 的某个子集 $S' \subseteq S$ 到集合 T 的映射，满足以下条件：

1. **单值性：**
   - 对任意 $x \in S'$，存在唯一的 $y \in T$ 使得 $f(x) = y$。
2. **部分性：**
   - 对 $x \in S \setminus S'$，映射 $f(x)$ 未定义。

形式化表示：

$$f : S \to T \quad \text{是定义在子集} \quad S' \subseteq S \quad \text{上的映射。}$$

定义 1.4.2 ()

部分双射是从集合 S 的某个子集 $S' \subseteq S$ 到集合 T 的某个子集 $T' \subseteq T$ 的映射，满足以下条件：

1. **单射性 (Injective)：**
   - 对任意 $x_1, x_2 \in S'$，若 $f(x_1) = f(x_2)$，则 $x_1 = x_2$。
2. **满射性 (Surjective)：**
   - 对任意 $y \in T'$，存在唯一的 $x \in S'$ 使得 $f(x) = y$。

形式化表示：

$$f : S \to T \quad \text{是定义在} \quad S' \subseteq S \quad \text{上的映射，且} \quad f : S' \to T' \quad \text{是双射。}$$

定义 1.4.3 ()
$a, b \in \mathbb{Z}$ 且 $a \neq 0$。如果存在一个整数 k，使得 $b = a \cdot k$，则称 a 整除 b，记作 $a \mid b$。

定义 1.4.4 ()
$a, b \in \mathbb{Z}$ 且 $a \neq 0$ 且 $b \neq 0$。如果存在一个正整数 d，满足以下条件：

1. $d \mid a$ 且 $d \mid b$（即 d 同时整除 a 和 b）；
2. 对于任意正整数 c，如果 $c \mid a$ 且 $c \mid b$，则 $c \leq d$。

那么，d 被称为 a 和 b 的最大公约数，记作 $\gcd(a, b) = d$。
数学符号表示：

$$\gcd(a, b) = \max \left\{ d \in \mathbb{N}^+ \,\middle|\, d \mid a \text{ 且 } d \mid b \right\}$$

定义 1.4.5 ()
$a, b \in \mathbb{Z}$ 且 $a \neq 0$ 且 $b \neq 0$。如果存在一个正整数 m，满足以下条件：

1. $a \mid m$ 且 $b \mid m$（即 m 同时是 a 和 b 的倍数）；

2. 对于任意正整数 n，如果 $a \mid n$ 且 $b \mid n$，则 $m \leq n$。

那么，m 被称为 a 和 b 的最小公倍数，记作 $\operatorname{lcm}(a,b) = m$。
数学符号表示：

$$\operatorname{lcm}(a,b) = \min\left\{m \in \mathbb{N}^+ \,\middle|\, a \mid m \text{ 且 } b \mid m\right\}$$

性质 1.4.5.1 ()
$a, b \in \mathbb{Z}$ 且 $a \neq 0$ 且 $b \neq 0$。有:

$$|a \times b| = \gcd(a,b) \times \operatorname{lcm}(a,b)$$

定义 1.4.6 ()
欧拉函数 对于任意正整数 n ，欧拉函数 $\varphi(n)$ 定义为：

$$\varphi(n) = |\{k \in \mathbb{Z} \mid 1 \leq k \leq n \text{ 且 } \gcd(k,n) = 1\}|$$

定义 1.4.7 ()
简化剩余系 设 n 是一个正整数，模 n 的简化剩余系是整数集合

$$\{a_1, a_2, \ldots, a_{\varphi(n)}\}$$

其中 $\forall i, j \in [1, \varphi(n)]$

- $1 \leq a_i \leq n$
- $\gcd(a_i, n) = 1$
- 对于所有 $i \neq j$，有 $a_i \not\equiv a_j \pmod{n}$

2 群论

2.1 幺半群

定义 2.1.1 ()
设 S 是一个集合。一个映射

$$S \times S \to S$$

称为 S 上的**合成法则**。对于 S 中的元素 x, y，它们的像称为它们的**乘积**，记作 xy（有时也写作 $x \cdot y$）。合成法则是一个二元运算，即它将两个元素映射到一个元素上。

性质 2.1.1.1 ()
一个有合成法则的集合对其合成法则（乘法）封闭，即对于任意 $a, b \in S$，有 $ab \in S$。

定义 2.1.2 ()
结构 $(M,\cdot)$ 被称为是一个**幺半群**（Monoid），若“.”（可省略不写）：$M^2 \to M$ 是在 M 上的一个合成法则且满足：

1. **结合律：**
$$\forall a,b,c \in M \implies (ab)c = a(bc)$$
2. **单位元：**
$$\exists e \in M(\forall a \in M \implies ea = ae = a)$$
上述中 e 称为**单位元**（Identity）。

在不致混淆的情况下，用 M 作为结构 $(M,\cdot)$ 的简写。
假设G是一个幺半群。如果 G 的合成法则是交换的，我们也称 G 是**交换的（或阿贝尔的）**。

例 2.1.3 ()

- 整数集 $\mathbb{Z}$ 是一个幺半群，其中乘法是合成法则，单位元是1。
- 非负整数集 $\mathbb{N}$ 是一个幺半群，其中加法是合成法则，单位元是0。
- 任意集合 S 上的所有函数构成一个幺半群，其中合成法则是函数复合，单位元是恒同映射。

性质 2.1.3.1 子幺半群 ()
单位元唯一：
$$\forall e_1,e_2 \in M, \forall a \in M \implies ae_1 = e_1a = ae_2 = e_2a = a \implies e_1 = e_2$$

证明:
$$e_1 = e_1e_2 = e_2 \square$$

定义 2.1.4 ()
按照惯例，我们约定空乘积等于单位元。
$$\prod_{v=1}^{0} x_v = e$$

性质 2.1.4.1 ()
设 G 是一个交换幺半群，$x_1,\ldots,x_n$ 是 G 的元素。设 ψ 是作用在整数集 $(1,\ldots,n)$ 上的一个置换。则
$$\prod_{v=1}^{n} x_{\psi(v)} = \prod_{v=1}^{n} x_v.$$

证明:
(这是不依赖其他定理的证明方式)
归纳法:
对于 $n=1$ 的情况是显然的。
假设对于 $n-1$ 成立。设 k 是一个整数，使得 $\psi(k)=n$。则

$$\prod_1^n x_{\psi(v)} = \prod_1^{k-1} x_{\psi(v)} \cdot x_{\psi(k)} \cdot \prod_1^{n-k} x_{\psi(k+v)}$$

$$= \prod_1^{k-1} x_{\psi(v)} \cdot \prod_1^{n-k} x_{\psi(k+v)} \cdot x_{\psi(k)}.$$

定义一个映射 φ：$(1,\ldots,n-1)$ 到自身，规则为

$$\varphi(v) = \psi(v) \quad \text{如果 } v < k,$$

$$\varphi(v) = \psi(v+1) \quad \text{如果 } v \geq k.$$

则

$$\prod_1^n x_{\psi(v)} = \prod_1^{k-1} x_{\varphi(v)} \prod_1^{n-k} x_{\varphi(k-1+v)} \cdot x_n$$

$$= \prod_1^{n-1} x_{\varphi(v)} \cdot x_n,$$

根据归纳假设，这等于 $x_1 \cdots x_n$□。

定义 2.1.5 ()

- 对于两个子集 $S, S' \subseteq G$，定义它们的乘积 SS' 为：

  $$SS' = \{xy \mid x \in S, y \in S'\}.$$

  注意到 $GG = G$
- 可以归纳地定义有限多个子集的乘积:

  $$S_1 S_2 \cdots S_n = \{x_1 x_2 \cdots x_n \mid x_i \in S_i\}.$$

- 对于子集$S \subseteq G$,元素$x \in G$，我们定义xS为

  $$xS = \{x\}S = \{xy \mid y \in S\}$$

定义 2.1.6 ()
设 G 是一个幺半群，$H \subseteq G$。H 是 G 的**子幺半群**,如果 H 满足以下条件：

- H 包含 G 的单位元 e。
- 对于任意 $x, y \in H$，有 $xy \in H$（即 H 对合成法则封闭）。

2.2 群的基本概念

定义 2.2.1 ()
结构$(G,\cdot)$被称为是一个**群(Group)**, 若“$\cdot$”(可省略不写):$G^2\to G$是在G上定义的一个二元乘法运算且满足:
(1)结合律:

$$\forall a,b,c\in G\Longrightarrow (ab)c=a(bc)$$

(2)恒等元:

$$\exists e\in G(\forall a\in G\Longrightarrow ea=ae=a)$$

上式中e称为**恒等元(Identity)**.
(3)元可逆:

$$\forall a\in G,\exists a'\in G(aa'=a'a=e)$$

上式中a称为a的**逆元(Inverse)**, 记作a^{-1}.
在不致混淆的情况下, 用G作为结构$(G,\cdot)$的简写.

性质 2.2.1.1 ()
恒等元唯一:

$$\forall e_1,e_2\in G,\forall a\in G,ae_1=e_1a=ae_2=e_2a=a\Longrightarrow e_1=e_2$$

证明:

$$e_1=e_1e_2=e_2\square$$

性质 2.2.1.2 阶(Order) ()
逆元唯一:

$$\forall a\in G,a'a=aa'=a''a=aa''=e\Longrightarrow a'=a''=a^{-1}$$

这同时也说明了任一元素的左逆等于右逆, 是唯一的.

证明:

$$a'=a'e=a'aa''=ea''=a''\square$$

性质 2.2.1.3 ()
逆元的逆元为自身:

$$\forall a\in G\Longrightarrow (a^{-1})^{-1}=a$$

证明:
由逆元定义及逆元唯一性可立即得到. □

性质 2.2.1.4 ()
元素积的求逆运算遵循反序法则:

$$\forall a,b\in G\Longrightarrow (ab)^{-1}=b^{-1}a^{-1}$$

证明:

$$ab(b^{-1}a^{-1})=(b^{-1}a^{-1})ab=e\square$$

性质 2.2.1.5 ()
方程有唯一解:

$$\forall a,b\in G\Longrightarrow \exists 唯一的x,y\in G(ax=b,ya=b)$$

证明:

$$x=a^{-1}b,y=ba^{-1}\square$$

性质 2.2.1.6 ()
左/右消去律成立:

$$\forall a,b,c\in G\Longrightarrow (ac=bc\Longrightarrow a=b\wedge ca=cb\Longrightarrow a=b)$$

证明:

$$ac=bc\Longrightarrow acc^{-1}=bcc^{-1}\Longrightarrow ae=be\Longrightarrow a=b$$

$$ca=cb\Longrightarrow c^{-1}ca=c^{-1}cb\Longrightarrow ea=eb\Longrightarrow a=b$$

性质 2.2.1.7 ()
简记连乘为乘方运算:

$$a^n:=\underbrace{aa\cdots a}_{n个a}(n\in\mathbb{Z}^+)$$

$$a^{-n}:=\underbrace{a^{-1}a^{-1}\cdots a^{-1}}_{n个a^{-1}}(n\in\mathbb{Z}^+)$$

$$a^0:=e$$

乘方之积遵循指数相加法则:

$$a^ma^n=a^{m+n}$$

性质 2.2.1.8 ()
乘方运算复合遵循指数相乘法则:

$$(a^m)^n=a^{mn}$$

定义 2.2.2 ()
阶(Order)
群$(G,\cdot)$中, 集合G的基数(集合中元素的个数)$|G|$称为群$(G,\cdot)$的**阶(Order)**, 记为$|(G,\cdot)|$或简记为$|G|$.

2.3 常用类型的群

例 2.3.1 ()
一个群G被称为是一个**Abel群(Abelian Group)**或**交换群(Commutative Group)**, 若乘法交换律成立:

$$\forall a,b\in G\Longrightarrow ab=ba$$

例 2.3.2 ()
若一个由S上的部分双射$(f:S\to S)$组成的集合在映射的复合运算下成为一个群，该集合称为集合S上的一个**变换群(Transformation Group)**, 记作$A(S)$.

例 2.3.3 ()
设 S 是一个非空集合，$\mathrm{Perm}(S)$ 表示 S 上所有**置换**的集合。$\mathrm{Perm}(S)$ 在映射的复合运算下构成一个群，称为 S 上的**对称群**，记作 $\mathrm{Sym}(S)$。
如果 S 是一个有限集合，且 $|S|=n$，则 $\mathrm{Sym}(S)$ 称为**对称群** S_n。此时，S_n 的阶数为 $n!$。

例 2.3.4 ()
设 S 是一个非空集合，$\mathrm{Sym}(S)$ 是 S 上的**对称群**,如果 G 是 $\mathrm{Sym}(S)$ 的一个子群，则称 G 为 S 上的一个**置换群**。

例 2.3.5 ()
一个群 G 如果存在一个元素 $a\in G$，使得 G 的每一个元素都可以表示为 a 的幂次（即 $G=\{a^n\mid n\in\mathbb{Z}\}$），则称 G 为**循环群**。元素 a 称为循环群的一个**生成元**。

例 2.3.6 ()
设$\mathbb{K}$是一个数域, 则全体n阶可逆矩阵在矩阵乘法运算下成为一个群, 称为数域$\mathbb{K}$上的n阶**一般线性群(General Linear Group)**, 记作$GL_n(\mathbb{K})$

例 2.3.7 ()
设$\mathbb{K}$是一个数域, 则全体行列式值为1的n阶可逆矩阵在矩阵乘法运算下成为一个群, 称为数域$\mathbb{K}$上的n阶**特殊线性群(Special Linear Group)**, 记作$SL_n(\mathbb{K})$

例 2.3.8 ()
设$n\in\mathbb{Z}^+-\{1\}$, 则模n的完全剩余系在同余加法运算下成为一个群, 称为模n**剩余类加法群(Remainder Plus Group)**, 记作$\mathbb{Z}/n\mathbb{Z}$. $|\mathbb{Z}/n\mathbb{Z}|=n$.

例 2.3.9 ()
设$n \in \mathbb{Z}^+ - \{1\}$, 则模$n$的既约剩余系在同余乘法运算下成为一个群, 称为模$n$**剩余类乘法群**, 记作$\mathbb{Z}/n\mathbb{Z}^*$. $|\mathbb{Z}/n\mathbb{Z}^*| = \varphi(n)$(其中$\varphi$为Euler函数).

例 2.3.10 ()
设$\mathbb{H} = \{\pm 1, \pm i, \pm j, \pm k\}$, 其中:

$$i^2 = j^2 = k^2 = -1$$

$$ij = -ji = k$$

$$jk = -kj = i$$

$$ki = -ik = j$$

$\mathbb{H}$称为**Hamilton四元数群(Hamilton's Quaternions)**.

2.4 群的基本结构

定义 2.4.1 ()
子群(Subgroup)
设$(G, \cdot_G)$是一个群, 则群$(H, \cdot_H)$称为是群G的一个**子群(Subgroup)**, 若$H \subseteq G \wedge \cdot_H = \cdot_G|_{H^2}$, 记作$(H, \cdot) \leq (G, \cdot)$.
显然有$(G, \cdot), (\{e\}, \cdot) \leq (G, \cdot)$, 称群$(G, \cdot)$与$(\{e\}, \cdot)$为$(G, \cdot)$的**平凡子群(Trivial Subgroup)**
$(H, \cdot) \leq (G, \cdot), (H, \cdot) \neq (G, \cdot)$记作$H < G$.

性质 2.4.1.1 ()
子群关系具有传递性:

$$(K, \cdot) \leq (H, \cdot), (H, \cdot) \leq (G, \cdot) \Longrightarrow (K, \cdot) \leq (G, \cdot)$$

记作$(K, \cdot) \leq (H, \cdot) \leq (G, \cdot)$.

证明:

$$(K, \cdot) \leq (H, \cdot), (H, \cdot) \leq (G, \cdot) \Longrightarrow K \subseteq H \subseteq G \Longrightarrow K \subseteq G$$

又K, H在G的运算下都构成群,

$$\Longrightarrow (K, \cdot) \leq (G, \cdot) \Longrightarrow (K, \cdot) \leq (H, \cdot) \leq (G, \cdot). \square$$

性质 2.4.1.2 生成子群(Generated Subgroup) ()
子群的等价判定条件:

$$H \leq G \iff (\forall a, b \in H \Longrightarrow ab \in H \wedge a^{-1} \in H) \iff (\forall a, b \in H \Longrightarrow ab^{-1} \in H)$$

证明:
(1)充分性:

$$H \leq G \Longrightarrow (\forall a, b \in H \Longrightarrow (ab \in H \wedge b^{-1} \in H)) \Longrightarrow (\forall a, b \in H \Longrightarrow ab^{-1} \in H)$$

(2)必要性-1:

$$\forall a, b \in H \Longrightarrow ab \in H, a^{-1} \in H \Longrightarrow e = aa^{-1} \in H$$

$$\forall a, b, c \in H, a, b, c \in G \Longrightarrow a(bc) = (ab)c$$

$\Longrightarrow H$在群G的运算下是一个群, 即$H \leq G$.
(3)必要性-2:

$$\forall a, b \in H, ab^{-1} \in H \Longrightarrow aa^{-1} = e \in H \Longrightarrow ea^{-1} = a^{-1} \in H$$

与(2)同理可证$H \leq G$.□

上述性质也可以等价写成下面这个更泛用的形式

性质 2.4.1.3 ()
记$H^{-1} = \{h^{-1} | h \in H\}$, 则$H \leq G \iff HH^{-1} = H$

证明:
证明略，仅为等价表示.

性质 2.4.1.4 ()
有限子群的判定条件可以减弱:
设$H \subseteq G, |H|$有限, 则:

$$\forall a, b \in H, ab \in H \Longrightarrow H \leq G$$

证明:
只需证$\forall a \in H, a^{-1} \in H$.
$|H| := n$, 根据抽屉原理有:

$$\exists i, j \in \{1, 2, \cdots, n+1\}(i > j, a^i = a^j) \Longrightarrow a^{i-j} = e \Longrightarrow a^{-1} = a^{i-j-1} \in H\square$$

性质 2.4.1.5 ()
设 G 是一个群，$\{H_i\}_{i \in I}$ 是 G 的一族子群（其中 I 是一个指标集）。定义它们的交集为：

$$H = \bigcap_{i \in I} H_i$$

那么H 是 G 的子群。

证明:
证明略。

定义 2.4.2 ()
生成子群(Generated Subgroup)
设$(G,\cdot)$是一个群, (集合)$S\subseteq G$, 则称

$$\bigcap_{\substack{(S_i,\cdot)\leq(G,\cdot)\\ S\subseteq S_i}} S_i$$

为由S生成的子群(Subgroup generated by S), 记作$\langle S\rangle$.
由单元集$\{a\}$生成的子群可简记为$\langle a\rangle$.

性质 2.4.2.1 ()
设$S\subseteq G$, 则:

$$\langle S\rangle=\{\prod_{i=1}^{n}a_i^{\varepsilon_i}|n\in\mathbb{N},a_i\in S,\varepsilon_i=\pm1\}$$

其中a_i可重复取S中元素.

证明:

$$S':=\{\prod_{i=1}^{n}a_i^{\varepsilon_i}|n\in\mathbb{N},a_i\in S,\varepsilon_i=\pm1\}'$$

(1)$S'\subseteq\langle S\rangle$:
$\langle S\rangle$是一个群,

$$\Longrightarrow\forall a,b\in\langle S\rangle,ab,a^{-1}\in\langle S\rangle$$

$$\forall a=\prod_{i=1}^{n}a_i^{\varepsilon_i}(n\in\mathbb{N},a_i\in S,\varepsilon_i=\pm1)\Longrightarrow a\in\langle S\rangle$$

$$\Longrightarrow S'\subseteq\langle S\rangle$$

(2)$(S',\cdot)\leq(G,\cdot)$:

$$\forall a=\prod_{i=1}^{m}a_i^{\varepsilon_i},b=\prod_{j=1}^{n}b_j^{\varepsilon_j'}(m,n\in\mathbb{N},a_i,b_j\in S,\varepsilon_i,\varepsilon_j'=\pm1)$$

$$a_{m+j}:=b_j,\varepsilon_{m+j}:=\varepsilon_j'$$

$$ab=\prod_{i=1}^{m+n}a_i^{\varepsilon_i},m+n\in\mathbb{N},a_i\in S,\varepsilon_i=\pm1$$

$$a^{-1}=\prod_{i=1}^{m}a_i^{-\varepsilon_i},m\in\mathbb{N},a_i\in S,-\varepsilon_i=\pm1$$

$$\Longrightarrow ab,a^{-1}\in S'$$

$\Longrightarrow S'$是一个群, 又$S'\subseteq G\Longrightarrow(S',\cdot)\leq(G,\cdot)$.
(3)$\langle S\rangle=(S',\cdot)$

$$\langle S\rangle=\bigcap_{\substack{(S_i,\cdot)\leq(G,\cdot)\\ S\subseteq S_i}}S_i=S'\cap\bigcap_{\substack{(S_i,\cdot)\leq(G,\cdot)\\ S\subseteq S_i}}S_i\subseteq S'$$

$$S'\subseteq\langle S\rangle,\langle S\rangle\subseteq S'\Longrightarrow\langle S\rangle=(S',\cdot)\square$$

定义 2.4.3 循环群(Cyclic Group) ()
一个群G称为是**循环群(Cyclic Group)**, 若$G = \langle a\rangle (a \in G)$.

定义 2.4.4 周期(Period) ()
若对于$a \in G$, $\exists$最小的$n \in \mathbb{Z}^+ : a^n = e$, 则称$n$为元素$a$的**周期(Period)**, 记作$|a|$(有时也称为$a$的**阶**).

性质 2.4.4.1 陪集/旁集(Coset) ()

$$|a| = |\langle a\rangle|$$

证明:
(1)$|a| \le |\langle a\rangle|$:

$$\langle a\rangle = \{\prod_{i=1}^{n} a_i^{\varepsilon_i} | n \in \mathbb{N}, a_i \in \{a\}, \varepsilon_i = \pm 1\} = \{a^i | i \in \mathbb{N}\}$$

$$a^i = a^j (i, j \in \mathbb{N}, i > j) \iff a^{i-j} = e \Longrightarrow i \ge i - j \ge |a|$$

$\Longrightarrow e, a, \cdots, a^{|a|-1} \in \langle a\rangle$互不相等.

$$\Longrightarrow |a| \le |\langle a\rangle|$$

(2)

$$\forall i \ge |a|, \exists j \equiv i \pmod{|a|} (a^i = a^j \wedge j < |a| (i, j \in \mathbb{N}))$$

$$\Longrightarrow \langle a\rangle = \{e, a, \cdots, a^{|a|-1}\}$$

$$\Longrightarrow |a| = |\langle a\rangle| \square$$

性质 2.4.4.2 ()

$$a^m = e \iff |a| \Big| m$$

证明:
必要性显然. 充分性的证明运用反证法. 假设$\exists m \in \mathbb{Z}^+ (a^m = e, \frac{m}{|a|} \notin \mathbb{Z}^+)$
根据带余数除法, $\exists k, r \in \mathbb{Z}^+ (m = k \cdot |a| + r, r < |a|)$

$$\Longrightarrow a^r = a^{m-k\cdot|a|} = a^m (a^{|a|})^{-k} = e, r < |a|$$

与$|a|$是a的周期矛盾. $\square$

性质 2.4.4.3 ()
设$|\langle a\rangle| = n$, 则a^m的阶为$\frac{n}{\gcd(m,n)}$.

证明:
记$d = \gcd(m,n)$. 一方面$n|\frac{mn}{d}$, 故$a^{m\frac{n}{d}} = e$. 另一方面，若存在正整数$t < \frac{n}{d}$满足$a^{mt} = e$, 则$n|mt$, 故$\frac{n}{d}\Big|\frac{m}{d}t$, 由于$\frac{m}{d}, \frac{n}{d}$互素, 可推知 $\frac{n}{d}\Big|t$, 与$0 < t < \frac{n}{d}$矛盾.

定义 2.4.5 ()
陪集/旁集(Coset)
设$H \leq G, a \in G, aH := \{ah|h \in H\}, Ha := \{ha|h \in H\}$, 称$aH$为子群$H$的一个**左陪集(Left Coset)**, Ha为子集H的一个**右陪集(Right Coset)**

定义 2.4.6 ()

陪集代表元(Coset Representative)
设 $H \leq G$，$a \in G$，若 $h \in H$，则称 ah 为 aH 的一**左陪集代表元 (Left Coset Representative)**。类似地，若 $h \in H$，则称 ha 为 Ha 的一个**右陪集代表元 (Right Coset Representative)**。

性质 2.4.6.1 ()
$K < H \leq G$，设 $\{x_i\}$ 是 K 在 H 中的一组（左）陪集代表元，$\{y_j\}$ 是 H 在 G 中的一组陪集代表元。那么我们断言 $\{y_j x_i\}$ 是 K 在 G 中的一组陪集代表元。

证明:

$$H = \bigcup_i x_i K \quad (\text{不交并}),$$
$$G = \bigcup_j y_j H \quad (\text{不交并}).$$

因此

$$G = \bigcup_{i,j} y_j x_i K.$$

我们必须证明这个并集是不交的，即 $y_j x_i$ 代表不同的陪集。假设

$$y_j x_i K = y_{j'} x_{i'} K$$

对于一对指标 (j,i) 和 (j',i')。在右边乘以 H，并注意到 $x_i, x_{i'}$ 在 H 中，我们得到

$$y_j H = y_{j'} H,$$

从而 $y_j = y_{j'}$。由此可以推出 $x_i K = x_{i'} K$，因此 $x_i = x_{i'}$

性质 2.4.6.2 覆盖性： ()

$$aH = bH \iff a^{-1}b \in H$$

$$Ha = Hb \iff ab^{-1} \in H$$

证明:
先对左陪集进行证明:
(1)充分性:

$$aH = bH \Longrightarrow (\forall h \in H \Longrightarrow \exists h' \in H(ah = bh'))$$
$$\Longrightarrow a^{-1}b = hh'^{-1} \in H$$

(2)必要性:

$$a^{-1}b \in H \Longrightarrow (\forall h \in H \Longrightarrow (ah = b(b^{-1}a)h = b(a^{-1}b)^{-1}h \in bH)) \Longrightarrow aH \subseteq bH$$

同理有$bH \subseteq aH \Longrightarrow aH = bH$
对于右陪集同理. □

性质 2.4.6.3 ()
$R := \{(a,b)|a^{-1}b \in H\}, R' := \{(a,b)|ab^{-1} \in H\}$是等价关系.

证明:
(1)自反性:

$$a^{-1}a = e \in H \Longrightarrow (a,a) \in R$$

(2)互逆性:

$$a^{-1}b \in H \Longrightarrow (a^{-1}b)^{-1} = b^{-1}a \in H$$
$$\Longrightarrow (a,b) \in R \Longrightarrow (b,a) \in R$$

(3)传递性:

$$a^{-1}b, b^{-1}c \in H \Longrightarrow a^{-1}bb^{-1}c = a^{-1}c \in H$$
$$\Longrightarrow (a,b),(b,c) \in R \Longrightarrow (a,c) \in R$$

对于R'同理. □

性质 2.4.6.4 ()

$$aH \neq bH \iff aH \cap bH = \varnothing$$
$$Ha \neq Hb \iff Ha \cap Hb = \varnothing$$

证明:
(1)必要性是显然的.
(2)充分性:
运用反证法. 假设$aH \neq bH, \exists g \in aH \cap bH$

$$\exists h_1, h_2 \in H : ah_1 = bh_2$$

$$\Longrightarrow a^{-1}b = h_1h_2^{-1} \in H \Longrightarrow aH = bH$$

与$aH \neq bH$矛盾. 对右陪集同理. □

性质 2.4.6.5 ()

$$H \leq G \Longrightarrow \forall a \in G, |aH| = |H|, |Ha| = |H|$$

证明:
考虑到群满足左/右消去律,

$$\forall h, h' \in H \Longrightarrow (ah = ah' \Longrightarrow h = h')$$

构造$\varphi : H \to aH : \varphi(h) = ah$.
则$\exists \varphi^{-1} : aH \to H : \varphi^{-1}(ah) = a^{-1}(ah) = h$
即φ是双射, 于是H和aH中的元素建立了一一对应关系.
$\Longrightarrow |aH| = |H|$
对于右陪集同理. □

性质 2.4.6.6 ()
$H \leq G \Longrightarrow G$ 是其子群 H 的陪集的不相交并集。

证明:
我们需要证明覆盖性和不相交性。
覆盖性：

$$\forall g \in G, g \in gH, \text{因为} g = g \cdot e.$$

不相交性： 性质 2.4.5.3 ✓
由于 G 中的每个元素都属于某个陪集，且任意两个不同的陪集没有公共元素，所以G 是其子群 H 的陪集的不相交并集。 □

定理 2.4.7 ()
Lagrange定理:

$$H \leq G \Longrightarrow |H| \Big| |G|$$

称$\dfrac{|G|}{|H|}$为子群H在群G中的**指数(Index)**, 记为$[G : H]$.

证明:

$$R := \{(a, b) | aH = bH\}$$

$$G/R = \{aH | a \in G\}$$

构造$\varphi: G \to G/R(a \mapsto aH)$
有φ将每个旁集中的全部$|H|$个元素映射到旁集本身上.
即R将G中全部元素划分成了$\dfrac{|G|}{|H|}$个部分, 每个部分的元素数量为$|H|$.
于是有$\dfrac{|G|}{|H|} \in \mathbb{Z}^+$. $\square$

性质 2.4.7.1 ()

$$\forall a \in G, |a| \Big| |G|$$

证明:

$$\langle a \rangle \leq G \Longrightarrow |\langle a \rangle| = |a| \Big| |G| \square$$

性质 2.4.7.2 Euler定理 ()
$\forall a \in G, a^{|G|} = e$.

证明:

$$a^{|G|} = (a^{|a|})^{[G:\langle a \rangle]} = e \square$$

性质 2.4.7.3 ()
$|G| = p, p$是素数$\Longrightarrow |G|$是循环群.

证明:

$$\exists a \in G : a \neq e \Longrightarrow |a| \neq 1$$
$$|\langle a \rangle| \Big| |G| \Longrightarrow |\langle a \rangle| = p = |G|$$
$$\langle a \rangle \subseteq G \Longrightarrow G = \langle a \rangle \square$$

定理 2.4.8 ()
Euler定理

$$\forall a, n \in \mathbb{Z}^+ : \gcd(a, n) = 1, a^{\varphi(n)} \equiv 1 \pmod{n}$$

其中φ为Euler函数.

证明:
考虑n的简化剩余系

$$A = \{\bar{i} \mid 1 \leq i \leq n-1, \text{ 且}i\text{与}n\text{互素}\}$$

则$|A| = \varphi(n)$. 由于$\gcd(a,n) = n$,所以$a \in A$, 有$aA = A$(这里群的运算为模n乘法), 考虑A中所有元素的积, 则

$$\Pi_{x\in A}x \equiv \Pi_{x\in A}ax \equiv a^{\varphi(n)}\Pi_{x\in A}x \pmod{n}$$

而$\Pi_{x\in A}x$与n仍然互素, 故可以消去他，便得到

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

取n为素数p马上可得Fermat小定理:

定理 2.4.9 Fermat小定理 ()
设p是素数, a不被p整除, 则

$$a^{p-1} \equiv 1 \pmod{p}$$

2.5 正规子群与商群

定义 2.5.1 ()
群G的一个子群$H \leq G$称为是G的一个**正规子群(Normal Subgroup)**, 若$\forall g \in G, gH = Hg$, 记为$H \trianglelefteq G$.
$H \trianglelefteq G, H \neq G$记为$H \triangleleft G$.
$\{e\}, G \trianglelefteq G$称为$G$的**平凡正规子群(Trivial Normal Subgroup)**, 没有非平凡正规子群的群称为**单群**.
当$N \trianglelefteq G$时, N的陪集$gN = Ng$简记为$\bar{g}$.
设M为群G的子群, 则

$$N_G(M) = \{g \in G | g^{-1}Mg = M\}$$

为G的子群, 称为M的**正规化子**.

性质 2.5.1.1 ()
显然, 子群M是正规子群当且仅当$N_G(M) = G$

性质 2.5.1.2 自然映射(Natural Projection) ()
正规子群的等价判定

$$\forall g \in G, gHg^{-1} = H \iff H \trianglelefteq G$$

证明:
(1)

$$H \trianglelefteq G \Longrightarrow \forall g \in G, gH = Hg$$
$$\Longrightarrow \forall g \in G, h \in H, \exists h' \in H : gh = h'g \Longrightarrow ghg^{-1} \in H \Longrightarrow gHg^{-1} \subseteq H$$
$$\forall g \in G, h \in H, g^{-1}hg \in H \Longrightarrow h = g(g^{-1}hg)g^{-1} \in gHg^{-1} \Longrightarrow H \subseteq gHg^{-1}$$
$$\Longrightarrow H \trianglelefteq G \Longrightarrow \forall g \in G, gHg^{-1} = H$$

(2)

$$\forall g \in G, gHg^{-1} = H \Longrightarrow \forall h \in H, \exists h' \in H : h' = ghg^{-1}$$

$$\Longrightarrow gh = h'g \Longrightarrow gH = Hg \Longrightarrow H \trianglelefteq G\square$$

性质 2.5.1.3 ()
$H \leq G, G$是Abel群$\Longrightarrow H \trianglelefteq G$

证明:

$$\forall g \in G, h \in H, gh = hg \Longrightarrow gH = Hg \Longrightarrow H \trianglelefteq G\square$$

性质 2.5.1.4 ()

$$H \leq G, [G : H] = 2 \Longrightarrow H \trianglelefteq G$$

证明:
$[G : H] = 2 \Longrightarrow H$只有两个左/右陪集, 其中一个为$H$本身.

$$\forall g \in G - H, h \in H, Hg \cap H = gH \cap H = \varnothing, |Hg| = |gH| = |H|$$

$$\Longrightarrow eH = He = H, gH = Hg = G - H \Longrightarrow H \trianglelefteq G\square$$

定义 2.5.2 ()
群G的子集$A, B \subseteq G$乘法定义为$AB = \{ab | a \in A, b \in B\}$

证明:
$[G : H] = 2 \Longrightarrow H$只有两个左/右陪集, 其中一个为$H$本身.

$$\forall g \in G - H, h \in H, Hg \cap H = gH \cap H = \varnothing, |Hg| = |gH| = |H|$$

$$\Longrightarrow eH = He = H, gH = Hg = G - H \Longrightarrow H \trianglelefteq G\square$$

性质 2.5.2.1 ()
$\forall K$满足$H \trianglelefteq K \leq G$,则$K \leq N_G(H)$.

证明:

$$\forall k \in K, h \in H, khk^{-1} \in H$$

$$\Longrightarrow kHk^{-1} = H$$

$$\Longrightarrow k \in N_G(H)$$

$$\Longrightarrow K \leq N_G(H)\square$$

性质 2.5.2.2 ()
群的子集乘法满足乘法结合律.

证明:

$$\forall A, B, C \subseteq G,$$
$$(AB)C = \{(ab)c | a \in A, b \in B, c \in C\}$$
$$A(BC) = \{a(bc) | a \in A, b \in B, c \in C\}$$
$$\forall a \in A, b \in B, c \in C, (ab)c = a(bc), \Longrightarrow (AB)C = A(BC)\square$$

性质 2.5.2.3 ()
在群的子集乘法定义下, $H \trianglelefteq G \Longrightarrow \forall \bar{a}, \bar{b} \in \bar{G}, \bar{a}\bar{b} = \overline{ab}$

证明:

$$\bar{a}\bar{b} = (aH)(bH) = a(Hb)H = a(bH)H = (ab)(HH) = (ab)H = \overline{ab}\square$$

性质 2.5.2.4 ()
$\bar{G}$是一个群 $\Longleftrightarrow$ $H \trianglelefteq G$.

证明:
(1)若$H \trianglelefteq G$, 则:
乘法封闭:

$$\forall \bar{a}, \bar{b} \in \bar{G}, \bar{a}\bar{b} = \overline{ab} \in \bar{G}$$

恒等元存在:

$$\forall \bar{a} \in \bar{G}, \bar{e}\bar{a} = \bar{a}\bar{e} = \bar{a}$$

逆元存在:

$$\forall \bar{a} \in \bar{G}, \bar{a}\overline{a^{-1}} = \bar{a^{-1}}\bar{a} = \overline{aa^{-1}} = \bar{e}$$

$\Longrightarrow \bar{G}$是一个群.
(2)若$\bar{G}$是一个群, 则:
单位元为陪集 H。因此，对任意 $aH \in \bar{G}$，有：

$$(H)(aH) = aH = Ha = (Ha)(H).$$

因此，H 是 G 的正规子群。
若 G/H 的乘法是良定义的，则对任意 $a, b \in G$ 和 $h_1, h_2 \in H$，必须满足：

$$(ah_1)(bh_2)H = (ab)H.$$

展开左边，我们得到：

$$ah_1bh_2H = ab(b^{-1}h_1b)h_2H.$$

由于 H 是正规子群，$b^{-1}h_1b \in H$，因此存在 $h_3 \in H$ 使得：

$$abh_3h_2 \in abH.$$

这表明 $h_3h_2 \in H$，从而 H 在共轭下封闭，即 $H \trianglelefteq G$。

定义 2.5.3 ()
设G是一个群, $H \trianglelefteq G$, 映射$f : G \to G/H$称为**自然映射(Natural Projection)**, 若$\forall g \in G, f(g) = \bar{g}$

定义 2.5.4 ()
设$H \trianglelefteq G, H$的全体左/右陪集构成的集族$\bar{G}$称为群G关于子群H的**商群(Quotient Group)**, 若在群的子集乘法下$\bar{G}$是一个群, 记作$\bar{G} = G/H$.

$$G/H = (G/\sim, \bar{\cdot})(a \sim b \iff ab^{-1} \in H)$$

例 2.5.5 ()
$SL_n(K)$ 是 $GL_n(K)$ 的正规子群.

例 2.5.6 ()
$H \leq G$,则 H 是 $N_G(H)$ 的正规子群.

定义 2.5.7 中心化子 ()

- 对单个元素：
  群 G 中元素 a 的**中心化子**定义为：
  $$C_G(a) = \left\{g \in G \mid gag^{-1} = a\right\},$$
- 对子集：
  群 G 的子集 $H \subseteq G$ 的**中心化子**定义为：
  $$C_G(H) = \left\{g \in G \mid ghg^{-1} = h,\ \forall h \in H\right\},$$

群 G 的**中心** $Z(G)$ 是 $C_G(G)$，即：

$$Z(G) = \{g \in G \mid gh = hg,\ \forall h \in G\}.$$

显然 $Z(G)$ 是 G 的一个正规子群。

2.6 同态与同构

定义 2.6.1 ()
设G_1, G_2是群, 映射$f: G_1 \to G_2$称为是**同态(Homomorphism)**, 若$\forall a, b \in G_1 : f(ab) = f(a)f(b)$.
称同态f为G上的**自同态(Endomorphism)**, 若$G_1 = G_2 = G$.
称同态f为**同构(Isomorphism)**, 若f是双射.
称同构f为G上的**自同构(Automorphism)**, 若$G_1 = G_2 = G$.
称群G_1与G_2**同构(Isomorphic)**, 若$\exists$同构$f: G_1 \to G_2$, 记为$G_1 \cong G_2$.
称同态$f: G \to \{e\}$为**平凡同态(Trivial Homomorphism)**.
称同构$f: G \to G$为**恒同自同构(Identity Automorphism)**, 若$\forall g \in G, f(g) = g$, 记作$I_d$.
称自同构$f_g: G \to G$为由元素g决定的**内自同构(Inner Automorphism)**, 若$g \in G, \forall a \in G, f_g(a) = gag^{-1}$.
称自然映射为**自然同态(Natural Homomorphism)**.

性质 2.6.1.1 ()
设同态$f: G \to G'$, 有$f(e) = e'$.

证明:

$$\forall g \in G, f(g) = f(eg) = f(e)f(g) \Longrightarrow f(e) = e' \square$$

性质 2.6.1.2 **核(Kernel)** ()

$$\forall g \in G, f(g^{-1}) = f(g)^{-1}$$

证明:

$$\forall g \in G, f(g)f(g^{-1}) = f(g^{-1})f(g) = f(e) = e' \Longrightarrow f(g^{-1}) = f(g)^{-1} \square$$

性质 2.6.1.3 ()

$$f: G \to G' \Longrightarrow f(G) \leq G'$$

证明:
(1)

$$\forall a, b \in G, f(a)f(b) = f(ab) \in f(G)$$

(2)

$$\forall g \in G, f(g)^{-1} = f(g^{-1}) \in f(G)$$

于是$f(G)$是一个群, 又有:

$$f(G) \subseteq G' \Longrightarrow f(G) \leq G' \square$$

性质 2.6.1.4 ()
同构关系是等价关系.

证明:
(1)自反性:
$\forall$群G, 恒同自同构I_d是G上的自同构, $\Longrightarrow G \cong G$.
(2)对称性:
$G_1 \cong G_2 \Longrightarrow \exists f : G_1 \to G_2$是双射.
$\Longrightarrow f^{-1} : G_2 \to G_1$是双射, 即$G_2 \cong G_1$.
(3)传递性:
$G_1 \cong G_2, G_2 \cong G_3 \Longrightarrow \exists f_1 : G_1 \to G_2, f_2 : G_2 \to G_3$都是双射.
$\Longrightarrow f_2 \circ f_1 : G_1 \to G_3$是双射, 即$G_1 \cong G_3$. $\square$

定义 2.6.2 ()
设G, G'是群, $f : G \to G'$是同态, 称集合$K = \{g | g \in G, f(g) = e'\}$是同态$f$的**核(Kernel)**, 记为$\operatorname{Ker} f$.

性质 2.6.2.1 ()

$$\operatorname{Ker} f \trianglelefteq G$$

证明:
(1)
$$\forall a, b \in \operatorname{Ker} f, f(ab) = f(a)f(b) = e' \Longrightarrow ab \in \operatorname{Ker} f$$
(2)
$$\forall g \in \operatorname{Ker} f, f(g^{-1}) = f(g)^{-1} = e' \Longrightarrow g^{-1} \in \operatorname{Ker} f$$

$$(1), (2) \Longrightarrow \operatorname{Ker} f \leq G'$$
(3)
$$\forall g \in G, h \in \operatorname{Ker} f, f(ghg^{-1}) = f(g)f(h)f(g^{-1}) = e' \Longrightarrow ghg^{-1} \in \operatorname{Ker} f$$
$$\Longrightarrow \operatorname{Ker} f \trianglelefteq G \square$$

定理 2.6.3 同态基本定理(第一群同态定理) ()
同态基本定理(第一群同态定理) 设$f : G \to G'$是同态, 则:

$$G/\operatorname{Ker} f \cong f(G)$$

证明:

$$\forall \bar{g} \in G/\operatorname{Ker} f, f(\bar{g}) = \{f(g)f(k) | k \in \operatorname{Ker} f\} = \{f(g)\}$$

$$\Longrightarrow f(\bar{g}_1)=f(\bar{g}_2)\iff f(g_1)=f(g_2)$$

构造$\bar{f}:G/\operatorname{Ker}f\to f(G):\bar{f}(\bar{g})=f(g)$有:

$$\bar{f}^{-1}(f(g))=\bar{g}$$

$$\bar{f}(\bar{g}_1\bar{g}_2)=f(g_1g_2)=f(g_1)f(g_2)=\bar{f}(\bar{g}_1)\bar{f}(\bar{g}_2)$$

即$\bar{f}$是双射且为同态, $\Longrightarrow G/\operatorname{Ker}f\cong f(G)$.□

定理 2.6.4 第二同态定理 ()

第二同态定理 设$N\trianglelefteq G,H\leq G$. 则$(H\cap N)\trianglelefteq H,\quad N\trianglelefteq NH\leq G,\quad$ 并且

$$NH/N\cong H/(H\cap N)$$

证明:

N是G的正规子群, 同时也一定是NH的子群, $N\trianglelefteq NH$. 而由$N\trianglelefteq G$, 故$NH=HN$, 而

$$NH(NH)^{-1}=NHH^{-1}N^{-1}=NHHN=NHN=NNH=NH$$

故$NH\leq G$. 构造映射$f:H\mapsto NH/N,\quad h\mapsto\overline{h}=Nh$, 容易发现$f$为满同态, 故$f(H)=NH/H$, 且$\operatorname{Ker}f=H\cap N$, 由同构基本定理即得

$$NH/N\cong H/(H\cap N)$$

定理 2.6.5 第三群同构定理 ()

第三群同构定理 设 $N\lhd G,M\lhd G,N\leqslant M$, 则 $G/M\cong\frac{G/N}{M/N}$.

证明:

由上个定理知$M/N\lhd G/N$; 由 $N\lhd G,N\leqslant M$ 知$N\lhd M$)

定理 2.6.6 对应定理 ()

设$f:G\to G'$是满同态, 则:

(1)

$$K\leq G'\Longrightarrow\operatorname{Ker}f\trianglelefteq f^{-1}(K)\leq G$$

其中$f^{-1}(K)=\{g|g\in G,f(g)\in K\}$

(2)

$$\bar{G}:=\{H|\operatorname{Ker}f\trianglelefteq H\leq G\},\bar{G}':=\{H'|H'\leq G'\}$$

$$\exists\text{双射}\bar{f}:\bar{G}\to\bar{G}'$$

(3)

$$\forall N\in\bar{G},N\trianglelefteq G\iff f(N)\trianglelefteq G'$$

(4)

$$\forall N\in\bar{G},N\trianglelefteq G\Longrightarrow G/N\cong G'/f(N)$$

证明:
(1)

$$f(\operatorname{Ker} f) = e' \in K \Longrightarrow \operatorname{Ker} f \subseteq f^{-1}(K) \Longrightarrow \operatorname{Ker} f \trianglelefteq f^{-1}(K)$$

$$\forall g_1, g_2 \in f^{-1}(K), f(g_1 g_2) = f(g_1) f(g_2) \in K \Longrightarrow g_1 g_2 \in f^{-1}(K)$$

$$\forall g \in f^{-1}(K), f(g^{-1}) = f(g)^{-1} \in K \Longrightarrow g^{-1} \in f^{-1}(K)$$

$\Longrightarrow f^{-1}(K)$是一个群.

$$\Longrightarrow f^{-1}(K) \subseteq G \Longrightarrow f^{-1}(K) \leq G$$

$$\Longrightarrow \operatorname{Ker} f \trianglelefteq f^{-1}(K) \leq G$$

(2)

$$\forall g_1, g_2 \in G, f(g_1) = f(g_2) \iff g_1^{-1} g_2 \in \operatorname{Ker} f \iff g_1 \operatorname{Ker} f = g_2 \operatorname{Ker} f$$

$$\forall H \leq G, \operatorname{Ker} f \trianglelefteq H \operatorname{Ker} f \leq G$$

$$\operatorname{Ker} f \trianglelefteq H \Longrightarrow$$

$$\forall H \operatorname{Ker} f \in \bar{G}, \bar{f}(H \operatorname{Ker} f) := f(H) \leq G'$$

$$\bar{f}^{-1} \circ f(g) = g \operatorname{Ker} f$$

有$\bar{f}$是一个双射.
(3)

$$N \trianglelefteq G \iff \forall g \in G, gNg^{-1} = N \iff f(gNg^{-1}) = f(N)$$

$$\iff f(g) f(N) f(g)^{-1} = f(N) \iff f(N) \trianglelefteq G'$$

(4)

$$\varphi :$$

2.7 置换群

定义 2.7.1 变换 ()
设S是一个集合, 双射$\varphi : S \to S$称为是S上的一个**变换**. 当S为有限集时, 称φ是S上的一个**置换**. 当S是可数集或有限集时, φ可记作:

$$\varphi = \begin{pmatrix} x_1 & x_2 & x_3 & \cdots & x_n & (\cdots) \\ \varphi(x_1) & \varphi(x_2) & \varphi(x_3) & \cdots & \varphi(x_n) & (\cdots) \end{pmatrix}$$

恒同映射对应的置换称为恒等置换(id)。

定义 2.7.2 逆置换 ()
置换的乘法运算定义为映射的复合, 但运算顺序改为从左往右:
设φ,ψ是集合S上的置换, 则

$$\varphi\psi := \psi \circ \varphi$$

$$\varphi^n := \underbrace{\varphi \circ \varphi \circ \cdots \circ \varphi}_{n个\varphi}(n \in \mathbb{Z}^+)$$

定义 2.7.3 ()
设 $\sigma \in S_n$ 是一个置换。如果存在一个置换 $\sigma^{-1} \in S_n$，使得

$$\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \mathrm{id},$$

其中 id 表示恒等置换,则称 σ^{-1} 为 σ 的**逆置换**。

定义 2.7.4 支持集 ()
设 $f : X \to X$ 是一个映射（或置换）, 其中 X 是一个集合。f 的**支持集**定义为：

$$\mathrm{Supp}(f) = \{x \in X \mid f(x) \neq x\}.$$

换句话说, 支持集是 X 中所有被 f 改变的元素组成的集合。

定义 2.7.5 独立的 ()
设 σ 和 τ 是两个置换。如果它们的支持集不相交，即：

$$\mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\tau) = \varnothing,$$

则称 σ 和 τ 是**独立的**。

性质 2.7.5.1 轮换/循环(Cycle) ()
如果置换 σ 和 τ 是独立的，则它们可交换，即：

$$\sigma \circ \tau = \tau \circ \sigma.$$

性质 2.7.5.2 ()
如果置换 σ 和 τ 是独立的，则复合置换 $\sigma \circ \tau$ 的支持集是：

$$\mathrm{Supp}(\sigma \circ \tau) = \mathrm{Supp}(\sigma) \cup \mathrm{Supp}(\tau).$$

定义 2.7.6 ()
设n元有限集$S : S = \{x_1, x_2, \cdots, x_n\}$, S上的置换φ称为是一个n元**轮换/循环(Cycle)**, 若:

$$\forall x_i \in S, \varphi(x_i) = x_{i+1}(x_{n+1} := x_1)$$

记为

$$\varphi = (x_1, x_2, \cdots, x_n)$$

此时该轮换的长度为n.
特别地,长度为2的轮换称为**对换(Transposition)**,记作(x, y).长度为1的轮换称为**单位轮换(Identity Cycle)**.

定义 2.7.7 ()
设 σ 是一个置换。置换 σ 的阶是满足

$$\sigma^k = \mathrm{id}$$

的最小正整数 k 。

性质 2.7.7.1 ()
设φ是n元循环, $\varphi^n = I_d$, 即φ的阶为n.

性质 2.7.7.2 轮换分解 ()
(**轮换分解**)任何有限置换都可表示为有限个相互独立的循环之积.

证明:
运用数学归纳法.
(1)对于单元集而言, $\varphi = I_d$是一个一元循环.
(2)假设对于一切元素数$\leq k$的置换成立, 则对$S := \{x_1, x_2, \cdots, x_{k+1}\}$ 上的置换φ:
考虑$x_1 \in S, S_1 := \{x_1, \varphi(x_1), \varphi^2(x_1), \cdots, \varphi^k(x_1)\}$, 有$|S_1| \leq k+1$
1'若$|S_1| = k+1$, 则$\varphi = (x_1, \varphi(x_1), \varphi^2(x_1), \cdots, \varphi^k(x_1))$是一个$k+1$元循环.
2'若$|S_1| < k+1$, 则可构造$\begin{cases} \varphi_1(x) = \varphi(x) & , x \in S_1 \\ \varphi_2(x) = \varphi(x) & , x \in (S - S_1) \end{cases}$
其中:

$$\varphi_1 = (x_1, \varphi(x_1), \varphi^2(x_1), \cdots, \varphi^{|S_1|-1}(x_1))$$

而φ_2是一个定义在$k+1-|S_1| < k$元集$S - S_1$上的置换. 根据归纳假设, φ_2可表示为有限个独立循环之积.
φ_1, φ_2都是S上的$k+1$元置换, 且它们支持集(等于定义域)之交为$\varnothing$, 即它们相互独立.
$\varphi = \varphi_1\varphi_2 = \varphi_2\varphi_1 \square$
常将置换记为独立循环之积的形式.

性质 2.7.7.3 对换分解 ()
任何一个轮换都可以表示为对换的乘积,尽管分解方式不唯一.

证明:
轮换 $(a_1\ a_2\ \cdots\ a_k)$ 的标准分解方式为:

$$(a_1\ a_2\ \cdots\ a_k) = (a_1\ a_k)(a_1\ a_{k-1})\cdots(a_1\ a_3)(a_1\ a_2).$$

另一种分解方式为：

$$(a_1\ a_2\ \cdots\ a_k) = (a_1\ a_2)(a_2\ a_3)\cdots(a_{k-1}\ a_k).$$

还有许多其他分解方式。 □

性质 2.7.7.4 ()
(**对换分解**)任何有限置换都可表示为有限个对换的乘积.

证明:
设φ是S上的置换, 根据轮换分解, φ可表示为有限个独立循环之积. 对于任一循环$(a_1\ a_2\ \cdots\ a_k)$, 根据上述证明, 可表示为对换的乘积. 故φ可表示为有限个对换的乘积. □

定义 2.7.8 奇置换 ()
设 $\sigma \in S_n$ 是一个置换。将 σ 表示为一系列对换的乘积：

$$\sigma = \tau_1\tau_2\cdots\tau_k,$$

其中 τ_i 是对换。如果 k 是奇数，则称 σ 为**奇置换**；如果 k 是偶数，则称 σ 为**偶置换**。
需要注意的是，虽然对换的表示方式不唯一，但置换的奇偶性（即 k 的奇偶性）是唯一的。

定义 2.7.9 变换群(或对称群) ()
任给一个集合A, 则其上的置换全体显然成群，称为A上的**变换群(或对称群)**, 记作$S(A)$. 若$|A| = n$有限, 同构意义下也记作S_n. 全体偶置换也成群, 称为**交错群**, 同构意义下记作A_n.

定理 2.7.10 ()
S_n与A_n的生成元系
(1)若将S_n看作$\{1, 2, \cdots, n\}$上的置换群, 则$(1\ 2), (1\ 3), \cdots, (1\ n)$可以生成$S_n$.
(2)$n \geq 3$时, 全体长度为3的轮换可以生成A_n

2.8 群的直积

定义 2.8.1 外直积(Outer Direct Product) ()
设$G_1, \cdots, G_n$是群, 称$G = G_1 \times G_2 \times \cdots \times G_n$为群$G_1, \cdots, G_n$的**外直积(Outer Direct Product)**.

性质 2.8.1.1 内直积(Inner Direct Product) ()
G在运算"$\cdot$" : $G \times G \to G : (a_1, a_2, \cdots, a_n) \cdot (b_1, b_2, \cdots, b_n) = (a_1b_1, a_2b_2, \cdots, a_nb_n)$是一个群.

证明:
(1)运算封闭性:

$$\forall (a_1, a_2, \cdots, a_n), (b_1, b_2, \cdots, b_n) \in G, a_ib_i \in G_i$$

$$\Longrightarrow (a_1, a_2, \cdots, a_n) \cdot (b_1, b_2, \cdots, b_n) \in G$$

(2)恒等元存在:

$$(a_1,\cdots,a_n)\cdot(e_1,\cdots,e_n)=(e_1,\cdots,e_n)\cdot(a_1,\cdots,a_n)=(a_1,\cdots,a_n)$$

(3)逆元存在:

$$(a_1,\cdots,a_n)\cdot(a_1^{-1},\cdots,a_n^{-1})=(a_1^{-1},\cdots,a_n^{-1})\cdot(a_1,\cdots,a_n)=(e_1,\cdots,e_n)$$

即G是一个群.

定义 2.8.2 ()
设群$H_1,\cdots,H_n\leq G,G$称为$H_1,\cdots,H_n$的**内直积(Inner Direct Product)**, 若:

$$(1)G=H_1H_2\cdots H_n$$

$$(2)\varphi:H_1\times H_2\times\cdots\times H_n\to G:(a_1,a_2,\cdots,a_n)\mapsto a_1a_2\cdots a_n\text{是同构.}$$

性质 2.8.2.1 ()

$$H_1,H_2,\cdots,H_n\trianglelefteq G$$

证明:
$\because\varphi$是同态,

$$\Longrightarrow\forall(a_1,a_2,\cdots,a_n),(b_1,b_2,\cdots,b_n)\in H_1\times H_2\times\cdots\times H_n,$$

$$\varphi(a_1b_1,a_2b_2,\cdots,a_nb_n)=a_1a_2\cdots a_nb_1b_2\cdots b_n$$

$$\Longrightarrow a_1b_1a_2b_2\cdots a_nb_n=a_1a_2b_1b_2\cdots b_n$$

不妨取$a_3=a_4=\cdots=a_n=b_3=b_4=\cdots=b_n=e$
有$a_1b_1a_2b_2=a_1a_2b_1b_2\Longrightarrow b_1a_2=a_2b_1$
$\because a_2,b_1$是任意的, $\Longrightarrow\forall g_1\in H_1,g_2\in H_2,g_1g_2=g_2g_1$

$$\Longrightarrow g_2H_1=H_1g_2$$

同理, $\forall g_i\in H_i,g_iH_1=H_1g_i$

$$\because H_1H_2\cdots H_n=G,$$

$$\Longrightarrow\forall g\in G,\exists g_1\in G_1,g_2\in G_2,\cdots,g_n\in G_n:g=g_1g_2\cdots g_n$$

$$\Longrightarrow\forall g\in G,gH_1=g_1g_2\cdots g_nH_1=H_1g_1g_2\cdots g_n=H_1g$$

$$\Longrightarrow H_1 \trianglelefteq G$$

同理, $H_1, H_2, \cdots, H_n \trianglelefteq G\square$

性质 2.8.2.2 作用群(Operator Group) ()

$$H_i \cap \bigcup_{\substack{1\leq j\leq n\\ j\neq i}} H_j = \{e\}$$

证明:
运用反证法.
$\because H_1, \cdots, H_n$是群, $\Longrightarrow e \in H_1, \cdots, H_n$.
$\Longrightarrow$假设$\exists H_i, H_j : \{e\} \subsetneqq H_i \cap H_j$.
不妨设$i = 1, j = 2$, 即$\exists h \neq e : h \in H_1 \cap H_2$.
$\because \varphi$是同构, $\Longrightarrow \exists \varphi^{-1} : G \to H_1 \times \cdots \times H_n : a_1 \cdots a_n \mapsto (a_1 \cdots, a_n)$

$$a_3 := \cdots := a_n := e$$

$$\Longrightarrow \forall (a_1, a_2), (b_1, b_1) \in H_1 \times H_2, a_1a_2 = b_1b_2 \Longrightarrow a_1 = b_1, a_2 = b_2$$

考虑$e, h \in H_1 \cap H_2, eh = he, (e, h) \neq (h, e)$, 矛盾.

$$\Longrightarrow H_i \cap \bigcup_{\substack{1\leq j\leq n\\ j\neq i}} H_j = \{e\}\square$$

性质 2.8.2.3 ()
内直积的等价判定:

$$\begin{cases} G = H_1H_2 \cdots H_n \\ H_1, H_2, \cdots, H_n \trianglelefteq G \\ H_i \cap \bigcup\limits_{\substack{1\leq j\leq n\\ j\neq i}} H_j = \{e\} \end{cases} \Longrightarrow \varphi\text{是同构.}$$

证明:

2.9 群对集合的作用

在这一章, 我们研究群对集合的作用, 其本质思想为创造群中的元素与集合上的置换的对应.

定义 2.9.1 ()
作用群(Operator Group)
群G称为是集合S上的一个**左/右作用群(Left/Right Operator Group)**, 其每个元素称为S上的一个**左/右作用(Left/Right Operator)**, 若定义了二元运算“$*$”: $G \times S \to S$(或$S \times G \to S$), 满足:
(1)

$$\forall x \in S, e * x = x(\text{或} x * e = x)$$

(2)

$$\forall a, b \in G, (ab) * x = a * (b * x)(\text{或} x * (ab) = (x * a) * b)$$

性质 2.9.1.1 ()
S上的一个左/右作用群G同构于S上变换群的一个子群. 或者说, 存在由G到S上的变换群的同态映射. 对每个这样的同态映射, 称为群G在集合S上的作用的一个**置换表示**.

这条性质告诉我们左、右作用群在同构意义下完全相同, 故下面统称: G是集合S上的作用群, 按左作用群的符号记.

定义 2.9.2 轨道(Orbit) ()
轨道(Orbit)
群G是集合S上的一个左作用群, 对于其中某个元素x, $G * x := \{g * x | g \in G\}$称为$x$在$G$作用下的**轨道(Orbit)**.

性质 2.9.2.1 正则表示 ()

$$\forall x, y \in S, G * x = G * y \vee G * x \cap G * y = \varnothing$$

如果根据”a可以经由G中某个元素作用后成为b”定义关系$a \sim b$, 容易发现这是一个等价关系, 且每个等价类恰好是一条轨道, 集合也便可以拆分为若干个轨道的无交并.

定义 2.9.3 正则表示 ()
若考虑群G在其元素集G上的作用, 考虑映射

$$\rho : G \mapsto S(G)$$

$$g \mapsto \rho(g)$$

其中$\rho(g)$为一个置换, 作用在s上为$\rho(g)(s) = gs$,则ρ为一个置换表示, 称为**左正则表示**, 同理若将g右乘可以定义**右正则表示**.

除了置换表示, 正则表示之外还有共轭表示等, 其均为群对集合元素的二元运算“$*$”的不同定义, 故不多赘述.

定理 2.9.4 ()
(By Cayley) 每个群均同构于某个置换群.

证明:
根据群的性质容易验证上述ρ为单射, 故G同构于$\rho(G)$.

定义 2.9.5 ()
稳定化子(Stabilizer)
集合S上的左作用群G中的元素g称为是$x \in S$的一个**稳定化子(Stabilizer)**, 若$g * x = x$. x的稳定化子全体构成的集合记为$\operatorname{stab} x$.

性质 2.9.5.1 ()

$$\forall x \in S, \operatorname{stab} x \leq G$$

证明:
(1)乘法封闭:

$$a, b \in \operatorname{stab} x \Longrightarrow \forall x \in S, (ab) * x = a * (b * x) = a * x = x \Longrightarrow ab \in \operatorname{stab} x$$

(2)恒等元存在:

$$e \in \operatorname{stab} x, \forall g \in \operatorname{stab} x, eg = ge = g$$

(3)逆元存在:

$$\forall g \in G, x \in A, a^{-1} * x = a^{-1} * (a * x) = e * x = x \Longrightarrow a^{-1} \in \operatorname{stab} S$$

$$\Longrightarrow \operatorname{stab} A \leq G \square$$

性质 2.9.5.2 西罗(Sylow)p-子群 ()

$$|G * x| = |G : \operatorname{stab} x|$$

证明:
对G关于子群$\operatorname{stab} x$作左陪集分解$G = g_1 \operatorname{stab} x \cup g_2 \operatorname{stab} x \cup \cdots \cup g_n \operatorname{stab} x$, 其中$n = |G : \operatorname{stab} x|$, 则$g_1 \operatorname{stab} x * x = g_1 * x$, $g_2 \operatorname{stab} x * x = g_2 * x, \cdots$, $g_n \operatorname{stab} x * x = g_n * x$, 于是

$$G * x = g_1 \operatorname{stab} x \cup g_2 \operatorname{stab} x \cup \cdots \cup g_n \operatorname{stab} x * x = g_1 * x, g_2 * x, \cdots g_n * x$$

于是$|G * x| = n = |G : \operatorname{stab} x|$

2.10 Sylow定理

定理 2.10.1 ()
设 G 是有限群, p 为素数, r 是正整数, p^r 是$|G|$的因子. 用 $N(p^r)$ 表示G的p'阶子群的个数. 则$N(p^r) \equiv 1 (\operatorname{mod} p)$.特别地, 若$p^r || G|$,则$G$至少存在一个$p^r$ 阶子群.

证明:

定义 2.10.2 ()
设G为$p^r n$阶群，其中p为素数,$r \geqslant 1, p \nmid n$, 则G的每个p^r阶子群均叫做G的**西罗(Sylow)p-子群**.

定理 2.10.3 Sylow定理 ()
设G为有限群，则
(1)对$|G|$的每个素因子p,均存在G的西罗p-子群；
(2) G的西罗 p-子群彼此共轭；
(3)G的西罗p-子群的个数模p余1.
(4)设P为G的一个西罗p-子群，则G的西罗p-子群的个数为$[G : N_G(P)]$.

性质 2.10.3.1 ()
设A为G的某个素数p的幂阶的子群, 则其一定包含于某个G的sylow-p子群.

性质 2.10.3.2 (Fratini) ()
设P是G的一个sylow-p子群, 且$N_G(P) \leq A \leq G$, 则$N_G(A) = A$

定理 2.10.4 ()

(Fratini)设$M \triangleleft G$, P为M的sylow-p子群. 则$G = MN_G(P)$

推论 2.10.4.1 ()
设p,q为素数, 则pq阶或p^2q阶群G一定不是单群.

2.11 有限生成Abel群

我们研究约束条件最小, 最"自由"的群, 自由群.

定义 2.11.1 ()
设S为任一集合，其若干个元素$(a_1 a_2 \cdots a_m)$并在一起称为**字**，我们认为两个字相等当且仅当这若干个元素个数相同且对应位置相同. 并定义字之间的运算为$(a_1 a_2 \cdots a_n)(b_1 b_2 \cdots b_m) = a_1 a_2 \cdots a_n b_1 b_2 \cdots b_m$ 令$\sum^*(S)$为S所有字的集合, 在上述运算下, 若令空的字$(\cdot)$为幺元, 则上述集合成一个含幺半群, 称为S上的**自由含幺半群**.

为了将自由含幺半群扩充为群, 我们需要保证其有逆元.

定义 2.11.2 ()
对一个集合S, 记$S^{-1} = \{a^{-1} | a \in S\}$, 此处的$(*)^{-1}$仅为记号, 他表示的是该元素在进行字之间的运算时, 满足$(a)(a^{-1}) = (a^{-1})(a) = (\cdot)$. 于是集合$F(S) = \sum^*(S \cup S^{-1})$关于字之间的运算成群, 称为集合$S$上的**自由群**. S称为$F(S)$的**基**, 显然S也是$F(S)$的一个生成元系. 若S为有限群, 则称$F(S)$为**有限**

生成自由群.

定理 2.11.3 ()
每个群都是自由群的商群, 每个有限生成群都是有限自由群的商群.

证明:
取M为G的一个生成元系, 定义$S = \{X_a | a \in M\}$, 这一步是构造了群结构与字结构之间的双射, 便于区分. 考虑映射$f : F(S) \to G$, 其中对于单个字有$f(X_a) = a$, $f(X_a^{-1}) = a^{-1}$, 对于一串字, 则令$f(X_1X_2\cdots X_n) = f(X_1)f(X_2)\cdots f(X_n)$, 依次定义的映射是有意义的. 容易发现$f$为群同态, 且是满的. 于是$G = f(F(S))$, 由群同态基本定理. $f(F(S)) \cong F(S)/\operatorname{Ker}$. 而当$M$为有限集时, S也为有限集, 故$F(S)$为有限生成自由群, 证毕.

我们可以发现, 一个群G上的自由群是最不受限制, "最大"的群, G便是自由群$F(G)$在一定的"限制"得到的. 或者说, 我们只需知道$F(G)$中的那些字串被映作了单位元, 就可以以此确定群G. 故研究群G的结构时, 只需对$\ker f$进行研究了. 此时, 我们考虑能生成$\ker f$的集合, 他们便决定了哪些字串会被映作单位元.

定义 2.11.4 ()
群的表现(presentation) 设S为一个非空集合, R为自由群$F(S)$的一个非空子集, 用$N(N \trianglelefteq F(S))$表示$R$生成的正规子群, 则商群$F(S)/N$ 称为由**生成元集**S和**定义关系集**R决定的群. 若群G同构于$F(S)/N$, 则$\{S|R\}$称为群G的一个**表现**. 特别的, 若S, R是有限的, 则称G是**有限表现的(finitely presented)**.

重述一下上述定义, 即

性质 2.11.4.1 ()
$\{S|R\}$是群G的一个表现当且仅当$F(S)/N(R) \cong G$, 其中$N(R)$为由R生成的$F(S)$的正规子群.

定义 2.11.5 自由Abel群 ()
自由Abel群 设S为任意集合, 记 $S' = \{aba^{-1}b^{-1} | \forall a, b \in S\} \subseteq F(S)$. 若群$G$以$\{S|S'\}$为表现, 则称$G$为基$S$上的**自由Abel群**.

不难发现, 自由Abel群除了交换性之外不再有任何约束关系. 此时, G中元素均可写成$a_1^{p_1}a_2^{p_2}\cdots a_n^{p_n}$的形式.

2.12 正规群列与可解群

本章介绍可解群, 首先我们给出换位子的定义, 它可以衡量群的可交换程度.

定义 2.12.1 换位子与换位子群 ()
换位子与换位子群
对元素a,b, 定义其**换位子**为 $[a, b] = aba^{-1}b^{-1}$, 容易验证任一群G的全体换位子成群, 称为G的**换位子群**, 可记作G'

容易发现, a,b可交换当且仅当$[a, b] = e$, G为Abel群当且仅当$G' = \{e\}$

性质 2.12.1.1 可解群 ()
$G' \triangleleft G$

证明:
对任意$g \in G$, 易知$g^{-1}[a,b]g = [g^{-1}ag, g^{-1}bg]$, 于是$g^{-1}G'g$ 即$g^{-1}Gg = G$全体换位子所成群, 也即$g^{-1}G'g = G', \forall g \in G$. 故得证.

性质 2.12.1.2 ()
设$N \triangleleft G$, 则G/N为Abel群当且仅当$G' \leq N$

证明:
若G/N为Abel群, 则对任意a, $b \in G$, 有$a^{-1}b^{-1}N = b^{-1}a^{-1}N$, 于是 $bab^{-1}a^{-1}N = N$, 即$[b,a] \in N$, 故$G' \leq N$.
另一方面, 若$G' \leq N$, 由于对任意$a, b \in G$, $abG' = ab[b^{-1}, a^{-1}]G' = baG'$, 于是$G/G'$为Abel群. 由第三群同构定理. $G/N \cong \frac{G/G'}{N/G'}$, 于是$G/N$同构于一个Abel群的商群. 故$G/N$为Abel群. 证毕.

现在记$(G')'$为$G^{(2)}$, $(G^{(2)})\prime = G^{(3)}$, 以此类推.

定义 2.12.2 ()
可解群
根据上上个性质, 我们得到一个正规群列 $G \triangleright G' \triangleright G^{(2)} \triangleright \cdots \triangleright G^{(i-1)} \triangleright G^{(i)} \triangleright \cdots$
若存在正整数n使得$G^{(n)} = \{e\}$, 则称G为**可解群**

性质 2.12.2.1 ()
可解群的子群和商群都是可解群.

证明:
设$H \leq G$, 则H的每个换位子都包含在G的换位子群中, 于是$H' \leq G'$, 依此类推$H^{(2)} \leq G^{(2)}, \cdots, H^{(i)} \leq G^{(i)}, \cdots, H^{(n)} \leq G^{(n)} = \{e\}$, 故$H^{(n)} = \{e\}$, 于是$H$为可解群.
容易验证, 可解群的任何一个同态像一定也是可解群, 故考虑自然映射即可证其商群一定为可解群.

性质 2.12.2.2 正规列 ()
设$N \trianglelefteq G$，则G是可解群当且仅当N与G/N均为可解群.

证明:
充分性已证. 当N与G/N均为可解群时, 考虑自然同态f, 由G/N可解, 可知存在n使得 $f(G^{(n)}) = (G/N)^{(n)} = \{e\}$ 故$G^{(n)} \leq N$, 而由N可解, 故$G^{(n)}$可解, 于是G可解.

定义 2.12.3 ()
设群G有一个子群列$G = G_0 \geq G_1 \geq G_2 \geq \cdots \geq G_n$, 其中$G_0 = G$, $G_n = \{e\}$, 若每个G_i为G_{i-1}的正规子群, 则称为**正规列** 若正规列中G_{i-1}/G_i均为单群, 则称为**合成列**. 一个正规列被称作**可解列**,

当G_{i-1}/G_i均为Abel群.

定理 2.12.4 ()
有限群必有合成列

定理 2.12.5 ()
群G是可解群当且仅当他有可解列.

性质 2.12.5.1 ()
有限群G是可解群当且仅当他有正规列, 且列中G_i/G_{i+1}均为素数阶循环群.

定理 2.12.6 ()
$n \geq 5$时, S_n不可解.

定理 2.12.7 ()
奇数阶有限群均为可解群

该定理由Burnside提出猜想, 后被证明. 证明过程很长故不写了.

2.13 低阶有限群的结构

3 环论

3.1 环的基本概念

定义 3.1.1 环(Ring) ()
环(Ring)
非空集合R称为是一个**环(Ring)**, 若在R上定义了两种运算: "$+$"和"$\cdot$", 且满足:
(1)$(R,+)$是一个加法群 (设其加法恒等元为0);
(2)乘法结合律成立:

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

(3)乘法分配律成立:

$$\forall a,b,c \in R, \begin{cases}(a+b)\cdot c = a\cdot c + b\cdot c\\ c\cdot(a+b) = c\cdot a + c\cdot b\end{cases}$$

*对环的乘法, "$\cdot$"通常可省略.
若$\exists e \in$环R: $\forall a \in R, ea = ae = a$, 称环$R$是一个**幺环(Unitary Ring)**

定义 3.1.2 交换环(Commutative Ring) ()
交换环(Commutative Ring)

环R称为是一个**交换环(Commutative Ring)**, 若:

$$\forall a, b \in R, ab = ba$$

定义 3.1.3 整环 ()
$a, b \in R : a, b \neq 0, ab = 0$, 称$a$是$b$的**左零因子**, b是a的**右零因子**.
无零因子的环称为**整环**.

性质 3.1.3.1 整环中适合消去律 ()
若R是一个整环, 则:

$$ab = ac \wedge a \neq 0 \Longrightarrow b = c$$

定义 3.1.4 除环 ()
除环
环R称为是一个**除环**, 若$R - \{0\}$在环乘法意义下是一个群.

定义 3.1.5 域(Field) ()
域(Field)
交换除环称为**域(Field)**.

定义 3.1.6 代数 ()
代数
定义了数乘运算的域称为代数.