第一章　群论

1.1　基本知识

1.1.1　集合

定义 1.1.1. f 的原像 f^{-1} 由谓纤维，

$$f^{-1}(C)=\{a\in A\mid f(a)\in C\}.$$

定义 1.1.2. f 为单射，如果 $a_1\neq a_2\Rightarrow f(a_1)\neq f(a_2)$。

定义 1.1.3. f 为满射，如果 f 映满 B。

定义 1.1.4. f 为双射，如果它是单射与满射。

定义 1.1.5. f 有左逆，如果有 g 满足 $g\circ f=I$。

定义 1.1.6. f 有右逆，如果有 h 满足 $f\circ h=I$。

定理 1.1.1. 设 $f:A\to B$，则下列结论成立：

1. 左逆存在当且仅当 f 为单射；
2. 右逆存在当且仅当 f 为满射；
3. f 为双射当且仅当左右逆存在且相等；
4. 若 A 与 B 等大有限，f 为双射当且仅当 f 为单射当且仅当 f 为满射。

证明. 若左右逆存在且分别为 h，则 $g=fgg=hfg=h$。 □

定义 1.1.7. A 到自身的双射谓置换。

定义 1.1.8. 二元关系为 $A\times A$ 上的子集，若 $(a,b)\in R$ 则 $a\sim b$。

定义 1.1.9. 二元关系为等价关系，如果它满足对称性、自反性与传递性。

定义 1.1.10. a 的等价类是所有满足 $x \sim a$ 的元素。

定义 1.1.11. A 的划分是并为 A 的非空无交集族。

定理 1.1.2. 等价关系与划分等价。

1.1.2 整数

定理 1.1.3. *Euclidean* 算法可以得到最大公因数。

$$\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ &\cdots \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n. \end{aligned}$$

则 r_n 为最大公因数。

推论 1.1.1. $r_n = \gcd(a, b)$ 为 a 和 b 的线性组合。

定义 1.1.12. 只能被 1 和自身整除的数称为质数。

定理 1.1.4. 若质数 $p|ab$，则 $p|a$ 或 $p|b$。

证明. 若 $p \nmid a$，则 $\gcd(a, p) = 1$ 故 $ax + py = 1$，$abx + pby = b$，故 $p|b$。 □

定理 1.1.5 (算术基本定理)**.** 质因数分解存在且唯一。

定理 1.1.6. 定义 $\varphi(n) = \#(\{a \mid a \leq n, \gcd(a, n) = 1\})$，则

$$\varphi(n) = \prod p_i^{\alpha_i - 1}(p_i - 1) = n \prod \left(1 - \frac{1}{p_i}\right).$$

证明. 鸽笼原理的直接应用。 □

1.1.3　剩余系

定义 1.1.13. 等价类 $\bar{a} = \{a + kn\}$ 记作 $\mathbb{Z}/n\mathbb{Z}$。

定理 1.1.7. $\mathbb{Z}/n\mathbb{Z}$ 上一般加减乘成立。

定理 1.1.8. $\mathbb{Z}/n\mathbb{Z}$ 的乘法群为

$$(\mathbb{Z}/n\mathbb{Z})^{\times} = \{\bar{a} \mid \gcd(a, n) = 1\}.$$

1.2　群论导论

1.2.1　群的定义

定义 1.2.1. 二元运算谓结合的，若结合律成立。谓交换的，若交换律成立。

例 1.2.1. 加、乘是交换、结合的。减法、叉乘既不交换也不结合。$a \star b = (a + b)/2$ 以及 $a \star b = ab + 1$ 交换但不结合。

定义 1.2.2. 若集合上有定义一结合且可逆的二元运算，则谓之群。

定义 1.2.3. 若相应的二元运算可逆，则谓 *abelian* 群。

例 1.2.2. $\mathbb{Z}$，$\mathbb{Q}$，$\mathbb{R}$ 与 $\mathbb{C}$ 关于加法成群。$\mathbb{Q} - \{0\}$ 与 $\mathbb{Q}^+$ 等关于乘法成群。

例 1.2.3. 向量空间、$\mathbb{Z}/n\mathbb{Z}$ 关于加法成群。$(\mathbb{Z}/n\mathbb{Z})^{\times}$ 关于乘法成群。

定义 1.2.4. (a, b) 在保留两个分量上的运算构成新的群，谓其直积。

命题 1.2.1. 对于群 G 和运算 $\star$，成立下列结论：

1. 群的单位元唯一；
2. 逆元 a^{-1} 唯一；
3. $(a^{-1})^{-1} = a$；
4. $(a \star b)^{-1} = b^{-1} \star a^{-1}$；
5. $a_1 \star a_2 \star \cdots \star a_n$ 可随意添加括号。

证明. 最后一条注意括号必定将表达式先分割成两部分，归纳即可。　□

命题 1.2.2. 对于群，$ax = b$ 与 $ya = b$ 有唯一解（不一定相等）。

只有在上述广义结合律被证明后，不添加括号的表达式才能没有歧义。

定义 1.2.5. *x 的阶 $|x|$ 谓满足 $x^n = 1$ 的最小正整数，不存在时取无穷。*

例 1.2.4. *一阶元仅有单位元。$(\mathbb{R} - \{0\})^\times$ 中 (-1) 为二阶元，其他非 1 元素为无穷阶。$\mathbb{Z}/9\mathbb{Z}$ 中 $\bar{6}$ 为三阶元。$(\mathbb{Z}/7\mathbb{Z})^\times$ 中 2 为三阶元。*

定义 1.2.6. *群 G 的乘法表谓 $a_i a_j$ 全体构成的矩阵。*

1.2.2　二面体群

定义 1.2.7. *二面体群 D_{2n} 谓正 n-边形全体对称操作的集合。*

鉴于对称操作可以视为函数，显然 D_{2n} 构成群。每个对称都可以由顶点 1 的目标序号 i 以及顶点 0 的目标序号确定，前者有 n 个选择而之后后者有两个。故 $|D_{2n}| = 2n$。

命题 1.2.3. *对原子旋转 ρ 与横轴反射 r，成立*

1. $|\rho| = n$ *且* $|r| = 2$;
2. $r \neq \rho^i$;
3. $\rho r = r\rho^{-1}$ *且* $\rho^i r = r\rho^{-i}$。

借此可以化简 r 与 ρ 的任意组合。

生成元和关系

定义 1.2.8. *子集 S 生成群 G，如果 G 中任何元素都可以写成 S 的元素及其逆的积，记作 $G = \langle S \rangle$。*

鉴于有限阶群的元素阶数有限，逆表示为积，故 G 可写成 S 中的积。

定义 1.2.9. *生成元之间的方程谓关系。*

例如 $\rho^n = 1$，$r^2 = 1$ 与 $\rho r = r\rho^{-1}$ 是关系，实际上 D_{2n} 的其他关系都可以由它们导出。

定义 1.2.10. *群的表达谓生成元和关系，记作 $G = \langle S | R_i \rangle$。*

例如，$D_{2n} = \langle \rho, r | \rho^n = 1, r^2 = 1, \rho r = r\rho^{-1} \rangle$。

例 1.2.5. $X = \langle x, y | x^n = y^2 = 1, xy = yx^2 \rangle$，则 $x = yx^2y = yxy \cdot yxy = x^4$，故 $x^3 = 1$，发生崩塌。

例 1.2.6. $X = \langle x, y | x^4 = y^3 = 1, xy = y^2x^2 \rangle$，则发生全盘崩塌。

证明. 只证 $x^3 = y^2x^4$，就有 $x = y = 1$。注意 $yxy = x^2$ 推出 $xyxy = x^3$，

$$\begin{aligned} x^3 &= y^2x^2y^{-1} \cdot y^2x^2y^{-1} \cdot y^2x^2y^{-1} \\ &= y^2x^2y \cdot x^2y \cdot x^2y^{-1} \\ &= xy \cdot yx \cdot xyx \cdot xy^{-1} \\ &= y^2x^2 \cdot yx \cdot y^2x^4y^{-1} \\ &= y^2x^2yxy = y^2x^4. \end{aligned}$$

□