1 介绍

1. 参考书: 近世代数引论 (冯克勤, 第三版); 代数学引论 (聂灵沼);
2. 成绩: 30% 平时成绩, 70% 期末考试;
3. 习题答案: 近世代数 300 题;
4. 集合等势: 两个集合之间存在一一映射;
5. 二元运算: 记 S 为非空集合, 从 $S \times S$ 到 S 的映射 $f : S \times S \to S$ 即 $(x, y) \mapsto f(x, y)$ 叫做集合 S 上的一个二元运算 (也称为运算的封闭性), 通常简记“$\cdot$”;
6. 代数研究的对象: 含有一个或多个二元运算的集合或结构的性质;

2 群

1. 结合律: 集合 S 上的二元运算 f 称为满足结合律, 是指 $f(f(x, y), z) = f(x, f(y, z)), x, y, z \in S$, 简记为 $(xy)z = x(yz)$;
2. 半群: 具有二元运算“$\cdot$”的集合 S, 若该运算满足结合律, 则 $(S, \cdot)$ 被称为半群;
3. 单位元 (幺元): 设 $(S, \cdot)$ 是半群, $e \in S$, 若对 $\forall x \in S$, 有 $xe = ex = x$, 则称 e 为半群 S 的单位元;
   (a) 单位元唯一: 若 $e, e' \in S$ 是单位元, $e = ee' = e'$;
   (b) 左右单位元:
      i. 左单位元: 若 $e_L \in G$ 满足 $\forall a \in G, e_L a = a$, 则 e_L 称为左单位元;
      ii. 右单位元: 若 $e_R \in G$ 满足 $\forall a \in G, a e_R = a$, 则 e_R 称为右单位元;
4. 含幺半群: 含有单位元的半群;
5. 群: 设 G 是一个非空集合, $(G, \cdot)$ 是群若 G 上的二元运算“$\cdot$”(封闭性) 满足:

(a) 结合律: $\forall a,b,c\in G,(ab)c=a(bc)$;

(b) 单位元 (幺元): $\exists e\in G:\forall a\in G,ea=ae=a$;

(c) 逆元: $\forall a\in G,\exists a^{-1}\in G,s.t.:a^{-1}a=aa^{-1}=e$;

6. 群的逆元唯一: 若 $a^{-1},a'^{-1}\in G$ 都是 a 的逆元, 则 $e=a^{-1}a=a'^{-1}a=aa^{-1}=aa'^{-1}$;

   (a) 含幺半群左右逆元相同: 设 $(G,\cdot)$ 为一个含幺半群, 若元素 $a\in G$ 有左逆元 a_L^{-1} 和右逆元 a_R^{-1}, 则 $a_L^{-1}=a_R^{-1}=a^{-1}$ 为 a 的逆元;

7. 交换群 (阿贝尔群): 满足交换律的群;

8. 设 $(M,\cdot)$ 是含幺半群, M^* 是半群 M 中的可逆元素全体, 则 $(M^*,\cdot)$ 是群;

9. 半群 $(G,\cdot)$ 是群, 当且仅当 (右单位元和右逆元定义同样成立):

   (a) G 有左单位元 e_L: 即 $\forall a\in G:e_La=a$;

   (b) $\forall a\in G$, 有左逆元 a^{-1}, 使得 $a^{-1}a=e_L$;

10. 半群 $(G,\cdot)$ 是群, 当且仅当: $\forall a,b\in G$, 方程 $ax=b$ 和 $ya=b$ 在 G 中均有解;

11. 有限半群 $(G,\cdot)$ 是群, 当且仅当左右消去率都成立: $ax=ay\Rightarrow x=y$ 且 $xa=ya\Rightarrow x=y$;

3 子群

1. 子群: 设 $(G,\cdot)$ 为群, S 是 G 的一个非空子集, 若 S 对 G 的运算"$\cdot$"也构成群, 则称 S 为 G 的子群, 表示为 $S\leq G$;

   (a) 真子群: 若 $S\neq G,S\leq G$, 则 S 是 G 的真子群, 记为 $S<G$;

   (b) 记号:

      i. 设 G 是一个群, A,B 是 G 的非空子集, $g\in G$, 记: $gA=\{ga|a\in A\}$, $Ag=\{ag|a\in A\}$, $AB=\{ab|a\in A,b\in B\}$, $A^{-1}=\{a^{-1}|a\in A\}$;

   (c) 平凡子群: 特殊的子群 e,G;

2. 子群的性质:
   (a) 若 $H \leq G$, 则 H 的单位元就是 G 的单位元;
   (b) $H_1, H_2 \leq G \Rightarrow H_1 \cap H_2 \leq G$;
   (c) $H_1, H_2 \leq G$, 则 $H_1 \cup H_2 \leq G \Leftrightarrow H_1 \subseteq H_2$ 或者 $H_2 \subseteq H_1$;
   (d) $H_1, H_2 \leq G$, 则 $H_1H_2 \leq G \Leftrightarrow H_1H_2 = H_2H_1$;
3. 子群的判定定理: 设 S 是群 G 的非空子集, 则下面三个命题等价:
   (a) S 是群 G 的子群;
   (b) $\forall a, b \in S$, 有 $ab \in S$ 和 $a^{-1} \in S$;
   (c) $\forall a, b \in S$, 有 $ab^{-1} \in S$;
4. 实数域上一般线性群的特殊子群:
   (a) n 次特殊线性群: $SL(n, \mathbb{R}) = \{A \in GL(n, \mathbb{R}) || A| = 1\}$;
   (b) n 次正交线性群: $O_n(\mathbb{R}) = \{A \in GL(n, \mathbb{R}) | A^tA = I_n\}$;
   (c) n 次特殊正交群: $SO_n(\mathbb{R}) = \{A \in GL(n, \mathbb{R}) | A^tA = I_n, |A| = 1\}$;
5. 元素的幂: 设 G 是群, $a \in G, n \in \mathbb{N}$, 定义 $a^n = a \cdots a(n$ 个$), a^0 = e$;
   (a) 注意: 一般 $a^nb^n \neq (ab)^n$, 只有 $ab = ba$ 时等号成立;
6. 元素的阶: 设 G 是群, $a \in G$, 使 $a^n = e$ 成立的最小正整数 n 称为元素的阶, 记作 $o(a)$; 若不存在正整数 n 满足上面的条件, 则称 a 的阶是无限的;
   (a) 若 $o(a) = n$, 则 $a^m = e \Leftrightarrow n|m$. $n|m$ 表示 n 整除 m, 即 $\frac{m}{n}$ 是整数;
   (b) 若 $o(a) = n$, 则对每个正整数 m, a^m 的阶是 $\frac{n}{(m,n)}$. (m, n) 表示 m 和 n 的最大公因数;
   (c) $a, b \in G, o(a) = m, o(b) = n$, 若 $(m, n) = 1$ 且 $ab = ba$, 则 $o(ab) = mn$;
      i. 若 $(m, n) = 1$ 不满足, 则 $o(ab) = \frac{mn}{(m,n)}$;
   (d) 若除单位元外其他元素都是 2 阶元, 则 G 是交换群;
7. 生成子群: 设 G 是群, $S \subseteq G$, 则 G 中包含 S 的最小子群 A 叫做由 S 生成的子群, 记作 $A =< S >$;

(a) 等价定义: A 是 G 中包含 S 的所有子群之交, $< S >= \{a_1...a_m | m \geq 0, a_i \in S \cup S^{-1}\}$; 当 $m = 0$ 时, $a_1...a_m = e$;

(b) 生成元系: 若 $G =< S >$, 则称 S 是 G 的一个生成元系;

(c) 有限生成群: 若 $G =< S >$, 且 S 是有限集合, 则称 G 为有限生成群;

(d) 循环群: 若 $G =< a >$, 则称 S 为循环群;

(e) n 阶有限群: 设 $G =< a >$ 为循环群, 若 $o(a) = n$, 则 G 为 n 阶有限群;

(f) 无限群: 设 $G =< a >$ 为循环群, 若 a 的阶无限, 则 G 为无限群;

8. 关系: 若 A 是集合, 集合 $A \times A$ 的一个子集 R 叫做集合 A 上的一个关系;

   (a) 如果 $(a, b) \in R$, 称 a 和 b 有关系 R, 写成 aRb;

9. 等价关系:

   (a) 自反性: $\forall a \in A, a \sim a$;

   (b) 对称性: 若 $a \sim b$, 则 $b \sim a$;

   (c) 传递性: 若 $a \sim b, b \sim c$, 则 $a \sim c$;

10. 等价类: 具有等价关系的元素全体称为一个等价类, 记作 $[a]$;

    (a) $a \in [a]$;

    (b) $\forall b, c \in [a] \Rightarrow b \sim c$;

    (c) $\forall b \in [a] \Rightarrow [b] = [a]$;

        i. 代表元: $[a]$ 中任取一个元素 b, 则可以称 b 为等价类 $[a]$ 的代表元;

    (d) 不同等价类不相交;

    (e) 若 $A = \cup_{i \in I}[a_i], [a_i], i \in I$ 两两不相交, 从每个等价类 $[a_i]$ 中取一个元素 b_i, 则 $R = \{b_i\}$ 具有性质: A 中每个元素都等价于 b_i, 而不同的 b_i 彼此不等价, 我们把这样的 R 叫做 A 对于等价关系 $\sim$ 的完全代表系. 于是 $A = \cup_{a \in R}[a]$(不相交);

11. 分拆: 若集合 $A = \cup_{i\in I} A_i$, $A_i, i \in I$ 两两不相交, 则称 $\{A_i | i \in I\}$ 是 A 的一个分拆;

    (a) 结论: A 上的等价关系与 A 上的分拆一一对应;

4 子群的陪集

1. 整数模 n 加法群: 设 n 为正整数, 在 $\mathbb{Z}$ 上定义关系 $a, b \in \mathbb{Z}, a \sim b \Leftrightarrow n|(a-b)$(即 $a \equiv b(mod\ n)$), 定义 $\bar{i} = \{m \in \mathbb{Z} | m \equiv i(\mod n)\}$, 则 $\mathbb{Z}_n = \{\bar{0}, \bar{1}, ..., \overline{n-1}\}$. 定义二元运算"+": $\bar{a} + \bar{b} = \overline{a+b}$, $\mathbb{Z}_n$ 关于"+"形成交换群, 形成整数模 n 加法群;

2. 设 G 是群, $A \leq G$, 定义 G 上的关系为 $g, h \in G, g \sim h \Leftrightarrow gh^{-1} \in A$, 则 $\sim$ 是 G 上的关系, 并且 $\forall g \in G, [g] = Ag$;

3. 右陪集: 由上面的引理知, 群 G 可以分拆称一些不同等价关系集合 Ag, 每个等价类 Ag 叫做 G 对于子群 A 的右陪集;

    (a) 右陪集代表元系: 如果 $R = \{g_i | i \in I\}$ 是 G 对于上述等价关系的完全代表元系, 则称它为 G 对 A 的右陪集代表元系;

    (b) 右陪集分解: 有 $G = \cup_{g\in R} Ag$, 称之为 G 对子群 A 的右陪集分解;

    (c) 指数: 不同右陪集的个数 $|R|$, 记为 $[G : A]$, 称为子群 A 对群 G 的指数 (指标);

4. 左陪集: 类似定义 gA 为 G 的左陪集, 左陪集代表元系, 左陪集分解等;

    (a) 左陪集与右陪集一一对应, 个数相等;

5. 集合的阶: 集合 G 中元素的个数, 记作 $|G|$ 或 $\#(G)$;

6. 拉格朗日 (Lagrange) 定理: 设 G 是有限群, $A \leq G$, 则 $|G| = |A| \cdot [G : A]$. 特别地, 群 G 的每个子群的阶都是 G 的阶的因子;

    (a) 素数阶群只有平凡子群;

    (b) 设 G 是有限群, 则 G 中每个元素 g 的阶均是 $|G|$ 的因子;

    (c) p(素数) 阶群 G 均是 Abel 群 (交换群);

        i. 素数阶群一定是循环群;

(d) 非 Abel 群的最小阶数是 6;

7. 设 G 是有限群, $A, B \leq G$, 则:

   (a) $|AB| = |A| \cdot |B| / |A \cap B|$;

   (b) 若 $A \leq B \leq G$, 则 $[G : A] = [G : B][B : A]$;

   (c) $[G : A \cap B] \leq [G : A][G : B]$. 若 $[G : A]$ 和 $[G : B]$ 互素, 则 $[G : A \cap B] = [G : A][G : B]$, 且 $AB = G$;

8. 共轭: 设 G 是群, $a, b \in G$, 称 $b^{-1}ab$ 为 a 的共轭元素;

   (a) 集合共轭: $A, B \subseteq G$, 若 $\exists g \in G, s.t. : g^{-1}Ag = B$ 称 A 与 B 共轭;

   (b) 共轭类: 群 G 的子集之间的共轭关系是等价关系, 每个等价类被称为共轭类;

      i. 集合 $g^{-1}Ag$ 与 A 之间一一映射;

      ii. 若 A 是有限集合, 则 $|g^{-1}Ag| = |A|$;

   (c) 共轭子群: 若子群 $A \leq G$, 则 $g^{-1}Ag \leq G$ 称为 A 的共轭子群;

9. 正规化子: 设 G 是群, 子集 $M \subseteq G$, 则 $N_G(M) = \{g \in G | g^{-1}Mg = M\}$ 是 G 的子群, 称之为 M 的正规化子;

10. 中心化子: 设 G 是群, 子集 $M \subseteq G$, 则 $C_G(M) = \{g \in G | g^{-1}ag = a, \forall a \in M\}$ 是 G 的子群, 称之为 M 的中心化子;

    (a) 中心: 记 $C(G) = C_G(G)$ 称为群 G 的中心;

    (b) 中心元素: C(G) 中的元素;

    (c) 一些结论:

       i. G 是交换群, 等价于 $G = C(G)$;

       ii. $C_G(M) \leq N_G(M)$;

       iii. $\forall a \in G, C_G(a) = N_G(a)$;

11. 若 G 是群, 子集 $M \subseteq G$, 则与 M 共轭的子集个数为 $[G : N_G(M)]$;

    (a) 设 G 是群, $a \in G$, 则与 a 共轭的元素个数等于 $[G : C_G(a)]$;

12. 设 p 为素数, $n \geq 1$, G 为 p^n 阶群, 则 $|C(G)| > 1$, 即 G 有非单位元的中心元素;

    (a) 设 p 为素数, p^2 阶群 G 为 Abel 群;

5 群的同态

1. 群的同态: 设 $(G,\cdot)$ 和 $(G',\circ)$ 是两个群, 若映射 $f:G\to G'$ 满足 $\forall a,b\in G$, 有 $f(a\cdot b)=f(a)\circ f(b)$, 则称 f 是群 G 到 G' 的同态;

   (a) 单同态: 若 f 是单射, 则 f 为单同态;

   (b) 满同态: 若 f 是满射, 则 f 是满同态;

   (c) 设 G,H 为群, $f:G\to H$ 是群的同态, 则 $f(e_G)=e_H$, 且 $\forall a\in G$, 有 $f(a^{-1})=f(a)^{-1}$. 即群同态将单位元映射到单位元, 逆元映射到逆元;

2. 同构: 若同态映射 f 是双射, 则 f 是群 G 到 G' 的同构. 记为 $f:G\tilde{\to}G'$ 或 $G\cong G'$. 同构的群被认为本质上是相同的;

   (a) 群 G 到自身的同态 (同构) 叫做群 G 的自同态 (自同构);

   (b) 记 $Aut(G)$ 为群 G 的自同构全体, 则它构成群;

3. 循环群的性质: 设 $G=<a>$ 是由 a 生成的循环群, 则:

   (a) 若 $o(a)=\infty$, 则 $G\cong(\mathbb{Z},+)$, 称 G 为无限循环群;

   (b) 若 $o(a)=n$, 则 $G\cong(\mathbb{Z}_n,+)$, 称 G 为 n 阶循环群;

   (c) 同阶循环群彼此同构;

   (d) $(\mathbb{Z},+)$ 的生成元只有 1 或 -1; $(\mathbb{Z}_n,+)$ 的生成元只能是 $\bar{a}$, 其中 $(a,n)=1$;

      i. 即若 $o(a)=\infty$, 则 G 的生成元只有 a 和 a^{-1}; 若 $o(a)=n$, 则 G 的生成元只有 $a^k(1\le k<n,(k,n)=1)$;

   (e) 循环群的子群仍然是循环群, 且:

      i. $(\mathbb{Z},+)$ 的全部子群 $H_m=<m>,m=0,1,2,...$;

      ii. $(\mathbb{Z}_n,+)$ 的全部子群为 $<\bar{0}>$ 和 $<\bar{d}>,d|n$;

   (f) 循环群的同构群:

      i. $(\mathbb{Z},+)$ 的自同构群 $Aut(\mathbb{Z})$ 是二元群;

      ii. $(\mathbb{Z}_n,+)$ 的自同构群 $Aut(\mathbb{Z}_n)$ 是同构于 $(\mathbb{Z}_n^*,\cdot)$;

4. 自共轭子群: 共轭子群只有自身的子群;

5. 正规子群: 设 G 是群, $N \leq G$ 称为 G 的正规子群, 若对 $\forall g \in G$, 有 $g^{-1}Ng = N$, 记为 $N \triangleleft G$(即 N 是 G 中的自共轭子群);

   (a) 等价条件:

      i. $N \triangleleft G$;

      ii. $\forall g \in G, gN = Ng$;

      iii. $N_G(N) = G$;

      iv. G 对于 N 的每个左陪集均是右陪集;

      v. $\forall g \in G, h \in N$, 有 $g^{-1}hg \in N$;

6. 商群: 设 G 是群, $N \triangleleft G$, 对 $\forall a \in G$, 记 $\bar{a} = Na = aN$. 在集合 $\bar{G} = \{\bar{a}|a \in G\}$ 上定义二元运算 $\bar{a} \cdot \bar{b} = \overline{ab}$. $\bar{G}$ 对此运算形成群 (幺元 $\bar{e}$, 逆元 $\bar{a}^{-1} = \overline{a^{-1}}$), 称为 G 对正规子群 N 的商群, 记为 $\bar{G} = G/N$;

   (a) 若 G 是有限群, 则 $|G/N| = [G : N] = [G]/|N|$;

7. 同态定理: 设 $f : G \to G'$ 是群的同态, 则:

   (a) $Imf = f(G) \leq G'$;

   (b) $Kerf = f^{-1}(e_{G'}) = \{g \in G|f(g) = e_{G'}\} \triangleleft G$;

   (c) 映射 $\pi : G \to G/Kerf, \pi(g) = gKerf$ 是满同态;

   (d) 存在唯一同态 $\bar{f} : G/Kerf \to G'$, 使得 $f = \bar{f} \circ \pi$, 且 $\bar{f}$ 是单同态 (称 $\bar{f}$ 是由 f 诱导的同态);

   (e) $Im\bar{f} = Imf$, 即 $\bar{f} : G/Kerf \tilde{\to} Imf$;

8. 同态基本定理: 设 $f : G \to G'$ 是群的同态, 则 $Imf = f(G)$ 是 G' 的子群, $Kerf = f^{-1}(e_{G'}) = \{g \in G|f(g) = e_{G'}\}$ 是 G 的正规子群, 并且有群同构 $\bar{f} : G/Kerf \tilde{\to} Imf, (\bar{g} \mapsto f(g))$;

   (a) 推论: 设 $f : G \to G'$ 是群的同态, 则

      i. f 是单同态 $\Leftrightarrow Kerf = \{e_G\}$;

      ii. 若 f 是满同态, 则有 (正则) 同构 $\bar{f} : G/Kerf \tilde{\to} G'$;

9. 设 G 是群, $N \triangleleft G$, 则 $\{M|N \leq M \leq G\} \leftrightarrow \{\text{subgroups of } G/N\}$, $\{M|N \leq M \leq G\} \leftrightarrow \{\text{invariant subgroups of } G/N\}$, 且对 $N \leq M \leq G$, 有 $M \triangleleft G \Leftrightarrow M/N \triangleleft G/N$;

10. 设G是群,$N, M \triangleleft G$,且$N \leq M$,则$N \triangleleft M, M/N \triangleleft G/N$,且$(G/N)/(M/N) \cong G/M$;

11. 设 G 是群, $N \triangleleft G$, 且 $H \leq G$, 则 $(H \cap N) \triangleleft H$, $N \triangleleft NH \leq G$, 并且 $NH/N \cong H/(H \cap N)$;

6 置换群

1. 置换: 非空集合 X 到自身的一一映射, 叫做 X 上的一个置换;

   (a) 若 $X = \{a_1, ..., a_n\}$ 是有限集合, 则它上面的置换 σ 通常可表示为 $\sigma = \begin{pmatrix} a_1 & ... & a_n \\ \sigma(a_1) & ... & \sigma(a_n) \end{pmatrix}$;

   (b) 置换的乘积: 置换的乘积定义为映射的复合 $(\sigma\tau)(a_i) = \sigma(\tau(a_i)), a_i \in X$;

   (c) 置换 σ 的逆: σ 作为 X 到 X 的映射的逆映射;

2. 对称群与置换群: 集合 X 上所有置换构成的集合记为 S_X, 称为集合 X 上对称群, 它的每个子群均称为集合 X 上的置换群, 它关于映射复合运算构成群;

   (a) n 元集合上的对称群 S_n, 其阶为 $|S_n| = n!$;

3. 固定与移动: 设 $X = \{1, ..., n\}, i \in X$ 和 $\sigma \in S_n$. 若 $\sigma(i) = i$ 称为 σ 固定 i, 若 $\sigma(i) \neq i$ 称为 σ 移动 i;

4. 轮换: 设 σ 固定 X 中的 $X/\{i_1, i_2, ..., i_r\}$, 若 $\sigma(i_{r-1}) = i_r, \sigma(i_r) = i_1$, 则称 σ 为一个长为 r 的轮换, 记为 $\sigma = (i_1 i_2 ... i_r)$;

   (a) 对换: 长为 2 的轮换仅交换 X 中的一对元素, 通常称为对换;

   (b) 不相交: 若 X 中的元素被一个置换 σ 移动, 必然被另一个 τ 固定, 则称两个置换不相交;

      i. 当两个置换 σ, τ 不相交时, 必然有 $\sigma\tau = \tau\sigma$;

      ii. 每个非恒等置换 $\sigma \in S_n$ 是长度大于 1 的不相交轮换的乘积;

   (c) 每个置换 $\sigma \in S_n$ 都可以写成对换的乘积;

i. 置换分解成对换乘积的方式不唯一, 但分解成对换乘积时, 对换个数的奇偶性不变;

A. 奇 (偶) 置换: 如果置换 $\sigma \in S_n$ 可以写成奇 (偶) 数个对换的乘积;

B. n 次交错群: 有所有的偶置换构成的群 $A_n := Kerf = \{偶置换\} \lhd S_n, f : S_n \to \{1, -1\}$ 被称为 n 次交错群, 有 $[S_n : A_n] = 2, |A_n| = \frac{n!}{2}(n \geq 2)$;

(d) 当 $n \geq 2$ 时, $\{(12), (13), ..., (1n)\}$ 是 S_n 的一个生成元系;

(e) 当 $n \geq 3$ 时, 全体长为 3 的轮换形成 A_n 的一个生成元系;

5. 置换的型: 置换 $\sigma \in S_n$, 将 σ 表示成不相交的轮换之积, 如果其中长为 r 的轮换共有 λ_r 个 $(1 \leq r \leq n)$, 则称 σ 的型为 $1^{\lambda_1}2^{\lambda_2}...r^{\lambda_r}$;

(a) 对称群 S_n 中两个置换共轭的充要条件是它们有相同的型;

(b) 单群: 只有平凡正规子群的群, 称为单群;

i. 元素个数大于 1 的交换群是单群 $\Leftrightarrow$ 它是素数阶 (循环) 群;

ii. 当 $n \geq 5$ 时, 交错群 A_n 是单群;

7 群在集合上的作用

1. 置换表示: 群 G 到 S_X 的同态 $f : G \to S_X$;

(a) 忠实表示: 若 f 为单射, 则称其为忠实表示;

(b) 等价关系: 设 $\rho : G \to S_X$ 是置换表示, 定义 X 上的关系"$\sim$"为 $\forall a, b \in X, a \sim b \Leftrightarrow \exists g \in G, s.t. ga = b$, 则 $\sim$ 为等价关系;

i. 等价类: 对任意 $a \in X$, a 所在的等价类 $[a] = Ga = \{ga | g \in G\}$;

(c) 轨道: 每个等价类叫做一个 $G-$ 轨道, 或简称轨道;

i. 拆分: 集合 X 的拆分 $X = \cup_{a \in I}[a]$(不交并)$= \cup_{a \in I}Ga$(不交并);

ii. 传递: 若 G 在 X 上的作用只有一个轨道, 则称 G 在 X 上是传递的;

(d) Cayley 定理: 每个群均同构于某个置换群;

2. 固定子群: 设群 G 作用在集合 X 上, 对 $\forall a \in X$, 记 $G_a = \{g \in G | ga = a\} (\leq G)$ 称为元素 a 的固定子群;

   (a) 轨道公式: 设 G 是有限群, G 作用于集合 X, $a \in X$, 则 $|G| = |G_a||[a]|$;

      i. 设 G 是 $2n$ 阶群, $2 \nmid n$, 则 G 必有指数为 2 的正规子群;

      ii. 设 G 是有限群, $|G| \geq 6$ 且 $|G| = 2 (\mathrm{mod}\ 4)$, 则 G 不是单群;

      iii. 设 G 是有限群, p 是 $|G|$ 的最小素因子, 如果 $N \leq G, [G : N] = p$, 则 $N \triangleleft G$;

3. 线性表示: $f : G \to GL(V)$;

4. $H \leq G \Rightarrow |H||G|$. 反之不成立, 即 $d||G|$, 群 G 未必有 d 阶子群;

5. Sylow 定理: 设 $p^r||G|$, 其中 p 为素数, 以 $N(n)$ 表示 G 中 n 阶子群的个数, 则 $N(p^r) = 1 (\mathrm{mod}\ p)$. 特别地, 若 $p^r||G|$, 则 G 至少存在一个 p^r 阶子群;

   (a) Sylow$-p$ 子群: 设 G 为 $p^r n$ 阶群, 其中 p 为素数, $r \geq 1, p \nmid n$, 则 G 的每个 p^r 阶子群均叫做 G 的西罗 $p-$ 子群;

   (b) 设 G 为有限群, 则:

      i. 对 $|G|$ 的每个素因子 p, 均存在 G 的西罗 $p-$ 子群;

      ii. G 的西罗 $p-$ 子群彼此共轭;

      iii. G 的西罗 $p-$ 子群的个数恒等于 $1 (\mathrm{mod}\ p)$;

      iv. 设 P 为 G 的一个西罗 $p-$ 子群, 则 G 的西罗 $p-$ 子群的个数为 $[G : N_G(P)]$;

   (c) 设素数 $p||G|$, 则 G 的每个 p 方幂阶的子群 B 均包含在 G 的某个西罗 $p-$ 子群内;

   (d) 设 P 是 G 的西罗 $p-$ 子群, $A \leq G$, 且 $N_G(P) \leq A$, 则 $N_G(A) = A$;

   (e) Fratini 定理: $M \triangleleft G$, P 为 M 的西罗 $p-$ 子群, 则 $G = MN_G(P)$;

6. 一些结论:

   (a) 设 p 和 q 是两个素数, 则 pq 阶群 G 不是单群;

   (b) 设 p 和 q 是两个素数, 则 p^2q 阶群 G 不是单群;

8 环

1. 环: 集合 R 及 R 上的两个二元运算组成的代数结构 $(R,+,\cdot)$, 满足:
   (a) 加法交换群及零元素: $(R,+)$ 是 Abel 群, 单位元记为 0_R(或 0), 称为环 R 的零元素;
   (b) 乘法结合律: $(R,\cdot)$ 是半群;
   (c) 分配律: $\forall a,b,c\in R$, 有 $\begin{cases} a(b+c)=ab+ac \\ (b+c)a=ba+ca \end{cases}$;
2. 交换环: 满足 $\forall a,b\in R$, 有 $ab=ba$ 的环;
3. 含幺环: R 是环, 且 $\exists 1_R\in R, s.t. \forall a\in R$, 有 $1_R\cdot a=a\cdot 1_R=a$. 其中 1_R 称为环 R 的幺元素, 简记为 1;
4. 环中的零元素唯一, 幺元素 (若有) 也唯一;
5. 记号: n 个 a 相加记为 na, n 个 a 相乘记为 a^n;
6. 环的性质: 设 $(R,+,\cdot)$ 为环, 则
   (a) $\forall a\in R, 0a=a0=0$;
   (b) $\forall a,b\in R, (-a)b=a(-b)=-(ab), (-a)(-b)=ab$;
   (c) $a_i,b_j\in R, i=1,...,n, j=1,...,m, \left(\sum\limits_{i=1}^{n}a_i\right)\left(\sum\limits_{j=1}^{m}b_j\right)=\sum\limits_{i=1}^{n}\sum\limits_{j=1}^{m}a_ib_j$;
   (d) $n\in\mathbb{Z}, a,b\in R$, 则 $(na)b=a(nb)=n(ab)$;
7. 零因子: R 是环, 且 $0\neq a\in R$,
   (a) 左零因子: 若 $\exists 0\neq b\in R, s.t. ab=0$, 则称 a 为左零因子;
   (b) 右零因子: 同理;
   (c) 零因子: 若 a 同时是左零因子和右零因子, 则称 a 为零因子;
8. 逆元: R 为含幺环, $a\in R$,
   (a) 左逆: 若 $\exists c\in R, s.t. ca=1$, 则称 a 左可逆, 并称 c 为 a 的左逆;
   (b) 右逆: 同理;
9. 可逆元: 若 a 左可逆且右可逆, 则有唯一逆元 a^{-1}, 称 a 为可逆元;

(a) 单位: 环 R 中的可逆元称为 R 中的单位;

10. 单位群: 含幺环中的全体单位形成乘法群, 称为 R 的单位群, 记作 $U(R)$;
11. 整环: 含幺交换环 R 中, $0 \neq 1$, 且 R 中没有零因子, 则称 R 为整环;
12. 体 (除环): 含幺环 R 中, $0 \neq 1$, 且 $U(R) = R\backslash\{0\}$, 则称 R 为体;

    (a) 含幺环 R 是体 $\Leftrightarrow (R\backslash\{0\}, \cdot)$ 成群;

13. 域: R 是体, 且 R 为交换环, 则称 R 为域;

    (a) 域是整环;

14. 整环, 体, 域中至少包含两个元素 0 和 1;
15. 子环: $(R, +, \cdot)$ 是环, $S \subseteq R$, 若 $(S, +, \cdot)$ 构成环, 则称 S 为 R 的子环;

    (a) 子体 (域): 若 $(S, +, \cdot)$ 是体 (域), 则称 S 为 R 的子体 (域);

    (b) 若 $S \subseteq R$ 是子环, 则 $\forall a, b \in S$, 有 $a - b, ab \in S$;

    (c) 平凡子环: $\{0\}, R$;

16. 设 S 是环 R 的子环, 加法商群 R/S 对乘法 $\overline{a} \cdot \overline{b} = \overline{ab}$ 成环的充要条件: $\forall r \in R, a \in S$, 有 $ra, ar \in S$;
17. 理想: 环 R 的子环 S 若满足: $\forall r \in R, a \in S$, 有 $ra, ar \in S$, 则称 S 为环 R 的理想;

    (a) 理想的判定: $S \subseteq R$ 是理想, 当且仅当

        i. $\forall a, b \in S, a - b \in S$;

        ii. $\forall r \in R, a \in S, ra, ar \in S$;

    (b) 平凡理想: $(0), R$;

18. 商环: 设 A 是环 R 的理想, 则 R/A 对自然定义的加法和乘法 $(\overline{a} \cdot \overline{b} = \overline{ab})$ 成环, 称之为 R 对于理想 A 的商环;
19. 单环: 只有平凡理想的环;
20. 一些结论:

    (a) $I \subseteq R$ 为理想, 若 $1_R \in I$, 则 $I = R$. 即体和域为单环;

(b) 整数环 $\mathbb{Z}$ 的全部子环: $m\mathbb{Z}, m \geq 0$. 它们也是 $\mathbb{Z}$ 的全部理想;

(c) $A_i, i \in I$ 为 R 的理想, 则 $\bigcap\limits_{i\in I} A_i$ 也是 R 的理想;

21. 集合 X 生成的理想: 子集 $X \subseteq R$, R 中包含 X 的最小理想称为由集合 X 生成的理想, 记为 (X);

22. 主理想: 由一个元素 $x \in R$ 生成的理想 (x) 被称为环 R 的主理想;

(a) 主理想整环 (PID): 若 R 是整环, 且 R 的每个理想都是主理想 $(x) = xR$, 则 R 被称为主理想整环;

9 环的同态

1. 环的同态: R, S 为环, 映射 $f : R \to S$ 满足 $\forall a, b \in R, f(a + b) = f(a) + f(b), f(ab) = f(a)f(b)$, 则称 f 为 R 到 S 的同态;

(a) 环同态 f 亦为加法群同态, 故 $f(0_R) = 0_S, f(-a) = -f(a)$;

(b) 单 (满) 同态: f 是同态, 且 f 为单 (满) 射, 则称 f 为单 (满) 同态;

i. 若 f 是满同态, 且 R, S 均有幺元, 则 $f(1_R) = 1_S$, 且 $a \in U(R) \Rightarrow f(a) \in U(S)$;

(c) 设 $f : R \to S$ 是环的同态:

i. 同态的像: 集合 $Imf = f(R) = \{f(r)|r \in R\}$, 同态的像是 S 的子环;

ii. 同态的核: 集合 $Kerf = f^{-1}(0_S) = \{r \in R|f(r) = 0_S\}$, 同态的核是 R 的理想;

2. 同构: 若 f 是环同态, 且 f 是一一映射, 则称 f 为环的同构;

(a) 若 f 是同构, 则 f^{-1} 也是同构;

3. 自同态 (同构): 同态 (同构)$f : R \to R$ 被称为自同态 (同构);

(a) 环的所有自同构 ($Aut(R)$) 关于复合运算构成群;

4. 嵌入: 若 $f : R \to S$ 是环的单同态, 则称 f 为环 R 到 S 的嵌入;

5. 第一同构定理: 设 $f : R \to S$ 是环的同态, 则 $Kerf$ 是 R 的理想, 并且 $\bar{f} : R/Kerf \to S(\bar{r} \to f(r))$ 是环的单同态 (嵌入);

(a) 特别的: $\bar{f}: R/Kerf \tilde{\to} Imf$;

6. 第二同构定理: 设 I, J 是环 R 的理想, 则 $I/(I \cap J) \tilde{=} (I+J)/J$;
7. 第三同构定理: 设 I, J 是环 R 的理想, 若 $I \subset J$, 则 $\frac{R/I}{J/I} \tilde{=} R/J$;
8. 若 I 是环 R 的理想, 则 $f: \{I \subseteq J \subseteq R, J是理想\} \to \{R/I的所有理想\}(J \to J/I)$ 是一一映射;
9. 环的特征: 设 R 是环, 若存在 $m \in \mathbb{Z}_+$, 使得 $\forall r \in R$, 有 $mr = 0$, 则称满足此条件的最小正整数 m 为 R 的特征, 记为 $charR$;
   (a) 若不存在这样的正整数, 则称 $charR = 0$;
10. 素子环: 含幺环 R 中同构于 $\mathbb{Z}$ 或 $\mathbb{Z}_m$ 的子环被称为 R 的素子环;
11. 设 R 是交换环, $charR = p$ 是素数, 则对 $\forall x, y \in R$, 有 $(x+y)^p = x^p + y^p$;
12. 设 R 是交换环, $charR = p$ 是素数, 则 $f: R \to R(r \to r^p)$ 是环的自同态;
13. 素理想: 若 R 的理想 P 满足下面的性质, 则称 P 为 R 的素理想:
    (a) $P \neq R$;
    (b) A, B 是 R 的任意两个理想, 若 $AB \subseteq P$, 则 $A \subseteq P$ 或 $B \subseteq P$;
14. 极大理想: 若 R 的理想 M 满足下面的性质, 则称 M 为 R 的极大理想:
    (a) $M \neq R$;
    (b) $\forall N \subseteq R$ 是 R 的理想, 若 $M \subseteq N \subseteq R$, 则 $N = M$ 或 $N = R$;
15. 设 R 是含幺交换环, P 是 R 的理想且 $P \neq R$, 则下面条件相互等价:
    (a) P 是 R 的素理想;
    (b) $\forall a, b \in R$, 若 $ab \in P$, 则 $a \in P$ 或 $b \in P$;
    (c) R/P 为整环;
16. 设 R 是含幺交换环, 则 R 是整环 $\Leftrightarrow (0)$ 为素理想;
17. 设 R 是含幺交换环, $M \subseteq R$ 是理想, 则 M 为 R 的极大理想 $\Leftrightarrow R/M$ 为域;

(a) 特别的: 含幺交换环 R 为域的充要条件是 (0) 为 R 的极大理想;

18. 含幺交换环的极大理想是素理想;

10 交换环中的因子分解

1. 基本概念: 设 R 是交换环, $a, b \in R$:

   (a) 整除: $a \neq 0$, 若 $\exists x \in R$, 使得 $ax = b$, 则称 a 整除 b(或 b 被 a 整除), 记为 $a|b$;

      i. 若 $\nexists x \in R$, 使得 $ax = b$ 则称 a 不能整除 b(或 b 不能被 a 整除), 记作 $a \nmid b$;

   (b) 因子: 若 $a|b$, 则称 a 为 b 的因子;

   (c) 倍元: 若 $a|b$, 则称 b 为 a 的倍元;

   (d) 相伴: 若 $a, b \neq 0$, 且有 $a|b$ 和 $b|a$, 则称元素 a 与 b 相伴, 记作 $a \sim b$($R\backslash\{0\}$ 上的等价关系);

2. 基本概念: 设 R 是含幺交换环, $a, b \in R$:

   (a) 真因子: 若 $a = bc, b, c \neq 0$ 且 $b, c \notin U(R)$, 则称 b 和 c 为 a 的真因子;

   (b) 不可约元: 若 $0 \neq a \in R, a \notin U(R)$, 且 a 没有真因子, 则称 a 为不可约元;

   (c) 素元: 设 $0 \neq p \in R, p \notin U(R)$, 且 $\forall a, b \in R$, 若 $p|(ab)$, 则 $p|a$ 或 $p|b$;

      i. 在整数环 $\mathbb{Z}$ 中, 不可约元与素元一致;

3. 设 R 是含幺交换环, $a, b, u \in R\backslash\{0\}$, $U(R)$ 为 R 的单位群, 则:

   (a) $a|b \Leftrightarrow (b) \subseteq (a)$; $a \sim b \Leftrightarrow (a) = (b)$;

   (b) $u \in U(R) \Leftrightarrow u \sim 1 \Leftrightarrow (u) = R \Leftrightarrow u|r, \forall r \in R$;

   (c) $a = bu, u \in U(R) \Rightarrow a \sim b$;

      i. 若 R 是整环, 则逆命题也成立;

   (d) R 是整环, a 为 b 的真因子 $\Leftrightarrow a \notin U(R), (b) \subseteq (a)$ 但 $(b) \neq (a)$;

4. 设 R 是整环, $p, c \in R\backslash\{0\}$, $S = \{(a) | a \in R, a \neq 0, a \notin U(R)\}$, 则:

(a) p 是素元 $\Leftrightarrow(p)$ 是非零素理想;

(b) c 是不可约元 $\Leftrightarrow(c)$ 为 S 中的极大元;

(c) R 中的素元必是不可约元;

(d) 若 R 是主理想整环, 则不可约元必是素元;

5. 唯一因子分解整环 (UFD): 满足下面条件的整环 R 被称为唯一因子分解整环:

   (a) 分解存在性: 每个非零非单位的元 $a \in R$ 均可写成 $a = c_1c_2...c_n$, 其中 $c_i, i = 1, ..., n$ 为不可约元;

   (b) 分解的唯一性: 若 $a = c_1c_2...c_n = d_1d_2...d_m$, 其中 c_i, d_j 均为 R 中的不可约元, 则 $n = m$, 并且存在集合 $\{1, 2, ..., n\}$ 的一个置换 σ, 使得 $c_i \sim d_{\sigma(i)}, i = 1, 2, ..., n$;

6. 设 R 是唯一分解整环, 则 R 有如下等价性质:

   (a) R 中不存在无限的元素序列 $a_1, a_2, ..., a_n, ...$, 使得每个 a_{i+1} 都是 a_i 的真因子;

   (b) 对于 R 中每个无限序列 $a_1, a_2, ..., a_n, ...$, 如果 $a_{i+1}|a_i (i = 1, 2, ...)$ 均成立, 则必有正整数 N, 使得 $a_N \sim a_{N+1} \sim ...$;

7. 若 R 为唯一分解整环, 则 R 中的不可约元必为素元;

8. 最大公因子: 设 R 是整环, $a, b \in R\backslash\{0\}$, d 若满足下面的条件, 则称其为 a 和 b 的最大公因子, 记作 (a, b):

   (a) $d|a, d|b$;

   (b) $\forall d'$ 满足 $d'|a, d'|b$, 有 $d'|d$;

   (c) 注意: 元素 a 和 b 的最大公因子不唯一, 因为与 (a, b) 相伴的元素均是 a 和 b 的最大公因子, 且是全部最大公因子;

9. 互素: 若 $(a, b) \sim 1$, 则称 a 与 b 互素;

10. 设 R 为整环, $a, b, c \in R\backslash\{0\}$, 则:

    (a) $c(a, b) \sim (ca, cb)$;

    (b) $(a, b) \sim 1, (a, c) \sim 1$, 则 $(a, bc) \sim 1$;

11. 设 R 为唯一分解整环, 则 R 中的任意两个非零元素 a, b 都有最大公因子;

12. 每个主理想整环 (PID) 都是唯一分解整环 (UFD);

13. 欧式整环 (ED): 设 $\mathbb{N}$ 是非负整数集合, 若整环 R 到 $\mathbb{N}$ 能定义一个映射 $\varphi : R \to \mathbb{N}$, 满足下面的性质, 则称该整环 R 为欧式整环:

    (a) $\varphi(x) = 0 \Leftrightarrow x = 0$;

    (b) $\forall a, b \in R, b \neq 0$, 均存在 $q, r \in R$, 使得 $a = bq + r$ 且 $\varphi(r) < \varphi(b)$;

14. 每个欧式整环 (ED) 都是主理想整环 (PID), 从而也是唯一分解整环 (UFD);

11 域扩张

1. 域扩张: 设 $\mathbb{F}$ 是域, 若 $\mathbb{F}$ 是域 $\mathbb{E}$ 的子域, 则称 $\mathbb{E}$ 为 $\mathbb{F}$ 的域扩张 (或简称扩张), 记为 $\mathbb{E}/\mathbb{F}$;

    (a) 此时, $\mathbb{E}$ 为 $\mathbb{F}$ 上的向量空间;

    (b) 次数: $\dim_{\mathbb{F}} \mathbb{E}$ 称为 $\mathbb{E}$ 关于 $\mathbb{F}$ 的次数, 记为 $[\mathbb{E} : \mathbb{F}]$;

    (c) 有限扩张: $[\mathbb{E} : \mathbb{F}] < \infty$. 反之为无限扩张;

2. 代数元: 设 $\mathbb{E}/\mathbb{F}$ 是域的扩张, $\alpha \in \mathbb{E}$, 若存在不全为零的 $a_0, a_1, ..., a_n \in \mathbb{F}$, 使得 $a_0 + a_1\alpha + ... + a_n\alpha^n = 0$, 则称 α 为 $\mathbb{F}$ 上的代数元;

    (a) 超越元: 不是代数元的, 称其为超越元;

    (b) 代数数: $\mathbb{C}/\mathbb{Q}$ 上的代数元;

    (c) 超越数: $\mathbb{C}/\mathbb{Q}$ 上的超越元;

3. 代数扩张: 设 $\mathbb{E}/\mathbb{F}$ 是域的扩张, 如 $\mathbb{E}$ 中的元均为 $\mathbb{F}$ 上的代数元, 则称 $\mathbb{E}$ 为 $\mathbb{F}$ 的代数扩张;

    (a) 超越扩张: 不是代数扩张的, 称为超越扩张;

4. 最小多项式: 设 $\mathbb{E}/\mathbb{F}$ 是域的扩张, $\alpha \in \mathbb{E}$ 是 $\mathbb{F}$ 上的代数元, 则有环同态 $\varphi : \mathbb{F}[x] \to \mathbb{E}(f(x) \to f(\alpha))$. 存在 $p(x) \in \mathbb{F}[x]$, 使得 $Ker\varphi = (p(x))$. 若 $p(x)$ 首项系数为 1, 则 $p(x)$ 唯一确定, 这样的 $p(x)$ 被称为 α 的极小多项式;

(a) $p(\alpha)=0$;

(b) $p(x)$ 是 $\mathbb{F}[x]$ 中的不可约元, 和素元;

(c) 若 $f(\alpha)=0$, 则 $p(x)|f(x)$;

5. 有限扩张是代数扩张;

6. 设 $\mathbb{E}/\mathbb{F}, \mathbb{F}/\mathbb{K}$ 是域的扩张, 则:

   (a) 望远镜公式: $[\mathbb{E}:\mathbb{K}]=[\mathbb{E}:\mathbb{F}][\mathbb{F}:\mathbb{K}]$;

   (b) $\mathbb{E}/\mathbb{K}$ 为有限扩张 $\Leftrightarrow \mathbb{E}/\mathbb{F}, \mathbb{F}/\mathbb{K}$ 均是有限扩张;

7. 单扩张: 设 $\mathbb{E}/\mathbb{F}$ 是晕的扩张, $\alpha\in\mathbb{E}$, 用 $\mathbb{F}(\alpha)$ 表示 $\mathbb{E}$ 中含 $\mathbb{F}$ 及 α 的最小子域, 称其为单扩张. 有 $\mathbb{F}(\alpha)=\{f(\alpha)/g(\alpha)|f(x),g(x)\in\mathbb{F}[x],g(\alpha)\neq 0\}$;

8. 设 $\mathbb{E}/\mathbb{F}$ 是域的扩张, $\alpha\in\mathbb{E}$ 是 $\mathbb{F}$ 上的代数元, 则 $\mathbb{F}(\alpha)=\mathbb{F}[\alpha]$, 且 $[\mathbb{F}(\alpha):\mathbb{F}]=\alpha$ 的极小多项式的次数;

9. 有限生成扩张: 设 $\mathbb{E}/\mathbb{F}$ 是域的扩张, 若存在有限个元 $\alpha_1,\alpha_2,...,\alpha_n\in\mathbb{E}$, 使得 $\mathbb{E}=\mathbb{F}(\alpha_1,\alpha_2,...,\alpha_n)$, 则称 $\mathbb{E}$ 是 $\mathbb{F}$ 的有限生成扩张;

10. 若 $\mathbb{E}=\mathbb{F}(\alpha_1,...,\alpha_n)$, 且 $\alpha_1,...,\alpha_n$ 为 $\mathbb{F}$ 上的代数元, 则 $\mathbb{E}/\mathbb{F}$ 是有限扩张;

11. 若 $\mathbb{E}/\mathbb{F}$ 是有限扩张, 则 $\mathbb{E}/\mathbb{F}$ 是有限生成扩张;

12. 设 $\mathbb{F}/\mathbb{K}$ 是代数扩张, u 是 $\mathbb{F}$ 上的代数元, 则 u 在 $\mathbb{K}$ 上也是代数元;

13. 设 $\mathbb{E}/\mathbb{F}, \mathbb{F}/\mathbb{K}$ 是域的扩张, 则 $\mathbb{E}/\mathbb{K}$ 是代数扩张 $\Leftrightarrow \mathbb{E}/\mathbb{F}, \mathbb{F}/\mathbb{K}$ 均是代数扩张;

14. 代数封闭域: 对域 $\mathbb{K}$, 若满足 u 是 $\mathbb{K}$ 的某个扩域中的元素, 并且 u 是 $\mathbb{K}$ 上的代数元, 则有 $u\in\mathbb{K}$, 那么称 $\mathbb{K}$ 为代数封闭域;

   (a) 代数闭包: 设 $\mathbb{F}/\mathbb{K}$ 为域的扩张, 若 $\mathbb{F}$ 为代数封闭域, 且 $\mathbb{F}/\mathbb{K}$ 是代数扩张, 则称 $\mathbb{F}$ 是 $\mathbb{K}$ 的代数闭包;