第八次习题课

方法提要、习题讲解和内容扩充

助教：邓先涛

2023 年 11 月 6 日

重点知识提要

重点知识提要

- 初等因子与不变因子：$M=\oplus_{i=1}^{s}\oplus_{j_i=1}^{r_i}N_{ij_i}$ 为第一标准分解；$M=\oplus_{k=1}^{l}M_k$ 为第二标准分解.

$$\begin{matrix} \mathrm{Ann}(N_{11}) & \mathrm{Ann}(N_{12}) & \cdots & \mathrm{Ann}(N_{1r_1}) \\ \mathrm{Ann}(N_{21}) & \mathrm{Ann}(N_{22}) & \cdots & \mathrm{Ann}(N_{2r_2}) \\ \vdots & \vdots & \cdots & \vdots \\ \mathrm{Ann}(N_{s1}) & \mathrm{Ann}(N_{12}) & \cdots & \mathrm{Ann}(N_{sr_s}) \end{matrix} \quad \mathrm{Ann}(M_1),\mathrm{Ann}(M_2),\cdots,\mathrm{Ann}(M_l).$$

- 主理想整环上有限生成模结构应用：有限 Abel 群的结构定理；有理标准型；Jordan 标准型.
- 域扩张的基本概念：扩张，单扩张，代数扩张.

第六章习题讲解

第六章第 15 题

试定出全部阶为 392 的交换群互不同构的类型.

有限交换群结构定理

思维拓展

试着分类阶为 12 的交换群和阶为 12 的群，以此观察有限生成模结构定理在有限 Able 群分类中的便利. 并由此思考什么叫做完全不变量.

证明

- 注意到 $392 = 2^3 \times 7^2$，初等因子分解

$$(2^3, 7^2), \qquad (2^3, 7, 7)$$
$$(2^2, 2, 7^2), \qquad (2^2, 2, 7, 7)$$
$$(2, 2, 2, 7^2), \qquad (2, 2, 2, 7, 7)$$

- 不变因子分解

$$(2^3 \times 7^2), \qquad (2^3 \times 7, 7)$$
$$(2^2 \times 7^2, 2), \qquad (2^2 \times 7, 2 \times 7)$$
$$(2 \times 7^2, 2, 2), \qquad (2 \times 7, 2 \times 7, 2)$$

一般情形的结果

设 $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$，试分析 n 阶交换群互不同构的类型的数目.

有限交换群结构定理和简单的组合

思维拓展

交换群是简单的，你能否给出 $n = p_1 p_2 \cdots p_r$ 阶群是交换群的等价条件？

证明

- 对于不同的素数 p，交换群不同的 p 子群相互独立.
- p^e 阶交换群的互不同构的类型为 e 的整数分拆数 $h(e)$. 如 $4 = 4 + 0 = 3 + 1 = 2 + 2 = 2 + 1 + 1 = 1 + 1 + 1 + 1$
- 所有数目就是 $h(e_1) \cdot h(e_2) \cdots h(e_r)$.

第六章第 16 题

不变因子为 $(3,3^2,3^2,3^5,3^7)$ 的交换群中 9 阶子群的个数.

有限交换群结构定理和简单的组合

证明

- 将题述条件下的群 G 写作
  $\mathbb{Z}/(3)\oplus\mathbb{Z}/(9)\oplus\mathbb{Z}/(9)\oplus\mathbb{Z}/(3^5)\oplus\mathbb{Z}/(3^7)$
- 阶为 9 的子群有两种类型：$\mathbb{Z}/(9)$ 和 $\mathbb{Z}/(3)\oplus\mathbb{Z}/(3)$.

- 9 阶循环子群个数：G 中每一个 9 阶元均可以生成一个 9 阶子群. G 中每一个 9 阶循环子群中存在 6 个 9 阶元.
- G 中 9 阶元个数 $=3\times 9^4-3^5=19440$.
- G 中 9 阶循环子群个数 $=19440/6=3240$.
- $\mathbb{Z}/(3)\times\mathbb{Z}/(3)$ 型群个数：G 中该类型群均由 2 个 3 阶循环群直和生成. G 中该类型群可以写成 6 种不同的直和方式.
- G 中 3 阶子群数量 $=(3^5-1)/2=121$.
- G 中 3×3 型子群数量 $=C_{121}^2/6=1210$.

例题补充

设 p 为素数，$G=\oplus_{i=1}^{r}\mathbb{Z}/(p)(r\geq 2)$，计算 G 中 p 阶子群和 p^2 阶子群的个数.

有限交换群结构定理和简单的组合

思维拓展

设 p 为素数，$G=\oplus_{i=1}^{r}\mathbb{Z}/(p^{e_i})(r\geq 2)$ 中 p^2 阶子群的个数？

证明

- p 阶子群个数：$A=(p^r-1)/(p-1)$
- p^2 阶循环子群个数：0
- $p\times p$ 型群中 p 阶子群个数：$\frac{p^2-1}{p-1}=p+1$
- $p\times p$ 型子群的个数：

$$\frac{C_A^2}{C_{p+1}^2}=\frac{(p^r-1)(p^r-p)}{(p+1)p(p-1)^2}$$

第六章第 21 题

设 F 是特征 0 的域，$A \in M_n(F)$，证明：A 幂零当且仅当 $\mathrm{tr}(A^i) = 0$，$\forall i = 1, 2, \cdots, n$.

代数闭域上的矩阵的 Jordan 标准型

思维拓展

该方法在特征 p 的域上是否有效，本质原因是什么？如何刻画特征 p 域上的幂零矩阵. 如何正确使用范德蒙矩阵解决该问题.

证明

- A 作 Jordan 分解，$A = \mathrm{diag}(C_1, \cdots, C_m)$. 这里 C_i 是标准 Jordan 矩阵，且可设后 $m - t$ 个特征值均为 0.
- 若 A 幂零，则 A^i 的特征值均为 0.
- 若 $\mathrm{tr}(A^i) = 0$，反设 A 非幂零，则 $A = \mathrm{diag}(B, C)$，$B = \mathrm{diag}(C_1, \cdots, C_t)$.
- $\mathrm{tr}(B^i) = 0$，考虑 B 的极小多项式 $m(x)$.
- $\mathrm{tr}(m(B)) = 0$ 与 $m(0) \neq 0$ 矛盾.

补充例题

设 $A \in M_5(\mathbb{C})$ 极小多项式为 $(\lambda-1)(\lambda-2)^2$，则 $\mathbb{C}^5$ 在矩阵 A 作用下作为 $\mathbb{C}[\lambda]$ 模的初等因子和不变因子有哪些可能？

初等因子与不变因子

思维拓展

设 $A \in M_5(\mathbb{C})$ 特征多项式为 $(\lambda-1)^3(\lambda-2)^2$，则 $\mathbb{C}^5$ 在矩阵 A 作用下作为 $\mathbb{C}[\lambda]$ 模的初等因子和不变因子有哪些可能？

证明

- 初等因子可能
- $\lambda-1, \lambda-1, \lambda-1, \quad (\lambda-2)^2$
- $\lambda-1, \lambda-1, \quad \lambda-2, (\lambda-2)^2$
- $\lambda-1, \quad \lambda-2, \lambda-2, (\lambda-2)^2$
- $\lambda-1, \quad (\lambda-2)^2, (\lambda-2)^2$
- 不变因子类似

第七章习题讲解

第七章第 3 题第 1 问第 2 问

设 L, M 为域 K 的子域，LM 为 K 中包含 L 和 M 的子域的交，设 $L \cap M = F$，$L = F(S)$，$M = F(T)$，证明：$LM = F(S \cup T) = M(S)$.

域中添加元素生成大域

思维拓展

两个域的交还是域？任意多个域的交还是域？

证明

- 注意到 $F(T), F(S) \subset F(S \cup T)$，因此 $LM \subset F(S \cup T)$.
- $S \subset L \subset LM$，$T \subset M \subset LM$，因此 $F(S \cup T) \subset LM$.
- 同理证明 $M(S) = F(S \cup T)$.

第七章第 3 题第 3 问

设 L, M 为域 K 的子域，LM 为 K 中包含 L 和 M 的子域的交，则 $L \cup M \subset LM$. 请给出 $LM = L \cup M$ 的等价条件.

域扩张中的基本运算

思维拓展

有没有更好的方法刻画 LM，特别的，定义集合 $L \cdot M = \{\sum_{i=1}^{n} a_i \cdot b_i | a_i \in L, b_i \in M\}$，$LM$ 与 $L \cdot M$ 之间有多大差别？何时相等？

证明

- 注意到 $M, L \subset LM$，因此 $L \cup M \subset LM$.
- 断言 $LM = L \cup M$ 当且仅当 L 与 M 有包含关系.
- 后推前：显然
- 前推后：若不然，则存在 $a \in M \setminus L$ 和 $b \in L \setminus M$. 验证 $ab \in LM$ 但 $ab \notin L \cup M$.

第七章第 6 题第 1 问

求扩域 $\mathbb{Q}(\sqrt{2},\sqrt{3})$ 和 $\mathbb{Q}(\sqrt{3},\sqrt{-1},\omega)$ 作为 $\mathbb{Q}$ 线性空间的一组基，其中 $\omega=\frac{-1+\sqrt{-3}}{2}$.

扩域中的元素表达

证明

- 将 $\mathbb{Q}(\sqrt{2},\sqrt{3})$ 看作 $\mathbb{Q}(\sqrt{2})(\sqrt{3})$，其中元素可以写作 $x+y\sqrt{3}$，这里 $x,y\in\mathbb{Q}(\sqrt{2})$.
- $\mathbb{Q}(\sqrt{2})$ 中的可以写作 $a+b\sqrt{2}$，其中 $a,b\in\mathbb{Q}$. $\mathbb{Q}(\sqrt{2},\sqrt{3})$ 中的元素写作 $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$.
- 验证 $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$ 是 $\mathbb{Q}$ 线性无关. 否则存在整数 a,b,c,d 使得 $a+b\sqrt{3}=c\sqrt{2}+d\sqrt{6}$ 矛盾.
- 第二个同样方法，只需要注意 $\mathbb{Q}(\sqrt{3},\sqrt{-1},\omega)=\mathbb{Q}(\sqrt{3},\sqrt{-1})$.

思维拓展

扩域的基并不容易找寻，如找到 $\mathbb{Q}\left(\sqrt{\sqrt{5}+\sqrt{3}},\sqrt{\sqrt{5}-\sqrt{3}}\right)$ 和 $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$ 的 $\mathbb{Q}$ 基，并证明.

彭老师课件 14 页 12 题

设 d_1 和 d_2 是两个无平方因子整数，证明 $\mathbb{Q}(\sqrt{d_1})$ 与 $\mathbb{Q}(\sqrt{d_2})$ 之间存在域同构当且仅当 $d_1 = d_2$.

扩域中的元素表达

证明

- 后推前显然，下证前推后，设 $\phi : \mathbb{Q}(\sqrt{d_1}) \to \mathbb{Q}(\sqrt{d_2})$ 为域同构. 令 $\phi(\sqrt{d_1}) = a + b\sqrt{d_2}$.
- 注意到 $\phi(s) = s, \forall s \in \mathbb{Q}$，立刻得到 $d_1 = (a + b\sqrt{d_2})^2 = a^2 + d_2 b^2 + 2ab\sqrt{d_2}$.
- $ab = 0$，无论 $a = 0$ 还是 $b = 0$ 均可以得到矛盾.

思维拓展

设 $\alpha, \beta \in \mathbb{C}$，那么 $\mathbb{Q}(\alpha)$ 与 $\mathbb{Q}(\beta)$ 之间存在域同构的充要条件是什么？

彭老师课件 14 页 15 题

设 F 是一个域，$G \subset F^{\times}$ 是 F 的有限乘法子群，证明：G 是循环群.

数论函数公式与莫比乌斯反演

证明

- 设 $|G| = n$，则 G 中元素的阶均为 n 的因子，记 $G_m = \{x \in G \mid \mathrm{ord}(x) = m\}$.
- G 的每一个元素均是属于某一个 G_m 中，立刻得到 $n = \sum_{m|n} |G_m|$.
- $|G_m| \leq \psi(m)$，这里 ψ 为欧拉函数. 且$\sum_{m|n} \psi(m) = n$.
- 推出 $G_n \neq 0$，因此存在 $g \in G_n$ 使得 $G =< g >$.

思维拓展

设 R 是一个整环，$G \subset R^{\times} := \{x \in R \mid \exists y, xy = 1\}$ 是 R 的有限乘法子群，那么 G 的结构如何？如果是一般的交换环呢？

问题补充和方法扩张

问题 1

如何刻画域的自同态数？如 $\alpha \in \mathbb{C}$，$\mathbb{Q}(\alpha)$ 有多少？如 $\mathbb{R}$ 有多少域自同态？如 $\mathbb{C}$ 有多少域同态？

简要说明

- 对于 $\mathbb{Q}(\alpha)$，自同态数依赖于 α 有多少可选择的像.
- 对于 $\mathbb{R}$，自同态数只有零同态和恒等自同构.
- 对于 $\mathbb{C}$，自同态数是复杂的，分为两类：限制在 $\mathbb{R}$ 上为恒等自同构；限制在 $\mathbb{R}$ 上不是 $\mathbb{R}$ 上的恒等自同构.

问题 2

设 α, β 是 $\mathbb{Q}$ 上的代数元，是否存在 γ 使得 $\mathbb{Q}(\gamma) = \mathbb{Q}(\alpha, \beta)$.

简要说明

- 如 $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
- 设 α 的极小多项式为 $f(x)$，全部根为 $\alpha = \alpha_1, \cdots, \alpha_n$， β 的极小多项式为 $g(x)$，全部根为 $\beta = \beta_1, \cdots, \beta_m$，
- 存在有理数 $b \in \mathbb{Q}$ 使得 $\alpha_i + b\beta_j \neq \alpha_1 + b\beta_1$ 对一切 $j \neq 1$ 成立. 令 $\gamma = \alpha_1 + b\beta_1$.
- 在 $\mathbb{C}$ 中有 $\gcd(f(\gamma - bx), g(x)) = x - \beta_1$，均是 $\mathbb{Q}(\gamma)$ 中的多项式.
- 推出 $\beta_1 \in \mathbb{Q}(\gamma)$，立刻得到 $\mathbb{Q}(\gamma) = \mathbb{Q}(\alpha, \beta)$.