第二次习题课

习题讲解、方法提要和内容扩充

助教：邓先涛

2023 年 9 月 18 日

重点知识提要

重点知识提要

- 四元数体的定义
- 理想的定义和运算：商环的定义；理想的交，和以及乘积；理想的生成集.
- 理想的分类：素理想和极大理想的定义与等价刻画.

测验题讲解

测验第 1 题

刻画剩余类环 $\mathbb{Z}/n\mathbb{Z}$ 的零因子和单位群.

Bézout's Lemma：若 $d = \gcd(a, b)$ 为最大公因子，则存在整数 u, v 使得 $d = ua + vb$.

思维拓展

设 $R = \mathbb{Z}/n\mathbb{Z}$，试刻画 $M_m(R)$(R 上的 m 阶方阵环) 的零因子.

证明

- 若 m 与 n 互素，则存在整数 u 和 v 使得 $um + vn = 1$，即 $\overline{m} \cdot \overline{u} = \overline{1}$.
- 若 $d = \gcd(m, n) > 1$，则 $n \mid m \cdot (n/d)$，其中 $\overline{n/d} \neq 0$.
- 综上所述，零因子即是小于 n 的正整数中与 n 不互素的所有元素；单位即是与 n 互素的所有元素.

测验第 2 题

用群论观点证明 Wilson 定理：若 p 是素数，则 $(p-1)! \equiv -1 \bmod p$.

- 模 p 的多项式的根：$f(x) \equiv 0 \bmod p$ 至多有 $\deg(f)$ 个根.
- 群的性质：逆元存在性.

思维拓展

用群论观点证明恒等式：$\sum_{m|n} \psi(m) = n$，其中 ψ 表示不大于 m 且与 m 互素的正整数个数.

证明

- 考虑 $x^2 \equiv 1 \bmod p$ 的解只有 $x = \pm 1$.
- $\mathbb{Z}/p\mathbb{Z}$ 的单位群包含 1 到 $p-1$ 的所有数.
- 任给 $\pm 1 \neq a \in (\mathbb{Z}/p\mathbb{Z})^\times$，存在 $a \neq b \in (\mathbb{Z}/p\mathbb{Z})^\times$ 使得 $ab \equiv 1 \bmod p$.
- 将 $(p-1)!$ 中出现的数按照上述方法进行两两配对，全部消去，即可完成证明.

第一章习题讲解

第一章第 34 题

设 I 是交换环 L 中的一个理想，定义 L 的一个子集 $\mathrm{rad}I = \{r \in L | \exists n \in \mathbb{N}, r^n \in I\}$，证明 $\mathrm{rad}I$ 是理想.

理想的定义：加法子群和乘法吸收性.

思维拓展

证明：$\mathrm{rad}I = \cap_{I \subset \mathfrak{p}} \mathfrak{p}$，$\mathfrak{p}$ 跑遍含 I 的全体素理想.

且有 $\mathrm{rad}(I_1 \cdot I_2) = \mathrm{rad}(I_1 \cap I_2) = \mathrm{rad}I_1 \cap \mathrm{rad}I_2$.

证明

- 任给 $r_1, r_2 \in \mathrm{rad}I$，考虑 $(r_1 - r_2)^{2n}$.
- 任给 $r \in \mathrm{rad}I$ 和 $a \in L$，考虑 $(ar)^n = a^n r^n$.

第一章第 36 题

设 $M_n(\mathbb{Q})$ 为有理数域上的 n 阶矩阵环，证明：$M_n(\mathbb{Q})$ 无非平凡的理想，被称作单环.

- 理想的定义
- 矩阵行列变换：行变换左乘，列变换右乘.

思维拓展

如果 R 是一个含幺单环，那么 $M_n(R)$ 是否也是单环？

证明

- 设 A 的第 i 行第 j 列元素 a_{ij} 非零，定义矩阵 e_{ij} 是第 i 行第 j 列元素为 1，其余为零的矩阵，则 $e_{si}Ae_{jt} = a_{ij}e_{st}$
- 因此 A 可以生成整个 $M_n(\mathbb{Q})$，为平凡理想.

第一章第 39 题

交换环 R 中，全体幂零元素的集合是一个理想.

二项式展开技巧以及理想的定义

思维拓展

将全体幂零元构成的理想称为幂零根，记为 $\mathfrak{N}$.

证明：$\mathfrak{N} = \cap_{\mathfrak{p}} \mathfrak{p}$，这里 $\mathfrak{p}$ 跑遍全体素理想.

证明

- 任给幂零元 a, b，有 $(a-b)^{2n} = 0$.
- 任给幂零元 a 及 $b \in R$，有 $(ab)^n = a^n b^n = 0$.

第三章习题讲解

第三章第 21 题

设 R 是交换环，$J(R)$ 是全体极大理想的交，任给 $a \in J(R)$，及 $x \in R$，证明：$1 - ax$ 可逆.

含幺交换环中有包含任一非单位的极大理想.

思维拓展

证明：$\{a \in R | 1 - ax \in R^{\times}, \forall x \in R\} = J(R)$.

证明

- 反设 $1 - ax$ 不可逆，取 $I_{\mathfrak{m}}$ 为包含它的极大理想.
- $a \in I_{\mathfrak{m}}$，推出 $ax \in I_{\mathfrak{m}}$，推出 $1 \in I_{\mathfrak{m}}$ 矛盾.

第三章第 23 题

设 R 是有限交换环，则 R 的素理想是极大理想.

有限整环是域.

思维拓展

有限整环是域，这句话完整的说法是：一个有限的无零因子的含幺交换环是域. 那么这里面的交换条件是否可以去掉？即一个有限的无零因子的含幺环是域？

证明

- 由于 R 是有限交换环，因此 $R/\mathfrak{p}$ 是有限整环，所以是域.
- $R/\mathfrak{p}$ 是域当且仅当 $\mathfrak{p}$ 是极大理想.

第三章第 30 题

设 p 为素数，n 为正整数，$R = \mathbb{Z}/p^n\mathbb{Z}$，证明：$R$ 的元素不是单位元便是幂零元；R 恰有一个素理想 P；R/P 是域.

- Bézout's Lemma
- 素理想定义：$ab \in P$ 推出 $a \in P$ 或 $b \in P$.

思维拓展

设 $n = p_1^{n_1} \cdots p_k^{n_k}$，刻画 $\mathbb{Z}/n\mathbb{Z}$ 中的全部理想和全部素理想.

证明

- 任给 R 中的元素 m，要么与 p 互素，则是 R 中的单位；要么被 p 整除，则 $m^n = 0$.
- P 是素理想，$0 = p^n \in P$ 推出 $p \in P$，即 P 包含了全部幂零元.
- 有限环的性质.

第三章第 40 题

证明 $\mathbb{Z}[x]$ 的理想 $I=(3,x^3+2x^2+2x-1)$ 不是主理想.

理想的生成元

思维拓展

任给 $\mathbb{Z}[x]$ 中的理想 I，总是存在有限多个 $f_i(x)(1\leq i\leq n)$，使得 $I=(f_1(x),\cdots,f_n(x))$.

证明

- 若不然，设 $I=(f(x))$，则 $3=f(x)g(x)$，推出 $f(x)$ 等于 3 或 1.
- 由于 $3\nmid x^3+2x^2+2x-1$，因此 $f(x)\neq 3$.
- 由于 $1\neq 3u(x)+(x^3+2x^2+2x-1)v(x)$，因此 $f(x)\neq 1$.

第三章第 53 题

整环 R 只有有限多个理想，则 R 是一个域.

理想的生成集

思维拓展

如果一个无限交换幺环只有有限多个理想，那么可以推出它是域吗？试构造一个例子.

证明

- 若不然，存在非单位 $a \in R$，任给正整数 n，定义 $I_n =< a^n >$.
- 若有 $n > m$ 使得 $I_n = I_m$，则 $a^n b = a^m$，推出 a 是单位矛盾. 有无穷多理想，矛盾.

问题补充和方法扩张

问题 1

如何理解素理想的“素”字？设 A 是交换环，A 中的素理想具有如下性质：

(1) 设 $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ 是素理想，若理想 $\mathfrak{a}$ 满足 $\mathfrak{a} \subset \cup_{i=1}^n \mathfrak{p}_i$，则存在 i 使得 $\mathfrak{a} \subset \mathfrak{p}_i$.

(2) 设 $\mathfrak{a}_1, \cdots, \mathfrak{a}_n$ 是理想，若素理想 $\mathfrak{p}$ 满足 $\cap_{i=1}^n \mathfrak{a}_i \subset \mathfrak{p}$，则存在 i 使得 $\mathfrak{a}_i \subset \mathfrak{p}$. 特别的，若 $\mathfrak{p} = \cap_{i=1}^n \mathfrak{a}_i$，则存在 i 使得 $\mathfrak{a}_i = \mathfrak{p}$.

简要说明

- 可以用整数环中的整除性质理解：$\gcd(n, p_1 \cdots p_n) \neq 1$，则存在 i 使得 $p_i \mid n$；$p \mid n_1 \cdots n_k$，则存在 i 使得 $p \mid n_i$.
- 证明参见 Atiyah 的《introduction to commutative algebra》第 8 页 prop 1.11

问题 2

试刻画 $\mathbb{Z}[x]$ 中的极大理想和素理想.

简要说明

- 最小数原理，对素理想中多项式的次数和素理想中的正整数进行讨论.
- 若 $I \cap \mathbb{Z} = \{0\}$，则在素理想中取次数最小的，首项系数最小的多项式，记为 $f(x)$. 验证 $f(x)$ 不可约，且 $I = (f(x))$.
- 若 $I \cap \mathbb{Z} \neq \{0\}$，则在素理想中取最小的正整数，记为 p. 在素理想中取次数最小的，首项系数等于 1 的多项式，记为 $f(x)$. 那么 p 是素数，$f(x)$ 不可约，且 $I = (p, f(x))$.