近世代数题型方法总结

tip：本笔记用于2026年夏令营数院保研考试，总结近世代数的问题与方法，加上近年试题。

（至2025年）

Author：张竞一. zhangjingyi@mail.ustc.edu.cn

期中部分

2026.4.11

1. 2024

一、判断题，只需判断下面陈述是对还是错，无需写出证明（每小题 3 分，共 33 分）。

√(1) 27 阶群的中心一定至少有 3 个元素。⇒ 对于 p^n 阶群，其中心至少有 p 个元素 —— p-群的中心非平凡

×(2) 8 阶群必为阿贝尔群。⇒ 由小阶群的结论：≤15阶群中，6.8.10.12.14阶群均有非Abel群

√(3) 循环群的商群必为循环群。⇒ 循环群子群为循环群，商群由生成元的陪集构成。 循环群 $\simeq \mathbb{Z}$ 或 $\mathbb{Z}_m$.

√(4) 31 阶群必为循环群。对其中元素，阶为1或31，于是∃ ord p=31，生成整个群

Abel：p^2 阶，p 阶

×(5) 设群 G 由元素 a 与 b 生成，且 a 与 b 的阶分别为 m 与 n。则 $|G| \leq mn$。考虑对称群：S_4 可由(12),(1234)构成，$|S_4|=24>2\times4=8$.

×(6) 设 G 为有限生成自由阿贝尔群。则存在 G 的真子群 A 使得 G 与 A 同构。

×(7) 存在 48 阶非交换单群。最小为60阶

×(8) 100 阶群中必有 4 阶元素。$100=2^2\times5^2$ 由Sylow定理知有4阶子群，但不意味着有4阶元，可能全为2阶元

m阶子群不意味着m阶元！

√(9) 25 阶群必为阿贝尔群。p^2阶，p阶群为Abel群。

×(10) 记 $S=\{A\in M_n(\mathbb{Z})\mid \det(A)\neq 0\}$，即 S 是由所有行列式非零的 $n\times n$ 整系数方阵构成的集合。则 S 按照矩阵的乘法构成群。封√ 幺√ 逆× 结√ ← 整系数方阵的逆不一定是整系数

×(11) 设 N 为群 M 的正规子群，M 为群 G 的正规子群。则 N 定为 G 的正规子群。正规子群没有传递性.

如 $\mathbb{Z}_2 \lhd K_4 \lhd S_4$. $\mathbb{Z}_2 \ntriangleleft S_4$，$\{1, a, b, ab\}$.

二、计算题，只需写出答案，无需写出计算过程（15 分）。

(1) 设 $G=\mathbb{Z}_{30}$ 且 A 是 G 中由 $\bar{5}$ 生成的子群。计算 $[G:A]$。$A=\{\bar{0},\bar{5},\cdots,\bar{25}\}$ 为6阶群，则 $[G:A]=5$

← 先写出群阶数.

(2) 写出 $\mathbb{Z}_9\oplus\mathbb{Z}_3\oplus\mathbb{Z}_{15}\oplus\mathbb{Z}_{25}$ 的初等因子与不变因子。

(3) 写出 1000 阶阿贝尔群所有可能的初等因子与对应的不变因子。

初等因子：分为素数幂

不变因子：分类，降序排列，按列相乘

(2). 初等因子：$\{3^2, 3, 3, 5, 5^2\}$，不变因子：$\{3, 15, 225\}$

(3). $1000=2^3\times5^3$. 初等因子：$\{2,2,2,5,5,5\}$ 对应的不变因子：$\{10,10,10\}$

初等因子	不变因子
$\{2,2,2,5,5,5\}$	$\{10,10,10\}$
$\{2,2,2,5,25\}$	$\{2,10,50\}$
$\{2,2,2,125\}$	$\{2,2,250\}$
$\{2,4,5,5,5\}$	$\{5,10,20\}$
$\{2,4,5,25\}$	$\{10,100\}$
$\{2,4,125\}$	$\{2,500\}$
$\{8,5,5,5\}$	$\{5,5,40\}$
$\{8,5,25\}$	$\{5,200\}$
$\{8,125\}$	$\{1000\}$

如此处题：3 : 3^2, 3, 3

5 : 5^2, 5.

↓ ↓ ↓

225 15 3

三、（10 分）找出所有从加法群 $\mathbb{Z}_{12}$ 到加法群 $\mathbb{Z}_{20}$ 的群同态。—— 群同态.

设同态为 f. 则 $f(k)\equiv kf(1) \bmod 20$. 有 $f(12)\equiv 0 \bmod 20 \Rightarrow 12f(1)\equiv 0 \bmod 20$. $f(1)=5.10.15.0$.

则 $f_a(k)=ka \bmod 20$ $a=0.5.10.15$.

单位元映到单位元

四、（8 分）设 A 为群 G 的子群，且 $[G:A]=2$。求证对任意的 $g\in G$ 有 $g^2\in A$。

$A\leq G$. $[G:A]=2$

① 若 $g\in A$. $gA=Ag$

② 若 $g\notin A$. 则有 $G=A\cup gA=Ag\cup A$（左右陪集分解）

由结论知 $A\lhd G$. 若 $g\in A$. $g^2\in A$ 成立. 若 $g\notin A$. 有商群中 $gA\neq 1$ 的阶为2. $(gA)^2=gAgA=A \Rightarrow gAg\in A$. 则 $Ag^2\in g^{-1}Ag=A \Rightarrow g^2\in A$. 证毕

五、（10 分）设 H 与 K 均为群 G 的正规子群，且 $G=HK$。求证存在群同构 $G/(H\cap K)\cong G/H\times G/K$。

—— $G/\ker f = \mathrm{Im} f$ 的应用.

设 $f: G\to G/H\times G/K$. 由于 $H.K\lhd G$. 且 $G=HK$. 则 h 与 k 可交换，于是 $\forall g\in G$. $g=hk$. $h\in H$. $k\in K$.

$g\mapsto(gH, gK)$

$f(g_1g_2)=(g_1g_2H, g_1g_2K)=(g_1Hg_2H, g_1Kg_2K)=f(g_1)f(g_2)$ 于是为群同态。满同态：对 $\forall(aH, bK)\in G/H\times G/K$. $\exists g$. $f(g)=(aH, bK)$

若 $f(g)=(gH, gK)=(H, K)$ 则有 $g\in H$ 且 $g\in K \Rightarrow g\in H\cap K$. 则 $\ker f=H\cap K$

由同态基本定理知有同构 $G/(H\cap K)\simeq G/H\times G/K$.

→ 是一定要说明的这样才有 $\mathrm{Im} f = G/H\times G/K$. 否则只能有 $\simeq \mathrm{Im} f$

六、（10 分）设 $|G|=360$ 且 G 为单群。设 G 存在阶为 60 的子群。求证 G 必同构于 A_6。

设 H 为 G 的 60阶子群. 则 $[G:H]=6$. 有陪集同态：$f: G\to S_6$. 有 $\ker G\lhd G$. 而 G 为单群. 又若 $\ker G=G$. 所有元素作用平凡. 矛盾. 于是 $\ker G=\{e\}$. 为单射.

于是 G 与 S_6 的一个360阶子群同构. 设为A. 有 $[S_6:A]=2$. A 为 S_6 正规子群. 则 $A=A_6$

七、（14 分）找出 A_4 的所有正规子群与所有西罗子群，并计算所有西罗子群的个数。

（找正规：置换群正规子群：型相同的元素会包含）

A_4: 1 1^4 id
8 $1'3'$ (123) (124) (134) (234) (132) (142) (143) (243)
3 2^2 (12)(34), (13)(24), (14)(23).

A_4非Abel群. 如 (12)(23)=(132)
(23)(12)=(123)

正规子群：型相同. 阶数为1或2或3或4或6或12.
{id} × × K_4 × (任何群自身都是自己正规子群)

则正规子群为{id}, $K_4 \trianglelefteq A_4$

Sylow子群：$12=2^2\times 3$. 对Sylow-2子群：N(4)=2n+1 | 3 n=0时 ✓ 为K_4
n=1时 A_4只有1个四阶子群. 矛盾!
Sylow-3子群：N(3)=3n+1 | 4 3阶群是循环群. 有4个. 为<(123)>, <(124)>, <(234)>, <(134)>.

2.2023

2. (20分) 设G是一个群, M, N是G的正规子群. $g^{-1}Mg=M$ $g^{-1}Ng=N$

(1) 证明: $M\cap N$是G的正规子群; — 证正规子群 要先证为子群

(2) 证明: 如果$M\cap N=\{1\}$, 那么M和N中的元素相乘可交换.

(1). 对∀g∈G 有$g^{-1}Mg=M$, $g^{-1}Ng=N$
先证为子群：显然. 正规：对∀x∈M∩N, $gxg^{-1}\in M$ 且 $gxg^{-1}\in N$ ⇒ $g(M\cap N)g^{-1}\subseteq M\cap N$.
于是 $M\cap N\subseteq g^{-1}(M\cap N)g$ 取g=g^{-1} 所有$g(M\cap N)g^{-1}=M\cap N$ 成立.

(2) 取m∈M, n∈N 考虑$mnm^{-1}n^{-1}$ 有 $mnm^{-1}\in N$, $nm^{-1}n^{-1}\in M$ ⇒ $mnm^{-1}n^{-1}\in M\cap N=\{1\}$ ⇒ mn=nm 于是可交换 (↳ 换位子证交换性.)

3. (20分) 设G是15阶群.

(1) 那么G的Sylow 3-子群和5-子群是否正规? G是否交换? 请说明理由.

. N(3)=3n+1 | 5 ⇒ n=0 正规. N(5)=5n+1 | 3 ⇒ n=0. 正规.
15阶群一定是Abel群. 设Sylow-3子群为P. 5子群为Q. 则 P.Q◁G. P∩Q={1} G=PQ 于是 G≅P×Q≅$\mathbb{Z}_{15}$ 为循环群.
因为PQ是G的子群. 则|PQ|=|G|=15.

$|PQ|=\frac{|P|\cdot|Q|}{|P\cap Q|}=15$
$|P\cap Q|$ | gcd(3,5) ⇒ |P∩Q|={e}

4. (20分) 以下在$\mathbb{Z}_n$上定义乘法运算$\bar{i}\cdot\bar{j}=\overline{ij}$, 把$\mathbb{Z}_n$ 中在乘法运算下的可逆元集合记作$\mathbb{Z}_n^*$, 已知$\mathbb{Z}_n^*$是一个群.

(1) 分类2024阶交换群, 列举初等因子和不变因子.

(2) 证明: $\mathbb{Z}_{11}^*$是一个循环群.

(3) 判断$\mathbb{Z}_8^*$是否是循环群(说明理由).

(4) 计算阶数$|\mathbb{Z}_{2024}^*|$, 并且判断$\mathbb{Z}_{2024}^*$是否是循环群(不需要解释).

(1). $2024=2^3\times 11\times 23$ 初等因子：{2,2,2,11,23}, {2,4,11,23}, {8,11,23}
不变因子：{2,2,506}, {2,1012}, {2024}. 事实上. (a,11)=1 的a均可逆

(2). $\mathbb{Z}_{11}=\{\bar{0},\bar{1},\dots,\overline{10}\}$ 于是 $\bar{1}^{-1}=\bar{1}$, $\bar{2}^{-1}=\bar{6}$, $\bar{3}^{-1}=\bar{4}$, $\bar{5}^{-1}=\bar{9}$, $\bar{7}^{-1}=\bar{8}$, $\overline{10}^{-1}=\overline{10}$. 即$\mathbb{Z}_{11}^*=\{\bar{1},\bar{2},\dots,\overline{10}\}$为循环群 生成元可为a=$\bar{2}$. 有
a=$\bar{2}$, $a^2=\bar{4}$, $a^3=\bar{8}$, $a^4=\bar{5}$, $a^5=\overline{10}$, $a^6=\bar{9}$, $a^7=\bar{7}$, $a^8=\bar{3}$, $a^9=\bar{6}$, $a^{10}=\bar{1}$. 生成整个群

(3). $\mathbb{Z}_8=\{\bar{0},\dots,\bar{7}\}$. 有 $\bar{1}^{-1}=\bar{1}$, $\bar{3}^{-1}=\bar{3}$, $\bar{5}^{-1}=\bar{5}$, $\bar{7}^{-1}=\bar{7}$. 即$\mathbb{Z}_8^*=\{\bar{1},\bar{3},\bar{5},\bar{7}\}$
不是循环群. 对∀a∈$\mathbb{Z}_8^*$. 有 $a^2\in\{\bar{1},a\}$ 无法生成整个群. (事实上. 同构为 $\mathbb{Z}_2^2\cong K_4$)

(4). $\mathbb{Z}_{2024}^*=\mathbb{Z}_8^*\times\mathbb{Z}_{11}^*\times\mathbb{Z}_{23}^*$ 故由(3)知非循环群.

5. (30分) (1) 在置换群S_6中把元素(354)[(123)(456)](345)表示为不想交轮换的乘积, 将(12345)表示为3-轮换的乘积.

(2) S_6有多少个5阶元? 有多少个Sylow 5-子群?

(3) 写出一个置换群S_6的Sylow 5-子群P(写出生成元即可, 下同).

(4) 写出置换群S_{10} 一个Sylow 5-子群.

(5) 记号如(3), $G=S_6$, 记P在G中的正规化子群为$N_G(P)$, 计算阶数$|N_G(P)|$, 并写出这个群的生成元.

(1). 1° 1 2 3 4 5 6 于是为(125)(346) 2° (12345)=(154)(123) 先用后轮换放在右边.
1 2 4 5 3 6
2 3 5 6 1 4
2 1 4 6 1 3

(2). S_6中5阶元只有5-轮换. 个数为 $C_6^5A_4^4=144$
$|S_6|=6!=720$. N(5)=5n+1 | 144 n=0,1,3,7
Sylow-5子群 阶数为5. 为循环群. 于是只能有5阶元—5-轮换. 即每个Sylow-5子群都包含1个单位元与4个5-轮换
于是个数为144/4=36个. 为36 Sylow-5子群. n=7.

(3). 可有一生成元为 (1 2 3 4 5)

(4). 25 || $|S_{10}|$, Sylow-5子群中只有25阶元. 在S_{10}中只有双5-轮换形式的置换为25阶元. 有一子群为 {(12345), (678910)} (不是5-轮换的乘积.. 否则已是阶为5) (注意. S_{10}的Sylow-5 是25阶群了故)

(5). 法一: $|N_G(P)|=\frac{|G|}{36}=20$. 生成元为 (1 2 3 4 5) → 还有1个4阶元τ. $\tau\sigma\tau^{-1}=\sigma^2$.
↑其就是个数. 此时为同阶Sylow-5子群数. τ=(2354)

3.2021

2. (10分) 设G是一个群, N是G的正规子群, H是G的子群. 证明: $H\cdot N$是G的子群.

那定: $e\in H, e\in N \Rightarrow e=ee\in HN\neq\phi$.

子群: $\forall h_1n_1, h_2n_2\in HN$. 只需证 $h_1n_1(h_2n_2)^{-1}\in HN$.

有 $h_1n_1n_2^{-1}h_2^{-1}$ 由 $N\lhd G$. $\exists n'\in N. h_2n_1n_2^{-1}h_2^{-1}=n'$ 则 $h_1n_1n_2^{-1}h_2^{-1}=h_1h_2^{-1}n'\in HN$.

tip: HN为子群 $\Rightarrow N$装$H\lhd G$

证子群先证那定条件 $ab^{-1}\in G$.

4.2020

(15分) 4. (1) 125阶Abel群的分类; (2) 证明: 125阶非交换群的中心是非平凡的, 而且是5阶的.

(1). $|G|=5^3$. 初等因子: $[5,5,5]$ $[5,5]$ $[125]$

不变因子: $[5,5,5]$. $[5,25]$. $[125]$

(2). 由定理会 5^3 阶群只中心非平凡, 又 $C(G)\leq G\Rightarrow |C(G)|$为$5^k$.

①若 $G=C(G)$. G交换. 矛盾

②若 $|C(G)|=5$. 则商群 $G/C(G)$是5阶群. 一定是循环群. 则G为Abel群. 矛盾

于是分解有$|C(G)|=5$. 证毕

若 $G/C(G)$循环. 则 G为Abel群.

$N\cap P\leq P$. $|N\cap P|=p^a$. $|N|=p^b\cdot m$. $a\leq b$. $(m,p)=1$

由 $r|a=b$. Q为N的Sp子群. $Q\subset N$. $Q\subset P\Rightarrow Q\subset N\cap P$.

则 $b=a\Rightarrow a=b$.

(10分) 7. 设G是一个有限群, $N\lhd G$, P为G的Sylow p-子群, 证明(1) 集合PN是G的子群; (2)$P\cap N$是N的Sylow p-子群.

(1). 么元存在. 封闭性. $\forall p_1n_1, p_2n_2\in PN$. $p_1n_1n_2^{-1}p_2^{-1}$ 有 $n'\in N$. $p_2n_1n_2^{-1}p_2^{-1}=n'\Rightarrow p_1n_1n_2^{-1}p_1^{-1}=p_1p_2^{-1}n'\in PN$. 则 PN为G子群.

$p_2n_1n_2^{-1}p_2^{-1}\in N$. 则 $p_1p_2^{-1}p_2n_1n_2^{-1}p_2^{-1}\in PN$.

(2). $N\cap P\leq P$. 设 $|N\cap P|=p^a$. $|N|=p^b\cdot m$. $(p,m)=1$. 则 $a\leq b$.

设 $N\cap P$ Sylow-p子群为 Q. 则 $|Q|=p^b$. 有 $Q\leq P$. $Q\leq N\Rightarrow Q\leq N\cap P$. 则 $b\leq a\Rightarrow a=b$ 矛盾. 即 $P\cap N$为N的Sylow-p子群.

证Sylow $p\Rightarrow$ 证p核数为素大.

(15分) 2. 设$\sigma=(2134)(156)(25)(237)\in S_7$. (1) 将$\sigma$写成不相交轮换的乘积; (2) 求和$\sigma$共轭的元素个数; (3) 求$S_7$中和$\sigma$可交换的偶置换的个数.

(1). $(15)(24)(376)$

(2). 型相同: $\frac{C_7^2C_5^2\times 2}{2}=210$ 两个对换是对称的.

(3). 中心化子元素为 $\frac{|G|}{210}=24$.

$|C_G(g)|=\frac{|G|}{|g\text{所在共轭类}|}$

因为有一半为12.

四、 (10 分) 若 n 阶有限群 G 为交换群, 且 n 是 G 中所有元素的阶的最小公倍数, 证明 G 是一个循环群.

由于G为有限Abel群. $\exists m_1,\cdots,m_k$ s.t. $G\simeq Z_{m_1}\times Z_{m_2}\times\cdots\times Z_{m_k}$ $m_1|m_2|\cdots|m_k$

有 $\text{lcm}(|g|\,|\,g\in G)=m_k=n$ 则 $G\simeq Z_{m_1}\times\cdots\times Z_n$. 由于$G$为Abel群. 又解有 $m_1=\cdots=m_{k-1}=0$. 即 $G\simeq Z_n$. 证毕

有限Abel群的结构

六、 (10 分) 简要证明交错群 A_5 不存在 30 阶子群.

$n\geq 5$时 A_n为单群.

有 $|A_5|=60$. 若存在30阶子群 E. 则 $[A_5:E]=2$ 则 E为正规子群. 而 A_5为单群. 矛盾! 于是无30阶子群.

七、 (10 分) 证明 35 阶群必为循环群.

对于 Sylow-5子群 P与Sylow-7子群 Q. 有 P,Q 且有1个. $PQ\leq G$ 且 $|PQ|=|G|\Rightarrow G=PQ$. $P\lhd G$ 且 $P\cap Q=\{1\}\Rightarrow G\simeq P\times Q\simeq Z_5\times Z_7\simeq Z_{35}$ 于是G为循环群.

5.2025

五、(8 分) 设 G 为有限群, $H\leqslant G$, $K\leqslant G$. 证明 $|HK|\cdot|H\cap K|=|H|\cdot|K|$.

定理: 若 $A,B\leq G$. 且G为有限群. 则 $|AB|\cdot|A\cap B|=|A|\cdot|B|$. 其中 $AB=\{ab\,|\,a\in A, b\in B\}$

$AB=\coprod_{1\leq i\leq[AB:A]}Ab_i$ $B=\coprod_{1\leq i\leq[B:A\cap B]}(A\cap B)b_i$

对 $Ab=Ab'\Leftrightarrow b'b^{-1}\in A\Leftrightarrow b'b^{-1}\in A\cap B\Leftrightarrow (A\cap B)b=(A\cap B)b'$ 于是两陪集含个数相等. 证毕

$HK=\coprod_{1\leq i\leq[HK:H]}Hh_ik$ $K=\coprod_{1\leq j\leq[K:H\cap K]}(H\cap K)k_j$

有 $Hk=Hk'\Leftrightarrow kk'^{-1}\in H\cap K\Leftrightarrow (H\cap K)k=(H\cap K)k'$ 证毕

$[HK:H]=[K:H\cap K]$ 即 $|HK|\cdot|H\cap K|=|H|\cdot|K|$

七、(10 分) 证明 S_5 没有 30 阶子群.

法一: 群作用

设 $H\leq S_5$. $|H|=30$. S_5作用在 H的左陪集空间 $S_5/H=\{gH\,|\,g\in S_5\}$ 上. 左乘则诱导群同态 $\varphi: S_5\to S_{S_5/H}$

$\ker\varphi=\bigcap_{g\in S_5}gHg^{-1}\leq H$. 又由同态基本定理 $S_5/\ker\varphi\simeq\text{Im}\varphi\leq S_6$. 且 $[S_5:\ker\varphi]\geq 24$. 于 $|\ker\varphi|$ 又知 S_5不正规子群只有$\{e\}$, A_5, S_5.

取有 $\ker\varphi=A_5$ 或 $\ker\varphi=S_5$. 即又 $\ker\varphi\leq H$. 矛盾! 故 H不存在.

群作用的基本操作

法二: A_5性质

有 $|HA_5|=\frac{|H|\cdot|A_5|}{|H\cap A_5|}=\frac{1800}{|H\cap A_5|}$. 又 $HA_5\leq G$: $\frac{1800}{|H\cap A_5|}|120$ 即 $15||H\cap A_5|$

若 $H\leq A_5$. 有 $[A_5:H]=2$. $H\lhd A_5$ 与 A_5单性矛盾. 若 $H\not\leq A_5$. $|H\cap A_5|=15$. 又 $H\cap A_5\leq A_5$. 而 A_5不存在15阶子群. 矛盾!

于是 $|H|=30$. $H\leq S_5$.

九、(10 分) 设 G 为有限乘法阿贝尔群, 如果 $|G|$ 为奇数, 那么任意 $x\in G$ 都有唯一的平方根, 即存在唯一的 $g\in G$ 使得 $g^2=x$.

$(2,|G|)=1$ $2m+|G|n=1$ 则 $x^{|G|}=e$ $g=x^m\Rightarrow g^2=x^{1-|G|n}=x$.

Bezout定理一般充有=若互素时应用.

$\exists$: $(2,|G|)=1$. 则 $\exists a,b\in\mathbb{Z}$. $2a+b|G|=1$. $\forall x\in G$. 有 $x^{|G|}=e$. 令 $g=x^a$ 则 $g^2=x\cdot(x^{|G|})^{-b}=x$.

!: 若 $g_1,g_2\in G$. $g_1^2=g_2^2=x$ 则 $g_1^2=g_2^2\Rightarrow(g_1g_2^{-1})^2=e$. 又 $(g_1g_2^{-1})^{|G|}=e\Rightarrow\text{ord}(g_1g_2^{-1})=(2,|G|)=1$. 即 $g_1g_2^{-1}=e$. $g_1=g_2$.

(2) 设 G 为 60 阶单群. 求 G 的 4 阶子群的个数 (需给出证明过程).

为Sylow-2-子群. $N(2^2)=2n+1|15$. 个数 $N=1,3,5,15$

若 $N=1$. 为正规子群. 与单群矛盾.

若 $N=3$. 诱导同态 $\varphi: G\to S_3$. 由 G 单. $\ker\varphi=\{e\}$ 或 G. → $\forall g\in G.\ gP_ig^{-1}=P_i$ 即 P_i 为 G 正规子群. $P_1,\cdots,P_3$ 共轭. 只有1个正规. 与3个矛盾.

↓ 单射. 但 $|G|>|S_3|$ 矛盾.

若 $N=5$. 诱导同态 $\varphi: G\to S_5$ 由 G 单 $\ker\varphi=\{e\}$ 或 G → 同理矛盾.

↓ 单射. 则 $G\le S_5$. 又 $[S_5:G]=2$. 则 $G=A_5$ 而 A_5 的4阶子群恰有5个. (为4-轮换. 如 $\{e(1234)\}$)

若 $N=15$. 有 $15=\frac{|G|}{|N_G(P)|}\Rightarrow|N_G(P)|=4$. 又 $P\le N_G(P)$ 结论有 $P=N_G(P)$. 则 $C_G(P)=P$.

$P\le C_G(P)\le N_G(P)$

对 x 为 P 中非单位元. $P\le C_G(x)$. $4\mid C_G(x)$. 又 $C_G(x)\le G$. 有 $|C_G(x)|=4.12.20.60$. (略. 不会考这么难)

↓ 则 $G=C_G(x)$. 不单矛盾.

综上. 5个4阶子群.

期末部分

2026.4.11

1.2025

P素 ⟺ R/p 整环

PID中素 ⟺ 极大 P极大 ⟺ R/p 域

练习 13.1 确定环 $\mathbb{R}[x]/((x^3-1)^3)$ 的全部素理想和极大理想.

定理 3 设 I 是环 R 的理想,以 N 表示商环 R/I 的所有理想构成的集合,M 表示环 R 中包含 I 的所有理想构成的集合. 则映射

$$f: M\to N,\quad J\mapsto J/I$$

是从 M 到 N 之上的一一对应.

在UFD $\mathbb{R}[x]$ 中. $(x^3-1)^3=(x-1)^3(x^2+x+1)^3$ 有 $I=((x^3-1)^3)$ 为主理想. 由对应定理:

知要求 $\mathbb{R}[x]$ 中包含 I 的素理想与极大理想. 又 $\mathbb{R}[x]$ 为PID. 素理想与极大理想等价

设为 $(f(x))$. $f(x)$ 为 $\mathbb{R}[x]$ 中不可约多项式. 又 $((x^3-1)^3)\subseteq(f(x))\Leftrightarrow f(x)\mid(x^3-1)^3\Rightarrow f(x)=x-1$ 或 x^2+x+1 于是在商环 $\mathbb{R}[x]/I$ 中对应为 $(x-1)/I$ 与 $(x^2+x+1)/I$

练习 13.2 找到所有环同态 $\varphi:\mathbb{Z}\to\mathbb{Z}_{20}$.

— 环同态计算

设环同态 $\varphi:\mathbb{Z}\to\mathbb{Z}_{20}$. $\varphi(n)=n\varphi(1)\in\mathbb{Z}_{20}$

对 $\varphi(1)$: $\varphi(1)=\varphi(1\cdot1)=\varphi^2(1)$ 即 $\bar a=\bar a^2$ 即 $a(a-1)\equiv0 \bmod 20$. 则 $4\mid a(a-1)$, $5\mid a(a-1)$ ⇒ (a 与 $a-1$ 互质) $4\mid a$ 或 $4\mid a-1$, $5\mid a$ 或 $5\mid a-1$ 则 $a=0.1.5.16$

故 $\varphi(n)=\bar0$ 或 $n \bmod 20$ 或 $5n \bmod 20$ 或 $16n \bmod 20$.

练习 13.3 设 $t_1,\cdots,t_n\in\mathbb{R}$ 两两不同,$a_1,\cdots,a_n\in\mathbb{R}$. 令 $I_i=(x-t_i)$.

- 验证:$I_i+I_j=\mathbb{R}[x],\forall i\neq j$. ← 证理想含整个环 只需证1在其中
- 计算 $\bigcap_{i=1}^n I_i$. ← 全交. 想到CRT.
- 求证: 存在多项式 $f(x)$, 满足 $\deg f\leqslant n-1, f(t_i)=a_i,\forall 1\leqslant i\leqslant n$. → 想到带余除法.

(1) $I_i+I_j=\{f(x)(x-t_i)+g(x)(x-t_j)\mid f.g\in\mathbb{R}[x]\}$. 令 $f(x)=\frac{1}{t_i-t_j}$, $g(x)=\frac{1}{t_j-t_i}$. 为1. 证毕.

(2) I_i 为所有能被 $x-t_i$ 整除的理想. 则有 $\bigcap_{i=1}^n I_i=(\prod_{i=1}^n(x-t_i))$

(3). 由CRT. $\varphi:\mathbb{R}[x]/\bigcap_{i=1}^n I_i\cong\prod_{i=1}^n(\mathbb{R}[x]/I_i)$ 直积 $\cong\mathbb{R}^n$ ← 结论: $\mathbb{R}[x]/(x-t)\cong\mathbb{R}$.

于是 $\exists\,\overline{f(x)}\in\mathbb{R}[x]/(g(x))$ $g(x)$ 为(2)中结果. 有 $\varphi(\overline{f(x)})=(a_1,\cdots,a_n)\Leftrightarrow\exists f(x)\in\mathbb{R}[x].\ f(t_i)=a_i$

带余除法: $f(x)=q(x)g(x)+r(x)$. $\deg r(x)\le n-1$ 则 $r(t_i)=f(t_i)-q(t_i)g(t_i)=a_i$ 则 $r(x)$ 即为所求.

练习 13.4 计算 $\mathbb{Z}[\sqrt{-3}]$ 的所有单位 (unit). 判断在这个环中,2 是否可约, 是否是素元.

对 $\frac{a+b\sqrt{3}i}{c+d\sqrt{3}i}\in\mathbb{Z}[\sqrt{-3}]$. 相乘 $=1=ac-3bd+(ad+bc)\sqrt{-3}$ 则 $\begin{cases}ac-3bd=1\\ad+bc=0\end{cases}\Rightarrow\begin{matrix}ac=1\\bd=0\end{matrix}$ 若 $b=0$. $ad=0\Rightarrow d=0$. $a=c=\pm1$ 若 $d=0$. $bc=0\Rightarrow b=0$. $a=c=\pm1$. 则有 $U(\mathbb{Z}[\sqrt{-3}])=\{\pm1\}$.

素: $a\mid cd\Rightarrow a\mid c$ 或 $a\mid d$

不可约: $a=cd$. $c.d\notin U(R)$

2是否可约: 有 $2=(a+b\sqrt{-3})(c-d\sqrt{-3})$ 为两非单位乘积. 则 $\begin{cases}ac-3bd=2\\ad+bc=0\end{cases}$ 整数解为 $(a.c)=(\pm1.\pm2).(\pm2.\pm1)$ 均非单位. 则2不可约.

2是否素元: $2\mid4=(1+\sqrt{-3})(1-\sqrt{-3})$ 但 $2\nmid(1+\sqrt{-3})$ 且 $2\nmid(1-\sqrt{-3})$. 则2非素元.

考试时需证

练习 13.5 记 $\lambda_5=\exp\frac{2\pi i}{5}$. 设 $K=\mathbb{Q}(\lambda+\lambda^{-1})$ (α), $L=\mathbb{Q}(\lambda)$.

- 计算 $[L:\mathbb{Q}]$, 计算 λ 在 $\mathbb{Q}$ 上的极小多项式. → 因为 $1,\cdots,\lambda^4$ 线性相关. $\lambda^4=-1-\lambda-\lambda^2-\lambda^3$. 则 $\mathbb{Q}(\lambda)$ 中 $1.\lambda.\lambda^2.\lambda^3$ 为基.
- 计算 $L:K$, 计算 λ 在 K 上的极小多项式.

(1). $L=a+b\lambda+c\lambda^2+d\lambda^3+e\lambda^4$. 则 $[L:\mathbb{Q}]=4$.

二者不可约性相同. 变形后使用Eisenstein判别法.

有 $\lambda^4+\lambda^3+\lambda^2+\lambda+1=0$ 设 $\varphi(x)=x^4+x^3+x^2+x+1$ 有 $\varphi(x+1)=x^4+5x^3+10x^2+10x+5$ 5为 $\mathbb{Q}$ 不可约元. 又 $5\mid5.10.10.5$. $5\nmid1$. $25\nmid5$. 故不可约.

则 $\varphi(x)$ 首一不可约且 $\varphi(\lambda)=0$. 则 $\varphi(x)$ 为 λ 在 $\mathbb{Q}$ 上极小多项式.

(2). 构造 $(x-\lambda)(x-\lambda^{-1})=x^2-\alpha x+1$. 不可约. 为极小多项式. 有 $\lambda^4+\lambda^3+\cdots+1=0\Rightarrow\alpha^2+\alpha-1=0$. 则为 α 在 $\mathbb{Q}$ 极小多项式. (首一. 不可约). 则 $[K:\mathbb{Q}]=2$ 于是 $[L:K]=\frac{[L:\mathbb{Q}]}{[K:\mathbb{Q}]}=\frac{4}{2}=2$

为 $f(x)=0$　为对称

练习 13.6

- 计算 x^8-1 在 $\mathbb{Q}[x]$ 中的所有不可约因子. — 无根就不可约只对 ≤3次成立
- 计算 x^8-1 在 $\mathbb{Z}_3[x]$ 中的所有不可约因子.

(1). $x^8-1=(x^4+1)(x^2+1)(x+1)(x-1)$ 4个不可约

(2). $x+1$. $x-1$ 在任何域不可约. x^2+1 在代入 $0.1.2$ 后非0. 不可约.

只是试探. 不是一定可约! x^4+1 要分析. 算后为 $x^4+1=(x^2+x+2)(x^2+2x+2)$ =者不可约

练习 13.7 证明 $f(x)=x^3+9x+6$ 在 $\mathbb{Q}[x]$ 中不可约. 设 u 为 f 的某个根. 计算 $1+u$ 在 $\mathbb{Q}(u)$ 中的逆. 写成 $\{1,u,u^2\}$ 的线性组合. → 二次系数为0. 能用Eisenstein判别法.

为3次. 只需证无有理根. 有可能的根为 $\frac{c}{d}$. $d=\pm1$. $c=\pm1.\pm2.\pm3.\pm6$. 代入均 $\neq0$. 无根. 故不可约

$(1+u)$ 逆: $(1+u)(a+bu+cu^2)=1$ 且 $u^3=-9u-6\Rightarrow(1+u)^{-1}=\frac{1}{2}-\frac{u}{4}+\frac{u^2}{4}$

见域想到扩张

见次数想到构造此次数的单代数扩张

练习 13.8 设域 K 上不可约多项式 $f(x)$ 的次数为 $n\geqslant1$. 考虑任意非零多项式 $g(x)\in K[x]$. 设 $h(x)$ 为 $f(g(x))$ 的某个不可约因子, 求证 h 的次数一定被 n 整除.

定理 4 设 F 是 K 的扩域,$u\in F$,并且 u 在 K 上代数. 则
(1) $K(u)=K[u]$;
(2) 存在唯一的不可约首1多项式 $f(x)\in K[x]$,$\deg f\geqslant1$,使得 $f(u)=0$,并且 $K(u)\cong K[x]/(f(x))$;
(3) $[K(u):K]=n$,其中 $n=\deg f$,从而 $K(u)/K$ 为有限扩张,并且 $\{1,u,u^2,\cdots,u^{n-1}\}$ 是向量空间 $K(u)$ 的一组 K-基;
(4) $K(u)/K$ 为(有限)代数扩张.

有 $g(\alpha)\in K(\alpha)$ 则 $K(g(\alpha))$ 为 $K(\alpha)$ 子域

为单代数扩张.

设 α 为 $h(x)$ 的根. 又 $h(x)\mid f(g(x))$. $f(g(\alpha))=0$. 构造域扩张 $K(g(\alpha))$. 由 f 在 K 上不可约. $[K(g(\alpha)):K]=n$.

由 h 在 K 上不可约. $[K(\alpha):K]=\deg h\triangleq d$

有 $K\subseteq K(g(\alpha))\subseteq K(\alpha)$. 则 $[K(\alpha):K]=[K(\alpha):K(g(\alpha))]\cdot[K(g(\alpha)):K]$

即 $d=n\cdot[K(\alpha):K(g(\alpha))]$ 有 $K(\alpha)$ 为 $K(g(\alpha))$ 为有限次扩域. 则 $[K(\alpha):K(g(\alpha))]$ 为正整数. 则 $n\mid d$. 证毕.

练习 13.9 设 R 为含幺交换环. 证明: 如下命题等价.

- R 只有一个极大理想.
- 若 M 为 R 中所有非单位元素构成的集合, 则 M 是一个理想.
- R 中存在极大理想 M, 使得对任意的 $m \in M, 1+m$ 是单位.

含单位的理想为整个环

①→② 设极大理想为 m. 对 $\forall a \in R$ 且 a 非单位. $(a) \neq R$. 则有 $(a) \subseteq m$ 即 $a \in m$. } R 中非单位元素含 $M=m$ 于是 M 同样为理想.
对 $\forall a \in m$. 有 $(a) \subseteq m \neq R$. 则 a 非单位.

②→③ 设 M 为全部非单位元构成的理想. 假设: $M \neq R$. 取 V 理想 I s.t. $M \subsetneq I \subsetneq R$. $\exists a \in I \setminus M$. 则 a 为单位. 则 $I = R$ 即 M 为 R 极大理想.
若 $\forall m \in M, 1+m$ 非单位. 则 $1+m \in M$. 则 $1 = (1+m) - m \in M$ 为单位矛盾! 则 $\forall m \in M, 1+m$ 为单位

③→① 若另一极大理想 $m' \neq M$. 则 $M+m'$ 为 R 理想. 又 M 极大. $M+m'=R$.
于是 $\exists m \in M, m' \in m'$. s.t. $m+m'=1$ 即 $m' = 1+(-m)$ 为单位. 但极大理想 $m' \subsetneq R$ 与 m' 为单位矛盾.

练习 13.10 设 $f(x,y)$ 是域 K 上非零不可约多项式.

- 视 $f(x,y) \in K(y)[x]$. 证明: 在环 $K(y)[x]$ 中, $f(x,y)$ 要么是单位 (unit), 要么仍是不可约的.
- 考虑非零多项式 $g(x,y) \in K[x,y]$, 且设 $g(x,y)$ 不被 $f(x,y)$ 整除. 求证: $f(x,y) = g(x,y) = 0$ 在 K 中至多只有有限多组解.

(1). 单位: $K(y)[x]$ 中单位为 $K(y)$ 中非零元. 即 $f(x,y) = f(y) \in K(y)$. 又 $f(x,y) \neq 0$. 则 $f(y) \neq 0$. 由 $f(x,y)$ 不可约 $\Rightarrow f(y)$ 在 $K(y)$ 中不可约. 为单位.
不可约: 若非单位. 即 $\deg_x f(x,y) \geq 1$. 若 f 本原. 则 f 不可约. 若 f 不本原. $f(x,y) = c(y) \cdot f_0(x,y)$ 由 $c(y)$ 为 $K(y)$ 中单位. f 在 $K[x,y]$ 中不可约. 则 f 一定本原. 不可约.

(2). 有 f, g. 由于 f 不可约. $\gcd(f,g)=1$. 由 Bezout 定理. 公共零点个数至多为 $\deg f \cdot \deg g$. 于是只有有限多个.

2. 2024

题目 1. （判断题，每题 3 分）

✗(1) $\mathrm{GL}(n,\mathbb{R})$ 是环。 可逆矩阵相加不一定可逆.
✗(2) $\mathbb{Z}$ 和 $2\mathbb{Z}$ 作为环是同构的。 $\mathbb{Z}$ 含幺, $2\mathbb{Z}$ 不含幺
✗(3) 假设 $f: R \to S$ 是环同态，且 R, S 都含幺，则 $f(1_R) = 1_S$。 不强制保单位元!
✓(4) $\mathbb{Z}_5[x,y]$ 是 UFD。 $\mathbb{Z}_5$ 为域. UFD. $\mathbb{Z}_5[x]$ 为 UFD. $\mathbb{Z}_5[x,y]$ 为 UFD.
✓(5) $\mathbb{Z}_5(x)[y]$ 是 PID。 $\mathbb{Z}_5(x)$ 为域. 则域上一元多项式环 $\mathbb{Z}_5(x)[y]$ 为 PID.
✓(6) UFD 中不可约元和素元等价。
✗(7) $\mathbb{C}$ 是 $\mathbb{Q}$ 的代数闭包 含超越元 → 但子理想不一定是极大理想
✗(8) 设 F/K 为域扩张，且 $[F:K] = \infty$，则 F/K 为超越扩张。 超越扩张一定有 $[F:E] = \infty$. 相反不正.
✓(9) $f(x) = 3x^3 + 4x^2 + 2x + 66$ 在 $\mathbb{Q}[x]$ 上不可约。 有理根定理无解. 又 $3 \nmid 2$. 与不可约等价
✓(10) $\mathbb{Q}\left[\dfrac{\sqrt{2}+1}{\sqrt{3}}\right]$ 是域。 若 α 为 K 上的数元. $K[\alpha] = K(\alpha)$

$\alpha = \frac{\sqrt{2}+1}{\sqrt{3}}$. 则 $\alpha^4 - 10\alpha^2 + 1 = 0$. 为代数元.

题目 2. （填空题，每题 3 分）

(1) 一有限域 K 的阶数为 8，则其特征是多少。 有限域阶为 p^n. 且 $\mathrm{char} = p$.
(2) 写出 $\mathbb{Z}/12\mathbb{Z}$ 的所有素理想。 与 $\mathbb{Z}$ 中含 12 元理想一一对应 (定理). 为 $\langle 0 \rangle, \langle 2 \rangle, \langle 3 \rangle, \langle 4 \rangle, \langle 6 \rangle, \langle 1 \rangle$. 素理想 $\Leftrightarrow R/I$ 为整环.

题目 3. （6 分）
证明 $\mathbb{Z}_3[x]/(x^3 - x^2 + 1) \cong \mathbb{Z}_3[x]/(x^3 - x^2 + x + 1)$（不需要写出同构映射）。

有 $\mathbb{Z}/12\mathbb{Z}/\langle 2 \rangle = \mathbb{Z}/2\mathbb{Z}$ 与 $\mathbb{Z}/12\mathbb{Z}/\langle 3 \rangle = \mathbb{Z}/3\mathbb{Z}$ 为整环

两多项式均以 $x=0, 1, 2$ 在 $\mathbb{Z}_3[x]$ 中 $\neq 0$. 故均在 $\mathbb{Z}_3[x]$ 中不可约. 因为 $\mathbb{Z}_3$ 上三次扩域所为 $3^3 = 27$. 一定同构.

设 R 为一有限的含幺交换环，证明其每一个素理想都是极大理想。

P 为素理想. 则 R/p 为整环. 又证 R/p 为域. 又证有限整环为域
定义 $f_a: x \mapsto ax$ $a \in R/p$. 若 $ax_1 = ax_2 \Rightarrow a(x_1 - x_2) = 0$. 整环无零因子 $\Rightarrow x_1 = x_2$ 为单射. 有限 $\Rightarrow$ 为满射. 为双射. $\exists b \in R/p$. $\varphi(b) = ab = 1$
于是 R/p 中每个非零元有乘法逆元. 则 R/p 为域.

题目 7. （18 分）
设 $R = \mathbb{Z}[x]$，而将 $\mathbb{Z}$ 视为 R 的子环。
(1) P 为 R 的素理想，证明 $P \cap \mathbb{Z}$ 是 $\mathbb{Z}$ 的素理想。 纯定义
(2) 在 (1) 的基础上，若进一步有 $P \cap \mathbb{Z} = (0)$，证明 P 是主理想。

理想: 减, 乘下封闭

(1) 证明: $\forall a.b \in P \cap \mathbb{Z}$. 则 $a.b \in P$ 且 $a.b \in \mathbb{Z}$. 则 $a - b \in P$. $a - b \in \mathbb{Z}$. 则 $a - b \in P \cap \mathbb{Z}$. 同理. $\forall r \in \mathbb{Z}$. $ra, ar \in P \cap \mathbb{Z}$. 为理想.
素: $ab \in P \cap \mathbb{Z}$. 则 $ab \in P$. 由 P 为素理想. $a \in P$ 或 $b \in P$. 则 $a \in P \cap \mathbb{Z}$ 或 $b \in P \cap \mathbb{Z}$. 则有 $P \cap \mathbb{Z}$ 为 $\mathbb{Z}$ 素理想

(2).

方法 1: 直接构造生成元（最基础，适合简单环）

适用场景：环结构简单，能直接找到生成元
步骤：

1. 任取 $i \in I$，证明 i 可表示为 $a \cdot r$ $(r \in R)$，即 $I \subseteq (a)$；
2. 证明 $a \in I$，故 $(a) \subseteq I$；
3. 因此 $I = (a)$，是主理想。

例子：证明 $\mathbb{Z}$ 中所有理想都是主理想

- 任取理想 $I \subseteq \mathbb{Z}$，若 $I = \{0\}$，则 $I = (0)$；
- 若 $I \neq \{0\}$，取 a 为 I 中最小正整数，任取 $n \in I$，由带余除法 $n = qa + r$，$0 \leq r < a$，得 $r = n - qa \in I$，故 $r = 0$，即 $n = qa \in (a)$，故 $I = (a)$。

方法 2: 利用「PID 的子理想仍是主理想」

适用场景：已知 R 是主理想整环 (PID)
结论：PID 中所有理想都是主理想，因此若 I 是 PID R 的理想，则 I 自动是主理想，无需额外证明。
常见 PID：域上一元多项式环 $F[x]$、$\mathbb{Z}$、$\mathbb{Z}[i]$ (高斯整数环) 等。

方法 3: 利用「商环结构 + 理想对应」

适用场景：通过商环的性质反推理想结构
核心定理：设 R 是交换环，I 是 R 的理想，若 R/I 是 PID，则 I 的包含 I 的理想都是主理想；
进阶用法：若 R 是 UFD，I 是素理想且 R/I 是 PID，则 I 是主理想 (如题目 7(2) 的 $\mathbb{Z}[x]$ 中 $P \cap \mathbb{Z} = (0)$ 的情况)。

方法 4: 利用「域上多项式环是 PID」(题目 7(2) 的核心方法)

适用场景：多项式环 $R[x]$，理想与系数环的交为零
步骤：

1. 设 R 是 UFD，F 是 R 的分式域 (如 $R = \mathbb{Z}, F = \mathbb{Q}$)，$I$ 是 $R[x]$ 的理想，且 $I \cap R = (0)$；
2. I 可延拓为 $F[x]$ 的理想 $IF[x]$，而 $F[x]$ 是 PID，故 $IF[x] = (f(x)), f(x) \in F[x]$；
3. 由高斯引理，取本原多项式 $g(x) \in R[x]$ 使得 $f(x) = c \cdot g(x)$ $(c \in F^\times)$，证明 $I = (g(x))$。

方法 6: 利用「贝祖等式 (Bezout's Identity)」

适用场景：证明两个元素生成的理想是主理想
核心定理：在 PID 中，对任意 a, b，$\gcd(a,b) = d$，则存在 $u, v \in R$ 使得 $ua + vb = d$，因此 $(a,b) = (d)$，是主理想。
例子：$\mathbb{Z}$ 中 $(4,6) = (2)$，因为 $2 = (-1) \cdot 4 + 1 \cdot 6$。

取方才域后即 PID

3. 2023

(8) 设L/K是一个域扩张, $\alpha \in L$是K上的代数元, $f(x) \in K[x]$, 那么$f(\alpha)$是K上的代数元. Y

(9) 包含无穷多个元素的域特征为0. N

(8). α为K代数元, $K(\alpha)$为K有限域的子域, 所有元为代数元. $f(\alpha)$为K上代数元

(9). $\mathbb{F}_p(x)$为$\mathbb{F}_p$上有理函数域. char $=p$.

(2) 构造有理数域Q的一个5次扩域, 并简要解释其为什么符合要求.

令 $K=\mathbb{Q}[x]/(x^5-2)$

由 Eisenstein判别法, x^5-2在$\mathbb{Q}$上不可约. (及 Gauss引理)

进而 K为Q的5次扩域 (1, x, x^2, x^3, x^4 为基)

定理 4 设 F 是 K 的扩域, $u \in F$, 并且 u 在 K 上代数. 则

(1) $K(u)=K[u]$;

(2) 存在唯一的不可约首 1 多项式 $f(x) \in K[x]$, $\deg f \geqslant 1$, 使得 $f(u)=0$, 并且 $K(u) \cong K[x]/(f(x))$;

(3) $[K(u): K]=n$, 其中 $n=\deg f$, 从而 $K(u)/K$ 为有限扩张, 并且 $\{1, u, u^2, \cdots, u^{n-1}\}$ 是向量空间 $K(u)$ 的一组 K-基;

(4) $K(u)/K$ 为(有限)代数扩张.

4.2020

(3) 列举 $\mathbf{Z}[x]$ 的所有素理想和所有的极大理想 (不需要分析过程).

$\mathbb{Z}[x]$ 非 PID:

二、$\mathbb{Z}[x]$ 不是 PID 的证明 (核心分析)

1. 反例: 理想 $I=(2, x)$ 不是主理想

理想定义: $I=\{2f(x)+xg(x) \mid f(x), g(x) \in \mathbb{Z}[x]\}$, 即所有常数项为偶数的整系数多项式。

步骤1: 验证 I 是理想

- 对任意 $a=2f_1+xg_1, b=2f_2+xg_2 \in I$, $a-b=2(f_1-f_2)+x(g_1-g_2) \in I$;
- 对任意 $h(x) \in \mathbb{Z}[x]$, $ha=2(hf_1)+x(hg_1) \in I$, 满足理想定义。

步骤2: 证明 I 不是主理想

假设 $I=(h(x))$, $h(x) \in \mathbb{Z}[x]$, 则:

1. 因为 $2 \in I$, 所以 $h(x) \mid 2$ ($h(x)$ 整除2), 故 $h(x)$ 只能是 $\pm 1, \pm 2$;
2. 若 $h(x)=\pm 1$, 则 $I=(1)=\mathbb{Z}[x]$, 但 $1 \notin I$ (1的常数项为1, 不是偶数), 矛盾;
3. 若 $h(x)=\pm 2$, 则 $I=(2)$, 但 $x \in I$ 而 $x \notin (2)$, 矛盾;

因此 I 不是主理想, 故 $\mathbb{Z}[x]$ 不是PID。

素: (0). (p). (f(x)) (p, f(x))

其中p素数, f(x)本原

极大: (p, f(x))

三、 (15 分) 设环 $R=\mathbf{Z}[x]$.

(1) 证明: 商环 $R/(x^3+x+1)$ 是整环但不是域.

整环: 即证 (x^3+x+1) 为素理想.

$x^3+x+1=(ax+b)(cx^2+dx+e)$ 在$\mathbb{Z}$中无解 $\Rightarrow x^3+x+1$在$\mathbb{Z}[x]$中不可约

由于$\mathbb{Z}[x]$是UFD, x^3+x+1是$\mathbb{Z}[x]$中已约元, 则(x^3+x+1)为素理想. 证毕

非域: 即证(x^3+x+1)非极大理想.

取理想 $J=(2, x^3+x+1)$ 有 $(x^3+x+1) \subsetneq J \subsetneq R$ 证毕

J是理想: $J=\{2f(x)+(x^3+x+1)g(x) \mid f, g \in \mathbb{Z}[x]\}$ 加法封闭

$\forall h \in \mathbb{Z}[x]$, $h(2f+(x^3+x+1)g) \in J$, $(2f+(x^3+x+1)g)h \in J$.

(4) 设 R 为一个唯一因子分解整环, 设 $b, c \in R$ 为非零元. (i) 问两个主理想的交 $(b) \cap (c)$ 是否仍是主理想? 若是, 请简要证明; 若否, 请举例. (ii) 问主理想的和 $(b)+(c)$ 是否仍为主理想? 若是, 请简要证明; 若否, 请举例.

(ii) 中 $(b)+(c)$ 不一定主理想. $R=\mathbb{Z}[x]$, $b=2$, $c=x$ 即可.

分解元素唯一表述

(i). 是. $(b) \cap (c)=\{r \in R \mid b \mid r$ 且 $c \mid r\}$. UFD中存在最小公倍元. 设 b, c 标准分解为 $b=u\prod_{i=1}^{n} p_i^{e_i}$, $c=v\prod_{i=1}^{n} p_i^{f_i}$, u, v为单位, p_i为互不相伴的不可约元

定义 $d=\prod_{i=1}^{n} p_i^{\max(e_i, f_i)}$ 则 $d=\text{lcm}(b, c)$. $b \mid d$, $c \mid d$ 且对 $\forall r \in (b) \cap (c)$, 有 $r \in (d)$

记号: $d \in (b) \cap (c)$, 则 $(d) \subseteq (b) \cap (c)$ $\Rightarrow (d)=(b) \cap (c)$ 为主理想

$r \in (b) \cap (c)$ 则 $r \in (d)$

5.2019

四、 (20分) 设p为奇素数。

1). 证明: 存在$c \in \mathbb{F}_p$使得x^2-c为$\mathbb{F}_p[x]$中不可约多项式;

当且仅当 c 非$\mathbb{F}_p$的平方元, 而平方元个数为 $\frac{p-1}{2}$, 非平方元也为 $\frac{p-1}{2}$ 个. 故可取 c 为非平方元. x^2-c 在 $\mathbb{F}_p[x]$ 中不可约.

三、 (20分) 令$f(x)=x^4-5x^3-2x^2+2x-2 \in \mathbb{Q}[x]$。

1). 求$f(x)$的一个有理数根;

2). 设$u \in \mathbb{R} \setminus \mathbb{Q}$为$f(x)$的一个非有理数实根, 求域扩张次数$[\mathbb{Q}(u): \mathbb{Q}]$;

3). 将$(1+u)^{-1}$表示成$1, u$和u^2的$\mathbb{Q}$-线性组合。

(1) 有理根只可能为 ± 1. ± 2 代入有1为根.

(2). 有 $[\mathbb{Q}(u): \mathbb{Q}]=\deg h(x)$. $h(x)$为u在$\mathbb{R}$最小多项式. 有 $f(x)=(x+1)(x^3-6x^2+4x-2)$ 则 $h(x)=x^3-6x^2+4x-2$ 首一 √ 不可约: 3次无有理根 √

于是 $[\mathbb{Q}(u): \mathbb{Q}]=3$

(3). 有 $h(x)=x^3-6x^2+4x-2$ 为u在$\mathbb{Q}$上最小多项式,

$u(1+u)(au^2+bu+c)=1 \Rightarrow au^3+(a+b)u^2+(b+c)u+c-1=0$.

则 $a : a+b : b+c : c-1=1 : -6 : 4 : -2$

$a=-\frac{1}{11}$ $b=\frac{7}{11}$ $c=-1$ $\Rightarrow (1+u)^{-1}=-\frac{1}{11}u^2+\frac{7}{11}u-1$

2). 域$\mathbb{Q}(\sqrt{-3})$同构于$\mathbb{Q}[x]/\langle x^2+x+1 \rangle$;

3). $\mathbb{R}[x]/\langle x^4+1 \rangle$不同构于$\mathbb{C}$的子环。

(3). $[\mathbb{R}[x]/(x^4+1): \mathbb{R}]=4$. $[\mathbb{C}: \mathbb{R}]=2$ 于是不可能同构.

(2) 有 ω 为$\mathbb{Q}$上5次代数元素. 则 $\mathbb{Q}(\omega) \simeq \mathbb{Q}[x]/(x^5-2)$

$\omega=\frac{-1+\sqrt{-3}}{2}$. 下证 x^5-2 为 ω 最小多项式, 首一 √ 不可约 √. 证毕

又 $\sqrt{3}=2\omega+1$ $\Rightarrow \mathbb{Q}(\sqrt{3})=\mathbb{Q}(\omega) \simeq \mathbb{Q}[x]/(x^5-2)$