

期 中 自 测 题

说明 这套题目的成绩与课程总成绩无关, 仅作为自我检测、查缺补漏使用, 对一般同学不做强制要求. 请有时间、有兴趣的同学自觉地在 **2** 小时内独立完成, 之后可交予助教批改.

1. (10 pts) 设 $\circ$ 和 $\otimes$ 是集合 X 上的含么二元运算, 其单位元分别为 $1_\circ$ 和 $1_\otimes$. 如果对任意的 $a, b, c, d \in X$, 总成立

$$(a \otimes b) \circ (c \otimes d) = (a \circ c) \otimes (b \circ d).$$

证明: $\circ$ 和 $\otimes$ 是相同的二元运算, 并且满足交换律和结合律.

2. (10 pts) 方程 $1517x + 481y = 222$ 是否有整数解. 如果有, 用欧氏算法求出一组整数解, 并给出通解.

3. (10 pts) 证明: 方程 $2^n \equiv 1 \pmod{n}$ 没有正整数解.

4. (20 pts) 设 n 是正整数, 定义

$$\text{rad}(n) := \prod_{\substack{p|n \\ p \text{ 是素数}}} p.$$

若 $r_1, \dots, r_{\varphi(n)}$ 是 n 的一个缩系, 证明: $r_1 + m, \dots, r_{\varphi(n)} + m$ 是 n 的缩系当且仅当 $\text{rad}(n) \mid m$.

5. (10 pts) 设 G 是一个有限群, H 是 G 的子群且 $|G| = m|H|$. 证明: 对任意的 $g \in G$, 总有 $g^{m!} \in H$.

6. 设 $A := \{a_1, \dots, a_n\}$ 是有限集, $f : A \times A \rightarrow A$ 是集合 A 上的二元运算. f 的运算表是如下表格

f	a_1	$\dots$	a_n
a_1	$f(a_1, a_1)$	$\dots$	$f(a_1, a_n)$
$\dots$	$\dots$	$\dots$	$\dots$
a_n	$f(a_n, a_1)$	$\dots$	$f(a_n, a_n)$

设 p 是素数, 令 $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{p-1}\}$ 是 p 元有限域. 考虑交换环

$$\mathbb{F}_p[i] := \{\bar{a} + \bar{b}i : \bar{a}, \bar{b} \in \mathbb{F}_p\}.$$

其上的加法与乘法分别定义如下

$$(\bar{a} + \bar{b}i) + (\bar{c} + \bar{d}i) := (\bar{a} + \bar{c}) + (\bar{b} + \bar{d})i,$$

$$(\bar{a} + \bar{b}i)(\bar{c} + \bar{d}i) := (\bar{ac} - \bar{bd}) + (\bar{ad} + \bar{bc})i.$$

(10 pts) 计算 $\mathbb{F}_2[i]$, $\mathbb{F}_3[i]$ 和 $\mathbb{F}_5[i]$ 的乘法表.

(10 pts) 证明有限整环一定是域.

(5 pts) 判断 $\mathbb{F}_2[i]$, $\mathbb{F}_3[i]$ 和 $\mathbb{F}_5[i]$ 哪些是整环, 哪些是域.

(5 pts) 谈谈你的发现, 言之有理即可.

7. (10 pts) 小作文: 谈谈你对这门课程的学习情况、学习感受以及对教学团队的建议, 畅所欲言即可.

期末复习题一

讲评时间: 2021/01/24 20:00 - 23:00 腾讯会议: 872 3773 5228

A 组

1. 设 $f: X \rightarrow Y$ 是集合间的映射, S 和 T 是 X 的子集. 证明

$$(a) f(S \cup T) = f(S) \cup f(T).$$

$$(b) f(S \cap T) \subset f(S) \cap f(T).$$

举一个 $f(S \cap T) \neq f(S) \cap f(T)$ 的例子.

2. 设 I_1, I_2 和 I_3 是 $\mathbb{Z}$ 的理想, 证明

$$I_1 \cap (I_2 + I_3) = (I_1 \cap I_2) + (I_1 \cap I_3).$$

如果将 $\mathbb{Z}$ 换为一般的含么交换环 R , 结论是否成立?

3. 证明 $\text{sgn}: S_n \rightarrow \{\pm 1\}$

$$\sigma \mapsto \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

是群同态. 记号 sgn 来源于拉丁文 signum .

4. 令 $S := \{4k + 1 : k \in \mathbb{Z}_+\}$. $q \in S$ 称为拟素数, 如果 q 不能分解为 2 个 S 中元素的乘积.

(a) 证明 S 对乘法封闭并列出前 6 个拟素数.

(b) 证明 S 中元素可分解为拟素数的乘积并举例说明该分解不唯一.

(c) 证明拟素数有无穷多个.

(d) 证明形如 $4k + 3$ 的素数有无穷多个.

5. 设 p 是素数, 证明 $p \mid n^p - n$ 对任意的 $n \in \mathbb{Z}$ 成立.

B 组

1. 设 G 是乘法群, 证明
 - (a) $x \mapsto x^{-1}$ 是群同构当且仅当 G 是 Abel 群.
 - (b) * 若 $x \mapsto x^3$ 是群的单同态, 则 G 是 Abel 群.
 - (c) * 举一个非 Abel 群的例子, 使得 $x \mapsto x^3$ 是群同态.
2. * 举例说明非 Abel 群中, 2 个有限阶元的乘积不一定是有限阶元.
3. 证明在同构意义下, n 阶群的个数 $\rho(n)$ 不超过 $\binom{n!}{n}$. 事实上, $\rho(n)$ 远小于此界, 但较好的估计至今没有找到.
4. 若域 F 没有非平凡子域, 则称 F 为素域. 证明在同构意义下, 素域只有 $\mathbb{Q}$ 和 $\mathbb{Z}/p\mathbb{Z}$, 其中 p 是任意素数.
5. 设 d_1 和 d_2 是无平方因子整数. 若 $d_1 \neq d_2$, 说明 $\mathbb{Q}(\sqrt{d_1})$ 和 $\mathbb{Q}(\sqrt{d_2})$ 不同构.
6. 环 R 的非零元素 x 称为幂零的, 如果存在 $n \in \mathbb{N}$ 使得 $x^n = 0$. 证明
 - (a) 若 $x \in R$ 是幂零的, 则 $1 - x \in R^\times$.
 - (b) 若 $a, b \in R$, 则 $1 - ab$ 可逆当且仅当 $1 - ba$ 可逆.
 - (c) * 若 R 是无限集, 则 $R \setminus R^\times$ 也是无限集.
7. 环 R 的元素 e 称为幂等的, 如果 $e^2 = e$. 特别地, 0 和 1 总是幂等元.
 - (a) 设 R 是交换环, $e \in R$ 是幂等元, 则 $R \cong (e) \times (1 - e)$.
 - (b) 若交换环 R 有非平凡幂等元, 则 R 不是整环.
 - (c) 说明 $\mathbb{F}_2[i]$ 没有非平凡幂等元, 但它不是整环.
 - (d) 给出 $\mathbb{F}_5[i]$ 与 $\mathbb{F}_5 \times \mathbb{F}_5$ 的所有同构.

PS. A 组题目要求所有同学全部掌握. B 组题目稍有难度, 除 * 外, 优秀的同学应当可以独立完成. * 不常规, 证明颇具技巧性.

1. 设 $f: X \rightarrow Y$ 是集合间的映射, S 和 T 是 X 的子集. 证明

(a) $f(S \cup T) = f(S) \cup f(T)$. $\checkmark$

(b) $f(S \cap T) \subset f(S) \cap f(T)$. Δ

举一个 $f(S \cap T) \neq f(S) \cap f(T)$ 的例子.

例子: $X = \{1, 2, 3\}$ $Y = \{1, 2\}$.

$f: \begin{matrix} 1 & \mapsto & 1 \\ 2 & \mapsto & 2 \\ 3 & \mapsto & 2 \end{matrix}$ $S = \{1, 2\}$, $T = \{1, 3\}$.

$f(S \cap T) = f(\{1\}) = \{1\}$.

$f(S) \cap f(T) = \{1, 2\} \cap \{1, 2\} = \{1, 2\}$.

2. 设 I_1, I_2 和 I_3 是 $\mathbb{Z}$ 的理想, 证明

$K[x, y] - I_1 = (x+y)$

$I_2 = (x), I_3 = (y)$.

$I_1 \cap (I_2 + I_3) = (I_1 \cap I_2) + (I_1 \cap I_3)$. $\checkmark$

$\mathbb{Z}[x]$. $I_2 = (2)$.

$I_3 = (x)$.

$I_1 = (x+2)$.

如果将 $\mathbb{Z}$ 换为一般的含么交换环 R , 结论是否成立? $\times$.

$I_1 = (a), I_2 = (b), I_3 = (c)$.

$(a) \cap ((b) + (c)) \stackrel{?}{=} ((a) \cap (b)) + ((a) \cap (c))$.

$I_1 \cap [I_2 + I_3 = (2, x)]$. $I_1 = (x+2)$.

$[a, (b, c)] \stackrel{?}{=} ([a, b], [a, c])$

$I_1 \cap I_2 = (2x+4)$.
 $I_1 \cap I_3 = (x(x+2))$

由素因子分解 $\Rightarrow \max\{x, \min\{y, z\}\} \stackrel{?}{=} \min\{\max\{x, y\}, \max\{x, z\}\}$.

不妨设 $y \geq z$.

① $x \geq y \geq z$

$\times$

$\times$

② $y \geq x \geq z$

$\times$

$\times$

③ $y \geq z \geq x$.

$\checkmark$

$\checkmark$

3. 证明 $\text{sgn}: S_n \rightarrow \{\pm 1\}$

$\sigma \mapsto \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i} = (-1)^K$. K 是 σ 的交错数.

是群同态. 记号 sgn 来源于拉丁文 signum.

4. 令 $S := \{4k+1: k \in \mathbb{Z}_+\}$. $q \in S$ 称为拟素数, 如果 q 不能分解为 2 个 S 中元素的乘积.

(a) 证明 S 对乘法封闭并列出前 6 个拟素数.

(b) 证明 S 中元素可分解为拟素数的乘积并举例说明该分解不唯一.

(c) 证明拟素数有无穷多个.

(d) 证明形如 $4k+3$ 的素数有无穷多个.

(a). $5, 9, 13, 17, 21, 25, 29$.

(b). $\frac{n}{n-1} \in S$. 往下归纳.

2个形如 $4k+3$ 的素数的乘积是拟素数.

$3^2 \cdot 7^2 = (3 \cdot 7) \cdot (3 \cdot 7)$.

$9 \cdot 49 = 21 \cdot 21$.

(c). 设 $q_1, \dots, q_n$ 是所有拟素数.

则 $4q_1 \dots q_n + 1 \in S$.

但它没有拟素数分解.

(d). 设 $p_1, \dots, p_n$ 是所有形如 $4k+3$ 的素数.

$N = 4p_1 \dots p_n + 3$ 它必有 $4k+3$ 的素因子.

但 $p_1, \dots, p_n \nmid N$.

但它没有拟素数分解.

5. 设 p 是素数, 证明 $p \mid n^p - n$ 对任意的 $n \in \mathbb{Z}$ 成立.

只需证明对 $n \in \mathbb{N}$ 成立.

用数学归纳法.

$$\begin{aligned} n'^p - n' - N &= n^p - n. \\ \text{若 } n \text{ 是负数, 总可以找 } n' \in \mathbb{N}. \\ p \mid N. \end{aligned}$$

$$\begin{aligned} n' &= n + x. \\ n'^p &= (n+x)^p. \end{aligned}$$

$$\begin{cases} n^p - (n-1)^p \equiv 1 \pmod{p} \\ (n-1)^p - (n-2)^p \equiv 1 \pmod{p} \\ \vdots \\ 1^p - 0^p \equiv 1 \pmod{p} \end{cases}$$

加起来. $n^p \equiv n \pmod{p}$.

1. 设 G 是乘法群, 证明

同态.

(a) $x \mapsto x^{-1}$ 是群同构当且仅当 G 是 Abel 群.

(b) * 若 $x \mapsto x^3$ 是群的单同态, 则 G 是 Abel 群.

(c) * 举一个非 Abel 群的例子, 使得 $x \mapsto x^3$ 是群同态.

$\langle x \mapsto x^2 \text{ 单同态} \Rightarrow G \text{ Abel 群} \rangle$

$$\begin{aligned} \text{(a). } xy^{-1} &= (yx)^{-1} = f(yx) = f(y)f(x) = y^{-1}x^{-1} \\ \boxed{xy^2} &= f(x)f(y) = f(xy) = (xy)^2 = \cancel{xy} \cancel{yx} \end{aligned}$$

$$\text{(b). } \underline{a^3b^3} = f(a)f(b) = \underline{f(ab)} = (ab)^3 = ababab.$$

$$a^2b^2 = baba = (ba)^2.$$

$$(ab)^4 = ((ab)^2)^2 = (b^2a^2)^2 = \underline{a^4b^4}$$

$$(ab)^4 = a(ba)^3b = af(ba)b = af(b)f(a)b = \underline{ab^3a^3b}.$$

$$f(ab) = a^3b^3 = b^3a^3 = f(ba) \Rightarrow ab = ba.$$

(c). p^3 阶群的分类, p 素数.

$$\exp G = \min \{k \mid g^k = e \ \forall g \in G\}.$$

$$G_p = \left\{ \begin{pmatrix} 1 & a & c \\ & 1 & b \\ & & 1 \end{pmatrix} \mid a, b, c \in \mathbb{F}_p \right\}.$$

每个元素都是 p 阶元.

海森堡群 over $\mathbb{F}_p$.

特别地, 取 $p=3$. G_3 是 27 阶群.

$x \mapsto x^3$ 是平凡同态.

2. * 举例说明非 Abel 群中, 2 个有限阶元的乘积不一定是有限阶元.

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ 4阶元.}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \text{ 3阶元.}$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = -\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ 无限阶元.}$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^3 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}.$$

3. 证明在同构意义下, n 阶群的个数 $\rho(n)$ 不超过 $\binom{n!}{n}$. 事实上, $\rho(n)$ 远小于此界, 但较好的估计至今没有找到.

乘法表.

G	

$n \times n$.

每一列都是 G 中元素的一个排列. 每一列都不同.

$n!$ 个不同排列. 取 n 个排列.

$$\text{乘法表个数} \leq \binom{n!}{n}.$$

$$G \leq S_{|G|}.$$

4. 若域 F 没有非平凡子域, 则称 F 为素域. 证明在同构意义下, 素域只有 $\mathbb{Q}$ 和 $\mathbb{Z}/p\mathbb{Z}$, 其中 p 是任意素数.

$$1 \in F. \text{ 若不存在 } n \text{ 使得 } \underbrace{1 + \dots + 1}_{n\uparrow} = 0.$$

$$\text{则 } \mathbb{Z} \xrightarrow{f} F \Rightarrow \mathbb{Q} \hookrightarrow F.$$

$$\begin{aligned} f(1) &= 1 \quad f(2) = 2 \quad \dots \quad f(n) = n. \\ 1 &= f(1) = f(n \cdot \frac{1}{n}) = \underbrace{f(\frac{1}{n}) + \dots + f(\frac{1}{n})}_{n\uparrow} \Rightarrow f(\frac{1}{n}) = \frac{1}{n}. \end{aligned}$$

$$\text{若存在 } n \text{ 使得 } \underbrace{1 + \dots + 1}_{n\uparrow} = 0. \text{ 不妨设 } n \text{ 是最小的.}$$

$$\mathbb{Z}/n\mathbb{Z} \hookrightarrow F. \text{ 但 } F \text{ 是域, } \Rightarrow n \text{ 是素数.}$$

5. 设 d_1 和 d_2 是无平方因子整数. 若 $d_1 \neq d_2$, 说明 $\mathbb{Q}(\sqrt{d_1})$ 和 $\mathbb{Q}(\sqrt{d_2})$ 不同构.

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}.$$

$$\mathbb{Q}(\sqrt{d_1}) \xrightarrow{f} \mathbb{Q}(\sqrt{d_2}).$$

$$1 \mapsto 1.$$

Ex 1.1.1. 1.1.1.

$$1 \mapsto 1.$$

$$f|_{\mathbb{Q}} = \text{id}. \quad f(a+b\sqrt{d_1}) = a+b f(\sqrt{d_1}) \in \mathbb{Q}(\sqrt{d_2}).$$

$$a+b f(\sqrt{d_1}) = c+d\sqrt{d_2}.$$

$$\Rightarrow f(\sqrt{d_1}) = \sqrt{d_2}. \quad \text{但这不可能}.$$

$$f(\sqrt{d_1}) \cdot f(\sqrt{d_1}) = f(d_1) = d_1.$$

$$\sqrt{d_2} \cdot \sqrt{d_2} = d_2.$$

6. 环 R 的非零元素 x 称为**幂零**的, 如果存在 $n \in \mathbb{N}$ 使得 $x^n = 0$. 证明

(a) 若 $x \in R$ 是幂零的, 则 $1-x \in R^\times$.

(b) 若 $a, b \in R$, 则 $1-ab$ 可逆当且仅当 $1-ba$ 可逆.

(c) * 若 R 是无限集, 则 $R \setminus R^\times$ 也是无限集.

(a). $\frac{1}{1-x} = 1+x+x^2+\dots + \boxed{x^n + \dots}$
0.

不妨设 $x^{n+1} \neq 0, x^n = 0$.

可以验证 $1+x+\dots+x^n$ 是 $1-x$ 的逆.

(b). 若 $1-ab$ 可逆.

$$c = \frac{1}{1-ab} = 1 + \underline{ab + abab + \dots} + (ab)^n + \dots$$

$$? d = \frac{1}{1-ba} = 1 + \underline{ba + baba + \dots} + (ba)^n + \dots$$

$$bca = ba + baba + bababa + \dots$$

d 应该是 $1+bca$ 的形式.

$$\text{若 } (1-ab)c = c(1-ab) = 1.$$

$$\underline{c - abc = 1} = c - cab.$$

$$\text{则 } (1-ba)(1+bca) = 1-ba + bca - babca.$$

$$= 1-ba + bca - b(c-1)a.$$

$$= 1-ba + bca - bca + ba$$

(c). R 不是体, R 是无限集. $R \setminus R^\times \neq \{0\}$. 若 $R \setminus R^\times$ 有限.

$\forall x \in R^\times$, x 左乘: $S \rightarrow S$ 双射.

$P: R^\times \rightarrow \boxed{S \text{ 到 } S \text{ 的双射}} \quad (\text{构成一个群, 复合运算}).$

$$x \mapsto x \text{ 左乘}.$$

$\text{Ker } P$ 是无限集. $R^\times$ 无限集.

$$R^\times / \text{Ker } P \hookrightarrow S \text{ 到 } S \text{ 的双射}.$$

$x \mapsto x^2$ 张.
 $\ker p$ 是无限集. $\left(\begin{array}{l} R^x \text{ 无限集.} \\ R^x = \bigsqcup_{x \in R^x} x + \ker p. \end{array} \right.$ 有限并.
 $\ker p$ 是无限集.

$R^x / \ker p \hookrightarrow \text{到 } \mathbb{N} \text{ 的映射.}$
 $\uparrow$
 有限集.

$\forall x \in \ker p, 1-x$ 都不可逆.

$1-x$ 左乘作用在 S 上是 0.

$$\boxed{\forall y \in S, y \neq 0, \text{ 可逆元 } r \in R^x \quad ry = 0 \Rightarrow y = 0.}$$

$\therefore \{1-x \mid x \in \ker p\}$ 是无穷个不可逆元.

7. 环 R 的元素 e 称为**幂等**的, 如果 $e^2 = e$. 特别地, 0 和 1 总是幂等元.

(a) 设 R 是交换环, $e \in R$ 是幂等元, 则 $\boxed{R \cong (e) \times (1-e)}$.

(b) 若交换环 R 有非平凡幂等元, 则 R 不是整环.

(c) 说明 $\mathbb{F}_2[i]$ 没有非平凡幂等元, 但它不是整环.

(d) 给出 $\mathbb{F}_5[i]$ 与 $\mathbb{F}_5 \times \mathbb{F}_5$ 的所有同构.

(a). $1 = e + (1-e)$

$R = Re + R(1-e)$.

只需证明直和. $Re \cap R(1-e) = 0$.

$\forall x \in Re \cap R(1-e), \exists r_1, r_2 \text{ s.t.}$

$x = r_1 e = r_2 (1-e)$.

$x \cdot e = r_1 e^2 = r_1 e = x$.

$x \cdot e = r_2 (1-e) e = 0$.

$\therefore x = 0$.

$I_1 = (e), I_2 = (1-e), \quad \underline{I_1 + I_2 = R}$.

$I_1 \cap I_2 = I_1 I_2 = 0$

$R \cong R / I_1 \cap I_2 \cong \underbrace{R / I_1}_{(1-e)} \times \underbrace{R / I_2}_{(e)}.$

(b). $R = S \times T \Rightarrow R$ 不是整环.

$(1,0)(0,1) = 0$.

(c). $\mathbb{F}_2[i]$ 没有幂等元. 直接验证.

z 在 $\mathbb{Q}(i)$ 分歧.

$\dots \sim \pi[i] \cong \mathbb{Z}[x] / \dots$

(c). $\mathbb{F}_2[i]$ 没有平方元. $\mathbb{F}_2[i] \cong \mathbb{F}_2[x]/(x^2+1)$

$$\mathbb{F}_2[i] \cong \mathbb{Z}[i]/(2) \cong \mathbb{Z}[i]/(2) \cong \mathbb{Z}[x]/(x^2+1)/(2)$$

$$\cong \mathbb{F}_2[x]/(x^2+1) \cong \mathbb{F}_2[x]/((x+1)^2)$$

5 在 $\mathbb{Q}(i)$ 中分裂.

$$(i+1)^2 = 1 - 1 + 2i = 0$$

$$(d). \mathbb{F}_5[i] \cong \mathbb{F}_5[x]/(x^2+1) \cong \mathbb{F}_5[x]/(x+3)(x+2) \cong \frac{\mathbb{F}_5[x]}{(x+3)} \times \frac{\mathbb{F}_5[x]}{(x+2)}$$

幂等元 $\rightarrow$ 幂等元.

$\mathbb{F}_5 \times \mathbb{F}_5$ 的幂等元只有 4 个 $(0,0) (1,1) (1,0) (0,1)$.

$\mathbb{F}_5[i]$ 的幂等元 $(i+3)^2 = 1+9+6i = 3+i$.

只有 4 个. $1-(i+3) = (2-i) = (3-i)$.

取决于 $3+i, 3-i$ 映射到哪.

$$\mathbb{F}_5[i] \rightarrow \mathbb{F}_5 \times \mathbb{F}_5$$

$$3+i \mapsto (1,0)$$

$$3-i \mapsto (0,1)$$

$$\mathbb{F}_5[i] \rightarrow \mathbb{F}_5 \times \mathbb{F}_5$$

$$3+i \mapsto (0,1)$$

$$3-i \mapsto (1,0)$$

$$G = \{e, a, b, c\}$$

G	e	a	b	c
e	e	a	b	c
a	a	a ²	ba	ca
b	b	ab	b ²	cb
c	c	ac	bc	c ²

$$\begin{array}{l} a^2 = b? \\ a^2 = c? \\ a^2 = e? \end{array}$$

	e	a	b	c
e	e	a	b	c
a	a	e	ba	ca
b	b	ab	b ²	cb
c	c	ac	bc	c ²

$$a^2 = e, b^3 = c$$

$$b^2 = a \Rightarrow b^4 = e$$

$\Rightarrow b$ 是 4 阶元.

$$\textcircled{1} a^2 = e, b^2 = a \Rightarrow \mathbb{Z}/4\mathbb{Z}$$

$$\textcircled{2} a^2 = e, b^2 = c$$

✓

$$c \mid c \quad ac \mid bc \quad c^2$$

$$\boxed{a^2 = b^2 = c^2 = e.}$$

$$\textcircled{2} \quad \frac{a^2=e \quad b^2=c}{bc=a \quad ba=e.} \quad \times.$$

$$\textcircled{3} \quad a^2=e \quad b^2=e.$$

G 中有 4 个元 $\leftarrow \frac{\mathbb{Z}/4\mathbb{Z}}{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}}$

$$a^2=b^2=c^2=e. \quad \mathbb{Z}/6\mathbb{Z}.$$

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

6 个元

$\{e, a, b, b^2, ab, ab^2\}$

$$ba = a^2 b^2$$

$$\begin{aligned} b^2 a &= b a b^2 \\ &= a b^4 = a b. \\ b^2 a b &= a b^2 \end{aligned}$$

S_3	e	a	b	b^2	ab	ab^2
e	e	a	b	b^2	ab	ab^2
a	a	e	ab	ab^2	b	b^2
b	b	ab^2	b^2	e	a	ab.
b^2	b^2	ab	e	b	ab^2	a.
ab	ab					
ab^2	ab^2					

期末复习题二

讲评时间: 2021/02/07 20:00 - 23:00. 腾讯会议: 872 3773 5228.

A 组

1. 证明 $\zeta := (2 + i)/(2 - i)$ 不是 n 次单位根.
2. 设 $f: A \rightarrow R$ 是含么交换环之间的同态. 证明多项式环 $A[x]$ 具有如下**泛性质**: 对于任意的元素 $t \in R$, 存在唯一的环同态 $\pi_t: A[x] \rightarrow R$ 满足 $\pi_t|_A = f$ 且 $\pi_t(x) = t$. 即有如下交换图

$$\begin{array}{ccc} A & \xrightarrow{f} & R \\ \downarrow & \nearrow \pi_t & \\ A[x] & & \end{array}$$

3. 设 F 是域, 计算 $F[x]$ 的保持 F 不变的自同构群. 提示: 利用 2.
4. 计算次数为 m 的 n 个变元的首一单项式的个数. 提示: 插空法.
5. 设 $f \in \mathbb{F}_p[x]$. 证明: 若 $f' = 0$, 则存在 $g \in \mathbb{F}_p[x]$ 使得 $f(x) = g^p(x)$.
6. 记 $p_k(x_1, \dots, x_n) = \sum_{i=1}^n x_i^k$, 证明如下 **Newton 公式**
 - (a) 若 $1 \leq k \leq n$, $p_k - p_{k-1}s_1 + \dots + (-1)^{k-1}p_1s_{k-1} + (-1)^kp_0s_k = 0$.
 - (b) 若 $k > n$, $p_k - p_{k-1}s_1 + \dots + (-1)^{n-1}p_{k-n+1}s_{n-1} + (-1)^np_{k-n}s_n = 0$.

其中, s_i 是第 i 个初等对称多项式.

7. 设 n 是奇数, 证明

- (a) 若 $n-1 \mid m$, 则 $\sum_{i=1}^{n-1} i^m \equiv -1 \pmod{n}$.
- (b) 若 $n-1 \nmid m$, 则 $\sum_{i=1}^{n-1} i^m \equiv 0 \pmod{n}$.

提示: 利用 6.

B 组

1. 在带有二元运算的集合 X 中, 可以在 n 个元素的乘积之间安插括号, 所有可能的安插方式的数目记为 l_n , 称为第 n 个 **Catalan 数**.

$$l_2 = 1. \quad x_1x_2$$

$$l_3 = 2. \quad (x_1x_2)x_3, x_1(x_2x_3)$$

$$l_4 = 5. \quad x_1((x_2x_3)x_4), x_1(x_2(x_3x_4)), (x_1x_2)(x_3x_4), ((x_1x_2)x_3)x_4, (x_1(x_2x_3))x_4.$$

$$(a) \text{ 证明 } l_n = \sum_{k=1}^{n-1} l_k l_{n-k}.$$

$$(b) \text{ 令 } l(x) = \sum_{n=1}^{\infty} l_n x^n, \text{ 证明 } l^2(x) = l(x) - x.$$

$$(c) \text{ 利用 } (1 + \lambda x)^{1/r} \text{ 的幂级数展开式计算 } l_n.$$

2. 设 F 是无限域, $c_0, c_1, \dots, c_n$ 是 F 中两两不同的元素. 证明对任意的 $b_0, b_1, \dots, b_n \in F$, 存在唯一的 $f \in F[x]$ 满足 $f(c_i) = b_i$ 且 $\deg f \leq n$.
提示: 有两种构造方法, **Lagrange 插值**和 **Newton 插值**, 它们的结果是相同的.

3. 设 $f \in \mathbb{C}[x]$, 记

$$S_0(f) := \{z \in \mathbb{C} : f(z) = 0\}, \quad S_1(f) := \{z \in \mathbb{C} : f(z) = 1\}.$$

证明: 若 $S_0(f) = S_0(g)$ 且 $S_1(f) = S_1(g)$ 则 $f = g$. 提示: 利用 $\mathbb{C}$ 是代数闭域, 说明 $|S_0(f) \cup S_1(f)| \geq 1 + \deg f$.

4. 设 $f \in \mathbb{C}[x]$ 非常数, 记 $\text{rad}(f)$ 为 f 的**互不相伴**一次因子乘积. 证明

$$\deg(f, f') \geq \deg f - \deg \text{rad}(f).$$

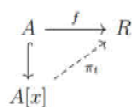
提示: 利用 $\mathbb{C}$ 是代数闭域和 $\mathbb{C}[x]$ 的唯一分解性.

5. 设 $f, g, h \in \mathbb{C}[x]$ 非常数且互素. 若 $f + g + h = 0$, 证明

$$\max\{\deg f, \deg g, \deg h\} \leq \deg \text{rad}(fgh) - 1.$$

提示: 此为 **Mason 定理**, 可以利用 4 证明, 也可以直接证明.

1. 证明 $\zeta := (2+i)/(2-i)$ 不是 n 次单位根.
2. 设 $f: A \rightarrow R$ 是含幺交换环之间的同态. 证明多项式环 $A[x]$ 具有如下泛性质: 对于任意的元素 $t \in R$, 存在唯一的环同态 $\pi_t: A[x] \rightarrow R$ 满足 $\pi_t|_A = f$ 且 $\pi_t(x) = t$. 即有如下交换图



3. 设 F 是域, 计算 $F[x]$ 的保持 F 不变的自同构群. 提示: 利用 2.
4. 计算次数为 m 的 n 个变元的首一单项式的个数. 提示: 插空法.

证明了唯一性, 还用证存在性吗?

命题是可以判断真假的陈述句.

“明天下雨”不是命题.

若 p , 则 q . “若 n 既是正整数, 又是负整数, 则 $n < 0$ 且 $n > 0$ ”

证: n 是正整数 $\Rightarrow n > 0$.

n 是负整数 $\Rightarrow n < 0$

满足条件的集合是空集.

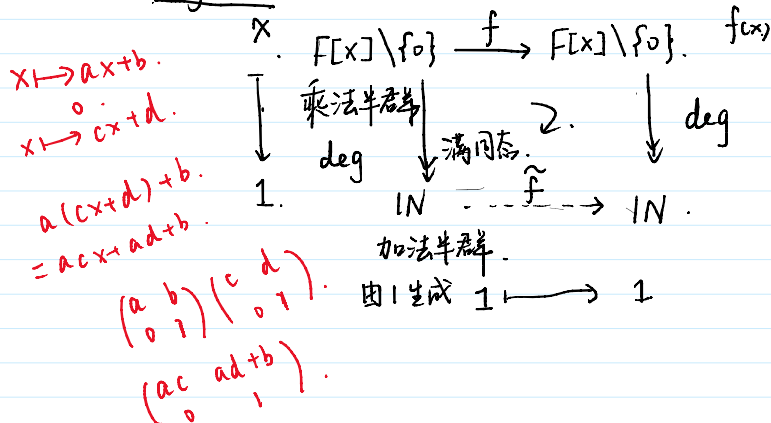
3. 由 2, 只需确定 x 的像.

$$x \mapsto a_0 + a_1x + \dots + a_nx^n = f(x).$$

若 $\deg f > 1$, 则 x 没有原像.

若 $\deg f = 0$, 则任何多项式的像都是常数.

$\therefore \deg f = 1$. 即 $x \mapsto ax + b$, $a \neq 0$. $\{(a, b) \mid a \neq 0\}$.



$$\begin{aligned} 1. \quad \zeta^n = 1 &\Rightarrow (2-i)^n = (2+i)^n = (2-i+2i)^n \\ &= (2-i)^n + \dots + (2i)^n \\ &= (2-i)^n + (2i)^n \text{ 在 } \mathbb{Z}[i] \text{ 中} \\ &\Rightarrow 5 \mid 2^n \text{ 不可能.} \end{aligned}$$

2. 唯一性. 若 π_t 存在.

$$\begin{aligned} &\pi_t(a_0 + a_1x + \dots + a_nx^n) \\ &= \pi_t(a_0) + \pi_t(a_1)\pi_t(x) + \dots + \pi_t(a_n)\pi_t(x)^n \\ &= f(a_0) + f(a_1)t + \dots + f(a_n)t^n \quad (*) \end{aligned}$$

$\therefore \pi_t$ 被唯一确定.

存在性. 用 (*) 定义 π_t , 验证环同态.

4. n 个变元, 次数为 m 的首一单项式.

$$x_1^{s_1} \dots x_n^{s_n}$$

$$(1) \quad s_1 + \dots + s_n = m, \quad s_i \geq 0.$$

对应 m 的一个 n -分拆.

$$\begin{array}{c} 0 \parallel 0 \dots 0 \parallel 0 \quad n \text{ 个 } 0 \\ x^2 y^2 z^2 \quad n=3, m=4. \end{array}$$

$$(2) \quad s'_1 + \dots + s'_n = m+n, \quad s'_i \geq 1.$$

(1) 与 (2) 的解有一一对应.

$$s_i \mapsto s_i + 1 \triangleq s'_i$$

$$\begin{array}{ccc} 0 & 0 & \dots & 0 & 0 & m+n \text{ 个 } 0 \\ \text{挡板板的位置} & m+n-1 & & & & (m+n-1) \\ \text{共 } n-1 \text{ 个挡板} & n-1 & & & & (n-1) \end{array}$$

5. 设 $f \in \mathbb{F}_p[x]$. 证明: 若 $f' = 0$, 则存在 $g \in \mathbb{F}_p[x]$ 使得 $f(x) = g^p(x)$.

$$\text{设 } f(x) = a_0 + a_1x + \dots + a_nx^n.$$

$$f'(x) = a_1 + 2a_2x + \dots + na_nx^{n-1} = 0$$

$$\Rightarrow p \mid ia_i, \quad i=1, \dots, n.$$

$$(1 \in \mathbb{F}_q[x] \quad q=p^n) \quad \checkmark$$

$$|1 \in \mathbb{F}_q^x| = q-1 = p^n-1. \quad a_0^{p^n} \equiv a_0 \pmod{p}.$$

$$\Rightarrow p \mid i a_i, i=1, \dots, n.$$

$$\Rightarrow p \mid i \text{ or } p \mid a_i.$$

$$f(x) = g(x^p) = g^p(x). \quad (a_0^p = a_0 \pmod p)$$

6. 记 $p_k(x_1, \dots, x_n) = \sum_{i=1}^n x_i^k$, 证明如下 Newton 公式

(a) 若 $1 \leq k \leq n$, $p_k - p_{k-1}s_1 + \dots + (-1)^{k-1}p_1 s_{k-1} + (-1)^k s_k = 0$. 为什么不是 p_0 ?

(b) 若 $k > n$, $p_k - p_{k-1}s_1 + \dots + (-1)^{n-1}p_{k-n+1}s_{n-1} + (-1)^n p_{k-n}s_n = 0$.

其中, s_i 是第 i 个初等对称多项式.

$$(y-x_1)(y-x_2)\dots(y-x_n) = y^n - s_1 y^{n-1} + s_2 y^{n-2} - \dots + (-1)^n s_n. \quad (1)$$

$$(y-x_1)(y-x_2)\dots(y-x_{n-1}) = (y-x_1)(y-x_2)\dots(y-x_{n-1})(y-0)^{\frac{1}{y}}. \quad (2)$$

$$= y^{n-1} - (s_1)_0 y^{n-2} + (s_2)_0 y^{n-3} - \dots + (-1)^n (s_n)_0.$$

① $k \geq n$ 时. 令 $y = x_0$. 代入 (1).

$$0 = x_0^n - s_1 x_0^{n-1} + s_2 x_0^{n-2} - \dots + (-1)^n s_n$$

乘 x_0^{k-n}

$$0 = x_0^k - s_1 x_0^{k-1} + s_2 x_0^{k-2} - \dots + (-1)^n s_n x_0^{k-n}.$$

对 i 求和.

$$0 = p_k - s_1 p_{k-1} + s_2 p_{k-2} - \dots + (-1)^n s_n p_{k-n}.$$

② $k \leq n$ 时. 令 $f_{k,n}(x_1, \dots, x_n) = p_k - p_{k-1}s_1 + \dots + (-1)^{k-1}p_1 s_{k-1} + (-1)^k k s_k$.

对 $r = n-k$ 归纳. 证 $f_{k,n} \equiv 0$.

$r=0$ 时, $n=k$. $\checkmark$ $f_{k,n} \equiv 0$.

假设 $r = n-k-1$ 时成立. $\checkmark$ $f_{k,n+1} \equiv 0$.

$$f_{k,n}(x_1, \dots, x_{n+1}, 0) = (p_k)_0 - (p_{k-1})_0 (s_1)_0 + \dots + (-1)^{k-1} (p_1)_0 (s_{k-1})_0 + (-1)^k k (s_k)_0$$

$$= f_{k,n+1}(x_1, \dots, x_{n+1}) \equiv 0.$$

$$\Rightarrow x_n \mid f_{k,n}.$$

类似地 $\Rightarrow x_1 \dots x_n \mid f_{k,n}$. 但 $\deg f_{k,n} \leq k \leq n \Rightarrow f_{k,n} \equiv 0$.

7. 设 p 是奇素数, 证明

(a) 若 $p-1 \mid m$, 则 $\sum_{i=1}^{p-1} i^m \equiv -1 \pmod p$. $\checkmark$

(b) 若 $p-1 \nmid m$, 则 $\sum_{i=1}^{p-1} i^m \equiv 0 \pmod p$. $\checkmark$

提示: 利用 6.

证法: $\sum_{i=1}^{p-1} i^m = p_m(1, 2, \dots, p-1)$

由于 $a^{p-1} \equiv 1 \pmod{p}$, $a \neq 0$.

$\therefore$ 若 $m \equiv m' \pmod{p-1}$, 则 $a^m \equiv a^{m'} \pmod{p}$.

$\therefore$ 不妨设 $0 \leq m < p-1$.

$m=0$ 时, $\sum_{i=1}^{p-1} i^0 = p-1 \equiv -1 \pmod{p}$.

$0 < m < p-1$ 时, $m=1$ 时, $\sum_{i=1}^{p-1} i^1 \equiv 0 \pmod{p}$. $\checkmark$.

$$\Leftrightarrow p_1(1, 2, \dots, p-1) \pmod{p} \checkmark.$$

设 $0 < m \leq k-1 < p-2$ 时, 成立. 即 $(1, 2, \dots, p-1), p_2(1, 2, \dots, p-1), \dots, p_{k-1}(1, 2, \dots, p-1) \equiv 0 \pmod{p}$.

由归纳假设, $p_k(1, 2, \dots, p-1) \equiv \pm k S_k(1, 2, \dots, p-1) \pmod{p}$.

在 $\mathbb{F}_p$ 上, $X^{p-1} - 1 = (X-1)(X-2)\dots(X-(p-1))$. Vieta 定理. $S_k = 0$, $1 < k < p-1$.

证法: 若 $p-1 \mid m$, 则 $\sum_{i=1}^{p-1} i^m = \sum_{i=1}^{p-1} 1 = p-1 \equiv -1 \pmod{p}$.

若 $p-1 \nmid m$, 则 $\exists 0 < a \leq p-1$ 使得 $a^m \not\equiv 1 \pmod{p}$.

$$\sum_{i=1}^{p-1} i^m \equiv \sum_{i=1}^{p-1} (ia)^m = \left(\sum_{i=1}^{p-1} i^m \right) a^m \pmod{p}.$$

若 $\sum_{i=1}^{p-1} i^m \not\equiv 0 \pmod{p}$, $\Rightarrow a^m \equiv 1 \pmod{p}$. 矛盾.

$\triangle A$ 整环, $f(x) \in A[x]$, $\deg f = n$, 则 f 的零点个数不超过 n . $\mathbb{Z} \hookrightarrow \mathbb{Q}$. 整环 $\hookrightarrow$ 分式域.

$\Rightarrow A$ 整环, $f, g \in A[x]$, $\deg f, \deg g \leq n$. 若 f, g 在 $n+1$ 个不同元素上取值相同. 则 $f=g$.

Pf. $h=f-g$, 则 $\deg h \leq n$, 但 h 在 $n+1$ 个点取值为 0 $\Rightarrow h \equiv 0$.

非整环不对! $x^2=x$. 幂等元, 不一定只有 0 和 1.

环的函数环. $\{f: R \rightarrow R\}$. $(f \cdot g)(r) = f(r) \cdot g(r)$.

$$(f+g)(r) = f(r) + g(r).$$

乘法单位: $r \mapsto 1$.

加法单位: $r \mapsto 0$.

命题: R 是无限整环, 则 $R[x] \hookrightarrow$ 函数环.

有限域不对! $\mathbb{F}_p$. 作为函数, $x \mapsto x^p$. $x \mapsto x$ 是一样的. 但 x^p 和 x 是不同的多项式.

Pf. $\forall f \in R[x]$, $f \neq 0$, 则 f 至多有 $\deg f$ 个零点.

但 R 是无限整环, $\therefore \exists r \in R$, $f(r) \neq 0$. $\therefore$ 作为函数, $f \neq 0$.

2. 设 F 是无限域, $c_0, c_1, \dots, c_n$ 是 F 中两两不同的元素. 证明对任意的 $b_0, b_1, \dots, b_n \in F$, 存在唯一的 $f \in F[x]$ 满足 $f(c_i) = b_i$ 且 $\deg f \leq n$.
提示: 有两种构造方法, Lagrange 插值和 Newton 插值, 它们的结果是相同的.

$$\text{设 } f(x) = a_0 + a_1 x + \dots + a_n x^n$$

$$\begin{cases} a_0 + a_1 c_0 + \dots + a_n c_0^n = b_0 \\ a_0 + a_1 c_1 + \dots + a_n c_1^n = b_1 \\ \vdots \\ a_0 + a_1 c_n + \dots + a_n c_n^n = b_n \end{cases}$$

$n+1$ 个关于 $a_0, \dots, a_n$ 的方程组.

由线性代数: 它有解且解唯一.

($c_0, \dots, c_n$ 互不相同).

$$\text{Lagrange 插值. } f(x) = \sum_{i=0}^n b_i \frac{(x-c_0) \dots (x-c_{i-1})(x-c_{i+1}) \dots (x-c_n)}{(c_i-c_0) \dots (c_i-c_{i-1})(c_i-c_{i+1}) \dots (c_i-c_n)}.$$

$$\text{Newton 插值. 设 } f(x) = u_0 + u_1(x-c_0) + u_2(x-c_0)(x-c_1) + \dots + u_n(x-c_0)(x-c_1) \dots (x-c_{n-1}).$$

$$b_0 = f(c_0) = u_0.$$

$$b_1 = f(c_1) = u_0 + u_1(c_1 - c_0) \Rightarrow u_1 = \frac{b_1 - b_0}{c_1 - c_0}.$$

$$b_2 = f(c_2) = u_0 + u_1(c_2 - c_0) + u_2(c_2 - c_0)(c_2 - c_1) \Rightarrow u_2.$$

$\vdots$

$$b_n = f(c_n) = \dots \Rightarrow u_n.$$

3. 设 $f \in \mathbb{C}[x]$, 记

$$S_0(f) := \{z \in \mathbb{C} : f(z) = 0\}, \quad S_1(f) := \{z \in \mathbb{C} : f(z) = 1\}.$$

证明: 若 $S_0(f) = S_0(g)$ 且 $S_1(f) = S_1(g)$ 则 $f = g$. 提示: 利用 $\mathbb{C}$ 是代数闭域, 说明 $|S_0(f) \cup S_1(f)| \geq 1 + \deg f$.

$$S_0(f) \cap S_1(f) = \emptyset \Rightarrow |S_0(f) \cup S_1(f)| = |S_0(f)| + |S_1(f)|.$$

若 $|S_0(f) \cup S_1(f)| \geq \deg f + 1$, 则 f 被唯一确定.

不同
f 在 $\deg f + 1$ 个^{不同}点上的取值
已知

$$\text{设 } f(x) = u_n \prod_{i=1}^s (x-c_i)^{e_i} \quad f(x)-1 = v_n \prod_{j=1}^t (x-d_j)^{f_j}.$$

$$c_i \in S_0(f).$$

$$d_j \in S_1(f).$$

$$\sum_{i=1}^s e_i = \deg f = \deg(f(x)-1) = \sum_{j=1}^t f_j.$$

$$|S_0(f)| = s \quad |S_1(f)| = t. \quad |S_0(f) \cup S_1(f)| = s+t.$$

$$f'(x) = \frac{\prod_{i=1}^s (x-c_i)^{e_i-1} \prod_{j=1}^t (x-d_j)^{f_j-1}}{\prod_{i=1}^s (x-c_i)^{e_i} \prod_{j=1}^t (x-d_j)^{f_j}}. \text{ 故有.}$$

$$\begin{aligned} \deg f - 1 = \deg f' &\geq \sum_{i=1}^s (e_i - 1) + \sum_{j=1}^t (f_j - 1) = \deg f - s + \deg f - t. \\ &= 2\deg f - |S_0(f) \cup S_1(f)|. \end{aligned}$$

$$\star |S_0(f) \cup S_1(f)| \geq \deg f + 1.$$

4. 设 $f \in \mathbb{C}[x]$ 非常数, 记 $\text{rad}(f)$ 为 f 的互不相伴一次因子乘积. 证明

$$\deg(f, f') \geq \deg f - \deg \text{rad}(f).$$

提示: 利用 $\mathbb{C}$ 是代数闭域 $\mathbb{C}[x]$ 的唯一分解性.

$$\text{设 } f = u \prod_i p_i^{e_i}, e_i \neq 0 / \text{rad } f = \prod_i p_i.$$

$$\forall i, f = p_i^{e_i} q_i, \quad f' = (p_i^{e_i} q_i)' = p_i^{e_i-1} (p_i q_i' + e_i q_i p_i').$$

$$\therefore \prod_i p_i^{e_i-1} \mid (f', f).$$

$$\therefore \deg f - \deg \text{rad } f \leq \deg(f', f).$$

5. 设 $f, g, h \in \mathbb{C}[x]$ 非常数且互素. 若 $f + g + h = 0$, 证明

$$\max\{\deg f, \deg g, \deg h\} \leq \deg \text{rad}(fgh) - 1.$$

$$\begin{cases} \deg f \leq \deg \text{rad}(fgh) - 1 \\ \deg g \leq \text{---} \\ \deg h \leq \text{---} \end{cases} \Leftrightarrow$$

提示: 此为 **Mason 定理**, 可以利用 4 证明, 也可以直接证明.

$$\text{记 } d_f = (f, f'), \quad d_g = (g, g'), \quad d_h = (h, h').$$

$$\therefore [d_f, d_g, d_h] \text{ 互素}.$$

$$\begin{cases} \deg d_f \geq \deg f - \deg \text{rad } f \\ \deg d_g \geq \deg g - \deg \text{rad } g \\ \deg d_h \geq \deg h - \deg \text{rad } h \end{cases}$$

$$\boxed{\begin{matrix} \deg d_f d_g d_h = \deg d_f + \deg d_g + \deg d_h \geq \deg f + \deg g + \deg h - (\deg \text{rad } f + \deg \text{rad } g + \deg \text{rad } h) \\ ? \mid \\ \deg f + \deg g - 1 \end{matrix}} \quad \checkmark, \quad = \deg f + \deg g + \deg h - \deg \text{rad}(fgh).$$

$$\deg g + \deg h - 1 \geq \deg d_f d_g d_h.$$

$$\deg f + \deg h - 1 \geq \deg d_f d_g d_h.$$

$$f + g + h = 0 \Rightarrow \underline{f + g = -h} \Rightarrow \underline{f' + g' = -h'}.$$

$$\begin{cases} f g' + g g' = -h g' \\ f' g + g' g = -h' g \end{cases} \Rightarrow f g' - g f' = -(h g' - g h').$$

$$\boxed{f g' - g f' \neq 0} \quad \text{若 } f g' - g f' = 0 \text{ 则 } f \mid g f' \Rightarrow f \mid f'. \text{ 不可行.}$$

$$\therefore d_f, d_g \mid f g' - g f' \quad d_h \mid h g' - g h'$$

$$\therefore d_f, d_g \mid fg' - gf' \quad d_h \mid hg' - gh'$$

$$\therefore d_f d_g d_h \mid fg' - gf' \quad \therefore \deg d_f d_g d_h \leq \deg(fg' - gf') \leq \deg f + \deg g - 1$$

Generating series . . 生成函数. 母函数.

例. $a_0 = -1, a_1 = 1, \underline{a_n = 2a_{n-1} + 3a_{n-2} + 3^n}$. 求 a_n .

考虑生成函数. $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n + \dots$

$$-2xf(x) = -2a_0x - 2a_1x^2 - 2a_2x^3 - \dots - 2a_{n-1}x^n - \dots$$

$$-3x^2f(x) = -3a_0x^2 - 3a_1x^3 - \dots - 3a_{n-2}x^n - \dots$$

$$(1 - 2x - 3x^2)f(x) = -1 + 3x + 3^2x^2 + \dots + 3^n x^n + \dots$$

$$\stackrel{||}{(1+x)(1-3x)} = -1 + \frac{3x}{1-3x} = \frac{6x-1}{1-3x}$$

$$f(x) = \frac{6x-1}{(1+x)(1-3x)^2} = \frac{A}{1+x} + \frac{B}{(1-3x)^2} + \frac{C}{1-3x}$$

两边乘 $x+1$, 令 $x=-1 \Rightarrow A = -\frac{7}{16}$.

两边乘 $(1-3x)^2$, 令 $x=\frac{1}{3} \Rightarrow B = \frac{3}{4}$.

两边乘 x , 令 $x \rightarrow \infty \Rightarrow 0 = A + 0 + (-\frac{1}{3})C \Rightarrow C = -\frac{21}{16}$.

$$f(x) = -\frac{7}{16(1+x)} + \frac{3}{4(1-3x)^2} - \frac{21}{16(1-3x)}$$

$$= \sum_{n=0}^{\infty} \frac{(4n-3)3^{n+1} - (-1)^n 7}{16} x^n$$

$$\therefore a_n = \frac{1}{16} [(4n-3)3^{n+1} - 7(-1)^n]$$

B1.

1. 在带有二元运算的集合 X 中, 可以在 n 个元素的乘积之间安插括号, 所有可能的安插方式的数目记为 l_n , 称为第 n 个 **Catalan 数**.

$$l_2 = 1. x_1 x_2$$

$$l_3 = 2. (x_1 x_2) x_3, x_1 (x_2 x_3)$$

$$l_4 = 5. (x_1 ((x_2 x_3) x_4), x_1 (x_2 (x_3 x_4)), (x_1 x_2) (x_3 x_4), ((x_1 x_2) x_3) x_4, (x_1 (x_2 x_3)) x_4.$$

(a) 证明 $l_n = \sum_{k=1}^{n-1} l_k l_{n-k}$. $(0 \ 0 \ (0 \ 0) \ (0 \ 0) \ 0 \ 0)$

(b) 令 $l(x) = \sum_{n=1}^{\infty} l_n x^n$, 证明 $l^2(x) = l(x) - x$.

$$y^2 = y - x$$

(c) 利用 $(1 + \lambda x)^{1/r}$ 的幂级数展开式计算 l_n .

$$l(x) = \frac{1 \pm \sqrt{1-4x}}{2}$$

舍去其中一个.

$$\frac{1 \pm \sqrt{1-4x}}{2} = \frac{1}{2} \pm \frac{1}{2} (1-4x)^{\frac{1}{2}}$$

$$l(x) = \frac{1 - \sqrt{1-4x}}{2} \Rightarrow l_n = \frac{1}{n} \binom{2n-2}{n-1}$$

A6.

6. 记 $p_k(x_1, \dots, x_n) = \sum_{i=1}^n x_i^k$, 证明如下 **Newton 公式**

(a) 若 $1 \leq k \leq n$, $p_k - p_{k-1}s_1 + \dots + (-1)^{k-1}p_1 s_{k-1} + (-1)^k k s_k = 0$.

(b) 若 $k > n$, $p_k - p_{k-1}s_1 + \dots + (-1)^{n-1}p_{k-n+1}s_{n-1} + (-1)^n p_{k-n}s_n = 0$.

其中, s_i 是第 i 个初等对称多项式.

$$f(t) = 1 + s_1 t + s_2 t^2 + \dots + s_n t^n = (1 + x_1 t)(1 + x_2 t) \dots (1 + x_n t)$$

$$\frac{d}{dt}(\ln f(t)) = \frac{f'(t)}{f(t)} = \frac{s_1 + 2s_2 t + 3s_3 t^2 + \dots + n s_n t^{n-1}}{1 + s_1 t + s_2 t^2 + \dots + s_n t^n}$$

$$\ln f(t) = \ln(1 + x_1 t) + \ln(1 + x_2 t) + \dots + \ln(1 + x_n t)$$

$$\begin{aligned} \frac{d}{dt}(\ln f(t)) &= \frac{x_1}{1+x_1 t} + \dots + \frac{x_n}{1+x_n t} \\ &= \sum_{i=1}^n x_i (1 - x_i t + x_i^2 t^2 - x_i^3 t^3 + \dots) \\ &= [p_1 - p_2 t + p_3 t^2 - p_4 t^3 + \dots] \end{aligned}$$

$$\therefore s_1 + 2s_2 t + 3s_3 t^2 + \dots + n s_n t^{n-1}$$

$$= (p_1 - p_2 t + p_3 t^2 - p_4 t^3 + \dots) (1 + s_1 t + s_2 t^2 + \dots + s_n t^n)$$

对应系数相等.

KSE

对应的系数相等.

KS_F

0次项 左边 = S_1 右边 = $P_1 \Rightarrow S_1 = P_1$

1次项 左边 = $2S_2$ 右边 = $-P_2 + S_1P_1 \Rightarrow P_2 - S_1P_1 + 2S_2 = 0$

2次项 左边 = $3S_3$ 右边 = $P_3 + S_2P_1 - P_2S_1 \Rightarrow P_3 - P_2S_1 + P_1S_2 - 3S_3 = 0$

⋮

$n-1$ 次项 左边 = nS_n 右边 = $\dots$

n 次项 左边 = 0 右边 = $\dots$

A4

1. 证明 $\zeta := (2+i)/(2-i)$ 不是 n 次单位根.

2. 设 $f: A \rightarrow R$ 是含幺交换环之间的同态. 证明多项式环 $A[x]$ 具有如

下**泛性质**: 对于任意的元素 $t \in R$, 存在唯一的环同态 $\pi_t: A[x] \rightarrow R$ 满足 $\pi_t|_A = f$ 且 $\pi_t(x) = t$. 即有如下交换图

$$\begin{array}{ccc} A & \xrightarrow{f} & R \\ \downarrow & \nearrow \pi_t & \\ A[x] & & \end{array}$$

3. 设 F 是域, 计算 $F[x]$ 的保持 F 不变的自同构群. 提示: 利用 2.

4. 计算次数为 m 的 n 个变元的首一单项式的个数. 提示: 插空法

维数. 1 ② ③ ④ 5

令 $n=2$. $k[x, y] = k \oplus (kx \oplus ky) \oplus (kx^2 \oplus kxy \oplus ky^2) \oplus \dots$

$\binom{m+2-1}{2-1} = \underline{m+1}$ 次数 0 1 2 3 4

维数是次数的函数. 有割裂 $a_m = n$ 次部分的维数.

$$H(t) = a_0 + a_1 t + a_2 t^2 + \dots + a_n t^n + \dots$$

称为 $k[x, y]$ 的 Hilbert 级数.

Koszul Resolution. $C_2^0 \quad C_2^1 \quad C_2^2$

$$0 \rightarrow k[x, y] \xrightarrow{1} k[x, y] \oplus k[x, y] \xrightarrow{1} k[x, y] \rightarrow k \rightarrow 0.$$

$$[a_{n+2} - 2a_{n+1} + a_n = 0]$$

$2a_{n+1} = a_{n+2} + a_n$ $C_3^0 \quad C_3^1 \quad C_3^2 \quad C_3^3$

$$a_n = n+1$$

$$Z(n+1) = n+3 + n+1$$

1 2 2 1.

代数学基础期末考试

2021 年 3 月 4 日，星期四，14:30–16:30

姓名：_____ 学号：_____ 所在院系：_____

题号	一	二	三	四	五	六	七	总 分
得分								
复查								

一、(15 分) (1) 求 2021^{2021} 的末三位数字。

(2) 对 2021 的每个素因子 p 找出一个模 p 原根。

二、（10 分） 令 $F_n = 2^{2^n} + 1, n \geq 1$ 。

(1). 证明 $(F_i, F_j) = 1, \forall i \neq j$ 。

(2). 利用 (1) 证明素数有无穷多个。

三、(15 分) 若正整数 n 满足 $\sum_{1 \leq d|n} d = 2n$, 则称 n 为完全数。

(1). 证明偶完全数具有形式 $2^{p-1}(2^p - 1)$, 其中 p 和 $2^p - 1$ 均为素数。

(2). 试找出 100 以内的所有完全数。

四、(15 分) 设 $n > 1$ 为正整数。令 $\zeta_n = e^{\frac{2\pi i}{n}}$ 为 n 次复单位根，其中 $i = \sqrt{-1}$ 。

(1). 设 $0 \leq k \leq n$ 为整数。试计算 $\prod_{0 \leq i \leq n-1, i \neq k} (\zeta_n^k - \zeta_n^i)$ 。

(2). 利用 (1) 中结论，计算 $\sin 1^\circ \sin 2^\circ \sin 3^\circ \cdots \sin 90^\circ$ 。

五、(10 分) 求所有素数 p 使得 $x^2 - 10$ 在 $\mathbb{F}_p[x]$ 中可约, 其中 $\mathbb{F}_p$ 为 p -元域。

六、(10 分) 对有理数 x , 令 $[x]$ 表示不超过 x 的最大整数。

(1). 对任意素数 p , p 在 $n!$ 中出现的指数恰为 $[\frac{n}{p}] + [\frac{n}{p^2}] + [\frac{n}{p^3}] + \cdots$;

(2). 对任意 $n = m_1 + m_2 + \cdots + m_k$, $k \geq 1$, $m_i \geq 1$, $\frac{n!}{m_1!m_2!\cdots m_k!}$ 为整数。

七、(35 分) 令 $\mathcal{A} = \{f \mid f: \mathbb{Z}_+ \rightarrow \mathbb{Q}\}$ 为取值在有理数域的数论函数全体。记 ϵ 为由 $\epsilon(1) = 1, \epsilon(n) = 0, \forall n \geq 2$ 给出的函数。考察 $\mathcal{A}$ 上运算：

$$(f + g)(n) = f(n) + g(n), \quad (fg)(n) = f(n)g(n), \quad (f * g)(n) = \sum_{1 \leq d|n} f(d)g\left(\frac{n}{d}\right).$$

- (1). 证明 $(\mathcal{A}, +, *)$ 形成一个含么交换环，其么元恰为 ϵ ；
- (2). 证明 $f(g * h) = (fg) * h + g * (fh), \forall f, g, h \in \mathcal{A}$ ；
- (3). 证明 $f \in \mathcal{A}$ 在运算 $*$ 下可逆当且仅当 $f(1) \neq 0$ ；记 f 的逆为 f^{-1} 。
- (4). 证明 $\mu * \mathbf{1} = \epsilon$ ，其中 μ 为莫比乌斯函数，即 $\mu(1) = 1, \mu(n) = (-1)^s$ 若 n 为 s 个互不相同的素数的乘积，否则 $\mu(n) = 0$ ， $\mathbf{1}$ 为值等于 1 的常值函数。
- (5). 证明所有非 0 的积性函数 (即 $f(mn) = f(m)f(n), \forall (m, n) = 1$) 在 $*$ 下形成一个群。
- (6). 设 $f \in \mathcal{A}$ 为非 0 积性函数。试求 f^{-1} 。
- (7). 试找出 $(\mathcal{A}, *)$ 中有限阶元。

1. (1) 求 $2021^{2021} \bmod 10^3$, 由于 $\varphi(10^3) = 400$, 故原式化为 $21^{21} \bmod 10^3$.

证法一. 二项展开得 $21^{21} \equiv (20 + 1)^{21} \equiv 1 + \binom{21}{1} 20 \equiv 421 \bmod 10^3$.

证法二. 参考课本例 4.30. 对 21 做二进制分解得 10101_2 .

$$\begin{aligned} a_0 &\equiv 21^1 \equiv 21 \bmod 10^3, \\ a_1 &\equiv 21^2 \cdot 21^0 \equiv 441 \bmod 10^3, \\ a_2 &\equiv 441^2 \cdot 21^1 \equiv 101 \bmod 10^3 \\ a_3 &\equiv 101^2 \cdot 21^0 \equiv 201 \bmod 10^3 \\ a_4 &\equiv 201^2 \cdot 21^1 \equiv 421 \bmod 10^3. \end{aligned}$$

故 $2021^{2021} \equiv 421 \bmod 10^3$.

(2) $\sqrt{2021} < 50$, 考虑 50 以下的素数. $2021 = 43 \times 47$.

模 47 的原根个数为 $\varphi(\varphi(47)) = \varphi(46) = \varphi(2)\varphi(23) = 22$.

模 47 的非二次剩余的个数为 23.

因此, 除 -1 外的非二次剩余都是模 47 的原根.

为方便改卷, 计算所有的二次剩余如下

$$\{1, 4, 9, 16, 25, 36, 2, 17, 34, 6, 27, 3, 28, 8, 37, 21, 7, 42, 32, 24, 18, 14, 12\}.$$

特别地, 5 是模 47 的最小原根.

课本习题 8.6 中令 $p = 23$, $q = 2p + 1 = 47$ 知 -2 是原根.

模 43 的原根个数为 $\varphi(\varphi(43)) = \varphi(42) = \varphi(2)\varphi(3)\varphi(7) = 12$.

模 43 的非二次剩余的个数为 21.

因此, 原根是阶不为 2, 3, 7, 6, 14, 21 的非二次剩余.

由欧拉判别法知, 若 a 是非二次剩余, 则 $a^{21} \equiv -1 \bmod 43$.

因此, 非二次剩余的阶不可能是 3, 7, 21. 需排除阶为 2, 6, 14 的情况.

即这些非二次剩余的 1, 3, 7 次幂不应为 -1 .

2 是非二次剩余但 $2^7 \equiv -1 \bmod 43$. 3 是二次剩余且

$$3^3 \equiv 27 \bmod 43, \quad 3^6 \equiv -2 \bmod 43, \quad 3^7 \equiv -6 \bmod 43$$

因此, 3 是模 43 的最小原根. 按照此法可得到全部原根.

2. 课本习题 3.9, 答案见 11.8 习题课讲义.

3. (1) 由课本例 3.22 知 $\sigma_1(n) := \sum_{d|n} d$ 是积性函数.

若 $n = 2^k m$ 是偶完全数, 其中 m 是奇数, $k \geq 1$, 则

$$\sigma_1(n) = 2n = 2^{k+1}m.$$

又因为 $\sigma_1(n) = \sigma_1(2^k)\sigma_1(m) = (2^{k+1} - 1)\sigma_1(m)$.

显然, $2^{k+1} - 1 \geq 3$ 是奇数, 故 $2^{k+1} - 1 \mid m$. 令 $m = (2^{k+1} - 1)l$, 则

$$2^{k+1}l = \sigma_1(m) = m + l + \text{others} = 2^{k+1}l + \text{others}.$$

因此, m 除了 1 和自身不能有其余因子, 从而 m 是素数且 $l = 1$.

由课本习题 3.10 知, m 为 Mersenne 素数. 从而 $k+1$ 是某个素数 p .

综上所述, $n = 2^{p-1}(2^p - 1)$.

(2) 容易验证, (1) 中的条件是充要的, 由此可以得到 100 以内的偶完全数 6 和 28. 要说明它们是 100 以内的所有完全数, 计算机比较擅长.

4. (1) 注意到 $x^n - 1 = \prod_{i=0}^{n-1} (x - \zeta_n^i)$. 因此

$$\prod_{i=1}^{n-1} (x - \zeta_n^i) = \frac{x^n - 1}{x - 1} = \sum_{i=0}^{n-1} x^i.$$

令 $x = 1$ 得, $\prod_{i=1}^{n-1} (1 - \zeta_n^i) = n$. 两端同乘 $(\zeta_n^k)^{n-1}$ 即可.

(2) 计算复平面上以原点, $e^{i\alpha}$, $e^{i\beta}$ 为顶点的等腰三角形的面积.

由两腰及其夹角正弦可得

$$\frac{1}{2} \cdot 1 \cdot 1 \cdot \sin |\alpha - \beta| = \sin \frac{|\alpha - \beta|}{2} \cos \frac{|\alpha - \beta|}{2}.$$

由底乘高可得

$$\frac{1}{2} \cdot |e^{i\alpha} - e^{i\beta}| \cdot \left(1 \cdot \cos \frac{|\alpha - \beta|}{2}\right).$$

两者比较得

$$2 \sin \frac{|\alpha - \beta|}{2} = |e^{i\alpha} - e^{i\beta}|.$$

令 $\zeta := e^{\frac{2\pi i}{180}}$, 固定 $\alpha = 0^\circ$, β 取遍 $2^\circ, 4^\circ, 6^\circ, \dots, 358^\circ$ 可得

$$2 \sin 1^\circ = |1 - \zeta|, 2 \sin 2^\circ = |1 - \zeta^2|, \dots, 2 \sin 89^\circ = |1 - \zeta^{89}|, 2 \sin 90^\circ = |1 - \zeta^{90}|.$$

$$2 \sin 179^\circ = |1 - \zeta^{179}|, 2 \sin 178^\circ = |1 - \zeta^{178}|, \dots, 2 \sin 91^\circ = |1 - \zeta^{91}|.$$

将它们乘起来, 利用 (1) 中的结论可得

$$2^{179} \cdot (\sin 1^\circ \sin 2^\circ \sin 3^\circ \cdots \sin 90^\circ)^2 = 180.$$

因此

$$\sin 1^\circ \sin 2^\circ \sin 3^\circ \cdots \sin 90^\circ = \frac{\sqrt{360}}{2^{90}}.$$

也可以考虑利用如下的 3 倍角公式进行配对计算

$$\sin 3\theta = 4 \sin \theta \sin(60^\circ - \theta) \sin(60^\circ + \theta).$$

5. 参考课本例 8.23 与习题 8.14. $10 \equiv 2 \pmod{4}$, 它的 conductor 为 40.

由中国剩余定理理解得的同余方程的解应该是按模 40 分类的.

$$x \equiv 1 \pmod{8}, \quad x \equiv 1 \pmod{5} \implies x \equiv 1 \pmod{40}.$$

$$x \equiv 1 \pmod{8}, \quad x \equiv 4 \pmod{5} \implies x \equiv 9 \pmod{40}.$$

$$x \equiv 7 \pmod{8}, \quad x \equiv 1 \pmod{5} \implies x \equiv 31 \pmod{40}.$$

$$x \equiv 7 \pmod{8}, \quad x \equiv 4 \pmod{5} \implies x \equiv 39 \pmod{40}.$$

$$x \equiv 3 \pmod{8}, \quad x \equiv 2 \pmod{5} \implies x \equiv 27 \pmod{40}.$$

$$x \equiv 3 \pmod{8}, \quad x \equiv 3 \pmod{5} \implies x \equiv 3 \pmod{40}.$$

$$x \equiv 5 \pmod{8}, \quad x \equiv 2 \pmod{5} \implies x \equiv 37 \pmod{40}.$$

$$x \equiv 5 \pmod{8}, \quad x \equiv 3 \pmod{5} \implies x \equiv 13 \pmod{40}.$$

综上所述, p 为 2, 5 以及形如模 40 余 1, 3, 9, 13, 27, 31, 37, 39 的素数.

6. (1) $1, 2, 3, \dots, n$ 中有哪些元素贡献了 p . 它们是形如 kp 的元素, 计数

$$\left[\frac{n}{p} \right].$$

$1, 2, 3, \dots, n$ 中形如 kp^2 的元素, 每个贡献了至少 2 个 p , 需要补上

$$\left[\frac{n}{p^2} \right].$$

$1, 2, 3, \dots, n$ 中形如 kp^3 的元素, 每个贡献了至少 3 个 p , 需要补上

$$\left[\frac{n}{p^3} \right].$$

以此类推, 原式得证.

(2) 只需说明如下事实

$$\left[\frac{n}{x} \right] \geq \sum_{i=1}^k \left[\frac{m_i}{x} \right].$$

(3) 补充一个知识点, 如何计算 $n!$ 的末尾有几个零.

这是在考虑 10 在 $n!$ 中的指数.

由于 $10 = 2 \times 5$, 而在 $n > 1$ 时, 2 在 $n!$ 中的指数必然大于 5 的指数(?)

因此, 10 在 $n!$ 中的指数就是 5 在 $n!$ 中的指数. 故 $n!$ 的末尾有

$$\sum_{k=1}^{\infty} \left[\frac{n}{5^k} \right]$$

个零.

7. (1) 交换律 $(f * g)(n) = \sum_{xy=n} f(x)g(y) = \sum_{xy=n} g(x)f(y) = (g * f)(n).$

单位元 $(f * \varepsilon)(n) = (\varepsilon * f)(n) = \sum_{xy=n} \varepsilon(x)f(y) = f(n).$

结合律 $((f * g) * h)(n) = \sum_{xyz=n} f(x)g(y)h(z) = (f * (g * h))(n).$

分配律 $(f * (g + h))(n) = \sum_{xy=n} f(x)(g + h)(y) = (f * g + f * h)(n).$