习题 1.1. 对于任何集合X, 我们用id_X表示X到自身的恒等映射. 设$f : A \to B$是集合间的映射, A是非空集合. 试证：

1. f为单射当且仅当存在$g : B \to A$, 使得$g \circ f = \mathrm{id}_A$;

2. f为满射当且仅当存在$h : B \to A$, 使得$f \circ h = \mathrm{id}_B$;

3. f为双射当且仅当存在唯一的$g : B \to A$, 使得$f \circ g = \mathrm{id}_B$, $g \circ f = \mathrm{id}_A$. 这里的$g$称为$f$的**逆映射**, 通常也记为$f^{-1}$. 证明双射的逆映射也是双射, 并讨论逆映射与映射的原像集合之间的关系.

1. 设$g \circ f = \mathrm{id}_A$. 若$f$不是单射, 则存在$x \neq y$使得$f(x) = f(y)$. 两边同时复合$g$可得$x = y$. 这就产生了矛盾. 若$f$是单射, 如何构造$g$? 我们来看一个具体的例子: 设$A := \{a, b\}$, $B := \{c, d, e\}$， $f(a) = c$, $f(b) = d$. g的定义如下图所示:

$$A \xrightarrow{f} B \xrightarrow{g} A$$

$$a \longrightarrow c \longrightarrow a$$

$$b \longrightarrow d \longrightarrow b$$

$$e \nearrow$$

容易验证, 无论$g(e) = b$还是$g(e) = a$, 都可以满足$g \circ f = \mathrm{id}_A$. 这说明, g的选取不一定唯一. 请同学们依据这个例子, 思考一般情形如何证明。

2. 请同学们仿照(1)进行证明, 并仔细体会(1)与(2)的对偶之处.

3. 若f是双射, 则f既是单射又是满射, 由(1)与(2)知, 存在$g : B \to A$, $h : B \to A$, 使得$g \circ f = \mathrm{id}_A$, $f \circ h = \mathrm{id}_B$. (3)似乎在告诉我们, $g = h$. 这是正确的吗? 事实上, 由于映射的复合满足结合律

$$g = g \circ \mathrm{id}_B = g \circ (f \circ h) = (g \circ f) \circ h = \mathrm{id}_A \circ h = h.$$

是唯一的(为什么?).

习题 1.2. 如果$f : A \to B$, $g : B \to C$均是一一对应, 则$g \circ f : A \to C$也是一一对应, 且$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

证明. 由**习题 1.1.(3)**可知, 只需验证

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = \mathrm{id}_C,$$

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = \mathrm{id}_A.$$

习题 1.4. 设$P(A)$是集合A的全部子集所构成的集族, $M(A)$为所有A到集合$\{0, 1\}$的映射所构成的集合. 试构造$P(A)$到$M(A)$的双射.

解. 任取$S \in P(A)$, 定义映射

$$f_S(x) := \begin{cases} 0, & x \in A \setminus S; \\ 1, & x \in S. \end{cases}$$

任取$f \in M(A)$, 定义集合$S_f := \{x \in A : f(x) = 1\}$. 则$S \mapsto f_S$与$f \mapsto S_f$互为逆映射. 当$A$是有限集时, $M(A)$中元素个数为$2^{|A|}$, 这是因为A中的任何一个元素的像只能为0或者1. 于是, $|P(A)| = |M(A)| = 2^{|A|}$, 这便证明了**习题 1.3.**

习题 1.5. 设X是无限集, Y是X的有限子集. 证明存在双射$X \setminus Y \to X$.

证明. 由于$X - Y$也是无限集, 它必然有可数子集S. 设$S := \{x_1, x_2, \cdots\}$, $Y := \{y_1, \cdots, y_n\}$. 容易构造$f : S \cup Y \to S$的双射如下

$$f(x) := \begin{cases} x_i, & x = y_i; \\ x_{n+i}, & x = x_i. \end{cases}$$

注意到, $X = (X \setminus (S \cup Y)) \cup (S \cup Y)$且$X \setminus Y = (X \setminus (S \cup Y)) \cup S$. 于是有双射$g : X \to X \setminus Y$

$$X\text{:}\ \boxed{X \setminus (S \cup Y)}\boxed{S}\boxed{Y} \to \boxed{X \setminus (S \cup Y)}\boxed{S}\ \text{:}X \setminus Y$$

$$g(x) := \begin{cases} f(x), & x \in S \cup Y; \\ x, & x \in X \setminus (S \cup Y). \end{cases}$$

请同学们自己写出f^{-1}与g^{-1}.

习题 1.9. 证明容斥原理.

证明. 尝试发现容斥原理. 由Venn图可知

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

由于集合的并满足结合律

$$\begin{aligned} |A \cup B \cup C| =& |(A \cup B) \cup C| = |A \cup B| + |C| - |(A \cup B) \cap C| \\ =& (|A| + |B| - |A \cap B|) + |C| - |(A \cap C) \cup (B \cap C)| \\ =& (|A| + |B| - |A \cap B|) + |C| - (|A \cap C| + |B \cap C| - |A \cap B \cap C|) \\ =& |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|. \end{aligned}$$

请同学们仿照计算$|A \cup B \cup C \cup D|$. 我们发现$|A_1 \cup \cdots \cup A_n|$总可以写成“1项和$-$2项和$+$3项和$-$4项和$+\cdots$”, 如何将这种规律转换成数学符号? 请同学们将容斥原理右侧的式子取$n = 2, 3, 4$展开体会. 结合以上计算心得, 用数学归纳法证明一般的容斥原理.

习题 1.6. 证明等价关系的三个条件是互相独立的, 也就是说, 已知任意两个条件不能推出第三个条件.

证明 举反例即可. 设$A = \{a, b, c\}$.

- $R_1 := \{(a,b),(a,a),(b,b),(c,c)\}$自反, 传递, 但不对称.
- $R_2 := \{(a,b),(b,a),(a,a),(b,b)\}$传递, 对称, 但不自反.
- $R_3 := \{(a,a),(b,b),(c,c),(a,b),(b,a),(b,c),(c,b)\}$自反, 对称, 但不传递.

习题 1.7. 设集合A中关系满足对称性和传递性, 且A中任意元素都和某元素有关系, 证明此关系为等价关系.

证明 设这个关系为R, 只需证明R满足自反性. 任取$a \in A$, 由条件知, 存在$b \in A$使得aRb. 由对称性知, bRa. 由传递性知, aRa.

习题 1.8. 设A, B是两个有限集合.

1. A到B的不同映射共有多少个?
2. A上不同的二元运算共有多少个?

解 (1) A中任意一个元素的像只有$|B|$种选择, 因此映射共$|B|^{|A|}$个.
(2) 二元运算是映射$A \times A \to A$, 共$|A|^{|A|^2}$个.

习题 1.13. $(-\frac{1}{2} + \mathrm{i}\frac{\sqrt{3}}{2})^3 = (\mathrm{e}^{\pm\frac{2\pi}{3}\mathrm{i}})^3 = 1$. $(1+\mathrm{i})^{4n} = (\sqrt{2}\mathrm{e}^{\frac{\pi}{4}\mathrm{i}})^{4n} = (-4)^n$.

习题 1.15. $|z - z_0| = r$.

习题 1.19. 证明如果复数z是实数α的n次方根, 则它的共轭$\bar{z}$也是α的n次方根.

证明 由于$\overline{z_1 \cdot z_2} = \bar{z_1} \cdot \bar{z_2}$, 故$\bar{z}^n = \overline{z^n} = \bar{\alpha} = \alpha$.

习题 1.20. $z \neq 1$时, 原方程可化为$\frac{(z+1)^n}{(z-1)^n} = -1 = \mathrm{e}^{(2k+1)\pi\mathrm{i}}$. 因此

$$\frac{z+1}{z-1} = \mathrm{e}^{\frac{2k+1}{n}\pi\mathrm{i}}.$$

解得$z=\frac{\mathrm{e}^{\frac{2k+1}{n}\pi\mathrm{i}}+1}{\mathrm{e}^{\frac{2k+1}{n}\pi\mathrm{i}}-1}$.

习题. 设X是一个集合, 令$S:=\{f:X\to X:f$是单射$\}$.

1. 证明S在复合运算下构成一个含幺半群.

2. 证明当X是有限集时, S在复合运算下构成一个群.

证明 (1) 幺元是恒等映射.

(2) X是有限集时, $|X|=|f(X)|$, 因此$f\in S$也是满射, 从而是双射. S中的元素都可逆, 构成一个群.

习题. 考察映射$\varphi:\mathbb{C}\to M_2(\mathbb{R})$.

$$\varphi(a+b\mathrm{i})=\begin{pmatrix}a&0\\0&a\end{pmatrix}+\begin{pmatrix}0&-b\\b&0\end{pmatrix}=\begin{pmatrix}a&-b\\b&a\end{pmatrix}.$$

经验证后发现,

$$\varphi((a+b\mathrm{i})+(c+d\mathrm{i}))=\varphi(a+b\mathrm{i})+\varphi(c+d\mathrm{i}),$$

$$\varphi((a+b\mathrm{i})(c+d\mathrm{i}))=\varphi(a+b\mathrm{i})\varphi(c+d\mathrm{i}).$$

定义矩阵$\begin{pmatrix}a&b\\c&d\end{pmatrix}$的转置为$\begin{pmatrix}a&c\\b&d\end{pmatrix}$. 验证$\varphi(z)$和$\varphi(\bar{z})$互为转置.

考察映射$\psi:\mathbb{H}\to M_2(\mathbb{C})$.

$$\begin{aligned}\psi(a+b\mathrm{i}+c\mathrm{j}+d\mathrm{k})&=\begin{pmatrix}a&0\\0&a\end{pmatrix}+\begin{pmatrix}0&-b\\b&0\end{pmatrix}+\begin{pmatrix}0&c\mathrm{i}\\c\mathrm{i}&0\end{pmatrix}+\begin{pmatrix}-d\mathrm{i}&0\\0&d\mathrm{i}\end{pmatrix}\\&=\begin{pmatrix}a-d\mathrm{i}&-b+c\mathrm{i}\\b+c\mathrm{i}&a+d\mathrm{i}\end{pmatrix}.\end{aligned}$$

ψ与φ是否具有类似的性质? 借助ψ理解$\mathbb{H}$的运算.

习题. 设α是$x^3-x-1=0$的一个根, 则$\mathbb{Q}[\alpha]$是一个域.

证明. 设$f, g \in \mathbb{Q}[x]$, 则$f(\alpha), g(\alpha) \in \mathbb{Q}[\alpha]$. 注意到

$$f(\alpha) = g(\alpha) \Longleftrightarrow f \equiv g \mod x^3 - x - 1.$$

由于$x^3 - x - 1$在$\mathbb{Q}[x]$不可约, 由Bezout定理, 任取$a \neq 0$, 存在$h \in \mathbb{Q}[x]$使得

$$(a + bx + cx^2)h \equiv 1 \mod x^3 - x - 1.$$

因此, 在$\mathbb{Q}[\alpha]$中, $(a + b\alpha + c\alpha^2)h(\alpha) = 1$.

定义 自然数集之间的同构是一个双射 $f:(\mathbb{N},0,s)\to(\mathbb{N}',0',s')$，满足 $f(0)=0'$ 且 $f(sx)=s'f(x)\quad\forall x\in\mathbb{N}$.

定理 自然数集在同构意义下唯一。

Proof. 设 $\mathbb{N}=\{0=\emptyset,\{\emptyset\},\{\emptyset\cup\{\emptyset\}\},\cdots\}$，$(\mathbb{N}',0',s')$ 是任一自然数集，定义 f 如下：

$f(0)=0'$ 假设 $f(x)\in\mathbb{N}$, 则定义 $f(sx)=s'f(x)$

令 $M=\{x\in\mathbb{N}|f$ 在 x 上有定义$\}$ 易用归纳公理证明 $M=\mathbb{N}$，即 f 良定。

下面证明 f 是单射且满射：

“满射”，考察 $\mathrm{Im}f\subseteq\mathbb{N}'$. 显然 $0'\in\mathbb{N}'$，若 $y\in\mathbb{N}'$，即存在 $x\in\mathbb{N}$ 使得 $f(x)=y$，则 $f(sx)=s'f(x)=s'y$，因此 $s'y\in\mathbb{N}'$，由归纳公理知 $\mathrm{Im}f=\mathbb{N}'$，即 f 是满射。

”单射”，考察 $A=\{y\in\mathbb{N}'|\ |f^{-1}(y)|=1\}$. 若 $|f^{-1}(0')|>1$，则存在 $0\neq x\in\mathbb{N}$ 使得 $f(x)=0'$，因此存在 $u\in\mathbb{N}$ 使得 $su=x$，因此 $0'=f(x)=f(su)=s'f(u)$，这与 $0'$ 不是任何元素的后继矛盾，故 $0'\in A$. 若 $y\in A$，设 $f(x)=y$，我们计算 $|f^{-1}(s'y)|$，若 $|f^{-1}(s'y)|>1$，则存在 $sx\neq v\in\mathbb{N}$ 使得 $f(v)=s'y$，显然 $v\neq 0$，故存在 $w\in\mathbb{N}$ 使得 $sw=v$ 因此 $s'f(w)=f(sw)=f(v)=s'y=s'f(x)$，因此由 s' 是单射知 $f(w)=y=f(x)$，再由 $y\in A$ 知 $w=x$，但这与 $sx\neq v=sw=sx$ 矛盾，故 $|f^{-1}(s'y)|=1$，即 $sy\in A$，由归纳公理知 $A=\mathbb{N}'$，故 f 是单射。 □

习　题　课

代数学基础

2020年11月8日

目录

整除

- 证明集合 $A = B$ 的常用手段是去证明 $A \subseteq B$ 且 $B \subseteq A$.
- 证明整数 $a = b$ 的常用手段是去证明 $a \mid b$ 且 $b \mid a$.

例题

Example

1. 设 m 是正整数且 a, b 是正奇数, 则

$$(m^a + 1, m^b + 1) = m^{(a,b)} + 1.$$

2. 设 m, a, b 是正整数且 $m > 1$, 则

$$(m^a - 1, m^b - 1) = m^{(a,b)} - 1.$$

证法一: 辗转相除法. 不妨设 $a > b$.

$$\begin{aligned}(m^a + 1, m^b + 1) =& (m^a - m^b, m^b + 1) = (m^{a-b} - 1, m^b + 1)\\ =& (m^{a-b} + m^b, m^b + 1).\end{aligned}$$

例题

- 若 $a-b>b$, 则 $(m^a+1, m^b+1)=(m^{a-2b}+1, m^b+1)$.
- 若 $a-b\leq b$, 则$(m^a+1, m^b+1)=(m^{2b-a}+1, m^b+1)$.

用 $a-2b$ 或 $2b-a$ 代替 a 重复上述讨论, 由辗转相除法可得结论.

注意: 每一次得到的幂次均为奇数, 这在做辗转相除的过程中, 以及最后一步得到结论的过程中都是非常关键的!

例题

证法二: 利用阶的性质.

记 $d := (m^a + 1, m^b + 1)$, $k := a/(a,b)$, $l := b/(a,b)$.

当 n 为奇数时, 我们有

$$x^n + y^n = (x+y)(x^{n-1} - x^{n-2}y + \cdots - xy^{n-2} + y^{n-1}) \qquad (1)$$

注意到 $m^a + 1 = \left(m^{(a,b)}\right)^k + 1$, $m^b + 1 = \left(m^{(a,b)}\right)^l + 1$. 由 (1) 式知

$$m^{(a,b)} + 1 \mid m^a + 1, \quad m^{(a,b)} + 1 \mid m^b + 1.$$

故 $m^{(a,b)} + 1 \mid d$.

例题

另一方面, 由 $d \mid m^a + 1$ 与 $d \mid m^b + 1$ 知

$$m^a \equiv -1 \mod d, \quad m^b \equiv -1 \mod d. \tag{2}$$

设 $l := \min\{k \in \mathbb{Z}_+ : m^k \equiv 1 \mod d\}$ 为 m 模 d 的阶.

$d = 2$ 时, $-1 \equiv 1 \mod d$. 因此, $l \mid (a, b)$. 故

$$m^{(a,b)} \equiv -1 \mod d.$$

$d \neq 2$ 时, 由 (2) 知 $l \nmid (a, b)$. 但

$$m^{2a} \equiv 1 \mod d, \quad m^{2b} \equiv 1 \mod d. \tag{3}$$

于是, $l \mid 2(a, b)$. 设 $(a, b) = ql + r$, 其中 $0 < r < l$, 则 $l \mid 2r$.

故 $l = 2r$. 于是

$$m^{(a,b)} \equiv m^{l/2} \equiv m^{kl/2} \equiv m^a \equiv -1 \mod d.$$

其中, $k := a/(a, b)$ 是奇数. 综上所述, $d \mid m^{(a,b)} + 1$.

课后题

习题 3.3.

设 m, n 为正整数, m 是奇数. 证明 $(2^m - 1, 2^n + 1) = 1$.

证法一: 记 $d := (2^m - 1, 2^n + 1)$, 则 $d \mid 2^m - 1$ 且 $d \mid 2^n + 1$.

注意到 $((2^m)^n - 1, 2^m - 1) = 2^m - 1$, $((2^n)^m + 1, 2^n + 1) = 2^n + 1$.

故 $2^m - 1 \mid 2^{mn} - 1$ 且 $2^n + 1 \mid 2^{mn} + 1$. 于是

$$d \mid (2^{mn} - 1, 2^{mn} + 1) = 1.$$

课后题

证法二: 记 $d := (2^m - 1, 2^n + 1)$, 则 $d \mid 2^m - 1$ 且 $d \mid 2^n + 1$.

$$2^m \equiv 1 \mod d \implies 2^{mn} \equiv 1^n \mod d, \tag{4}$$

$$2^n \equiv -1 \mod d \implies 2^{mn} \equiv (-1)^m \mod d. \tag{5}$$

由于 m 是奇数, 结合 (4) 和 (5) 知, $-1 \equiv 1 \mod d$. 故 $d \mid 2$.
又因为 d 是奇数, 从而 $d = 1$.

课后题

习题 3.4.

设 n 为正整数, 证明

1. $(a^n, b^n) = (a, b)^n$
2. 设 a, b 是互素的正整数, $ab = c^n$, 则 $a = (a, c)^n$, $b = (b, c)^n$.

证明: (1) 记 $d := (a, b)$, 则 $d^n \mid a^n$ 且 $d^n \mid b^n$, 故 $d \mid (a^n, b^n)$.

另一方面, 记 $k := a/d$, $l := b/d$, 则 $(k, l) = 1$. 此时

$$a^n = k^n d^n, \quad b^n = l^n d^n.$$

由 Bézout 定理知, 存在整数 x, y 使得

$$xk + yl = 1 \tag{6}$$

课后题

对 (6) 式两端同时 n 次方可知

$$x^n k^n + \big((xk)^{n-1} y + (xk)^{n-2} y^2 l + \cdots + xky^{n-1} l^{n-2} + y^n l^{n-1}\big) l = 1.$$

由 Bézout 定理知, $(k^n, l) = 1$. 类似可得

$$(k^n, l^n) = 1.$$

由 Bézout 定理知, 存在整数 r, s 使得

$$rk^n + sl^n = 1 \tag{7}$$

对 (7) 式两端同乘 d^n 知

$$ra^n + sb^n = d^n. \tag{8}$$

课后题

(8) 式说明 d^n 在 a^n 和 b^n 生成的理想中. 由课本定理 3.6 知, 此理想即为 (a^n, b^n) 生成的主理想. 故 $(a^n, b^n) \mid d^n$.

(2) 由 (1) 知, $(a, c)^n = (a^n, c^n) = (a^n, ab) = a$.

目录

二元线性不定方程

Definition

设 a, b, c 是整数, 形如

$$ax + by = c \tag{9}$$

的不定方程称为一个二元线性不定方程.

1. 若 $c = 0$, 称该方程为齐次的.
2. 若 $c \neq 0$, 称该方程为非齐次的.

二元线性齐次不定方程的解集具有以下结构:

Theorem

设 $a = a_0(a, b)$, $b = b_0(a, b)$, $c = 0$, 则方程 *(9)* 的全部解为

$$(x, y) := (b_0 t, -a_0 t), \quad t \in \mathbb{Z}. \tag{10}$$

二元线性不定方程

证明: 显然, (10) 式是方程 (9) 的解.

另一方面, 方程 (9) 的任何一组整数解都是过原点的直线

$$ax + by = 0$$

上的整点. 这些整点用直线的参数方程表示即为 (10) 式.

二元线性不定方程

二元线性非齐次不定方程的解集具有以下结构:

Theorem

设 $a = a_0(a,b)$, $b = b_0(a,b)$, 则方程 *(9)* 的全部解为

$$(x,y) := (x_0 + b_0 t, y_0 - a_0 t), \quad t \in \mathbb{Z}. \tag{11}$$

其中, (x_0, y_0) 是方程 *(9)* 的任意一组特解. 特别地, 可通过辗转相除法得到方程 *(9)* 的一组特解 *(*课本例 *3.9)*.

证明: 显然, (11) 式是方程 (9) 的解.

另一方面, 若 (x_1, y_1) 和 (x_2, y_2) 是方程 (9) 的两个解, 则

$$(x_1 - x_2, y_1 - y_2)$$

是相应齐次方程的解.

课后题

习题 3.6.

设 a, b 为正整数且 $(a, b) = 1$. 考虑方程

$$ax + by = n. \tag{12}$$

证明:

1. 当 $n > ab - a - b$ 时, 方程 (12) 有非负整数解.
2. 当 $n = ab - a - b$ 时, 方程 (12) 没有非负整数解.

证明: 方程 (12) 的解为

$$(x, y) := (nx_0 + bt, ny_0 - at), \quad t \in \mathbb{Z}.$$

其中, (x_0, y_0) 为方程 $ax + by = 1$ 的一组解.

课后题

1. $a = 1$ 时, (x_0, y_0) 可取 $(1, 0)$. 此时, $ab - a - b = -1$, 命题成立.
2. $b = 1$ 时, 类似.
3. $a > 1$ 且 $b > 1$ 时, 不妨设 $a \geq b$, 则

$$ab - a - b = a(b - 1) - b \geq a - b \geq 0.$$

此时, x_0 和 y_0 不可能全为正整数.

若 $n > ab - a - b$, 则 $n > 0$. 不妨设 $x_0 \leq 0$, 则 $nx_0 \leq 0$. 记

$$k := \min\{t : nx_0 + bt \geq 0\}.$$

我们证明: $ny_0 - ak \geq 0$. 否则 $ny_0 - ak \leq -1$, 即 $k \geq (1 + ny_0)/a$.

课后题

此时

$$\begin{aligned} nx_0 + b(k-1) \geq & nx_0 + b\left(\frac{1+ny_0}{a} - 1\right) && (13)\\ = & \frac{1}{a}(anx_0 + any_0 + b - ab) && (14)\\ = & \frac{1}{a}(n + b - ab) > -1. && (15) \end{aligned}$$

故 $k-1 \in \{t : nx_0 + bt \geq 0\}$. 这与 k 的最小性矛盾.

若 $n = ab - a - b$, 则 $x = b - 1 - b(y+1)/a$. 由于 $(a, b) = 1$ 且 x 是整数, 故 $a \mid y+1$. 设 $y + 1 = ad$. 若 $x = b - 1 - bd \geq 0$, 则 $d \leq 0$. 此时 $y = ad - 1 \leq -1$.

课后题

习题 3.7.

设 $n > 1$ 为整数, 如果对于任何整数 m, 或者 $n \mid m$ 或者 $(n, m) = 1$, 证明 n 是素数.

证明: 若 n 不是素数, 则存在整数 a, b 使得 $n \mid ab$ 但 $n \nmid a$, $n \nmid b$. 由 n 的性质知 $(n, a) = 1 = (n, b)$. 上述两个 Bézout 等式相乘可得 $(n, ab) = 1$. 这与 $n \mid ab$ 矛盾.

习题 3.8.

设 $n > 2$ 为整数, 证明 n和 $n!$ 之间必有素数.

证明: 由于 $2, \cdots, n$ 都不是 $n! - 1$ 的因子, 故 $n + 1, \cdots, n! - 1$ 之间必有 $n! - 1$ 的素因子.

目录

课后题

习题 3.9.

1. 设 m 为正整数, 证明: 如果 2^m+1 为素数, 则 m 为 2 的方幂.
2. 对 $n \in \mathbb{N}$, 记 $F_n := 2^{2^n}+1$. 这称为费马数. 证明: 若 $m > n$, 则 $F_n \mid F_m - 2$.
3. 证明: 如果 $m \neq n$, 则 $(F_m, F_n) = 1$. 由此证明素数无穷多.

证明: (1) 若 m 不是 2 的方幂, 则存在不为 1 的正奇数 s 使得 $m = 2^r s$. 考虑

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}).$$

令 $a = 2^{2^r}$, $b = -1$, $n = s$, 则 $2^{2^r}+1$ 整除 $2^{2^r s} - (-1)^s = 2^m + 1$.

(2) $F_m - 2 = (F_n - 1)^{2^{m-n}} - 1 \equiv (-1)^{2^{m-n}} - 1 \mod F_n$.

课后题

事实上: $F_n = F_0F_1\cdots F_{n-1}+2$.

1. $n=1$ 时, $F_0+2=3+2=5=F_1$.
2. 设 $F_n = F_0F_1\cdots F_{n-1}+2$
3. $F_0\cdots F_n+2=(F_n-2)F_n+2=(2^{2^n}-1)(2^{2^n}+1)+2=F_{n+1}$.

(3) 不妨设 $m>n$, 由 (2) 知, $F_m = dF_n+2$. 由辗转相除法知

$$(F_m,F_n)=(2,F_n)=1.$$

事实上: $F_m = F_{m-1}+2^{2^{m-1}}F_0\cdots F_n\cdots F_{m-2}$.

由于 (F_m,F_n) 整除 F_m 和 F_n, 因此也整除 F_{m-1} 和 $F_0\cdots F_{m-1}$.

于是, $(F_m,F_n)\mid F_m-F_0\cdots F_{m-1}=2$. 但 (F_m,F_n) 是奇数.

若素数只有 k 个, 由抽屉原理, F_n 与 F_{n+k} 之间, 必有不互素的.

课后题

习题 3.10.

1. 设 m, n 都是大于 1 的整数, 证明: 如果 $m^n - 1$ 是素数, 则 $m = 2$ 且 n 是素数.
2. 设 p 是素数, 记 $M_p := 2^p - 1$, 这称为梅森数. 证明: 如果 p, q 是不同的素数, 则 $(M_p, M_q) = 1$.

证明: (1) 若 $m \neq 2$ 则 $m - 1 \mid m^n - 1$.

当 $m = 2$ 时, 若 $n = pq$ 不是素数, 则 $2^p - 1 \mid (2^p)^q - 1$.

(2) $(M_p, M_q) = M_{(p,q)} = M_1 = 1$.

课后题

习题 3.11.

设 a, b 是整数且 $a \neq b$, n 是正整数. 如果 $n \mid a^n - b^n$, 则

$$n \mid \frac{a^n - b^n}{a - b}.$$

证明: $n = p$ 是素数时, 若 $p \nmid a - b$, 则命题显然成立.

若 $p \mid a - b$, 则 $a \equiv b \mod p$. 故

$$\frac{a^p - b^p}{a - b} \equiv pa^{p-1} \equiv 0 \mod p.$$

$n = pm$, p 是素数时. 记 $A := a^m$, $B := b^m$, 则

$$\frac{a^n - b^n}{a - b} = \frac{A^p - B^p}{A - B} \frac{a^m - b^m}{a - b}.$$

对 m 与 $(a^m - b^m)/(a - b)$ 继续做类似的事情即可.

目录

课后题

习题 3.12.

设 n 是正整数. 证明:

1. n 为完全平方数的充要条件是 $\sigma_0(n)$ 为奇数.
2. $\sigma_0(n) \leq 2\sqrt{n} + 1$.
3. n 的正约数之积为 $n^{\sigma_0(n)/2}$.

证明: (1) 注意到, n 是完全平方数当且仅当 $v_{p_i}(n)$ 都是偶数. 而

$$\sigma_0(n) = \prod_{i=1}^{s} \big(v_{p_i}(n) + 1\big).$$

(2) $\sigma_0(n) = A + B \leq 2A = 2\sqrt{n}$, 其中

$$A := \sum_{\substack{1 \leq d \leq \sqrt{n} \\ d \mid n}} 1, \quad B := \sum_{\substack{\sqrt{n} < d \leq n \\ d \mid n}} 1.$$

课后题

(3) 设 $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, 则存在如下集合的双射

$$\{d \in \mathbb{N} : d \mid n\} \longleftrightarrow \{(a_1, \cdots, a_s) \in \mathbb{N}^s : 0 \leq a_i \leq \alpha_i,\ 1 \leq i \leq s\}.$$

注意到, 左边集合的元素相乘对应着右边集合的元素相加.

因此, 左边集合中所有元素的乘积对应着

$$\sum_{i=1}^{s} \sum_{a_i=0}^{\alpha_i} (a_1, \cdots, a_s) = \left(\frac{\alpha_i}{2} \prod_{i=1}^{s} (1 + \alpha_i) \right)_{1 \leq i \leq s} = (\alpha_i \sigma_0(n)/2)_{1 \leq i \leq s}.$$

这个元素即为 $n^{\sigma_0(n)/2}$.

目录

有限域上的不可约多项式

Definition

设 p 是素数, 则 $\mathbb{Z}/p\mathbb{Z}$ 是一个域, 称为 p 元有限域, 记为 $\mathbb{F}_p$. 用 $N_p(d)$ 表示 $\mathbb{F}_p[x]$ 中的 d 次首项系数是一的不可约多项式的个数.

Example

考察 $\mathbb{F}_2[x]$ 中的首一不可约多项式.

1. $d=1$ 时, 全部的首一多项式为 x 和 $x+1=x-1$, 都不可约.
2. $d=2$ 时, 全部的首一多项式为

$$x^2, \quad x^2+1=(x+1)^2, \quad x^2+x+1, \quad x^2+x=x(x+1).$$

只有 x^2+x+1 不可约.

特别地, $x(x+1)(x^2+x+1)=x^4+x=x^{2^2}-x$.

有限域上的不可约多项式

一般地, 我们有如下定理:

Theorem

设 $n \geq 1$, 在 $\mathbb{F}_p[x]$ 中

$$x^{p^n} - x = \prod_{d|n} \prod_{\deg f = d} f(x). \tag{16}$$

其中, $f(x) \in \mathbb{F}_p[x]$ 首一不可约.

对 (16) 式两端同取 deg 可得

Corollary

$$p^n = \sum_{d|n} dN_p(d).$$

有限域上的不可约多项式

设 $g(n) := p^n$, $f(d) := dN_p(d)$. 由习题 3.15 莫比乌斯反演公式知

Theorem

$$N_p(n) = \frac{1}{d}\sum_{d|n}\mu(d)p^{n/d}$$

Example

$$N_p(2) = \frac{1}{2}(p^2 - p), \quad N_p(2) = \frac{1}{3}(p^3 - p),$$

$$N_p(12) = \frac{1}{12}(p^{12} - p^6 - p^4 + p^2).$$

目录

单位群

Definition

设 R 是含幺交换环, 称 $r \in R$ 为 R 中的单位, 若存在 $r' \in R$ 使得

$$rr' = 1_R.$$

R 中所有的单位在乘法运算下构成一个群 $R^\times$, 称为 R 的单位群.

Example

$$\mathbb{Z}^\times = \{1, -1\} \cong \mathbb{Z}/2\mathbb{Z}$$

范映射

Definition

设 d 是无平方因子的整数, 定义如下的范映射 $N : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}$

$$N(a + b\sqrt{d}) := a^2 - db^2.$$

Lemma

N 是含幺乘法半群之间的同态, 即

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

Corollary

若 $\alpha = a + b\sqrt{d} \in \left(\mathbb{Z}[\sqrt{d}]\right)^\times$, 则 $N(\alpha) \in \mathbb{Z}^\times$, 即

$$a^2 - db^2 = \pm 1. \tag{17}$$

佩尔方程

Definition

方程 (17) 称为佩尔方程.

可以看出, 求解佩尔方程与计算 $\left(\mathbb{Z}[\sqrt{d}]\right)^{\times}$ 有密切联系.

事实上, 我们有如下两个定理.

Theorem (Lagrange)

设 d 是无平方因子的正整数, 佩尔方程 $a^2 - db^2 = 1$ 有非平凡解.

Theorem

$\alpha = a + b\sqrt{d} \in \left(\mathbb{Z}[\sqrt{d}]\right)^{\times}$ 当且仅当 (a, b) 是方程 *(17)* 的解.

高斯整数环的单位群

Example

考察高斯整数环 $\mathbb{Z}[\sqrt{-1}]$.

- $a^2+b^2=1$ 的整数解为 $(1,0),(-1,0),(0,1),(0,-1)$.
- $a^2+b^2=-1$ 无整数解.

因此, $\left(\mathbb{Z}[\sqrt{-1}]\right)^\times=\{\pm 1,\pm\sqrt{-1}\}\cong\mathbb{Z}/4\mathbb{Z}$.

11.22 习题课

4.1 连续 n 个整数中恰有一个被 n 整除

Sol: 只需证这 n 个数构成模 n 的一个完系

不妨设为 $m, m+1, \cdots, m+n-1$ 而易见 $m+i \not\equiv m+j \bmod n \quad 0 \le i \ne j < n$

即两两不在同一剩余类中，又恰有 n 个数，故构成模 n 完系

4.2 $T(n) \equiv n \bmod 11$

Sol: 设 $n = a_m \cdots a_0 = \sum_{i=0}^{m} a_i \times 10^i \quad (a_m \ne 0,\ 0 \le a_i \le 9)$

则有 $n \equiv \sum_{i=0}^{m} (-1)^i a_i = T(n) \bmod 11$

4.4 较为简单，这里只做其中一道： $n^2 \equiv 0, 1 \bmod 3$

这由 $n \equiv 0, \pm 1 \bmod 3$ 立得

此题很多同学将 n 设为 $n = 3k, 3k+1, 3k+2$ 再将 n^2 展开来做

这实际就是 $n \equiv 0, \pm 1 \bmod 3$，大家现在有模算术这个工具，就尽量不要回到原始的做法中去

4.5 a 奇，$n \in \mathbb{N}_+$ 则 $a^{2^n} \equiv 1 \bmod 2^{n+2}$

Sol: 归纳： $n=1$ ： $a \equiv \pm 1, \pm 3 \bmod \underset{\parallel}{2^3} \Rightarrow a^2 \equiv 1 \bmod 2^3$
8

设对 $n-1$ 成立，即 $a^{2^{n-1}} \equiv 1 \bmod 2^{n+1}$

依定义 $a^{2^{n-1}} = 2^{n+1} t + 1$

则 $a^{2^n} = (a^{2^{n-1}})^2 = 2^{2n+2} t^2 + 2^{n+2} t + 1 \Rightarrow a^{2^n} \equiv 1 \bmod 2^{n+2}$

或平方差公式： $a^{2^n} - 1 = (a^{2^{n-1}} + 1)(a^{2^{n-1}} - 1) = \cdots$

$$= \underbrace{\prod_{i=1}^{n-1} (a^{2^{n-i}} - 1)}_{\text{有因子 } 2^{n-1}} \underbrace{(a^{2^1} - 1)}_{\text{有因子 } 2^3 \text{（由上）}}$$

由 a 奇 $\Rightarrow$

4.6 (1) $n\geq 3$, $\varphi(n)$ 为偶数

Sol: 直接利用 $\varphi(n)$ 的表达式：设 $n=p_1^{\alpha_1}\cdots p_s^{\alpha_s}$，则 $\varphi(n)=p_1^{\alpha_1-1}(p_1-1)\cdots$

若 n 有奇素因子 p_1，则 $2\mid p_1-1\mid \varphi(n)$

若 $n=2^s$，由 $n\geq 3$ 知 $s\geq 2$

则 $2\mid 2^{s-1}\mid \varphi(n)$

或配对法：由 $n\geq 3$，对 $1\leq k\leq n$，有 $(n,k)=1 \Leftrightarrow (n,n-k)=1$

将 k 与 $n-k$ 配对

但需有 $k\neq n-k$，保证它们两两不同

若 $k=n-k$，则 $n=2k$，$(n,k)=k=1 \Rightarrow n=2$，不可能

由此知 $\varphi(n)$ 偶

(2) $\sum\limits_{\substack{1\leq k\leq n\\(k,n)=1}} k=\frac{1}{2}n\varphi(n)$，其中 $n\geq 2$

Sol: $n=2$ 时，显然

$n\geq 3$，仍作配对：$\sum\limits_{\substack{1\leq k\leq n\\(k,n)=1}}[k+(n-k)]=2\sum\limits_{\substack{1\leq k\leq n\\(k,n)=1}} k$

$=$

$n\varphi(n)$

4.7 $m,n\in\mathbb{N}_+$，$m=nt$，则 $\{x\in\mathbb{Z}: x\equiv r \bmod n\}=\bigsqcup\limits_{i=0}^{t-1}\{x\in\mathbb{Z}: x\equiv r+in \bmod m\}$

(易见它们确实两两无交)

Sol: 右 $\subset$ 左 显然

左 $\subset$ 右：$\forall x\equiv r \bmod n$，有 $x-r=nl$

考虑 $l\equiv i \bmod t$，$0\leq i<t$

$\Downarrow$

$nl\equiv ni \bmod nt$

$\Rightarrow x-r\equiv nl\equiv ni \bmod m$

4.8 直接给出结果： $x \equiv 15 \bmod 23$
$x \equiv 18 \bmod 37$

（请大家化简为 $x \equiv a \bmod m$ 其中 $|a| < m$）

一般地，考虑 $ax \equiv b \bmod m$ 有解 $\Leftrightarrow (a,m) \mid b$

记 $d = (a,m)$

则 $ax \equiv b \bmod m \Leftrightarrow \frac{a}{d} x \equiv \frac{b}{d} \bmod \frac{m}{d}$，再求 $\frac{a}{d}$ 模 $\frac{m}{d}$ 的逆 c

$\Leftrightarrow x \equiv \frac{b}{d} \cdot c \bmod \frac{m}{d}$ （即 $\frac{a}{d} \cdot c \equiv 1 \bmod \frac{m}{d}$）

$\overset{4.7}{\Leftrightarrow} x \equiv \frac{b}{d} \cdot c + i\frac{m}{d} \bmod m$, $0 \le i < d$

4.10 只需注意到 $p\bar{a} = \overline{pa}$
$n\bar{a} = \overline{na}$

4.11 Wilson： p 素，则 $(p-1)! \equiv -1 \bmod p$

Sol： 实际上就是把 $\mathbb{F}_p^\times$ 中的所有元素乘法

而 $\mathbb{F}_p^\times$ 是一个乘法群，可以考虑任一元素 x 与其逆元配对

这样它们乘起来 $x \cdot x^{-1} = 1$，就会“消失”在式子中

故只需要看 $x = x^{-1}$ 的元素，这样的元素在式子中只出现一次，故不会被消去

Rmk：这里的 1 实际上指 $\bar{1}$

$x = x^{-1} \Leftrightarrow x^2 = 1 \Leftrightarrow x^2 - 1 = 0$

$\Leftrightarrow p \mid x^2 - 1 = (x+1)(x-1)$

$\Leftrightarrow p \mid x+1$ or $p \mid x-1 \Leftrightarrow x = 1$ or $x = -1$

（同时成立 $\Leftrightarrow p = 2$）

故 $(p-1)! \equiv -1 \bmod p$

4.12 p 奇素数，若 $\{\bar{r}_1, \dots, \bar{r}_{p-1}\} = \{\bar{r}_1', \dots, \bar{r}_{p-1}'\} = \{\bar{1}, \dots, \overline{p-1}\}$

则 $\{\overline{r_1 r_1'}, \dots, \overline{r_{p-1} r_{p-1}'}\} \neq \{\bar{1}, \dots, \overline{p-1}\}$

反证：若相等，由 4.11 $r_1 r_1' \cdots r_{p-1} r_{p-1}' \equiv -1 \bmod p$

但同时有 $r_1 \cdots r_{p-1} \equiv -1 \bmod p$，$r_1' \cdots r_{p-1}' \equiv -1 \bmod p$

$\Rightarrow r_1 r_1' \cdots r_{p-1} r_{p-1}' \equiv 1 \bmod p$

$\Rightarrow 1 \equiv -1 \bmod p \Rightarrow p = 2$，矛盾

4.13 $\varphi(360)=96$, $\varphi(429)=240$

4.15 $m,n\in\mathbb{N}_+$, $(m,n)=1$, 则 $m^{\varphi(n)}+n^{\varphi(m)}\equiv 1 \mod mn$

Sol: 分别由 Euler 定理 $\begin{cases} m^{\varphi(n)}+n^{\varphi(m)}\equiv n^{\varphi(m)}\equiv 1 \mod m \\ m^{\varphi(n)}+n^{\varphi(m)}\equiv m^{\varphi(n)}\equiv 1 \mod n \end{cases}$

$\Downarrow (m,n)=1$

$m^{\varphi(n)}+n^{\varphi(m)}\equiv 1 \mod mn$

4.16 $(a,10)=1$, 则 $a^{20}\equiv 1 \mod 100$

Sol: $(a,10)=1 \Rightarrow \begin{cases}(a,2^2)=1\\(a,5^2)=1\end{cases}$ Euler Thm $\Rightarrow$ $a^{\varphi(2^2)}\equiv a^2\equiv 1 \mod 4 \Rightarrow a^{20}\equiv 1 \mod 4$; $a^{\varphi(5^2)}\equiv a^{20}\equiv 1 \mod 25$ $\Rightarrow (4,25)=1 \Rightarrow a^{20}\equiv 1 \mod 100$

2. $x\in G$, $o(x)<\infty$ 利用以下事实: $\left(x^n=1 \overset{\forall n}{\Leftrightarrow} y^n=1\right) \Rightarrow o(x)=o(y)$

因为 若 $x^n=1\Rightarrow y^n=1$ 则 $o(y)\mid o(x)$

对称地 $o(x)\mid o(y)$

题目比较简单, 就不一一验证了

只看(3): $o(xy)=o(yx)$; 设 $o(xy)=n$

则 $(xy)^n=\underbrace{xy\,xy\cdots xy}_{n-1\text{个}yx}\,xy=1 \Rightarrow \underbrace{yx\cdot yx\cdots yx}_{n\text{个}yx}\cdot y=y$ (利用一个 y)

消去 y 即可

3. $gh=hg$, 则 $o(gh)\mid [o(g),o(h)]$ (所有限)

Sol: 利用 $x^n=1\Rightarrow o(x)\mid n$ 即可

若 $(o(g),o(h))=1$ 则有 $o(gh)\mid o(g)o(h)$

考虑 $(gh)^{o(gh)o(g)}=1 \Rightarrow o(h)\mid o(gh)o(g) \Rightarrow o(h)\mid o(gh)$ ($(o(h),o(g))=1$)

$h^{o(gh)o(g)}$

同理 $o(g)\mid o(gh)$

或还可利用: 若 $o(x)=n$, 则 $o(x^k)=\frac{n}{(n,k)}$: $(gh)^{o(gh)}=1 \Rightarrow g^{o(gh)}=(h^{-1})^{o(gh)}$

阶为 $\frac{o(g)}{(o(g),o(gh))}=\frac{o(h)}{(o(h),o(gh))}$ ($(o(h),o(g))=1$)

$\Rightarrow o(h)o(g)\mid o(gh)$

再整理上式即可

一、回顾群、群同构的概念

群 { 集合 G
满足某些条件的二元运算 $\cdot : G \times G \to G$ { (i) 结合律
(ii) 单位元
(iii) 逆元

群的代数结构具体来讲就是它的二元运算

什么时候可以把两个群视作一样的？

它们的代数结构应该保持一致

这种一致性通过一个映射来连接、体现

让我们自己来给出这样的映射的定义，应该从哪些方面考虑？

设 G、H 为群，

定义：$f: G \to H$ 称为同构，若它满足：

$(G, \cdot_G)$
$(H, \cdot_H)$

I. 集合层面：双射

II. 代数结构层面：保持二元运算：$f(a \cdot_G b) = f(a) \cdot_H f(b)$ (*)

(*') { 结合律：这是自动满足的
单位元：$f(1_G) = 1_H$
逆元：$f(a^{-1}) = (f(a))^{-1}$

我们可以如此给出同构的定义，而仔细考虑可以发现 (*) ⇒ (*')

故在定义中我们可以略去 (*')

若两个群同构，我们是无法从二元运算的角度说出它们的区别的

大家遇到其他的代数结构（环、模、线性空间、赋范空间、内积空间等）也可以这样去考虑其同构的定义（即保持其代数结构）

二、关于循环群的一个命题

• 设群 G 的阶为 n，则 G 是循环群 $\Leftrightarrow$ $d\mid n$，至多存在一个 d 阶子群

Sol: $\Rightarrow$ 是已经证明过的，大家可以看教材推论 6.20，一个抽象但简洁的证明

$\Leftarrow$ 我们对 G 进行如下划分

$$G=\bigsqcup_{1\le d\mid n} S_d \qquad S_d:=\{x\in G: o(x)=d\}$$

即按元素的阶划分

只需证 $S_n\neq\varnothing$ 即可：

对 $\forall d$，若 $S_d\neq\varnothing$，则对 $\forall g\in S_d$

$\langle g\rangle$ 为 G 的 d 阶子群

由条件，G 中若存在 d 阶子群则唯一；若存在，记其为 H_d

故对 $\forall g\in S_d$，有 $g\in\langle g\rangle=H_d$（d 阶循环群）

即 $S_d\subseteq H_d\cong Z_d$　Z_d 中 d 阶元个数为 $\varphi(d)$

$\Rightarrow H_d$ 中 d 阶元个数也为 $\varphi(d)\Rightarrow |S_d|\le\varphi(d)$

则由 $G=\bigsqcup_{d\mid n} S_d$，有 $n=|G|=\sum_{1\le d\mid n}|S_d|\le\sum_{1\le d\mid n}\varphi(d)=n$

$\Rightarrow |S_d|=\varphi(d)$ 特别的，$|S_n|=\varphi(n)\ge 1$，即 $S_n\neq\varnothing$

应用：• 设 k 为域，$G\le k^\times=k-0_k$，若 $|G|<\infty$，则 G 是循环群

Sol: 对 $\forall d\mid|G|$，若 G 有 d 阶子群，记其为 H_d

则对 $\forall h\in H_d$，有 $h^d=1_k\Rightarrow h$ 是多项式 x^d-1_k 的根

即 H_d 中所有元素都是 x^d-1 的根，但 x^d-1 在 k 上至多有 d 个根

而 $|H_d|=d$，故 $H_d=\{x^d-1$ 在 k 上的根$\}$

这样我们就证明了 G 若有 d 阶子群，则它必是 H_d

这即是至多唯一性.

再由前一命题知 G 循环群

特别的，若 k 是有限域，则 $k^\times$ 是循环群，如 $\mathbb{F}_p$，而 $\mathbb{F}_p^\times$ 的生成元我们称为原根

Rmk: 对于域 k，多项式环 $k[x]$ 上的 n 次多项式在 k 中至多有 n 个根

（这在后面会讲到）

课程

三、子集生成的代数结构

设有群 G，子集 $S \subset G$，我们有定义：

由 S 生成的子群 := 包含 S 的最小子群，记为 $\langle S \rangle$

$$= \bigcap_{S \subseteq H \leq G} H$$

rmk: $H \leq G$ 指 H 是 G 子群

我们来思考 $\langle S \rangle$ 至少应包含哪些元素？

S 中任意有限多元素的乘积：$a_1 \cdots a_m$，$\forall m \geq 0$，$a_i \in S$

及其逆：$a_m^{-1} \cdots a_1^{-1}$

rmk: $m=0$ 时，规定为 1_G

故至少应包含 $\{ a_1 \cdots a_m : \forall m \geq 0,\ a_i \in S \cup S^{-1} \}$ 其中 $S^{-1} = \{ x^{-1} : x \in S \}$

可以验证，以上集合其实已经是一个群，故 $= \langle S \rangle$

对于环 R（先假设它不含么，也不交换），子集 $X \subset R$

考虑由 X 生成的理想 := 包含 X 的最小理想，记为 $\langle X \rangle$

$$= \bigcap_{X \subseteq I \lhd R} I$$

rmk: $I \lhd R$ 指 I 是 R 理想

$\langle X \rangle$ 至少应该包含什么？

回顾理想的定义：对 $(R, +, \cdot)$，$I \lhd R \Leftrightarrow$
- $(I, +)$ 是加法子群
- 倍元封闭：$ar, ra \in I$，$\forall a \in I$，$\forall r \in R$

$(I, +)$ 加法子群 $\Rightarrow$ $\mathbb{Z}X = \{ \sum_1^n m_i x_i : m_i \in \mathbb{Z},\ x_i \in X,\ \forall n \in \mathbb{N} \} \subset \langle X \rangle$

（同样，$n=0$ 时规定和式为 0_R）

倍元封闭 $\Rightarrow$ $RX + XR + RXR \subset \langle X \rangle$

其中 $RX = \{ \sum_1^n r_i x_i : r_i \in R,\ x_i \in X,\ \forall n \in \mathbb{N} \}$

故至少应有 $X \supset \mathbb{Z}X + RX + XR + RXR$，而我们可验证，右边实际上已经是一个理想，故有等号成立

$$X = \mathbb{Z}X + RX + XR + RXR$$

可↓合并

若 R 交换，则 $X = \mathbb{Z}X + RX$

↓

若 R 还含么，则 $X = RX$　　$\sum m_i x_i = \sum (m_i \cdot 1_R) x_i \in RX$

由一个元素生成的理想称为主理想；对含么交换环 R，$a \in R$ 有 $\langle a \rangle = aR$

四. 陪集与正规子群

先看一些记号：设 $H, N \leq G$

记 $HN := \{hn : h \in H, n \in N\}$（它不一定是子群）

若取 $H = \{a\}$，其实就是陪集 aN

另外，易见 $H \cdot H = H$

（以上我们实际上定义了一个二元运算

$\cdot \quad \mathcal{P}(G) \times \mathcal{P}(G) \to \mathcal{P}(G)$

$\mathcal{P}(G)$ 指 G 的幂集）

考查具体的例子 $(\mathbb{Z}, +)$，我们曾利用一个整数 n 将 $\mathbb{Z}$

划分为 n 个模 n 的同余类 $[0], \cdots, [n-1]$

我们知道，划分和等价关系是一一对应的，而如上划分

对应的就是我们熟知的同余关系：

$$a \sim b \Leftrightarrow n \mid a-b \Leftrightarrow a-b \in n\mathbb{Z}$$

也记为 $a \equiv b \bmod n$

其等价类 $[k] = k + n\mathbb{Z}$

注意到 $n\mathbb{Z}$ 是 $\mathbb{Z}$ 的一个加法子群（实际上 $\mathbb{Z}$ 的加法子群都是这样的形式）

故我们也可以说以上等价关系是

根据子群 $n\mathbb{Z}$ 来定义的：$a \sim b \Leftrightarrow a-b \in n\mathbb{Z}$

我们考虑一般的群 $(G, \cdot)$，仍选以上，对给定子群 $H \leq G$

我们依据 H 来对 G 中元素进行一个分类

即给出一个等价关系

可定义 $a \sim b \Leftrightarrow ab^{-1} \in H$

（对于 $\mathbb{Z}$，是 $a-b \in n\mathbb{Z}$

减法其实就是加法逆

故此处我们改为乘法逆）

a 的等价类：Ha，称为右陪集

（老师课上讲的是左陪集，

在概念上它们是对称的）

由此我们给出 G 的划分 $G = \bigsqcup_{i \in I} Ha_i$

以上等价关系的商集 $G/\sim$ 就是 $\{Ha_i : i \in I\}$，我们记 $G/H = G/\sim$

（因为这个 $\sim$ 是根据 H 得到的）

对于 $\mathbb{Z}$，$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n = \{\bar{0}, \cdots, \overline{n-1}\}$ 仍有自然的加法群结构：$\bar{a} + \bar{b} = \overline{a+b}$

可以看作是从 $\mathbb{Z}$ 的加法“继承”而来的

那么对于一般的群 $(G, \cdot)$ 和 $H \leq G$ 呢？

对于 $(G,\cdot)$，$H\leq G$，我们当然希望在 G/H 上定义一个自然的乘法

使其成为群

$$G/H=\{Ha : a\in G\}$$

自然地，我们想让它继承 G 的乘法：$(Ha)\circ(Hb):=Hab$

新定义的二元运算是否合理？

即若 $Ha=Ha'$，$Hb=Hb'$

应有 $Hab=Ha'b'$

即 $\begin{cases} a\sim a' \Leftrightarrow a=h_1a' \\ b\sim b' \Leftrightarrow b=h_2b' \end{cases} \overset{?}{\Rightarrow} ab\sim a'b' \Leftrightarrow ab(a'b')^{-1}\in H$

$$\Downarrow$$

$$ab(a'b')^{-1}=h_1a'h_2(a')^{-1}\overset{?}{\in}H$$

实际上这是不一定的，(这可能是我们遇到的第一个定义有可能不合理的例子)

我们需要添加其他的条件来保证该定义的合理性

易见，若 G 交换，$h_1a'h_2(a')^{-1}=h_1h_2\in H$

但这样的条件太强了，我们希望找到该定义合理的充要条件：

$$Hab\Leftrightarrow Ha'b' \quad \forall a'\in Ha,\ \forall b'\in Hb$$

$$\Leftrightarrow H\underline{Ha}\,\underline{Hb}=Hab$$

$$\parallel$$

$$HaHb$$

$$\Leftrightarrow HaH=Ha \Leftrightarrow HaHa^{-1}=H$$

$$\Leftrightarrow aHa^{-1}\subseteq H\ (\forall a)$$

大家可以自己验证这些 $\Leftrightarrow$ 的正确性

我们称满足 $aHa^{-1}\subseteq H$，$\forall a\in G$ 的子群为 G 的正规子群 (or 不变子群)

记 $H\lhd G$

此时我们可验证 $(G/H,\circ)$ 构成一个群 $\begin{cases} 1_{G/H}=H \\ (Ha)^{-1}=Ha^{-1} \end{cases}$

实际上我们证明了，$(G/H,\circ)$ 是一个群 $\Leftrightarrow$ H 是 G 的正规子群

$\downarrow$

称为 G 关于 H 的商群

对 $\forall G$，它有平凡的正规子群 $\{1_G\}$，G

可以验证以下 $H \lhd G$ 的等价定义：(1) $aHa^{-1} = H \quad \forall a \in G$

(2) $Ha = aH \quad \forall a \in G$

对于一般的群 H，称 gHg^{-1} 为 H 的共轭子群

对于 $x \in G$，形如 gxg^{-1}，$(g \in G)$ 的元素称为 x 的共轭元

而对 $H \lhd G$，有 $gHg^{-1} = H$ $(\forall g \in G)$，即 H 中任一元素的任一共轭元都还在 H 中

故 H 是若干共轭类的并，这给我们如何去寻找 G 的正规子群提供了一个思路；

实际上是定义共轭关系：

x 共轭 $y \Leftrightarrow \exists g \in G$ 使 $y = gxg^{-1}$

其等价类称为共轭类

（共轭这个概念会在群作用中出现得更多）

对 $H \lhd G$

由 Lagrange 定理，若 $|G| < \infty$，则 $|G/H| = |G|/|H|$

当然，即便 G 是无穷限的，也可能有 G/H 是有限阶群

在某种程度上，我们研究有限的东西总是更容易些

若 G/H 还有非平凡的正规子群，我们可以继续商下去

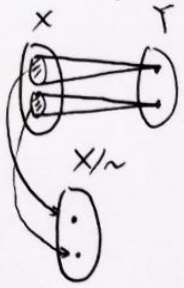
没有非平凡正规子群的群，称之为单群

五. 同态基本定理

先看任一映射 $f: X \to Y$　　这里 X, Y 仅为集合，没有任何结构

我们希望将其"改造"为一个双射（或严格地，诱导一个双射）

f 可能不是单射的原因：多个元素对应一个元素



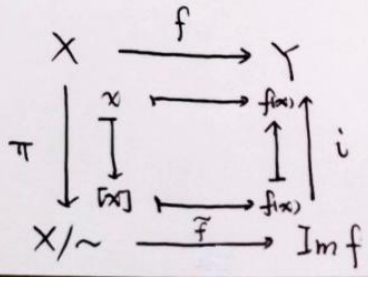
我们可以把 $\mathcal{R}$ 映成同一元素的元素视为一个元素

这实际上就是定义了一个等价关系：对 $x, x' \in X$，$x \sim x' \Leftrightarrow f(x) = f(x')$

考虑自然映射 $\pi: X \to X/\sim$，$x \mapsto [x]$　　定义 $\tilde{f}: X/\sim \to \mathrm{Im} f$，$[x] \mapsto f(x)$　　$i: \mathrm{Im} f \to Y$，$y \mapsto y$

（其合理性显然）　$\tilde{f}$ 为双射

有交换图



将其应用到各种代数结构上

可得 同态基本定理

考虑 群同态 $f: G \to H$

可以得一个由 f 诱导的双射 $\tilde{f}: G/\sim \to \mathrm{Im} f$

我们期盼它是一个同构：

$G/\sim = \{[a] : a \in G\}$　　$a \sim b \Leftrightarrow b \in [a] \Leftrightarrow f(a) = f(b)$

$\Leftrightarrow f(ab^{-1}) = 1_H$

$\Leftrightarrow ab^{-1} \in \ker f := f^{-1}(1_H)$

故这个等价关系实际上由 $\ker f$ 决定

而易验证 $\ker f \lhd G$，$\mathrm{Im} f \leq H$，于是一个同态

故 $\tilde{f}$ 是一个群同构

得到 (群) 同态第一基本定理：对同态 $f: G \to H$，它诱导一个同构 $\tilde{f}: G/\ker f \xrightarrow{\sim} \mathrm{Im} f$

应用到环上大家可以自己思考

六. 环的中国剩余定理：设 R 为含幺环，$I_1, \cdots, I_n \lhd R$

$I_i + I_j = R \quad (\forall i \neq j)$，则 $R/(I_1 \cap \cdots \cap I_n) \cong \prod_{i=1}^{n} (R/I_i)$

Sol：考虑自然映射 $\pi: R \to \prod_{i=1}^{n} (R/I_i)$，$r \mapsto (\bar{r}, \cdots, \bar{r})$　这里都记为 $\bar{r}$，但实际上不是一个东西

易见 π 是环同态，$\ker\pi = \pi^{-1}(0) = I_1 \cap \cdots \cap I_n$

由环同态基本定理：$R/I_1 \cap \cdots \cap I_n \cong \mathrm{Im}\,\pi$

只需证 π 为满射：对 $\forall (\bar{r}_1, \cdots, \bar{r}_n) \in \prod_{i=1}^{n} (R/I_i)$

可写为 $(\bar{r}_1, \cdots, \bar{r}_n) = r_1 e_1 + \cdots + r_n e_n$

其中 $e_i = (\bar{0}, \cdots, \underset{\text{第}i\text{个}}{\bar{1}}, \cdots, \bar{0})$，故只需证 $\pi^{-1}(e_i) \neq \varnothing$

考虑 $e_1 = (\bar{1}, \bar{0}, \cdots \bar{0})$ 由 $\begin{cases} I_1 + I_2 = R \\ \cdots \\ I_1 + I_n = R \end{cases} \Rightarrow \exists \begin{cases} r_{12} + r_2 = 1 \\ r_{1n} + r_n = 1 \end{cases} \Rightarrow \begin{cases} r_2 = 1 - r_{12} \\ r_n = 1 - r_{1n} \end{cases}$

其中 $r_{1i} \in I_1$，$r_i \in I_i$ $(2 \leq i \leq n)$

令 $r = \underset{\in I_2 \cap \cdots \cap I_n}{r_2 \cdots r_n} = (1 - r_{12}) \cdots (1 - r_{1n})$　易见 $\pi(r) = e_1$

对其他 e_i 同理，故 π 满射

Rmk：条件 $I_i + I_j = R = \langle 1 \rangle$，若 $R = \mathbb{Z}$，就是 $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z} \Leftrightarrow (m, n) = 1$

故我们可称以上理想 I_i, I_j 是互素的

实际上以上条件可改为 $I_i + \prod_{j \neq i} I_j = R$，结论仍成立，其中 $I_2 \cdots I_n$ 是由 $\{ r_2 \cdots r_n : \forall r_i \in I_i \}$ 生成的理想

中国科学技术大学
UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA
Hefei,Anhui.230026 The People's Republic of China

代数学基础习题课：12月6日

6.2. 证明：$\frac{3}{5}+\frac{4}{5}i \in \mathbb{C}^\times$ 的阶无穷.（该题很多同学错.）

使用归纳法证明以下结论：

$$\left(\frac{3}{5}+\frac{4}{5}i\right)^n = \frac{a_n}{5^n}+\frac{b_n}{5^n}i \qquad \begin{matrix} b_n \equiv 4 \pmod 5 \\ a_n \equiv 3 \pmod 5 \end{matrix}$$

$n=1$ 时结论成立

$n=k$ 时 ✓

$n=k+1$

$$\frac{a_n}{5^n}+\frac{b_n}{5^n}i = \left(\frac{a_{n-1}}{5^{n-1}}+\frac{b_{n-1}}{5^{n-1}}i\right)\left(\frac{3}{5}+\frac{4}{5}i\right)$$

$$= \frac{3a_{n-1}-4b_{n-1}}{5^n} + \frac{4a_{n-1}+3b_{n-1}}{5}i$$

$$a_n \equiv 3a_{n-1}-4b_{n-1} \equiv 3\times 3 - 4\times 4 \equiv 3 \pmod 5$$

$$b_n \equiv 4a_{n-1}+3b_{n-1} \equiv 4\times 3 + 3\times 4 \equiv 4 \pmod 5$$

从而 $\left(\frac{3}{5}+\frac{4}{5}i\right)^n \neq 0$

6.5. 直接去证明该群满足交换性. 这个群满足 $x^2=1$

$$ab = bbabaa = b(ba)(ba)a$$
$$= ba.$$

6.6. x 在群中阶是 n. x^k 阶：$\frac{n}{(n,k)}$.

6.8. (1) 2阶元. 满足：$x^2 \equiv 1 \pmod{p^k}$ $\Rightarrow (x-1)(x+1) \equiv 0 \pmod{p^k}$

$\Rightarrow x \equiv 1 \pmod{p^k}$（一阶元舍去）

or $x \equiv -1 \pmod{p^k}$

(2) $\prod_{g \in (\mathbb{Z}/p^k\mathbb{Z})^\times} g = (-1)\cdot\left(\prod_{g \in (\mathbb{Z}/p\mathbb{Z})^\times} g\cdot g^{-1}\right)^{\frac{1}{2}} \equiv -1 \pmod p$（配对）

(3) 由(2)结论可得

中国科学技术大学
UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA
Hefei, Anhui. 230026 The People's Republic of China

6.19. (1) $a^{20}=1$ 设 $a=g^k$ 则 $g^{20k}=1$

$\Rightarrow 100 \mid 20k \Rightarrow 5 \mid k$ $\quad a=g^{5t}$ $(0\le t\le 20,\ t\in\mathbb{Z})$

(2) 这个题有些同学做错. 注意本题中所定义是什么!

其实是可以用到 6.6 的结论.

$a=g^k$ a 的阶是 $\dfrac{n}{(n,k)}=\dfrac{100}{(100,k)}$

$\Rightarrow (100,k)=5$

$k=5, 15, 25, 45, 55, 65, 85, 95$

6.20. $\mathbb{Q}$ 不是循环群. 反证法. 设 $\mathbb{Q}=\langle g\rangle$

则 $\frac{q}{2}$ 无法用 g 表示

有限生成. $\langle g_1,\cdots,g_k\rangle$ 则 $\exists$ 有理数 $\frac{q_0}{p_0}$. $(p_0,q_0)=1$ $\forall (p_0,p_i)=1$ $(1\le i\le k)$

$g_i=\frac{p_i}{q_i}$ $(p_i,q_i)=1$ 则 $\frac{q_0}{p_0}$ 不可由 $g_1,\cdots,g_k$ 表示.

6.21. S^1 是什么?

一维球面. 即 $S^1=\{x\mid |x|=1\}$

用复数去看, 就是模长为 1 的点构成的单位圆,

S^1 的有限阶子群, 将元素的幅角限制在 $(0, 2\pi]$.

则有幅角最小的元. 设为 $g=e^{i\theta}$. 若 $\exists h\neq e^{ki\theta}$

则设 h 的幅角 α, $t\theta\le\alpha<(t+1)\theta$ $\Rightarrow$ hg^{-t} 的幅角小于 θ 矛盾.

故群中所有元均是 g^k. 设群的阶为 m. 则 $g^m=1$ $\Rightarrow$ $g=e^{\frac{2\pi i}{m}}$

中国科学技术大学
UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA
Hefei, Anhui. 230026 The People's Republic of China

8.1. 注意到若 g, h 均是原根

$$\begin{cases} g^{\frac{p-1}{2}} \equiv -1 \pmod p \\ h^{\frac{p-1}{2}} \equiv -1 \pmod p \end{cases} \Rightarrow (gh)^{\frac{p-1}{2}} \equiv 1 \pmod p \text{ 不是原根}$$

8.2. 由费马小定理知 $a^{p-1} \equiv 1 \pmod p$.

设 a 的阶为 n. $a^n \equiv 1 \pmod p$ $n \mid p-1$

若 $\frac{p-1}{n} \neq 1$. $\exists$ q 素数 $q \mid \frac{p-1}{n}$ 则 $n \mid \frac{p-1}{q}$

$\Rightarrow a^{\frac{p-1}{q}} \equiv 1 \pmod p$ 矛盾

$\Rightarrow \frac{p-1}{n} = 1$ a 是原根

反之. 由原根定义即知

8.3. a 在 a^n-1 中的阶 $a^n \equiv 1 \pmod{a^n-1}$

而 $a^m < a^n - 1$ $m < n$ 时

阶是 n.

由欧拉定理 $(a^n-1, a) = 1$, $a^{\varphi(a^n-1)} \equiv 1 \pmod{\varphi a^n-1}$.

$\Rightarrow n \mid \varphi(a^n-1)$

8.5. $p=3$ 时原根: 2

$p=5$ 原根: 2, 3

$p=7$ 原根: 3, 5

$p=11$ 原根: 2. 6. 7. 8

$p=13$. 2. 6. 7. 11

$p=17$ 3. 5. 6. 7. 10. 11. 12. 14

$p=19$ 2. 3. 10. 13. 14. 15

$p=23$ 5. 7. 10. 11. 14. 15. 17. 19. 20. 21

中国科学技术大学
UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA
Hefei,Anhui.230026 The People's Republic of China

8.5 (2). 7^2 原根： 2

5^{10} 原根： 2.

(只写一个. 其它的可由这个原根推出)

8.6. 12的阶只能为 1,2 或 p 或 2p. (因为 $2^{2p} \equiv 1 \pmod q$)

而 $2^2 \equiv 3 \pmod q$ $q>3$.

只用看 $2^p \equiv 1 ? \pmod q$

推论 8.20. 结合欧拉判别法. 告诉了我们答案.

习题1:

(1) 什么样的元会出现在 G^m 中.

形如 $g^{t(m,n)}$

$g^k = g^{tm}$ 则 $k \equiv tm \pmod n$

$k = tm + rn$.

$\Rightarrow k = (m,n)\cdot s$. ✓

(2). $a = g^{tm+rn}$

$g^{\frac{tn}{(m,n)}+r}$ $0 \le t \le (m,n)-1$. 一共 (m,n) 个.

中国科学技术大学
UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA
Hefei,Anhui.230026 The People's Republic of China

期中自测题：

1. 令 $a=1_{\otimes}$ $c=1_{\circ}$ $b=1_{\circ\otimes}$ $d=1_{\otimes}$

$\Rightarrow (a\otimes b)\circ(c\otimes d) = 1_{\circ}\circ 1_{\circ} = 1_{\circ}$

$(a\circ c)\otimes(b\circ d) = 1_{\otimes}\otimes 1_{\otimes} = 1_{\otimes}$

$\Rightarrow 1_{\circ} = 1_{\otimes}$ 令 $b=1$ $c=1$ $\Rightarrow$ $a\circ d = a\otimes d$ $\circ$与$\otimes$相同

令 $a=1$. $d=1$ $\Rightarrow$ ~~$a\otimes b$~~ 左 $= b\circ c$

右 $= c\otimes b$.

$\Rightarrow b\circ c = c\circ b$ 交换.

令 $a=1$ $b\circ(c\circ d) = a(b\circ d) \Rightarrow$ $b\circ(d\circ c) = (b\circ d)\circ c$

(运用了交换律).

2. $\begin{cases} x = 42+13t \\ y = -132-41t \end{cases}$ ~~取特解等辗转相同除~~

化简为 $41x+13y=6$.

$(41, 13)=1$

3. $2^n \equiv 1 \pmod n$ • 取 n 的最小素因子 p. p奇.

$2^n \equiv 1 \pmod p \Rightarrow (p-1, n) \neq 1$

但 p 是 n 最小素因子. 矛盾

$\Rightarrow 2^n \equiv 1 \pmod p$.

4. $\Rightarrow$ $\forall$ 素数 $p \mid n$.

若 $p \nmid m$. 则 $\exists r$ st $r \equiv -m \pmod p$. (中国剩余定理)
$r \equiv 1$ (其它素因子).

$r+m \equiv 0 \pmod p$

$p \mid r+m$ $\quad r_1+m, \dots r_{\varphi(n)}+m$ 不为缩系.

$\Rightarrow p \mid m \Rightarrow \mathrm{rad}(n) \mid m$

$\Leftarrow$ 只用验证两个: ① $(r_i+m, n)=1 \Leftarrow (r_i+m, p)=1$ $\forall p \mid n$.

② $r_i+m \not\equiv r_j+m \pmod n$ (显然)

5. ~~若 $g^{m+1}=1$~~. 对于 H 作陪集分解. 由拉格朗日定理:

$$G = \bigsqcup_{1 \le i \le m} a_i H$$

考虑 $g^1, g^2, \dots g^m, g^{m+1}$. 由抽屉原理知, $\exists g^i$ 与 g^j 在于同一陪集.

$g^i = a_k h_1$

$g^j = a_k h_2$ $\quad (g^{-j})^{-1} = (a_k h_2)^{-1} = h_2^{-1} a_k^{-1}$

$g^{i-j} = h_2^{-1} h_1 \in H$ $\quad g^{j-i} \in H$

而 $0 < |i-j| \le m$ $\quad i-j \mid m! \Rightarrow g^{m!} \in H$ 事

6. (1).

(2) $\forall a \in R$ $\exists n$ s.t $a^n = 1$ $a^{n-1} = a^{-1}$

(3). $F_2[i]$, $F_3[i]$; $F_5[i]$
非整环 是域 不是整环

(4) $4k+3$ 域
$4k+1$ 不是整环

$4k+1$: $a^2 + b^2 \equiv 0 \pmod p$.

$a^2 + 1 \equiv 0 \pmod p$ $p = 4k+1$ 时.

$\Rightarrow (a+i)(a-i) \equiv 0 \pmod p$.

$4k+3$: $(a+bi)(c+di) \equiv 0 \pmod p$.

$$\begin{cases} ac - bd \equiv 0 \pmod p \\ ad + bc \equiv 0 \pmod p \end{cases}$$

若其中 a, b, c, d 有一为0. 则 $a+bi$, $c+di$ 中有一元为0.

否则 $ac \equiv bd \pmod p \Rightarrow a \equiv bdc^{-1} \pmod p$

$ad \equiv -bc \pmod p \Rightarrow a \equiv -bcd^{-1} \pmod p$

$\Rightarrow bdc^{-1} \equiv -bcd^{-1} \pmod p$

$\Rightarrow dc^{-1} \equiv -cd^{-1} \pmod p$

$\Rightarrow d^2 + c^2 \equiv 0 \pmod p$ 该方程无解

$\Rightarrow (dc^{-1})^2 + 1 \equiv 0 \pmod p$

习　题　课

Legendre Symbol

2020 年 12 月 13 日

目录

习题

习题 8.7

设 p 是素数且 $p \equiv 1 \mod 4$. 证明

1. $\sum\limits_{\substack{r=1 \\ \left(\frac{r}{p}\right)=1}}^{p-1} r = \frac{1}{4}p(p-1).$
2. $\sum\limits_{a=1}^{p-1} a\left(\frac{a}{p}\right) = 0.$
3. $\sum\limits_{k=1}^{\frac{1}{2}(p-1)} \left[\frac{k^2}{p}\right] = \frac{1}{24}(p-1)(p-5).$

习题

因为 $p \equiv 1 \mod 4$, 所以 -1 是模 p 的二次剩余. 于是

$$\left(\frac{p-r}{p}\right) = \left(\frac{-r}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{r}{p}\right) = \left(\frac{r}{p}\right).$$

(1) 若 r 是模 p 的二次剩余, 则 $p-r$ 也是模 p 的二次剩余. 模 p 的二次剩余个数为 $\frac{1}{2}(p-1)$ 是偶数, 将 r 与 $p-r$ 配对即可.

(2) 由 (1) 知, 二次剩余的和为 $\frac{1}{4}p(p-1)$, 因此非二次剩余的和为

$$\frac{1}{2}p(p-1) - \frac{1}{4}p(p-1) = \frac{1}{4}p(p-1).$$

习题

(3) 利用课本 (8.13) 知

$$k^2 = p\left[\frac{k^2}{p}\right] + r_k, \quad 0 < r_k < p$$

由于 $r_k - r_l \equiv k^2 - l^2 \mod p$. 若 $1 \le k < l \le \frac{1}{2}(p-1)$ 则

$$p \nmid (k+l)(k-l) = k^2 - l^2.$$

因此, 这 $\frac{1}{2}(p-1)$ 个 r_k 模 p 两两不同且都是二次剩余. 由 (1) 知

$$\sum_{k=1}^{\frac{1}{2}(p-1)} p\left[\frac{k^2}{p}\right] = \sum_{k=1}^{\frac{1}{2}(p-1)} k^2 - \sum_{k=1}^{\frac{1}{2}(p-1)} r_k = \frac{1}{24}p(p^2-1) - \frac{1}{4}p(p-1).$$

习题

习题 8.8

设 $p > 3$ 是素数. 证明

1. $\sum\limits_{\substack{r=1 \\ \left(\frac{r}{p}\right)=1}}^{p-1} r \equiv 0 \mod p.$
2. $\sum\limits_{a=1}^{p-1} a \left(\dfrac{a}{p}\right) \equiv 0 \mod p.$

(1) 记 $R := \left\{\overline{r} \in \mathbb{F}_p^\times : \left(\dfrac{r}{p}\right) = 1\right\}$, $S := \left\{\overline{s} \in \mathbb{F}_p^\times : \left(\dfrac{s}{p}\right) = -1\right\}$.

习题

由于 $p > 3$, 存在 $\overline{a} \in S$ 且 $\overline{a} \neq -\overline{1}$. 由 a 的乘法作用定义的映射

$$\begin{aligned} \mu_a : & \mathbb{F}_p \to \mathbb{F}_p \\ & \overline{x} \mapsto \overline{ax}. \end{aligned}$$

是域的自同构且 $\mu_a(S) = R$, $\mu_a(R) = S$. 于是

$$\sum_{\overline{r} \in R} \overline{r} = -\sum_{\overline{s} \in S} \overline{s} = -\sum_{\overline{r} \in R} \mu_a(\overline{r}) = -a \sum_{\overline{r} \in R} \overline{r}.$$

注意到 $\overline{a}$ 的选取使得 $\overline{a+1} \neq \overline{0}$.

(2) $\displaystyle\sum_{a=1}^{p-1} a \left(\frac{a}{p}\right) \equiv \sum_{\overline{r} \in R} \overline{r} - \sum_{\overline{s} \in S} \overline{s} \mod p.$

习题

习题 8.9

设 p 是奇素数, a 是整数.

1. 证明: 同余方程 $x^2 - y^2 \equiv a \mod p$ 必有解.
2. 若 (x, y) 和 (x', y') 是上述同余方程的解, 称它们等价, 如果

$$x \equiv x' \mod p \quad y \equiv y' \mod p.$$

证明: 若 $p \nmid a$, 则 (1) 中同余方程的解的个数是 $p - 1$.
若 $p \mid a$, 则 (1) 中同余方程的解的个数是 $2p - 1$.

(1) 记 $X := \left\{\overline{x}^2 : \overline{x} \in \mathbb{F}_p\right\}$, $Y := \left\{\overline{a} + \overline{y}^2 : \overline{y} \in \mathbb{F}_p\right\}$.
此时, 同余方程有解等价于 $X \cap Y \neq \varnothing$.

习题

由于 p 是奇素数, 设 $p = 2n + 1$.

X 中的元素由 $\frac{1}{2}(p-1) = n$ 个平方剩余和 0 构成, 故 $|X| = n+1$.

Y 中的元素是由 X 整体平移 $\bar{a}$ 个单位构成, 故 $|Y| = n + 1$.

由于 $X \cup Y \subset \mathbb{F}_p$, 由容斥原理知

$$\begin{aligned} |X \cap Y| =& |X| + |Y| - |X \cup Y| \\ \geq& |X| + |Y| - |\mathbb{F}_p| \\ =& (n+1) + (n+1) - (2n+1) \\ =& 1. \end{aligned}$$

(2) $p \mid a$ 时, $\bar{x}^2 = \bar{y}^2$ 的解集为

$$S := \{(x, \pm x) : x \in \mathbb{F}_p\}.$$

$(x, x) \sim (x, -x)$ 当且仅当 $p \mid 2x$, 这等价于 $\bar{x} = 0$, 故 $|S| = 2p - 1$.

习题

$p \nmid a$ 时. 令 $\overline{u} := \overline{x} + \overline{y}$, $\overline{v} := \overline{x} - \overline{y}$ 则

$$\overline{x} = \frac{1}{2}(\overline{u} + \overline{v}), \quad \overline{y} = \frac{1}{2}(\overline{u} - \overline{v}).$$

显然, $(x, y) \sim (x', y')$ 当且仅当 $(u, v) \sim (u', v')$.
于是, 方程转化为

$$\overline{a} = \overline{x}^2 - \overline{y}^2 = (\overline{x} + \overline{y})(\overline{x} - \overline{y}) = \overline{uv}.$$

其解集为

$$S := \{(\overline{u}, \overline{u}^{-1}\overline{a}) : \overline{u} \in \mathbb{F}_p^\times\}.$$

故 $|S| = p - 1$.

习题

习题 8.10

p 是奇素数, $f(x)=ax^2+bx+c$ 且 $p\nmid a$. 记 $D:=b^2-4ac$. 证明

$$\sum_{x=0}^{p-1}\left(\frac{f(x)}{p}\right)=\begin{cases}-\left(\frac{a}{p}\right), & p\nmid D,\\ (p-1)\left(\frac{a}{p}\right), & p\mid D.\end{cases}$$

$$\left(\frac{f(x)}{p}\right)=\left(\frac{a\left(\left(x+\frac{b}{2a}\right)^2-\frac{D}{4a^2}\right)}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{\left(x+\frac{b}{2a}\right)^2-\frac{D}{4a^2}}{p}\right)$$

$p\mid D$ 时. 若 $x\neq -\frac{b}{2a}$, 则 $\left(\frac{f(x)}{p}\right)=\left(\frac{a}{p}\right)$. 否则, $\left(\frac{f(x)}{p}\right)=0$.

习题

$p \nmid D$ 时, $\left(x+\dfrac{b}{2a}\right)^2-\dfrac{D}{4a^2}$ 是否为二次剩余, 决定 $\left(\dfrac{f(x)}{p}\right)$ 符号.
上述问题等价于是否存在整数 y, (x,y) 是下列同余方程的解

$$\left(x+\frac{b}{2a}\right)^2-\frac{D}{4a^2}\equiv y^2 \mod p.$$

由习题 8.9 知, 上述同余方程有 $p-1$ 个不等价的解.
若对于某个特定的 x, 存在这样的 y, 则 $(x,\pm y)$ 都是方程的解.
因此, 同一个 x 会对应两个不等价的解.
满足条件的 x 有 $\dfrac{1}{2}(p-1)$ 个.
不满足条件的 x 有 $p-\dfrac{1}{2}(p-1)=\dfrac{1}{2}(p+1)$ 个.

习题

习题 8.11

设 a 是奇数, 则

$$x^2 \equiv a \mod 2^k, \quad (k \geq 3)$$

有解的充要条件是

$$a \equiv 1 \mod 8.$$

在此条件成立时恰有四个解: 如果 x_0 是一个解, 则

$$\pm x_0, \ \pm x_0 + 2^{k-1}$$

是所有解.

若方程有解, 则 x 必为奇数, 从而模 8 只可能为 $1, 3, 5, 7$.
无论那种情况, $x^2 \equiv 1 \mod 8$.

习题

若 $a = 8n + 1$, 设 $x = 2m + 1$.
下面确定 m 的取值, 使 x 成为方程的解.
此时应有 $2^k \mid x^2 - a$. 注意到

$$x^2 - a = (2m + 1)^2 - (8n + 1) = 4m(m + 1) - 8n.$$

由于 m 与 $m + 1$ 一奇一偶, 于是 $8 \mid 4m(m + 1) - 8n = x^2 - a$. 故

$$2^{k-3} \mid \frac{1}{8}(x^2 - a) = \frac{1}{2}m(m + 1) - n.$$

下证 $S := \left\{ \frac{1}{2}m(m + 1) : 0 \leq m \leq 2^{k-3} - 1 \right\}$ 是模 2^{k-3} 的完系.
从而, 存在整数 m 使得 $\frac{1}{2}m(m + 1) - n \equiv 0 \mod 2^{k-3}$.
由于 $|S| = 2^{k-3}$, 只需证明 S 内的元素模 2^{k-3} 两两不同.

习题

设 $0 \le v < u \le 2^{k-3} - 1$ 且

$$\frac{1}{2}u(u+1) \equiv \frac{1}{2}v(v+1) \mod 2^{k-3}.$$

那么 $2^{k-2} \mid u(u+1) - v(v+1) = (u-v)(u+v+1)$.
由于 $u-v$ 与 $u+v+1$ 一奇一偶

$$2^{k-2} \mid u-v \text{ 或 } 2^{k-2} \mid u+v+1.$$

但是 $1 \le u-v, u+v+1 \le 2^{k-2} - 2$. 这不可能.
若 $x = 2m+1$ 和 $x' = 2m'+1$ 都是方程的解, 则

$$2^k \mid x^2 - x'^2 = 4(m+m'+1)(m-m').$$

$$2^{k-2} \mid m+m'+1 = \frac{1}{2}(x+x') \text{ 或 } 2^{k-2} \mid m-m' = \frac{1}{2}(x-x').$$

目录

思考题

Corollary

设 $k \geq 2$, 则

$$\varphi : (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{k-2}\mathbb{Z}) \cong (\mathbb{Z}/2^k\mathbb{Z})^\times$$
$$(a, b) \mapsto (2^{k-1} - 1)^a 5^b.$$

思考题

思考题

证明: 形如 $8n+1, 8n+3, 8n+5, 8n+7$ 的素数有无穷多个.

(1) $8n+1$. 考虑分圆多项式

$$\Phi_8(x) = x^4 + 1.$$

设 $p_1, \cdots, p_r$ 是所有的形如 $8n+1$的素数. 令

$$N = (p_1 \cdots p_r + 1)^4 + 1.$$

若 p 是奇数 N 的一个素因子, 则 $p \neq 2$ 且

$$(p_1 \cdots p_r + 1)^4 \equiv -1 \mod p$$

于是 $p_1 \cdots p_r + 1$ 模 p 的阶是 8. 由 Fermat 小定理知, $8 \mid p-1$. 因此, $p = p_i$ 对某个 $1 \leq i \leq r$ 成立. 于是得到如下矛盾

$$N = (p_1 \cdots p_r + 1)^4 + 1 \equiv 2 \mod p.$$

思考题

(2) $8n+3$. 考虑多项式 x^2+2
设 $p_1, \cdots, p_r$ 是所有的形如 $8n+3$ 的素数. 令

$$N := (p_1 \cdots p_r)^2 + 2.$$

设 p 是 N 的一个素因子, 则 p 是奇数且 -2 是模 p 的平方剩余.

$$p \equiv 1, 3 \mod 8.$$

由于 $(8n+3)^2 \equiv 1 \mod 8$, 故 $N \equiv 3 \mod 8$.
因此, N 的素因子不可能全部模 8 余 1, 故存在 $p \equiv 3 \mod 8$.
此时, $p = p_i$ 对某个 $1 \le i \le r$ 成立. 于是得到如下矛盾

$$N = (p_1 \cdots p_r)^2 + 2 \equiv 2 \mod p.$$

思考题

(3) $8n+5$. 考虑多项式 x^2+4.
设 $p_1, \cdots, p_r$ 是所有的形如 $8n+5$ 的素数. 令

$$N := (p_1 \cdots p_r)^2 + 4.$$

设 p 是 N 的一个素因子, 则 p 是奇数且 -4 是模 p 的平方剩余.

$$p \equiv 1, 5 \mod 8.$$

由于 $(8n+5)^2 \equiv 1 \mod 8$, 故 $N \equiv 5 \mod 8$.
因此, N 的素因子不可能全部模 8 余 1, 故存在 $p \equiv 5 \mod 8$.
此时, $p = p_i$ 对某个 $1 \le i \le r$ 成立. 于是得到如下矛盾

$$N = (p_1 \cdots p_r)^2 + 4 \equiv 4 \mod p.$$

思考题

(4) $8n+7$. 考虑多项式 x^2-2.
设 $p_1, \cdots, p_r$ 是所有的形如 $8n+7$ 的素数. 令

$$N := (p_1 \cdots p_r)^2 - 2.$$

设 p 是 N 的一个素因子, 则 p 是奇数且 2 是模 p 的平方剩余.

$$p \equiv 1, 7 \mod 8.$$

由于 $(8n+7)^2 \equiv 1 \mod 8$, 故 $N \equiv 7 \mod 8$.
因此, N 的素因子不可能全部模 8 余 1, 故存在 $p \equiv 7 \mod 8$.
此时, $p = p_i$ 对某个 $1 \le i \le r$ 成立. 于是得到如下矛盾

$$N = (p_1 \cdots p_r)^2 - 2 \equiv -2 \mod p.$$

目录

三角函数特殊值

高中生小明正在学三角函数, 他计算了如下表格

d	mod 4	$\cos\frac{2\pi}{4\lvert d\rvert}$	$\mathrm{i}\sin\frac{2\pi}{4\lvert d\rvert}$
-1	3		$\sqrt{-1}$
2	2	$\frac{\sqrt{2}}{2}$	
-2	2		$\frac{\sqrt{-2}}{2}$
3	3	$\frac{\sqrt{3}}{2}$	
-5	3		$\frac{\sqrt{-5}-\sqrt{-1}}{4}$
6	2	$\frac{\sqrt{6}+\sqrt{2}}{4}$	
-6	2		$\frac{\sqrt{-6}+\sqrt{-2}}{4}$
10	2	$\frac{\sqrt{10}+\sqrt{2}+2\sqrt{5-\sqrt{5}}}{8}$	
-10	2		$\frac{\sqrt{-10}+\sqrt{-2}-2\sqrt{\sqrt{5}-5}}{8}$

小明的猜想

小明又陆续算了几个例子, 它发现

$$\cos\frac{2\pi}{3}+\mathrm{i}\sin\frac{2\pi}{3}=-\frac{1}{2}+\frac{\sqrt{-3}}{2}$$

$$\cos\frac{2\pi}{5}+\mathrm{i}\sin\frac{2\pi}{5}=\frac{\sqrt{5}-1}{4}+\frac{\sqrt{-10-2\sqrt{5}}}{4}$$

小明的猜想

设 d 是一个无平方因子的整数, 令 $\zeta_n := \cos\frac{2\pi}{n}+\mathrm{i}\sin\frac{2\pi}{n}$.

1. 若 $d>0$ 且 $d\equiv 1 \mod 4$, 则 $\sqrt{d}$ 出现在 $\zeta_{|d|}$ 的实数部分.
2. 若 $d<0$ 且 $d\equiv 1 \mod 4$, 则 $\sqrt{d}$ 出现在 $\zeta_{|d|}$ 的虚数部分.
3. 若 $d>0$ 且 $d\equiv 2,3 \mod 4$, 则 $\sqrt{d}$ 出现在 $\zeta_{4|d|}$ 的实数部分.
4. 若 $d<0$ 且 $d\equiv 2,3 \mod 4$, 则 $\sqrt{d}$ 出现在 $\zeta_{4|d|}$ 的虚数部分.

目录

数学解释

Definition

$$G(p) := \sum_{a \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right) \zeta_p^a$$

称为模 p 的 Gauss 和.

Lemma

$$G^2(p) = \begin{cases} p, & p \equiv 1 \mod 4, \\ -p, & p \equiv 3 \mod 4. \end{cases}$$

$$G^2(p) = \sum_{a,b \in \mathbb{F}_p^\times} \left(\frac{ab}{p}\right) \zeta_p^{a+b} = \sum_{a,b \in \mathbb{F}_p^\times} \left(\frac{ab^{-1}}{p}\right) \zeta_p^{a+b}.$$

数学解释

令 $c = ab^{-1}$, 则

$$G^2(p) = \sum_{b,c\in\mathbb{F}_p^\times} \left(\frac{c}{p}\right) \zeta_p^{bc+b} = \sum_{c\in\mathbb{F}_p^\times} \left(\frac{c}{p}\right) \sum_{b\in\mathbb{F}_p^\times} \zeta_p^{b(c+1)}.$$

对 $x^p - 1$ 使用 Vieta 定理知, $\sum_{n=0}^{p-1} \zeta_p^n = 0$. 又因为 $\sum_{a\in\mathbb{F}_p^\times} \left(\frac{a}{p}\right) = 0$.

1. $c \neq -\overline{1}$ 时, $\sum_{b\in\mathbb{F}_p^\times} \zeta_p^{b(c+1)} = -1$.
2. $c = -\overline{1}$ 时, $\sum_{b\in\mathbb{F}_p^\times} \zeta_p^{b(c+1)} = p - 1$.

$$G^2(p) = (p-1)\left(\frac{-1}{p}\right) + \left(\frac{-1}{p}\right) = p\left(\frac{-1}{p}\right).$$

数学解释

通过计算 $G^2(p)$, Gauss 给出了二次互反律的一种证明.
事实上, Gauss 通过若干年的研究, 确定了 $G(p)$ 的符号.

Theorem (Gauss)

$$G(p) := \begin{cases} \sqrt{p}, & p \equiv 1 \mod 4, \\ \sqrt{-p}, & p \equiv 3 \mod 4. \end{cases}$$

使用线性代数可以给出这个定理较为初等的证明.
另一种证明需要使用有限群上的 Fourier 变换.

Lemma

$$G(p) = \sum_{t=0}^{p-1} \zeta_p^{t^2}.$$

数学解释

利用二次剩余和 Legendre 符号, 我们给出上述引理的一个证明.

$$\begin{aligned}\sum_{t=0}^{p-1}\zeta_p^{t^2} &= \sum_{a=0}^{p-1}\left(\left(\frac{a}{p}\right)+1\right)\zeta_p^a \\ &= G(p)+\sum_{a=0}^{p-1}\zeta_p^a = G(p).\end{aligned}$$

Definition

$$S(n) := \sum_{t=0}^{n-1}\zeta_n^{t^2}.$$

目录

Vandermonde 矩阵与行列式

令 $m_{rs} := \zeta_n^{(r-1)(s-1)}$, 考察如下 $n \times n$ 阶 Vandermonde 矩阵

$$M(n) := (m_{rs}) = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \zeta_n & \zeta_n^2 & \cdots & \zeta_n^{n-1} \\ 1 & \zeta_n^2 & \zeta_n^4 & \cdots & \zeta_n^{2(n-1)} \\ 1 & \zeta_n^3 & \zeta_n^6 & \cdots & \zeta_n^{3(n-1)} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \zeta_n^{n-1} & \zeta_n^{2(n-1)} & \cdots & \zeta_n^{(n-1)^2} \end{pmatrix}$$

则 $\mathrm{tr} M(n) = S(n)$, 并且

$$\det M(n) = \prod_{0 \le r < s \le n-1} (\zeta_n^s - \zeta_n^r).$$

$M(n)$ 和 $\mathbb{Z}/n\mathbb{Z}$ 上的 Fourier 变换可能相差一个常数倍.

$M(n)$ 的性质

Lemma

1. $M^2(n)$ 的特征值为 $\pm n$.
2. n 为奇数, $\det M(n) = \mathrm{i}^{\binom{n}{2}} n^{n/2}$. $M^2(n)$ 的特征子空间维数

$$\dim V_n = \frac{1}{2}(n+1), \quad \dim V_{-n} = \frac{1}{2}(n-1).$$

3. n 为偶数, $\det M(n) = \mathrm{i}^{\binom{n}{2}+1} n^{n/2}$. $M^2(n)$ 的特征子空间维数

$$\dim V_n = \frac{n}{2}+1, \quad \dim V_{-n} = \frac{n}{2}-1.$$

我们只说明如何确定 $\det M(n)$ 的符号, 其余作为线性代数的练习.

$M(n)$ 的性质

$$\begin{aligned}\det M(n) &= \prod_{r<s}(\zeta_n^s - \zeta_n^r) = \prod_{r<s}(\mathrm{e}^{\frac{2\pi \mathrm{i}s}{n}} - e^{\frac{2\pi \mathrm{i}r}{n}}) \\ &= \prod_{r<s}\mathrm{e}^{\frac{\pi \mathrm{i}(s+r)}{n}}(\mathrm{e}^{\frac{\pi \mathrm{i}(s-r)}{n}} - \mathrm{e}^{\frac{-\pi \mathrm{i}(s-r)}{n}}) \\ &= \mathrm{i}^{\binom{n}{2}}\prod_{r<s}\mathrm{e}^{\frac{\pi \mathrm{i}(s+r)}{n}}\prod_{r<s}2\sin\left(\frac{(s-r)\pi}{n}\right).\end{aligned}$$

$$\begin{aligned}\sum_{r<s}^{n-1}(r+s) &= \sum_{s=r+1}^{n-1}\sum_{r=0}^{n-2}(r+s) = \sum_{s=r+1}^{n-1}\frac{1}{2}s(s+2s-1) \\ &= \frac{1}{2}n(n-1)^2.\end{aligned}$$

$M(n)$ 的性质

由于 $0 \leq r < s \leq n-1$, $0 < \dfrac{(s-r)\pi}{n} < \pi$. 因此

$$\prod_{r<s} 2\sin\left(\frac{(s-r)\pi}{n}\right) > 0.$$

从而, $\det M(n)$ 的符号完全由下式确定

$$\mathrm{i}^{\binom{n}{2}} \prod_{r<s} \mathrm{e}^{\frac{\pi\mathrm{i}(s+r)}{n}} = \mathrm{i}^{\binom{n}{2}} \mathrm{e}^{\frac{(n-1)^2\pi\mathrm{i}}{2}} = \mathrm{i}^{(n-1)^2\binom{n}{2}}.$$

定理的证明

由于 $M(n)$ 的特征值只能是 $\pm\sqrt{n}$ 和 $\pm\sqrt{-n}$. 因此

$$\det M(n) = (\sqrt{n})^a(-\sqrt{n})^b(\mathrm{i}\sqrt{n})^c(-\mathrm{i}\sqrt{n})^d = \mathrm{i}^N\sqrt{n}.$$

$$\mathrm{tr}M(n) = (a-b)\sqrt{n} + (c-d)\mathrm{i}\sqrt{n}.$$

其中 $N := 2b + c - d$. 下面确定 $a - b$ 和 $c - d$ 的取值.

定理的证明

当 $n = p$ 是奇素数时, 由特征子空间的维数知

$$a + b = \frac{1}{2}(p + 1), \quad c + d = \frac{1}{2}(p - 1).$$

此时, $\mathrm{tr}M(p) = S(p) = G(p)$. 由引理知

1. 若 $p \equiv 1 \mod 4$, 则 $a - b = \pm 1$, $c - d = 0$.

$$N \equiv \binom{p}{2} \mod 4 \Longrightarrow 2b \equiv \binom{p}{2} \mod 4$$

2. 若 $p \equiv 3 \mod 4$, 则 $a - b = 0$, $c - d = \pm 1$.

$$N \equiv \binom{p}{2} \mod 4 \Longrightarrow c - d \equiv \binom{p}{2} - (a + b) \mod 4.$$

定理的证明

Corollary

1. 若 $p \equiv 1 \mod 4$, 则 $a - b = 1$.
2. 若 $p \equiv 3 \mod 4$, 则 $c - d = 1$.

若 $p \equiv 1 \mod 4$, 则

$$\begin{aligned} a - b &= (a + b) - 2b \\ &\equiv \frac{1}{2}\left((p+1) - p(p-1)\right) \mod 4 \\ &\equiv \frac{1}{2}((p+1) - (p-1)) \mod 4. \end{aligned}$$

定理的证明

若 $p \equiv 3 \mod 4$, 则

$$\begin{aligned} c-d &\equiv \frac{1}{2}p(p-1)-(a+b) \mod 4 \\ &\equiv \frac{1}{2}(p(p-1)-(p+1)) \mod 4 \\ &\equiv \frac{1}{2}(3(p-1)-(p+1)) \mod 4 \end{aligned}$$

一般地, 通过计算 $\mathrm{tr}M^2(n)$, 我们有以下定理

Theorem

$$S(n)=\begin{cases} \sqrt{n}, & n \equiv 1 \mod 4, \\ 0, & n \equiv 2 \mod 4, \\ \sqrt{-n}, & n \equiv 3 \mod 4, \\ \sqrt{n}+\sqrt{-n}, & n \equiv 0 \mod 4. \end{cases}$$

目录

二次互反律的证明

Theorem (Gauss)

设 p, q 为奇素数, 令 $p^* := \left(\frac{-1}{p}\right) p$, 则

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right).$$

由 Gauss 和的性质知 $G^2(p) = p^*$.
一方面, 由 Euler 判别法知

$$G^{q+1}(p) \equiv \left(\frac{p^*}{q}\right) p^* \mod q.$$

这是因为

$$G^{q-1}(p) = (G^2(p))^{\frac{q-1}{2}} = {p^*}^{\frac{q-1}{2}}.$$

二次互反律的证明

另一方面, 由 Newton 二项式定理知

$$\begin{aligned} G^{q+1}(p) &= G(p)\left(\sum_{a\in\mathbb{F}_p^\times}\left(\frac{a}{p}\right)\zeta_p^a\right)^q \\ &\equiv G(p)\sum_{a\in\mathbb{F}_p^\times}\left(\frac{a}{p}\right)\zeta_p^{qa} \mod q \\ &\equiv G(p)\sum_{k\in\mathbb{F}_p^\times}\left(\frac{q^{-1}k}{p}\right)\zeta_p^{k} \mod q \\ &\equiv \left(\frac{q}{p}\right)p^* \mod q. \end{aligned}$$

习　题　课

Polynomial

2020 年 12 月 20 日

目录

习题

习题 8.12

计算 $\left(\frac{17}{23}\right), \left(\frac{19}{37}\right), \left(\frac{60}{79}\right), \left(\frac{92}{101}\right)$.

$$\left(\frac{17}{23}\right) = \left(\frac{23}{17}\right) = \left(\frac{6}{17}\right) = \left(\frac{2}{17}\right)\left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

$$\left(\frac{19}{37}\right) = \left(\frac{37}{19}\right) = \left(\frac{-1}{19}\right) = -1$$

$$\left(\frac{60}{79}\right) = \left(\frac{4}{79}\right)\left(\frac{3}{79}\right)\left(\frac{5}{79}\right) = -\left(\frac{1}{3}\right)\left(\frac{-1}{5}\right) = -1$$

$$\left(\frac{92}{101}\right) = \left(\frac{4}{101}\right)\left(\frac{23}{101}\right) = \left(\frac{101}{23}\right) = \left(\frac{9}{23}\right) = 1$$

习题

习题 8.13

1. 确定以 -3 为二次剩余的素数.
2. 确定以 5 为二次剩余的素数.

(1) 若 $p = 2, 3$, 则 -3 是二次剩余.
若 $p \neq 3$ 是奇素数, 则

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{p-1}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right).$$

由于 $\mathbb{F}_3^{\times 2} = \{\overline{1}\}$, 故 $p \equiv 1 \mod 3$.
(2) 若 $p = 2, 5$, 则 5 是二次剩余.
若 $p \neq 5$ 是奇素数, 则 $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$.
由于 $\mathbb{F}_5^{\times 2} = \{\overline{1}, \overline{4}\}$, 故 $p \equiv 1, 4 \mod 5$.

习题

习题 8.14

求所有素数 p, 使得 x^2-15 在 $\mathbb{F}_p[x]$ 中可约.

若 $p=2$, 则 $x^2-\overline{15}=x^2+\overline{1}=(x+1)^2$ 可约.
若 $p=3,5$, 则 $x^2-\overline{15}=x^2$ 可约.
若 $p\neq 3,5$ 是奇素数, 则 $\left(\frac{15}{p}\right)=\left(\frac{3}{p}\right)\left(\frac{5}{p}\right)=(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)\left(\frac{p}{5}\right)$.
因此, p 应满足下列 8 个同余方程组中的一个

$$
\begin{aligned}
&p\equiv 1 \mod 4, \quad p\equiv 1 \mod 3, \quad p\equiv 1 \mod 5, && (1)\\
&p\equiv 1 \mod 4, \quad p\equiv 1 \mod 3, \quad p\equiv 4 \mod 5, && (2)\\
&p\equiv 1 \mod 4, \quad p\equiv 2 \mod 3, \quad p\equiv 2 \mod 5, && (3)\\
&p\equiv 1 \mod 4, \quad p\equiv 2 \mod 3, \quad p\equiv 3 \mod 5. && (4)
\end{aligned}
$$

习题

$$p \equiv 3 \mod 4, \quad p \equiv 1 \mod 3, \quad p \equiv 2 \mod 5, \tag{5}$$
$$p \equiv 3 \mod 4, \quad p \equiv 1 \mod 3, \quad p \equiv 3 \mod 5, \tag{6}$$
$$p \equiv 3 \mod 4, \quad p \equiv 2 \mod 3, \quad p \equiv 1 \mod 5, \tag{7}$$
$$p \equiv 3 \mod 4, \quad p \equiv 2 \mod 3, \quad p \equiv 4 \mod 5. \tag{8}$$

由中国剩余定理知 $f : \mathbb{Z}/60\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. 计算得

$$\begin{aligned}
\overline{a} &:= f^{-1}(\overline{1}, \overline{0}, \overline{0}) = \overline{2} \times \overline{3} \times \overline{5} = \overline{45}, \\
\overline{b} &:= f^{-1}(\overline{0}, \overline{1}, \overline{0}) = \overline{4} \times \overline{2} \times \overline{5} = \overline{40}, \\
\overline{c} &:= f^{-1}(\overline{0}, \overline{0}, \overline{1}) = \overline{4} \times \overline{3} \times \overline{3} = \overline{36}.
\end{aligned}$$

习题

于是, 上述 8 个同余方程的解分别为

$$
\begin{aligned}
\overline{x}_1 &= \overline{a} + \overline{b} + \overline{c} = \overline{1}, \\
\overline{x}_2 &= \overline{a} + \overline{b} + 4\overline{c} = \overline{49}, \\
\overline{x}_3 &= \overline{a} + 2\overline{b} + 2\overline{c} = \overline{17}, \\
\overline{x}_4 &= \overline{a} + 2\overline{b} + 3\overline{c} = \overline{53}, \\
\overline{x}_5 &= 3\overline{a} + 1\overline{b} + 2\overline{c} = \overline{7}, \\
\overline{x}_6 &= 3\overline{a} + \overline{b} + 3\overline{c} = \overline{43}, \\
\overline{x}_7 &= 3\overline{a} + 2\overline{b} + 1\overline{c} = \overline{11}, \\
\overline{x}_8 &= 3\overline{a} + 2\overline{b} + 4\overline{c} = \overline{1}.
\end{aligned}
$$

习题

习题 8.15

设 $p = 4k + 1$ 是素数, a 是 k 的因子. 证明: $\left(\frac{a}{p}\right) = 1$.

若 $a = \pm 1$, 则 $\left(\frac{\pm 1}{p}\right) = 1$.

若 $a = 2$, 则 $p \equiv 1 \mod 8$, 从而 $\left(\frac{2}{p}\right) = 1$.

若 a 是 k 的奇素因子, 设 $k = ad$, 则

$$\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right) = \left(\frac{4ad + 1}{a}\right) = \left(\frac{1}{a}\right) = 1.$$

由 Legendre 符号的乘性知, 命题成立.

习题

习题 8.15

设 $n > 1, p = 2^n + 1$ 是素数. 证明: 模 p 的原根之集与模 p 的二次非剩余之集相同.

原根不是二次剩余. 设 g 是模 p 的原根, 则 $g^{\frac{p-1}{2}} \equiv -1 \mod p$.
若 g 是二次剩余, 则 $g \equiv a^2 \mod p$. 于是, 由 Fermat 小定理知

$$g^{\frac{p-1}{2}} = a^{p-1} \equiv 1 \mod p.$$

这说明 $p = 2$, 矛盾.

非二次剩余是原根. 若 g 是非二次剩余, 则 $\left(\frac{g}{p}\right) = -1$.

由 Euler 判别法知, $g^{\frac{p-1}{2}} \equiv -1 \mod p$.
由于 $p - 1 = 2^n$ 仅有素因子 2, g 的阶只能是 $p - 1$.

习题

习题 8.17

设 p 是奇素数, 证明: $\mathbb{F}_p[x]$ 中形如 $x^2+\alpha x+\beta$ 的二次多项式中, 共有 $\frac{1}{2}p(p-1)$ 个不可约多项式. 一般的计数公式见 11.8 讲义.

由于 $\mathbb{F}_p$ 是域, 二次多项式 $f(x)$ 可约等价于 $f(x)$ 在 $\mathbb{F}_p$ 上有根. 这等价于 $f(x)$ 分裂为两个一次因子的乘积.
于是, 所有的二次首一可约多项式构成的集合为

$$R:=\{(x-\overline{a})(x-\overline{b}):a,b\in\mathbb{F}_p\}.$$

其中, 有重根的多项式有 p 个, 没有重根的多项式有 $\binom{p}{2}$ 个.

于是, 二次首一不可约多项式的个数为 $p^2-|R|=\frac{1}{2}p(p-1)$.

目录

思考题

思考题 1

1. 设 R 为整环, 证明 $(R[x])^\times = R^\times$.
2. 举例说明若 R 不为整环, (1) 中等号可以不成立.

(1) 由于 R 是 $R[x]$ 的子环, 故 $R^\times \subseteq (R[x])^\times$.
若 $f \in (R[x])^\times$, 则存在 $g(x) \in R[x]$ 使得 $f(x)g(x) = 1$.
由于 R 是整环, 故

$$0 = \deg 1 = \deg f(x)g(x) = \deg f(x) + \deg g(x).$$

于是, $\deg f(x) = \deg g(x) = 0$. 从而, $f(x) \in R^\times$.
(2) 令 $R := \mathbb{Z}/4\mathbb{Z}$,

$$(\overline{2}x + 1)^2 = \overline{4}x^2 + \overline{4}x + \overline{1} = \overline{1}.$$

思考题

思考题 2

设 $f(x)=3x^3-5x^2-x+5$, $g(x)=x^2+2x+3$. 在 $\mathbb{C}[x]$ 中求 $g(x)$ 除 $f(x)$ 的商 $q(x)$ 及余项 $r(x)$.

$$3xg(x)=3x^3+6x^2+9x$$

$$f(x)-3xg(x)=-11x^2-10x+5$$

$$-11g(x)=-11x^2-22x-33.$$

$$-11x^2-10x+5-(-11)g(x)=12x+38.$$

$$f(x)=(3x-11)g(x)+(12x+38).$$

$$q(x)=3x-11,\quad r(x)=12x+38.$$

思考题

思考题 3

设 $p, q, m \in \mathbb{C}$, 在 $\mathbb{C}[x]$ 中考虑

1. p, q, m 满足什么条件时, $(x-m)^2 \mid x^3 + px + q$.
2. p, q 满足什么条件时, 存在 m 使得 $(x-m)^2 \mid x^3 + px + q$.

(1) 设 $x^3 + px + q = (x-a)(x-m)^2$. 比较系数知

$$2m + a = 0, \quad 2ma + m^2 = p, \quad -am^2 = q.$$

$$p = -3m^2, \quad q = 2m^3.$$

(2) 将 (1) 中的条件视为 (p, q) 的参数方程, 则得到方程的判别式.

$$\Delta = -4p^3 - 27q^2 = 0.$$

目录

多项式环的商环

设 k 是一个数域.

Lemma

设 $f(x) \in k[x]$ 且 $\deg f(x) = d > 0$, 则

$$k[x]/(f) = \{a_0 + a_1 x + \cdots + a_{d-1} x^{d-1} + (f) : a_i \in k\}$$

是 d 维 k-线性空间. 若 $f(x)$ 不可约, 则 $k[x]/(f)$ 是一个域.

设 $g(x) \in R[x]$, 对 $g(x)$ 做带余除法

$$g(x) = q(x)f(x) + r(x), \quad \deg r(x) < \deg f(x) = d.$$

于是, $g(x) \equiv r(x) \mod f(x)$.

多项式环的商环

若 $\overline{g}(x) \in k[x]/(f)$ 非零, 则 $g(x) \notin (f)$. 由 $f(x)$ 不可约知

$$\gcd(f(x), g(x)) = 1.$$

由 Bézout 定理知, 存在 $s(x), t(x) \in k[x]$ 使得

$$s(x)g(x) + t(x)f(x) = 1.$$

故 $s(x)g(x) \equiv 1 \mod f(x)$. 从而, $\overline{g}(x)$ 在 $k[x]/(f)$ 中可逆.

1. 注意 $\mathbb{Z}/n\mathbb{Z}$ 与 $k[x]/(f)$, n 是素数与 f 不可约的相似之处.
2. 特别地, 若 $\deg f(x) = 1$, 则 $k[x]/(f) \cong k$.

多项式环的商环

Lemma

设 $f(x) \in k[x]$ 首一不可约. 若 α 是 f 的一个根, 则 f 是以 α 为根的首一多项式中次数最小的, 称为 α 的最小多项式, 记作 f_α.

首先, α 的最小多项式 f_α 一定存在. 做带余除法

$$f(x) = q(x)f_\alpha(x) + r(x).$$

若 $r(x) \neq 0$, 则 $\deg r(x) < \deg f_\alpha(x)$ 且 $r(\alpha) = 0$, 这与 f_α 次数最小矛盾. 故 $f_\alpha(x) \mid f(x)$. 由于 $f(x)$ 不可约, 故 $f(x) = f_\alpha(x)$.

Lemma

设 $f_\alpha \in k[x]$ 是 α 的最小多项式, 则 $k[x]/(f_\alpha) \cong k[\alpha] = k(\alpha)$.

令 $\varphi : k[x] \to k[\alpha]$, $g \mapsto g(\alpha)$. 显然, 这是一个满射.
若 $\varphi(g) = 0$, 则 $g(\alpha) = 0$. 由最小多项式的性质知, $f_\alpha \mid g$.
因此, $\ker\varphi \subseteq (f_\alpha)$. 又因为 $\varphi(f_\alpha) = 0$, 故 $\ker\varphi = (f_\alpha)$.

应用举例

Example

1. $\mathbb{C} = \mathbb{R}(\mathrm{i}) \cong \mathbb{R}[x]/(x^2+1)$.
2. 设 d 是无平方因子的整数, 则 $\mathbb{Q}(\sqrt{d}) \cong \mathbb{Q}[x]/(x^2-d)$.
3. 设 $p \equiv 3 \mod 4$, 则 -1 不是模 p 的平方剩余. 从而, $x^2+\overline{1}$ 在 $\mathbb{F}_p$ 中不可约. 故 $\mathbb{F}_p[x]/(x^2+\overline{1}) \cong \mathbb{F}_p[\mathrm{i}]$ 是域.

$\mathbb{R}[x]$ 中的不可约多项式至多为二次, 这某种程度上解释了为什么数域的扩充到复数域就停止了.

多项式的重根

Definition

设 $\alpha \in k$ 是 $f(x) \in k[x]$ 的一个根, 称 α 是 $f(x)$ 的 m 重根, 如果存在 $g(x) \in k[x]$ 使得

1. $g(\alpha) \neq 0$.
2. $f(x) = (x-\alpha)^m g(x)$.

Lemma

设 $\alpha \in k$ 是 $f(x) \in k[x]$ 的一个根, α 是 $f(x)$ 的 m 重根当且仅当

$$\gcd\left(f(x), f^{(m-1)}(x)\right) \neq 1, \quad \gcd\left(f(x), f^{(m)}(x)\right) = 1.$$

其中, $f^{(m)}(x)$ 是 $f(x)$ 的 n 阶形式微分.

证明是使用 Leibniz 求导法则. 留作数学分析练习.

应用举例

Example

设 $p \equiv 1 \mod 4$, 则 -1 是模 p 的平方剩余. 从而, $x^2 + \overline{1}$ 在 $\mathbb{F}_p$ 中有根, 故

$$x^2 + \overline{1} = (x - \overline{a})(x - \overline{b}).$$

$\overline{2}$ 在 $\mathbb{F}_p$ 中可逆, $(x^2 + \overline{1})' = \overline{2}x$ 的根为 $\overline{0}$. 但 $\overline{0}$ 不是 $x^2 + \overline{1}$ 的根. 故 $\gcd\left(x^2 + \overline{1}, (x^2 + \overline{1})'\right) = 1$. 从而, $x^2 + \overline{1}$ 没有重根, 即 $\overline{a} \neq \overline{b}$. 故 $x - \overline{a}$ 与 $x - \overline{b}$ 互素. 由中国剩余定理知

$$\begin{aligned} \mathbb{F}_p[x]/(x^2 + \overline{1}) &= \mathbb{F}_p[x]/(x - \overline{a})(x - \overline{b}) \\ &\cong \mathbb{F}_p[x]/(x - \overline{a}) \times \mathbb{F}_p[x]/(x - \overline{b}) \\ &\cong \mathbb{F}_p \times \mathbb{F}_p. \end{aligned}$$

应用举例

Example

容易验证 $\varphi : \mathbb{F}_p[x]/(x^2+\overline{1}) \cong \mathbb{F}_p[i]$, $x \mapsto \mathrm{i}$ 是同构. 因此

1. $p \equiv 1 \mod 4$ 时, $\mathbb{F}_p[i] \cong \mathbb{F}_p \times \mathbb{F}_p$ 有零因子.
2. $p = 2$ 时, $\mathbb{F}_2[i] \cong \mathbb{F}_2[x]/(x+1)^2$ 有幂零元.

Corollary

设 $f(x) = x^2 + 1$, 则

1. $p = 2$ 时, $f(x) = (x+1)^2$ 可约且有重根.
2. $p \equiv 1 \mod 4$ 时, $f(x) = (x+\overline{a})(x-\overline{a})$ 可约且分裂为两个互素的一次因子的乘积.
3. $p \equiv 3 \mod 4$ 时, $f(x)$ 不可约.

目录

平方和问题

Example

1. $p = 5$ 时, $x^2 + \overline{1} = (x + \overline{2})(x - \overline{2})$. 令 $x = \mathrm{i}$, 则

$$(\mathrm{i} + 2)(\mathrm{i} - 2) = -1 - 4 = -5.$$

2. $p = 17$时, $x^2 + \overline{1} = (x + \overline{4})(x - \overline{4})$. 令 $x = \mathrm{i}$, 则

$$(\mathrm{i} + 4)(\mathrm{i} - 4) = -1 - 16 = -17$$

Corollary (Fermat)

1. $p = 2$ 时, $2 = (1 + \mathrm{i})(1 - \mathrm{i}) = 1^2 + 1^2$.
2. $p \equiv 1 \mod 4$ 时, $p = (a + b\mathrm{i})(a - b\mathrm{i}) = a^2 + b^2$.
3. $p \equiv 3 \mod 4$ 时, p 不可表平方和.

平方和问题

考虑如下的乘法含幺半群的同态

$$f : \mathbb{Z}[\mathrm{i}] \to \mathbb{N}.$$

$$\alpha := a + b\mathrm{i} \mapsto a^2 + b^2.$$

$$\beta := c + d\mathrm{i} \mapsto c^2 + d^2.$$

$$(ac - bd)^2 + (ad + bc)^2 = f(\alpha\beta) = f(\alpha)f(\beta) = (a^2 + b^2)(c^2 + d^2)$$

Corollary (Fermat)

设 $n \in \mathbb{N}$, 方程 $x^2 + y^2 = n$ 有整数解当且仅当 n 的形如 $4k + 3$ 的素因子的幂指数都是偶数.

更多例子请参考 《Primes of the Form $x^2 + ny^2$》.

平方和问题

Example (Lagrange)

设 $p > 5$ 是素数, $x^2 + 5$ 在 $\mathbb{F}_p$ 中分裂当且仅当

$$p \equiv 1, 3, 7, 9 \mod 20.$$

因此, 若 $x^2 + 5y^2 = p$ 有整数解, 则 $p \equiv 1, 3, 7, 9 \mod 20$.
由于 $-5 \equiv 3 \mod 4$, 其 Minkowski 界为

$$M := \frac{2}{\pi}\sqrt{|-5 \times 4|} < 3.$$

故 $p \equiv 1, 3, 7, 9 \mod 20$ 时, 必有 $x^2 + 5y^2 = p$ 或 $x^2 + 5y^2 = 2p$.
由奇偶性讨论知 $x^2 + 5y^2 \equiv 0, 1, 5, 6 \mod 8$, 故

1. 若 p 模 20 余 $1, 9$, 则 $2p$ 模 8 余 2. 故 $x^2 + 5y^2 = p$ 有解.
2. 若 p 模 20 余 $3, 7$, 则 p 模 8 余 $3, 7$. 故 $x^2 + 5y^2 = 2p$ 有解.

目录

多项式的判别式

设 $f(x)=x^2+bx+c\in k[x]$. 由之前的讨论知

1. $k[x]/(f)$ 是 2 维 k-线性空间.
2. $e_1:=1, e_2:=x$ 是 $k[x]/(f)$ 的一组 k-基.

考察 x 的左乘作用诱导的线性变换

$$\begin{aligned}\mu_x : k[x]/(f) &\to k[x]/(f)\\ \overline{g} &\mapsto x\overline{g}\end{aligned}$$

则 μ_x 在 e_1, e_2 下的矩阵 M_x 为

$$\mu_x(1,x)=(x,x^2)=(x,-bx-c)=(1,x)\begin{pmatrix}0 & -c\\ 1 & -b\end{pmatrix}=(1,x)M_x.$$

记 $\mathrm{tr}(x):=\mathrm{tr}(\mu_x)=\mathrm{tr}M_x$.

多项式的判别式

容易看出 $\mathrm{tr}(x^n) = \mathrm{tr}(M_x^n)$. 计算得

$$M_x^2 = \begin{pmatrix} -c & bc \\ -b & b^2 - c \end{pmatrix}.$$

$$\mathrm{tr}(e_1e_1) = \mathrm{tr}(1) = 2,$$
$$\mathrm{tr}(e_1e_2) = \mathrm{tr}(e_2e_1) = \mathrm{tr}(x) = -b,$$
$$\mathrm{tr}(e_2e_2) = \mathrm{tr}(x^2) = b^2 - 2c.$$

$$\begin{aligned} \Delta :&= \det \begin{pmatrix} \mathrm{tr}(e_1e_1) & \mathrm{tr}(e_1e_2) \\ \mathrm{tr}(e_2e_1) & \mathrm{tr}(e_2e_2) \end{pmatrix} = \det \begin{pmatrix} 2 & -b \\ -b & b^2 - 2c \end{pmatrix} \\ &= 2(b^2 - 2c) - b^2 = b^2 - 4c. \end{aligned}$$

注. tr, Δ 与基的选取无关.

多项式的判别式

现在考虑 $f(x) = x^3 + bx^2 + cx + d \in k[x]$.
$e_1 := 1, e_2 := x, e_3 := x^2$ 是 $k[x]/(f)$ 的一组 k-基.

$$\mu_x(1, x, x^2) = (x, x^2, -bx^2 - cx - d) = (1, x, x^2) \begin{pmatrix} 0 & 0 & -d \\ 1 & 0 & -c \\ 0 & 1 & -b \end{pmatrix}$$

$$M_x^2 = \begin{pmatrix} 0 & -d & bd \\ 0 & -c & bc - d \\ 1 & -b & b^2 - c \end{pmatrix}, \quad M_x^3 = \begin{pmatrix} -d & bd & dc - b^2 d \\ -c & bc - d & c^2 - b^2 c + bd \\ -b & b^2 - c & 2bc - b^3 - d \end{pmatrix}$$

多项式的判别式

$$M_x^4 = \begin{pmatrix} bd & cd - b^2d & d^2 - 2bcd + b^3d \\ bc - d & c^2 - b^2c + bd & 2cd - 2bc^2 - b^2d + b^3c \\ b^2 - c & 2bc - d - b^3 & 2bd - 3b^2c + b^4 + c^2 \end{pmatrix}$$

$$\begin{aligned} \Delta &= \det \begin{pmatrix} \mathrm{tr}(e_1e_1) & \mathrm{tr}(e_1e_2) & \mathrm{tr}(e_1e_3) \\ \mathrm{tr}(e_2e_1) & \mathrm{tr}(e_2e_2) & \mathrm{tr}(e_2e_3) \\ \mathrm{tr}(e_3e_1) & \mathrm{tr}(e_3e_2) & \mathrm{tr}(e_3e_3) \end{pmatrix} \\ &= \det \begin{pmatrix} 3 & -b & b^2 - 2c \\ -b & b^2 - 2c & 3bc - b^3 - 3d \\ b^2 - 2c & 3bc - b^3 - 3d & b^4 + 4bd + 2c^2 - 4b^2c \end{pmatrix} \\ &= b^2c^2 - 4c^3 - 4b^3d - 27d^2 + 18bcd. \end{aligned}$$

特别地, 对于 $x^3 + px + q$. 令 $b = 0$, $c = p$, $d = q$, 则

$$\Delta = -4p^3 - 27q^2.$$

多项式的判别式

Definition

设 $f(x) \in k[x]$ 是首一多项式且 $\deg f(x) = d \geq 2$. 若 $\alpha_1, \cdots, \alpha_d$ 是 $f(x)$ 的 d 个根, 则 $f(x)$ 的判别式定义为

$$\Delta := \prod_{1 \leq i < j \leq d} (\alpha_j - \alpha_i)^2.$$

Corollary

设 $f(x) \in k[x]$ 是首一多项式且 $\deg f(x) = d \geq 2$, 则

1. $\Delta = 0$ 当且仅当 $f(x)$ 有重根.
2. $\Delta > 0$ 当且仅当 $f(x)$ 的虚根个数为 4 的倍数.
3. $\Delta < 0$ 当且仅当 $f(x)$ 的虚根个数不是 4 的倍数.

多项式的判别式

Theorem

设 $f(x) \in k[x]$ 是首一多项式且 $\deg f(x) = d \geq 2$. 令 $e_i := x^{i-1}$, $1 \leq i \leq d$ 是 $k[x]/(f)$ 的一组 k-基, 则

$$\Delta = \det(\mathrm{tr}(e_i e_j)).$$

证明需要使用 Vandermonde 行列式, 留作线性代数练习.
上述定理避免了计算多项式的根. 由于矩阵 $(\mathrm{tr}(e_i e_j)) \in M_d(k)$

Corollary

设 $f(x) \in k[x]$ 是首一多项式且 $\deg f(x) = d \geq 2$, 则 $\Delta \in k$.

练习. 计算四次方程的判别式.

习　题　课

代数学基础

2021 年 11 月 3 日

目录

习题

习题 5.1.

1. 设 n 是正整数, $a \in F$. 证明: $x - a \mid x^n - a^n$.
2. 设 n 是正奇数, $a \in F$. 证明: $x + a \mid x^n + a^n$.

低情商: 用中学的因式分解.
高情商: 课本定理 5.13. $f(a) = 0 \Leftrightarrow x - a \mid f(x)$.

习题 5.2.

用 Euclid 算法求 $\gcd(f(x), g(x))$.

注意. 计算结果要化为首一多项式.
这道题可以很明显看出存在抄作业现象.

习题

习题 5.3.

设 m, n 是正整数. 证明: $\gcd(x^m - 1, x^n - 1) = x^{(m,n)} - 1$.

低情商: 辗转相除法. 与整数类似, 见 11.8 讲义.
高情商: 由习题 5.15 知

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

由唯一分解性知

$$\gcd(x^m - 1, x^n - 1) = \prod_{d|(m,n)} \Phi_d(x) = x^{(m,n)} - 1.$$

习题

习题 5.4.

设 $f(x), g(x) \in F[x]$ 且 $(f(x), g(x)) = 1$, 则 $(f(x^n), g(x^n)) = 1$.

由 Bézout 定理

$$s(x)f(x) + t(x)g(x) = 1 \Rightarrow s(x^n)f(x^n) + t(x^n)g(x^n) = 1.$$

习题 5.5.

求 $u(x), v(x) \in \mathbb{Q}[x]$ 使得

$$x^m u(x) + (1-x)^n v(x) = 1.$$

注意到

$$1 = 1^{m+n} = (x + (1-x))^{m+n} = x^m u(x) + (1-x)^n v(x).$$

习题

习题 5.6.

设 $f, g \in F[x]$ 非常数且 f, g 不相伴. 若 $d := \gcd(f, g)$, 证明

1. 存在多项式 $u(x)$ 与 $v(x)$ 使得 $\deg u(x) < \deg g(x) - \deg d(x)$ 且 $d(x) = f(x)u(x) + g(x)v(x)$.
2. 此时 $\deg v(x) < \deg f(x) - \deg d(x)$.
3. (1) 中的多项式 $u(x), v(x)$ 是唯一确定的.

约化为 $d(x) = 1$. 此时, $f(x), g(x)$ 互素且不全为常数.
存在性.

- 若 $g(x) \in F^\times$, 令 $u(x) := 0$, $v(x) := 1/g(x)$.
- 若 $f(x) \in F^\times$, 令 $v(x) := 0$, $u(x) := 1/f(x)$.
- 若 $f(x), g(x) \notin F$, 则有 Bézout 等式

$$f(x)u'(x) + g(x)v'(x) = 1.$$

习题

若 $\deg u'(x) \geq \deg g(x) \geq 1$, 则有带余除法

$$u'(x) = q(x)g(x) + r(x), \quad 0 \leq \deg r(x) < \deg g(x).$$

$$f(x)r(x) + g(x)(f(x)q(x) + v'(x)) = 1.$$

令 $u(x) := r(x)$, $v(x) := f(x)q(x) + v'(x)$ 即可.
唯一性. 若有另一组 $u'(x), v'(x)$ 满足要求, 则

$$f(x)(u(x) - u'(x)) + g(x)(v(x) - v'(x)) = 0.$$

由于 $f(x), g(x)$ 互素, 故 $f(x) \mid v(x) - v'(x)$ 且 $g(x) \mid u(x) - u'(x)$.

$$\deg(u(x) - u'(x)) < \deg g(x), \quad \deg(v(x) - v'(x)) < \deg f(x).$$

于是, $u(x) = u'(x)$ 且 $v(x) = v'(x)$.

习题

习题 5.8

设 $f(x) \in \mathbb{R}, a \in \mathbb{R}$. 决定 a 在下述多项式的零点重数

1. $g(x) := f(x) - f(a) - f'(a)(x-a) - \dfrac{f''(a)}{2}(x-a)^2$.
2. $g(x) := f(x) - f(a) - \dfrac{x-a}{2}(f'(x) + f'(a))$.

1. 若 $\deg f \leq 2$, 则 $g(x) = 0$.
2. 若 $\deg f \geq 3$, 则 a 在 $g(x)$ 的重数为 a 在 $f(x)$ 的重数 $+3$.

习题 5.9.

证明多项式 $f_n(x) := \sum_{k=0}^{n} \dfrac{x^k}{k!}$ 无重根.

$$(f_n, f_n') = (f_n, f_{n-1}) = (x^n, f_{n-1}) = 1.$$

习题

习题 5.11.

设 $f(x) \in \mathbb{Q}[x]$ 不可约, 则 $f(x)$ 没有多重复根.

在 $\mathbb{C}[x]$ 中用辗转相除法计算 $\gcd(f, f')$. 做带余除法

$$f(x) = q(x)f'(x) + r(x), \quad \deg r(x) < \deg f'(x).$$

由于 $f(x), f'(x) \in \mathbb{Q}[x]$, $q(x), r(x) \in \mathbb{Q}[x]$. 由于 $f(x)$ 在 $\mathbb{Q}[x]$ 中不可约, 故 $\gcd(f, f') = 1$.

习题5.14.

设 $f(x) \in \mathbb{F}_p[x]$ 且 $\deg f = p - 2$. 若对所有 $\alpha \in \mathbb{F}_p^\times$ 有 $f(\alpha) = \alpha^{-1}$, 试确定 $f(x)$.

令 $g(x) := xf(x) - 1$, 则 $g(x)$ 在 $\mathbb{F}_p$ 上有 $p - 1$ 个根. 于是

$$g(x) = a(x-1)(x-2)\cdots(x-(p-1)) = ax^{p-1} - 1, \quad a \in \mathbb{F}_p^\times.$$

目录

分圆多项式

记 Δ_n 为 S^1 的 n 阶子群, 其中的元素记为 μ_n, 称为 n 次单位根. 考虑循环群间的同构

$$\begin{aligned} f : (\mathbb{Z}/n\mathbb{Z}, +) &\cong (\Delta_n, *) \\ \overline{a} &\mapsto \mu_n^a. \end{aligned}$$

称 $f\left((\mathbb{Z}/n\mathbb{Z})^\times\right)$ 中的元素为 n 次本原单位根, 记为 ζ_n.

Definition

n 次分圆多项式定义为

$$\Phi_n(x) := \prod_{\substack{1\le m\le n \\ (m,n)=1}} (x - \zeta_n^m).$$

练习. 计算前 12 个分圆多项式.

分圆多项式

下述引理给出了 $\Phi_d(x)$ 的递推公式.

Lemma

对任意正整数 n

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

一方面, 若 $d \mid n$ 则 $\zeta_d \in \Delta_n$, 故 $\zeta_d^n - 1 = 0$.
另一方面, 若 $\mu_n \in \Delta_n$, 则它的阶为某个 $d \mid n$. 故 $\Phi_d(\mu_n) = 0$.
$\Phi_d(x)$ 的根是 Δ_n 中的 d 阶元, 故 $\Phi_d(x)$ 彼此互素.
$x^n - 1$ 无重根, 故两个首一多项式相等.

Corollary

$\deg \Phi_d(x) = \varphi(d)$ 且 $n = \sum_{d|n} \varphi(d)$.

分圆多项式

通过计算分圆多项式的例子, 我们有以下发现.

Corollary

$$\Phi_n(x) \in \mathbb{Z}[x].$$

$\Phi_1(x) = x - 1$. 设 $m < n$ 时, $\Phi_m(x) \in \mathbb{Z}[x]$, 则

$$f(x) := \prod_{\substack{m|n \\ m \neq n}} \Phi_m(x) \in \mathbb{Z}[x].$$

在 $\mathbb{Z}[x]$ 中做带余除法

$$x^n - 1 = q(x)f(x) + r(x), \quad \deg r(x) < \deg f(x).$$

又因为在 $\mathbb{C}[x]$ 中 $x^n - 1 = f(x)\Phi_n(x)$, 故

$$f(x)(\Phi_n(x) - q(x)) = r(x).$$

比较次数知 $r(x) = 0$.

分圆多项式

Theorem (Gauss)

$\Phi_n(x)$ 在 $\mathbb{Z}[x]$ 中不可约.

若 $f(x) \in \mathbb{Z}[x]$ 是 $\Phi_n(x)$ 的一个不可约因子, 则在 $\mathbb{Z}[x]$ 中 有分解

$$\Phi_n(x) = f(x)g(x).$$

其中 $f(x), g(x)$ 首一. 我们证明 $\Phi_n(x)$ 的根都是 $f(x)$ 的根.
取素数 $p \nmid n$. 取 $f(x)$ 的一个根 α, 则 α^p 是 $\Phi_n(x)$ 的根.
若 α^p 不是 $f(x)$ 的根, 则它是 $g(x)$ 的根. 故 $f(x) \mid g(x^p)$. 模 p 知

$$g(x)^p \equiv g(x^p) \mod p.$$

从而, 在 $\mathbb{F}_p[x]$ 中 $f(x)$ 的某个不可约因子 $h(x) \mid g(x)$. 故
$h^2(x) \mid \Phi_n(x)$. 这与 $x^n - 1$ 在 $\mathbb{F}_p[x]$ 中无重根矛盾.

目录

一些引理

Dedekind 给出了素数 p 的分歧判定, 这是代数数论中的重要结果.

Lemma (Dedekind)

设 $f \in \mathbb{Z}[x]$ 首一不可约, 则 f 模 p 有重根当且仅当 f 的判别式是 p 的倍数.

有限群是对称群的子群, 这是群作用的简单结果.

Lemma

设 G 是有限群且 $|G| = n$, 则 G 是 S_n 的子群.

Dedekind 定理与 Frobenius 密度定理

Dedekind 发现了 f 模 p 的分解型与 $\mathrm{Gal}(f)$ 中的元素的对应关系.

Theorem (Dedekind)

设 $f \in \mathbb{Z}[x]$ 首一不可约, $p \nmid \mathrm{disc}(f)$. 若 f 模 p 有如下不可约分解

$$f \equiv \prod_{i=1}^{k} f_i \mod p$$

则 $\mathrm{Gal}(f)$ 包含形如 $(\deg f_1, \deg f_2, \cdots, \deg f_k)$ 的轮换.

Frobenius 给出了上述对应的定量刻画.

Theorem

使得 f 模 p 具有某个固定分解型的素数 p 的密度与该分解型对应的元素在 $\mathrm{Gal}(f)$ 中的密度相同. 特别地, 对于 $\mathrm{Gal}(f)$ 中的每个元素, 至少有一个素数 p 使得 f 模 p 具有相应的分解型.

模任何素数 p 都可约的充要条件

Corollary

设 $f \in \mathbb{Z}[x]$ 首一不可约

1. f 模某个素数 p 不可约当且仅当 $\mathrm{Gal}(f)$ 包含 $\deg f$-轮换.
2. f 模任何素数 p 都可约当且仅当 $\mathrm{Gal}(f)$ 不包含 $\deg f$-轮换.

分圆多项式的 Galois 群是 Abel 群.

Lemma

$\mathrm{Gal}(\Phi_n(x)) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

由于 $|\mathrm{Gal}(\Phi_n(x))| = \deg \Phi_n(x)$. 若 $\mathrm{Gal}(\Phi_n(x))$ 不是循环群, 则它不包含 $\deg \Phi_n(x)$-轮换.

Corollary

若模 n 无原根, 则 $\Phi_n(x)$ 模任何素数 p 都可约.

一个例子

我们计算一个具体的例子验证上述结论.

Example

考虑 $\Phi_8(x) = x^4 + 1$, 则

$$\mathrm{Gal}(x^4 + 1) \cong (\mathbb{Z}/8\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

任何素数 p 都满足下列情况之一.

1. 若 -1 是模 p 的平方剩余, 则有 $a^2 = -1$. 此时

$$x^4 + 1 = x^4 - a^2 = (x^2 + a)(x^2 - a).$$

2. 若 p 是奇素数且 ± 2 是模 p 的平方剩余, 则有 $b^2 = \pm 2$. 此时

$$x^4 + 1 = (x^2 + 1)^2 \mp 2x^2 = (x^2 \pm 1)^2 - b^2x^2.$$

习　题　课

代数学基础

2021 年 1 月 10 日

目录

习题

习题 9.1.

设 $f(x) \in \mathbb{Z}[x]$ 且

$$f(0) \equiv f(1) \equiv 1 \mod 2.$$

证明: $f(x)$ 没有整数根.

多项式的赋值映射满足以下交换图

$$\begin{array}{ccc} \mathbb{Z}[x] & \xrightarrow{\mathrm{ev}_a} & \mathbb{Z} \\ \downarrow & & \downarrow \\ \mathbb{F}_p[x] & \xrightarrow{\mathrm{ev}_{\overline{a}}} & \mathbb{F}_p \end{array}$$

若 $a \in \mathbb{Z}$ 是 $f(x)$ 的根, 则 $f(a) = 0$ 且

$$f(\overline{a}) \equiv f(a) \mod 2.$$

习题

习题 9.2.

对于 $n \in \mathbb{Z}$, 证明 $x^n + x^{-n}$ 是关于 $x + x^{-1}$ 的整系数多项式.

问题约化为 $n \in \mathbb{N}$, 用数学归纳法.

1. $n = 0$ 时, 令 $f_0(t) = 2$, 则 $f_0(t) \in \mathbb{Z}[t]$ 且
$$x^0 + x^{-0} = 2 = f_0(x + x^{-1}).$$
2. $n = 1$ 时, 令 $f_1(t) = t$, 则 $f_1(t) \in \mathbb{Z}[t]$ 且
$$x + x^{-1} = f_1(x + x^{-1}).$$
3. 设 $n \geq 2$ 时, 对所有的 $0 \leq k < n$ 时, 存在 $f_k(t) \in \mathbb{Z}[t]$ 使得
$$x^k + x^{-k} = f_k(x + x^{-1}).$$

习题

则

$$\left(x^{n-1}+x^{-(n-1)}\right)\left(x+x^{-1}\right)=\left(x^{n}+x^{-n}\right)+\left(x^{n-2}+x^{-(n-2)}\right).$$

故

$$x^{n}+x^{-n}=f_{n-1}(x+x^{-1})f_{1}(x+x^{-1})-f_{n-2}(x+x^{-1}).$$

令 $f_n(t):=f_{n-1}(t)f_1(t)-f_{n-2}(t)$, 则 $f_n(t)\in\mathbb{Z}[t]$ 且

$$x^{n}+x^{-n}=f_{n}(x+x^{-1}).$$

习题

习题 9.3.

设 $f(x), g(x) \in \mathbb{Z}[x]$ 且 $f(x), g(x) \neq 0$. 证明: $c(fg) = c(f)c(g)$.

由课本引理 9.7 知, 以下表示唯一

$$f(x) = c(f)f_1(x), \quad g(x) = c(g)g_1(x)$$

其中 $f_1(x), g_1(x) \in \mathbb{Z}[x]$ 本原且首项系数为正. 注意到

$$f(x)g(x) = c(f)c(g)f_1(x)g_1(x).$$

其中 $f_1(x)g_1(x) \in \mathbb{Z}[x]$ 本原且首项系数为正. 故

$$c(fg) = c(f)c(g).$$

习题

习题 9.4.

设 $f \in \mathbb{Z}[x]$ 是本原多项式, $g \in \mathbb{Q}[x]$, 则 $fg \in \mathbb{Z}[x] \Leftrightarrow g \in \mathbb{Z}[x]$.

1. 若 $g(x) = 0$, 结论显然成立.
2. 若 $g(x) \neq 0$, 则 $g(x) = c(g)g_1(x)$, 其中 $g_1(x) \in \mathbb{Z}[x]$ 本原.

$$f(x)g(x) = c(g)f(x)g_1(x).$$

其中, $f(x)g_1(x) \in \mathbb{Z}[x]$ 本原. 故

$$f(x)g(x) \in \mathbb{Z}[x] \Leftrightarrow c(g) \in \mathbb{Z} \Leftrightarrow g(x) \in \mathbb{Z}[x].$$

习题

习题 9.5.

多项式 $3x^3+2x^2-1$ 在 $\mathbb{C}$ 上有三个不同的根, 记为 r_1, r_2 与 r_3. 求多项式 $f(x) \in \mathbb{Z}[x]$ 使得它的根为 r_1^2, r_2^2, r_3^2.

$$3x^3+2x^2-1 = 3\left(x^3+\frac{2}{3}x^2-\frac{1}{3}\right)$$

其判别式为

$$\operatorname{disc}(3x^3+2x^2-1) = -4\times\left(\frac{2}{3}\right)^3 - 27\times\left(\frac{1}{3}\right)^2 = -\frac{113}{27}.$$

故 r_1, r_2 和 r_3 是互不相同的根.

习题

设 $f(x)=(x-r_1^2)(x-r_2^2)(x-r_3^2)=x^3+ax^2+bx+c,\ (a,b,c\in\mathbb{C}).$

由 Vieta 定理知

$$r_1^2+r_2^2+r_3^2=-a,\quad r_1^2r_2^2+r_2^2r_3^2+r_3^2r_1^2=b,\quad r_1^2r_2^2r_3^2=-c.$$

对方程 $3x^3+2x^2-1$ 使用 Vieta 定理知

$$r_1+r_2+r_3=-\frac{2}{3},\quad r_1r_2+r_2r_3+r_3r_1=0,\quad r_1r_2r_3=\frac{1}{3}.$$

简单计算知

$$r_1^2+r_2^2+r_3^2=(r_1+r_2+r_3)^2-2(r_1r_2+r_2r_3+r_3r_1).$$

$$r_1^2r_2^2+r_2^2r_3^2+r_3^2r_1^2=(r_1r_2+r_2r_3+r_3r_1)^2-2r_1r_2r_3(r_1+r_2+r_3).$$

习题

习题 9.6.

$f(x) = x^3 - x^2 - 4x + 1$ 在 $\mathbb{C}$ 中有三个不同的根 x_1, x_2, x_3. 计算

$$F := x_1^2(x_2 + x_3) + x_2^2(x_3 + x_1) + x_3^2(x_1 + x_2).$$

计算知, $\gcd(f, f') = 1$, 故 x_1, x_2 与 x_3 互不相同. 由 Vieta 定理知

$$\begin{aligned} F &= x_1^2(x_2 + x_3) + x_2^2(x_3 + x_1) + x_3^2(x_1 + x_2) \\ &= (x_1 + x_2 + x_3)(x_1x_2 + x_2x_3 + x_3x_1) - 3x_1x_2x_3 \\ &= 1 \times (-4) - 3 \times (-1) = -4 + 3 = -1. \end{aligned}$$

注. 习题 9.5, 9.6 均涉及初等对称多项式的相关内容.

习题

习题 9.7.

设 $p \in \mathbb{Z}[x]$ 不可约. 若 $f, g \in \mathbb{Z}[x]$ 且 $p \mid fg$, 则 $p \mid f$ 或 $p \mid g$.

与课本引理 5.10 的证明相同. 若 $p(x) \nmid f(x), g(x)$, 则

$$\gcd(p(x), f(x)) = \gcd(p(x), g(x)) = 1.$$

于是, 在 $\mathbb{Z}[x]$ 中成立如下 Bézout 等式

$$f(x)u(x) + p(x)v(x) = 1, \quad g(x)s(x) + p(x)t(x) = 1.$$

两式相乘知 $\gcd(p(x), f(x)g(x)) = 1$.

Example

1. 若 $f \in \mathbb{Z}[x]$ 不可约且 $\deg f \geq 1$, 则 f 是本原的.
2. 素数 p 在 $\mathbb{Z}[x]$ 中不可约但不是本原的.
3. 零次本原多项式只有 ± 1.

习题

习题 9.8.

证明下列多项式在 $\mathbb{Q}[x]$ 中不可约

1. $f(x) = x^4 + 3x + 5$.
2. $g(x) = x^5 + 4x^4 + 2x^3 + 6x^2 - x + 5$.

由于都是本原多项式, 只需证明在 $\mathbb{Z}[x]$ 中不可约.

1. $f(x)$ 在 $\mathbb{F}_2$ 中没根且不被 $\mathbb{F}_2[x]$ 中的二次不可约多项式整除.
2. $g(x)$ 在 $\mathbb{F}_3$ 中没根且不被 $\mathbb{F}_3[x]$ 中的二次不可约多项式整除.

注. 我们将在最后一小节给出 $\mathbb{Q}[x]$ 中多项式不可约的充要条件.

习题

习题 9.9.

设 $n > 1$ 是正整数. 证明 $x^{n-1} + \cdots + x + 1$ 在 $\mathbb{Q}[x]$ 中不可约当且仅当 n 是素数.

1. 若 $n = p$ 是素数, 由课本例 9.12 知

$$x^{p-1} + \cdots + x + 1 = \Phi_p(x).$$

2. 若 n 不是素数, 取 d 为 n 的一个非平凡因子, 由习题 5.15 知

$$\Phi_d(x) \mid \frac{x^n - 1}{x - 1} = x^{n-1} + \cdots + x + 1.$$

习题

习题 9.10.

设 $a_1, \cdots, a_n$ 是互不相同的整数. 证明

$$f(x) = (x - a_1) \cdots (x - a_n) - 1$$

在 $\mathbb{Q}[x]$ 中不可约.

$f(x)$ 是本原多项式, 只需证明 $f(x)$ 在 $\mathbb{Z}[x]$ 中不可约.
若 f 可约, 则存在 $g, h \in \mathbb{Z}[x]$, 满足 $\deg g, h \geq 1$ 且 $f = gh$.
由于 $g(a_i)h(a_i) = f(a_i) = -1$, 故 $g(a_i) + h(a_i) = 0$, $i = 1, \cdots, n$.
于是, $g(x) + h(x)$ 在 $\mathbb{Z}$ 上至少有 n 个根.
但 $\deg(g(x) + h(x)) \leq \max\{\deg g(x), \deg h(x)\} < \deg f = n$.
故 $g(x) + h(x) \equiv 0$. 从而, $f(x) = -g^2(x) \leq 0$. 这不可能.

目录

S_n 对方程的作用

我们只考虑 $\mathbb{Q}[x]$ 中次数大于等于 1 的无重根的首一多项式.
设 $f(x) \in \mathbb{Q}[x]$ 且 $\deg f(x) = n$, 则 $f(x)$ 在 $\mathbb{C}$ 中有 n 个根.
记这 n 个根为 $\alpha_1, \cdots, \alpha_n$. 令 $R_f := \{\alpha_1, \cdots, \alpha_n\}$.
对 $\sigma \in S_n$, 定义 $\sigma : R_f \to R_f$, $\sigma(\alpha_i) := \alpha_{\sigma(i)}$.
显然, σ 是双射, 称为 σ 对 R_f 的作用.
若 $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$. 定义

$$\sigma(f) := (x - \alpha_{\sigma(1)}) \cdots (x - \alpha_{\sigma(n)}).$$

显然, $\sigma(f) = f$. 故 σ 是 f 的一个对称.

例子

Example (We fix a runnig example)

令 $f(x) := (x-\sqrt{2})(x+\sqrt{2})(x-\sqrt{3})(x+\sqrt{3})$. 记

$$\alpha_1 := \sqrt{2}, \quad \alpha_2 := -\sqrt{2}, \quad \alpha_3 := \sqrt{3}, \quad \alpha_4 := -\sqrt{3}.$$

令 $\sigma := (12), \tau := (23) \in S_4$, 则

$$\sigma(\sqrt{2}) = -\sqrt{2},\ \sigma(-\sqrt{2}) = \sqrt{2},\ \sigma(\sqrt{3}) = \sqrt{3},\ \sigma(-\sqrt{3}) = -\sqrt{3}.$$

$$\tau(\sqrt{2}) = \sqrt{2},\ \tau(-\sqrt{2}) = \sqrt{3},\ \tau(\sqrt{3}) = -\sqrt{2},\ \tau(-\sqrt{3}) = -\sqrt{3}.$$

直觉上, σ 的作用比 τ 更自然、合理.

Question A

σ 和 τ 有什么区别?

可迁子群

为了强调 S_n 对 R_f 和 f 的作用, 我们有时将 S_n 记为 S_f.

Definition

称 $G \leq S_f$ 可迁, 若对任意 $\alpha_i, \alpha_j \in R_f$, 存在 $\sigma \in G$, $\sigma(\alpha_i) = \alpha_j$.

Example

1. 对任意的 $f \in \mathbb{Q}[x]$, S_f 本身是可迁的.
2. $\langle \sigma, \tau \rangle \leq S_4$ 不可迁. 它无法将 α_1 作用成 α_4.
3. $n \geq 3$ 时, $A_n \triangleleft S_n$ 是可迁的, 它包含所有的 3–轮换.

1. 形象地说, 若 $G \leq S_f$ 可迁, 则 f 的任何一个根 α 在 G 的作用下都可以跑遍所有根, 即 $\mathcal{O}_\alpha := \{\sigma(\alpha) : \sigma \in G\} = R_f$.
2. $\mathcal{O}_\alpha$ 称为 α 在 G 下的轨道, 即 $G \leq S_f$ 可迁, 则 R_f 单轨道.
3. 若 $G \leq S_f$ 可迁, 则 G 不能太小. 事实上, $n \mid |G|$.

可迁子群

一个很自然的问题是

Question B

1. 如何判断 $G \leq S_f$ 是可迁的?
2. 进一步地, S_f 的可迁子群有没有分类?

当 n 比较大时, 我并不知道一般的结果.

目录

域的自同构

设 $\varphi : F \to K$ 是域之间的环同态, 则 $\ker\varphi \lhd F$.
由于域没有非平凡理想, 故 $\ker\varphi$为 0 或 F.
因此, 域的非零环同态为嵌入. 特别地, 域的非零自同态为同构.
记 $\mathrm{Aut}(K)$ 为域 K 的自同构群. 设 $K/\mathbb{Q}$ 是域的有限扩张, 即 $K \cong \mathbb{Q}[x]/(p(x))$, 其中 $p(x) \in \mathbb{Q}[x]$ 不可约. 定义

$$\mathrm{Aut}(K/\mathbb{Q}) := \{\sigma \in \mathrm{Aut}(K) : \sigma|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}\}.$$

Example

令 $K := \mathbb{Q}(\mathrm{i}) = \{a + b\mathrm{i} : a, b \in \mathbb{Q}\}$. 若 $\sigma \in \mathrm{Aut}(K/\mathbb{Q})$, 则

$$\sigma(a + b\mathrm{i}) = \sigma(a) + \sigma(b)\sigma(\mathrm{i}) = a + b\sigma(\mathrm{i}).$$

上式中, 我们利用了 $\sigma|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$. 于是, σ 由 $\sigma(\mathrm{i})$ 的取值唯一决定.
注意到, $\sigma(\mathrm{i})\sigma(\mathrm{i}) = \sigma(\mathrm{i}^2) = \sigma(-1) = -1$. 故 $\sigma(\mathrm{i}) = \pm\mathrm{i}$.
于是, $\mathrm{Aut}(K/\mathbb{Q})$ 中只有两个元素, 恒等和复共轭.

方程的分裂域和 Galois 群

Definition

设 $f \in \mathbb{Q}[x]$, $\deg f = n$, $R_f = \{\alpha_1, \cdots, \alpha_n\}$.

1. 称 $\mathbb{C}$ 中包含 $\mathbb{Q}$ 和 R_f 的最小域为 f 的分裂域, 记为 E_f.
2. 称 $\mathrm{Gal}(f) := \mathrm{Aut}(E_f/\mathbb{Q})$ 为 f 的 Galois 群.
3. 称 $\alpha \in E_f$ 在 $\mathrm{Gal}(f)$ 下的轨道 $\mathcal{O}_\alpha$ 中的元素为 α 的共轭元.

1. E_f 是 $\mathbb{C}$ 中所有包含 $\mathbb{Q}$ 和 $\alpha_1, \cdots, \alpha_n$ 的域之交.
2. $E_f/\mathbb{Q}$ 是有限扩张, 即 $E_f \cong \mathbb{Q}[x]/(p)$, 其中 $p \in \mathbb{Q}[x]$ 不可约. 此时, 不一定有 $f = p$. 例如 $f(x) := x^3 - 2 \in \mathbb{Q}[x]$ 不可约, 故 $\mathbb{Q}[x]/(f) \cong \mathbb{Q}(\sqrt[3]{2})$. 它不包含 $f(x)$ 的复根, 故 $\mathbb{Q}(\sqrt[3]{2}) \neq E_f$.
3. $E_f = \mathbb{Q}(\alpha_1, \cdots, \alpha_n)$ 且 $\mathrm{Gal}(f) \leq S_f$. 故 $\alpha \in R_f$ 时, $\mathcal{O}_\alpha \subset R_f$.
4. $\alpha, \beta \in E_f$, 则 $\mathcal{O}_\alpha = \mathcal{O}_\beta$ 或 $\mathcal{O}_\alpha \cap \mathcal{O}_\beta = \varnothing$. 故 $R_f = \bigsqcup_{\alpha \in R_f} \mathcal{O}_\alpha$.

例子

Example (Answer A)

回到之前的例子, 令 $f(x) := (x^2-2)(x^2-3)$, 则

$$E_f = \mathbb{Q}(\sqrt{2},\sqrt{3}) = \{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} : a,b,c,d \in \mathbb{Q}\}.$$

容易验证, σ 可延拓为 $\mathrm{Gal}(f)$ 中的元素, 即 $\sigma : E_f \to E_f$

$$a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \mapsto a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}.$$

在延拓的意义下 $\sigma \in \mathrm{Gal}(f)$ 但 $\tau \notin \mathrm{Gal}(f)$. 这是因为

$$\tau(2) = \tau(-\sqrt{2})\tau(-\sqrt{2}) = \sqrt{3}\cdot\sqrt{3} = 3.$$

故 $\tau|_{\mathbb{Q}} \neq \mathrm{id}_{\mathbb{Q}}$.

例子

事实上, $\mathrm{Gal}(f) = \{\mathrm{id}, (12), (34), (12)(34)\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
对任意的 $\sigma \in \mathrm{Gal}(f)$

$$\sigma(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b\sigma(\sqrt{2}) + c\sigma(\sqrt{3}) + d\sigma(\sqrt{6}).$$

注意到, $\sigma(\sqrt{6}) = \sigma(\sqrt{2})\sigma(\sqrt{3})$, 故 σ 由 $\sqrt{2}$ 和 $\sqrt{3}$ 处的取值决定.
又因为 σ 必须满足

$$\sigma(\sqrt{2})\sigma(\sqrt{2}) = 2, \quad \sigma(\sqrt{3})\sigma(\sqrt{3}) = 3.$$

故 σ 的取值只有四种可能.

1. $\mathrm{Gal}(f)$ 作用在 R_f 上都是置换, 从而是 S_f 的子群.
2. R_f 中的共轭根为 $\mathcal{O}_{\pm\sqrt{2}} = \{\pm\sqrt{2}\}$, $\mathcal{O}_{\pm\sqrt{3}} = \{\pm\sqrt{3}\}$.
3. $R_f = \{\pm\sqrt{2}, \pm\sqrt{3}\} = \mathcal{O}_{\sqrt{2}} \sqcup \mathcal{O}_{\sqrt{3}}$.

目录

Galois 理论

我们已经知道, 若 $\alpha \in \mathbb{Q}$, 则对任意的 $\sigma \in \mathrm{Gal}(f)$, 都有 $\sigma(\alpha) = \alpha$.

Theorem

$f \in \mathbb{Q}[x]$, $\alpha \in E_f$, 则 $\alpha \in \mathbb{Q}$ 当且仅当任意 $\sigma \in \mathrm{Gal}(f)$, $\sigma(\alpha) = \alpha$.

设 $\sigma \in \mathrm{Gal}(f)$, 定义 σ 对 $g(x) \in E_f[x]$ 的作用.
若 $g(x) := x^m + b_{m-1}x^{m-1} \cdots + b_1 x + b_0 \in E_f[x]$, 则

$$\begin{aligned}\sigma(g(x)) :&= x^m + \sigma(b_{m-1})x^{m-1} \cdots + \sigma(b_1)x + \sigma(b_0) \\ &= (x - \sigma(\beta_1)) \cdots (x - \sigma(\beta_m)).\end{aligned}$$

其中, $R_g = \{\beta_1, \cdots, \beta_m\}$.

Corollary (系数判定)

$g(x) \in E_f[x]$, 则 $g(x) \in \mathbb{Q}[x]$ 当且仅当任意 $\sigma \in \mathrm{Gal}(f)$, $\sigma(g) = g$.

1. 若 $g \in \mathbb{Q}[x]$, 则 σ 作用在 g 的系数上保持不动, 故 $\sigma(g) = g$.
2. 若 $\sigma(g) = g$ 对任意的 $\sigma \in \mathrm{Gal}(f)$ 成立, 则 σ 作用在 g 的系数上保持不动. 于是, 这些系数都在 $\mathbb{Q}$ 中, 故 $g \in \mathbb{Q}[x]$.

Corollary (共轭根判定)

设 $g(x) \in E_f[x]$, 则 $g(x) \in \mathbb{Q}[x]$ 当且仅当 $R_g = \bigsqcup_{\alpha \in R_g} \mathcal{O}_\alpha$.

1. 若 $R_g = \bigsqcup_{\alpha \in R_g} \mathcal{O}_\alpha$, 则 $\mathrm{Gal}(f)$ 作用在 R_g 是置换. 故 $\sigma(g) = g$ 对任意的 $\sigma \in \mathrm{Gal}(f)$ 成立, 从而 $g \in \mathbb{Q}[x]$.
2. 若 $g \in \mathbb{Q}[x]$, $R_g \neq \bigsqcup_{\alpha \in R_g} \mathcal{O}_\alpha$, 则存在 $\sigma \in \mathrm{Gal}(f)$, $\alpha \in R_g$ 使得 $\sigma(\alpha) \notin R_g$, 但 $\sigma(\alpha) \in R_{\sigma(g)}$, 故 $\sigma(g) \neq g$. 这与 $g \in \mathbb{Q}[x]$ 矛盾.

例子

注. 条件 $R_g = \bigsqcup_{\alpha \in R_g} \mathcal{O}_\alpha$ 意味着 $\mathrm{Gal}(f)$ 作用在 R_g 上是封闭的.

Example

令 $f(x) := (x-\sqrt{2})(x+\sqrt{2})(x-\sqrt{3})(x+\sqrt{3})$

$$g(x) := (x-\sqrt{2})(x+\sqrt{2}), \quad h(x) := (x-\sqrt{2})(x-\sqrt{3}).$$

$\mathrm{Gal}(f) = \{\mathrm{id}, (12), (34), (12)(34)\}$.

1. $R_g = \mathcal{O}_{\pm\sqrt{2}}$, 故 $g \in \mathbb{Q}[x]$.
2. $\sqrt{2} \in R_h$, 但 $\mathcal{O}_{\sqrt{2}} \not\subseteq R_h$, 从而 $h \notin \mathbb{Q}[x]$.

虚根成对出现

我们之前的讨论是在 $\mathbb{Q}$ 上进行的, 对 $\mathbb{R}$ 也有类似的结果.

Example

$f(x) = x^2 + 1 \in \mathbb{R}[x]$, 则 $E_f = \mathbb{C}$ 且 $\mathrm{Gal}(f)$ 只包含恒等和复共轭.

1. $z \in \mathbb{C}$ 是实数当且仅当 $z = \overline{z}$.
2. 若 $z \in \mathbb{R}$, 则 $\mathcal{O}_z = \{z\}$.
3. 若 z 是虚数, 则 $\mathcal{O}_z = \{z, \overline{z}\}$.
4. $g(x) \in \mathbb{C}[x]$ 是实系数多项式当且仅当虚根成对出现.

目录

不可约判定

Lemma

$f \in \mathbb{Q}[x]$, $\alpha \in R_f$, 则 $\mathcal{O}_\alpha$ 对应的多项式 g 是 f 在 $\mathbb{Q}[x]$ 中的因子.

令 $g(x) := \prod_{\beta \in \mathcal{O}_\alpha} (x - \beta)$, 则 $g \in E_f[x]$ 且 $R_g = \mathcal{O}_\beta$, 其中 $\beta \in R_g$.

于是, $g \in \mathbb{Q}[x]$. 注意到, $R_g = \mathcal{O}_\alpha \subset R_f$, 故 $g \mid f$.

Corollary

$f(x) \in \mathbb{Q}[x]$ 且 $\deg f = n$, 则 $f(x)$ 不可约当且仅当 $\mathrm{Gal}(f)$ 可迁.

$\mathrm{Gal}(f)$ 可迁当且仅当 R_f 单轨道当且仅当 f 在 $\mathbb{Q}[x]$ 中不可约.

分圆多项式的不可约性

设 $\Phi_n(x)$ 为 n 次分圆多项式, 则 $\mathrm{Gal}(\Phi_n) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.
对于 $m \in (\mathbb{Z}/n\mathbb{Z})^\times$, m 对 n 次本原单位根 ζ_n 的作用为

$$m : \zeta_n \mapsto \zeta_n^m.$$

若 ζ_n^i, ζ_n^j 是两个不同的 n 次本原单位根, 则 $(i, n) = (j, n) = 1$.
于是, 下列关于 x 的同余方程有解

$$xi \equiv j \mod n.$$

设 k 为上述同余方程的解, 则 $(k, n) = 1$, 从而 $k \in \mathrm{Gal}(\Phi_n)$. 此时

$$k : \zeta_n^i \mapsto \zeta_n^{ki} = \zeta_n^j.$$

故 $\mathrm{Gal}(\Phi_n)$ 可迁, 从而 $\Phi_n(x)$ 不可约.

$\mathbb{R}[x]$ 中的不可约多项式

我们之前的讨论是在 $\mathbb{Q}$ 上进行的, 对 $\mathbb{R}$ 也有类似的结果.

Example

设 $f(x) \in \mathbb{R}[x]$, 则 $f(x)$ 不可约当且仅当

1. $\deg f(x) = 2$, $f(x)$ 有一对共轭虚根.
2. $\deg f(x) = 1$, $f(x)$ 有一个实根.

由代数基本定理, $f(x)$ 在 $\mathbb{C}$ 中分裂.
由于 $\mathrm{Aut}(\mathbb{C}/\mathbb{R})$ 只有恒等和复共轭, 故 $|\mathrm{Gal}(f)| \leq 2$.
若 $f(x)$ 不可约, 则 $\mathrm{Gal}(f)$ 作用在 R_f 上可迁, 从而 $|R_f| \leq 2$.

1. $|R_f| = 1$ 时, f 有唯一实根.
2. $|R_f| = 2$ 时, $|\mathrm{Gal}(f)| = 2$, 从而 $\mathrm{Gal}(f)$ 包含复共轭. 由于 $\mathrm{Gal}(f)$ 作用在 R_f 上可迁, 故 f 必有一对共轭虚根.

习　题　课

代数学基础

2021 年 1 月 17 日

目录

习题

习题 7.3.

$$\sigma := \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}, \quad \tau := \begin{pmatrix} 1 & 2 & \cdots & n \\ a_n & a_{n-1} & \cdots & a_1 \end{pmatrix}$$

$$n(\sigma) + n(\tau) = \frac{1}{2} n(n-1).$$

令 $X := \{(i,j) : \sigma(i) > \sigma(j),\ i < j\}$, $Y := \{(i,j) : \tau(i) > \tau(j),\ i > j\}$.

容易验证, $f : X \to Y,\ (i,j) \mapsto (n+1-i, n+1-j)$ 是集合间的双射. 由定义知

$$n(\sigma) = |X| = |Y|.$$

$$n(\tau) = \frac{1}{2} n(n-1) - |Y| = \frac{1}{2} n(n-1) - n(\sigma).$$

习题

习题 7.4.

讨论置换 $\sigma := \begin{pmatrix} 1 & 2 & \cdots & n \\ n & n-1 & \cdots & 1 \end{pmatrix}$ 的奇偶性.

由习题 7.3 知 $n(\sigma) = \frac{1}{2}n(n-1)$.

1. $n \equiv 0, 1 \mod 4$ 时, σ 是偶置换.
2. $n \equiv 2, 3 \mod 4$ 时, σ 是奇置换.

习题 7.5.

$\sigma := \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$ 何时交错数最大.

1. 由习题 7.3 知 $n(\sigma) \leq \frac{1}{2}n(n-1)$.
2. 习题 7.4 中的置换交错数恰好为 $\frac{1}{2}n(n-1)$.

习题

习题 7.7.

证明 S_n 中奇置换的阶一定是偶数.

1. 奇置换 $\sigma \in S_n$ 可以表示成奇数个对换的乘积.
2. 对任意的奇数 k, σ^k 也是奇数个对换的乘积.
3. 若 $\mathrm{ord}(\sigma) = k$ 是奇数, 则 $\mathrm{id} \in S_n$ 是奇数个对换的乘积.

习题 7.10.

G 为群, $\sigma, \tau \in G$ 满足 $\langle\sigma\rangle \cap \langle\tau\rangle = \{\mathrm{id}\}$, $\sigma\tau = \tau\sigma$. 若 $\mathrm{ord}(\sigma) = m$, $\mathrm{ord}(\tau) = n$, 则 $\mathrm{ord}(\sigma\tau) = [m, n]$.

若 $\sigma^k\tau^k = (\sigma\tau)^k = \mathrm{id} \in \langle\sigma\rangle \cap \langle\tau\rangle$, 则

1. $\sigma^k\tau^k \in \langle\tau\rangle \Rightarrow \sigma^k \in \langle\tau\rangle \Rightarrow \sigma^k \in \langle\sigma\rangle \cap \langle\tau\rangle \Rightarrow \sigma^k = \mathrm{id} \Rightarrow m \mid k.$
2. $\sigma^k\tau^k \in \langle\sigma\rangle \Rightarrow \tau^k \in \langle\sigma\rangle \Rightarrow \tau^k \in \langle\sigma\rangle \cap \langle\tau\rangle \Rightarrow \tau^k = \mathrm{id} \Rightarrow n \mid k.$

习题

习题 7.11.

证明 S_n 中型为 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$ 的置换共有 $n!/\prod_{i=1}^{n} i^{\lambda_i}\lambda_i!$ 个. 由此证明

$$\sum_{\lambda}\frac{1}{\prod_{i=1}^{n} i^{\lambda_i}\lambda_i!}=1,$$

其中 $\lambda:=(\lambda_1,\lambda_2,\cdots,\lambda_n)$, $\lambda_i\in\mathbb{N}$, $i=1,\cdots,n$ 且

$$\sum_{i=1}^{n} i\lambda_i=n.$$

1. 一个 $i-$轮换有 i 种不同的写法 (每一种写法由 1 的位置唯一确定).
2. λ_i 个两两不相交的 $i-$轮换的乘积共 $i^{\lambda_i}\lambda_i!$ 种写法.
3. λ 取遍所有的型, 一共得到 $n!$ 个置换.

习题

习题 7.12.

证明 A_4 没有 6 阶子群.

1. A_4 的 6 阶子群是正规子群.
2. 正规子群是共轭类的并.
3. A_4 一共有 4 个共轭类, 它们无法组成 6 元集合.

习题 7.14

设 $\alpha, \beta \in S_n$. 证明

1. $\alpha\beta\alpha^{-1}\beta^{-1} \in A_n$
2. $\alpha\beta\alpha^{-1} \in A_n$ 当且仅当 $\beta \in A_n$.

S_n 中的两个元素具有相同的型当且仅当它们共轭.

1. β 和 β^{-1} 具有相同的奇偶性.
2. $\alpha\beta\alpha^{-1}$ 和 β 具有相同的型.

习题

习题 7.15.

设 $\sigma \in S_n$, 则存在 $\alpha, \beta \in S_n$, $\sigma = \alpha\beta$ 且 $\alpha^2 = \beta^2 = \mathrm{id}$.

由于 $\sigma \in S_n$ 可以写成互不相交的轮换的乘积, 因而只需对轮换证明. 易知

$$(ab)(bc) = (bc)(ac) = (ac)(ab)$$

$$\begin{aligned}
(x_1x_2\cdots x_n) &= (x_1x_2)(x_2x_3)\cdots(x_{n-1}x_n) \\
&= (x_2x_3)\cdots(x_{n-1}x_n)(x_1x_n) \\
&= (x_2x_n)(x_2x_3)\cdots(x_{n-2}x_{n-1})(x_1x_n) \\
&= (x_2x_n)(x_3x_4)\cdots(x_{n-2}x_{n-1})(x_2x_{n-1})(x_1x_n) \\
&= \cdots \\
&= (x_2x_n)(x_3x_{n-1})(x_4x_{n-2})\cdots(x_3x_{n-2})(x_2x_{n-1})(x_1x_n) \\
&= \prod_{\substack{i<j \\ i+j=n+2}} (x_ix_j) \prod_{\substack{k<l \\ k+l=n+1}} (x_kx_l).
\end{aligned}$$

注. 最后一小节会给出这个式子的几何解释.

习题

习题 7.16.

设 $|X| = m$, $|Y| = n$, $\sigma \in S_X$, $\tau \in S_Y$. 令 $\xi \in S_{X\times Y}$ 由如下给出

$$\xi(x, y) := (\sigma(x), \tau(y)), \quad x \in X,\ y \in Y.$$

设 $\varepsilon : S_n \to \{\pm 1\}$ 是非平凡的群同态, 试以 $\varepsilon(\sigma)$ 与 $\varepsilon(\tau)$ 表示 $\varepsilon(\xi)$.

设 $\sigma = (i_1 i_2 \cdots i_k)(j_1 j_2 \cdots j_l)\cdots$, 令

$$\xi_X(x, y) := (\sigma(x), y), \quad \xi_Y(x, y) := (x, \tau(y)), \quad x \in X,\ y \in Y.$$

易知, $\xi = \xi_X\xi_Y = \xi_Y\xi_X$. 由于

$$\xi_X = \prod_{y\in Y} \big((i_1, y)(i_2, y)\cdots(i_k, y)\big)\big((j_1, y)(j_2, y)\cdots(j_l, y)\big)\cdots$$

故 $\varepsilon(\xi_X) = \varepsilon^n(\sigma)$. 同理, $\varepsilon(\xi_Y) = \varepsilon^m(\tau)$. 故

$$\varepsilon(\xi) = \varepsilon(\xi_X\xi_Y) = \varepsilon(\xi_X)\varepsilon(\xi_Y) = \varepsilon^n(\sigma)\varepsilon^m(\tau).$$

目录

中心化子

Definition

设 G 是群, S 是 G 的非空子集, 定义 S 在 G 中的中心化子为

$$C_G(S) := \{g \in G : gs = sg,\ s \in S\}.$$

特别地, 称 $C_G(G)$ 为群 G 的中心, 记作 $Z(G)$.

Lemma

1. $C_G(S)$ 是 G 的子群. 证明留作练习.
2. 若 G 是有限群且 $G/Z(G)$ 是循环群, 则 $Z(G) = G$. 即 G 是交换群.

任取 $a, b \in G$, 由于 $G/Z(G)$ 是循环群, 存在 $g \in G$, $u, v \in Z(G)$ 使得

$$a = g^r u, \quad b = g^s v.$$

故 $ab = (g^r u)(g^s v) = g^{r+s} uv = (g^s v)(g^r u) = ba$.

习题

习题 7.17.

1. $G = S_4$, $g = (12)(34)$, 计算 $C_G(g)$.
2. $G = \mathrm{SL}_2(\mathbb{R})$, $g = \mathrm{diag}(a, a^{-1})$, $a \in \mathbb{R}^\times$. 计算 $C_G(g)$.

(1) 设 $\sigma \in S_4$ 且 $\sigma g = g\sigma$, 则 $(12)(34) = g = \sigma g \sigma^{-1} = (\sigma(1)\sigma(2))(\sigma(3)\sigma(4))$.

1. $\sigma(1) = 1$ 时, $\sigma(2) = 2$, 故 $\sigma = 1$ 或 $\sigma = (34)$.
2. $\sigma(1) = 2$ 时, $\sigma(2) = 1$, 故 $\sigma = (12)$ 或 $\sigma = (12)(34)$.
3. $\sigma(1) = 3$ 时, $\sigma(2) = 4$, 故 $\sigma = (13)(24)$ 或 (1324).
4. $\sigma(1) = 4$ 时, $\sigma(2) = 3$, 故 $\sigma = (14)(23)$ 或 (1423).

故 $C_G(g) \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
(2) 若 $a = \pm 1$, 则 $C_G(g) = G$.
若 $a \neq \pm 1$, 则 $C_G(g) = \{\mathrm{diag}(x, x^{-1}) : x \in \mathbb{R}^\times\}$.

目录

群的生成元

Definition

设 G 是一个群, S 是 G 的非空子集, 则

$$\langle S\rangle := \{s_1 \cdots s_n : s_i \in S,\ 1 \le i \le n,\ n \in \mathbb{Z}_+\}$$

是 G 的子群, 称为 S 生成的子群. S 中的元素称为该子群的一组生成元.

Lemma

设 $n \ge 2$, 则

1. 所有 2–轮换是 S_n 的生成元.
2. $(12), (13), \cdots, (1n)$ 是 S_n 的生成元.
3. $(12), (23), \cdots, (n-1, n)$ 是 S_n 的生成元.
4. $(12), (123\cdots n)$ 是 S_n 的生成元.

S_n 的生成元

1. $(x_1x_2\cdots x_n)=(x_1x_2)(x_2x_3)\cdots(x_{n-1}x_n)$.
2. $(xy)=(1x)(1y)(1x)$.
3. 考虑 $(xy)\in S_n$, 用归纳法证明 (xy) 可由 $(12),(23),\cdots,(n-1,n)$ 表示.
   不妨设 $x<y$. 当 $y-x=1$ 时, $(xy)=(x,x+1)$.
   设 $y-x=k$ 时, (xy) 可由 $(12),(23),\cdots,(n-1,n)$ 表示.
   则 $y-x=k+1$ 时, $(xy)=(x,x+1)(x+1,y)(x,x+1)$.
4. 令 $\sigma=(123\cdots n)$, 则 $\sigma^x(12)\sigma^{-x}=(\sigma^x(1),\sigma^x(2))=(x+1,x+2)$.

Lemma

设 $n\geq 3$, 则

1. 所有 3–轮换 是 A_n 的生成元.
2. $(1xy)$ 是 A_n 的生成元.
3. $(12x)$ 是 A_n 的生成元.
4. $(x,x+1,x+2)$ 是 A_n 的生成元.
5. $(1x,x+1)$ 是 A_n 的生成元.
6. 若 n 是奇数, (123) 和 $(123\cdots n)$ 生成 A_n.
7. 若 n 是偶数, (123) 和 $(23\cdots n)$ 生成 A_n.

A_n 的生成元

1. 设 $\sigma \in A_n$, 则 $\sigma = \tau_1 \cdots \tau_r$. 其中 r 是偶数, $\tau \in S_n$ 是对换.
   若 τ_i 和 τ_{i+1} 有一个公共元素, 不妨设 $\tau_i = (xy)$, $\tau_{i+1} = (yz)$, 则
   $$\tau_i \tau_{i+1} = (xy)(yz) = (xyz).$$
   若 τ_i 和 τ_{i+1} 不相交, 则 $n \geq 4$, 不妨设 $\tau_i = (ab)$, $\tau_{i+1} = (cd)$, 则
   $$\tau_i \tau_{i+1} = (ab)(cd) = (ab)(bc)(bc)(cd) = (abc)(bcd).$$
2. $(xyz) = (1xy)(1yz)$.
3. $n \geq 4$ 时, $(1xy) = (12y)(12y)(12x)(12y)$.
4. $n \geq 5$ 时, $(12x) = (12, x-2)(12, x-1)(x-2, x-1, x)(12, x-2)(12, x-1)$.
   对 $(12, x-2)$ 和 $(12, x-1)$ 用归纳假设.
5. $(x, x+1, x+2) = (1x, x+1)(1, x+1, x+2)$.
6. 令 $\sigma = (123 \cdots n)$, 则 $\sigma \in A_n$ 且 $\sigma^x (123) \sigma^{-x} = (x+1, x+2, x+3)$.
7. 令 $\sigma = (234 \cdots n)$, 则 $\sigma \in A_n$ 且 $\sigma^x (123) \sigma^{-x} = (1, x+2, x+3)$.

目录

正 n 边形的对称

Definition

设 Δ_n 是 $\mathbb{R}^2$ 中单位圆的内接正 n 边形, σ 是 $\mathbb{R}^2$ 内绕原点的旋转或是关于过原点直线的反射. 若 σ 可限制为 Δ_n 到自身的双射, 则称 σ 为 Δ_n 的一个对称. Δ_n 的所有对称构成的集合记为 D_n.

Example

r_k 为绕原点顺时针旋转 $2k\pi/n$, t 为 Δ_n 的某个对称轴的反射, 则 $r_k, t \in D_n$.

Lemma

D_n 是 S_n 的子群且 $|D_n| = 2n$. 称 D_n 为正 n 边形的二面体群.

将 Δ_n 的顶点逆时针依次标记为 $1, 2, \cdots, n$. 任意的 $\sigma \in D_n$, σ 作用在顶点集上是置换, 并且 σ 由这 n 个顶点处的取值唯一确定. 故 D_n 是 S_n 的子集.

正 n 边形的对称

容易发现, D_n 中的旋转不会改变顶点的排列方向, 即 $1, 2, \cdots, n$ 是顺时针排列还是逆时针排列. 但 D_n 中的反射必然改变顶点的排列方向.
因此, 非平凡的反射和旋转不可能相同.
D_n 有 n 个不同的旋转和 n 个不同的反射, 故 $|D_n| \geq 2n$.
设 $\sigma \in S_n$, 若 $\sigma \in D_n$, 则 σ 不会改变顶点的邻接关系.
若 $\sigma(1) = i$, 则 $\sigma(2) = i - 1$ 或 $i + 1$. 无论那种情况, σ 都被唯一确定.
因此, S_n 中不改变顶点邻接关系的元素至多有 $2n$ 个. 故 $|D_n| \leq 2n$.
设 $\sigma, \tau \in D_n$, 则 $\sigma\tau^{-1} \in D_n$.
否则 $\sigma\tau^{-1}$ 为 S_n 中不改变顶点邻接关系的元素, 但它又不在 D_n 中, 这不可能.

Lemma

设 σ 为绕原点顺时针旋转 $2\pi/n$, τ 为 Δ_n 的某个反射, 则 $\sigma, \tau \in D_n$ 且

$$D_n = \{\mathrm{id}, \sigma, \sigma^2, \cdots, \sigma^{n-1}, t, \sigma t, \sigma^2 t, \cdots, \sigma^{n-1} t\}.$$

特别地, σ, τ 是 D_n 的一组生成元.

若 $\sigma^i t^k = \sigma^j t^l$, 则 $\sigma^{i-j} = t^{l-k}$. 故 $n \mid i - j$ 且 $2 \mid l - k$, 从而 $i = j$ 且 $l = k$.

n–轮换作为正 n 边形的旋转

设 $\sigma = (x_1 x_2 \cdots x_n) \in S_n$, 将 Δ_n 的顶点逆时针依次排列为 $x_1, x_2, \cdots, x_n$, 则 σ 对 Δ_n 的作用为顺时针旋转 $2\pi/n$. 故 $\sigma \in D_n$.
取 D_n 中的一个反射 τ, 则 $\sigma = \sigma(\tau\tau) = (\sigma\tau)\tau$.
令 $\alpha = \sigma\tau$, $\beta = \tau$, 则 $\alpha, \beta \in D_n$ 是反射, 故 $\alpha^2 = \beta^2 = \mathrm{id}$ 且 $\sigma = \alpha\beta$.
显然, 这个分解不唯一.
特别地, 设 τ_1 为过 x_1 和 x_n 中点的反射, 则

$$\tau_1 = \prod_{\substack{i<j \\ i+1=n+1}} (x_i x_j).$$

设 τ_2 为过顶点 x_1 的反射, 则

$$\tau_2 = \prod_{\substack{k<l \\ k+l=n+2}} (x_k x_l).$$

$\tau_2\tau_1$ 即为顺时针旋转 $2\pi/n$. 故 $\sigma = \tau_2\tau_1$, 此即习题 7.15 中的公式.

例题

习题 7.18.

设 f 是四元多项式, 令

$$G_f := \{\sigma \in S_4 : (\sigma)(f) = f\}.$$

证明 G_f 是 S_4 的子群, 并求下列多项式的 G_f

1. $f = x_1x_2 + x_3x_4$.
2. $f = x_1x_2x_3x_4$.

若 $\alpha, \beta \in G_f$, 则

$$(\alpha\beta^{-1})(f) = (\alpha\beta^{-1})(\beta(f)) = \alpha(\beta^{-1}\beta(f)) = \alpha(f) = f.$$

故 $\alpha\beta^{-1} \in G_f$. 因此, G_f 是子群.

1. 考虑长宽不等的矩形, 把 x_1, x_2 放到一组对顶点上, x_3, x_4 放到另一组对顶点上. 该矩形的对称群即为 G_f, 它是著名的 Klein 四元群 K_4.
2. $G_f = S_4$.

Fermat's Last Theorem for Polynomials

定理. $n \geq 3$ 时, 方程 $f^n + g^n = h^n$ 在 $\mathbb{C}[x]$ 中没有非平凡解.

证明. 不妨设 f, g, h 没有公因子. 由单位根的性质知

$$f^n = h^n - g^n = \prod_{i=0}^{n-1}(h - \zeta_n^i g). \tag{$*$}$$

若 $0 \leq i < j \leq n-1$, 由辗转相除法知

$$\gcd(h - \zeta_n^i g, h - \zeta_n^j g) = \gcd(g, h) = 1.$$

令 $d := \deg h + \deg g$, 则 $h - \zeta_n^i g$ 的根至多为 d 重. 由于 f^n 的根至少为 n 重且 $h - \zeta_n^i g$ 之间没有公共根, 由 $(*)$ 知, 必有 $d \geq n \geq 3$. 下面对 d 做递降.

由于 $n \geq 3$, 由课本定理 5.11 知, 存在不全为常数的 $a, b, c \in \mathbb{C}[x]$ 使得

$$h - g = a^n, \quad h - \zeta_n g = b^n, \quad h - \zeta_n^2 g = c^n.$$

将 $b^n - a^n = (1 - \zeta_n)g$ 与 $b^n - \zeta_n a^n = (1 - \zeta_n)h$ 代入 $h - \zeta_n^2 g = c^n$ 得

$$(\lambda a)^n + (\mu b)^n = c^n, \quad \lambda, \mu \in \mathbb{C}.$$

于是, $\lambda a, \mu b, c$ 也是方程的一组非平凡解, 它满足 $\deg \lambda a + \deg \mu b < d$.

注. 1. 上述证明非常简洁, 角落是可以写得下的.

2. 课本定理 5.11 说明 $\mathbb{C}[x]$ 中的多项式具有唯一分解性质. 这在证明中起到了至关重要的作用.

3. Kummer 关于 Fermat 大定理的工作与此类似. 在整数的情形下, 需要考虑 $\mathbb{Z}[\zeta_n]$ 是否具有唯一分解性质. 当 $n \leq 19$ 时, $\mathbb{Z}[\zeta_n]$ 是唯一分解的. 一般情况下, $\mathbb{Z}[\zeta_n]$ 中的分式理想具有唯一分解性质. 至此, 我们发现理想是比数更本质的东西! 由此开启代数数论新纪元!

4. 上述证明参考自《Algebra, Chapter 0》– Paolo Aluffi, V. Exercise 4.25, 第280页.

下面我们给出该定理的另一种证明.

Mason. 设 $f, g, h \in \mathbb{C}[x]$ 不全为常数, 它们互素且满足 $f + g = h$, 则

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

其中, 多项式的 rad 定义为其互不相同的一次因子的乘积. 从而, $\deg \operatorname{rad}(f)$ 指的是 f 的互不相同的零点的个数.

定理的另一种证明. 不妨设 f, g, h 没有公因子. 注意到

$$\deg \operatorname{rad}(f^n g^n h^n) = \deg \operatorname{rad}(fgh) \leq \deg f + \deg g + \deg h.$$

由于 f, g, h 不全为常数, $\deg f + \deg g + \deg h > 0$. 由 Mason 定理知

$$\max\{n \deg f, n \deg g, n \deg h\} \leq \deg f + \deg g + \deg h - 1.$$

$$\begin{aligned} n(\deg f + \deg g + \deg h) &\leq 3(\deg f + \deg g + \deg h) - 3 \\ &< 3(\deg f + \deg g + \deg h). \end{aligned}$$

从而, $n < 3$.

注. 1. $n = 2$ 时, 对任意的 $f \in \mathbb{C}[x]$, 总有 $(1 - f^2)^2 + (2f)^2 = (1 + f^2)^2$.

2. Mason 定理的整数版本即为大名鼎鼎的 *abc* 猜想. 日本数学家望月新一 (Mochizuki) 宣称他证明了该猜想. 数学界对此有一定的争议.

3. 与多项式类似, *abc* 猜想可以证明 Fermat 大定理.

4. 相比于 *abc* 猜想, Mason 定理的证明只需要熟悉多项式的次数、形式微分、重根等概念, 但有一定的技巧性. 同学们可查阅相关资料.

总结. 多项式是容易的, 但整数是困难的!

互　反　律

定义 1. 设 $K/\mathbb{Q}$ 是域的有限 Galois 扩张. 若 $\mathrm{Gal}(K/\mathbb{Q})$ 是 Abel 群, 则称 K 是 Abel 数域.

Kronecker-Weber. Abel 数域是分圆域 $\mathbb{Q}(\zeta_m)$ 的子域, 其中 $\zeta_n := \mathrm{e}^{\frac{2\pi \mathrm{i}}{n}}$.

设 $K \subset \mathbb{Q}(\zeta_m)$ 且 $K \subset \mathbb{Q}(\zeta_n)$, 则

$$K \subset \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{(m,n)}).$$

于是, 存在包含 K 的最小分圆域 $\mathbb{Q}(\zeta_D)$, 它是所有包含 K 的分圆域的交.

定义 2. 上述 D 称为 Abel 数域 K 的导子 (conductor).

事实 1. 若 d 是无平方因子整数, 令 $K := \mathbb{Q}(\sqrt{d})$, 则 K 是 Abel 数域且

1. $d \equiv 1 \mod 4$ 时, K 的导子为 $|d|$.
2. $d \equiv 2, 3 \mod 4$ 时, K 的导子为 $4|d|$.

定义 3. 设 d 是无平方因子的整数, 令 $K := \mathbb{Q}(\sqrt{d})$. $d \equiv 2, 3 \mod 4$ 时

1. 称素数 p 在 K 上分歧, 若 $x^2 - d$ 在 $\mathbb{F}_p$ 上有重根.
2. 称素数 p 在 K 上惯性, 若 $x^2 - d$ 在 $\mathbb{F}_p$ 上不可约.
3. 称素数 p 在 K 上分裂, 若 $x^2 - d$ 在 $\mathbb{F}_p$ 上可约但没有重根.

定义 3′. 设 d 是无平方因子的整数, 令 $K := \mathbb{Q}(\sqrt{d})$. $d \equiv 1 \mod 4$ 时

1. 称素数 p 在 K 上分歧, 若 $x^2 - x + \dfrac{1-d}{4}$ 在 $\mathbb{F}_p$ 上有重根.
2. 称素数 p 在 K 上惯性, 若 $x^2 - x + \dfrac{1-d}{4}$ 在 $\mathbb{F}_p$ 上不可约.
3. 称素数 p 在 K 上分裂, 若 $x^2 - x + \dfrac{1-d}{4}$ 在 $\mathbb{F}_p$ 上可约但没有重根.

我们把分歧、惯性和分裂统称为 p 的分解类型.

二次互反律. 设 d 是无平方因子的整数, 令 $K := \mathbb{Q}(\sqrt{d})$. 若 K 的导子为 D 且 $\mathbb{Z}$ 中的素数 p, q 满足 $p \equiv q \mod D$, 则 p, q 在 K 上有相同的分解类型.

如果承认事实 1, 即使忽略红色部分, 上述二次互反律的含义对大家来说依然是明确的.

例 1. 取 $d = -1$ 则 $d \equiv 3 \mod 4$. 于是, $x^2 + 1$ 在 $\mathbb{F}_p$ 上的分解给出了 p 在 $\mathbb{Q}(\mathrm{i})$ 上的分解类型. 这需要考虑 -1 是否为模 p 的平方剩余. 此时, $\mathbb{Q}(\mathrm{i})$ 的导子为 4.

练习 1. 验证二次互反律: 若 $\mathbb{Z}$ 中的素数 p, q 满足 $p \equiv q \mod 4$, 则 p, q 在 $\mathbb{Q}(\mathrm{i})$ 上有相同的分解类型.

练习 2. 仿照课本例 8.23 验证一个 $d \equiv 1 \mod 4$ 时二次互反律的例子.

练习 3. 尝试使用 Gauss 的二次互反律证明二次互反律. 体会这两个二次互反律本质上是相同的.

高次互反律应该是什么样子的?

Abel 数域的互反律. 设 K 是 Abel 数域, 若 K 的导子为 D 且 $\mathbb{Z}$ 中的素数 p, q 满足 $p \equiv q \mod D$, 则 p, q 在 K 上有相同的分解类型.

上述定理中分解类型的定义需要用到代数整数环.

上述定理确实简洁漂亮, 但看似美好的背后有着巨大的漩涡: 导子 D 的确定是比较困难的!