习题 - 代数学

Jun

2020 年 9 月 19 日

1 基本概念

问题 1.1. 定义欧拉函数 $\varphi : \mathbb{N}^{\times} \to \mathbb{C}$, $\varphi(n)$ 的值为 $0, 1, \cdots, n-1$ 中与 n 互素的元素个数. 即 $\varphi(n) = \#\{x \in \mathbb{N}, 0 \leq x \leq n-1 | (x, n) = 1\}$.

(1) $\varphi(n) = \#\left(\mathbb{Z}/n\right)^{\times}$

证明. 由 Bezout 定理, $(a, n) = 1 \Leftrightarrow \exists b, c, \text{s.t.} ab + cn = 1$. 因此

$\left(\mathbb{Z}/n\right)^{\times} = \left\{\bar{a} \in \mathbb{Z}/n : \exists \bar{b} \in \mathbb{Z}/n, \text{s.t.} \bar{a} \cdot \bar{b} = \bar{1}\right\} = \{\bar{a} \in \mathbb{Z}/n : (a, n) = 1\}$ □

(2) 欧拉函数 φ 是积性函数. 即若 m, n 互素, 则有 $\varphi(mn) = \varphi(m)\varphi(n)$

证明. 构造如下数表

$$
\begin{array}{cccccc}
1 & 2 & \cdots & r & \cdots & m \\
m+1 & m+2 & \cdots & m+r & \cdots & 2m \\
2m+1 & 2m+2 & \cdots & 2m+r & \cdots & 3m \\
\vdots & \vdots & & \vdots & & \vdots \\
(n-1)m+1 & (n-1)m+2 & \cdots & (n-1)m+r & \cdots & nm
\end{array}
$$

那么 $\varphi(mn)$ 表示数表中与 mn 互素的数的个数, 也就是与 m, n 同时互素的数的个数 (由于 m, n 互素).

由带余除法, 任意一个 $s \in \{1, 2, \ldots, mn\}$ 可以写为 □

(3) 若 n 的素因子分解为 $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ (其中 $p_1, p_2, \ldots, p_r$ 为互异素数, $e_i \geq 1, i = 1, 2, \ldots, r$). 则

$$\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p^i}\right)$$

引理. 若 p 为素数, 则 $\varphi(p^m) = p^m\left(1-\frac{1}{p}\right)$

证明. 除了 p 的倍数以外的数都与 p^m 互素. □

2 群论

问题 2.1. 设 $G = \{x_1, x_2, \ldots, x_n\}$ 为有限群. 定义群矩阵 A, A 的第 i 行 j 列为 $x_i x_j^{-1}$. 则 A 有如下分解:

$$A = x_1A_1 + x_2A_2 + \cdots + x_nA_n,\ \text{其中}A_i\text{为置换矩阵}$$

因此有映射 $\varphi : x_i \mapsto A_i$. 证明:

(1) $\{A_1, A_2, \ldots, A_n\}$ 是一个群.

(2) $\varphi(x_ix_j) = \varphi(x_i)\varphi(x_j)$, 即 φ 为群同构.

证明. (1) (提示) 注意到置换矩阵相乘仍为置换矩阵

(2) (提示) 考虑第 ij 位置, 设 $x_ix_j^{-1} = x_k$, 则 $x_kx_j = x_i$. 固定 x_k, 让 j 跑遍 1~n, 就有

$$x_k(x_1, x_2, \ldots, x_n) = (x_1, x_2, \ldots, x_n)A_k$$

容易验证

$$x_lx_k(x_1, x_2, \ldots, x_n) = x_l(x_1, x_2, \ldots, x_n)A_k = (x_1, x_2, \ldots, x_n)A_lA_k$$

□

注. 这个例子告诉我们一个常用思路: 群中的乘法不好考虑时, 可以固定其中一个变元, 并将群看作一个线性空间, 取定其上的一组基, 转而考虑该变元在这组基上的作用 (线性变换).

3 环论

4 域论

问题 4.1. 设 V 为 n 维实线性空间, $M \subseteq \mathrm{End}V$, 满足

(1) $\mathrm{id} \in M, 0 \notin M$;

(2) 若 $\mathscr{A},\mathscr{B}\in M$, 则 $\mathscr{A}\mathscr{B}\in M$ 或 $\mathscr{B}\mathscr{A}\in M$;

(3) 若 $\mathscr{A},\mathscr{B}\in M$, 则 $\mathscr{A}\mathscr{B}=\mathscr{B}\mathscr{A}$ 或 $\mathscr{A}\mathscr{B}=-\mathscr{B}\mathscr{A}$;

(4) 若 $\mathscr{A}\in M$ 且 $\mathscr{A}\neq\pm\mathrm{id}$, 则存在 $\mathscr{B}\in M$, s.t. $\mathscr{A}\mathscr{B}=-\mathscr{B}\mathscr{A}$

证明: M 中的元素个数不超过 $2n^2$.

(朱富海 < 给大一学生的 Galois 理论 > 问题 1.33)

证明. (提示: 证明一个集合元素个数不超过线性空间的维数, 可以去证明这个集合的元素是线性无关的. 此处 n^2 暗示维数, $\mathscr{A},-\mathscr{A}$ 可以同时出现, 所以有个 2 倍.)

首先证明 $\forall\mathscr{A}\in M$, 都有 $\mathscr{A}^2=\pm\mathrm{id}$.

任取 $\mathscr{A}\in M$, 由 (2) 得 $\mathscr{A}^2\in M$. 如果 $\mathscr{A}^2\neq\pm\mathrm{id}$, 则由 (4), $\exists\mathscr{B}\in M$, s.t.$\mathscr{A}^2\mathscr{B}=-\mathscr{B}\mathscr{A}^2$. 另一方面, 若 $\mathscr{A}\mathscr{B}=\mathscr{B}\mathscr{A}$, 则 $\mathscr{A}^2\mathscr{B}=\mathscr{A}(\mathscr{A}\mathscr{B})=\mathscr{A}(\mathscr{B}\mathscr{A})=(\mathscr{A}\mathscr{B})\mathscr{A}=\mathscr{B}\mathscr{A}^2$; 若 $\mathscr{A}\mathscr{B}=-\mathscr{B}\mathscr{A}$, 则 $\mathscr{A}^2\mathscr{B}=\mathscr{A}(\mathscr{A}\mathscr{B})=\mathscr{A}(-\mathscr{B}\mathscr{A})=-(\mathscr{A}\mathscr{B})\mathscr{A}=\mathscr{B}\mathscr{A}^2$. 即总有 $\mathscr{A}^2\mathscr{B}=\mathscr{B}\mathscr{A}^2$. 所以 $M\ni\mathscr{A}^2\mathscr{B}=0$, 这与 (1) 矛盾.

然后证明 M 中不同且不互为相反数的元素线性无关.

(反证法) 假设 M 中不同且不互为相反数的元素线性相关, 那么一定可以找到一个最小的 n, 使得 M 中不同且不互为相反数的 n 个元素线性相关. 设 $\mathscr{A}_1,\mathscr{A}_2,\cdots,\mathscr{A}_n\in M$ 互不相同且 $\forall i\neq j$, $\mathscr{A}_i+\mathscr{A}_j\neq 0$, $\mathscr{A}_1,\mathscr{A}_2,\cdots,\mathscr{A}_n$ 线性相关. $\exists k_i\neq 0$, s.t. $\sum_{i=1}^n k_i\mathscr{A}_i=0$. 不妨设 $\mathscr{A}_1=\pm\mathrm{id}$(否则考虑 $\sum_{i=1}^n k_i\mathscr{A}_1\mathscr{A}_i=0$), 则 $\mathscr{A}_2,\cdots,\mathscr{A}_n\neq\pm\mathrm{id}$.

由 $\mathscr{A}_n\neq\pm\mathrm{id}$ 和 (4) 可知 $\mathscr{C}\in M$, s.t. $\mathscr{A}_n\mathscr{C}=-\mathscr{C}\mathscr{A}_n$. 不妨假设对 $1\leq i\leq t$, $\mathscr{A}_i\mathscr{C}=\mathscr{C}\mathscr{A}_i$; 对 $t+1\leq i\leq n-1$, $\mathscr{A}_i\mathscr{C}=-\mathscr{C}\mathscr{A}_i$. 对式子

$$\sum_{i=1}^{n-1}k_i\mathscr{A}_i=-k_n\mathscr{A}_n$$

分别用 $\mathscr{C}$ 左作用和右作用, 得

$$\sum_{i=1}^{t}k_i\mathscr{C}\mathscr{A}_i+\sum_{i=t}^{n-1}k_i\mathscr{C}\mathscr{A}_i=-k_n\mathscr{C}\mathscr{A}_n$$

$$\sum_{i=1}^{t}k_i\mathscr{A}_i\mathscr{C}+\sum_{i=t}^{n-1}k_i\mathscr{A}_i\mathscr{C}=-k_n\mathscr{A}_n\mathscr{C}$$

由于对 $t+1\leq i\leq n$, $\mathscr{A}_i\mathscr{C}=-\mathscr{C}\mathscr{A}_i$. 故将两式相加, 得到

$$\sum_{i=1}^{t}k_i\mathscr{C}\mathscr{A}_i=0$$

而 $t \leq n-1$, 与 n 的最小性矛盾.

因此, M 中不同且不互为相反数的元素线性无关. 而 $\dim M \leq n^2$. 故 $|M| \leq 2n^2$. □

问题 4.2 (Dedekind-Artin)**.** 设 G 是一个幺半群, $\mathbb{K}$ 是一个域 (则 $K^* := \mathbb{K} - \{0\}$ 是一个群). $\sigma_1, \sigma_2, \ldots, \sigma_n$ 是两两不同的非零同态 $G \to K^*$, 则它们在 $\mathbb{K}$ 上线性无关.

证明. 假设存在这样的一组非零同态, 使得它们在 $\mathbb{K}$ 上线性无关, 则一定能找到其中元素个数最少的一组. 设 n 是满足

$$a_1\sigma_1 + \cdots + a_n\sigma_n = 0,\ a_i \in \mathbb{K}\text{不全为}0$$

的最小的正整数. 则 $n \geq 2$, a_i 均不为 0.

因为 σ_1, σ_2 不同, 故 $\exists z \in G$ 使得 $\sigma_1(z) \neq \sigma_2(z)$. 对于任意 $x \in G$, 都有

$$a_1\sigma_1(xz) + \cdots + a_n\sigma_n(xz) = 0$$

由于 σ_i 是同态, 则有

$$a_1\sigma_1(z)\sigma_1 + \cdots + a_n\sigma_n(z)\sigma_n = 0$$

两边同除 σ_1 并与第一个式子相减, 得

$$\left(a_2\frac{\sigma_2(z)}{\sigma_1(z)} - a_2\right)\sigma_2 + \cdots + \left(a_n\frac{\sigma_n(z)}{\sigma_1(z)} - a_n\right)\sigma_n = 0$$

其第一个系数就不为 0, 且比第一个式子少一个元素, 这与 n 的最小性矛盾.

因此, 任意一组两两不同的非零同态 $G \to K^*$ 在 $\mathbb{K}$ 上线性无关. □

问题 4.3 (Artin)**.** 设 $\mathbb{E}$ 为数域, G 为 $\mathrm{Aut}\mathbb{E}$ 的有限子群

$$\mathbb{F} = \mathbb{E}^G = \{\alpha \in \mathbb{E} \mid \phi(\alpha) = \alpha, \forall \phi \in G\}$$

则 $|G| \geq [\mathbb{E} : \mathbb{F}]$.

证明. 设 $G = \{\sigma_1 = \mathrm{id}, \sigma_2, \ldots, \sigma_n\}$. 要证 $[\mathbb{E} : \mathbb{F}] \leq |G| = n$, 只要证 $\mathbb{E}$ 上任意 $n+1$ 个元素在 $\mathbb{F}$ 上线性相关.

$\forall \alpha_1, \alpha_2, \ldots, \alpha_n, \alpha_{n+1} \in \mathbb{E}$, 则 $\mathbb{E}$ 上的线性方程组

$$\begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_{n+1}) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_{n+1}) \\ \vdots & \vdots & & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_1(\alpha_{n+1}) \end{pmatrix}_{n\times(n+1)} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_{n+1} \end{pmatrix} = 0$$

必有非 0 解 (未知数的个数大于方程个数).

考虑其中包含非 0 元素最少的非零解 $\begin{pmatrix} b_1 & b_2 & \cdots & b_m & 0 & \cdots & 0 \end{pmatrix}$, 其中 $b_i \neq 0, i = 1, 2, \ldots, m$. 不妨设 $b_1 = 1$, (否则考虑 $\begin{pmatrix} 1 & \dfrac{b_2}{b_1} & \cdots & \dfrac{b_m}{b_1} & 0 & \cdots & 0 \end{pmatrix}$).

方程组两边用 σ_i 作用, 由 σ_i 是同态, 可以得到 $\begin{pmatrix} \sigma_i(b_1) & \sigma_i(b_2) & \cdots & \sigma_i(b_m) & 0 & \cdots & 0 \end{pmatrix}$ 是一组非零解, 其中 $\sigma_i(b_1) = \sigma_i(1) = 1$. 将两组解相减, 得

$$\begin{pmatrix} 0 & \sigma_i(b_2) - b_2 & \cdots & \sigma_i(b_m) - b_m & 0 & \cdots & 0 \end{pmatrix}$$

也是一组非零解. 但这组解比 $\begin{pmatrix} b_1 & b_2 & \cdots & b_m & 0 & \cdots & 0 \end{pmatrix}$ 含有更少的非零元, 因此它只能是零解, 即

$$\sigma_i(b_j) = b_j,\ \forall 1 \leq i \leq n,\ 1 \leq j \leq m$$

由 $\mathbb{F}$ 的定义知 $b_j \in \mathbb{F}$, $\forall 1 \leq j \leq m$. 所以

$$0 = \sum_{j=1}^{n+1} \sigma_1(\alpha_j) b_j = \sum_{j=1}^{n+1} \mathrm{id}(\alpha_j) b_j = \sum_{j=1}^{n+1} b_j \alpha_j$$

这表明 $\alpha_1, \ldots, \alpha_{n+1}$ 在 $\mathbb{F}$ 上线性相关. $\square$