《瀚海之巅》2024 第 2 期 · 征解解答

中国科大数学科学学院团委　《瀚海之巅》项目组

日期：2024 年 4 月 19 日

1. 我们来考察有限阿贝尔群的对偶群 (**dual group**) 的相关性质. 对阶为 n 的有限阿贝尔群 G, 定义 $\hat{G}$ 是所有 $G \to \mathbb{C}_{\neq 0}$ 的积性复值函数构成的集合, 也就是说, 对任意 $e \in \hat{G}$, 以及任意 $a, b \in G$, $e(a \cdot b) = e(a)e(b)$.
   (a) $\hat{G}$ 是群. 验证 $\hat{G}$ 在以下运算下构成阿贝尔群:
   $$(e_1 \cdot e_2)(a) = e_1(a)e_2(a),\ \forall a \in G.$$
   (b) 证明: 对任意 $e \in \hat{G}$, 以及任意 $a \in G$, $e(a)$ 是某个 n 次单位根.
   (c) $\hat{G}$ 的阶. 研究所有 $G \to \mathbb{C}$ 的复值函数构成的向量空间 V, 在 V 上定义 Hermite 内积
   $$(f, g) = \frac{1}{n}\sum_{a \in G} f(a)\overline{g(a)}.$$
   (i) 证明: $\hat{G}$ 的元素在上述内积下构成一组标准正交向量组, 进而 $|\hat{G}| \leq n$.
   (ii) 证明: $\hat{G}$ 的元素在上述内积下构成一组标准正交基, 进而 $|\hat{G}| = n$.
   (d) $\hat{G}$ 的结构. 证明: $\hat{G} \cong G$.

供题人: 胡洁洋

证明. (a) 对任意 $e_1, e_2 \in \hat{G}$, 和任意 $a, b \in \hat{G}$,

$$(e_1 \cdot e_2)(a \cdot b) = e_1(a \cdot b)e_2(a \cdot b) = e_1(a)e_2(a)e_1(b)e_2(b) = (e_1 \cdot e_2)(a)(e_1 \cdot e_2)(b),$$

从而 $e_1 \cdot e_2 \in \hat{G}$.

结合律: 任取 $e_1, e_2, e_3 \in \hat{G}$, 和 $a \in G$, 有

$$[(e_1 \cdot e_2) \cdot e_3](a) = [e_1 \cdot (e_2 \cdot e_3)](a) = e_1(a)e_2(a)e_3(a),$$

从而 $(e_1 \cdot e_2) \cdot e_3 = e_1 \cdot (e_2 \cdot e_3)$, 结合律成立.

单位元存在性: 令 $e_{\mathrm{Id}} = 1, \forall a \in G$, 不难验证其为 $\hat{G}$ 的单位元.

逆元存在性: 对 $e \in \hat{G}$, 令 $e^{-1}(a) = e(a)^{-1}$, 不难验证 $e^{-1} \in \hat{G}$, 且 $e_{\mathrm{Id}} = e \cdot e^{-1} = e^{-1} \cdot e$.

同时, 任取 $e_1, e_2 \in \hat{G}$, 类似可验证 $e_1 \cdot e_2 = e_2 \cdot e_1$.

综上, $\hat{G}$ 构成阿贝尔群.

(b) 设 1_G 是 G 的单位元. $e(1_G) = e(1_G \cdot 1_G) = e(1_G)^2$, 得 $e(1_G) = 1$. 又对任意

$a \in G$, $a^n = 1_G$, 从而

$$1 = e(1_G) = e(a^n) = e(a)e(a^{n-1}) = \cdots = e(a)^n,$$

即 $e(a)$ 是某个 n 次单位根.

(c) (i) 一方面, 对任意 $e \in \hat{G}$,

$$(e, e) = \frac{1}{n}\sum_{a\in G} e(a)\overline{e(a)} = \frac{1}{n}\sum_{a\in G} |e(a)|^2 = 1,$$

另一方面, 对 $e_1, e_2 \in \hat{G}$, $e_1 \neq e_2$, 下证 $(e_1, e_2) = 0$. 任取 $b \in G$ 满足 $e_1(b) \neq e_2(b)$.

$$\begin{aligned}
(e_1, e_2) &= \frac{1}{n}\sum_{a\in G} e_1(a)\overline{e_2(a)} \\
&= \frac{1}{n}\sum_{a\in G} (e_1 \cdot e_2^{-1})(a) \\
&= \frac{1}{n}\sum_{a\in G} (e_1 \cdot e_2^{-1})(ab \cdot b^{-1}) \\
&= \frac{(e_1 \cdot e_2^{-1})(b)^{-1}}{n}\sum_{a\in G} (e_1 \cdot e_2^{-1})(ab) \\
&= \frac{(e_1 \cdot e_2^{-1})(b)^{-1}}{n}\sum_{a\in G} (e_1 \cdot e_2^{-1})(a) \\
&= (e_1 \cdot e_2^{-1})(b)^{-1}(e_1, e_2),
\end{aligned}$$

由 $(e_1 \cdot e_2^{-1})(b) \neq 1$, 我们有 $(e_1, e_2) = 0$. 进而 $\hat{G}$ 的元素在上述内积下构成一组标准正交向量组. 平凡地, $\dim V = n$, 而正交向量组必为线性无关组, 故 $|\hat{G}| \leq n$.

(ii) 我们只需验证任意 $f : G \to \mathbb{C}$ 都是 $\hat{G}$ 中元素的线性组合. 考虑证明

$$f = \frac{n}{|\hat{G}|}\sum_{e\in\hat{G}} (f, e)e.$$

引理. 对任意 $a \neq 1_G$, 有

$$\sum_{e\in\hat{G}} e(a) = 0.$$

引理证明: 先说明存在 $e_0 \in \hat{G}$, $e_0(a) \neq 1$. 由有限阿贝尔群的结构定理, 设

$$G \cong \mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \cdots \times \mathbb{Z}_{p_l^{k_l}}.$$

同构映射 φ 将 a 映为 $(\overline{\alpha_1}, \overline{\alpha_2}, \cdots, \overline{\alpha_l})$, 不失一般性, $\overline{\alpha_1} \neq \overline{0}$. 取

$$e_0(\varphi^{-1}(\overline{\beta_1}, \overline{\beta_2}, \cdots, \overline{\beta_l})) = \exp\left(\frac{2\beta_1\pi i}{p_1^{k_1}}\right), \forall \beta_1, \beta_2, \cdots, \beta_l \in \mathbb{Z},$$

即满足条件. 进而, 类似 (i),

$$\sum_{e\in\hat{G}} e(a) = \sum_{e\in\hat{G}} (e\cdot e_0)(a) = e_0(a)\sum_{e\in\hat{G}} e(a),$$

我们有

$$\sum_{e\in\hat{G}} e(a) = 0.$$

回原题. 任取 $a\in G$,

$$\begin{aligned}
\frac{n}{|\hat{G}|}\sum_{e\in G}(f,e)e(a) &= \frac{1}{|\hat{G}|}\sum_{e\in\hat{G}} e(a)\sum_{b\in G} f(b)\overline{e(b)} \\
&= \frac{1}{|\hat{G}|}\sum_{b\in G} f(b)\sum_{e\in\hat{G}} e(ab^{-1}) \\
&= \frac{1}{|\hat{G}|}f(a)\sum_{e\in\hat{G}} e(aa^{-1}) + \frac{1}{|\hat{G}|}\sum_{\substack{b\in\hat{G}\\ b\neq a}} f(b)\sum_{e\in\hat{G}} e(ab^{-1}) \\
&= f(a) + \frac{1}{|\hat{G}|}\sum_{\substack{b\in\hat{G}\\ b\neq a}} f(b)\sum_{e\in\hat{G}} e(ab^{-1}) \\
&= f(a).
\end{aligned}$$

故

$$f = \frac{n}{|\hat{G}|}\sum_{e\in\hat{G}}(f,e)e.$$

由此, $\hat{G}$ 的元素在上述内积下构成一组标准正交基, 进而 $|\hat{G}| = n$.

(d) 分三步证明.

第一步: 结论对有限循环群成立. 考虑 n 阶循环群 $G = \langle a\rangle$. 则 $e(a^k) = e(a)^k$, 进而 e 由 $e(a)$ 完全决定, 构造映射 $\psi: G\to\hat{G}$, $[\psi(a^k)](a^m) = \exp\left(\dfrac{2km\pi i}{n}\right)$, 不难验证确实是同构映射.

第二步: 证明 $\widehat{G_1\times G_2}\cong\hat{G}_1\times\hat{G}_2$. 注意对任意 $e\in\hat{G}$, 存在 $e_i\in\hat{G}_i(i=1,2)$, 使得对任意 $g_i\in G_i(i=1,2)$, $e(g_1,g_2) = (e_1(g_1),e_2(g_2))$, 对任意 $e_i\in\hat{G}_i(i=1,2)$, 也有唯一的 e 与它们对应, 进而得证.

第三步: 证明本问题. 注意到

$$\begin{aligned}
\hat{G} &\cong \mathbb{Z}_{p_1^{k_1}}\times\widehat{\mathbb{Z}_{p_2^{k_2}}\times\cdots}\times\mathbb{Z}_{p_l^{k_l}} \\
&\cong \mathbb{Z}_{p_1^{k_1}}\times\widehat{\mathbb{Z}_{p_2^{k_2}}\times\cdots}\times\mathbb{Z}_{p_{l-1}^{k_{l-1}}}\times\widehat{\mathbb{Z}_{p_l^{k_l}}} \\
&\cdots \\
&\cong \widehat{\mathbb{Z}_{p_1^{k_1}}}\times\widehat{\mathbb{Z}_{p_2^{k_2}}}\times\cdots\times\widehat{\mathbb{Z}_{p_l^{k_l}}} \\
&\cong \mathbb{Z}_{p_1^{k_1}}\times\mathbb{Z}_{p_2^{k_2}}\times\cdots\times\mathbb{Z}_{p_l^{k_l}} \\
&\cong G.
\end{aligned}$$

命题得证.

□

2. (范德蒙德行列式的推广) 在平稳随机过程的研究中, 出现了下述行列式:

$$\Delta_n(k_1,x_1;\ldots;k_m,x_m)=\begin{vmatrix} M_{k_1}^n(x_1)\\ M_{k_2}^n(x_2)\\ \vdots\\ M_{k_m}^n(x_m)\end{vmatrix},$$

其中 $x_1,x_2,\ldots,x_m$ 是未知量; $k_1,\ldots,k_m$ 是正整数, $k_1+k_2+\cdots+k_m=n$; $M_k^n(x)$ 是 $k\times n$ 阶矩阵, 形如

$$M_k^n(x)=\begin{pmatrix} 1 & x & x^2 & \cdots & x^{n-1}\\ 0 & 1 & \binom{2}{1}x & \cdots & \binom{n-1}{1}x^{n-2}\\ 0 & 0 & 1 & \cdots & \binom{n-1}{2}x^{n-3}\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & 0 & \ldots & \binom{n-1}{k-1}x^{n-k}\end{pmatrix}.$$

证明:

$$\Delta_n(k_1,x_1;\ldots;k_m,x_m)=\prod_{1\leqslant i<j\leqslant m}(x_j-x_i)^{k_ik_j}.$$

供题人: 郭维基

证明. 对 n 做归纳, 当 $n=2$ 时, 结论显然成立. 假设小于 n 时结论均成立, 当 n 时, 将 $\Delta_n(k_1,x_1;\ldots;k_m,x_m)$ 的每一列乘以 x_1 , 然后用后一列减去这一乘积. 注意到 $\binom{n+1}{m+1}-\binom{n}{m+1}=\binom{n}{m}$, 故有

$$M_{k_1}^n(x_1)\to M_{k_1,1}^n(x_1)=\begin{pmatrix} 1 & 0 & 0 & 0 & \cdots & 0\\ 0 & 1 & x_1 & x_1^2 & \cdots & x_1^{n-2}\\ 0 & 0 & 1 & \binom{2}{1}x_1 & \cdots & \binom{n-2}{1}x_1^{n-3}\\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & 0 & \cdots & \cdots & \binom{n-2}{k_1-2}x_1^{n-k_1}\end{pmatrix}$$

而对于任一 $i=2,3,\ldots,m$ 有

$$M_{k_i}^n(x_i)\to M_{k_i,1}^n(x_i)=$$

$$\begin{pmatrix} 1 & x_i-x_1 & x_i(x_i-x_1) & x_i^2(x_i-x_1) & \cdots & x_i^{n-2}(x_i-x_1)\\ 0 & 1 & (x_i-x_1)+x_i & \binom{2}{1}x_i(x_i-x_1)+x_i^2 & \cdots & \binom{n-2}{1}x_i^{n-3}(x_i-x_1)+x_i^{n-2}\\ 0 & 0 & 1 & (x_i-x_1)+\binom{2}{1}x_i & \cdots & \binom{n-2}{2}x_i^{n-4}(x_i-x_1)+\binom{n-2}{1}x_i^{n-3}\\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & 0 & \cdots & \cdots & \binom{n-2}{k_i-1}x_i^{n-k_i-1}(x_i-x_1)+\binom{n-2}{k_i-2}x_i^{n-k_i}\end{pmatrix}$$

现在将 Δ_n 按 $M_{k_1,1}^n$ 的第一行展开, 则 $M_{k_1,1}(x_1)$ 的剩余部分即为 $M_{k_1-1}^{n-1}(x_1)$. 对于 $M_{k_i}^n(x_i)(i\neq 1)$ 的剩余部分, 先将第一行公因式的 (x_i-x_1) 提取出来, 再用第二行

减去第一行, 然后第二行也有了公因式 $(x_i - x_1)$, 将这一公因式提取出来后又用第三行减去第二行, 第三行也有了公因式 $(x_i - x_1)\cdots\cdots$ 如此反复进行下去, 最终会得到 $M_{k_i}^{n-1}(x_i)$, 并且总共提取出来了 k_i 个 $(x_i - x_1)$. 于是, 经过上面的变形, 我们得到

$$\Delta_n(k_1, x_1; \ldots; k_m, x_m) = \prod_{i=2}^{m} (x_i - x_1)^{k_i} \Delta_{n-1}(k_1 - 1, x_1; \ldots; k_m, x_m) \tag{1}$$

而由归纳假设, 我们有

$$\Delta_{n-1}(k_1 - 1, x_1; \ldots; k_m, x_m) = \prod_{2 \leqslant i < j \leqslant m} (x_j - x_i)^{k_i k_j} \prod_{t=2}^{m} (x_t - x_1)^{(k_1 - 1)k_t} \tag{2}$$

将 (2) 代入 (1) 即得所求证. □

3. (a) 证明: 存在无穷多个正整数 n, 使得 $\sigma(n)\varphi(n)$ 不为完全平方数;
   (b) 证明: 存在无穷多个正整数 n, 使得 $\sigma(n)\varphi(n)$ 为完全平方数.

供题人: 邓博文

证明. (a) 取 n 为素数, 此时 $\sigma(n)\varphi(n) = n^2 - 1$ 不为完全平方数, 这样的 n 有无穷多个.

(b) 设素数从小到大排列为 $p_1 < p_2 < \cdots$. 若满足 $\sigma(n)\varphi(n)$ 为完全平方数的 n 只有有限个, 取正整数 α 使得这些 n 的最大素因子不超过 p_α. 由素数定理, 存在充分大的 $\varepsilon \in \mathbb{N}^*$, 使得

$$\#\left\{p | p\text{是素数}, p \in \left(\frac{p_\varepsilon + 1}{2}, p_\varepsilon\right]\right\} > \alpha.$$

设 $\beta \in \mathbb{N}^*$ 满足

$$p_\beta \leq \frac{p_\varepsilon + 1}{2} < p_{\beta+1},$$

则

$$\varepsilon - \beta = \pi(p_\varepsilon) - \pi(\frac{p_\varepsilon + 1}{2}) > \alpha,$$

即 $\varepsilon - \alpha > \beta$. 定义函数 $g : \mathbb{N}^* \mapsto \mathbb{N}^*$,

$$g(t) = \prod_{\substack{p\text{为素数} \\ v_p(t)\text{为奇数}}} p.$$

注意到

$$\prod_{i=\alpha+1}^{\beta} (p_i^2 - 1) = 2^{2\varepsilon - 2\alpha} \prod_{i=\alpha+1}^{\varepsilon} \frac{p_i - 1}{2} \prod_{i=\alpha+1}^{\varepsilon} \frac{p_i + 1}{2},$$

从而

$$\Omega\left(\prod_{i=\alpha+1}^{\varepsilon} p_i^2 - 1\right) \leq \frac{p_\varepsilon + 1}{2}.$$

而对任意集合 $A \subseteq \{\alpha + 1, \alpha + 2, \cdots, \varepsilon\}$,

$$g\left(\prod_{i \in A} (p_i^2 - 1)\right) \in \left\{\prod_{i=1}^{\beta} p_i^{r_i} \middle| r_i \in \{0, 1\}, 1 \leq i \leq \beta\right\},$$

从而 $g\left(\prod_{i\in A}(p_i^2-1)\right)$ 的取值至多有 2^β 种可能. 又这样的 A 一共有 $2^{\varepsilon-\alpha}$ 个, 且 $2^{\varepsilon-\alpha}>2^\beta$, 故存在两个不同的集合 $A_1,A_2\subseteq\{\alpha+1,\alpha+2,\cdots,\varepsilon\}$, 使得

$$g\left(\prod_{i\in A_1}(p_i^2-1)\right)=g\left(\prod_{i\in A_2}(p_i^2-1)\right),$$

这说明

$$\prod_{i\in A_1}(p_i^2-1)\prod_{i\in A_2}(p_i^2-1)$$

为完全平方数, 进而

$$\prod_{i\in A_1\Delta A_2}(p_i^2-1)$$

为完全平方数. 取非空集合 $A'=A_1\Delta A_2$, 令

$$l=\prod_{i\in A'}p_i,$$

则

$$\sigma(l)\varphi(l)=\prod_{i\in A_1\Delta A_2}(p_i^2-1)$$

为完全平方数. 又 l 含有大于 p_α 的素因子, 这与反证假设矛盾, 原命题得证.

□

4. 设 $P_0(x_0,y_0),P_1(x_1,y_1),\cdots,P_n(x_n,y_n)$ 是平面直角坐标系 xOy 中的 $n+1$ 个整点, 其横坐标满足 $x_1-x_0,x_2-x_1,\cdots,x_n-x_{n-1}$ 是互异的正整数, 纵坐标满足 $y_0<y_1<\cdots<y_n$, 且斜率满足

$$\frac{y_1-y_0}{x_1-x_0}<\frac{y_2-y_1}{x_2-x_1}<\cdots<\frac{y_n-y_{n-1}}{x_n-x_{n-1}}.$$

已知对 $i=0,1,\cdots,n-3$, 在直线 $P_iP_{i+1},P_{i+1}P_{i+1},P_{i+2}P_{i+3}$ 所围成三角形的内部与边界上只有两个整点 (即 P_{i+1} 与 P_{i+2}). 求证:$x_1-x_0,x_2-x_1,\cdots,x_n-x_{n-1}$ 至多有 2^{n-1} 种可能的大小顺序.

供题人: 徐子健

证法 1, 徐子健. 先证明如下引理.

引理.

$$x_2-x_1<\max\{x_1-x_0,x_3-x_2\}.$$

引理证明: 不妨设 $P_1(0,0)$ 再设 $P_2(p,q)$, 那么我们知道 p,q 互质.

设 $pp'\equiv1\pmod q,qq'\equiv1\pmod p$ 且 $p'\in\{1,2,\cdots,q-1\},q'\in\{1,2,\cdots,p-1\}$.

由 $pp'+qq'\equiv1\pmod p,pp'+qq'\equiv1\pmod q$ 且 p,q 互质知 $pp'+qq'\equiv1\pmod{pq}$. 又由于 $1<pp'+qq'<2pq$ 故

$$pp'+qq'=pq+1.$$

考虑点 $X(q',q-p')$ 于是有

$$\frac{q-p'}{q'}<\frac{q}{p}.$$

故 X 在 P_1P_2 下方. 由题设, X 在 P_0P_1 或者 P_2P_3 下方.

若 X 在 P_0P_1 下方, 设 $P_0(-p_1,-q_1)$, 于是

$$\frac{q-p'}{q'}<\frac{q}{p_1}<\frac{q}{p}.$$

于是

$$p_1(q-q')+1\le q_1q',pq_1\le p_1q-1.$$

相乘得

$$q'(p_1q-1)\ge pp_1(q-p')+p.$$

于是

$$p_1=p_1(pp'+qq'-pq)\ge p+q'>p.$$

此即 $x_2-x_1<x_1-x_0$.

若 X 在 P_2P_3 下方, 设 $P_3(p+p_2,q+q_2)$, 于是

$$\frac{q}{p}<\frac{q_2}{p_2}<\frac{p'}{p-q'}.$$

于是

$$p_2q+1\le pq_2,q_2(p-1')\le p_2p'-1.$$

相乘得

$$p(p_2p'-1)\ge(p-q')(p_2q+1).$$

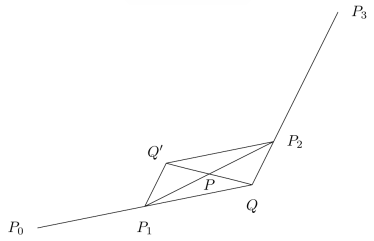
于是

$$p_2=p_2(pp'+qq'-pq)\ge 2p-q'>p.$$

此即 $x_2-x_1<x_3-x_2$.

引理的叙述对 $P_i,P_{i+1},P_{i+2},P_{i+3}$ 都成立, 反复使用即可得到结论. □

证法 2, 杨文颜. 类似地我们也要证明证法 1 中的引理, 然而为了证明之我们先来证明一个引理.



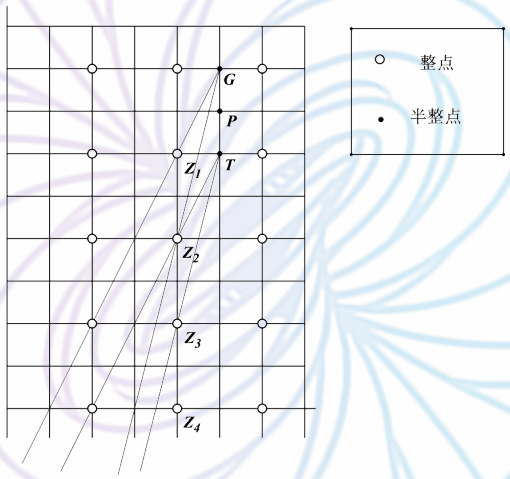
我们构作平行四边形 P_1QP_2Q', 由题设平行四边形 P_1QP_2Q' 内仅有 P_1,P_2 为整点.

引理 1. 称坐标为整数或半整数的点为半整点. 若 $x_2-x_1>1$ 且 $y_2-y_1>1$, 则平行四边形 P_1QP_2Q' 内仅有 P_1,P,P_2 为半整点.

引理 1 证明. 仅对 P 的横纵坐标均为半整数的情形证明, 其余两种情形类似.

若不然, 不妨设平行四边形 P_1QP_2Q' 包含如图所示的 G,P,T 三个整点.(包含横向的三个半整点同理会与 $y_2-y_1>1$ 矛盾)

由于 P_0P_1 斜率为正, 且平行四边形 P_1QP_2Q' 不能包含 Z_1 作为整点除非 $Z_1=P_1$ 但这与 $x_2-x_1>1$ 矛盾. 故 P_1 一定位于 GZ_1 这条线下方, 故我们可以看出 GZ_1 和 TZ_2 这一条平行带状区域内只有 $Z_2=P_1$ 是可能的, 但这与 $x_2-x_1>1$ 矛盾. 又由于平行四边形 P_1QP_2Q' 不能包含 Z_2 作为整点, 故 P_1 一定位于 GZ_2 这条线的下方. 重复上述过程, P_1 无论选取在何处总会得到矛盾.



我们回到主要引理[1]的证明.

$x_2-x_1=1$ 或 $y_2-y_1=1$ 时引理显然成立. 下设 $x_2-x_1>1, y_2-y_1>1$. 由引理 1, 平行四边形 P_1QP_2Q' 内仅有 P_1,P,P_2 为半整点. 由 Minkowski 定理可知 $S_{P_1QP_2Q'}\le 1$. 记 $Q(x,y)$ 可以得到

$$S_{P_1QP_2Q'}=-(y-y_1)(x_2-x)+(y_2-y)(x-x_1)\le 1.$$

即

$$\frac{y_2-y}{x_2-x}-\frac{y-y_1}{x-x_1}\le\frac{1}{(x_2-x)(x-x_1)}\le\frac{4}{(x_2-x_1)^2}.$$

记 $p_1=y_1-y_0, q_1=x_1-x_0, p_2=y_3-y_2, q_2=x_3-x_2, p=y_2-y_1, q=x_2-x_1$. 于是我们得到

$$LHS=\frac{p_1q_2-p_2q_1}{q_1q_2}\le\frac{4}{q^2}=RHS.$$

[1]指证法 1 中的引理.

若 $p_1q_2-p_2q_1\geq 4$, 则 $q_1q_2\geq q^2$, 故 $\max\{q_1,q_2\}\geq q$. 现在只需考虑 $p_1q_2-p_2q_1=1,2,3$ 的情形.

引理 2. 若 $p_1q_2-p_2q_1=n$, 则 $nq\geq q_1+q_2$.

引理 2 证明. 此时 $\dfrac{p_1}{q_1}<\dfrac{p}{q}<\dfrac{p_2}{q_2}$, 故 $p_1qq_2<pq_1q_2<p_2q_1q$, 而 $pq_1q_2-p_1qq_2=(pq_1-p_1q)q_2\geq q_2, p_2q_1q-pq_1q_2=(p_2q-pq_2)q_1\geq q_1$, 而 $p_2q_1q-p_1qq_2=q(p_2q_1-p_1q_2)=n$, 即得.

设 $p_1q_2-p_2q_1=1$, 由引理 2 与上述结果 $q\geq q_1+q_2$, 而 $q_1q_2\geq\dfrac{1}{4}q^2$, 故 $4q_1q_2\geq(q_1+q_2)^2$ 即 $(q_1-q_2)^2\leq 0$, 矛盾!

设 $p_1q_2-p_2q_1=2$, 由引理 2 与上述结果 $2q\geq q_1+q_2$, 而 $q_1q_2\geq\dfrac{1}{2}q^2$, 故 $8q_1q_2\geq(q_1+q_2)^2$, 矛盾!

设 $p_1q_2-p_2q_1=3$, 由引理 2 与上述结果 $3q\geq q_1+q_2$, 而 $q_1q_2\geq\dfrac{3}{4}q^2$, 故 $12q_1q_2\geq(q_1+q_2)^2$, 矛盾!

故引理成立. □

5. 证明: 对 $n\in\mathbb{N}^*$,

$$\begin{vmatrix} 1 & \frac{1}{2} & \frac{1}{3} & \cdots & \frac{1}{n} \\ \frac{1}{2} & 1 & \frac{1}{2} & \cdots & \frac{1}{n-1} \\ \frac{1}{3} & \frac{1}{2} & 1 & \cdots & \frac{1}{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{1}{n} & \frac{1}{n-1} & \frac{1}{n-2} & \cdots & 1 \end{vmatrix}>0.$$

供题人: 邓博文

证明. 命题等价于

$$\sum_{i=1}^{n}\sum_{j=1}^{n}\frac{1}{1+|i-j|}x_ix_j$$

为正定二次型, 也即

$$\sum_{i=1}^{n}\sum_{j=1}^{n}\frac{a_ia_j}{1+|i-j|}\geq 0,$$

等号成立当且仅当 $a_1=a_2=\cdots=a_n=0$.

断言 1.

$$\sum_{k\in\mathbb{Z}}\mathrm{e}^{ikx}r^{|k|}=\frac{1-r^2}{1-2r\cos x+r^2}.(r<1)$$

断言 1 证明.

$$\begin{aligned} LHS&=-1+\sum_{k=0}^{+\infty}\mathrm{e}^{ikx}r^k+\sum_{k=0}^{+\infty}\mathrm{e}^{-ikx}r^k\\ &=-1+\frac{1}{1-r\mathrm{e}^{ix}}+\frac{1}{1-r\mathrm{e}^{-ix}}\\ &=RHS. \end{aligned}$$

断言 2.

$$\sum_{k\in\mathbb{Z}}\frac{1}{1+|k|}\mathrm{e}^{ikx}=\int_0^1\frac{1-r^2}{1-2r\cos x+r^2}\mathrm{d}r>0.$$

断言 2 的证明.

$$\begin{aligned}LHS&=\sum_{k\in\mathbb{Z}}\int_0^1 r^{|k|}\mathrm{d}r\cdot\mathrm{e}^{ikx}\\&=\int_0^1\sum_{k\in\mathbb{Z}}r^{|k|}\mathrm{e}^{ikx}\mathrm{d}r\\&=\int_0^1\sum_{k\in\mathbb{Z}}\mathrm{e}^{ikx}r^{|k|}\mathrm{d}r\\&=\int_0^1\frac{1-r^2}{1-2r\cos x+r^2}\mathrm{d}r\\&>0.\end{aligned}$$

断言 3. 对 $k\in\mathbb{Z}_{\neq 0}$,

$$\int_0^{2\pi}\mathrm{e}^{ikx}\mathrm{d}x=0.$$

此断言平凡地成立.

从而结合断言 3,

$$\begin{aligned}&\int_0^{2\pi}\left(\sum_{k\in\mathbb{Z}}\frac{1}{1+|k|}\mathrm{e}^{ikx}\right)\left|\sum_{k=1}^n a_k\mathrm{e}^{ikx}\right|^2\mathrm{d}x\\=&\int_0^{2\pi}\left(\sum_{k\in\mathbb{Z}}\frac{1}{1+|k|}\mathrm{e}^{ikx}\right)\left(\sum_{k=1}^n a_k\mathrm{e}^{ikx}\right)\left(\sum_{k=1}^n a_k\mathrm{e}^{-ikx}\right)\mathrm{d}x\\=&\int_0^{2\pi}\left(\sum_{k\in\mathbb{Z}}\frac{1}{1+|k|}\mathrm{e}^{ikx}\right)\left(\sum_{1\le s,t\le n}a_sa_t\mathrm{e}^{i(s-t)x}\right)\mathrm{d}x\\=&\int_0^{2\pi}\sum_{1\le s,t\le n}a_sa_t\mathrm{e}^{i(t-s)x}\frac{1}{1+|s-t|}\mathrm{e}^{i(s-t)}\mathrm{d}x\\=&2\pi\sum_{1\le s,t\le n}\frac{a_sa_t}{1+|s-t|},\end{aligned}$$

则由断言 2,

$$\sum_{1\le i,j\le n}\frac{a_ia_j}{1+|i-j|}=\frac{1}{2\pi}\int_0^{2\pi}\left(\sum_{k\in\mathbb{Z}}\frac{1}{1+|k|}\mathrm{e}^{ikx}\right)\left|\sum_{k=1}^n a_k\mathrm{e}^{ikx}\right|^2\mathrm{d}x\ge 0.$$

取等时, $\forall x\in(0,2\pi)$,

$$\sum_{k=1}^n a_k\mathrm{e}^{ikx}=0.$$

故对任意 $x_1, x_2, \cdots, x_n \in (0, 2\pi)$, 有

$$\begin{cases} \mathrm{e}^{ix_1}a_1 + \mathrm{e}^{2ix_1}a_2 + \cdots + \mathrm{e}^{nix_1}a_n = 0, \\ \mathrm{e}^{ix_2}a_1 + \mathrm{e}^{2ix_2}a_2 + \cdots + \mathrm{e}^{nix_2}a_n = 0, \\ \qquad \cdots \\ \mathrm{e}^{ix_n}a_1 + \mathrm{e}^{2ix_n}a_2 + \cdots + \mathrm{e}^{nix_n}a_n = 0, \end{cases}$$

系数行列式

$$\begin{vmatrix} \mathrm{e}^{ix_1} & \mathrm{e}^{2ix_1} & \cdots & \mathrm{e}^{nix_1} \\ \vdots & \vdots & & \vdots \\ \mathrm{e}^{ix_n} & \mathrm{e}^{2ix_n} & \cdots & \mathrm{e}^{nix_n} \end{vmatrix} = \prod_{j=1}^{n} \mathrm{e}^{ix_j} \prod_{1 \le s < t \le n} (e^{ix_t} - e^{ix_s}),$$

取定一组 $(x_1, \cdots, x_n)$, 使得 $\prod\limits_{1 \le s < t \le n} (e^{ix_t} - e^{ix_s}) \neq 0$, 这表明 $a_1 = a_2 = \cdots = a_n = 0$. 进而, 原命题成立.

□

6. 设 $\mathcal{A} \subset \mathcal{P}(X)$ 是一个代数, $\mathcal{A}_\sigma$ 是 $\mathcal{A}$ 中集合的可数并的全体, $\mathcal{A}_{\sigma\delta}$ 是 $\mathcal{A}_\sigma$ 中集合的可数交的全体. 设 μ 是 $\mathcal{A}$ 上的一个预测度, $\mu^\star(E) = \inf\left\{\sum\limits_{i=1}^{\infty} \mu(E_i) : E_i \in \mathcal{A}, E \subset \bigcup\limits_{i=1}^{\infty} E_i\right\}$ 是 μ 诱导的外测度, 证明:
   (1) 对于任意 $E \in X$ 以及 $\epsilon > 0$, 存在 $A \in \mathcal{A}_\sigma$ 满足 $E \subset A$ 且 $\mu^\star(A) \le \mu^\star(E) + \epsilon$.
   (2) 如果 $\mu^\star(E) < \infty$, 则 E 是 $\mu^\star$-可测的当且仅当存在 $B \in \mathcal{A}_{\sigma\delta}$ 满足 $E \subset B$ 且 $\mu^\star(B \setminus E) = 0$.
   (3) 设 (X, M, μ) 是一个测度空间, $\mu^\star(E) = \inf\{\sum\limits_{i=1}^{\infty} \mu(E_i) : E_i \in M, E \subset \bigcup\limits_{i=1}^{\infty} E_i\}$ 是 μ 诱导的外测度, $M^\star$ 是 $\mu^\star$-可测集全体, $\widehat{\mu} = \mu^\star|_{M^\star}$. 证明: $\widehat{\mu}$ 是 μ 的完备化的饱和化.

供题人: 李梦喆

证明. (1) 根据 $\mu^\star$ 定义知, $\forall \epsilon > 0$, $\exists E_i \in \mathcal{A}$, 使得 $E \subset \bigcup\limits_{i=1}^{\infty} E_i$ 且 $\sum\limits_{i=1}^{\infty} \mu(E_i) \le \mu^\star(E) + \epsilon$, 令 $A = \bigcup\limits_{i=1}^{\infty} E_i$, 则 $A \in \mathcal{A}_\sigma$ 满足 $E \subset A$, $\mu^\star(A) = \mu^\star(\sum\limits_{i=1}^{\infty} E_i) \le \sum\limits_{i=1}^{\infty} \mu^\star(E_i) \le \mu^\star(E) + \epsilon$.

(2) ($\Longrightarrow$): 根据 (1), 存在 $A_n \in \mathcal{A}$, 满足 $E \subset A_n$ 且 $\mu^\star(A_n) \le \mu^\star(E) + \frac{1}{n}$. 因为 E 是 $\mu^\star-$ 可测的, $\mu^\star(A_n) = \mu^\star(A_n \cap E) + \mu^\star(A_n \cap E^c) = \mu^\star(E) + \mu^\star(A_n \setminus E)$. 因为 $\mu^\star(E) < \infty$, 两边同时减去 $\mu^\star(E)$ 得到 $\mu^\star(A_n \setminus E) = \mu^\star(A_n) - \mu^\star(E)$. 令 $B = \bigcap\limits_{n=1}^{\infty} A_n$, 则 $E \subset B$, $0 \le \mu^\star(B \setminus E) \le \mu^\star(A_n \setminus E) = \mu^\star(A_n) - \mu^\star(E) \le \frac{1}{n}$, 令 $n \to \infty$ 得 $\mu^\star(B \setminus E) = 0$.

($\Longleftarrow$): 根据定义, 我们只要证明对于任意的 $A \subset X$, $\mu^\star(A) \geqslant \mu^\star(A \cap E) + \mu^\star(A \cap E^c)$. 由 $Carathéodory$ 定理知 B 是 $\mu^\star-$ 可测的, 因此 $\mu^\star(A) = \mu^\star(A \cap$

$B)+\mu^\star(A\cap B^c)$. 所以我们只需证明 $\mu^\star(A\cap B)+\mu^\star(A\cap B^c)\geqslant\mu^\star(A\cap E)+\mu^\star(A\cap E^c)$. 因为 $A\cap B\supset A\cap E$, 因此 $\mu^\star(A\cap B)\geqslant\mu^\star(A\cap E)$. 由于 $\mu^\star(A\cap E)\leq\mu^\star(E)<\infty$, 因此我们只需证明 $\mu^\star(A\cap B^c)\geqslant\mu^\star(A\cap E^c)$. 根据条件知 $\mu^\star(B\cap E^c)=\mu^\star(B\setminus E)=0$. 注意到 $A\cap E^c\subseteq(A\cap B^c)\cup(B\cap E^c)$, 因此 $\mu^\star(A\cap B^c)=\mu^\star(A\cap B^c)+\mu^\star(B\cap E^c)\geqslant\mu^\star(A\cap E^c)$.

(3) 我们记 M 的完备化为 $\overline{M}$, M 的饱和化为 $\widetilde{M}$. 我们先证明以下三个引理

引理 1. 如果 $E\in M^\star$ 且 $\mu^\star(E)<\infty$, 则 $E\in\overline{M}$.

引理 1 证明. 因为 $E\in M^\star$, 所以 E 和 E^c 都是 $\mu^\star-$ 可测的. 根据 (2), 存在 B_1、$B_2\in M$, 使得 $E\subset B_1,\mu^\star(B_1\setminus E)=0,E^c\subset B_2,\mu^\star(B_2\setminus E)=0$. 因此 $E=B_2^c\cup(E\setminus B_2^c)$, $B_2^c\in M$, $E\setminus B_1^c\subset B_1\setminus B_1^c=B_1\cap B_2$, 由完备化的定义知我们只需证明 $\mu^\star(B_1\cap B_2)=0$. 由于 $B_1\cap B_2\subset(B_1\cap E^c)\cup(B_2\cap E)$, 因此 $0\leq\mu^\star(B_1\cap B_2)\leq\mu^\star(B_1\cap E^c)+\mu^\star(B_2\cap E)=0$, 这就推出 $\mu^\star(B_1\cap B_2)=0$.

引理 2. $\forall E\subset X,\exists B\in M$, 满足 $E\subset B$ 且 $\mu^\star(B)=\mu^\star(E)$.

引理 2 证明. 根据 (1), 存在 $A_n\in M$, 满足 $E\subset A_n$ 且 $\mu^\star(A_n)\leq\mu^\star(E)+\frac{1}{n}$. 令 $B=\bigcap\limits_{n=1}^{\infty}A_n$, 则 $E\subset B$ 且 $\mu^\star(E)\leq\mu^\star(B)\leq\mu^\star(E)+\frac{1}{n}$, 令 $n\to\infty$, 即得 $\mu^\star(B)=\mu^\star(E)$.

引理 3. 如果 $A\in\overline{M}$, 则 $A\in M^\star$ 且 $\mu^\star(A)=\overline{\mu}(A)$.

引理 3 证明. 根据完备化的定义, 设 $A=E\cup F$, 其中 $E\in M$, $F\subset N$, $\mu(N)=0$. 因此 $\mu^\star(F)\leq\mu^\star(N)=\mu(N)=0\Longrightarrow\mu^\star(F)=0.\forall P\subset X$, $\mu^\star(P\cap F)\leq\mu^\star(F)=0$, 因此 $\mu^\star(P)\geqslant\mu^\star(P\cap F^c)=\mu^\star(P\cap F^c)+\mu^\star(P\cap F)$, 所以 F 是 $\mu^\star-$ 可测的. 因为 $E\in M\subset M^\star$, 所以 E 也是 $\mu^\star-$ 可测的 $\Longrightarrow$ $A=E\cup F$ 是 $\mu^\star-$ 可测的, 即 $A\in M^\star$. 根据定义, $\overline{\mu}(A)=\mu(E)=\mu^\star(E)$. 而 $\mu^\star(E)\leq\mu^\star(A)=\mu^\star(E\cup F)\leq\mu^\star(E)+\mu^\star(F)=\mu^\star(E)$, 因此 $\mu^\star(A)=\mu^\star(E)=\overline{\mu}(A)$.

回到原题, 我们首先证明 $\widetilde{\overline{M}}=M^\star$. 任取 $E\in M^\star$, 对于 $\forall A\in\overline{M}$, 其中 A 满足 $\overline{\mu}(A)<\infty$, 由引理 3 知 $A\in M^\star$ 且 $\mu^\star(A)=\overline{\mu}(A)$, 因此 $E\cap A\in M^\star$ 且 $\mu^\star(E\cap A)\leq\mu^\star(A)<\infty$, 再由引理 1 知 $E\cap A\in\overline{M}$. 因此 $E\in\widetilde{\overline{M}}$, 故 $M^\star\subset\widetilde{\overline{M}}$. 反过来, 任取 $E\in\widetilde{\overline{M}}$, 我们只需证明对于 $\forall A\subset X,\mu^\star(A)\geqslant\mu^\star(A\cap E)+\mu^\star(A\cap E^c)$. 由引理 2 知存在 $B\in M$, 满足 $A\subset B$ 且 $\mu^\star(B)=\mu^\star(A)$, 由外测度的单调性知我们只需证明 $\mu^\star(B)\geqslant\mu^\star(B\cap E)+\mu^\star(B\cap E^c)$. 若 $\mu^\star(B)=\infty$, 则不等式自然成立, 下讨论 $\overline{\mu}(B)=\mu(B)=\mu^\star(B)<\infty$ 的情况. 此时由饱和化的定义知因为 E、$E^c\in\widetilde{\overline{M}}$, 所以 $E\cap B$、$E^c\cap B\in\overline{M}$, 由引理 3 和测度的可加性知 $\mu^\star(B)=\overline{\mu}(B)=\overline{\mu}(B\cap E)+\overline{\mu}(B\cap E^c)=\mu^\star(B\cap E)+\mu^\star(B\cap E^c)$. 因此, $\widetilde{\overline{M}}\subset M^\star$, 综上我们便证明了 $\widetilde{\overline{M}}=M^\star$. 以下证明 $\widetilde{\mu}=\mu^\star$. 任取 $E\in M^\star$, 若

$E \in \overline{M}$, 由饱和测度定义知 $\widetilde{\overline{\mu}}(E) = \overline{\mu}(E) = \mu^\star(E)$；若 $E \notin \overline{M}$, 则由引理 1 知 $\mu^\star(E) = \infty$, 由饱和测度定义知 $\widetilde{\overline{\mu}}(E) = \infty = \mu^\star(E)$.

□

7. 设 $A(t), B(t)$ 和 $C(t)$ 是三个实值连续可微函数, 满足方程组:

$$\begin{cases} A' = 4\dfrac{(B-C)^2 - A^2}{BC} \\ B' = 4\dfrac{(A-C)^2 - B^2}{AC} \\ C' = 4\dfrac{(A-B)^2 - C^2}{AB}. \end{cases}$$

在给定初值条件 $A(0) = A_0 > 0, B(0) = B_0 > 0, C(0) = C_0 > 0$ 的情况下, 求证:

(1) 该方程组的解的右行最大存在区间有限.

(2) 设这个最大的右行区间为 $[0, T)$, 则 $\lim\limits_{t\to T} A(t) = \lim\limits_{t\to T} B(t) = \lim\limits_{t\to T} C(t) = 0$, 且 $\lim\limits_{t\to T} \frac{A(t)}{B(t)} = \lim\limits_{t\to T} \frac{B(t)}{C(t)} = 1$.

供题人: 计科羽

证明. 由对称性, 我们可以假设初值的大小关系 $A_0 \le B_0 \le C_0$, 然后证明 $A(t) \le B(t) \le C(t)$ 对任意 $t \in [0, T)$ 成立:

$$(B-A)' = 4\frac{(C-A)^2B - B^3 - (B-C)^2A + A^3}{ABC} = 4(B-A)\frac{C^2 - (A+B)^2}{ABC}.$$

由于 $\frac{C^2-(A+B)^2}{ABC}$ 为 $[0, T)$ 光滑函数, 且 $B_0 - A_0 \ge 0$, 可知 $B(t) - A(t) \ge 0$ 对 $\forall t \in [0, T)$ 成立, 同理 $C(t) \ge B(t)$ 对 $\forall t \in [0, T)$ 成立.

现在做 (1), 为此研究 C 的变化:

$$C' = -8 + \frac{4(A^2 + B^2 - C^2)}{AB} \le -8 + \frac{4A}{B} \le -4.$$

这表明 $T < +\infty$, 否则 C 会在有限时间内变为 0, 这是不允许的.

下面对 C 的上界进行控制, 为此, 计算:

$$\left(\frac{C-A}{A}\right)' = \frac{C'A - A'C}{A^2} = 8\left(\frac{C-A}{A}\right)\left(\frac{B-A-C}{AB}\right) \le 0.$$

于是 $\frac{C-A}{A} \le \frac{C_0-A_0}{A_0}$, 由此可得 $C(t) \le \lambda A(t), \forall t \in [0, T)$, 这表明

$$\lim_{t\to T^-} A(t) = \lim_{t\to T^-} B(t) = \lim_{t\to T^-} C(t) = 0.$$

最后来证 (2), 为此只需要证 $\lim\limits_{t\to T^-} \dfrac{C(t) - A(t)}{A(t)} = 0$. 假设不然, 则

$$\left| \int_0^T \frac{\mathrm{d}}{\mathrm{d}t}\left[\log\left(\frac{C-A}{A}\right)\right] \mathrm{d}t \right| < +\infty.$$

根据前面的计算, 这表明

$$\left| \int_0^T \frac{B-A-C}{AB} \mathrm{d}t \right| < +\infty.$$

由于 $-\frac{C}{AB} \le \frac{B-A-C}{AB} \le -\frac{1}{B}$, 可知 $\frac{B-A-C}{AB} \sim -\frac{1}{A} (t \to T^-)$, 于是只需研究 A^{-1} 作为

$[0,T]$ 上瑕积分的敛散性.

$$A' = -8 + 4\frac{B^2 + C^2 - A^2}{BC} \geq -8 + 4\frac{C}{B} \geq -4 \lim_{t\to T^-} A(t) = 0.$$

得到 $A(t) \leq 4(T-t)$, 故 $A^{-1} \geq \frac{1}{4(T-t)}$, 它在 $[0,T]$ 上的积分发散! 这样便得到矛盾. 由此

$$\lim_{t\to T^-} \frac{C(t)}{A(t)} = 1 \Rightarrow \lim_{t\to T^-} \frac{B(t)}{C(t)} = \lim_{t\to T^-} \frac{A(t)}{B(t)} = 1.$$

评论. 此题背景是 Ricci 流理论中的 Isenberg-Jackson 定理, 其具体研究了在对称性充分好的 $\mathbb{S}^3$ 上, 给定初始度量后相应 Ricci 流的解的性态. 为此, 视 $\mathbb{S}^3 = SU(2)$ 为李群并考虑其李代数生成元

$$x_1 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, x_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, x_3 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

之后取 $\{x_1, x_2, x_3\}$ 的对偶左不变 1-形式 $\{\sigma^1, \sigma^2, \sigma^3\}$. 则 $\mathbb{S}^3$ 上的度量可以表示为

$$g = A\sigma^1 \otimes \sigma^1 + B\sigma^2 \otimes \sigma^2 + C\sigma^3 \otimes \sigma^3.$$

将其代入 Ricci 流方程 $\frac{\partial g(t)}{\partial t} = -2\mathrm{Ric(g(t))}$ 中就可计算得到题目中的方程.

在该题目结论的基础上, 还可进一步得到

$$\lim_{t\to T^-} \frac{A(t)}{4(T-t)} = \lim_{t\to T^-} \frac{B(t)}{4(T-t)} = \lim_{t\to T^-} \frac{C(t)}{4(T-t)} = 1.$$

这表明度量 $\frac{1}{4(T-t)}g(t)$ 在 $t \to T^-$ 时收敛于 $\mathbb{S}^3$ 上标准度量, 这就是 Ricci 流研究中常用的爆破技巧.

□

8. A 是一个戴德金整环, K 为其分式域, $L|K$ 为一个可分扩张,N 为 L 的伽罗瓦闭包, $\mathfrak{p}$ 为 A 的素理想, 证明: $\mathfrak{p}$ 在 L 上完全分裂当且仅当 $\mathfrak{p}$ 在 N 上完全分裂.

供题人: 励随之

证明. 记 A 在 L 中的整闭包为 B, 在 N 中的整闭包为 C, 熟知 B, C 都是戴德金整环, 考察 $\mathfrak{p}$ 在其中的分解情况

$$\mathfrak{p} = \prod_{i=1}^{n} \mathfrak{p}_i = \prod_{i=1}^{n} \prod_{j=1}^{m_i} \mathfrak{q}_{i,j}.$$

其中 $\mathfrak{p}_i$ 是 B 的素理想,$\mathfrak{q}_{i,j}$ 是 C 的素理想,$\mathfrak{p}_i = \prod_{j=1}^{m_i} \mathfrak{q}_{i,j}$.

假设 $\mathfrak{p}$ 在 N 上完全分裂, 则 $\mathfrak{q}_{i,j}$ 两两不同,$[C/\mathfrak{q}_{i,j} : A/\mathfrak{p}] = 1$. 由于理想的唯一分解性, 这当然给出 $\mathfrak{p}_i$ 是 B 中互不相同的素理想, 并且 $B/\mathfrak{p}_i$ 作为 $C/\mathfrak{q}_{i,j}$ 的子域, 自然有 $\mathfrak{p}_i$ 在 $\mathfrak{p}$ 上惯性度数为 1, 即 $\mathfrak{p}$ 在 L 上完全分裂.

反之设 $\mathfrak{p}$ 在 L 上完全分裂. 记 $G = \mathrm{Gal}(N|K), H = Gal(N|L), P_{\mathfrak{p}}$ 为所有在 $\mathfrak{p}$ 上的 B 的素理想构成的集合,$\mathfrak{P}$ 为某个在 $\mathfrak{p}$ 上的 C 中素理想,$G_{\mathfrak{P}} = \{\sigma \in G | \sigma\mathfrak{P} = \mathfrak{P}\}$,$H\backslash G/G_{\mathfrak{P}}$ 为 G 关于 H 和 $G_{\mathfrak{P}}$ 的双陪集, 熟知如下双射:

$$H\backslash G/G_{\mathfrak{P}} \to P_{\mathfrak{p}} : H\sigma G_{\mathfrak{P}} \to \sigma\mathfrak{P} \cap L.$$

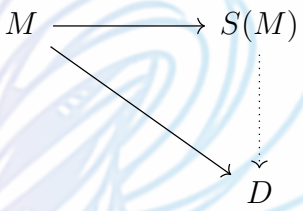
$\mathfrak{p}$ 在 L 中完全分裂即 $|P_{\mathfrak{p}}| = [L:K] = [G:H]$, 即双陪集的个数与 H 的右陪集个数一致, 而双陪集为有限个右陪集的不交并, 因此有 $H\sigma G_{\mathfrak{P}} = H\sigma, \forall \sigma \in G$, 这就给出 $G_{\mathfrak{P}}$ 的所有共轭都在 H 中, 记 $G_{\mathfrak{P}}$ 生成的正规子群为 $N(G_{\mathfrak{P}})$, 那么 $N(G_{\mathfrak{P}}) \leq H$, 根据伽罗瓦对应, 其对应于比 L 大的 K 的某个正规扩张, 由于 N 是正规闭包, 因此就是 N, 这说明 $N(G_{\mathfrak{P}}) = 1$, 给出 $G_{\mathfrak{P}} = 1$, 而在 $\mathfrak{p}$ 上的 C 中不同的素理想和 $G/G_{\mathfrak{P}}$ 一一对应, 因此在 C 中共有 $|\mathrm{Gal}(N|K)| = |N:K|$ 个素理想在 $\mathfrak{p}$ 上, 根据基本等式即知 $\mathfrak{p}$ 在 N 上完全分裂.

□

9. 我们将构造两个含幺交换环 R, S, 使得 R, S 不同构, 但多项式环 $R[T]$ 与 $S[T]$ 同构.

   (a) 前置: 对称代数 (Symmetric Algebra)

      i. 定义: 设 A 为含幺交换环, M 为 $A-$ 模,$S(M)$ 是一个 $A-$ 代数, 使得对所有 $A-$ 代数 D, 以及 $A-$ 模同态 $M \to D$, 存在唯一 A 代数同态 $S(M) \to D$ 使得以下图表交换.



      以下证明几个对称代数的简单性质:

      ii. $S(M)$ 具有唯一性.

      iii. 对自由模 $M = \oplus_{i=1}^{n} AX_i, S(M) = A[X_1, \ldots, X_n]$; 对 $M = \oplus_{i=1}^{n} AX_i/(Ay_1 + \cdots + Ay_m), S(M) = A[X_1, \ldots, X_n]/(y_1 + \cdots + y_m)$.

      iv. $S(M \oplus N) = S(M) \otimes_A S(N)$.

   (b) 令 $A = \mathbb{R}[X,Y,Z]/(X^2+Y^2+Z^2-1) = \mathbb{R}[x,y,z]$, 其中 x, y, z 分别为 X, Y, Z 在商环中的像.

      i. 令

$$\phi : A^3 \to A$$

$$(a,b,c) \longmapsto ax + by = cz$$

      令 $E = \ker\phi$, 则 $A^3 \xrightarrow{\sim} E \oplus A$(提示: 用分裂引理 (splitting lemma)).

      ii. 证明 $S(E)[T] \xrightarrow{\sim} A[P,Q,T]$, 其中 P, Q, T 为多项式环的变元.

      iii. 证明 $S(E) = A[U,V,W]/(xU + yV + zW)$.

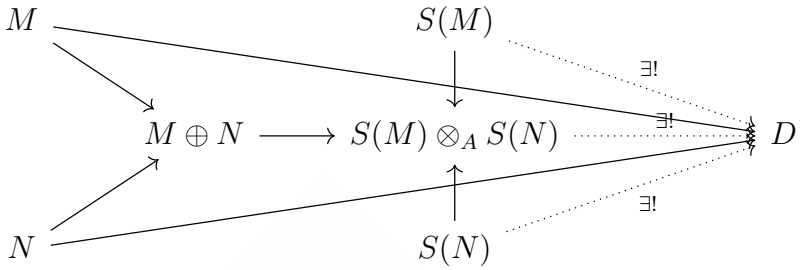
      iv. 证明 $S(E)$ 与 $A[P,Q]$ 不同构.

供题人: 孙之棋

证明. (a) ii: 泛性质具有唯一性.

iii: 略

iv: 由交换图知.



(b) i.

$$0 \longrightarrow E \longrightarrow A^3 \underset{\psi}{\overset{\phi}{\rightleftarrows}} A \longrightarrow 0$$

$$a(x,y,z) \longmapsto a$$

ii. $S(E)[T]$=$S(E) \otimes_A A[T]$=$S(E \oplus A)$=$S(A^3) = A[P,Q,T]$.

iii. 由 (a).iii.

iv. 若 $\varphi : A[P,Q] \to S(E)$ 为同构. $A[P,Q]$ 与 $S(E)$ 中的可逆元均只有 $\mathbb{R}$, 故 $\varphi(\mathbb{R}) = \mathbb{R}$. 并且 $\mathrm{Aut}(\mathbb{R}) = \{\mathrm{Id}\}$. 故该映射保持 R. 容易验证 $A[P,Q], A[U,V,W]/(xU+yV+zW)$ 中方程 $X^2+Y^2+Z^2=1$ 的解均在 A 中, 故 $\varphi(A) = A$. 复合上 A 的自同构, 不妨设 φ 保持 A 中所有元素. 设 $c = \varphi(P), c' = \varphi(Q)$. 设 $c = c_0 + c_1 + \ldots, c' = c'_0 + c'_1 + \ldots$. 其中 c_i, c'_i 均为 i 次齐次式. 注意到 $Ac_1 + Ac'_1 = (AU + AV + AW)/(xU + yV + zW) = E$. 但容易证明 E 不可被两个元素生成, 由此得出矛盾.

□