پاسخ سوالات مسابقه دانشجویی ریاضی دانشگاه صنعتی شریف، اسفند ۱۳۹۰

گردآوری: خشایار فیلُم

روز اول

سوال ۱. *۲۰۱۲ نقطه در $\mathbb{R}^2$ داریم. ثابت کنید یک چندجمله‌ای غیرصفر با درجه حداکثر ۶۲ و ضرایب حقیقی مانند $P(x,y)$ وجود دارد که همه‌ی این نقاط روی منحنی $P(x,y)=0$ واقع باشند.* (طراح: عرفان صلواتی)

پاسخ سوال ۱. *مجموعه‌ی همه‌ی چندجمله‌ای‌های دومتغیره با ضرایب حقیقی و درجه‌ی حداکثر ۶۲ را با Π نمایش می‌دهیم. نگاشت $T:\Pi\to\mathbb{R}^{2012}$ را نگاشتی می‌گیریم که به هر عضو Π مقادیر آن را در نقاط مذکور در مساله نسبت می‌دهد. به وضوح Π یک فضای برداری و T نگاشتی خطی است. از طرفی مجموعه‌ی زیر یک پایه برای Π تشکیل می‌دهد:*

$$\{x^iy^j \mid i,j\geq 0, i+j\leq 62\}$$

که ۲۰۱۶ عضوی است(تعداد اعضای آن تعداد جواب‌های نامنفی نامعادله‌ی $i+j\leq 62$ است و لذا برابر $\binom{64}{2}$ است.) بنابراین $\dim(\Pi)=2016$. پس $\ker(T)$ عضوی ناصفر مانند $P(x,y)$ دارد که همان چندجمله‌ای مطلوب است.

سوال ۲. *فرض کنید A یک ماتریس $n\times n$ با درایه‌های در یک میدان دلخواه F باشد. ثابت کنید ماتریس قطری D با درایه‌های در F موجود است به طوری که $A+D$ وارون‌پذیر باشد.* (طراح: دکتر جعفری، روزبه فرهودی)

پاسخ سوال ۲. *حکم را با استقرا بر $n\in\mathbb{N}$ ثابت می‌کنیم. در پایه‌ی استقرا، حالت $n=1$ بدیهی است؛ کافی است قرارداد:*

$$D=\begin{cases}[1] & A=0\\ [0] & A\neq 0\end{cases}$$

فرض کنید حکم برای n درست باشد. درستی آن را برای $n+1$ ثابت می‌کنیم: یک ماتریس $(n+1)\times(n+1)$، $A=[a_{ij}]_{1\leq i,j\leq n+1}$ با درایه‌های در F در نظر بگیرید. بلوک $n\times n$ پایین و راست A را $A'\in M_n(F)$ می‌گیریم (شکل ۱).

بنابر فرض استقرا، به ازای یک ماتریس قطری $n\times n$، D' با درایه‌های در F؛ $\det(A'+D')\neq 0$.

ماتریس‌های قطری $(n+1)\times(n+1)$ای به صورت شکل ۲ تعریف می‌کنیم.

برای اثبات حکم استقرا کافی است نشان داد که حداقل یکی از $\det(A+D_1)$ و $\det(A+D_0)$ ناصفر است که این هم از آن‌جا نتیجه می‌شود که با بسط دترمینان نسبت به سطر اول:

$$\det(A+D_1)-\det(A+D_0)=\det(A'+D')\neq 0$$

سوال ۳. *دنباله‌ی $\{a_n\}_{n=1}^{\infty}$ با جملات مثبت که $\lim_{n\to\infty}a_n=\infty$ داده شده است. نشان دهید دنباله‌ی نزولی $\{b_n\}_{n=1}^{\infty}$ با جملات مثبت وجود دارد به طوری که $\sum_{n=1}^{\infty}b_n<\infty$ و $\sum_{n=1}^{\infty}a_nb_n=\infty$.* (طراح: علی خزلی)

$$A=\left(\begin{array}{c|c} \frac{a_{11}}{a_{21}} & \frac{a_{12}\ \cdots\ a_{1(n+1)}}{A'} \\ \vdots & \\ a_{(n+1)1} & \end{array}\right)$$

شکل ۱: ماتریس A

$$D_1=\left(\frac{1}{0}\middle|\frac{0}{D'}\right),\ D_0=\left(\frac{0}{0}\middle|\frac{0}{D'}\right)$$

شکل ۲: ماتریس‌های قطری تعریف شده

پاسخ سوال ۳. *چون $\lim_{n\to\infty}$، از جایی به بعد a_nها از ۱ بیشتراند، مثلا با شروع از مکان k_1+1ام و به دلیل مثبت بودن جملات دنباله می‌توان نوشت: $a_n>0$ برای $1\le n\le k_1$. با استفاده‌ی مجدد از $\lim_{n\to\infty}a_n=\infty$، اگر از مکان k_1+1ام به اندازه‌ی کافی، مثلا k_2 واحد جلو برویم، a_n از ۲ بیشتر می‌شود. لذا برای $k_1+1\le n\le k_1+k_2$ داریم $a_n>1$ (به دلیل روش انتخاب k_1) در حالی که اگر $n\ge k_1+k_2+1$، a_n از ۲ بیشتر می‌شود. دوباره به دلیل $\lim_{n\to\infty}a_n=\infty$، اگر در میان nهایی که از k_1+k_2 بیشترند، n به اندازه‌ی کافی بزرگ شود، a_n از ۳ هم بیشتر خواهد بود. پس عدد طبیعی k_3ای موجود است که برای $n\ge k_1+k_2+k_3+1$ داریم $a_n>3$ در حالی که اگر $k_1+k_2+1\le n\le k_1+k_2+k_3$، $a_n>2$.*

با تکرار این روند، به دنباله‌ی $\{k_m\}_{m=1}^{\infty}$ از اعداد طبیعی می‌رسیم، با این ویژگی که برای $\sum_{j=1}^{m-1}k_j+1\le n\le\sum_{j=1}^{m}k_j$ داریم $a_n>(m-1)$. بنابراین در واقع دنباله حالتی به صورت زیر دارد:

$$\overbrace{a_1,\dots,a_{k_1}}^{\text{جملات بزرگتر از ۰}},\overbrace{a_{k_{1+2}},\dots,a_{k_1+k_2}}^{\text{جملات بزرگتر از ۱}},\overbrace{a_{k_1+k_2+1},\dots,a_{k_1+k_2+k_3}}^{\text{جملات بزرگتر از ۲}},\dots$$

از این روند ساختن k_jها به طور استقرایی، واضح است که اگر $k_1,\dots,k_m$ انتخاب شده باشند، چون از جایی به بعد a_nها از $m+1$ بیشترند، می‌توان k_{m+1} را (که تنها باید ویژگی $n>\sum_{j=1}^{m+1}k_j \Leftarrow a_n>m+1$ را برآورده کند) آنقدر بزرگ گرفت که

$$m^2k_m<(m+1)^2k_{m+1}$$

لذا دنباله‌ی $\{k_m\}_{m=1}^{\infty}$ از اعداد طبیعی را داریم، به قسمی که $\{m^2k_m\}_{m=1}^{\infty}$ صعودی است و برای $n>\sum_{j=1}^{m}k_j$ خواهیم داشت $a_n>m$.

حال قرار می‌دهیم:

$$b_n:=\frac{1}{m^2k_m}\quad \sum_{j=1}^{m-1}k_j+1\le n\le\sum_{j=1}^{m}k_j \ \text{برای}$$

در نتیجه $\{b_n\}_{n=1}^{\infty}$ دنباله‌ای نزولی و با جملات مثبت خواهد بود که:

$$\sum_{n=1}^{\infty}b_n=\sum_{m=1}^{\infty}k_m\left(\frac{1}{m^2k_m}\right)=\sum_{m=1}^{\infty}\frac{1}{m^2}<\infty$$

تنها ویژگی باقی‌مانده بررسی واگرا بودن سری $\sum_{n=1}^{\infty}a_nb_n$ است. توجه کنید که برای هر $m\in\mathbb{N}$:

$$\sum_{\sum_{j=1}^{m-1}k_j+1\le n\le\sum_{j=1}^{m}k_j}a_nb_n=\frac{1}{m^2k_m}\sum_{\sum_{j=1}^{m-1}k_j+1\le n\le\sum_{j=1}^{m}k_j}a_n>\frac{m-1}{m^2}$$

و نامساوی آخر به این دلیل است که در مجموع k_m تا جمله داریم که همگی از $m-1$ بیشترند. بنابراین

$$\sum_{m=1}^{\infty} \sum_{\sum_{j=1}^{m-1} k_j+1 \leq n \leq \sum_{j=1}^{m} k_j} a_n b_n > \sum_{m=1}^{\infty} \frac{m-1}{m^2} = \infty$$

چون تمامی $a_n b_n$ها مثبت‌اند، این واگرایی سری $\sum_{n=1}^{\infty} a_n b_n$ را به دست می‌دهد.

سوال ۴. اعداد طبیعی n و m به طوری که $2m \leq n$ داده شده‌اند و f تابعی است که به هر زیرمجموعه m عضوی
$N = \{1, \ldots, n\}$
یک عدد حقیقی منسوب می‌کند. اگر برای هر زیرمجموعه $m-1$ عضوی K از N داشته باشیم

$$\sum_{j \in N-K} f(K \cup \{j\}) = 0$$

نشان دهید برای هر زیرمجموعه m عضوی A از N داریم

$$\sum f(B) = (-1)^m f(A)$$

که این جمع روی تمام زیرمجموعه‌های m عضوی B از N که با A اشتراک ندارند، زده می‌شود. (طراح: خشایار فیلُم)

پاسخ سوال ۴. برای هر $0 \leq r \leq m$ قرار می‌دهیم $S_r = \sum_{|B|=m, |B \cap A|=r} f(B)$ (توجه کنید که چون $2m \leq n$، حتما چنین زیرمجموعه‌ی Bای از N موجود است). خواسته‌ی مساله اثبات $S_n = (-1)^m f(A)$ است، به علاوه اگر زیرمجموعه‌ی m عضوی B از $N = \{1, \ldots, n\}$ چنان باشد که $|B \cap A| = m$، آن‌گاه $A = B$ و لذا $S_m = f(A)$. پس به منظور حل مساله، نسبت S_{r+1}/S_r را می‌یابیم. بدین منظور $0 \leq r < m$ را تثبیت کنید. کمیت زیر را به دو روش می‌شماریم:

$$(*) T = \sum_{|B|=m, |B \cap A|=r} \sum_{x \in N-B, y \in B-A} f(B \cup \{x\} - \{y\})$$

روش اول محاسبه‌ی مجموع T در (*): روی $x \in N-B$ دو حالت داریم. حالت اول آن‌که x در $A-B$ باشد و حالت دوم آن‌که در $N - A \cup B$ باشد. در حالت اول که $x \in A-B$ و $y \in B-A$، اشتراک زیرمجموعه‌ی m عضوی $B \cup \{x\} - \{y\}$ از N با A برابر $|A \cap B| + 1 = r+1$ است و در حالت دوم که $x \in N - A \cup B$ و $y \in B-A$، اشتراک زیرمجموعه‌ی m عضوی $B \cup \{x\} - \{y\}$ از N با A برابر $|A \cap B| = r$ است. حال تعیین می‌کنیم که زیرمجموعه‌ی m عضوی‌ای همچون C از $N = \{1, \ldots, n\}$ که اشتراک‌اش با A، r یا $r+1$ عضوی باشد، چندبار در مجموع (*) به صورت $B \cup \{x\} - \{y\}$ ظاهر می‌گردد. پس فرض کنید که به ازای زیرمجموعه‌ی m عضوی B از N با $|A \cap B| = r$ و عناصر $x \in N-B$ و $y \in B-A$ داشته باشیم $C = B \cup \{x\} - \{y\}$. حالت اول آن است که $x \in A-B$. پس اشتراک $C = B \cup \{x\} - \{y\}$ با A برابر است با $(A \cap B) \cup \{x\}$ و لذا $r+1$ عضوی است. چون با تعیین x و y، B معین می‌گردد، تنها تعداد حالاتی که (با تثبیت C) برای چنین x و yای رخ می‌دهد را می‌شماریم. همان‌گونه که گفتیم، x به مجموعه‌ی $r+1$ عضوی $A \cap C$ تعلق دارد و لذا برای آن $r+1$ حالت داریم. چون $y \in B-A$ و $y \notin C$، برای y به تعداد

$$|N - (A \cup C)| = |N| - |A| - |C| + |A \cap C| = n - 2m + r + 1$$

حالت داریم. لذا در مجموع (*)، هر C با $|C| = m$ و $|A \cap C| = r+1$، $(r+1)(n-2m+r+1)$ بار ظاهر می‌گردد.
حالت دیگر آن است که در $C = B \cup \{x\} - \{y\}$ داشته باشیم $x \in N - (A \cup B)$ و $y \in B-A$. دوباره چون با تعیین چنین x و yای زیرمجموعه‌ی m عضوی B به طور یکتا تعیین می‌گردد، تعداد حالت‌های x و y را می‌شماریم. اینجا $A \cap C = A \cap B$ و لذا r عضوی است. باید $x \in C - A$ ولذا برای x

$$|A - C| = |A| - |A \cap C| = m - r$$

حالت داریم. در مورد y هم توجه کنید که مشابه بالا $y \in N - (A \cup C)$ که اینجا به دلیل $|A \cap C| = r$، به تعداد

$$|N - (A \cup C)| = |N| - |A| - |C| + |A \cap C| = n - 2m + r$$

حالت دارد. در نتیجه در مجموع (*)، هر C با $|C|=m$ و $|A\cap C|=r$، $(m-r)(n-2m+r)$ ظاهر می‌گردد. از این موارد:

$$T=(r+1)(n-2m+r+1)S_{r+1}+(m-r)(n-2m+r)$$

روش دوم محاسبه‌ی مجموع T در (*):

$$T=\sum_{|B|=m,|B\cap A|=r}\sum_{y\in B-A}\sum_{x\in N-B}f((B-\{y\})\cup\{x\})$$

با اعمال فرض مساله به زیرمجموعه‌ی $n-1$ عضوی $B-\{y\}$ از $N=\{1,\dots,n\}$ داریم:

$$0=\sum_{x\in N-(B-\{y\})}f((B-\{y\})\cup\{x\})=f(B)+\sum_{x\in N-B}f((B-\{y\})\cup\{x\})$$

حال با قرار دادن در بالا:

$$T=-\sum_{|B|=m,|B\cap A|=r}\sum_{y\in B-A}f(B)=-\sum_{|B|=m,|B\cap A|=r}|B-A|.f(B)=-(m-r)S_r$$

با مقایسه‌ی دو مقداری که برای T حاصل شد:

$$(r+1)(n-2m+r+1)S_{r+1}+(m-r)(n-2m+r)S_r=-(m-r)S_r$$

$$\Rightarrow(r+1)(n-2m+r+1)S_{r+1}=-(m-r)(n-2m+r+1)S_r$$

(چون $0\le r<m$، $n-2m+r+1$ ناصفر است.)

$$\Rightarrow(r+1)S_{r+1}=-(m-r)S_r$$

حال با ضرب تمامی تساوی‌های $(r+1)S_{r+1}=-(m-r)S_r$ برای $0\le r<m$ خواهیم داشت $S_m=(-1)^mS_0$ که همان حکم مطلوب است.

سوال ۵. فرض کنید $\mathbb{D}=\{z\in\mathbb{C}:|z|<1\}$ و $\partial\mathbb{D}=\{z\in\mathbb{C}:|z|=1\}$. ثابت کنید هر تابع تحلیلی $f:\mathbb{D}\to\mathbb{D}$ که به طور پیوسته به $\partial\mathbb{D}$ گسترش می‌یابد و $f(\partial\mathbb{D})\subset\partial\mathbb{D}$ به صورت حاصلضرب توابع موبیوس است (تابع موبیوس تابعی به شکل $z\mapsto e^{i\theta}\frac{z-\alpha}{1-\bar\alpha z}$ است که $\theta\in\mathbb{R}$ و $\alpha\in\mathbb{D}$). (طراح: **دکتر خاندانی، عرفان صلواتی**)

پاسخ سوال ۵. ابتدا توجه کنید که تعداد صفرهای f درون D متناهی است، چرا که اگر این‌گونه نباشد و f در یک دنباله‌ی نامتناهی $\{a_n\}_{n=1}^\infty$ از نقاط دو به دو متمایز D صفر شود، به دلیل فشردگی $\bar D=D\cup\partial D$، با جایگزین کردن $\{a_n\}_{n=1}^\infty$ با زیردنباله‌ای از آن در صورت لزوم، دنباله‌ی مذکور از ریشه‌های دو به دو متمایز f به یک $a\in\bar D=D\cup\partial D$ همگرا می‌شود که آن هم به دلیل پیوستگی نگاشت $\bar D\to\bar D$ حاصل از توسیع $f:D\to D$، باید ریشه‌ی f باشد. ولی به دلیل $f(\partial D)\subset\partial D$ که در مفروضات مساله آمده، f نمی‌تواند بر ∂D صفر شود. پس $\lim_{n\to\infty}a_n=a\in D$ و لذا صفرهای تابع هولومورف $f:D\to D$، در a نقطه‌ی انباشتگی دارند. از آن‌جا که a_nها ریشه‌های دو به دو متمایزی از f بودند، هر همسایگی محذوف به دلخواه کوچک حول a ریشه‌ای از f را دربردارد. پس بنابر اصل یگانگی $f:D\to D$ متحد با صفر می‌شود، ولی در این صورت گسترش یافته‌ی پیوسته‌ی $f:\bar D\to\bar D$ از آن هم باید متحد با صفر باشد که دوباره با $f(\partial D)\subset\partial D$ در تناقض است. بنابراین $f:D\to D$ حداکثر متناهی‌تا ریشه دارد که آن‌ها را $\alpha_1,\dots,\alpha_k$ می‌نامیم. تکرر هر α_i به عنوان ریشه‌ای از f متناهی و عددی همچون $m_i\ge 0$ است، چرا که دوباره اگر تمامی مشتقات f در ریشه‌ی α_i از آن صفر شوند، با در نظر گرفتن سری تیلور حول α_i، به $f\equiv 0$ می‌رسیم که دیدیم امکان‌پذیر نیست. از طرف دیگر می‌دانیم که برای هر $\alpha\in D$،

$$\begin{cases}D\to D\\ z\mapsto\frac{z-\alpha}{1-\bar\alpha z}\end{cases}$$

تابع موبیوس و نگاشت هولومورفی است که به صورت نگاشت پیوسته‌ی $\bar D\to\bar D$ای که ∂D را به درون ∂D تصویر می‌کند، گسترش می‌یابد. به علاوه تنها ریشه‌ی آن $\alpha\in D$ است. پس

$$g(z):=\frac{f(z)}{\prod_{i=1}^k(\frac{z-\alpha_i}{1-\bar\alpha_i z})^{m_i}}$$

یک نگاشت هولومورف $g : D \to D - \{0\}$ ارائه می‌دهد (چرا که تنها ریشه‌های f، $\alpha_1, \dots, \alpha_k \in D$ بودند و آن هم با تکرر $m_1, \dots, m_k \geq 0$.) که توسیع پیوسته‌ی $g : \bar{D} \to \mathbb{C}$ از آن با $g(\partial D) \subset \partial D$ موجود است. پس اگر نشان دهیم که چنین gای باید تابع ثابت با مقدار $e^{i\theta}$ $(\theta \in \mathbb{R})$ باشد، نتیجه می‌شود که:

$$\forall z \in D : f(z) = e^{i\theta} \prod_{i=1}^{k} (\frac{z - \alpha_i}{1 - \bar{\alpha}_i z})^{m_i}$$

و لذا f همان‌گونه که می‌خواستیم، ضرب توابع موبیوس می‌شود. از آن‌جا که به دلیل $g(\partial D) \subset \partial D$، g حداکثر یک مقدار ω با $|\omega| = 1$ را می‌پذیرد. تنها کافی است ثابت بودن g را نشان داد و بنابراین مساله به حکم زیر تقلیل می‌یابد:

(*) $g : D \to D - \{0\}$ را تابع هولومورفی بگیرید که می‌توان آن را به طور پیوسته بر نقاط ∂D هم تعریف کرد به قسمی که $g(\partial D) \subset \partial D$. چنین تابعی باید ثابت باشد.

می‌توان حداقل سه اثبات برای (*) ارائه کرد:

اثبات اول) از ایده‌ی استاندارد "اصل انعکاس شوارتز[1]" استفاده می‌کنیم. چون برای هر $z \in \partial D$ داریم $|g(z)| = 1$، اگر $|z| = 1$ آن‌گاه $g(z) = 1/\overline{g(\frac{1}{\bar{z}})}$. پس چون $g : D \to D - \{0\}$ تابعی هولومورف بود،

$$\begin{cases} h : \mathbb{C} \to \mathbb{C} - \{0\} \\ h(z) = \begin{cases} g(z) & |z| \leq 1 \\ 1/\overline{g(\frac{1}{\bar{z}})} & |z| \geq 1 \end{cases} \end{cases}$$

هم این‌گونه است. ولی توجه کنید که:

$$\lim_{|z| \to \infty} h(z) = \lim_{|z| \to \infty} 1/\overline{g(\frac{1}{\bar{z}})} = 1/\overline{g(0)} \in \mathbb{C}$$

پس تابع هولومورف $h : \mathbb{C} \to \mathbb{C} - \{0\}$ کراندار است و بنابراین، بنابر قضیه‌ی لیوویل باید ثابت باشد. از آن‌جا که $h|_D = g$، این ثابت بودن g را هم نتیجه می‌دهد.

اثبات دوم) فرض کنید تابع هولومورف $g : D \to D - \{0\}$ ثابت نباشد. پس بنابر قضیه‌ای یک نگاشت باز خواهد بود: $g(D)$ بازی از $D - \{0\}$ است. ولی توجه کنید که بستار $g(D)$ در $\mathbb{C}$، یعنی $\overline{g(D)}$، به جز $g(D)$ تنها نقاط

$$\partial D = \{z \in \mathbb{C} : |z| = 1\}$$

را می‌تواند دربر داشته باشد. چرا که اگر $\{g(b_n)\}_{n=1}^{\infty}$ دنباله‌ای از اعضای $g(D)$ باشد که در آن $\{b_n\}_{n=1}^{\infty}$ دنباله‌ای از اعضای D است و $\lim_{n\to\infty} g(b_n) = c$ آنگاه $c \in g(D) \cup \partial D$. چرا که به دلیل فشردگی $\bar{D} = \{z \in \mathbb{C} \mid |z| \leq 1\}$، دنباله‌ی مذکور از نقاط D، زیردنباله‌ای به شکل $\{b'_n\}_{n=1}^{\infty}$ دارد که به عضوی از $\bar{D}$ همچون b' همگراست: $\lim_{n\to\infty} b'_n = b' \in \bar{D}$. پس چون g به طور پیوسته به کل $\bar{D}$ گسترش می‌یابد $c = g(b')$ و حال اگر $b' \in D$ آن‌گاه $c \in D$ (چرا که $g : D \to D - \{0\}$ بود) و اگر $b' \in \partial D$، از فرض (*)، یعنی $g(\partial D) \subset \partial D$ نتیجه می‌شود $c \in \partial D$. لذا $g(D)$ بازی از $D - \{0\}$ است که بستار آن $\overline{g(D)}$، به جز $g(D)$ حداکثر می‌تواند اعضای ∂D را دربر داشته باشد. باید وجود چنین بازی را به تناقض کشاند: از آن‌جا که $\overline{g(D)}$ فشرده است، نقطه‌ای از آن مانند $x \in \overline{g(D)}$ موجود است که فاصله‌اش از $0 \in \mathbb{C}$ حداقل ممکن است. همان‌گونه که گفتیم $\overline{g(D)} \subset g(D) \cup \partial D$، $g(D)$ بازی از $D - \{0\}$ و لذا فاصله‌ی اعضایش از مبدا کمتر از یک است در حالی که $\partial D = \{z \in \mathbb{C} \mid |z| =\}$. پس $x \in g(D)$. با استفاده از باز بودن $g(D)$، اگر $\epsilon > 0$ به اندازه‌ی کافی کوچک باشد $(1 - \epsilon)x \in g(D)$. این در حالی است که

$$|(1 - \epsilon)x| = (1 - \epsilon).|x| < |x|$$

که با روش انتخاب x تناقض دارد.

اثبات سوم) (این اثبات ممکن است اندکی فراتر از سطح استاندارد دروس دوره‌ی کارشناسی باشد.) در نمودار زیر

---

[1] Schwarz reflection principal

$$\begin{tikzcd} & \mathbb{C} \arrow[d, "z \mapsto e^{۲\pi i z}"] \\ \bar{D} \arrow[r, "g"] \arrow[ur, dotted, "\tilde{g}"] & \mathbb{C} - \{۰\} \end{tikzcd}$$

نگاشت عمودی

$$\begin{cases} \mathbb{C} \to \mathbb{C} - \{۰\} \\ z \mapsto e^{۲\pi i z} \end{cases}$$

یک نگاشت پوششی است و $g : \bar{D} \to \mathbb{C} - \{۰\}$ همان نگاشت پیوسته‌ی حاصل از توسیع $g : D \to D - \{۰\}$ در (*) است. لذا چون $\bar{D}$ همبند ساده (و در واقع انقباض‌پذیر) است، یک ترفیع پیوسته‌ی $\tilde{g} : \bar{D} \to \mathbb{C}$ که در نمودار با خط‌چین نمایش داده شده، موجود است: نگاشت پیوسته‌ی $\tilde{g} : \bar{D} \to \mathbb{C}$ که نمودار را جابه‌جایی می‌کند. تحدید $\tilde{g}$ به درون $\bar{D}$ یعنی دیسک واحد $D = \{z \in \mathbb{C} \mid |z| < ۱\}$ هولومورف است، چرا که

$$\begin{tikzcd} & \mathbb{C} \arrow[d, "z \mapsto e^{۲\pi i z}"] \\ \bar{D} \arrow[r, "g|_D"] \arrow[ur, "\tilde{g}|_D"] & \mathbb{C} - \{۰\} \end{tikzcd}$$

جابه‌جایی، $g|_D$ هولومورف و نگاشت عمودی ظاهر شده در نمودار، موضعا همیومورفیسم است. تجزیه‌ی $\tilde{g}$ به جمع جزء حقیقی و موهومی‌اش را به صورت $\tilde{g} = u + iv$ بگیرید. با توجه به نمودار جابه‌جایی فوق، برای $z \in \partial D$:

$$|g(z)| = |e^{۲\pi i \tilde{g}(z)}| = |e^{۲\pi i(u(z)+iv(z))}| = |e^{-v(z)}| = ۱ \Rightarrow v(z) = ۰$$

حال $v : \bar{D} \to \mathbb{R}$ تابعی پیوسته است که $v|_D$ هارمونیک است یعنی لاپلاسین آن صفر است (چرا که جزء موهومی تابع هولومورف $\tilde{g} : D \to \mathbb{C}$ است) و بر ∂D؛ $v = ۰$. در این صورت باید $v \equiv ۰$ چرا که توابع هارمونیک در اصل ماکسیمم صدق می‌کنند. یک روش دیگر بیان آن این است که v جواب معادله‌ی لاپلاس بر D است که بر ∂D صفر است و در نتیجه $v \equiv ۰$. پس جزء موهومی تابع هولومورف $\tilde{g} : D \to \mathbb{C}$ صفر است و بنابراین $\tilde{g}$ و لذا $g = e^{۲\pi i \tilde{g}}$ ثابت هستند.

روز دوم

سوال ۱. اگر $f:[\circ,\text{۱}]\to\mathbb{R}$ تابعی پیوسته باشد که برای هر $\circ\le x,y\le \text{۱}$،
$$xf(y)+yf(x)\le \text{۱}$$
ثابت کنید $\int_\circ^\text{۱} f(x)\mathrm{d}x\le\frac{\pi}{\text{۴}}$ و با ذکر مثال نشان دهید $\frac{\pi}{\text{۴}}$ کرانی دقیق است. (طراح: سوال مسابقه‌ی *IMC* در ۱۹۹۸)

پاسخ سوال ۱. انتگرال $\int_\circ^\text{۱} f(x)\mathrm{d}x$ را با تغییر متغیرهای $x=\cos\theta$ و $x=\sin\theta$ بازنویسی می‌کنیم و معادلات زیر بدست می‌آید:
$$\int_\circ^\text{۱} f(x)\mathrm{d}x=\int_\circ^{\frac{\pi}{\text{۲}}} f(\sin\theta)\cos\theta\mathrm{d}\theta$$
$$\int_\circ^\text{۱} f(x)\mathrm{d}x=\int_{\frac{\pi}{\text{۲}}}^\circ f(\cos\theta)(-\sin\theta)\mathrm{d}\theta=\int_\circ^{\frac{\pi}{\text{۲}}} f(\cos\theta)\sin\theta\mathrm{d}\theta$$
از جمع دو تساوی فوق داریم:
$$\text{۲}\int_\circ^\text{۱} f(x)\mathrm{d}x=\int_\circ^{\frac{\pi}{\text{۲}}}[f(\sin\theta)\cos\theta+f(\cos\theta)\sin\theta]\mathrm{d}\theta\le\frac{\pi}{\text{۲}}\Rightarrow\int_\circ^\text{۱} f(x)\mathrm{d}x\le\frac{\pi}{\text{۴}}$$
زیرا که با استفاده از نامساوی صورت مسئله داریم:
$$f(\sin\theta)\cos\theta+f(\cos\theta)\sin\theta\le\text{۱}$$
برای برقراری تساوی توجه کنید که با توجه به بالا کافی است
$$\forall\theta\in[\circ,\frac{\pi}{\text{۲}}]:f(\sin\theta)\cos\theta+f(\cos\theta)\sin\theta=\text{۱}$$
لذا با توجه به اتحاد $\cos^\text{۲}\theta+\sin^\text{۲}\theta=\text{۱}$، یک ایده تعریف $f:[\circ,\text{۱}]\to\mathbb{R}$ به قسمی که $f(\sin\theta)=\cos\theta$ و $f(\cos\theta)=\sin\theta$ برای هر $\theta\in[\circ,\frac{\pi}{\text{۲}}]$. پس $f(x)=\sqrt{\text{۱}-x^\text{۲}}$ باید تساوی را برقرار کند. این را در ادامه تحقیق خواهیم کرد:
$$\forall\circ\le x,y\le\text{۱}:xf(y)+yf(x)=x\sqrt{\text{۱}-y^\text{۲}}+y\sqrt{\text{۱}-x^\text{۲}}$$
$$=\sin(\arcsin(x))\cos(\arcsin(y))+\sin(\arcsin(y))\cos(\arcsin(x))$$
$$=\sin(\arcsin(x)+\arcsin(y))\le\text{۱}$$
$$\int_\circ^\text{۱} f(x)\mathrm{d}x=\int_\circ^\text{۱}\sqrt{\text{۱}-x^\text{۲}}\mathrm{d}x=\text{مساحت ربع دایره به شعاع ۱}=\frac{\pi}{\text{۴}}$$

سوال ۲. برای $n=\text{۱},\text{۲},\ldots$ فرض کنید $C_n\subset\mathbb{R}^n$ یک زیرمجموعه‌ی فشرده و ناتهی باشد به طوری که $C_{n+\text{۱}}\subset C_n\times\mathbb{R}$. ثابت کنید دنباله‌ی حقیقی $x_\text{۱},x_\text{۲},x_\text{۳},\ldots$ وجود دارد به طوری که برای هر n، $(x_\text{۱},x_\text{۲},\ldots,x_n)\in C_n$. (طراح: علی خزلی)

پاسخ سوال ۲. برای هر $i\le k$، $\pi_i:\mathbb{R}^k\to\mathbb{R}^i$ را نگاشت تصویر بر i مولفه‌ی اول می‌گیریم:
$$\pi_i(y,\ldots,y_k)=(y_\text{۱},\ldots,y_i)$$
دنباله‌ی مطلوب در صورت مساله را به طور استقرایی می‌سازیم. توجه کنید که برای هر $k\ge i$، $\pi_i(C_k)$ زیرمجموعه‌ای فشرده از $\mathbb{R}^i$ است. برای هر $n\ge\text{۱}$، $C_{n+\text{۱}}\subset C_n\times\mathbb{R}$ و در نتیجه با اعمال نگاشت پیوسته‌ی $\pi_\text{۱}$؛ $\pi_\text{۱}(C_{n+\text{۱}})\subset\pi_\text{۱}(C_n)$. پس دنباله‌ی تودرتو از زیرمجموعه‌های فشرده‌ی ناتهی $\mathbb{R}$ داریم:
$$\cdots\subset\pi_\text{۱}(C_\text{۳})\subset\pi_\text{۱}(C_\text{۲})\subset\pi_\text{۱}(C_\text{۱})$$

و لذا $\cap_{j=1}^{\infty}\pi_1(C_j)$ ناتهی است؛ x_1 را عضوی از آن بگیرید. حال x_2 را چنان می‌گیریم که $(x_1,x_2)\in\cap_{j=2}^{\infty}\pi_2(C_j)$. برای هر $n\geq 2$، $C_{n+1}\subset C_n\times\mathbb{R}$ و در نتیجه با اعمال نگاشت پیوسته‌ی π_2؛ $\pi_2(C_{n+1})\subset\pi_2(C_n)$ و بنابراین به دنباله‌ای تودرتو از زیرمجموعه‌های فشرده‌ی ناتهی $\mathbb{R}^2$ داریم:

$$\cdots\subset\pi_2(C_4)\subset\pi_2(C_3)\subset\pi_2(C_2)$$

اشتراک هر یک از این‌ها با زیرمجموعه‌ی بسته‌ی $\{x_1\}\times\mathbb{R}$ از $\mathbb{R}^2$ ناتهی است، چرا که از روش انتخاب x_1، برای هر $n\geq 1$، C_n عضوی با مولفه اول x_1 دارد. پس دنباله‌ی تودرتوی دیگری از زیرمجموعه‌های فشرده‌ی ناتهی $\mathbb{R}^2$ داریم:

$$\cdots\subset\pi_2(C_4)\cap\{x_1\}\times\mathbb{R}\subset\pi_2(C_3)\cap\{x_1\}\times\mathbb{R}\subset\pi_2(C_2)\cap\{x_1\}\times\mathbb{R}$$

و لذا دوباره این اشتراک ناتهی است یا معادلا به ازای x_2ای؛ $(x_1,x_2)\in\cap_{j=2}^{\infty}\pi_2(C_j)$. ادامه‌ی فرآیند ساختن x_iها با همین روند استقرایی پیش می‌رود؛ فرض کنید $x_1,\ldots,x_i$ چنان ساخته شده باشند که:

$$\forall 1\leq k\leq i:(x_1,\ldots,x_k)\in\cap_{j=k}^{\infty}\pi_k(C_j)$$

x_{i+1} را چنان می‌یابیم که این برای $k=i+1$ هم برقرار شود:

$$(x_1,\ldots,x_{i+1})\in\cap_{j=i+1}^{\infty}\pi_{i+1}(C_j)$$

از همان ایده‌ی بالا استفاده می‌کنیم: دنباله‌ی زیر از زیرمجموعه‌های فشرده و تودرتو $\mathbb{R}^{i+1}$ را داریم(تودرتو بودن به دلیل $C_{n+1}\subset C_n\times\mathbb{R}$):

$$\cdots\subset\pi_{i+1}(C_{i+3})\cap\{(x_1,\ldots,x_i)\}\times\mathbb{R}\subset\pi_{i+1}(C_{i+2})\cap\{(x_1,\ldots,x_i)\}\times\mathbb{R}\subset\pi_{i+1}(C_{i+1})\cap\{(x_1\ldots,x_i)\}\times\mathbb{R}$$

که تمامی آن‌ها به دلیل آن‌که $(x_1,\ldots,x_i)\in\cap_{j=i}^{\infty}\pi_i(C_j)$ یا معادلا اینکه هر یک از C_nها که $n\geq i$، عضوی دارند که i مولفه‌ی اولش همان $(x_1,\ldots,x_i)$ است ناتهی هستند. پس اشتراک زیرمجموعه‌های فشرده‌ی فوق، ناتهی است و لذا به ازای x_{i+1} مناسبی:

$$(x_1,\ldots,x_i,x_{i+1})\in\cap_{j=i+1}^{\infty}\pi_{i+1}(C_j)$$

پس دنباله‌ی $x_1,x_2,\ldots$ را ساختیم به قسمی که برای هر $i\geq 1$، $(x_1,\ldots,x_i)\in\cap_{j=i}^{\infty}\pi_i(C_j)$. علی‌الخصوص $(x_1,\ldots,x_i)\in\pi_i(C_i)=C_i$ (توجه کنید که $C_i\subset\mathbb{R}^i$ بود) برای هر $i\geq 1$ و بنابراین این همان دنباله‌ی مطلوب است که حل را تکمیل می‌کند.

تذکر ۱. ایده‌ی این سوال از "قضیه‌ی توسیع کولموگروف[2]" در نظریه‌ی احتمال گرفته شده است.

تذکر ۲. اگر به جای فضای اقلیدسی $\mathbb{R}^n$، مکعب فشرده‌ی I^n در صورت مساله قرار گیرد، می‌توان حکم را به سادگی از قضیه‌ی تیخونوف[3] نتیجه گرفت: فرض کنید برای هر عدد طبیعی n، $C_n\subset I^n$ فشرده باشد ($I=[0,1]$ بازه‌ی واحد) و $C_{n+1}\subset C_n\times I$. هدف اثبات وجود دنباله‌ی $x_1,x_2,\ldots$ از عناصر I است، با این ویژگی که برای هر $n\in\mathbb{N}$؛ $(x_1,\ldots,x_n)\in C_n$. بنابر قضیه‌ی تیخونوف در توپولوژی عمومی، فضای

$$I^{\infty}=\{(y_j)_{j=1}^{\infty}\in I^{\infty}\mid\forall j\in\mathbb{N}:y_j\in I\}$$

در توپولوژی حاصلضربی فشرده است. حال کافی است زیر مجموعه‌ی بسته‌ی زیر از آن را در نظر گرفت:

$$\tilde{C}_n=\{(y_j)_{j=1}^{\infty}\in I^{\infty}\mid(y_1,\ldots,y_n)\in C_n\}$$

(مکمل $\tilde{C}_n$، $(I^n-C_n)\times I\times I\cdots$ و لذا در توپولوژی حاصلضربی بر I^{∞} باز است). این‌ها زیرمجموعه‌های بسته‌ی فضای توپولوژیک فشرده و هاسدورف I^{∞} هستند و لذا فشرده‌اند و به علاوه به دلیل شرط $C_{n+1}\subset C_n\times I$، تودرتو و به دلیل ناتهی بودن C_nها، ناتهی هم هستند. بنابراین

$$\cdots\subset\tilde{C}_3\subset\tilde{C}_2\subset\tilde{C}_1$$

دنباله‌ای تودرتو از زیرمجموعه‌های فشرده‌ی ناتهی فضای فشرده‌ی I^{∞} می‌شود و بنابراین یک عنصر $(x_j)_{j=1}^{\infty}$ از I^{∞} در اشتراک $\cap_{n=1}^{\infty}\tilde{C}_n$ واقع است. این همان دنباله‌ی مطلوب است، چرا که از تعریف $\tilde{C}_n$ داریم:

$$(x_j)_{j=1}^{\infty}\in\tilde{C}_n\iff(x_1,\ldots,x_n)\in C_n$$

---
[2] Kolmogorov extension theorem
[3] Tychonoff's theorem

تذکر ۳. با اندکی ویرایش راه‌حلی که در بالا برای حالت خاصی که در آن C_nها زیرمجموعه‌های فشرده‌ی I^n اند بیان شد، می‌توان برای مساله در همان صورت اولیه‌اش، حلی جدید مبتنی بر قضیه‌ی تیخونوف ارائه کرد: هر $C_n \subset \mathbb{R}^n$ فشرده است. پس می‌توان بازه‌ی بسته‌ی $[a_n, b_n]$ را یافت به قسمی که مولفه‌ی nام تمامی عناصر C_n در $[a_n, b_n]$ واقع باشد. $C_{n+1} \subset C_n \times \mathbb{R}$، $C_{n+2} \subset C_{n+1} \times \mathbb{R}$ و ... نشان می‌دهند که حکم مشابهی برای مولفه‌ی nام عناصر هر C_k با $k \geq n$ برقرار است. پس بازه‌های بسته‌ی $[a_1, b_1], [a_2, b_2], \ldots$ را خواهیم داشت به قسمی که:

$$\forall n \in \mathbb{N} : C_n \subset [a_1, b_1] \times \cdots \times [a_n, b_n]$$

حال کافی است همان استدلال بیان شده در تذکر ۲ را، به فضای توپولوژیک $\prod_{n=1}^{\infty}[a_n, b_n]$ در توپولوژی حاصلضربی (که بنابر قضیه‌ی تیخونوف، فشرده است) اعمال کرد.

سوال ۳. فرض کنید برای گروه G نگاشت $x \to x^n$ یک ایزومورفیسم باشد. ثابت کنید برای هر $x, y \in G$ داریم

$$x^{n-1}y = yx^{n-1}$$

(n یک عدد طبیعی داده شده است.) (*طراح: سوال معروفی است!*)

پاسخ سوال ۳. به دلیل همریختی بودن

$$\begin{cases} G \to G \\ x \mapsto x^n \end{cases}$$

برای هر $b, c \in G$ داریم: $(bc)^n = b^n c^n$. با تثبیت یک عنصر دلخواه $x \in G$، این نتیجه می‌دهد که:

$$\forall a \in G : (xax^{-1})^n = x^n a^n (x^{-1})^n \Rightarrow xa^n x^{-1} = x^n a^n x^{-n} \Rightarrow a^n x^{n-1} = x^{n-1} a^n$$

پس x^{n-1} با هر عنصر G که به شکل a^n باشد، جابه‌جایی می‌شود. ولی به دلیل پوشایی همریختی مذکور، اگر $y \in G$ دلخواه باشد، به ازای $a \in G$ای $y = a^n$ و حال با قرار دادن در تساوی $a^n x^{n-1} = x^{n-1} a^n$ داریم:

$$x^{n-1}y = yx^{n-1}$$

سوال ۴. اعداد صحیح a, b, c به‌طوری‌که c فرد و خالی از مربع است و $a^2 + bc = -1$ داده شده است. نشان دهید اعداد صحیح A, B, C, D وجود دارد به طوری که $AD - BC = 1$ و $AC + BD = a$ و $C^2 + D^2 = c$ به طور همزمان برقرار شوند.
(*طراح: به توضیحات پس از راه‌حل مراجعه کنید!*)

پاسخ سوال ۴. ایده‌ی حل استفاده از حلقه‌ی اعداد صحیح گاوسی یا $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ است. خواص مقدماتی این حلقه را یادآوری می‌کنیم:

$\mathbb{Z}[i]$ یک .P.I.D است و برای هر $a + bi$ متعلق به آن می‌توان نرم را به صورت $N(a + bi) = a^2 + b^2$ تعریف کرد و اگر عددی اول باشد، $a + bi$ در $\mathbb{Z}[i]$ عنصری تحویل‌ناپذیر یا معادلا اول است. به علاوه اگر p یک عدد اول به فرم $p \overset{4}{\equiv} 1$ باشد، قضیه‌ای استاندارد حکم می‌کند که $x, y \in \mathbb{Z}$ موجودند به قسمی که $x^2 + y^2 = p$. پس در $\mathbb{Z}[i]$، $(x + iy)(x - iy) = p$. لذا $N(x + iy) = N(x - iy) = \sqrt{N(p)} = p$ و بنابراین $x \pm iy$ هر دو عناصری اول از $\mathbb{Z}[i]$اند. پس تجزیه‌ی عدد اول p با $p \overset{4}{\equiv} 1$ در $\mathbb{Z}[i]$ به صورت $p = \alpha\bar{\alpha}$ خواهد بود که α عنصری اول از $\mathbb{Z}[i]$ است.

حال مساله را حل می‌کنیم: $a^2 + bc = -1$ و لذا $b, c \mid a^2 + 1$. پس هیچ‌یک از b و c عامل اولی مانند q با $q \overset{4}{\equiv} 3$ ندارد. چرا که آنگاه $q \mid a^2 + 1$ و بنابراین $q \mid 1$ که تناقض است. پس تمامی عوامل فرد b و c به فرم $4k + 1$اند. اگر هر دوی b و c فرد باشند $b, c \overset{4}{\equiv} 1$ و لذا $a^2 \overset{4}{\equiv} -1 - bc \overset{4}{\equiv} 2$ که امکان‌پذیر نیست. پس چون c بنابر فرض مساله فرد است باید b زوج باشد. اگر $4 \mid b$ آنگاه $-1 \overset{4}{\equiv} a^2 + bc \overset{4}{\equiv} a^2$ که امکان‌پذیر نیست. پس b به شکل $4k + 2$ است. در جمع‌بندی این موارد، اعداد اول $p_1, \ldots, p_r$ و $q_1, \ldots, q_s$ با $p_1, \ldots, p_r, q_1, \ldots, q_s \overset{4}{\equiv} 1$ موجودند که $b = \pm 2q_1 \ldots q_s$ و $c = \pm p_1 \ldots p_r$. از آن‌چه که درباره‌ی تجزیه‌ی اعداد اول به فرم $4k + 1$ در $\mathbb{Z}[i]$ بیان گردید، اعداد $\alpha_1, \ldots, \alpha_r \in \mathbb{Z}[i]$ و $\beta_1, \ldots, \beta_s \in \mathbb{Z}[i]$ موجودند که عناصری اول از $\mathbb{Z}[i]$اند و:

$$\forall 1 \leq t \leq r : \alpha_t\bar{\alpha}_t = p_t, \forall 1 \leq j \leq s : \beta_j\bar{\beta}_j = q_j \Rightarrow N(\alpha_t) = p_t, N(\beta_j) = q_j$$

حال در $\mathbb{Z}[i]$ می‌توان نوشت:

$$a^۲+۱=-bc \Rightarrow (a+i)(a-i)=-bc=\pm ۲(\alpha_۱\bar{\alpha}_۱)\cdots(\alpha_r\bar{\alpha}_r)(\beta_۱\bar{\beta}_۱)\cdots(\beta_s\bar{\beta}_s)$$
$$=\pm((۱+i)\alpha_۱\cdots\alpha_r\beta_۱\cdots\beta_s)(\overline{(۱+i)\alpha_۱\cdots\alpha_r\beta_۱\cdots\beta_s})$$

چون برای هر $۱\le t\le r$ و $۱\le j\le s$، α_t و β_j عناصر اولی از $\mathbb{Z}[i]$ هستند، $\alpha_t|(a+i)(a-i)$ و $\beta_j|(a+i)(a-i)$ که از تساوی فوق حاصل می‌شوند نشان می‌دهند که $\alpha_t|a+i$ یا $\alpha_t|a-i$ یا معادلا با توجه به $\overline{a+i}=a-i$: $\alpha_t|a+i$ یا $\bar{\alpha}_t|a+i$ و به طور مشابه $\beta_j|a+i$ یا $\bar{\beta}_j|a+i$.

پس با جابه‌جا کردن α_t و $\bar{\alpha}_t$ یا β_j و $\bar{\beta}_j$ در صورت لزوم، فرض می‌کنیم که برای هر $۱\le t\le r$ و $۱\le j\le s$؛ $\alpha_t|a+i$ و $\beta_j|a+i$. به علاوه $۱\pm i$ هم در $\mathbb{Z}[i]$ به دلیل $N(۱\pm i)=۲$ اول‌اند. پس $۱+i|a+i$ یا $۱-i|a+i$ که دوباره بنابر تقارن و عوض کردن جای a و $-a$ در صورت لزوم، فرض می‌کنیم که $۱+i|a+i$. پس $۱+i,\alpha_۱,\ldots,\alpha_r$ و همچنین $\beta_۱,\ldots,\beta_s$ عوامل اولی از $a+i$ در $\mathbb{Z}[i]$ هستند.

حال اگر تجزیه‌ی $a+i$ در $\mathbb{Z}[i]$ را به صورت $a+i=\gamma_۱\cdots\gamma_u$ بگیریم، از بالا:

$$(\gamma_۱\cdots\gamma_u)(\overline{\gamma_۱\cdots\gamma_u})$$
$$=\pm((۱+i)\alpha_۱\cdots\alpha_r\beta_۱\cdots\beta_s)(\overline{(۱+i)\alpha_۱\cdots\alpha_r\beta_۱\cdots\beta_s})$$

حال از یکتایی تجزیه به سادگی نتیجه می‌گردد که

$$\gamma_۱\cdots\gamma_u=\pm(۱+i)\alpha_۱\cdots\alpha_r\beta_۱\cdots\beta_s$$

چرا که هر γ_i باید در سمت راست هم ظاهر شود و اگر یکی از $\bar{\alpha}_t$ یا $\bar{\beta}_j$ باشد، چون α_t یا β_j هم عوامل اول $a+i$ هم بودند، باید α_t یا β_j، هردوی $a\pm i$ و لذا a را بشمارند. در هر حال چون α_t عامل c در $\mathbb{Z}[i]$ و β_j عامل b در $\mathbb{Z}[i]$ بودند، a و c یا a و b در $\mathbb{Z}[i]$ نسبت به هم اول نیستند. ولی این تناقض است چرا که $a^۲+bc=-۱$ نشان می‌دهد که a و b و همچنین a و c در $\mathbb{Z}$ نسبت به هم متباین‌اند. پس

$$a+i=\gamma_۱\cdots\gamma_u=\pm(۱+i)\alpha_۱\cdots\alpha_r\beta_۱\cdots\beta_s$$

حال قرار می‌دهیم

$$\alpha_۱\cdots\alpha_r=C+Di$$

$$\pm(۱+i)\beta_۱\cdots\beta_s=A-Bi$$

که در آن A، B، C و D صحیح‌اند. پس $a+i=(A-Bi)(C+Di)$. لذا با در نظر گرفتن اجزا حقیقی و موهومی $AC+BD=a$ و $AD-BC=۱$. به علاوه

$$C^۲+D^۲=N(Ci+D)=N(\alpha_۱\cdots\alpha_r)=p_۱\cdots p_r=c$$

پس $A,B,C,D\in\mathbb{Z}$ خواص مطلوب را برآورده می‌کنند.

تذکر. ایده‌ی این سوال در ابتدا از عمل گروه $SL(۲,\mathbb{Z})$ بر نیم‌صفحه‌ی بالا یعنی $\mathcal{H}=\{z\in\mathbb{C}\mid Imz>۰\}$ گرفته شد. عضو

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in SL(۲,\mathbb{Z})$$

بر $\mathcal{H}$ با تبدیلات خطی-کسری به صورت $z\mapsto\frac{az+b}{cz+d}$ عمل می‌کند. در این عمل اعضایی از $SL(۲,\mathbb{Z})$ (به جز $\pm I$) بیضوی[۴] نامیده می‌شوند که نقطه‌ی ثابتی در عمل بر $\mathcal{H}$ داشته باشند و می‌توان نشان داد که شرط لازم و کافی برای برآورده شدن این شرط آن است که تریس این ماتریس به $\{۰,\pm۱\}$ تعلق داشته باشد. می‌توان نشان داد که نقاطی از $\mathcal{H}$ که بیضوی یعنی نقطه‌ی ثابت عنصری به جز $\pm I$ از $SL(۲,\mathbb{Z})$ باشند، یا در مدار عمل iاند یا در مدار عمل $\exp(\frac{۲\pi i}{۶})$.

ایده‌ی طرح سوال این بود که عنصری از $SL(۲,\mathbb{Z})$ با تریس صفر که لاجرم به شکل

$$\begin{pmatrix} a & b \\ c & -a \end{pmatrix}$$

[۴] elliptic

با $-1 = a^2 + bc$ خواهد بود، در نظر گرفته شود و نقطه‌ی ثابت تبدیل خطی-کسری $z \mapsto \frac{az+b}{cz+d}$ متناظر محاسبه گردد و اینکه این نقطه از $\mathcal{H}$ در مدار i باشد، معادل است با وجود $A, B, C, D \in \mathbb{Z}$ با خواص مذکور.

البته پس از امتحان متوجه شدیم که متاسفانه سوال تکراری است و یک بار در دوره‌های المپیاد ریاضی دبیرستانی مطرح شده است!

سوال ۵. فرض کنید G یک زیرگروه از $GL_n(\mathbb{Z})$ (ماتریس‌های $n \times n$ با درایه‌های صحیح و $\det = \pm 1$) است که برای هر $g \in G$ عدد $m \geq 1$ وجود دارد به طوری که $g^m = 1$. ثابت کنید:

الف) عدد طبیعی N وجود دارد به طوری که برای هر $g \in G$ داریم $g^N = 1$

ب) G یک گروه متناهی است و یک کران برای مرتبه‌ی آن برحسب تابعی از n بیابید.

(طراح: دکتر غلامزاده محمودی)

پاسخ سوال ۵. حل قسمت الف: هر $g \in G$ ماتریسی $n \times n$ با درایه‌های صحیح است که $g^m = I_n$ و لذا چندجمله‌ای مینیمال g چندجمله‌ای $x^m - 1$ را می‌شمارد. ولی این چندجمله‌ای و در نتیجه چندجمله‌ای مینیمال g ریشه‌ی تکراری ندارند و بنابراین g قطری‌پذیر است و درایه‌های روی قطر آن باید ریشه‌های واحد باشند، چرا که مقادیر ویژه‌ی g باید در $x^m - 1 = 0$ صدق کنند. پس هر $g \in GL(n, \mathbb{Z})$ را می‌توان بر $\mathbb{C}$ قطری کرد و درایه‌های روی قطر، ریشه‌های واحد خواهند بود. ولی این ریشه‌ها باید در چندجمله‌ای مشخصه‌ی g هم که چندجمله‌ای تکین از درجه‌ی n و با ضرایب صحیح است صدق کنند. لذا باید چندجمله‌ای مینیمال ریشه‌ی واحد مذکور بر $\mathbb{Q}$، چندجمله‌ای درجه‌ی nای را بشمارد. ولی می‌دانیم که اگر $\omega \in \mathbb{C}$ یک ریشه‌ی اولیه‌ی kام واحد باشد، یعنی k کوچکترین عددی باشد که $\omega^k = 1$، آن‌گاه چندجمله‌ای مینیمال ω از چندجمله‌ای‌های موسوم به دایره‌بُر[5] و از درجه‌ی $\phi(k)$ است. پس اگر یک ریشه‌ی اولیه‌ی kام واحد، مقدار ویژه‌ی یکی از عناصر G باشد، باید $\phi(k) \leq n$. ولی $\lim_{m\to\infty} \phi(m) = \infty$. پس تعداد kهایی از این دست متناهی است و لذا اگر N' را بزرگترین عدد طبیعی‌ای بگیریم که $\phi(N') \leq n$، هر مقدار ویژه‌ی یکی از عناصر $g \in G$ مانند ω، باید $\omega^{N'!} = 1$ را برآورده کند. چرا که اگر k کوچکترین عدد طبیعی‌ای باشد که برای این ω، $\omega^k = 1$ (یعنی ω ریشه‌ی اولیه‌ی kام واحد باشد) چندجمله‌ای مینیمال ω بر $\mathbb{Q}$ چندجمله‌ای از درجه‌ی $\phi(k) \leq n$ خواهد بود و لذا $k \leq N'$. پس چون $k \mid N'!$:

$$\omega^k = 1 \Rightarrow \omega^{N'!} = 1$$

حال قرار می‌دهیم $N := N'!$. آن‌چه بیان شد نشان می‌دهد که برای هر $g \in G$، مقادیر ویژه‌ی $g^N \in GL(n, \mathbb{Z})$ همگی ۱ اند. ولی این ماتریس قطری‌پذیر است چرا که g این‌گونه بود و ماتریس قطری‌پذیری که تمامی مقادیر ویژه‌اش ۱ باشند همانی است. پس این N خاصیت مطلوب را برآورده می‌کند: $g^N = I_n$ برای هر $g \in G$.

حل قسمت ب:

راه‌حل اول(دکتر غلامزاده) - $GL(n, \mathbb{Z})$ و به تبع آن G را می‌توان زیرمجموعه‌ای از فضای برداری متناهی‌البعد $M(n, \mathbb{Q})$ متشکل از ماتریس‌های $n \times n$ با درایه‌های گویا گرفت. پس زیرمجموعه‌ای متناهی از G مانند $\{A_1, \ldots, A_l\}$ موجود است به قسمی که هر عنصر G را می‌توان به صورت ترکیب خطی با ضرایب گویا از $A_1, \ldots, A_l$ نوشت(در واقع برای انتخاب A_iها کافی است زیرمجموعه‌ای از G با حداکثر تعداد عضو ممکن را در نظر گرفت که عناصرش بر $\mathbb{Q}$ مستقل باشند). با توجه به اینکه G زیرگروهی از $GL(n, \mathbb{Z})$ است، نگاشتی به صورت زیر داریم:

$$(*) \begin{cases} G \to \mathbb{Z}^l \\ A \mapsto (tr(AA_1), \ldots, tr(AA_l)) \end{cases}$$

(tr نماد تابعک تریس است). برد این نگاشت متناهی است زیرا از (الف) به ازای Nای، $g^N = I_n$ برای هر $g \in G$ و لذا مقادیر ویژه‌ی هر عنصر g به مجموعه‌ی متناهی $\{e^{\frac{2\pi i k}{N}} \mid 0 \leq k < N\}$ تعلق دارند و بنابراین $tr(g)$ که جمع n مقدار ویژه‌ی g است، حداکثر N^n حالت دارد. پس در نگاشت $G \to \mathbb{Z}^l$ که در (*) تعریف شد، هر مولفه حداکثر N^n حالت دارد و لذا تعداد اعضای برد این نگاشت از N^{nl} تجاوز نمی‌کند. پس اگر یک‌به‌یک بودن $G \to \mathbb{Z}^l$ ثابت شود، نتیجه می‌شود که G متناهی است و

[5] Cyclotomic

$|G| \leq N^{nl}$. برای اثبات یک‌به‌یک بودن فرض کنید $A, B \in G$ چنان باشند که برای هر $1 \leq i \leq l$: $tr(AA_i) = tr(BA_i)$. لذا چون روش انتخاب $\{A_1, \ldots, A_l\}$ هر عنصر G را می‌توان به صورت یک ترکیب خطی A_iها با ضرایب گویا توصیف کرد:

$$\forall g \in G : tr(Ag) = tr(Bg)$$

علی‌الخصوص برای $g = B^{-1} \in G$: $tr(AB^{-1}) = tr(I_n)$. پس جمع n مقدار ویژه (با حساب تکرر) از $AB^{-1} \in G$، n است. ولی دیدیم که تمامی این مقدار ویژه‌ها ریشه‌های Nام واحد هستند ولذا از $AB^{-1} = I_n$ نتیجه می‌شود $A = B$. پس نشان دادیم که $|G| \leq N^{nl}$.

چون زیرمجموعه‌ی $\{A_1, \ldots, A_l\}$ از $M(n, \mathbb{Q})$ مستقل خطی بود پس $l \leq n^2$. N هم باید تنها این ویژگی را داشته باشد که برای هر $g \in G$، $g^N = I_n$ و در حل (الف) دیدیم که بدین منظور کافی است قرار داد $N = \prod_{\{k \in \mathbb{N} | \phi(k) \leq n\}} k$. لذا کرانی برای $|G|$ بدین شرح است:

$$|G| \leq N^{nl} \leq N^{n^3} \Rightarrow |G| \leq \Big(\prod_{\{k \in \mathbb{N} | \phi(k) \leq n\}} k\Big)^{n^3}$$

راه‌حل دوم(دکتر جعفری) - دوباره N را مشابه قسمت (الف) عدد طبیعی‌ای بگیرید با این ویژگی که برای هر $g \in G$، g^N همانی باشد. p را عدد اولی بگیرید که نسبت به N اول است. با در نظر گرفتن درایه‌های عناصر $GL(n, \mathbb{Z})$ به پیمانه‌ی p، به یک همریختی گروهی $G \to GL(n, \mathbb{Z}_p)$ می‌رسیم که درایه‌های هر $A \in G$ را به پیمانه‌ی p در نظر می‌گیرد. ادعا می‌کنیم که این همریختی گروهی یک‌به‌یک است و این امر نتیجه خواهد داد که $|G| \leq |GL(n, \mathbb{Z}_p)|$.

فرض کنید $A \in G$ در هسته‌ی این همریختی باشد، یعنی با درایه‌های بر میدان $\mathbb{Z}_p$: $\bar{A} = I_n$. لذا ماتریس $n \times n$، B با درایه‌های صحیح موجود است که $A = I_n + pB$. با نوشتن آن به صورت $A = I_n + p^k B$ به ازای $k \geq 1$ مناسبی، می‌توان فرض کرد که حداقل یک درایه‌ی B بر p بخش‌پذیر نیست، چرا که اگر چنین kای موجود نباشد، $B = 0$ و لذا $A = I_n$ که همان چیزی است که در پی آنیم. پس A را به شکل $I_n + p^k B$ که $k \geq 1$ و B را با ویژگی مذکور بگیرید. چون در $GL(n, \mathbb{Z})$، $A^N = I_n$، داریم:

$$(I_n + p^k B)^N = I_n \Rightarrow \sum_{i=1}^{N} \binom{N}{i} p^{ki} B^i = 0 \Rightarrow NB = -\sum_{i=2}^{N} \binom{N}{i} p^{k(i-1)} B^i$$

با توجه به اینکه این تساوی‌ها میان ماتریس‌های با درایه‌های صحیح هستند، نتیجه می‌شود که p^k همه‌ی درایه‌های NB را می‌شمارد. ولی p نسبت به N اول بود و حداقل یکی از درایه‌های B را عاد نمی‌کرد. بنابراین به تناقض می‌رسیم و یک‌به‌یک بودن

$$G \to GL(n, \mathbb{Z}_p)$$

ثابت می‌شود. کران $|G|$ را هم می‌توان تعداد اعضای $GL(n, \mathbb{Z}_p)$ گرفت.