תרגול 23

מספר אלגברי $\alpha\in\mathbb{R}$, הוא שורש של פולינום $f\in\mathbb{Q}[x]$, f מתוקן.

לוקחים f ממעלה מינימלית. אז f אי פריק יחיד. $f=f_1\cdot f_2$

$\underset{\text{אי פריק}}{f=Irr(\alpha)}$. נגדיר **המעלה של α** היא $\deg Irr(\alpha)$.

דוגמאות: המעלה של $\frac{1}{2}$ היא 1. המעלה של $\sqrt{2}$ היא 2.

<u>משפט Liouville</u>: אם $\alpha\in\mathbb{R}$ אלגברי ממעלה $n>1$ אז קיים קבוע כלשהו $c=c(\alpha)>0$ כך ש- $\forall p,q\in\mathbb{Z}\ (q>0)\ |\alpha-\frac{p}{q}|>\frac{c}{q^n}$ (*) (c לא תלוי ב- p ו- q!)

<u>הוכחה</u>: נבנה $0<c<1$. אז (*) נכון טריוויאלית עבור $p,q\in\mathbb{Z}$ כך ש- $|\alpha-\frac{p}{q}|>1$.

לכן מספיק למצוא $0<c<1$ כך ש (*) מתקיים עבורם $|\alpha-\frac{p}{q}|\leq 1$ (p ו- q שמקיימים זאת).

במקרה זה $\frac{p}{q}$ חסום.

יהי $f(x)=a_nx^n+\ldots+a_0$ פולינום אי פריק (ב- $\mathbb{Q}[x]$) עבור α עם $a_i\in\mathbb{Z}$.

(כלומר $f(\alpha)=0$). נניח בה"כ: $\gcd(a_n,\ldots,a_0)=1$ (אחרת נחלק).

אז $\forall\frac{p}{q}\in\mathbb{Q}.\ f(\frac{p}{q})\neq 0$ (כי $\deg(\alpha)>1$). לכן:

$$|q^nf(\tfrac{p}{q})|=|a_np^n+a_{n-1}p^{n-1}q+\ldots+a_0q^n|\underset{\uparrow}{\geq}1$$

הבי"ת השמאלי שלם $\neq 0$.

מתקיים: $f(\frac{p}{q})=f(\frac{p}{q})-\overset{0}{\overline{f(\alpha)}}=(\frac{p}{q}-\alpha)\cdot f'(\xi)$ ממשפט לגרנז' (קבוע), $\xi\in\mathbb{R}$ בין α ל- $\frac{p}{q}$.

ξ חסום. $|\xi|\leq|\alpha|+1$ כי $|\frac{p}{q}-\alpha|\leq 1$. לכן $f'(\xi)$ חסום ($\neq 0$ כי אחרת $f(\frac{p}{q})=0$)

$|f'(\xi)|<c_1$ עבור $|\xi|\leq|\alpha|+1$, c_1 תלוי ב- α אבל לא ב- p,q.

וקיבלנו:
$$|\alpha-\frac{p}{q}|=\frac{|f(\frac{p}{q})|}{|f'(\xi)|}=\frac{|q^nf(\frac{p}{q})|}{q^n|f'(\xi)|}$$

$q^n|f(\frac{p}{q})|\geq 1$. $q^n\cdot f'(\xi)<c_1\cdot q^n$. $|\alpha-\frac{p}{q}|>\frac{1}{c_1q^n}$ עבור $|\frac{p}{q}-\alpha|\leq 1$

נבחר: $c=\min(\frac{1}{c_1},\frac{1}{2})$ אז $|\alpha-\frac{p}{q}|>\frac{c}{q^n}$ (אם $|\frac{p}{q}-\alpha|<1$ לפי החישוב,

אם $|\frac{p}{q}-\alpha|\geq 1$ ברור כי $c<1$). ■

<u>מסקנה</u>: יהי $(s_i)=s_1,s_2,s_3,\ldots$ סדרה אינסופית, $s_i=\pm 1$. אז המספר

$\xi=1+\frac{s_1}{2^{1!}}+\frac{s_2}{2^{2!}}+\frac{s_3}{2^{3!}}+\ldots$ הוא טרנסנדנטי! ($\xi:=\sum_{i=1}^{\infty}\frac{s_i}{2^{i!}}+1$)

<u>הוכחה</u>: ξ אי רציונלי, כי בפיתוח שלו (הבינארי או העשרוני) זהו שבר בלי מחזור.

נניח בשלילה שהוא כן אלגברי. נגדיר $q_n=2^{(n-1)!}$.

<u>המשך הוכחה:</u> נגדיר $p_n = q_n\left(1+\frac{s_1}{2^{1!}}+\dots+\frac{s_{n-1}}{2^{(n-1)!}}\right)$, $p_n \in \mathbb{Z}$.

אז $\left|\xi - \frac{p_n}{q_n}\right| \le \underbrace{\frac{1}{2^{n!}} + \frac{1}{2^{(n+1)!}} + \dots}_{(**)}$.

עבור $k \geq 1$ מתקיים $2^{(n+k)!} \geq 2^{n!\cdot(n+k)} \geq (2^{n!})^k$

לכן הסדרה שסמנו (**) קטנה מ- $\cancel{b_j = \frac{1}{(2^{n!})^j}}$ $\sum_{j=1}^{\infty}\frac{1}{(2^{n!})^j} + \frac{1}{2^{n!}}$.

זוהי סדרה הנדסית ולכן $\left|\xi - \frac{p_n}{q_n}\right| \le \frac{1}{2^{n!}} + \frac{\frac{1}{2^{n!}}}{1-\frac{1}{2^{n!}}} \le$

$$\le 2\cdot\frac{\frac{1}{2^{n!}}}{1-\frac{1}{2^{n!}}} \le \frac{4}{2^{n!}} = \frac{4}{(q_n)^n}$$

$\Leftarrow$ ξ טרנסצנדנטי! נניח בשלילה ש- ξ היה מס' אלגברי ממעלה m

אז לפי משפט ליוביל קיים $c>0$ כך ש- $\left|\xi - \frac{p}{q}\right| > \frac{c}{q^m}$ עבור כל p, q.

אבל עבור ξ שלנו מתקיים: $c < (q_n)^m\left|\xi - \frac{p_n}{q_n}\right| \le (q_n)^m\frac{4}{q_n^n} = \frac{4}{q_n^{n-m}} \xrightarrow{n\to\infty} 0$

לכן ξ טרנס.

(הוא לא אלגברי ושם מעלה $m>1$ שאינו רציונלי. לכן אינו אלגברי ממעלה $m=1$).

משוואות Pell[3]

$x^2 - 2y^2 = 1$ נרצה למצוא $x, y \in \mathbb{Z}$. פתרון טריוויאלי: $x=1, y=0$. $x^2 = 1+2y^2$

עבור $y=1$ יוצא 3, עבור $y=2$ יוצא $9 \Leftarrow$ $x=3, y=2$ זה פתרון.

לכן גם $x=\pm1, y=0$, $x=\pm3, y=\pm2$.

נרצה למצוא את כל הפתרונות.

$\alpha = x+\sqrt{2}y$. α פתרון אם x, y פתרון.

$\alpha' = x-y\sqrt{2}$. $N(\alpha) = \alpha\cdot\alpha' = x^2-2y^2$ אגב, לא הכרח חיובית!

$x, y \in \mathbb{Z} \Rightarrow N(\alpha) \in \mathbb{Z}$

נסמן $\beta = z+t\sqrt{2}$. אז:

$$(\alpha\beta)' = ((x+y\sqrt{2})(z+t\sqrt{2}))' = (xz+2ty-(yz+tx)\sqrt{2}) = \alpha'\beta'$$

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

הוכחנו $N(\alpha\beta) = N(\alpha)\cdot N(\beta)$. אם α פתרון אז $N(\alpha)=1$.

אם β גם פתרון אז $N(\beta)=1$, אז $N(\alpha\beta)=1 \Rightarrow \alpha\beta$ גם פתרון.

$\alpha = 3+2\sqrt{2}$, אין לנו עוד פתרון, אז $\beta=\alpha$

$\alpha^2 = 17+12\sqrt{2} \Rightarrow (17,12)$ פתרון. אכן $17^2 - 2\cdot12^2 = 1$ לכן $\forall k\ \alpha^k$ הוא פתרון!

$\boxed{\text{OMG אוזי לו חבורה?!}}$

המשך תמ"ס:

$\alpha^{-1}=?$, $N(\alpha)=1 \Leftarrow 1=\alpha'\alpha$

אז נגדיר $\alpha^{-1}=\underset{x-y\sqrt2}{\alpha'}$ (כאשר $x^2-2y^2=1$).

אז יש איבר הופכי.

קיבלנו שאם יש α,β פתרונות אז $\alpha\beta, \alpha^{-1}$ פתרונות.

וזו חבורה ← $\{\alpha^n \mid n\in\mathbb{Z}\}$ כולם פתרונות.

$\alpha=3+2\sqrt2$, נקבל $\alpha^n=++$, $\alpha^{-n}=+-$ ⇐ לא מקבלים $-3-2\sqrt2$

ולכן אנו נזהה הפתרונות.

אם α פתרון אז $\{\pm\alpha^n \mid n\in\mathbb{Z}\}$ פתרונות.

האם יש פתרון שניתן לקבל ממנו את כל הפתרונות? במקרה שלנו כן.

$\alpha_0=3+2\sqrt2$ הוא הפתרון היסודי. נוכיח בהמשך.

משוואות Pell:

$x^2-dy^2=1$, $1<d\in\mathbb{Z}$, d אינו ריבוע (אחרת $x^2-(\sqrt{d}y)^2=1$ ויש רק פתרונות טריוויאליים)

משוואות אלו נקראות משוואות Pell.

האם יש אינסוף פתרונות? פתרון שממנו ניתן לקבל את כולם? כן, יש!!

אנו מחפשים $x,y\in\mathbb{Z}$ או $x+\sqrt{d}y\in\mathbb{Z}[\sqrt{d}]$

לפעמים אפשר לחפש $dy^2+1=x^2$, נציב $y=1,2,\dots$, ונקבל את הפתרון היסודי די מהר (ברוב המקרים).

בנוגע שאלה השעור הקודם:

אפשר לשים לב שבמבחן Solovey-Strasse לבדיקת ראשוניות בודקים מבנה חבורה. אם $b^{\frac{n-1}{2}}\equiv\left(\frac{b}{n}\right)$ אז b אינו עד.

לכן $M=\{b \mid b^{\frac{n-1}{2}}\equiv\left(\frac{b}{n}\right)\}$ (עבור n שאינו ראשוני) היא תת חבורה כי
$(b_1b_2)^{\frac{n-1}{2}}\equiv\frac{b_1b_2}{n}$

$M\neq(\mathbb{Z}/n\mathbb{Z})^*$ תכונה של תת חבורה.

$\exists I\in\mathbb{Z}\ \ |M|\cdot I=|(\mathbb{Z}/n\mathbb{Z})^*|=\varphi(n)$ לכן [illegible]: $|\mathbb{Z}/n\mathbb{Z}|\cdot|M|\geq\frac{1}{2}\varphi(n)$

$|M|\leq\frac{1}{2}\varphi(n)$