בלה

12 באוגוסט 2025

הוכחה: יהי $0 < K < \infty, d \in (0,1]$ ונגדיר

$$f_n(x) = n + Kx^d$$

נראה שהפונקציה היא K לישפיצית עבור $x, y \in [0,1]$

$$|f_n(x) - f_n(y)| = \left|\left(n + Kx^d\right) - \left(n + Ky^d\right)\right| = \left|Kx^d - Ky^d\right| = K\left|x^d - y^d\right|$$

נסתכל על הפונקציה $f : [0,1] \to \mathbb{R}$ הנתונה על־ידי $f(x) = x^d$, זו פונקציה קעורה (כי הנגזרת היא מונוטונית יורדת ממש, $f'(x) = dx^{d-1}$, היא קעורה כי $0 < d < 1$ אז זה די ברור, אבל אם $d = 1$ זו פונקציה קבועה שהיא מונוטונית יורדת חלש).
מדף התכונות של הפונקציה בויקיפדיה, כאן, תכונה 6 , מתקיים

$$f(x) + f(y) \geq f(x+y) \iff -f(x+y) \geq -f(x) - f(y)$$

וזה מצויין ליהודים, כי אם ניקח $y \in [0,1]$ זה אומר שמתקיים עבור $g : [y,1] \to \mathbb{R}$ הנתונה על־ידי

$$g(x) = x^d - y^d - (x-y)^d = f(x) - f(y) - f(x-y)$$

זה בידיוק אומר שמתקיים $g(x) \leq 0$, אז אם נחזור לביטוי ממקודם שמצאנו

$$|f_n(x) - f_n(y)| = K\left|x^d - y^d\right| \leq K|x-y|^d$$

$\square$

טענה 0.1: נניח כי A, B בנות־מנייה. אז $A \times B$ בת־מנייה.

הוכחה של יאיר: בתרגיל הבית הוכחתם ש־$\mathbb{N} \times \mathbb{N}$ היא בת־מנייה ובתרגול ראיתם כי אם $|A| = |C|, |B| = |D|$ אזי $|A \times B| = |C \times D|$ ומשילוב שתי הטענות, הטענה נובעת. $\square$

הוכחה של נעה: למה צריך בכלל את החלק השני? הרי אם יש לי A, B בנות־מנייה, זה אומר שקיימות $f : A \to \mathbb{N}, g : B \to \mathbb{N}$ חד־חד ערכיות ועל.

עכשיו, $A \times B$ זה הרי $\{(a,b) \mid a \in A, b \in B\}$ אבל אם נגדיר $h : A \times B \to \mathbb{N} \times \mathbb{N}$ על־ידי $h(a,b) = (f(a), g(b))$ יש לנו חד־חד ערכיות ועל קורדינאטה קורדינאטה, אז זו פונקציה חד־חד ערכית ועל לקבוצה בת־מנייה, ולכן גם $A \times B$ קבוצה בת־מנייה. $\square$

$$4 = S(3) = \left\{\underbrace{\{\{\{\emptyset\}, \emptyset\}, \{\emptyset\}, \emptyset\}}_{=3}, \{\{\emptyset\}, \emptyset\}, \{\emptyset\}, \emptyset\right\}$$

$$\prod_{n<\omega} A_n = \left\{f : \mathbb{N} \to \bigcup A_n \mid \forall n < \omega, f(n) \in A_n\right\} \neq \emptyset$$

כל פונקציה בוחרת איבר אחד מ־A_n, אז זה כל הפונקציות בחירה מעל הסדרה A_n ו־$|A_n| = 2$ אז כל $f(n)$ יכול לקחת שני ערכים בידיוק, אז המכפלה זה סט כל הפונקציות מ־$\mathbb{N}$ ל־2 איברים (שיכול להיות ששונים זה מזה).
נגדיר $\varphi_n : A_n \to \{0,1\}$, אז כל $f \in \prod A_n$ ונגדיר $f \mapsto (\varphi_0(f(0)), \varphi_1(f(1)), \cdots) \in \{0,1\}^{\mathbb{N}}$ (זה מוגדר היטב כי $f(n) \in A_n$ מהגדרת המכפלה) ואז

$$\Phi : \prod_{n<\omega} A_n \to \{0,1\}^{\mathbb{N}}$$

הנתונה על־ידי

$$\Phi(f)(n) = \varphi_n(f(n))$$

היא חד־חד ערכית ועל:
חד־חד ערכית: כי אם $g \neq f$ עבור $n \in \mathbb{N}$ אז $f(n) \neq g(n)$ ולכן $\varphi_n(f(n)) \neq \varphi_n(g(n))$ ואז $\Phi(f)(n) \neq \Phi(g)(n)$
על: נובע מכך שניתן לקחת כל סדרה בינארית (b_n) ולהגדיר f לפיה על־ידי $f(n) = \varphi_n^{-1}(b_n)$ (כזכור φ_n חד־חד ערכית ועל מהגדרת שיוויון עוצמות). ראינו ש־$\left|\{0,1\}^{\mathbb{N}}\right| = \aleph_0$ ומצאנו איזומורפיזם ולכן מהגדרת שיוויון עוצמות גם $\left|\prod_{n<\omega} A_n\right| = \aleph_0$

שאלה 1

צריך לפרק את הפולינום x^8-1 מעל השדה $\mathbb{F}_{13}$.

פתרון: ראשית מתקיים

$$x^8-1=(x^4+1)(x^4-1)=(x^2-1)(x^2+1)(x^4+1)=(x-1)(x+1)(x^2+1)(x^4+1)$$

וגם $x+12\underset{\bmod 13}{\equiv}x-1$, ווגם את x^2+1 אפשר לפרק מעל $\mathbb{F}_{13}$ כי אם נציב $i\in\{0,\cdots,12\}$ נקבל ש־$i\in\{5,8\}\Longleftrightarrow 0\underset{\bmod 13}{\equiv}i^2+1$ ולכן יש לנו שורשים אז הפולינום יכול להתפרק

$$x^2+1\underset{\bmod 13}{\equiv}(x-5)(x-8)\underset{\bmod 13}{\equiv}(x+8)(x+5)$$

יש לי עוד לאן לפרק את x^4+1 מעל $\mathbb{F}_{13}$ וזה בעצם $\Phi_8(x)$, אז אפשר בתהליך קצר ארוך של בדיקה האם יש פיתרון ב־$\mathbb{F}_{13}$ לאחד מהבאים

1. $12\underset{\bmod 13}{\equiv}x^4$ על־ידי חישוב לכל $i\in\{0,\cdots,12\}$ האם $12\underset{\bmod 13}{\equiv}i^4$
2. האם יש פירוק $(x^2+ax+1)(x^2+bx+1)(\bmod 13)$
3. האם יש פירוק $(x^2+ax+c)(x^2+bx+d)(\bmod 13)$

כאשר את שני האחרונים זה פשוט לפתור מערכות משוואות כמו בלינארית, ואז יוצא שהפירוק הוא $x^4+1=(x^2+5)(x^2+8)$, ובסך־הכל

$$x^8-1\underset{\bmod 13}{\equiv}(x+12)(x+1)(x+5)(x+8)(x^2+5)(x^2+8)$$

השאלה היא האם יש דרך קצרה יותר שאני מפספסת: בעיקר לפירוק של x^4+1: חשבתי משהו בכיוון של מה השדה פיצול של $\Phi_8(x)$ מעל $\mathbb{F}_{13}$ ויצא לי ש־$\mathbb{F}_{169}=\mathbb{F}_{13^2}$ הוא הראשון שמכיל שורש יחידה מסדר 8, אז החבורת גלואה היא מסדר 2 ופועלת על 4 השורשים בהצמדה בזוגות (וגם עם הפרובניוס) $x\mapsto x^{13}$, אבל אז אני חוזרת לאותה נקודה

$$\Phi_8(x)=(x-\alpha)(x-\alpha^{13})(x-\beta)(x-\beta^{13})=(x^2-(\alpha+\alpha^{13})x+\alpha\alpha^{13})(x^2-(\beta+\beta^{13})x+\beta\beta^{13})$$

$\square$

שאלה 2

צריך להוכיח שקיימת פונקציה $f : \mathbb{N} \to \mathbb{N}$ הנתונה על־ידי $f(n) = n^2$.

הוכחה: ניזכר שהגדרנו $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ להיות $n \cdot m = \underbrace{n + \cdots + n}_{m \text{ פעמים}}$ ובהרצאה ראינו ש־$\mathbb{N} \times \mathbb{N}$ היא קבוצה (נובע מאקסיומת הזוג הלא סדור, אקסיומת ההחלפה ואקסיומת האיחוד).

נגדיר את התכונה $P(n,m) := m = n \cdot n$ ואז מאקסיומת ההפרדה $F = \{(n,m) \in \mathbb{N} \times \mathbb{N} \mid P(n,m)\}$ קיימת.

נגדיר

$$f = \{(x,y) \in \mathbb{N} \times \mathbb{N} \mid y = x \cdot x\}$$

זו פונקציה, כי לכל $x \in \mathbb{N}$ קיים ויחיד $\square$

שאלה 3

נוכיח כי $\min : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ היא פונקציה, כלומר נראה כי היא קבוצה המקיימת את תנאי הפונקציה.

הוכחה: שוב $\mathbb{N} \times \mathbb{N}$ קבוצה כי מכפלה קרטזית מגדירה קבוצות וגם $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$ היא קבוצה.
ונגדיר

$$\min(x, y) = \begin{cases} x & x \leq y \\ y & y < x \end{cases}$$

היות והטבעיים הוא סדר טוב מתקיים אחד מהבאים בידיוק: או ש־$x \leq y$ או ש־$y < x$ ולכן הפונקציה מוגדרת היטב.
נגדיר את התכונה $P(x, y, z)$ להיות $z = \min(x, y)$ ולכן מאקסיומת ההפרדה הקבוצה הבאה מוגדרת והיא מקיימת את תנאי הפונקציה

$$f = \{((x, y), z) \in (\mathbb{N} \times \mathbb{N}) \times \mathbb{N} \mid P(x, y, z)\}$$

$\square$

שאלה 4

יהיו $a, b \in \mathbb{R}$ כך שמתקיים $a < b$ ותהיי f פונקציה רציפה בקטע $[a, b]$ כך ש־$f(x) > 0$ לכל $x \in [a, b]$.

סעיף א'

ניתן אינסוף דוגמאות שונות לפונקציות $g : [a, b] \to \mathbb{R}$ המקיימות $\forall x \in [a, b], |g(x)| = f(x)$.

הוכחה: לכל $n \in \mathbb{N}$ נגדיר את

$$\forall x \in [a, b], s_n(x) = \begin{cases} 1 & s \\ -1 & s \end{cases}$$

$\square$

סעיף ב'

נמצא את כל הפונקציות הרציפות $g : [a, b] \to \mathbb{R}$ המקיימות $\forall x \in [a, b], |g(x)| = f(x)$.

הוכחה: היות ו־$f(x) > 0$, עלינו לקיים $g(x) = \pm f(x)$.

נטען שבגלל הדרישה לרציפות $g(x)$ חייב להתקיים $g(x) = \pm f(x)$ בלבד (זאת אומרת, הרציפות של g גוררת שאין החלפת סימן):

נניח בשלילה שלא כך ולכן יש לנו $g_3(x) : [a, b] \to \mathbb{R}$ רציפה המקיימת $|g_3(x)| = f(x)$ שמחליפה סימן ב־$x_0 \in [a, b]$ כלשהו.

יהי $x_0 \in [a, b]$ כך ש־g_3 מחליפה בו סימן, לפי הגדרת הגבול זה אומר (בלי הגבלת הכלליות לכיוון)

$$\lim_{x \to x_0^-} g_3(x) = f(x_0), \quad \lim_{x \to x_0^+} g_3(x) = -f(x_0)$$

g_3 רציפה בכל $[a, b]$ ולכן רציפה ב־x_0, אז מהגדרת הגבול מתקיים

$$\lim_{x \to x_0^-} g_3(x) = \lim_{x \to x_0^+} g_3(x)$$

אבל בגלל ש־$f(x) > 0$, לא ייתכן ש־$f(x) = -f(x)$ כי התכונה הזאת מתקיימת רק עבור $f(x) = 0$, אז

$$f(x_0) \neq -f(x_0) \Rightarrow \lim_{x \to x_0^-} g_3(x) \neq \lim_{x \to x_0^+} g_3(x)$$

בסתירה לרציפות g_3, ולכן אין g_3 המחליפה סימן ועל־כן $g_1(x) = f(x), g_2(x) = -f(x)$ הן הפונקציות הרציפות היחידות המקיימות

$$\forall x \in [a, b], \forall i \in [2], |g_i(x)| = f(x)$$

$\square$

שאלה 5

נחשב את סכום החזקות השלישיות של הפולינום $x^3 - x + 1$.

פתרון: נסמן ב־r_1, r_2, r_3 את השורשים של הפולינום ואנחנו רוצים לחשב את $r_1^3 + r_2^3 + r_3^3$.

באופן כללי, לכל $i \in \{1, 2, 3\}$ מתקיים $r_i^3 = r_i - 1$, אז $r_1^3 + r_2^3 + r_3^3 = r_1 + r_2 + r_3 - 3$ ונטען שהתשובה היא -3:
נחשב

$$\begin{aligned}(x - r_1)(x - r_2)(x - r_3) &= x^3 - x^2 r_3 - x^2 r_1 + x r_1 r_3 - x^2 r_2 + x r_2 r_3 + r_1 r_2 r_3 x - r_1 r_2 r_3 \\ &= x^3 - x^2(r_1 + r_2 + r_3) + x r_1 r_2 r_3 - r_1 r_2 r_3\end{aligned}$$

נסמן ב־a, b, c, d את המקדמים של הפולינום שלנו $ax^3 + bx^2 + cx + d$ ובמקרה שלנו $a = 1, b = 0, c = -1, d = 1$, ולכן עם השורשים לעיל זה אמור להתאים למקדמים של הפולינום כמובן, אז

$$a = 1, b = (r_1 + r_2 + r_3) = 0, c = r_1 r_2 r_3 = 1, c = -r_1 r_2 r_3 = -1$$

ולכן

$$r_1^3 + r_2^3 + r_3^3 = r_1 + r_2 + r_3 - 3 = -3$$

□

שאלה 6

נמצא את הפולינום המינימלי של $\sqrt{5}+\sqrt{3}$ מעל $\mathbb{Q}$, נראה שהוא אי־פריק מעל $\mathbb{Q}$, אי־פריק מעל $\mathbb{Z}[t]$ שנהיה פריק מודלו p לכל מודולו p.

הוכחה: נסמן $\alpha=\sqrt{3}+\sqrt{5}$, אז

$$\alpha=\sqrt{3}+\sqrt{5}\Longleftrightarrow\alpha^2=3+2\sqrt{3}\sqrt{5}+5\Longleftrightarrow\alpha^2-8=2\sqrt{3}\sqrt{5}\Longleftrightarrow\alpha^4-16\alpha^2+64=60\Longleftrightarrow\alpha^4-16\alpha^2+4$$

נשתמש בשיטה של "Rational root theorem" ממטלה 2:

הערה (תזכורת – Rational root theorem): $f\in\mathbb{Q}[x]$ עם מקדמים שלמים ונסמן $f(x)=a_nx^n+\dots+a_1x+a_0$.
אם $\frac{r}{s}\in\mathbb{Q}$ שורש של f אז $s\mid a_n, r\mid a_0$

במקרה שלנו $s=1$ ו־$r=\pm1,\pm2,\pm4$, הצבה קצרה מביאה לנו שכל תוצאה לא מניבה 0 ולכן אין שורש מעל $\mathbb{Q}$ וזה אומר שאין גורם לינארי (זה בעצם אומר שאין פיצול למכפלה של $f=gh$ כאשר $\deg(g)=1,\deg(h)=3$ או ההפך).
נשאר לבחון האם יש פיצול למכפלה של $f=gh$ עם $\deg(g)=\deg(h)=2$, אז נניח בשלילה שהוא פריק, ולכן

$$\alpha^4-16\alpha^2+4=(\alpha^2+a\alpha+b)(\alpha^2+c\alpha+d)=\alpha^4+c\alpha^3+d\alpha^2+a\alpha^3+ac\alpha^2+ad\alpha+b\alpha^2+bc\alpha+bd=$$
$$\alpha^4+\alpha^3(c+a)+\alpha^2(d+ac+b)+\alpha(ad+bc)+bd$$

אז $c+a=0\Rightarrow a=-c$ וכן $bd=4$ ולכן

$$ad+bc=0\Longleftrightarrow -cd+bc=0\Longleftrightarrow bc=cd\ (2)$$

וכן

$$d+ac+b=-16\Longleftrightarrow d-c^2+b=-16$$

מ־(2) יש 2 אופציות, או ש־$c=0$ או ש־$c\neq0$.
אם $c\neq0$ אז נחלק את (2) בו ונקבל $b=d$ ולכן מכך ש־$bd=4$ אז $b=\pm2$ אבל אז למשוואה $d+ac+b=-16$ אין פיתרון כי או ש־$-4=-16$ או ש־$4=-16$ וכמובן שניהם לא נכונים.
אז $c=0$, ולכן $d+b=-16$ וגם $bd=4$, אבל גם פה נובע ש־$b=d=\pm2$ ושוב אין פיתרון ולכן ההנחה בשלילה לא נכונה והפולינום אי־פריק מעל $\mathbb{Q}$.
עכשיו, נזכר בלמה השנייה של גאוס: f פולינום אי־פריק ב־$\mathbb{Z}[\alpha]$ אם ורק אם f פרימיטיבי ואי־פריק ב־$\mathbb{Q}[\alpha]$, ונשים לב שאכן הפולינום שלנו הוא פרימטיבי כי

$$\operatorname{cont}(\alpha^4-16\alpha^2+4)=\operatorname{cont}(1,-16,4)=\gcd(1,-16,4)=1$$

ולכן הפולינום הוא פרימיטיבי ועל־כן אי־פריק מעל $\mathbb{Z}[\alpha]$ מהלמה השנייה של גאוס.
נשאר רק להראות שהוא פריק מודלו p לכל מודולו p: נסמן $y=\alpha^2$ אז $\alpha^4-16\alpha^2+4\mapsto y^2-16y+7$ ומתקיים

$$\Delta=((-16)^2-4(1))4=256-16=240$$

□

שאלה 7

יהי f פולינום אי־פריק מעל שדה K ויהי L שדה הפיצול שלו. נניח ש־$G = \mathrm{Gal}(L/K)$ היא אבלית ונוכיח שכל שורש של f יוצר L.

הוכחה: נניח שלא ככה, ולכן עבור α שורש של f מתקיים $E = K(\alpha)$ ו־$E \subsetneq L$ ונשים לב ש־$[K(\alpha) : K] = \deg(f)$.

מהתאמת גלואה, יש התאמה חד־חד ערכית ועל בין $H \le \mathrm{Gal}(L/K)$ לבין שדות ביניים $K \subseteq E \subseteq L$.

היות ו־G אבלית, נובע כי כל תת־חבורה שלה היא נורמלית ולכן בפרט $H = \mathrm{Gal}(L/K(\alpha)) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\alpha) = \alpha\}$ זאת־אומרת, $K(\alpha) = L^H$ ובגלל שכל תת־חבורה אבלית היא נורמלית

$$K(\sigma(\alpha)) = L^H = L^{\mathrm{Gal}(L/K(\sigma(\alpha)))} = L^{\sigma H \sigma^{-1}} = L^H = K(\alpha)$$

זה בדיוק אומר שכל השורשים של f יוצרים את אותו שדה ביניים $K(\alpha)$, אבל זה בדיוק ההגדרה של שדה פיצול ושדה פיצול יחיד עד־כדי איזומורפיזם ולכן $L \subseteq K(\alpha)$ זאת־אומרת $L = K(\alpha)$ בסתירה להנחה. $\square$

שאלה 8

שאלה 4 – מועד א' תשפ"ב של שיא.

יהי התחום $D=\left\{\begin{pmatrix}x\\y\\z\end{pmatrix}\in\mathbb{R}^3\mid x+y+z=1\right\}$ ותהיי $f:\mathbb{R}^3\to\mathbb{R}$ הפונקציה הנתונה על־ידי $f(x,y,z)=x^2+2y^2+3z^2$.

נקבע האם f משיגה מינימום ומקסימום ב־D ואם כן נחשב את הערך.

פתרון:

שיטה ראשונה: בעזרת הלגראנז'יאן:

הגדרה 0.1 (הלגראנז'יאן): תהיי $B\subseteq\mathbb{R}^k$ פתוחה ו־$f,g_1,\cdots,g_n:B\to\mathbb{R}$ גזירות ברציפות עבור $n+1\le k$.

נגדיר את הקבוצה

$$A\coloneqq\{x\in B\mid g_1(x)=\cdots=g_n(x)=0\}$$

נניח כי לכל $a\in A$ מתקיים ש־$\nabla g_1(a),\cdots,\nabla g_n(a)\in\mathbb{R}^k$ בלתי־תלויים לינארית.

נגדיר את **הלגראנז'יאן** $\mathcal{L}:\mathbb{R}^n\times B\to\mathbb{R}$ באמצעות

$$\mathcal{L}(\lambda,x)=f(x)-\sum_{i=1}^{n}\lambda_i g_i(x)$$

תהיי $(\lambda,a)\in\mathbb{R}^n\times A$ נקודת קריטית של הלגראנז'יאן ונסמן $\hat{H}=H\mathcal{L}_{(\lambda,a)}$. אז מתקיים

1. a היא מינימום מקומי של $f|_A$ אם $H\mathcal{L}_a^\lambda$ חיובית בהחלט על $\ker(Dg_a)$ ולפי ההסיאן המוגבל זה קורה אם $(-1)^n\det\left(\hat{H}_i\right))>0$ לכל $2n+1\le i\le k+n$
2. a היא מקסימום מקומי של $f|_A$ אם $H\mathcal{L}_a^\lambda$ שלילית בהחלט על $\ker(Dg_a)$ ולפי ההסיאן המוגבל זה קורה אם $(-1)^{n+i}\det\left(\hat{H}_i\right))>0$ לכל $2n+1\le i\le k+n$
3. a היא אוכף של $f|_A$ אם $H\mathcal{L}_a^\lambda$ אינה מוחלטת על $\ker(Dg_a)$ ולפי ההסיאן המוגבל זה קורה אם $\det\left(\hat{H}_{2n+1}\right),\cdots,\det\left(\hat{H}_i\right)$ בעלי סימנים המתאימים לאחד משני המקרים הקודמים אבל ל־$\det\left(\hat{H}_{i+1}\right)$ יש סימן הפוך

אז נגדיר $g(x,y,z)=x+y+z-1$ ונשים לב ש־$Dg_{(x,y,z)}=\begin{pmatrix}1&1&1\end{pmatrix}\neq 0$ לכל $(x,y,z)\in\mathbb{R}^3$ נובע שניתן להשתמש בשיטת הלגראנז'יאן, והלגראנז'יאן נתון על־ידי

$$\mathcal{L}(\lambda,x,y,z)=x^2+2y^2+3z^2-\lambda x-\lambda y-\lambda z+\lambda$$

נחשב את הנקודות הקריטיות של $\mathcal{L}$ זוהי כמובן פונקציה רציפה

$$D\mathcal{L}_{(\lambda,x,y,z)}=\begin{pmatrix}-x-y-z+1 & 2x-\lambda & 4y-\lambda & 6z-\lambda\end{pmatrix}$$

נשווה ל־0 ונפתור את מערכת המשוואות

$$\begin{aligned}2x-\lambda=0&\Longrightarrow 2x=\lambda\\4y-\lambda=0&\Longrightarrow 4y=\lambda\\6z-\lambda=0&\Longrightarrow 6z=\lambda\\-x-y-z+1=0&\Longrightarrow x+y+z=1\end{aligned}$$

אז

$$2x=4y=6z\Longrightarrow x=2y=3z$$

ולכן

$$x+y+z=1\underset{x=2y}{\iff}3y+z=1\iff z=1-3y$$

אבל אבל

$$x=3z\iff x=3-9y\iff 11y=3\iff y=\frac{3}{11}$$

אז בסך־הכל

$$x = \frac{6}{11}, y = \frac{3}{11}, z = \frac{2}{11}, \lambda = \frac{12}{11}$$

ואכן גם מתקיימים

$$x + y + z = \frac{3}{11} + \frac{6}{11} + \frac{2}{11} = \frac{11}{11} = 1 \checkmark$$

$$\frac{12}{11} = 2 \cdot \frac{6}{11} = 4 \cdot \frac{3}{11} = 6 \cdot \frac{2}{11} \checkmark$$

ולכן יש נקודה אחת חשודה לקיצון והיא $(\lambda, x, y, z) = \left(\frac{12}{11}, \frac{6}{11}, \frac{3}{11}, \frac{2}{11}\right)$, נחשב את ההסיאן של $\mathcal{L}$:

$$H\mathcal{L}_{(\lambda,x,y,z)} = \begin{pmatrix} 0 & -1 & -1 & -1 \\ -1 & 2 & 0 & 0 \\ -1 & 0 & 4 & 0 \\ -1 & 0 & 0 & 6 \end{pmatrix}$$

צריך לבדוק את המינורים הראשיים מסדר מסדרים 3 ו-4.

מתקיים $(-1)^3 \det(H\mathcal{L}) = 44$ ועבור המינור מסדר 3 מתקיים $(-1)^3 \det \begin{pmatrix} 0 & -1 & -1 \\ -1 & 2 & 0 \\ -1 & 0 & 4 \end{pmatrix} = 6$ ולכן זו נקודת מינימום יחידה.

□

שאלה 9

שאלה 4 ממטלה 11 של דניאל: תהיי $f:\mathbb{R}^3\to\mathbb{R}$ הנתונה על־ידי $f(x,y,z)=2x+2y+3z$.
נסביר ונמצא למה f מקבלת ערך מקסימלי ומינימלי בקבוצה $A:=\left\{(x,y,z)\in\mathbb{R}^3 \mid x^2+y^2+3z^3=35,\ \ x+y+z=7\right\}$.

הוכחה: נטען ש־A קבוצה קומפקטית ולכן f שהיא פונקציה רציפה (פולינום בכמה משתנים) מקבלת עליה מינימום ומקסימום.
נגדיר $B:=\left\{(x,y,z)\in\mathbb{R}^3 \mid x^2+y^2+3z^3=35\right\}$ ונטען ש־B סגורה וחסומה ולכן לפי משפט היינה־בורל נקבל שהיא קומפקטית.
סגורה: אם $(x_n,y_n,z_n)_{n=1}^{\infty}$ סדרה ב־B שמתכנסת ל־(x,y,z) ובפרט $x_n\to x, y_n\to y, z_n\to z$.
לכל $n\in\mathbb{N}$ מתקיים $x_n^2+y_n^2+3z_n^2=35$ לכן מאריתמטיקה של גבולות נסיק שמתקיים $(x,y,z)=\lim_{n\to\infty} x_n^2+y_n^2+3z_n^2=35$ ולכן $(x,y,z)\in B$.
חסומה: נשים לב שמתקיים $\frac{x^2}{35}+\frac{y^2}{35}+\frac{z^2}{\frac{35}{3}}=1$ וזה בבירור חסום כי לדוגמה x מקבל ערך מקסימלי כאשר $y=z=0$ ואז $x=\sqrt{35}$.
אז B סגורה וחסומה ולכן לפי משפט היינה־בורל היא קומפקטית.
נגדיר $C:=\left\{(x,y,z)\in\mathbb{R}^3 \mid x+y+z=7\right\}$, זו בבירור קבוצה לא חסומה אבל זו כן קבוצה סגורה כי אם $(x_n,y_n,z_n)_{n=1}^{\infty}$ קבוצה ב־C שמתכנסת ל־(x,y,z) בפרט $x_n\to x, y_n\to y, z_n\to z$.
לכל $n\in\mathbb{N}$ מתקיים $x_n+y_n+z_n=7$ ולכן מאריתמטיקה של גבולות נסיק שמתקיים $x+y+z=\lim_{n\to\infty} x_n+y_n+z_n=7$ ולכן $(x,y,z)\in C$, אז C קבוצה סגורה.
נשים לב ש־$A=B\cap C$ ובהרצאה ראינו שחיתוך סופי של קבוצות סגורות הוא סגור (זה נובע מכך שאיחוד סופי של קבוצות פתוחות הוא פתוח, וקבוצה סגורה היא קבוצה שהמשלים שלה הוא פתוח ועם כללי דה־מורגן נקבל את הנדרש).
אז A קבוצה סגורה אבל מהגדרה $A\subseteq B$ ש־B קומפקטית וראינו שתת־קבוצה סגורה של קבוצה קומפקטית היא קומפקטית, ולכן A קומפקטית ולכן בהכרח f שרציפה מקבלת עליה מינימום ומקסימום.
אם f מינימום/מקסימום בנקודה פנימית של A, נוכל לבדוק לפי איפוס הגרדיאנט

$$\nabla f(x,y,z)=(2\ \ 2\ \ 3)\neq(0\ \ 0\ \ 0)$$

אז אין אף נקודה פנימית שבה f מקבלת מינימום/מקסימום, ולכן נצטרך להשתמש בשיטת כופלי לגראנז' (כי הנקודות קיצון מתקבלות רק על השפה של האילוצים).
נגדיר $g_1:\mathbb{R}^3\to\mathbb{R}$ על־ידי $g_1(x,y,z)=x^2+y^2+3z^2-35$ ו־$g_2:\mathbb{R}^3\to\mathbb{R}$ על־ידי $g_2(x,y,z)=x+y+z-7$ וכמובן ש־g_1,g_2 דיפרנציאביליות ברציפות כי אלו פולינומים ומתקיים

$$\nabla g_1(x,y,z)=(2x\ \ 2y\ \ 6z),\ \ \nabla g_2(x,y,z)=(1\ \ 1\ \ 1)$$

יש לנו בפועל שלוש משוואות של אילוצים שאנחנו יכולים להוציא

$$\nabla f(x,y,z)=\lambda\nabla g_1(x,y,z)+\mu\nabla g_2(x,y,z)\iff(2\ \ 2\ \ 3)=\lambda(2x,2y,6z)+\mu(1\ \ 1\ \ 1)$$

בבירור $\lambda\neq0$ כי $(2\ \ 2\ \ 3)$ ו־$(1\ \ 1\ \ 1)$ בלתי תלויים לינארית ולכן $y=\frac{2-\mu}{\lambda}=x$ ואם נציב $y=x$ באילוץ השני נקבל

$$z=7-2x$$

ומהצבה באילוץ הראשון

$$2x^2+3(7-2x)^2=35\iff x=2,4$$

ולכן הנקודות הן $(2,2,3),(4,4,-1)$ ומתקיים $f(2,2,3)=17, f(4,4,-1)=13$ ולכן המינימום הוא 13 בנקודה $(4,4,-1)$ והמקסימום הוא 17 בנקודה$(2,2,3)$.
אפשר גם בצורה אלימה לפתור את מערכת המשוואות אז נקבל מערכת משוואות

$$\begin{gathered}2=2x\lambda+\mu\implies\mu=2-2x\lambda\\2=2y\lambda+\mu\implies\mu=2-2y\lambda\\3=6z\lambda+\mu\implies\mu=3-6z\lambda\\x^2+y^2+3z^2=35\\x+y+z=7\end{gathered}$$

אבל אני אוותר. $\square$

שאלה 10

$$f:\mathbb{R}^2\to\mathbb{R},\ \ f(x)=f\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{cases}\frac{x_1^3}{x_1^2+x_2^2} & x_1\neq 0 \text{ או } x_2\neq 0\\ 0 & x_1=x_2=0\end{cases}$$

$$f\begin{pmatrix}t\\0\end{pmatrix}\underset{t\neq 0}{=}\frac{t^3}{t^2}\Longrightarrow \partial_{x_1}f(0)=\lim_{t\to 0}\frac{f\left(\begin{smallmatrix}t\\0\end{smallmatrix}\right)-f\left(\begin{smallmatrix}0\\0\end{smallmatrix}\right)}{t}=\lim_{t\to 0}\frac{\frac{t^3}{t^2}}{t}=1$$

$$\partial_{x_2}f(0)=\lim_{t\to 0}\frac{f\left(\begin{smallmatrix}0\\t\end{smallmatrix}\right)-f\left(\begin{smallmatrix}0\\0\end{smallmatrix}\right)}{t}=\lim_{t\to 0}=\frac{\frac{0}{0+t^2}}{t}=\lim_{t\to 0}\frac{0}{t}=0$$

שאלה 11

תהיי $B := \{(x,y) \in \mathbb{R}^2 \mid x^2 - xy + y^2 < 2\}$ ונחשב את האינטגרל $\int_B (x^2 - xy + y^2)dxdy$ באמצעות משפט חילוף משתנה.

פתרון:

משפט 0.1 (משפט חילוף משתנה – תזכורת): תהיינה $A, B \subseteq \mathbb{R}^k$ קבוצות פתוחות ו־$g : A \to B$ דיפאומורפיזם (חד־חד ערכית, על, גזירה ברציפות ובעלת הופכית גזירה ברציפות) ו־$f : B \to \mathbb{R}$ פונקציה רציפה.
אז f אינטגרבילית על B אם ורק אם הפונקציה $|x \mapsto (f \circ g)(x)|\det(Dg_x)$ אינטגרבילית על A ובמקרה זה מתקיים

$$\int_B f(t)dt = \int_A (f \circ g)(x)|\det(Dg_x)|dx$$

הקבוצה B מהווה אליפסה סביב הראשית שאינה מקבילה לצירים, ולכן נצטרך לבצע חילוף משתנה לינארי כדי להפוך את האליפסה לעיגול. נשתמש בהשלמה לריבוע:

$$x^2 - xy + y^2 = \left(x - \frac{1}{2}y\right)^2 - \frac{1}{4}y^2 + y^2 = \left(x - \frac{1}{2}y\right)^2 + \left(\frac{\sqrt{3}}{2}y\right)^2$$

נבצע את חילוף המשתנה הלינארי $\begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} x - \frac{1}{2}y \\ \frac{\sqrt{3}}{2}y \end{pmatrix}$ ואז

$$T^{-1} = \begin{pmatrix} 1 & -\frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{pmatrix}^{-1}$$

נזכר שמתקיים $\det(T^{-1}) = \frac{1}{\det(T)}$ ולכן

$$dxdy = \left|\det(T^{-1})\right|dudv = \frac{2}{\sqrt{3}}dudv$$

נסמן $A = T(B) = B_2(0) \setminus \{0\}$ אז ממשפט חילוף משתנה, הפונקציה f אינטגרבילית על B אם ורק אם $f \circ T^{-1}$ אינטגרבילית על A ומתקיים

$$\int_B f(x,y)dxdy = \int_A u^2 + v^2 \cdot \frac{s}{\sqrt{3}}dudv = \frac{2}{\sqrt{3}} \underset{\text{קוטביות}}{=} \frac{2}{\sqrt{3}} \int_0^{2\pi} \int_0^2 r^2 dr d\theta = \frac{2}{\sqrt{3}} \int_0^{2\pi} \left[\frac{r^3}{3}\right]_{r=0}^{r=2} d\theta = \frac{24\pi}{3\sqrt{3}}$$

□

שאלה 12

תהיי

$$C := \{(x,y)\in\mathbb{R}^2 \mid x>0,\ y>0,\ 1<xy<3,\ x^2<y^2<x^2+1\}$$

ונחשב באמצעות משפט חילוף משתנה את האינטגרל

$$\int_C (y^2-x^2)^{xy}(x^2+y^2)dxdy$$

פתרון:

משפט 0.2 (משפט חילוף משתנה – תזכורת): תהיינה $A,B\subseteq\mathbb{R}^k$ קבוצות פתוחות ו־$g:A\to B$ דיפאומורפיזם (חד־חד ערכית, על, גזירה ברציפות ובעלת הופכית גזירה ברציפות) ו־$f:B\to\mathbb{R}$ פונקציה רציפה.
אז f אינטגרבילית על B אם ורק אם הפונקציה $|(\det(Dg_x)|(f\circ g)(x) \mapsto x$ אינטגרבילית על A ובמקרה זה מתקיים

$$\int_B f(t)dt = \int_A (f\circ g)(x)|\det(Dg_x)|dx$$

נשים לב שמהאילוץ $x^2<y^2<x^2+1$ אנחנו מקבלים $0<y^2-x^2<1$ לכן הגיוני שנגדיר $\binom{u}{v}=\binom{xy}{y^2-x^2}$ ואז

$$J=\begin{pmatrix}\frac{\partial u}{\partial x} & \frac{\partial u}{\partial y}\\ \frac{\partial v}{\partial x} & \frac{\partial v}{\partial v}\end{pmatrix}=\begin{pmatrix}y & x\\ -2x & 2y\end{pmatrix}$$

אז

$$\det(J)=2y\cdot .y+x\cdot 2x=2(x^2+y^2)$$

ולכן

$$dxdy=\left|\det(J^{-1})\right|dudv \Longrightarrow dxdy=\frac{1}{2(x^2+y^2)}dudv$$

אז תחום האינטגרציה שלנו יהיה $A=\{(u,v)\in\mathbb{R}^2 \mid 1<u<3, 0<v<1\}$ ולכן

$$\int_C f(x,y)dxdy=\int_A \frac{v^u\cancel{(x^2+y^2)}}{2\cancel{(x^2+y^2)}}dudv=\frac{1}{2}\int_A v^u dudv=\frac{1}{2}\int_0^1\int_1^3 v^u dudv=\frac{1}{2}\int_0^1\left[\frac{v^u}{\ln(v)}\right]_{u=1}^{u=3}dv$$
$$=\frac{1}{2}\int_0^1\frac{v^3}{\ln(v)}-\frac{v}{\ln(v)}dv$$

אבל האינטגרל האחרון הוא לא אינטגרל שאנחנו יודעים לחשב, ולכן נשתמש במשפט פוביני

$$\frac{1}{2}\int_0^1\int_1^3 v^u dudv=\frac{1}{2}\int_1^3\int_0^1 v^u dvdu=\frac{1}{2}\int_1^3\left[\frac{v^{u+1}}{u+1}\right]_{v=0}^{v=1}=\frac{1}{2}\int_1^3\frac{1^{u+1}}{u+1}du=\frac{1}{2}\int_1^3\frac{1}{u+1}du=\frac{1}{2}[\ln(u+1)]_{u=1}^{u=3}$$
$$=\frac{1}{2}(\ln(4)-\ln(2))$$

$$T^{-1}=\begin{pmatrix}1 & 1\\ 0 & -1\end{pmatrix}$$

□

שאלה 13

צטטי והוכיחי את משפט הקירוב האופטימלי של טורי פורייה.

הוכחה: **ניסוח:** יהי $(V,\langle\cdot,\cdot\rangle)$ מרחב מכפלה פנימית ותהיי $(v_n)_{n=1}^{\infty}\in V$. יהיו $v\in V$ ו־$N\in\mathbb{N}$, אזי מתקיים

$$\min_{\alpha_n\in\mathbb{C}}\left\|v-\sum_{i=1}^{N}\alpha_n v_n\right\|=\left\|v-\sum_{i=1}^{N}\underbrace{\frac{\langle v_n,v\rangle}{\|v_n\|^2}}_{\text{מקדמי פורייה}}v_n\right\|$$

כלומר, מקדמי פורייה נותנים את הקירוב הטוב ביותר לטור.

הוכחה:

$$\langle v-\sum_{i=1}^{N}\alpha_n v_n,v-\sum_{i=1}^{N}\alpha_n v_n\rangle=\|v\|^2-\sum_{i=1}^{N}\overline{\alpha_n}\langle v_n,v\rangle-\sum_{i=1}^{N}\alpha_n\langle v,v_n\rangle+\sum_{i=1}^{N}|\alpha_n|^2\|v_n\|^2$$

נסמן $x_n=\frac{\langle v_n,v\rangle}{\|v_n\|^2}$ ונקבל

$$\left\|v-\sum_{i=1}^{N}\alpha_n v_n\right\|^2=\|v\|^2-\sum_{i=1}^{N}\left(\overline{\alpha_n}x_n-\alpha_n\overline{x_n}+|\alpha_n|^2\right)\|v_n\|^2$$

נשים לב שמתקיים

$$|\alpha_n-x_n|^2=(\alpha_n-x_n)(\overline{\alpha_n}-\overline{x_n})=|\alpha_n|^2-\overline{\alpha_n}x_n-\alpha_n\overline{x_n}+|x_n|^2$$

ולכן

$$\left\|v-\sum_{i=1}^{N}\alpha_n v_n\right\|^2=\|v\|^2+\sum_{i=1}^{N}\left(|\alpha_n-x_n|^2-|x_n|^2\right)\|v_n\|^2$$

אז יש לנו ביטוי שתלוי רק ב־α_n ולכן הוא מקסימלי כאשר $|\alpha_n-x_n|$ מתאפס, כלומר $\alpha_n=x_n$ ואז

$$\min_{\alpha_n\in\mathbb{C}}\left\|v-\sum_{i=1}^{N}\alpha_n v_n\right\|^2=\|v\|^2-\sum_{i=1}^{N}|x_n|^2\|v_n\|^2$$

□

שאלה 14

צטטי והוכיחי את עקרון המקומיות.

הוכחה: **ניסוח:** תהיי $f:\mathbb{R}\to\mathbb{R}$ מחזורית עם מחזור 2π ואינטגרבילית רימן על $[-\pi,\pi]$.
נסמן

$$S_N(x)=\frac{a_0}{2}+\sum_{k=1}^{N}(a_k\cos(kx)+b_k\sin(kx))$$

אז לכל $0<\delta\le\pi$ ולכל $x\in\mathbb{R}$ מתקיים

$$\lim_{N\to\infty}S_N(x)-\frac{1}{\pi}\int_0^{\delta}(f(x+u)+f(x-u))D_N(u)du=0$$

כאשר

$$D_N(u)=\frac{\sin\left((N+\frac{1}{2})u\right)}{2\sin(\frac{u}{2})}$$

גרעין דירכלה.

הוכחה: מנוסחת דירכלה אנחנו יודעים שמתקיים

$$S_N(x)=\frac{1}{\pi}\int_0^{\pi}(f(x+u)+f(x-u))D_N(u)du$$

ולכן ניתן לכתוב

$$\begin{aligned}S_N(x)-\frac{1}{\pi}\int_0^{\delta}(f(x+u)+f(x-u))D_N(u)du&=\frac{1}{\pi}\int_0^{\pi}(f(x+u)+f(x-u))D_N(u)du-\frac{1}{\pi}\int_0^{\delta}(f(x+u)+f(x-u))D_N(u)du\\&=\frac{1}{\pi}\int_{\delta}^{\pi}(f(x+u)+f(x-u))D_N(u)du\\&=\int_{\delta}^{\pi}\frac{f(x+u)+f(x-u)}{2\sin(\frac{u}{2})}\sin\left(\left(N+\frac{1}{2}\right)u\right)du\end{aligned}$$

נגדיר $\varphi(u)=\frac{f(x+u)+f(x-u)}{2\sin(\frac{u}{2})}$ ונשים לב שהיא אינטגרבילית ומוגדרת בכל $[\delta,\pi]$ מאריתמטיקה של פונקציות אינטגרביליות.
נזכיר את **הלמה של רימן:** $f:[-\pi,\pi]\to\mathbb{R}$ אינטגרבילית רימן על $[-\pi,\pi]$ אזי מתקיים

$$\lim_{N\to\infty}\int_{-\pi}^{\pi}f(x)\cos(Nx)dx=\lim_{N\to\infty}\int_{-\pi}^{\pi}f(x)\sin(Nx)dx=0$$

ולכן בשילוב עם הלמה של רימן ומה שמצאנו מתקיים

$$\lim_{N\to\infty}S_N(x)-\frac{1}{\pi}\int_0^{\delta}f(x+u)D_N(u)du=\lim_{N\to\infty}\int_{\delta}^{\pi}\frac{f(x+u)}{2\sin(\frac{u}{2})}\sin\left(\left(N+\frac{1}{2}\right)u\right)du=0$$

$\square$

שאלה 15

צטטי והוכיחי את משפט "התכנסות נקודתית של טורי פורייה".

הוכחה: **ניסוח:** תהיי $f:\mathbb{R}\to\mathbb{R}$ מחזורית עם מחזור 2π.

יהיו $x_0\in\mathbb{R}$ ו־$\pi \geq \delta > 0$ ונניח ש־f מקיימת את תנאי ליפשיץ ב־x_0. כלומר, יש $C>0$ ו־$u\in(0,\delta)$ כך שמתקיים

$$|f(x_0-u)-f(x_0-0)|\leq Cu, |f(x_0+u)-f(x_0+0)|\leq Cu$$

תחת תנאים אלו מתקיים

$$\lim_{N\to\infty} S_n(x_0)=\frac{f(x_0+0)+f(x_0-0)}{2}$$

הוכחה: נוכיח תכילה שמתקיים

$$\lim_{N\to\infty}\frac{1}{\pi}\int_0^\delta D_N(u)du=\frac{1}{2}$$

נגדיר $g:\mathbb{R}\to\mathbb{R}$ על־ידי $g(t)=\frac{1}{2}$ אז

$$a_0=\frac{1}{\pi}\int_{-\pi}^{\pi}g(t)dt=\frac{2\pi}{2\pi}=1, a_k=\frac{1}{2\pi}\int_{-\pi}^{\pi}\cos(kt)dt=\frac{1}{2\pi}\int_{-\pi}^{\pi}\sin(kt)dt=b_k$$

אז מעיקרון המקומיות מתקיים

$$\lim_{N\to\infty}\underbrace{S_N^g(x)}_{=\frac{1}{2}}-\frac{1}{\pi}\int_0^\delta\left(\underbrace{g(x+u)}_{=\frac{1}{2}}+\underbrace{g(x-u)}_{=\frac{1}{2}}\right)D_n(u)du=0\Longrightarrow\frac{1}{\pi}\int_0^\delta D_n(u)du=\frac{1}{2}$$

בפרט, מכפל בקבוע נקבל

$$\frac{1}{\pi}\int_0^\delta(f(x_0+0)+f(x_0-0))D_n(u)du=\frac{f(x_0+0)+f(x_0-0)}{2}$$

לכל f שמקיימת את תנאי המשפט. אז נפעיל שוב את עיקרון המקומיות ונקבל

$$\lim_{N\to\infty}S_N^f(x_0)-\frac{f(x_0+0)+f(x_0-0)}{2}=\lim_{N\to\infty}\frac{1}{\pi}\int_0^\delta(f(x_0+u)+f(x_0-u)-f(x_0+0)-f(x_0-0))D_n(u)du\ (\star)$$

נגדיר $\varphi(u)=\frac{f(x_0+u)+f(x_0-u)-f(x_0+0)-f(x_0-0)}{2\pi\sin(\frac{u}{2})}$ ולכן

$$(\star)=\lim_{N\to\infty}\int_0^\delta\varphi(u)\sin\left(\left(N+\frac{1}{2}\right)u\right)du$$

נראה כי $\varphi(u)$ אינטגרבילית על $[0,\delta]$ ואז מהלמה של רימן נוכל לסיים. ואכן, $\varphi(u)$ אינטגרבילית על $[\varepsilon,\delta]$ לכל $\varepsilon>0$ מאריתמטיקה של פונקציות אינטגרביליות ולכן מספיק שנראה חסימות ב־0:

$$|\varphi(u)|\underset{\text{אי־שיוויון המשולש}}{\leq}\frac{|f(x_0+u)-f(x_0+u)|+|f(x_0-u)-f(x_0-u)|}{2\pi\sin(\frac{u}{2})}\underset{\text{ליפשיציות}}{\leq}\frac{2Cu}{2\pi\sin(\frac{u}{2})}=\frac{Cu}{\pi\sin(\frac{u}{2})}$$

ונשים לב שמלופיטל $\frac{u}{\sin(\frac{u}{2})}\underset{u\to0}{\to}2$ ולכן $\frac{Cu}{\pi\sin(\frac{u}{2})}$ חסום וקיבלנו ש־$\varphi(u)$ אינטגרבילית על $[0,\delta]$ ולכן נוכל להשתמש בלמה של רימן ולקבל

$$\lim_{N\to\infty}\int_0^\delta\varphi(u)\sin\left(\left(N+\frac{1}{2}\right)u\right)du=0\ \checkmark$$

נזכיר את **הלמה של רימן**: $f:[-\pi,\pi]\to\mathbb{R}$ אינטגרבילית רימן על $[-\pi,\pi]$ אזי מתקיים

$$\lim_{N\to\infty}\int_{-\pi}^{\pi}f(x)\cos(Nx)dx=\lim_{N\to\infty}\int_{-\pi}^{\pi}f(x)\sin(Nx)dx=0$$

$\square$

שאלה 16

נסחי והוכיחי את משפט האוסדרוף.

הוכחה:

ניסוח: יהי (X,d) מרחב מטרי ותהיי $A \subseteq X$. A חסומה לחלוטין אם ורק אם לכל $(x_n)_{n=1}^{\infty} \subseteq A$ יש תת–סדרה קושי.

הוכחה:

$\Longrightarrow$ נניח כי לכל $(x_n)_{n=1}^{\infty} \subseteq A$ יש תת–סדרה קושי ונרצה להראות שהיא חסומה לחלוטין.
יהי $\varepsilon > 0$ ונניח בשלילה שהיא לא חסומה לחלוטין, ולכן לכל $x_1 \in A$ קיים $x_2 \in A$ כך שמתקיים $d(x_1,x_2) \geq \varepsilon$ ובאותו אופן יש $x_3 \in A$ כך שמתקיים $d(x_2,x_3) \geq \varepsilon$. נמשיך אינדוקטיבית ונבנה סדרה $(x_n)_{n=1}^{\infty}$ כזאת, אבל זו סדרה שבה המרחק בין כל שני איברים הוא יותר מ־ε ולכן בפרט אין לה תת־סדרה קושי, וזו סתירה להנחה ש־A לא חסומה לחלוטין.
$\Longleftarrow$ נניח כי A חסומה לחלוטין ונרצה להראות שלכל סדרה $(x_n)_{n=1}^{\infty} \subseteq A$ יש תת־סדרה קושי.
תהיי $(x_n)_{n=1}^{\infty} \subseteq A$ סדרה. מהנחת החסימות לחלוטין, עבור $\varepsilon = 1$ יש $B_{\varepsilon=1}^{1}$ כדור המכיל אינסוף מאיברי הסדרה $(x_n)_{n=1}^{\infty}$ ונסמן $V^0 = A$.
נגדיר $V^1 = V^0 \cap B_{\varepsilon=1}^{1}$ ומתקיים $\operatorname{diam}(V^1) \leq 2$ וגם V^1 חסומה לחלוטין (כתת־קבוצה של קבוצה חסומה לחלוטין).
נמשיך אינדוקטיבית ונגדיר $V^k = V^{k-1} \cap B_{\varepsilon=\frac{1}{k}}^{k}$ ומתקיים $\operatorname{diam}(V^k) \leq \frac{2}{k}$ ונשים לב שמתקיים $A = V^0 \supset V^1 \supset \cdots V^{k-1} \supset V^k$ $(\star)$.
נבחר אם־כך $x_{n_1} \in V^1, x_{n_2} \in V^2, \cdots, x_{n_k} \in V^k$ כך שמתקיים $n_k < n_l$ לכל $k < l$ ומתקיים $d\left(x_{n_k}, x_{n_{k+1}}\right) < \frac{1}{k} \xrightarrow[k\to\infty]{} 0$ בגלל $(\star)$ ולכן $\left(x_{n_k}\right)_{k=1}^{\infty}$ היא סדרת קושי. $\square$

שאלה 17

נסחי והוכיחי את המשפט שבמרחב הילברט המרחק לקבוצה קמורה וסגורה (ולא ריקה) מתקבל.

הוכחה:

ניסוח: יהי $\left(V, \sqrt{\langle \cdot\,, \cdot \rangle}\right)$ מרחב הילברט (כלומר, מרחב מכפלה פנימית שלם) עם הנורמה המושרית מהמכפלה הפנימית.

תהיי $\emptyset \neq U \subseteq V$, קבוצה קמורה וסגורה ב־$V$ ונגדיר לכל $f \in V$, $\mathrm{Dist}(f, U) = \inf_{u \in U} \|f - u\|$.

אז קיים ויחיד $g \in U$ כל שמתקיים $\mathrm{Dist}(f, U) = \|f - g\|$.

הוכחה: תהיי $g_1 \in U$, אם מתקיים $\mathrm{Dist}(f, U) = \|f - g_1\|$ סיימנו. אחרת, יש $g_2 \in U$ כך שמתקיים $\mathrm{Dist}(f, U) \leq \|f - g_2\| < \|f - g_1\|$.

נגדיר $a_n = \|f - g_n\|$ לכל $n \in \mathbb{N}$ ונקבל סדרה מונוטונית יורדת ממש כך שמתקיים $\lim_{n\to\infty} a_n = \mathrm{Dist}(f, U)$.

נראה כעת שהסדרה היא קושי, לשם כך עלינו להראות **למה**: במרחב מכפלה פנימית מתקיים *כלל המקבילית*, כלומר לכל $x, y \in V$

$$\|x + y\|^2 + \|x - y\|^2 = 2(\|x\|^2 + \|y\|^2)$$

הוכחת הלמה: זה נובע ישירות מהגדרת המכפלה הפנימית

$$\begin{aligned}
\|x + y\|^2 + \|x - y\|^2 &= \langle x + y, x + y \rangle + \langle x - y, x - y \rangle \\
&= \langle x, x \rangle + \langle x, y \rangle + \overline{\langle x,y \rangle} + \langle y, y \rangle + \langle x, x \rangle - \langle x, y \rangle - \overline{\langle x,y \rangle} + \langle y, y \rangle \\
&= 2\langle x, x \rangle + 2\langle y, y \rangle \\
&= 2(\|x\| + \|y\|)
\end{aligned}$$

נשתמש בלמה, מתקיים

$$\begin{gathered}
\left\|g_i - g_j\right\|^2 = \left\|g_i - g_j + f - f\right\|^2 = \left\|\left(f - g_j\right) - (f - g_i)\right\|^2 = 2\|f - g_i\|^2 + 2\left\|f - g_j\right\|^2 - \left\|2f - g_i - g_j\right\|^2 \\
= \|f - g_i\|^2 + 2\left\|f - g_j\right\|^2 - 4\left\|f - \frac{g_i - g_j}{2}\right\|^2 \underset{\substack{\text{קמורה U} \\ \frac{g_i - g_j}{2} \in U}}{\leq} 2\|f - g_i\|^2 + 2\left\|f - g_j\right\| - 4\,\mathrm{Dist}\,(f, U)^2 \\
\underset{\substack{j\to\infty \\ i\to\infty}}{\longrightarrow} 2\,\mathrm{Dist}\,(f, U)^2 + 2\,\mathrm{Dist}\,(f, U)^2 - 4\,\mathrm{Dist}\,(f, U)^2 = 0
\end{gathered}$$

ולכן $(a_n)_{n=1}^{\infty}$ היא סדרת קושי ומהיות המרחב השלם נובע שהיא מתכנסת ולכן קיים $g_0 \in V$ כך שמתקיים $\lim_{n\to\infty} a_n = g_0$ אבל U קבוצה סגורה ולכן $g_0 \in U$.

יחידות: ניזכר שפונקציית המרחק היא אינווריאטית להזזה וקבוצה היא קמורה וסגורה אם ורק אם גם ההזזה של היא קבוצה קמורה וסגורה, ולכן מספיק שנראה עבור המקרה של $f = 0$.

נניח בשלילה שהמרחק לא יחיד, ולכן יש $g_1 \neq g_2 \in U$ כך שמתקיים $d = \mathrm{Dist}(0, U) = \|g_1\| = \|g_2\|$.

נגדיר $w = \frac{g_1 + g_2}{2} \underset{\text{קמירות}}{\in} U$ ונחשב

$$\|w\|^2 = \frac{1}{4}\left(\|g_1\|^2 + \|g_2\|^2 + 2\Re(\langle g_1, g_2 \rangle)\right) \underset{\text{אי־שיוויון קושי־שוורץ}}{\leq} \frac{1}{4}\left(\|g_1\|^2 + \|g_2\|^2 + \|g_1\|\|g_2\|\right) - \frac{1}{4}(d^2 + d^2 + 2d^2) = d^2$$

יש שיוויון אם ורק אם g_1, g_2 תלויים לינארית:

אם g_1, g_2 לא תלויים לינארית אז יש אי־שיוויון חלש ואז $\|w\|^2 < d^2$ וזו סתירה להנחה, ולכן יש תלות לינארית.

בלי הגבלת הכלליות, $g_2 = \alpha g_1$ ומההנחה $\alpha \neq 1 \in \mathbb{C}$. אבל $\|g_1\| = |\alpha|\|g_2\| \Longrightarrow \|g_1\| = \|g_2\|$ ולכן $|\alpha| = 1$ אז

$$\begin{gathered}
\|w\|^2 = \frac{1}{4}\left(\|g_1\|^2 + \|g_2\|^2 + 2\Re(\langle g_1, g_2 \rangle)\right) = \frac{1}{4}(d^2 + d^2 + 2\Re(\langle g_1, \alpha g_2 \rangle)) = \frac{1}{4}(d^2 + d^2 + 2\Re(\alpha)^2 d^2) = \frac{d^2}{2}(1 + \Re(\alpha)) \\
\underset{\Re(\alpha)<1}{<} \frac{d^2}{2}(1 + 1) = d^2
\end{gathered}$$

וזאת שוב סתירה, ולכן ההנחה שלנו של שני ערכים שונים היא סתירה ועל־כן יש רק ערך אחד שמביא את המרחק.

$\square$

שאלה 18

צטטי והוכיחי את משפט הקירוב של ויירטשראס.

הוכחה:

ניסוח: תהיי $f \in C[0,1]$. אז קיימת $(P_n)_{n=1}^{\infty}$ סדרת פולינומים כך שמתקיים $P_n \rightrightarrows f$ (מתכנס במידה שווה).

הוכחה: נתחיל מרידוד הבעיה, נגדיר $g(x) = f(x) - f(0) - x(f(1) - f(0))$ כלומר $f(x) = g(x) + f(0) + x(f(1) - f(0))$ אז החלק המוסף הוא פולינום ועל־כן רציף ולכן מספיק לבחון את הקירוב ל־g, בלי הגבלת הכלליות נגדיר $f(0) = f(1) = 0$.

נגדיר $F : \mathbb{R} \to \mathbb{R}$ על־ידי $F(x) = \begin{cases} f(x) & x\in[0,1] \\ 0 & x\in\mathbb{R}\setminus[0,1] \end{cases}$ זו פונקציה רציפה במידה שווה על כל הישר $\mathbb{R}$ (מההנחה שעשינו).

נגדיר $P_n(x) = \int_{-1}^{1} F(x+u)Q_n(u)du$ כאשר $Q_n = C_n(1-u^2)^n$ ו־C_n הוא קבוע נרמול כך שיתקיים $\int_{-1}^{1} Q_n(u)du = 1$.

מהגדרת התומך, $F(x+u) \neq 0$ אם ורק אם $x+u \in [0,1]$ כלומר $u \in [-x, 1-x]$ ולכן

$$\int_{-x}^{1-x} F(x+u)Q_n(u)du = \int_{0}^{1} F(t)Q_n(t-x)dt$$

ומהמשפט היסודי, מהיות Q_n פולינום נקבל ש־P_n פולינום.

F רציפה, אז עבור $\varepsilon > 0$ יש $\delta > 0$ כך שאם $|x-y| \leq 2\delta$ אזי $|F(x) - F(y)| < \varepsilon$. נחשב

$$\begin{aligned}
|P_n(x) - F(x)| &= \left| \int_{-1}^{1} F(x+u)Q_n(u)du - F(x) \right| \\
&\underset{(1)}{=} \left| \int_{-1}^{1} F(x+u)Q_n(u)du - \int_{-1}^{1} F(x)Q_n(u)du \right| \\
&\underset{(2)}{\leq} \int_{-1}^{1} |F(x+u) - F(x)|Q_n(u)du \\
&\leq \underbrace{\int_{-1}^{\delta} |F(x+u) - F(x)|Q_n(u)du}_{I_1} + \underbrace{\int_{-\delta}^{\delta} |F(x+u) - F(x)|Q_n(u)du}_{I_2} + \underbrace{\int_{\delta}^{1} |F(x+u) - F(x)|Q_n(u)du}_{I_3}
\end{aligned}$$

כאשר (1) נובע מהיות $\int_{-1}^{1} Q_n(u)du = 1$ ו־(2) זה אי־שוויון המשולש האינטגרלי.

מרציפות F ישר נקבל

$$I_2 < \varepsilon \int_{-\delta}^{\delta} Q_n(u)du \leq \varepsilon \int_{-1}^{1} Q_n(u)du = \varepsilon$$

וכן מהרציפות נובע ש־F חסומה, ולכן קיים $0 < M \in \mathbb{R}$ חסם ואז

$$I_3 \leq 2M \int_{\delta}^{1} Q_n(u) = 2MC_n \int_{\delta}^{1} (1-u^2)^n \leq 2MC_n \underbrace{(1-\delta^2)}_{\text{סופרמום}} \underbrace{(1-\delta)}_{\text{גבולות אינטגרציה}} \leq 2MC_n(1-u^2)^n$$

כעת, נרצה לחסום את C_n ונזכור שהוא מנרמל כך שיתקיים $\int_{-1}^{1} Q_n(u)du = 1$, אז

$$\int_{-1}^{1} (1-u^2)^n du \geq \int_{\frac{-1}{\sqrt{n}}}^{\frac{1}{\sqrt{n}}} (1-u^2)^n du \underset{(1)}{\geq} 2\int_{0}^{\frac{1}{\sqrt{n}}} (1-u^2)^n du \underset{(2)}{\geq} 2\int_{0}^{\frac{1}{\sqrt{n}}} 1 - nu^2 du$$

$$\geq 2\left[u - \frac{nu^3}{3}\right]_{u=0}^{u=\frac{1}{\sqrt{n}}} = \frac{2}{\sqrt{n}} - \frac{2n\frac{1}{\sqrt{n}^3}}{3} = \frac{2}{\sqrt{n}} - \frac{2}{3\sqrt{n}} = \frac{4}{3\sqrt{n}} \geq \frac{1}{\sqrt{n}} \Longrightarrow C_n \leq \sqrt{n}$$

כאשר (1) נובע מהיות הפונקציה סימטרית על קטע סימטרי, (2) זה אי־שוויון ברנולי.

נבחין שהקטעים I_1, I_3 הם סימטריים ולכן בסך־הכל מתקיים $|P_n(x) - F(x)| < \varepsilon + 4MC_n(1-\delta^2)^n \xrightarrow[n\to\infty]{} 0$

כלומר, לכל $n \in \mathbb{N}$ יש $n > M$ כך שמתקיים לכל $x \in \mathbb{R}$ $|P_n(x) - F(x)| < 2\varepsilon$ וזה בדיוק אומר $P_n \underset{\mathbb{R}}{\rightrightarrows} f$ ובפרט $P_n \underset{[0,1]}{\rightrightarrows} f$. □

שאלה 19

צטטי והוכיחי את משפט סטון־ויירשטראס.

הוכחה:

ניסוח: יהי (X,ρ) מרחב מטרי ו־$K\subseteq X$ קבוצה קומפקטית. נסתכל על המרחב $(C(K),\|\cdot\|_\infty)$ כאשר

$$C(K):=\{f:K\to\mathbb{R}\mid f\text{ רציפה}\},\qquad \|\cdot\|_\infty=\sup_{x\in K}|f(x)|$$

תהיי $A\subseteq C(K)$ אלגברה, מפרידה בין נקודות ואינה מתאפסת באף נקודה. אז $\overline{A}=C(K)$.

הוכחה: נשתמש בשתי למות ללא הוכחה **למה 1**: A אלגברה בתנאי המשפט ויהיו $x_1,x_2\in X$ ו־$c_1,c_2\in\mathbb{R}$.

אז יש $f\in A$ כך שמתקיים $f(x_1)=c_1, f(x_2)=c_2$.

למה 2: אם A אלגברה ב־$C(K)$ אז גם $\overline{A}$ אלגברה ב־$C(K)$.

כעת נוכיח שתי למות נוספות:

למה 3: A אלגברה בתנאי המשפט ו־$f\in A$, אז $|f|\in\overline{A}$.

הוכחת למה 3: יהי $\varepsilon>0$, מספיק להוכיח שיש $\varphi\in\overline{A}$ כך שמתקיים $\sup_{x\in K}|f(x)-\varphi(x)|<\varepsilon$.

ניקח $d=\sup_{x\in K}|f(x)|$ ונגדיר $g(t):[-d,d]\to\mathbb{R}$ על־ידי $g(t)=|t|$ זו פונקציה רציפה ולכן ממשפט הקירוב של ויירשטראס יש $(P_n)_{n=1}^\infty$ סדרת פולינום כך שלכל $t\in[-d,d]$ מתקיים $||t|-P_n(x)|<\varepsilon$ ולכן בפרט לכל $x\in K$ מתקיים גם $||f(x)|-P_n(f(x))|<\varepsilon$ אז $\varphi=P_n(f(x))\in\overline{A}$ ונקבל $|f|\in\overline{A}$.

למה 4: אם $f,g\in\overline{A}$ אז $\max(f,g),\min(f,g)\in\overline{A}$.

הוכחת למה 4: נגדיר $\min(f,g)=\frac{f+g-|f-g|}{2}$, $\max(f,g)=\frac{f+g+|f-g|}{2}$ ויחד עם למות 2,3 זה מסיים (המקרה הכללי באינדוקציה).

הוכחת המשפט: יהיו $\varepsilon>0, f\in C(K), x\in K$. נרצה לבנות פונקציה g_x כך שיתקיים

1. $g_x\in\overline{A}$ 2. $g_x(x)=f(x)$ 3. $\forall t\in K,\ g_x(t)>f(t)-\varepsilon$

מהלמה הראשונה, לכל $y\in K$ יש $h_y\in A$ כך שמתקיים $h_y(x)=f(x), h_y(y)=f(y)$ ולכן נגדיר $J_y=\{t\in K\mid h_y(t)>f(t)-\varepsilon\}$, ברור $y\in J_y$ וזה כיסוי פתוח של K ומהקומפקטיות יש לו תת־כיסוי סופי, כלומר $K=\bigcup_{i=1}^n J_{y_i}$.

נגדיר $g_x=\max\left(h_{y_1},\cdots h_{y_n}\right)$ ומהלמה הרביעית נקבל $g_x\in\overline{A}$ ומתקיים $h_{y_1}(x)=\cdots=h_{y_n}=f(x)$ ולכן $g_x(x)=f(x)$.

לכל $t\in K$ יש $i\in[n]$ כך ש־$t\in h_{y_i}$ ולכן $g_x(t)\ge h_{y_i}(t)>f(t)-\varepsilon$.

נגדיר $\hat{J}_x=\{t\in K\mid g_x(t)<f(t)+\varepsilon\}$ וכמובן $x\in\hat{J}_x$ ושוב זה כיסוי פתוח של K ומהקומפקטיות $K=\bigcup_{i=1}^m\hat{J}_{x_i}$ ונגדיר $\varphi(t)=\min\left(g_{x_1}(t),\cdots,g_{x_m}(t)\right)$ ולכן $t\in K$ יש $j\in[m]$ כך שמתקיים $t\in\hat{J}_{x_j}$ ואז $g_{x_j}(t)<f(t)+\varepsilon$ ולכן בפרט $\varphi(t)\le g_{x_j}(t)<f(t)+\varepsilon$ וגם $\varphi(t)=g_{x_j}(t)>f(t)-\varepsilon$ ולכן בפרט $\|\varphi-f\|_\infty$ כלומר $\overline{A}=C(K)$. $\square$

שאלה 20

עבור $p\neq 3$ ראשוני נגדיר K_p שדה הפיצול של הפולינום x^9-1 מעל $\mathbb{F}_p$.
נמצא את כל חבורות גלואה האפשריות $G\big(K_p/\mathbb{F}_p\big)$.

הוכחה: ראשית, שדה הפיצול הוא יחיד עד־כדי איזומורפיזם וידוע ש־$K_p=\mathbb{F}_p(\xi_9)$, ולכן מטענה שראינו על חבורות גלואה של הרחבות ציקלוטומיות מתקיים $\mathrm{Gal}\big(K_p/\mathbb{F}_p\big)\simeq(\mathbb{Z}/9\mathbb{Z})^\times=\{1,2,4,5,7,8\}$.
זו חבורה מגודל 6 וגם $\varphi_{\text{אוילר}}(9)=6$ ולכן המחלקים האפשריים של חבורה מסדר 6 הם $\{1,2,3,6\}$ אז $\mathrm{ord}_9(p)\in\{1,2,3,6\}$.
אנחנו רוצים למצוא את ה־n המינימלי כך ש־$\mathbb{F}_{p^n}$ מכיל את ξ_9, אז זה בידיוק ה־n המינימלי כך ש־$9\mid(p^n-1)$ כאשר $n\in\{1,2,3,6\}$ ו־$p\neq 3$ ראשוני. אז

1. עבור $9\mid(p^1-1)$ נבחר $p=19$ שראשוני ואז $19-1=18\underset{\bmod 9}{\equiv}0$ כלומר $19\underset{\bmod 9}{\equiv}1$
2. עבור $9\mid(p^2-1)$ נשים לב ש־$p=2$ לא מתאים, עבור $p=5$ נקבל $25\underset{\bmod 9}{\not\equiv}1$ אז לא מתאים, עבור $p=7$ נקבל $49\underset{\bmod 9}{\not\equiv}1$ אז גם לא מתאים, עבור $p=9$ כמובן שלא מתאים, $p=11$ אז $11^2=121\underset{\bmod 9}{\not\equiv}1$ וגם $13^2=169\underset{\bmod 9}{\not\equiv}1$ ועבור $p=17$ נקבל $17^2\underset{\bmod 9}{\equiv}1$ כלומר $p=17$ מקיים את מה שרצינו
3. עבור $9\mid(p^3-1)$ ברור ש־$p\neq 2$ ואז עבור $p=5$ נקבל $125-1=124\underset{\bmod 9}{\not\equiv}0$ ועבור $p=7$ נקבל $7^3=343\underset{\bmod 9}{\equiv}1$ אז $p=7$
4. עבור $9\mid(p^6-1)$ אם נבחר $p=2$ נקבל $2^6=64\underset{\bmod 9}{\equiv}1$

עשיתי את כל החישובים בכוח, אפשר גם לא בכוח?

□

שאלה 21

נמצא במפורש את כל ההרחבות הריבועיות של $\mathbb{Q}(\xi_{21})$.

הוכחה: הפולינום המינימלי הוא $\Phi_{21}(x)$ שאין שום מצב שאזכור אותו, אז נתעלם ממנו. מתקיים

$$\varphi_{\text{אויילר}}(21) = |\{x \in [20] \mid \gcd(21, x) = 1\}| = |\{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}| = 12$$

ולפי משפט שראיינו מתקיים $[\mathbb{Q}(\xi_{21}) : \mathbb{Q}] = 12$ ולכן לפי עוד משפט שראינו מתקיים $\mathrm{Gal}(\mathbb{Q}(\xi_{21})/\mathbb{Q}) \simeq (\mathbb{Z}/21\mathbb{Z})^\times =$ $\{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$ היא אכן חבורה מסדר 12.

במטלה ראינו שמשפט השאריות הסיני רלוונטי לחבורות הכפליות ולכן

$$(\mathbb{Z}/21\mathbb{Z})^\times \simeq (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/7\mathbb{Z})^\times \simeq C_2 \times C_6 \simeq C_6 \times C_2 \underset{\text{משפט המיון}}{\simeq} (C_2 \times C_2) \times C_3$$

יש 3 תתי־חבורות מסדר 2, אחת מסדר 3, אחת מסדר 4 ו־3 מסדר 6 (גוגל).

מהתאמת גלואה, יש התאמה חד־חד ערכית ועל בין תתי־חבורות לבין שדות ביניים כך שלכל תת־חבורה מתאים שדה ביניים כך שדרגת ההרחבה של שדות היא האינדקס של של תת־החבורה (כלומר, תת־חבורה מסדר 6 היא מאינדקס 2 ולכן מובילה להרחבה ריבועית):

סדר תת־החבורה	אינדקס	דרגת ההרחבה
1	12	12
2	6	6
3	4	4
4	3	3
6	2	2
12	1	1

לפי תרגיל 7.5.13 "שראינו" בסיכומים של מיכאל מתקיים $\mathbb{Q}(\xi_3, \xi_7) = \mathbb{Q}(\xi_{21})$ ו־ξ_3, ξ_7 הם בלתי תלויים לינארית (הם יוצרים הרחבה מדרגה 12 ביחד בעוד שהדרגה של המכפלה שלהם היא $\varphi_{\text{אויילר}}(3) \cdot \varphi_{\text{אויילר}}(7) = 2 \cdot 6 = 12$ והפולינומים המינימליים שלהם זרים, אז אין תלות לינארית ביניהם).

נזכור שתת־חבורה של חבורה אבלית היא תמיד חבורה נורמלית וכל חבורה כזאת וויתרתי באמצע. $\square$

שאלה 22

נוכיח שלא בהכרח אם $f \in \mathbb{F}[x]$ פולינום אי־פריק וספרבילי מדרגה n ו־E שדה פיצול שלו אז ב־$\mathrm{Gal}(E/F)$ יש איבר מסדר n.

הוכחה: ניקח $F = \mathbb{Q}$ ואת $f(x) = x^4 - 10x^2 + 1$.

ראשית הוא אי־פריק באמצעות Rational root theorem כי $r = \pm 1 \mid a_0 = 1$ וגם $s = \pm 1 \mid a_n = 1$.

אז $f(1) = 1^4 - 10 + 1 = -8, f(-1) = (-1)^4 - 10 \cdot (-1)^2 + 1 = -8$ אז אין לו שורשים ב־$\mathbb{Q}$ אז בפרט זה אומר שלא ניתן לפרק אותו למכפלה של פולינום מדרגה 1 ועם פולינום מדרגה 3.

אז אם הוא פריק, יש לו פירוק למכפלה של דרגות 2, כלומר

$$\begin{aligned} x^4 - 10x^2 + 1 &= (x^2 + ax + b)(x^2 + cx + d) = x^4 + cx^3 + dx^2 + ax^3 + acx^2 + adx + bx^2 + bcx + bd \\ &= x^4 + x^3(a+c) + x^2(d + ac + b) + x(ad + bc) + bd \end{aligned}$$

אז

$$bd = 1 \Longleftrightarrow b = d = 1 \lor b = d = (-1)$$
$$a + c = 0 \Longleftrightarrow a = -c$$
$$ad + bc = 0 \Longleftrightarrow ad = -bc \Longleftrightarrow -cd = -bc$$

אם $a = c = 0$ אז $d + ac + b = d + b = 10$ וזה לא ייתכן כי $b = d = 1 \lor b = d = -1$. אז $c \neq 0$.

$$d + ac + b = 10 \Longleftrightarrow d - c^2 + b = 10 = \begin{cases} c^2 = -8 ✗ & d = b = 1 \\ c^2 = -12 ✗ & d = b = (-1) \end{cases}$$

אז שוב הגענו למצב שאין פיתרון ולכן $f(x)$ אי־פריק מעל $\mathbb{Q}$.

הוא ספרבילי, כי $f'(x) = 4x^3 - 20x = 4x(x^2 - 5)$ כלומר השורשים הם $x = 0, x = \pm\sqrt{5}$ אבל $f(0) \neq 0 \land f\left(\sqrt{5}\right) \neq 0 \land f\left(-\sqrt{5}\right) \neq 0$ (הם לא שורשים של f וראינו ששורש של f הוא שורש מרובה אם ורק אם $f'(x) = 0$).

נרצה למצוא את השורשים של f: נגדיר $y = x^2$ ואז f נהפך להיות $y^2 - 10y + 1$, מנוסחת השורשים

$$y = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} = \frac{10 \pm \sqrt{100 - 4}}{2} = \frac{10 \pm \sqrt{96}}{2} = \frac{10 \pm \sqrt{16 \cdot 6}}{2} = \frac{10 \pm 4\sqrt{6}}{2} = 5 \pm 2\sqrt{6}$$

כלומר $\sqrt{5 + 2\sqrt{6}}, \sqrt{5 - 2\sqrt{6}}, -\sqrt{5 + 2\sqrt{6}}, -\sqrt{5 - 2\sqrt{6}}$ הם השורשים של f.

נניח כעת שאפשר לפשט את הביטוי הזה, כלומר

$$\sqrt{5 + 2\sqrt{6}} = \sqrt{a} + \sqrt{b} \Longleftrightarrow 5 + 2\sqrt{6} = a + b + 2\sqrt{ab} \Longleftrightarrow \{a + b = 5 \quad ab = 6 \Longleftrightarrow a = 2, b = 3$$

אז בעצם $E = \mathbb{Q}\left(\sqrt{3}, \sqrt{2}\right)$ ולכן $[E : \mathbb{Q}] = 4$ ואנחנו יודעים שמתקיים $|\mathrm{Gal}(E/\mathbb{Q})| = 4$ ויש רק שני חבורות מסדר 4 והן $\mathbb{Z}_4, V_4$ (חבורת קליין והחבורה הציקלית מסדר 4).

נטען שזו חייבת להיות חבורת קליין: חבורת גלואה מכילה את כל האוטומורפיזמים שהם תמורות על השורשים.

נסמן $\alpha = \sqrt{2} + \sqrt{3}, \beta = \sqrt{2} - \sqrt{3}$ אז ייתכן רק $\sigma : \sqrt{\alpha} \mapsto -\sqrt{\alpha}, \tau : \sqrt{\beta} \mapsto -\sqrt{\beta}$ ואז ייתכן שחבורת גלואה מכילה רק את אוטומורפיזם הזהות, הנגדי ל־$\sqrt{\alpha}$, הנגדי ל־$\sqrt{\beta}$ והאוטומורפיזם ששולח לנגדי של $\sqrt{\alpha}, \sqrt{\beta}$.

כל איבר פה הוא מסדר 2 ואין אף איבר מסדר 4 ולכן לא ייתכן שהחבורה תהיה איזומורפית לחבורה הציקלית מסדר 4 ולכן $\mathrm{Gal}(E/\mathbb{Q}) \simeq V_4$.

אז זה מהווה דוגמה נגדית לטענה. $\square$

שאלה 23

נמצא את $\left|\operatorname{Aut}\left(\mathbb{Q}\left(\sqrt[n]{2}\right)/\mathbb{Q}\right)\right|$ עבור $n \in \mathbb{N}$.

פתרון: הפולינום המינימלי של השדה $\mathbb{Q}\left(\sqrt[n]{2}\right)$ הוא $f(x) = x^n - 2$.

שדה הפיצול מעל $\mathbb{Q}$ יהיה $F = KL$ עבור $K = \mathbb{Q}(\xi_n)$ ו־$L = \mathbb{Q}\left(\sqrt[n]{2}\right)$ אז הסדר של חבורת גלואה יהיה

$$[F : \mathbb{Q}] = \frac{[K : \mathbb{Q}] \cdot [L : \mathbb{Q}]}{[K \cap L : \mathbb{Q}]} = \frac{n\varphi_{\text{אויילר}}(n)}{[K \cap L : \mathbb{Q}]} = \frac{n\varphi_{\text{אויילר}}(n)}{m}$$

ונתקעתי פה כי זה לא בחומר מסתבר?

f אי־פריק מקריטריון אייזנשטיין מעל $\mathbb{Z}[x]$ עם $p = 2$ ומתקיים $\operatorname{cont}(x^n - 2) = \gcd(1, 2) = 1$ ולכן מהלמה השנייה של גאוס הוא אי־פריק מעל $\mathbb{Q}$ ועל־כן $\left[\mathbb{Q}\left(\sqrt[n]{2}\right) : \mathbb{Q}\right] = n$.

השורשים של הפולינום נתונים על־ידי $\sqrt[n]{2}\xi^k$ עבור $0 \le k \le n - 1$, $\xi = e^{\frac{2\pi i}{n}}$.

כלומר, $\operatorname{Gal}\left(\mathbb{Q}\left(\sqrt[n]{2}\right)/\mathbb{Q}\right) \simeq \mathbb{Z}/n\mathbb{Z}$ כי היא נוצרת על־ידי איבר אחד ($\sqrt[n]{2} \mapsto \sqrt[n]{2}\xi^k$ עבור $0 \le k \le n - 1$). $\square$

שאלה 24

נוכיח שהטענה הבאה לא נכונה: עבור $n \in \mathbb{N}$, שדה הפיצול של $x^n - 2$ מעל $\mathbb{Q}$ הוא מדרגה $n \cdot \varphi_{\text{אויילר}}(n)$.

הוכחה: ראינו כבר ש־$\sqrt{2} \in \mathbb{Q}(\xi_8) = \mathbb{Q}\left(\sqrt{2}, i\right)$ (בגלל שמצאנו את כל השדות ביניים של $\mathbb{Q}(\xi_8)$).
שדה הפיצול של $x^8 - 2$ הוא $\mathbb{Q}\left(\sqrt[8]{2}, i\right)$ שהוא מדרגה 16 מעל $\mathbb{Q}$ בעוד

$$8 \cdot \varphi_{\text{אויילר}}(8) = 8 \cdot |\{x \in \{1, \cdots, 7\} \mid \gcd(x, 8) = 1\}| = 8 \cdot |\{1, 3, 5, 7\}|) = 8 \cdot 4 = 32$$

נשים לב

$$\left[\mathbb{Q}\left(\sqrt[8]{2}, i\right) : \mathbb{Q}\right] = 8 \cdot 2 = 16$$

כי $\sqrt[8]{2}$ הוא שורש של הפולינום $x^8 - 2$ שהוא אי־פריק מעל $\mathbb{Q}$ עם קריטריון אייזנשטיין עם $p = 2$ $\square$

שאלה 25

יהי E שדה הפיצול של $f(x) = x^7 + x^6 + x^3 + x^2 + x + 1 \in \mathbb{F}_2[x]$. נמצא את הגודל של E ונמצא את טיפוס האיזומורפיזם של $\text{Gal}(E/\mathbb{F}_2)$.

הוכחה: ל־f יש שורש יחיד ב־$\mathbb{F}_2$ כי $\mathbb{F}_2 = \{0,1\}$ ומתקיים

$$f(1) = 1+1+1+1+1+1 = 6 = 0$$
$$f(0) = 0+0+0+0+0+1 = 1 \neq 0$$

אז $x = 1$ הוא שורש, כלומר $f(x) = (x+1)g(x)$ עבור $g(x) \in \mathbb{F}_2[x]$ פולינום מדרגה 6 ואם נעשה חלוקת פולינומים

$$\frac{x^7+x^6+x^3+x^2+x+1}{x+1} = \frac{(x+1)(x^6)+x^3+x^2+x+1}{x+1} = x^6 + \frac{x^3+x^2+x+1}{x+1} = x^6 + \frac{(x+1)x^2+x+1}{x+1}$$
$$= x^6 + x^2 + \frac{x+1}{x+1} = x^6+x^2+1 = g(x)$$

אין שורש ל־$g(x)$ כי $g(0) = 1 \neq 0, g(1) = 3 = 1 \neq 0$.

נשים לב $(x^3+x+1)(x^3+x+1) \underset{\in\mathbb{F}_2[x]}{=} x^6+x^2+1$ וזה כבר פולינום אי־פריק כי הוא מדרגה 3 ובלי שורשים ולפי מטלה 1 נקבל שהוא אי־פריק. אז

$$f(x) = x^7+x^6+x^3+x^2+x+1 = (x+1)(x^3+x+1)^2$$

בשביל השדה פיצול נצטרך להוסיף את השורשים של x^3+x+1 אז אם נסמן ב־α את השורש של הפולינום הזה ונסתכל על $E = \mathbb{F}_2(\alpha)$.

הוספנו את α, כלומר הוספנו אופציה לביטוי לינארי אז החזקות שיכולות להיות הן של α עד חזקת 2, אז כל איבר ב־$\mathbb{F}_2(\alpha)$ הוא מהצורה

$$a_0 + a_1\alpha + a_2\alpha^2 \ (a_0, a_1, a_2 \in \mathbb{F}_2)$$

ולכן בסיס להרחבה הוא

$$\{1, \alpha, \alpha^2\}$$

צריך להראות שהבסיס בלתי־תלוי לינארי ובשביל זה צריך להראות ש־α, α^2 בלתי־תלויים לינארית: כי אם הם היו תלויים לינארית, היה צריך להתקיים

$$a_1\alpha + a_2\alpha^2 = 0 (a_1, a_2 \in \mathbb{F}_2)$$

אם $a_1 = a_2 = 0$, סיימנו. אם $a_1, a_2 = 1$ אז $\alpha(1+\alpha) = 0 \iff \alpha + \alpha^2 = 0$ וזו סתירה לאי־פריקות שמצאנו.

נשאר $(a_1 = 1 \wedge a_2 = 0) \vee (a_1 = 0 \wedge a_2) = 1$ ושניהם מובילים לאותה סתירה על האי־פריקות שמצאנו.

אז זה אכן בסיס, ויש לנו $2^3 = 8$ אפשרויות לאיברים, כלומר כל האיברים בהרחבה הם

$$\{0, 1, \alpha, \alpha^2, 1+\alpha, 1+\alpha^2, \alpha+\alpha^2, 1+\alpha+\alpha^2\}$$

אז $|E| = 8 = 2^3$, אז $E = \mathbb{F}_2(\alpha) = \mathbb{F}_{2^3}$ (כי יש רק שדה אחד עם 8 איברים).

עובר טיפוס האיזומורפיזם לפי משפט שראינו יתקיים $\text{Gal}(E/\mathbb{F}_2) = \text{Gal}(\mathbb{F}_{2^3}/\mathbb{F}_2) = \mathbb{Z}/3\mathbb{Z}$.

□