פתרון מטלה 04 — מבנים אלגבריים 2, 80446

9 במאי 2025

שאלה 1

תהיי L/F הרחבת שדות ויהיו $g,h\in F[x]$. נוכיח שה־gcd של g,h כאיברים של $L[x]$ (שמכיל את $F[x]$) זהה ל־gcd שלהם ב־$F[x]$.

הוכחה: נסמן

$$d=\gcd(g,h)\in F[x]$$
$$D=\gcd(g,h)\in L[x]$$

בכיוון הראשון, מתקיים $d(x)=a(x)g(x)+b(x)h(x)$, אבל D מחלק את g,h ולכן גם $D\mid d$.

בכיוון השני, ב־$L[x]$, d הוא פולינום שמחלק את g,h ולכן מהגדרה הוא מחלק גם את ה־gcd שלהם ולכן $d\mid D$.

מצאנו שגם $D\mid d$ וגם $d\mid D$ ולכן $d=D$. $\square$

שאלה 2

יהי F שדה.

סעיף א'

תהיינה $f,g,h\in F[x]$ ו־$c\in F$.

תת־סעיף א'

נראה שמתקיימת הזהות $(g+h)'=g'+h'$.

הוכחה: נסמן $g=\sum_{i=0}^{n}a_ix^i, h=\sum_{j=0}^{m}b_jx^j$ ולכן $g'=\sum_{i=1}^{n}ia_ix^{i-1}, h'=\sum_{j=1}^{m}jb_jx^{j-1}$ ואז

$$g'+h'=\sum_{i=1}^{n}ia_ix^{i-1}+\sum_{j=1}^{m}jb_jx^{j-1}$$

מצד שני, מתקיים

$$(g+h)'=\left(\sum_{k=0}^{p}(a_k+b_k)x^k\right)'=\sum_{k=1}^{p}k(a_k+b_k)x^{k-1}\underset{\star}{=}\sum_{i=1}^{n}ia_ix^{i-1}+\sum_{j=1}^{m}jb_jx^{j-1}=g'+h'$$

כאשר $(\star)$ כאשר המעבר $\star$ נובע מכך שחל מהאינדקסים, בפוטנציאל הם 0.

מצאנו שאכן מתקיימת הזהות $(g+h)'=g'+h'$. $\square$

תת־סעיף ב'

נראה שמתקיימת הזהות $(c\cdot g)'=c\cdot g'$.

הוכחה: נשים לב שמתקיים

$$(cg)'=\left(\sum_{i=0}^{n}ca_ix^i\right)'=\sum_{i=1}^{n}ica_ix^{i-1}=c\sum_{i=1}^{n}ia_ix^{i-1}=cg'$$

$\square$

תת־סעיף ג'

נראה שמתקיימת הזהות $(g\cdot h)'=g'\cdot h+g\cdot h'$

הוכחה: שוב נסמן

$$g=\sum_{i=0}^{n}a_ix^i,\qquad h=\sum_{j=0}^{m}b_jx^j$$

מצד אחד מתקיים

$$(g\cdot h)'=\left(\sum_{i=0}^{n}a_ix^i\sum_{j=0}^{m}b_jx^j\right)'=\left(\sum_{i=0}^{n}\sum_{j=0}^{m}a_ib_jx^{i+j}\right)'\underset{(\star)}{=}\sum_{k=1}^{n+m}kc_kx^{k-1}$$

כאשר $(\star)$ נובע מהגדרת המכפלה בין טורים כאשר $c_k=\sum_{i+j=k}a_ib_j$. מצד שני מתקיים

$$g'\cdot h+g\cdot h'=\sum_{i=1}^{n}ia_ix^{i-1}\cdot h+g\cdot\sum_{j=1}^{m}jb_jx^{j-1}=\sum_{i=1}^{n}ia_ix^{i-1}\cdot\sum_{j=0}^{m}b_jx^j+\sum_{j=1}^{m}jb_jx^{j-1}\cdot\sum_{i=0}^{n}a_ix^i$$

$$=\sum_{i=1}^{n}\sum_{j=0}^{m}ia_ib_jx^{i-1+j}+\sum_{j=1}^{m}\sum_{i=0}^{n}ja_ib_jx^{j-1+i}=\sum_{k=1}^{m+n}\left(\sum_{i+j=k+1}ia_ib_j\right)x^k+\sum_{k=1}^{m+n}\left(\sum_{i+j=k+1}jb_ja_i\right)x^k$$

$$=\sum_{k=1}^{m+n}\left(\sum_{i+j=k+1}ia_ib_j+\sum_{i+j=k+1}jb_ja_i\right)x^k=\sum_{k=1}^{m+n}\left(\sum_{i+j=k}(i+j)a_ib_j\right)x^k=\sum_{k=1}^{m+n}kc_kx^{k-1}=(g\cdot h)'$$

כאשר האינדקס של $k=i+j$ זה סכימת כל הזוגות $k=(i,j)$ כאשר $1\le k\le m+n$ ו־c_k כמקודם. $\square$

סעיף ב'

נוכיח את המקרה הפרטי הבא של כלל לופיטל (L'Hôpital):
אם $a \in F$ הוא שורש של $g \in F[x]$ כך ש-$g(x) = h(x) \cdot (x-a)$ אז $g'(a) = h(a)$.
הוכחה: ראשית, מההנחה ש-$a \in F$ הוא שורש של g נקבל ש-$(x-a) \mid g$, ולכן קיימת $h(x) \in F[x]$ כך שיתקיים $g(x) = h(x) \cdot (x-a)$.
מהסעיף הקודם נקבל שמתקיים

$$g'(x) = (h(x) \cdot (x-a))' = h'(x)(x-a) + h(x)(x-a)' = h'(x)(x-a) + h(x)$$

שכן הנגזרת של פולינום ממעלה 1 הוא המקדם של האיבר המוביל ובמקרה שלנו זה 1.
אבל a הוא שורש של g, ולכן בהצבה נקבל

$$g'(a) = h'(x) \underbrace{(a-a)}_{0} + h(a) = h(a)$$

□

שאלה 3

בכל סעיף נבדוק האם הפולינום הוא ספרבילי מעל $\mathbb{Q}$ ונמצא שורש כפול ב־$\mathbb{Q}$ במידה ויש כזה.

סעיף א'

הפולינום $f = x^3 - 3x + 2$.

פתרון: נשים לב ש־$f(1) = 1^3 - 3 \cdot 1 + 2 = 1$ ולכן 1 הוא שורש של הפולינום 1 ומתקיים $(x-1) \mid f$.

נבחן מה הריבוי שלו ובשביל זה נבצע חלוקת פולינומים

$$\frac{x^3-3x+2}{x-1} \Rightarrow x^2 + \frac{x^2-3x+2}{x-1} \Rightarrow x^2 + x + \frac{-2x+2}{x-1} \Rightarrow x^2 + x - 2 = (x-1)(x+2)$$

משמע מתקיים

$$x^3 - 3x + 2 = (x-1)^2(x+2) = (x^2-2x+1)(x+2) = x^3 + 2x^2 - 2x^2 - 4x + x + 2 = x^3 - 3x + 2$$

ולכן מצאנו ש־$(x-1)$ הוא שורש מרובה עם ריבוי 2 ב־f ולכן f לא פולינום ספרבילי. □

סעיף ב'

הפולינום $f = x^3 - 7x + 6$.

פתרון: f ממעלה 3 ולכן ניתן להשתמש באלגוריתם ממטלה 2 כדי לבחון אם יש לו שורשים.

נסמן $a_n = 1$ ו־$a_1 = 6$, ולכן $r \in \{\pm 1, \pm 3, \pm 2\}$, $s = 1$, נבחן את כל המקרים האפשריים

1. $r = s = 1$ ואז

$$f\left(\frac{r}{s}\right) = f(1) = 1^3 - 7 \cdot 1 + 6 = 1 - 7 + 6 = 0$$

2. $s = 1, r = -1$ ואז

$$f\left(\frac{r}{s}\right) = f(-1) = (-1)^3 - 7 \cdot (-1) + 6 = -1 + 7 + 6 = 12 \neq 0$$

3. $s = 1, r = 2$

$$f\left(\frac{r}{s}\right) = f(2) = 2^3 - 7 \cdot 2 + 6 = 8 - 14 + 6 = 0$$

4. $s = 1, r = -2$

$$f\left(\frac{r}{s}\right) = f(-2) = (-2)^3 - 7 \cdot (-2) + 6 = -8 + 14 + 6 = 12 \neq 0$$

5. $s = 1, r = 3$

$$f\left(\frac{r}{s}\right) = f(3) = 3^3 - 7 \cdot 3 + 6 = 27 - 21 + 6 = 12 \neq 0$$

6. $s = 1, r = -3$

$$f\left(\frac{r}{s}\right) = f(-3) = (-3)^3 - 7 \cdot (-3) + 6 = -27 + 14 + 6 = 0$$

ולכן $\{1, 2, -3\}$ הם קבוצת השורשים של f, שכן f ממעלה 3 ולכן יש לו לכל היותר 3 שורשים. עוד מתקיים

$$(x-1)(x-2)(x+3) = (x^2-3x+2)(x+3) = x^3 + 3x^2 - 3x^2 - 9x + 2x + 6 = x^3 - 7x + 6$$

ולכן כל אחד מהשורשים של f הוא עם ריבוי 1 ולכן מהגדרה הוא ספרבילי. □

סעיף ג'

הפולינום $f = x^4 - 4x^3 + 6x^2 - 4x + 1$.

פתרון: המקדמים של f שלמים ולכן ניתן להשתמש באלגוריתם ממטלה 2: נמצא $\frac{r}{s} \in \mathbb{Q}$ שבר מצומצם כך ש־$r \mid a_0$ ו־$s \mid a_n$ ונבחן האם $\frac{r}{s}$ הוא שורש של f, משמע האם $f\left(\frac{r}{s}\right) = 0$.

נשים לב שייתכן רק $r, s \in \{\pm 1\}$ ולכן המקרים $r = s = 1 \wedge r = s = -1$ זהים וגם $r = 1, s = -1 \wedge r = -1, s = 1$ גם כן שווים.

בלי הגבלת הכלליות נבדוק:

1. $r = s = 1$

$$f\left(\frac{r}{s}\right) = f(1) = 1^4 - 4 \cdot 1^3 + 6 \cdot 1^2 - 4 \cdot 1 + 1 = 1 - 4 + 6 - 4 + 1 = 0$$

2. $r = 1, s = -1$

$$f\left(\frac{r}{s}\right) = f\left(\frac{1}{-1}\right) = f(-1) = 1^4 - 4 \cdot (-1)^3 + 6 \cdot (-1)^2 - 4 \cdot (-1) + 1 = 16 \neq 0$$

ולכן $x = 1$ הוא שורש של f, נבצע חילוק פולינומים

$$\begin{aligned} \frac{x^4 - 4x^3 + 6x^2 - 4x + 1}{x - 1} &= x^3 + \frac{-3x^3 + 6x^2 - 4x + 1}{x - 1} = x^3 - 3x^2 + \frac{3x^2 - 4x + 1}{x - 1} \\ &= x^3 - 3x^2 + 3x + \frac{-x + 1}{x - 1} = x^3 - 3x^2 + 3x - 1 = g \end{aligned}$$

שוב נעשה את אותו התהליך כמקודם ושוב $r, s \in \{\pm 1\}$, נבדוק כל אופציה

1. $r = s = 1$

$$g\left(\frac{r}{s}\right) = g(1) = 1^3 - 3 \cdot 1^2 + 3 \cdot 1 - 1 = 0$$

2. $r = 1, s = -1$

$$g\left(\frac{r}{s}\right) = g\left(\frac{1}{-1}\right) = g(-1) = (-1)^3 - 3 \cdot (-1)^2 + 3 \cdot (-1) - 1 = 8 \neq 0$$

ושוב $x = 1$ הוא שורש של g, נבצע שוב חילוק פולינומים

$$\frac{x^3 - 3x^2 + 3x - 1}{x - 1} = x^2 + \frac{-2x^2 + 3x - 1}{x - 1} = x^2 - 2x + \frac{x - 1}{x - 1} = x^2 - 2x + 1 = h$$

אבל אנחנו כבר יודעים ש־h מתפרק מעל $\mathbb{Q}[x]$ ל־$h = x^2 - 2x + 1 = (x - 1)^2$, ולכן בסך־הכל קיבלנו

$$f = x^4 - 4x^3 + 6x^2 - 4x + 1 = (x - 1)^4$$

לכן ל־f יש שורש אחד עם ריבוי מסדר 4 ולכן בהגדרה הוא אינו פולינום ספרבילי. $\square$

שאלה 4

נקבע בכל סעיף האם ההרחבה שדות הנתונה היא נורמלית.

סעיף א'

נראה שההרחבה $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)/\mathbb{Q}$ היינה נורמלית.

הוכחה: נסתכל על הפולינום $f=(x^2-2)(x^2-3)$. אנחנו יודעים ששדה הפיצול שלו צריך להכיל את $\sqrt{2},\sqrt{3}$ ואנחנו יודעים שההרחבה המינימלית שמכילה את האיברים האלו היא בידיוק $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$, ולכן זה שדה הפיצול של הפולינום f.

ראינו שלהיות הרחבה נורמלית זה שקול ללהיות שדה פיצול של פולינום כלשהו ולכן ההרחבה $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)/\mathbb{Q}$ היא הרחבה נורמלית. $\square$

סעיף ב'

נראה שההרחבה $\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}$ אינה נורמלית.

הוכחה: נניח בשלילה שההרחבה $\mathbb{Q}\left(\sqrt[3]{2}\right)$ היינה נורמלית, ולכן כל $p\in\mathbb{Q}[x]$ אי־פריק עם שורש ב־$\mathbb{Q}\left(\sqrt[3]{2}\right)$ מתפצל לגורמים לינאריים ב־$\mathbb{Q}\left(\sqrt[3]{2}\right)[x]$.

בפרט, זה נכון עבור הפולינום $f=x^3-2$ שהוא אי־פריק ב־$\mathbb{Q}$ (ממטלה 1, זה פולינום ממעלה 3 שהשורשים שלו לא ב־$\mathbb{Q}$ ולכן אי־פריק).

נשים לב ש־$\alpha=\sqrt[3]{2}\in\mathbb{Q}\left(\sqrt[3]{2}\right)$ ו־α הוא שורש של f, ולכן $x-\alpha\mid f$ לגורמים לינאריים ב־$\mathbb{Q}\left(\sqrt[3]{2}\right)$.

אנחנו כבר יודעים ששאר השורשים של f הם מעל המרוכבים: נסמן $\omega=-\frac{1}{2}+\frac{\sqrt{3}}{2}i$ ואז $\omega\sqrt[3]{2},\omega^2\sqrt[3]{2}$ הם גם שורשים של f.

f ממעלה 3 ולכן יש לו לכל היותר 3 שורשים, משמע מצאנו את כולם, ולכן חלוקה בגורם $x-\alpha$ (שהוא השורש הממשי של f) תשאיר אותנו עם מכפלה של איברים שאינם ב־$\mathbb{Q}\left(\sqrt[3]{2}\right)$ (מרוכבים) ולכן בפרט לא יכול להתפצל למכפלה של גורמים לינאריים ב־$\mathbb{Q}\left(\sqrt[3]{2}\right)[x]$ וזאת סתירה ולכן ההרחבה $\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}$ אינה נורמלית. $\square$

סעיף ג'

נראה שההרחבה $\mathbb{Q}\left(\sqrt[3]{2},\omega\sqrt[3]{2}\right)/\mathbb{Q}(\omega)$ כאשר $\omega=-\frac{1}{2}+\frac{\sqrt{3}}{2}i$ שורש יחידה פרימיטיבי מסדר 3 היא הרחבה נורמלית.

הוכחה: שוב נסתכל על הפולינום $f=x^3-2$, אנחנו יודעים שהשורשים שלו הם $\left\{\sqrt[3]{2},\omega\sqrt[3]{2},\omega^2\sqrt[3]{2}\right\}$, אם נראה ש־$\omega^2\sqrt[3]{2}\in\mathbb{Q}\left(\sqrt[3]{2},\omega\sqrt[3]{2}\right)$, סיימנו (כי f יתפצל לחלוטין ב־$\mathbb{Q}\left(\sqrt[3]{2},\omega\right)$ ולכן מהשקילות נקבל שההרחבה היא נורמלית).

נשים לב שמתקיים

$$(1)\ \left[\mathbb{Q}\left(\sqrt[3]{2}\right):\mathbb{Q}\right]=3,\ (2)\ [\mathbb{Q}(\omega):\mathbb{Q}]=2$$

כאשר (1) נובע מכך ש־x^3-2 הוא הפולינום המינימלי ב־$\mathbb{Q}\left(\sqrt[3]{2}\right)$ והוא ממעלה 3 ו־(2) נובע מכך שהפולינום המינימלי הוא x^2+x+1 והוא ממעלה 2.

מכפליות הדרגה מתקיים

$$\left[\mathbb{Q}\left(\sqrt[3]{2},\omega\right):\mathbb{Q}\right)]=\left[\mathbb{Q}\left(\sqrt[3]{2}\right):\mathbb{Q}\right]\cdot[\mathbb{Q}(\omega):\mathbb{Q}]=2\cdot 3=6$$

ולכן הבסיס של $\mathbb{Q}\left(\sqrt[3]{2},\omega\right)$ הוא

$$B_{\mathbb{Q}\left(\sqrt[3]{2},\omega\sqrt[3]{2}\right)}=\left\{1,\sqrt[3]{2},\sqrt[3]{4},\omega,\sqrt[3]{2}\omega,\omega\sqrt[3]{4}\right\}$$

כאשר $B_{\mathbb{Q}\left(\sqrt[3]{2}\right)}=\left\{1,\sqrt[3]{2},\sqrt[3]{4}\right\},B_{\mathbb{Q}\left(\omega\sqrt[3]{2}\right)}=\left\{1,\omega\sqrt[3]{2}\right\}$.

נשים לב ש־$\omega^2\sqrt[3]{2}$ אם כך הוא צירוף לינארי של איברי הבסיס ולכן $\omega^2\sqrt[3]{2}\in\mathbb{Q}\left(\sqrt[3]{2},\omega\right)$ ונקבל ש־f מתפצל לחלוטין ב־$\mathbb{Q}\left(\sqrt[3]{2},\omega\sqrt[3]{2}\right)/\mathbb{Q}(\omega)$ וההרחבה הזאת נורמלית. $\square$

שאלה 5

עבור $a,b,c\in\mathbb{Q}$ שאינם כולם 0, נמצא נוסחה מפורשת ל־$x,y,z\in\mathbb{Q}$ כך שמתקיים

$$\left(a+b\cdot\sqrt[3]{5}+c\cdot\sqrt[3]{5^2}\right)=x+y\cdot\sqrt[3]{5}+z\cdot\sqrt[3]{5^2}$$

כלומר, נוסחה מפורשת להופכי של איבר ב־$\mathbb{Q}\left(\sqrt[3]{5}\right)$.

פתרון: נסמן $\omega=-\frac{1}{2}+\frac{\sqrt{3}}{2}i$ ונגדיר

$$S=\left(a+b\cdot\omega\sqrt[3]{5}+c\cdot\omega^2\sqrt[3]{5^2}\right)\cdot\left(a+b\cdot\omega^2\sqrt[3]{5}+c\cdot\omega\sqrt[3]{5^2}\right)$$

אנחנו יודעים כבר $\omega^2+\omega+1=0\Rightarrow\omega^2+\omega=-1,\omega^3=1,\omega^2=\overline{\omega}$, נחשב ונקבל עם הזהויות הללו

$$\begin{aligned}S&=a^2+ab\cdot\omega^2\sqrt[3]{5^2}+ac\cdot\omega\sqrt[3]{5^2}+ab\cdot\omega\sqrt[3]{5}+\sqrt[3]{5^2}b^2+bc\cdot5\omega^2+ac\cdot\omega^2\sqrt[3]{5^2}+bc\cdot5\omega+5\sqrt[3]{5}c^2\\&=a^2+b^2\sqrt[3]{5^2}+5c^2\sqrt[3]{5}+\underbrace{ab\cdot\omega^2\sqrt[3]{5}+ab\cdot\omega\sqrt[3]{5}}_{(\star)}+\underbrace{ac\cdot\omega\sqrt[3]{5^2}+ac\cdot\omega^2\sqrt[3]{5^2}}_{(\star\star)}+\underbrace{bc\cdot5\omega+bc\cdot5\omega^2}_{(\star\star\star)}\\&=a^2+\sqrt[3]{5^2}b^2+5\sqrt[3]{5}c^2+\underbrace{-ab\sqrt[3]{5}}_{(\star)}+\underbrace{-ac\sqrt[3]{5^2}}_{(\star\star)}+\underbrace{-5bc}_{(\star\star\star)}\end{aligned}$$

כאשר $(\star),(\star\star),(\star\star\star)$ נובעים מהזהות $\omega^2+\omega=-1$ וקיבלנו ש־$S\in\mathbb{Q}\left(\sqrt[3]{5}\right)$ (שכן $\sqrt[3]{5^2}$ הוא בבסיס של הרחבה זאת כפי שראינו בשאלה הקודמת).

נסמן $\alpha=(a+b\sqrt[3]{5}+c\sqrt[3]{5^2}$ ונראה כעת $S\cdot\alpha\in\mathbb{Q}$ על־ידי חישוב

$$\begin{aligned}S\cdot\alpha&=\left(a^2+\sqrt[3]{5^2}b^2+5\sqrt[3]{5}c^2-ab\sqrt[3]{5}-ac\sqrt[3]{5^2}-5bc\right)\left(a+b\sqrt[3]{5}+c\sqrt[3]{5^2}\right)\\&=a^3+5b^3+25c^3-15abc+\cancel{\sqrt[3]{5}a^2b}+\cancel{\sqrt[3]{5^2}a^2c}+\cancel{\sqrt[3]{5^2}b^2a}+\cancel{5\sqrt[3]{5}b^2c}+\cancel{5\sqrt[3]{5}ac^2}+\cancel{5\sqrt[3]{5^2}c^2b}\\&\quad-\cancel{\sqrt[3]{5}a^2b}-\cancel{\sqrt[3]{5^2}ab^2}-\cancel{\sqrt[3]{5^2}a^2c}-\cancel{5\sqrt[3]{5}ac^2}-\cancel{5\sqrt[3]{5}b^2c}-\cancel{5\sqrt[3]{5^2}bc^2}\\&=a^3+5b^3+25c^3-15abc\end{aligned}$$

ולכן קיבלנו $S\cdot\alpha\in\mathbb{Q}$.

נבחר אם כך $\frac{S}{S\cdot\alpha}$ ונקבל

$$\frac{S}{S\cdot\alpha}\cdot\alpha=1\iff\frac{S}{S\cdot\alpha}=\alpha^{-1}=\left(a+b\sqrt[3]{5}+c\sqrt[3]{5^2}\right)^{-1}$$

ולכן

$$x=\frac{a^3-5abc}{a^3+5b^3+25c^3},y=\frac{5b^3-5abc}{a^3+5b^3+25c^3},z=\frac{25c^3-5abc}{a^3+5b^3+25c^3}$$

□

שאלה 6

נפרק את הפולינום $f(x,y,z) = x^3 + y^3 + z^3 - 3xyz \in \mathbb{Z}[x,y,z]$ לגורמים אי־פריקים.

פתרון: בתור התחלה, נגיע לחזקות 3 של x, y:

$$(x+y)^3 = (x+y)^2(x+y) = (x^2+2yx+y^2)(x+y) = x^3+yx^2+2yx^2+2y^2x+y^2x+y^3 = x^3+3yx^2+3y^2x+y^3$$

ולכן

$$x^3+y^3+z^3-3xyz = (x+y)^3+z^3-3xyz-3yx^2-3y^2x = (x+y)^3+z^3-3xy(x+y+z)$$

ננסה לפרק את הביטוי $(x+y)^3+z^3$ עם גורם $x+y+z$ כדי שיתאים לגורם הימני שלנו

$$\begin{aligned}(x+y)^3+z^3 &= ((x+y)+z)((x+y)^2-(x+y)z+z^2)\\ &= (x+y)^3\cancel{-(x+y)^2z}+\cancel{(x+y)z^2}+\cancel{z(x+y)^2}\cancel{-(x+y)z^2}+z^3\\ &= (x+y)^3+z^3 \ (\text{טריק "הלא עשיתי כלום"})\end{aligned}$$

ולכן

$$x^3+y^3+z^3-3xyz = (x+y)^3+z^3-3xy(x+y+z) = (x+y+z)((x+y)^2-(x+y)z+z^2-3xy)$$

נסדר את הביטוי הימני

$$(x+y)^2-(x+y)z+z^2-3xy = x^2+2yx+y^2-xz-yz+z^2-3xy = x^2+y^2+z^2-xz-yz-xy$$

בסך־הכל קיבלנו

$$x^3+y^3+z^3-3xyz = (x+y+z)(x^2+y^2+z^2-xz-yz-xy)$$

הגורם $x+y+z$ הוא פולינום אי־פריק ממעלה 1, ונשאר רק להראות שגם $x^2+y^2+z^2-xz-yz-xy$ הוא אי־פריק, נסתכל עליו בעוד דרך

$$\begin{aligned}(x^2+y^2+z^2-xz-yz-xy) &= \frac{1}{2}((x-y)^2+(y-z)^2+(z-x)^2)\\ &= \frac{1}{2}(x^2-2xy+y^2+y^2-2yz+z^2-z^2-2zx+x^2)\\ &= \frac{1}{2}(2x^2-2xy+2y^2-2yz+z^2-2zx)\\ &= x^2+y^2+z^2-xz-yz-xy \ (\text{שוב טריק "הלא עשיתי כלום"})\end{aligned}$$

נבחן מתי הביטוי $(x-y)^2+(y-z)^2+(z-x)^2$ מתאפס: יש לנו סכום של איברים חיובים ולכן הוא מתאפס אם ורק אם כל איבר בסכום מתאפס וזה קורה אם ורק אם $x=y=z=0$.

לכן כל גורם במכפלה לעיל הוא אי־פריק והגענו לביטוי הנדרש. $\square$