

משפט פרובניוס

יהי \mathbb{L} מכיל את \mathbb{R} שדה ממימד n (אם מסתכלים עליו כמרחב לינארי מעל \mathbb{R}) לאו דווקא קומוטטיבי בכפל (ab) לאו דווקא שווה (ba).

\mathbb{L} הוא \mathbb{R} או \mathbb{C} או \mathbb{H} .

הוכחה:

תחילה נקבע $\mathbb{I} = \{z \in \mathbb{L} \mid z^2 \in \mathbb{R}, z^2 \leq 0\}$ כקבוצת המספרים ה'מדומים'.
נשים לב $\mathbb{I} \cap \mathbb{R} = \{0\}$.

נוכיח בשלבים:

(A) א. ברור שלכל $z \in \mathbb{I}$ ו $\alpha \in \mathbb{R}$ מתקיים $\alpha z \in \mathbb{I}$.

ב. אם $z \in \mathbb{I}$ אזי $0 \neq z \in \mathbb{I}$.

$$(z^{-1})^2 = (z^2)^{-1} \leq 0$$

ג. כל מספר x הוא סכום של ממשי ומדומה יחידים.

הוכחה:

נתבונן ב $1, x, x^2, \dots, x^{n+1}$. בגלל שיש יותר מ- n מספרים ברשימה, הם תלויים לינארית מעל \mathbb{R} .

$$a_0 + a_1 x + \dots + a_n x^n = 0$$

יש משפט: כל פולינום עם מקדמים ממשיים מתפרק לגורמים ממעלה קטנה או שווה 2.

$$\alpha \prod (x - \beta_i) \prod (x^2 + a_i x + b_i) = 0$$

לכן, אחד מהגורמים מתאפס.

או ש- $\beta_i = x$, כלומר, x ממשי.

$$x^2 + a_i x + b_i = 0$$

בגלל ש $x^2 + a_i x + b_i$ לא מתפרק לגורמים לינאריים מעל \mathbb{R} , ניתן להציגו כ $(x + c)^2 + d$ כאשר $d > 0$. בגלל ש-

$$(x + c)^2 + d = 0, \text{ מתקיים } (x + c)^2 = -d$$

$c \in \mathbb{R}$. וכאמור $x = z - c$ וסיימנו.

יחידות:

אם, $a + z = a' + z'$ (כאשר a ו a' ממשיים ו z ו z' מדומים). נסמן $(a - a')$ ב c .

$$c + z = z'$$

$$c^2 + 2cz + z^2 = z'^2$$

$$2cz = z'^2 - c^2 - z^2$$

ממשי = מדומה ולכן שניהם 0.

אם $c=0$, אז $a=a'$, ולכן $z = z'$ וקיימת יחידות.

אם $z=0$, אז $c = z' = 0$ וגם במקרה זה קיימת יחידות.

(B) לכל $s, r \in \mathbb{R}, u, v \in \mathbb{I}$

א. $uv + vu \in \mathbb{R}$

ב. $ru + sv \in \mathbb{I}$ (מרחב לינארי מעל \mathbb{R}).

הוכחה:

אם u, v כפולה ממשית זה של זה, שתי הטענות ברורות.

נסמן:

$$\begin{aligned} & uv + vu = a + z \\ & ru + sv = a_0 + z_0 \\ & r^2u^2 + s^2v^2 + rs(uv + vu) = a_0^2 + 2a_0z_0 + z_0^2 \\ & \text{נשווה חלקים מדומים.} \\ & rsz = 2a_0z_0 \end{aligned}$$

אם $z=0$ טענה א. נכונה. כמו כן: או $a_0 = 0$ או $z_0 = 0$

אם $a_0=0$, טענה ב. נכונה.

אם $a_0 \neq 0$ וגם $z_0 = 0$, אז $ru + sv = a_0$

$$ru = a_0 - sv$$

וקיבלנו שתי הצגות שונות שמספר הוא סכום של ממשי ומדומה. סתירה.

אם $z \neq 0$:

אם $a_0 = 0$, טענה ב. נכונה. אחרת $z = z_0 \frac{rs}{2a_0}$ ולכן $ru + sv = a_0 + \frac{rs}{2a_0}z$ משוואה זו נכונה לכל s .

$$ru + s'v = a'_0 + \frac{rs'}{2a'_0}z \text{ נקבל כי } s \neq s'$$

נכפול משוואה עליונה ב $\frac{s'}{a'_0}$. נכפול משוואה תחתונה ב $\frac{s}{a_0}$. נחסר את התוצאות:

$$\left(\frac{s'}{a'_0} - \frac{s}{a_0}\right)ru + \left(\frac{1}{a'_0} - \frac{1}{a_0}\right)ss'v = \frac{s'}{a'_0}a_0 - \frac{s}{a_0}a'_0$$

אם $\left(\frac{1}{a'_0} - \frac{1}{a_0}\right)$ מתאפס, בגלל שונות s, s' , אינו מתאפס. ולהפך. ולכן, בגלל ש- u, v בלתי תלויים לינארית אגף ימין אינו מתאפס.

נעביר אחד משני הגורמים המדומים לאגף ימין ונקבל חוסר יחידות בפירוק ממשי-מדומה. סתירה.

טענה ב. הוכחה. נציב $s=v=1$:

$$u + v \in \mathbb{I}$$

$$v^2 \in \mathbb{R}, u^2 \in \mathbb{R} \implies (u + v)^2 \in \mathbb{R}$$

$$(u + v)^2 - v^2 - u^2 = uv + vu \in \mathbb{R}$$

טענה א. הוכחה.

(C) אם קיימים $u, v, w \in \mathbb{I}$, כך ש $uv = w$, ו $u^2 = v^2 = -1$ אזי,

$$u^2 = v^2 = w^2 = -1 \quad (0)$$

$$uv = -vu = w \quad (1)$$

$$vw = -vw = u \quad (2)$$

$$wu = -wu = v \quad (3)$$

הוכחה:

$$(uv)(vu) = uvvu = -uu = 1$$

$$vu = (uv)^{-1} \in \mathbb{I}$$

$$uv, vu \in \mathbb{I}$$

ולכן $uv+vu \in \mathbb{I}$ ומצד שני, ממשי (טענה B) ב. ו-א).

$$uv+vu=0 \text{ ולכן}$$

$$uv = -vu$$

$$w^2 = uvuv = -vuuv = -1, \text{ ולכן,}$$

הוכחנו (0 ו 1).

אם נוכיח ש $vw = u$, מטעמי סימטריה נוכיח את (2 ו 3).

$$vw = vu\tau = -u\tau v = u$$

וזהו.

לסיכום נברר את מימד \mathbb{I} מעל \mathbb{R} .

אם $\dim \mathbb{I} = 0$, $\mathbb{I} = \mathbb{R}$, בגלל יחידות ההצגה.

אם $\dim \mathbb{I} = 1$, $\mathbb{I} = \mathbb{C}$.

נבחר $i_0 \in \mathbb{I}$.

$$i = \frac{i_0}{\sqrt{-i_0^2}}$$

$$i^2 = \frac{i_0^2}{-i_0^2} = -1$$

בגלל ש $\dim \mathbb{I} = 1$ כל מספר מדומה ניתן להצגה כ ia כאשר a ממשי.

מכאן ואילך \mathbb{I} מתנהג כמו \mathbb{C} .

אם $\dim \mathbb{I} > 1$, נבחר $i_0, z_0 \in \mathbb{I}$, בלתי תלויים לינארית.

$$i = \frac{i_0}{\sqrt{-i_0^2}}$$

$$i^2 = \frac{i_0^2}{-i_0^2} = -1$$

$$iz_0 = z_0 + a \quad (a \in \mathbb{R} \text{ ו } z \in \mathbb{I})$$

$$j_0 = z_0 + ia$$

$j_0 \in \mathbb{I}$, כי הוא סכום של שני מדומים, ו $ij_0 = iz_0 - a = z \in \mathbb{I}$.

$$j = \frac{j_0}{\sqrt{-j_0^2}}$$

$$j^2 = \frac{j_0^2}{-j_0^2} = -1$$

בגלל ש j כפולה ממשית של j_0 נובע ש $ij \in \mathbb{I}$.

נגדיר $ij = k$. שמקיים, יחד עם i, j , את תכונות \mathbb{H} (מחלק \mathbb{C})).

לכן, $\dim \mathbb{I} \geq 3$.

אם $\dim \mathbb{I} = 3$, $\mathbb{I} = \mathbb{H}$.

אחרת, קיים l_0 שהוא l_0 ו i, j, k בת"ל.

$$il_0 = a + x$$

$$x, y, z \in \mathbb{I} \vee a, b, c \in \mathbb{R}$$

$$.jl_0 = b + y$$

$$.kl_0 = c + z$$

$$.l_1 = l_0 + ia + jb + kc \in \mathbb{I} \text{ נסמן}$$

$$il_1 = il_0 - a + kb - jc = x + a - a + kb - jc = x + kb - jc$$

אין מחוברים ממשיים ונותר מספר מדומה.

$$.il_1, jl_1, kl_1 \in \mathbb{I} \text{ ולכן}$$

$$.l = \frac{l_1}{\sqrt{-l_1^2}}$$

, $l^2 = -1$ וכל התכונות הסימטריות בין i, j, k , מתקיימות גם עליו. לכן,

$$kl = -lk = -lij = ilj = -ijl = -kl$$

סתירה!

\mathbb{L} שווה \mathbb{R} או \mathbb{C} או \mathbb{H} .

- כל פולינום עם מקדמים ממשיים מתפרק לגורמים ממקדמים שלמים, ממעלה קטנה או שווה 2. נפרק אותו לגורמים מרוכבים לינאריים. לכל שורש מרוכב קיים גם השורש הצמוד לו. נרשום אותו כך: $\alpha \prod (x - a_i) \prod (x - b_i)(x - \bar{b}_i)$ כאשר a_i הם השורשים השלמים, b_i ו \bar{b}_i הם השורשים המרוכבים.

$$\alpha \prod (x - a_i) \prod (x - b_i)(x - \bar{b}_i) = \alpha \prod (x - a_i) \prod (x^2 - x(b_i + \bar{b}_i) + b_i \bar{b}_i)$$

נשים לב ש $b_i + \bar{b}_i$ ו $b_i \bar{b}_i$ הם ממשיים, והנה הפירוק!