משפט פְרוֹבניוּס

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 $\mathbb{H}$.

<u>הוכחה:</u>

תחילה נקבע $\mathbb{I} = \{z \in \mathbb{L} | z^2 \in \mathbb{R}, z^2 \leq 0\}$ 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 $0 \neq z \in \mathbb{I}$ אזי $z^{-1} \in \mathbb{I}$.
$(z^{-1})^2 = (z^2)^{-1} \leq 0$.
ג. כל מספר x הוא סכום של ממשי ומדומה יחידים.
<u>הוכחה:</u>
נתבונן ב $1, x, x^2 \dots x^{n+1}$. בגלל שיש יותר מ-n מספרים ברשימה, הם תלויים לינארית מעל $\mathbb{R}$.
$a_0 + a_1 x + \dots + a_n x^n = 0$, וזה פולינום עם <u>מקדמים ממשיים</u>!
יש משפט: <u>כל פולינום עם מקדמים ממשיים מתפרק לגורמים ממעלה קטנה או שווה 2</u>.
$\alpha \prod(x - \beta_i) \prod(x^2 + a_i x + b_i) = 0$ כאשר $\alpha, \beta_i, a_i, b_i \in \mathbb{R}$.
לכן, אחד מהגורמים מתאפס.
או ש-$x = \beta_i$, כלומר, x ממשי.
או ש-$x^2 + a_i x + b_i = 0$
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-
$(x + c)^2 + d = 0$, מתקיים $(x + c)^2 = -d$ נסמן $x + c = z$. מכאן נובע ש-$z \in \mathbb{I}$.
$c \in \mathbb{R}$. וכאמור $x = z - c$. וסיימנו.

יחידות:
אם, $a + z = a' + z'$ (כאשר a ו'a ממשיים וz 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. $ru + sv \in \mathbb{I}$ ($\mathbb{I}$ מרחב לינארי מעל $\mathbb{R}$).

<u>הוכחה:</u>

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

נסמן:

$uv + vu = a + z$.

$ru + sv = a_0 + z_0$.

$r^2u^2 + s^2v^2 + rs(uv + vu) = a_0^2 + 2a_0z_0 + z_0^2$.

$\boxed{z, z_0 \in \mathbb{I} \text{ ו } a, a_0 \in \mathbb{R}}$

נשווה חלקים מדומים.

$rsz = 2a_0z_0$.

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 $ru + sv = a_0$,
ואז $ru = a_0 - sv$
וקיבלנו שתי הצגות שונות שמספר הוא סכום של ממשי ומדומה. סתירה.

אם z≠0:

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

יהי $s \neq s'$, נקבל כי $ru + s'v = a_0' + \frac{rs'}{2a_0'}z$.

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', $\left(\frac{s'}{a_0'} - \frac{s}{a_0}\right)$, 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:

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

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

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

טענה א. הוכחה.

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

0) $u^2 = v^2 = w^2 = -1$.

1) $uv = -vu = w$.

2) $vw = -vw = u$.

3) $wu = -wu = v$.

<u>הוכחה:</u>

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

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

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

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

ולכן $uv+vu=0$.

$uv =-vu$.

ולכן, $w^2 = uvuv = -vuuv = -1$.

הוכחנו 0) ו 1).

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

$vw = vuv = -uvv = u$.

וזהו.

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

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

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

נבחר $i_0 \in \mathbb{I}$.

יהי $i = \frac{i_0}{\sqrt{-i_0^2}}$.

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

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

מכאן ואילך $\mathbb{L}$ מתנהג כמו $\mathbb{C}$.

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

יהי $i = \frac{i_0}{\sqrt{-i_0^2}}$.

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

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

נתבונן ב $j_0 = z_0 + ia$.

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

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

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

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 C)).

לכן, $dim\mathbb{I} \geq 3$.

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

אחרת, קיים l_0 שהוא ו i, j, k בת"ל.

$il_0 = a + x$.

$jl_0 = \mathrm{b} + \mathrm{y}$.

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

$kl_0 = \mathrm{c} + \mathrm{z}$.

נסמן $l_1 = l_0 + i\mathrm{a} + j\mathrm{b} + k\mathrm{c} \in \mathbb{I}$.

$$il_1 = il_0 - \mathrm{a} + k\mathrm{b} - j\mathrm{c} = \mathrm{x} + \mathrm{a} - \mathrm{a} + k\mathrm{b} - j\mathrm{c} = \mathrm{x} + k\mathrm{b} - j\mathrm{c}$$

אין מחוברים ממשיים ונותר מספר מדומה.

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

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

$l^2 = -1$, 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 $\mathbb{H}$.

נספח

- 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: $\alpha\prod(x-a_i)\prod(x-b_i)\left(x-\bar{b}_i\right)$ כאשר a_i הם השורשים השלמים, וb_i ו $\bar{b}_i$ הם השורשים המרוכבים.

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

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