Velika Fermaova teorema u $\mathbb{C}[t]$

Sva celobrojna rešenja j-ne $\boxed{x^2+y^2=z^2}$ dobijamo iz "polinomnog rešenja"

$$(t^2-1)^2+(2t)^2=(t^2+1)^2\,,$$ stavljanjem $t\in\mathbb{Q}$

- Posmatrajmo j-nu

$$\boxed{x^p+y^p=z^p}\,,$$ za $\boxed{p\geq 3}$

Ona ima beskonačno mnogo rešenja u $\mathbb{C}^3$ $\left(z=(x^p+y^p)^{\frac{1}{p}}\right)$ a za svako takvo rešenje $(x_0,y_0,z_0)\in\mathbb{C}^3$ imamo i rešenje $(x_0\cdot g(t),\ y_0\cdot g(t),\ z_0\cdot g(t))\in\mathbb{C}[t]^3$, za sve polinome $g(t)$

Takva rešenja ćemo zvati <u>trivijalna</u>. Rešenja koja <u>nisu</u> tog oblika zovemo <u>netrivijalna</u>.

T [Velika Fermaova teorema za polinome] [Liouville, 1851.]
Ne postoji netrivijalno rešenje $(x(t),y(t),z(t))\in\mathbb{C}[t]^3$ j-he $\boxed{x(t)^p+y(t)^p=z(t)^p}$ za $p\geq 3$. (1)

▼ Pretp. da $\exists$ netrivijalno rešenje za $p\geq 3$ u kome su onda $xyz\neq 0$.
Dodatno možemo pp. da x,y,z nemaju zajednički polinomni faktor (inače podelimo tim faktorom).
Dodatno možemo pp. : da su koprosti u parovima.

Diferenciramo (1):

$$p \cdot x^{p-1} \cdot x' + p \cdot y^{p-1} \cdot y' = p \cdot z^{p-1} \cdot z'$$

$$x^{p-1} \cdot x' + y^{p-1} \cdot y' = z^{p-1} \cdot z' \qquad (2)$$

Ideja: posmatrajmo (1)+(2) kao sistem linearnih jednačina sa koef. u $\mathbb{C}[t]$, po "promenljivim x^{p-1}, y^{p-1}, z^{p-1}"

$y' \cdot (1) - y \cdot (2)$: ($yy' - yy' = 0$ uz y^{p-1})

$$x^{p-1}(xy' - yx') = z^{p-1}(zy' - yz')$$

$\mathbb{C}[t]$ ima jedinstvenu faktorizaciju na ireducibilne (proste) faktore (kao i $\mathbb{Z}$), pa iz

$$x^{p-1} \mid z^{p-1}(zy' - yz')$$

i x uzajamno prosto sa z (x i z nemaju zajedničkih ireduc. faktora)

$\rightarrow$

$$x^{p-1} \mid zy' - yz' \qquad (3)$$

- Ako je ovde $zy' - yz' = 0$, onda je $\left(\frac{y}{z}\right)' = 0$ pa bi $y = c \cdot z$ za neku konstantu $c \in \mathbb{C}$, pa bi y i z imali zajedničkih ireducibilnih faktora, što smo već eliminisali.
- Dakle $zy' - yz' \neq 0$ pa iz (3) sledi

$$(p-1) \cdot \deg(x) \leq \deg(zy' - yz') \leq \deg(y) + \deg(z) - 1$$

jer je $\deg(y') = \deg(y) - 1$, $\deg(z') = \deg(z) - 1$.

Dodamo $\deg(x)$ na obe strane:

$$p \cdot \deg(x) < \deg(x) + \deg(y) + \deg(z)$$

Desna strana je simetrična po x, y, z. Ali levu stranu smo tabode mogli da dobijemo analogno i za y i za z tj. važe i nejednakosti:

$$p \cdot \deg(y) < \deg(x) + \deg(y) + \deg(z)$$
$$p \cdot \deg(z) < \deg(x) + \deg(y) + \deg(z)$$

Saberemo sve tri i podelimo sa $\deg(x) + \deg(y) + \deg(z)\ (>0)$:

$p < 3$ ↯

$a + b = c$ u $\mathbb{C}[t]$

Da li prethodno možemo da nekako uopštimo?

Richard Mason (1983): da li u prstenu polinoma možemo da rešimo j-nu:

$$\boxed{a + b = c}$$

Bez smanjenja opštosti, odmah možemo pretp. da su $abc \neq 0$

i da su u a, b, c u parovima kosprosti, tj. da svaka 2 nemaju zajednički ireducibilni faktor.

(Jer, ako imaju 2, imao bi i 3., pa bismo podelili tim ireducibilnim faktorom.)

- Diferenciramo:

$$a' + b' = c'$$

Ideja opet dolazi iz Linearne algebre. Definišimo

$$\Delta(t) := \begin{vmatrix} a(t) & b(t) \\ a'(t) & b'(t) \end{vmatrix}$$

Onda:

$$\Delta(t) = \begin{vmatrix} a(t) & b(t)+a(t) \\ a'(t) & b'(t)+a'(t) \end{vmatrix} = \begin{vmatrix} a(t) & c(t) \\ a'(t) & c'(t) \end{vmatrix} \quad (*)$$

: slično, dodavanjem 2. kolone prvoj:

$$\Delta(t) = \begin{vmatrix} c(t) & b(t) \\ c'(t) & b'(t) \end{vmatrix}$$

- Opet, $\Delta(t) \neq 0$, jer bi u suprotnom $ab' - a'b = 0$, $\left(\frac{a}{b}\right)' = 0$ tj. b bi bio skalarni ($\in \mathbb{C}$) umnožak od a, kontradikcija.

- Osnovna teorema algebre: svi polinomi $\neq 0$ iz $\mathbb{C}[t]$ se faktorišu na linearne faktore.

Tj. svi ireducibilni faktori u $\mathbb{C}[t]$ su linearni polinomi.

• Neka je α koren polinoma $a(t)$ i neka

$(t-\alpha)^e \parallel a(t)$ (najveći stepen $(t-\alpha)$ koji deli $a(t)$)

$\Leftrightarrow$

$a(t) = (t-\alpha)^e \cdot U(t)$, gde $(t-\alpha) \nmid U(t)$

tj. $U(\alpha) \neq 0$.

Onda:

$$a'(t) = e\,(t-\alpha)^{e-1} \cdot U(t) + (t-\alpha)^e \cdot U'(t)$$

$$= (t-\alpha)^{e-1} \cdot V(t)$$

gde je $V(t) = U'(t)(t-\alpha) + e \cdot U(t)$. Odavde vidimo da je

$$NZD\left(t-\alpha, V(t)\right) = NZD\left(t-\alpha, eU(t)\right) = 1,$$ pa je

$(t-\alpha)^{e-1} \parallel a'(t)$

• Onda je:

$$\Delta(t) = a(t)\,b'(t) - a'(t)\,b(t)$$

$$= (t-\alpha)^{e-1} \cdot W(t)$$

gde je

$W(t) := U(t) \cdot (t-\alpha) \cdot b'(t) - V(t) \cdot b(t)$;

$NZD\left(t-\alpha, W(t)\right) = NZD\left(t-\alpha, V(t)\cdot b(t)\right) = 1$

Dakle: (4)

$$(t-\alpha)^{e-1} \parallel \Delta(t) \longrightarrow \boxed{(t-\alpha)^{e} \mid \Delta(t)\cdot(t-\alpha)}$$

Sada $a(t) = c\prod_{\substack{\alpha \text{ prolazi} \\ \text{različitim} \\ \text{korenima od } a(t)}} (t-\alpha)^{e} = c\cdot(t-\alpha_1)^{e_1}(t-\alpha_2)^{e_2}\cdots(t-\alpha_k)^{e_k}$

$\uparrow$ $\mathbb{C}$ $\qquad \alpha_i \neq \alpha_j$, $e_i \geq 1$

Kad pomnožimo relacije (4) za svaki ireducibilni faktor (koren) od $a(t)$ dobijamo:

$$a(t) \mid \Delta(t)\cdot \underbrace{\prod_{a(\alpha)=0}(t-\alpha)}_{(t-\alpha_1)(t-\alpha_2)\cdots(t-\alpha_k)}$$

- Ali, potpuno analognim razmatranjem, dobijamo analogne relacije i za $b(t)$; za $c(t)$, a kako $a(t)$, $b(t)$, $c(t)$ nemaju zajedničke korene (jer su u parovima uzajamno prosti), sledi:

$$\boxed{a(t)\cdot b(t)\cdot c(t) \mid \Delta(t)\cdot \prod_{(abc)(\alpha)=0}(t-\alpha)}$$

$\longrightarrow$

$$\deg(a)+\deg(b)+\deg(c) \leq \deg(\Delta) + \#\{\alpha\in\mathbb{C} : (abc)(\alpha)=0\}$$

(broj)

Sa druge strane, iz 3 različite fle za $\Delta(t)$ iz (*) dobijamo:

$$\deg(\Delta) \leq \begin{cases} \deg(a) + \deg(b) - 1 \\ \deg(a) + \deg(c) - 1 \\ \deg(c) + \deg(b) - 1 \end{cases}$$

Kada ove nejednakosti nadovežemo na prethodnu, dobijamo 3 nejednakosti:

$$\deg(a), \deg(b), \deg(c) < \#\{\alpha \in \mathbb{C} : (abc)(\alpha) = 0\}$$

Dakle dokazali smo:

(T) [abc - teorema za polinome]

Ako $a(t), b(t), c(t) \in \mathbb{C}[t]$ nemaju zajedničke korene i ako čine netrivijalno rešenje j-ne

$$\boxed{a(t) + b(t) = c(t)},$$

onda je

$$\max\{\deg(a), \deg(b), \deg(c)\} < \#\text{ različitih korena } a(t)\cdot b(t)\cdot c(t) = 0.$$

Primedba Ova ocena je najbolja (najoštrija) moguća. Npr.

$$\underbrace{(2t)^2}_{a(t)} + \underbrace{(t^2-1)^2}_{b(t)} = \underbrace{(t^2+1)^2}_{c(t)}$$

Različiti korijeni od $a(t) \cdot b(t) \cdot c(t)$ su $0, 1, -1, i, -i$ tj. $\#=5$, a $\deg(c) = \deg(b) = 4$, $\deg(a) = 2$. ◿