VILNIAUS UNIVERSITETAS
MATEMATIKOS IR INFORMATIKOS FAKULTETAS
MATEMATIKOS INSTITUTAS

Lukas Maciulevičius

Apie dviejų algebrinių skaičių sandaugos laipsnį

On the Degree of Product of two Algebraic Numbers

Magistro baigiamasis darbas

Leidžiu ginti .....
Darbo vadovas prof. Paulius Drungilas

Vilnius 2020

Turinys

Įvadas

Skaičius $\alpha \in \mathbb{C}$ vadinamas *algebriniu*, jei jis yra kokio nors nenulinio polinomo su racionaliais koeficientais šaknis. Mažiausio laipsnio normuotas [1] polinomas $p(x) \in \mathbb{Q}[x]$, turintis šaknį α, vadinamas algebrinio skaičiaus α *minimaliuoju polinomu*, o jo laipsnis vadinamas algebrinio skaičiaus α *laipsniu*.

Trejetas $(a, b, c) \in \mathbb{N}^3$ vadinamas *S-trejetu* (atitinkamai *P-trejetu*), jei egzistuoja trys algebriniai skaičiai α, β ir γ, kurių laipsniai atitinkamai a, b ir c, tokie, kad $\alpha + \beta + \gamma = 0$ (atitinkamai $\alpha\beta\gamma = 1$).

Straipsnyje [4] Drungilas, Dubickas ir Smyth iškėlė uždavinį rasti visus S-trejetus $(a, b, c) \in \mathbb{N}^3$. Minėtame straipsnyje taip pat iškeltas panašus uždavinys apie skaičių kūnus. Priminsime, jog kiekvienas kūnas $K \subseteq \mathbb{C}$ savyje turi pokūnį $\mathbb{Q}$, todėl į kūną K galime žiūrėti kaip į tiesinę erdvę virš kūno $\mathbb{Q}$.[2] Kūno K, kaip tiesinės erdvės virš kūno $\mathbb{Q}$, dimensija vadinama šio kūno *laipsniu* ir žymima $[K : \mathbb{Q}]$. Jei $[K : \mathbb{Q}] < \infty$, tai K vadinamas *skaičių kūnu*. Tuo tarpu kūnų K ir L *kompozitu* vadinamas mažiausias kūnas KL, toks, kad $K \subseteq KL$ ir $L \subseteq KL$. Trejetas $(a, b, c) \in \mathbb{N}^3$ vadinamas *C-trejetu*, jeigu egzistuoja skaičių kūnai K ir L, kurių laipsniai atitinkamai a ir b, tokie, kad kompozito KL laipsnis lygus c.

Straipsnyje [4] Drungilas, Dubickas ir Smyth nustatė visus (išskyrus vieną) S-trejetus (a, b, c), kuriuose $a \leqslant b \leqslant c$ ir $b \leqslant 6$ (neišnagrinėtas liko trejetas $(6, 6, 8)$), taip pat nustatė visus C-trejetus (a, b, c), kuriuose $a \leqslant b \leqslant c$ ir $b \leqslant 6$. Straipsnyje [3] Drungilas, Dubickas ir Luca įrodė, jog $(6, 6, 8)$ nėra S-trejetas, taip pat pratęsė S-trejetų ir C-trejetų (a, b, c), $a \leqslant b \leqslant c$, charakterizaciją iki atvejo, kai $b \leqslant 7$.

1 teiginys ([4])**.** *Jeigu $(a, b, c) \in \mathbb{N}^3$ yra C-trejetas, tai jis yra ir S-trejetas, ir P-trejetas.*

2 teorema ([2])**.** *Jei (a, b, c) yra S-trejetas, tai jis yra ir P-trejetas.*

Taigi visi [4] ir [3] straipsniuose nustatyti S-trejetai kartu yra ir P-trejetai. Tačiau šie trejetai dar neišsemia *visų* P-trejetų (a, b, c), kuriuose $a \leqslant b \leqslant c$ ir $b \leqslant 7$.

Šiame darbe nagrinėjamus klausimus galima suskirstyti į dvi dalis.

[1] Kurio vyriausias koeficientas lygus 1.

[2] Tikrai, kūnas K yra uždaras elementų sudėties bei daugybos iš kūno $\mathbb{Q}$ elementų atžvilgiu, be to, šios dvi operacijos tenkina visus tiesinės erdvės apibrėžimo reikalavimus.

P-trejetų charakterizacija Šiame darbe nagrinėjami P-trejetai (a, b, c), tenkinantys sąlygas $a \leqslant b \leqslant c$ ir $b \leqslant 7$, t.y. įrodomas toks teiginys:

3 teorema. *P-trejetai (a, b, c), tenkinantys sąlygas $a \leqslant b \leqslant c$ ir $b \leqslant 7$, pateikti 1 lentelėje, išskyrus galbūt kai kuriuos iš apvestų trejetų.*

$b\backslash a$	1	2	3	4	5	6	7
1	1						
2	2	2, 4					
3	3	3, 6	3, 6, 9				
4	4	4, 8	6, 12	4, 6, 8, 12, 16			
5	5	10	15	5, (10), 20	5, 10, 20, 25		
6	6	6, 12	6, 9, 12, 18	6, (8), 12, 24	(10), (15), 30	6, 8, 9, 12, 15, 18, 24, 30, 36	
7	7	14	21	(7), (14), 28	35	7, (14), (21), 42	7, 14, 21, 28, 42, 49

1 lentelė: Visi P-trejetai (a, b, c), $b \leqslant 7$, galbūt išskyrus apvestus trejetus

Taip pat pavyko gauti keletą teiginių apie specialaus pavidalo trejetus:

4 teorema. *Trejetas $(n-1, n, n)$, $n \geqslant 2$, yra P-trejetas tada ir tik tada, kai n - pirminis.*

5 teorema. [3] *Trejetas (p, t, t), kur p - pirminis ir $t \geqslant p > 2$, yra P-trejetas tada ir tik tada, kai $p|t$.*

Neredukuojami C-trejetai Straipsnyje [4] iškelta hipotezė:

6 hipotezė (Dalinis variantas [4, Conjecture 4])**.** *Jei (a, b, c), $(a', b', c') \in \mathbb{N}^3$ yra C-trejetai, tai (aa', bb', cc') taip pat yra C-trejetas.*

Straipsnyje [2] įrodyta, jog ši hipotezė teisinga, jei atsakymas į taip vadinamą *Atvirkštinį Galua Teorijos Uždavinį* yra teigiamas. *Atvirkštinis Galua Teorijos Uždavinys* klausia, ar kiekviena baigtinė grupė yra kokio nors normaliojo kūnų plėtinio $K : \mathbb{Q}$ Galua grupė (žr. [6]).

7 teiginys ([2, Theorem 1.3])**.** *Jei kiekviena baigtinė grupė yra tam tikro kūno $\mathbb{Q}$ normaliojo plėtinio Galua grupė, tai 6 hipotezė yra teisinga.*

[3] Šis teiginys apibendrina 12 lemą.

Šią teoremą galima performuluoti tokiu būdu. Įveskime žymėjimą:

$$(a, b, c)(a', b', c') := (aa',\ bb',\ cc'), \tag{1}$$

čia $a, b, c, a', b', c' \in \mathbb{N}$. Kalbant kitais žodžiais, 7 teorema sako: jei atsakymas į *Atvirkštinį Galua Teorijos Uždavinį* yra teigiamas, tai visų C-trejetų aibė (1) lygybe apibrėžtos daugybos atžvilgiu sudaro pusgrupę. Natūralu klausti, kurie šios pusgrupės elementai yra „neredukuojami“.

8 apibrėžimas. C-trejetą (A, B, C) vadinsime neredukuojamu, jeigu jo negalima užrašyti pavidalu

$$(A, B, C) = (a, b, c)(a', b', c'),$$

kur (a, b, c), (a', b', c') yra C-trejetai ir $(a, b, c) \neq (1, 1, 1)$ bei $(a', b', c') \neq (1, 1, 1)$.

Šiame darbe įrodyta, jog tam tikri specialaus pavidalo C-trejetai yra neredukuojami:

9 teorema. *C-trejetai* $(n, n, n(n-1))$, $n \geqslant 2$, *yra neredukuojami.*[4]

[4]Žinoma, jog $(n, n, n(n-1))$ iš tiesų yra C-trejetas su visais natūraliaisiais skaičiais $n \geqslant 2$ (žr. [4, Proposition 29, (ii)]).

1 skyrius

Pagalbiniai rezultatai

10 lema ([4, Lemma 14]). *Jeigu (a, b, c) yra P-trejetas, tai $c | \operatorname{mbk}(a, b) \cdot t$ su tam tikru $t \leqslant \operatorname{dbd}(a, b)$.*

11 lema ([5, Lemma 7]). *Tarkime natūralieji skaičiai $a \leqslant b \leqslant c$ tenkina nelygybę $ab < 2c$. Jei trejetas (a, b, c) nėra C-trejetas, tai jis nėra ir P-trejetas.*

12 lema ([4, Theorem 8]). *Trejetas $(2, t, t) \in \mathbb{N}^3$ yra P-trejetas tada ir tik tada, kai $2|t$ arba $3|t$.*

Tarkime p yra pirminis skaičius. Laipsnio rodiklį, kuriuo p įeina į skaičiaus n kanoninį išskaidymą pirminiais dauginamaisiais, pažymėkim $\operatorname{ord}_p(n)$ (jeigu n nesidalija iš p, tai susitarkim, jog $\operatorname{ord}_p(n) = 0$). Sakysime, jog trejetas $(a, b, c) \in \mathbb{N}^3$ *tenkina eksponentinę trikampio nelygybę pirminio skaičiaus p atžvilgiu*, jeigu

$$\operatorname{ord}_p(a) + \operatorname{ord}_p(b) \geqslant \operatorname{ord}_p(c),\ \operatorname{ord}_p(a) + \operatorname{ord}_p(c) \geqslant \operatorname{ord}_p(b) \text{ ir}$$
$$\operatorname{ord}_p(b) + \operatorname{ord}_p(c) \geqslant \operatorname{ord}_p(a).$$

13 lema ([4, Proposition 28]). *Tarkime trejetas $(a, b, c) \in \mathbb{N}^3$ tenkina eksponentinę trikampio nelygybę kiekvieno pirminio skaičiaus atžvilgiu. Tuomet kiekvienam P-trejetui $(a', b', c') \in \mathbb{N}^3$ trejetas (aa', bb', cc') taip pat yra P-trejetas.*

14 lema ([4, Proposition 21]). *Tarkime α ir β yra atitinkamai m - tojo ir n - tojo laipsnio algebriniai skaičiai virš kūno $\mathbb{Q}$. Tegul $\alpha_1 := \alpha, \alpha_2, \ldots, \alpha_m$ yra visi skirtingi skaičiaus α algebriniai jungtiniai, o $\beta_1 := \beta, \beta_2, \ldots, \beta_n$ - visi skirtingi β algebriniai jungtiniai. Jeigu β laipsnis virš kūno $\mathbb{Q}(\alpha)$ lygus n, tai visi skaičiai $\alpha_i\beta_j$, $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant n$, yra algebriniai jungtiniai virš $\mathbb{Q}$ (kai kurie gali ir kartotis).*

Tegul $\alpha_1, \alpha_2, \ldots, \alpha_n$ yra visos separabilaus n-tojo laipsnio polinomo $f(x) \in \mathbb{Q}[x]$ šaknys, $n \geqslant 2$. *Multiplikatyviuoju sąryšiu* tarp šaknų $\alpha_1, \ldots, \alpha_n$ vadiname sąryšį, pavidalo

$$\prod_{i=1}^{n} \alpha_i^{k_i} \in \mathbb{Q},$$

kur $k_i \in \mathbb{Z}$. Multiplikatyvųjį sąryšį vadinsime trivialiuoju, jei $k_1 = k_2 = \cdots = k_n$.

15 lema ([1, Theorem 1]). *Tarkime $f(x) \in \mathbb{Q}[x]$ yra neredukuojamas virš $\mathbb{Q}$ pirminio laipsnio $p > 2$ polinomas, be to $f(x) \neq x^p + a_0$. Tuomet neegzistuoja netrivialaus multiplikatyviojo sąryšio tarp $f(x)$ šaknų $\alpha_1, \alpha_2, \ldots, \alpha_p$.*

2 skyrius

Įrodymai

3 teoremos įrodymas. Ieškosime P-trejetų (a, b, c), tenkinančių sąlygas $a \leqslant b \leqslant c$ ir $b \leqslant 7$. Remdamiesi 10 lema, atrenkame visus kandidatus (visi jie surašyti 2 lentelėje):

$b\backslash a$	1	2	3	4	5	6	7
1	1						
2	2	2, 4					
3	3	3, 6	3, 6, 9				
4	4	4, 8	4, 6, 12	4, 6, 8, 12, 16			
5	5	5, 10	5, 15	5, (10), 20	5, 10, 15, 20, 25		
6	6	6, 12	6, 9, 12, 18	6, (8), 12, 24	6, (10), (15), 30	6, 8, 9, 10, 12, 15, 18, 24, 30, 36	
7	7	7, 14	7, 21	(7), (14), 28	7, 35	7, (14), (21), 42	7, 14, 21, 28, 35, 42, 49

2 lentelė: Kandidatai į P-trejetus

Šioje lentelėje laikomės tokių žymėjimų:

- Mėlynai pažymėti trejetai yra S-trejetai ir daugiau S-trejetų šioje lentelėje nėra (straipsniuose [3] ir [4] įrodyta, jog tai iš tiesų yra visi S-trejetai (a, b, c), tenkinantys sąlygą $b \leqslant 7$). Taigi, remiantis 2 teiginiu, visi šie trejetai kartu yra ir P-trejetai.
- Žaliai pažymėti trejetai irgi yra P-trejetai: $(2, 3, 3)$ yra P-trejetas pagal 12 lemą, trejetai $(3, 6, 9)$ ir $(3, 4, 6)$ - pagal 13 lemą, $(4, 5, 5)$ ir $(6, 7, 7)$ - pagal 4 teiginį, o $(6, 6, 8)$ - pagal [4, Remark 39].

- Raudonai pažymėti trejetai nėra P-trejetai: $(3,4,4)$, $(5,6,6)$, $(3,7,7)$, $(5,7,7)$ - pagal 5 teiginį, $(2,5,5)$ ir $(2,7,7)$ - pagal 12 lemą, $(3,5,5)$ ir $(6,6,10)$ - atitinkamai pagal 17 ir 16 teiginius, o $(5,5,15)$ ir $(7,7,35)$ - pagal 11 lemą.

- Apvesti trejetai dar neištirti.

□

16 teiginys. *Trejetas* $(6,6,10)$ *nėra P-trejetas.*

Įrodymas. Teoremos [4, Theorem 38] įrodymą nesunku performuluoti multiplikatyviajam atvejui (vietoje α ir β algebrinių jungtinių skaičių sumų nagrinėjant jų sandaugas). Naudodami tuos pačius žymėjimus galiausiai gausim, jog $\beta_6^6 \in \mathbb{Q}$, vadinasi β minimalusis polinomas yra pavidalo $x^6 - r_2$, $r_2 \in \mathbb{Q}$. Teoremos [4, Theorem 38] įrodyme α ir β sukeitę vietomis, gausim, jog α minimalus polinomas taip pat yra pavidalo $x^6 - r_1$, $r_1 \in \mathbb{Q}$. Taigi $\alpha = \sqrt[6]{r_1}\varepsilon_6$ ir $\beta = \sqrt[6]{r_2}\varepsilon_6'$, kur ε_6 ir ε_6' yra tam tikros 6-tojo laipsnio šaknys iš vieneto. Tuomet skaičius $\alpha\beta = \sqrt[6]{r_1 r_2}\varepsilon_6\varepsilon_6'$ yra polinomo $x^6 - r_1 r_2$ šaknis, vadinasi $\deg(\alpha\beta) \leqslant 6$, o tai yra prieštara. □

4 teoremos įrodymas. Tarkime n - pirminis. Tegul $\zeta_n = e^{\frac{2\pi i}{n}}$. Tuomet ζ_n, o kartu ir $\frac{1}{\zeta_n}$, yra $(n-1)$-ojo laipsnio algebriniai skaičiai[1]. Imkime $\alpha = \frac{1}{\zeta_n}$, $\beta = \sqrt[n]{2}\zeta_n$ ir $\gamma = \frac{1}{\sqrt[n]{2}}$. Tuomet $\alpha\beta\gamma = 1$, taigi trejetas $(n-1, n, n)$, kur n - pirminis, yra P-trejetas.

Įrodysime į priešingą pusę. Tarkime $(n-1, n, n)$ yra P-trejetas. Tuomet egzistuoja tokie algebriniai skaičiai α ir β, kad $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n-1$, $[\mathbb{Q}(\beta) : \mathbb{Q}] = n$ ir $[\mathbb{Q}(\alpha\beta) : \mathbb{Q}] = n$. Kadangi $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\alpha, \beta)$ ir $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha, \beta)$, tai abu skaičiai $n-1$ ir n dalija skaičių $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$, be to $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] \leqslant (n-1)n$. Kadangi $\operatorname{dbd}(n, n-1) = 1$, tai $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = (n-1)n$. Tuomet $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] = n$ ir $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\beta)] = n-1$.

Tarkime $\beta_1 := \beta, \beta_2, \ldots, \beta_n$ - visi skaičiaus β algebriniai jungtiniai. Visi skaičiai

$$\alpha\beta_1, \alpha\beta_2, \ldots, \alpha\beta_n \tag{2.1}$$

yra paporiui skirtingi. Kadangi algebrinio skaičiaus $\alpha\beta$ laipsnis lygus n, tai, remiantis 14 teiginiu, skaičiai (2.1) yra visi $\alpha\beta$ algebriniai jungtiniai. Taigi visų (2.1) skaičių sandauga $\alpha^n\beta_1\beta_2\cdots\beta_n$ yra nenulinis racionalusis skaičius. Tačiau taip pat $\beta_1\beta_2\ldots\beta_n \in \mathbb{Q} \setminus \{0\}$, taigi $\alpha^n \in \mathbb{Q} \setminus \{0\}$. Pažymėkim $\alpha^n := r$.

Tegul α minimalusis polinomas yra

$$x^{n-1} + r_{n-2}x^{n-2} + \cdots + r_1 x + r_0,\ r_i \in \mathbb{Q},\ i = 0, 1, \ldots, n-2.$$

[1]Prisiminkime, jog skaičiaus $\zeta_n = e^{\frac{2\pi i}{n}}$ minimalusis polinomas vadinamas *n-tuoju ciklotominiu polinomu*. Gerai žinoma, jog n-tojo ciklotominio polinomo laipsnis lygus $\varphi(n)$, kur φ žymi Oilerio funkciją. Be to $(\zeta_n)^m \neq 1$ su kiekvienu natūraliuoju $m < n$. (žr. [7]).

Jeigu $\alpha \neq 0$ yra k-tojo laipsnio algebrinis skaičius, tai $\frac{1}{\alpha}$ taip pat yra k-tojo laipsnio algebrinis skaičius.

Lygybės $\alpha^{n-1} + r_{n-2}\alpha^{n-2} + \cdots + r_1\alpha + r_0 = 0$ abi puses daugindami iš α ir naudodamiesi pažymėjimu $\alpha^n = r$, gauname

$$r_{n-2}\alpha^{n-1} + r_{n-3}\alpha^{n-2} + \cdots + r_0\alpha + r = 0 \Rightarrow$$
$$\alpha^{n-1} + \frac{r_{n-3}}{r_{n-2}}\alpha^{n-2} + \cdots + \frac{r_0}{r_{n-2}}\alpha + \frac{r}{r_{n-2}} = 0$$

(kadangi $r \neq 0$, tai ir $r_{n-2} \neq 0$, priešingu atveju α būtų žemesnio nei $(n-1)$-ojo laipsnio algebrinis skaičius). Kadangi kiekvienam algebriniam skaičiui egzistuoja vienintelis minimalusis polinomas, tai

$$\frac{r_{n-3}}{r_{n-2}} = r_{n-2},\ \frac{r_{n-4}}{r_{n-2}} = r_{n-3},\ \ldots\ \frac{r_0}{r_{n-2}} = r_1,\ \frac{r}{r_{n-2}} = r_0.$$

Iš šių lygybių gauname, jog $r = r_{n-2}^n$. Taigi $\alpha^n = r_{n-2}^n \Rightarrow \alpha = r_{n-2}\zeta_n$, kur ζ_n yra n-tojo laipsnio šaknis iš vieneto. Jeigu ζ_n nėra primityvioji n-tojo laipsnio šaknis iš vieneto, tai α yra mažesnio nei $(n-1)$-ojo laipsnio algebrinis skaičius, - prieštara. Taigi ζ_n yra primityvioji šaknis. Vadinasi α laipsnis lygus n-tojo ciklotominio polinomo laipsniui, t.y. $\phi(n) = n-1$. Tačiau ši lygybė teisinga tada ir tik tada, kai n - pirminis. Įrodymas baigtas. □

5 teoremos įrodymas. Tarkime $t \geqslant p > 2$ ir $p|t$, t.y. $t = pk$, kur $k \in \mathbb{N}$. Trejetas $(1, k, k)$ yra P-trejetas $\forall k \in \mathbb{N}$, o trejetas (p, p, p) tenkina eksponentinę trikampio nelygybę. Taigi trejetas $(p, t, t) = (p \cdot 1, p \cdot k, p \cdot k)$ yra P-trejetas pagal 13 lemą.

Teiginį įrodysime į kitą pusę. Tarkime (p, t, t) yra P-trejetas. Sakykime priešingai, jog $p \nmid t$. Tuomet egzistuoja tokie algebriniai skaičiai α ir β, kad $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p$ ir $[\mathbb{Q}(\beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha\beta) : \mathbb{Q}] = t$. Kadangi pagal prielaidą $p \nmid t$, tai galime įsitikinti, jog $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] = t$ ir $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\beta)] = p$, todėl, remiantis 14 lema, skaičiai $\alpha_i\beta_j$, $1 \leqslant i \leqslant p$, $1 \leqslant j \leqslant t$, yra visi skaičiaus $\alpha\beta$ algebriniai jungtiniai (su pasikartojimais). Iš viso $\alpha\beta$ turi t algebrinių jungtinių (įskaitant patį skaičių $\alpha\beta$). Visi skaičiai $\alpha\beta_1, \alpha\beta_2, \ldots, \alpha\beta_t$ yra skirtingi, taigi jie išsemia visus $\alpha\beta$ algebrinius jungtinius. Todėl

$$(\alpha\beta_1)(\alpha\beta_2)\cdots(\alpha\beta_t) = \alpha^t(\beta_1\beta_2\cdots\beta_t) \in \mathbb{Q} \Rightarrow \alpha^t \in \mathbb{Q},$$

tačiau α yra pirminio laipsnio algebrinis skaičius, todėl, pagal 15 lemą, α minimalusis polinomas yra pavidalo $x^p - c$, $c \in \mathbb{Q}$ (atkreipkim dėmesį, jog mūsų nagrinėjamu atveju $p > 2$, kaip ir reikalaujama 15 lemoje).

Turime, jog α yra polinomo $x^t - r$ šaknis, kur $r \in \mathbb{Q}$. Taigi α minimalusis polinomas $x^p - c$ dalija polinomą $x^t - r$. Vadinasi kiekviena polinomo $x^p - c$ šaknis yra ir polinomo $x^t - r$ šaknis. Tame tarpe $\sqrt[p]{c}\zeta_p$ yra polinomo $x^t - r$ šaknis; čia $\sqrt[p]{c}$ yra aritmetinė p-tojo laipsnio šaknis iš c, o $\zeta_p = e^{\frac{2\pi i}{p}}$. Taigi

$$(\sqrt[p]{c})^t\zeta_p^t = r \in \mathbb{R} \Rightarrow \zeta_p^t \in \mathbb{R} \Rightarrow \sin\left(\frac{2\pi t}{p}\right) = 0 \Rightarrow \frac{2\pi t}{p} = \pi k,\ k \in \mathbb{Z} \Rightarrow 2t = pk.$$

Vadinasi $2t$ dalijasi iš pirminio skaičiaus p. Pagal prielaidą $p \nmid t$, todėl $p|2$, tačiau $p > 2$. Tokiu būdu gauname prieštarą. Taigi $p|t$. □

17 teiginys. *Trejetas* $(3,5,5)$ *nėra P-trejetas.*

Pastaba. Šis teiginys išplaukia iš 5 teoremos. Vis dėlto čia pateiksime dar vieną jo įrodymą.

Įrodymas. Tarkime priešingai. Tuomet egzistuoja tokie algebriniai skaičiai α ir β, kad $[\mathbb{Q}(\alpha):\mathbb{Q}]=3$, $[\mathbb{Q}(\beta):\mathbb{Q}]=5$ ir $[\mathbb{Q}(\alpha\beta):\mathbb{Q}]=5$. Pažymėkime $\alpha_1:=\alpha$, α_2, α_3 - visi skirtingi α algebriniai jungtiniai, o $\beta_1:=\beta,\beta_2,\beta_3,\beta_4,\beta_5$ - visi β algebriniai jungtiniai. Analogiškai, kaip anksčiau, įsitikiname, kad $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}(\alpha)]=5$ ir $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}(\beta)]=3$. Taigi, remiantis 14 teiginiu, visi skaičiai $\alpha_i\beta_j$, $1\leqslant i\leqslant 3$, $1\leqslant j\leqslant 5$, yra algebriniai jungtiniai. Skaičiai $\alpha\beta_1,\alpha\beta_2,\alpha\beta_3,\alpha\beta_4,\alpha\beta_5$ yra paporiui skirtingi, taigi jie yra *visi* skaičiaus $\alpha\beta$ algebriniai jungtiniai. Jų visų sandauga $\alpha^5(\beta_1\beta_2\beta_3\beta_4\beta_5)$ yra racionalusis skaičius, tačiau $\beta_1\beta_2\beta_3\beta_4\beta_5\neq 0$ taip pat yra racionalusis skaičius, taigi $\alpha^5:=r\in\mathbb{Q}$.

Tegul skaičiaus α minimalusis polinomas yra $x^3+r_2x^2+r_1x+r_0$. Lygybės $\alpha^3+r_2\alpha^2+r_1\alpha+r_0=0$ abi puses padauginę iš α^2 gauname $r_2\alpha^4+r_1\alpha^3+r_0\alpha^2+r=0$, taigi nenulinis (nes $r\neq 0$) polinomas $r_2x^4+r_1x^3+r_0x^2+r$ dalijasi iš α minimaliojo polinomo $x^3+r_2x^2+r_1x+r_0$. Turime, kad

$$\begin{aligned}r_2x^4+r_1x^3+r_0x^2+r=&(x^3+r_2x^2+r_1x+r_0)(r_2x+(r_1-r_2^2))\\&+((r_0-2r_1r_2+r_2^3)x^2+(r_1r_2^2-r_0r_2-r_1^2)x+(r+r_0r_2^2-r_0r_1)),\end{aligned}$$

vadinasi

$$\begin{cases}r_0-2r_1r_2+r_2^3=0\\r_1r_2^2-r_0r_2-r_1^2=0\\r-r_0r_1+r_0r_2^2=0\end{cases}. \tag{2.2}$$

Iš pirmosios lygybės išreiškę r_0 ir įstatę į antrąją lygybę, gauname $r_2^4-r_1r_2^2-r_1^2=0$. Iš čia gauname, kad $r_2^2=\frac{1}{2}(r_1+r_1\sqrt{5})$, tačiau r_2^2 yra racionalusis skaičius, todėl $r_1=0$. Tuomet $r_2=0$ ir iš (2.2) lygybių gauname, kad $r=0$, o tai prieštara. □

9 teoremos įrodymas. Tarkime priešingai, jog

$$(n,n,n(n-1))=(a_1,b_1,c_1)(a_2,b_2,c_2), \tag{2.3}$$

kur (a_1,b_1,c_1) ir (a_2,b_2,c_2) yra C-trejetai, be to $(a_1,b_1,c_1)\neq(1,1,1)$ ir $(a_2,b_2,c_2)\neq(1,1,1)$.

Skaičius c_1 ir c_2 galime užrašyti pavidalu $c_1=d_1^{(n)}d_1^{(n-1)}$ ir $c_2=d_2^{(n)}d_2^{(n-1)}$, kur

- $d_i^{(n)}|n$ ir $d_i^{(n-1)}|n-1$ $(i=1,2)$,
- $d_1^{(n)}d_2^{(n)}=n$ ir $d_1^{(n-1)}d_2^{(n-1)}=n-1$.

Kadangi pagal mūsų prielaidą (a_1,b_1,c_1) yra C-trejetas, tai a_1 dalija skaičių $c_1=d_1^{(n)}d_1^{(n-1)}$, tačiau $\operatorname{dbd}(a_1,d_1^{(n-1)})=1$, todėl $a_1|d_1^{(n)}$[2]. Analogiškai, $a_2|d_2^{(n)}$.

[2]Turime, jog $a_1|n$ ir $d_1^{(n-1)}|n-1$. Kadangi $\operatorname{dbd}(n,n-1)=1$, tai ir $\operatorname{dbd}(a_i,d_i^{(n-1)})=1$.

Prisiminkim, jog $a_1a_2 = n$. Jeigu $a_1 < d_1^{(n)}$, tai

$$d_1^{(n)}d_2^{(n)} = n = a_1a_2 < d_1^{(n)}a_2 \Rightarrow d_2^{(n)} < a_2,$$

todėl $a_2 \nmid d_2^{(n)}$, - prieštara. Vadinasi $a_1 = d_1^{(n)}$ ir $a_2 = d_2^{(n)}$.

Analogiškai gauname, jog $b_1 = d_1^{(n)}$ ir $b_2 = d_2^{(n)}$. Taigi, praleisdami viršutinius indeksus (n), o vietoje $(n-1)$ rašydami $'$, išraišką (2.3) galime perrašyti taip:

$$(n, n, n(n-1)) = (d_1, d_1, d_1d_1')(d_2, d_2, d_2d_2').$$

Turime, jog $d_1' < d_1$ arba $d_2' < d_2$. Tikrai,

- $\mathrm{dbd}(d_1', d_1) = \mathrm{dbd}(d_2', d_2) = 1$ ir skaičiai d_1, d_2, d_1' bei d_2' nėra visi kartu lygūs 1, todėl $d_1' \neq d_1$ ir $d_2' \neq d_2$;
- jei $d_1' > d_1$ ir $d_2' > d_2$, tai $n(n-1) = c_1c_2 = d_1d_1'd_2d_2' > (d_1d_2)^2 = n^2$, - prieštara.

Nemažindami bendrumo tarkime, jog $d_1' < d_1$, t.y. $d_1' \leqslant d_1 - 1$. Tada

$$d_2d_2' = \frac{n}{d_1} \cdot \frac{n-1}{d_1'} \geqslant \frac{n}{d_1} \cdot \frac{n-1}{d_1 - 1} > \left(\frac{n}{d_1}\right)^2 = d_2^2,$$

nes $d_1 < n$. Tačiau nelygybė $d_2d_2' > d_2^2$ prieštarauja tam, kad (d_2, d_2, d_2d_2') yra C-trejetas, nes kiekvienam C-trejetui (a, b, c) teisinga nelygybė $c \leqslant ab$.

Vadinasi mūsų pradinė prielaida neteisinga ir trejetas $(n, n, n(n-1))$ yra neredukuojamas. □

On the Degree of Product of two Algebraic Numbers

Summary

The triplet (a, b, c) of positive integers is said to be product-feasible if there exist algebraic numbers α, β and γ of degrees (over $\mathbb{Q}$) a, b and c, respectively, such that $\alpha\beta\gamma = 1$. This work extends the investigation of product-feasible triplets started by Drungilas, Dubickas and Smyth. More precisely, for all but eight positive integer triplets (a, b, c) with $a \leqslant b \leqslant c$ and $b \leqslant 7$, we decide whether it is product-feasible. Moreover, a result related to reducibilty of so called compositum-feasible triplets is obtained. The triplet (a, b, c) of positive integers is said to be compositum-feasible if there exist number fields K and L of degree a and b respectively such that the degree of the compositum KL equals c. We have showed that triplets of the form $(n, n, n(n-1))$, $n \geqslant 2$, cannot be written as $(n, n, n(n-1)) = (aa', bb', cc')$, where (a, b, c) and (a', b', c') are compositum-feasible triplets both different from $(1, 1, 1)$.

Literatūra

[1] Michael Drmota and Mariusz Skał ba. “On multiplicative and linear independence of polynomial roots”. In: *Contributions to general algebra, 7 (Vienna, 1990)*. Hölder-Pichler-Tempsky, Vienna, 1991, pp. 127–135.

[2] Paulius Drungilas and Artūras Dubickas. “On degrees of three algebraic numbers with zero sum or unit product”. In: *Colloq. Math.* 143.2 (2016), pp. 159–167.

[3] Paulius Drungilas, Artūras Dubickas, and Florian Luca. “On the degree of compositum of two number fields”. In: *Math. Nachr.* 286.2-3 (2013), pp. 171–180.

[4] Paulius Drungilas, Artūras Dubickas, and Chris Smyth. “A degree problem for two algebraic numbers and their sum”. In: *Publ. Mat.* 56.2 (2012), pp. 413–448.

[5] Paulius Drungilas and Lukas Maciulevičius. “A degree problem for the compositum of two number fields”. In: *Lith. Math. J.* 59.1 (2019), pp. 39–47.

[6] Christian U. Jensen, Arne Ledet, and Noriko Yui. *Generic polynomials*. Vol. 45. Mathematical Sciences Research Institute Publications. Constructive aspects of the inverse Galois problem. Cambridge University Press, Cambridge, 2002, pp. x+258.

[7] Daniel A. Marcus. *Number fields*. Universitext. Springer-Verlag, New York-Heidelberg, 1977, pp. viii+279.