**VILNIAUS UNIVERSITETAS**
MATEMATIKOS IR INFORMATIKOS FAKULTETAS
TIKIMYBIŲ TEORIJOS IR SKAIČIŲ TEORIJOS KATEDRA

**Paulius Virbalas**

# Apie dviejų algebrinių skaičių, kurių laipsniai $p+1$, sumos ir sandaugos laipsnius

## A Degree Problem for two Algebraic Numbers of Degree p+1 for Their Product and Sum

Magistro baigiamasis darbas

Leidžiu ginti ......................................

Darbo vadovas prof. habil. dr. Artūras Dubickas

Vilnius 2020

# Turinys

# 1 skyrius

# Įvadas

Skaičius $\alpha \in \mathbb{C}$ vadinamas *algebriniu skaičiumi*, jei jis yra kokio nors nenulinio polinomo su racionaliaisiais koeficientais šaknis. Mažiausio laipsnio normuotas polinomas $p(x) \in \mathbb{Q}[x]$, kurio šaknis yra $\alpha$, vadinamas algebrinio skaičiaus $\alpha$ *minimaliuoju polinomu*, o jo laipsnis vadinamas algebrinio skaičiaus $\alpha$ *laipsniu* ir žymimas $\deg(\alpha)$.

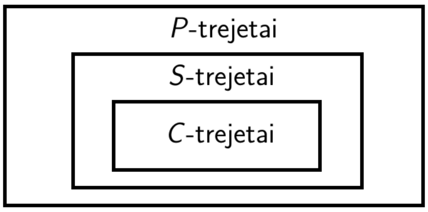
Drungilas, Dubickas ir Smyth 2012 metų straipsnyje [4] iškėlė uždavinį rasti visus trejetus $(a, b, c) \in \mathbb{N}^3$, kuriems egzistuoja trys algebriniai skaičiai $\alpha, \beta, \gamma$, kurių laipsniai atitinkamai $a, b, c$, tokie, kad $\alpha + \beta + \gamma = 0$. Kitų autorių šis klausimas taip pat suformuluotas „mathoverflow" virtualiame matematikos forume 2010 metais tokia forma: nustatyti galimas skaičiaus $\alpha + \beta$ laipsnio reikšmes, jei algebrinių skaičių $\alpha$ ir $\beta$ laipsniai atitinkamai lygūs $a$ ir $b$ [`http://mathoverflow.net/questions/30151/`].

Trejetas $(a, b, c) \in \mathbb{N}^3, a \leqslant b \leqslant c$, vadinamas $S$*-trejetu* (atitinkamai $P$*-trejetu*), jei egzistuoja trys algebriniai skaičiai $\alpha, \beta, \gamma$, kurių laipsniai atitinkamai $a, b$ ir $c$, tokie, kad $\alpha + \beta + \gamma = 0$ (atitinkamai $\alpha\beta\gamma = 1$). Skaičių trejetas $(a, b, c) \in \mathbb{N}^3, a \leqslant b \leqslant c$, vadinamas $C$*-trejetu*, jei egzistuoja skaičių kūnai $K$ ir $L$, kurių laipsniai atitinkamai $a$ ir $b$, tokie, kad kūnų $K$ ir $L$ kompozito $KL$ laipsnis lygus $c$, čia kompozitu $KL$ žymimas mažiausias toks kūnas $KL$, kad $K \subseteq KL$ ir $L \subseteq KL$.

Straipsnyje [4] bei jo tęsiniuose [3],[2],[5] buvo suformuluoti sąryšiai tarp $P$-trejetų, $S$-trejetų ir $C$-trejetų. Jei trejetas yra $C$-trejetas, tai jis yra ir $S$-trejetas, ir $P$- trejetas [4, Teiginys 1]. Atvirkštinis teiginys nėra teisingas. Pagal [4, Teiginys 29,(ii)] trejetas $(4, 4, 6)$ yra $S$-trejetas, bet nėra $C$-trejetas. Drungilas, Dubickas ir Luca [3] įrodė, jog kiekvienas $S$-trejetas yra ir $P$-trejetas. Atvirkštinis teiginys vėlgi nėra teisingas. Tegu:

$$\alpha = (-1 - i\sqrt{3})/4, \quad \beta = \sqrt[3]{2}, \quad \gamma = (-1 + i\sqrt{3})/\sqrt[3]{2}.$$

Skaičių $\alpha, \beta, \gamma$ laipsniai atitinkamai lygūs $2, 3, 3$. Be to, $\alpha\beta\gamma = 1$. Vadinasi, trejetas $(2, 3, 3)$ yra $P$-trejetas, tačiau pagal [4, Teorema 5] $(2, 3, 3)$ nėra $S$-trejetas. Aptarti sąryšiai tarp $C$-trejetų, $S$-trejetų ir $P$-trejetų iliustruoti 1.1 pav.




1.1 pav.: Sąryšiai tarp $C$-trejetų, $S$-trejetų ir $P$-trejetų

Iš pastarųjų teiginių seka, jog jei trejetas $(a, b, c)$ nėra $P$-trejetas, tai jis nėra nei $S$-trejetas, nei $C$-trejetas. Iki šio baigiamojo magistro darbo rašymo datos yra rasti visi $C$-trejetai $(a, b, c)$, kuriuose $b \leqslant 9$ [4],[3],[5] bei visi $S$-trejetai $(a, b, c)$, kuriuose $b \leqslant 7$ [4],[3].

Drungilas, Dubickas ir Smyth [4, Teorema 38] nustatė, jog trejetas $(6, 6, 10)$ nėra $S$-trejetas. Pagrindinis baigiamojo magistro darbo „Uždavinys apie dviejų algebrinių skaičių sandaugos laipsnį“ tikslas apibendrinti įrodymo metodą, kurį taikant buvo nustatyta, jog trejetas $(6, 6, 10)$ nėra $S$-trejetas. Gautas rezultatas suformuluotas teoremoje.

**1 teorema.** *Tegu $k$ - teigiamas sveikasis, o $p$ - pirminis. Tuomet:*

*(i) Jei $\frac{p+1}{k} = 1$, tai trejetas $(p+1, p+1, kp)$ yra $C$-trejetas, $S$-trejetas ir $P$-trejetas.*

*(ii) Jei $\frac{p+1}{k} = 2$, tai trejetas $(p+1, p+1, kp)$ yra $S$-trejetas ir $P$-trejetas, bet nėra $C$-trejetas.*

*(iii) Jei $\frac{p+1}{k} \notin \{1, 2\}$, tai trejetas $(p+1, p+1, kp)$ nėra nei $P$-trejetas, nei $S$-trejetas, nei $C$-trejetas.*

Pavyzdžiui, kai $p = 5, k = 2$ turime, jog $\frac{p+1}{k} = \frac{5+1}{2} = 3$. Vadinasi, pagal teoremos $(iii)$ dalį trejetas $(6, 6, 10)$ nėra $P$-trejetas. Tuomet $(6, 6, 10)$ nėra nei $S$-trejetas, nei $C$-trejetas. Tolimesniame skyriuje pateikiamas 1 teoremos įrodymas.

# 2 skyrius

# Teoremos įrodymas

Teoremos dalys $(i)$ ir $(ii)$ išplaukia tiesiogiai iš [4, Teiginys 29]. Pagrindinis šio baigiamojo magistro darbo rezultatas suformuluotas $(iii)$ dalyje.

$(i)$ $\frac{p+1}{k} = 1$, tad $p+1 = k$. Pagal [4, Teiginys 29,(i)] trejetas $(n, n, n(n-1))$ yra $C$-trejetas. Paėmę $n = p+1$ gauname, jog $(p+1, p+1, kp)$ yra $C$-trejetas, $S$-trejetas ir $P$-trejetas.

$(ii)$ $\frac{p+1}{k} = 2$, tad $\frac{p+1}{2} = k$. Vadinasi, $(p+1)$ - lyginis. Kai $n$ - lyginis, trejetas $(n, n, \frac{n(n-1)}{2})$ yra $S$-trejetas, bet nėra $C$-trejetas [4, Teiginys 29,(ii)]. Paėmę $n = p+1$ gauname, jog $(p+1, p+1, kp)$ yra $S$-trejetas ir $P$-trejetas, bet nėra $C$-trejetas.

$(iii)$ Tarkime, jog egzistuoja toks $k$, kad $\frac{p+1}{k} \notin \{1, 2\}$ ir trejetas $(p+1, p+1, kp)$ yra $P$-trejetas, t.y. galima rasti tokius tris algebrinius skaičius $\alpha, \beta, \gamma$, jog $\alpha\beta\gamma = 1$ ir $\alpha, \beta, \gamma$ laipsniai atitinkamai lygūs $p+1, p+1, kp$. Kadangi $\mathbb{Q}(\alpha\beta) \subseteq \mathbb{Q}(\alpha, \beta)$ ir $\mathbb{Q}(\alpha\beta) = \mathbb{Q}(\gamma^{-1}) = \mathbb{Q}(\gamma)$, tai $\mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\alpha, \beta)$. Vadinasi, $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$ dalijasi iš $kp$. Taip pat turime, jog $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\alpha, \beta)$, tad $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$ dalijasi ir iš $p+1$. Tegu $\mathrm{DBD}(x, y)$ ir $\mathrm{MBK}(x, y)$ žymi dviejų natūraliųjų skaičių $x$ ir $y$ atitinkamai didžiausią bendrą daliklį ir mažiausią bendrą kartotinį. Iš pastarųjų teiginių išplaukia, jog $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$ dalijasi iš $\mathrm{MBK}(kp, p+1)$. Tarkime, jog $\mathrm{DBD}(kp, p+1) = d$. Tuomet $\mathrm{DBD}(k, p+1) = d$ ir todėl $\frac{k}{d} \in \mathbb{N}$. Be to, $\mathrm{MBK}(kp, p+1) = \frac{kp(p+1)}{d}$. Taigi turime

$$\frac{kp(p+1)}{d} \leqslant [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]. \tag{2.1}$$

Kita vertus

$$[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] \leqslant [\mathbb{Q}(\alpha):\mathbb{Q}]\cdot[\mathbb{Q}(\beta):\mathbb{Q}] = (p+1)(p+1). \tag{2.2}$$

Apjungus (2.1) ir (2.2) gauname, jog $\frac{kp(p+1)}{d} \leqslant (p+1)(p+1)$ arba $\frac{kp}{d} \leqslant (p+1)$. Akivaizdu, jog tuomet $\frac{k}{d} = 1$. Vadinasi, $\mathrm{DBD}(p+1, kp) = k$ ir

$$\frac{p+1}{k} \in \mathbb{N}. \tag{2.3}$$

Be to, $\mathrm{MBK}(kp, p+1) = p(p+1)$, tad $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] \,\vdots\, p(p+1)$. Tačiau $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] \leqslant (p+1)(p+1)$, todėl $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] = p(p+1)$. Gautus rezultatus iliustruoja diagrama (2.4).

$$\begin{tikzcd}
 & \mathbb{Q}(\alpha) \arrow[dr, dash, "p"] & \\
\mathbb{Q} \arrow[ur, dash, "p+1"] \arrow[r, dash, "kp"] \arrow[dr, dash, "p+1"'] & \mathbb{Q}(\gamma) \arrow[r, dash, "\frac{p+1}{k}"] & \mathbb{Q}(\alpha,\beta) \\
 & \mathbb{Q}(\beta) \arrow[ur, dash, "p"'] &
\end{tikzcd} \tag{2.4}$$

Iš diagramos matome, kad skaičiaus $\beta$ laipsnis virš $\mathbb{Q}(\alpha)$ lygus $p$. Vadinasi, vienas skaičiaus $\beta$ algebrinis jungtinis priklauso kūnui $\mathbb{Q}(\alpha)$. Neprarasdami bendrumo tarkime, jog tai $\beta_1$. Tuomet egzistuoja toks polinomas $f(x) \in \mathbb{Q}[x]$, kad

$$\beta_1 = f(\alpha). \tag{2.5}$$

Tegu $\beta_1, \beta_2, ..., \beta_{p+1}$ žymi visus skaičiaus $\beta$ algebrinius jungtinius virš $\mathbb{Q}$. Imkime $\mathbb{Q}(\alpha,\beta)/\mathbb{Q}$ normaliojo uždarinio Galua grupės automorfizmą $\sigma_j$, kuris perveda $\beta_1$ į $\beta_j$. Paveikę juo lygybę (2.5) gauname, kad

$$\beta_j = f(\alpha_j) \tag{2.6}$$

su kiekvienu $j = 1, 2, ..., p+1$, čia $\alpha_1 = \alpha, \alpha_2, ..., \alpha_{p+1}$ - skaičiaus $\alpha$ algebriniai jungtiniai. Nesiaurindami bendrumo laikykime, jog $\beta = \beta_2 = f(\alpha_2)$. Tuomet $\gamma^{-1} = \alpha_1\beta_2 = \alpha_1 \cdot f(\alpha_2)$ ir $\mathbb{Q}(\gamma) = \mathbb{Q}(\gamma^{-1}) = \mathbb{Q}(\alpha_1 \cdot f(\alpha_2))$. Be to, $\mathbb{Q}(\beta_2) = \mathbb{Q}(f(\alpha_2)) \subseteq \mathbb{Q}(\alpha_2)$. Tačiau $[\mathbb{Q}(\beta_2):\mathbb{Q}] = [\mathbb{Q}(\alpha_2):\mathbb{Q}] = p+1$. Vadinasi, $\mathbb{Q}(\beta_2) = \mathbb{Q}(\alpha_2)$. Gautus rezultatus iliustruoja diagrama (2.7).

$$
\begin{tikzcd}
 & \mathbb{Q}(\alpha_1) \arrow[dr, dash, "p"] & \\
\mathbb{Q} \arrow[ur, dash, "p+1"] \arrow[r, dash, "kp"] \arrow[dr, dash, "p+1"'] & \mathbb{Q}(\alpha_1 \cdot f(\alpha_2)) \arrow[r, dash, "\frac{p+1}{k}"] & \mathbb{Q}(\alpha_1, \alpha_2) \\
 & \mathbb{Q}(\alpha_2) \arrow[ur, dash, "p"'] &
\end{tikzcd}
\tag{2.7}
$$

Analogiškai gauname, jog $\mathbb{Q}(\beta_j) = \mathbb{Q}(f(\alpha_j)) = \mathbb{Q}(\alpha_j)$ visiems $j \in \{1, 2, ..., p+1\}$. Parodysime, jog tuomet bet kurio $\alpha_i$ laipsnis virš $\mathbb{Q}(\alpha_j)$ lygus $p$ su visais $j \in \{1, 2, ..., p+1\} \setminus \{i\}$. Fiksuokime $j \in \{2, 3, ..., p+1\}$. Kadangi $\alpha_2$ laipsnis virš $\mathbb{Q}(\alpha_1)$ lygus $p$ (žr. diagramą (2.7)), tai $\alpha_j$ ir $\alpha_2$ yra algebriniai jungtiniai virš $\mathbb{Q}(\alpha_1)$. Vadinasi, $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$ normaliojo uždarinio Galua grupėje galime rasti automorfizmą $\sigma$ tokį, kad $\sigma(\alpha_2) = \alpha_j$ ir $\sigma(\alpha_1) = \alpha_1$. Tuomet turime, jog $\sigma(\gamma^{-1}) = \sigma(\alpha_1 \cdot f(\alpha_2)) = \alpha_1 \cdot f(\alpha_j)$. Taigi $\alpha_1 \cdot f(\alpha_j)$ yra skaičiaus $\gamma^{-1}$ algebrinis jungtinis, todėl jo laipsnis virš $\mathbb{Q}$ lygus $kp$. Gautus rezultatus iliustruoja diagrama (2.8).

$$
\begin{tikzcd}
 & \mathbb{Q}(\alpha_1) \arrow[dr, dash, "p"] & \\
\mathbb{Q} \arrow[ur, dash, "p+1"] \arrow[r, dash, "kp"] \arrow[dr, dash, "p+1"'] & \mathbb{Q}(\alpha_1 \cdot f(\alpha_j)) \arrow[r, dash, "\frac{p+1}{k}"] & \mathbb{Q}(\alpha_1, \alpha_j) \\
 & \mathbb{Q}(\alpha_j) \arrow[ur, dash, "p"'] &
\end{tikzcd}
\tag{2.8}
$$

Pastebėkime, jog skaičiaus $\alpha_1$ laipsnis virš $\mathbb{Q}(\alpha_j)$ lygus $p^r$, todėl visi skaičiai $\{\alpha_1, \alpha_2, \alpha_3, ..., \alpha_{p+1}\} \setminus \{\alpha_j\}$ yra skaičiaus $\alpha_1$ algebriniai jungtiniai virš $\mathbb{Q}(\alpha_j)$. Vadinasi, bet kurio $\alpha_i$ laipsnis virš $\mathbb{Q}(\alpha_j)$ lygus $p$ su visais $i \in \{1, 2, ..., p+1\} \setminus \{j\}$. Taigi visi skaičiai $\alpha_i \cdot f(\alpha_j)$, kai $i \neq j$, yra algebriniai jungtiniai virš $\mathbb{Q}$. Nagrinėkime iš jų tuos, kurių indeksams galioja $i < j$ (žr. (2.9)).

$$
\begin{aligned}
\alpha_1 \cdot f(\alpha_2) \\
\alpha_1 \cdot f(\alpha_3)\ , \alpha_2 \cdot f(\alpha_3) \\
\alpha_1 \cdot f(\alpha_4)\ , \alpha_2 \cdot f(\alpha_4)\ , \alpha_3 \cdot f(\alpha_4) \\
... \\
\alpha_1 \cdot f(\alpha_{p+1})\ , \alpha_2 \cdot f(\alpha_{p+1})\ , ..., \alpha_p \cdot f(\alpha_{p+1}).
\end{aligned}
\tag{2.9}
$$

Pagal tokį pasirinkimą turime $\frac{p(p+1)}{2}$ skaičiaus $\gamma^{-1} = \alpha_1 \cdot f(\alpha_2)$ algebrinių jungtinių virš $\mathbb{Q}$. Skaičiaus $\gamma^{-1}$ laipsnis virš $\mathbb{Q}$ lygus $kp$. Pagal teoremos prielaidą $\frac{p+1}{k} \notin \{1, 2\}$, be to $\frac{p+1}{k} \in \mathbb{N}$ (2.3). Vadinasi, $\frac{p+1}{k} > 2$ ir iš čia $\frac{p(p+1)}{2} > kp$, todėl kažkurie du algebriniai jungtiniai iš (2.9) yra lygūs, t.y.:

$$\alpha_a \cdot f(\alpha_b) = \alpha_c \cdot f(\alpha_t) \tag{2.10}$$

su tam tikrais $a < b, c < t$ ir $a \neq c$ arba $b \neq t$. Tačiau pastebėkime, jog jei $b = t$, tai $\alpha_a = \alpha_c$, ir tuomet $a = c$, prieštara. Analogiškai, jei $a = c$, tai $f(\alpha_b) = f(\alpha_t)$, ir tuomet $\beta_b = \beta_t$, tad $b = t$, prieštara. Vadinasi, $a \neq c$ ir $b \neq t$. Nesiaurindami bendrumo laikykime, jog $a < c$. Tuomet $a < c < t$ ir $t \notin \{a, b, c\}$.

Nagrinėkime $\mathbb{Q}(\alpha_1)/\mathbb{Q}$ normaliojo uždarinio Galua grupę $G$, veikiančią kaip $S_{p+1}$ pogrupis indeksų $\{1, 2, ..., p + 1\}$ atžvilgiu, t.y., jei $\sigma \in G$, tai $\sigma(\alpha_j) = \alpha_{\sigma(j)}$, čia $j = 1, 2, ..., p+1$. Diagramoje (2.7) matome, jog $[\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}] = p(p+1)$. Kadangi $\mathbb{Q}(\alpha_1, \alpha_2) \subseteq G$, tai grupės $G$ eilė dalijasi iš $p$. Pagal Koši teoremą [1, Teorema 15.1], grupėje $G$ egzistuoja elementas $\tau$, kurio eilė lygi $p$. Vadinasi, $\tau$ turi būti $p$-ciklas (jo išskaidymas nepriklausomų ciklų sandauga negali susidėti iš daugiau nei vieno ciklo). Taigi, $\tau = (i_1\ i_2 ...\ i_p)$ su skirtingais skaičiais $i_1, i_2, ..., i_p \in \{1, 2, ..., p + 1\}$. Nesiaurindami bendrumo laikykime, jog $p + 1 \notin \{i_1\ , i_2\ , ..., i_p\}$. Tuomet $\tau(\alpha_{p+1}) = \alpha_{p+1}$. Parinkime $\sigma \in G$ tokį, kuris perveda $\alpha_t$ į $\alpha_{p+1}$. Paveikę juo lygybę 2.10, gauname

$$\alpha_i \cdot f(\alpha_j) = \alpha_k \cdot f(\alpha_{p+1}) \tag{2.11}$$

čia $i, j, k \in \{1, 2, ..., p\}$. Elementu $\tau$ paveikę lygybę (2.11) gauname

$$\begin{aligned} \alpha_{\tau(i)} \cdot f(\alpha_{\tau(j)}) &= \alpha_{\tau(k)} \cdot f(\alpha_{p+1}) \\ \alpha_{\tau^2(i)} \cdot f(\alpha_{\tau^2(j)}) &= \alpha_{\tau^2(k)} \cdot f(\alpha_{p+1}) \\ &\cdots \\ \alpha_{\tau^{p-1}(i)} \cdot f(\alpha_{\tau^{p-1}(j)}) &= \alpha_{\tau^{p-1}(k)} \cdot f(\alpha_{p+1}). \end{aligned} \tag{2.12}$$

Elemento $\tau \in S_{p+1}$ orbita, kuriai priklauso aibės $\{1, 2, ..., p+1\}$ elementas $l$, vadinama aibė, sudaryta iš elementų $l, \tau(l), \tau^2(l), ..., \tau^r(l)$, čia $r$ - toks mažiausias teigiamas sveikasis skaičius, kad $\tau^r(l) = l$. Žymime $orb_l(\tau) = \{l, \tau(l), \tau^2(l), ..., \tau^r(l)\}$.

Nagrinėkime šias elemento $\tau$ orbitas:

$$orb_i(\tau) = \{i, \quad \tau(i), \quad \tau^2(i), ..., \quad \tau^{p-1}(i)\}$$

$$orb_j(\tau) = \{j, \quad \tau(j), \quad \tau^2(j), ..., \quad \tau^{p-1}(j)\}$$

$$orb_k(\tau) = \{k, \quad \tau(k), \quad \tau^2(k), ..., \quad \tau^{p-1}(k)\}$$

Kadangi $\{i, j, k\} \in \{i_1, i_2, ..., i_p\}$, tai $orb_i(\tau) = orb_j(\tau) = orb_k(\tau) = \{1, 2, ..., p\}$. Vadinasi, sudauginę 2.11 ir visas $p-1$ lygybes iš 2.12 turime:

$$\prod_{i=1}^{p} \alpha_i \cdot \prod_{i=1}^{p} f(\alpha_i) = \prod_{i=1}^{p} \alpha_i \cdot (f(\alpha_{p+1}))^p \tag{2.13}$$

Remiantis 2.6 ir 2.13 turime:

$$(\beta_{p+1})^{p+1} = (f(\alpha_{p+1}))^{p+1} = f(\alpha_1) \cdot f(\alpha_2) \cdot ... \cdot f(\alpha_{p+1}) = \beta_1 \cdot \beta_2 \cdot ... \cdot \beta_{p+1} \in \mathbb{Q}$$

Vadinasi, $(\beta_{p+1})^{p+1} \in \mathbb{Q}$. Tegu $(\beta_{p+1})^{p+1} = u$. Tuomet $\beta_{p+1}$ yra polinomo $f(x) = x^{p+1} - u$ šaknis. Normuoto polinomo $f(x)$ laipsnis lygus $p+1$, todėl $f(x)$ - skaičiaus $\beta$ minimalusis polinomas virš $\mathbb{Q}$ ir $u = \beta^{p+1}$.

Kadangi skaičių $\alpha$ ir $\beta$ laipsniai virš $\mathbb{Q}$ lygūs, tai uždavinys apie dviejų skaičių sandaugos laipsnį yra simetriškas $\alpha$ ir $\beta$ atžvilgiu. Tad analogiškai gauname, jog $\alpha$ minimalusis polinomas virš $\mathbb{Q}$ yra $g(x) = x^{p+1} - v$, čia $v = \alpha^{p+1}$.

Turime, jog $(\alpha\beta)^{p+1} = uv$, tad $(\alpha\beta)^{p+1} \in \mathbb{Q}$. Vadinasi, $(p+1) \vdots \deg(\alpha\beta)$. Tačiau $\deg(\alpha\beta) = \deg(\gamma^{-1}) = \deg(\gamma) = kp$, tad $(p+1) \vdots kp$, prieštara. Vadinasi, jei $\frac{p+1}{k} \notin \{1, 2\}$, tai trejetas $(p+1, p+1, kp)$ nėra $P$-trejetas. Iš to seka, jog jis nėra nei $S$-trejetas, nei $C$-trejetas.

# A Degree Problem for two Algebraic Numbers of Degree $p+1$ for Their Product and Sum

Summary

The triplet $(a, b, c) \in \mathbb{N}^3$ is said to be *product-feasible* (resp. *sum-feasible*) if there exist three algebraic numbers $\alpha, \beta, \gamma$ of degrees $a, b, c$ such that $\alpha\beta\gamma = 1$ (resp. $\alpha + \beta + \gamma = 0$). In this work it is shown that for all positive integers $k$ and every prime $p$ such that $\frac{p+1}{k} \notin \{1, 2\}$, the triplet $(p+1, p+1, kp)$ is not product-feasible and consequently not sum-feasible. This theorem generalizes Theorem 38 of [2], where Drungilas, Dubickas and Smyth established that the triplet $(6, 6, 10)$ is not sum-feasible.

# Literatūra


[1] R.A. Beezer, T.W. Judson, *Abstract Algebra*, Orthogonal Publishing L3C, Michigan, 2015.

[2] P. Drungilas, A. Dubickas, *On degrees of three algebraic numbers with zero sum or unit product,* Colloq. Math. **143(2)** (2016), 159–167.

[3] P. Drungilas, A. Dubickas, F. Luca, *On the degree of compositum of two number fields,* Math. Nachr. **286(2-3)** (2013), 171–180.

[4] P. Drungilas, A. Dubickas, C. Smyth, *A degree problem for two algebraic numbers and their sum,* Publ. Mat. **46** (2012), 571–585.

[5] P. Drungilas, L. Maciulevičius, *A degree problem for the compositum of two number fields,* Lith. Math. J. **59(1)** (2019), 39–47.