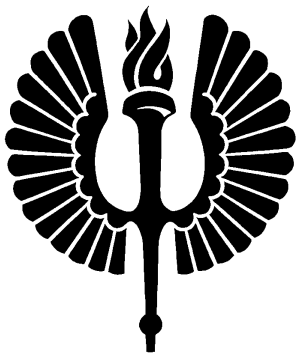


SHIRSHOVIN LAUSE PI-ALGEBROISSA

Mikko Huikuri

Pro gradu -tutkielma

Syyskuu 2013

MATEMATIIKAN JA TILASTOTIETEEN LAITOS

TURUN YLIOPISTO

TURUN YLIOPISTO
Matematiikan ja tilastotieteen laitos

HUIKURI MIKKO: Shirshovin lause PI-algebroissa
Pro gradu -tutkielma, 50 s.
Matematiikka
Syyskuu 2013

Tässä työssä esitetään venäläisen matemaatikon A.I. Shirshovin teorioita ja tuloksia sanojen kombinatoriikasta. Lisäksi näytetään miten ne soveltuvat PI-algebrojen maailmaan.

Shirshovin tuloksia tarkasteltaessa käsitellään sanoja erillisinä kombinatorisina objekteina ja todistetaan Shirshovin Lemma, joka on tämän työn perusta. Lemman mukaan tarpeeksi pitkille sanoille saadaan tiettyä säännönmukaisuutta ja se todistetaan kolme kertaa. Ensimmäisestä saadaan tarpeeksi pitkän sanan olemassaolo. Toinen todistus mukailee Shirshovin alkuperäistä todistusta. Kolmannessa todistuksessa annetaan tarpeeksi pitkälle sanalle paremmin käytäntöön soveltuva raja.

Tämän jälkeen käsitellään sanoja algebrallisina objekteina. Työn päätuloksena todistetaan Shirshovin Korkeuslause, jonka mukaan jokainen äärellisesti generoidun PI-algebran alkio on sanojen $\omega_1^{k_1} \cdots \omega_d^{k_d}$ lineaarikombinaatio, missä sanojen ω_i pituudet sekä indeksi i ovat rajatut.

Shirshovin Korkeuslauseesta seuraa suoraan positiivinen ratkaisu Kurochin ongelmaan PI-algebroilla sekä saadaan raja alkioiden lukumäärälle, jolla algebra generoituu moduliksi. Lisäksi esitetään toisena sovelluksena ilman todistuksia Shirshovin soveltuvuus Jacobsonin radikaalin nilpotenttisuuteen.

Pääsääntöisenä lähteenä käytetään A. Kanel-Belowin ja L. H. Rowenin kirjaa: Computational aspects of polynomial identities.

Asiasanat: Algebra, PI, Shirshov, Sanojen kombinatoriikka, Affiini algebra, Kuroch, Radikaali, Multilinearisointi, ω-sana, monomi, moduli

Sisältö

1 Johdanto

Matematiikassa *sana* tarkoittaa tietystä annetusta joukosta muodostettujen kirjaimien tai symbolien jonoa. Sanat voidaan ajatella äärellisinä tai äärettöminä symbolijonoina, lisäksi sanoja voidaan käsitellä erillisinä kombinatorisina objekteina –esimerkiksi bittisarja– tai algebrallisina ei-kommutatiivisina objekteina –esimerkiksi polynomin yksittäisen summan tekijän muuttujajono.

Polynomi-identiteetti -algebralla –lyhyesti *PI-algebralla*– tarkoitetaan sitä, että annetun joukon alkiot toteuttavat ei-kommutatiivisen polynomi-identiteetin; toisin sanoen on olemassa sellainen polynomi, kutsutaan myös *identiteetiksi*, joka häviää identtisesti kaikilla annetun joukon alkioilla. Identiteetti on *polynomi-identiteetti (PI)*, jos ainakin yksi sen kertoimista on ± 1. Esimerkiksi joukko A on kommutatiivinen tarkalleen silloin, kun $ab - ba = 0$ kaikilla joukon A alkioilla a ja b. Tällöin polynomi $xy - yx$ on joukon A identiteetti. Näin ollen polynomi-identiteetit yleistävät kommutatiivisuuden.

PI-teoria tuli ensimmäisen kerran esille Dehnin [3], [12] tutkimuksissa. Dehnin tarkoituksena oli kuvata Desarguian tasojen leikkauksien teoriaa polynomisessa muodossa jakoalgebran D suhteen. Amitsur täydensi Dehnin työtä [3], [13] kehittämällä rationaalisten identiteettien teorioita. Näin PI-teorian idea oli lähtenyt liikkeelle. Wagner esitti [2] tärkeän yhteyden matriisien ja polynomi-identiteettien välille todistamalla, että jokainen matriisialgebra yli kunnan toteuttaa PI:n.

PI-teorialla on vahva yhteys äärellisulotteiselle esitysteorialle, koska algebran esitys on homomorfismi kuvaus matriisialgebralle. Kuroch esitti 1940-luvulla Burnsiden ongelmaa vastaavan kysymyksen algebroille: *onko jokaisella äärellisesti generoidulla algebralla, yli kunnan, aina äärellinen dimensio*? Golod ja Shafarevich [23], [24] esittivät Kurochin ongelmalle vastaesimer-

kin: äärellisesti generoitu nil-algebra, jolla on ääretön dimensio. Matematiikassa ongelmaa ei kuitenkaan aina nähdä vain yksittäisenä ongelmana, joka pitää ratkaista, vaan myös suuntana uusille tutkimuksille. Ennen Golod ja Shafarevichin vastaesimerkkiä Kurochin ongelma antoi suunnan uusille tutkimuksille PI-teorian puolella. Kaplansky todisti [20] Kurochin ongelman todeksi PI-algebroilla kunnan K suhteen. Kaplansky käytti hyväkseen Levitskyn todistamaa tulosta [18], jonka mukaan äärellisesti generoitu algebra on niin sanotusti *nilpotentti*, jos jokainen tämän algebran alkio on nilpotentti. Kaplanskyn todistus perustuu renkaiden rakenneteoriaan, eikä todistus juurikaan käytä polynomi-identiteettien ominaisuuksia hyväksi.

A.I. Shirshov näki Kurochin ongelman hieman eri valossa ja keksi käyttää kombinatorista lähystymistapaa. Ongelman ratkaisu seuraa nimittäin suoraan *Shirshovin Korkeuslauseesta*, jonka mukaan jokainen äärellisesti generoidun PI-algebran alkio on sanojen $\omega_1^{k_1} \cdots \omega_d^{k_d}$ lineaarikombinaatio, missä sanojen ω_i pituudet sekä indeksi d ovat rajatut. Päinvastoin kuin Kaplanskyn todistuksessa, Shirshov ei käyttänyt rakenneteorian tuloksia lainkaan. Shirshov käytti todistuksessaan myös hyvin vähän alkion kokonaisuuden ominaisuutta. Korkeuslauseesta seuraa myös riittävä ehto Kurochin –sekä myös Levitskyn– ongelman tarkasteluun: algebrassa täytyy olla vain äärellinen määrä kokonaisia alkioita –vastaavasti myös nilpotentteja alkioita. Lisäksi Korkeuslause toteutuu algebroilla yli kommutatiivisen renkaan.

Tämän työn päätarkoituksena on esittää kombinatorisia teorioita Shirshovin Korkeuslauseen taustalla, todistaa Shirshovin Korkeuslause sekä soveltaa näitä Kurochin ongelmaan. Lisäksi työssä esitetään Razmyslov-Kemer-Braunin -lause ilman todistuksia. Lauseen mukaan niin sanottu *Jacobsonin radikaali* on nilpotentti äärellisesti generoidun PI-algerban suhteen – Shirshovin teorioiden avulla tämä toteutuu kaikilla karakteristikoilla. Tässä

työssä käytetään pääsääntöisenä lähteenä A. Kanel-Belowin ja L. H. Rowenin kirjaa [3], jossa on koottu yhteen hajallaan esiintyviä tuloksia ja teorioita PI-algebroista.

Työn ensimmäisessä osassa esitetään sanat diskreetteinä kombinatorisina objekteina ja annetaan pohja Shirshovin teorioille. Shirshovin Korkeuslauseen todistus perustuu *Shirshovin Lemmaan*, joka todistetaan ensimmäisen luvun lopussa. Lemman mukaan tarpeeksi pitkille sanoille saadaan tiettyä säännönmukaisuutta; sanat ovat joko jaksollisia tai tietyssä mielessä maksimaalisia. Työssä annetaan Shirshovin Lemmalle kolme eri todistusta. Ensimmäinen todistus on pelkästään kombinatorinen ja todistaa ainoastaan ”tarpeeksi pitkän” sanan olemassa olon. Toinen todistus tehdään kaksoisinduktiolla [3] ja se mukailee pääsääntöisesti Shirshovin alkuperäistä todistusta. Johtuen kaksoisinduktiosta ”tarpeeksi pitkästä” sanasta tulee kuitenkin ”liian” pitkä eikä sillä ole käytännön sovelluksissa juurikaan hyötyä [3]. Kolmannessa todistuksessa rajoitetaan sanan pituutta käytännössä paremmin toimivaksi.

Toisessa osassa käsitellään sanoja algebrallisina ei-kommutatiivisina objekteina ja todistetaan Shirshovin Korkeuslause. Tässä osassa määritellään tarkemmin PI-algebra sekä yhdistetään sanojen kombinatorinen voima polynomeihin; toisin sanoen ajatellaan polynomien yksittäisiä monomeita sanoina, jolloin sanojen ominaisuuksia voidaan käyttää hyväksi. PI-algebrojen teoriaan ja niiden konstruktioon voi tutustua syvällisemmin esimerkiksi L. H. Rowenin kirjoista [7] ja [8] sekä N. Jacobsonin kirjoista [10] ja[16].

Työn kolmannessa osassa käsitellään muutamia sovelluksia, miten Shirshovin teoriat soveltuvat PI-algebrojen käsittelyyn. Tässä osassa esitetään Shirshovin todistama tulos motivoimaan polynomi-identiteettien käyttöä algebroissa. Ensimmäisenä sovelluksena todistetaan jo mainitut Kurochin ja

Levitzkyn ongelmat. Shirshovin Korkeuslauseesta seuraa suoraan, että Kurochin –sekä myös Levitskyn– ongelma on tosi PI-algebroissa. Ratkaisun tuloksena saadaan myös raja alkioiden lukumäärälle, jolla algebra generoituu moduliksi. Tätä rajaa parannetaan vielä todistamalla Kurochin ongelma uudestaan ilman Shirshovin Korkeuslauseen käyttöä –sovelluksena Shirshovin muille teorioille. Toisena sovelluksena näytetään ilman todistuksia niin sanotun Jacobsonin radikaalin nilpotenttisuus äärellisesti generoitujen PI-algebrojen suhteen. Razmyslov osoitti [21], että kaikille äärellisesti generoiduille algebroille, jotka toteuttavat niin sanotun Capellin identiteetin, Jacobsonin radikaali on nilpotentti. Kemer todisti [11], että jokainen äärellisesti generoitu algebra, jonka karakteristika on 0, toteuttaa Capellin identiteetin. Näin ollen Jacobsonin radikaali on nilpotentti karakteristikalla 0. Shirshovin Korkeuslauseen avulla tämä toteutuu kaikilla karakteristikoilla.

2 Shirshovin Lemma

Formuloidaan Shirshovin Lemma käyttäen hyväksi sanoja, jotka ovat äärellisestä symboli joukosta (ts. aakkostosta) valittujen symbolien jonoja. Lemma itsessään sanoo, että tarpeeksi pitkille sanoille saadaan tiettyä säännönmukaisuutta; sanat ovat joko

(i) jaksollisia siinä mielessä, että ne sisältävät korkeaa potenssia olevan tekijän tai

(ii) maksimaalisia tietyllä (myöhemmin esitettävällä) tavalla.

Esitetään Lemmalle Shirshovin omasta todistuksesta poikkeava todistus, joka kertoo ainoastaan "tarpeeksi pitkän sanan" olemassa olon. Tämä olisi jo sellaisenaan riittävä useisiin sovelluksiin. Aloitetaan ensin muutamilla sanoja koskevilla määrittelyillä ja lauseilla, jonka jälkeen katsotaan sanoja hieman laajemmin ennen kuin siirrytään Shirshovin Lemman todistamiseen.

2.1 Määritelmiä

Olkoon Σ äärellinen joukko symboleita (tai *kirjaimia*) eli *aakkosto*. Valitaan singleton joukko, joka ei kuulu aakkostoon, ja merkitään sitä $\{1\}$.

Määritelmä 2.1 Jonoa

$$(\omega) = (x_1, x_2, \ldots),$$

sanotaan *sanaksi aakkostossa* Σ, missä $x_i \in \Sigma \cup \{1\}$ sekä $x_i = 1$ aina, kun indeksi i on tarpeeksi suuri (ts. on olemassa alkio $N \in \mathbb{N}$ siten, että $x_i = 1$ aina, kun $i \geq N$). Määritellään lisäksi *tyhjä sana* $(1, 1, 1, \ldots)$.

Sana on *redusoitu*, jos seuraava ehto toteutuu:

(i) jos $x_k = 1$ jollakin indeksin k arvolla, niin $x_i = 1$ jokaisella indeksin $i \geq k$ arvoilla.

Yksinkertaistetaan merkintöjä kirjoittamalla redusoitu sana $(x_1, x_2, \ldots, x_d, 1, 1, \ldots)$ yksinkertaisemmin muodossa $x_1 x_2 \cdots x_d$ sekä tyhjä sana $(1, 1, \ldots)$ muodossa 1. Sanan $\omega = (x_1, \ldots x_d, 1, 1, \ldots) = x_1 \cdots x_d$ *pituus* on d ja sitä merkitään $|\omega| = d$; tyhjän sanan pituus on 0.

Olkoon Σ^* *kaikkien (redusoitujen) sanojen joukko*. Upotetaan nyt aakkosto $\Sigma \cup \{1\}$ joukkoon Σ^* kuvauksella

$$u \mapsto (u, 1, 1, \ldots).$$

Tämän injektion avulla voidaan aakkostoa Σ ajatella joukon Σ^* osajoukkona. Jatkossa sanalla tarkoitetaan redusoitua sanaa. Lisäksi sovitaan; jos aakkosto $\Sigma = \{\emptyset\}$, niin $\Sigma^* = \{1\}$.

Määritelmä 2.2 Pari $(M, \cdot)$ on *monoidi*, jos operaatio $\cdot$ on joukossa M määritelty assosiatiivinen binäärioperaatio sekä joukossa M on olemassa neutraalialkio.

Nyt kaikkien sanojen joukossa Σ^* voidaan määritellä binäärioperaatio $\cdot$, joka liittää kaksi jonoa yhteen:

(i) $1 \cdot 1 = 1$,

(ii) $x_1 x_2 \cdots x_i \cdot y_1 y_2 \cdots y_j = x_1 x_2 \cdots x_i y_1 y_2 \cdots y_j$.

Tämä binäärioperaatio on selvästi assosiatiivinen. Lisäksi selvästi $1 \cdot \omega = \omega \cdot 1 = \omega$ aina, kun $\omega \in \Sigma^*$, joten Määritelmän 2.2 mukaan kaikkien sanojen joukko Σ^* on monoidi, jonka neutraalialkio on tyhjä sana 1. Vastaavasti

kaikkien ei–tyhjien sanojen joukko $\Sigma^+ = \Sigma^*/\{1\}$ on *puoliryhmä* (binäärioperaatio on assosiatiivinen).

Määritelmä 2.3 Monoidi (vastaavasti myös puoliryhmä) M on *vapaa*, jos sille on olemassa sellainen osajoukko $N \subseteq M$, että jokainen joukon M alkio voidaan esittää yksikäsitteisesti osajoukon N alkioiden tulona. Tällöin joukkoa N kutsutaan myös joukon M *kannaksi*.

Huomautus 2.4 Selvästi monoidi $\Sigma^* = (\Sigma^*, \cdot)$ (vastaavasti puoliryhmä $\Sigma^+ = (\Sigma^+, \cdot)$) on Määritelmän 2.3 mukaan aakkoston Σ generoima *vapaa monoidi* (vastaavasti *vapaa puoliryhmä*). Tarkempaan tarkasteluun voi tutustua kirjassa [8].

Sana u on äärellisen sanan ω *tekijä*, jos on olemassa sanat v ja w siten, että

$$\omega = vuw.$$

Jos edellä $v = 1$, niin sana u on *vasen tekijä* tai *prefiksi* (vastaavasti jos $w = 1$, niin sana u on *oikea tekijä* tai *suffiksi*). Merkitään sanan ω kaikkien prefiksien joukkoa *pref*(ω) (vastaavasti suffiksien joukkoa *suf*(ω)), lisäksi olkoon $\mathrm{pref}_k(\omega)$ sanan ω vasemmanpuoleinen k-pituinen tekijä (jos $|\omega| < k$ määritellään $\mathrm{pref}_k(\omega) = \omega$). Sanan oikeanpuoleinen k-pituinen tekijä $\mathrm{suf}_k(\omega)$ määritellään vastaavasti. Sanan ω *tekijöihinjako* on mikä tahansa jono sanoja $u_1, \ldots, u_d$, joille

$$\omega = u_1 \cdots u_d.$$

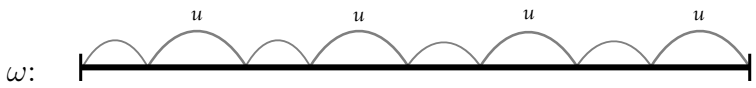
Edellinen on *L-tekijöihinjako* jos kaikki alkiot u_i ovat joukossa L. Nyt voidaan merkitä

$$L^* = \{u_1 \cdots u_d \,|\, d \geq 0, u_i \in L\},$$

$$L^+ = \{u_1 \cdots u_d \,|\, d \geq 1, u_i \in L\}.$$

Joukko L^* on monoidin Σ^* alimonoidi, jonka *generoi* joukko $L \subseteq \Sigma^*$ (vastaavasti joukko L^+ on aliryhmä, jonka generoi joukko L). Jokaisella sanalla $\omega \in L^*$ on siis olemassa ainakin yksi L-tekijöihinjako ja, jos se on yksikäsitteinen, on L^* vapaa, jonka kanta on L. Tällöin joukkoa L sanotaan myös *koodiksi*.

Sanan ω tekijää u sanotaan *n-moninkerraksi*, jos tekijällä u on n erillistä esiintymää, jotka eivät mene limittäin, sanassa ω:



Jos nämä esiintymät ovat peräkkäin sitä sanotaan *n-potenssiksi* ja merkitään u^n. Erityistapauksessa, jossa $n = 2$, sana u^2 on *neliö*. Todetaan, että potenssi voidaan antaa myös rationaalilukuna esimerkiksi jos $|u| = |v|$, niin $uvuvu = (uv)^{2\frac{1}{2}}$. Sana ω on *jaksollinen*, jaksona u, jos se on muotoa u^k, missä $k \in \mathbb{Q}$ ja $k > 1$.

Yksi tärkeimpiä määritelmiä tässä työssä on sanojen *leksikograaffinen järjestys*. Jos indeksi $i \in \mathbb{N}$, niin jokaiselle kirjaimelle x_i (ko. aakkostossa) annetaan arvo i ja järjestämme näistä kirjaimista saadut sanat järjestykseen ensimmäisen kirjaimen mukaan, missä indeksien i arvot eroavat, tai sana on toisen sanan aito prefiksi.

Määritelmä 2.5 Olkoon $(\Sigma, <)$ täydellisesti järjestetty. Relaatio $<_l$ on *sanojen leksikograaffinen järjestys* jos se toteuttaa seuraavat ehdot

$$\omega_1 <_l \omega_2 \iff \begin{cases} (i) & \omega_2 = \omega_1 v & v \neq 1 \text{ tai} \\ (ii) & \omega_1 = uxv \text{ ja } \omega_2 = uyv' & x < y, \end{cases}$$

missä $x, y \in \Sigma$ ja $u, v, v' \in \Sigma^*$.

Tyhjä sana 1 on sanojen minimaalialkio ts. $1 \leq_l u$ aina, kun $u \in \Sigma^*$. Selvästi edellisen määritelmän mukaan $(\Sigma^*, <_l)$ on täydellisesti järjestetty joukko; järjestys on refleksiivinen, transitiivinen, antisymmetrinen sekä kaikki joukon alkiot ovat vertailtavissa.

Lause 2.6 *Olkoot $u, v \in \Sigma^*$. Leksikograaffinen järjestys $<_l$ toteuttaa seuraavat ehdot*

(i) jos $u <_l v$, niin $tu <_l tv$, aina kun $t \in \Sigma^*$;

(ii) jos $u <_l v$ ja $u \notin \text{pref}(v)$, niin $uw <_l vw'$, kaikille $w, w' \in \Sigma^*$.

Todistus.
(i) Olkoon $t \in \Sigma^*$ mielivaltainen, $x \neq 1$ sekä $a, b \in \Sigma$, ja $a < b$. Jos nyt $u <_l v$, niin määritelmän 2.5 mukaan:

$$v = ux \Rightarrow tv = tux \Rightarrow tu <_l tv$$

tai

$$\begin{cases} u = pas \\ v = pbs' \end{cases} \Rightarrow \begin{cases} tu = tpas \\ tv = tpbs' \end{cases} \Rightarrow tu <_l tv$$

(ii) Koska $u \notin \text{pref}(v)$, niin voidaan päätellä

$$u <_l v \Rightarrow \begin{cases} u = pas_1 \\ v = pbs_1' \end{cases} \Rightarrow \begin{cases} uw = pas_1 w \\ vw' = pbs_1' w' \end{cases} \Rightarrow \begin{cases} uw = pas \\ vw' = pbs' \end{cases}.$$

Tällöin määritelmän 2.5 mukaan $uw <_l uw'$. □

2.2 ω-sana

Laajennetaan näkökantaa sanoihin menemällä äärellispituisista sanoista äärettömiin sanoihin.

Määritelmä 2.7 Oikealta äärettömään jatkuvaa symbolien jonoa, jossa ei esiinny alkiota 1, kutsutaan *äärettömäksi sanaksi*. Siitä käytetään myös nimitystä *ω-sana*.

Äärellinen sana u on ω-sanan h *tekijä*, jos on olemassa äärellinen sana v ja ω-sana h' siten, että

$$h = vuh'.$$

Jos edellä $v = 1$, niin sana u on *ω-sanan prefiksi* ja h' on *ω-sanan h suffiksi*.

Huomautus 2.8 Jos ω-sana h on toisen ω-sanan h' prefiksi, niin $h = h'$.

Äärellisen sanan ja ω-sanan yhdistelmä tuottaa luonnollisella tavalla ω-sanan; jos $n \in \mathbb{Z}$, jokainen ω-sana h voidaan jakaa yksikäsitteisesti tekijöihin

$$h = vh',$$

missä $|v| = n$ ja h' on jäljelle jäävä ω-sana. Tarkoitetaan jatkossa sanalla äärellistä sanaa ja äärettömän sanan käytöstä mainitaan erikseen.

Merkinnällä u^∞ tarkoitetaan sanaa, jossa sana u toistuu äärettömän monta kertaa peräkkäin. *Jaksollisessa ω-sanassa h* on muotoa u^∞ oleva oikeanpuoleinen tekijä (tässä vasen tekijä voi olla myös tyhjä sana). Jakso u valitaan aina niin, että u itsessään ei ole jaksollinen, toisin sanoen u ei ole minkään äärellisen sanan aito potenssi

Lause 2.9 *Olkoon h sanan uh vasen tekijä, missä h on joko äärellinen sana tai ω-sana. Tällöin h on sanan u^∞ vasen tekijä. Toisin sanoen, jos h on ω-sana, niin $h = u^\infty$.*

Todistus. Oletuksesta seuraa, että uh on sanan u^2h vasen tekijä. Jatkamalla tätä nähdään, että kaikilla arvoilla $k \in \mathbb{N}$, $u^k h$ on sanan $u^{k+1}h$ vasen tekijä.

Nyt transitiivisuudesta seuraa, että h on myös sanan $u^{k+1}h$ vasen tekijä. Ensimmäiseksi jos h on äärellinen sana, niin väite seuraa, kun $k \to \infty$. Toiseksi jos h on ω-sana ja $k \to \infty$, niin h on ω-sanan u^∞ vasen tekijä. Tämä on mahdollista vain jos $h = u^\infty$. $\square$

Olkoon nyt $\nu_n(h)$ ω-sanan h eri *n-tekijöiden* (n pituisten tekijöiden) lukumäärä. Esimerkiksi $\nu_1(h)$ tarkoittaa eri kirjaimien lukumäärää ω-sanassa h. Selvästi $\nu_n(h) \leq l^n$ aina, kun $n \in \mathbb{N}$. Seuraava huomautus on tärkeä, vaikka sen tarkastelu on triviaalia.

Huomautus 2.10

(i) Olkoon v mielivaltainen ω-sanan h n-tekijä. Tästä saadaan $(n+1)$-tekijä yksinkertaisesti lisäämällä siihen seuraava kirjain, joten $\nu_{n+1}(h) \geq \nu_n(h)$.

(ii) Jos $\nu_{n+1}(h) = \nu_n(h)$, tällöin jokaista annettua n-tekijää v kohti on olemassa yksikäsitteinen $(n+1)$-tekijä, jonka prefiksi on v. Jos olisi olemassa sellaiset vx_i ja vx_j, jotka molemmat ovat ω-sanan h tekijöinä, niin (i)-kohdan mukaan kaikki muut $(n+1)$-tekijät alkavat n-tekijällä. Tällöin $\nu_{n+1}(h) > \nu_n(h)$ ja saadaan ristiriita.

Lause 2.11 (Coven-Hedland) *Oletetaan, että on olemassa sellaiset vakiot m ja n, että $\nu_{n+1}(h) = \nu_n(h) = m$. Tällöin ω-sana h on jaksollinen, jonka jakson pituus on $\leq m$.*

Todistus. Olkoot $h = x_{i_1}x_{i_2}x_{i_3}\ldots$ ω-sana, sekä

$$v_j = x_{i_j}x_{i_{j+1}}\ldots x_{i_{j+n-1}}$$

ω-sanan h kohdassa j oleva n-tekijä, missä $1 \leq j \leq m+1$. Tällöin $v_1, \ldots, v_{m+1}$ ovat n pituisia sanoja. Oletuksen mukaan kaksi näistä sanoista ovat yhtäsuuria; $v_j = v_k$, missä $j < k \leq m+1$, tarkemmin sanoen $j \leq m$.

Olkoon nyt h_j ω-sana, joka alkaa kohdasta j. Huomautuksen 2.10 kohdan (ii) mukaan jokainen n pituinen jakso kirjaimia ω-sanasta h määrittelee seuraavan kirjaimen yksikäsitteisesti, joten ω-sanan h_j määritelee sen vasen tekijä v_j. Nyt

$$\begin{cases} h_j = v_j h_1 \\ h_k = v_k h_2 \end{cases} \Longrightarrow^{(ii)} h_1 = h_2,$$

josta seuraa, että

$$h_j = h_k = x_{i_j} \dots x_{i_{k-1}} h_j,$$

jolloin $h_j = u^\infty$, missä $u = x_{i_j} \dots x_{i_{k-1}}$. Näin ollen $|u| = k-j \leq m$; tarkemmin sanoen

$$h = x_{i_1} \dots x_{i_{j-1}} h_j$$

on jaksollinen. $\square$

2.3 Shirshovin Lemma

Äärettömien sanojen käytännön tehokkuus äärellisiin sanoihin verrattuna tulee esille Shirshovin lemman todistuksessa. Shirshovin itsensä alunperin esittämä todistus perustuu kaksoisinduktion käyttöön. Tässä esitetty toisenlainen todistus perustuu puhtaasti kombinatorisiin tekniikoihin.

Olkoon S_d *symmetrinen ryhmä* d-alkioisen joukon suhteen.

Määritelmä 2.12 Jono $(\omega_1, \omega_2, \dots, \omega_d)$ ei-tyhjiä sanoja on sanan $\omega = u\omega_1\omega_2 \dots \omega_d v$ *d-jako*, jos jokaiselle ei-triviaalille permutaatiolle $\sigma \in S_d$

$$\omega_1\omega_2 \cdots \omega_d >_l \omega_{\sigma(1)}\omega_{\sigma(2)} \cdots \omega_{\sigma(d)}.$$

Jos sanalla ω on d-jako, sanotaan sanaa *d-jaetuksi*. Vastaavasti sana on *d-jaoton*, jos sillä ei ole olemassa d-jakoa. Seuraava lemma antaa riittävän ehdon sanan d-jaettavuudelle.

Lemma 2.13 *Olkoon ω sana, joka sisältää d kappaletta erillisiä d-tekijöitä leksikograaffisesti laskevassa järjestyksessä, missä mikään näistä tekijöistä ei ole toisen leksikograaffisesti suuremman tekijän prefiksi. Toisin sanoen ω on muotoa*

$$s_0 u_1 s_1 u_2 \cdots s_{d-1} u_d s_d,$$

missä $u_1 >_l u_2 >_l \cdots >_l u_d$ sekä $u_{i+1} \notin \mathrm{pref}(u_i)$. Tällöin ω on d-jaettu.

Todistus. Merkitään $\omega_i = u_i s_i$. Lauseen 2.6 mukaan sanat ω_i muodostavat myös laskevan ketjun

$$\omega_1 >_l \omega_2 >_l \cdots >_l \omega_d,$$

koska mikään sanoista u_i ei ole minkään toisen sanan u_j aito prefiksi. Edelleen mikään sanoista ω_i ei ole jonkun toisen sanan ω_j aito prefiksi. Lauseen 2.6 kohdan (i) mukaan:

$$\omega_1 \omega_2 \cdots \omega_i >_l \omega_1 \omega_2 \cdots \omega_{i+k}$$

aina, kun $1 \leq i \leq d-1$ ja $1 \leq k \leq d-i$. Nyt lauseen 2.6 kohdan (ii) mukaan leksikograaffisen järjestyksen suunta säilyy vaikka molemmille puolille lisätään mielivaltaiset oikeanpuoleiset tekijät. Tästä saadaan:

$$\omega_1 \omega_2 \cdots \omega_i \cdots \omega_d >_l \omega_1 \omega_2 \cdots \omega_{\sigma(i)} \cdots \omega_{\sigma(d)}$$

aina, kun $1 \leq i \leq d$. $\square$

Edellisen lemman tekijöiden u_i oletus toteutuu, jos kaikki tekijät u_i ovat myös yhtäpitkät. Näin ollen ekvivalentisti sana on *d-jaettu*, jos se sisältää vähintään d kappaletta erillisiä d pituisia tekijöitä leksikograaffisesti laskevassa järjestyksessä. Vastaavasti määritellään äärettömille sanoille; ω-sana on *d-jaettu*, jos se sisältää vähintään d kappaletta erillisiä d pituisia tekijöitä leksikograaffisesti laskevassa järjestyksessä.

Lemma 2.14 (König) *Olkoot Σ äärellinen aakkosto sekä $X \subset \Sigma^+$ mielivaltainen ääretön osajoukko. Tällöin on olemassa sellainen ω-sana h, että jokainen sen tekijä u on tekijänä äärettömän monessa joukon X alkiossa*

Todistus. Olkoon sana $u \in X$. Nyt on olemassa äärettömän monta sellaista sanaa $u \in X$, että sama kirjain x_1 esiintyy sanassa u kohdassa 1. Äärettömän moni näistä sanoista toteuttaa seuraavan:

$$u_1 u_2 = x_1 x_2,$$

jollekin kirjaimelle x_2. Samaan tapaan siellä esiintyy kirjain x_3. Jatketaan tätä induktiivisesti ja saadaan ω-sana $x_1 x_2 x_3 \cdots$, jonka jokainen tekijä on tekijänä äärettömän monessa joukon X sanassa. $\square$

Kutsutaan tekijää *toistuvaksi* (unconfined), jos se esiintyy ω-sanassa tekijänä äärettömän monta kertaa. Vastaavasti se on *ei-toistuva* (confined), jos se esiintyy vain äärellisen monta kertaa. Sanotaan vielä ω-sanaa h *tiheäksi* (recurrent), jos jokainen sen tekijä $u \in F(h)$ esiintyy äärettömän monta kertaa.

Määritelmä 2.15 ω-sana h on *tasaisesti tiheä* (uniformly recurrent), jos kaikille tekijöille $u \in F(h)$ on olemassa sellainen luku $k \in \mathbb{N}$, että jokainen tekijä $v \in F(h)$ toteuttaa seuraavan ehdon:

$$|v| \geq k \Rightarrow u \in F(v).$$

Lemma 2.16 (Fürstenberg) *Olkoon h mielivaltainen ω-sana. Tällöin on olemassa sellainen tasaisesti tiheä ω-sana h', että $F(h') \subseteq F(h)$.*

Todistus. Olkoot h mielevaltainen ω-sana sekä $u \in F(h)$. Määritellään luku $g(h, u)$ seuraavasti:

$$g(h, u) = \mathrm{Sup}\{|v| : v \in F(h),\, u \notin F(v)\}.$$

Tässä $g(h, u) = \infty$, jos ω-sanalla h on mielivaltaisen pitkiä tekijöitä, joissa ei esiinny tekijää u.

Olkoot nyt $u_1, u_2, \ldots$ mielivaltaiset ω-sanan h tekijät ja konstruoidaan ääretön ketju ω-sanoja seuraavasti:

Olkoon $t_0 = h$.

Olkoon $i > 0$. Jos $u_i \in F(t_{i-1})$ ja $g(t_{i-1}, u_i) < \infty$, niin $t_i = t_{i-1}$. Päinvastaisessa tilanteessa olkoon X ääretön joukko tekijöitä $v \in F(t_{i-1})$ siten, että $u_i \notin F(v)$. Käyttäen nyt hyväksi Lemmaa 2.14 konstruoidaan sana t_i lähtien joukosta X, toisin sanoen sanan t_i jokainen tekijä on tekijänä äärettömän monessa joukon X alkiossa.

Jos tässä konstruktiossa sana v on tekijänä sanassa t_j sekä $v = u_k$, missä $j \geq k$, niin tällöin $g(t_j, v) \leq g(t_{k-1}, v) < \infty$.

Olkoon $i > 0$. Valitaan nyt jokaisesta sanasta t_i pituutta i oleva tekijä v_i. Olkoon V_i ääretön joukko näitä tekijöitä toisin sanoen $V_i = \{v_i \mid |v_i| = i,\ t_i = v_i t'\}$. Lemman 2.14 mukaan on olemassa sellainen ω-sana h', että jokainen sen tekijä on tekijänä äärettömän monessa joukon V_i sanassa.

Tällöin jos $v = u_k \in F(h')$, niin $v \in F(t_j)$, jollakin arvolla $j > k$. Tästä seuraa, että $g(t_j, v) < \infty$. Lisäksi vielä $g(h', v) < \infty$, koska $F(h') \subset F(t_j)$. Jolloin siis h' on tasaisesti tiheä. $\square$

Seuraavassa lauseessa saadaan ω-sanoille selkeä kahtiajako d-jaettujen ja jaksollisten välille. Tämä on hyvin olennainen osa Shirshovin Lemman todistusta.

Lause 2.17 *Jokaisella ω-sanalla h on joko d-jako tai se on jaksollinen, jonka jakson pituus on $< d$.*

Todistus. Oletetaan ensin, että ω-sanalla h on d kappaletta toistuvia d-tekijöitä $v_1, \ldots, v_d$. Koska nämä tekijät ovat samanpituisia, niin mahdollisesti

uudelleen indeksoimalla voidaan olettaa, että $v_1 >_l \cdots >_l v_d$. Muodostetaan sana h' induktiivisesti; valitaan sanan v_1 ensimmäinen esiintymä. Seuraavaksi valitaan sanan v_2 ensimmäinen esiintymä, joka alkaa sanan v_1 jälkeen. Jatkamalla tätä induktiivisesti saadaan ω-sanan h tekijä $h' = v_1 u_1 \cdots u_{d-1} v_d$. Sanat v_i eivät mene päällekkäin, joten ω-sanalla h on d-jako.

Nyt voimme olettaa, että ω-sanalla h on vähemmän kuin d kappaletta toistuvia d-tekijöitä. Selvästi ω-sanalla h on sellainen (äärellinen) vasen tekijä w, joka sisältää kaikki ei-toistuvat d-tekijät. Olkoon nyt $h = wh^*$. Tällöin oletuksen mukaan ω-sanan h^* kaikki d-tekijät ovat toistuvia. Näin ollen ω-sanalla h^* on vähemmän kuin d kappaletta d pituisia tekijöitä, toisin sanoen $\nu_d(h^*) < d$. Mutta selvästi $\nu_1(h^*) \geq 1$, joten Huomautuksen 2.10 (kohdan (i)) perusteella on olemassa sellainen $n \leq d$, jolle $\nu_n(h^*) = \nu_{n+1}(h^*) < d$. Nyt lauseesta 2.11 seuraa, että ω-sana h^* on jaksollinen, jonka jakson pituus on $< d$. $\square$

Olkoot nyt h d-jaoton ω-sana sekä $\beta(\ell, k, d, h)$ pienin vakio arvoista β, jolle h sisältää muotoa vu^k olevan prefiksin siten, että $|v| \leq \beta$ ja $|u| \leq d$. Lauseen 2.17 mukaan $\beta(\ell, k, d, h)$ on olemassa ja on korkeintaan ω-sanan h prefiksin v pituus, missä v on pienin mahdollinen. Shirshovin Lemman todistuksessa osoitetaan, että $\beta(\ell, k, d, h)$ on rajoitettu funktiolla, joka ei riipu ω-sanan h valinnasta.

Lemma 2.18 (Shirshovin lemma) *Olkoot $\ell, k, d \in \mathbb{N}$ ja Σ täydellisesti järjestetty ℓ-alkioinen aakkosto. Tällöin on olemassa sellainen luku $\beta = \beta(\ell, k, d)$, että kaikki d-jaottomat sanat $\omega \in \Sigma^*$, missä $|\omega| \geq \beta(\ell, k, d)$, sisältää muotoa u^k olevan alisana, jolle $|u| \leq d$.*

Todistus. Väitetään, että jokaista kolmikkoa (ℓ, k, d) kohden on olemassa sellainen vakio $\beta(\ell, k, d)$ siten, että kaikille d-jaottomille ω-sanoille h,

$\beta(\ell, k, d, h) \leq \beta(\ell, k, d)$. Tehdään vastaoletus ja määritellään seuraava joukko:

$$P = \{v_j \mid h = v_j h', |v_j| = j, j \geq 1, \beta(\ell, k, d, h) > \gamma\},$$

missä $\gamma \in \mathbb{N}$ ja prefiksi v_j ei ole jaksollinen eikä sisällä d-jaettua tekijää. Nyt Lemmojen 2.14 ja 2.16 mukaan on olemassa sellainen (tasaisesti) tiheä ω-sana q, että sen jokainen tekijä on tekijänä ainakin yhdessä joukon P sanassa. Nyt Lauseen 2.17 mukaan sanalla q on d-jako tai se on jaksollinen. Ensimmäiseksi jos q on jaksollinen se sisältää potenssia k olevan tekijän, jonka siis täytyy olla tekijänä ainakin yhdesssä sanassa v_j, mistä seuraa ristiriita. Toiseksi jos sanalla q on d-jaettu tekijä, niin sen täytyy myös olla tekijänä ainakin yhdessä sanassa v_j. Tästä seuraa jälleen ristiriita. □

2.4 Funktion $\beta(\ell, k, d)$ kasvu

Edellisessä luvussa todistettiin Shirshovin Lemma käyttäen hyväksi kombinatorisia menetelmiä sekä ω-sanoja. Kuitenkaan Lemman todistus ei sano arvosta $\beta(\ell, k, d)$ muuta, kuin sen olemassaolon, joka sellaisenaan riittääkin moniin sovelluksiin. Todistetaan Shirshovin Lemma nyt uudestaan, jolloin saadaan funktion $\beta(\ell, k, d)$ arvoille selkeä raja.

2.4.1 Shirshovin Lemman toinen todistus

Mukaillaan Shirshovin Lemman todistuksessa hänen alkuperäistä ideaa [3]. Alkuun tästä Lemmasta otetaan hieman heikompi versio, jossa ei ole mitään vaatimuksia toistetun sanan u pituudesta:

Todistus tehdään kaksoisinduktiolla parametrien d ja ℓ suhteen. Jos $d = 1$, niin $\beta(\ell, k, d) = 1$, koska tällöin jokaisella sanalla on 1-jako. Jos $\ell = 1$, niin voidaan valita $\beta = k$ sekä $v = x_1$.

Oletetaan $\beta(l-1,k,q)$ ja $\beta(p,k,d-1)$ tunnetuiksi kaikilla parametrien p ja q arvoilla.

Olkoon ω mielivaltainen sana, joka ei sisällä muotoa v^k olevaa tekijää. Lasketaan seuraavaksi tarpeeksi suuri $\beta = \beta(\ell,k,d)$ niin, että sanalla ω on d-jako aina, kun $|\omega| \geq \beta$.

Etsitään kirjaimen x_ℓ esiintymät sanassa ω:

$$\omega = v_0 x_\ell^{t(1)} v_1 x_\ell^{t(2)} v_2 \cdots x_\ell^{t(m)} v_m.$$

Tässä siis jokainen v_i sana on joukosta $\{x_1,\ldots,x_{\ell-1}\}$ sekä $v_i \neq 1$ aina, kun $i \in \{1,\ldots,m-1\}$, erityisesti sanat v_0 ja v_m voivat siis olla tyhjiä. Induktio parametrin ℓ suhteen on käsitelty, ellei $|v_i| < \beta(\ell-1,k,d)$. Sanan ω oletuksesta saadaan myös, että $t(i) < k$ aina, kun $i \in \{1,\ldots,m-1\}$.

Muodostetaan uusi aakkosto Σ':

$$\Sigma' = \{v_1 x_\ell^{t(2)}, v_2 x_\ell^{t(3)}, \ldots, v_{m-1} x_\ell^{t(m)}\}.$$

Näin ollen jokainen uusi kirjain $x' \in \Sigma'$ alkaa jollakin kirjaimella x_j, missä $1 \leq j \leq \ell-1$. Määritellään tälle aakkostolle myös uusi järjestys $>'$:

$$v_{i-1} x_\ell^{t(i)} >' v_{j-1} x_\ell^{t(j)} \iff v_{i-1} x_\ell^{t(i)} >_\ell v_{j-1} x_\ell^{t(j)}.$$

Tämä järjestys on selvästi aakkoston Σ' täydellinen järjestys ja se indusoi vastaavalle alimonoidille Σ'^* leksikograaffisen järjestyksen, jota merkitään vastaavasti $>'_l$.

Arvioidaan aakkoston Σ' alkioiden määrää. Aikaisemmin todettiin, että $|v_i| < \beta(\ell-1,k,d)$, sekä jokaiselle sanan v_i kirjaimelle on $\ell-1$ mahdollisuutta. Tällöin on olemassa korkeintaan $\ell^{\beta(\ell-1,k,d)}$ mahdollisuutta sanaksi v_i. Kertomalla tämä kaikilla mahdollisilla potenssin $t(i)$ arvoilla nähdään, että kirjainten lukumäärä aakkostossa Σ' on korkeintaan $k\ell^{\beta(\ell-1,k,d)}$.

Väite 1. Olkoot $f, g \in \Sigma'^*$ ja $f >'_l g$. Tällöin $f >_l g$ alkuperäisessä aakkostossa Σ.

Oletetaan ensin, että g ei ole vasen tekijä sanassa f. Nyt $f = uxr$ ja $g = uys$, missä $u, r, s \in \Sigma'^*$ ja $x, y \in \Sigma'$ sekä $x >'_l y$. Oletetaan myös, että $x = v_{i-1}x_\ell^{t(i)}$ ja $y = v_{j-1}x_\ell^{t(j)}$.

Tapaus 1. Jos $v_{i-1} >_l v_{j-1}$, niin selvästi $f >_l g$.

Tapaus 2. Olkoon $v_{i-1} = v_{j-1}$. Tällöin $t(i) > t(j)$. Nyt $f = uv_{i-1}x_\ell^{t(i)}r$ ja $g = uv_{j-1}x_\ell^{t(j)}s$. Koska sana g ei ole vasen tekijä sanassa f, niin $s \neq 1$. Tällöin sana s alkaa jollain kirjaimista $\{x_1, \ldots, x_{\ell-1}\}$, joten $x_\ell >_l s$. Tästä seuraa, että $f >_l g$.

Nyt voidaan jatkaa loppuun Shirshovin Lemman todistusta. Merkitään

$$\omega = v_0x_\ell^{t(1)}v_1x_\ell^{t(2)}v_2 \cdots x_\ell^{t(m)}v_m = v\omega',$$

missä $v = v_0x_\ell^{t(1)}$ ja $\omega' = v_1x_\ell^{t(2)}v_2 \cdots x_\ell^{t(m)}v_m$. Olkoon

$$\beta(l, k, d) = \beta(l-1, k, d) + k + \beta(kl^{\beta(l-1,k,d)}, k, d-1).$$

Tällöin ainakin yksi seuraavista vaihtoehdoista on tosi:

$$\begin{aligned} &(i) && |v_0| \geq \beta(\ell - 1, k, d) \text{ tai} \\ &(ii) && t(1) \geq k \text{ tai} \\ &(iii) && |\omega'| \geq \beta(k\ell^{\beta(\ell-1,k,d)}, k, d-1). \end{aligned}$$

Vaihtoehdon (i) toteutuessa Shirshovin Lemma pitää paikkansa, koska induktio-oletuksen nojalla sana v_0 (ja siis myös sana ω) sisältää d-jaetun tekijän.

Vaihtoehdon (ii) toteutuessa Shirshovin Lemma pitää myös paikkansa, koska tällöin ω sisältää tekijän x_ℓ^k.

Oletetaan siis, että kohta (*iii*) toteutuu. Nyt parametrin d induktion nojalla, sana ω' on $(d-1)$-jaettu järjestyksen $>_l'$ suhteen ja näin ollen myös järjestyksen $>_l$ suhteen. Tästä seuraa, että

$$\omega' = \omega_0\omega_1 \cdots \omega_{d-1}$$

sekä $\omega_0\omega_1 \cdots \omega_{d-1} >_l \omega_0\omega_{\pi(1)} \cdots \omega_{\pi(d-1)}$ kaikille $1 \neq \pi \in S_{d-1}$. Joten ω sisältää tekijän

$$(x_\ell^{t(1)}\omega_0)\omega_1 \cdots \omega_{d-1}$$

Tämä on d-jaettu leksikograaffisessa järjestyksessä $>_l$, koska kaikki sanat $\omega_1, \ldots, \omega_{d-1}$ alkavat kirjaimilla, jotka ovat $<_l x_\ell$. Näin ollen Shirshovin Lemman heikompi versio on todistettu.

Jäljelle jää vielä rajoittaa toistetun tekijän u pituutta. Tätä varten tarvitaan muutamia lisäkäsitteitä jaksollisuudesta. Äärellisiä sanoja ω ja ω' sanotaan *konjugaateiksi*, jos $\omega = uv$ ja $\omega' = vu$ sopivilla sanan ω tekijöillä u, v. Tällöin erityisesti ω' on sanan ω^2 tekijä. Lisäksi määritellään *kierto* $\delta : \Sigma^* \to \Sigma^*$ seuraavasti: $\delta(vx) = xv$ aina, kun $v \in \Sigma^*$ ja $x \in \Sigma$. Toisin sanoen kierretään viimeinen kirjain ensimmäiseksi.

Lemma 2.19 *Olkoon $\omega = uv = vu$, missä $u, v \neq 1$. Tällöin ω on jaksollinen jaksolla, joka jakaa* $\mathrm{syt}(|u|, |v|)$ *sekä u, v ovat jaksollisia samalla jaksolla kuin ω.*

Todistus. Voidaan olettaa, että $|u| \leq |v|$. Tällöin u on sanan v vasen tekijä ts. $v = uv'$. Nyt $uuv' = \omega = vu = uv'u$, joten $uv' = v'u$. Induktiolla pituuden $|\omega|$ suhteen nähdään, että uv' on jaksollinen jaksolla $\hat{u}$, jonka pituus jakaa $\mathrm{syt}(|u|, |v'|)$. Merkitsemällä $u = \hat{u}^i$ ja $v' = \hat{u}^j$ nähdään, että $v = \hat{u}^{i+j}$ ja $\omega = \hat{u}^{2i+j}$. $\square$

Huomautus 2.20 Joukko $\{\delta^k(u) \mid 0 \leq k < |u|\}$ on kaikkien sanan u konjugaattien joukko. Lemmasta 2.19 seuraa, että $\delta^k(u) = u$, missä $0 < k < |u|$ tarkalleen silloin, kun u on jaksollinen jaksolla, jonka pituus jakaa potenssin k. Näin ollen saadaan seuraavanlainen kahtiajako:

(i) Sanalla u on jakso, joka on pienempi kuin d. Toisin sanoen $\delta^k(u) = u$, missä $0 < k < d$.

(ii) joukon $\{\delta^k(u) \mid 0 \leq k < d\}$ alkiot ovat sanan u^2 eri tekijöitä. Tässä tapauksessa Lauseen 2.13 mukaan u^{2d} on d-jaollinen.

Käyttämällä tätä jakoa Shirshovin Lemman heikompaan versioon saadaan seuraava vahvempi tulos:

Lause 2.21 *Olkoon ω d-jaoton ja $|\omega| \geq \beta(\ell, k, d)$, missä $k \geq 2d$. Tällöin ω sisältää muotoa u^k olevan tekijän, missä $|u| \leq d$.*

Todistus. Sana ω sisältää jo tekijän u^k, koska $|\omega| \geq \beta(\ell, 2d, d)$. Valitaan tällainen u jonka pituus on minimaalinen; tarkemmin sanoen u ei ole jaksollinen. Nyt jos $|u| > d$, niin edellisen Huomautuksen 2.20 kohta (i) ei toteudu, joten u^{2d} on d-jaollinen. Tästä seuraa, että sanalla ω on d-jako. □

Näin Shirshovin Lemma saatiin todistettua toisella tavalla, koska parametri k voidaan korvata parametrien k ja $2d$ maksimilla. Kuitenkin funktiolle $\beta(\ell, k, d)$ saatu raja kasvaa todella nopeasti (johtuen kaksoisinduktiosta).

Funktion $\beta(\ell, k, d)$ kasvua osoittaa intuitiiviset arviot [5]

$$\beta(\ell+1, k, d) \gg (\ell+1)^{\beta(\ell,k,d)} \gg \cdots \gg (\ell+1)^{\ell^{\cdot^{\cdot^{\cdot^{2}}}}},$$

missä $\gg$ ei tarkoita samaa kertaluokkaa olevaa vaan, että vasen puoli kasvaa ”oleellisesti” nopeammin kuin oikea puoli.

2.4.2 Sanan ω pituuden tarkennus

Tarkennetaan Shirshovin funktiota $\beta(\ell, k, d)$ antamalla sille paremmin käytäntöön sopiva raja. Tätä varten tarvitaan seuraavaa kahtiajakoa.

Lemma 2.22 *Olkoon v sana, jonka pituus on $\geq dk$. Tällöin jompikumpi seuraavista on voimassa:*

(i) sanalla v on tekijä u^k, jolle $|u| \leq d$ tai

(ii) sana v sisältää d kappaletta sellaisia tekijöitä, joista mitkään eivät ole toistensa aitoja prefiksejä, toisin sanoen kaikki tekijät ovat vertailtavia määritelmän 2.5 kohdan (ii) mukaan.

Todistus. Kohta (ii) on selvä, ellei ole olemassa sellaista vakiota j, $0 \leq j < d$, että $\delta^j(v) = v$. Tässä tapauksessa Lemman 2.19 mukaan v on jaksollinen, jonka jakson pituus on $\text{syt}(d, j)$. Tässä $\text{syt}(d, j) \leq \frac{d}{2}$, joten jakso u toistuu ainakin k kertaa sanassa v, mistä seuraa kohta (i). □

Määritelmä 2.23 Kutsutaan sanaa ω (k, d)-*Shirshov redusoituvaksi*, jos sanalla ω on tekijä u^k, missä $|u| \leq d$ tai sillä on d-jako.

Tarkastellaan nyt vaihtoehtoa (ii) Lemmassa 2.22, jolloin siis $\beta > dk$, ja etsitään sellaista pituutta β, jolle kaikki pidemmät sanat ovat Shirshov redusoituvia. Tällöin β on yläraja suureelle $\beta(\ell, k, d)$. Annetaan kaksi esimerkkiä milloin sana on Shirshov redusoituva.

Määritelmä 2.24 Sanaa ω sanotaan *Shirshov sallituksi*, jos sillä on muotoa u^k oleva tekijä, missä $|u| \geq 1$, tai se sisältää d kappaletta sellaisia tekijöitä, jotka eivät ole toistensa aitoja prefiksejä.

Nyt Lemman 2.22 mukaan mikä tahansa dk pituinen sana on Shirshov sallittu. Mutta tällöin Lauseen 2.13 perusteella, jos sanalla ω on Shirshov

sallittu tekijä d-monikertana, niin ω on Shirshov redusoituva. Tällöin etsitään siis pienintä lukua β, joka toteuttaa tämän ehdon.

Nopein tapa tehdä tämä on valita kaikki sanat joiden pituus on dk. Näitä sanoja on ℓ^{dk} kappaletta. Jos sanalla ω on $d\ell^{dk}$ kappaletta tekijöitä, joiden jokaisen pituus on dk, niin tällöin ainakin yhdellä näistä tekijöistä on d-moninkerta ja on Shirshov sallittu, koska sen pituus on dk. Näin ollen, sanalla ω on d-jako. Tällöin voidaan valita

$$\beta = d^2 k \ell^{dk}.$$

Jotta tätä arvioita voidaan pienentää monia näistä sanoista täytyy jättää vielä ulkopuolelle. Haetaan siis vastausta seuraavaan kysymykseen: ”mitkä ehdot sanan pitää toteuttaa, jotta Lemman 2.22 ehto (ii) ei toteudu?” Tätä varten pitää tarkastella tarkemmin sanan jaksollisuutta.

Määritelmä 2.25 Olkoon sana ω muotoa $u^k r$, missä r on tekijän u prefiksi, tällöin sanaa ω kutsutaan *osajaksolliseksi.* Jos sana ω on muotoa $vu^k r$, missä r on tekijän u prefiksi, niin sitä kutsutaan *valejaksolliseksi* sekä prefiksiä v *esijaksoksi.* Sanan ω *tyyppi* on pienin mahdollinen pituus $|v| + |u|$.

Osajaksollinen sana on vasemmalta oikealle symmetrinen. Tarkemmin sanoen, jos $\omega = u^k r$, missä $u = rr'$, niin $\omega = r(r'r)^k$.

Lemma 2.26 *Ensimmäisen kirjaimen poistaminen valejaksollisesta sanasta pienentää sen esijaksoa yhdellä.*

Todistus. Olkoon $\omega = vu^k r$ muotoa oleva sana, missä $v \neq 0$. Tällöin poistamalla sanan v ensimmäinen kirjain, pienentää $|v|+|u|$ yhdellä. Mutta esijakso ei voi pienentyä enempää kuin yhdellä, koska tällöin lisäämällä ensimmäinen kirjain takaisin saataisiin sanalle ω alkuperäistä pienempi esijakso. □

Käytetään jälleen ω-sanoja hyväksi todistusten yksinkertaistamiseksi. Tässä ω-sanan *esijakso* tarkoittaa jaksollisen ω-sanan $h = vh'$ vasenta tekijää v, jolle $|v|$ on pienin mahdollinen.

Lause 2.27

(i) Olkoon $h = vuh' = vh'$ ω-sana. Tällöin h' on muotoa u^∞, joten h on jaksollinen, jonka esijakso on vasen tekijä sanasta v.

(ii) Olkoon $\omega = vu\omega'$ äärellinen sana, missä $|u| < |\omega|$ ja $v\omega'$ on sanan ω vasen tekijä. Tällöin sanalla ω on esijaksona sanan v vasen tekijä ja ω' on jaksollinen jaksolla u.

Todistus. (i) Sovelletaan Lausetta 2.9 yhtälöön $uh' = h'$. Kohta(ii) on edellinen kohta uudelleenesitettynä, johon yhdistetään Lemma 2.19. □

Muodostetaan jälleen yksi kahtiajako, joka on avain asemassa, kun Shirshovin funktiolle annetaan käytännöllisempi raja.

Lemma 2.28 *Olkoot $|\omega| \geq 2d$ ja*

$$\omega = u_0\omega' = v_1u_1\omega' = v_2u_2\omega' = \cdots = v_{d-1}u_{d-1}\omega',$$

missä $|v_i| = i$ ja $|u_i| = d-i$. Tällöin toinen seuraavista ehdoista on voimassa:

(i) sanat $u_i\omega'$ muodostavat ketjun leksikograaffisen järjestyksen suhteen:

$$u_0\omega' <_\ell u_1\omega' <_\ell \cdots <_\ell u_{d-1}\omega' \quad tai \quad u_0\omega' >_\ell u_1\omega' >_\ell \cdots >_\ell u_{d-1}\omega'$$

(ii) ω' on jaksollinen jollain jaksolla u ja ω on valejaksollinen, jonka tyyppi on $< d$.

Todistus. Jos nyt jokin $u_j\omega'$ on sanan $u_i\omega'$ prefiksi, missä $i < j$. Toisin sanoen $u_i = u_j u$. Tällöin ω' on sanan $u\omega'$ prefiksi, joten Lauseen 2.27 kohdasta (ii) seuraa, että ω' on jaksollinen jaksolla u. Koska nyt

$$v_j u_j = v_i u_i = v_i u_j u,$$

nähdään, että esijakso sisältyy sanaan $v_i u_j$ ja tyyppi $\leq |v_i u_j| + |u| < d$. $\square$

Kutsutaan nyt sanaa ω *d-kriittiseksi*, jos sen tyyppi on d, mutta vasemman tekijän $\text{pref}_{|\omega|-1}(\omega)$ tyyppi on $d-1$.

Huomautus 2.29 Mielivaltainen d-kriittinen sana ω voidaan kirjoittaa muodossa $vu^k x_i$, missä

$$|v| + |u| = d - 1.$$

Näin ollen, $|\omega| \leq d - 1 + (d-1)(k-1) + 1 = dk - k + 1$.

Arvioidaan nyt lukua β tarkemmin. Ajatellaan pituudeltaan $\geq dk$ olevan sanan "äärimmäistä tapausta"; toisin sanoen sana ω on Shirshov sallittu, mutta sen vasen tekijä ω_0, joka saadaan jättämällä viimeinen kirjain pois, ei ole Shirshov sallittu. Nyt Lemman 2.28 mukaan, sanan ω_0 tyyppi on $< d$. Jos nyt oletetaan, että $|\omega| > (d-1)k$ ja sanan ω tyyppi on $< d$, niin sen jakson u pituus on $\leq d-1$ sekä sen esijakson v pituus $\leq d-1-|u|$. Tästä seuraa, että vu^k esintyy sanassa ω_0, joten ω_0 oli alunperinkin Shirshov sallittu. Voidaan siis olettaa, että sanan ω tyyppi on $\geq d$. Nyt Lemman 2.26 avulla nähdään, että sanan ω tyyppi on d ja sanan ω_0 tyyppi on $d-1$; toisin sanoen, ω on d-kriittinen.

Tarkemmin sanoen, mielivaltainen sana, jonka pituus on $\geq dk$ eikä se ole Shirshov redusoituva, sisältää d-kriittisen prefiksin, jonka pituus on $< dk$. Lasketaan seuraavaksi kaikki tällaiset tekijät.

Lause 2.30 *Olkoon* $|\Sigma| = \ell$

(i) Kaikkien d-kriittisten t pituisten sanojen lukumäärä on korkeintaan $d(\ell-1)\ell^{d-1}$.

(ii) Kaikkien d-kriittisten sanojen, joiden pituus $\leq t$*, lukumäärä on korkeintaan* $d(\ell-1)\ell^{d-1}t$.

(iii) Kaikkien d-kriittisten sanojen, mitkä eivät sisällä potenssia k olevaa tekijää (jonka pituus on $\leq d$*), lukumäärä on korkeintaan* $d^2k(\ell-1)\ell^{d-1}$.

Todistus. (i) $d-1$-pituinen prefiksi voidaan valita ℓ^{d-1} tavalla. Tämä voidaan erotella jaksoiksi ja esijaksoiksi d eri tavalla. Viimeinen kirjain voidaan valita $\ell - 1$ eri tavalla.

(ii) Yhdistettynä kohtaan (i), mahdollisia eri pituuksia on nyt t kappaletta.

(iii) Huomautuksen 2.29 mukaan d-kriittisen sanan, joka ei sisällä potenssia k olevaa tekijää, pituus on $< dk$. Tällöin sovelletaan kohtaa (ii) ja merkitään siinä $t = dk$. □

Lause 2.31 (Shirshovin funktion tarkempi raja)
Olkoon Shirshovin Lemman 2.18 oletukset voimassa. Tällöin

$$\beta(\ell, k, d) \leq d^4k^2(\ell-1)\ell^{d-1}.$$

Todistus. Olkoon ω mielivaltainen pituudeltaan $> d^4k^2(\ell-1)\ell^{d-1}$ oleva sana. Edellisestä tarkastelusta nähdään, että hajottamalla tämä dk pituisiin tekijöihin, niin jokainen näistä tekijöistä sisältää d-kriittisen tekijän. Tästä saadaan vähintään $d^3k(\ell-1)\ell^{d-1}$ kappaletta erilisiä d-kriittisiä tekijöitä. Lauseen 2.30 kohdan (iii) mukaan vähintään d kappaletta näistä tekijöistä ovat samoja. Näin ollen, ω on Shirshov redusoituva valituilla parametrin arvoilla (vertaa Lemma 2.13). □

3 Shirshov ja affiinit PI-algebrat

Aikaisemmin käsiteltiin sanoja diskreettisinä kombinatorisina objekteina. Sanoja voidaan ajatella myös diskreettisinä algebrallisina ei-kommutatiivisina objekteina [9], minkä avulla voidaan tarkastella Shirshovin Lemman ja affiinien PI-algebrojen yhteyttä.

Esitetään tässä kappaleessa määritelmä affiinille PI-algeralle, sekä niiden teoriaa. Sovelluksena Shirshovin Lemmaan, tämä kappale tähtää Shirshovin Korkeuslauseeseen ja sen todistamiseen. Lauseella on paljon tärkeitä renkaisiin liittyviä sovelluksia, joista useimmat riippuvat Lauseen seurauksesta:

Olkoon $A = C\langle a_1, \ldots, a_m \rangle$ äärellisesti generoitu PI-algebra, missä C on kommutatiivinen rengas. Valitaan joukosta A tietty, myöhemmin esitettävä, äärellinen joukko alkioita, jotka ovat kokonaisia renkaan C suhteen. Tällöin algebra A on äärellisesti generoitu C-moduli.

Erikoisen asian tästä tekee se, että valittuja algebrallisia alkioita on ainoastaan äärellinen määrä, vaikkakin ne on valittu generoivasta joukosta.

3.1 Määritelmiä

Välitön yleistys vektoriavaruudelle on modulin käsite.

Määritelmä 3.1 Olkoon R rengas. Abelin ryhmää $(M, +)$ sanotaan *(vasemmaksi) R-moduliksi*, jos siinä on määritelty *modulikertolasku*

$$(r, m) \mapsto r \circ m = rm, \text{ missä } r \in R,\ m \in M,$$

joka täyttää seuraavat ehdot:

$RM0$. $rm \in M$ kun $r \in R$, $m \in M$,
$RM1$. $r(m_1 + m_2) = rm_1 + rm_2$ kun $r \in R$, $m_1, m_2 \in M$,
$RM2$. $(r_1 + r_2)m = r_1m + r_2m$ kun $r_1, r_2 \in R$, $m \in M$
$RM3$. $(r_1r_2)m = r_1(r_2m)$ kun $r_1, r_2 \in R$, $m \in M$
$RM4$. $1m = m$ kun $m \in M$.

Määritelmä 3.2 Olkoot M ja M' R-moduleja. Kuvausta

$$\Phi : M \to M'$$

sanotaan *R-modulihomomorfismiksi*, jos se täyttää seuraavat ehdot:

$MH1$. $\Phi(m_1 + m_2) = \Phi(m_1) + \Phi(m_2)$ aina, kun m_1, $m_2 \in M$,
$MH2$. $\Phi(rm_1) = r\Phi(m_1)$ aina, kun $r \in R$, $m_1 \in M$.

Modulin käsite on vektoriavaruuden välitön yleistys ja niiden teoria rakentuu samaan tapaan kuin vektoriavaruuksienkin. Erityisesti kaikki vektoriavaruuksia koskevat tulokset, joiden todistuksessa ei tarvita skalaarikunnan jakolaskua, pätevät myös moduleihin [6].

Määritelmä 3.3 C-modulin M sanotaan olevan *vapaa*, jos jokaista epätyhjää alkiota $m \in M$ kohden on olemassa yksikäsitteinen $n \in \mathbb{N}$ sekä yksikäsitteiset alkiot $c_1, c_2 \ldots, c_n \in C$ ja $x_1, x_2, \ldots, x_n \in X \subset M$, niin

$$m = c_1x_1 + c_2x_2 + \cdots + c_nx_n.$$

Määritelmässä 3.3 yksikäsitteisyys vaatimus on voimassa sekä modulin alkioilla, että myös renkaan alkioilla. Lisäksi voidaan todistaa, että jokaiselle joukolle X on olemassa vapaa C-moduli $F(X)$, joka toteuttaa seuraavan universaali ominaisuuden.

Lause 3.4 *Olkoot M mielivaltainen C-moduli sekä $\phi : X \to M$ mielivaltainen kuvaus. Tällöin on olemassa yksikäsitteinen C-modulihomomorfismi $\Phi : F(X) \to M$ siten, että $\Phi(x) = \phi(x)$ aina, kun $x \in X$.*

Algebralla tarkoitetaan systeemiä, joka koostuu epätyhjästä joukosta sekä äärellisestä määrästä operaattoreita.

Määritelmä 3.5 Järjestettyä paria (A, O) sanotaan *algebraksi*, missä A on jokin epätyhjä joukko alkioita ja O joukko (äärellisiä) operaattoreita. Yleensä algebrasta käytetään merkintää A parin (A, O) sijaan.

Määritelmä 3.6 Olkoon K mielivaltainen kunta. Joukko A on *(assosiatiivinen) algebra* kunnan K suhteen (lyhyemmin K*-algebra*) jos

(i) A on rengas,

(ii) Joukon A additiivinen ryhmä on K-moduli ja $a1 = a$ aina, kun alkio $a \in A$ sekä alkio 1 on joukon A ykkösalkio.

(iii) $\alpha \cdot (a_1 * a_2) = (\alpha \cdot a_1) * a_2 = a_1 * (\alpha \cdot a_2)$ aina, kun alkiot $\alpha \in K$ ja $a_1, a_2 \in A$

Määritelmässä 3.6 kuntaa K voidaan tarkastella myös kommutatiivisena ryhmänä C. Toisin sanoen (assosiatiivinen) algebra yli kommutatiivisen renkaan C on additiivinen Abelin ryhmä A, jolla on sekä renkaan, että C-modulin rakenteet siten, että renkaan kertolasku on C-bilineaarinen, toisin sanoen renkaan kertolasku on C-lineaarinen jokaiselle tekijälle:

$$c \cdot (a_1 * a_2) = (c \cdot a_1) * a_2 = a_1 * (c \cdot a_2)$$

aina, kun alkiot $c \in C$ ja $a_1, a_2 \in A$. Tarkempaa konstruktiota sekä teorioita on esitetty Jacobsonin kirjassa [10].

Olkoot jatkossa C kommutatiivinen rengas, jossa on ykkösalkio 1, K mielivaltainen kunta sekä Σ numeroituva määrä muuttujia. *Vapaa algebra* (muuttujien joukon Σ suhteen) on vapaa C-moduli, jonka kanta muodostuu kaikista sanoista aakkoston Σ suhteen. C-modulista saadaan C-algebra, kun joukon Σ tulo määritellään sanojen tulona luonnollisella tavalla, joten kahden eri alkion tulo on näin yksikäsitteisesti määritelty. Näin määriteltyä vapaata (assosiatiivista) C-algebraa merkitään $C\langle\Sigma\rangle$ ja sen alkioita kutsutaan *polynomeiksi*.

Nyt siis $C\langle\Sigma\rangle$ on vapaa C-moduli, jonka kanta muodostuu joukon Σ^* alkioista. Nyt jokainen alkio $f \in C\langle\Sigma\rangle$ voidaan siis kirjoittaa yksikäsitteisesti muodossa $\sum c_j h_j$, missä $h_j \in \Sigma^*$. Alkioita $h = c_j h_j$ kutsutaan polynomin f *monomeiksi*. Jos vielä polynomin korkeimman asteen kerroin on 1, niin polynomia sanotaan *pääpolynomiksi*.

Määritelmä 3.7 Olkoon $\deg_i h$ symbolin x_i esiintymien lukumäärä monomissa h, ja monomin *aste* $\deg h = \sum_i \deg_i h$. Polynomeille aste määritellään siinä esiintyvien monomien asteiden maksimiksi.

Huomautus 3.8 Sanojen joukossa aste tarkoittaa sanan pituutta.

Määritelmä 3.9 Muuttuja x_i *esiintyy* polynomissa f jos $\deg_i f > 0$; jos polynomissa f esiintyy ainoastaan muuttujat $x_1, \ldots, x_n$, niin sitä merkitään $f(x_1, \ldots, x_n)$.

Jokaiselle algebra homomorfismille $C\langle\Sigma\rangle \to A$, missä $x_i \mapsto a_i$ aina, kun $1 \leq i \leq n$, merkitään polynomin f kuvaa $f(a_1, \ldots, a_n)$.

Huomautus 3.10 Olkoot A mielivaltainen algebra kommutattivisen renkaan C suhteen sekä alkiot $\{a_1, \ldots, a_n\} \subseteq A$. Tällöin on olemassa yksikäsitteinen algebra homomorfismi $\Phi : C\langle\Sigma\rangle \to A$ siten, että $\Phi(x_i) = a_i$ aina, kun

$1 \leq i \leq n$. Määritellään siis

$$\Phi(x_{i_1} \cdots x_{i_n}) = a_{i_1} \cdots a_{i_n},$$

joka laajennetaan lineaarisesti koko algebraan $C\langle\Sigma\rangle$.

Määritelmä 3.11 Olkoot A mielivaltainen C-algebra sekä $f = f(x_1, \ldots, x_n) \in C\langle\Sigma\rangle$. Alkio f on C-algebran A *polynomi identiteetti*, jos

$$f(a_1, \ldots, a_n) = 0$$

kaikilla n-tuplilla $(a_1, \ldots, a_n) \in \Pi_{i=1}^{n} A$.

Määritelmä 3.12 Algebra A yli kommutatiivisen renkaan C on *polynomi identiteetti algebra renkaan C suhteen* (lyhyemmin PI-algebra yli renkaan C), jos on olemassa sellainen pääpolynomi $f \in C\langle\Sigma\rangle$, että alkio f on polynomi identiteetti algebrassa A.

Määritelmä 3.13 PI-algebra A on *PI-astetta d*, jos algebra A toteuttaa astetta d olevan polynomi identiteetin.

Oletetaan tässä luvussa, että A on PI-algebra yli kommutatiivisen renkaan C. Yksiä tärkeimpiä esimerkkejä PI-algebroista ovat matriisialgebra $\mathcal{M}_n(C)$ sekä äärellisulotteiset algebrat yli kunnan [3].

Esimerkki 3.14

(i) Jokainen kommutatiivinen algebra toteuttaa identiteetin $f = [x_1, x_2] = x_1x_2 - x_2x_1$.

(ii) Ensimmäisiä tutkimusten kannalta mielenkiintoinen algebran identiteetti on *Wagnerin identiteetti* matriisialgebralle $\mathcal{M}_2(K)$ [16]. Olkoot

matriisi

$$a_0 = \begin{pmatrix} p & q \\ r & -p \end{pmatrix}$$

ja $a, b, c \in \mathcal{M}_2(K)$ mielivaltaiset matriisit. Tällöin matriisi

$$a_0^2 = \begin{pmatrix} p^2 + qr & 0 \\ 0 & p^2 + qr \end{pmatrix}$$

on diagonaalimatriisi, joten se kommutoi kaikkien matriisien kanssa algebran $\mathcal{M}_2(K)$ suhteen. Olkoon $\mathrm{tr}(a)$ matriisin a jälkifunktio, toisin sanoen matriisin lävistäjä alkioiden summa. Koska nyt

$$\begin{aligned} [a,b] &= \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}\begin{pmatrix} y_1 & y_2 \\ y_3 & y_4 \end{pmatrix} - \begin{pmatrix} y_1 & y_2 \\ y_3 & y_4 \end{pmatrix}\begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \\ &= \begin{pmatrix} x_2y_3 - y_2x_3 & \cdots \\ \cdots & x_3y_2 - y_3x_2 \end{pmatrix} = \begin{pmatrix} P & Q \\ R & -P \end{pmatrix}, \end{aligned}$$

missä alkiot P, Q ja R ovat polynomeja sekä $\mathrm{tr}([a,b]) = 0$ kommutatiivisen algebran suhteen, niin $[[a,b]^2, c] = 0$ aina, kun $a, b, c \in \mathcal{M}_2(K)$. Tästä seuraa, että

$$(x_1x_2 - x_2x_1)^2x_3 - x_3(x_1x_2 - x_2x_1)^2$$

on algebran $\mathcal{M}_2(K)$ identiteetti.

(iii) Olkoon $p \in \mathbb{P}$. Fermat'n pieni lause sanoo, että jokainen $n = p^t$ alkioinen kunta K toteuttaa yhtälön $a^n = a$ aina, kun $a \in K$. Toisin sanoen $x_1^n - x_1$ on kunnan K identiteetti.

(iv) Jokainen Boolean algebra toteuttaa identiteetin $x^2 - x$.

PI-algebrojen kanssa on tarpeen määritellä tietyn tyyppisiä polynomeja. Sanotaan, että polynomi $f(x_1, \ldots, x_n)$ on *homogeeninen* kohdassa x_i jos muuttujalla x_i on sama aste jokaisessa polynomin f monomissa. Polynomi f on *homogeeninen* jos se on homogeeninen jokaisella muuttujalla.

Määritelmä 3.15 Monomi h on *lineaarinen* kohdassa x_i, jos $\deg_i h = 1$. Polynomi f on *lineaarinen* kohdassa x_i, jos jokainen polynomin f monomi on lineaarinen kohdassa x_i. Polynomi $f(x_1, \ldots, x_n)$ on *multilineaarinen*, jos f on lineaarinen kaikilla $x_1, \ldots, x_n$. Toisin sanoen f on *n-lineaarinen*.

Olkoon $f(x_1, \ldots, x_n)$ multilineaarinen polynomi. Valitaan tästä polynomista mielivaltainen nollasta eroava monomi h. Nimeämällä muuttujat sopivasti uudestaan voidaan olettaa, että $h = \alpha x_1 x_2 \cdots x_n$, missä $\alpha \in C$ ja C on kommutatiivinen rengas. Näin ollen multilineaarisen polynomin yleinen muoto on

$$f(x_1, \ldots, x_n) = cx_1 x_2 \cdots x_n + \sum_{1 \neq \sigma \in S_n} \alpha_\sigma x_{\sigma(1)} x_{\sigma(2)} \cdots x_{\sigma(n)}.$$

Jos C on lisäksi kunta, voidaan edellinen yhtälö jakaa puolittain alkiolla c ja olettaa, että $c = 1$.

3.2 Polynomi identiteetti vs. multilineaarinen identiteetti

Nyt tulee esiin kysymys, onko polynomi identiteettien ja multilineaaristen identiteettien välillä jokin yhteys. Vastausta haettaessa aloitetaan *multilinearisoinnilla*, jota kuvataan seuraavaksi.

Määritelmä 3.16 (multilinearisointi) Oletetaan, että polynomissa $f(x_1, \ldots, x_m)$ muuttujan x_i aste on $n_i > 1$. Tarkastellaan muuttujaa x_i, ja

määritellään *osittainen linearisointi*

$$\begin{aligned}&\triangle_i f(x_1,\ldots,x_{i-1},x_i,x_i',x_{i+1},\ldots,x_m) = \\ &\quad f(\ldots,x_i+x_i',\ldots)-f(\ldots,x_i,\ldots)-f(\ldots,x_i',\ldots),\end{aligned}$$

missä x_i' on uusi muuttuja.

Selvästi $\triangle_i f$ on algebran A identiteetti, jos f on sellainen, koska uusi muuttuja otetaan myös algebrasta A. Kuitenkin kaikki monomit, joissa muuttuja x_i on astetta n_i, häviää osittaisessa linearisoinnissa $\triangle_i f$, koska yhtälön

$$(x_i+x_i')^{n_i}-x_i^{n_i}-x_i'^{n_i} = x_i^{n_i}+x_i'^{n_i}+\cdots-x_i^{n_i}-x_i'^{n_i}.$$

maksimi aste on pienempi kuin n_i. Jäljelle jäävissä monomeissa muuttuja x_i' korvaa muuttujan x_i joissakin tapauksissa, mutta ei kaikissa. Näin ollen näille monomeilla muuttujan x_i aste on $< n_i$ ja maksimi aste on $n_i - 1$.

Huomautus 3.17 Koska edellinen proseduuri on hyvin tärkeä, nimetään muuttujia hieman paremmin. Merkitään muuttujaa x_i muuttujalla x_1 sekä muita muuttujia x_j muuttujalla y_j. Merkitään myös astetta n_i yksinkertaisemmin asteella n.

(i) Nyt määritelmän 3.16 polynomi on $f(x_1; y_1, \ldots, y_m)$ ja osittainen linearisointi

$$\begin{aligned}&\triangle_1 f(x_1,x_2;y_1,\ldots,y_m) = \\ &\quad f(x_1+x_2;y_1,\ldots,y_m)-f(x_1;y_1,\ldots,y_m)-f(x_2;y_1,\ldots,y_m),\end{aligned}$$

missä x_2 on uusi muuttuja.

(ii) Toistamalla tämä proseduuri $n-1$ kertaa, ottamalla joka kerralla uusi muuttuja x_i, saadaan kohdissa $x_1,\ldots,x_n$ lineaarinen polynomi $\bar{f}(x_1,\ldots,x_n;y_1,\ldots,y_m)$, joka säilyttää ainoastaan ne monomit h, joissa muuttuja x_1 oli alunperin astetta n. Jokaista tällaista polynomin f

monomia h kohden polynomissa $\bar{f}$ on $n!$ kappaletta monomeita, jotka palautuu takaisin monomiin h, kun jokainen muuttuja x_i korvataan muuttujalla x_1. Nyt aina, kun f on homogeeninen kohdassa x_1, niin

$$\bar{f}(x_1, \ldots, x_1; y_1, \ldots, y_m) = n! f(x_1; y_1, \ldots y_m). \tag{1}$$

Jos karakteristika on 0, niin alkiolla $n!$ on olemassa käänteisalkio. Näin ollen polynomi f on *palautettu* polynomista $\bar{f}$. Polynomia $\bar{f}$ sanotaan polynomin f *linearisoinniksi* kohdassa x_1.

(iii) Toistamalla linearisointi jokaiselle polynomin f muuttujalle saadaan multilineaarinen polynomi, jota kutsutaan polynomin f *multilinearisoinniksi*.

Jos karakteristika ei ole nolla kohtaa (ii) kannattaa hieman parantaa. Kirjoitetaan

$$\triangle_1 f = \sum_{j=1}^{n-1} f_j(x_1, x_2; y_1, \ldots, y_m),$$

missä $\deg_1 f_j = j$ (sekä näin ollen $\deg_2 f_j = n-j$). Tällöin jokaiselle indeksille j saadaan $\bar{f} = \bar{f}_j$, toisin sanoen, polynomi $\bar{f}$ saadaan tekemällä multilinearisointi prosessi mille tahansa polynomille f_j, ensin muuttujalle x_1 ja sitten muuttujalle x_2. Näin yhtälö (1) saadaan muotoon

$$\bar{f}(x_1, \ldots, x_1, x_2, \ldots, x_2; y_1, \ldots, y_m) = j!(n-j)! \triangle_1 f.$$

Esimerkki 3.18 Otetaan muutama esimerkki linearisoinnista:

(i) $\triangle_1(x_1^2 + x_1) = (x_1 + x_2)^2 + (x_1 + x_2) - (x_1^2 + x_1) - (x_2^2 + x_2) = x_1x_2 + x_2x_1$.

(ii) Kun funktioon x_1^n sovelletaan operaatiota $\triangle_1$ $(n-1)$-kertaa, saadaan $\sum_{\pi \in S_n} x_{\pi(1)} \cdots x_{\pi(n)}$

Määritelmä 3.19 Olkoon $\mathrm{id}(A)$ kaikkien PI-algebran A identiteettien joukko.

Huomautus 3.20 *Vandermonde matriisi* (α_u^{j-1}) on muotoa

$$\begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{m-1} \\ 1 & \alpha_2 & \cdots & \alpha_2^{m-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_m & \cdots & \alpha_m^{m-1} \end{pmatrix},$$

missä alkiot α_i ovat kunnan K erillisiä alkioita. Tällöin matriisilla on käänteismatriisi.

Lause 3.21 *Olkoon K ääretön kunta. Tällöin jokainen algebran A identiteetti voidaan korvata homogeenisillä identiteetteillä; lisäksi jokainen algebran A identiteetti voidaan kirjoittaa ekvivalentisti polynomien summana, joka muodostuu homogeenisista identiteeteistä.*

Todistus. Olkoon $f(x_1, \ldots, x_m) \in \mathrm{id}(A)$. Merkitään $f = \sum_{u=0}^{k} f_u$, missä jokainen f_u on sellaisten polynomin f monomien summa, jotka ovat astetta u kohdassa x_1. Valitaan mielivaltaiset erilliset alkiot $\alpha_0, \ldots, \alpha_k \in K$. Tällöin kaikilla $a_i \in A$

$$0 = f(\alpha_u a_1, \ldots, a_m) = \sum_{j=0}^{k} \alpha_u^j f_u(a_1, \ldots, a_m);$$

Olkoon v pystyvektori jonka alkiot ovat $f_0(a_1, \ldots, a_m), \ldots, f_k(a_1, \ldots, a_m)$. Näin saadaan matriisiyhtälö $(\alpha_u^{j-1})v = 0$, missä matriisi (α_u^{j-1}) on Vandermonden matriisi, jolla on käänteismatriisi, koska alkiot α_i ovat erillisiä. Näin ollen matriisiyhtälöllä on yksikäsitteinen ratkaisu $f_u(a_1, \ldots, a_m) = 0$ aina, kun $0 \leq u \leq k$. Jokainen polynomi f_u on siis algebran A identiteetti. Toistetaan sama proseduuri jokaiselle muuttujalle x_i, joten polynomi f voidaan korvata homogeenisilla identiteeteillä. $\square$

Lause 3.22 *Jos A on PI-algebra yli kunnan K, jonka karakteristika on nolla, niin joukon $\mathrm{id}(A)$ määrittelee multilineaariset identiteetit; toisin sanoen, algebra A toteuttaa mielivaltaisen identiteetin tarkalleen silloin, kun A toteuttaa multilineaarisen identiteetin*

Todistus. Olkoon polynomi f algebran A identiteetti. Tarkastellaan linearisointi prosessia $\triangle_i$ uudestaan. Olkoon $\mathcal{A}$ PI-algebran A multilineaaristen identiteettien joukko. Palautetaan polynomi f joukon $\mathcal{A}$ polynomeista. Lauseen 3.21 perusteella polynomi f voidaan korvata summana homogeenisiä polynomeja, jotka myös ovat algebran A identiteettejä. Nyt Huomautuksen 3.17 kohdan (ii) mukaan f saadaan palautettua polynomeista $\mathcal{A}$. $\square$

Edellisen lauseen perusteella riittää tarkastella algebrojen A_1 ja A_2, joiden karakteristika on nolla, multilineaarisia identiteettejä, jotta voidaan todeta, että $\mathrm{id}(A_1) = \mathrm{id}(A_2)$.

Huomautus 3.23 Jos karakteristika on $p \neq 0$ tilanne on hieman erilainen, koska identiteetit eivät välttämätttä ole multilineaarisista johdettuja. Kuitenkin Lausetta 3.22 voidaan hieman tarkentaa. Voidaan nimittäin osoittaa [3], jos kunnan K karakteristika on mielivaltainen, tällöin jos algebra A toteuttaa mielivaltaisen polynomi identiteetin, niin algebra A toteuttaa myös tämän multilinearisoinnin; toisin sanoen kaikille karakteristikoille identiteetin multilinearisointi on myös identiteetti.

3.3 Sana affiinissa algebrassa

Määritelmä 3.24 Algebra A on *affiini K-algebra*, jos A on äärellisesti generoitu algebra kunnan K suhteen; toisin sanoen affiini algebra on muotoa $A = K\langle a_1, \ldots, a_\ell \rangle$.

Olkoon $A = C\langle a_1, \ldots, a_\ell \rangle$ affiini algebra kommutatiivisen renkaan C suhteen. Valitaan aakkosto $\Sigma = \{x_1, \ldots, x_\ell\}$, ja muodostetaan kaikkien sanojen joukko Σ^*, joka on äärellisesti generoitu monoidi aakkoston Σ suhteen. Olkoon $\omega \in \Sigma^*$ mielivaltainen sana ja merkitään $\bar{\omega}$ sanan ω kuvaa Huomautuksen 3.10 homomorfismin $\Phi : C\langle\Sigma\rangle \to A$ suhteen ja kutsutaan $\bar{\omega}$ *sanaksi algebrassa* A. Tarkastellaan sanaa affiinissa algebrassa ja näytetään polynomi identiteettien yhteys d-jaollisuuteen.

Määritelmä 3.25 Olkoon $W \subseteq \Sigma^*$ sanojen joukko. Merkitään $\bar{W} = \{\bar{\omega} \mid \omega \in W\}$ *sanojen joukkoa algebrassa* A kuvauksen Φ suhteen.

Joukko $\bar{W}$ *virittää* algebran A osajoukon S, jos jokainen alkio osajoukossa S voidaan kirjoittaa muodossa

$$\sum_{\omega \in W} c_\omega \bar{\omega},$$

missä $c_\omega \in C$.

Määritelmä 3.26 Sanaa $\bar{\omega}$ sanotaan A-*minimaaliseksi*, jos mitkään sanan $\omega \in W$ leksikograaffisesti pienempien sanojen kuvat eivät viritä sanaa $\bar{\omega}$.

3.4 Shirshovin korkeus

Joukossa $\Sigma = \{x_1, \ldots, x_\ell\}$ kaikkien m-pituisten sanojen lukumäärä on ℓ^m. Selvästi myös sanojen, joiden pituus on $\leq m$, lukumäärä on

$$\ell^m + \ell^{m+1} + \cdots + 1 = \frac{\ell^{m+1} - 1}{\ell - 1}$$

Määritelmä 3.27

(i) Olkoon $k_i \geq 1$. Sana s on *korkeutta* μ *oleva Shirshovin sana* sanojen joukon $W \subset \Sigma^*$ suhteen, jos $s = u_{i_1}^{k_1} \cdots u_{i_\mu}^{k_\mu}$, missä $u_i \in W$ kaikilla indeksin i arvoilla. Indekseille on sallittua, että $i_j = i_{j'}$, vaikka $j \neq j'$.

(ii) Olkoon $\widehat{W}_\mu$ kaikkien joukon W Shirshovin sanojen joukko, joiden korkeus on $\leq \mu$. Algebralla A on *korkeus* μ joukon W suhteen, jos $\widehat{W} = \{\bar{\omega} \mid \omega \in \widehat{W}_\mu\}$ virittää algebran A. Tällöin joukon $\widehat{W}$ sanotaan olevan *Shirshovin A-kanta.*

Tavoitteena nyt on löytää mielivaltaiselle sanalle d-kappaletta sellaisia tekijöitä, jotka mitkään eivät ole toistensa aitoja prefiksiä. Seuraavassa huomautuksessa on yksi tällainen menetelmä.

Huomautus 3.28 Olkoot u ja v sanoja, joista kumpikaan ei ole toisen aito prefiksi. Tällöin $u^{d-1}v$ sisältää d kappaletta tekijöitä, joille:

(i) Jos $v <_l u$, niin $v <_l uv <_l u^2v <_l \cdots <_l u^{d-1}v$.

(ii) Jos $v >_l u$, niin $v >_l uv >_l u^2v >_l \cdots >_l u^{d-1}v$.

Joten Lauseen 2.13 mukaan jokainen sana, missä $u^{d-1}v$ esiintyy moninkertana vähintään d kertaa, on d-jaettu.

Lause 3.29 (Shirshovin korkeuslause) *Olkoon $A = C\langle a_1, \ldots, a_\ell\rangle$ affiini PI-algebra, minkä PI-aste on d. Olkoon W joukko sanoja, joiden pituudet ovat $\leq d$. Tällöin $\widehat{W}$ on Shirshovin A-kanta; algebran A korkeus on $\leq (d^2\ell^{2d} + 1)(\lceil \frac{\beta(\ell,2d,d)}{d} \rceil + 2)$ joukon W suhteen. Toisin sanoen joukko $\{\bar{w}_1^{k_1} \cdots \bar{w}_\mu^{k_\mu} \mid w_i \in W, k_i \geq 0\}$ virittää PI-algebran A.*

Todistus. Olkoot $\beta = \beta(\ell, 2d, d)$ Shirshovin lemman mukaiset sekä $\beta' = \lceil \frac{\beta}{d} \rceil$. Lisäksi olkoon

$$\mu = \mu(\ell, d) = (d^2\ell^{2d} + 1)(\beta' + 2).$$

Voidaan olettaa, että sana ω on d-jaoton. Todistetaan, että sanan ω korkeus yli sanojen $\{u \mid |u| < d\}$ on korkeintaan μ.

Määritellään prosessi, jolla jaetaan sana ω tietynlaisiin tekijöihin. Tämä johtaa myöhemmin yo. väitteeseen.

(1) Jos $|\omega| < \beta + d$ lopetetaan siihen.

(2) Oletetaan, että $|\omega| \geq \beta + d$ ja merkitään $\omega = \omega'\omega''$, missä $|\omega'| \geq \beta$ ja $\omega'' = d$. Näin ollen ω' on myös d-jaoton. Nyt Shirshovin Lemman 2.18 mukaan ω' sisältää muotoa $u_1^{k_1'}$ olevan tekijän, missä $k_1' \geq 2d$. Toisin sanoen sanan ω' prefiksi on $s_0 u_1^{k_1'}$.

(3) Merkitään $\omega' = s_0 u_1^{k_1} \omega^*$, missä k_1 on maksimaalinen; tällöin $k_1 \geq 2d$ ja $|s_0| < \beta$.

$(3)_{(a)}$ Jos $|\omega^*| < |u_1|$, lopetetaan tähän.

$(3)_{(b)}$ Muulloin merkitään $\omega^* = v_1\omega_1^*$, missä $|v_1| = |u_1|$. Tällöin $\omega = s_0 u_1^{k_1} v_1 \omega_1$, missä u_1 sekä v_1 ovat vertailukelpoisia.

Tähän lopetetaan ensimmäinen askel.

Toistetaan sama prosessi sanalle ω_1: Jos $|\omega_1| < \beta + d$ lopetetaan. Muuten jatketaan samaan tapaan kuin edellisessä: $\omega_1 = s_1 u_2^{k_2} v_2 \omega_2$, missä $|s_1| < \beta$, $|u_2| = |v_2| \leq d$, $k_2 \geq 2d$ sekä u_2 ja v_2 ovat vertailtavissa. Jatketaan samaa prosessia kunnes saadaan

$$\omega = s_0 u_1^{k_1} v_1 s_1 u_2^{k_2} v_2 s_2 u_3^{k_3} v_3 \cdots s_{t-1} u_t^{k_t} \omega_t',$$

missä $|\omega_t'| < \beta + d$. Edellisessä lisäksi $|s_j| < \beta$, $k_j \geq 2d$, $|u_j| = |v_j| \leq d$ sekä sanat u_j ja v_j ovat vertailtavissa, kaikilla j.

Ajatellaan tätä sanaa jonona tekijöitä, joiden pituus on $\leq d$. Tätä varten partitioidaan jokainen s_i korkeintaan d pituisiksi tekijöiksi (jokaisessa sanassa s_i näitä tekijöitä on β' kappaletta). Sanan ω korkeuden päättelyssä voidaan jättää potenssit k_i huomioimatta ja laskea yhteen luvut β' jokaista sanaa s_i kohti sekä luvun 1 kaikkia sanoja u_i ja v_i kohti. Näin ollen sanan ω korkeus on korkeintaan

$$t\beta' + t + (t-1) + \beta' + 1 < (t+1)(\beta' + 2).$$

Toisaalta, viimeiset $|u_i| + |v_i| \leq 2d$ kappaletta kirjaimia määrittelee termin $u_i^d v_i$ (sillä ne määrittävät sanat u_i ja v_i); nyt koska $|u_i| \leq d$, niin termille $u_i^d v_i$ on vähemmän kuin ℓ^{2d} kappaletta erilaisia mahdollisuuksia aina, kun pituus $|u_i|$ annettu, ja kun lasketaan pituuden kaikki d eri mahdollisuudet, saadaan termille $u_i^d v_i$ kokonaisuudessaan vähemmän kuin $d\ell^{2d}$ kappaletta mahdollisuuksia.

Jos nyt $t \geq d^2\ell^{2d} = d(d\ell^{2d})$, jokin muotoa $u^d v$ olevan sanan täytyy toistua d kertaa sanassa ω. Tämä on ristiriidassa sen kanssa, että sana ω on d-jaoton (Huomautuksen 3.28 mukaan). Näin ollen $t < d^2\ell^{2d}$, josta seuraa, että sanan ω korkeus on pienempi kuin $(d^2\ell^{2d} + 1)(\beta' + 2) = \mu$. $\square$

4 Sovelluksia PI-algebroihin

Tarkastellaan kahta algebrallisesti tärkeää sovellusta Shirshovin teorioille; Kurochin ja Levitzkyn ongelmat sekä myöhemmin määriteltävä Jacobsonin radikaalin nilpotenttisuus, joista jälkimmäinen esitetään ilman todistuksia.

Motivaatio polynomi identiteettien käytölle on tarjota eräänlainen vähennys proseduuri, missä sanat voidaan korvata niiden lineerikombinaatioilla, jotka ovat leksikograaffisesti pienempiä.

Lause 4.1 (Shirshov) *Olkoon affiinissa algebrassa A astetta d oleva polynomi identiteetti. Tällöin jokainen d-jaettu sana $\omega \in \Sigma^*$ voidaan lausua algebrassa A sanan ω d-jaon blokkien permutaatioiden, toisin sanoen uudelleen järjestettyjen d-jaon tekijöiden, lineaarikombinaatioina, missä permutoidut sanat ovat $<_\ell \omega$.*

Todistus. Koska algebra A on PI-algebra, se toteuttaa myös multilineaarisen identiteetin

$$x_1 \cdots x_d - \sum_{\sigma \neq 1, \sigma \in S_d} \alpha_\sigma x_{\sigma(1)} \cdots x_{\sigma(d)};$$

toisin sanoen kaikilla alkoilla $a_i \in A$

$$a_1 \cdots a_d - \sum_{\sigma \neq 1, \sigma \in S_d} \alpha_\sigma a_{\sigma(1)} \cdots a_{\sigma(d)} = 0.$$

Tällöin yllä oleva yhtälö toteutuu erityisesti affiinin algebran sanalla $\bar{\omega} = \bar{\omega}_1 \cdots \bar{\omega}_d$:

$$\bar{\omega}_1 \cdots \bar{\omega}_d = \sum_{\sigma \neq 1, \sigma \in S_d} \alpha_\sigma \bar{\omega}_{\sigma(1)} \cdots \bar{\omega}_{\sigma(d)}.$$

Summassa olevat sanat ovat kaikki leksikograaffisesti pienempiä kuin $\omega_1 \cdots \omega_d$, mikä todistaa väitteen. $\square$

Edellisen lauseen perusteella mielivaltainen A-minimaalinen sana on d-jaoton.

Huomautus 4.2 Kun polynomi identiteettiä käytetään d-jaettujen sanojen pienentämiseen leksikograaffisen järjestyksen suhteen, se ei muuta sanoissa käytettyjä kirjaimia vaan ainoastaan järjestää ne uudelleen.

4.1 Kurochin ja Levitzkyn ongelmat

Algebran A alkiota x sanotaan *nilpotentiksi*, jos on olemassa vakio $k \in \mathbb{N}$ niin, että $x^k = 0$. *Nil algebralla* tarkoitetaan algebraa, joka sisältää ainoastaan nilpotentteja alkioita. Algebra taas on *nilpotentti*, jos sillä on seuraava ominaisuus:

$$\text{On olemassa sellainen alkio } n \in \mathbb{N}, \text{ että } A^n = 0.$$

Määritelmä 4.3 Algebran alkio x on *kokonainen* kunnan K suhteen, jos on olemassa sellaiset alkiot $a_1, \ldots, a_{n-1} \in K$, että

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1} x = 0.$$

Shirshovin Lemman avulla päästään nyt tarkastelemaan muutamaa tärkeää algebrallista ongelmaa:

(i) *Levitzkin ongelma*: Onko äärellisesti generoitu algebra, jonka jokainen alkio on nilpotentti, aina nilpotentti?

(ii) *Kuroschin ongelma*: Onko äärellisesti generoitu K-algebra, jonka jokainen alkio on kokonainen algebran K suhteen, aina äärellisesti generoitu K-moduli?

Molemmissa ongelmissa vastaus on kielteinen [22], [23]. Kuitenkin PI-algebran tapauksessa vastaus molempiin ongelmiin on kyllä. Tällöin oletusta voidaan myös jopa heikentää.

Lause 4.4 *Olkoon A äärellisesti generoitu K-algebra, generaattoreina alkiot $a_1, \ldots, a_\ell$. Oletetaan myös, että A toteuttaa astetta d olevan polynomi identiteetin.*

(i) Jos nyt kaikilla indeksin $i \in [1, \ell]$ arvoilla, alkioiden a_i mielivaltainen tulo, jossa on korkeintaan d kappaletta alkioita a_i, on nilpotentti, niin K-algebra A on nilpotentti.

(ii) Jos nyt kaikilla indeksin $i \in [1, \ell]$ arvoilla, alkioiden a_i mielivaltainen tulo, jossa on korkeintaan d kappaletta alkioita a_i, on kokonainen algebran K suhteen, niin K-algebra A on äärellisesti generoitu K-moduli.

Todistus. Algebra A toteuttaa multilineaarisen identiteetin. Olkoot $\Sigma = \{x_1, \ldots, x_\ell\}$ täydellisesti järjestetty aakkosto ja

$$\phi : K_+\langle\Sigma\rangle \to A$$

algebra homomorfismi, missä $\phi(x_i) = a_i$ sekä $J = \ker(\phi)$. Olkoot lisäksi k sellainen vakio, että $k \geq 2d$ sekä $\beta = \beta(\ell, k, d)$ Lemmassa 2.18 oleva vakio.

Kohdan (i) todistus. Olkoon $\phi(u)^k = 0$, kaikille sanoille $u \in \Sigma^+$, joiden pituus on korkeintaan d. Jokainen vähintään pituudeltaan β oleva sana $\omega \in \Sigma^*$ sisältää joko potenssia p olevan tekijän u, $0 < |u| \leq d$, tai on d-jaollinen. Jälkimmäisessä tapauksessa Lauseen 4.1 mukaan ω on lineaarikombinaatio (modulo J) sanoista, jotka ovat samanpituisia kuin ω ja pienempiä kuin ω leksikograaffisessa järjestyksessä. Koska näitä sanoja on ainoastaan äärellinen määrä, päätellään induktiivisesti, että ω on saman pituisten sanojen lineaarikombinaatio (modulo J), joista jokainen sisältää potenssia k olevan tekijän u^k, missä $0 < |u| \leq d$. Näin ollen $\phi(\omega) = 0$ ja algebra A on nilpotentti. Näin kohta (i) on todistettu.

Kohdan (ii) *todistus.* Todistetaan tämä Shirshovin Korkeuslauseen 3.29 seurauksena, jonka mukaan joukko $\{\bar{w}_1^{k_1} \cdots \bar{w}_\mu^{k_\mu} \mid w_i \in W, k_i \geq 0\}$ virittää PI-algebran A.

Jos nyt mielivaltainen sana $\bar{\omega}$ on kokonainen kunnan K suhteen aina, kun $\omega \in W \subset \Sigma^*$, missä sanojen joukko W vastaa Shirshovin Korkeuslauseen 3.29 vastaavaa joukkoa. Nyt $\bar{\omega}$ toteuttaa pääpolynomi yhtälön $\phi(\omega)^{k_\omega} = a_1\phi(\omega)^{k_\omega - 1} + \cdots + a_{k_\omega - 1}\phi(\omega)$, joillakin $a_i \in K$. Tällöin jokainen sana $\bar{\omega}^{k_\omega}$ voidaan ekvivalentisti korvata pienemmällä potenssilla, joten algebra A on äärellisesti generoitu K-moduli. $\square$

Lasketaan edellisessä lauseessa kohdan (ii) määräämä alkioiden lukumäärä, jolloin algebra on K-moduli. Todistuksen mukaan sanojen, joiden korkeus on μ, lukumäärä joukon W suhteen, jossa jokainen eksponentti on $\leq k$ on todella iso:

$$((k+1)|W|)^\mu,$$

missä $|W| = \frac{\ell^{d+1}-1}{\ell-1}$. Tämän takia todistetaan edellisen lauseen kohta (ii) erikseen, ilman Lauseen 3.29 käyttöä, jolloin saadaan parempi raja.

Todistus. (Lause 4.4 (ii)) Olkoot m maksimaalinen aste, jolle jokainen äärellisen joukon $\{\bar{\omega} \mid \omega \in W\}$ alkio on kokonainen sekä $k = \max(d, m)$. sekä $\beta = \beta(\ell, k, d)$ Lemmassa 2.18 oleva vakio. Nyt jokainen vähintään pituudeltaan β oleva sana $\omega \in \Sigma^*$ sisältää joko potenssia p olevan tekijän u, $0 < |u| \leq d$, tai on d-jaollinen. Jälkimmäisessä tapauksessa Lauseen 4.1 mukaan ω on lineaarikombinaatio sanoista, jotka ovat samanpituisia kuin ω ja leksikograaffisesti pienempiä kuin ω. Näitä sanoja on äärellinen määrä, joten iduktiivisesti pääteltynä ω on saman pituisten sanojen lineaarikombinaatio, joista jokainen sisältää potenssia k olevan tekijän u^k, missä $0 < |u| \leq d$. Koska sanojen kokonaisuutta voidaan käyttää pienentämään potenssia k,

niin Lemman 2.18 mukaan sana $\bar{\omega}$ on A-minimaalinen tarkalleen silloin, kun $\omega \leq \beta$. $\square$

Huomautus 4.5 Edellisestä todistuksesta seuraa, että Lauseessa 4.4 (ii) termien lukumäärä, mikä tarvitaan virittämään algebra A kunnan K suhteen, on $(\ell^{m+1} - 1)/(\ell - 1)$, missä $m = \beta(\ell, k, d)$.

4.2 Shirshov ja Jacobsonin radikaali

Shirshovin Korkeuslauseen avulla voidaan todistaa myöhemmin määriteltävä Jacobsonin radikaalin nilpotenttisuus kaikille karakteristikoille. Esitetään tässä tarvittavat tulokset ilman todistuksia. Todistuksiin voi tutustua tarkemmin kirjassa [3].

Määritelmä 4.6 Rengas R toteuttaa *ACC (Ascending Chain Condition)* ominaisuuden, jos jokainen sen ihanteiden I_i mielivaltainen ketju

$$I_1 \subset \cdots \subset I_n \subset \cdots ,$$

on äärellinen. Toisin sanoen, on olemassa positiivinen vakio $k \in \mathbb{Z}_+$ siten, että

$$I_k = I_{k+1} = \cdots$$

Määritelmä 4.7 Olkoot R mielivaltainen rengas, joka toteuttaa ACC ominaisuuden. Kaikkien renkaan R maksimaalisten ideaalien leikkausta kutsutaan renkaan R *Jacobsonin radikaaliksi* $J(R)$.

Razmyslov todisti [21], että Jacobsonin radikaali $J(A)$, affiinille algebralle A, on nilpotentti aina, kun A toteuttaa seuraavaksi esitettävän *Capellin identiteetin.*

Määritelmä 4.8 Olkoon $\sigma \in S_n$, missä S_n on symmetrinen ryhmä. Määritellään permutaation σ *merkki*, jota merkitään $\mathrm{sgn}(\sigma)$:

$$\mathrm{sgn}(\sigma) = \begin{cases} +1 & \text{, jos permutaatio } \sigma \text{ sisältää parillisen määrän inversioita,} \\ -1 & \text{, jos inversioiden määrä on pariton.} \end{cases}$$

Määritelmä 4.9 Polynomia

$$c_n = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) x_{\sigma(1)} x_{n+1} x_{\sigma(2)} x_{n+2} \cdots x_{2n-1} x_{\sigma(n)} x_{2n},$$

sanotaan *Capellin polynomiksi* ja se esitetään usein muodossa

$$c_n(x; y) = c_n(x_1, \ldots, x_n, y_1, \ldots, y_n) = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) x_{\sigma(1)} y_1 x_{\sigma(2)} y_2 \cdots x_{\sigma(n)} y_n,$$

josta voidaan helpommin erottaa permutoidut muuttujat kiinnitetyistä.

Lause 4.10 (Razmyslov) *Olkoon A affiini algebra, joka toteuttaa Capelli identiteetin c_{n+1}. Tällöin $J(A)$ on nilpotentti.*

Kemer todisti lisäksi [11] karakteristikalle 0, että kaikki affiinit algebrat toteuttavat Capellin identiteetin. Shirshovin Korkeuslauseen avulla voidaan todistaa Kemerin lause kaikille karakteristikoille [3].

Lause 4.11 (Kemer) *Jokainen affiini PI-algebra $A = K\langle a_1 \ldots, a_\ell \rangle$, jonka PI-aste on d, toteuttaa Capelli identiteetin c_n, jossa n riippuu ainoastaan luvuista ℓ ja d.*

Näin ollen kaikille karakteristikoille affiinin algebran Jacobsonin radikaali on nilpotentti. Braun todisti myös saman [22] käyttäen täysin erilaista lähestymistapaa.

Lause 4.12 (Razmyslov-Kemer-Braun) *Mielilvaltaiselle affiinille PI-algebralle (yli kunnan) Jacobson radikaali on nilpotentti.*

Kirjallisuutta

[1] M. Lothaire: *Combinatorics on Words*. Cambridge University Press 1983, 1997.

[2] W. Wagner: *Uber die Grundlagen der projektiven Geometrie und allgemeine Zahlsysteme*. Math. Z. 113, s. 528-567, (1937).

[3] A. Kanel-Belov and L. H. Rowen: *Computational aspects of polynomial identities*. A K Peters, Ltd, 2005.

[4] A. R. Kemer: *Nonmatrix varieties with polynomial growth and finitely generated PI-algebras*. Ph.D. Dissertation, Novosibirsk 1981.

[5] J. Karhumäki: *Ramsey theory and related topics*. Fall 2004, http://www.math.utu.fi/en/home/karhumak/Ramsey.pdf

[6] D. S.Dummit and R. M. Foote: *Abstract algebra -third edition*. John Wiley and Sons, inc. 2004.

[7] L. H. Rowen: *Ring Theory II*, Acad. Press Pure and Applied Math., Vol. 128, New York (1988).

[8] L.H. Rowen: *Polynomial identities in ring theory*. Acad. Press Pure and applied math., Vol 84, New York (1980).

[9] J. Berstel and J. Karhumäki: *Compinatorics on words - A tutorial*, Bulletin EATCS, 79, s. 178-228, (Helmikuu 2003).

[10] N. Jacobson: *The theory of rings*, American mathematical society, New York (1943).

[11] A. R. Kemer: *Capelli identities and nilpotency of the radical of a finitely generated PI-algebra*, Soviet Math. Dokl. 22, no. 3, s. 750-753, (1981).

[12] M. Dehn: *Uber die Grundlagen der projektiven geometric und allgemeine zahlsysteme*, Math. ann. 85, s. 184-193, (1922).

[13] S. A. Amitsur: *Rational identities and applications to algebra and geometry*, J. Algebra 3, s. 304-359, (1966).

[14] J. Justin and G. Pirillo: *Shirshov's theorem and ω-permutability of semigroups*, Advances in mathematics 87, s. 151-159, (1991).

[15] G. Pirillo: *A proof of Shirshov's theorem*, Advances in mathematics 124, s. 94-99, (1996).

[16] N. Jacobson: *PI-algebras, An Introduction*, Lecture notes in mathematics 441, Springer-Verlag, Berlin-Heidelberg-New York, (1975).

[17] A. Ya. Below: *The Kurosh problem, height theorem, nilpotency of the radical, and algebraicity identity*, Journal of mathematical science, Vol. 154, No. 2 (2008)

[18] J. Levitzki: *On a problem of Kurosch*, Bull. amer. math soc. 52, s. 1033-1035, (1946).

[19] N. Jacobson: *Structure theory for algebraic algebras of bounded degree*, Ann. of math. s.695-707, (1945).

[20] I. Kaplansky: *Topological representation of algebras. II*, Trans. amer. math. soc. 66, s. 464-491, (1949).

[21] Yu. P. Razmyslov: *The Jacobson radical in PI-algebras*, Algebra and logic 13, s. 192-204, (1974).

[22] A. Braun: *The nilpotency of the radical in a finitely generated PI-ring*, J. algebra 89, s. 375-396, (1984).

[23] E. S. Golod: *On nil-algebras and residually finite p-groups*, Eng. kielinen käännös: Trans. amer. math. soc. v. 48, (1965).

[24] E.S. Golod, I.R. Shafarevich: *On class field towers*, Eng. kielinen käännos: Trans. amer. math. soc. v. 48 (1965).