Tampereen yliopisto

Riku Anttila

ÄÄRELLISISTÄ KUNNISTA

Informaatioteknologian ja viestinnän tiedekunta
Kandidaattitutkielma
Maaliskuu 2020

Tiivistelmä

Riku Anttila: Äärellisistä kunnista
Kandidaattitutkielma
Tampereen yliopisto
Matematiikan ja tilastotieteen tutkinto-ohjelma
Maaliskuu 2020

Tässä tutkielmassa tarkastelemme äärellisiä kuntia, eli kuntia, jotka ovat joukkoina äärellisiä.

Tutkielmassa esitämme q-alkioisen kunnan olemassaoloehdon ja osoitamme sen olevan isomorfiaa vaille yksikäsitteinen. Käymme myös läpi äärellisen kunnan alikunnan ominaisuuksia sekä lyhyesti äärellisten kuntien Galois'n teoriaa.

Avainsanat: Kuntalaajennus, alikunta, polynomirengas, Frobeniuksen automorfismi, Galois'n ryhmä

Tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck -ohjelmalla.

Sisältö

1 Johdanto

Tässä tutkielmassa tarkastelemme äärellisiä kuntia ja todistamme niiden keskeisiä tuloksia. Alussa esittelemme kuntateorian käsitteitä, kuten kuntalaajennus ja minimaalinen polynomi, sekä käymme läpi näihin liittyviä tuloksia. Sen jälkeen tarkastelemme äärellisen kunnan karakteristikan ominaisuuksia.

Luvussa 3 osoitamme q-alkioisen kunnan olevan isomorfiaa vaille yksikäsitteinen sekä annamme riittävän ja välttämättömän ehdon q-alkioisen kunnan olemassaololle. Jälkimmäisen todistuksessa hyödynnämme Frobeniuksen automorfismia, jonka myös esittelemme tässä luvussa. Kun olemme todistaneet q-alkioisen kunnan yksikäsitteisyyden, merkitsemme q-alkioista kuntaa notaatiolla $\mathbb{F}_q$.

Seuraavaksi luvussa 4 tarkastelemme äärellisen kunnan alikuntia ja muun muassa määritämme kaikki kunnan $\mathbb{F}_q$ alikunnat. Lopuksi luvussa 5 käymme lyhyesti läpi äärellisten kuntien Galois'n teoriaa. Tässä osoitamme kuntalaajennuksen $\mathbb{F}_{q^m}/\mathbb{F}_q$ Galois'n ryhmän olevan syklinen, ja esitämme yhden sen sovelluksista.

Oletamme lukijan hallitsevan algebran perusteet. Erityisesti lukijan tulisi tuntea polynomirenkaiden perusominaisuudet. Lisäksi oletamme lukijan hallitsevan lukuteorian peruskäsitteet, kuten aritmetiikan peruslause ja pienin yhteinen jaettava.

2 Kuntateorian peruskäsitteitä

2.1 Määritelmiä ja perustuloksia

Määritelmä 2.1. Kunta on *äärellinen*, mikäli se on joukkona äärellinen.

Esimerkki 2.2. Algebran peruskursseilta tiedämme, että $\mathbb{Z}_p$ on kunta kaikilla alkuluvuilla p. Koska $|\mathbb{Z}_p| = p$, niin se on äärellinen kunta.

Määritelmä 2.3. Kunta L on kunnan K *laajennus*, mikäli K on kunnan L alikunta. Tällöin merkitsemme L/K ja kutsumme tätä *kuntalaajennukseksi*.

Huomautus. Jos on olemassa rengashomomorfismi $K \to L$, tulkitsemme kunnan K sen isomorfisena kuvana. Huomaa että tässä K ja L ovat kuntia, jolloin rengashomomorfismi $K \to L$ on välttämättä injektio.

Määritelmä 2.4. Kuntalaajennuksen L/K *aste* $[L : K]$ on vektoriavaruuden L dimensio K-vektoriavaruutena. Tässä skalaarilla kertominen ja vektorien summa ovat siis kunnan L alkioiden tulo ja summa ja tämä todellakin määrittää K-vektoriavaruuden. Mikäli $[L : K] < \infty$, niin L/K on *äärellinen kuntalaajennus*.

Esimerkki 2.5. Tarkastellaan kuntalaajennusta $\mathbb{C}/\mathbb{R}$. Koska joukko $\{1, i\}$ on $\mathbb{R}$-vektoriavaruuden $\mathbb{C}$ kanta, niin $[\mathbb{C} : \mathbb{R}] = 2$.

Määritelmä 2.6. Olkoon L/K kuntalaajennus. Tällöin alkio $\alpha \in L$ on *algebrallinen* yli K:n, mikäli se on jonkin K-kertoimisen polynomin juuri. Jos jokainen kunnan L alkio on algebrallinen yli K:n, niin L/K on *algebrallinen kuntalaajennus*.

Lause 2.7. *Äärellinen kuntalaajennus on algebrallinen.*

Todistus. Ks. [3, s. 55]. □

Määritelmä 2.8. Olkoon L/K kuntalaajennus. Alkioiden $\alpha_1, \ldots, \alpha_n \in L$ *virittämä kunta* yli K:n on suppein kunnan K laajennuksista, joka sisältää alkiot $\alpha_1, \ldots, \alpha_n$. Tästä kuntalaajennuksesta käytämme merkintää $K(\alpha_1, \ldots, \alpha_n)$.

Määritelmä 2.9. Olkoon L/K kuntalaajennus ja $\alpha \in L$ algebrallinen yli K:n. Pääpolynomi $f \in K[x]$ on alkion α *minimaalinen polynomi* yli K:n, mikäli seuraavat ehdot ovat voimassa:

(i) α on polynomin f juuri,

(ii) polynomin f aste on pienin kaikista K-kertoimisista ei-nollapolynomeista, jotka toteuttavat ehdon (i).

Lause 2.10. *Olkoon L/K kuntalaajennus ja $\alpha \in L$ algebrallinen yli K:n. Tällöin sille on olemassa minimaalinen polynomi yli K:n. Lisäksi jos $f \in K[x]$ on pääpolynomi ja $\alpha \in L$ sen juuri, niin f on alkion α minimaalinen polynomi yli K:n, jos ja vain jos se on jaoton.*

Todistus. Ks. [1, s. 74]. □

Lause 2.11. *Olkoon L/K kuntalaajennus ja $\alpha \in L$ algebrallinen yli K:n. Tällöin $K(\alpha) = \{ \sum_{k=0}^{n} b_k \alpha^k \mid n \in \mathbb{N}, b_k \in K \}$ ja $[K(\alpha) : K] = \deg(f)$, missä f on alkion α minimaalinen polynomi.*

Todistus. Ks. [1, s. 89]. □

Lause 2.12. *Olkoon K kunta ja $f \in K[x]$ jaoton. Tällöin $K[x]/\langle f \rangle$ on kunta. Lisäksi $[K[x]/\langle f \rangle : K] = \deg(f)$ ja $K[x]/\langle f \rangle$ sisältää polynomin f juuren. Tässä siis K tulkitaan kanonisen projektion, eli kuvauksen $\pi \colon K[x] \to K[x]/\langle f \rangle$, $\pi(g) = g + \langle f \rangle$ kaikilla $g \in K[x]$, kuvana.*

Todistus. Ks. [4, s. 176]. □

Määritelmä 2.13. Kunnan *K kertolaskuryhmä* on ryhmä $(K \setminus \{0\}, \cdot)$. Merkitään $K^* = K \setminus \{0\}$.

Lause 2.14. *Kunnan kertolaskuryhmän äärellinen aliryhmä on syklinen.*

Todistus. Ks. [4, s. 134]. □

Lause 2.15. *Olkoot L äärellinen kunta ja K sen alikunta. Tällöin $L = K(\alpha)$ jollain $\alpha \in L$.*

Todistus (vrt. [2, s. 51]). Lauseen 2.14 nojalla $L \setminus \{0\} = L^* = \langle \alpha \rangle$ jollain $\alpha \in L$. Tässä siis $\langle \alpha \rangle$ on alkion α virittämä aliryhmä. Mutta tällöinhän $L = K(\alpha)$ ja väite on tällä osoitettu. □

2.2 Karakteristikan ominaisuuksia

Määritelmä 2.16. Kunnan K *karakteristika* on pienin positiivinen kokonaisluku n, jolle pätee $n \cdot 1 = 0$. Mikäli tällaista kokonaislukua ei ole olemassa, niin kunnan K karakteristika on 0. Merkitsemme tätä lukua notaatiolla $\text{char}(K)$.

Lause 2.17. *Äärellisen kunnan karakteristika on alkuluku.*

Todistus (vrt. [2, s. 16]). Olkoon K äärellinen kunta. Koska kunnan karakteristika on joko 0 tai alkuluku, niin riittää osoittaa, että $n \cdot 1 = 0$ jollain $n \in \mathbb{Z}_+$. Nyt Lagrangen lauseen nojalla $|K| \cdot 1 = 0$ ja $|K| \in \mathbb{Z}_+$. □

Lause 2.18. *Olkoon K kunta ja p alkuluku. Tällöin K on kunnan $\mathbb{Z}_p$ kuntalaajennus, jos ja vain jos* $\text{char}(K) = p$.

Todistus (vrt. [4, s. 183]). ”⇒” Jos K on kunnan $\mathbb{Z}_p$ laajennus, niin niillä on sama ykkösalkio. Tällöin niillä on sama karakteristika, joten $\text{char}(K) = \text{char}(\mathbb{Z}_p) = p$.

”⇐” Oletetaan, että $\text{char}(K) = p$ ja tarkastellaan rengashomomorfismia $\varphi\colon \mathbb{Z} \to K$, $\varphi(n) = n \cdot 1$ kaikilla $n \in \mathbb{Z}$. Ensinnäkin $1 \notin \ker(\varphi)$ ja $p \in \ker(\varphi)$, joten $\ker(\varphi)$ on renkaan $\mathbb{Z}$ ei-triviaali ideaali. Lisäksi koska p on alkuluku, niin $\ker(\varphi) = p\mathbb{Z}$. Nyt ensimmäisestä isomorfialauseesta seuraa

$$\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/\ker(\varphi) \cong \varphi(\mathbb{Z}) \subseteq K.$$

Näin ollen K on kunnan $\mathbb{Z}_p$ kuntalaajennus. □

Seuraus 2.19. *Jos K on äärellinen kunta ja* $\text{char}(K) = p$*, niin K on kunnan $\mathbb{Z}_p$ kuntalaajennus.*

Lause 2.20. *Olkoon K äärellinen kunta ja K/F kuntalaajennus. Tällöin $|K| = |F|^t$, missä $t = [K : F]$. Erityisesti jos* $\text{char}(K) = p$*, niin $|K| = p^k$, missä $k = [K : \mathbb{Z}_p]$.*

Todistus (vrt. [2, s. 48]). Lineaarialgebrasta tiedämme, että k-dimensioisen F-vektoriavaruuden ja joukon F^k välillä on olemassa bijektio. Erityisesti löydämme bijektion joukkojen K ja F^t välille. Siispä $|K| = |F^t| = |F|^t$. Lisäksi jos $\text{char}(K) = p$, niin lauseen 2.18 nojalla K on kunnan $\mathbb{Z}_p$ laajennus ja täten $|K| = |\mathbb{Z}_p|^k = p^k$, missä $k = [K : \mathbb{Z}_p]$. □

Esimerkki 2.21. Koska 6 ei ole alkuluvun potenssi, niin ei ole olemassa 6-alkioista kuntaa.

3 Yksikäsitteisyys ja olemassaolo

Tästä eteenpäin K on kunta ja $p > 0$ sen karakteristika, ellei toisin mainita.

3.1 Äärellisen kunnan yksikäsitteisyys

Määritelmä 3.1. Polynomin $f \in K[x]$ sanotaan *lohkeavan* kunnassa K, mikäli se voidaan esittää K-kertoimisten ensimmäisen asteen polynomien tulona.

Määritelmä 3.2. Polynomin $f \in K[x]$ *juurikunta* yli K:n on suppein kunnan K laajennus, jossa f lohkeaa. Toisin sanoen jos L on edellä mainittu kunta, sekä L/F ja F/K kuntalaajennuksia, missä $F \subset L$, niin f ei lohkea kunnassa F.

Huomautus. Oletetaan että $f \in K[x]$ ja L on kunnan K sellainen laajennus, missä f lohkeaa. Tällöin suoraan määritelmistä seuraa, että jos $\alpha_1, \ldots, \alpha_n \in L$ ovat polynomin f kaikki juuret, niin polynomin f juurikunta yli K:n on $K(\alpha_1, \ldots, \alpha_n)$.

Esimerkki 3.3. Tarkastellaan kuntalaajennusta $\mathbb{C}/\mathbb{R}$ ja polynomia $f = x^2+1 \in \mathbb{R}[x]$. Polynomi f lohkeaa kunnassa $\mathbb{C}$, sillä $f = (x + i)(x - i)$. Lisäksi $\mathbb{C} = \mathbb{R}(i)$, joten $\mathbb{C}$ on polynomin f juurikunta yli $\mathbb{R}$:n.

Lause 3.4. *Olkoon $f \in K[x]$. Tällöin polynomille f on olemassa juurikunta yli K:n. Lisäksi jos L_1 sekä L_2 ovat polynomin f juurikuntia yli K:n, niin on olemassa isomorfismi $\phi\colon L_1 \to L_2$, jolle pätee $\phi(\alpha) = \alpha$ kaikilla $\alpha \in K$.*

Todistus. Ks. [1, s. 105]. □

Lause 3.5. *Jos $|K| = p^t$, niin K on polynomin $f = x^{p^t} - x \in \mathbb{Z}_p[x]$ juurikunta yli $\mathbb{Z}_p$:n.*

Todistus (vrt. [1, s. 290]). Koska K^* on ryhmä ja $|K^*| = p^t - 1$, niin Lagrangen lauseesta seuraa $\alpha^{p^t-1} = 1$ kaikilla $\alpha \in K^*$. Tällöin $\alpha^{p^t} = \alpha(\alpha^{p^t-1}) = \alpha$ kaikilla $\alpha \in K^*$. Lisäksi $0^{p^t} = 0$, joten $\alpha^{p^t} = \alpha$ kaikilla $\alpha \in K$. Siis jokainen kunnan K alkio on polynomin f juuri, jolloin polynomilla f on ainakin p^t eri juurta kunnassa K. Toisaalta koska polynomin f aste on p^t, se lohkeaa kunnassa K. Nimittäin

$$f = \prod_{\alpha \in K} (x - \alpha).$$

Lisäksi f ei voi lohjeta missään kunnan K aidossa alikunnassa. Huomaa vielä, että $\text{char}(K) = p$, jolloin K on kunnan $\mathbb{Z}_p$ laajennus. Näin ollen K on polynomin f juurikunta yli $\mathbb{Z}_p$:n. □

Lause 3.6. *Olkoot K_1 ja K_2 äärellisiä ja samankokoisia kuntia. Tällöin $K_1 \cong K_2$.*

Todistus (vrt. [1, s. 290]). Merkitään $q = |K_1| = |K_2|$. Lauseen 2.20 nojalla voidaan olettaa, että $q = p^t$ jollain alkuluvulla p ja $t \in \mathbb{Z}_+$. Tällöin lauseesta 3.5 seuraa, että kunnat K_1 ja K_2 ovat polynomin $x^{p^t} - x \in \mathbb{Z}_p[x]$ juurikuntia yli $\mathbb{Z}_p$:n. Näin ollen lauseen 3.4 nojalla $K_1 \cong K_2$. □

3.2 Frobeniuksen automorfismi

Lause 3.7. *Kuvaus $\Phi\colon K \to K,\ \alpha \mapsto \alpha^p$ kaikilla $\alpha \in K$ on rengashomomorfismi. Lisäksi jos K on äärellinen, niin Φ on rengasautomorfismi.*

Todistus (vrt. [1, s. 113 ja 292]). Olkoot $\alpha, \beta \in K$. Ensinnäkin

$$\Phi(\alpha\beta) = (\alpha\beta)^p = \alpha^p\beta^p = \Phi(\alpha)\Phi(\beta).$$

Nyt binomikaavan avulla saadaan

$$\Phi(\alpha+\beta) = (\alpha+\beta)^p = \sum_{j=0}^{p} \binom{p}{j} \alpha^j \beta^{p-j}.$$

Koska $p \mid \binom{p}{j}$ kaikilla $1 \le j \le p-1$, niin tällöin

$$\sum_{j=0}^{p} \binom{p}{j} \alpha^j \beta^{p-j} = \alpha^p + \beta^p.$$

Siis

$$\Phi(\alpha+\beta) = \alpha^p + \beta^p = \Phi(\alpha) + \Phi(\beta).$$

Myös $\Phi(1) = 1^p = 1$ ja näin ollen Φ on rengashomomorfismi.

Oletetaan sitten, että K on äärellinen. Koska rengashomomorfismi kahden kunnan välillä on injektio ja injektio kahden yhtäsuuren äärellisen joukon välillä on bijektio, niin kuvaus Φ on rengasautomorfismi. □

Edellä mainittu kuvaus tunnetaan nimellä *Frobeniuksen endomorfismi*. Jos se lisäksi on automorfismi, sitä usein kutsutaan *Frobeniuksen automorfismiksi*. Jatkossa Φ on Frobeniuksen endomorfismi.

Huomautus. Vaikka Φ riippuu kunnasta K ja luvusta p, jätämme nämä merkitsemättä, mikäli sekaantumisen vaaraa ei ole.

Seuraus 3.8. *Jos $t \in \mathbb{Z}_+$, niin kuvaus $\varphi\colon K \to K,\ \alpha \mapsto \alpha^{p^t}$ kaikilla $\alpha \in K$ on rengashomomorfismi. Lisäksi jos K on äärellinen, niin φ on rengasautomorfismi.*

Todistus (vrt. [1, s. 292]). Koska $\varphi = \Phi^t$, niin se on rengashomomorfismien yhdisteenä rengashomomorfismi. Lisäksi jos K on äärellinen, niin φ on rengasautomorfismien yhdisteenä rengasautomorfismi. □

3.3 Olemassaoloehto

Lause 3.9. *Jos $t \in \mathbb{Z}_+$, niin joukko $E = \{\, \alpha \in K \mid \alpha^{p^t} = \alpha \,\}$ on kunnan K alikunta. Lisäksi jos polynomi $f = x^{p^t} - x \in \mathbb{Z}_p[x]$ lohkeaa kunnassa K, niin E on polynomin f juurikunta yli $\mathbb{Z}_p$:n.*

Todistus (vrt. [1, s. 117 ja s. 290]). Selvästi $0, 1 \in E$, joten $E \neq \emptyset$. Havaitaan, että

$$E = \{\, \alpha \in K \mid \Phi^t(\alpha) = \alpha \,\}$$

ja seurauksen 3.8 nojalla Φ^t on rengashomomorfismi. Valitaan $\alpha, \beta \in E$ ja tarkastellaan seuraavia tapauksia:

(i) Oletetaan, että $p = 2$. Tällöin $1 = -1$, ja saadaan

$$\Phi^t(\alpha - \beta) = \Phi^t(\alpha) + \Phi^t(-1)\Phi^t(\beta) = \alpha + (-1)^{p^t}\beta = \alpha + \beta = \alpha - \beta.$$

(ii) Oletetaan sitten, että $p \neq 2$. Tässä tapauksessa p on pariton alkuluku, jolloin

$$\Phi^t(\alpha - \beta) = \Phi^t(\alpha) + \Phi^t(-1)\Phi^t(\beta) = \alpha + (-1)^{p^t}\beta = \alpha - \beta.$$

Siis kummassakin tapauksessa $\Phi^t(\alpha - \beta) = \alpha - \beta$ ja siten $\alpha - \beta \in E$. Lisäksi

$$\Phi^t(\alpha\beta) = \Phi^t(\alpha)\Phi^t(\beta) = \alpha\beta,$$

ja jos $\alpha \neq 0$, niin

$$\Phi^t(\alpha^{-1}) = \Phi^t(\alpha)^{-1} = \alpha^{-1}.$$

Täten $\alpha\beta, \alpha^{-1} \in E$ ja näin ollen E on kunnan K alikunta.

Oletetaan sitten, että polynomi $f = x^{p^t} - x \in \mathbb{Z}_p[x]$ lohkeaa kunnassa K. Nyt $\alpha \in K$ on polynomin f juuri täsmälleen silloin, kun $\alpha \in E$. Siis polynomi f

lohkeaa myös kunnassa E, ja jokainen kunnan E alkio on polynomin f juuri. Mutta tällöinhän f ei voi lohjeta missään kunnan E aidossa alikunnassa. Huomaa vielä, että E on kunnan $\mathbb{Z}_p$ laajennus, sillä $1 \in E$. Siispä E on polynomin f juurikunta yli $\mathbb{Z}_p$:n. □

Määritelmä 3.10. Polynomi $f \in K[x]$ on *separoituva*, jos sen jokainen juuri sen juurikunnassaan on yksinkertainen. Toisin sanoen polynomilla f on asteensa verran erisuuria juuria sen juurikunnassa.

Määritelmä 3.11. Polynomin $f = \sum_{k=0}^{n} a_k x^k \in K[x]$ *muodollinen derivaatta* on polynomi $f' = \sum_{k=1}^{n} k a_k x^{k-1}$.

Esimerkki 3.12. Kunnan $\mathbb{R}$ polynomien muodollinen derivaatta on sama kuin analyysistä tuttu polynomin derivaatta.

Lause 3.13. *Polynomi $f \in K[x]$ on separoituva, jos ja vain jos* $\operatorname{syt}(f, f') = 1$.

Todistus. Ks. [1, s. 110]. □

Lause 3.14. *Polynomin $f = x^{p^t} - x \in \mathbb{Z}_p[x]$ juurikunta yli $\mathbb{Z}_p$:n sisältää täsmälleen p^t alkiota.*

Todistus (vrt. [1, s. 290]). Olkoon L polynomin f juurikunta yli $\mathbb{Z}_p$:n. Tarkastellaan joukkoa

$$E = \{ \alpha \in E \mid \alpha^{p^t} = \alpha \}.$$

Ensinnäkin havaitaan, että $\alpha \in L$ on polynomin f juuri, täsmälleen silloin kun $\alpha \in E$. Nyt koska

$$f' = p^t x^{p^t - 1} - 1 = -1,$$

niin $\operatorname{syt}(f, f') = 1$. Siis f on lauseen 3.13 nojalla separoituva polynomi, eli sillä on täsmälleen p^t eri juurta kunnassa L. Toisaalta E koostuu polynomin f juurista kunnassa L, joten $|E| = p^t$ ja lisäksi lauseen 3.9 nojalla E on kunnan L alikunta. Huomaa, että tällöin E on kunnan $\mathbb{Z}_p$ laajennus. Siispä se on polynomin f juurikunta yli $\mathbb{Z}_p$:n. Näin ollen $L = E$ ja erityisesti $|L| = p^t$. □

Olemme nyt osoittaneet q-alkioisen kunnan olevan isomorfiaa vaille yksikäsitteinen. Lisäksi se on olemassa, jos ja vain jos q on alkuluvun potenssi. Jatkossa q on alkuluvun p potenssi ja merkitsemme q-alkioista kuntaa notaatiolla $\mathbb{F}_q$. Erityisesti merkitsemme $\mathbb{Z}_p = \mathbb{F}_p$.

4 Äärellisten kuntien alikunnista

4.1 Alikuntaehto

Lause 4.1. *Olkoon R kommutatiivinen rengas, sekä olkoot $n, k \in \mathbb{Z}_+$, missä $k \mid n$. Tällöin $x^k - 1 \mid x^n - 1$ polynomirenkaassa $R[x]$.*

Todistus (vrt. [3, s. 213]). Asetetaan $n = mk$, $m \in \mathbb{Z}_+$ ja osoitetaan väite induktiolla luvun m suhteen.

Perusaskel $m = 1$ on selvä, sillä tällöin $n = k$. Tehdään induktio-oletus, että $x^{mk} - 1 = (x^k - 1)g$ jollain $g \in R[x]$. Tällöin

$$\begin{aligned} x^{(m+1)k} - 1 &= (x^k - 1)x^{mk} + (x^{mk} - 1) \\ &= (x^k - 1)x^{mk} + (x^k - 1)g \\ &= (x^k - 1)(x^{mk} + g). \end{aligned}$$

Siis $x^k - 1 \mid x^{(m+1)k} - 1$. Väite seuraa nyt induktioperiaatteesta. □

Seuraus 4.2. *Olkoon R kommutatiivinen rengas, sekä olkoot $n, k, t \in \mathbb{Z}_+$ missä $k \mid n$. Tällöin $x^{t^k} - x \mid x^{t^n} - x$ polynomirenkaassa $R[x]$.*

Todistus (vrt. [3, s. 213]). Tarkastellaan aluksi polynomeja $x^n - 1, x^k - 1 \in \mathbb{Z}[x]$. Edellisen lauseen nojalla $x^n - 1 = (x^k - 1)g$ jollain $g \in \mathbb{Z}[x]$. Nyt sijoittamalla t polynomiin $x^n - 1$ saadaan

$$t^n - 1 = (t^k - 1)g(t).$$

Siis $t^k - 1 \mid t^n - 1$. Nyt soveltamalla uudestaan lausetta 4.1 saadaan

$$x^{t^k - 1} - 1 \mid x^{t^n - 1} - 1$$

polynomirenkaassa $R[x]$. Näin ollen $x^{t^k} - x \mid x^{t^n} - x$. □

Lause 4.3. *Kunta $\mathbb{F}_{p^n}$ on isomorfinen kunnan $\mathbb{F}_{p^m}$ jonkin alikunnan kanssa, jos ja vain jos $n \mid m$.*

Todistus (vrt. [3, s. 213], [1, s. 293]). ”⇒” Oletetaan, että on E on kunnan $\mathbb{F}_{p^m}$ alikunta ja $E \cong \mathbb{F}_{p^n}$. Tällöin $|E| = p^n$ ja lauseen 2.20 nojalla

$$p^m = |\mathbb{F}_{p^m}| = |E|^t = p^{tn},$$

missä $t \in \mathbb{Z}_+$. Siis $m = tn$, joten $n \mid m$.

"$\Leftarrow$" Oletetaan, että $n \mid m$. Riittää osoittaa, että polynomi $f = x^{p^n} - x$ lohkeaa kunnassa $\mathbb{F}_{p^m}$. Nimittäin tällöin lauseen 3.9 nojalla $K = \{ \alpha \in \mathbb{F}_{p^m} \mid \alpha^{p^n} = \alpha \}$ olisi kunnan $\mathbb{F}_{p^m}$ alikunta sekä polynomin f juurikunta yli $\mathbb{F}_p$:n, jolloin $K \cong \mathbb{F}_{p^n}$.

Merkitään $g = x^{p^m} - x$. Seurauksen 4.2 nojalla $f \mid g$ ja koska $\mathbb{F}_{p^m}$ on polynomin $g \in \mathbb{F}_p[x]$ juurikunta yli $\mathbb{F}_p$:n, niin f lohkeaa kunnassa $\mathbb{F}_{p^m}$. Nimittäin

$$\prod_{\alpha \in \mathbb{F}_{p^m}} (x - \alpha) = g = fh,$$

jollain $h \in \mathbb{F}_{p^m}[x]$. Siispä $K = \{ \alpha \in \mathbb{F}_{p^m} \mid \alpha^{p^n} = \alpha \}$ on etsimämme kunnan $\mathbb{F}_{p^m}$ alikunta. □

Esimerkki 4.4. Jos $m \in \mathbb{Z}_+$, niin $\mathbb{F}_q$ on isomorfinen kunnan $\mathbb{F}_{q^m}$ alikunnan kanssa, sillä $q = p^t$, missä $t \in \mathbb{Z}_+$ ja $q^m = p^{tm}$. Käänteinen väite on myös voimassa. Nimittäin jos $\mathbb{F}_{q_1}$ on isomorfinen kunnan $\mathbb{F}_{q_2}$ alikunnan kanssa, lauseen 2.20 nojalla $q_2 = q_1^m$ jollain $m \in \mathbb{Z}_+$. Siispä jos meillä on äärellinen kunta L ja sen alikunta K, niin voimme olettaa, että $L = \mathbb{F}_{q^m}$ ja $K = \mathbb{F}_q$.

Seuraus 4.5. *Jos $n \mid m$, missä $n, m \in \mathbb{Z}_+$ niin kunta $\mathbb{F}_{p^m}$ sisältää täsmälleen yhden alikunnan, joka on isomorfinen kunnan $\mathbb{F}_{p^n}$ kanssa.*

Todistus (vrt. [2, s. 49-50]). Edellisen lauseen nojalla kunnalla $\mathbb{F}_{p^m}$ on alikunta K, mikä on isomorfinen kunnan $\mathbb{F}_{p^n}$ kanssa. Huomaa, että tällöin K olisi polynomin $f = x^{p^t} - x \in \mathbb{F}_p[x]$ juurikunta yli $\mathbb{F}_p$:n ja siten

$$K = \{ \alpha \in \mathbb{F}_{p^m} \mid \alpha^{p^n} = \alpha \},$$

Tästä nyt seuraa p^n-alkioisen alikunnan yksikäsitteisyys. □

Lause 4.6. *Kunnassa $\mathbb{F}_q$ on m-asteinen jaoton polynomi kaikilla $m \in \mathbb{Z}_+$. Lisäksi jos g on m-asteinen jaoton polynomi kunnassa $\mathbb{F}_q$, niin kunta $\mathbb{F}_{q^m}$ sisältää polynomin g juuren.*

Todistus (vrt. [2, s. 51]). Olkoon $m \in \mathbb{Z}_+$ ja tarkastellaan kuntaa $\mathbb{F}_{q^m}$ sekä sen alikuntaa $\mathbb{F}_q$. Lauseen 2.15 nojalla $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$ jollain $\alpha \in \mathbb{F}_{q^m}$. Olkoon $f_\alpha \in \mathbb{F}_q[x]$ alkion α minimaalinen polynomi yli $\mathbb{F}_q$:n. Huomaa, että tämä on olemassa, sillä $\mathbb{F}_{q^m}/\mathbb{F}_q$ on lauseen 2.7 nojalla äärellisenä kuntalaajennuksena algebrallinen. Täten lauseen 2.11 nojalla

$$m = [\mathbb{F}_{q^m} : \mathbb{F}_q] = [\mathbb{F}_q(\alpha) : \mathbb{F}_q] = \deg(f_\alpha).$$

Koska $f_\alpha \in \mathbb{F}_q$ on jaoton ja se on astetta m, niin se on etsimämme polynomi.

Olkoon $g \in K[x]$ m-asteinen jaoton polynomi. Lauseen 2.12 nojalla $\mathbb{F}_q[x]/\langle g \rangle$ on kunta ja se sisältää polynomin g juuren. Lisäksi $[\mathbb{F}_q[x]/\langle g \rangle : \mathbb{F}_q] = m$, joten $\mathbb{F}_q[x]/\langle g \rangle \cong \mathbb{F}_{q^m}$. □

4.2 Esimerkkejä

Esimerkki 4.7. Tarkastellaan kuntaa $\mathbb{F}_{2^{10}}$. Lauseen 4.3 nojalla tämän alikunnat ovat $\mathbb{F}_2$, $\mathbb{F}_{2^2}$, $\mathbb{F}_{2^5}$ ja $\mathbb{F}_{2^{10}}$. Lisäksi seurauksen 4.5 nojalla kunnalla $\mathbb{F}_{2^{10}}$ on täsmälleen neljä alikuntaa.

Itse asiassa edellinen yleistyy helposti hyödyntämällä aritmetiikan peruslausetta. Tarkastellaan kuntaa $\mathbb{F}_{p^n}$, missä $n \in \mathbb{Z}_+$, ja olkoon

$$\prod_{j=1}^{m} p_j^{k_j}$$

luvun n alkulukuhajotelma. Nyt jos $m \in \mathbb{Z}_+$, niin $m \mid n$ täsmälleen silloin, kun luvun m alkulukuhajotelma on muotoa

$$\prod_{j=1}^{m} p_j^{t_j},$$

missä $0 \leq t_j \leq k_j$ kaikilla $j = 1, \ldots, m$. Näin ollen kunnan $\mathbb{F}_{p^n}$ alikuntien lukumäärä on

$$\prod_{j=1}^{m} (k_j + 1).$$

Määritelmä 4.8 (vrt. [3, s. 42])**.** Olkoon L kunta. Jos F ja K ovat sen alikuntia, niin näiden *yhdiste* (eng. *composite*) on suppein kunnan L alikunta, joka sisältää molemmat kunnat F ja K. Tälle kunnalle käytämme merkintää FK.

Esimerkki 4.9. Tarkastellaan kuntia $\mathbb{F}_{p^n}$ ja $\mathbb{F}_{p^m}$. Lauseen 4.3 nojalla nämä ovat kunnan $\mathbb{F}_{p^{nm}}$ alikuntia, joten voimme määrittää kunnan $\mathbb{F}_{p^n}\mathbb{F}_{p^m}$. Merkitään $t = \mathrm{pyj}(n, m)$. Ensinnäkin $t | nm$, jolloin $\mathbb{F}_{p^t}$ on kunnan $\mathbb{F}_{p^{nm}}$ alikunta. Toisaalta jos $\mathbb{F}_{p^n}$ ja $\mathbb{F}_{p^m}$ olisivat kunnan $\mathbb{F}_{p^k}$ alikuntia jollain $k \in \mathbb{Z}_+$, niin $n \mid k$ ja $m \mid k$. Tällöin myös $t \mid k$ ja siten $\mathbb{F}_{p^t}$ olisi kunnan $\mathbb{F}_{p^k}$ alikunta. Lisäksi $n \mid t$ ja $m \mid t$ ja näin ollen

$$\mathbb{F}_{p^n}\mathbb{F}_{p^m} = \mathbb{F}_{p^t}.$$

5 Äärellisten kuntien Galois'n teoriaa

Määritelmä 5.1. Kuntalaajennuksen L/K *Galois'n ryhmä* on joukko

$$\{\, \sigma \colon L \to L \mid \sigma \text{ on automorfismi, jolle pätee } \sigma(\alpha) = \alpha \text{ kaikilla } \alpha \in K \,\}.$$

Merkitään edellä mainittua joukkoa Gal(L/K).

Esimerkki 5.2. Olkoon $\sigma \colon \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$, $\sigma(\alpha) = \alpha^q$ kaikilla $\alpha \in \mathbb{F}_{q^m}$. Tällöin $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$.

Todistus. Tässä siis $q = p^t$, missä $t \in \mathbb{Z}_+$, ja $\sigma(\alpha) = \alpha^{p^t}$ kaikilla $\alpha \in \mathbb{F}_{q^m}$. Nyt seurauksen 3.8 nojalla σ on rengasautomorfismi. Lisäksi jos $\alpha \in \mathbb{F}_q$, niin α on polynomin $x^q - x$ juuri ja täten $\sigma(\alpha) = \alpha$. Näin ollen $\sigma \in \mathrm{Gal}(L/K)$. □

Lause 5.3. *Kuntalaajennuksen L/K Galois'n ryhmä on ryhmä kuvausten yhdistämisen suhteen.*

Todistus (vrt. [1, s. 125]). Ensinnäkin $\mathrm{id}_L \in \mathrm{Gal(L/K)}$, sillä se on isomorfismi ja $\mathrm{id}_L(\alpha) = \alpha$ kaikilla $\alpha \in K$. Olkoot $\sigma, \tau \in \mathrm{Gal}(L/K)$. Koska σ on isomorfismi $L \to L$, niin samoin on σ^{-1}. Lisäksi jos $\alpha \in K$, niin $\sigma(\alpha) = \alpha$, jolloin $\sigma^{-1}(\alpha) = \alpha$. Siis $\sigma^{-1} \in \mathrm{Gal}(L/K)$.

Nyt $\sigma\tau$ on isomorfismien yhdisteenä isomorfismi $L \to L$, sekä

$$\sigma\tau(\alpha) = \sigma(\alpha) = \alpha$$

kaikilla $\alpha \in K$. Täten $\sigma\tau \in \mathrm{Gal}(L/K)$ ja näin ollen $\mathrm{Gal}(L/K)$ on ryhmä. □

Lause 5.4. *Olkoon L/K kuntalaajennus, $\sigma \in \mathrm{Gal}(L/K)$ ja $f \in K[x]$. Tällöin jos $\alpha \in L$ on polynomin f juuri, niin samoin on $\sigma(\alpha)$.*

Todistus (vrt. [1, s. 126]). Merkitään

$$f = b_0 + b_1 x + \cdots + b_n x^n,$$

missä $b_0, b_1 \ldots, b_n \in K$ ja $n \in \mathbb{N}$. Olkoon $\alpha \in L$ polynomin f juuri. Nyt

$$\begin{aligned} f(\sigma(\alpha)) &= b_0 + b_1\sigma(\alpha) + \cdots + b_n\sigma(\alpha)^n \\ &= \sigma(b_0) + \sigma(b_1)\sigma(\alpha) \cdots + \sigma(b_n)\sigma(\alpha^n) \\ &= \sigma(b_0 + b_1\alpha + \cdots + b_n\alpha^n) \\ &= \sigma(f(\alpha)) = \sigma(0) = 0. \end{aligned}$$

Täten $\sigma(\alpha)$ on myös polynomin f juuri. □

Lause 5.5. *Olkoon L/K kuntalaajennus ja $\alpha \in L$ algebrallinen yli K:n. Jos $\sigma, \tau \in \mathrm{Gal}(K(\alpha)/K)$, joilla $\tau(\alpha) = \sigma(\alpha)$, niin $\sigma = \tau$.*

Todistus (vrt. [1, s. 126]). Olkoon $\beta \in K(\alpha)$. Lauseen 2.11 nojalla

$$\beta = \sum_{k=0}^{n} b_k \alpha^k,$$

missä $n \in \mathbb{N}$ ja $b_k \in K$ kaikilla $k = 0, \ldots, n$. Nyt saadaan

$$\begin{aligned}
\sigma(\beta) &= \sigma(\sum_{k=0}^{n} b_k \alpha^k) \\
&= \sum_{k=0}^{n} b_k \sigma(\alpha)^k \\
&= \sum_{k=0}^{n} b_k \tau(\alpha)^k \\
&= \tau(\sum_{k=0}^{n} b_k \alpha^k) \\
&= \tau(\beta).
\end{aligned}$$

Siis $\sigma = \tau$. □

Lause 5.6. *Kuntalaajennuksen $\mathbb{F}_{q^m}/\mathbb{F}_q$ Galois'n ryhmä on isomorfinen ryhmän $\mathbb{Z}_m$ kanssa, ja sen virittää kuvaus $\sigma\colon \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}, \sigma(\alpha) = \alpha^q$ kaikilla $\alpha \in \mathbb{F}_{q^m}$.*

Todistus (vrt.[2, s. 53-54]). Esimerkin 5.2 nojalla $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. Osoitamme ensin, että

$$|\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)| \leq m$$

ja sen jälkeen osoitamme, että $|\langle\sigma\rangle| = m$. Väite olisi tällä todistettu, sillä tällöinhän σ virittäisi ryhmän $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$.

Lauseen 2.15 nojalla $\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha)$ jollain $\alpha \in \mathbb{F}_{q^m}$ ja sen minimaalinen polynomi f_α kunnassa $\mathbb{F}_q$ on astetta m. Huomaa, että tällöin polynomilla f_α on korkeintaan m eri juurta. Nyt lauseen 5.4 nojalla $\sigma(\alpha)$ on myös polynomin f_α juuri kaikilla $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. Toisaalta lauseesta 5.5 saadaan, että alkion α kuva määrää yksikäsitteisesti jokaisen kuvauksen $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. Siispä täytyy olla $|\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)| \leq m$.

Huomaa, että jos $\beta \in \mathbb{F}_{q^m}$, niin β on polynomin $x^{q^m} - x$ juuri. Tästä nyt seuraa, että $\sigma^m = \mathrm{id}_{\mathbb{F}_{q^m}}$, sillä $\sigma^m(\beta) = \beta^{q^m} = \beta$ kaikilla $\beta \in \mathbb{F}_{q^m}$. Siispä väitteen todistamiseksi

riittää osoittaa, että $\sigma^k \neq \sigma^n$ kaikilla $0 < k < n \leq m$. Nimittäin tällöinhän $|\langle\sigma\rangle| = m$ sekä

$$\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) = \langle\sigma\rangle \cong \mathbb{Z}_m.$$

Tämän osoittamiseksi tehdään vastaoletus, että on olemassa sellaiset $n, k \in \mathbb{Z}_+$, joilla $\sigma^n = \sigma^k$ ja $0 < k < n \leq m$. Tällöin $\sigma^{n-k} = \mathrm{id}_{\mathbb{F}_{q^m}}$, eli $\sigma^{n-k}(\beta) = \beta$ kaikilla $\beta \in \mathbb{F}_{q^m}$ ja edelleen yhtäpitävästi jokainen $\beta \in \mathbb{F}_{q^m}$ on polynomin $g = x^{q^{n-k}} - x$ juuri. Huomaa, että $n - k > 0$, joten g ei ole vakiopolynomi. Lisäksi sillä on q^m eri juurta kunnassa $\mathbb{F}_{q^m}$. Mutta tällöinhän $q^m \leq q^{n-k}$, jolloin $m \leq n - k$, mikä on mahdotonta. Siispä hylätään vastaoletus ja väite on tällä todistettu. □

Lause 5.7. *Olkoon $f \in \mathbb{F}_q[x]$ jaoton m-asteinen polynomi. Tällöin sen juurikunta yli $\mathbb{F}_q$:n on $\mathbb{F}_{q^m}$. Lisäksi jos $\alpha \in \mathbb{F}_{q^m}$ on sen juuri, niin polynomin f kaikki juuret ovat muotoa α^{q^i}, missä $i = 0, \ldots, m-1$.*

Todistus (vrt. [2, s. 52]). Lauseen 4.6 nojalla $\mathbb{F}_{q^m}$ sisältää polynomin f juuren α. Lisäksi lauseesta 2.11 seuraa, että $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$, joten $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. Nimittäin $\mathbb{F}_{q^m}$ on m-dimensioinen $\mathbb{F}_q$-vektoriavaruus ja $\mathbb{F}_q(\alpha) \subseteq \mathbb{F}_{q^m}$.

Lauseen 5.6 nojalla

$$\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) = \{\, \sigma^i \mid i = 0, \ldots, m-1 \,\},$$

missä σ on sama kuin esimerkissä 5.2. Koska $\sigma^i \neq \sigma^j$, aina kun $0 \leq i < j \leq m-1$, niin lauseesta 5.5 seuraa

$$\sigma^i(\alpha) \neq \sigma^j(\alpha)$$

eli $\alpha^{q^i} \neq \alpha^{q^j}$, kun $1 \leq i < j \leq m$. Lisäksi $\sigma^i(\alpha) = \alpha^{q^i} \in \mathbb{F}_{q^m}$ on polynomin f juuri kaikilla $i = 0 \ldots m-1$, jolloin $\mathbb{F}_{q^m}$ sisältää m erisuurta polynomin f juurta. Täten f lohkeaa kunnassa $\mathbb{F}_{q^m}$ ja sen juuret ovat muotoa α^{q^i}, missä $i = 0, \ldots, m-1$. Toisaalta tällöinhän

$$\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha) = \mathbb{F}_q(\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}})$$

ja täten $\mathbb{F}_{q^m}$ on polynomin f juurikunta yli $\mathbb{F}_q$: n. □

Seuraus 5.8. *Olkoon $f \in \mathbb{F}_q[x]$ jaoton. Tällöin f on separoituva.*

Todistus. Merkitään $\deg(f) = m$ ja olkoon $\alpha \in \mathbb{F}_{q^m}$ polynomin f juuri. Edellisen lauseen todistuksessa havaittiin, että $\alpha^i \neq \alpha^j$, aina kun $0 \leq i < j \leq m-1$ ja α^{q^i} on polynomin f juuri kaikilla $0 \leq i \leq m-1$. Täten polynomilla f on m eri juurta kunnassa $\mathbb{F}_{q^m}$ ja näin ollen f on separoituva. □

Lähteet

[1] Cox, D. *Galois theory*. New Jersey: John Wiles & Sons, inc., 2004

[2] Lidl, R ja Niederreiter, H. *Finite fields*. Massachusets: Addison-Welsey, 1983.

[3] Roman, S. *Field theory*. New York: Springer, 1995

[4] Rowen, L. Algebra: groups, rings and fields, Massachusetts, A K Peters/CRC Press, 1995.