

Kuntalaajennokset

10. Esimerkki: äärelliset kunnat

Ennen kuin ruvetaan käsittelemään kuntalaajennosten teoriaa yleisemmin, tarkastellaan hieman äärellisten kuntien rakennetta sekä erästä tapaa, jonka avulla niitä voidaan konstruoida. Samalla tutustutaan niihin menetelmiin, joita yleisen teorian kehittämisessä tullaan tarvitsemaan.

Palautetaan aluksi mieleen kunnan karakteristikan ja alkukunnan käsitteet.

MÄÄRITELMÄ 10.1. Olkoon K kunta. Pienintä positiivista kokonaislukua n , jolle pätee

$$\underbrace{1 + \cdots + 1}_{n \text{ kpl}} = 0,$$

kutsutaan K :n *karakteristikaksi* ja merkitään $\text{char}(K)$. Jos tällaista lukua ei ole olemassa, sanotaan että karakteristika on nolla.

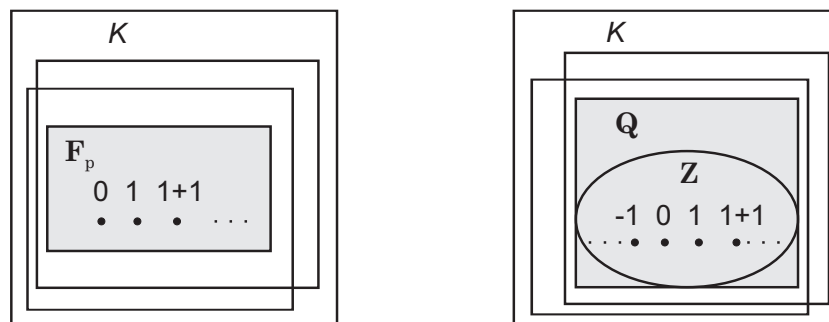
Kunnan karakteristika on aina alkuluku, jos se ei ole nolla. Jos karakteristika p on positiivinen, niin minkä tahansa alkion p :s monikerta on nolla, sillä osittelulain nojalla pätee $(a + \cdots + a) = a(1 + \cdots + 1) = 0$ kaikilla a .

Jos K on kunta, mikä tahansa K :n alikunta sisältää kaikki ykkösalkion monikerrat. Toisaalta karakteristikan ollessa $p > 0$ ykkösalkion monikerrat muodostavat renkaan \mathbb{Z}_p kanssa isomorfisen alistruktuurin, joka on kunta. Tätä kuntaa merkitään symbolilla \mathbb{F}_p ja nimitetään kunnan K *alkukunnaksi*. Toisaalta, jos K :n karakteristika on 0, niin ykkösalkion monikerrat muodostavat rakenteen, joka on isomorfinen renkaan \mathbb{Z} kanssa. Jokainen K :n alikunta sisältää paitsi nämä monikerrat, myös niiden käänteisalkiot. Täten alikunnan täytyy sisältää myös kunta, joka on isomorfinen \mathbb{Z} :n osamääräkunnan \mathbb{Q} kanssa. Näistä havainnoista saadaan seuraava lause (katso myös kuva 19).

LAUSE 10.2. *Jokainen kunta sisältää yksikäsitteisen minimaalisen alikunnan, jota nimitetään alkukunnaksi. Jos kunnan karakteristika on alkuluku p , tämä alkukunta on isomorfinen jäännösluokkakunnan \mathbb{F}_p kanssa. Jos karakteristika on nolla, alkukunta on isomorfinen rationaalilukujen kunnan \mathbb{Q} kanssa.*

Äärellinen kunta ei voi sisältää ääretöntä alkukuntaa, joten äärellisen kunnan karakteristikan on välttämättä oltava positiivinen. Sen sijaan äärettömän kunnan karakteristika voi olla yhtä hyvin positiivinen tai nolla.

Äärellisen kunnan rakenne on itse asiassa hyvin tarkoin määrätty. Ensimmäisen viitteen tästä seikasta antaa seuraava lause, joka rajoittaa vaihtoehdot äärellisen kunnan alkuiden lukumäärälle.



KUVA 19. Jokainen kunta sisältää yksikäsitteisen minimaalisen alikunnan.

LAUSE 10.3. *Jos K on äärellinen kunta, niin $|K| = p^n$, missä p on K :n karakteristika ja n jokin positiivinen kokonaisluku.*

TODISTUS. Samastetaan kunnan K alkukunta ja \mathbb{F}_p . Nyt K on \mathbb{F}_p -algebra, kun skalaarikertolaskuna on kunnan sisäinen kertolasku. Erityisesti K on siis äärellinen \mathbb{F}_p -vektoriavaruus, joten sillä on äärellinen dimensio. Merkitään K :n kantaa $\{b_1, \dots, b_n\}$. Jokainen K :n alkioiden voidaan nyt kirjoittaa yksikäsitteisessä muodossa

$$x_1 b_1 + x_2 b_2 + \dots + x_n b_n,$$

missä $x_i \in \mathbb{F}_p$ kaikilla i . Tällaisia lineaarikombinaatioita on yhtä paljon kuin mahdollisia kerroinjonoja (x_1, \dots, x_n) , eli p^n kappaletta. Siispä $|K| = p^n$. \square

Myöhemmin tullaan osoittamaan, että jokaista alkulukupotenssia p^n kohti on olemassa kunta, jonka koko on p^n , ja että tämä kunta on isomorfaa vaille yksikäsitteinen. Tarkastellaan tämän luvun lopuksi, miten tällaisia kuntia voidaan periaatteessa konstruoida.

Lähdetään liikkeelle alkukunnasta \mathbb{F}_p . Oletetaan, että $f \in \mathbb{F}_p[X]$ on jaoton polynomi, jonka aste on $n > 0$. Esimerkin 6.10 perusteella polynomin f virittämä ideaali $\langle f \rangle$ on maksimaalinen. Näin ollen tekijärengas $\mathbb{F}_p[X]/\langle f \rangle$ on kunta. Tämä kunta koostuu polynomien sivuluokista $\bar{g} = g + \langle f \rangle$. Nolla- ja ykkösalkiot ovat vastaavasti vakiopolynomien 0 ja 1 sivuluokat; näitä luokkia merkitään yksinkertaisesti $\bar{0} = 0$ ja $\bar{1} = 1$.

LAUSE 10.4. *Kunnan $\mathbb{F}_p[X]/\langle f \rangle$ alkioiden lukumäärä on p^n .*

TODISTUS. Merkitään $\mathbb{F}_p[X]/\langle f \rangle = K$. Ideaali $\langle f \rangle$ on \mathbb{F}_p -modulin $\mathbb{F}_p[X]$ alimoduli, sillä $ag \in \langle f \rangle$ kaikilla $g \in \langle f \rangle$ ja $a \in \mathbb{F}_p$. Näin ollen K on \mathbb{F}_p -tekijämoduli. Edellisen lauseen todistuksen perusteella riittää osoittaa, että K :lla on kanta, jonka pituus on n .

Tarkastellaan monomeja X^i , missä $i \in \{0, \dots, n-1\}$, ja näistä muodostettua lineaarikombinaatiota

$$g = \sum_{i=0}^{n-1} a_i X^i, \quad \text{missä } a_i \in \mathbb{F}_p \text{ kaikilla } i.$$

Sivuluokka \bar{g} on vastaavasti joukon $B = \{1, \bar{X}, \dots, \bar{X}^{n-1}\}$ lineaarikombinaatio, kertoiminaan edelleen skalaarit a_i . Oletetaan, että $\bar{g} = 0$. Tällöin $g \in \langle f \rangle$, eli f jakaa

$g:n$, mutta $g:n$ aste on pienempi kuin n , joten $g:n$ on oltava nollapolynomi. Siispä $a_i = 0$ kaikilla i , mistä seuraa, että joukko B on vapaa.

Oletetaan sitten, että $h \in \mathbb{F}_p[X]$ on mielivaltainen. Jakoyhtälöstä seuraa, että $h = qf + r$, missä $r:n$ aste on pienempi kuin n . Nyt $h - r \in I$ eli $\bar{h} = \bar{r}$. Toisaalta r on muotoa $a_0 + a_1X + \dots + a_{n-1}X^{n-1}$, joten \bar{h} voidaan esittää joukon B alkioiden lineaarikombinaationa. Joukko B on siis \mathbb{F}_p -vektoriavaruuden K kanta. \square

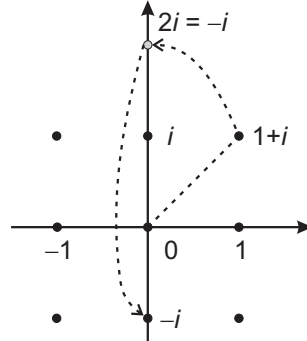
ESIMERKKI 10.5. Toisen asteen polynomi $f = X^2 + 1$ on jaoton kunnassa $\mathbb{F}_3 = \{-1, 0, 1\}$, koska mikään kunnan alkioista ei ole sen juuri. Tekijärengas $K = \mathbb{F}_3[X]/\langle f \rangle$ on kunta, joka koostuu alkioiden 1 ja \bar{X} lineaarikombinaatioista:

$$K = \{0, 1, -1, \bar{X}, \bar{X} + 1, \bar{X} - 1, -\bar{X}, -\bar{X} + 1, -\bar{X} - 1\}.$$

Kyseessä on siis 9 alkion kunta, jonka laskutoimitukset periytyvät polynomirenkkaan $\mathbb{F}_3[X]$ laskutoimituksista. Toisaalta, kuten algebroissa yleensä, kertolaskun määrittämiseksi riittää selvittää kannan alkioiden kertotaulu. Huomataan, että

$$\bar{X}^2 = (\bar{X}^2 + 1) - 1 = 0 - 1 = -1.$$

Siispä alkio \bar{X} on luvun -1 (tarkemmin sanottuna ykkösalkion $1 + I$ vasta-alkion) neliöjuuri. Merkitään nyt $\bar{X} = i$, jolloin kunnan K kertolaskua voidaan ajatella "modulaarisena" kompleksilukujen kertolaskuna. Esimerkiksi $(1+i)^2 = 1+2i+i^2 = 2i = -i$.



KUVA 20. Kunnan \mathbb{F}_3 kaksiuulotteinen laajennos. Kertolasku toimii kuten kompleksiluvuilla.