Kuntalaajennokset

10. Esimerkki: Äärelliset kunnat

Ennen kuin ruvetaan käsittelemään kuntalaajennoksia yleisesti, tarkastellaan hieman äärellisten kuntien rakennetta ja konstruktiota. Samalla tutustutaan niihin menetelmiin, joita teorian kehittämisessä tullaan tarvitsemaan.

Palautetaan aluksi mieleen kunnan karakteristikan ja alkukunnan käsitteet.

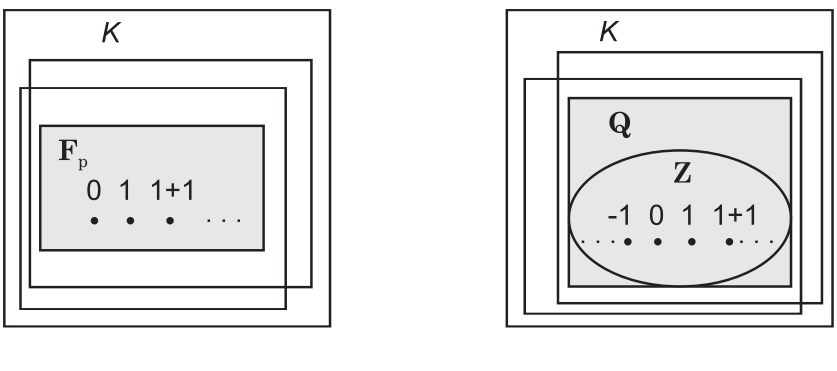
Määritelmä 10.1. Olkoon K kunta. Pienintä positiivista kokonaislukua n, jolle pätee

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

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

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

Jos K on kunta, mikä tahansa 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 $\mathbb{Z}$:n osamääräkunta $\mathbb{Q}$. Näistä havainnoista saadaan seuraava lause.



Kuva 20. Jokainen kunta sisältää yksikäsitteisen minimaalisen alikunnan.

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.*

Jokaisen äärellisen kunnan karakteristika on välttämättä positiivinen, mutta äärettömän kunnan karakteristika voi olla yhtä hyvin positiivinen tai nolla. Osoittautuu, että äärellisen kunnan rakenne on muutenkin hyvin tarkoin määrätty. Seuraava lause antaa rajoituksen äärellisen kunnan alkioiden lukumäärälle.

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 alkio voidaan nyt kirjoittaa yksikäsitteisessä muodossa

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

missä $x_i \in \mathbb{F}_p$ kaikilla i. Tällaisia lineaarikombinaatioita on tuloperiaatteen mukaan p^n kappaletta, joten $|K| = p^n$. □

Myöhemmin tullaan osoittamaan, että jokaista alkulukupotenssia p^n kohti on olemassa kunta, jonka koko on p^n, ja että tämä kunta on isomorfiaa vaille yksikäsitteinen. Tarkastellaan seuraavaksi, 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 $n > 0$. Polynomien jakoyhtälöstä seuraa (todistus jätetään harjoitustehtäväksi), että polynomin f virittämä ideaali $\langle f \rangle$ on alkuideaali. Edelleen sivulla 48 olevan esimerkin perusteella $\langle f \rangle$ on maksimaalinen. Näin ollen tekijärengas $\mathbb{F}_p[X]/\langle f \rangle$ on kunta. Se koostuu sivuluokista $\overline{g} = g + \langle f \rangle$. Nolla- ja ykkösalkiot ovat vastaavasti vakiopolynomien 0 ja 1 sivuluokat; näitä luokkia merkitään yksinkertaisesti $\overline{0} = 0$ ja $\overline{1} = 1$.

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

Todistus. Merkitään $\mathbb{F}_p[X]/\langle f \rangle = K$. Huomataan, että $\langle f \rangle$ 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

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

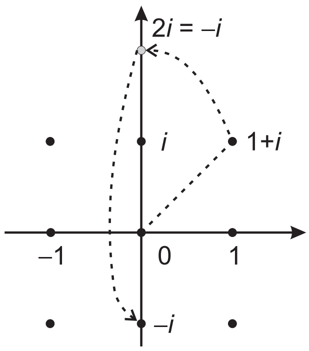
Sivuluokka $\overline{g}$ on joukon $B = \{1, \overline{X} \dots, \overline{X}^{n-1}\}$ lineaarikombinaatio, kertoiminaan skalaarit a_i. Oletetaan, että $\overline{g} = 0$, jolloin $g \in \langle f \rangle$. Nyt f jakaa g:n, mutta g:n aste on pienempi kuin n, joten g:n on oltava nollapolynomi. Siispä $a_i = 0$ kaikilla i, mistä seuraa, että joukko B on vapaa.

Oletetaan sitten, että $h \in \mathbb{F}_p[X]$ on mielivaltainen. Jakoyhtälöstä seuraa, että $h = fq+r$, missä r:n aste on pienempi kuin n. Tällöin $h-r \in I$ eli $\overline{h} = \overline{r}$. Toisaalta r on muotoa $a_0 + a_1X + \cdots + a_{n-1}X^{n-1}$, joten $\overline{h} = \overline{r}$ voidaan esittää lineaarikombinaationa joukon B alkioista. Kyseinen joukko 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 $\overline{X}$ lineaarikombinaatioista:

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

K on siis 9 alkion kunta. Lisäksi $\overline{X}^2 = (\overline{X}^2 + 1) - 1 = 0 - 1 = -1$, eli alkio $\overline{X}$ on luvun -1 (oikeastaan ykkösalkion $1+I$ vasta-alkion) neliöjuuri. Kuten algebroissa yleensä, kannan alkioiden kertotaulu määrittää koko kunnan K:n kertolaskun. Merkitään vielä $\overline{X} = i$, jolloin K:n kertolaskua voidaan ajatella “modulaarisena” kompleksilukujen kertolaskuna. Esimerkiksi $(1 + i)^2 = 1 + 2i - 1 = 2i = -i$.



KUVA 21. Kunnan $\mathbb{F}_3$ kaksiulotteinen laajennos. Kertolasku toimii kuten kompleksiluvuilla.