12. Yleiset laajennokset

Tässä luvussa tutustutaan kuntalaajennoksiin liittyviin peruskäsitteisiin.

12.1. Kuntalaajennos ja sen aste.

MÄÄRITELMÄ 12.1. Kunnan K *laajennos* L on mikä tahansa kunnan K ylikunta eli kunta, joka sisältää K:n alikuntanaan. Laajennosta merkitään L/K (lausutaan "L yli K:n"), ja kuntaa K kutsutaan laajennoksen *lähtökunnaksi.*

Luvussa 10 nähtiin, että kunnan K ylikunta L on myös K-algebra, skalaarikertolaskuna L:n kertolasku. Kunnan K laajennos voidaan itse asiassa määritellä hieman yleisemmin niin, että se on mikä tahansa K-algebra, joka on samalla kunta. Tällainen laajennos kuitenkin sisältää K:n kanssa isomorfisen alikunnan, jolloin tilanne käytännössä palautuu tässä esitettyyn.

Koska kunnan K laajennos on K-vektoriavaruus, sillä on hyvin määritelty dimensio.

MÄÄRITELMÄ 12.2. Kuntalaajennoksen L/K *aste* on L:n dimensio K-vektoriavaruutena. Astetta merkitään $[L : K]$, ja se voi olla joko positiivinen kokonaisluku tai ääretön.

Jos $[L : K]$ on äärellinen, laajennosta nimitetään *äärelliseksi laajennokseksi*, muuten kyseessä on *ääretön laajennos.*

Esimerkkejä kuntalaajennoksista:

- Kompleksilukujen kunta $\mathbb{C}$ on reaalilukujen $\mathbb{R}$ äärellinen laajennos. Pari $\{1, i\}$ muodostaa $\mathbb{C}$:n kannan, joten $[\mathbb{C} : \mathbb{R}] = 2$.
- Kunta $\mathbb{R}$ on $\mathbb{Q}$:n ääretön laajennos: esimerkiksi joukko $\{2^{1/n} \mid n \in \mathbb{N}\}$ on vapaa $\mathbb{Q}$:n suhteen, joten laajennoksella $\mathbb{R}/\mathbb{Q}$ ei ole äärellistä kantaa. Samoin $\mathbb{C}$ on $\mathbb{Q}$:n ääretön laajennos.
- Luvussa 10 käsiteltiin laajennoksia $K/\mathbb{F}_p$, missä $K = \mathbb{F}_p[X]/\langle f\rangle$ ja f oli jokin jaoton polynomi. Huomattiin, että tällaisen laajennoksen aste on sama kuin polynomin f aste.
- Jos K on kunta, polynomialgebra $K[X]$ on ääretönulotteinen K-algebra, joka sisältää K:n (samastettuna vakiopolynomien kanssa). Polynomialgebra ei kuitenkaan ole kunta, joten se ei ole K:n laajennos. Sen osamääräkunta on K-kertoimisten *rationaalilausekkeiden* joukko $K(X)$. Tämä joukko, joka koostuu osamääristä f/g, missä $f, g \in K[X]$ ja $g \neq 0$, on kunta ja sellaisena kunnan K laajennos. Kunta $K(X)$ sisältää alirenkaan $K[X]$, joten $[K(X) : K] = \infty$.

Seuraava lause koskee peräkkäisten laajennoksien asteita.

LAUSE 12.3. *Olkoon $K \subset L \subset M$ jono kuntia. Tällöin*

$$[M : K] = [M : L] \cdot [L : K].$$

Jos jompikumpi asteista $[M : L]$ ja $[L : K]$ on ääretön, niin $[M : K]$ on ääretön.

TODISTUS. Olkoot $\{a_i\}_{i\in I}$ ja $\{b_j\}_{j\in J}$ jotkin laajennosten L/K ja M/L kannat. Osoitetaan, että joukko $B = \{a_i, b_j \mid i \in I, j \in J\}$ on laajennoksen M/K kanta.

Ensinnäkin jokainen $x \in M$ on muotoa $\sum_j y_j b_j$ oleva lineaarikombinaatio, missä $y_j \in L$ kaikilla j. Toisaalta jokainen y_j on muotoa $\sum_i x_{ij} a_i$, missä $x_{ij} \in K$ kaikilla i. Täten $x = \sum_{i,j} x_{ij} a_i b_j$, joten joukko B virittää M:n K-vektoriavaruutena.

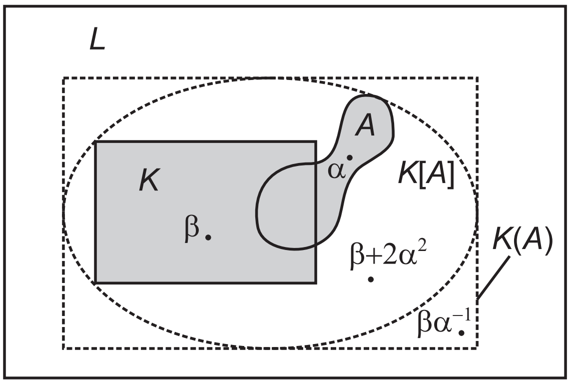
Osoitetaan sitten, että B on vapaa. Oletetaan, että $\sum_{i,j} x_{ij} a_i b_j = 0$, missä $x_{ij} \in K$ kaikilla i. Joukko $\{b_j\}$ on vapaa L-avaruudessa M, ja $\sum_i x_{ij} a_i \in L$ kaikilla j, joten $\sum_i x_{ij} a_i = 0$ kaikilla j. Edelleen joukko $\{a_i\}$ on vapaa K-avaruudessa L, joten $x_{ij} = 0$ kaikilla i ja j. Täten joukko B on laajennoksen M/K kanta. Siitä, että B on vapaa, seuraa erityisesti, että $a_i b_j \neq a_k b_l$, kun $i \neq k$ ja $j \neq l$. Näin saadaan lopulta $[M : K] = |B| = |I| \cdot |J| = [L : K][M : L]$. Tämä sisältää myös sen tapauksen, että $[L : K]$ tai $[M : L]$ on ääretön. □

Edellisestä lauseesta seuraa muun muassa, että jos $K \subset L \subset M$ ovat kuntia ja $[M : K] = n$, niin asteet $[M : L]$ ja $[L : K]$ ovat luvun n tekijöitä. Erityisesti, jos n on alkuluku, niin laajennoksella M/K ei ole epätriviaaleja alilaajennoksia L/K.

12.2. Virittäminen. Kuntalaajennoksen käsittelyä helpottaa huomattavasti, jos tiedetään sen olevan joidenkin tiettyjen alkioiden virittämä. Kuntalaajennoksen virittäminen ei tässä yhteydessä tarkoita samaa kuin sen virittäminen vektoriavaruutena. Erityisesti äärellisviritteisen kuntalaajennoksen asteen ei tarvitse välttämättä olla äärellinen.

Määritelmä 12.4. Olkoon L kunnan K laajennos, ja A joukko L:n alkioita. *Joukon A virittämä laajennoksen L/K alirengas* $K[A]$ on pienin L:n alirengas, joka sisältää sekä kunnan K että osajoukon A. *Joukon A virittämä laajennoksen L/K alilaajennos* $K(A)$ on puolestaan pienin L:n alikunta, joka sisältää sekä kunnan K että osajoukon A. Jos $A = \{a_1, \dots, a_n\}$ on äärellinen, merkitään $K[A] = K[a_1, \dots, a_n]$ ja $K(A) = K(a_1, \dots, a_n)$. Tässä tapauksessa kuntaa $K(a_1, \dots, a_n)$ nimitetään K:n *äärellisviritteiseksi* laajennokseksi.

Koska alirenkaiden mielivaltainen leikkaus on alirengas ja sama pätee kunnille, joukot $K[A]$ ja $K(A)$ voidaan määritellä niiden alirenkaiden tai -kuntien leikkauksena, jotka sisältävät kunnan K sekä joukon A. Näin voidaan perustella joukkojen $K[A]$ ja $K(A)$ olemassaolo, mikä ei seuraa suoraan määritelmästä.



Kuva 23. Joukon A virittämät laajennoksen K/L alirengas $K[A]$ ja alilaajennos $K(A)$

Polynomialgebrat ovat vapaita äärellisviritteisiä algebroja. Sijoitushomomorfismista saadaan merkittävä yhteys K-kertoimisten polynomialgebrojen ja K:n äärellisviritteisten kuntalaajennosten välille. Seuraava lause konkretisoi tätä yhteyttä.

LAUSE 12.5. *Olkoon L kunnan K laajennos, ja olkoot $a_1, \ldots, a_n \in L$. Tällöin*
$$K[a_1, \ldots, a_n] = \{f(a_1, \ldots, a_n) \mid f \in K[X_1, \ldots, X_n]\}$$
ja
$$K(a_1, \ldots, a_n) = \left\{ \frac{f(a_1, \ldots, a_n)}{g(a_1, \ldots, a_n)} \mid f, g \in K[X_1, \ldots, X_n],\ g(a_1, \ldots, a_n) \neq 0 \right\}.$$
Lisäksi $K(a_1, \ldots, a_n)$ on renkaan $K[a_1, \ldots, a_n]$ osamääräkunta.

TODISTUS. Olkoon $\varphi : K[X] \to L$ alkioihin $a_1, \ldots, a_n$ liittyvä sijoitushomomorfismi. Tämän algebrahomomorfismin kuva on $\{f(a_1, \ldots, a_n) \mid f \in K[X]\}$, ja se on algebran L alialgebra, siis alirengas. Toisaalta mikä tahansa L:n alirengas M, joka sisältää kunnan K lisäksi alkiot $a_1, \ldots, a_n$, sisältää myös kaikki näistä alkioista muodostettujen tulojen K-lineaariset kombinaatiot, joten $f(a_1, \ldots, a_n) \in M$ kaikilla $f \in K[X]$. Näin ollen $\operatorname{Im} \varphi \subset M$, mistä seuraa, että $K[a_1, \ldots, a_n] = \operatorname{Im} \varphi$. Renkaan $K[a_1, \ldots, a_n]$ osamääräkunta Q puolestaan koostuu alkioista p/q, missä $p, q \in K[a_1, \ldots, a_n]$ ja $q \neq 0$. Jokainen L:n alikunta, joka sisältää alkiot a_i, sisältää myös renkaan $K[a_1, \ldots, a_n]$ ja edelleen edellä mainitut osamäärät p/q. Täten $K(a_1, \ldots, a_n) = Q$. $\square$

ESIMERKKI 12.6. Laajennoksen $\mathbb{C}/\mathbb{Q}$ alilaajennos $\mathbb{Q}(i)$ koostuu osamääristä $f(i)/g(i)$, missä $f, g \in \mathbb{Q}[X]$ ja $g \neq 0$. Koska $i^2 = -1$, voidaan rajoittua ensimmäisen asteen polynomeihin. Tällöin
$$\mathbb{Q}(i) = \left\{ \frac{a + bi}{c + di} \mid a, b, c, d \in \mathbb{Q},\ c \neq 0 \text{ tai } d \neq 0 \right\}.$$
Edelleen $(c + di)^{-1} = q(c - di)$, missä $q = (c^2 + d^2)^{-1} \in \mathbb{Q}$, joten voidaan kirjoittaa
$$\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\} = \mathbb{Q}[i].$$
Joukko $\{1, i\}$ virittää $\mathbb{Q}$-vektoriavaruuden $\mathbb{Q}[i]$. Lisäksi 1 ja i ovat lineaarisesti riippumattomia $\mathbb{Q}$:n suhteen, joten $\{1, i\}$ on avaruuden $\mathbb{Q}[i]$ kanta. Laajennoksen $\mathbb{Q}(i)/\mathbb{Q}$ asteeksi saadaan näin ollen $[\mathbb{Q}(i) : \mathbb{Q}] = 2$.

Toisaalta voidaan osoittaa, että $\mathbb{Q}$:n laajennoksella $\mathbb{Q}(\pi) \subset \mathbb{R}$ ei ole äärellistä kantaa. Äärellisviritteinen ei siis välttämättä tarkoita samaa kuin äärellinen.

Äärettönviritteisten laajennosten ominaisuudet voidaan useimmiten palauttaa äärellisviritteiseen tapaukseen seuraavan lauseen avulla.

LAUSE 12.7. *Olkoon L kunnan K laajennos, ja olkoon $A \subset L$. Jos $\alpha \in K(A)$, niin $\alpha \in K(a_1, \ldots, a_n)$ joillain $a_1, \ldots, a_n \in A$. Täten*
$$K(A) = \bigcup \{K(a_1, \ldots, a_n) \mid n \in \mathbb{N},\ a_1, \ldots, a_n \in A\}.$$

TODISTUS. Merkitään $F = \bigcup \{K(a_1, \ldots, a_n) \mid a_i \in A\}$. Jokainen äärellisviritteinen kunta $K(a_1, \ldots, a_n)$, missä $a_i \in A$ kaikilla i, sisältyy kuntaan $K(A)$. Täten $F \subset K(A)$. Toisaalta F sisältää kunnan K sekä joukon A, joten jos se on kunta, täytyy sen sisältää myös $K(A)$. Osoitetaan siis, että F on kunta. Olkoot

$\alpha, \beta \in F$. Tällöin $\alpha \in K(a_1, \ldots, a_n)$ ja $\beta \in K(b_1, \ldots, b_m)$ joillain $a_i, b_i \in A$. Nyt alkiot $\alpha \pm \beta$, $\alpha\beta$ ja α/β ovat kunnassa $F(a_1, \ldots, a_n, b_1, \ldots, b_m)$, ja tämä kunta puolestaan sisältyy yhdisteeseen F. Siispä F on kunta, ja $K(A) = F$. $\square$