15. Laajennosten väliset homomorfismit

Rakenteiden väliset homomorfismit auttavat selvittämään rakenteiden suhteita toisiinsa. Rakenteen sisäiset isomorfismit — eli niin sanotut automorfismit — auttavat vastaavasti rakenteen omien ominaisuuksien selvittämisessä. Automorfismit muodostavat aina ryhmän, ja tällä tavoin ryhmäteoriasta tuttuja tuloksia päästään käyttämään hyväksi uusilla alueilla. Kuntalaajennosten yhteydessä automorfismien tutkiminen johtaa Galois'n teoriaan, jolla on lukemattomia sovelluksia lukuteoriassa ja yleisten kuntien teoriassa.

15.1. Homomorfismin määritelmä ja Galois'n ryhmä.

MÄÄRITELMÄ 15.1. Kunnan K laajennosten välistä kuntahomomorfismia σ kutsutaan *K-laajennosten homomorfismiksi* tai lyhyemmin *K-homomorfismiksi*, jos $\sigma(a) = a$ kaikilla $a \in K$.

Kuntalaajennosten välinen kuntahomomorfismi σ on siis K-homomorfismi, jos se kiinnittää lähtökunnan K. Tämä on yhtäpitävää se kanssa, että σ on samalla K-algebrahomomorfismi, jolloin se säilyttää skalaarikertolaskun. Jos nimittäin σ on K-algebrojen välinen homomorfismi, niin kaikilla $a \in K$ pätee $\sigma(a) = \sigma(a.1) = a.\sigma(1) = a$. Toisaalta, jos σ on mielivaltainen K:n kiinnittävä kuntahomomorfismi, niin $\sigma(ab) = \sigma(a)\sigma(b) = a\sigma(b)$.

Koska kuntahomomorfismit ovat aina injektioita, myös laajennosten väliset homomorfismit ovat injektioita. Lisäksi, jos $[L_1 : K] = [L_2 : K] < \infty$, niin laajennosten L_1 ja L_2 välinen homomorfismi on surjektio, koska se on injektio kahden samanulotteisen vektoriavaruuden välillä. Erityisesti äärellisen laajennoksen K-homomorfismit ovat aina bijektioita: niin sanottuja *K-automorfismeja*.

MÄÄRITELMÄ 15.2. Kunnan K laajennoksen L *Galois'n ryhmä* $\mathrm{Gal}(L/K)$ on kaikkien K-automorfismien $\sigma : L \to L$ muodostama ryhmä.

Galois'n ryhmä on siis kaikkien L:n automorfismien ryhmässä $\mathrm{Aut}(L)$ se aliryhmä, joka kiinnittää lähtökunnan K.

Tarkastellaan joukon X virittämää kunnan K laajennosta $K(X)$. Koska jokainen K-automorfismi säilyttää alkioiden tulot ja K-kertoimiset lineaarikombinaatiot, nähdään, että virittäjäalkioiden kuvat määrittävät automorfismin täysin. Puetaan tämä havainto täsmälliseen muotoon seuraavassa lemmassa.

LEMMA 15.3. *Olkoon $K(X)$ joukon X virittämä K:n laajennos, ja olkoot $\sigma, \tau \in \mathrm{Gal}(K(X)/K)$. Jos $\sigma|_X = \tau|_X$, niin $\sigma = \tau$.*

15.2. Juurten kuvautuminen. Osoittautuu, että kuntalaajennosten väliset homomorfismit kuvaavat polynomien juuria toisikseen. Tämä tarjoaa erittäin hyödyllisen tavan päästä käsiksi erityisesti algebrallisten laajennosten välisiin homomorfismeihin.

LAUSE 15.4. *Olkoon $\sigma : L_1 \to L_2$ jokin K-laajennosten homomorfismi, ja olkoon $\alpha \in L_1$ algebrallinen lähtökunnan K suhteen. Jos polynomille $f \in K[X]$ pätee $f(\alpha) = 0$, niin $f(\sigma(\alpha)) = 0$. Lisäksi $\min(K, \alpha) = \min(K, \sigma(\alpha))$.*

TODISTUS. Merkitään $f = b_0 + b_1X + \cdots + b_nX^n$. Koska $b_i \in K$ kaikilla i ja σ on K-homomorfismi, nähdään että $\sigma(b_i) = b_i$ kaikilla i. Täten

$$f(\sigma(\alpha)) = \sum_i b_i\sigma(\alpha)^i = \sum_i \sigma(b_i)\sigma(\alpha)^i = \sigma(f(\alpha)) = \sigma(0) = 0.$$

Lisäksi, jos $p = \min(K, \alpha)$, niin $p(\sigma(\alpha)) = 0$, joten alkion $\sigma(\alpha))$ minimipolynomi jakaa p:n. Toisaalta p on jaoton pääpolynomi, joten täytyy olla $p = \min(K, \sigma(\alpha))$. □

KOROLLAARI 15.5. *Jos L on kunnan K äärellinen laajennos, niin* $\mathrm{Gal}(L/K)$ *on äärellinen ryhmä.*

TODISTUS. Laajennos on äärellinen, jos ja vain jos se on äärellisen monen algebrallisen alkion virittämä. Olkoon $L = K(\alpha_1, \ldots, \alpha_n)$, ja olkoon p_i alkion α_i minimipolynomi kaikilla i. Jokainen K-automorfismi määräytyy täysin sen mukaan, mihin virittäjäalkiot kuvautuvat. Toisaalta edellisen lauseen mukaan jokainen α_i voi kuvautua vain jollekin polynomin p_i juurista, joita on äärellinen määrä. Yhteensä erilaisia automorfismeja on siis vain äärellisen monta. □

ESIMERKKI 15.6. Tarkastellaan laajennosta $\mathbb{C}/\mathbb{R}$. Voidaan helposti osoittaa, että kuvaukset id sekä $\sigma : a + bi \mapsto a - bi$ ovat $\mathbb{R}$-automorfismeja. Koska lisäksi $\mathbb{C} = \mathbb{R}(i)$, jokainen $\mathbb{R}$-automorfismi määräytyy sen perusteella, miten se kuvaa alkion i. Tämän alkion minimipolynomi on $p = X^2 + 1$, ja sillä on juurina i ja $-i$. Lauseen 15.4 perusteella jokainen $\mathbb{R}$-automorfismi τ permutoi p:n juuria, joten täytyy päteä joko $\tau(i) = i$ tai $\tau(i) = -i$. Edellisessä tapauksessa $\tau = \mathrm{id}$, jälkimmäisessä $\tau = \sigma$. Täten $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, \sigma\}$.

Lauseen 15.4 tulos voidaan myös kääntää: jos α ja α' ovat jonkin jaottoman polynomin juuria, niin löytyy sellainen automorfismi, joka kuvaa alkion α alkiolle α'. Tämän tuloksen todistaminen jätetään myöhemmäksi.

15.3. Galois'n teorian peruslause. Kuntalaajennoksen automorfismiryhmän rakenteen selvittäminen auttaa laajennoksen ominaisuuksien tutkimisessa. Tärkeä vastaavuus saadaan liittämällä automorfismiryhmän aliryhmät niihin kuntiin, jotka niiden alkiot kiinnittävät. Tutkitaan seuraavaksi tätä niin kutsuttua *Galois'n yhteyttä*.

Jokaiseen K:n laajennokseen L liittyy automorfismiryhmä $\mathrm{Gal}(K/L)$. Toisaalta jokaiseen L:n kunta-automorfismien joukkoon $S \subset \mathrm{Aut}(L)$ voidaan liittää *kiintokunta*

$$\mathrm{Fix}(S, L) = \{a \in L \mid \sigma(a) = a \text{ kaikilla } \sigma \in S\}.$$

On helppo nähdä, että kiintokunta todellakin on kunta, jolloin se on kunnan L alikunta. Lisäksi, jos S sisältää vain K-automorfismeja eli $S \subset \mathrm{Gal}(L/K)$, niin $K \subset \mathrm{Fix}(S, L)$ eli $\mathrm{Fix}(S, L)$ on kunnan K laajennos.

Oletetaan seuraavassa, että L on kunta, ja yksinkertaistetaan merkintöjä kirjoittamalla $\mathrm{Gal}(L/K) = \mathrm{Gal}(K)$ ja $\mathrm{Fix}(S, L) = \mathrm{Fix}(S)$. Kiintokuntien ja Galois'n ryhmien välille saadaan seuraavan lauseen mukainen vastaavuus.

LAUSE 15.7. *Olkoon L kunta. Tällöin seuraavat ehdot pätevät:*

a) *Jos $K_1 \subset K_2$ ovat L:n alikuntia, niin* $\mathrm{Gal}(K_2) \leq \mathrm{Gal}(K_1)$.

b) *Jos* $S_1 \subset S_2 \subset \mathrm{Aut}(L)$, *niin* $\mathrm{Fix}(S_2) \subset \mathrm{Fix}(S_1)$.
c) *Jos* $S \subset \mathrm{Aut}(L)$, *niin* $\mathrm{Fix}(S) = \mathrm{Fix}(\mathrm{Gal}(\mathrm{Fix}(S)))$.
d) *Jos* K *on jokin kunnan* L *alikunta, niin* $\mathrm{Gal}(K) = \mathrm{Gal}(\mathrm{Fix}(\mathrm{Gal}(K)))$.

Todistus. Väitteet (a) ja (b) seuraavat suoraan kiintokunnan ja Galois'n ryhmän määritelmistä. Todistetaan väitteet (c) ja (d).

Oletetaan ensin, että S on jokin kunnan L automorfismien joukko, ja merkitään $K = \mathrm{Fix}(S)$. Koska S:n alkiot kiinnittävät K:n, niin $S \subset \mathrm{Gal}(K)$. Kohdasta (b) seuraa, että $\mathrm{Fix}(\mathrm{Gal}(K)) \subset \mathrm{Fix}(S) = K$. Toisaalta jokainen ryhmän $\mathrm{Gal}(K)$ alkio kiinnittää K:n, joten $K \subset \mathrm{Fix}(\mathrm{Gal}(K))$.

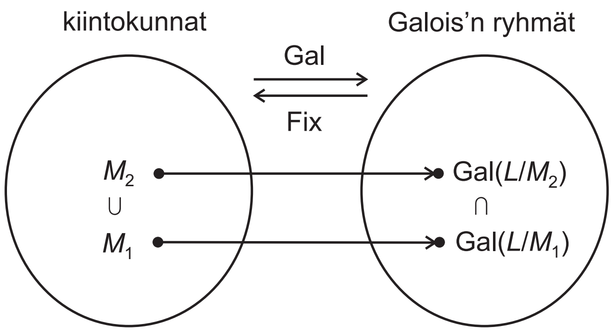
Oletetaan sitten, että K on kunnan L alikunta, ja merkitään $H = \mathrm{Gal}(K)$. Nyt $K \subset \mathrm{Fix}(\mathrm{Gal}(K))$, joten kohdan (a) mukaan

$$\mathrm{Gal}(\mathrm{Fix}(\mathrm{Gal}(K))) \subset \mathrm{Gal}(K) = H.$$

Toisaalta jokainen H:n alkio kiinnittää kunnan $\mathrm{Fix}(H)$, joten $H \subset \mathrm{Gal}(\mathrm{Fix}(H))$. $\square$

Yllä olevan lauseen sanoma on, että on olemassa bijektiivinen, inkluusiosuunnan kääntävä vastaavuus Galois'n ryhmien $\mathrm{Gal}(L/M) \leq \mathrm{Gal}(L/K)$ ja kiintokuntien $\mathrm{Fix}(S, L) \subset L$ välillä, missä $K \subset M \subset L$ ja S on ryhmän $\mathrm{Gal}(L/K)$ osajoukko. Tämän vastaavuuden antaa kuvaus $M \mapsto \mathrm{Gal}(L/M)$, ja sen käänteisvastaavuus on muotoa $H \mapsto \mathrm{Fix}(H, L)$. Vastaavuuden bijektiivisisyys seuraa lauseen kohdista (c) ja (d): Jos $M_1, M_2 \subset L$ ovat kaksi kiintokuntaa, joille pätee $\mathrm{Gal}(M_1) = \mathrm{Gal}(M_2)$, niin $M_1 = \mathrm{Fix}(\mathrm{Gal}(M_1)) = \mathrm{Fix}(\mathrm{Gal}(M_2)) = M_2$. Toisaalta, jos $H \leq \mathrm{Gal}(L)$ on mikä hyvänsä Galois'n ryhmä, niin $\mathrm{Fix}(H)$ on kiintokunta, jolle pätee $\mathrm{Gal}(\mathrm{Fix}(H)) = H$.

Lauseen ehdot toteuttavaa vastaavuutta kutsutaan yleisesti *Galois'n vastaavuudeksi* tai *Galois'n yhteydeksi*. Sellainen esiintyy monilla muillakin aloilla, esimerkiksi algebrallisessa geometriassa polynomijoukkojen ja niiden sisältämien polynomien yhteisten nollakohtien joukkojen välillä.



Kuva 28. Galois'n yhteys liittää toisiinsa kiintokunnat ja niiden Galois'n ryhmät

Määritelmä 15.8. Olkoon L kunnan K laajennos. Kuntaa M, jolle pätee $K \subset M \subset L$, kutsutaan laajennoksen L/K *välikunnaksi*.

Jos S on joukko K-automorfismeja, niin kiintokunta $\mathrm{Fix}(S, L)$ sisältää K:n. Täten $\mathrm{Fix}(S, L)$ on laajennoksen L/K välikunta.

Olisi hyödyllistä, jos lauseen 15.7 määrittelemä bijektiivinen vastaavuus voitaisiin ulottaa *kaikkien* ryhmän $\mathrm{Gal}(L/K)$ aliryhmien ja *kaikkien* laajennoksen L/K välikuntien välille. Erityisesti jos laajennos L/K on äärellinen, pystyttäisiin tällöin löytämään kaikki kyseisen laajennoksen välikunnat tutkimalla laajennoksen äärellistä Galois'n ryhmää.

Haluttaisiin siis osoittaa, että jokainen ryhmän $\mathrm{Gal}(L/K)$ aliryhmä olisi Galois'n ryhmä ja jokainen L/K:n välikunta olisi kiintokunta. Kuitenkin voi käydä esimerkiksi niin, että $\mathrm{Gal}(L/K)$ kiinnittää muutakin kuin lähtökunnan K. Tällöin triviaali välikunta K ei ole minkään aliryhmän $H \leq \mathrm{Gal}(L/K)$ kiintokunta. Tämä antaa aiheen seuraavaan määritelmään.

MÄÄRITELMÄ 15.9. Algebrallista laajennosta L/K kutsutaan *Galois'n laajennokseksi*, jos $K = \mathrm{Fix}(\mathrm{Gal}(L/K), L)$.

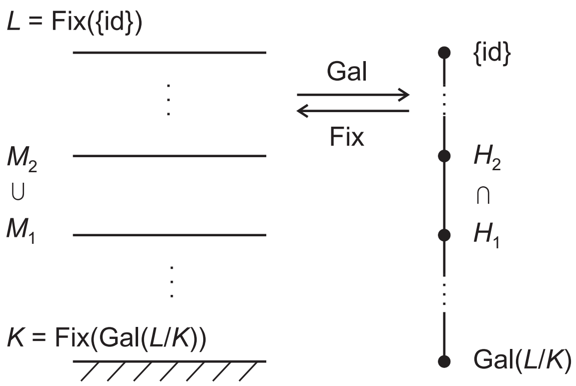
Kunnan K algebrallinen laajennos on siis Galois'n laajennos (tai lyhyemmin, predikatiivina: Galois), jos kaikkien K-automorfismien kiinnittämä joukko on täsmälleen K.

ESIMERKKI 15.10. Laajennoksen $\mathbb{C}/\mathbb{R}$ Galois'n ryhmä on $\{\mathrm{id}, \sigma\}$, missä σ on kompleksikonjugointi $a + bi \mapsto a - bi$. Kompleksikonjugoinnille pätee $\sigma(x) = x$ jos ja vain jos $x \in \mathbb{R}$, joten $\mathbb{C}$ on $\mathbb{R}$:n Galois'n laajennos.

Osoittautuu, että jos laajennos L/K on Galois'n laajennos, niin jokainen laajennos L/M, missä M on L/K:n välikunta, on myös Galois. Tästä seuraa puolestaan, että jokainen välikunta on kiintokunta (nimittäin $M = \mathrm{Fix}(\mathrm{Gal}(L/M))$) ja lopulta jokainen Galois'n ryhmän aliryhmä on Galois'n ryhmä.

LAUSE 15.11 (Galois'n teorian peruslause). *Oletetaan, että L on kunnan K äärellinen Galois'n laajennos. Tällöin kuvaus $M \mapsto \mathrm{Gal}(L/M)$ antaa bijektiivisen, inkluusiosuunnan kääntävän vastaavuuden laajennoksen L/K välilaajennosten sekä ryhmän $\mathrm{Gal}(L/K)$ aliryhmien välillä. Tämän vastaavuuden käänteisvastaavuus on $H \mapsto \mathrm{Fix}(H, L)$.*

TODISTUS. Sivuutetaan. $\square$



KUVA 29. Galois'n laajennokseen liittyvän Galois'n ryhmän jokainen aliryhmä vastaa jotain välikuntaa