16. Valikoituja aiheita

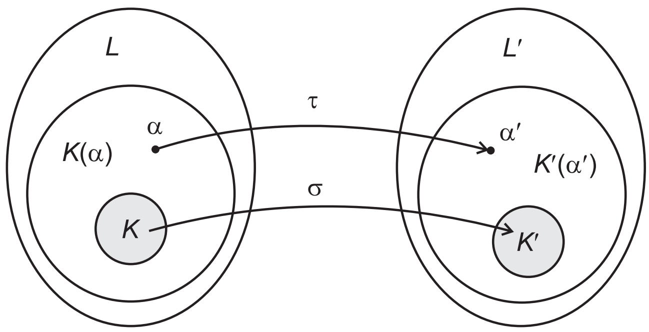
Materiaalin viimeisessä luvussa käydään läpi väliinjääneitä kuntalaajennoksiin liittyviä tuloksia ja tutustutaan vielä hieman tarkemmin Galois'n teoriaan.

16.1. Isomorfismien jatkaminen. On hyödyllistä tietää, millaisessa tilanteessa kuntien välinen isomorfismi voidaan laajentaa algebrallisten laajennosten väliseksi isomorfismiksi.

Kuntien välistä homomorfismia $\sigma : K \to K'$ vastaa polynomirenkaiden homomorfismi $K[X] \to K'[X]$, joka kuvaa polynomin $\sum_i a_i X^i$ polynomille $\sum_i \sigma(a_i) X^i$. Myös tätä johdettua homomorfismia merkitään kirjaimella σ, mikäli sekaantumisen vaaraa ei ole. Seuraava lemma kertoo, millä tavalla annettua kuntaisomorfismia voidaan jatkaa yksinkertaiseen algebralliseen laajennokseen.

LAUSE 16.1. *Oletetaan, että $\sigma : K \to K'$ on kuntaisomorfismi. Olkoon f jokin jaoton K-kertoiminen polynomi, olkoon α polynomin f juuri jossain K:n laajennoksessa L, ja olkoon α' vastaavasti polynomin $\sigma(f)$ juuri jossain K':n laajennoksessa L'. Tällöin on olemassa isomorfismi $\tau : K(\alpha) \to K'(\alpha)$, jolle pätee*

$$\tau|_K = \sigma \quad \text{ja} \quad \tau(\alpha) = \alpha'.$$



KUVA 30. Isomorfismi voidaan jatkaa yksinkertaiseen laajennokseen.

TODISTUS. Merkitään $g = \sigma(f)$. Koska f on jaoton ja $f(\alpha) = 0$, alkion α minimipolynomi on f:n liittoalkio. Täten f virittää alkioon α liittyvän sijoitushomomorfismin ytimen. Vastaava pätee polynomille $g \in K'[X]$, sillä se on myös jaoton. Algebrojen homomorfialauseesta saadaan K-algebrojen isomorfismit

$$\varphi : K[X]/\langle f \rangle \to K(\alpha) \qquad \text{ja} \qquad \psi : K'[X]/\langle g \rangle \to K'(\alpha).$$

Toisaalta kaava $h \mapsto \sigma(h) + \langle g \rangle$ määrittelee surjektiivisen rengashomomorfismin $\chi : K[X] \to K'[X]/\langle g \rangle$. Tämän homomorfismin ydin on $\langle f \rangle$, joten algebrojen homomorfialauseesta saadaan isomorfismi $\overline{\chi} : K[X]/\langle f \rangle \to K'[X]/\langle g \rangle$. Nyt yhdistetty kuvaus $\tau = \psi \circ \overline{\chi} \circ \varphi^{-1} : K(\alpha) \to K(\alpha')$ on kuntaisomorfismi, jolle pätee

$$\tau : \alpha \overset{\varphi^{-1}}{\mapsto} X + \langle f \rangle \overset{\overline{\chi}}{\mapsto} X + \langle g \rangle \overset{\psi}{\mapsto} \alpha'.$$

Lisäksi $\tau|_K = \sigma$, sillä φ ja ψ kuvaavat vakiopolynomit vastaavasti kuntien K ja K' alkioille. $\square$

ESIMERKKI 16.2. Yllä olevaa lausetta voidaan käyttää myös tilanteessa, jossa K ja K' ovat sama kunta ja $\sigma = \mathrm{id}_K$. Jos tällöin α ja α' ovat saman jaottoman polynomin juuria, niin on olemassa isomorfismi $K(\alpha) \cong K(\alpha')$, joka kuvaa $\alpha \mapsto \alpha'$ ja joka kiinnittää lähtökunnan K. Esimerkiksi polynomi $X^4 - 2$ on jaoton $\mathbb{Q}$:n suhteen, ja sillä on kompleksijuuret $\pm\sqrt[4]{2}$ ja $\pm i\sqrt[4]{2}$. On siis olemassa muun muassa $\mathbb{Q}$-isomorfismi $\sigma : \mathbb{Q}(\sqrt[4]{2}) \to \mathbb{Q}(i\sqrt[4]{2})$, jolle pätee $\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$, sekä automorfismi $\tau \in \mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q})$, jolle pätee $\sigma(\sqrt[4]{2}) = -\sqrt[4]{2}$.

Osoittautuu, että kuntaisomorfismi voidaan aina laajentaa jopa juurikuntien isomorfismiksi. Tämän tuloksen todistus perustuu Zornin lemmaan. Oletetaan, että $\sigma : K \to K'$ on jokin K-isomorfismi. Olkoon $S = \{f_i\}_{i \in I}$ joukko K-kertoimisia polynomeja, ja olkoon $S' = \{\sigma(f_i)\}$ vastaava joukko K'-kertoimisia polynomeja. Olkoon lisäksi L polynomijoukon S jokin juurikunta K:n suhteen, ja L' vastaavasti S':n jokin juurikunta kunnan K' suhteen.

LAUSE 16.3 (Isomorfismien jatkaminen). *Olkoon $\alpha \in L$, ja olkoon p alkion α minimipolynomi K:n suhteen. Olkoon lisäksi $\alpha' \in L'$ mikä tahansa polynomin $\sigma(p)$ juuri. Tällöin löytyy isomorfismi $\tau : L \to L'$, jolle pätee $\tau|_K = \sigma$ ja $\tau(\alpha) = \alpha'$.*

TODISTUS. Olkoon $\mathcal{F}$ kaikkien parien (F, φ) joukko, missä F on kunnan L alikunta ja $\varphi : F \to L'$ on kuntahomomorfismi, jolle pätee $\varphi|_K = \sigma$. Tämä joukko sisältää parin (K, σ), joten $\mathcal{F} \neq \emptyset$. Joukko $\mathcal{F}$ voidaan varustaa osittaisjärjestyksellä määrittelemällä $(F, \varphi) \leq (F', \varphi')$ silloin, kun $F \subset F'$ ja $\varphi'|_F = \varphi$. Olkoon $\{(F_i, \varphi_i)\}_{i \in I}$ jokin ketju osittaisjärjestyksessä $\mathcal{F}$. Määrittelemällä

$$F = \bigcup_{i \in I} F_i \quad \text{ja} \quad \varphi(a) = \varphi_i(a), \quad \text{kun } a \in F_i,$$

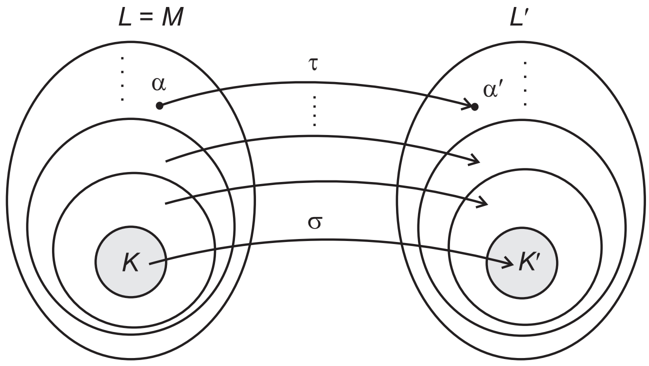
saadaan hyvin määritelty pari $(F, \varphi) \in \mathcal{F}$, joka on ketjun $\{(F_i, \varphi_i)\}_{i \in I}$ yläraja. Zornin lemman perusteella joukossa $\mathcal{F}$ on maksimaalinen alkio (M, τ).

Osoitetaan, että $M = L$ ja $\tau(M) = L'$. Jos $M \subsetneq L$, niin löytyy jokin polynomi $f \in S$, jonka kaikki juuret eivät ole kunnassa M. Olkoon α jokin tällainen juuri, ja olkoon $p = \min(K, \alpha)$. Merkitään $q = \sigma(p) \in S'$. Koska L' on joukon S' juurikunta, löytyy jokin $\alpha' \in L'$, jolle pätee $q(\alpha) = 0$. Lauseen 16.1 perusteella on olemassa isomorfismi $\varphi : M(\alpha) \to \tau(M)(\alpha')$, jolle pätee $\varphi|_M = \tau$. Tämä on ristiriidassa parin (M, τ) maksimaalisuuden kanssa, joten $M = L$. Lisäksi on helppo osoittaa, että juurikunnan kuva $\tau(L)$ on puolestaan polynomijoukon S' juurikunta kunnan K' suhteen, mistä seuraa, että $\tau(L) = L'$. $\square$

Isomorfismien jatkamislausetta käytetään usein konstruoimaan annetun laajennoksen automorfismeja eli Galois'n ryhmän alkioita. Lisäksi siitä seuraa suoraan juurikuntien ja algebrallisten sulkeumien yksikäsitteisyys.

KOROLLAARI 16.4. *Olkoon K kunta, ja olkoon S joukko K-kertoimisia polynomeja. Kaikki S:n juurikunnat kunnan K suhteen ovat isomorfisia K:n laajennoksina. Erityisesti kaikki K:n algebralliset sulkeumat ovat isomorfisia.*

TODISTUS. Koska $\mathrm{id} : K \to K$ on kuntaisomorfismi, isomorfismien jatkamislauseesta saadaan K-laajennosten isomorfismi minkä tahansa kahden S:n juurikunnan välille. Toinen väite seuraa tästä suoraan, sillä kunnan K algebrallinen sulkeuma on samalla kaikkien K-kertoimisten polynomien joukon juurikunta. $\square$



KUVA 31. Isomorfismi voidaan jatkaa juurikuntien isomorfismiksi.

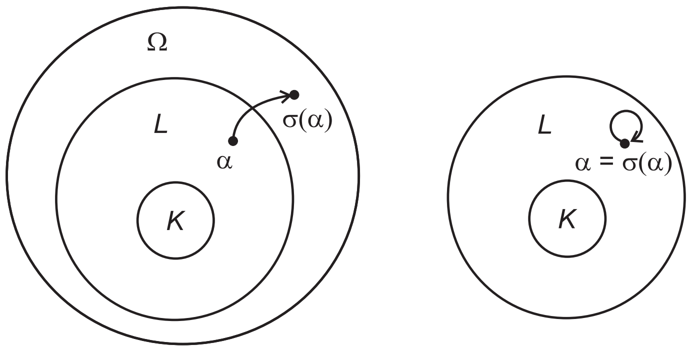
Nyt kun on todistettu algebrallisen sulkeuman olemassaolo ja yksikäsitteisyys isomorfiaa vaille, voidaan algebrallisista laajennoksista puhuttaessa aina rajoittua sopivan alkukunnan algebrallisen sulkeuman alikuntiin. Mikä tahansa algebrallinen laajennos nimittäin sisältyy johonkin algebralliseen sulkeumaan, ja kahden sulkeuman välinen isomorfismi kuvaa myös kyseisen laajennoksen tuon ennalta valitun sulkeuman alilaajennokseksi.

16.2. Galois'n laajennosten karakterisoinnista. Algebrallinen laajennos L/K on Galois, jos K on suurin L:n alikunta, jonka kaikki K-automorfismit kiinnittävät. Mitä enemmän K-automorfismeja on, sitä suuremman joukon ne kiinnittävät. Voidaan siis päätellä intuitiivisesti, että laajennos on Galois, jos siinä voidaan määritellä mahdollisimman suuri määrä K-automorfismeja.

Olkoon L kunnan K algebrallinen laajennos, ja olkoon Ω jokin K:n algebrallinen sulkeuma (jotka ovat siis kaikki keskenään isomorfisia). Isomorfismien jatkamislauseen perusteella jokainen L:n K-automorfismi voidaan jatkaa Ω:n K-automorfismiksi. Mutta mitkä Ω:n automorfismeista rajoittuvat L:n automorfismeiksi? Koska jokaisen K-kertoimisen jaottoman polynomin juuri voidaan isomorfismien jatkamislauseen perusteella kuvata toiselle saman polynomin juurelle, täytyisi L:n sisältää kaikki nämä juuret, jos se sisältää niistä yhdenkin, muuten joukko L ei ole vakaa kyseisessä kuvauksessa. Laajennoksen L täytyisi siis olla jonkin polynomijoukon juurikunta. Tätä ehtoa kutsutaan *normaalisuusehdoksi*: kunnan L kuvaa jossakin Ω:n K-automorfismissa σ kutsutaan L:n konjugaatiksi, ja normaalisuus takaa, että jokaiselle L:n konjugaatille pätee $\sigma(L) \subset L$. (Vertaa tätä aliryhmän normaalisuuden käsitteeseen.)

Laajennoksen automorfismien määrä voi rajoittua toisellakin tavalla. Jaottoman polynomin jokaisen juuren voi kuvata mille tahansa toiselle juurelle, mutta joskus käy niin, että erillisten juurien lukumäärä on pienempi kuin polynomin aste. Toisin sanoen jotkin polynomin ensimmäisen asteen tekijöistä ovat samoja. Tämä vähentää myös erilaisten automorfismien määrää.

MÄÄRITELMÄ 16.5. Olkoon K kunta, ja olkoon $p \in K[X]$ jokin jaoton polynomi. Oletetaan, että L on K:n laajennos ja $\alpha \in L$. Jos p on jaollinen polynomilla $(X - \alpha)^n$ jollain $n > 1$, sanotaan, että α on polynomin p *moninkertainen juuri*. Jos p:llä ei ole lainkaan moninkertaisia juuria juurikunnassaan K:n suhteen, sanotaan, että p on K:n suhteen *separoituva*.



Kuva 32. Algebrallisen laajennoksen automorfismeja menetetään, jos juuret kuvautuvat laajennoksen ulkopuolelle tai itselleen.

Polynomia f kutsutaan separoituvaksi, jos sen jokainen jaoton tekijä on separoituva. Polynomin separoituvuuden selvittämiseksi on olemassa näppärä testi, joka hyödyntää polynomin derivaatan käsitettä. Vaikka polynomialgebrassa ei voidakaan yleensä määritellä metriikkaa eikä raja-arvoja, polynomeja voidaan silti derivoida muodollisesti tutuilla derivointikaavoilla.

Lemma 16.6. *Olkoon K kunta, ja olkoon $f \in K[X]$ polynomi, joka ei ole vakio. Tällöin f on separoituva, jos ja vain jos* $\operatorname{syt}(f, f') = 1$.

Todistus. Osoitetaan ensin, että jos $f, g \in K[X]$ ja L on K:n laajennos, niin f ja g ovat keskenään jaottomia renkaassa $L[X]$, jos ja vain jos ne ovat keskenään jaottomia renkaassa $K[X]$. Toinen suunta on selvä, joten oletetaan, että $\operatorname{syt}(f, g) = 1$ renkaassa $K[X]$. Tällöin $af + bg = 1$ joillain $a, b \in K[X]$. Tämä yhtälö pätee myös renkaassa $L[X]$, joten $\operatorname{syt}(f, g) = 1$ myös renkaassa $L[X]$.

Oletetaan nyt, että $\operatorname{syt}(f, f') = 1$, ja tarkastellaan f:n jakokuntaa L. Jos $\alpha \in L$ on sellainen, että $f = (X - \alpha)^2 \cdot g$, niin

$$f' = 2(X - \alpha) \cdot g + (X - \alpha)^2 \cdot g' = (X - \alpha)(2g + (X - \alpha)g'),$$

joten $X - \alpha$ jakaa myös polynomin f'. Tämä on ristiriita sen kanssa, että f ja f' ovat keskenään jaottomia renkaassa $L[X]$.

Oletetaan sitten, että polynomi f jakautuu juurikunnassaan L erillisiksi ensimmäisen asteen tekijöiksi, ja merkitään $f = \prod_{i=1}^{n}(X - \alpha_i)$, missä luvut $\alpha_i \in L$ ovat erillisiä. Tulon derivointisäännön nojalla

$$f' = \sum_{i=1}^{n} \prod_{i \neq j} (X - \alpha_j).$$

Nyt jokaisella k pätee $f'(\alpha_k) = \prod_{k \neq j}(X - \alpha_j) \neq 0$, joten polynomeilla f ja f' ei ole yhteisiä juuria. Olkoon nyt $d \in K[X]$ jokin polynomien f ja f' yhteinen tekijä. Koska L on polynomin f juurikunta ja d on f:n tekijä, myös d:n kaikki juuret löytyvät kunnasta L. Lisäksi jokainen näistä juurista on polynomien f ja f' yhteinen juuri, koska d jakaa molemmat polynomit. Tällaisia juuria ei ole, joten polynomin d täytyy olla vakio. Täten polynomien f ja f' suurin yhteinen tekijä on yksikkö. $\square$

Laajennoksen alkiota nimitetään separoituvaksi, jos sen minimipolynomi on separoituva. Koko laajennos on separoituva, jos sen jokainen alkio on separoituva. Seuraava lause, jonka todistuksen perusideaa hahmoteltiin yllä, esittää tärkeimmän tavan karakterisoida Galois'n laajennokset.

LAUSE 16.7. *Oletetaan, että L on kunnan K algebrallinen laajennos. Seuraavat ehdot ovat yhtäpitäviä:*

i) *L/K on Galois'n laajennos.*
ii) *L/K on normaali ja separoituva.*
iii) *L on jonkin separoituvista polynomeista koostuvan joukon juurikunta kunnan K suhteen.*

Jos lähtökunnan karakteristika on nolla, derivaattatestin perusteella jokainen laajennos on separoituva. Jos nimittäin f on jaoton polynomi ja polynomeilla f ja f' on yhteinen tekijä g, joka ei ole vakio, niin g:n täytyy olla f:n liittoalkio. Silloin $\deg(f) = \deg(g)$, mutta koska $\deg(f') = \deg(f) - 1$, niin g ei voi olla polynomin f' tekijä. Näin saadaan vielä eräs karakterisointi Galois'n laajennoksille siinä tapauksessa, että separoituvuutta ei tarvitse erikseen mainita.

LAUSE 16.8. *Oletetaan, että L on kunnan K algebrallinen laajennos ja K:n karakteristika on nolla. Tällöin L/K on Galois, jos ja vain jos se on jonkin polynomijoukon juurikunta K:n suhteen.*

16.3. Äärelliset kunnat. Luvussa 10 nähtiin, että jokaisen äärellisen kunnan koko on p^n, missä p on alkuluku ja n positiivinen kokonaisluku. Nyt voidaan lopulta osoittaa, että jokaista tällaista lukua p^n kohti on olemassa kyseistä kertalukua oleva kunta. Lisäksi kaikki samaa kertalukua olevat kunnat ovat keskenään isomorfisia.

LAUSE 16.9. *Olkoon p alkuluku ja n positiivinen kokonaisluku. On olemassa kunta K, jonka koko on p^n. Lisäksi tämä kunta on isomorfiaa vaille yksikäsitteinen.*

TODISTUS. Olkoon Ω kunnan $\mathbb{F}_p$ algebrallinen sulkeuma. Tarkastellaan polynomia $f = X^{p^n} - X$, ja merkitään sen juurten joukkoa $L \subset \Omega$. On helppo nähdä, että joukko L on kunnan Ω alikunta. Tällöin L myös sisältää välttämättä alkukunnan $\mathbb{F}_p$. Lisäksi $f' = p^n \cdot X^{p^n-1} - 1 = -1$, joten derivaattatestin perusteella f on separoituva kunnan $\mathbb{F}_p$ suhteen. Siispä kaikki f:n juuret ovat erillisiä, joten kunnan L koko on p^n.

Olkoon sitten M mikä tahansa kunta, jonka koko on p^n. Tämä kunta sisältää alkukuntanaan kunnan K, joka on isomorfinen kunnan $\mathbb{F}_p$ kanssa. Koska $|M^*| = p^n - 1$, niin $a^{p^n-1} = 1$ kaikilla $a \in M^*$. Täten jokainen kunnan M alkio on polynomin f juuri (sillä myös 0 on f:n juuri). Toisaalta polynomilla f on korkeintaan p^n juurta, joten M on f:n juurikunta kunnan K suhteen. Isomorfismien jatkamislauseesta seuraa, että kaikki tällaiset juurikunnat ovat keskenään isomorfisia. □

Äärellisten kuntien multiplikatiivisilla ryhmillä on sellainen merkittävä ominaisuus, että ne ovat kaikki syklisiä. Tämän osoittamiseksi käytetään ryhmän *eksponentin* käsitettä. Ryhmän G eksponentti $\exp(G)$ on pienin positiivinen kokonaisluku m, jolle pätee $g^m = 1$ kaikilla $g \in G$. Toisin sanoen eksponentti on ryhmän alkioiden kertalukujen pienin yhteinen jaettava.

LEMMA 16.10. *Olkoon G vaihdannainen ryhmä. Tällöin löytyy alkio $g \in G$, jonka kertaluku on* $\exp(G)$.

TODISTUS. Koska K^* on vaihdannainen, se voidaan kirjoittaa p-ryhmien suorana tulona $G_1 \times \cdots \times G_n$, missä $|G_i| = p_i^{k_i}$ kaikilla i (todistus harjoitustehtävä). Olkoon $g_i \in G_i$ se alkio, jonka kertaluku ryhmässä G_i on suurin, ja olkoon tämä kertaluku m_i. Ryhmän G_i jokaisen alkion kertaluku on jokin p_i:n potenssi, mistä seuraa, että $h^{m_i} = 1$ kaikilla $h \in G_i$.

Olkoon nyt $g = (g_1, g_2, \ldots, g_n) \in G$, ja olkoon g:n kertaluku m, jolloin erityisesti $\exp(G) \geq m$. Toisaalta jokaisella i pätee nyt $g_i^m = 1$, mistä seuraa, että $m_i | m$. Jos siis $h = (h_1, \ldots, h_n) \in G$, niin

$$h^m = (h_1^m, \ldots, h_n^m) = (1, \ldots, 1).$$

Täten myös epäyhtälö $\exp(G) \leq m$ pätee, joten g on alkio, jonka kertaluku on $\exp(G)$. $\square$

LAUSE 16.11. *Jos kunta K on äärellinen, niin $(K^*, \cdot)$ on syklinen ryhmä.*

TODISTUS. Merkitään $m = \exp(K^*)$. Jokaisella $g \in K^*$ pätee $g^m = 1$, joten jokainen ryhmän K^* alkio on polynomin $X^m - 1$ juuri. Tällä polynomilla on kuitenkin korkeintaan m juurta, joten $|K^*| \leq m$. Toisaalta edellisen lemman mukaan m on jonkin alkion $g \in K^*$ kertaluku, joten $|K^*| = m$, ja g virittää ryhmän $|K^*|$. $\square$

16.4. Polynomien ratkeavuus. Galois pystyi nimeään kantavan teorian avulla lopulta selvittämään täsmälleen, mitkä rationaalikertoimiset polynomit voidaan ratkaista kuntalaskutoimitusten ja juurenoton avulla. Tämä tulos riippuu vahvasti siitä, että tiettyihin kuntalaajennosten ketjuihin liittyy Galois'n ryhmän normaali jono, minkä osoittamiseksi puolestaan täytyy tuntea seuraava Galois'n teorian peruslauseen jatko-osa.

LAUSE 16.12 (Galois'n teorian peruslause, 2. osa). *Oletetaan, että L/K on äärellinen Galois'n laajennos, ja merkitään $G = \mathrm{Gal}(L/K)$. Jos $H = \mathrm{Gal}(L/M)$, missä M on jokin laajennoksen K/L välikunta, niin*

$$[L : M] = |H| \quad \textit{ja} \quad [M : K] = [G : H].$$

Lisäksi H on normaali G:ssä, jos ja vain jos M/K on Galois'n laajennos. Tässä tapauksessa $G/H \cong \mathrm{Gal}(M/K)$.

$$\begin{tikzcd}
L \arrow[r, leftrightarrow] \arrow[d, dash, "{[L:M]}"] & \{\mathrm{id}\} \arrow[d, dash, "H"] \\
M \arrow[r, leftrightarrow] \arrow[d, dash, "{[M:K]}"] & H \arrow[d, dash, "G/H"] \\
K \arrow[r, leftrightarrow] & G
\end{tikzcd}$$

TODISTUS. Sivuutetaan. □

Tutustutaan seuraavaksi polynomin ratkeavuuden määritelmään. Se muistuttaa huomattavasti geometrisen konstruoituvuuden ehtoa.

MÄÄRITELMÄ 16.13. Kunta L on kunnan K *juurilaajennos*, jos on olemassa jono kuntia

$$K = K_0 \subset K_1 \subset \cdots \subset K_r = L,$$

missä $K_{i+1} = K_i(a_i)$ jollain $a_i \in K_{i+1}$, ja lisäksi $a_i^{n_i} \in F_i$ jollain $n_i \in \mathbb{N}$.

Jos $n = \max\{n_i\}$, missä luvut n_i ovat kuten edellisessä määritelmässä, sanotaan, että L/K on *kertaluvun* n juurilaajennos.

Oletetaan, että $f \in K[X]$. Jos on olemassa juurilaajennos L/K, jossa f jakautuu ensimmäisen asteen tekijöihin, sanotaan, että f on *juurtamalla ratkeava.* Käytännössä tämä tarkoittaa sitä, että f:n juuret voidaan kirjoittaa lausekkeina, joissa esiintyy yhteen-, vähennys-, kerto- ja jakolaskun lisäksi mielivaltaisia juurilausekkeita. Seuraava Évariste Galois'n todistama lause julkaistiin vasta hänen kuolemansa jälkeen vuonna 1843.

LAUSE 16.14 (Galois). *Olkoon K kunta, jonka karakteristika on 0, ja olkoon $f \in K[X]$. Olkoon L polynomin f juurikunta K:n suhteen. Tällöin f on juurtamalla ratkeava, jos ja vain jos* $\mathrm{Gal}(L/K)$ *on ratkeava ryhmä.*

TODISTUS. (Hahmotelma.) Oletetaan, että f on juurtamalla ratkeava, jolloin on olemassa kertaluvun n juurilaajennos M/K, joka sisältää juurikunnan L. Nyt M/K ei välttämättä ole Galois'n laajennos, mutta se on separoituva, koska $\mathrm{char}(K) = 0$. Olkoon $\overline{M}$ laajennoksen M/K *normaali sulkeuma* eli pienin normaali laajennos, joka sisältää kunnan M. Tällöin laajennos $\overline{M}/K$ on Galois. Teknisistä syistä asetetaan $K_1 = K(\omega)$, missä ω on $e^{2\pi i/n}$, ykkösen n:s juuri. Voidaan osoittaa, että $\overline{M}/K_1$ on edelleen kertaluvun n juurilaajennos, joten on olemassa kuntien jono

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_r = \overline{M},$$

missä $K_{i+1} = K_i(a_i)$ ja $a_i^n \in K_i$. Tässä kuntajonossa jokainen laajennos K_{i+1}/K_i on Galois, ja jokainen $\mathrm{Gal}(K_{i+1}/K_i)$ on vaihdannainen ryhmä.

Merkitään $G = \mathrm{Gal}(\overline{M}/K)$ ja $H_i = \mathrm{Gal}(\overline{M}/K_i)$. Galois'n teorian peruslauseen perusteella on olemassa aliryhmien jono

$$G = H_0 \geq H_1 \geq \cdots \geq H_r = 1. \qquad (*)$$

Peruslauseen toisen osan mukaan H_{i+1} on normaali ryhmässä H_i kaikilla i, sillä K_{i+1}/K_i on Galois'n laajennos. Jono $(*)$ on siis normaali jono. Koska lisäksi tekijä $H_i/H_{i+1} \cong \mathrm{Gal}(K_{i+1}/K_i)$ on vaihdannainen ryhmä kaikilla i, nähdään, että G on ratkeava ryhmä. Ratkeavien ryhmien teorian perusteista seuraa, että myös $\mathrm{Gal}(L/K) \cong G/\mathrm{Gal}(\overline{M}/L)$ on ratkeava.

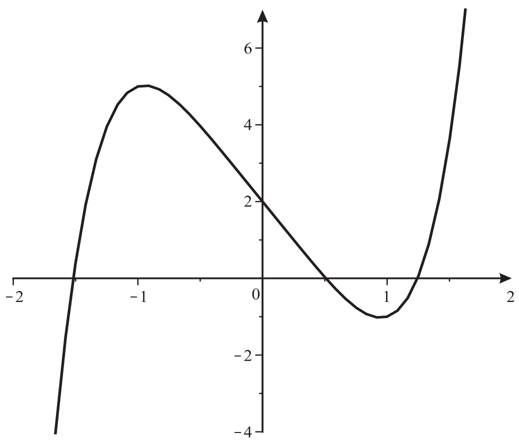
Toinen suunta etenee samalla periaatteella mutta vaatii vielä enemmän teknisiä aputuloksia. □

Voidaan kysyä, mitä hyötyä Galois'n lauseesta oikeastaan on. Näyttää nimittäin siltä, että sen selvittämiseksi, onko jokin polynomi juurtamalla ratkeava, on tunnettava sen juurikunnan Galois'n ryhmä. Tämän juurikunnan tunteminen taas tuntuu edellyttävän sitä, että juuret on jo löydetty. Käytännössä kuitenkin voidaan vähäisistä juurten luonnetta koskevista tiedoista päätellä ryhmien teorian avulla yhtä ja toista juurikunnan Galois'n ryhmästä, vaikka itse juuria ei tunnettaisi. Seuraavassa tästä eräs esimerkki.

Esimerkki 16.15. Tarkastellaan polynomia $f = X^5 - 4X + 2$. Tämä polynomi on Eisensteinin kriteerin perusteella jaoton $\mathbb{Q}$:n suhteen, joten sillä ei ole rationaalijuuria. Toisaalta piirtämällä polynomifunktion $x \mapsto f(x)$ kuvaaja voidaan päätellä, että f:llä on kolme reaalijuurta, joten se voidaan jakaa tuloksi

$$f = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3) \cdot g,$$

missä $\alpha_i \in \mathbb{R}$ kaikilla i, ja g on toisen asteen reaalikertoiminen polynomi.



Kuva 33. Polynomifunktion $f(x) = x^5 - 4x + 2$ kuvaaja.

Olkoon $L \subset \mathbb{C}$ polynomin f juurikunta, jolloin L/K on Galois'n laajennos. Polynomilla f on yhteensä viisi kompleksijuurta, ja jokainen juurikunnan $\mathbb{Q}$-automorfismi määräytyy siitä, miten se permutoi näitä juuria. Voidaan siis päätellä, että $\mathrm{Gal}(L/K)$ on isomorfinen jonkin ryhmän S_5 aliryhmän kanssa. Polynomi f on jaoton, joten se on itse jokaisen juurensa minimipolynomi. Tästä nähdään, että

$$[L : K] = [L : \mathbb{Q}(\alpha_1)] \cdot [\mathbb{Q}(\alpha_1) : \mathbb{Q}] = [L : \mathbb{Q}(\alpha_1)] \cdot 5.$$

Galois'n peruslauseen toisen osan perusteella $|\,\mathrm{Gal}(L/K)| = [L : K]$, joten ryhmän $\mathrm{Gal}(L/K)$ kertaluku on jaollinen viidellä. Cauchyn lauseesta seuraa, että $\mathrm{Gal}(L/K)$ sisältää alkion, jonka kertaluku on 5. Ryhmässä S_5 kaikki tällaiset alkiot ovat 5-syklejä. Toisaalta tiedetään, että toisen asteen polynomin g juuret ovat toistensa kompleksikonjugaatteja, joten kompleksikonjugoinnin rajoittuma juurikuntaan L on $\mathbb{Q}$-automorfismi, joka vaihtaa keskenään polynomin f ei-reaaliset juuret ja pitää reaaliset paikallaan. Ryhmässä S_5 tämä alkio on transpositio.

On varsin suoraviivaista osoittaa, että 5-sykli ja transpositio riittävät virittämään koko ryhmän S_5, mistä seuraa, että $\mathrm{Gal}(L/K) \cong S_5$. Koska S_5 ei ole ratkeava, myöskään polynomi f ei ole juurtamalla ratkeava.

Jo ennen Galois'ta oli tunnettua, että n:nnen asteen polynomiyhtälöllä ei ole yleistä ratkaisukaavaa, mikäli $n \geq 5$. Sen olivat nimittäin todistaneet itsenäisesti Ruffini[21] vuonna 1799 ja Abel vuonna 1824. Galois'n lause tarkentaa tätä tulosta näyttämällä täsmälleen, millä yksittäisillä polynomeilla on ratkaisukaava ja millä ei. Tulos voidaan myös johtaa Galois'n lauseesta, kun muistetaan, että S_n ei ole ratkeava millään $n \geq 5$.

LAUSE 16.16 (Abelin–Ruffinin lause). *Olkoon K kunta, jonka karakteristika on nolla. Jos $n \geq 5$, niin n:nnen asteen K-kertoimisella polynomilla ei ole yleistä kaavaa juurten löytämiseksi.*

TODISTUS. Yleinen n:nnen asteen polynomi on muotoa

$$f = (X - Y_1)(X - Y_2)\cdots(X - Y_n) = X^n - s_1X^{n-1} + \cdots + (-1)^n s_n,$$

missä jokainen Y_i on tuntematon parametri ja jokainen $s_i \in K[Y_1, \ldots, Y_n]$ on ns. *symmetrinen polynomi.* Esimerkiksi

$$\begin{aligned} s_1 &= Y_1 + Y_2 + \cdots + Y_n \\ s_2 &= Y_1Y_2 + Y_1Y_3 + \cdots + Y_2Y_3 + \cdots + Y_{n-1}Y_n \\ &\vdots \\ s_n &= Y_1Y_2\cdots Y_n. \end{aligned}$$

Polynomin f kertoimet ovat siis kunnassa $K_0 = K(s_1, \ldots, s_n) \subset K(Y_1, \ldots, Y_n)$. Jos on olemassa ratkaisukaava yleiselle n:nnen asteen polynomille, täytyy polynomin f olla juurtamalla ratkeava kunnan K_0 suhteen.

Polynomin f juurikunta on $L = K(Y_1, \ldots, Y_n)$. Galois'n ryhmän $\mathrm{Gal}(L/K_0)$ alkiot määräytyvät siitä, miten ne permutoivat virittäjiä Y_i, joten $\mathrm{Gal}(L/K_0)$ on isomorfinen jonkin symmetrisen ryhmän S_n aliryhmän kanssa. Toisaalta mikä tahansa tuntemattomien permutaatio kiinnittää jokaisen symmetrisen polynomin s_i, joten $\mathrm{Gal}(L/K_0) \cong S_n$. Koska S_n ei ole ratkeava, kun $n \geq 5$, myöskään f ei ole juurtamalla ratkeava. Tämä todistaa väitteen. □

LOPPU

[21]Paolo Ruffini (1765–1822), italialainen filosofi ja matemaatikko