LUKU 4

# Vaihdannaiset kunnat

Tässä luvussa kunnalla tarkoitetaan vaihdannaista kuntaa, ellei toisin mainita. Lisäksi algebrat oletetaan ykkösellisiksi, liitännäisiksi ja vaihdannaisiksi ja algebrahomomorfismit ykkösellisiksi. Tämä merkitsee, että algebrat ovat vaihdannaisia renkaita ja niiden homomorfismit rengashomomorfismeja.

## 4.1. Laajennukset

Olkoon $K$ kunta. Tavoitteena on tutkia $K$-algebroja, jotka ovat vaihdannaisia renkaita. Rakenteeltaan yksinkertaisimmat niiden joukossa ovat kuntia.

MÄÄRITELMÄ 4.1.1. Kunnan $K$ *laajennus* on $K$-algebra $E$, joka on renkaana (vaihdannainen) kunta. Laajennuksen $E$ *alilaajennus* on sen alialgebra, joka on kunta.

Olkoon $E$ jokin kunnan $K$ laajennus. Ykkösellisen $K$-algebran $E$ kanoninen homomorfismi (struktuurihomomorfismi, ks. 2.3)

$$u\colon K \to E, \quad \lambda \mapsto \lambda.1,$$

on tällöin injektiivinen, sillä sen ydin on kunnan $K$ ainoa aito ideaali $\{0\}$ (lause 1.8.2). (Koko $u$ ei ole 0, koska kunnassa $E$ pätee $1 \neq 0$.) Kanoninen homomorfismi $u$ kuvaa siten kunnan $K$ isomorfisesti laajennuksen $E$ alikunnalle $u(K)$.

Kääntäen, jos $E$ on kunta ja $u\colon K \to E$ on homomorfismi, niin $E$ varustettuna skalaarikertolaskulla

$$K \times E \to E, \quad (\lambda, x) \mapsto u(\lambda)x,$$

on $K$-algebra (ks. 2.3) ja siten $K$:n laajennus. Tämä voidaan ilmaista täsmällisemmin sanomalla, että $(E, u)$ on $K$:n laajennus.

*Esimerkki* 1) Olkoon $L$ kunnan $K$ ylikunta. Kanoninen inkluusio

$$j\colon K \to L$$

on tällöin homomorfismi, ja sillä varustettu $(L, j)$ on $K$:n laajennus.

Käytännössä tällaisia "luonnollisia laajennuksia" esiintyy usein, ja niissä ei inkluusiota merkitä näkyviin.

*Huomautus.* Myös yleisen laajennuksen $(E, u)$ tapauksessa samastetaan $K$ usein kuvansa $u(K)$ kanssa, ellei ole sekaannuksen vaaraa, ja tällöin jätetään $u$ pois merkinnöistä.

**Aste.** Olkoon $K$ kunta ja $A$ jokin $K$-algebra, esimerkiksi laajennus. Tällöin $A$ on $K$-kertoiminen vektoriavaruus, ja sillä on hyvin määritelty dimensio $\dim_K(A)$, joka on sen kaikkien kantojen $(a_i)_{i\in I}$ yhteinen mahtavuus

$$\dim_K(A) = \mathrm{Card}(I).$$

Tämä todistetaan kuten Lineaarialgebra I:n kurssissa, jos $A$:lla on äärellinen virittäjäperhe. Muussa tapauksessa on tässä luvussa riittävää sanoa, että dimensio on ääretön, merkiten $\dim_K(A) = \infty$ eri mahtavuuksia tarkemmin erottelematta.

MÄÄRITELMÄ 4.1.2. $K$-algebran $A$ *aste* $[A : K]$ on sen dimensio vektoriavaruutena kunnan $K$ suhteen. Algebra $A$ on *äärellinen*, kun sen aste on äärellinen.

LAUSE 4.1.3. *Olkoon $E$ kunnan $K$ laajennus ja $A$ jokin $E$-algebra. Tällöin $A$ on $K$-algebra ja sen aste on*

$$[A : K] = [A : E][E : K].$$

*Erityisesti, jos $F$ on $E$:n laajennus, niin se on $K$:n laajennus ja sen aste on*

$$[F : K] = [F : E][E : K].$$

*Todistus.* Olkoot $u\colon K \to E$ ja $v\colon E \to A$ laajennuksen $E$ ja $E$-algebran $A$ struktuurihomomorfismit. Yhdistämällä saadaan homomorfismi

$$v \circ u\colon K \xrightarrow{u} E \xrightarrow{v} A,$$

joka määrittelee $K$-algebrastruktuurin $A$:ssa.

Asteiden vertailemiseksi oletetaan, että $(a_i)_{i\in I}$ on jokin $E$-algebran $A$ kanta ja $(b_j)_{j\in J}$ jokin $K$-algebran $E$ kanta. Osoitetaan, että $A$:n alkioperhe

$$(b_j a_i)_{(j,i)\in J\times I}$$

on sen kanta $K$-kertoimisena vektoriavaruutena.

Jokaisella $A$:n alkiolla $x$ on esitys

$$x = \sum_{i\in I} \xi_i a_i,$$

missä $(\xi_i)_{i\in I}$ on äärelliskantajainen $E$:n alkioperhe. Jokaisella kertoimella $\xi_i$ on puolestaan esitys

$$\xi_i = \sum_{j\in J} \lambda_{ji} b_j = \sum_{j\in J} u(\lambda_{ji}) b_j,$$

missä vain äärellisen moni $\lambda_{ji} \in K$ $(j \in J)$ on nollasta eroava, ja kaikki häviävät, kun $\xi_i = 0$.

Koska vain äärellisen moni $\xi_i$ on nollasta erova, perhe $(\lambda_{ji})_{(j,i)\in J\times I}$ on äärelliskantajainen ja alkiolle $x$ saadaan esitys

$$x = \sum_{j,i} u(\lambda_{ji}) b_j a_i$$

perheen $(b_j a_i)$ alkioiden lineaarisena yhdistelmänä.

On vielä osoitettava, että perhe $(b_j a_i)$ on vapaa kunnan $K$ suhteen. Olkoon

$$\sum_{j,i} u(\lambda_{ji}) b_j a_i = 0$$

jokin lineaarinen relaatio, missä $(\lambda_{ji})$ on äärelliskantajainen $K$:n alkioperhe. Tämä voidaan kirjoittaa kaksinkertaiseksi summaksi

$$\sum_{i\in I}\Big(\sum_{j\in J} \lambda_{ji} b_j\Big) a_i = 0,$$

ja koska perhe $(a_i)$ on vapaa, sen kuntaan $E$ kuuluvat kertoimet häviävät:

$$\sum_{j\in J} \lambda_{ji} b_j = 0 \qquad (i \in I).$$

Koska perhe $(b_j)$ on vapaa kunnan $K$ suhteen, ovat kaikki kertoimet $\lambda_{ji} = 0$, eli lineaarinen relaatio on triviaali.

Jos joukot $I$ ja $J$ ovat äärellisiä, saadaan algebran $A$ asteeksi kunnan $K$ suhteen lauseke

$$[A : K] = \mathrm{Card}(J \times I) = \mathrm{Card}(I)\mathrm{Card}(J) = [A : E][E : K].$$

Sama pätee, jos $I$ tai $J$ on ääretön, kun tulkitaan tulo äärettömäksi aina kun yksikin tekijä on ääretön.

Viimeinen, laajennusta $F$ koskeva väite on erikoistapaus yllä todistetusta. □

Korollaari 4.1.4. *Olkoot $K$, $E$ ja $F$ kolme kuntaa ja $K \subset E \subset F$. Jos $[F : K]$ on äärellinen, niin asteet $[F : E]$ ja $[E : K]$ ovat äärellisiä ja asteen $[F : K]$ tekijöitä.* □

Korollaari 4.1.5. *Olkoot $K$, $E$ ja $F$ kolme kuntaa, $K \subset E \subset F$ ja $[F : K]$ äärellinen. Tällöin*

$$E = F \;\Leftrightarrow\; [E : K] = [F : K]$$

*ja*

$$E = K \;\Leftrightarrow\; [F : E] = [F : K].$$

*Todistus.* Ehto

$$[E : K] = [F : K] = [F : E][E : K]$$

on yhtäpitävä sen kanssa, että $F$:n dimensio $E$-kertoimisena vektoriavaruutena on $[F : E] = 1$. Koska $E$ on itse $F$:n yksiulotteinen aliavaruus, tämä merkitsee, että $F = E$.

Samalla tavoin $[F : E] = [F : K]$ on yhtäpitävä sen kanssa, että $[E : K] = 1$ eli $E = K$. □

*Esimerkki* 2) Jos aste $[F : K] = p$ on alkuluku, niin korollaarin 4.1.4 nojalla

$$[E : K] = 1 \quad \text{tai} \quad [E : K] = p.$$

Tällöin siis joko $E = K$ tai $E = F$ (kor. 4.1.5). Alkulukuasteisella laajennuksella ei siten ole "välikuntia".

**Adjunktio.** Olkoon $K$ kunta, $E$ sen laajennus ja $(x_i)_{i\in I}$ perhe $E$:n alkioita. Perheen virittämä laajennuksen $E$ alialgebra on (ks. 2.4)

$$K[(x_i)_{i\in I}] = \{u((x_i)_{i\in I}) \mid u \in K[(X_i)_{i\in I}]\}.$$

Se ei yleensä ole $E$:n alikunta eli alilaajennus. Pienin alkiot $x_i$ sisältävä $E$:n alilaajennus saadaan muodostamalla kaikki algebran $K[(x_i)_{i\in I}]$ alkioiden osamäärät. Näin saadaan *perheen* $(x_i)_{i\in I}$ *virittämä* laajennuksen $E$ *alilaajennus*

$$K((x_i)_{i\in I}) = \{pq^{-1} \mid p, q \in K[(x_i)_{i\in I}], q \neq 0\},$$

eli laajennus, joka on saatu *adjungoimalla* alkiot $x_i$ kuntaan $K$.

Laajennus $K((x_i)_{i\in I})$ riippuu vain joukosta $A = \{x_i \mid i \in I\}$ ja usein merkitään lyhyesti

$$K(A) = K((x_i)_{i\in I}).$$

Vastaavasti merkitään $K[A] = K[(x_i)_{i\in I}]$, jolloin $K(A)$ on $K[A]$:n jakokunta.

Erityisesti, jos $I$ on äärellinen, niin alkiot voidaan luetella; esimerkiksi, jos $I = \{1, 2, \ldots, n\}$, niin käytetään merkintää

$$K(x_1, x_2, \ldots, x_n).$$

MÄÄRITELMÄ 4.1.6. Kunnan $K$ laajennus $E$ on *äärellistyyppinen*, jos sillä on äärellinen virittäjäperhe, eli

$$E = K((x_i)_{i\in I}),$$

missä $I$ on äärellinen.

*Esimerkki* 3) Jokainen kunnan äärellinen laajennus (määr. 4.1.2) on äärellistyyppinen, sillä se on jokaisen kantansa virittämä laajennus.

### Harjoitustehtäviä

1) Olkoon $E$ kunnan $K$ laajennus ja olkoot $A$ ja $B$ sen osajoukkoja. Osoitettava, että $K(A \cup B) = K(A)(B) = K(B)(A)$.

2) Olkoon $E = K(x)$ kunnan $K$ äärellinen laajennus, jonka aste on pariton. Osoitettava, että $E = K(x^2)$. (Tarkastellaan astetta $[E : K(x^2)]$.)

## 4.2. Algebralliset laajennukset

Olkoon $K$ kunta ja $A$ jokin $K$-algebra. Jokaiseen algebran $A$ alkioon $x$ liittyy sijoitushomomorfismi

$$\varphi\colon K[X] \to A, \quad f = \sum_{n\in\mathbf{N}} a_n X^n \mapsto f(x) = \sum_{n\in\mathbf{N}} a_n x^n.$$

Sen ytimeen kuuluvat polynomit $f = \sum_n a_n X^n$ vastaavat äärelliskantajaisia $K$:n alkioperheitä $(a_n)_{n\in\mathbf{N}}$, jotka toteuttavat ehdon

$$\sum_n a_n x^n = 0.$$

Nämä ovat siis $K$-kertoimisia lineaarisia relaatioita alkion $x$ potenssien $x^n$ ($n \in \mathbf{N}$) välillä, ja niitä sanotaan $K$-kertoimisiksi *algebrallisiksi relaatioiksi* alkiolle $x$.

Voidaan erottaa kaksi vaihtoehtoa. Ensinnäkin perhe $(x^n)_{n\in\mathbf{N}}$ voi olla vapaa kunnan $K$ suhteen. Silloin sijoitushomomorfismin ydin on $\{0\}$, joten se on isomorfismi kuvalleen

$$\varphi\colon K[X] \xrightarrow{\sim} K[x].$$

Tällöin alkion $x$ virittämän alialgebran aste $[K[x] : K]$ on ääretön, ja sanotaan, että $x$ on *transkendenttinen* $K$:n suhteen. (Sille ei ole algebrallisia relaatioita triviaalia relaatiota lukuunottamatta.)

Jos taas perhe $(x^n)_{n\in\mathbf{N}}$ on sidottu kunnan $K$ suhteen, niin jollakin luonnollisella luvulla $n \geq 1$ potenssit

$$1, x, x^2, \ldots, x^n$$

ovat lineaarisesti riippuvat $K$:n suhteen. Tällöin on olemassa epätriviaali algebrallinen relaatio

$$f(x) = 0,$$

missä $f \in K[X]$, $f \neq 0$ ja $\deg(f) \leq n$.

Jos $n \geq 1$ on pienin mahdollinen, niin potenssit

$$1, x, x^2, \ldots, x^{n-1}$$

ovat lineaarisesti riippumattomat kunnan $K$ suhteen, mutta $x^n$ voidaan esittää muodossa

$$x^n = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1},$$

missä kertoimet $a_0$, $a_1$, …, $a_{n-1} \in K$ ovat yksikäsitteisesti määrätyt.

Polynomi

$$f = X^n - \sum_{k=0}^{n-1} a_k X^k \in K[X]$$

toteuttaa tällöin ehdon $f(x) = 0$, ja sen aste $\deg(f) = n$ on alin mahdollinen epätriviaalien algebrallisten relaatioiden joukossa. Sen määrittelee yksikäsitteisesti vaatimus, että korkeimman potenssin kerroin on 1, eli että se on *pääpolynomi*.

Tällöin sanotaan, että alkio $x$ on *algebrallinen* kunnan $K$ suhteen, $n$ on sen *aste* ja $f$ sen *minimaalipolynomi* $K$:n suhteen.

LAUSE 4.2.1. *Olkoon $A$ $K$-algebra, $x$ $K$:n suhteen algebrallinen $A$:n alkio, $n$ sen aste ja $f \in K[X]$ sen minimaalipolynomi $K$:n suhteen.*

i) *Jos $g \in K[X]$, niin $g(x) = 0$ jos ja vain jos $g$ on jaollinen $f$:llä.*

ii) *Kuvauksesta $g \mapsto g(x)$ saadaan tekijäalgebraan siirtymällä isomorfismi*

$$K[X]/(f) \xrightarrow{\sim} K[x],$$

*ja potenssit $1, x, \ldots, x^{n-1}$ muodostavat $K$-algebran $K[x]$ kannan. Erityisesti sen aste on $[K[x] : K] = n$.*

iii) *Jos $A$ on kokonaisalue, niin $K[x]$ on kunta ja $f$ on jaoton polynomi, ainoa jolla $f(x) = 0$ ja johtava kerroin on 1.*

iv) *Alkio $x$ on kääntyvä $A$:ssa, jos ja vain jos $f(0) \neq 0$, ja tällöin $x^{-1} \in K[x]$.*

*Todistus.* i) Jokainen polynomi $g \in K[X]$ voidaan esittää muodossa $g = qf + r$, missä $q$, $r \in K[X]$ ja $r = 0$ tai $\deg(r) < n$, ja siten

$$g(x) = r(x),$$

koska $f(x) = 0$. Koska minimaalipolynomin $f$ aste $n$ on pienin mahdollinen yhtälön $g(x) = 0$ toteuttavien polynomien $g \neq 0$ joukossa, ehto $g(x) = 0$ on yhtäpitävä sen kanssa, että $r = 0$ eli $g$ on jaollinen $f$:llä.

ii) Olkoon $\varphi\colon K[X] \to A$ sijoitushomomorfismi $g \mapsto g(x)$. Sen ydin $\mathfrak{a} = \mathrm{Ker}(\varphi)$ on algebran $K[X]$ ideaali, joka yllä esitetyn mukaan on sama kuin minimaalipolynomin $f$ virittämä ideaali $(f)$. Homomorfialauseen nojalla saadaan homomorfismista $\varphi$ siten isomorfismi

$$K[X]/(f) \xrightarrow{\sim} K[x].$$

Lisäksi yllä on nähty, että jokainen algebran $K[x]$ alkio $g(x)$ ($g \in K[X]$) voidaan kirjoittaa muotoon

$$r(x) = c_0 + c_1 x + \cdots c_{n-1} x^{n-1},$$

missä $c_i \in K$ $(0 \leq i \leq n-1)$. Potenssit $1, x, \ldots x^{n-1}$ virittävät siten algebran $K[x]$. Luvun $n$ valinnan nojalla ne ovat toisaalta lineaarisesti riippumattomat. Ne muodostavat siis algebran $K[x]$ kannan, jossa on $n$ alkiota.

iii) Olkoon $A$ kokonaisalue ja olkoon $a \in K[x]$, $a \neq 0$. Osoitetaan, että $a$:lla on käänteisalkio $K[x]$:ssä.

Tarkastellaan kuvausta $u\colon K[x] \to K[x]$, $y \mapsto ay$. Se on $K$-lineaarinen, ja sen ydin on $\{0\}$, koska $K[x]$ on kokonaisalue ja $a \neq 0$. Koska $K[x]$ on äärellisulotteinen kohdan ii) nojalla, $u$ on myös surjektiivinen. (Sen matriisin aste on $n$.)

On siis olemassa sellainen alkio $b \in K[x]$, että $u(b) = 1$. Mutta tämä merkitsee, että $ab = 1$ eli että $b$ on $a$:n käänteisalkio. Algebra $K[x]$ on siis kunta.

On vielä osoitettava, että $f$ on jaoton. Olkoon $f = gh$, missä $g$, $h \in K[X]$. Tällöin

$$g(x)h(x) = f(x) = 0,$$

ja koska $K[x]$ on kokonaisalue, joko $g(x) = 0$ tai $h(x) = 0$. Kohdan i) mukaan tämä merkitsee, että $g$ tai $h$ on jaollinen $f$:llä ja toinen tekijä on vakio. Siis $f$ on jaoton.

Lisäksi jaottomat polynomit $g \in K[X]$, jotka toteuttavat ehdon $g(x) = 0$, ovat $f$:n vakiokerrannaisia, joten $f$ on ainoa, jonka johtava kerroin on 1.

iv) Polynomi $f$ voidaan kirjoittaa muotoon

$$f(X) = Xg(X) + a,$$

missä $g \in K[X]$, $\deg(g) = n - 1$ ja $a = f(0) \in K$ on $f$:n vakiotermi. Jos $a = 0$, niin $0 = f(x) = xg(x)$, missä $g(x) \neq 0$, koska $\deg(g) < n$. Alkio $x$ ei silloin voi olla kääntyvä.

Jos taas $a \neq 0$, niin on olemassa käänteisalkio $a^{-1} \in K$ ja yhtälöstä $xg(x) + a = 0$ seuraa

$$x(-a^{-1}g(x)) = 1.$$

Alkiolla $x$ on siis tällöin algebraan $K[x]$ kuuluva käänteisalkio

$$x^{-1} = -a^{-1}g(x).$$

□

Korollaari 4.2.2. *Olkoon $A$ $K$-algebra. Alkio $x \in A$ on algebrallinen $K$:n suhteen, jos ja vain jos sen virittämä alialgebra $K[x]$ on äärellinen.*

*Todistus.* Jos $x$ on algebrallinen $K$:n suhteen, niin lauseen 4.2.1 kohdassa ii) on osoitettu, että $K[x]$ on äärellinen. Jos taas $x$ on transkendenttinen, niin $K[x]$ ei ole äärellinen, koska $(x^n)_{n\in\mathbf{N}}$ on sen vapaa ääretön perhe. □

Korollaari 4.2.3. *Jos $A$ on äärellinen $K$-algebra, niin sen jokainen alkio on algebrallinen $K$:n suhteen.*

*Todistus.* Alkion $x \in A$ virittämän alialgebran $K[x]$ aste on korkeintaan $[A : K]$. Jos $A$ on äärellinen, niin myös $K[x]$ on äärellinen, ja siten $x$ on algebrallinen $K$:n suhteen korollaarin 4.2.2 nojalla. □

Korollaari 4.2.4. *Olkoon $E$ kunnan $K$ laajennus, $A$ $E$-algebra ja $x \in A$ alkio, joka on algebrallinen $K$:n suhteen. Silloin*

i) *$x$ on algebrallinen $E$:n suhteen,*
ii) *$x$:n minimaalipolynomi $E$:n suhteen jakaa $x$:n minimaalipolynomin $K$:n suhteen, ja*
iii) *$x$:n aste $E$:n suhteen on enintään yhtä suuri kuin sen aste $K$:n suhteen.*

*Todistus.* Voidaan olettaa, että $K$ on $E$:n alikunta. (Samastetaan alkiot $\lambda \in K$ kuviensa $\lambda.1 \in E$ kanssa.) Olkoon $f \in K[X]$ alkion $x$ minimaalipolynomi.

Tällöin $f$ on myös $E$-kertoiminen polynomi, ja ehdosta $f(x) = 0$ seuraa siten, että $x$ on algebrallinen $E$:n suhteen ja $f$ on jaollinen $x$:n minimaalipolynomilla $g \in E[X]$ kunnan $E$ suhteen (lause 4.2.1, i).

Tällöin myös $x$:n aste $E$:n suhteen eli $\deg(g)$ on enintään sama kuin $\deg(f)$ eli $x$:n aste $K$:n suhteen. □

*Esimerkkejä.* 1) Imaginaariyksikkö $i$ on algebrallinen rationaalilukujen kunnan suhteen, sen aste on 2 ja minimaalipolynomi on

$$f(X) = X^2 + 1 \in \mathbf{Q}[X].$$

Kompleksiluku $i$ on algebrallinen myös kunnan $\mathbf{Q}$ laajennuksen $\mathbf{R}$ suhteen. Sen aste on 2 ja minimaalipolynomi on $f$ myös $\mathbf{R}$:n suhteen.

Sen virittämä $\mathbf{R}$:n laajennuksen $\mathbf{C}$ alialgebra $\mathbf{R}[i]$ on äärellinen ja sillä on kanta 1, $i$ (lause 4.2.1, ii). Kokonaisalueena se on kunta (lause 4.2.1, iii), nimittäin koko kompleksilukujen kunta

$$\mathbf{C} = \mathbf{R} + \mathbf{R}i = \mathbf{R}[i].$$

2) Reaaliluku $\sqrt{2}$ on algebrallinen kunnan $\mathbf{Q}$ suhteen, sen aste on 2 ja minimaalipolynomi on

$$f(X) = X^2 - 2 \in \mathbf{Q}[X].$$

Sen virittämä $\mathbf{Q}$:n laajennuksen $\mathbf{R}$ alialgebra $\mathbf{Q}[\sqrt{2}]$ on kunta (lause 4.2.1, iii) ja siten sama kuin adjunktiolla saatu laajennus

$$\mathbf{Q}(\sqrt{2}) = \mathbf{Q}[\sqrt{2}] = \mathbf{Q} + \mathbf{Q}\sqrt{2} \subset \mathbf{R}.$$

MÄÄRITELMÄ 4.2.5. Kunnan $K$ laajennus $E$ on *algebrallinen* ($K$:n suhteen), jos sen jokainen alkio on algebrallinen $K$:n suhteen. Laajennus, joka ei ole algebrallinen on *transkendenttinen*.

LAUSE 4.2.6. *Jos $E$ on kunnan $K$ äärellinen laajennus ja sen aste on $n$, niin $E$ on $K$:n algebrallinen laajennus ja sen jokaisen alkion aste $K$:n suhteen on asteen $n$ tekijä.*

*Todistus.* Jokainen $E$:n alkio $x$ on algebrallinen $K$:n suhteen korollaarin 4.2.3 mukaan. Lisäksi sen virittämä alialgebra $K[x]$ on kunta, koska $E$ on kokonaisalue (lause 4.2.1, iii), joten sen aste $[K[x] : K]$ on $E$:n asteen $n$ tekijä (kor. 4.1.4). □

LAUSE 4.2.7. *Olkoon $E$ kunnan $K$ äärellistyyppinen laajennus, jonka virittäjät $a_1, \ldots, a_m$ ovat algebrallisia $K$:n suhteen. Silloin $E$ on $K$:n äärellinen laajennus.*

*Jos $n_i$ on alkion $a_i$ aste kunnan $K(a_1, \ldots, a_{i-1})$ suhteen ($1 \leq i \leq m$), niin $E$:n aste $K$:n suhteen on $n_1 n_2 \cdots n_m$ ja alkiot*

$$a_1^{\nu_1} a_2^{\nu_2} \cdots a_m^{\nu_m} \qquad (0 \leq \nu_i \leq n_i - 1)$$

*muodostavat sen kannan. Erityisesti* $E = K[a_1, \ldots, a_m]$.

*Todistus.* Jos $m = 1$, niin väite pätee lauseen 4.2.1 kohdan ii) mukaan. Edetään induktiivisesti olettaen, että $E' = K(a_1, \ldots, a_{m-1})$ on äärellinen $K$:n laajennus, ja että alkiot

$$a_1^{\nu_1} a_2^{\nu_2} \cdots a_{m-1}^{\nu_{m-1}} \qquad (0 \leq \nu_i \leq n_i - 1)$$

muodostavat sen kannan. Tällöin $E$ on alkion $a_m$ virittämä $E'$:n laajennus:

$$E = K(a_1, \ldots, a_m) = E'(a_m).$$

Koska $a_m$ on algebrallinen $E'$:n suhteen, laajennus $E$ on sama kuin $a_m$:n virittämä $E'$-algebra $K[a_m]$ ja

$$a_m^{\nu_m} \qquad (0 \leq \nu_m \leq n_m - 1)$$

on sen kanta $E'$:n suhteen (lause 4.2.1, ii, iii). Lauseen 4.1.3 nojalla $E$ on äärellinen myös kunnan $K$ suhteen ja lauseen todistus osoittaa, että alkiot

$$(a_1^{\nu_1} \cdots a_{m-1}^{\nu_{m-1}}) a_m^{\nu_m} \qquad (0 \leq \nu_i \leq n_i - 1)$$

muodostavat sen kannan $K$:n suhteen.

Erityisesti jokainen $E$:n alkio on alkioiden $a_1, \ldots, a_m$ virittämässä alialgebrassa, eli $E = K[a_1, \ldots, a_m]$. □

Korollaari 4.2.8. *Olkoon $E$ kunnan $K$ laajennus ja $A$ sen osajoukko. Jos jokainen $A$:n alkio on algebrallinen $K$:n suhteen, niin $K(A)$ on $K$:n algebrallinen laajennus ja $K[A] = K(A)$.*

*Todistus.* Jokainen laajennuksen $K(A)$ alkio voidaan esittää osamääränä

$$x = pq^{-1},$$

missä $p$, $q$ ovat $A$:n virittämän alialgebran $K[A]$ alkioita ja $q \neq 0$.

Tällöin $p$ ja $q$ ovat esitettävissä $A$:n alkioiden $K$-kertomisina polynomeina, ja koska näissä on vain äärellisen monta monomia, on olemassa sellainen $A$:n äärellinen osajoukko

$$F = \{a_1, \ldots, a_m\},$$

että $p$ ja $q$ ovat jo sen virittämässä alialgebrassa $K[F]$.

Kun jokainen $a_i$ on algebrallinen $K$:n suhteen, niin lauseen 4.2.7 nojalla $K[F]$ on $K$:n äärellinen laajennus ja sama kuin kunta $K(F)$. Tällöin $K[F]$ sisältää alkioiden $p$ ja $q$ ohella myös niiden osamäärän $x$ ja tämä on siten algebrallinen $K$:n suhteen (kor. 4.2.3).

Lisäksi alialgebran $K[F]$ alkiona $x$ on myös alialgebrassa $K[A]$; siis nähdään, että $K[A] = K(A)$. □

**Algebrallisuuden transitiivisuus.**

LAUSE 4.2.9. *Olkoot $E$ ja $F$ kunnan $K$ laajennuksia ja $K \subset E \subset F$. Tällöin $F$ on algebrallinen $K$:n suhteen, jos ja vain jos $E$ on algebrallinen $K$:n suhteen ja $F$ on algebrallinen $E$:n suhteen.*

*Todistus.* Jos $F$ on algebrallinen $K$:n suhteen, niin sen alikunta $E$ on myös algebrallinen $K$:n suhteen ja lisäksi $F$ on algebrallinen välikunnan $E$ suhteen (kor. 4.2.4).

Oletetaan kääntäen, että $E$ on algebrallinen $K$:n suhteen ja $F$ on algebrallinen $E$:n suhteen. On osoitettava, että jokainen $F$:n alkio $x$ on algebrallinen $K$:n suhteen.

Joka tapauksessa $x$ on algebrallinen $E$:n suhteen. Olkoon $g \in E[X]$ sen minimaalipolynomi ja olkoon $A$ polynomin $g$ kertoimien joukko. Tällöin $g$ kuuluu polynomialgebraan $K(A)[X]$. Alkio $x$ on siis algebrallinen kunnan $K(A)$ suhteen, joten sen virittämä laajennus

$$K(A \cup \{x\}) = K(A)(x)$$

on $K(A)$:n äärellinen laajennus.

Toisaalta $A$ on $E$:n äärellinen osajoukko ja oletuksen mukaan sen alkiot ovat algebrallisia $K$:n suhteen. Lauseen 4.2.7 nojalla $K(A)$ on siten $K$:n äärellinen laajennus. Laajennusten asteiden kertolaskuominaisuudesta (lause 4.1.3) seuraa silloin, että $K(A \cup \{x\})$ on $K$:n äärellinen laajennus. Sen alkiona $x$ on siis algebrallinen $K$:n suhteen. □

MÄÄRITELMÄ 4.2.10. Kunnan $E$ alikunta $K$ on *algebrallisesti suljettu $E$:ssä*, jos jokainen $K$:n suhteen algebrallinen $E$:n alkio on $K$:ssa.

LAUSE 4.2.11. *Jos $E$ on kunnan $K$ laajennus, niin kaikkien $K$:n suhteen algebrallisten $E$:n alkioiden joukko $L$ on $E$:n alilaajennus, joka on algebrallisesti suljettu $E$:ssä.*

*Todistus.* Korollaarin 4.2.8 nojalla joukon $L$ virittämä alilaajennus $K(L)$ on algebrallinen $K$:n suhteen. Kaikki sen alkiot ovat silloin joukossa $L$, joka on siis sama kuin laajennus $K(L)$.

Jos lisäksi $x$ on jokin $L$:n suhteen algebrallinen $E$:n alkio, niin sen virittämä laajennus $L(x)$ on algebrallinen paitsi $L$:n myös $K$:n suhteen lauseen 4.2.9 nojalla. Mutta tällöin $x$ kuuluu joukkoon $L$, ja tämä on siten algebrallisesti suljettu $E$:ssä. □

Lauseessa määritetelty laajennus $L$ on $E$:n suurin alilaajennus, joka on algebrallinen kunnan $K$ suhteen, ja sitä sanotaan $K$:n *algebralliseksi sulkeumaksi laajennuksessa $E$*.

*Esimerkki* 3) Kompleksilukuja, jotka ovat algebrallisia rationaalilukujen kunnan $\mathbf{Q}$ suhteen sanotaan *algebrallisiksi luvuiksi*. Esimerkiksi $\sqrt{2}$ ja kaikkien kokonaislukukertoimisten polynomiyhtälöiden $f(x) = 0$ juuret ovat algebrallisia lukuja.

Algebrallisten lukujen joukko on lauseen 4.2.11 perusteella kunta, *algebrallisten lukujen kunta* $\mathbf{A} \subset \mathbf{C}$. Koska se on algebrallisesti suljettu

$\mathbf{C}$:ssä, se sisältää kaikki luvut, jotka voidaan muodostaa ratkaisemalla polynomiyhtälöitä, joiden kertoimet ovat $\mathbf{A}$:ssa.

*Huomautus.* Koska polynomien $f \in \mathbf{Q}[X]$ joukko on numeroituva, ja jokaisella polynomilla on vain äärellinen määrä juuria, algebrallisten lukujen kunta $\mathbf{A}$ on numeroituva. Se on siten vain pieni osa koko kompleksilukujen kunnasta $\mathbf{C}$, jonka muut luvut ovat *transkendenttilukuja*.

**Sovellus: Geometriset konstruktiot.**

MÄÄRITELMÄ 4.2.12. Tason $\mathbf{R}^2$ *kuvio* on sen osajoukko $G$, jonka alkioita sanotaan kuvion $G$ *pisteiksi*.

*Kuvion $G$ suoralla* tarkoitetaan kahden $G$:n pisteen kautta kulkevaa suoraa. *Kuvion $G$ ympyrä* on ympyrä, jonka keskipiste ja jokin kehän piste ovat $G$:ssä.

*Geometrinen konstruktio* kuviossa $G$ on pistejono

$$P_1, P_2, \ldots, P_n \in \mathbf{R}^2,$$

missä $P_i$ on kuvion $G \cup \{P_1, \ldots, P_{i-1}\}$ kahden suoran tai kahden ympyrän tai suoran ja ympyrän leikkauspiste $(1 \leq i \leq n)$.

Piste $P \in \mathbf{R}^2$ *saadaan geometrisella konstruktiolla* kuviosta $G$, jos on olemassa sellainen geometrinen konstruktio $P_1, \ldots, P_n$ kuviossa $G$, missä $P_n = P$.

Jokaiseen tason pisteeseen $P = (x, y) \in \mathbf{R}^2$ liittyy kunta

$$K_P = \mathbf{Q}(x, y),$$

ja samoin jokaiseen kuvioon $G \subset \mathbf{R}^2$ liittyy kunta

$$K_G = \mathbf{Q}\Big(\bigcup_{P \in G} K_P\Big),$$

joka on pienin pisteiden $P \in G$ koordinaatit sisältävä $\mathbf{R}$:n alikunta.

LAUSE 4.2.13. *Jos piste $P = (x, y)$ saadaan kuviosta $G \subset \mathbf{R}^2$ geometrisella konstruktiolla, niin sen koordinaatit $x$ ja $y$ ovat algebrallisia kunnan $K_G$ suhteen ja niiden virittämän laajennuksen aste on luvun* 2 *potenssi:*

$$[K_G(x, y) : K_G] = 2^k \qquad , \; k \in \mathbf{N}.$$

*Todistus.* Olkoon $P_1, \ldots, P_n$ jokin sellainen geometrinen konstruktio $G$:ssä, missä $P_n = P$. Olkoon $P_i = (x_i, y_i)$ $(1 \leq i \leq n)$ ja olkoon

$$K_i = K_G(x_1, y_1, \ldots, x_i, y_i) \qquad (0 \leq i \leq n).$$

Tällöin jokainen $K_i$ on sitä edeltävän kunnan $K_{i-1}$ laajennus. Osoitetaan, että laajennuksen aste on enintään 2.

Piste $P_i$ on kahden kuvion $G \cup \{P_1, \ldots, P_{i-1}\}$ suoran tai ympyrän leikkauspiste. Näiden kertoimet ovat kunnassa $K_{i-1}$ ja leikkauspiste $(x_i, y_i)$ saadaan laskemalla enintään yksi neliöjuuri $\sqrt{z_i}$, missä $z_i \in K_{i-1}$ (harj. teht.). Laajennus

$$K_i = K_{i-1}(x_i, y_i)$$

on tällöin joko sama kuin $K_{i-1}$ tai $K_{i-1}(\sqrt{z_i})$, ja sen aste on 1 tai 2.

Asteen multiplikatiivisuudesta (lause 4.1.3) seuraa tällöin

$$[K_n : K_0] = [K_n : K_{n-1}] \cdots [K_1 : K_0] = 2^m,$$

missä $0 \leq m \leq n$. Koska pisteen $P = P_n$ koordinaatit $x$, $y$ ovat kunnassa $K_n$, niiden virittämän alilaajennuksen aste kunnan $K_G = K_0$ suhteen on korollaarin 4.1.4 nojalla asteen $2^m$ tekijä $2^k$ $(0 \leq k \leq m)$. □

*Esimerkkejä.* 4) *Ympyrän neliöinti.* On konstruoitava geometrisesti neliö $Q$, jolla on sama pinta-ala kuin annetulla ympyrällä $C$.

Valitaan koordinaatisto siten, että $C$ on yksikköympyrä. Se kuuluu kuvioon $G$, joka sisältää origon $P_0 = (0, 0)$ ja jonkin kehän pisteen $P_1$. Koordinaatistoa kääntämällä voidaan asettaa $P_1 = (1, 0)$.

Jos voidaan geometrisesti konstruoida neliö $Q$, jolla on pinta-ala $\pi$, niin se voidaan asettaa esimerkiksi siten, että sen kärjet ovat $P_0$ ja $P_2 = (\sqrt{\pi}, 0)$ sekä kaksi muuta pistettä.

Koska kuvion $G$ kunta on $\mathbf{Q}$, on $\mathbf{Q}(\sqrt{\pi})$ silloin lauseen 4.2.13 nojalla $\mathbf{Q}$:n äärellinen laajennus. Tämä on kuitenkin mahdotonta, koska $\pi$ on transkendenttiluku (*Lindemann*, 1882), ja siten jo alilaajennuksen $\mathbf{Q}(\pi)$ aste on ääretön.

Ympyrän neliöinti harpilla ja viivoittimella on siis mahdotonta.

5) *Kuution kahdennus.* On konstruoitava sellaisen kuution särmä (jana), jonka tilavuus on kaksi kertaa (särmänsä avulla) annetun kuution tilavuus.

Annetun särmän päätepisteiksi voidaan valita $P_0 = (0, 0)$ ja $P_1 = (1, 0)$. Ne muodostavat kuvion $G$, jonka kunta on $\mathbf{Q}$. Jos konstruktio onnistuu, voidaan esimerkiksi piste $P_2 = (\sqrt[3]{2}, 0)$ konstruoida geometrisesti $G$:ssä.

Luku $\sqrt[3]{2}$ on polynomin $f(X) = X^3 - 2 \in \mathbf{Q}[X]$ juuri, ja tämä on jaoton, koska sillä ei ole yhtään rationaalista juurta, joten se on minimaalipolynomi. Pisteen $P_2$ kunnan $\mathbf{Q}(\sqrt[3]{2})$ aste $\mathbf{Q}$:n suhteen on siis 3. Koska tämä ei ole luvun 2 potenssi, konstruktio on mahdoton.

6) *Kulman kolmiajako.* On jaettava annettu kulma kolmeen yhtä suureen osaan harpilla ja viivoittimella.

Tarkastellaan kuviota $G$, jonka muodostavat origo $P_0 = (0, 0)$, piste $P_1 = (1, 0)$ ja jokin kolmas piste $P_2$. Jaettavan kulman kärkenä on $P_0$ ja sen kyljet kulkevat pisteiden $P_1$ ja $P_2$ kautta.

Voidaan olettaa, että piste $P_2$ on yksikköympyrällä, koska se voidaan konstruoida kulman kyljen ja yksikköympyrän leikkauspisteenä. Tällöin on $P_2 = (\cos 3\alpha, \sin 3\alpha)$ jollakin reaaliluvulla $\alpha$. Jos jako onnistuu, saadaan geometrinen konstruktio pisteelle $P_3 = (\cos \alpha, \sin \alpha)$.

Trigonometristen funktioiden yhteenlaskukaavoista saadaan yhtälö

$$\cos 3\alpha = 4 \cos^3 \alpha - 3 \cos \alpha.$$

Kun valitaan jaettavaksi kulmaksi $2\pi/3$, on $P_2 = (-\frac{1}{2}, \frac{\sqrt{3}}{2})$. Kuvion $G$ kunta on tällöin

$$K_G = \mathbf{Q}(\sqrt{3}),$$

ja sen aste $\mathbf{Q}$:n suhteen on $[K_G : \mathbf{Q}] = 2$. Toisaalta $P_3 = (x, y)$, missä $x$ toteuttaa jaottoman polynomiyhtälön

$$4x^3 - 3x + \frac{1}{2} = 0.$$

Sen virittämän laajennuksen aste $[\mathbf{Q}(x) : \mathbf{Q}]$ on siis 3.

Jos geometrinen konstruktio onnistuu, on kunnan $K_G$ laajennuksen $K_G(x, y)$ aste luvun 2 potenssi, ja siten

$$[K_G(x, y) : \mathbf{Q}] = [K_G(x, y) : K_G][K_G : \mathbf{Q}] = 2^k \cdot 2$$

jollakin $k \in \mathbf{N}$. Koska $\mathbf{Q}(x) \subset K_G(x, y)$, on

$$[\mathbf{Q}(x) : \mathbf{Q}] = 2^l,$$

missä $0 \leq l \leq k + 1$, vastoin yllä todistettua. Konstruktio on siten mahdoton.

7) *Säännöllinen p-kulmio*, kun $p$ on alkuluku.

Geometriset konstruktiot voidaan suorittaa reaalisen tason asemasta myös kompleksitasossa $\mathbf{C}$ tulkiten pisteet $P = (x, y)$ kompleksiluvuiksi $z = x + iy$. Lause 4.2.13 pätee tällöin edelleen oleellisesti samalla todistuksella. Pisteiden ja kuvioiden kunnat vain ovat $\mathbf{C}$:n alikuntia.

Säännöllisen $p$-kulmion kärkinä yksikköympyrällä ovat binomiyhtälön $z^p - 1 = 0$ juuret eli $p$:nnet *ykkösenjuuret*. Binomilla $Z^p - 1$ on triviaali tekijä $Z - 1$ ja toinen tekijä

$$Z^{p-1} + Z^{p-2} + \cdots + Z + 1 \in \mathbf{Q}[Z]$$

on jaoton, kun $p$ on alkuluku. (Tämä seuraa esim. Eisensteinin kriteeriosta, lause 3.3.9; ks. esim. 3.3.2.)

Säännöllisen $p$-kulmion kunta on $\mathbf{Q}(z)$, missä $z$ on eräs ykkösenjuuri (esim. $e^{2\pi i/p}$) ja sen aste on

$$[\mathbf{Q}(z) : \mathbf{Q}] = p - 1,$$

kun $p$ on alkuluku. Näin saadaan seuraava tulos.

*Jos säännöllinen p-kulmio, missä p on alkuluku, voidaan konstruoida harpilla ja viivoittimella, niin $p = 2^k + 1$ jollakin $k \in \mathbf{N}$.*

Ei ole vaikea nähdä, että $2^k + 1$ on jaollinen, jos $k$ ei ole luvun 2 potenssi. Alkulukuja $p = 2^{2^t} + 1$ sanotaan *Fermat'n alkuluvuiksi*. Ainoat tunnetut ovat arvoja $t = 0, 1, 2, 3, 4$ ja $k = 1, 2, 4, 8, 16$ vastaavat luvut

$$p = 3, 5, 17, 257, 65537.$$

(Seuraavalla luvulla $2^{32} + 1$ on tekijä 641, jonka löysi *Euler*.)

Kääntäen *Gauss* osoitti 1798 (*Disquisitiones arithmetique*, 1801), että säännöllinen $p$-kulmio voidaan konstruoida harpilla ja viivoittimella, kun $p$ on Fermat'n alkuluku (tai yleisemmin tällaisten tulo).

**Harjoitustehtäviä**

1) Olkoon $\alpha \in \mathbf{C}$ polynomin $f = X^3 + X^2 + X + 2$ juuri. Esitettävä $(\alpha - 1)^{-1}$ muodossa $a\alpha^2 + b\alpha + c$, missä $a$, $b$, $c \in \mathbf{Q}$.

2) Olkoon $E = \mathbf{Q}(\sqrt{2}, \sqrt{3})$ ja $\xi = \sqrt{2} + \sqrt{3} \in E$. Osoitettava:
i) $\sqrt{3} \notin \mathbf{Q}(\sqrt{2})$. (Muuten olisi $\sqrt{3} = x + y\sqrt{2}$, missä $x$, $y \in \mathbf{Q}$.)
ii) $[E : \mathbf{Q}(\sqrt{2})] = 2$ ja $[E : \mathbf{Q}] = 4$.
iii) $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$ on $E$:n kanta kunnan $\mathbf{Q}$ suhteen.
iv) $\sqrt{2} \in \mathbf{Q}(\xi)$ ja $\sqrt{3} \in \mathbf{Q}(\xi)$. (Lasketaan $\xi^3$.)
Pääteltävä, että $E = \mathbf{Q}(\xi)$, ja etsittävä $\xi$:n minimaalipolynomi $\mathbf{Q}$:n suhteen.

3) Olkoon $\xi = \sqrt[4]{2} \in \mathbf{R}$. Osoitettava, että
i) $\xi$:n minimaalipolynomi $\mathbf{Q}$:n suhteen on $f = X^4 - 2$;
ii) $\mathbf{Q}(\xi)$:n ainoa aito alilaajennus $E \neq \mathbf{Q}$ on $\mathbf{Q}(\sqrt{2})$. (Etsitään ensin $\xi$:n minimaalipolynomi $E$:n suhteen. Se on $f$:n tekijä, jonka aste on $[\mathbf{Q}(\xi) : E]$.)

4) Olkoon $E$ kunnan $K$ laajennus. Osoitettava:
i) Jos $A$ on $E$:n alialgebra, $x \in A$ algebrallinen $K$:n suhteen ja $x \neq 0$, niin $x^{-1} \in A$.
ii) Jos $x \in E$, $x \neq 0$ ja $x^{-1} \in K[x]$, niin $x$ on algebrallinen $K$:n suhteen.
Pääteltävä, että $E$ on $K$:n algebrallinen laajennus, jos ja vain jos jokainen $E$:n ali-$K$-algebra on kunta.

5) Olkoot $x = \cos 2\pi/5$ ja $y = \sin 2\pi/5$ yksikköympyrään piirretyn säännöllisen viisikulmion kärjen koordinaatit. Osoitettava, että $\mathbf{Q}$:n laajennuksen $\mathbf{Q}(x, y)$ aste on 4 tai 2. ($x = (\zeta + \zeta^{-1})/2$, missä $\zeta = e^{2\pi i/5}$ toteuttaa ehdon $\sum_{i=-2}^{2} \zeta^i = 0$.)

6) Olkoon $K$ kunta, $E$ sen laajennus ja $x \in E$ transkendenttinen $K$:n suhteen. Osoitettava:
i) Jos $y \in K(x)$, niin $y = p(x)q(x)^{-1}$, missä $p$, $q \in K[X]$ ja $q \neq 0$.
ii) Jos $p$, $q \in K[X]$, $q \neq 0$ ja $y \in E \setminus K$, niin $p - yq \neq 0$.
iii) Jos $y \in K(x)$, mutta $y \notin K$, niin $x$ on algebrallinen $K(y)$:n suhteen.
Pääteltävä, että $K$ on algebrallisesti suljettu laajennuksessa $K(x)$ (eli $K(x)$ on $K$:n *puhtaasti transkendenttinen* laajennus).

## 4.3. Algebrallisesti suljetut laajennukset

Tässä pykälässä tutkitaan kuntia, joita ei voi laajentaa algebrallisesti.

LAUSE 4.3.1. *Olkoon $K$ kunta. Seuraavat ehdot ovat yhtäpitävät.*

a) *Jokainen $K[X]$:n polynomi, joka ei ole vakio, on tulo asteen* 1 *polynomeista.*

b) *Jokaisella $K[X]$:n polynomilla, joka ei ole vakio, on ainakin yksi juuri kunnassa $K$.*
c) *Jokaisen $K[X]$:n jaottoman polynomin aste on* 1.
d) *Jokaisen kunnan $K$ algebrallisen laajennuksen aste on* 1.

*Todistus.* Ehdosta a) seuraa välittömästi c), koska jaottomalla polynomilla on vain yksi tekijä.

c) $\Rightarrow$ b): Olkoon $f \in K[X]$ polynomi, joka ei ole vakio. Tarkastellaan sen tekijöitä $g \in K[X]$, jotka eivät ole vakioita, ja valitaan niistä sellainen, jonka aste on pienin mahdollinen.

Tällainen tekijä on välttämättä jaoton, joten ehdon c) ollessa voimassa se on $g = aX + b$, missä $a$, $b \in K$ ja $a \neq 0$. Tällöin $x = -ba^{-1}$ on kunnassa $K$ ja $g(x) = 0$. Koska $g$ jakaa polynomin $f$, sen juuri $x$ on myös $f$:n juuri.

b) $\Rightarrow$ a): Olkoon $f \in K[X]$ polynomi, joka ei ole vakio. Oletetaan, että ehto b) on voimassa, ja osoitetaan induktiolla $f$:n asteen $n$ suhteen, että $f$ on tulo asteen 1 tekijöistä. Väite on selvä, jos $n = 1$.

Olkoon $n > 1$ ja $a \in K$ jokin $f$:n juuri. Tällöin $f = (X - a)g$, missä $g \in K[X]$ ja $\deg(g) = n - 1 > 0$. Induktio-oletuksen nojalla $g$ voidaan esittää tulona

$$g = \prod_{k=1}^{n-1} h_k,$$

missä jokaisen polynomin $h_k \in K[X]$ aste on 1. Kun asetetaan $h_n = X - a$, saadaan siis polynomille $f$ tuloesitys

$$f = \prod_{k=1}^{n} h_k,$$

missä jokaisen tekijän aste on 1.

c) $\Rightarrow$ d): Olkoon $L$ jokin kunnan $K$ algebrallinen laajennus. Merkintöjen yksinkertaistamiseksi voidaan samastaa $K$ kuvansa kanssa kunnassa $L$, ja olettaa, että $L$ on $K$:n ylikunta.

Olkoon $x$ jokin kunnan $L$ alkio. Oletuksen nojalla se on algebrallinen kunnan $K$ suhteen. Olkoon $f \in K[X]$ sen minimaalipolynomi $K$:n suhteen.

Koska $L$ on kokonaisalue, $f$ on jaoton (lause 4.2.1, iii), ja siten kohdan c) nojalla $f = X - a$ jollakin $a \in K$. Mutta tällöin ehdosta $f(x) = 0$ seuraa $x = a$. Siis saadaan $L = K$ ja edelleen $[L : K] = 1$.

d) $\Rightarrow$ c): Olkoon $f \in K[X]$ jaoton polynomi. Sen aste on $n \geq 1$, ja sen virittämä pääideaali $(f) \subset K[X]$ on maksimaalinen (kuten Algebra I:ssä osoitetaan).

Tekijäalgebra $L = K[X]/(f)$ on tällöin kunta (kor. 1.8.3) ja siten $K$:n laajennus. Tuntemattoman $X$ luokka $x \in L$ toteuttaa ehdot $f(x) = 0$ ja $L = K[x]$. Alkio $x$ ja sen virittämä laajennus $L$ ovat siis algebrallisia $K$:n suhteen.

Koska $f$ on jaoton, se on vakiokerrointa vaille sama kuin $x$:n minimaalipolynomi. Laajennuksen $L = K[x]$ aste on siten polynomin $f$ aste $n$ (lause 4.2.1, ii). Jos ehto d) on voimassa, on siis $n = 1$. □

MÄÄRITELMÄ 4.3.2. Kunta $K$ on *algebrallisesti suljettu*, jos se toteuttaa lauseen 4.3.1 ehdot a) - d).

*Esimerkki* 1) Kompleksilukujen kunta $\mathbf{C}$ on algebrallisesti suljettu. Ehto b) tunnetaan nimellä *algebran peruslause* (*Gauss*, 1799). (Eräs todistus esitetään Funktioteoria I:n kurssissa.)

LAUSE 4.3.3. *Jos $\Omega$ on algebrallisesti suljettu kunta ja $K$ on sen alikunta, niin $K$:n algebrallinen sulkeuma $\bar{K}$ laajennuksessa $\Omega$ on algebrallisesti suljettu kunta.*

*Todistus.* Olkoon $f \in \bar{K}[X]$ polynomi, joka ei ole vakio. Se on myös algebran $\Omega[X]$ polynomi, joten sillä on juuri $x \in \Omega$, koska $\Omega$ toteuttaa lauseen 4.3.1 ehdon b).

Tällöin $x$ on algebrallinen kunnan $\bar{K}$ suhteen, ja koska $\bar{K}$ on algebrallisesti suljettu $\Omega$:ssa (lause 4.2.11), $x$ kuuluu kuntaan $\bar{K}$. Lauseen 4.3.1 ehto b) on siis voimassa myös kunnassa $\bar{K}$, joka on siten algebrallisesti suljettu. □

*Esimerkki* 2) Algebrallisten lukujen kunta $\mathbf{A}$ on $\mathbf{Q}$:n algebrallinen sulkeuma kunnassa $\mathbf{C}$ (ks. esim. 4.2.3). Koska $\mathbf{C}$ on algebrallisesti suljettu (ks. esim. 4.3.1), myös $\mathbf{A}$ on algebrallisesti suljettu kunta.

**Upotuslause.**

LAUSE 4.3.4. *Olkoon $K$ kunta, $E$ sen algebrallinen laajennus ja $\Omega$ jokin $K$:n algebrallisesti suljettu laajennus. Silloin on olemassa $K$-homomorfismi $u\colon E \to \Omega$.*

*Todistus.* Tarkastellaan pareja $(E', u)$, missä $E'$ on $E$:n alilaajennus ja $u$ on $K$-homomorfismi $E' \to \Omega$. Olkoon $(E', u)$ maksimaalinen tällainen pari. (Jos $[E : K]$ on äärellinen, voidaan valita suurin aste $[E' : K]$; muuten nojaudutaan Zornin lemmaan.) On riittävää osoittaa, että $E' = E$.

Olkoon $x \in E$. Koska $x$ on algebrallinen $K$:n suhteen, se on algebrallinen myös $E'$:n suhteen (ks. kor. 4.2.4). Olkoon $f \in E'[X]$ sen minimaalipolynomi $E'$:n suhteen. Tällöin on olemassa kanoninen isomorfismi (lause 4.2.1, ii)

$$E'[X]/(f) \xrightarrow{\sim} E'[x]. \tag{1}$$

Olkoon $g \in \Omega[X]$ polynomi, joka saadaan korvaamalla polynomin $f$ kertoimet kuvillaan homomorfismissa $u$. Koska $\Omega$ on algebrallisesti suljettu, polynomilla $g$ on juuri $y \in \Omega$.

Struktuurihomomorfismilla $u$ varustettuna $\Omega$ on kunnan $E'$ laajennus. Olkoon $\varphi\colon E'[X] \to \Omega$ sijoitushomomorfismi $h \mapsto h(y)$. (Kunnan

$E'$ laajennuksessa $(\Omega, u)$ pätee silloin

$$\varphi\Big(\sum_k \alpha_k X^k\Big) = \sum_k \alpha_k . y^k = \sum_k u(\alpha_k) y^k .)$$

Tällöin erityisesti $\varphi(f) = g(y) = 0$, joten ideaali $(f)$ sisältyy homomorfismin $\varphi$ ytimeen. Hajotelmalauseen nojalla saadaan siten $E'$-homomorfismi $E'[X]/(f) \to \Omega$ ja siitä isomorfismin (1) avulla $K$-homomorfismi

$$u' \colon E'[x] \to \Omega,$$

joka jatkaa struktuurihomomorfismin $u \colon E' \to \Omega$.

Parin $(E', u)$ maksimaalisuuden perusteella on $E'[x]$ silloin sama kuin $E'$, eli $x$ on $E'$:n alkio. Koska $x$ on mielivaltainen $E$:n alkio, on $E'$ siis koko $E$, ja $u$ on $K$-homomorfismi $E \to \Omega$. □

Koska kuntien homomorfismit ovat injektiivisiä, voidaan sanoa, että $u$ on laajennuksen $E$ *upotus* kuntaan $\Omega$. Tällainen upotus ei yleensä ole yksikäsitteinen. Seuraavaksi tutkitaan, millaisia ovat kuvat $u(E) \subset \Omega$.

Tarkastelu perustuu siihen, että polynomin $f \in K[X]$ juuren $x \in E$ kuva $u(x) \in \Omega$ on toteuttaa ehdon $f(u(x)) = 0$. Kuvassa $u(E)$ voi siis olla vain alkioiden $x \in E$ minimaalipolynomien juuria.

**Juurikunnat.** Olkoon $K$ kunta. Tarkastellaan algebran $K[X]$ polynomeja $f_i$ $(i \in I)$, jotka eivät ole vakioita.

MÄÄRITELMÄ 4.3.5. Kunnan $K$ laajennus $E$ on $K[X]$:n polynomiperheen $(f_i)_{i\in I}$ *juurikunta*, jos

i) jokainen $f_i$ hajoaa $E[X]$:ssä asteen 1 polynomien tuloksi, ja

ii) $E = K(\bigcup_{i\in I} R_i)$, missä $R_i$ on $f_i$:n juurien joukko $E$:ssä $(i \in I)$.

*Huomautus.* Polynomin juuret eivät muutu, kun se kerrotaan vakiolla $c \in K$, $c \neq 0$. Siten voidaan tarvittaessa olettaa, että polynomi $f_i$ on pääpolynomi (eli sen korkeimman potenssin kerroin on 1).

LAUSE 4.3.6. *Olkoon $K$ kunta ja $(f_i)_{i\in I}$ perhe $K[X]$:n polynomeja, jotka eivät ole vakioita. Silloin on olemassa perheen $(f_i)_{i\in I}$ juurikunta.*

*Todistus.* Voidaan olettaa, että jokainen $f_i$ on pääpolynomi ja että $I$ ei ole tyhjä. (Sillä $E = K$ on juurikunta, jos $I = \emptyset$.)

Oletetaan aluksi, että perheessä on vain yksi polynomi $f$, ja osoitetaan juurikunnan olemassaolo induktiolla sen asteen $n \geq 1$ suhteen.

Jos $n = 1$, niin $f = X - a$ jollakin $a \in K$, ja siten $E = K(a) = K$ on $f$:n juurikunta. Yleisessä tapauksessa valitaan jokin $f$:n jaoton tekijä $h \in K[X]$, ja muodostetaan $K$:n laajennus

$$L = K[X]/(h),$$

jossa tuntemattoman $X$ luokka $a \in L$ toteuttaa yhtälön $h(a) = 0$ ja virittää koko laajennuksen: $L = K[a] = K(a)$.

Tällöin $a$ on myös $f$:n juuri, joten $f$ voidaan kirjoittaa muotoon

$$f = (X - a)g,$$

missä $g \in L[X]$ on asteen $n-1$ polynomi. Induktio-oletuksen nojalla polynomilla $g$ on juurikunta $E$, joka on $L$:n laajennus. Tämä merkitsee, että $g$ on algebrassa $E[X]$ tulo

$$g = \prod_{i=1}^{n-1}(X - a_i),$$

ja juuret $a_i$ virittävät laajennuksen $E = L(a_1, \ldots, a_{n-1})$.

Jos merkitään $a_0 = a$, saadaan tuloesitys

$$f = \prod_{i=0}^{n-1}(X - a_i)$$

algebrassa $E[X]$. Koska lisäksi

$$E = K(a_0)(a_1, \ldots, a_{n-1}) = K(a_0, \ldots, a_{n-1}),$$

$E$ on polynomin $f$ juurikunta.

Jos polynomeja on useita, mutta vain äärellinen määrä, voidaan muodostaa tulo

$$f = \prod_{i \in I} f_i \in K[X],$$

joka ei ole vakio. Yllä esitetyn nojalla sillä on juurikunta $E$, ja koska $f$:n juurien joukko on yhdiste polynomien $f_i$ juurien joukoista, $E$ on myös äärellisen perheen $(f_i)_{i\in I}$ juurikunta.

Työläin tapaus on se, jossa joukko $I$ on ääretön. Osoitetaan ensin, että kunnalla $K$ on laajennus $K_1$, jossa jokaisella polynomilla $f_i$ on juuri. Tarkastellaan polynomialgebraa $A = K[(X_i)_{i\in I}]$. Jokaiseen polynomiin $f_i$ liittyy algebran $A$ polynomi $f_i(X_i)$. Olkoon $\mathfrak{a} \subset A$ perheen $(f_i(X_i))_{i\in I}$ virittämä ideaali. Osoitetaan, että se on aito ideaali eli $\mathfrak{a} \neq A$.

Jos $\mathfrak{a}$ sisältää alkion 1, niin on olemassa esitys

$$1 = \sum_{j \in J} g_j f_j(X_j), \tag{2}$$

missä $J$ on $I$:n äärellinen osajoukko ja $g_j \in A$ $(j \in J)$.

Yllä esitetyn mukaan äärellisellä perheellä $(f_j)_{j\in J}$ on juurikunta $E$. Jokaista indeksiä $j \in J$ kohti on silloin olemassa sellainen $x_j \in E$, että $f_j(x_j) = 0$. (Tässä käytetään oletusta, että $f_j$ ei ole vakio.) Valitaan lisäksi alkiot $x_i \in E$ mielivaltaisesti, kun $i \in I \setminus J$. Sijoittamalla arvot $x_i$ yhtälöön (2) saadaan tällöin

$$1 = \sum_{j \in J} g_j((x_i)_{i\in I}) f_j(x_j) = 0.$$

Tämä ristiriita osoittaa, että 1 ei voi kuulua ideaaliin $\mathfrak{a}$.

Krullin lauseen 1.7.7 nojalla $\mathfrak{a}$ sisältyy johonkin maksimaaliseen ideaaliin $\mathfrak{m} \subset A$. Tekijäalgebra $K_1 = A/\mathfrak{m}$ on silloin kunta (kor. 1.8.3), ja siten $K$:n laajennus.

Koska $\mathfrak{m}$ sisältää polynomit $f_i(X_i)$ $(i \in I)$, tuntemattomien $X_i$ luokat $x_i \in K_1$ toteuttavat ehdot $f_i(x_i) = 0$ ja ovat siten algebrallisia $K$:n suhteen. Ne virittävät laajennuksen $K_1$ myös $K$-algebrana (vrt. kor. 4.2.8)

$$K_1 = K[(x_i)_{i\in I}] = K((x_i)_{i\in I}).$$

Voidaan olettaa, että $K$ on $K_1$:n alikunta (samastetaan kuvansa kanssa). Polynomit $f_i$ voidaan nyt kirjoittaa tuloiksi

$$f_i = (X - x_{i1})f_{1i},$$

missä $x_{i1} = x_i \in K_1$ ja $f_{1i} \in K_1[X]$ $(i \in I)$. Jos $f_i$:n aste on 1, polynomi $f_{1i}$ on vakio 1, koska $f_i$ on pääpolynomi. Toistetaan konstruktio niillä polynomeilla $f_{1i}$, jotka eivät ole vakioita. Näin saadaan jono ylikuntia

$$K \subset K_1 \subset K_2 \subset \cdots,$$

jotka toteuttavat kaikilla $i \in I$ ehdot

i) jos $\deg(f_i) > n$, niin

$$f_i = \prod_{k=1}^{n}(X - x_{ik})f_{ni},$$

missä $x_{ik} \in K_k$ $(1 \leq k \leq n)$ ja $f_{ni} \in K_n[X]$;

ii) jos $\deg(f_i) = m \leq n$, niin

$$f_i = \prod_{k=1}^{m}(X - x_{ik}),$$

missä $x_{ik} \in K_k$ $(1 \leq k \leq m)$.

Lisäksi jokainen $K_n$ on polynomien $f_i$ niiden juurien $x_{ik}$ virittämä laajennus, joilla $1 \leq k \leq \min(n, \deg(f_i))$. Yhdiste

$$E = \bigcup_{n\in\mathbf{N}} K_n$$

on tällöin perheen $(f_i)_{i\in I}$ juurikunta. □

Juurikuntien tärkein ominaisuus on yksikäsitteisyys isomorfismia vaille. Ne antavat siten keinon tarkastella kunnan algebrallisia laajennuksia "sisäisten" käsitteiden (polynomien) avulla. Todistus perustuu siihen, että isomorfismi kuvaa polynomin juuret toisessa juurikunnassa sen juurille toisessa juurikunnassa. Koska polynomeilla voi olla useita juuria, isomorfismi ei kuitenkaan ole yleensä yksikäsitteinen.

LAUSE 4.3.7. *Olkoon $K$ kunta ja $(f_i)_{i\in I}$ perhe $K[X]$:n polynomeja, jotka eivät ole vakioita. Olkoot $E$ ja $F$ kaksi $K$:n laajennusta, jotka kumpikin ovat perheen $(f_i)_{i\in I}$ juurikuntia. Silloin on olemassa $K$-isomorfismi $u\colon E \xrightarrow{\sim} F$.*

*Todistus.* Voidaan olettaa, että jokainen $f_i$ on pääpolynomi. Kuten lauseen 4.3.4 todistuksessa, valitaan maksimaalinen pari $(E', u)$, missä $E'$ on $E$:n alilaajennus ja $u\colon E' \to F$ on $K$-homomorfismi.

Olkoon $x \in E$ jonkin polynomin $f_i$ juuri. Osoitetaan, että se kuuluu kuntaan $E'$. Joka tapauksessa $x$ on algebrallinen $E'$:n suhteen (kor. 4.2.4). Olkoon $g \in E'[X]$ sen minimaalipolynomi. Silloin on olemassa (lause 4.2.1, ii) kanoninen isomorfismi

$$E'[X]/(g) \xrightarrow{\sim} E'[x].$$

Lisäksi $f_i$ on jaollinen $g$:llä, koska $f_i(x) = 0$ (lause 4.2.1, i). On siis olemassa esitys

$$f_i = gh,$$

missä $h \in E'[X]$. Kun sovelletaan homomorfismia $u$ polynomien kertoimiin, saadaan yhtälö

$$f_i = g'h',$$

missä $g'$, $h' \in F[X]$ ovat polynomien $g$ ja $h$ kuvat. Polynomi $f_i$ säilyy, koska sen kertoimet ovat kunnassa $K$.

Koska myös $F$ on perheen $(f_i)_{i\in I}$ juurikunta, $f_i$ voidaan hajottaa tuloksi

$$f_i = \prod_{k=1}^{n}(X - y_k),$$

missä $y_k \in F$ $(1 \leq k \leq n)$. Koska polynomien jako alkutekijöihin renkaassa $F[X]$ on järjestystä vaille yksikäsitteinen, ja $g'$ on pääpolynomi, joka jakaa $f_i$:n, se on tulo

$$g' = \prod_{k\in J}(X - y_k),$$

missä $J$ on jokin joukon $\{1, 2, \ldots, n\}$ epätyhjä osajoukko. Siten laajennuksessa $F$ on olemassa polynomin $g'$ juuri $y = y_k$.

Olkoon $\varphi\colon E'[X] \to F$ ehdon $\varphi(X) = y$ määräämä sijoitushomomorfismi, kun tulkitaan $F$ struktuurihomomorfismilla $u$ varustetuksi $E'$-algebraksi. Tällöin siis pätee kaikilla $E'[X]$:n polynomeilla

$$\varphi\Big(\sum_k \alpha_k X^k\Big) = \sum_k u(\alpha_k)y^k.$$

Erityisesti $\varphi(g) = g'(y) = 0$, joten ydin $\mathrm{Ker}(\varphi)$ sisältää $g$:n virittämän ideaalin $(g) \subset E'[X]$.

Hajotelmalauseesta saadaan silloin $E'$-homomorfismi

$$u'\colon E'[x] \cong E'[X]/(g) \to F,$$

joka toteuttaa ehdon $u'(x) = \varphi(X) = y$. Tällöin $u'$ on myös $K$-homomorfismi ja sen rajoittuma laajennukseen $E'$ on $u$. Maksimaalisuuden nojalla on siten $E'[x] = E'$ eli $x \in E'$.

Yllä on osoitettu, että kaikki polynomien $f_i$ juuret ovat laajennuksessa $E'$. Koska juuret toisaalta virittävät juurikunnan $E$, on siis $E'$ sama kuin koko $E$, ja siten $u$ on $K$-homomorfismi $E \to F$.

Homomorfismi $u$ on injektiivinen, koska $E$ on kunta. (Sen ydin on ainoa aito ideaali $\{0\} \subset E$ (lause 1.8.2).) Vielä on osoitettava, että $u$ on surjektiivinen.

Jokaisella polynomilla $f_i$ $(i \in I)$ on esitys

$$f_i = \prod_{k=1}^{n} (X - x_k),$$

missä $x_k \in E$ $(1 \leq k \leq n)$. Soveltamalla polynomien kertoimiin homomorfismia $u$ saadaan toinen esitys

$$f_i = \prod_{k=1}^{n} (X - u(x_k)),$$

missä $u(x_k) \in F$ $(1 \leq k \leq n)$. Tämä merkitsee, että polynomin $f_i$ juurien joukko laajennuksessa $F$ on

$$R_i' = \{u(x_k) \mid 1 \leq k \leq n\} = u(R_i),$$

missä $R_i$ on $f_i$:n juurien joukko $E$:ssä.

Erityisesti jokainen joukko $R_i'$ $(i \in I)$ sisältyy $u$:n kuvaan, ja koska niiden yhdiste virittää koko juurikunnan $F$, saadaan siten

$$F = K\Big(\bigcup_{i \in I} R_i'\Big) \subset u(E).$$

Homomorfismi $u$ on siis bijektiivinen. □

**Kunnan algebrallinen sulkeuma.** Olkoon $K$ kunta.

MÄÄRITELMÄ 4.3.8. Kunnan $K$ *algebrallinen sulkeuma* on kunnan $K$ algebrallinen laajennus, joka on algebrallisesti suljettu.

*Esimerkkejä.* 3) Kompleksilukujen kunta $\mathbf{C}$ on kunnan $\mathbf{R}$ algebrallinen sulkeuma (ks. esimm. 4.2.1 ja 4.3.1)

4) Jos $\Omega$ on jokin $K$:n algebrallisesti suljettu laajennus, niin $K$:n algebrallinen sulkeuma $\bar{K}$ laajennuksessa $\Omega$ on algebrallisesti suljettu (lause 4.3.3) ja siten $K$:n algebrallinen sulkeuma.

Erityisesti algebrallisten lukujen kunta $\mathbf{A} \subset \mathbf{C}$ (ks. esim. 4.3.2) on kunnan $\mathbf{Q}$ algebrallinen sulkeuma.

LAUSE 4.3.9. *Kunnan $K$ laajennus $\Omega$ on $K$:n algebrallinen sulkeuma, jos ja vain jos*

i) *$\Omega$ on algebrallinen $K$:n suhteen, ja*
ii) *jokainen $K[X]$:n polynomi, joka ei ole vakio, jakautuu $\Omega[X]$:ssa asteen 1 tekijöiden tuloksi.*

*Todistus.* Ehtojen välttämättömyys seuraa suoraan määritelmistä 4.3.8 ja 4.3.2 sekä lauseen 4.3.1 kohdasta a).

Oletetaan kääntäen, että ehdot i) ja ii) ovat voimassa. On osoitettava, että $\Omega$ on algebrallisesti suljettu. Olkoon $\Omega'$ jokin sen algebrallinen laajennus. Lauseen 4.3.1 kohdan d) nojalla on riittävää osoittaa, että $[\Omega' : \Omega] = 1$.

Voidaan olettaa, että $\Omega$ on $\Omega'$:n alilaajennus. Algebrallisten laajennusten transitiivisuuden (lause 4.2.9) nojalla $\Omega'$ on algebrallinen myös $K$:n suhteen.

Olkoon $x$ jokin $\Omega'$:n alkio ja $f \in K[X]$ sen minimaalipolynomi $K$:n suhteen. Ehdon ii) mukaan on silloin olemassa esitys

$$f = \prod_{i=1}^{n} (X - x_i),$$

missä $x_i \in \Omega$ $(1 \leq i \leq n)$. Alkio $x$ on tällöin jokin juurista $x_i$. Se on siis kunnassa $\Omega$, ja siten $\Omega' = \Omega$. □

LAUSE 4.3.10. *Jokaisella kunnalla $K$ on algebrallinen sulkeuma. Jos $\Omega$ ja $\Omega'$ ovat kaksi $K$:n algebrallista sulkeumaa, niin on olemassa $K$-isomorfismi $u\colon \Omega \xrightarrow{\sim} \Omega'$.*

*Todistus.* Olkoon $(f_i)_{i \in I}$ perhe, jonka muodostavat kaikki algebran $K[X]$ polynomit vakioita lukuunottamatta. Lauseen 4.3.6 perusteella sillä on juurikunta $\Omega$.

Korollaarin 4.2.8 nojalla $\Omega$ on algebrallinen $K$:n suhteen, koska sen virittävät polynomien $f_i$ juuret, ja nämä ovat algebrallisia $K$:n suhteen. Lisäksi juurikunnan määritelmän 4.3.5 perusteella jokainen polynomi $f_i$ jakautuu algebrassa $\Omega[X]$ asteen 1 tekijöihin. Lauseen 4.3.9 ehdot ovat siten voimassa laajennuksessa $\Omega$, joten se on kunnan $K$ algebrallinen sulkeuma.

Jos $\Omega$ ja $\Omega'$ ovat kaksi kunnan $K$ algebrallista sulkeumaa, niin kumpikin on perheen $(f_i)_{i \in I}$ juurikunta. (Itse asiassa niiden kaikki alkiot ovat jonkin polynomin $f_i$ juuria.) Juurikuntien yksikäsitteisyyslauseen 4.3.7 nojalla on siten olemassa $K$-isomorfismi $u\colon \Omega \to \Omega'$. □

Yleensä kahden kunnan $K$ algebrallisen sulkeuman välillä on paljon isomorfismeja, jotka kuvaavat jokaisen algebran $K[X]$ polynomin juuret eri tavoin permutoiden.

KOROLLAARI 4.3.11. *Olkoot $\Omega$ ja $\Omega'$ alikuntiensa $K$ ja $K'$ algebrallisia sulkeumia. Tällöin jokainen isomorfismi $u\colon K \xrightarrow{\sim} K'$ voidaan jatkaa isomorfismiksi $v\colon \Omega \xrightarrow{\sim} \Omega'$.*

*Todistus.* Olkoon $u\colon K \xrightarrow{\sim} K'$ jokin kuntien välinen isomorfismi. Yhdistetyllä struktuurihomomorfismilla $K \xrightarrow{u} K' \to \Omega'$ varustettuna $\Omega'$ on tällöin $K$:n laajennus. Se on lisäksi algebrallisesti suljettu ja algebrallinen $K$:n suhteen, koska se on algebrallinen $K'$:n suhteen.

Tämä merkitsee, että $(\Omega', u)$ on myös $K$:n algebrallinen sulkeuma. Lauseen 4.3.10 perusteella on tällöin olemassa $K$-isomorfismi

$$v\colon \Omega \xrightarrow{\sim} (\Omega', u),$$

ja se jatkaa $u$:n, koska kaikilla $\lambda \in K$ kunnassa $\Omega'$ pätee

$$v(\lambda.1) = \lambda.v(1) = u(\lambda)v(1) = u(\lambda).1\,.$$

□

**Harjoitustehtäviä**

1) Osoitettava, että jokainen algebrallisesti suljettu kunta on ääretön.

2) Kuvailtava polynomin $X^3 - 2$ juurikuntaa kunnan $\mathbf{Q}$ suhteen ja määritettävä sen aste.

3) Kuvailtava polynomin $X^4+X^2+1$ juurikuntaa kunnan $\mathbf{Q}$ suhteen ja määritettävä sen aste.

4) Olkoon $K$ kunta, $f \in K[X]$ polynomi, jonka aste on $n > 0$, ja $E$ jokin $f$:n juurikunta $K$:n suhteen. Osoitettava:

i) Jos $f = gh$, missä $g, h \in K[X] \setminus K$, niin $g$:llä on juurikunta $L \subset E$ ja $E$ on $h$:n juurikunta $L$:n suhteen.

ii) Jos $f$ on jaoton $K[X]$:ssä, $x \in E$ on sen juuri ja $L = K(x)$, niin $f = (X-x)g$, missä $g \in L[X]$, ja $E$ on $g$:n juurikunta $L$:n suhteen.

Pääteltävä induktiolla, että aste $[E : K]$ on luvun $n!$ tekijä. (Jos $n = p + q$, niin $n!$ on jaollinen tulolla $p!q!$.)

## 4.4. Konjugaatit ja normaalit laajennukset

Olkoon $K$ kunta ja $\Omega$ jokin sen algebrallinen sulkeuma. Oletetaan merkintöjen yksinkertaistamiseksi, että $K$ on $\Omega$:n alikunta.

Jos $E$ on mikä tahansa $K$:n algebrallinen laajennus, niin upotuslauseen 4.3.4 nojalla on olemassa $K$-homomorfismeja

$$u\colon E \to \Omega.$$

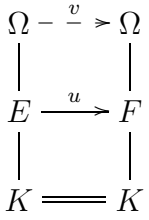
Kuvat $u(E)$ ovat tällöin isomorfisia $E$:n kanssa. Tässä pykälässä tutkitaan tällaisia keskenään isomorfisia $\Omega$:n alilaajennuksia.

Voidaan olettaa, että $E$ on $\Omega$:n alilaajennus. Tällöin $\Omega$ on algebrallinen $E$:n suhteen, joten se on myös $E$:n algebrallinen sulkeuma.

Jos $u\colon E \to \Omega$ on jokin $K$-homomorfismi, niin

$$F = u(E) \subset \Omega$$

on $K$:n laajennus ja $\Omega$ on myös $F$:n algebrallinen sulkeuma. Korollaarin 4.3.11 perusteella on silloin olemassa isomorfismi $v\colon \Omega \to \Omega$, joka jatkaa $u$:n.



Tällöin $v$ on $K$-homomorfismi kuten $u$, koska $v(\lambda) = u(\lambda) = \lambda$ kaikilla $\lambda \in K$. Isomorfismi $v$ on siis laajennuksen $\Omega$ $K$-automorfismi.

MÄÄRITELMÄ 4.4.1. Kunnan $K$ algebrallisen sulkeuman $\Omega$ alilaajennukset $E$ ja $F$ ovat toistensa *konjugaatteja* ($K$:n suhteen) $\Omega$:ssa, jos on olemassa sellainen $\Omega$:n $K$-automorfismi $u$, että $u(E) = F$.

Vastaavasti algebrallisen sulkeuman $\Omega$ alkiot $x$ ja $y$ ovat toistensa *konjugaatteja* (eli *liittoalkioita*) $K$:n suhteen, jos $u(x) = y$ jollakin $\Omega$:n $K$-automorfismilla $u$.

*Esimerkki* 1) Kompleksilukujen kunta $\mathbf{C}$ on kunnan $\mathbf{R}$ algebrallinen sulkeuma. Kuvaus $u\colon \mathbf{C} \to \mathbf{C}$, joka vie kompleksiluvun $z$ konjugaattiluvulleen $\bar{z}$, on $\mathbf{C}$:n $\mathbf{R}$-automorfismi. Luvut $z$ ja $\bar{z}$ ovat siten toistensa konjugaatteja kunnan $\mathbf{R}$ suhteen.

LAUSE 4.4.2. *Olkoot $K$ kunta, $\Omega$ sen algebrallinen sulkeuma, $x$, $y \in \Omega$ ja $f \in K[X]$ alkion $x$ minimaalipolynomi $K$:n suhteen. Silloin seuraavat ehdot ovat yhtäpitävät.*

a) $f(y) = 0$ ;
b) *$f$ on $y$:n minimaalipolynomi $K$:n suhteen;*
c) *on olemassa $K$-isomorfismi $u\colon K(x) \xrightarrow{\sim} K(y)$, jolla on $u(x) = y$ ;*
d) *$y$ on $x$:n konjugaatti $K$:n suhteen.*

*Näiden ollessa voimassa myös alilaajennukset $K(y)$ ja $K(x)$ ovat toistensa konjugaatteja $K$:n suhteen.*

*Todistus.* a) $\Rightarrow$ b): Olkoon $g \in K[X]$ alkion $y$ minimaalipolynomi $K$:n suhteen. Jos $f(y) = 0$, niin $f$ on jaollinen polynomilla $g$. Koska kumpikin on jaoton pääpolynomi, on tällöin välttämättä $g = f$.

b) $\Rightarrow$ c): Lauseen 4.2.1, ii) mukaan on olemassa kanoninen $K$-isomorfismi

$$K[X]/(f) \xrightarrow{\sim} K[x] = K(x),$$

jossa tuntemattoman $X$ luokan kuva on $x$. Jos $f$ on myös $y$:n minimaalipolynomi, niin samoin saadaan $K$-isomorfismi

$$K[X]/(f) \xrightarrow{\sim} K[y] = K(y).$$

Yhdistämällä tämä edellisen isomorfismin käänteiskuvaukseen saadaan $K$-isomorfismi

$$u\colon K(x) \xrightarrow{\sim} K[X]/(f) \xrightarrow{\sim} K(y),$$

joka toteuttaa ehdon $u(x) = y$.

c) $\Rightarrow$ d): Algebrallisesti suljettu laajennus $\Omega$ on kummankin alilaajenuksensa $K(x)$ ja $K(y)$ algebrallinen sulkeuma. Jokainen $K$-isomorfismi $u\colon K(x) \to K(y)$ voidaan siten korollaarin 4.3.11 mukaan jatkaa $K$-automorfismiksi $v\colon \Omega \to \Omega$.

Jos lisäksi $u(x) = y$, niin samoin on $v(x) = y$, joten $x$ ja $y$ ovat toistensa konjugaatteja $K$:n suhteen.

d) $\Rightarrow$ a): Olkoon $u$ laajennuksen $\Omega$ $K$-automorfismi, joka toteuttaa ehdon $u(x) = y$. Yhdistetty homomorfismi

$$K[X] \to \Omega \xrightarrow{u} \Omega, \qquad g \mapsto u(g(x)),$$

on $K$-homomorfismi, joten se on sijoitushomomorfismi, jossa $X \mapsto u(x) = y$, eli kuvaus $g \mapsto g(y)$. Kun $g = f$, saadaan erityisesti

$$f(y) = f(u(x)) = u(f(x)) = 0.$$

Tällöin myös $u(K(x)) = K(u(x)) = K(y)$, joten $K(x)$ ja $K(y)$ ovat toistensa konjugaatteja $K$:n suhteen. □

*Esimerkkejä.* 2) Algebrallisten lukujen kunta $\mathbf{A}$ on kunnan $\mathbf{Q}$ algebrallinen sulkeuma (esim. 4.3.4). Luvuilla $i$ ja $-i$ on sama minimaalipolynomi $X^2 + 1$ kunnan $\mathbf{Q}$ suhteen.

Ne ovat siten toistensa konjugaatteja $\mathbf{Q}$:n suhteen (lause 4.4.2, b), eli on olemassa $\mathbf{Q}$-automorfismi $u\colon \mathbf{A} \to \mathbf{A}$, joka vie $i$:n $-i$:lle. Eräs tällainen on kompleksinen konjugointi $u\colon z \mapsto \bar{z}$. Erityisesti luvut $x + iy \in \mathbf{Q}(i)$ ($x$, $y \in \mathbf{Q}$) ja $x - iy$ ovat toistensa konjugaatteja kunnan $\mathbf{Q}$ suhteen.

3) Algebralliset luvut $\sqrt{2}$ ja $-\sqrt{2}$ ovat toistensa konjugaatteja kunnan $\mathbf{Q}$ suhteen, koska niillä on sama minimaalipolynomi $X^2 - 2 \in \mathbf{Q}[X]$.

Ehdon $u(\sqrt{2}) = -\sqrt{2}$ toteuttava $\mathbf{Q}$-isomorfismi

$$u\colon \mathbf{Q}(\sqrt{2}) \xrightarrow{\sim} \mathbf{Q}(-\sqrt{2}) = \mathbf{Q}(\sqrt{2})$$

on $x + y\sqrt{2} \mapsto x - y\sqrt{2}$. Luvut $x + y\sqrt{2}$ ja $x - y\sqrt{2}$ ($x$, $y \in \mathbf{Q}$) ovat siis toistensa konjugaatteja kunnan $\mathbf{Q}$ suhteen.

KOROLLAARI 4.4.3. *Kunnan $K$ algebrallisen sulkeuman $\Omega$ alkion $x$ konjugaattien lukumäärä $\Omega$:ssa on äärellinen ja enintään sama kuin $x$:n aste $K$:n suhteen.*

*Todistus.* Olkoon $f \in K[X]$ alkion $x$ minimaalipolynomi $K$:n suhteen. Lauseen 4.4.2 kohdan a) mukaan jokainen $x$:n konjugaatti $y \in \Omega$ on $f$:n juuri. Koska $\Omega$ on kokonaisalue, polynomilla $f$ on enintään sen asteen osoittama määrä juuria $\Omega$:ssa. □

LAUSE 4.4.4. *Jos $E$ on kunnan $K$ algebrallinen laajennus, niin jokainen $E$:n $K$-endomorfismi $u$ on $E$:n automorfismi.*

*Todistus.* Voidaan olettaa, että $E$ on jonkin $K$:n algebrallisen sulkeuman $\Omega$ alilaajennus. Jokainen $K$-endomorfismi $u\colon E \to E$ on $E$:n isomorfismi kuvalle $u(E)$. Koska $\Omega$ on sekä $E$:n että $u(E)$:n algebrallinen sulkeuma, $u$ voidaan jatkaa $K$-automorfismiksi $v\colon \Omega \to \Omega$ (kor. 4.3.11). Jokaisen alkion $x \in E$ kuva $u(x) \in E$ on tällöin $x$:n konjugaatti $K$:n suhteen, koska se on sama kuin $v(x)$.

Olkoon $F_x$ joukko, jonka muodostavat alkion $x \in E$ kuntaan $E$ kuuluvat konjugaatit $K$:n suhteen. Jos $y \in F_x$, niin $u(y) \in E$ on yllä esitetyn nojalla $y$:n konjugaatti $K$:n suhteen. Se on silloin myös $x$:n

konjugaatti $K$:n suhteen, koska sillä sama minimaalipolynomi kuin $y$:llä ja $x$:llä. Tämä merkitsee, että $u(y)$ on myös $F_x$:n alkio; siis saadaan

$$u(F_x) \subset F_x.$$

Toisaalta $u$ on injektiivinen, ja $F_x$ on äärellinen. Joukossa $u(F_x)$ on siten yhtä monta alkiota kuin joukossa $F_x$, joten täytyy olla

$$u(F_x) = F_x$$

kaikilla $x \in E$. Koska $E$ on yhdiste joukoista $F_x$, tästä seuraa

$$u(E) = u\Big(\bigcup_{x\in E} F_x\Big) = \bigcup_{x\in E} F_x = E.$$

Jokainen $K$-endomorfismi $u\colon E \to E$ on siis bijektiivinen. □

Lause 4.4.5. *Olkoon $E$ kunnan $K$ algebrallinen sulkeuman $\Omega$ alilaajennus. Tällöin seuraavat ehdot ovat yhtäpitävät.*

a) *Jokainen $K$-homomorfismi $u\colon E \to \Omega$ kuvaa $E$:n itseensä.*
b) *Jokainen $K$-automorfismi $u\colon \Omega \to \Omega$ kuvaa $E$:n itseensä.*
c) *Jokaisen alkion $x \in E$ konjugaatit $\Omega$:ssa kuuluvat kuntaan $E$.*
d) *Jokaisen alkion $x \in E$ minimaalipolynomi $K$:n suhteen on tulo asteen 1 tekijöistä algebrassa $E[X]$.*
e) *Jokainen jaoton polynomi $f \in K[X]$, jolla on ainakin yksi juuri $E$:ssä, hajoaa asteen 1 tekijöihin algebrassa $E[X]$.*
f) *$E$ on jonkin polynomiperheen $(f_i)_{i\in I}$ ($f_i \in K[X], f_i \notin K$) juurikunta.*

*Todistus.* a) ⇔ b): Jokainen $K$-homomorfismi $u\colon E \to \Omega$ on jonkin $K$-automorfismin $v\colon \Omega \to \Omega$ rajoittuma (kor. 4.3.11). Ehto $u(E) \subset E$ on tällöin yhtäpitävä ehdon $v(E) \subset E$ kanssa.

d) ⇔ e): Jokainen jaoton polynomi $f \in K[X]$, jolla on juuri $x \in E$, on vakiokerrointa vaille sama kuin $x$:n minimaalipolynomi. Se hajoaa siten asteen 1 tekijöihin, jos ja vain jos minimaalipolynomilla on sama ominaisuus.

c) ⇔ d): Olkoon $f \in K[X]$ alkion $x \in E$ minimaalipolynomi $K$:n suhteen. Koska $\Omega$ on algebrallisesti suljettu, $f$ voidaan esittää tulona

$$f = \prod_{i=1}^{n}(X - x_i),$$

missä $x_i \in \Omega$ ($1 \le i \le n$). Alkion $x$ konjugaatit ovat tällöin juuret $x_i$, ja ne kuuluvat kuntaan $E$, jos ja vain jos $f$ on asteen 1 tekijöiden tulo algebrassa $E[X]$.

b) ⇒ c): Olkoon $x$ $E$:n alkio ja $y \in \Omega$ jokin sen konjugaatti $K$:n suhteen. Tällöin siis $y = u(x)$ jollakin $\Omega$:n $K$-automorfismilla $u$. Jos ehto b) on voimassa, on siis $y = u(x) \in E$.

c) ⇒ b): Olkoon $u\colon \Omega \to \Omega$ jokin $K$-automorfismi. Jos $x \in E$, niin $y = u(x)$ on $x$:n konjugaatti $\Omega$:ssa $K$:n suhteen. Ehdon c) ollessa voimassa $y$ on $E$:n alkio. Tällöin siis $u(E) \subset E$.

d) $\Rightarrow$ f): Olkoon $(f_i)_{i\in I}$ perhe, jossa ovat kaikki $E$:n alkioiden minimaalipolynomit $K$:n suhteen. Ehdon d) ollessa voimassa jokainen $f_i$ on tulo asteen 1 tekijöistä algebrassa $E[X]$. Koska niiden juuret virittävät $E$:n, $E$ on tällöin perheen $(f_i)_{i\in I}$ juurikunta.

f) $\Rightarrow$ b): Olkoon $E$ jonkin polynomiperheen $(f_i)_{i\in I}$ juurikunta ($f_i \in K[X]$, ei vakio). Olkoon $R_i$ polynomin $f_i$ juurien $x \in E$ joukko ($i \in I$). Jos $u\colon \Omega \to \Omega$ on jokin $K$-automorfismi, niin se permutoi jokaisen polynomin $f_i$ juuret, eli $u(R_i) = R_i$ kaikilla $i \in I$.

Juurikuntana $E$ on juurien yhdessä virittämä laajennus

$$E = K\Big(\bigcup_{i\in I} R_i\Big),$$

ja tästä seuraa

$$u(E) = K\Big(\bigcup_{i\in I} u(R_i)\Big) = E.$$

□

Määritelmä 4.4.6. Kunnan $K$ algebrallinen laajennus $E$ on *normaali*, jos lauseen 4.4.5 ehto e) on voimassa.

*Huomautus.* Myös muut lauseen ehdot ovat voimassa, kun $\Omega$ on jokin $E$:n sisältävä $K$:n algebrallinen sulkeuma.

Korollaari 4.4.7. *Kunnan $K$ algebrallisen sulkeuman $\Omega$ alilaajennus $E$ on normaali, jos ja vain jos se on sama kuin jokainen konjugaattinsa $\Omega$:ssa.*

*Todistus.* Laajennus $E$ on normaali, jos ja vain jos jokainen $\Omega$:n $K$-automorfismi $u$ toteuttaa ehdon $u(E) \subset E$ (lause 4.4.5, b). Lauseen 4.4.4 mukaan tämä on yhtäpitävään sen kanssa, että $u(E) = E$ eli $E$:n konjugaatti $u(E)$ on sama kuin $E$. □

Korollaari 4.4.8. *Olkoot $E$ ja $F$ kaksi kunnan $K$ algebrallista laajennusta ja $E \subset F$. Jos $F$ on $K$:n normaali laajennus, niin se on myös $E$:n normaali laajennus.*

*Todistus.* Olkoon $\Omega$ jokin $F$:n sisältävä $K$:n algebrallinen sulkeuma. Jos $u\colon \Omega \to \Omega$ on $E$-automorfismi, niin $u$ on myös $K$-lineaarinen eli $K$-automorfismi. Jokainen $F$:n konjugaatti $u(F)$ kunnan $E$ suhteen on siten myös $F$:n konjugaatti $K$:n suhteen.

Jos $F$ on normaali $K$:n laajennus, niin $u(F) = F$ korollaarin 4.4.7 nojalla, ja kääntäen tästä seuraa, että $F$ on normaali $E$:n laajennus. □

*Huomautus.* Monet normaalin laajennuksen alilaajennukset eivät yleensä ole normaaleja. Samoin jos $E$ on $K$:n normaali laajennus ja $F$ on $E$:n normaali laajennus, $F$ ei välttämättä ole $K$:n normaali laajennus. (Normaalisuus ei siis ole transitiivinen ominaisuus.)

**Normaalilaajennusten virittäjäjoukot.** Olkoon $A$ kunnan $K$ algebrallisen sulkeuman $\Omega$ osajoukko. Olkoon $B$ joukon $A$ alkioiden kaikkien konjugaattien joukko; $B$ on siis yhdiste joukoista $u(A)$, missä $u$ on $\Omega$:n $K$-automorfismi:

$$B = \bigcup_u u(A).$$

Tarkastellaan normaaleja alilaajennuksia $N \subset \Omega$, jotka sisältävät joukon $A$. Jos $u\colon \Omega \to \Omega$ on $K$-automorfismi, niin $u(A)$ sisältyy $N$:n konjugaattiin $u(N)$, joka on sama kuin $N$ (kor. 4.4.7). Laajennus $N$ sisältää siis joukkojen $u(A)$ yhdisteen $B$ ja siten myös sen virittämän laajennuksen:

$$K(B) \subset N.$$

Toisaalta jokainen $\Omega$:n $K$-automorfismi $u$ kuvaa $A$:n alkioiden konjugaatit toisille konjugaateille, joten $u(B) = B$ ja edelleen

$$u(K(B)) = K(u(B)) = K(B).$$

Konjugaattien joukon $B$ virittämä laajennus $K(B)$ on siis normaali. Se on pienin joukon $A$ sisältävä normaali laajennus eli $A$:n *virittämä* $K$:n *normaali laajennus* algebrallisessa sulkeumassa $\Omega$.

LAUSE 4.4.9. *Olkoon $E$ kunnan $K$ algebrallisen sulkeuman $\Omega$ alilaajennus ja $N$ $E$:n virittämä $K$:n normaali laajennus. Jos $E = K(A)$, missä $A \subset E$, niin $N = K(B)$, missä $B$ on $A$:n alkioiden konjugaattien joukko $\Omega$:ssa.*

*Todistus.* Normaali laajennus $N$ sisältää konjugaattien virittämän laajennuksen $K(B)$, koska se sisältää joukon $A$ ohella sen alkioiden konjugaatit. Toisaalta $K(B)$ on normaali, kuten edellä on nähty, ja sisältää laajennuksen $E = K(A)$, koska $A \subset B$.

Laajennus $K(B)$ on siten pienin $E$:n sisältävä normaali laajennus, eli se on sama kuin $N$. □

KOROLLAARI 4.4.10. *Jos $E$ on kunnan $K$ äärellinen laajennus, niin sen virittämä $K$:n normaali laajennus $N$ on myös äärellinen.*

*Todistus.* Äärellisellä laajennuksella $E$ on äärellinen äärellinen virittäjäjoukko $A$ (esim. kanta). Sen alkioiden konjugaattien joukko $B$ on myös äärellinen, koska jokaisella alkiolla on vain äärellisen monta konjugaattia (kor. 4.4.3). Joukon $B$ virittämä algebrallinen laajennus $N = K(B)$ on tällöin myös äärellinen (lause 4.2.7). □

**Harjoitustehtäviä**

1) Olkoon $\zeta = \sqrt{i} = \sqrt{2}(1+i)/2 \in \mathbf{C}$. Osoitettava:
i) $[\mathbf{Q}(\zeta) : \mathbf{Q}(i)] = 2$ ja $[\mathbf{Q}(\zeta) : \mathbf{Q}] = 4$.
ii) $f = X^4 + 1$ on $\zeta$:n minimaalipolynomi kunnan $\mathbf{Q}$ suhteen.
iii) $\zeta$:n konjugaatit $\mathbf{C}$:ssä $\mathbf{Q}$:n suhteen ovat $\zeta$, $-\zeta$, $\zeta^3$ ja $-\zeta^3$.

Pääteltävä, että $\mathbf{Q}(\zeta)$ on $f$:n juurikunta ja $\mathbf{Q}$:n normaali laajennus.

2) Olkoon $\xi = \sqrt[4]{2} \in \mathbf{R}$. Osoitettava:

i) $\mathbf{Q}(\xi)$ on $\mathbf{Q}(\sqrt{2})$:n ja samoin $\mathbf{Q}(\sqrt{2})$ on $\mathbf{Q}$:n asteen 2 normaali laajennus.

ii) $\xi$:n konjugaatit $\mathbf{C}$:ssä kunnan $\mathbf{Q}$ suhteen ovat $\xi$, $-\xi$, $i\xi$ ja $-i\xi$.

Pääteltävä, että $\mathbf{Q}(\xi)$ ei ole $\mathbf{Q}$:n normaali laajennus ja että $\mathbf{Q}(\xi, i)$ on $\xi$:n virittämä $\mathbf{Q}$:n normaali laajennus. Määritettävä $\mathbf{Q}$:n laajennusten $\mathbf{Q}(\xi, i)$ ja $\mathbf{Q}(i\xi)$ asteet.

3) Olkoon $K$ kunta, $\Omega$ jokin $K$:n algebrallinen sulkeuma, $N \subset \Omega$ $K$:n normaali laajennus, $E \subset N$ alilaajennus ja $u\colon E \to \Omega$ $K$-homomorfismi. Osoitettava, että $u(E) \subset N$ ja että $u$ voidaan jatkaa $N$:n $K$-automorfismiksi.

## 4.5. Separoituvat algebralliset laajennukset

Olkoon $K$ kunta ja $\Omega$ jokin sen algebrallinen sulkeuma. Jos $E$ on $K$:n algerallinen laajennus, niin on olemassa $K$-homomorfismeja

$$u\colon E \to \Omega.$$

Yleensä tällaisia homomorfismeja on useita. Tässä pykälässä tutkitaan tarkemmin niiden lukumäärää.

*Esimerkki* 1) Olkoon $E = K(x)$ yhden alkion $x \in \Omega$ virittämä $K$:n äärellinen laajennus. Jos $u\colon K(x) \to \Omega$ on $K$-homomorfismi, niin se määrittelee isomorfismin kuvalle

$$u\colon K(x) \xrightarrow{\sim} K(y) \subset \Omega,$$

missä $y = u(x) \in \Omega$ on $x$:n konjugaatti $K$:n suhteen (lause 4.4.2, c).

Kääntäen jokaiseen $x$:n konjugaattiin $y \in \Omega$ liittyy yksikäsitteinen ehdon $u(x) = y$ toteuttava $K$-homomorfismi $u\colon K(x) \to \Omega$. Kuvaus $u \mapsto u(x)$ on siten bijektio

$$\mathrm{Hom}_{K-\mathrm{alg}}(K(x), \Omega) \xrightarrow{\sim} F_x,$$

missä $F_x$ on alkion $x$ konjugaattien $y \in \Omega$ joukko.

Koska alkion $x$ konjugaatit $K$:n suhteen ovat samat kuin sen minimaalipolynomin $f \in K[X]$ juuret, homomorfismien $u\colon K(x) \to \Omega$ lukumäärä on enintään sama kuin $x$:n aste $\deg(f)$. Lisäksi se on sama kuin aste, jos ja vain jos polynomin $f$ juuret $\Omega$:ssa ovat yksinkertaiset.

**Separoituvat polynomit.**

LAUSE 4.5.1. *Olkoon $f \in K[X]$ polynomi, $f \neq 0$. Seuraavat ehdot ovat yhtäpitävät:*

a) *$f$ ja sen derivaatta $f'$ ovat keskenään jaottomat $K[X]$:ssä.*

b) *On olemassa sellainen $K$:n laajennus $L$, että $f$ hajoaa $L[X]$:ssä tuloksi asteen $\leq 1$ tekijöistä, joilla ei ole yhteisiä juuria.*

c) *$f$:n juuret $K$:n algebrallisessa sulkeumassa $\Omega$ ovat yksinkertaiset.*

*Todistus.* a) $\Rightarrow$ c): Olkoot $f$ ja $f'$ keskenään jaottomat. Jos $a \in \Omega$ on $f$:n juuri, niin $f$ on jaollinen $a$:n minimaalipolynomilla $g \in K[X]$. Tällöin $f'(a) \neq 0$, koska muuten myös $f'$ olisi jaollinen $g$:llä, ja siten $f$:n juuri $a$ on yksinkertainen.

c) $\Rightarrow$ b): Jos $\Omega$ on $K$:n algebrallinen sulkeuma, niin polynomi $f$ voidaan esittää tulona

$$f = c(X - a_1) \cdots (X - a_n),$$

missä $c \in K$, $c \neq 0$, ja $a_1, \ldots, a_n \in \Omega$. Jos juuret $a_i$ ovat yksinkertaiset, niin tekijöillä $c$, $X - a_1$, $\ldots$, $X - a_n$ ei ole yhteisiä juuria.

b) $\Rightarrow$ a): Olkoon $L$ sellainen $K$:n laajennus, että $f$ on tulo

$$f = c\prod_{i=1}^{n}(X - a_i),$$

missä $c \in K$, $c \neq 0$, ja tekijöillä $X - a_i$ on eri juuret $a_1, \ldots, a_n \in L$.

Tällöin $f$:n derivaatta on summa

$$f' = c\sum_{i=1}^{n}\prod_{j\neq i}(X - a_j),$$

missä jokainen $f$:n jaoton tekijä $X - a_i$ jakaa kaikki termit yhtä lukuunottamatta, joten se ei ole $f'$:n tekijä. Polynomit $f$ ja $f'$ ovat silloin keskenään jaottomat $L[X]$:ssä ja siten myös $K[X]$:ssä. □

MÄÄRITELMÄ 4.5.2. Polynomi $f \in K[X]$ on *separoituva*, jos se on $\neq 0$ ja toteuttaa lauseen 4.5.1 ehdot.

Käytännössä kätevin ehto on tavallisesti a). Jos polynomi on jaoton, on vielä yksinkertaisempiakin ehtoja.

LAUSE 4.5.3. *Jos $f \in K[X]$ on jaoton polynomi, niin seuraavat ehdot ovat yhtäpitävät:*

a) *$f$ on separoituva.*
b) *On olemassa $K$:n laajennus $L$, jossa $f$:llä on yksinkertainen juuri.*
c) *$f$:n derivaatta $f' \neq 0$.*
d) *Kunnan $K$ karakteristika on 0, tai $p \neq 0$ ja $f \notin K[X^p]$.*

*Todistus.* a) $\Rightarrow$ b): Koska jaoton polynomi $f$ ei ole vakio, sillä on ainakin yksi juuri $x$ jossakin $K$:n algebrallisessa sulkeumassa $L = \Omega$. Jos $f$ on separoituva, niin juuri $x$ on yksinkertainen (lause 4.5.1, c).

b) $\Rightarrow$ c): Olkoon $L$ jokin $K$:n laajennus, jossa $f$:llä on yksinkertainen juuri $x$. Tällöin $f'(x) \neq 0$, joten polynomi $f'$ ei voi olla 0.

c) $\Leftrightarrow$ d): Olkoon $f = \sum_{n\in\mathbf{N}} a_n X^n$, missä $(a_n) \in K^{(\mathbf{N})}$. Derivaatta on tällöin

$$f' = \sum_{n\in\mathbf{N}} n a_n X^{n-1}.$$

Jos kunnan $K$ karakteristika on 0, ehto $f' = 0$ merkitsee, että $na_n$ on 0 kaikilla $n \in \mathbf{N}$. Tämä on yhtäpitävää sen kanssa, että $a_n = 0$, kun $n > 0$, koska tällöin $n$ on kääntyvä kunnassa $K$. Koska jaoton polynomi ei ole vakio, on siis aina $f' \neq 0$.

Jos kunnan $K$ karakteristika on $p \neq 0$, niin $na_n = 0$, kun $n$ on $p$:n kerrannainen. Tällöin $f' = 0$ merkitsee, että $a_n = 0$, kun $n \neq kp$ ($k \in \mathbf{N}$) eli yhtäpitävästi

$$f = \sum_{k \in \mathbf{N}} a_{kp}(X^p)^k \in K[X^p].$$

c) $\Rightarrow$ a): Jos $f'$ ei ole 0, niin se ei ole jaollinen $f$:llä, koska sen aste on alempi kuin $\deg(f)$. Kun $f$ on jaoton $K[X]$:ssä, $f$ ja $f'$ ovat silloin keskenään jaottomat, eli $f$ on separoituva (lause 4.5.1, a). □

**Homomorfismien lineaarinen riippumattomuus.** Olkoon $A$ $K$-algebra ja $L$ jokin $K$:n laajennus. Jokainen $K$-algebrojen homomorfismi $u\colon A \to L$ on $K$-lineaarinen kuvaus. Niiden joukko on siten lineaarikuvausten joukon osajoukko

$$\mathrm{Hom}_{K-\mathrm{alg}}(A, L) \subset \mathrm{Hom}_K(A, L).$$

Toisaalta $\mathrm{Hom}_K(A, L)$ on vektoriavaruus kunnan $L$ suhteen, koska se on kaikkien kuvausten $A \to L$ muodostaman avaruuden $L^A$ aliavaruus (additiivinen aliryhmä ja vakaa skalaarikertolaskun suhteen).

Lause 4.5.4 (Dedekind). *Jos $A$ on $K$-algebra ja $L$ on $K$:n laajennus, niin homomorfismien joukko* $\mathrm{Hom}_{K-\mathrm{alg}}(A, L)$ *on vapaa avaruudessa* $\mathrm{Hom}_K(A, L)$ *kunnan $L$ suhteen.*

*Todistus.* Olkoot $u_1, \ldots, u_n\colon A \to L$ eri $K$-algebrahomomorfismeja, ja olkoon

$$\sum_{i=1}^{n} \alpha_i u_i = 0, \tag{1}$$

lineaarinen relaatio, jossa $\alpha_1, \ldots, \alpha_n \in L$.

Todistetaan induktiolla $n$:n suhteen, että jokainen $\alpha_i$ on 0. Jos $n = 0$, ei ole mitään osoitettavaa. Oletetaan, että $n \geq 1$ ja että väite pätee, kun homomorfismeja on $n - 1$.

Lineaarisesta relaatiosta (1) saadaan kaikilla $x, y \in A$

$$\sum_{i=1}^{n-1} \alpha_i[u_i(x) - u_n(x)]u_i(y) = \sum_{i=1}^{n} \alpha_i u_i(xy) - u_n(x) \sum_{i=1}^{n} \alpha_i u_i(y) = 0,$$

eli uusi lineaarinen relaatio

$$\sum_{i=1}^{n-1} \alpha_i[u_i(x) - u_n(x)]u_i = 0,$$

missä kertoimet $\alpha_i[u_i(x) - u_n(x)]$ ovat kunnassa $L$.

Induktio-oletuksen nojalla on tällöin

$$\alpha_i[u_i(x) - u_n(x)] = 0 \qquad (1 \leq i \leq n-1)$$

kaikilla $x \in A$. Koska $u_i(x) \neq u_n(x)$ jollakin $x \in A$, kun $i \neq n$, ja $L$ on kunta, tästä seuraa

$$\alpha_i = 0 \qquad (1 \leq i \leq n-1).$$

Silloin relaatio (1) supistuu muotoon $\alpha_n u_n = 0$, ja tästä seuraa lopuksi $\alpha_n = 0$, koska $u_n(1) = 1$. □

KOROLLAARI 4.5.5. *Jos $L$ on kunnan $K$ laajennus ja $E$ on $K$:n äärellinen laajennus, niin $K$-homomorfismien $u\colon E \to L$ lukumäärä on enintään sama kuin laajennuksen $E$ aste $[E : K]$.*

*Todistus.* Olkoon $n = [E : K]$ ja $(x_1, \ldots, x_n)$ jokin $E$:n kanta $K$:n suhteen. Tällöin jokaista jonoa $(y_1, \ldots, y_n) \in L^n$ vastaa yksikäsitteinen $K$-lineaarinen kuvaus

$$u\colon E \to L,$$

joka toteuttaa ehdot $u(x_i) = y_i$ $(1 \leq i \leq n)$. Kuvaus $u \mapsto (u(x_i))_{1 \leq i \leq n}$ on siten $L$-lineaarinen isomorfismi

$$\mathrm{Hom}_K(E, L) \xrightarrow{\sim} L^n.$$

Koska algebrahomomorfismien $E \to L$ joukko on vapaa (lause 4.5.4), sen alkioiden lukumäärä voi ylittää dimensiota

$$\dim_L \mathrm{Hom}_K(E, L) = n.$$

□

*Huomautus.* Sama todistus pätee, jos $E$ on äärellinen $K$-algebra $A$.

**Laajennuksen separoituva aste.** Olkoon $E$ kunnan $K$ äärellinen laajennus ja $\Omega$ jokin $K$:n algebrallinen sulkeuma.

MÄÄRITELMÄ 4.5.6. Kunnan $K$ laajennuksen $E$ *separoituva aste*

$$[E : K]_s$$

on $K$-homomorfismien $u\colon E \to \Omega$ lukumäärä.

Koska algebralliset sulkeumat ovat isomorfisia (lause 4.3.10), separoituva aste ei riipu $\Omega$:n valinnasta. Korollaarin 4.5.5 nojalla pätee epäyhtälö

$$[E : K]_s \leq [E : K].$$

> Myöhemmin nähdään, että yhtälö pätee, jos kunnan $K$ karakteristika on 0 (esim. 4.5.2). Jos karakteristika on $p > 0$, voidaan osoittaa, että $[E : K] = p^e[E : K]_s$ jollakin kokonaisluvulla $e \geq 0$.

LAUSE 4.5.7. *Jos $E$ ja $F$ ovat kaksi kunnan $K$ äärellistä laajennusta ja $E \subset F$, niin*

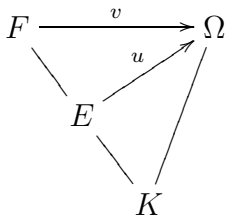
$$[F : K]_s = [F : E]_s[E : K]_s.$$

*Todistus.* Olkoon $u\colon E \to \Omega$ jokin $K$-homomorfismi. Tällöin $(\Omega, u)$ on $E$:n algebrallinen sulkeuma, ja $K$-homomorfismi

$$v\colon F \to \Omega$$

jatkaa $u$:n, jos ja vain jos se on $E$-homomorfismi

$$v\colon F \to (\Omega, u).$$




Koska tällaisten $K$-homomorfismien lukumäärä on $[F : E]_s$, niin kaikkien $K$-homomorfismien $v\colon F \to \Omega$ lukumäärä, eli separoituva aste $[F : K]_s$, on sama kuin $[F : E]_s$ kertaa $K$-homomorfismien $u\colon E \to \Omega$ lukumäärä. □

**Separoituvat algebralliset alkiot.** Olkoon $K$ kunta ja $E$ sen laajennus, jonka ei tarvitse olla algebrallinen.

LAUSE 4.5.8. *Olkoon $E$ kunnan $K$ laajennus, $x \in E$ algebrallinen $K$:n suhteen ja $f \in K[X]$ alkion $x$ minimaalipolynomi $K$:n suhteen. Seuraavat ehdot ovat yhtäpitävät.*

a) $[K(x) : K]_s = [K(x) : K]$.
b) *$f$ on separoituva.*
c) *$x$ on $f$:n yksinkertainen juuri.*

*Todistus.* a) ⇔ b): Laajennuksen aste $[K(x) : K]$ on sama kuin minimaalipolynomin aste $\deg(f)$. Separoituva aste $[K(x) : K]_s$ on taas sama kuin $x$:n konjugaattien eli $f$:n eri juurien lukumäärä (ks. esim. 4.5.1). Asteet ovat siis samat, jos ja vain jos polynomin $f$ juuret ovat yksinkertaiset eli $f$ on separoituva.

b) ⇔ c): Jos $f$ on separoituva, niin sen jokainen juuri on yksinkertainen. Kääntäen $f$ on separoituva, jos sillä on yksinkertainen juuri, koska se on jaoton (lause 4.5.3, b). □

MÄÄRITELMÄ 4.5.9. Olkoon $E$ kunnan $K$ laajennus ja $x \in E$ algebrallinen $K$:n suhteen. Tällöin $x$ on *separoituva* $K$:n suhteen, jos

$$[K(x) : K]_s = [K(x) : K].$$

KOROLLAARI 4.5.10. *Jos $x \in E$ on jonkin polynomin $g \in K[X]$ yksinkertainen juuri, niin $x$ on separoituva $K$:n suhteen.*

*Todistus.* Jos $g(x) = 0$, niin $x$ on algebrallinen $K$:n suhteen, ja $g$ on jaollinen sen minimaalipolynomilla $f \in K[X]$. Jos $x$ on $g$:n yksinkertainen juuri, niin se on myös $f$:n yksinkertainen juuri. Lauseen 4.5.8 nojalla $x$ on siten separoituva $K$:n suhteen. □

KOROLLAARI 4.5.11. *Jos $x \in E$ on algebrallinen ja separoituva $K$:n suhteen, niin $x$ on algebrallinen ja separoituva jokaisen $K$:n laajennuksen $K' \subset E$ suhteen.*

*Todistus.* Olkoon $f \in K[X]$ $x$:n minimaalipolynomi $K$:n suhteen. Tällöin $f$ voidaan tulkita myös $K'[X]$:n polynomiksi ja $x$ on sen yksinkertainen juuri (lause 4.5.8, c). Korollaarin 4.5.10 nojalla $x$ on siten separoituva $K'$:n suhteen. □

**Separoituvat algebralliset laajennukset.**

LAUSE 4.5.12. *Olkoon $E$ kunnan $K$ äärellinen laajennus. Seuraavat ehdon ovat yhtäpitävät.*

a) $[E : K] = [E : K]_s$.
b) *Jokainen $E$:n alkio on separoituva $K$:n suhteen.*
c) $E = K(x_1, \ldots, x_n)$, *missä jokainen* $x_i$ $(1 \leq i \leq n)$ *on separoituva $K$:n suhteen.*

*Todistus.* a) $\Rightarrow$ b): Jos $x \in E$ ei ole separoituva $K$:n suhteen, niin

$$[K(x) : K]_s < [K(x) : K].$$

Koska $[E : K(x)]_s \leq [E : K(x)]$, tästä seuraa lauseiden 4.1.3 ja 4.5.7 perusteella

$$[E : K]_s < [E : K].$$

b) $\Rightarrow$ c): Koska $E$ on $K$:n äärellinen laajennus, sillä on äärellinen virittäjäperhe $(x_1, \ldots, x_n)$, ja ehdon b) ollessa voimassa jokainen $x_i$ on separoituva $K$:n suhteen.

c) $\Rightarrow$ a): Käytetään induktiota $n$:n suhteen. Jos $n = 0$, niin kumpikin aste $[E : K]$ ja $[E : K]_s$ on 1. Olkoon $n > 0$ ja $E' = K(x_1, \ldots, x_{n-1})$.

Kun $x_n$ on separoituva $K$:n suhteen, se on separoituva myös $E'$:n suhteen (kor. 4.5.11) eli

$$[E'(x_n) : E']_s = [E'(x_n) : E'].$$

Koska $E'(x_n) = E$ ja induktio-oletuksen nojalla $[E' : K]_s = [E' : K]$, Lauseista 4.1.3 ja 4.5.7 seuraa

$$[E : K]_s = [E : K].$$

□

MÄÄRITELMÄ 4.5.13. Kunnan $K$ algebrallinen laajennus $E$ on *separoituva*, jos sen jokainen alkio on separoituva $K$:n suhteen.

*Esimerkki* 2) Jos kunnan $K$ karakteristika on 0, niin jokainen jaoton polynomi $f \in K[X]$ on separoituva (lause 4.5.3, d), joten jokainen $K$:n algebrallinen laajennus $E$ on separoituva. Sama pätee yleisemmin, kun $K$ on ns. *perfekti* kunta (teht. 2).

**Harjoitustehtäviä**

1) Olkoon $K$ kunta, jonka karakteristika on $p \neq 0$, ja olkoon $L$ sen äärellinen laajennus, jonka aste $[L : K]$ ei ole jaollinen $p$:llä. Osoitettava, että $L$ on separoituva $K$:n suhteen.

2) Olkoon $K$ kunta, jonka karakteristika on alkuluku $p$. Osoitettava:
i) Kuvaus $x \mapsto x^p$ on kunnan $K$ endomorfismi.
ii) $K^p = \{x^p \mid x \in K\}$ on $K$:n alikunta.
iii) Jos $f$ on jaoton $K[X]$:ssä, niin $f \notin K^p[X^p]$. (Ensin $K^p[X^p] = (K[X])^p$.)
iv) Jos $K$ on äärellinen tai algebrallisesti suljettu, niin $K^p = K$.
v) Jos $K^p = K$, niin jokainen jaoton polynomi $f \in K[X]$ on separoituva.

Kuntaa $K$ sanotaan *perfektiksi*, kun sen karakteristika on 0 tai sitten $p \neq 0$ ja $K^p = K$.

3) Olkoon $K$ kunta, jonka karakteristika on alkuluku $p$, ja $\alpha$ jonkin sen algebrallisen laajennuksen alkio. Osoitettava, että $\alpha$ on separoituva $K$:n suhteen, jos ja vain jos $K(\alpha) = K(\alpha^p)$. (Jos $\alpha$ on separoituva $K$:n suhteen, niin se on separoituva myös $K(\alpha^p)$:n suhteen ja sen minimaalipolynomi on polynomin $X^p - \alpha^p$ tekijä.)

## 4.6. Galois'n laajennukset

Olkoon $K$ kunta ja $\Omega$ jokin sen algebrallinen sulkeuma. Tutkitaan mahdollisuuksia esittää $\Omega$:n alkioita toisten, mielellään yksinkertaisempien, alkioiden avulla. Tämä merkitsee vastaamista siihen, milloin alkio kuuluu eräiden toisten virittämään laajennukseen.

Olkoon aluksi $x$ jokin $\Omega$:n alkio. Jos $y$ on sen virittämässä laajennuksessa $K(x) = K[x]$, niin se voidaan esittää muodossa

$$y = f(x) = \sum_n a_n x^n,$$

missä $f = \sum_n a_n X^n \in K[X]$. Kaikilla $K$-automorfismeilla $u\colon \Omega \to \Omega$ pätee tällöin

$$u(y) = \sum_n a_n u(x)^n = f(u(x)).$$

Jos erityisesti $u$ on sellainen $K$-automorfismi, jolla $u(x) = x$, niin myös $u(y) = f(x) = y$. Tämä on siis välttämätön ehto sille, että $y$ olisi alkion $x$ virittämässä laajennuksessa.

Ehto ei kuitenkaan ole yleisesti riittävä.

*Esimerkki* 1) Olkoon $K$:n karakteristika $p > 0$ ja $y \in \Omega$ alkion $x$ $p$:s juuri $\sqrt[p]{x}$. Ehdosta $u(x) = x$ seuraa tällöin binomikaavan nojalla

$$(u(y) - y)^p = u(y^p) - y^p = u(x) - x = 0.$$

Tästä seuraa $u(y) = y$, vaikka $y$ ei olisi laajennuksessa $K(x)$ (jolloin $y$:n minimaalipolynomi $X^p - x \in K[X]$ ei ole separoituva).

Jos $N$ on alkioiden $x$ ja $y$ virittämä $K$:n normaali laajennus (joka on äärellinen, ks. lause 4.4.9) tai jokin muu ne sisältävä $K$:n normaali laajennus, niin $u(N) = N$ (kor. 4.4.7). Tällöin on riittävää tarkastella $K$-automorfismeja

$$\sigma\colon N \xrightarrow{\sim} N,$$

sillä ne ovat $\Omega$:n $K$-automorfismien rajoittumia (kor. 4.3.11).

Tarkastellaan aluksi erikoistapausta $K(x) = K$, jossa ehto $\sigma(x) = x$ pätee kaikilla laajennuksen $N$ $K$-automorfismeilla $\sigma$, ja tutkittavaksi jää, milloin ehdosta $\sigma(y) = y$ seuraa $y \in K$.

LAUSE 4.6.1. *Olkoon $N$ kunnan $K$ algebrallinen laajennus ja $G$ sen $K$-automorfismien ryhmä. Seuraavat ehdot ovat yhtäpitävät.*

a) *Jokainen $N$:n alkio, jonka $G$ kiinnittää, on $K$:n kuvassa.*
b) *$N$ on $K$:n normaali ja separoituva laajennus.*
c) *Jokaisen $N$:n alkion minimaalipolynomi $K$:n suhteen on renkaassa $N[X]$ tulo asteen 1 tekijöistä, joilla on eri juuret.*

*Todistus.* b) $\Leftrightarrow$ c): Lauseen 4.4.5 mukaan $N$ on normaali, jos ja vain jos sen jokaisen alkion minimaalipolynomi on $N[X]$:ssä tulo asteen 1 tekijöistä, ja lauseen 4.5.12 nojalla lisäksi separoituva, jos ja vain jos nämä juuret ovat yksinkertaiset.

a) $\Rightarrow$ c): Olkoon $x$ jokin $N$:n alkio ja $f \in K[X]$ sen minimaalipolynomi $K$:n suhteen. Olkoon $A$ polynomin $f$ laajennukseen $N$ kuuluvien juurien joukko, ja olkoon $g \in N[X]$ separoituva pääpolynomi

$$g = \prod_{y \in A} (X - y) = \sum_{n \in \mathbf{N}} \alpha_n X^n,$$

jonka juurina ovat $A$:n alkiot.

Olkoon $\sigma \in G$ jokin $N$:n $K$-automorfismi. Jos $y \in N$ on $f$:n juuri, niin $f(\sigma(y)) = \sigma(f(y)) = 0$. Tämä merkitsee, että $\sigma$ permutoi joukon $A$ alkiot. Polynomin $g$ kuva automorfismissa $\sigma$ on silloin

$$\sum_{n \in \mathbf{N}} \sigma(\alpha_n) X^n = \prod_{y \in A} (X - \sigma(y)) = \prod_{y \in A} (X - y) = \sum_{n \in \mathbf{N}} \alpha_n X^n,$$

ja siten $\sigma(\alpha_n) = \alpha_n$ kaikilla $n \in \mathbf{N}$.

Ehdon a) ollessa voimassa kertoimet $\alpha_n$ ovat siis kunnassa $K$ (tai täsmällisemmin sanottuna sen kuvassa $K.1 \subset N$, jonka kanssa se voidaan samastaa), ja $g$ voidaan tulkita algebran $K[X]$ polynomiksi.

Toisaalta $g(x) = 0$, koska $x$ on joukossa $A$, joten $g$ on jaollinen minimaalipolynomilla $f$. Koska $g$ on pääpolynomi ja se jakaa $f$:n renkaassa $N[X]$, sen täytyy olla sama kuin $f$. Nähdään siis, että $f = g$ on tulo asteen 1 tekijöistä $X - y$, joilla on eri juuret $y \in A$.

c) $\Rightarrow$ a): Olkoon $x$ jokin $N$:n alkio, joka ei ole $K$:n kuvassa, ja olkoon $f \in K[X]$ sen minimaalipolynomi $K$:n suhteen. Ehdon c) ollessa voimassa $f$:llä on tällöin esitys

$$f = \prod_{y \in A} (X - y),$$

missä $A$ on $f$:n juurien $y \in N$ joukko.

Koska $x$ ei ole $K$:ssa, aste $\deg(f)$ on vähintään 2, ja koska $f$:n juuret ovat yksinkertaiset, sillä on juuri $y$, joka ei ole $x$. Alkiolla $x$ on siten konjugaatti $y \neq x$ $K$:n suhteen.

Jos $\Omega$ on jokin $N$:n sisältävä $K$:n algebrallinen sulkeuma, niin on olemassa sellainen $K$-automorfismi $u\colon \Omega \to \Omega$, että $\sigma(x) = y$. Koska $N$ on normaali (ehto b), on $u(N) = N$. Tällöin $u$ rajoittuu $K$-automorfismiksi $\sigma\colon N \to N$, joka kuuluu ryhmään $G$ ja täyttää ehdon

$$\sigma(x) = u(x) = y \neq x.$$

Ryhmä $G$ ei siis kiinnitä alkiota $x$, joka ei ole $K$:n kuvassa. □

MÄÄRITELMÄ 4.6.2. Kunnan $K$ laajennus $N$ on *Galois'n laajennus*, jos se on algebrallinen ja toteuttaa lauseen 4.6.1 ehdot.

Olkoon $A$ jokin $K$:n algebrallisen sulkeuman $\Omega$ osajoukko. Jos $K$:n Galois'n laajennus $N \subset \Omega$ sisältää joukon $A$, niin se sisältää myös sen alkioiden konjugaatit, koska se on normaali. Lisäksi jokainen $A$:n alkio on tällöin separoituva $K$:n suhteen.

Olkoon $B$ joukon $A$ alkioiden $x$ konjugaattien $y \in \Omega$ joukko. Jos jokainen $x \in A$ on separoituva $K$:n suhteen, niin konjugaatit $y \in B$ ovat myös separoituvia, koska niillä on samat minimaalipolynomit $K$:n suhteen (ks. lause 4.5.8). Tällöin $A$:n (ja $K(A)$:n) virittämä normaali laajennus (lause 4.4.9)

$$N = K(B)$$

on separoituva $K$:n suhteen. Tämä seuraa lauseesta 4.5.12, sillä jokainen $K(B)$:n alkio on jossakin alilaajennuksessa $K(B')$, missä $B'$ on $B$:n äärellinen osajoukko.

Kun $A$:n alkiot ovat separoituvia $K$:n suhteen, niiden konjugaattien joukon $B$ virittämä laajennus $N = K(B)$ on siis Galois'n laajennus, joukon $A$ *virittämä* $K$:n *Galois'n laajennus*.

*Esimerkki* 2) Olkoon $(f_i)_{i\in I}$ perhe algebran $K[X]$ polynomeja, jotka eivät ole vakioita. Jos jokainen $f_i$ on separoituva, niin perheen juurikunta $N$ on $K$:n Galois'n laajennus, koska se on normaali, ja sen virittävät polynomien $f_i$ juuret ovat separoituvia $K$:n suhteen.

**Galois'n ryhmä.**

MÄÄRITELMÄ 4.6.3. Olkoon $N$ kunnan $K$ Galois'n laajennus. Laajennuksen $N$ *Galois'n ryhmä* kunnan $K$ suhteen on $N$:n $K$-automorfismien ryhmä $\mathrm{Gal}(N/K)$ (merk. myös $G(N/K)$ tai $G_{N/K}$).

Jos Galois'n laajennus $N$ on $K$:n äärellinen laajennus, niin ryhmä $\mathrm{Gal}(N/K)$ on myös äärellinen ja sen kertaluku on (lause 4.5.12)

$$(\mathrm{Gal}(N/K) : 1) = [N : K]_s = [N : K].$$

(Jos $\Omega$ on $K$:n algebrallinen sulkeuma ja $N \subset \Omega$, niin jokainen $K$-homomorfismi $u\colon N \to \Omega$ vastaa $N$:n automorfismia.) Tulos voidaan myös kääntää. Tämä on Artinin lause, joka todistetaan myöhemmin.

*Esimerkki* 3) Olkoon $f \in K[X]$ separoituva polynomi ja $A$ sen juurien joukko jossakin $K$:n algebrallisessa sulkeumassa $\Omega$. Separoituvuuden johdosta juurien lukumäärä on $n = \deg(f)$.

Polynomin $f$ juurikunta $N = K(A)$ on tällöin $K$:n Galois'n laajennus (esim. 4.6.2). Jokainen $K$-automorfismi $\sigma\colon N \to N$ permutoi $f$:n juuret: $\sigma(A) = A$. Rajoittumakuvaus $\sigma \mapsto \sigma|A$ on siten homomorfismi

$$\mathrm{Gal}(N/K) \to \mathfrak{S}_A,$$

joka on injektiivinen, koska joukko $A$ virittää $N$:n. Homomorfismin kuva on symmetrisen ryhmän $\mathfrak{S}_A$ aliryhmä (eli $A$:n permutaatioryhmä) $\Gamma$, jota sanotaan *polynomin $f$ Galois'n ryhmäksi*.

Erityisesti nähdään, että Galois'n ryhmän kertaluku on enintään sama kuin symmetrisen ryhmän $\mathfrak{S}_n$ kertaluku:

$$(\mathrm{Gal}(N/K) : 1) \leq n!\,.$$

Jos kertaluvut ovat samat, niin sanotaan, että $f$ on *yleinen asteen $n$ polynomi*. Tällöin sen Galois'n ryhmä on siis isomorfinen täyden symmetrisen ryhmän $\mathfrak{S}_n$ kanssa.

*Esimerkki* 4) Olkoon $f = X^2 + aX + b \in K[X]$ separoituva 2. asteen polynomi. Se voidaan hajottaa tuloksi

$$f = (X - x)(X - y),$$

missä $x$ on $f$:n juuri jossakin $K$:n algebrallisessa sulkeumassa $\Omega$, ja $y = -x - a \in K(x)$, $y \neq x$. Polynomin $f$ juurikunta $\Omega$:ssa on silloin $N = K(x, y) = K(x)$, ja sen Galois'n ryhmälle on kaksi mahdollisuutta.

Ensinnäkin, jos $x$ kuuluu kuntaan $K$, niin $N = K$ ja Galois'n ryhmä on triviaali. Jos taas $x \notin K$, niin $f$ on jaoton $K[X]$:ssä, ja sen toinen juuri $y$ on $x$:n konjugaatti $K$:n suhteen. Tällöin on siis olemassa $N$:n $K$-automorfismi $\sigma$, joka vie alkion $x$ konjugaatille $y$ ja permutaationa $y$:n taas takaisin $x$:lle. Polynomin $f$ Galois'n ryhmä on siten koko symmetrinen ryhmä $\Gamma = \mathfrak{S}_{\{x,y\}}$.

*Esimerkki* 5) Polynomi $f = X^3 - 2$ on jaoton $\mathbf{Q}[X]$:ssä, koska sillä ei ole rationaalista juurta. Sen juuret kompleksilukujen kunnassa ovat

$$\xi_1 = \sqrt{2}, \quad \xi_2 = \xi_1\zeta, \quad \xi_3 = \xi_1\zeta^2,$$

missä $\zeta = e^{2\pi i/3}$ on kolmas ykkösenjuuri.

Olkoon $A = \{\xi_1, \xi_2, \xi_3\}$ polynomin $f$ juurien joukko ja $\Gamma \subset \mathfrak{S}_A$ sen Galois'n ryhmä. Koska $f$ on jaoton, juuret ovat toistensa konjugaatteja, ja siten ryhmässä $\Gamma$ on ainakin kolme alkiota.

Toisaalta juurikunta $N = \mathbf{Q}(A)$ sisältää alkion $\zeta = \xi_2/\xi_1$, ja se toteuttaa yhtälön

$$\zeta^2 + \zeta + 1 = 0.$$

Koska $\zeta$ ei ole rationaalinen, laajennuksen $\mathbf{Q}(\zeta)$ aste $\mathbf{Q}$:n suhteen on siten 2. Tästä seuraa, että Galois'n ryhmän kertaluku

$$(\Gamma : 1) = [N : \mathbf{Q}] = [N : \mathbf{Q}(\zeta)][\mathbf{Q}(\zeta) : \mathbf{Q}]$$

on parillinen. Koska kertaluku jakaa ryhmän $\mathfrak{S}_A$ kertaluvun 6, sen täytyy olla 6. Galois'n ryhmä on siis koko symmetrinen ryhmä

$$\Gamma = \mathfrak{S}_A \cong \mathfrak{S}_3,$$

eli $f = X^3 - 2 \in \mathbf{Q}[X]$ on yleinen kolmannen asteen polynomi.

**Artinin lause.** Olkoon $N$ kunta ja $G$ jokin sen automorfismeista muodostuva ryhmä. Tällöin

$$K = N^G = \{x \in N \mid \sigma(x) = x \text{ kaikilla } \sigma \in G\}$$

on kunnan $N$ alikunta, jota sanotaan ryhmän $G$ *kiintokunnaksi*.

Lisäksi kunta $N$ on $K$:n laajennus ja jokainen kuvaus $\sigma \in G$ on sen $K$-automorfismi. Automorfismijoukko $G$ on siten kunnan $N$ suhteen vapaa joukko vektoriavaruudessa $\mathrm{Hom}_K(N, N)$ (lause 4.5.4).

Jos erityisesti $N$ on $K$:n äärellinen laajennus, niin ryhmä $G$ on äärellinen ja sen kertaluku toteuttaa ehdon (kor. 4.5.5)

$$(G : 1) \leq [N : K]. \tag{1}$$

Kääntäen pätee seuraava tulos.

LAUSE 4.6.4 (Artin). *Olkoon $N$ kunta, $G$ äärellinen ryhmä $N$:n automorfismeja ja $K = N^G$ sen kiintokunta. Tällöin*

i) $[N : K] = (G : 1)$ *on äärellinen,*
ii) $N$ *on $K$:n Galois'n laajennus, ja*
iii) $\mathrm{Gal}(N/K) = G$.

*Todistus.* Olkoon $G = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$, missä $n = (G : 1)$ on $G$:n kertaluku ja $\sigma_1 = \mathrm{Id}_N$.

i) Olkoot $x_1, \ldots, x_m$ kunnan $N$ alkioita. Osoitetaan, että ne ovat lineaarisesti riippuvia $K$:n suhteen, jos $m > n$. Tarkastellaan tätä varten avaruuden $N^n$ vektoreita

$$y_j = (\sigma_1(x_j), \ldots, \sigma_n(x_j)) \qquad (1 \leq j \leq m).$$

Jos $m$ on suurempi kuin avaruuden dimensio $\dim_N(N^n) = n$, on olemassa epätriviaali lineaarinen relaatio

$$\sum_{j=1}^{m} \lambda_j y_j = 0,$$

missä kertoimet $\lambda_j$ $(1 \leq j \leq n)$ ovat kunnassa $N$. Voidaan olettaa, että $y_1, \ldots, y_{m-1}$ ovat lineaarisesti riippumattomat $N$:n suhteen, kun tarvittaessa lukumäärää $m$ vähennetään. (Jäljelle voi jäädä $m \leq n$, mutta se ei vaikuta lineaariseen riippuvuuteen.)

Tällöin välttämättä $\lambda_m \neq 0$, ja kertomalla sen käänteisalkiolla saadaan lineaarinen relaatio, jossa $\lambda_m = 1$. Osoitetaan, että silloin kaikki kertoimet ovat kunnassa $K$.

Vektoreiden $y_j$ koordinaateista saadaan lineaarinen yhtälöryhmä

$$\sum_{j=1}^{m} \lambda_j \sigma_i(x_j) = 0 \qquad (1 \le i \le n).$$

Tästä seuraa kaikilla $\sigma \in G$ ja $1 \le i \le n$

$$\sum_{j=1}^{m} \sigma(\lambda_j)\sigma_i(x_j) = \sigma\Big(\sum_{j=1}^{m} \lambda_i(\sigma^{-1}\sigma_i)(x_j)\Big) = 0,$$

koska $\sigma^{-1}\sigma_i$ on jokin $\sigma_{i'} \in G$. Ehdon $\sigma(\lambda_m) = 1$ nojalla, näistä saadaan erotuksina yhtälöt

$$\sum_{j=1}^{m-1} [\lambda_j - \sigma(\lambda_j)]\sigma_i(x_j) = 0 \qquad (1 \le i \le n)$$

eli yhtäpitävästi lineaariset relaatiot

$$\sum_{j=1}^{m-1} [\lambda_j - \sigma(\lambda_j)]y_j = 0.$$

Koska $y_1, \ldots, y_{m-1}$ olivat lineaarisesti riippumattomat, kertoimien täytyy toteuttaa ehdot

$$\lambda_j = \sigma(\lambda_j)$$

kaikilla $\sigma \in G$, ja ne ovat siten ryhmän $G$ kiintokunnassa $K$.

Vektorien $y_j$ ensimmäisistä koordinaateista saadaan $K$-kertoiminen epätriviaali lineaarinen relaatio

$$\sum_{j=1}^{m} \lambda_j x_j = 0.$$

Tämä merkitsee, että jokainen $N$:n perhe, jossa on $m > n$ alkiota, on sidottu, ja siten aste $[N : K]$ on enintään sama kuin $n$. Erityisesti $N$ on $K$:n äärellinen laajennus, joten epäyhtälö (1) on käytettävissä, ja sen nojalla saadaan

$$[N : K] = n.$$

ii) Koska $K$ on ryhmään $G$ kuuluvien automorfismien kiintokunta, se on myös kaikkien $N$:n $K$-automorfismien kiintokunta. Lauseen 4.6.1 ehdon a) perusteella $N$ on siten $K$:n Galois'n laajennus.

iii) Joka tapauksessa $G$ on Galois'n ryhmän $\mathrm{Gal}(N/K)$ aliryhmä. Lisäksi ryhmillä on sama kertaluku, koska

$$(\mathrm{Gal}(N/K) : 1) = [N : K] = n$$

kuten edellä on osoitettu. Galois'n ryhmän $\mathrm{Gal}(N/K)$ täytyy siis olla sama kuin $G$. □

**Galois'n teorian peruslause.** Olkoon $K$ kunta. Tarkastellaan sen äärellisiä Galois'n laajennuksia $N$. Päämääränä on osoittaa, että $N$:n alilaajennukset vastaavat kääntäen yksikäsitteisesti sen Galois'n ryhmän aliryhmiä. Oletetaan, että $K$ on $N$:n alikunta.

LEMMA 4.6.5. *Jos $E$ on $N$:n alilaajennus, niin $N$ on $E$:n Galois'n laajennus, ja* $\mathrm{Gal}(N/E)$ *on ryhmän* $\mathrm{Gal}(N/K)$ *aliryhmä.*

*Todistus.* Olkoon $x$ jokin $N$:n alkio. Se on algebrallinen myös $E$:n suhteen, ja sen minimaalipolynomi $f \in E[X]$ kunnan $E$ suhteen jakaa sen minimaalipolynomin $g \in K[X]$ kunnan $K$ suhteen $E[X]$:ssä (kor. 4.2.4) ja myös $N[X]$:ssä.

Toisaalta $g$ on $N[X]$:ssä tulo asteen 1 tekijöistä (lause 4.6.1, c), joilla on eri juuret. Polynomilla $f$ on silloin sama ominaisuus, joten lauseen 4.6.1 ehto c) on voimassa myös $E$:n suhteen, ja siksi $N$ on $E$:n Galois'n laajennus.

Koska jokainen $N$:n $E$-automorfismi on myös $K$-automorfismi, on selvää, että $\mathrm{Gal}(N/E)$ on $\mathrm{Gal}(N/K)$:n aliryhmä. □

LEMMA 4.6.6. *Jos $H$ on ryhmän* $\mathrm{Gal}(N/K)$ *aliryhmä, niin sen kiintokunta $E = N^H$ on $N$:n alilaajennus, ja* $\mathrm{Gal}(N/E) = H$.

*Todistus.* Koska $K$ on ryhmän $\mathrm{Gal}(N/K)$ kiintokunta, se sisältyy aliryhmän $H$ kiintokuntaan $E$, ja siten $E$ on $K$:n laajennus.

Lisäksi $H$ on äärellinen, koska äärellisen laajennuksen $N$ Galois'n ryhmä on äärellinen. Artinin lauseen nojalla $H$ on silloin $N$:n Galois'n ryhmä kiintokuntansa $E$ suhteen (lause 4.6.4, iii). □

LAUSE 4.6.7. *Olkoon $N$ kunnan $K$ äärellinen Galois'n laajennus ja $G = \mathrm{Gal}(N/K)$. Silloin on olemassa kääntäen yksikäsitteinen vastaavuus,* Galois'n vastaavuus*,*

$$\{N\text{:n alilaajennukset}\} \longleftrightarrow \{G\text{:n aliryhmät}\},$$

*missä alilaajennusta $E \subset N$ vastaa aliryhmä* $\mathrm{Gal}(N/E) \subset G$*, ja aliryhmää $H \subset G$ vastaa alilaajennus $N^H \subset N$.*

*Todistus.* Jos $E$ on $N$:n alilaajennus, niin Galois'n ryhmä $H = \mathrm{Gal}(N/E)$ on $G$:n aliryhmä (lemma 4.6.5), ja sen kiintokunta $N^H$ on $E$ (lause 4.6.1, a).

Jos taas $H$ on $G$:n aliryhmä, niin sen kiintokunta $E = N^H$ on $N$:n alilaajennus, jonka Galois'n ryhmä $\mathrm{Gal}(N/E)$ on $H$ (lemma 4.6.6). □

*Huomautus.* Lauseen keskeinen sisältö on, että mielivaltaisen kunnan (separoituvat äärelliset) laajennukset voidaan löytää (ainakin periaatteessa) tarkastelemalla *äärellisiä ryhmiä.*

KOROLLAARI 4.6.8.

i) *Jos $E$ ja $E'$ ovat $N$:n alikuntia, jotka sisältävät $K$:n, niin*

$$E \subset E' \;\Leftrightarrow\; \mathrm{Gal}(N/E) \supset \mathrm{Gal}(N/E').$$

ii) *Jos $H$ ja $H'$ ovat* $\mathrm{Gal}(N/K)$*:n aliryhmiä, niin*

$$H \subset H' \;\Leftrightarrow\; N^H \supset N^{H'}.$$

*Todistus.* Olkoot $E$, $E'$ kaksi $N$:n alilaajennusta ja

$$H' = \mathrm{Gal}(N/E), \quad H = \mathrm{Gal}(N/E')$$

niitä vastaavat $\mathrm{Gal}(N/K)$:n aliryhmät.

Jos $E \subset E'$, niin jokainen $N$:n $E'$-automorfismi on $E$-automorfismi eli $H \subset H'$. Kääntäen, jos $H \subset H'$, niin $H$ kiinnittää jokaisen $N$:n alkion, jonka $H'$ kiinnittää, eli $N^H \supset N^{H'}$. Tämä todistaa kummankin kohdan, koska $N^H = E'$ ja $N^{H'} = E$. □

Korollaari 4.6.9. *Olkoot $E_1$, $E_2$ kaksi $K$:n sisältävää $N$:n alikuntaa ja $H_i = \mathrm{Gal}(N/E_i)$ $(i = 1, 2)$. Tällöin kaikilla $\sigma \in G$ pätee*

$$\sigma(E_1) = E_2 \;\Leftrightarrow\; \sigma H_1 \sigma^{-1} = H_2.$$

*Todistus.* Jos $\tau \in G$, niin kaikilla $x \in E_1$ pätee

$$\tau\sigma(x) = \sigma(x) \;\Leftrightarrow\; \sigma^{-1}\tau\sigma(x) = x.$$

Automorfismi $\tau$ kiinnittää siten alikunnan $\sigma(E_1)$ alkiot, jos ja vain jos $\sigma^{-1}\tau\sigma$ kuuluu Galois'n ryhmään $\mathrm{Gal}(N/E_1) = H_1$ eli yhtäpitävästi $\tau \in \sigma H_1 \sigma^{-1}$. Alilaajennusta $\sigma(E_1)$ vastaava aliryhmä on siis

$$\mathrm{Gal}(N/\sigma(E_1)) = \sigma H_1 \sigma^{-1},$$

ja tämä on $H_2$, jos ja vain jos $\sigma(E_1) = E_2$. □

Korollaari 4.6.10. *Olkoon $E$ $K$:n sisältävä $N$:n alikunta ja $H =$* $\mathrm{Gal}(N/E)$ *vastaava $G$:n aliryhmä.*

*Silloin $E$ on $K$:n Galois'n laajennus, jos ja vain jos $H$ on $G$:n normaali aliryhmä, ja näiden ehtojen ollessa voimassa rajoittumakuvaus $\sigma \mapsto \sigma|E$ indusoi isomorfismin*

$$G/H \xrightarrow{\sim} \mathrm{Gal}(E/K).$$

*Todistus.* Koska $N$ on $K$:n separoituva laajennus (lause 4.6.1, b), sen jokainen alkio on separoituva $K$:n suhteen, ja siten sen jokainen alilaajennus $E$ on myös separoituva.

Kunnan $K$ laajennus $E$ on siis Galois'n laajennus, jos ja vain jos se on normaali (lause 4.6.1, b), eli yhtäpitävästi $E$ on sama kuin jokainen konjugaattinsa $u(E) \subset \Omega$, missä $\Omega$ on jokin $E$:n sisältävä $K$:n algebrallinen sulkeuma ja $u$ on sen $K$-automorfismi (kor. 4.4.7).

Voidaan olettaa, että $\Omega$ sisältää myös laajennuksen $N$, jolloin jokainen $\sigma \in G$ on jonkin $K$-automorfismin $u\colon \Omega \to \Omega$ rajoittuma (kor. 4.3.11). Tällöin $u(E) = \sigma(E)$, joten $E$ on $K$:n normaali laajennus, jos ja vain jos $\sigma(E) = E$ kaikilla $\sigma \in G$. Korollaarin 4.6.9 mukaan tämä merkitsee, että $\sigma H \sigma^{-1} = H$ kaikilla $\sigma \in G$ eli että $H$ on $G$:n normaali aliryhmä.

Kun $E$ on $K$:n normaali laajennus, jokainen $K$-automorfismi $\sigma \in G$ rajoittuu $E$:n automorfismiksi, ja näin saadaan homomorfismi

$$\varphi\colon G = \mathrm{Gal}(N/K) \to \mathrm{Gal}(E/K),$$

Homomorfismi $\varphi$ on surjektiivinen, koska jokainen $E$:n $K$-automorfismi voidaan jatkaa ensin $\Omega$:n $K$-automorfismiksi, ja tällainen rajoittuu $N$:n $K$-automorfismiksi. Lisäksi $\varphi$:n ydin on

$$\mathrm{Ker}(\varphi) = \{\sigma \in G \mid \sigma|E = \mathrm{Id}_E\} = \mathrm{Gal}(N/E) = H.$$

Homomorfialauseen nojalla $\varphi$ indusoi siten isomorfismin

$$G/H \xrightarrow{\sim} \mathrm{Gal}(E/K).$$

□

**Harjoitustehtäviä**

1) Olkoon $E$ kunnan $K$ äärellinen separoituva laajennus. Osoitettava, että $E$:llä on vain äärellisen monta alilaajennusta. (Tarkastellaan $E$:n virittämää Galois'n laajennusta.)

2) Olkoon $f = X^3 + X^2 - 2X - 1$. Osoitettava:
i) $f$ on jaoton renkaassa $\mathbf{Q}[X]$.
ii) Jos $\zeta \in \mathbf{C}$, $\zeta \neq 1$ ja $\zeta^7 = 1$, niin $\sum_{i=0}^{6} \zeta^i = 0$ ja $f(\zeta + \zeta^{-1}) = 0$.
iii) $f$:n juuret $\mathbf{C}$:ssä ovat $\alpha = \zeta + \zeta^{-1}$, $\beta = \zeta^2 + \zeta^{-2} = \alpha^2 - 2$ ja $\gamma = \zeta^3 + \zeta^{-3} = \alpha^3 - 3\alpha$, missä $\zeta = e^{2\pi i/7}$.
iv) $N = \mathbf{Q}(\alpha)$ on kunnan $\mathbf{Q}$ Galois'n laajennus.
Pääteltävä, että $\mathrm{Gal}(N/\mathbf{Q})$ on 3-alkioinen syklinen ryhmä, jonka virittäjä $\sigma$ toteuttaa ehdot $\sigma(\alpha) = \beta$, $\sigma(\beta) = \gamma$ ja $\sigma(\gamma) = \alpha$.

3) Olkoon $\zeta = \sqrt{i} = (1+i)\sqrt{2}/2$ ja $N = \mathbf{Q}(\zeta)$ polynomin $f = X^4+1$ juurikunta $\mathbf{Q}$:n suhteen (teht. 4.4.1). Etsittävä
i) Galois'n ryhmä $G = \mathrm{Gal}(N/\mathbf{Q})$. (Toiminta virittäjällä $\zeta$.)
ii) $G$:n toiminta $N$:n alkioilla $\sqrt{2}$ ja $i\sqrt{2}$. (Esitetään kannan $1, \zeta, \zeta^2, \zeta^3$ avulla.)
iii) $G$:n aliryhmät ja vastaavat $N$:n alikunnat.

4) Olkoon $\xi = \sqrt[4]{2}$, $N = \mathbf{Q}(\xi, i)$ polynomin $f = X^4 - 2$ juurikunta $\mathbf{Q}$:n suhteen (teht. 4.4.2) ja $G = \mathrm{Gal}(N/\mathbf{Q})$. Osoitettava:
i) $[N : \mathbf{Q}(\xi)] = 2$ ja $[N : \mathbf{Q}] = 8$.
ii) On olemassa yksikäsitteinen automorfismi $\tau \in \mathrm{Gal}(N/\mathbf{Q}(\xi)) \subset G$, jolla $\tau(\xi) = \xi$ ja $\tau(i\xi) = -i\xi$.
iii) Jos $\sigma, \sigma' \in G$ ja $\sigma(\xi) = \sigma'(\xi)$, niin $\sigma = \sigma'$ tai $\sigma = \sigma'\tau$.
iv) On olemassa yksikäsitteinen $\sigma \in G$, jolla $\sigma(\xi) = i\xi$ ja $\sigma(i\xi) = -\xi$. (Jos $\sigma(\xi) = i\xi$, niin $\sigma(i\xi) \neq \sigma(-\xi) = -i\xi$.)

5) Tehtävän 4 merkinnöin osoitettava, että $G$:n alkiot $\sigma$ ja $\tau$ toteuttavat ehdot $\sigma^4 = \varepsilon$ (neutraalialkio), $\tau^2 = \varepsilon$ ja $(\sigma\tau)^2 = \varepsilon$, eli $\sigma\tau = \tau\sigma^{-1}$

ja $\tau\sigma = \sigma^{-1}\tau$, ja pääteltävä, että $G$ on *diedriryhmä* $D_4$ (neliön symmetriaryhmä), jossa on 4-alkioinen syklinen aliryhmä $H = \{\varepsilon, \sigma, \sigma^2, \sigma^3\}$ (neliön kierrot) ja lisäksi 4 alkiota $\tau$, $\sigma\tau$, $\sigma^2\tau$ ja $\sigma^3\tau$, joiden kertaluku on 2 (neliön peilaukset).

6) Olkoon $\xi = \sqrt[4]{2}$, $N = \mathbf{Q}(\xi, i)$ polynomin $f = X^4 - 2$ juurikunta $\mathbf{Q}$:n suhteen ja $G = \mathrm{Gal}(N/\mathbf{Q})$ (teht. 4, 5). Etsittävä $G$:n aliryhmät, joiden kertaluku on 4 (3 tapausta, yksi syklinen), sekä niiden kiintokunnat.

## 4.7. Abelin laajennukset

MÄÄRITELMÄ 4.7.1. Kunnan $K$ laajennus $E$ on $K$:n *Abelin laajennus*, jos se on Galois'n laajennus ja sen Galois'n ryhmä on vaihdannainen.

*Huomautus. Abel* osoitti 1800-luvun alussa, että yhtälö $f(x) = 0$, missä $f$ on separoituva polynomi, on "algebrallisesti ratkeava" kuten 2., 3. ja 4. asteen yhtälöt, jos sen Galois'n ryhmä (ks. esim. 4.6.3) on vaihdannainen eli *Abelin ryhmä*.

LAUSE 4.7.2. *Jos $N$ on kunnan $K$ Abelin laajennus, niin $N$:n jokainen alilaajennus $E$ on myös $K$:n Abelin laajennus.*

*Todistus.* Vaihdannaisen ryhmän $\mathrm{Gal}(N/K)$ jokainen aliryhmä on normaali. Erityisesti alilaajennusta $E$ vastaava aliryhmä $\mathrm{Gal}(N/E)$ on siis normaali. Korollaarin 4.6.10 nojalla $E$ on silloin $K$:n Galois'n laajennus ja sen Galois'n ryhmä on isomorfinen vaihdannaisen tekijäryhmän $\mathrm{Gal}(N/K)/\mathrm{Gal}(N/E)$ kanssa. □

Tärkeimmät Abelin laajennukset saadaan ns. ykkösenjuurista.

*Esimerkki* 1) Algebrallinen luku

$$\zeta = \sqrt{i} = (1+i)\sqrt{2}/2$$

on kahdeksas ykkösenjuuri: $\zeta^8 = 1$. Se toteuttaa yhtälön

$$\zeta^4 + 1 = 0,$$

jonka juuret kompleksilukujen kunnassa ovat $\zeta$:n parittomat potenssit

$$\begin{aligned}
\zeta_1 &= \zeta,\\
\zeta_2 &= \zeta^3 = (-1+i)\sqrt{2}/2,\\
\zeta_3 &= \zeta^5 = (-1-i)\sqrt{2}/2,\\
\zeta_4 &= \zeta^7 = (1-i)\sqrt{2}/2.
\end{aligned}$$

Kaikki juuret kuuluvat laajennukseen $\mathbf{Q}(\zeta)$, joka on siis polynomin $X^4 + 1$ juurikunta $\mathbf{Q}$:n suhteen ja siten $\mathbf{Q}$:n Galois'n laajennus (esim. 4.6.2, polynomi on separoituva).

Juurikunta sisältää myös luvut

$$i = \zeta^2 \quad \text{ja} \quad \sqrt{2} = \zeta + \zeta^7,$$

ja kääntäen $\zeta$ on näiden virittämässä laajennuksessa. Tästä seuraa

$$\mathbf{Q}(\zeta) = \mathbf{Q}(i, \sqrt{2}).$$

Koska $\sqrt{2}$:n aste $\mathbf{Q}$:n suhteen on 2 , ja $i$:n aste $\mathbf{Q}(\sqrt{2})$:n suhteen on samoin 2 (minimaalipolynomit ovat $X^2 - 2$ ja $X^2 + 1$), luvun $\zeta$ aste $\mathbf{Q}$:n suhteen on

$$[\mathbf{Q}(\zeta) : \mathbf{Q}] = [\mathbf{Q}(i, \sqrt{2}) : \mathbf{Q}(\sqrt{2})][\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2 \cdot 2 = 4.$$

Polynomi $X^4 + 1$ on siten $\zeta$:n minimaalipolynomi $\mathbf{Q}$:n suhteen. Sen juuret $\zeta_i$ $(1 \leq i \leq 4)$ ovat $\zeta$:n konjugaatit $\mathbf{Q}$:n suhteen ja jokaiseen liittyy $\mathbf{Q}$-isomorfismi

$$\sigma_i \colon \mathbf{Q}(\zeta) \to \mathbf{Q}(\zeta_i),$$

joka toteuttaa ehdon $\sigma_i(\zeta) = \zeta_i$ (lause 4.4.2). Koska $\mathbf{Q}(\zeta_i)$ on $\mathbf{Q}(\zeta)$:n alilaajennus, jolla on sama aste 4, jokainen $\sigma_i$ on $\mathbf{Q}(\zeta)$:n automorfismi, ja ne muodostavat siten koko Galois'n ryhmän:

$$\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}.$$

Automorfismi $\sigma_1$ on identtinen kuvaus ja suoralla laskulla todetaan, että jokainen $\sigma_i$ toteuttaa ehdon

$$\sigma_i^2 = \sigma_1.$$

(Esimerkiksi $\sigma_2^2(\zeta) = \sigma_2(\zeta_2) = \sigma_2(\zeta^3) = \sigma_2(\zeta)^3 = (\zeta^3)^3 = \zeta^9 = \zeta$.)

Ryhmä $\mathrm{Gal}(\mathbf{Q}(\zeta) : \mathbf{Q})$ on siten *Kleinin neliryhmä* ja vaihdannainen (ks. Algebra I). Helposti nähdään myös, että polynomin $X^4 + 1$ Galois'n ryhmä $\Gamma \subset \mathfrak{S}_4$ (ks. esim. 4.6.3) muodostuu juurien parillisista permutaatioista. Se on siis alternoivan ryhmän $\mathfrak{A}_4$ aliryhmä (ks. esim. 1.5.5)

$$H = \{s \in \mathfrak{A}_4 \mid s^2 = \mathrm{Id}\} = \{\mathrm{Id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}.$$

(Esimerkiksi $\sigma_2(\zeta) = \zeta^3$, $\sigma_2(\zeta^3) = (\zeta^3)^3 = \zeta$, $\sigma_2(\zeta^5) = (\zeta^3)^5 = \zeta^7$ ja $\sigma_2(\zeta^7) = (\zeta^3)^7 = \zeta^5$, joten vastaava permutaatio on $(1\,2)(3\,4)$.)

Galois'n ryhmällä on kolme epätriviaalia aliryhmää $H_i = \{\sigma_1, \sigma_i\}$ $(i = 2, 3, 4)$, ja niiden kiintokunnat $\mathbf{Q}(i)$, $\mathbf{Q}(i\sqrt{2})$ ja $\mathbf{Q}(\sqrt{2})$ ovat $\mathbf{Q}$:n Abelin laajennuksia, joiden ryhmät ovat 2-alkioisia syklisiä ryhmiä.

.

**Ykkösenjuuret.** Olkoon $K$ kunta.

MÄÄRITELMÄ 4.7.3. Kunnan $K$ alkio $\zeta$ on *ykkösenjuuri*, jos $\zeta^n = 1$ jollakin kokonaisluvulla $n > 0$. Tällöin $\zeta$ on $n$:s ykkösenjuuri.

*Huomautus.* Ykkösenjuuret ovat siis ne kunnan $K$ multiplikatiivisen ryhmän $K^* = K \setminus \{0\}$ alkiot, joilla on äärellinen kertaluku. Jos $K$ on äärellinen, kaikki alkiot $\zeta \in K^*$ ovat ykkösenjuuria.

Jokaisella kokonaisluvulla $n > 0$ kunnan $K$ $n$:nsien ykkösenjuurien joukolle käytetään merkintää

$$\mu_n(K) = \{\zeta \in K \mid \zeta^n = 1\}$$

ja vastaavasti kaikkien ykkösenjuurien joukolle merkintää

$$\mu_\infty(K) = \{\zeta \in K \mid \zeta^n = 1 \text{ jollakin } n > 0\}.$$

Jokainen $\mu_n(K)$ on multiplikatiivisen ryhmän $K^*$ aliryhmä, koska ehdoista $\zeta^n = \eta^n = 1$ seuraa $(\zeta/\eta)^n = 1$. Lisäksi

$$\mu_n(K) \subset \mu_m(K),$$

kun $m$ on $n$:n kerrannainen. Tästä seuraa, että

$$\mu_\infty(K) = \bigcup_{n>0} \mu_n(K)$$

on myös $K^*$:n aliryhmä. Jos näet $\zeta \in \mu_n(K)$ ja $\eta \in \mu_m(K)$ ovat kaksi ykkösenjuurta, niin $\zeta$, $\eta$ ja myös $\zeta/\eta$ ovat ryhmässä $\mu_{nm}(K)$.

*Esimerkki* 2) Rationaalilukujen kunnassa $\mu_n(\mathbf{Q})$ on $\{1, -1\}$, kun $n$ on parillinen, ja $\{1\}$, kun $n$ on pariton.

Yleisesti jokainen ryhmä $\mu_n(K)$ on äärellinen, ja sen kertaluku toteuttaa ehdon

$$(\mu_n(K) : 1) \leq n,$$

koska polynomilla $X^n - 1$ on enintään $n$ juurta kokonaisalueessa $K$. Seuraava aputulos on keskeinen ryhmien $\mu_n(K)$ teoriassa.

LEMMA 4.7.4. *Jos $G$ on ryhmän $K^*$ äärellinen aliryhmä, niin se on syklinen ja sama kuin $\mu_n(K)$, missä $n = (G : 1)$ on $G$:n kertaluku.*

*Todistus.* 1° Jokaisen alkion $\zeta \in G$ kertaluku on Lagrangen lauseen nojalla $n$:n tekijä, joten se toteuttaa ehdon $\zeta^n = 1$. Siten $G$ on ryhmän $\mu_n(K)$ aliryhmä. Koska jälkimmäisen kertaluku on enintään $n$, ryhmät ovat samat:

$$G = \mu_n(K).$$

2° Jokaista luvun $n$ tekijää $d$ kohti olkoon $G_d$ niiden $G$:n alkioiden joukko, joiden kertaluku on $d$. Olkoon $d$ sellainen, että $G_d$ ei ole tyhjä. Jokainen $\zeta \in G_d$ virittää silloin $G$:n syklisen aliryhmän

$$H = \{1, \zeta, \zeta^2, \ldots, \zeta^{d-1}\},$$

jonka kertaluku on $d$. Kohdan 1° nojalla $H$ on siis sama kuin $\mu_d(K)$.

Erityisesti nähdään, että $G_d$ on sama kuin ryhmän $\mu_d(K)$ virittäjien joukko. Jos $\zeta \in G_d$, niin $\zeta^k$ virittää koko ryhmän $\mu_d(K)$, jos ja vain jos $\text{syt}(k, d) = 1$. Tällaisten eksponenttien $k$ lukumäärä välillä $[0, d-1]$ on $\varphi(d)$, missä $\varphi$ on Eulerin funktio (ks. Algebra I). Näin saadaan:

*Jos $G_d \neq \emptyset$, niin $\mu_d(K)$ on $d$-alkioinen syklinen ryhmä, ja*

$$\text{Card}(G_d) = \varphi(d).$$

3° Olkoon $d > 0$ jokin luvun $n$ tekijä. Jos $x \in \mathbf{Z}$ ja $0 \leq x < n$, niin $\text{syt}(x, n) = d$, jos ja vain jos $x = kd$, missä $0 \leq k < n/d$ ja

$$\text{syt}(k, n/d) = 1.$$

Ehdon täyttävien lukujen $x$ lukumäärä on siten $\varphi(n/d)$. Kun käydään läpi kaikki $n$:n tekijät $d$, saadaan kaikki välin $[0, n-1]$ luvut ja siten yhtälöt

$$n = \sum_{d|n} \varphi(n/d) = \sum_{d|n} \varphi(d),$$

missä jälkimmäisessä summassa $n$:n tekijä $d$ on korvattu $n/d$:llä.

4° Koska jokaisella $G$:n alkiolla on kertaluku $d$, joka on $n$:n tekijä, $G$ on yhdiste joukoista $G_d$. Kohtien 2° ja 3° nojalla saadaan siten

$$n = \mathrm{Card}(G) = \sum_{d|n} \mathrm{Card}(G_d) \leq \sum_{d|n} \varphi(d) = n.$$

Tämä on mahdollista vain, jos jokaisella $n$:n tekijällä $d$ pätee yhtälö

$$\mathrm{Card}(G_d) = \varphi(d).$$

Erityisesti täytyy olla $G_n \neq \emptyset$, ja siten $G = \mu_n(K)$ on syklinen ryhmä kohdan 2° nojalla. □

Tulos osoittaa myös, että yhtälö

$$(\mu_n(K) : 1) = n$$

on voimassa, jos ja vain jos on olemassa ykkösenjuuria $\zeta \in \mu_n(K)$, joiden kertaluku on $n$, eli ne toteuttavat ehdot

$$\zeta^n = 1, \quad \zeta^k \neq 1 \quad (0 < k < n).$$

Tällainen $\zeta$ on *primitiivinen n:s ykkösenjuuri*, ja se virittää koko ryhmän $\mu_n(K)$.

LAUSE 4.7.5. *Olkoon $K$ kunta ja $n > 0$ kokonaisluku.*

i) *$\mu_n(K)$ on syklinen ryhmä ja sen kertaluku on $n$:n tekijä.*
ii) *Jos $K$ on algebrallisesti suljettu ja $\mathrm{char}(K) = 0$ tai $\mathrm{char}(K) = p \neq 0$ ja $p \nmid n$, niin $(\mu_n(K) : 1) = n$.*
iii) *Jos $\mathrm{char}(K) = p \neq 0$, niin $\mu_{np^r}(K) = \mu_n(K)$ kaikilla $r \in \mathbf{N}$.*

*Todistus.* i) Ryhmä $\mu_n(K)$ on joka tapauksessa äärellinen. Sen kertaluku olkoon $m \leq n$. Lemman 4.7.4 nojalla $\mu_n(K)$ on syklinen ja sama kuin $\mu_m(K)$.

Vielä on osoitettava, että $m$ on $n$:n tekijä. Tarkastellaan jakoyhtälöä

$$n = qm + r,$$

missä $q$, $r \in \mathbf{N}$ ja $0 \leq r < m$. Olkoon $\zeta$ jokin syklisen ryhmän $\mu_m(K)$ virittäjä eli primitiivinen $m$:s ykkösenjuuri. Silloin yhtälöstä

$$1 = \zeta^n = (\zeta^m)^q \zeta^r = \zeta^r$$

seuraa $r = 0$, ja siten $n = qm$ on jaollinen $m$:llä.

ii) Jos $\mathrm{char}(K) = 0$, tai $\mathrm{char}(K) = p \neq 0$ mutta $p \nmid n$, niin polynomi $X^n - 1$ ja sen derivaatta $nX^{n-1}$ ovat keskenään jaottomat, koska $n$ on kääntyvä $K$:ssa ja $K[X]$:ssä pätee yhtälö

$$n^{-1}X.(nX^{n-1}) - (X^n - 1) = 1.$$

Lauseen 4.5.1 nojalla $X^n-1$ on silloin separoituva, joten $K$:n ollessa algebrallisesti suljettu, sillä on $n$ eri juurta $\zeta \in \mu_n(K)$.

iii) Jos $\mathrm{char}(K) = p \neq 0$, niin kuvaus $x \mapsto x^{p^r}$ on $K$:n endomorfismi ja injektiivinen kuten kaikki kuntien homomorfismit. Ehdot $\zeta^{np^r} = 1$, eli $(\zeta^n)^{p^r} = 1^{p^r}$, ja $\zeta^n = 1$ ovat siten yhtäpitävät kaikilla $\zeta \in K$. □

*Esimerkki* 3) Kompleksilukujen kunta on algebrallisesti suljettu ja sen karakteristika on 0. Kaikilla kokonaisluvuilla $n > 0$ on

$$\mu_n(\mathbf{C}) = \{e^{2\pi ik/n} \mid 0 \leq k < n\}$$

$n$-alkioinen syklinen ryhmä. Primitiiviset $n$:nnet ykkösenjuuret ovat $e^{2\pi ik/n}$, missä $0 < k < n$ ja $\mathrm{syt}(k, n) = 1$, ja niiden lukumäärä on $\varphi(n)$.

**Ykkösenjuurikunnat.** Olkoon $K$ kunta ja $n \geq 1$ kokonaisluku. Oletetaan lisäksi, että $n$ ei ole jaollinen $K$:n karakteristikalla $p$ siinä tapauksessa, että tämä ei ole 0.

MÄÄRITELMÄ 4.7.6. Kunnan $K$ laajennus $E$ on $K$:n $n$:s *ykkösenjuurikunta*, jos se on polynomin $X^n - 1$ juurikunta $K$:n suhteen.

Syklisen ryhmän $\mu_n(E)$ kertaluku on tällöin $n$ (ks. lause 4.7.5, ii), ja koska se virittää juurikunnan $E$, jokainen primitiivinen $n$:s ykkösenjuuri $\zeta \in \mu_n(E)$ virittää jo yksin koko laajennuksen:

$$E = K(\zeta).$$

Koska kaikki $n$:nnet ykkösenjuuret ovat $\zeta^k$ $(0 \leq k < n)$, polynomilla $X^n - 1$ on $E[X]$:ssä hajotelma

$$X^n - 1 = \prod_{k=0}^{n-1}(X - \zeta^k).$$

LAUSE 4.7.7. *Jos $R_n$ on kunnan $K$ $n$:s ykkösenjuurikunta, niin*

i) *$R_n$ on $K$:n äärellinen Abelin laajennus,*
ii) *$\mathrm{Gal}(R_n/K)$ on isomorfinen ryhmän $(\mathbf{Z}/n\mathbf{Z})^*$ jonkin aliryhmän kanssa ja*
iii) *$[R_n : K]$ on $\varphi(n)$:n tekijä.*

*Todistus.* i) Koska $n \neq 0$ kunnassa $K$, polynomi $X^n - 1 \in K[X]$ on separoituva (lause 4.7.5, ii). Sen juurikuntana $R_n$ on siten $K$:n äärellinen Galois'n laajennus (esim. 4.6.2). Kohdasta ii) seuraa, että Galois'n ryhmä on vaihdannainen.

ii) Olkoon $\zeta \in \mu_n(R_n)$ jokin primitiivinen $n$:s ykkösenjuuri. Jos $\sigma$ on jokin $R_n$:n automorfismi, niin $\sigma(\zeta)$ on myös primitiivinen $n$:s ykkösenjuuri, sillä se toteuttaa ehdon

$$\sigma(\zeta)^n = \sigma(\zeta^n) = \sigma(1) = 1,$$

ja lisäksi kaikilla kokonaisluvuilla $k \in [1, n-1]$

$$\sigma(\zeta)^k = \sigma(\zeta^k) \neq \sigma(1) = 1,$$

koska $\zeta^k \neq 1$ ja $\sigma$ on bijektiivinen. Koska $\zeta$ ja $\sigma(\zeta)$ ovat ryhmän $\mu_n(R_n)$ virittäjiä, on siis $\sigma(\zeta) = \zeta^k$ jollakin kokonaisluvulla $k$, joka toteuttaa ehdon $\mathrm{syt}(k, n) = 1$.

Koska $\zeta^k$ riippuu vain $k$:n jäännösluokasta modulo $n$, jokaiseen $R_n$:n $K$-automorfismiin $\sigma \in \mathrm{Gal}(R_n/K)$ liittyy täten yksikäsitteinen jäännösluokka

$$\chi_n(\sigma) = \bar{k} \in (\mathbf{Z}/n\mathbf{Z})^*.$$

On riittävää osoittaa, että kuvaus

$$\chi_n \colon \mathrm{Gal}(R_n/K) \to (\mathbf{Z}/n\mathbf{Z})^*$$

on injektiivinen homomorfismi.

Olkoot $\sigma$, $\tau$ kaksi $R_n$:n $K$-automorfismia ja $k$, $l$ sellaisia kokonaislukuja, että $\sigma(\zeta) = \zeta^k$ ja $\tau(\zeta) = \zeta^l$. Yhtälöistä

$$(\sigma\tau)(\zeta) = \sigma(\zeta^l) = \sigma(\zeta)^l = \zeta^{kl}$$

seuraa silloin

$$\chi_n(\sigma\tau) = \overline{kl} = \chi_n(\sigma)\chi_n(\tau).$$

Kuvaus $\chi_n$ on siis homomorfismi.

Lisäksi ehto $\chi_n(\sigma) = \bar{1}$ merkitsee, että $\sigma$ kiinnittää laajennuksen $R_n$ virittäjän $\zeta$ ja siten kaikki muutkin sen alkiot. Homomorfismin $\chi_n$ ydin on siis triviaali, joten se on injektiivinen.

iii) Galoin'n laajennuksen aste $[R_n : K]$ on sama kuin sen Galois'n ryhmän $\mathrm{Gal}(R_n/K)$ kertaluku. Kun tämä on isomorfinen ryhmän $(\mathbf{Z}/n\mathbf{Z})^*$ aliryhmän kanssa, sen kertaluku on Lagrangen lauseen nojalla jälkimmäisen ryhmän kertaluvun $\varphi(n)$ tekijä. □

*Huomautus.* Lauseen todistuksessa määritelty upotus

$$\chi_n \colon \mathrm{Gal}(R_n/K) \hookrightarrow (\mathbf{Z}/n\mathbf{Z})^*$$

on *kanoninen* eli ei riipu ykkösenjuuren $\zeta$ valinnasta. Jos näet $\zeta'$ on toinen primitiivinen $n$:s ykkösenjuuri, niin $\zeta' = \zeta^j$ jollakin $j \in \mathbf{Z}$, ja tällöin kaikilla $\sigma \in \mathrm{Gal}(R_n/K)$ pätee

$$\sigma(\zeta') = \sigma(\zeta)^j = \zeta^{kj} = (\zeta')^k,$$

kun $k \in \mathbf{Z}$ ja $\sigma(\zeta) = \zeta^k$.

*Esimerkki* 4) Kunnan $\mathbf{Q}$ laajennus $\mathbf{Q}(i)$ on sen neljäs ykkösenjuurikunta $R_4$, koska $i$ on primitiivinen neljäs ykkösenjuuri.

Laajennuksen aste on $[\mathbf{Q}(i) : \mathbf{Q}] = 2$. Galois'n ryhmä $\mathrm{Gal}(\mathbf{Q}(i)/\mathbf{Q})$ on 2-alkioinen syklinen ryhmä, jonka virittäjä $\sigma$ toteuttaa ehdon $\sigma(i) = -i = i^3$. Kanoninen homomorfismi

$$\chi_4 \colon \mathrm{Gal}(R_4/\mathbf{Q}) \to (\mathbf{Z}/4\mathbf{Z})^* = \{\bar{1}, \bar{3}\}$$

on isomorfismi.

Algebrallinen luku $\zeta = \sqrt{i}$ (ks. esim. 4.7.1) on primitiivinen 8:s ykkösenjuuri. Muut primitiiviset 8:nnet ykkösenjuuret ovat $\zeta$:n konjugaatit $\zeta^3$, $\zeta^5$ ja $\zeta^7$. Jokaista näistä vastaa ykkösenjuurikunnan $R_8 = \mathbf{Q}(\zeta)$ automorfismi ja kanoninen homomorfismi

$$\chi_8 \colon \mathrm{Gal}(R_8/\mathbf{Q}) \to (\mathbf{Z}/8\mathbf{Z})^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$$

on bijektiivinen.

*Huomautus.* Kanoninen homomorfismi $\chi_n$ on bijektiivinen, jos ja vain jos primitiiviset $n$:nnet ykkösenjuuret ovat toistensa konjugaatteja kunnan $K$ suhteen. Tämä pätee kaikilla kokonaisluvuilla $n > 0$, kun $K$ on rationaalilukujen kunta $\mathbf{Q}$ (*Gauss*).

**Äärelliset eli Galois'n kunnat.** Olkoon $K$ äärellinen kunta. Sen karakteristika on alkuluku $p$, koska jokainen kunta, jonka karakteristika on 0, on ääretön.

Olkoon $P$ kunnan $K$ alkukunta. Se on voidaan samastaa kunnan $\mathbf{Z}/p\mathbf{Z}$ kanssa. Kunta $K$ on $P$:n laajennus, jonka aste $n = [K : P]$ on äärellinen. Vektoriavaruutena $P$:n suhteen $K$ on silloin isomorfinen avaruuden $P^n$ kanssa, joten sen alkioiden lukumäärä on karakteristikan $p$ potenssi $q = p^n$.

Kunnan $K$ multiplikatiivinen ryhmä $K^* = K \setminus \{0\}$ on myös äärellinen ja sen kertaluku on $q - 1$. Lemman 4.7.4 nojalla se on syklinen ja sama kuin ykkösenjuurten ryhmä

$$K^* = \mu_{q-1}(K).$$

Erityisesti jokainen $x \in K^*$ toteuttaa ehdon

$$x^{q-1} = 1,$$

ja tästä seuraa kaikilla $x \in K$ yhtälö

$$x^q = x.$$

Polynomin $X^q - X$ juurina ovat siten kunnan $K$ kaikki $q$ alkiota. Sen jokaisen juuren täytyy silloin olla yksinkertainen, ja sillä on tuloesitys

$$X^q - X = \prod_{x \in K} (X - x).$$

(Myös voidaan todeta, että $X^q - X$ on separoituva, koska sen juuret eivät ole derivaatan $-1$ nollakohtia.)

Tämä merkitsee, että *$K$ on polynomin $X^q - X$ juurikunta $P$:n suhteen ja myös $P$:n $q - 1$:s ykkösenjuurikunta.*

*Esimerkki* 5) Jos $p$ on alkuluku, niin $\mathbf{Z}/p\mathbf{Z}$ on äärellinen kunta, joten sen multiplikatiivinen ryhmä $(\mathbf{Z}/p\mathbf{Z})^*$ on syklinen. Jokaista lukua $a \in \mathbf{Z}$, jonka luokka virittää ryhmän $(\mathbf{Z}/p\mathbf{Z})^*$ sanotaan *primitiiviseksi juureksi modulo $p$.*

Lause 4.7.8.

i) *Äärellisen kunnan alkioiden lukumäärä on sen karakteristikan $p$ potenssi $q = p^n$.*
ii) *Jos $p$ on alkuluku, $n > 0$ ja $q = p^n$, niin polynomin $X^q - X$ juurikunnassa $\mathbf{F}_q$ kunnan $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ suhteen on $q$ alkiota.*
iii) *Kunta, jossa on $q = p^n$ alkiota, on isomorfinen kunnan $\mathbf{F}_q$ kanssa.*
iv) *$\mathbf{F}_q^*$ on syklinen ryhmä, jonka kertaluku on $q - 1$.*

*Todistus.* Kohdat i) ja iv) on todistettu edellä, ja iii) seuraa siitä, että alkukunnat, joiden karakteristika on $p$, voidaan samastaa, ja polynomin $X^q - X$ juurikunnat alkukunnan suhteen ovat isomorfiset (lause 4.3.7).

ii) Olkoon $\Omega$ jokin kunnan $\mathbf{F}_p$ algebrallinen sulkeuma, ja olkoon

$$u\colon \Omega \to \Omega, \quad x \mapsto x^q,$$

homomorfismi, joka saadaan iteroimalla $n$:sti homomorfismia $x \mapsto x^p$. Se on $\Omega$:n automorfismi, koska jokaisella polynomilla $X^q - x$ $(x \in \Omega)$ on juuri $\Omega$:ssa.

Automorfismin $u$ kiintokunta

$$K = \{x \in \Omega \mid x^q = x\}$$

on $\Omega$:n alikunta, ja se sisältää täsmälleen polynomin $X^q - X$ juuret algebrallisessa sulkeumassa $\Omega$. Se on silloin eräs polynomin $X^q - X$ juurikunta $\mathbf{F}_q$. Koska polynomi on separoituva, juurien ja samalla kunnan $\mathbf{F}_q$ alkioiden lukumäärä on $q$. □

KOROLLAARI 4.7.9. *Kunnan $\mathbf{F}_q$ äärelliset laajennukset ovat isomorfisia kuntien $\mathbf{F}_{q^m}$ $(m > 0)$ kanssa, ja ne ovat $\mathbf{F}_q$:n Abelin laajennuksia.*

*Todistus.* Olkoon $K$ kunnan $\mathbf{F}_q$ äärellinen laajennus, jonka aste on $[K : \mathbf{F}_q] = m$. Sen alkioiden lukumäärä on silloin $q^m$, joten se on isomorfinen kunnan $\mathbf{F}_{q^m}$ kanssa (lause 4.7.8, iii).

Toisaalta $\mathbf{F}_{q^m}$ on myös polynomin $X^{q^m-1} - 1$ juurikunta jokaisen alikuntansa suhteen. Se on siten eräs kunnan $\mathbf{F}_q$ ykkösenjuurikunta ja siksi sen Abelin laajennus (lause 4.7.7, i). □

*Huomautus.* Itse asiassa $\mathrm{Gal}(\mathbf{F}_{q^m}/\mathbf{F}_q)$ on syklinen ryhmä, jonka virittää $\mathbf{F}_q$-automorfismi $x \mapsto x^q$.

**Sykliset laajennukset.**

MÄÄRITELMÄ 4.7.10. Kunnan $K$ laajennus $E$ on *syklinen*, jos se on $K$:n Galois'n laajennus ja $\mathrm{Gal}(E/K)$ on syklinen.

Jokainen syklinen laajennus on siis Abelin laajennus.

*Esimerkki* 6) Jos $E$ on kunnan $K$ Galois'n laajennus, jonka aste on alkuluku $p$, niin $\mathrm{Gal}(E/K) \cong \mathbf{Z}/p\mathbf{Z}$ on syklinen.

Olkoon $K$ kunta ja $E$ sen syklinen laajennus, jonka aste on $n$. Koska syklisen ryhmän aliryhmät ja tekijäryhmät ovat syklisiä, jokainen $E$:n alilaajennus $F$ on myös $K$:n syklinen laajennus (ks. lause 4.7.2). Samoin $E$ on $F$:n syklinen laajennus.

Olkoon $K$ kunta ja $n \geq 1$ kokonaisluku. Oletetaan lisäksi, että $n$ ei ole jaollinen $K$:n karakteristikalla $p$ siinä tapauksessa, että tämä ei ole 0. Seuraavissa lauseissa ratkaistaan täydellisesti kysymys, millaisia ovat asteen $n$ sykliset laajennukset, kun

$$(\mu_n(K) : 1) = n$$

eli $K$ *sisältää kaikki $n$:nnet ykkösenjuuret* (missä tahansa laajennuksessa; ks. lause 4.7.5, ii).

LAUSE 4.7.11. *Jos $K$ sisältää $n$:nnet ykkösenjuuret ja $a \in K^*$, niin*

i) *binomin $X^n - a$ juurikunta $E$ kunnan $K$ suhteen on syklinen,*
ii) *$E = K(\theta)$, missä $\theta^n = a$,*
iii) *$[E : K] = d$ on luvun $n$ tekijä.*

*Todistus.* ii) Olkoon $\theta \in E$ jokin binomin $X^n - a$ juuri. Jos $\theta' \in E$ on sen toinen juuri, niin

$$(\theta'/\theta)^n = a/a = 1.$$

Osamäärä $\zeta = \theta'/\theta$ on siis $n$:s ykkösen juuri ja siten oletuksen nojalla kunnassa $K$. Juuren $\theta$ virittämä laajennus $K(\theta)$ sisältää täten kaikki binomin $X^n - a$ juuret, joten se on sen koko juurikunta $E$.

i) Binomi $X^n - a$ ja sen derivaatta $nX^{n-1}$ ovat keskenään jaottomat $K[X]$:ssä, koska $n \neq 0$ kunnassa $K$. Binomi on siis separoituva, joten sen juurikunta $E$ on $K$:n Galois'n laajennus (esim. 4.6.2).

Olkoon $\theta \in E$ jokin binomin juuri. Kaikilla Galois'n ryhmän alkioilla $\sigma \in \mathrm{Gal}(E/K)$ on silloin voimassa

$$\sigma(\theta)^n = \sigma(\theta^n) = \sigma(a) = a,$$

koska $\sigma$ on $K$-automorfismi. Yllä esitetyn nojalla (kohta ii) on siis

$$\sigma(\theta) = \zeta_\sigma \theta,$$

missä $\zeta_\sigma \in \mu_n(K)$. Osoitetaan, että kuvaus $\sigma \mapsto \zeta_\sigma$ on injektiivinen homomorfismi

$$\mathrm{Gal}(E/K) \hookrightarrow \mu_n(K).$$

Jos $\sigma$, $\tau \in \mathrm{Gal}(E/K)$, niin

$$\sigma\tau(\theta) = \sigma(\zeta_\tau \theta) = \zeta_\tau \sigma(\theta) = \zeta_\tau \zeta_\sigma(\theta),$$

koska $\zeta_\tau \in K$ ja $\sigma$ on $K$-lineaarinen. Siis saadaan

$$\zeta_{\sigma\tau} = \zeta_\sigma \zeta_\tau,$$

eli kuvaus on homomorfismi. Lisäksi se on injektiivinen, koska ehdosta $\zeta_\sigma = 1$ seuraa $\sigma(\theta) = \theta$, ja siten $\sigma$ on koko laajennuksen $E = K(\theta)$ identtinen automorfismi.

Koska Galois'n ryhmä $\mathrm{Gal}(E/K)$ on isomorfinen syklisen ryhmän $\mu_n(K)$ jonkin aliryhmän kanssa, se on myös syklinen ryhmä.

iii) Laajennuksen aste $[E : K] = d$ on sama kuin sen Galois'n ryhmän kertaluku. Koska tämä on isomorfinen ryhmän $\mu_n(K)$ aliryhmän kanssa, sen kertaluku on luvun $(\mu_n(K) : 1) = n$ tekijä. □

*Huomautus.* Jos $(\mathrm{Gal}(E/K) : 1) = d$, niin kaikilla $\sigma \in \mathrm{Gal}(E/K)$ pätee

$$\zeta_\sigma^d = \zeta_{\sigma^d} = 1,$$

koska $\sigma^d$ on $E$:n identtinen kuvaus, ja siten

$$\sigma(\theta^d) = \sigma(\theta)^d = (\zeta_\sigma \theta)^d = \theta^d.$$

Alkio $\theta^d$ kuuluu siis tällöin Galois'n ryhmän kiintokuntaan $K$.

Kääntäen, jos $\theta^d \in K$, niin $\zeta_\sigma \in \mu_d(K)$ kaikilla $\sigma \in \mathrm{Gal}(E/K)$, ja siksi $(\mathrm{Gal}(E/K) : 1) \leq d$. Aste $[E : K]$ on siis *pienin luvun $n$ tekijä $d$, jolla $\theta^d$ kuuluu kuntaan $K$.*

Seuraava lause on oleellisesti edellisen käänteislause. Sillä on ollut keskeinen merkitys perinteisessä yhtälöiden algebrallisen ratkaisemisen teoriassa.

LAUSE 4.7.12. *Jos $K$ sisältää $n$:nnet ykkösenjuuret ja $E$ on $K$:n asteen $n$ syklinen laajennus, niin $E = K(\theta)$, missä $\theta$ on jonkin jaottoman binomin $X^n - a \in K[X]$ juuri.*

*Todistus.* Olkoon $\sigma$ jokin syklisen ryhmän $\mathrm{Gal}(E/K)$ virittäjä. Ryhmän eri alkiot ovat siis tällöin $\sigma^k$ $(0 \leq k \leq n-1)$.

Olkoon $\zeta \in \mu_n(K)$ jokin primitiivinen $n$:s ykkösenjuuri ja muodostetaan $E$:n automorfismien $\sigma^k$ lineaarinen yhdistelmä

$$u = \sum_{k=0}^{n-1} \zeta^k \sigma^k \in \mathrm{Hom}_K(E, E).$$

Koska homomorfismit ovat lineaarisesti riippumattomat (lause 4.5.4), $u$ ei ole 0-homomorfismi. On siis olemassa sellainen $t \in E$, että

$$\theta = u(t) = \sum_{k=0}^{n-1} \zeta^k \sigma^k(t) \neq 0.$$

Tällainen alkio $\theta$ on ns. *Lagrangen resolventti*, ja se toteuttaa ehdon

$$\begin{aligned} \sigma(\theta) &= \sigma(t + \zeta\sigma(t) + \cdots + \zeta^{n-1}\sigma^{n-1}(t)) \\ &= \sigma(t) + \zeta\sigma^2(t) + \cdots + \zeta^{-1}t \\ &= \zeta^{-1}\theta, \end{aligned}$$

koska $\zeta^n = 1$ ja $\sigma^n(t) = t$. Alkiolla $\theta$ on silloin $n$ eri konjugaattia

$$\sigma^k(\theta) = \zeta^{-k}\theta \qquad (0 \leq k \leq n-1)$$

kunnan $K$ suhteen. Sen aste on siis sama kuin $[E : K] = n$, joten se virittää koko laajennuksen:

$$E = K(\theta).$$

Lisäksi $\theta^n = a$ kuuluu ryhmän $\mathrm{Gal}(E : K)$ kiintokuntaan $K$, koska kaikilla ryhmän alkioilla $\sigma^k$

$$\sigma^k(\theta^n) = \sigma^k(\theta)^n = (\zeta^{-k}\theta)^n = \theta^n.$$

Tällöin $\theta$ on binomin $X^n - a \in K[X]$ juuri, ja tämä on jaoton, koska $\theta$:n aste $K$:n suhteen on $n$. □

*Esimerkki* 7) Olkoon $K$ kunta, jonka karakteristika ei ole 2, ja olkoon

$$f = X^2 + aX + b \in K[X]$$

jaoton polynomi. Polynomi $f$ on separoituva, koska sen derivaatta $f' = 2X + a$ ei ole 0 (lause 4.5.3, iii). Sen juurikunta $E$ kunnan $K$ suhteen on tällöin $K$:n Galois'n laajennus (esim. 4.6.2), jonka Galois'n ryhmä on 2-alkioinen syklinen ryhmä

$$\mathrm{Gal}(E/K) = \{1_E, \sigma\}.$$

Polynomin $f$ juuret $E$:ssä ovat $x$, $x' = \sigma(x)$, ja

$$f = (X - x)(X - x'),$$

eli $a = -x - x'$ ja $b = xx'$. Koska $\mu_2(K) = \{1, -1\}$, eräs Lagrangen resolventti on

$$\theta = x + (-1)\sigma(x) = x - x'.$$

($\theta \neq 0$, koska $x \neq x'$). Sen neliö on kunnan $K$ alkio

$$\theta^2 = x^2 - 2xx' + x'^2 = (x + x')^2 - 4xx' = a^2 - 4b,$$

jota sanotaan polynomin $f$ *diskriminantiksi*, ja $E = K(\theta)$, koska kumpikin $f$:n juuri on $\theta$:n virittämässä laajennuksessa:

$$x = (-a + \theta)/2, \quad x' = (-a - \theta)/2.$$

**Yhtälöiden algebrallinen ratkeavuus.** Olkoon $K$ kunta.

MÄÄRITELMÄ 4.7.13. Kunnan $K$ laajennus $E$ on $K$:n *juurroslaajennus*, jos $E = K(x)$, missä $x^n = a$ jollakin $a \in K$, ja tällöin $x$ on alkion $a$ $n$:s juuri l. *juurros*.

Laajennus $E$ on $K$:n *iteroitu juurroslaajennus*, jos on olemassa jono $(K_i)_{0 \leq i \leq m}$, missä $K_0 = K$, $K_m = E$ ja $K_i$ on $K_{i-1}$:n juurroslaajennus, kun $1 \leq i \leq m$.

Iteroitu juurroslaajennus on siis laajennus, joka voidaan esittää muodossa

$$E = K(x_1, x_2, \ldots, x_m),$$

missä jokainen virittäjä $x_i$ $(1 \leq i \leq m)$ toteuttaa ehdon

$$x_i^{n_i} \in K(x_1, \ldots, x_{i-1})$$

jollakin kokonaisluvulla $n_i > 0$, eli $x_i = \sqrt[n_i]{a_i}$, missä $a_i$ on esitettävissä sitä edeltävien juurrosten $x_1, \ldots, x_{i-1}$ avulla.

*Esimerkki* 8) Olkoon $K = \mathbf{Q}$, $x_1 = \sqrt{2}$ ja $x_2 = \sqrt{1+\sqrt{2}}$. Tällöin $E = \mathbf{Q}(x_1, x_2) = \mathbf{Q}(x_2)$ on $\mathbf{Q}$:n iteroitu juurroslaajennus.

MÄÄRITELMÄ 4.7.14. Yhtälö $f(x) = 0$, missä $f \in K[X]$, $f \neq 0$, on *juurroksilla ratkeava* l. *algebrallisesti ratkeava*, jos $f$:n juurikunta sisältyy johonkin $K$:n iteroituun juurroslaajennukseen.

Ehto voidaan ilmaista myös sanomalla, että yhtälön juuret voidaan esittää peräkkäisten juurilausekkeiden avulla.

Oletetaan jatkossa, että *kunnan $K$ karakteristika on* 0. Tämä tarvitaan, jotta tarkasteltavat laajennukset olisivat separoituvia ja Galois'n teoria olisi käytettävissä. (Vaihtoehtoisesti voitaisiin olettaa, että $\mathrm{char}(K)$ on suurempi kuin tutkittavien polynomien asteet.)

LEMMA 4.7.15. *Jokaisen binomin $f = X^n - a \in K[X]$ Galois'n ryhmä on ratkeava.*

*Todistus.* Jos $a = 0$, binomin $f$ juurikunta on $K$, ja sen Galois'n ryhmä on triviaali. Voidaan siis olettaa, että $a \neq 0$. Tällöin $f$ ja $f'$ ovat keskenään jaottomat $K[X]$:ssä, koska

$$n^{-1} X f' - f = a.$$

Binomi $f$ on silloin separoituva (lause 4.5.1) ja sen juurikunta $N$ on $K$:n Galois'n laajennus (esim. 4.6.2).

Olkoot $x_1, \ldots, x_n \in N$ binomin $n$ eri juurta. Osamäärät

$$x_i/x_1 = \zeta_i \qquad (1 \leq i \leq n)$$

ovat tällöin $n$:nsiä ykkösenjuuria, koska $(x_i/x_1)^n = a/a = 1$. Koska niiden lukumäärä on $n$, niiden virittämä $N$:n alilaajennus

$$E = K(\mu_n(N)) \subset N$$

on $K$:n $n$:s ykkösenjuurikunta. Tällöin

$$N = K(x_1, \ldots, x_n) = E(x_1, \zeta_2 x_1, \ldots, \zeta_n x_1) = E(x_1)$$

on kunnan $E$ syklinen laajennus (lause 4.7.11).

Ykkösenjuurikunta $E$ puolestaan on $K$:n Abelin laajennus (lause 4.7.7). Sitä vastaava Galois'n ryhmän $G = \mathrm{Gal}(N/K)$ aliryhmä $H = \mathrm{Gal}(N/E)$ on siis normaali, ja tekijäryhmä $G/H$ on isomorfinen Galois'n ryhmän $\mathrm{Gal}(E/K)$ kanssa (kor. 4.6.10).

Koska $E$ on $K$:n Abelin laajennus, $G/H$ on vaihdannainen ja siten ratkeava ryhmä. Koska syklinen ryhmä $H$ on myös ratkeava, ryhmä $G$ on ratkeava (lause 1.5.7, ii). □

*Huomautus.* Galois'n ryhmän $\mathrm{Gal}(N/K)$ ei tarvitse olla vaihdannainen, vaikka sillä on normaali aliryhmä, joka on vaihdannainen samoin kuin vastaava tekijäryhmä. Esimerkiksi ryhmässä $\mathfrak{S}_3$ on syklinen aliryhmä $\mathfrak{A}_3$, ja tekijäryhmä $\mathfrak{S}_3/\mathfrak{A}_3 \cong \mathbf{Z}/2\mathbf{Z}$ on samoin syklinen.

KOROLLAARI 4.7.16. *Jos $a_i \in K$ ja $n_i > 0$ $(1 \leq i \leq m)$, niin polynomin $f = \prod_{i=1}^{m}(X^{n_i} - a_i)$ Galois'n ryhmä on ratkeava.*

*Todistus.* Jos $m = 0$, väite on triviaalisti tosi. Olkoon $m > 0$, ja oletetaan, että polynomin $f' = \prod_{i=1}^{m-1}(X^{n_i} - a_i)$ Galois'n ryhmä on ratkeava.

Olkoon $N$ polynomin $f$ juurikunta $K$:n suhteen ja $N' \subset N$ polynomin $f'$ juurien virittämä alilaajennus. Silloin $N$ on binomin $X^{n_m} - a_m$ juurikunta kunnan $N'$ suhteen, joten Galois'n ryhmä $\mathrm{Gal}(N/N')$ on ratkeava (lemma 4.7.15). Se on myös ryhmän $\mathrm{Gal}(N/K)$ normaali aliryhmä, koska $f'$:n juurikunta $N'$ on normaali $K$:n suhteen, ja tekijäryhmä

$$\mathrm{Gal}(N/K)/\mathrm{Gal}(N/N')$$

on isomorfinen ryhmän $\mathrm{Gal}(N'/K)$ kanssa (kor. 4.6.10).

Koska $\mathrm{Gal}(N'/K)$ on oletettu ratkeavaksi ja $\mathrm{Gal}(N/N')$ on ratkeava, $\mathrm{Gal}(N/K)$ on ratkeava (lause 1.5.7, ii). □

Seuraava lause esittää Galois'n yhtälöjen ratkeavuutta koskevan teorian päätuloksen.

LAUSE 4.7.17 (Galois). *Olkoon $f \in K[X]$, $f \neq 0$ ja $\mathrm{char}(K) = 0$ (tai $\mathrm{char}(K) > \deg(f)$). Silloin yhtälö $f(x) = 0$ on algebrallisesti ratkeava, jos ja vain jos polynomin $f$ Galois'n ryhmä on ratkeava.*

*Todistus.* Olkoon $N$ polynomin $f$ juurikunta $K$:n suhteen. Oletetaan aluksi, että yhtälö $f(x) = 0$ on algebrallisesti ratkeava, ja että $E$ on jokin $N$:n sisältävä $K$:n iteroitu juurroslaajennus.

Tällöin on olemassa jono $(K_i)_{0 \leq i \leq m}$, missä $K_0 = K$, $K_m = E$ ja kaikilla $i \in [1, m]$ on voimassa

$$K_i = K_{i-1}(x_i),$$

missä $x_i^{n_i} = a_i \in K_{i-1}$ jollakin $n_i > 0$. Olkoon $L_i$ laajennuksen $K_i$ virittämä $K$:n normaali laajennus $(1 \leq i \leq m)$. Se on separoituva ja siten $K$:n Galois'n laajennus.

Osoitetaan induktiolla $m$:n suhteen, että laajennuksen $L = L_m$ Galois'n ryhmä on ratkeava. Olkoon $L' = L_{m-1}$ ja $\mathrm{Gal}(L'/K)$ ratkeava.

Laajennuksen $K_m = K(x_1, \ldots, x_m)$ virittämä normaali laajennus $L$ on alkioiden $x_i$ $(1 \leq i \leq m)$ konjugaattien virittämä $K$:n laajennus (lause 4.4.9). Olkoon

$$B = \{y_1, \ldots, y_n\} \subset L$$

alkion $x_m$ konjugaattien joukko $K$:n suhteen. Koska $L'$ sisältää alkioiden $x_1, \ldots, x_{m-1}$ konjugaatit, saadaan siten

$$L = K(L' \cup B) = L'(y_1, \ldots, y_n).$$

Lisäksi jokainen $y_j^{n_m}$ on alkion $x_m^{n_m} = a_m \in K_{m-1}$ konjugaatti $K$:n suhteen, joten $y_j^{n_m} = b_j \in L'$. Tämä merkitsee, että $L$ on polynomin

$$\prod_{j=1}^{n}(X^{n_j} - b_j) \in L'[X]$$

juurikunta $L'$:n suhteen, ja siten Galois'n ryhmä $\mathrm{Gal}(L/L')$ on ratkeava (kor. 4.7.16).

Koska ryhmän $\mathrm{Gal}(L'/K)$ kanssa isomorfinen tekijäryhmä

$$\mathrm{Gal}(L/K)/\mathrm{Gal}(L/L')$$

on induktio-oletuksen mukaan ratkeava, on myös $\mathrm{Gal}(L/K)$ ratkeava (lause 1.5.7, ii), ja samoin on ratkeava sen tekijäryhmän

$$\mathrm{Gal}(L/K)/\mathrm{Gal}(L/N)$$

kanssa isomorfinen Galois'n ryhmä $\mathrm{Gal}(N/K)$ (lause 1.5.7, i).

Oletetaan kääntäen, että $\mathrm{Gal}(N/K)$ on ratkeava. On osoitettava, että yhtälö $f(x) = 0$ on algebrallisesti ratkeava. Olkoon

$$n = [N : K] = (\mathrm{Gal}(N/K) : 1)$$

ja $R$ kunnan $K$ $n$:s ykkösenjuurikunta. Koska $N$ sisältää alkioittensa konjugaatit, sen virittämä $R$:n laajennus $E = R(N)$ on normaali ja siten Galois'n laajennus.

Jokainen $R$-automorfismi $\sigma\colon E \to E$ on myös $K$-automorfismi ja vie siksi $K$:n normaalin laajennuksen $N$ itselleen. Rajoittumahomomorfismi

$$\mathrm{Gal}(E/R) \to \mathrm{Gal}(N/K), \quad \sigma \mapsto \sigma|N,$$

on tällöin injektiivinen, koska $N$ virittää $E$:n. Siten myös $\mathrm{Gal}(E/R)$ on ratkeava (lause 1.5.7, i), ja sen kertaluku on $n$:n tekijä.

Ryhmällä $G = \mathrm{Gal}(E/R)$ on siis kompositiojono $(G_i)_{0\le i\le m}$, missä jokainen tekijä $G_i/G_{i+1}$ $(0 \le i \le m-1)$ on syklinen ja sen kertaluku $d_i$ jakaa luvun $n$.

Aliryhmiä $G_i$ vastaavat $E$:n alilaajennukset $E_i = E^{G_i}$ muodostavat jonon peräkkäisiä laajennuksia

$$R = E_0 \subset E_1 \subset \cdots \subset E_m = E.$$

Tällöin $\mathrm{Gal}(E/E_i) = G_i$ kaikilla $i \in [0, m]$, ja koska $G_{i+1}$ on $G_i$:n normaali aliryhmä, kun $0 \le i \le m-1$, $E_{i+1}$ on $E_i$:n Galois'n laajennus ja $\mathrm{Gal}(E_{i+1}/E_i)$ on isomorfinen tekijäryhmän $G_i/G_{i+1}$ kanssa ja siten $d_i$-alkioinen syklinen ryhmä.

Koska $d_i$ on $n$:n tekijä, $R$ sisältää $d_i$:nnet ykkösenjuuret, joten $E_{i+1}$ on $E_i$:n juurroslaajennus (lause 4.7.12). Lisäksi $R$ on $K$:n juurroslaajennus virittäjänään jokin primitiivinen $n$:s ykkösenjuuri. Tästä seuraa, että $E$ on $K$:n iteroitu juurroslaajennus, ja koska se sisältää juurikunnan $N$, yhtälö $f(x) = 0$ on algebrallisesti ratkeava. □

*Esimerkki* 9) Jos polynomin $f$ aste on $n$, niin sen Galois'n ryhmä $\Gamma$ voidaan tulkita symmetrisen ryhmän $\mathfrak{S}_n$ aliryhmäksi (ks. esim. 4.6.3), ja koko ryhmäksi, kun $f$ on yleinen asteen $n$ polynomi.

Toisaalta $\mathfrak{S}_n$ on ratkeava, kun $n \leq 4$ (esim. 1.5.8). Yhtälö $f(x) = 0$ on siten algebrallisesti ratkeava, kun $n \leq 4$. Tämä on klassinen tulos. Ratkaisukaavat tapauksessa $n = 3$ esitti *Cardano* ja tapauksessa $n = 4$ hänen oppilaansa *Ferrari*. Cardano julkaisi ratkaisut 1545.

Kun $n \geq 5$, ryhmä $\mathfrak{S}_n$ ei ole ratkeava (esim. 1.5.9). Yleinen yhtälö $f(x) = 0$ ei siis ole algebrallisesti ratkeava, kun sen aste on $n \geq 5$. Tämän todisti tapauksessa $n = 5$ *Abel* 1824. Välttämättömän ja riittävän ehdon esitti *Galois* 1832, mutta se julkaistiin vasta 1846.

KOROLLAARI 4.7.18 (Abel). *Jos* $\mathrm{char}(K) = 0$ *ja polynomin* $f \in K[X]$, $f \neq 0$, *Galois'n ryhmä on vaihdannainen, niin yhtälö* $f(x) = 0$ *on algebrallisesti ratkeava* (*ns.* Abelin yhtälö).

*Todistus.* Vaihdannainen ryhmä on ratkeava. □

**Harjoitustehtäviä**

Olkoon $K$ kunta, jonka karakteristika ei ole 2 eikä 3, ja $f = X^3 + pX + q \in K[X]$.

1) Osoitettava:

i) $f$ on separoituva, jos ja vain jos $4p^3 + 27q^2 \neq 0$. (Lasketaan $\mathrm{syt}(f, f')$.)

ii) Jos $f$ ei ole separoituva, niin $K$ on $f$:n juurikunta. ($f$:llä ja $f'$:lla on yhteinen juuri $K$:ssa.)

Olkoon lisäksi $N$ $f$:n juurikunta $K$:n suhteen, $f = (X - x_1)(X - x_2)(X - x_3) \in N[X]$, $p_k = \sum_i x_i^k \in N$ $(k \in \mathbf{N})$ ja $\Delta = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3) \in N$ $f$:n *differentti*.

2) Osoitettava:

i) $p_k + p\,p_{k-2} + q\,p_{k-3} = 0$ kun $k \geq 3$ (*Newtonin kaavat*).

ii) $p_0 = 3$, $p_1 = 0$, $p_2 = -2p$, $p_3 = -3q$ ja $p_4 = 2p^2$.

iii) $\Delta = -\det(A)$, missä $A = (x_i^j)_{1 \leq i \leq 3, 0 \leq j \leq 2}$.

iv) $\Delta^2 = \det(p_{i+j})_{0 \leq i,j \leq 2}$. (Lasketaan $A^{\mathsf{T}}A$.)

v) $f$:n *diskriminantti* $D = \Delta^2$ on $-4p^3 - 27q^2 \in K$.

Olkoon lisäksi $f$ separoituva, $\Gamma \subset \mathfrak{S}_3$ sen Galois'n ryhmä ja $E = K(\Delta) \subset N$.

3) Osoitettava:

i) Jos $\sigma \in \mathrm{Gal}(N/K)$, niin $\sigma(\Delta) = \varepsilon(\sigma)\Delta$, missä $\varepsilon(\sigma) = \pm 1$ on vastaavan juurten permutaation merkki.

ii) $\mathrm{Gal}(N/E) \xrightarrow{\sim} \Gamma \cap \mathfrak{A}_3$, ja siten $N = E$ tai $[N : E] = 3$.

iii) $f$ on jaoton, jos ja vain jos $\Gamma = \mathfrak{S}_3$ tai $\Gamma = \mathfrak{A}_3$.

Pääteltävä, että $\Gamma = \mathfrak{S}_3$, jos ja vain jos $f$ on jaoton ja $D$ ei ole neliö $K$:ssa.

Olkoon lisäksi $R = K(\zeta)$, missä $\zeta \neq 1$ on 3:s ykkösenjuuri, sekä $\theta_1 = (x_1 + \zeta x_2 + \zeta^2 x_3)/3 \in R(N)$ ja $\theta_2 = (x_1 + \zeta^2 x_2 + \zeta x_3)/3 \in R(N)$ (kaksi Lagrangen resolventtia).

4) Osoitettava:

i) $R = K(\sqrt{-3})$, missä $\sqrt{-3} \in R$ on binomin $X^2 + 3$ juuri. ($\zeta^2 + \zeta + 1 = 0$.)

ii) $x_1 = \theta_1 + \theta_2$, $x_2 = \zeta^2\theta_1 + \zeta\theta_2$ ja $x_3 = \zeta\theta_1 + \zeta^2\theta_2$ (*Cardanon kaavat*).

iii) $\theta_1\theta_2 = -p/3$ ja $\theta_1^3 + \theta_2^3 = (\theta_1 + \theta_2)(\theta_1 + \zeta\theta_2)(\theta_1 + \zeta^2\theta_2) = -q$.

Pääteltävä, että $\theta_1^3$ ja $\theta_2^3$ ovat polynomin $Y^2 + qY - (p/3)^3$ juuret

$$-\frac{q}{2} \pm \frac{\sqrt{-3}\sqrt{D}}{18} \in K(\sqrt{-3}, \sqrt{D})$$

ja että $R(N) = R(\theta_1, \theta_2)$ on $K$:n iteroitu juurroslaajennus.