IV Kohti Galois'n teoriaa

1. Hiukan lineaarialgebraa

1.1. Määritelmä. Olkoon $\boldsymbol{K} = (K, +, \cdot)$ kunta (ns. *kerroinkunta*). Joukko V varustettuna yhteenlaskulla $+: V \times V \to V$ ja skalaarikerronnalla $\cdot: K \times V \to V$ on $\boldsymbol{K}$-vektoriavaruus, jos

1) $(V, +)$ on Abelin ryhmä,
2 kaikilla $a, b \in K$ ja $v \in V$ pätee

$$a(bv) = (ab)v$$

ja

3) kaikilla $a, b \in K$, $v, w \in V$

$$(a + b)v = av + bv \text{ ja}$$
$$a(v + w) = av + aw.$$

Useat reaalisten ja kompleksisten vektoriavaruuksien tulokset yleistyvät miltei sanasta sanaan muuttumattomina.

1.2. Määritelmä. Olkoon V $\boldsymbol{K}$-vektoriavaruus ja $S \subseteq V$. S on *vapaa*, jos kaikille eri vektoreille $v_0, \ldots, v_{n-1} \in S$ ($n \in \mathbb{N}$) ja mielivaltaisille $a_0, \ldots, a_{n-1} \in K$ pätee: Jos $\sum_{i=0}^{n-1} a_i v_i = 0$, niin $a_0 = \cdots = a_{n-1} = 0$. S on V:n virittäjäjoukko, jos jokainen $v \in V$ voidaan esittää muodossa $v = \sum_{i=0}^{n-1} a_i v_i$ joillakin $a_i \in K$, $v_i \in S$, $i \in \{0, \ldots, n-1\}$. S on V:n *kanta*, jos se on vapaa virittäjäjoukko.

1.3. Lause. *Jokaisella vektoriavaruudella on kanta. Itse asiassa jokainen minimaalinen virittäjäjoukko tai maksimaalinen vapaa joukko on kanta. Kannat ovat keskenään yhtämahtavia, ts. jos* B *ja* B' *ovat molemmat* $\boldsymbol{K}$*-vektoriavaruuden* V *kantoja, niin on olemassa bijektio* $f: B \to B'$. □

1.4. Määritelmä. $\boldsymbol{K}$-vektoriavaruuden V *dimensio* on $\dim(V) = |B|$, missä B on mikä tahansa V:n kanta.

1.5. Lause. *Olkoon* $\boldsymbol{L} = (L, +, \cdot)$ *kunnan* $\boldsymbol{K} = (K, +, \cdot)$ *kuntalaajennus. Tällöin* L *voidaan tulkita* $\boldsymbol{K}$*-vektoriavaruudeksi käyttämällä yhteenlaskuna kunnan* $\boldsymbol{L}$ *yhteenlaskua ja skalaarikerrontana kertolaskun rajoittumaa* $\cdot\restriction(K \times L)$.

Todistus. Tulos on ilmeinen pienen teknisen tarkastuksen jälkeen: Kunta-aksioomien mukaan $(L, +)$ on Abelin ryhmä. Kertolaskun liitäntälaista ja kunnan osittelulaista seuraavat muut vektoriavaruuden aksioomat. □

Tästä seuraa uusi todistus seuraavalle:

1.6. Lause. *Äärellisen kunnan koko on (ykkösestä eroava) alkulukupotenssi.*

Todistus. Olkoon $\boldsymbol{K} = (K, +, \cdot)$ äärellinen kunta. Tarkastellaan kuvausta

$$f\colon \mathbb{Z} \to K,\ f(n) = n \cdot 1.$$

Monikertojen laskusääntöjen mukaan tämä on homomorfismi: Kun $m, n \in \mathbb{Z}$, niin

$$f(m + n) = (m + n) \cdot 1 = m \cdot 1 + n \cdot 1 = f(m) + f(n) \text{ ja}$$
$$f(m \cdot n) = (m \cdot n) \cdot 1 = (m \cdot 1) \cdot (n \cdot 1) = f(m)f(n).$$

Koska $\mathbb{Z}$ on ääretön ja K äärellinen, f ei voi olla injektio, vaan on olemassa

$$p = \min\{\, n \in \operatorname{Ker} f \mid n > 0 \,\} = \min\{\, n \in \mathbb{Z}_+ \mid n \cdot 1 = 0 \,\}$$

ja $\operatorname{Ker} f = p\mathbb{Z}$. Toisaalta p on selvästi $\boldsymbol{K}$:n karakteristika, joten p on alkuluku. Siis ideaali $p\mathbb{Z}$ on maksimaalinen ideaali ja $(\operatorname{Im} f, +, \cdot) \cong (\mathbb{Z}/p\mathbb{Z}, +, \cdot) = \mathbb{Z}_p$. $\boldsymbol{K}$:lla on siis $\mathbb{Z}_p$:n kanssa isomorfinen alikunta, joten K voidaan tulkita $\mathbb{Z}_p$-vektoriavaruudeksi. Koska K on äärellinen, niin $k = \dim K \in \mathbb{Z}_+$ ja $|K| = p^k$. □

2. Algebralliset ja transkendenttiset alkiot

2.1. Määritelmä. Olkoon $\boldsymbol{L}$ kunnan $\boldsymbol{K} = (K, +, \cdot)$ kuntalaajennus. Alkion $a \in L$ sanotaan olevan *algebrallinen alikunnan $\boldsymbol{K}$ suhteen* eli *$\boldsymbol{K}$-algebrallinen*, jos se toteuttaa $\boldsymbol{K}$-kertoimisen polynomiyhtälön, ts. jollakin $p \in K[x] \setminus \{0\}$ pätee $p(a) = 0$. Alkio a on *transkendenttinen $\boldsymbol{K}$*:n suhteen (eli *$\boldsymbol{K}$-transkendenttinen*), jos se ei ole $\boldsymbol{K}$-algebrallinen.

Algebrallisella luvulla tarkoitetaan $\mathbb{Q}$-algebrallista kompleksilukua. Vastaavasti *transkendenttisella luvulla* tarkoitetaan $\mathbb{Q}$-transkendenttista kompleksilukua.

2.2. Esimerkki. i ja $\sqrt{2}$ ovat algebrallisia, sillä $i^2 + 1 = 0$ ja $\sqrt{2}^2 - 2 = 0$. Lukujen π ja e tiedetään olevan transkendenttisia. $\sqrt{\pi}$ on $\mathbb{Q}(\pi)$ algebrallinen, sillä $\sqrt{\pi}^2 - \pi = 0$.

2.3. Määritelmä. Olkoon $\boldsymbol{L} = (L, +, \cdot)$ kunnan $\boldsymbol{K}$ kuntalaajennus, jolloin L on luonnollisella tavalla $\boldsymbol{K}$-vektoriavaruus. Tämän vektoriavaruuden dimensiota kutsutaan vastaavan kuntalaajennuksen ($\boldsymbol{K}$:sta $\boldsymbol{L}$:ään) *asteeksi* ja merkitään $[\boldsymbol{L} : \boldsymbol{K}]$:lla. Siis $[\boldsymbol{L} : \boldsymbol{K}] = \dim L$. Tämä kuntalaajennus on *äärellisasteinen*, jos $[\boldsymbol{L} : \boldsymbol{K}] \in \mathbb{Z}_+$, muuten *ääretönasteinen*.

2.4. Lause. *Olkoon $\boldsymbol{L}$ kunnan $\boldsymbol{K}$ äärellisasteinen kuntalaajennus. Tällöin jokainen $t \in L$ on $\boldsymbol{K}$-algebrallinen.*

Todistus. Koska $[L : K]$, niin jono $(t^i \mid i \in \mathbb{N})$ ei voi olla vapaa, kun $t \in L$. Siis on olemassa $n \in \mathbb{N}$ ja kertoimet $a_0, \ldots, a_n \in K$, joille $\sum_{i=0}^{n} a_i t^i = 0$, vaikka $a_n \neq 0$. Siis $p = \sum_{i=0}^{n} a_i x^i \in K[x]$ on polynomi, jolle $p(t) = 0$, joten t on K-algebrallinen. □

2.5. Lause. *Olkoon $\boldsymbol{L}$ kunnan $\boldsymbol{K} = (K, +, \cdot)$ kuntalaajennus ja $t \in L$ $\boldsymbol{K}$-algebrallinen alkio. Tällöin on olemassa yksikäsitteinen jaoton pääpolynomi $p \in K[x]$, jolle $p(t) = 0$. Tällöin $\boldsymbol{K}[t] = \boldsymbol{K}(t) \cong \boldsymbol{K}[x]/\langle p\rangle$. Tämä isomorfismi voidaan valita niin, että kaikilla $a \in K$ pätee $a \mapsto a + \langle p\rangle$ ja $t \mapsto x + \langle p\rangle$.*

Todistus. Lähdetään liikkeelle sijoitushomomorfismista $e_t\colon L[x] \to L$. Tämän rajoittuma $h = e_t{\restriction}K[x]$ on selvästi epimorfismi (eli surjektiivinen homomorfismi) renkaasta $\boldsymbol{K}[x]$ renkaaseen $\boldsymbol{K}[t]$. Homomorfismin h ydin $\operatorname{Ker} h$ koostuu niistä polynomeista $p \in K[x]$, joille $h(p) = p(t) = 0$. Koska t on $\boldsymbol{K}$-algebrallinen, niin $\operatorname{Ker} h \neq \{0\}$. Koska $\boldsymbol{K}[x]$ on pääideaalialue, on olemassa $p \in K[x] \setminus \{0\}$, jolle $\operatorname{Ker} h = \langle p\rangle$. Koska $\langle p\rangle = \langle c^{-1}p\rangle$, missä c on polynomin p korkeimman asteen termin kerroin, niin polynomin voidaan olettaa olevan pääpolynomi.

p on jaoton, sillä jos olisi $p = qr$, missä $q, r \in K[x]$, $\deg(q) < \deg(p)$ ja $\deg(r) < \deg(p)$, niin yhtälöstä $0 = p(t) = q(t)r(t)$ seuraisi $q(t) = 0$ tai $r(t) = 0$ eli $q \in \langle p\rangle$ tai $r \in \langle p\rangle$, mistä seuraisi ristiriita $\deg(q) \geqslant \deg(p)$ tai $\deg(r) \geqslant \deg(p)$. Polynomin p yksikäsitteisyys seuraa siitä, että jos $\langle p\rangle = \langle p^*\rangle$, niin p ja p^* olisivat liittopolynomeja, jolloin niiden pitäisi olla pääpolynomeina olla sama polynomi.

Renkaiden isomorfialauseen mukaan

$$\boldsymbol{K}[t] = (\operatorname{Im} h, +, \cdot) \cong \boldsymbol{K}[x]/\operatorname{Ker} h = \boldsymbol{K}[x]/\langle p\rangle.$$

Koska p on jaoton, ideaali $\langle p\rangle$ on maksimaalinen, joten $\boldsymbol{K}[t] \cong \boldsymbol{K}[x]/\langle p\rangle$ on kunta. Toisaalta $\boldsymbol{K}[t]$ on pienin $\boldsymbol{L}$:n alikunta, joka sisältää joukon $K \cup \{t\}$. Siis $\boldsymbol{K}[t] = \boldsymbol{K}(t)$. □

2.6. Seuraus. *Olkoot $\boldsymbol{L}$, $\boldsymbol{K}$ ja t kuten edellä sekä $u \in L$. Jos u on myös $\boldsymbol{K}$-algebrallinen alkio ja saman jaottoman pääpolynomin juuri kuin t, niin on olemassa $f\colon \boldsymbol{K}(t) \cong \boldsymbol{K}(u)$, jolle $f{\restriction}K = \mathrm{id}_K$ ja $f(t) = f(u)$.*

Todistus. Valitaan jaoton pääpolynomi p, jolle $p(t) = p(u) = 0$. Tällöin p on yksikäsitteinen, joten lauseen mukaan $\boldsymbol{K}(t) = \boldsymbol{K}[t] \cong \boldsymbol{K}[x]/\langle p\rangle \cong \boldsymbol{K}[u] = \boldsymbol{K}(u)$, missä lauseen mukaisille isomorfismeille pätee kaikilla $a \in K$ $a \mapsto a + \langle p\rangle \mapsto a$ ja lisäksi $t \mapsto x + \langle p\rangle \mapsto u$. □

2.7. Esimerkki.

a) Polynomi $x^3 - 2$ on jaoton polynomirenkaassa $(\mathbb{Q}[x], +, \cdot)$ Eisensteinin kriteerion nojalla. $\sqrt[3]{2}$ ja $e^{i2\pi/3}\sqrt[3]{2}$ ovat tämän kompleksijuuria. Siis on olemassa isomorfismi

$$\left(\mathbb{Q}\left[\sqrt[3]{2}\right], +, \cdot\right) \cong \left(\mathbb{Q}\left[e^{\frac{i2\pi}{3}}\sqrt[3]{2}\right], +, \cdot\right),$$

joka pitää rationaaliluvut paikoillaan. Huomaa, että $\mathbb{Q}[\sqrt[3]{2}] \neq \mathbb{Q}[e^{\frac{i2\pi}{3}}\sqrt[3]{2}]$, sillä $\mathbb{Q}[\sqrt[3]{2}] \subseteq \mathbb{R}$, mutta $e^{\frac{i2\pi}{3}}\sqrt[3]{2} \notin \mathbb{R}$.

b) Syklotominen polynomi $\Phi_5 = x^4+x^3+x^2+x+1 \in \mathbb{Q}[x]$ on jaoton. Koska $(x-1)\Phi_5 = x^5-1$, niin Φ_5:n juuret ovat ω, ω^2, ω^3, ω^4, missä $\omega = e^{\frac{i2\pi}{5}}$. Selvästi $\mathbb{Q}[\omega] = \mathbb{Q}[\omega^2]$, sillä $((\omega)^2)^3 = \omega$. Edellisen seurauksen mukaan on olemassa isomorfismi

$$f\colon (\mathbb{Q}[\omega], +, \cdot) \cong (\mathbb{Q}[\omega^2], +, \cdot),$$

jolle $f{\restriction}\mathbb{Q} = \mathrm{id}_{\mathbb{Q}}$ ja $f(\omega) = \omega^2$, mutta tämä isomorfismihan on itse asiassa kunnan $(\mathbb{Q}[\omega], +, \cdot)$ automorfismi, koska $\mathbb{Q}[\omega] = \mathbb{Q}[\omega^2]$.

2.8. Lause. *Olkoon $\boldsymbol{L}$ kunnan $\boldsymbol{K} = (K, +, \cdot)$ kuntalaajennus ja $t \in L$ $\boldsymbol{K}$-algebrallinen. Tällöin $[K(t) : K] = \deg p$, missä p on se yksikäsitteinen jaoton pääpolynomi, jolle $p(t) = 0$.*

Todistus. Merkitään $n = \deg p$. Väitetään, että $\{1, t, \ldots, t^{n-1}\}$ on $\boldsymbol{K}$-vektoriavaruuden $K(t) = K[t]$ kanta. Ensinnäkin $\{1, t, \ldots, t^{n-1}\}$ on vapaa, sillä jos $a_0, \ldots, a_{n-1} \in K$ ovat sellaisia, että

$$\sum_{i=0}^{n-1} a_i t^i = 0,$$

niin $q = \sum_{i=0}^{n-1} a_i x^i = 0$ on polynomi, jolle $q(t) = 0$, ts. $q \in \langle p \rangle$ eli $p \mid q$, vaikka $\deg(q) < n$. Siis $q = 0$ ja $a_0 = \cdots = a_{n-1} = 0$. Toisaalta jokaisella $k \in \mathbb{N}$ on jakoyhtälön mukaan olemassa sellaiset $q, r \in K[x]$, että $x^k = qp + r$, missä $\deg(r) < \deg(p) = n$. Siis

$$t^k = q(t) \cdot p(t) + r(t) = q(t) \cdot 0 + r(t) = r(t),$$

ts. t^k on ilmaistavissa summana

$$t^k = \sum_{i=0}^{n-1} r_i t^i.$$

Koska $\{ t^k \mid k \in \mathbb{N} \}$ on $K[t]$:n virittäjäjoukko, tämä osoittaa, että myös $\{1, t, \ldots, t^{n-1}\}$ on. □

2.9. Lause. *Olkoon $\boldsymbol{L} = (L, +, \cdot)$ kunnan $\boldsymbol{K} = (K, +, \cdot)$ kuntalaajennus ja edelleen $\boldsymbol{E} = (E, +, \cdot)$ kunnan $\boldsymbol{L}$ kuntalaajennus. Tällöin*

$$[\boldsymbol{E} : \boldsymbol{K}] = [\boldsymbol{E} : \boldsymbol{L}][\boldsymbol{L} : \boldsymbol{K}].$$

Huomautus. Äärettömässä tapauksessa tämä tarkoittaa ns. kardinaalituloa.

Todistus. Merkitään $m = [\boldsymbol{L} : \boldsymbol{K}]$ ja $n = [\boldsymbol{E} : \boldsymbol{L}]$. Valitaan $\boldsymbol{K}$-vektoriavaruudelle L kanta A, jolloin $|A| = m$, ja $\boldsymbol{L}$-vektoriavaruudelle E kanta B, jolle puolestaan $|B| = n$. Väitetään, että

$$AB = \{ ab \mid a \in A,\ b \in B \}$$

on $\boldsymbol{K}$-vektoriavaruuden E kanta. Osoitetaan ensin, että AB on virittäjäjoukko. Olkoon $t \in E$. Koska B on $\boldsymbol{L}$-vektoriavaruuden E kanta, niin

$$t = \sum_{b \in B} \lambda_b b,$$

missä summa on oleellisesti äärellinen, ts. $\lambda_b \neq 0$ vain äärellisen monella $b \in B$, ja kertoimet λ_b, $b \in B$, ovat L:ssä. Koska A on puolestaan $\boldsymbol{K}$-vektoriavaruuden L virittäjäjoukko, niin jokaista $b \in B$ vastaa esitys

$$\lambda_b = \sum_{a \in A} \mu_{ab} a,$$

missä kertoimet $\mu_{ab} \in K$ ja summat ovat oleellisesti äärellisiä. Siis

$$t = \sum_{b\in B} \lambda_b b = \sum_{b\in B} \left(\sum_{a\in A} \mu_{ab} a \right) b = \sum_{a\in A, b\in B} \mu_{ab}(ab),$$

mikä osoittaa AB:n olevan virittäjäjoukko.

Osoitetaan, että AB on vapaa (ja itse asiassa myös $ab \neq a'b'$, kun $a, a' \in A$, $b, b' \in B$ ja $(a, b) \neq (a', b')$). Olkoot siis $\mu_{ab} \in K$, kun $(a, b) \in A \times B$, ja oletetaan, että näistä kertoimista vain äärellisen moni on nollasta poikkeava. Oletetaan lisäksi, että

$$\sum_{a\in A, b\in B} \mu_{ab} ab = 0.$$

Koska B on vapaa ($\boldsymbol{L}$-vektoriavaruudessa E) ja

$$0 = \sum_{a\in A, b\in B} \mu_{ab} ab = \sum_{b\in B} \underbrace{\left(\sum_{a\in A} \mu_{ab} a \right)}_{\in L} b,$$

niin jokaisella $b \in B$ pätee

$$\sum_{a\in A} \mu_{ab} a = 0.$$

Koska A on vapaa $\boldsymbol{K}$-vektoriavaruudessa L, saadaan tästä edelleen $\mu_{ab} = 0$ jokaisella $a \in A$ ja $b \in B$. Siis AB on vapaa virittäjäjoukko eli kanta ja

$$[\boldsymbol{E} : \boldsymbol{K}] = |AB| = |A||B| = mn = [\boldsymbol{E} : \boldsymbol{L}][\boldsymbol{L} : \boldsymbol{K}]. \quad \square$$

2.10. Lause. *Olkoon $\boldsymbol{E}$ kunnan $\boldsymbol{K} = (K, +, \cdot)$ kuntalaajennus. Merkitään L:llä kunnan $\boldsymbol{E}$ $\boldsymbol{K}$-algebrallisten alkioiden joukkoa. Tällöin L on suljettu laskutoimitusten suhteen ja itse asiassa $\boldsymbol{L} = (L, +, \cdot)$ on $\boldsymbol{K}$:n kuntalaajennus.*

Todistus. Jokainen $a \in K$ on tietysti polynomin $x - a \in K[x]$ juuri, joten tällaiset a ovat $\boldsymbol{K}$-algebrallisia. Siis $K \subseteq L$.

Olkoot $a, b \in L$. Koska a ja b ovat $\boldsymbol{K}$-algebrallisia, on olemassa jaottomat polynomit $p, q \in K[x]$, joille $p(a) = 0$ ja $q(b) = 0$. Edelleen

$$[\boldsymbol{K}(a) : \boldsymbol{K}] = \deg(p)$$

ja

$$[\boldsymbol{K}(b) : \boldsymbol{K}] = \deg(q),$$

joten vastaavat kuntalaajennukset ovat äärellisiä. Koska $q \in K[x] \subseteq K(a)[x]$ ja $q(b) = 0$, niin b on myös $K(a)$-algebrallinen ja

$$[\boldsymbol{K}(a)(b) : K(a)] = [K(a, b) : K(a)] \leqslant [K(b) : K],$$

joten

$$[\boldsymbol{K}(a,b):\boldsymbol{K}] = [\boldsymbol{K}(a,b):\boldsymbol{K}(a)][\boldsymbol{K}(a):\boldsymbol{K}]$$

on äärellinen. Koska $\boldsymbol{K}(a,b)$ on äärellinen $\boldsymbol{K}$:n kuntalaajennus, niin kaikki $K(a,b)$:n alkiot ovat $\boldsymbol{K}$-algebrallisia. Erityisesti tämä pätee alkioihin $a+b$, ab, $-a$ ja a^{-1} (kunhan $a \neq 0$). Summa summarum: L on suljettu laskutoimitusten, vasta-alkioiden ja nollasta eroavien alkioiden käänteisalkioiden suhteen, joten $\boldsymbol{L} = (L,+,\cdot)$ on $\boldsymbol{E}$:n alikunta. Koska $K \subseteq L$, niin $\boldsymbol{L}$ on $\boldsymbol{K}$:n kuntalaajennus. □

2.11. Esimerkki. $\sqrt{2}$, $\sqrt[3]{7}$ ja $\sqrt[5]{11}$ ovat algebrallisia, koska ne ovat kukin jonkin polynomeista x^2-2, x^3-7 ja x^5-11 juuria. Siis myös

$$\frac{\sqrt[5]{11}}{\sqrt{2}-\sqrt[3]{7}}$$

on algebrallinen.

3. Harppi ja viivotin -konstruktiot

Kun $a,b \in \mathbb{C}$, $a \neq b$, merkitään $C(a,b)$:llä a-keskistä ympyrää, joka kulkee b:n kautta, ts.

$$C(a,b) = \{\, z \in \mathbb{C} \mid |z-a| = |b-a| \,\}$$

ja merkitään $L(a,b)$:llä suoraa, joka kulkee pisteiden a ja b kautta, ts.

$$L(a,b) = \{\, \lambda a + (1-\lambda)b \mid \lambda \in \mathbb{R} \,\}.$$

3.1. Määritelmä. Olkoon $U \subseteq \mathbb{C}$. Kun $a,b \in U$, niin $C(a,b)$ ja $L(a,b)$ ovat S:stä *yhdellä askeleella konstruoituvia ympyröitä ja suoria*. Piste $z \in \mathbb{C}$ on joukosta U *yhdellä askeleella konstruoituva*, jos $z \in S \cup T$, missä S ja T ovat eri joukkoja ja U:sta yhdellä askeleella konstruoituvia ympyröitä tai suoria.

Kompleksitason piste $z \in \mathbb{C}$ on *konstruoituva*, jos on olemassa jono

$$(a_0,\ldots,a_n),$$

missä $a_0 = 0$, $a_1 = 1$ ja jokaisella $i \in \{2,\ldots,n\}$ piste a_i on yhdellä askeleella konstruoituva joukosta $\{a_0,\ldots,a_{i-1}\}$.

3.2. Lause. *Harpilla ja viivoittimella konstruoituvien pisteiden joukko muodostaa kompleksilukujen alikunnan.* □

3.3. Lause. *Jos z on harpilla ja viivoittimella konstruoituva, niin $[\mathbb{Q}(z):\mathbb{Q}] = 2^n$ jollakin $n \in \mathbb{N}$.*

Todistus. (hahmotelma) Konstruoituvuudesta seuraa, että on olemassa alkiot $a_0,\ldots,a_n \in \mathbb{C}$, joille $[\mathbb{Q}(a_0,\ldots,a_i):\mathbb{Q}(a_0,\ldots,a_{i-1})] \in \{1,2\}$. □

3.4. Lause. *Kuution kahdentaminen harpilla ja viivottimella on mahdotonta, ts.* $\sqrt[3]{2}$ *ei ole konstruoituva.*

Todistus. (Pelkkä idea) $x^3 - 2 \in \mathbb{Q}[x]$ on jaoton, $\sqrt[3]{2}$ sen juuri, siis $[\mathbb{Q}(\sqrt[3]{2})] = 3 \neq 2^n$, kun $n \in \mathbb{N}$. □

4. Galois'n teoriaa

4.1. Määritelmä. Olkoon $\boldsymbol{K} = (K, +, \cdot)$ ja $a \in K[x]$, missä $\deg(a) > 0$. Kunta $\boldsymbol{L} = (L, +, \cdot)$ on *juurikunta*, jos $\boldsymbol{L}$ on $\boldsymbol{K}$:n kuntalaajennus, jossa a jakaantuu ensimmäisen asteen tekijöihin, ts.

$$a = c \prod_{i=0}^{n} (x - t_i)$$

joillakin $c \in K, t_0, \ldots, t_{n-1} \in L$ ($n = \deg(a)$), ja näillä parametrien arvoilla $L = K(t_0, \ldots, t_{n-1})$.

4.2. Esimerkki. $(\mathbb{Q}(\sqrt{2}), +, \cdot)$ on polynomin $x^2 - 2 \in \mathbb{Q}[x]$ juurikunta.

4.3. Lause. *Jokaisella kuntakertoimisella epävakiolla polynomilla on juurikunta, joka on isomorfiaa vaille yksikäsitteinen.*

Todistus. (hahmotelma) Olkoon $a \in K[x]$, missä $\boldsymbol{K} = (K, +, \cdot)$ on kunta ja $\deg(a) > 0$. Laskuharjoituksissa on todistettu, että on olemassa $(K, +, \cdot)$:n kuntalaajennus $(E, +, \cdot)$, jossa a jakaantuu ensimmäisen asteen tekijöihin. Olkoot $t_0, \ldots, t_{n-1}$ kuten juurikunnan määritelmässä; tällöin $L = K(t_0, \ldots, t_{n-1})$ on halutunlainen. Yksikäsitteisyys osoitetaan oleellisesti induktiolla; induktioaskel käyttää tietoa, että

$$\boldsymbol{K}(t) \cong \boldsymbol{K}(t^*) \cong \boldsymbol{K}/\langle a \rangle,$$

kun a on jaoton ja t, t^* a:n juuria jossakin $\boldsymbol{K}$:n kuntalaajennuksessa. □

4.4. Seuraus. *(Moore) Kun* p *on alkuluku ja* $n \in \mathbb{Z}_+$*, niin on olemassa isomorfiaa vaille yksikäsitteinen kunta, jossa on* p^n *alkiota.*

Todistus. Laskuharjoituksissa on todistettu, että tällainen kunta on aina olemassa. Yksikäsitteisyyden todistamiseksi riittää osoittaa, että tällainen kunta $\boldsymbol{K} = (K, +, \cdot)$ on aina polynomin $x^{p^n} - x \in (\mathbb{Z}/p\mathbb{Z})[x]$ juurikunta.

Olkoon $a \in K$. Jos $a = 0$, niin $a^{p^n} = 0^{p^n} = 0$, joten a on tällöin polynomin $x^{p^n} - x$ juuri. Oletetaan, että $a \neq 0$, jolloin a on kertolaskuryhmän $(K^*, \cdot)$ alkio ($K^* = K \setminus \{0\}$). Alkiolla a on äärellinen kertaluku h, jolle pätee Lagrangen lauseen nojalla $h \mid p^n - 1$. Siis myös $a^{p^n - 1} = 1$, mistä seuraa $a^{p^n} - a = a(a^{p^n - 1} - 1) = a \cdot (1 - 1) = 0$. Siis jokainen $a \in K$ on polynomin $x^{p^n} - x$ juuri. Koska polynomilla $x^{p^n} - x$ on korkeintaan p^n juurta, tämä merkitsee, että polynomi $x^{p^n} - x$ väistämättä jakaantuu ernsimmäisen kertaluvun tekijöihin $\boldsymbol{K}$:ssa, joten $\boldsymbol{K}$ on sen juurikunta. □

4.5. Määritelmä. Kunta $\boldsymbol{L}$ on kunnan $\boldsymbol{K}$ *juurroslaajennus*, jos on olemassa sellaiset kunnat $\boldsymbol{K}_i = (K_i, +, \cdot)$, $i \in \{0, \ldots, n\}$, että jokaiselle $i \in \{0, \ldots, n-1\}$ on olemassa $t_i \in K_i$, jolle pätee

$$K_{i+1} = K_i(t_i)$$

ja jollakin $h_i \in \mathbb{Z}_+$

$$t_i{}^{h_i} = 1$$

sekä

$$\boldsymbol{K}_0 = \boldsymbol{K} \text{ ja } \boldsymbol{K}_n = \boldsymbol{L}.$$

Kuntia $\boldsymbol{K}_i$ kutsutaan *välikunniksi* ja jonoa

$$\boldsymbol{K} = \boldsymbol{K}_0 \leqslant \boldsymbol{K}_1 \leqslant \cdots \leqslant \boldsymbol{K}_n = \boldsymbol{L}$$

laajennustorniksi.

Yleinen ongelma on siis: Kun $a \in K[x]$, $\deg(a) > 0$ on annettu, onko olemassa kunnan $(K, +, \cdot)$ juurroslaajennus, joka sisältää a:n juurikunnan.

4.6. Määritelmä. Olkoon $\boldsymbol{K} = (K, +, \cdot)$ kunta ja $a \in K[x]$, missä $\deg(a) > 0$. Polynomin a sanotaan olevan *juurtamalla* ratkaistavissa, jos on olemassa kunnan $\boldsymbol{K}$ juurroslaajennus $\boldsymbol{L}$, joka sisältää polynomin a juurikunnan.

4.7. Määritelmä. Tarkastellaan kuntalaajennusta kunnasta $\boldsymbol{K} = (K, +, \cdot)$ kuntaan $\boldsymbol{L} = (L, +, \cdot)$. Tämän kuntalaajennuksen *Galois'n ryhmä* on automorfismien joukko

$$\mathrm{Gal}(\boldsymbol{L}/\boldsymbol{K}) = \{\, f\colon \boldsymbol{L} \cong \boldsymbol{L} \mid f{\restriction}K = \mathrm{id}_K \,\}$$

varustettuna kuvausten yhdistämisellä.

Huomautus. Selvästi

$$\mathrm{Gal}(\boldsymbol{L}/\boldsymbol{K}) \subseteq \mathrm{Sym}(L) = \{\, f\colon L \to L \mid f \text{ on bijektio} \,\}.$$

On suoraviivaista osoittaa, että $(\mathrm{Gal}(\boldsymbol{L}/\boldsymbol{K}), \circ)$ on itse asiassa $(\mathrm{Sym}(L), \circ)$:n aliryhmä.

4.8. Lause. *Olkoon $\boldsymbol{L} = (L, +, \cdot)$ polynomin $a \in K[x]$ juurikunta, $t_0, \ldots, t_{n-1}$ a:n juuret $\boldsymbol{L}$:ssä ja $f \in \mathrm{Gal}(\boldsymbol{L}/\boldsymbol{K})$*

a) Kun $i \in \{0, \ldots, n-1\}$, niin jollakin $j \in \{0, \ldots, n-1\}$ pätee $f(t_i) = t_j$.

b) Jos jokaisella $i \in \{0, \ldots, n-1\}$ pätee $f(t_i) = t_i$, niin $f = \mathrm{id}_L$.

c) $(\mathrm{Gal}(\boldsymbol{L}/\boldsymbol{K}), \circ)$ on isomorfinen symmetrisen ryhmän $\mathbf{Sym}(\{t_0, \ldots, t_{n-1}\})$ aliryhmän kanssa.

Todistus. (hahmotelma)

a) Merkitään $a = \sum_{k=0}^{n} a_k x^k \in K[x]$. Koska t_i on a:n juuri ja $f \in \mathrm{Gal}(\boldsymbol{L}/\boldsymbol{K})$, niin

$$a(t_i) = \sum_{k=0}^{n} a_k t_i{}^k = 0,$$

mistä seuraa

$$0 = f(0) = f(a(t_i)) = f\left(\sum_{k=0}^{n} a_k {t_i}^k\right) = \sum_{k=0}^{n} f(a_k) f(t_i)^k = \sum_{k=0}^{n} a_k f(t_i)^k = a(f(t_i))$$

eli $f(t_i)$ on a:n juuri. Siis $f(t_i) = t_j$ jollakin $j \in \{0, \ldots, n-1\}$.

b) Koska $\boldsymbol{L} = \boldsymbol{K}(t_0, \ldots, t_{n-1})$, niin kaikki $\boldsymbol{L}$:n alkiot voidaan kirjoittaa rationaalilausekkeina juurten $t_0, \ldots, t_{n-1}$ avulla. Todellakin: $\boldsymbol{L}$ on renkaan $\boldsymbol{K}[t_0, \ldots, t_{n-1}]$ jakokunta. Siis jokaisella $u \in L$ on esitys $u = cd^{-1}$, missä $c, d \in K[t_0, \ldots, t_{n-1}]$, ja on helppoa nähdä, että $f(c) = c$ ja $f(d) = d$, joten $f(u) = u$.

b) Koska $\boldsymbol{L} = \boldsymbol{K}(t_0, \ldots, t_{n-1})$, niin kaikki $\boldsymbol{L}$:n alkiot voidaan kirjoittaa rationaalilausekkeina juurten $t_0, \ldots, t_{n-1}$ avulla. Todellakin: $\boldsymbol{L}$ on renkaan $\boldsymbol{K}[t_0, \ldots, t_{n-1}]$ jakokunta. Siis jokaisella $u \in L$ on esitys $u = cd^{-1}$, missä $c, d \in K[t_0, \ldots, t_{n-1}]$, ja on helppoa nähdä, että $f(c) = c$ ja $f(d) = d$, joten $f(u) = u$.

c) Kyseinen isomorfismi on $f \mapsto f\restriction\{t_0, \ldots, t_{n-1}\}$. □

Edellinen lause palauttaa kysymyksen, onko polynomi juurtamalla ratkaistavissa, ryhmäteoreettiseksi ongelmaksi. Galois'n teorian kannalta keskeinen ryhmäteoreettinen käsite on ryhmän ratkeavuus. Aikapulan takia tässä tyydytään hahmottelemaan tähän liittyvä teoriankehittely.

4.9. Lause. *Juurroslaajennusten Galois'n ryhmät ovat ratkeavia.* □

4.10. Fakta. Viiden alkion symmetrinen ryhmä ei ole ratkeava.

4.11. Fakta. Polynomin $x^5 - 4x + 2 \in \mathbb{Q}[x]$ juurikunnan Galois'n ryhmä on isomorfinen 5 alkion symmetrisen ryhmän kanssa.