Matematiikan laitos
AlgebraII
Harjoitus 13
28.04.2011
Ratkaisuehdotuksia
Aleksandr Pasharin

1. Osoita, että jokainen algebrallisesti suljettu kunta on ääretön.

   Ratkaisu: Olkoon $K = \{x_1, \ldots, x_n\}$ äärellinen kunta. Tarkastellaan polynomi $f \in K[X]$, joka on määritelty kaavalla

   $$f = (X - x_1)(X - x_2)\cdots(X - x_n) + 1 = \prod_{i=1}^{n}(X - x_n) + 1.$$

   Tällöin f ei ole vakiopolynomi, mutta kaikilla $x \in K$ pätee $f(x) = 1 \neq 0$. Näin ollen f:llä ei ole juuria K:ssä. Erityisesti K ei voi olla algebrallisesti suljettu.

2. Etsi seuraavissa tapauksissa jokin polynomin f juurikunta kunnan K suhteen ja selvitä sen aste K:n laajennoksena:
   a) $f = X^3 - 2$, $K = \mathbb{Q}$
   b) $f = X^4 - 7$, $K = \mathbb{Q}$
   a) $f = X^4 - 7$, $K = \mathbb{F}_{11}$.

   Ratkaisu: a) Kompleksilukujen kunnassa $\mathbb{C}$ f:llä on kolme eri juurta,

   $$x_0 = \sqrt[3]{2},$$

   $$x_1 = \sqrt[3]{2}(\cos(2\pi/3) + i\sin(2\pi/3)) = x_0\xi, \text{ ja}$$

   $$x_2 = \sqrt[3]{2}(\cos(4\pi/3) + i\sin(4\pi/3)) = x_0\xi^2,$$

   missä $\xi = \cos(2\pi/3) + i\sin(2\pi/3)$ on primitiivinen ykkösen kuutiojuuri $\mathbb{C}$:ssä. Koska $\mathbb{C}$:ssä pätee

   $$f = (X - x_0)(X - x_1)(X - x_2),$$

   niin $\mathbb{C}$:n alikunta $L = \mathbb{Q}(x_0, x_1, x_2)$ on f:n juurikunta määritelmän mukaan. Koska

   $$\xi = x_1/x_0 \in L \text{ ja } x_1 = x_0\xi, x_2 = x_0\xi^2,$$

   niin $L = \mathbb{Q}(x_0, \xi)$.

   Eisensteinin kriteerin nojalla f on jaoton $\mathbb{Q}$:n suhteen. Näin ollen se on x_0:n minimipolynomi, joten

   $$[\mathbb{Q}(x_0) : \mathbb{Q}] = 3 = \deg f.$$

Ykkösenjuuri ξ on puolestaan polynomin $X^3 - 1$ juuri. Tämä polynomi ei kuitenkaan ole jaoton, sillä se on jaollinen polynomilla $X-1$. Toisaalta 1 onkin tämän polynomin ainoa reaalinen juuri, joten

$$\frac{X^3-1}{X-1} = X^2 + X + 1$$

on jaoton $\mathbb{R}[X]$:ssä (se on toisen asteen polynomi jolla ei ole juuria). Erityisesti se on myös jaoton alikunnan $\mathbb{Q}(x_0) \subset \mathbb{R}$ suhteen. Näin ollen ξ:n aste $\mathbb{Q}(x_0)$:n suhteen on 2, joten

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(x_0)] \cdot [\mathbb{Q}(x_0) : \mathbb{Q}] = 2 \cdot 3 = 6.$$

b) Kompleksilukujen kunnassa $\mathbb{C}$ yhtälöllä $x^4 = 7$ on neljä eri juurta, $x_0 = \sqrt[4]{7}$, $x_1 = -\sqrt[4]{7}$, $x_2 = \sqrt[4]{7}i$, $x_3 = -\sqrt[4]{7}i$. Näin ollen $L = \mathbb{Q}(x_0, x_1, x_3, x_4)$ on polynomin $X^4 - 7$ juurikunta $\mathbb{Q}$:n suhteen. Kuten a)-kohdassa helposti nähdään, että $L = \mathbb{Q}(\sqrt[4]{7}, i)$. Eisensteinin kriteerin nojalla $X^4 - 7$ on jaoton $\mathbb{Q}$:n suhteen, joten se on $\sqrt[4]{7}$:n minimipolynomi $\mathbb{Q}$:n suhteen. Näin ollen $[\mathbb{Q}(\sqrt[4]{7}) : \mathbb{Q}] = 4$. Lisäksi i:n minimipolynomi $\mathbb{R}$:n suhteen on $X^2 + 1$, joten se on myös minimipolynomi alikunnan $\mathbb{Q}(\sqrt[4]{7})$ suhteen. Näin ollen

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[4]{7})] \cdot [\mathbb{Q}(\sqrt[4]{7}) : \mathbb{Q}] = 4 \cdot 2 = 8.$$

c)**Pohdinta:** Olkoon L jokin polynomin $f = X^4 - 7$ juurikunta $\mathbb{F}_{11}$:n suhteen. Polynomin derivaatalla $f' = 4X^3$ on tasan yksi juuri 0 (sillä $4 \neq 0$ L:ssä, jonka karakteristiikka on 11), joka ei ole f:n juuri. Näin ollen f:llä on L:ssä tasan 4 eri juurta x_0, x_1, x_2, x_3. Koska $x_i^4 = 7$ kaikilla $i = 1, \ldots, 4$, niin L:n alkiot $1, x_0/x_1, x_0/x_2, x_0/x_3$ ovat polynomin $X^4 - 1$ eri juuret L:ssä, mistä seuraa, että L sisältää kaikki neljännet ykkösenjuuret eli sisältää polynomin $X^4 - 1$ juurikunnan L'.
Kääntäen jos L' on polynomin $X^4 - 1$ juurikunta K:n suhteen, niin se sisältää 4 erilaista alkiota $1, t_0, t_1, t_2$, jotka ovat neljännet ykkösenjuuret. Jos L on jokin L':n laajennus jossa on alkio α jolle pätee $\alpha^4 = 7$, niin $\alpha t_0, \alpha t_1, \alpha t_2$ ovat myöskin polynomin $X^4 - 7$ juuret L:ssä, mistä seuraa, että $L'(\alpha) \subset L$ on haluttu f:n juurikunta.
Tästä tarkastelusta seuraa, että riittää ensin muodostaa polynomin $X^4 - 1$ juurikunta, eli lisätä kaikki neljännet ykkösenjuuret ja sitten muodostaa jokin tämän laajennus jossa polynomilla f on ainakin yksi juuri.

Varsinainen ratkaisu: Tarkastellaan ensin neljännet ykkösenjuuret K:ssä. Käymällä läpi kunnan 11 alkiota tai käyttämällä Suomisen Lausetta 4.7.5 nähdään, että

$$\mu_4(\mathbb{F}_{11}) = \{x \in \mathbb{F}_{11} : x^4 = 1\} = \{1, -1\}.$$

Näin ollen $\mathbb{F}_{11}[X]$:ssä pätee

$$X^4 - 1 = (X-1)(X+1)(X^2+1),$$

missä $X^2+1 \in \mathbb{F}_{11}[X]$ on jaoton, sillä se on toisen asteen polynomi, jolla ei ole juuria. Näin olleen voidaan muodostaa 2-ulotteinen laajennos

$$L = \mathbb{F}_{11}[X]/(X^2+1).$$

Tässä kunnassa yhtälöllä $x^4 = 1$ on ainakin uudet juuret $\bar{X}$ ja $-\bar{X}$. Siis L sisältää ainakin neljä polynomin X^4-1 juurta. Toisaalta niitä ei voi olla enemmän kuin 4 ja $L[X]$:ssä polynomi jakautuu ensimmäisen asteen tekijöihin. Näin ollen $L = K(\bar{X})$ on polynomin X^4-1 juurikunta. Lisäksi $[E:K] = 2$. Huomaa, että $\bar{X}^2 = -1$.

Alkutarkastelun nojalla nyt riittää löytää yksi f:n juuri. Mutta itse asiassa sellainen löytyy jo L:stä sillä

$$(\pm 1 \pm \bar{X})^4 = (1 \pm 2\bar{X} + \bar{X}^2)^2 = (1 \pm 2\bar{X} - 1)^2 = 4\bar{X}^2 = 4 \cdot (-1) = -4 = 7.$$

Näin ollen $K(1+\bar{X}) = K(\bar{X}) = L$ on etsitty f:n juurikunta. Laajennuksen aste on edelleenkin 2.

Huomautus: Polynomin X^4-7 juuret L:ssä löytyy vaikkapa seuraavaksi. Jos $x^4 = 7$, niin $y = x^2$ toteuttaa yhtälön $y^2 = 7$, joten ratkaistaan ensin se. Jokainen alkio voidaan kirjoittaa muotoon $y = a + b\bar{X}$, joten saadaan ehto

$$a^2 + 2ab\bar{X} - b^2 = 7.$$

Tästä seuraa, että $a = 0$ tai $b = 0$. Edellisessä tapauksessa saadaan ehto $b^2 = -7 = 4$, jonka juuret ovat $b = \pm 2$. Jälkimmäisessä tapauksessa saadaan ehto $a^2 = 7$, jolla ei ole ratkaisuja K:ssä, kuten nähdään esim. käymällä läpi kaikki alkiot. Jäljellä on ratkaista yhtälö $x^2 = \pm 2\bar{X}$. Taas kirjoitetaan $x = a + b\bar{X}$, jolloin saadaan

$$a^2 + 2ab\bar{X} - b^2 = \pm 2\bar{X} \text{ eli}$$
$$(a-b)(a+b) = a^2 - b^2 = 0, ab = \pm 1.$$

Ensimmäinen ehto antaa $a = \pm b$, joten toinen supistuu muotoon $a^2 = \pm 1$, jolla on ratkaisut $a = \pm 1$. Näin saadaan ratkaisut $\pm 1 \pm \bar{X}$.

Huomautus 2: Määritelmän mukana juurikunnassa L polynomi voidaan hajoittaa ensim. asteen tekijöihin,

$$X^4 - 7 = (X - (1+\bar{X}))(X - (1-\bar{X}))(X - (-1+\bar{X}))(X - (-1-\bar{X})).$$

Koska $(X-(1+\bar{X}))(X-(1-\bar{X})) = X^2 - 2X + 2$ ja $(X-(-1+\bar{X}))(X-(-1-\bar{X})) = X^2 + 2X + 2$ voidaan nyt jäkiviisana

todeta, että $X^4 - 7$ ei ole jaoton $\mathbb{F}_{11}[X]$:ssä ja sen hajotelma jaottomiin tekijöihin on

$$X^4 - 7 = (X^2 - 2X + 2)(X^2 + 2X + 2).$$

Tässä oikeanpuolen polynomit ovat varmasti jaottomia, sillä ne ovat toisen asteen polynomeja, joilla ei ole juuria $\mathbb{F}_{11}$:ssä.
Näin ollen toinen tapa konstruoida juurikunta olisi seuraava. Löydetään ensin hajotelma

$$X^4 - 7 = (X^2 - 2X + 2)(X^2 + 2X + 2).$$

Yksi tapa löytää se on huomata, että $X^4 - 7 = X^4 + 4$ kunnassa $\mathbb{F}_{11}$. Hajotelma $X^4 + 4 = (X^2 - 2X + 2)(X^2 + 2X + 2)$ taas löytyy jo $\mathbb{Z}[X]$ vaikkapa ratkaistamalla yhtälö $x^4 = -4$ kompleksilukujen kunnassa.
Seuraavaksi todetaan, että molemmat polynomit $X^2 \pm 2X + 2$ ovat jaottomia $\mathbb{F}_{11}[X]$:ssä, sillä ne ovat toisen asteen polynomit, joilla ei ole juuria (jokaisen polynomin juuri olisi alkuperäisen polynomin $X^4 - 7$ juuri, mutta sillä ei ole juuria $\mathbb{F}_{11}$:ssä).
Näin ollen voidaan muodostaa esim. laajennus $L = K[X]/(X^2 + 2X + 2)$, jonka aste on 2, ja jossa polynomilla $X^2 + 2X + 2$ löytyy juuri $x = \bar{X}$. Mutta tästä seuraa, että $X^2 + 2X + 2$ on $L[X]$:ssä jaollinen polynomilla $X - x$ ja osamäärän täytyy olla ensimmäisen asteen polynomi $X - y$. Näin ollen $L[X]$:ssä polynomi $X^2 + 2X + 2$ jakautuu ensimmäisen asteen tekijöihin. Lisäksi tarkastelemalla vaikkapa polynomin derivaatta, nähdään, että polynomilla ei ole kaksinkertaisia juuria. Näin ollen $x \neq y$. Lisäksi helposti nähdään, että $-x$ ja $-y$ ovat polynomin $X^2 - 2X + 2$ juuret. Ei ole vaikeata tarkistaa, että alkiot $x, y, -x, -y$ ovat kaikki eri alkiot. Esimerkiksi $x \neq -x$, sillä $x \neq 0$ ja kunnan karakteristikka ei ole 2. Jos taas esim. x on molemman polynomin juuri, niin vähentämällä toinen polynomi toisesta nähdään, että $x = 0$, mikä on mahdotonta.
Näin ollen laajenuksessa L polynomilla $X^4 - 7$ on neljä eri juurta, joista yksi on koko laajennuksen virittäjä $\bar{X}$. Tästä seuraa, että L on etsitty juurikunta, jonka aste on 2.

3. Osoita, että $\mathbb{Q}(\sqrt{2}) \ncong \mathbb{Q}(\sqrt{3})$ (kuntina).

Ratkaisu: Riittää osoittaa, että $\mathbb{Q}(\sqrt{3})$:ssä ei ole sellaista alkiota x, jolle päteisi yhtälö $x^2 = 2$. Tehdään vasta-oletus - olkoon $x = a + b\sqrt{3}$, $a, b \in \mathbb{Q}$, jolle $x^2 = 2$. Tällöin

$$a^2 + 2ab\sqrt{3} + 3b^2 = 2, \text{ joten}$$

$ab = 0$, sillä $\sqrt{3}$ ei ole rationaaliluku. Siis $a = 0$ tai $b = 0$. Jos $b = 0$, niin $a^2 = 2$, mikä on mahdotonta, sillä $a \in \mathbb{Q}$. Muuten $3b^2 = 2$. Helposti nähdään, että sekin on mahdotonta (todistus samalla tavalla kuin todistus sille, että $\sqrt{2}$ on irrationaalinen).

4. a) Osoita, että algebrallisten lukujen joukko

$$\mathbb{A} = \{\alpha \in \mathbb{C} | \alpha \text{ on algebrallinen } \mathbb{Q}\text{:n suhteen}\}$$

on kunta.

b) Olkoon Ω alkukunnan $\mathbb{F}_p$ algebrallinen sukeuma. Osoita, että polynomin $X^{p^n} - X$ juurten joukko Ω:ssa on kunta.

Ratkaisu: a) Koska $0, 1 \in \mathbb{Q}$ ovat selvästi algebrallisia $\mathbb{Q}$:n suhteen, riittää osoittaa, että kahden algebrallisen luvun $x, y \in \mathbb{C}$ summa, tulo ja osamäärä ovat algebrallisia. Koska x on algebrallinen, niin $\mathbb{Q}(x)$ on$\mathbb{Q}$:n äärellinen laajennus. Koska y on algebrallinen $\mathbb{Q}$:n suhteenm, se on myös algebrallinen $\mathbb{Q}(x)$:n suhteen, joten $[\mathbb{Q}(x, y) : \mathbb{Q}(x)] < \infty$. Näin ollen (Lause 12.3) $\mathbb{Q}(x, y)$ on äärellinen $\mathbb{Q}$:n laajennus. Lauseen 13.7 nojalla se on algebraallinen. Erityisesti alkiot $x + y, xy, x/y \in \mathbb{Q}(x, y)$ ovat algebrallisia $\mathbb{Q}$:n suhteen.

b)Palautetaan mieleen, että jos kunnan K karakteriistikka on $p < \infty$, niin kaikilla $x, y \in K$ pätee

$$(x + y)^p = x^p + y^p.$$

Induktiolla tästä helposti seuraa kaikilla $n \in \mathbb{N}_+$.

$$(x + y)^{p^n} = x^{p^n} + y^{p^n}.$$

Merkitään $L = \{x \in \Omega : x^{p^n} = x\}$. Tällöin selvästi $0, 1 \in L$. Lisäksi jos $x, y \in L$, niin

$$(x + y)^{p^n} = x^{p^n} + y^{p^n} = x + y,$$

$$(xy)^{p^n} = x^{p^n} y^{p^n} = xy, (1/y)^{p^n} = 1/y^{p^n} = 1/y.$$

Näin ollen L on alikunta.

5. Olkoon Ω kunnan K algebrallinen sulkeuma. Kunnan K algebrallista laajennosta $L \subseteq \Omega$ kutsutaan *normaaliksi*, jos jokaisella K-automorfismilla $\sigma : \Omega \to \Omega$ pätee $\sigma(L) \subseteq L$. Osoita, että minkä tahansa polynomijoukon juurikunta K:n suhteen on K:n normaali laajennos.

Ratkaisu: Olkoon L polynomijoukon $\{f_i : i \in I\} \subset K[X]$ juurikunta. Tällöin erityisesti on olemassa joukko $x_j, j \in J$, siten että $L = K((x_j)_{j \in J})$ ja jokainen x_j on jonkun polynomin f_i

juuri. Olkoon $\sigma\colon \Omega \to \Omega$ K-automorfismi. Riittää osoittaa, että $\sigma(x_j) \in L$ jokaisella $j \in J$. Olkoon f_i polynomi, jonka juuri on x_j. Tällöin $\sigma(x_j)$ on myös f_i:n juuri. Koska L oli juurikunta, se sisältää kaikki f_i:n juuret, erityisesi $\sigma(x_j)$.

6. Selvitä seuraavissa tapauksissa laajennoksen L/K Galois'n ryhmä. Jos laajennos on Galois'n laajennos, etsi kaikki välilaajennokset L/M, missä $K \subseteq M \subseteq L$.
   a) $L = \mathbb{Q}(\sqrt{2})$, $K = \mathbb{Q}$,
   b) $L = \mathbb{Q}(\sqrt[3]{2})$, $K = \mathbb{Q}$,
   c) $L = \mathbb{Q}(\sqrt{2}, i)$, $K = \mathbb{Q}$.

   Ratkaisu: a) Olkoon $\sigma\colon L \to L$ K-automorfismi. Tällöin $\sigma(\sqrt{2})$ määrää σ:n yksikäsitteisesti. Lisäksi $\sigma(\sqrt{2})$:llä on sama minimipolynomi $X^2 - 2$ kuin $\sqrt{2}$:llä. Siis $\sigma(\sqrt{2}) = \pm\sqrt{2}$. Tästä seuraa, että $\sigma = \mathrm{id}$ tai $\sigma(x + y\sqrt{2}) = x - y\sqrt{2}$. Kääntäen nämä selvästi ovat K-homomorfismejä. Näin ollen Galois'n ryhmä on kahden alkion syklinen ryhmä. Laajennos on normaali ja separoituva, sillä se on polynomin $X^2 - 2$ juurikunta, ja tällä polynomillä ei ole kaksoisjuuria. Aitoja epätriviaaleja välilaajennoksia ei ole, sillä laajennoksen aste on alkuluku.

   b) Alkion $\sqrt[3]{2}$ minimipolynomin X^3-2 muut juuret $\sqrt[3]{2}(\cos(2\pi/3)+ i\sin(2\pi/3))$ ja $\sqrt[3]{2}(\cos(4\pi/3) + i\sin(4\pi/3))$ eivät sisälly L:ään, joten L ei ole normaali laajennos, eikä sitten myöskään Galois'n laajennos. Lisäksi samasta syystä jos $\sigma\colon L \to L$ on K-homomorfismi, niin $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$, joten L:n Galois'n ryhmä on triviaali ryhmä $\{\mathrm{id}\}$.

   c) L on polynomien X^2-2 ja X^2+1 juurikunta $\mathbb{Q}$:n suhteen, joten se on normaali laajennos. Lisäksi näillä polynomeilla ei ole kaksoisjuuria, joten laajennos on separoituva. Näin ollen L on Galois'n laajennus, jonka aste on 4.
   Jos $\sigma\colon L \to L$ on K-homomorfismi, niin $\sigma(\sqrt{2}) = \pm\sqrt{2}$ ja $\sigma(i) = \pm i$. Näin ollen Galois'n ryhmän alkiot ovat $\mathrm{id}, \alpha, \beta, \gamma$, joille $\alpha(\sqrt{2}) = \sqrt{2}$, $\alpha(i) = -i$, $\beta(\sqrt{2}) = -\sqrt{2}$, $\beta(i) = i$ ja $\gamma = \beta \circ \alpha$. Galois'n ryhmä on siis Kleinin neliryhmä. Välilaajennoksia vastaavat aliryhmät. Aidot epätriviaalit aliryhmät ovat $\{\mathrm{id}, \alpha\}$, $\{\mathrm{id}, \beta\}$ ja $\{\mathrm{id}, \gamma\}$. Ne vastaa 2-ulottesia kiintopistekuntia $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$ ja $\mathbb{Q}(\sqrt{2}i)$. Muita aitoja epätriviaalia välilaajennuksia ei ole.