Matematiikan laitos
AlgebraII
Harjoitus 11
10.04.2011
Ratkaisuehdotuksia
Aleksandr Pasharin

1. Tutki, mitkä seuraavista polynomeista ovat jaottomia renkaassa

	(a)	X^2+Y^2-1	(d)	X^3-Y^2-X
$\mathbb{Q}[X,Y]$:	(b)	X^2-Y^2-X	(e)	$X^3-Y^3+X^2$
	(c)	X^2-Y^2	(f)	$3XY^2-XY+2$

Ratkaisu: Olkoon $A=\mathbb{Q}[X]$ ja olkoon K kokonaisalueen A osamääräkunta. Harj.10 Teht. 2 nojalla on olemassa luonnollinen $\mathbb{Q}$-isomorfismi

$$\mathbb{Q}[X,Y]\cong\mathbb{Q}[X][Y]=A[Y].$$

Lauseen 11.8 nojalla A on tekijöihinjakorengas. Lauseesta 11.5 seuraa tällöin, että polynomi $f\in A[Y]$ on jaoton jos ja vain jos f on primitiivinen ja jaoton $K[Y]$:ssä. Huomaa, että kaikki tehtävässä esiintyvät polynomit ovat primitiivisia, kun ne ajatellaan $A[Y]$:n alkioina.

a) Renkaassa $A[Y]$ tämä on polynomi

$$P=Y^2+(X^2-1),$$

missä X^2-1 on vakiotermi. Sen hajotelma alkutekijöihin A:ssä on

$$X^2-1=(X-1)(X+1).$$

Erityisesti esimerkiksi $X-1$ on jaoton A:n alkio, joka on kaikkien polynomin kertoimien tekijä, paitsi korkeamman asteen kertoimen 1, lisäksi $(X-1)^2$ ei ole X^2-1:n tekijä. Eisensteinin kriteerin (Lause 11.6) nojalla P on jaoton $K[Y]$:ssä. Koska se on primitiivinen, se on myös jaoton $A[Y]$:ssä.

b) Samalla tavalla kuin a)-kohdassa, näemme, että X on vakiokertoimen $X^2-X=X(X-1)$:n tekijä, jonka neliö ei ole X^2-1:n tekijä. Lisäksi X ei ole korkeamman asteen kertoimen -1 tekijä. Koska muut kertoimet ovat nollia, Eisensteinin kriteerin sovellus implikoi, että polynomi on jaoton $A[Y]$:ssä.

c) Pätee

$$X^2-Y^2=(X-Y)(X+Y),$$

joten polynomi ei ole jaoton.

d) Vakiokertoimen $X^3 - X = X(X-1)(X+1)$ kaikki jaottomat termit toteuttavat Eisensteinin kriteerin, joten polynomi on jaoton.

e) Samoin, vakiotermin $X^3 + X^2 = X^2(X+1)$ tekijä $X+1$ toteuttaa Eisensteinin kriteerin. Polynomi on jaoton.

f) Tällä kertaa jaoton alkio X jakaa kaikki kertoimet, paitsi vakiokerrointa 2 ja X^2 ei jakaa $3X$. Eisensteinin kriteerin nojalla polynomi on jaoton.

2. Olkoon E kunnan K laajennos ja olkoot A ja B sen osajoukkoja. Osoita, että $K(A \cup B) = K(A)(B) = K(B)(A)$.

Ratkaisu: $K \subset K(A) \subset K(A)(B)$, $A \subset K(A) \subset K(A)(B)$ ja $B \subset K(A)(B)$. Koska $K(A \cup B)$ on pienin laajennus, jolla on nämä ominaisuudet, pätee

$$K(A \cup B) \subset K(A)(B).$$

Kääntäen $K \subset K(A \cup B)$ ja $A \subset A \cup B \subset K(A \cup B)$. Näin ollen $K(A) \subset K(A \cup B)$. Toisaalta $B \subset A \cup B \subset K(A \cup B)$, joten

$$K(A)(B) \subset K(A \cup B).$$

Siis

$$K(A \cup B) = K(A)(B).$$

Kun A ja B vaihdetaan keskenään, saadaan

$$K(B)(A) = K(B \cup A) = K(A \cup B).$$

3. Olkoon $E = K(x)$ kunnan K äärellinen laajennos, jonka aste on pariton. Osoita, että $E = K(x^2)$.

Ratkaisu: Tarkastellaan laajennus $E' = K(x^2)$. Koska $\alpha = x^2 \in K(x)$, pätee

$$K \subset E' \subset E.$$

Alkio $x \in E$ on algebrallinen E':n suhteen, sillä se toteuttaa yhtälön

$$x^2 - \alpha = 0$$

eli on polynomin $X^2 - \alpha \in E'[X]$ juuri. Selvästi pätee $E = E'(x)$. Lauseen 13.4 nojalla E:n aste E':n suhteen on korkeintaan 2. Jos $[E' : E] = 2$, saadaan Lauseen 12.3 avulla

$$[E : K] = [E : E'][E' : K] = 2[E' : K],$$

eli $[E : K]$ on parillinen. Tämä on ristiriidassa oletuksen kanssa. Näin ollen $[E' : E] = 1$, eli $E = E' = K(x^2)$.

4. (a) Olkoon R rengas ja $b \in R$. Osoita, että kuvaus $\tau_b : R[X] \to R[X]$, missä $\sum_i a_i X^i \mapsto \sum_i a_i (X + b)^i$, on rengasisomorfismi. Päättele, että $f \in R[X]$ on jaoton, jos ja vain jos $\tau_b(f)$ on jaoton.
   (b) Olkoon p alkuluku. Osoita, että $X^p - 1 = (X - 1)g$, missä $g \in \mathbb{Z}[X]$ on jaoton kunnan $\mathbb{Q}$ suhteen.

Ratkaisu: (a) τ_b on sijoitushomomorfismi, jonka määrää yksikäsitteisesti ehto $\tau_b(X) = X + b$. Helposti nähdään, että sijoitushomomorfismi, jolle $X \mapsto X - b$, on τ_b:n käänteiskuvaus, vrt. Harj. 9 teht. 4. Näin olleen, τ_b on isomorfismi. Jaottomuus selvästi säilyy rengasisomomorfismeissa.

b) Tarkastellaan $\tau_1(X^p - 1)$. Pätee

$$\tau_1(X^p - 1) = (X+1)^p - 1 = \sum_{k=0}^{p} \binom{p}{k} X^k - 1 = X^p + pX^{p-1} + \ldots + pX = Xh,$$

missä

$$h = \sum_{k=0}^{p-1} \binom{p}{k+1} X^k = X^{p-1} + pX^{p-2} + \ldots + p.$$

Osoitetaan, että tämän polynomin kaikki kertoimet, paitsi X^{p-1}:n kerroin, ovat jaollisia p:llä. On siis osoitettavaa, että p jakaa binomikertoimen $a = \binom{p}{k} = \frac{p!}{(p-k)!k!}$ kun $0 < k < p$. Huomataan, että

$$p! = ak!(p - k)!.$$

Luvun $k! = 1 \cdot 2 \cdots k$ jokainen alkulukutekijä on jonkun $l \leq k < p$ tekijä, joten se ei voi olla p. Samasta syystä $(p - k)!$ ei ole jaollinen p:llä. Koska p on alkuluku,tästä seuraa, että p ja $k!(p - k)!$ ovat keskenään jaottomia. Toisaalta p jakaa luvun $p! = ak!(p - k)!$. Harj. 10 Teht. 6b) nojalla p jakaa $a = \binom{p}{k}$.

Näin ollen $\mathbb{Z}$:n alkuluku p jakaa kaikki polynomin h kertoimet, paitsi korkeamman asteen kerrointa. Lisäksi p^2 ei jakaa vakiotermin, joka on tasan p. Eisensteinin kriteerin (Lause 11.6)

nojalla h on jaoton $\mathbb{Q}[X]$:ssä. Näin olleen

$$\tau_1(X^p - 1) = Xh,$$

missä h on jaoton. Soveltamalla tähän käänteiskuvausta τ_{-1} saadaan

$$X^p - 1 = (X - 1)g,$$

missä $g = \tau_{-1}h$ on jaoton.

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

   Ratkaisu: Seuraavat yhtälöt ovat yhtäpitäviä,

$$(\alpha - 1)^{-1} = a\alpha^2 + b\alpha + c,$$

$$1 = (a\alpha^2 + b\alpha + c)(\alpha - 1) = a\alpha^3 + (b - a)\alpha^2 + (c - b)\alpha - c$$

   Toisaalta $\alpha^3 + \alpha^2 + \alpha + 2 = 0$, mistä seuraa, että

$$\alpha^3 = -\alpha^2 - \alpha - 2,$$

   Näin ollen

$$a\alpha^3 + (b - a)\alpha^2 + (c - b)\alpha - c = (b - 2a)\alpha^2 + (c - b - a)\alpha - (c + 2a).$$

   Näin ollen riittää, että toteuttuu yhtälö

$$(b - 2a)\alpha^2 + (c - b - a)\alpha - (c + 2a) = 1.$$

   Se selvästi toteuttuu, jos

$$b - 2a = 0,$$

$$c - b - a = 0,$$

$$c + 2a = -1.$$

   Ensimmäisestä ja toisesta yhtälöstä seuraa, että $b = 2a$, joten $c = a + b = 3a$. Tällöin viimeinen yhtälö antaa $5a = -1$, joten $a = -\frac{1}{5}$, $b = 2a = -\frac{2}{5}$ ja $c = 3a = -\frac{3}{5}$.

   Näin ollen

$$(\alpha - 1)^{-1} = -\frac{1}{5}\alpha^2 - \frac{2}{5}\alpha - \frac{3}{5}.$$

6. Määritä seuraavissa tapauksissa joukon A virittämän laajennoksen L/K alilaajennoksen $K(A)$ aste:
   (a) $K = \mathbb{Q}$, $L = \mathbb{R}$, $A = \{\sqrt{2}\}$.
   (b) $K = \mathbb{Q}$, $L = \mathbb{C}$, $A = \{\sqrt{2}, i\}$.
   (c) $K = \mathbb{F}_2$, $L = \mathbb{F}_2[X]/\langle X^5 + X^3 + 1\rangle$, $A = \{\overline{X}^2\}$.

Ratkaisu: a) Alkion $\sqrt{2}$ minimipolynomi $\mathbb{Q}$:n suhteen on X^2-2. Tämä on jaoton esim. Eisensteinin kriteerin nojalla, tai koska se on toisen asteen polynomi jolla ei ole juuria $\mathbb{Q}$:ssä. Lauseen 13.4 nojalla $\mathbb{Q}(\sqrt{2})$:n aste on 2.

b) Toisen asteen polynomi X^2+1 on jaoton $\mathbb{R}$:ssä, esim. koska sillä ei ole juuria, ja sen aste on 2. Erityisesti se on jaoton myös $\mathbb{Q}(\sqrt{2})$:n suhteen, sillä se on R:n alikunta. Se on siis alkion $i \in \mathbb{C}$ minimipolynomi $\mathbb{Q}(\sqrt{2})$:n suhteen, joten Lauseen 13.4 aste $[\mathbb{Q}(\sqrt{2})(i) : \mathbb{Q}(\sqrt{2})]$ on 2. Lisäksi Teht. 2 nojalla $\mathbb{Q}(\sqrt{2})(i) = \mathbb{Q}(A)$. Lauseesta 12.3 ja a)-kohdasta seuraa, että

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

c) Osoitetaan ensin, että L on tosiaankin kunta. Riittää osoittaa, että $\langle X^5 + X^3 + 1\rangle$ on maksimaalinen ideaali $\mathbb{F}_2[X]$:ssä. Koska $\mathbb{F}_2[X]$ on pääideaalirengas, riittää osoittaa, että polynomi $X^5 + X^3 + 1 \in \mathbb{F}_2[X]$ on jaoton (Harj. 9 Teht. 6).

Tehdään vasta-oletus: $X^5 + X^3 + 1 = PQ$, missä $\deg P \geq 1, \deg Q \geq 1$. Koska polynomin aste on 5, voidaan olettaa, että joko $\deg P = 1$ ja $\deg Q = 4$ tai $\deg P = 2, \deg Q = 3$. Ensimmäisessä tapauksessa P:llä, joten myös $X^5 + X^3 + 1$:llä, on juuri, mikä ei pidä paikkaansa - molemmat $\mathbb{F}_2$:n alkiot saa tällä polynomillä arvon 1. Näin ollen $\deg P = 2, \deg Q = 3$ ja samasta syystä kuten yllä P:llä ja Q:llä ei ole juuria. Renkaassa $\mathbb{F}_2[X]$ on vain 4 toisen asteen polynomia, ja helposti nähdään, että $X^2 + X + 1$ on ainoa, jolla ei ole juuria. Näin ollen $P = X^2+X+1$. Samalla tavalla nähdään, että Q on joko polynomi X^3+X^2+1 tai polynomi X^3+X+1. Laskemalla nähdään, että tällöin

$$PQ = (X^2+X+1)(X^3+X^2+1) = X^5+X^4+X^2+X^4+X^3+X+X^3+X^2+1 = X^5+X+1 \text{ tai}$$
$$PQ = (X^2+X+1)(X^3+X+1) = X^5+X^3+X^2+X^4+X^2+X+X^3+X+1 = X^5+X^4+1,$$

joista kumpikin vaihtoehto ei ole polynomi $X^5 + X^3 + 1$. Näin ollen polynomi on jaoton ja L on kunta.

Koska L:n aste K:n suhteen on alkuluku 5, lauseesta 12.3 seuraa, että jokainen välilaajennos M on joko K tai L (kts. huomautus lauseen 12.3 jälkeen). Koska $\bar{X}^2 \notin K$, tästä seuraa, että $K(A) = L$. Vaihtoehtoisesti voidaan huomata, että $L = K(\bar{X})$ ja sen aste 5 on pariton luku, joten sama johtopäätös seuraa tehtävästä 3. Näin ollen $K(A)$:n aste on 5.