Matematiikan laitos
AlgebraII
Harjoitus 10
06.04.2011
Ratkaisuehdotuksia
Aleksandr Pasharin

1. Osoita, että polynomit X^2-X+1 ja X^3+X+1 ovat jaottomia renkaassa $\mathbb{F}_2[X]$ mutta eivät renkaassa $\mathbb{F}_3[X]$. Muodosta vastaavat kunnan $\mathbb{F}_2$ laajennokset ja ratkaise niissä yhtälöt $a^3 = 1$ ja $b^4 + b^2 = 1$.

   Ratkaisu: Jos K on kunta, niin toisen tai kolmannen asteen polynomi $P \in K[X]$ on jaoton jos ja vain jos sillä ei ole juuria K:ssä. Riittää siis tarkistaa onko polynomeilla juuria. Kunnassa $\mathbb{F}_2$ saadaan

$$\bar{0}^2 - \bar{0} + \bar{1} = \bar{1} \neq \bar{0},$$
$$\bar{1}^2 - \bar{1} + \bar{1} = \bar{1} \neq \bar{0},$$
$$\bar{0}^3 + \bar{0} + \bar{1} = \bar{1} \neq \bar{0},$$
$$\bar{1}^3 + \bar{1} + \bar{1} = \bar{1} \neq \bar{0}.$$

   Näin ollen polynomeillä $X^2 - X + 1$ ja $X^3 + X + 1$ ei ole juuria $\mathbb{F}_2$, joten ne ovat jaottomia $\mathbb{F}_2[X]$.
   Sen sijaan renkaassa $\mathbb{F}_3$ molemmilla polynomilla on juuri, sillä

$$\bar{2}^2 - \bar{2} + 1 = \bar{3} = 0 \text{ ja}$$
$$\bar{1}^3 + \bar{1} + \bar{1} = \bar{3} = \bar{0}.$$

   Näin ollen renkaassa $\mathbb{F}_3[X]$ molemmat polynomit ovat jaollisia.

   Kunnan $\mathbb{F}_2$ laajennus $A = \mathbb{F}_2[X]/\langle X^2-X+1\rangle$ on 2-ulotteinen $\mathbb{F}_2$:n suhteen. Sen kanta $\mathbb{F}_2$-vektoriavaruutena on $\bar{1}, \bar{X}$ (vrt. Lauseen 10.4 todistus) ja tämän kannan kertotaulu on

$\cdot$	1	X
1	1	X
X	X	$X+1.$

   Tässä siis samastamme $\mathbb{F}_2[X]$:n alkio ja sen kuva tekijärenkassa A. Huomaa, että tekijärenkaassa pätee $X^2 - X + 1 = 0$, josta seuraa, että

$$X \cdot X = X^2 = X - 1 = X + 1,$$

   sillä kunnan karakteristiikka on 2, joten erityisesti $-1 = 1$.

Vastaavasti kunnan $\mathbb{F}_2$ laajennus $B = \mathbb{F}_2[X]/\langle X^3 + X + 1\rangle$ on 3-ulotteinen. Sen kanta $\mathbb{F}_2$-vektoriavaruutena on $\bar{1}, \bar{X}, \bar{X}^2$ ja tämän kannan kertotaulu on

$\cdot$	1	X	X^2
1	1	X	X^2
X	X	X^2	$X+1$
X^2	X^2	$X+1$	X^2+1.

Molemmat laajennukset A ja B ovat kuntia, sillä polynomit $X^2 - X + 1$ ja $X^3 + X + 1$ ovat jaottomia $\mathbb{F}_2$:ssä, joten niiden virittämät ideaalit ovat maksimaalisia.

Ratkaistaan vielä yhtälöt $a^3 = 1$ ja $b^4 + b^2 = 1$ molemmassa laajenuksessa. Selvästi 0 ei ole yhtälön $a^3 = 1$ juuri. Toisaalta $A^* = A \setminus \{0\}$ ja $B^* = B \setminus \{0\}$ ovat ryhmiä kertolaskun suhteen, sillä A ja B ovat kuntia. Ryhmässä A^* on tasan 3 alkiota, joten jokaisen A^*:n alkion kertaluku (multiplikaativisessa ryhmässä $(A^*, \cdot)$) on kolmella jaollinen ja

$$a^3 = 1$$

pätee jokaisella $a \in A^*$. Yhtälöllä on siis tasan kolme ratkaisua A:ssä - 1, X ja $X + 1$. Ryhmän B^* kertaluku on 7, joten ainoa sen alkio joka toteuttaa yhtälön $a^3 = 1$ on neutraalialkio 1. Yhtälöllä on siis vain yksi ratkaisu B:ssä.
Näytetään, että yhtälö $b^4 + b^2 = 1$ on yhtäpitävä A:ssä ja B:ssä yhtälön $b^2 + b + 1 = 0$. Nimittäin molemman kunnan karakteristiikka on 2, joten

$$(x + y)^2 = x^2 + y^2 \text{ ja } -x = x$$

kaikilla $x, y \in A(B)$. Tästä seuraa, että

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

joten yhtälö $b^4 + b^2 - 1 = 0$ on yhtäpitävä yhtälön $b^2 + b + 1 = 0$ kanssa (ollaan kokonaisalueessa). Toisaalta helposti nähdään, että

$$a^3 - 1 = (a - 1)(a^2 + a + 1)$$

missä tahansa renkaassa. Tästä nähdään, että kunnassa A yhtälön $a^3 - 1 = 0$ juuret X ja $X + 1$ ovat myös yhtälön $a^2 + a + 1$ juuret ja kääntäen jokainen tämän yhtälön juuri on myös yhtälön $a^2 + a + 1$ juuret. Tästä seuraa, että yhtäpitävän yhtälön $b^4 + b^2 = 1$ juuret ovat tasan X ja $X + 1$.

Toisaalta samasta syystä B:ssä jokainen yhtälön $a^2 + a + 1 = 0$ juuri on myös yhtälön $a^3 - 1 = 0$ ratkaisu. Mutta tällä on vain ratkaisu $a = 1$, joka ei toteuda yhtälön $a^2 + a + 1 = 0$. Näin

olleen myös yhtäpitävällä yhtälöllä $b^4 + b^2 = 1$ ei ole ratkaisuja B:ssä.

2. (a) Olkoon R rengas. Osoita, että $R[X, Y] \cong R[X][Y]$ R-algebroina.
   (b) Osoita, että jos R on kokonaisalue, joka ei ole kunta, niin $R[X]$ ei ole pääideaalirengas. Päättele tämän avulla, että $\mathbb{Z}[X]$ ei ole pääideaalirengas. (Vihje: tarkastele ideaalia $\langle X, c\rangle$, missä $c \neq 0$ ei ole R:n yksikkö.)
   (c) Osoita (b)-kohdan avulla, että jos K on kunta ja $n \geq 2$, niin $K[X_1, \ldots, X_n]$ ei ole pääideaalirengas.

Ratkaisu: a) Käytetään polynomialgebrojen universaaliominaisuuksia. Ensin huomataan, että määritelmän mukaan $R[X, Y]$ on R-algebra, mutta $R[X][Y]$ on $R[X]$-algebra. Kuitenkin R on $R[X]$:n alirengas (samastetaan nollaasteisten polynomien alirenkaan kanssa), joten $R[X][Y]$ voidaan pitää myös R-algebrana luonnollisena tavalla (vrt. Harj. 6 teht. 6).
Toisaalta (yksikäsitteinen) sijoitushomomorfismi $f\colon R[X] \to R[X, Y]$ jolle pätee $f(X) = X$ määrittelee $R[X, Y]$:ään $R[X]$-algebran struktuurin, kun määritellään

$$P(X)\cdot Q(X, Y) = f(P(X))Q(X, Y), P(X) \in R[X], Q(X, Y) \in R[X, Y].$$

Huomaa, että f on itse asiassa injektiivinen upotus, jonka kuvassa on tasan ne $R[X, Y]$:n polynomit, joissa "ei esiinny"Y:n potenssejä.

Määritellään R-sijoitushomomorfismi $\varphi\colon R[X, Y] \to R[X][Y]$, jolle pätee $\varphi(X) = X \in R[X] \subset R[X][Y], \varphi(Y) = Y \in R[X][Y]$ ja $R[X]$- sijoitushomomorfismi $\psi\colon R[X][Y] \to R[X, Y]$, jolle pätee $\psi(Y) = Y \in R[X, Y]$. Tällöin ψ on erityisesti myös R-homomorfismi ja $\psi(X) = X = f(X)$. Osoitetaan ensin, että φ on myös $R[X]$-homomorfismi. On siis osoitettava, että

$$\varphi(PQ) = \varphi(f(P)Q) = P\varphi(Q)$$

kun $P \in R[X], Q \in R[X, Y]$. Kiinnitetään $P \in R[X]$. Kuvaukset $Q \mapsto \varphi(PQ)$ ja $Q \mapsto P\varphi(Q)$ ovat molemmat R-homomorfismit $R[X, Y] \to R[X][Y]$ (tarkista!), joten polynomialgebran $R[X, Y]$ universaaliominaisuuden nojalla ne yhtyvät, jos ne saavat samat arvot kun $Q \in \{X, Y\}$. Riittää siis osoittaa, että

$$\varphi(PX) = P\varphi(X),$$
$$\varphi(PY) = P\varphi(Y).$$

Näiden yhtälöiden mollemmat puoleet ovat taas P:n suhteen R-homomorfismit $R[X] \to R[X][Y]$, joten $R[X]$:n universaaliominaisuuden nojalla riittää tarkastella vain tapaus $P = X$. Kaiken kaikkia saadaan siis, että yhtälö

$$\varphi(PQ) = \varphi(f(P)Q) = P\varphi(Q)$$

riittää osoittaa vain kun $P = X$ ja $Q \in \{X, Y\}$. Suora lasku osoittaa, että

$$\varphi(X^2) = X^2 = X\varphi(X),$$
$$\varphi(XY) = XY = X\varphi(Y).$$

Olemme osoittaneet, että φ on $R[X]$-homomorfismi.

Nyt voimme todettaa, että $\varphi\circ\psi$ on $R[X]$-homomorfismi $R[X][Y] \to R[X][Y]$, joka kuvaa virittäjän Y itselleen. Universaaliominaisuuden nojalla

$$\varphi \circ \psi = \mathrm{id}.$$

Samoin $psi \circ \varphi$ on R-homomorfismi $R[X, Y] \to R[X, Y]$ joka kuvaa virittäjät X ja Y itselleen, joten myös

$$\psi \circ \varphi = \mathrm{id}.$$

Erityisesti φ on siis R-homomorfismi.

b) Olkoon $c \in R \setminus \{0\}$ sellainen alkio, jolla ei ole käänteisalkiota R:ssä. Osoitetaan, että $R[X]$:n ideaali $I = \langle X, c\rangle$ ei ole yhden alkio virittämä. Tehdään vasta-oletus: $I = \langle P\rangle$, missä $P \in R[X]$. Tällöin erityisesti pätee

$$c = PQ \text{ jollakin } Q \in R.$$

Koska c on nollaulotteinen polynomi $R[X]$:ssä ja R on kokonaisalue, myös P:n ja Q on oltava vakiopolynomit, eli $P = p \in R$. Toisaalta

$$X = Qp \text{ jollakin } Q \in R[X],$$

mistä seuraa, että $Q = aX + b$ on 1:n asteen polynomi ja $ap = 1$. Näin ollen p on yksikkö R:ssä, joten se on kääntyvä myös $R[X]$:ssä ja sen virittämä ideaali I on itse asiassa koko rengas $R[X]$. Erityisesti siis $1 \in I = \langle X, c\rangle$, joten on olemassa polynomit P, Q, joille

$$1 = XP + cQ.$$

Tarkastelemalla taas molempien puolien vakiokertomia nähdään, että

$$1 = cq_0,$$

eli c on kääntyvä. Saadaan ristiriitä oletuksen kanssa.

c) Väite pätee itse asiassa mielivaltaiselle kokonaisalueelle R. Samalla tavalla kuin kohdassa a) nähdään yleisesti, että

$$R[X_1, \ldots, X_n] \approx R[X_1, \ldots X_{n-1}][X_n]$$

R-agebroina. Koska $R[X]$ on kokonaisalue, tästä seuraa induktiolla, että myös $R[X_1, \ldots, X_n]$ on kokonaisalue. b)-kohdan nojalla riittää todeta, että $R[X_1, \ldots X_{n-1}]$ ei ole kunta. Tämä on

selvä, koska ainoat kääntyvät polynomit ovat vakiopolynomit.

3. Osoita, että jos F on kunta ja $f, g \in F[X]$ ja $\deg(g) \geq 1$, niin on olemassa yksikäsitteiset polynomit $f_0, f_1, \ldots, f_r \in F[X]$ s.e. $\deg(f_i) < \deg(g)$ kaikilla i ja

$$f = f_0 + f_1 g + f_2 g^2 \cdots + f_r g^r.$$

Ratkaisu: Jos f voidaan kirjoittaa muotoon $f = f_0 + f_1 g + f_2 g^2 \cdots + f_r g^r$, missä $\deg(f_i) < \deg(g)$ kaikilla i, niin

$$f = f_0 + gh, \text{ missä}$$
$$h = f_1 + f_2 g + \cdots + f_r g^{r-1}.$$

Koska vaaditaan, että $\deg(f_0) < \deg(g)$, niin jakoyhtälön (Lause 11.6) nojalla f_0 ja h ovat olemassa ja yksikäsitteiset. Näin ollen väite voi todistaa induktiolla f:n asteen suhteen. Jos $\deg f = 0$, niin valitaan $f_0 = f$ ja $h = 0$, jolloin yksikäsitteisyys seuraa jakoyhtälön nojalla.

Jos taas $\deg f > 0$ ja oletetaan, että väite pätee h:lle kun $\deg h < \deg f$, niin löydetään ensin f_0 ja h, siten että

$$f = f_0 + gh, \deg f_0 < \deg g.$$

Koska F on kokonaisalue ja $\deg g \geq 1$, niin pätee $\deg h < \deg f$. Induktioletuksesta seuraa, että h voidaan kirjoittaa muotoon

$$h = f_1 + f_2 g + \cdots + f_r g^{r-1},$$

missä $\deg f_i < \deg g$ kaikilla $i = 1, \ldots, r$ yksikäsitteisellä tavalla. Tällöin

$$f = f_0 + g(f_1 + f_2 g + \cdots + f_r g^{r-1}) = f_0 + f_1 g + f_2 g^2 \cdots + f_r g^r,$$

missä f_i:t yksikäsitteisiä, sillä h yksikäsitteinen ja induktio-oletus pätee h:lle.

4. Osoita, että Eukleideen rengas on pääideaalirengas.

Ratkaisu: Olkoon R Eukleideen rengas ja $\varepsilon\colon R \setminus \{0\} \to \mathbb{N}$ sen Eukleideen kuvaus.
Olkoon I R:n ideaali. Jos $I = \{0\}$, I on pääideaali. Muuten valitaan $x \in I \setminus \{0\}$ jolla on I:n alkioista pienin arvo $\varepsilon(x)$. Tällöin selvästi $\langle x \rangle \subset I$. Osoitetaan, että $I \subset \langle x \rangle$. Olkoon $y \in I$. Tällöin

$$y = ax + r,$$

missä $a \in R$ ja $r \in R$ sellainen, että $r = 0$ tai $\varepsilon r < \varepsilon x$. Toisaalta

$$r = y - ax \in I,$$

sillä I on ideaali. Koska x on valittu niin, että sillä on pienin arvo $\varepsilon(x)$ joukossa $I \setminus \{0\}$, niin vaihtoehto $\varepsilon r < \varepsilon x$ johtaa ristiriitaan. Näin ollen $r = 0$, joten $y = ax \in \langle x \rangle$.

5. Olkoon A kokonaisalue ja $P = A\setminus\{0\}$.
   (a) Osoita, että
   $$xA^* \leq yA^* \Leftrightarrow x|y$$
   on hyvinmääritelty järjestysrelaatio tekijämonoidissa P/A^*.
   (b) Olkoon E järjestetyn joukon P/A^* epätyhjä osajoukko. Osoita, että mikäli E:ssä ei ole minimaalista alkiota, niin P:ssä on sellainen jono $(x_n)_{n\in\mathbb{N}}$, että $x_{n+1}|x_n$ ja $x_n \not| x_{n+1}$ kaikilla $n \in \mathbb{N}$.

Ratkaisu: Huomataan, että $xA^* = yA^*$ jos ja vain jos $x = ya$ jollakin $a \in A^*$. Harj. 9 teht 5.a) sanoo, että tämä on totta, jos ja vain jos x ja y ovat liittoalkiot eli $x|y$ ja $y|x$.

Oletetaan, että $xA^* = x'A^*$ ja $yA^* = y'A^*$. Oletetaan myös, että $x|y$. Tällöin $x'|x$, $x|y$ ja $y|y'$, joten järjestysrelaation $|$ transitiivisuuden nojalla $x'|y'$.
Näin ollen tekijärelaatio $\leq$ on hyvinmääritelty. Sen transitiivisuus ja refleksiivisyys seuraavat | vastaavista ominaisuuksista. Osoitetaan vielä anti-symmetrisyys. Oletetaan, että $xA^* \leq yA^*$ ja $yA^* \leq xA^*$. Tällöin $x|y$ ja $y|x$, joten x ja y ovat toistensa liittoalkiot joten $xA^* = yA^*$.

b) Jono x_n konstruoidaan induktiolla n:n suhteen siten että $x_nA^* \in E$ kaikilla $n \in \mathbb{N}$. Alkio x_0 valitaan mielivaltaisesti.
Oletetaan, että x_n on valittu. Tällöin x_nA^* ei ole E:n minimaalinen alkio, joten on olemassa $x_{n+1}A^* \in E$ jolle $yA^* < x_nA^*$, jolloin $x_{n+1} \not| x_n$ ja $x_{n+1}|x_n$.

6. Olkoon A tekijöihinjakorengas ja $x, y \in A\setminus\{0\}$ keskenään jaottomat. Osoita:
   (a) Jos $z \in A\setminus\{0\}$, $x|z$ ja $y|z$, niin $xy|z$ eli xy on x:n ja y:n pienin yhteinen kerrannainen.
   (b) Jos $z \in A\setminus\{0\}$ ja $x|yz$, niin $x|z$.

Ratkaisu: a) Olkoot

$$x = p_1 p_2 \cdots p_k,$$

$$y = q_1 q_2 \cdots q_l$$

alkulukuhajotelmat. Koska x ja y ovat keskenään jaottomat, p_i ei ole q_j:n liittoalkio millään $i = 1, \ldots, k$, $j = 1, \ldots, l$. Koska jako jaottomiin tekijöihon on oleellisesti yksikäsitteinen ja $x|z$, $y|z$, jokainen p_i ja q_j esiintyy z:n alkulukuhajotelmassa. Näin ollen

$$xy = p_1 p_2 \cdots p_k q_1 q_2 \cdots q_l | z.$$

b) Nyt $x|yz$ ja $y|yz$, joten a)-kohdan nojalla $xy|yz$. Supistamalla y saadaan $x|z$.