Matematiikan laitos
AlgebraII
Harjoitus 6
22.06.2011
Ratkaisuehdotuksia
Aleksandr Pasharin

1. Olkoon R vaihdannainen rengas. Osoita, että joukon X virittämä ideaali on
$$\langle X \rangle = \{\sum_{i \in I} a_i x_i : I \text{ äärellinen }, a_i \in R, x_i \in X\}.$$

   Ratkaisu: Merkitään
$$A = \{\sum_{i \in I} a_i x_i : I \text{ äärellinen }, a_i \in R, x_i \in X\}.$$
   Kun valitaan I:ksi yhden alkio joukon $\{1\}$, $a_1 = 1$ ja $x_i \in X$ mielivaltaiseksi, nähdään, että
$$X \subset A.$$
   Jos X on epätyhjä, tästä jo seuraa, että A on epätyhjä. Jos taas X on tyhjä, niin palautetaan mieleen, että summa yli tyhjän joukon, joka on eräs äärellinen indeksijoukokko, tulkitaan nolla-alkioksi $0 \in R$. Näin olleen ainakin $0 \in A$. Jos
$$x = \sum_{i \in I} a_i x_i, y = \sum_{j \in J} b_j x_j \in A,$$
   niin
$$x - y = \sum_{k \in I \sqcup J} c_k x_k,$$
   missä $c_k = a_k$ kun $k \in I$, $c_k = -a_k$ kun $k \in J$ ja $I \sqcup J$ on erillinen yhdiste. Näin ollen $x - y \in A$. Jos $a \in R$, niin
$$rx = \sum_{i \in I} (ra_i) x_i \in A.$$
   Näin ollen A on ideaali, joka sisältää X:n.
   Jos B on mikä tahansa R:n ideaali ja $X \subset B$, niin B selvästi sisältää kaikki alkiot jotka ovat muotoa
$$\sum_{i \in I} a_i x_i,$$
   missä $a_i \in R$ ja $x_i \in X$. Näin ollen $A \subset B$. Siis A on pienin ideaali joka sisältää X:n.

2. Olkoon R vaihdannainen rengas ja A sen ideaali. Osoita:
   (a) A on alkuideaali, jos ja vain jos R/A on kokonaisalue.

(b) A on maksimaalinen, jos ja vain jos R/A on kunta.

Ratkaisu: Olkoon A ideaali. Tällöin R/A on kokonaisalue jos ja vain jos kaikilla xA, yA jotka eivät ole nollaalkio R/A:ssä pätee $(xA)\cdot(yA) = xyA \neq 0$. Tämä voidaan ilmaista myös muodossa jos $x, y \notin A$ niin myös $xy \notin A$. Yhtäpitävästi R/A on kokonaisalue jos ja vain jos $xy \in A$ implikoi, että $x \in A$ tai $y \in A$. Siis R/A on kokonaisalue jos ja vain jos A on alkuideaali.

Osoitetaan seuraavaksi, että A on maksimaalinen jos ja vain jos R/A on kunta. Olkoon $x \notin A$. Tehtävästä 1 seuraa, että A:n ja x:n virittämä ideaali $A[x]$ voidaan esittää muodossa

$$A[x] = \{rx + a : r \in R, a \in A\},$$

koska A on ideaali. A on maksimaalinen jos ja vain jos $A \neq R$, mutta $A[x] = R$ jokaisella $x \notin A$, mikä on yhtäpitävä sen kanssa, että $1 \in A[x]$. Siis $A \neq R$ on maksimaalinen jos ja vain jos jokaisella $x \notin A$ on olemassa $r \in R, a \in A$ joille

$$1 = rx + a.$$

Jos tämä toteutuu niin R/A:ssä toteuttuu $\bar{r}\bar{x} = \bar{1}$, eli jokaisella nollasta eroavalla alkiolla $\bar{x} = x + A$:llä on käänteisalkio R/A:llä eli R/A on kunta. Kääntäen jos jokaisella $x \notin A$ on olemassa $r \in R$ jolle $\bar{r}\bar{x} = \bar{1}$, niin on olemassa $a \in A$ jolle

$$rx = 1 + a,$$

joten $1 = rx - a \in A[x]$ ja $A[x] = R$. Siis A on maksimaalinen.

3. (Renkaiden homomorfialause). Olkoot A ja B renkaita ja olkoon $f : A \to B$ homomorfismi. Osoita:
   (a) f:n ydin on A:n kaksipuolinen ideaali,
   (b) f:n kuva on B:n alirengas,
   (c) f:n kanonisesta hajotelmasta

$$f : A \xrightarrow{\pi} A/\operatorname{Ker}(f) \xrightarrow{\bar{f}} \operatorname{Im}(f) \xrightarrow{j} B,$$

   missä π on kanoninen surjektio ja j kanoninen injektio, saadaan renkaiden isomorfismi

$$\bar{f} : A/\operatorname{Ker}(f) \xrightarrow{\cong} \operatorname{Im}(f).$$

Ratkaisu: Jos $f : A \to B$ on rengashomomorfismi, niin se on erityisesti Abelin ryhmien $(A, +)$ ja $(B, +)$ ryhmähomomorfismi. Näin ollen f:n ydin ja f:n kuva B:ssä ovat ainakin vastaavasti A:n ja B:n aliryhmät. Jos $a \in \operatorname{Ker}(f)$ ja $r \in R$ niin

$$f(rx) = f(r)f(x) = f(r)\cdot 0 = 0 = 0\cdot f(r) = f(x)f(r) = f(xr),$$

joten $rx, xr \in \operatorname{Ker}(f)$. Siis $\operatorname{Ker}(f)$ on kaksipuolinen ideaali ja tekijärengas $A/\operatorname{Ker}(f)$ on määritelty. Ryhmien isomorfialauseista saadaan, että indusoitu kuvaus $\bar{f} : A/\operatorname{Ker}(f) \to \operatorname{Im}(f)$ on ainakin ryhmien välinen isomorfismi. Koska

$$\bar{f}(1+A) = f(1) = 1 \text{ ja}$$

$$\bar{f}((x+A)(y+A)) = \bar{f}(xy+A) = f(xy) = f(x)f(y) = \bar{f}(x+A)\bar{f}(y+A)$$

se on jopa rengashomomorfismi.

Jäljelle jää osoittaa, että $\operatorname{Im}(f)$ on B:n alirengas. $1 \in \operatorname{Im}(f)$ koska

$$f(1) = 1.$$

Jos $b = f(x), c = f(y)$, niin

$$bc = f(xy) \in \operatorname{Im}(B).$$

Koska yllä on jo todettu, että $\operatorname{Im}(f)$ on additiivinen aliryhmä, väite seuraa.

4. Olkoon R vaihdannainen rengas ja $S^{-1}R$ sen jakorengas osajoukon S suhteen. Todista seuraavat väitteet:
   (a) $S^{-1}R$ on vaihdannainen rengas, laskutoimituksina $a/b \cdot c/d = (ac)/(bd)$ ja $a/b + c/d = (ad + bc)/(bd)$.
   (b) Kanoninen kuvaus $\eta : a \mapsto a/1$ on rengashomomorfismi.
   (c) Jos $s \in S$, kuva-alkiolla $\eta(s) \in S^{-1}R$ on käänteisalkio.
   (d) Kanoninen kuvaus η on injektio, jos ja vain jos S ei sisällä nollanjakajia.
   (e) $S^{-1}R$ on nollarengas, jos ja vain jos $0 \in S$.

Ratkaisu: a)Palautetaan ensin mielen $S^{-1}R$:n konstruktion. Oletetaan, että S sisältää yksikön 1 ja on suljettu kertolaskun suhteen. Joukkona $S^{-1}R$ on $R \times S/\sim$, missä $\sim$ on ekvivalenssirelaatio, joka on määritelty seuraavasti,

$$(a, b) \sim (c, d) \text{ joss } s(ad - bc) = 0 \text{ jollakin } s \in S.$$

Todetaan ensin, että tämä tosiaankin on ekvivalenssirelaatio. Pari (a, b) on relaatiossa itseensä kanssa, koska $1 \cdot (ab - ab) = 0$. Jos $s(ad - bc) = 0$, niin $s(cb - da) = 0$, joten relaatio on myös symmetrinen. Oletetaan, että $(a, b) \sim (c, d)$ ja $(c, d) \sim (e, f)$. Tällöin on olemassa $s, s' \in S$ siten, että

$$sad = sbc,$$

$$s'cf = s'de.$$

Tällöin

$$(ss'd)(af - be) = (ss')(adf - bde) = ss'(bcf - bdf) = 0,$$

joten $(a,b) \sim (e,f)$, sillä $ss'd \in S$.
Parin (a,b) ekvivalenssiluokalle käytetään yleensä merkintä a/b, selkeyden vuoksi käytetään tässä tehtävässä myös merkintä $[a,b]$.
Osoitetaan ensin, että a)-kohdassa annetun laskutoimitukset ovat hyvin määriteltyjä, eli yhteensopivia ekvivalenssirelaation $\sim$ kanssa. Oletetaan, että $(a,b) \sim (a',b')$ ja $(c,d) \sim (c',d')$. Tällöin on olemassa $s, s' \in S$ siten että

$$s(ab' - a'b) = 0 = s'(cd' - c'd).$$

Tällöin siis

$$sab' = sa'b \text{ ja } s'cd' = s'c'd.$$

Nyt

$$ss'(ac)(b'd') = s(ab')s'(cd') = (sa'b)(s'c'd) = ss'(a'c')(bd),$$

$$ss'(ad+bc)(b'd') = s'(s(ab'))(dd')+s(bb')(s'(cd')) = s'(sa'b)(dd')+s(bb')(s'c'd) = ss'(a'd'+b'c')(bd).$$

Koska $ss' \in S$, niin

$$(ac, bd) \sim (a'c', b'd')$$

ja

$$(ad + bc, bd) \sim (a'd' + b'c', b'd').$$

Näin ollen laskutoimitukset ovat hyvin määriteltyjä $S^{-1}R$:ssä.
Osoitetaan seuraavaksi, että $(S^{-1}R, +, \cdot)$ on vaihdannainen rengas. Olkoot $a, c, e \in R, b, d, f \in S$. Laskemalla saadaan

$$([a,b]+[c,d])+[e,f] = [ad+bc, bd]+[e,f] = [(ad+bc)f+bde, (bd)f] = [a(df)+b(cf+de), b(df)] =$$

$$= [a,b] + [cf + de, df] = [a,b] + ([c,d] + [e,f]),$$

$$[a,b] + [c,d] = [ad + bc, bd] = [cb + da, db] = [c,d] + [a,b],$$

$$[0,1] + [a,b] = [0b + 1a, 1b] = [a,b] = [a,b] + [0,1],$$

$$[a,b] + [-a,b] = [ab + (-a)b, bb] = [ab - ab, bb] = [0, bb] = [0,1],$$

sillä

$$0 \cdot 1 = 0 \cdot bb,$$

joten

$$(0, bb) \sim (0,1).$$

Näin ollen $(S^{-1}R, +)$ on vaihdannainen ryhmä, neutraalialkiona $[0,1]$. Alkion $[a,b]$ vasta-alkio on $[-a,b]$.

Seuraavaksi tutkitaan kertolaskua. Laskemalla saadaan

$$([a,b]\cdot[c,d])\cdot[e,f] = [ac,bd]\cdot[e,f] = [(ac)e,(bd)f] = [a(ce),b(df)] = [a,b]\cdot[ce,df] = [a,b]\cdot([c,d]\cdot[e,f]$$

$$[a,b] \cdot [c,d] = [ac, bd] = [ca, db] = [c,d] \cdot [a,b],$$

$$[a,b] \cdot [1,1] = [a1, b1] = [a,b] = [1,1] \cdot [a,b].$$

Siis $(R, \cdot)$ on vaihdannainen monoidi, neutraalialkiona $[1, 1]$.
Jäljellä on osittelulait. Koska kertolasku on vaihdannainen riittää todistaa vain toinen osittelulaista. Ensin huomataan, että kaikilla $s \in S$ pätee

$$[as, bs] = [a, b].$$

Tämä seuraa siitä, että $(as)b = (bs)a$. Lasketaan

$$([a, b]+[c, d])\cdot[e, f] = [ad+bc, bd]\cdot[e, f] = [(ad+bc)e, (bd)f] = [(ad+bc)ef, (bd)ff] =$$

$$[(ae)(df)+(bf)(ce), (bf)(df)] = [ae, bf]+[ce, df] = [a, b]\cdot[e, f]+[c, d]\cdot[e, f].$$

b) Kanoninen kuvaus $\eta : a \mapsto a/1$ on rengashomomorfismi:

$$\eta(a) + \eta(b) = a/1 + b/1 = (a \cdot 1 + b \cdot 1)/(1 \cdot 1) = (a + b)/1 = \eta(a + b),$$

$$\eta(a)\eta(b) = a/1 \cdot b/1 = (ab)/(11) = (ab)/1 = \eta(ab),$$

$$\eta(1) = 1/1 = [1, 1],$$

joka on $S^{-1}R$:n kertolaskun neutraalialkio.

c) Olkoon $s \in S$. Tällöin

$$s/1 \cdot 1/s = s/s = 1/1 = 1.$$

d) Oletetaan, että S sisältää nollanjakajan. Tällöin on olemassa $s \in S$ ja $a \in R, a \neq 0$ joille $sa = 0$. Tämä voidaan kirjoittaa muotoon

$$s(a \cdot 1 - 0 \cdot 1) = 0,$$

josta nähdään, että $(a, 1) \sim (0, 1)$, joten

$$\eta(a) = a/1 = 0/1 = \eta(0),$$

vaikka $a \neq 0$. Siis η ei ole injektio.
Oletetaan, että S ei sisällä nollanjakaija. Olkoot $a, b \in R$ joille $\eta(a) = \eta(b)$. Tällöin siis

$$[a, 1] = [b, 1]$$

eli on olemassa $s \in S$ siten, että $s(a\cdot 1-b\cdot 1) = 0$ eli $s(a-b) = 0$. Koska s ei ole nollanjakaja on oltava $a - b = 0$ eli $a = b$. Siis η on injektio.

e)$S^{-1}R$ on nollarengas jos ja vain jos se nollaalkio ja yksikköalkio ovat sama alkio eli jos ja vain jos

$$[1, 1] = [0, 1].$$

Tämä taas toteuttuu jos ja vain jos on olemassa $s \in S$ jolle pätee $s(1 \cdot 1 - 0 \cdot 1) = 0$ eli jos ja vain jos on olemassa $s \in S$ jolle $s = 0$. Siis $S^{-1}R$ on nollarengas jos ja vain jos se sisältää nollan.

5. Tarkastellaan polynomien $f = X^4 - 1$ ja $g = X^3 + X$ virittämää ideaalia polynomirenkaassa $\mathbb{Z}[X]$.
   (a) Etsi jokin $h \in \mathbb{Z}[X]$, jolle pätee $\langle h \rangle = \langle f, g \rangle$.
   (b) Osoita, että tekijärenkaassa $\mathbb{Z}[X]/\langle f, g \rangle$ on alkio a, jolle pätee $a^2 = -1$.

Ratkaisu: a) Jaetaan ensin polynomit f ja g jaottomiin tekijöihin polynomirenkaassa $\mathbb{Z}[X]$,

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

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

Nähdään, että ainoa yhteinen tekijä on polynomi $h = X^2 + 1$, joka on silloin siis f:n ja g:n suurin yhteinen tekijä (eli *syt*) $\mathbb{Z}[X]$:ssä. Yleisestä jaollisuusteoriasta silloin seuraa, että h:n virittämä ideaali on sama kuin f:n ja g:n yhdessä virittämä ideaali. Tämä voidaan nähdä myös suoraan nojauttumatta jaollisuusteorian tuloksiin seuraavasti. Ensinnäkin h on f:n ja g:n tekijä, eli $f = ah$, $g = bh$ joillakin $a, b \in \mathbb{Z}[X]$ (yllä laskettiin, että itse asiassa $a = X^2 - 1$ ja $b = X$).Tästä seuraa, että $f, g \in \langle h \rangle$, joten myös

$$\langle f, g \rangle \subset \langle h \rangle.$$

Toisaalta h voidaan esittää muodossa $xf + yg$, sillä

$$f = (X^2 - 1)h = X^2 h - h = (Xh)g - h, \text{ joten}$$

$$h = (Xh)g + (-1)f.$$

Tämä meinaa sitä, että $h \in \langle f, g \rangle$, joten

$$\langle h \rangle \subset \langle f, g \rangle.$$

b) Olkoon $a = \bar{X}$ alkion X luokka tekijärenkaassa $\mathbb{Z}[X]/\langle f, g \rangle$. Koska $X^2 + 1 = h$ tekijärenkaassa saadaan

$$a^2 + 1 = \bar{h} = 0.$$

Näin ollen $a^2 = -1$.

6. Olkoon R rengas, jolla on ideaali A ja alirengas S. Todista seuraavat väitteet:
   (a) Jokainen R/A-moduli on myös R-moduli, mutta kaikki R-modulit eivät ole R/A-moduleja.
   (b) Jokainen R-moduli on myös S-moduli, mutta kaikki S-modulit eivät ole R-moduleja.

Ratkaisu: a) Olkoon M R/A moduli. Tällöin M:stä tulee R-moduli luonnollisella tavalla, kun määritellään

$$ra = (r + A)a$$

jokaisella $r \in R, a \in A$. Näin ollen jokainen R/A moduli on myös R-moduli. Käänteinen ei päde - esimerkiksi olkoot $R = \mathbb{Z}$, $A = n\mathbb{Z}$, $n > 0$. Tällöin R-modulit ovat täsmälleen vaihdannaiset ryhmät kun taas R/A modulit ovat sellaiset vaihdannaiset ryhmät G, joissa jokaisella alkiolla $x \in G$ pätee

$$nx = 0$$

(kts. esimerkit sivuilla 54-55). Näin ollen esimerkiksi ryhmä $(\mathbb{Z}, +)$ on $\mathbb{Z}$-moduli, mutta se ei voi olla $\mathbb{Z}_n$-moduli millään $n > 0$.

b) Olkoon M R-moduli. Tällöin rajoittumalla R:n toiminta alirenkaan S saadaan M:ssä määriteltyä S-modulin struktuurin. Käänteinen ei päde - olkoot esimerkiksi $R = \mathbb{Q}, S = \mathbb{Z}$. Tällöin mikä tahansa vaihdannainen ryhmä on S-moduli. Tutkitaan milloin vaihdannainen ryhmä $(G, +)$ on $\mathbb{Q}$-moduli. Jos G:ssä on määritely $\mathbb{Q}$:n toiminta, joka tekee siitä $\mathbb{Q}$-modulin, niin erityisesti jokaisella alkiolla $x \in G$ ja jokaisella $n \in \mathbb{N}$ G:ssä on olemassa alkio

$$y = \frac{1}{n}x,$$

jolle pätee $ny = x$. Jos käytetään multiplikaativista merkintä G:ssä, niin tämä voidaan myös ilmaista sanomalla, että jokaisella alkiolla on olemassa n:s juuri kaikilla $n \in \mathbb{N}$. Tällaisia ryhmiä sanotaan jaollisiksi ryhmiksi (engl. divisible group). Koska kaikki Abelin ryhmät selvästi eivät ole jaollisia, tästä saadaan esimerkkejä $\mathbb{Z}$-moduleista jotka eivät voi olla $\mathbb{Q}$-moduleita.