Matematiikan laitos
AlgebraII
Harjoitus 9
01.04.2011
Ratkaisuehdotuksia
Aleksandr Pasharin

1. Algebraa kutsutaan *äärellisviritteiseksi*, jos se sisältää sellaisen äärellisen osajoukon $X = \{x_1, \ldots, x_n\}$, että jokainen algebran alkio voidaan kirjoittaa lineaarikombinaatioina joukon X alkioiden äärellisistä tuloista. Osoita, että jokainen äärellisviritteinen ykkösellinen, liitännäinen ja vaihdannainen R-algebra on isomorfinen jonkin R-kertoimisen polynomialgebran tekijäalgebran kanssa.

   Ratkaisu: Olkoon A äärellisviritteinen, ykkösellinen, liitännäinen ja vaihdannainen R-algebra. Olkoon $X = \{x_1, \ldots, x_n\}$ sen äärellinen virittäjäjoukko. Lauseen 9.11 (Polynomialgebran universaaliominaisuus) nojalla on olemassa (yksikäsitteinen) R-algebrahomomorfismi $\varphi\colon R[X_1, \ldots, x_n] \to A$ jolle pätee $\varphi(X_i) = x_i$ kaikilla $i = 1, \ldots, n$. Kuvajoukko $\varphi(R[X_1, \ldots, x_n])$ on A:n alialgebra, joka sisältää joukon X. Koska se on alialgebra se sisältää kaikki X:n alkioiden muodostamat (äärelliset) tulot ja samasta syystä vastaavasti kaikkien sellaisten lineaariset kombinaatiot. Näin ollen se on koko algebra A, eli φ on surjektio. Tästä seuraa, että φ määrää algebraisomorfismin

   $$R[X_1, \ldots, x_n]/\operatorname{Ker}(\varphi) \approx A.$$

2. Olkoon A vaihdannainen rengas. Olkoot $u \in A[X]$ ja $v \in A[Y]$ polynomeja sekä $w = u(v) \in A[Y]$. Olkoon B jokin ykkösellinen, liitännäinen ja vaihdannainen A-algebra ja $y \in B$. Osoita, että $w(y) = u(v(y))$.

   Ratkaisu: Lauseen 9.11 nojalla on olemassa yksikäsitteiset A-algebrahomomorfismit $f\colon A[X] \to A[Y]$ ja $g\colon A[Y] \to B$, joille $f(X) = v$ ja $g(Y) = y$. Määritelmän mukaan $w = u(v) = f(u)$, $w(y) = g(w)$ ja $v(y) = g(v)$.
   Tarkastellaan A-algebrahomomorfismi $h = g \circ f\colon A[X] \to B$. Tällöin $h(X) = g(f(X)) = g(v) = v(y)$ ja se on ainoa A-algebrahomomorfismi $h\colon A[X] \to B$ jolla on tämä on ominaisuus. Nyt

   $$w(y) = g(w) = g(f(u)) = h(u) = u(v(y)).$$

3. Olkoon A vaihdannainen rengas. Olkoon $u \circ v = u(v)$, kun $u, v \in A[X]$. Osoita, että $(u \circ v) \circ w = u \circ (v \circ w)$ kaikilla $u, v, w \in A[X]$.

   Ratkaisu: Sovelletaan tehtävän 2 tulosta tapauksessa $X = Y$, $B = A[X]$, $y = w$. Merkitään $z = u(v) = u \circ v \in A[X]$. Saadaan

   $$(u \circ v) \circ w = z(w) = u(v(w)) = u(v \circ w) = u \circ (v \circ w).$$

   Huomautus: Operaatio $\circ$ on formaali algebrallinen versio polynomien yhdistämisestä kun ne ajatellaan polynomikuvauksina.

4. Näytä, että kokonaisalueella A polynomialgebran $A[X]$ kaikki automorfismit (eli A-isomorfismit $f : A[X] \to A[X]$) ovat sijoitushomomorfismeja $P \mapsto P(\lambda X + \mu)$, missä $\lambda \in A^*$, $\mu \in A$.

   Ratkaisu: Olkoon $f\colon A[X] \to A[X]$ A-automorfismi. Olkoon $Q = f(X)$ ja $n = \deg Q$. Koska A on kokonaisalue jokaisella $m \in \mathbb{N}$ pätee

   $$\deg f(X^m) = \deg Q^m = m \deg Q = mn.$$

   Tästä seuraa, että m-asteisen polynomin $P \in A[X]$ kuva $f(P)$ on mn-asteinen polynomi. Jos $n = 0$ $f(A[X]) \subset A$ koostuu vain 0-asteisista polynomeista, joten f ei voi olla surjektio. Jos taas $n > 1$, niin 0-asteiset polynomit kuvautuu 0-asteisiksi joka tapauksessa ja kun $m \geq 1$ m-asteinen polynomi kuvautuu polynomiksi, jonka aste on $mn > m \leq 1$. Näin ollen $f(A[X])$ ei voi sisältää 1-asteisia polynomia, mikä on taas mahdotonta, sillä f on surjektio. Näin ollen $m = 1$ eli

   $$f(X) = \lambda X + \mu, \lambda, \mu \in A, \lambda \neq 0.$$

   Olkoon $g\colon A[X] \to A[X]$ f:n käänteiskuvaus. Tällöin g on myös A-automorfismi, joten yllä todistetun nojalla

   $$g(X) = \lambda' X + \mu', \lambda', \mu' \in A, \lambda' \neq 0.$$

   Tällöin

   $$X = g(f(X)) = g(\lambda X + \mu) = \lambda g(X) + \mu = \lambda(\lambda' X + \mu') + \mu = \\ = (\lambda\lambda')X + (\lambda\mu' + \mu),$$

   josta erityisesti seuraa, että

   $$1 = \lambda\lambda' = \lambda'\lambda,$$

   joten $\lambda \in A^*$.

   Kääntäen helposti nähdään, että ehdolla $f(X) = \lambda X + \mu$, $\lambda \in A^*$, $\mu \in A$ määritely yksikäsitteinen A-algebrahomomorfismi $A[X] \to A[X]$ on isomorfismi, sillä A-algebrahomomorfismille

$g\colon A[X] \to A[X]$, joka on määritely ehdolla $g(X) = \lambda^{-1}(X - \mu)$ on f:n käänteiskuvaus.

5. Oletetaan, että R on kokonaisalue. Todista seuraavat väitteet:
   (a) Alkiot $a, b \in R$ ovat liittoalkioita, jos ja vain jos $a = bc$ jollakin yksiköllä $c \in R$.
   (b) Jos $a, b \in R \setminus \{0\}$ ovat liittoalkioita ja $a = bc$, niin c on yksikkö.
   (c) Kaikki yksiköt ovat toistensa liittoalkioita.

   Ratkaisu: Oletetaan, että a ja b ovat toistensa liittoalkiot, eli $a|b$ ja $b|a$. Tällöin on olemassa $c, d \in R$ joille

   $$a = bc \text{ ja } b = ad.$$

   Tästä saadaan $b = ad = b(cd)$. Jos $b = 0$, niin myös $a = bc = 0$, joten $a = bc$ kun valitaan esim. $c = 1$, joka on yksikkö. Muuten supistamalla b (tämä on mahdollista, sillä R on kokonaisalue) saadaan $cd = 1$, mistä seuraa, että c on yksikkö. a)-kohdan toinen suunta ja b)-kohta on todistettu.

   Kääntäen oletetaan, että $a = bc$ jollakin yksiköllä $c \in R$. Tällöin selvästi $b|a$, toisaalta kertomalla c:n käänteisalkiolla saadaan $ac^{-1} = b$, mistä seuraa, että $a|b$. Siis a ja b ovat toistensa liittoalkiot.

   Jos a ja b ovat yksiköt, niin myös $c = b^{-1}a$ on yksikkö. Koska $a = bc$ a)-kohdan perusteella a ja b ovat toistensa liittoalkiot.

6. Olkoon R pääideaalirengas ja $0 \neq a \in R$. Osoita, että seuraavat ehdot ovat yhtäpitävät:
   (a) a on alkualkio.
   (b) a on jaoton.
   (c) $\langle a \rangle$ on maksimaalinen ideaali.

   Ratkaisu: Lauseen 11.4 nojalla jokainen alkualkio on jaoton alkio itse asiassa mielivaltaisessa kokonaisalueessa.

   Olkoon a jaoton alkio. Sen virittämä ideaali on

   $$I = \langle a \rangle = \{ar | r \in R\}.$$

   Jos $I = R$, niin erityisesti $1 \in I$, josta seuraa, että on olemassa $r \in R$ jolle $ar = 1$. Tämä on mahdotonta, sillä jokainen jaoton alkio ei ole yksikkö. Näin ollen I on R:n aito ideaali. Oletetaan, että J on ideaali ja $I \subset J$. Riittää osoittaa, että $J = I$ tai $J = R$. Koska R on pääideaalirengas J on yhden alkion virittämä, eli on olemassa $b \in R$ jolle pätee

$$J = \langle b \rangle = \{br | r \in R\}.$$

Koska $I \subset J$ niin erityisesti on olemassa $r \in R$ jolle $a = rb$. Erityisesti b on a:n tekijä. Koska a on jaoton, b on yksikkö tai a:n liittoalkio. Edellisessä tapauksessa $J = R$, jälkimmäisessä $J = I$. Siis I on maksimaalinen.

Oletetaan, että

$$I = \langle a \rangle = \{ar | r \in R\}$$

on maksimaalinen ideaali. Osoitetaan, että a on alkualkio. Oletetaan, että $a|bc$ ja osoitetaan että $a|b$ tai $a|c$. Olkoon

$$J = \langle a, b \rangle = \{ar + bs | r, s \in R\}$$

alkioiden a ja b virittämä ideaali. Pätee $I \subset J$. Koska I on maksimaalinen, niin $J = I$ tai $J = R$. Jos $J = I$, niin erityisesti $b \in I$, jolloin $a|b$. Jos taas $J = R$, niin erityisesti $1 \in J$, jolloin on olemassa $r, s \in R$ joille

$$1 = ra + sb.$$

Tästä saadaan

$$c = c \cdot 1 = c(ra + sb) = a(rc) + s(bc) = a(rc + sd),$$

missä $d \in R$ sellainen, että $ad = bc$ (olemassa, koska $a|bc$). Näin ollen $a|c$.

Siis a on alkualkio.