Matematiikan ja tilastotieteen laitos
Algebra I
Harjoitus 10, 6.–8.4. ja 16.–17.4.2009
Teri Soultanis, 4 sivua

1. Olkoot I ja J renkaan R ideaaleja. Osoita, että myös

$$I + J = \{a + b \mid a \in I,\, b \in J\}$$

on R:n ideaali.

Ratk. Koska $0 = 0+0 \in I+J$, niin $I+J \neq \emptyset$. Jos $a = i+j \in I+J$, niin $-a = (-i)+(-j) \in I+J$, koska I ja J ovat ideaaleja. Samoin, jos $a_1 = i_1+j_1 \in I+J$ ja $a_2 = i_2+j_2 \in I+J$, niin $a_1+a_2 = (i_1+j_1)+(i_2+j_2) = (i_1+i_2)+(j_1+j_2) \in I+J$. Olkoon sitten $a = i+j \in I+J$ ja $r \in R$. Nyt $ra = r(i+j) = ri+rj \in I+J$. Samoin $ar = (i+j)r = ir+jr \in I+J$.
Nämä seikat yhdessä todistavat $I+J$:n R:n ideaaliksi.

2. (Kompleksilukuja osaaville tai "kompleksilukujen pikakurssi".) Olkoon $R = \{m+ni \mid m,n \in \mathbb{Z}\} \subset \mathbb{C}$ Gaussin kokonaislukujen joukko (i imaginääriyksikkö, $i^2 = -1$).
a) Osoita, että R on kompleksilukujen renkaan $\mathbb{C}$ alirengas.
b) Osoita, että R on pääideaalirengas eli että sen jokainen ideaali on muotoa $\langle a \rangle = Ra$ jollain $a \in R$. *Ohje.* Olkoon $I \neq \{0\}$ renkaan R ideaali. Lukujen $m+ni \in I \setminus \{0\}$ itseisarvojen $|m+ni| = \sqrt{m^2+n^2} > 0$ joukossa on selvästikin pienin eli jokin joukon $I \setminus \{0\}$ alkio a on lähimpänä origoa. Osoita, että joukko Ra on kompleksitason erään neliöverkon kärkien joukko (piirrä!). Osoita, että jos $z \in I \setminus Ra$, niin on olemassa $b \in Ra$, jolla $|b-z| < |a|$, ja johda tästä ristiriita.

Ratk.
a) Näytetään ensin, että R on $\mathbb{C}$:n aliryhmä yhteenlaskun suhteen. Selvästi $0 = 0+0i \in R$. Jos $a = n+mi \in R$ ja $b = x+yi \in R$ (eli $n,m,x,y \in \mathbb{N}$), niin $a-b = n+mi-x-yi = (n-x)+(m-y)i \in R$. Tämä todistaa R:n aliryhmäksi yhteenlaskun suhteen.
Näytetään vielä, että R on vakaa kertolaskun suhteen. Olkoot taas $a = n+mi$ ja $b = x+yi$ R:n alkioita. Silloin $ab = (n+mi)(x+yi) = nx-my+i(ny+mx) \in R$. Lisäksi $\mathbb{C}$:n ykkösalkiolle 1 on $1 = 1+0i \in R$. Siis R on $\mathbb{C}$:n alirengas.
b) Olkoon $\{0\} \neq I$ R:n ideaali. Vihjeen mukaisesti löydämme $I \setminus \{0\}$:n alkion $a = a_1 + a_2 i$, joka minimoi etäisyyden origoon. Tulemme todistamaan, että $I = Ra$, $Ra = \{ra : r \in R\}$. Koska

$$Ra = \{(n+mi)(a_1+a_2i) : n,m \in \mathbb{Z}\} = \{n(a_1+a_2i)+m(-a_2+a_1i) : n,m \in \mathbb{Z}\},$$

joukkoa Ra voidaan ajatella (toisiaan vastassa kohtisuorassa olevien!) vektoreiden (a_1,a_2) ja $(-a_2,a_1)$ kokonaislukukertoimisten lineaarikombinaatioiden joukkona. Kuvasta näemme selvästi, että tämä on ruudukko neliöiden kärkipisteitä; näiden neliöiden sivun pituus on $|a|$. Jos $z \in I \setminus Ra$, niin z on jonkin tällaisen neliön sisällä ja silloin sitä lähimmän kärkipisteen $b \in Ra \subset I$ etäisyys on korkeintaan $|b-z| \leq (\sqrt{2}/2)|a| < |a|$. Kuitenkin $b-z \in I$, ja koska a minimoi etäisyyden origoon $I \setminus \{0\}$:n alkioiden joukossa, on oltava $b-z = 0$, joka on ristiriita, sillä $b \in Ra$, mutta $z \notin Ra$. Tämä tarkoittaa, että $I = Ra = \langle a \rangle$.

3.
a) Määritä renkaan $\mathbb{Z}$ ideaali $\langle 693, 714, 1925\rangle$ eli etsi sille virittäjä.
b) Laske Eulerin φ-funktion arvo $\varphi(60)$.

Ratk.
a) Huomataan aluksi, että $\operatorname{syt}(693, 714, 1925) = 7$ ($693 = 3^2 \cdot 7 \cdot 11, 714 = 2 \cdot 3 \cdot 7 \cdot 17$ ja $1925 = 5^2 \cdot 7 \cdot 11$). Siis $\langle 693, 714, 1925\rangle = \langle 7\rangle$.

b) Käytetään luentojen s. 91 kaavaa

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right),$$

jossa $n = p_1^{s_1} \cdots p_k^{s_k}$ on n:n alkutekijähajotelma.
Nyt $60 = 2^2 \cdot 3 \cdot 5$, joten $\varphi(60) = 60 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 16$.

4. Olkoon R kokonaisalue, jonka karakteristika $p = \operatorname{char}(R)$ on positiivinen. Osoita, että kuvaus $f\colon R \to R$, jolla $f(a) = a^p$ kaikilla $a \in R$, on injektiivinen rengashomomorfismi (summan säilyvyydestä ks. luennot). Mikä kuvaus f on, jos $R = \mathbb{Z}_p$?

Ratk. Olkoot $a, b \in R$. Nyt

$$f(a+b) = (a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}.$$

Kuitenkin, jos $0 < k < p$, niin p jakaa $\binom{p}{k}$:n ja silloin (kokonaisalueen karakteristikan määritelmän mukaan) tätä vastaava termi häviää. Jäljelle jäävät siis termit $k = 0$ ja $k = p$, joten

$$f(a+b) = (a+b)^p = a^p + b^p = f(a) + f(b).$$

(Tämä on siis s. 93 kaava, jonka todistus on kertauksen vuoksi lisätty ratkaisuun.) Lisäksi kokonaisalue on kommutatiivinen kertolaskunsa suhteen, joten

$$f(ab) = (ab)^p = \overbrace{(ab)\cdots(ab)}^{p} = a^p b^p = f(a)f(b).$$

Lopuksi vielä $f(1_R) = 1_R^p = 1_R$. Nämä seikat todistavat f:n rengashomomorfismiksi.
Todistetaan injektiivisyys tarkastelemalla ydintä. Jos $a \in R$ ja $f(a) = 0_R$, niin $a^p = 0_R$, ja koska R on kokonaisalue (eikä sillä siis ole nollatekijöitä), niin tästä seuraa $a = 0_R$. Siispä $\ker f = \{0_R\}$ ja f injektio.
Jos p on alkuluku ja kokonaisalueeksi otetaan $R = \mathbb{Z}_p$ niin $f = \mathrm{id}$ Fermat'n pienen lauseen perusteella: $a^p \equiv a \mod p$ kun p ei jaa a:ta. Eli $\overline{a}^p = \overline{a}$ kaikilla $\overline{a} \in \mathbb{Z}_p$.

5. Renkaan R ideaali I on *maksimaalinen*, jos $I \neq R$ ja jos jokaiselle R:n ideaalille J ehdosta $I \subset J$ seuraa, että $J = I$ tai $J = R$. Olkoon R kommutatiivinen rengas ja I sen ideaali. Osoita, että I on R:n maksimaalinen ideaali jos ja vain jos tekijärengas R/I on kunta.

Ratk. 1 Oletetaan että I on R:n maksimaalinen ideaali. Koska R on kommutatiivinen, niin R/I on kommutatiivinen, ja koska $I \neq R$, niin $R/I \neq \{0 + I\}$.

Näytetään että tekijärenkaan R/I alkiot nolla-alkiota lukuunottamatta ovat kääntyviä, mikä tekee R/I:stä kunnan. Olkoon $a+I \in R/I$, $a \notin I$ (jolloin $a+I$ ei ole nolla-alkio I). Ideaalien Ra ja I summa sisältää siis I:n aidosti (sillä $a \in (Ra+I) \setminus I$), joten $Ra+I = R$. Erityisesti alkiolla $1_R = 1$ on esitys $1 = i + ra$ missä $i \in I$ ja $r \in R$. Tästä seuraa siis, että $ra - 1 \in I$, jolloin $r+I$ on $a+I$:n käänteisalkio: $(r+I)(a+I) = ra + I = 1 + I$.
Oletetaan sitten, että R/I on kunta. Tällöin $I \neq R$, muuten tekijärengas olisi yksiö (ja kunnassa on vähintään kaksi alkiota). Olkoon J R:n ideaali, jolle $I \subsetneq J$. Riittää näyttää, että tällöin $J = R$. Tätä varten olkoon $a \in J \setminus I$ ja $r \in R$ sellainen, että $r+I$ on $a+I$:n käänteisalkio. Siis $ra - 1 \in I \subset J$. Toisaalta $ra \in J$, koska J on ideaali. Nyt $ra \in J$ ja $ra \in 1 + J$, joten löytyy $j \in J$ niin, että $ra = 1 - j$, mistä seuraa $1 = ra + j \in J$. Mutta silloin $R = 1R \subset J \subset R$ ja väite seuraa.

Ratk. 2 Tehtävän voi ratkaista myös käyttämällä sivun 95 lausetta 2: Kommutatiivinen rengas $R \neq \{0\}$ on kunta jos ja vain jos sen ainoat ideaalit ovat $\{0\}$ ja R.
Merkitään symbolilla p kanonista homomorfismia $p : R \to R/I$, $p(r) = r + I$.
Oletetaan siis, että I on R:n maksimaalinen ideaali, ja merkitään $K = R/I$. Koska R on kommutatiivinen, on myös K kommutatiivinen, ja koska $I \neq R$, on $K \neq \{0_K\}$. Olkoon nyt $J' \neq \{0_K\}$ K:n ideaali. Koska p on rengashomomorfismi, niin $J = p^{-1}(J')$ on R:n ideaali. Koska $p(I) = \{0_K\} \subset J'$, niin $I \subset J$. Koska $J' \neq \{0_K\}$, niin $J \neq I$, siispä $J = R$. Nyt $J' = p(J) = p(R) = K$, joten K on kunta.
Oletetaan sitten, että $K = R/I$ on kunta, eli sen ideaalit ovat täsmälleen $\{0\}$ ja K (taas pätee $I \neq R$ sillä muuten $K = \{0\}$). Olkoon J R:n ideaali, $I \subsetneq J$ ja $J' = p(J) = \{j + I : j \in J\}$. Tällöin J' on K:n ideaali, sillä p on surjektiivinen rengashomomorfismi. Toisaalta $J' \neq \{0\}$, sillä on olemassa alkio $j \in J \setminus I$, jolloin $j + I \neq I$. Oletuksen mukaan siis $J' = K$. Saadaan $p(R) = K = J' = p(J)$, josta $R = J + I \subset J$. Täten $J = R$.

6. Tarkastellaan verkossa olevan luentomateriaalin sivulla 94 kunnan määritelmän jälkeen esitettyä seuraavaa yritystä antaa kunnalle yhtäpitävä määritelmä (eli *luonnehdinta*, *karakterisointi*): Kolmikko $(K, +, \cdot)$, jossa K on joukko ja $+$ sekä $\cdot$ ovat K:n laskutoimituksia, on kunta, jos ja vain jos $(K, +)$ on Abelin ryhmä (olkoon 0 sen neutraalialkion merkintä), $(K\{0\}, \cdot)$ on Abelin ryhmä ja $a(b + c) = ab + ac$ kaikilla $a, b, c \in K$. Kunta tietysti täyttää nämä ehdot.
a) Osoita, että käänteinen ei päde eli että ehdot täyttävä kolmikko $(K, +, \cdot)$ ei välttämättä ole kunta tarkastelemalla esimerkkiä, jossa $K = \{0, 1\}$ on joukko $(1 \neq 0)$ laskutoimituksin $+$ ja $\cdot$, joilla $0 + 0 = 1 + 1 = 0$, $0 + 1 = 1 + 0 = 1$, $0 \cdot 0 = 1 \cdot 0 = 0$ ja $0 \cdot 1 = 1 \cdot 1 = 1$ (siis todellakin asetetaan $0 \cdot 1 = 1$).
b) Etsi alun ehtojen täydennykseksi niin suppea lisäehto kuin vain osaat saadaksesi luonnehdinnan kunnalle.

Ratk.
a) Jos $(K, +, \cdot)$ on kunta, niin kaikilla $a \in K$ on $0a = (0 + 0)a = 0a + 0a$, josta $0a = 0$. Tehtävänannon struktuurilla ei ole tätä ominaisuutta, joten se ei voi olla kunta. Kuitenkin se täyttää karakterisointiyrityksen ehdot: $(K, +)$ on isomorfinen ryhmän $(\mathbb{Z}_2, +)$ kanssa, joten se on Abelin ryhmä nolla-alkionaan 0. Joukko $K \setminus \{0\}$ on yksiö, siis triviaali (Abelin) ryhmä. Myös osittelulaki on

voimassa:

$$
\begin{aligned}
0(0+0) &= 0 \cdot 0 = 0 = 0 + 0 = 0 \cdot 0 + 0 \cdot 0 \\
0(0+1) &= 0 \cdot 1 = 1 = 0 + 1 = 0 \cdot 0 + 0 \cdot 1 \\
0(1+0) &= 0 \cdot 1 = 1 = 1 + 0 = 0 \cdot 1 + 0 \cdot 0 \\
0(1+1) &= 0 \cdot 0 = 0 = 1 + 1 = 0 \cdot 1 + 0 \cdot 1 \\
1(0+0) &= 1 \cdot 0 = 0 = 0 + 0 = 1 \cdot 0 + 1 \cdot 0 \\
1(0+1) &= 1 \cdot 1 = 1 = 0 + 1 = 1 \cdot 0 + 1 \cdot 1 \\
1(1+0) &= 1 \cdot 1 = 1 = 1 + 0 = 1 \cdot 1 + 1 \cdot 0 \\
1(1+1) &= 1 \cdot 0 = 0 = 1 + 1 = 1 \cdot 1 + 1 \cdot 1.
\end{aligned}
$$

b) Riittävä lisäehto on esimerkiksi seuraava: $0a = 0$ kaikilla $a \in K$. Muotoilemme siis seuraavan väitteen (karakterisointi kunnalle):
Kolmikko $(K, +, 0)$ on kunta jos ja vain jos

1. $(K, +)$ on Abelin ryhmä. Olkoon 0 sen nolla-alkio,
2. $(K \setminus \{0\}, \cdot)$ on Abelin ryhmä. Olkoon 1 sen ykkösalkio,
3. $a(b + c) = ab + ac$ kaikilla $a, b, c \in K$ sekä vielä
4. $0a = 0$ kaikilla $a \in K$ (riittää kaikilla $a \in K \setminus \{0\}$).

Jos $a \in K$, niin $a0 = a(0 + 0) = a0 + a0$, josta $a0 = 0$. Tämä yhdessä neljännen ehdon kanssa takaa tulon vaihdannaisuuden ($ab = ba$) myös silloin, kun toinen tulontekijöistä on nolla. Tulon liitännäisyys $a(bc) = (ab)c$ pätee, kun $a, b, c \in K \setminus \{0\}$, ja lisäehdon nojalla myös silloin, kun jokin alkioista a, b, c on nolla (muodossa $a(bc) = 0 = (ab)c$). Koska $1 \cdot a = a$, kun $a \in K \setminus \{0\}$, ja koska myös $1 \cdot 0 = 0$, niin 1 on $(K, \cdot)$:n neutraalialkio. Siis $(K, +, \cdot)$ on kommutatiivinen rengas. Lisäksi $1 \neq 0$. Lopuksi, koska $(K \setminus \{0\}, \cdot)$ on ryhmä, jokaisella nollasta eroavalla alkiolla on käänteisalkio, ja täten $(K, +, \cdot)$ on kunta.
Huom. Toinen mahdollinen vaihtoehto olisi asettaa myös toispuoleinen osittelulaki $(a + b)c = ac + bc$ kaikilla $a, b, c \in K$. Yleensä tätä ei tarvitse kunnan määritelmässä erikseen mainita, sillä se seuraa tulon vaihdannaisuudesta, mutta luonnehdinnassamme tulon vaihdannaisuus on taattu vain $K \setminus \{0\}$:ssa (eli ei välttämättä koko K:ssa). Tämä on itse asiassa se seikka, joka karakterisointiyrityksessä menee pieleen.