Algebra, syksy 1999, kotitehtävät 12-13, ratkaisuja

1. $\langle(1,1)\rangle = \{(0,0),(1,1),(2,0),(3,1),(4,0),(5,1)\}$. Siinä on 6 alkiota, ja ryhmässä G on 12 alkiota. Niinpä sivuluokkia on 2 ja tekijäryhmä on

$$G/N = \{\{(0,0),(1,1),(2,0),(3,1),(4,0),(5,1)\},\{(0,1),(1,0),(2,1),(3,0),(4,1),(5,0)\}\} \cong \mathbf{Z}_2.$$

2. Ensiksikin, kun a, $x \in G$, tulos $f(x) = axa^{-1}$ on täysin määrätty joukon G alkio; f siis on funktio $G \to G$.
Homomorfisuus: $f(xy) = a(xy)a^{-1} = axa^{-1}aya^{-1} = f(x)f(y)$.
Injektiivisyys: Jos $f(x) = f(y)$ eli $axa^{-1} = aya^{-1}$, saadaan vasemmalta ja oikealta supistamalla $x = y$.
Surjektiivisuus: Jos $x \in G$ (maalijoukko), niin alkio $a^{-1}xa \in G$ (lähtöjoukko) kuvautuu alkiolle x, sillä $f(a^{-1}xa) = a(a^{-1}xa)a^{-1} = x$.
3. Kyseessä todella on funktio, sillä nollasta poikkeavan kompleksiluvun moduli on yksikäsitteinen aidosti positiivinen reaaliluku. Olkoot $a + bi$, $c + di \in \mathbf{C} \setminus \{0\}$. Silloin

$$\begin{aligned} f((a+bi)*(c+di)) &= f(ac-bd+(ad+bc)i) = \sqrt{(ac-bd)^2+(ad+bc)^2} \\ &= \sqrt{a^2c^2-2acbd+b^2d^2+a^2d^2+2adbc+b^2c^2} = \sqrt{a^2c^2+a^2d^2+b^2c^2+b^2d^2}. \\ f(a+bi)\cdot f(c+di) &= \sqrt{a^2+b^2}\sqrt{c^2+d^2} = \sqrt{(a^2+b^2)(c^2+d^2)} \\ &= \sqrt{a^2c^2+a^2d^2+b^2c^2+b^2d^2} \end{aligned}$$

Mitkä kompleksiluvut $x + yi$ kuvautuvat reaalilukujen kertolaskun neutraalialkiolle eli luvulle 1, eli mille kompleksiluvuille $x + yi$ on $\sqrt{x^2+y^2} = 1$? Tämä toteutuu jos ja vain jos $x^2 + y^2 = 1$ eli $x + yi$ on yksikköympyrän kehällä. Siis ydin $\ker f = \{\, z \,:\, |z| = 1 \,\}$.
4. Yhdistetty kuvaus $g \circ f : G \to G''$ on todella määritelty.
Homomorfisuus: Kaikilla $a, b \in G$ on

$$(g\circ f)(a\cdot b) = g\big(f(a\cdot b)\big) = g\big(f(a)*f(b)\big) = g\big(f(a)\big) \times g\big(f(b)\big) = (g\circ f)(a) \times (g\circ f)(b).$$

Tehtävä: Mitkä siis ovat laskutoimitukset missäkin ryhmässä ?
Ytimet: Jokainen $a \in G$, jolle $f(a) = e'$, kuvautuu yhdistetyssä alkiolle e''. Täten $\ker f \subseteq \ker(g \circ f)$. Osajoukkous on usein aito, äärimmilläänhän $\ker f$ voi olla pelkkä $\{e\}$ ja toisaalta $\ker(g \circ f)$ voi olla vaikka koko G. Keksi esimerkki tällaisesta tilanteesta!
5. Isomorfismi f ryhmältä $(G, +)$ ryhmälle $(G, \oplus)$ on bijektio, joten sillä on käänteiskuvaus, ja sekin on bijektio, $f^{-1} : G' \to G$.
Sen homomorfisuus: olkoot $a', b' \in G'$. Silloin on olemassa vieläpä tasan yhdet sellaiset $a, b \in G$, että $f(a) = a'$ ja $f(b) = b'$, eli $a = f^{-1}(a')$ ja $b = f^{-1}(b')$. Edelleen $f(a+b) = f(a) \oplus f(b) = a' \oplus b'$. Täten

$$f^{-1}(a' \oplus b') = a + b = f^{-1}(a') + f^{-1}(b').$$

6. Neutraalialkion ominaisuuden $0_R = 0_R + 0_R$ ja osittelulain avulla saadaan yhtälö

$$0_R \cdot a = (0_R + 0_R)\cdot a = 0_R \cdot a + 0_R \cdot a,$$

mistä supistamalla $0_R = 0_R \cdot a$. Toinen väite samaan tapaan.
7. Olkoot $a, b, c \in R$. Osittelulain mukaan $a(b-c) = a\big(b + (-c)\big) = ab + a(-c)$ ja Lauseen 11.5 kohdan 2 mukaan $a(-c) = -(ac)$. Siis $a(b-c) = ab + a(-c) = ab + (-(ac)) = ab - ac$. Toinen osa samaan tapaan.
8. Muut oletukset ovat kuten kokonaisalueen määritelmässä, joten riittää todistaa tulon nollasäännön voimassaolo:
Olkoot $a, b \in R$ siten, että $ab = 0_R$. Jos $b = 0_R$, väite pätee. Oletetaan, että $b \neq 0_R$. Koska $0b = 0_R$, niin $ab = 0_Rb$. Supistussäännön mukaan nyt saadaan supistaa alkiolla $b \neq 0_R$, jolloin saadaan $a = 0_R$.
9. Esitetyt operaatiot ovat selvästi laskutoimituksia joukossa $\mathbf{Z}$.

(i) $(Z, \oplus)$ *on Abelin ryhmä:* Liitännäisyys:

$$\begin{aligned}
a \oplus (b \oplus c) &= a \oplus (b + c - 1) = a + b + c - 1 - 1, \\
(a \oplus b) \oplus c &= (a + b - 1) \oplus c = a + b - 1 + c - 1
\end{aligned}$$

Koska $a \oplus b = a + b - 1 = b + a - 1 = b \oplus a$, on $\oplus$ vaihdannainen. Laskutoimituksen $\oplus$ neutraalialkio on 1, sillä $1 \oplus x = 1 + x - 1 = x$ kaikille $x \in Z$.
Vasta-alkiot: Olkoon x alkion a vasta-alkio. Silloin $a \oplus x = 1 \Leftrightarrow a + x - 1 = 1 \Leftrightarrow x = 2 - a$. Siis $2 - a$ on luvun a vasta-alkio.
(ii) kertolasku on liitännäinen, sillä

$$\begin{aligned}
a \odot (b \odot c) &= a \odot (b + c - bc) = a + (b + c - bc) - a(b + c - bc) \\
&= a + b + c - bc - ab - ac + abc, \\
(a \odot b) \odot c &= (a + b - ab) \odot c = (a + b - ab) + c - (a + b - ab)c \\
&= a + b - ab + c - ac - bc + abc
\end{aligned}$$

(iii) Kertolasku on vaihdannainen, sillä $a \odot b = a + b - ab = b + a - ba = b \odot a$.
(iv) Ykkösalkio: koetetaan ratkaista kertolaskun neutraalialkio yhtälöstä $a \odot e = a$:

$$a \odot e = a \Leftrightarrow a + e - ae = a \Leftrightarrow e - ae = 0 \Leftrightarrow e(1 - a) = 0 \Leftrightarrow e = 0.$$

Nolla kelpaa, sillä myös $0 \odot a = 0 + a - 0 \cdot a = a$.
(v) Osittelulait: Malliksi ensimmäinen

$$\begin{aligned}
a \odot (b \oplus c) &= a \odot (b + c - 1) = a + (b + c - 1) - a(b + c - 1) \\
&= a + b + c - 1 - ab - ac + a = 2a + b + c - ab - ac - 1 \\
(a \odot b) \oplus (a \odot c) &= (a + b - ab) \oplus (a + c - ac) = (a + b - ab) + (a + c - ac) - 1 \\
&= a + b - ab + a + c - ac - 1 = 2a + b + c - ab - ac - 1
\end{aligned}$$

(vi) Tulon nollasääntö: Oletetaan, että $a \odot b = 1$. Siis $a + b - ab = 1$ eli $a(1 - b) = 1 - b$. Mikäli b ei ole yksi, voidaan tässä supistaa luvulla $(1 - b)$, ja saadaan, että $a = 1$.
10. Kompleksilukujen yhteenlasku on vaihdannainen ja liitännäinen, neutraalialkio $0 = 0 + 0i \in \mathbf{Z}[i]$, ja jos $x + yi \in \mathbf{Z}[i]$, niin vasta-alkio $-x - yi \in \mathbf{Z}[i]$.
Kompleksilukujen kertolasku on liitännäinen ja vaihdannainen, joten se on sitä myös joukossa $\mathbf{Z}[i]$. Kertolaskun neutraalialkio $1 = 1 + 0i \in \mathbf{Z}[i]$. Osittelulait ovat voimassa joukossa $\mathbf{C}$, joten ne ovat voimassa myös joukossa $\mathbf{Z}[i]$.
Puuttuu enää *tulon nollasääntö*. Mutta tunnetusti *minkä tahansa* kahden kompleksiluvun tulo on nolla vain jos ainakin toinen tulon tekijöistä on nolla!
11. a) Renkaan Z_{12} idempotentit alkiot ovat 0, 1, 4 ja 9.
b) Kaikissa renkaissa on idempotentteja alkioita, ainakin yhteenlaskun neutraalialkio, sillä $0_R \cdot 0_R = 0_R$; ks. tehtävä 6: Lause 11.4).
c) Jos R on kokonaisalue, niin 0_R ja 1_R ovat selvästi idempotentteja. Osoitetaan, että kokonaisalueessa ei muita sellaisia olekaan.
Oletetaan, että kokonaisalueessa R on idempotentti alkio $x \neq 0_R$, ts. $x^2 = x = x \cdot 1_r$. Koska $x \neq 0_R$, seuraa supistussäännöstä $x = 1_R$.
12. Kunnan F kertolasku on suljettu joukossa $F \setminus \{0_F\}$, koska kunta on kokonaisalue (Lause 11.11) eikä siinä siten ole nollantekijöitä. Kunnan määritelmän mukaan kunnan kertolasku on liitännäinen ja vaihdannainen, sillä on neutraalialkiona ykkösalkio ja jokaisella nollasta poikkeavalla alkiolla on käänteisalkio kertolaskun suhteen.
13. Kuten monisteen Esimerkki 91; pitää kuitenkin muistaa, että nyt laskutoimitusten tulosten pitää olla "kokonaislukumuotoa" $a + b\sqrt{7}$.
14. a) $U(\mathbf{Z}) = \{-1, 1\}$, $U(\mathbf{Z}_{12}) = \{1, 5, 7, 11\}$ ja $U(\mathbf{Z}_7) = \mathbf{Z}_7 \setminus \{0\}$.
b) Olkoon R ykkösellinen rengas. Nyt $U(R) = \{x \in R \,|\, \exists x^{-1} \in R : xx^{-1} = x^{-1}x = 1_R\}$. Heti nähdään, että ainakin $1_R \in U(R)$, joten siellä on neutraalialkio. Toiseksi, jos $x \in U(R)$, niin myös $x^{-1} \in U(R)$. Kertolaskun liitännäisyys periytyy osajoukkoon. Suurin ongelma onkin, *onko kertolasku*

suljettu. Olkoot $x, y \in U(R)$. Silloin ovat olemassa x^{-1} ja y^{-1}. Arvataan vanhojen tietojen perusteella, että pitää olla $(xy)^{-1} = y^{-1}x^{-1}$. Nyt $y^{-1}x^{-1} \in R$ ja liitännäisyydellä: $(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = x1_R x^{-1} = xx^{-1} = 1_R$. Samoin $(y^{-1}x^{-1})(xy) = 1_R$. Siis $xy \in U(R)$ ja kertolasku suljettu.
15. a) T on alirengas: Ensiksi, $T \subseteq M(R)$, OK.
1) Laskutoimitukset suljettuja: summa selvä, tulo:

$$\begin{pmatrix} a & a \\ 0_R & 0_R \end{pmatrix}\begin{pmatrix} b & b \\ 0_R & 0_R \end{pmatrix} = \begin{pmatrix} ab & ab \\ 0_R & 0_R \end{pmatrix}.$$

Neutraalialkio nollamatriisi O on samaa muotoa kuin T:n alkiot, samoin yhteenlaskun vasta-alkio:

$$O = \begin{pmatrix} 0_R & 0_R \\ 0_R & 0_R \end{pmatrix} \in T, \qquad -\begin{pmatrix} a & a \\ 0_R & 0_R \end{pmatrix} = \begin{pmatrix} -a & -a \\ 0_R & 0_R \end{pmatrix} \in T.$$

Siis alirengas. Kokonaisalue?
Koska R oli kokonaisalueena kertolaskun suhteen vaihdannainen, on sitä myös T, sillä

$$\begin{pmatrix} a & a \\ 0_R & 0_R \end{pmatrix}\begin{pmatrix} b & b \\ 0_R & 0_R \end{pmatrix} = \begin{pmatrix} ab & ab \\ 0_R & 0_R \end{pmatrix} = \begin{pmatrix} ba & ba \\ 0_R & 0_R \end{pmatrix} = \begin{pmatrix} b & b \\ 0_R & 0_R \end{pmatrix}\begin{pmatrix} a & a \\ 0_R & 0_R \end{pmatrix}.$$

Ykkösalkio on, kuten seuraavasta näkyy (mitä laskusääntöjä tarvitaan?):

$$\begin{pmatrix} a & a \\ 0_R & 0_R \end{pmatrix}\begin{pmatrix} 1_R & 1_R \\ 0_R & 0_R \end{pmatrix} = \begin{pmatrix} a & a \\ 0_R & 0_R \end{pmatrix} = \begin{pmatrix} 1_R & 1_R \\ 0_R & 0_R \end{pmatrix}\begin{pmatrix} a & a \\ 0_R & 0_R \end{pmatrix}.$$

Kahden T:n matriisin tulo (ks. ylin kaavarivi) on nollamatriisi jos ja vain jos $ab = 0_R$, mikä kokonaisalueessa tarkoittaa $a = 0_R$ tai $b = 0_R$. Siis toinen matriiseista on nollamatriisi.
Kyseessä on kokonaisalue. Kunta?
Ei välttämättä, esimerkiksi $(R, +, \cdot) := (\mathbf{Z}, +, \cdot)$ on kokonaisalue, mutta esimerkiksi kaikilla $a \in \mathbf{Z}$ on

$$\begin{pmatrix} 2 & 2 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & a \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = 1_T.$$

16. Tässä siis laskutoimitukset ovat $+_{11}$ ja $*_{11}$. Yhtälöt voidaan laskea puolittain yhteen, jolloin termit $3y$ supistuvat ja saadaan (laskusääntöjä sopivasti noudattaen, teehän tarkemmin!)

$$\left\{\begin{array}{rcrcr} 2x & + & 3y & = & 2 \\ 4x & - & 3y & = & -3 \end{array}\right. \Leftrightarrow \left\{\begin{array}{rcrcr} 2x & + & 3y & = & 2 \\ 6x & + & 0y & = & 10 \end{array}\right. \Leftrightarrow \left\{\begin{array}{rcl} 3y & = & 2-2x \\ x & = & 9 \end{array}\right. \Leftrightarrow \left\{\begin{array}{rcl} x & = & 9 \\ y & = & 2. \end{array}\right.$$

17. Todellisuudessa – perustele teoriaamme käyttäen – renkaiden joukko sisältää kokonaisalueet ja kunnat taas ovat kokonaisalueiden joukon sisällä. Lisäksi tiedetään, että äärellisiä kokonaisalueita, jotka eivät ole kuntia, on vain yhden alkion rengas, muut ovat äärettömiä. Muille äärellisille riittää siis nollantekijöiden tutkiminen myös kunnaksi todistettaessa. Ks. myös tehtävä 15. Siis:
Kuntia: $\mathbf{R}$, $\mathbf{C}$, $\mathbf{Z}_{17}$, $(\{0, 4, 8, 12, 16\}, +_{20}, *_{20})$ ja T_1
Kokonaisalueita, muttei kuntia: $\mathbf{Z}$
Vain renkaita: $\mathbf{Z}_{16}$, $5\mathbf{Z}$, $M(\mathbf{R})$, $M(\mathbf{Z}_2)$ ja T_2
18-19. Huomautetaan tässä vain, että ISETL-tehtävässä 6 oli ehkä harhaan johtava opastus, jos nollantekijät tyystin karistetaan pois, aiheutuu siitä tilanteen redusoituminen triviaaliksi nollan muodostamaksi kokonaisalueeksi. Mutta, jos tutkitaan kaikki $\mathbf{Z}_{12}$:n aliryhmät, niin havaitaan – ehkä vähän yllättävästikin, vrt. tehtävä 17 – että $\{0, 4, 8\}$ on jopa kunta! Ykkösalkio on 4.
20. Vastaa palautekyselyyn sähköisesti (linkki annettu sp:lla).