Algebra I, 2. kurssikoe ke 29.4.2009/ratkaisut ja arvosteluperusteita (Jouni Luukkainen), 2 sivua (sijoitettu myös kurssin kotisivulle)

1. Olkoon G additiivinen Abelin ryhmä. Osoita, että G:n yhteenlasku $f\colon G\times G\to G$, $(x,y)\mapsto x+y$, on ryhmähomomorfismi ja että ryhmät $\mathrm{Ker}(f)$ ja G ovat keskenään isomorfiset.

Ratk. Myös tuloryhmä $G\times G$ on Abelin ryhmä. Jos $z,z'\in G\times G$, niin $z=(x,y)$ ja $z'=(x',y')$ joillain $x,y,x',y'\in G$, jolloin

$$\begin{aligned} f(z+z') &= f((x,y)+(x',y')) = f(x+x',y+y') = (x+x')+(y+y') = (x+y)+(x'+y') \\ &= f(x,y)+f(x',y') = f(z)+f(z'). \end{aligned}$$

Siis f on ryhmähomomorfismi.

Määritetään $\mathrm{Ker}(f)$. Jos $z=(x,y)\in G\times G$, niin $z\in\mathrm{Ker}(f)\iff x+y=f(z)=0_G\iff y=-x$. Siis $\mathrm{Ker}(f)=\{(x,-x)\mid x\in G\}$.

Projektiokuvaus $\mathrm{pr}_1\colon G\times G\to G$, $(x,y)\mapsto x$, on ryhmähomomorfismi, jolloin sen rajoittumakin $g=\mathrm{pr}_1|\colon \mathrm{Ker}(f)\to G$ on ryhmähomomorfismi. Kuvauksella g on käänteiskuvaus $h\colon G\to\mathrm{Ker}(f)$, $x\mapsto(x,-x)$, sillä $h(g(x,-x))=h(x)=(x,-x)$ ja $g(h(x))=g(x,-x)=x$ kaikilla $x\in G$. Siis g on bijektio ja täten ryhmäisomorfismi. **Vaihtoehtoisesti** g:n homomorfisuuden sijasta voitaisiin osoittaa, että h on homomorfismi:

$$h(x+y)=(x+y,-(x+y))=(x+y,-x-y)=(x,-x)+(y,-y)=h(x)+h(y),\quad \text{kun } x,y\in G.$$

Arvostelusta. Kuvauksen f homomorfisuus 3 p (siitä $G\times G$:n yhteenlaskun käyttö 1 p ja G:n vaihdannaisuuden käyttö 1 p), ytimen $\mathrm{Ker}(f)$ määrittäminen 1 p ja isomorfismin g (tai sen käänteisisomorfismin h) konstruointi 2 p.

2. a) Määritä positiiviset kokonaisluvut n, joilla multiplikatiivisen ryhmän $\mathbb{Z}_n^*$ kertaluku on 4.

b) Osoita, että millään positiivisella kokonaisluvulla n ei additiivisen ryhmän $\mathbb{Z}_n$ niiden alkioiden lukumäärä, jotka yksinään virittävät $\mathbb{Z}_n$:n, ole 31.

Ratk. Kun $n\in\mathbb{N}_+$, niin sekä multiplikatiivisen ryhmän $\mathbb{Z}_n^*$ kertaluku $|\mathbb{Z}_n^*|$ että additiivisen ryhmän $\mathbb{Z}_n$ niiden alkioiden lukumäärä, jotka yksinään virittävät $\mathbb{Z}_n$:n, ovat kumpikin Eulerin φ-funktion arvo $\varphi(n)$. (Itse asiassa kullekin $m\in\{0,1,\dots,n-1\}$ seuraavat ehdot ovat yhtäpitävät: alkio $\overline{m}\in\mathbb{Z}_n$ virittää additiivisen ryhmän $\mathbb{Z}_n$ eli $\mathbb{Z}_n=\langle\overline{m}\rangle$; $\overline{m}\in\mathbb{Z}_n^*$ eli $\overline{m}$ on kääntyvä renkaassa $\mathbb{Z}_n$; ja $\mathrm{syt}(m,n)=1$.) Tiedetään, että

$$\varphi(n)=n\prod_{p\in\mathbb{P},\,p|n}\left(1-\frac{1}{p}\right),$$

jossa $\mathbb{P}$ on alkulukujen joukko.

a) On siis määritettävä luvut $n\in\mathbb{N}_+$, joilla $\varphi(n)=4$. Olkoon n tällainen, $p\in\mathbb{P}$, $k\in\mathbb{N}_+$, $p^k|n$ ja $p^{k+1}\not|n$. Tällöin luvun $p^k(1-1/p)=p^{k-1}(p-1)$ on oltava luvun $4=2^2$ positiivinen tekijä eli siis 1, 2 tai 4; jos $k\geq 2$, on siis oltava $p=2$ ja $k\in\{2,3\}$; jos taas $k=1$, on oltava $(p-1)|4$ eli $p-1\in\{1,2,4\}$ eli siis $p\in\{2,3,5\}$. Täten n on muotoa $n=2^a\cdot 3^b\cdot 5^c$ joillain $a\in\{0,1,2,3\}$ ja $b,c\in\{0,1\}$. Näistä kelvolliset tapaukset ovat $n\in\{2^3,2^2\cdot 3,2\cdot 5,5\}=\underline{\{5,8,10,12\}}$.

b) On siis osoitettava, että $\varphi(n)\neq 31$ kaikilla $n\in\mathbb{N}_+$. Tehdään vastaoletus, että on olemassa $n\in\mathbb{N}_+$, jolla $\varphi(n)=31$. Olkoon $p\in\mathbb{P}$, $k\in\mathbb{N}_+$, $p^k|n$ ja $p^{k+1}\not|n$. Tällöin luvun $p^k(1-1/p)=p^{k-1}(p-1)$ on oltava luvun 31 positiivinen tekijä eli siis 1 tai 31 (sillä 31 on alkuluku); täten on oltava $k=1$ ja $p-1\in\{1,31\}$ eli $p\in\{2,32\}\cap\mathbb{P}=\{2\}$. Mutta tästä seuraa, että $n=2$, jolloin $\varphi(n)=\varphi(2)=2(1-1/2)=1$, ristiriita.

Arvostelusta. a)-kohdan palauttaminen yhtälön $\varphi(n)=4$ ratkaisemiseen, b)-kohdan palauttaminen siihen, että yhtälöllä $\varphi(n)=31$ ei ole ratkaisuja ja $\varphi(n)$:n kaava olivat kukin 1 p arvoisia.

3. Olkoon R kommutatiivinen rengas. Renkaan R *alkuideaali* on R:n ideaali $P\neq R$, jolla kaikilla $a,b\in R$ ehdosta $ab\in P$ seuraa, että $a\in P$ tai $b\in P$. Osoita, että jos I on R:n ideaali, niin tekijärengas R/I on kokonaisalue jos ja vain jos I on R:n alkuideaali.

Ratk. Kerrataan, että *kokonaisalue* on kommutatiivinen rengas, joka ei ole nollarengas ja jossa ei ole nollanjakajia.

Oletetaan ensin, että I on R:n alkuideaali. Koska R on kommutatiivinen, niin tekijärengas R/I on joka tapauksessa kommutatiivinen. Koska $I \neq R$, niin $R/I \neq \{0_{R/I}\}$. Olkoon $x, y \in R/I$ ja $xy = 0_{R/I}$. Tällöin $x = a + I$ ja $y = b + I$ joillain $a, b \in R$. Koska $(ab) + I = (a + I)(b + I) = xy = 0_{R/I} = 0_R + I$, niin $ab \in I$ ja siis $a \in I$ tai $b \in I$, sillä I on alkuideaali. Tällöin vastaavasti $x = 0_{R/I}$ tai $y = 0_{R/I}$. Täten renkaassa R/I ei ole nollanjakajia. Siis R/I on kokonaisalue.

Oletetaan sitten, että I on renkaan R ideaali, jolla R/I on kokonaisalue. Koska $R/I \neq \{0_{R/I}\}$, niin $I \neq R$. Olkoon $a, b \in R$ ja $ab \in I$. Merkitään $x = a + I \in R/I$ ja $y = b + I \in R/I$. Tällöin $xy = (a + I)(b + I) = (ab) + I = 0_R + I = 0_{R/I}$. Koska renkaassa R/I ei ole nollanjakajia, tästä seuraa, että $x = 0_{R/I}$ tai $y = 0_{R/I}$. Täten vastaavasti $a \in I$ tai $b \in I$. Siis I on R:n alkuideaali.

Huom. Tapauksessa $R = \mathbb{Z}$ tulos on sikäli tuttu, että luennoissa on osoitettu, että luvulle $n \in \mathbb{N}_+$ on $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ kokonaisalue jos ja vain jos n on alkuluku, ja että toisaalta on helppo nähdä, että $n \in \mathbb{N}_+$ on alkuluku jos ja vain jos $\mathbb{Z}$:n ideaali $n\mathbb{Z}$ on alkuideaali. (Myös luvulle $n = 0$ on $\mathbb{Z}_n = \mathbb{Z}$ kokonaisalue ja $n\mathbb{Z} = \{0\}$ alkuideaali.)

Arvostelusta. Kokonaisalueen määritelmä termi "nollantekijä" mainiten 1 p. Muotoilu $xy = 0 \Longrightarrow x = 0$ tai $y = 0$ ehdolle, että renkaassa R/I ei ole nollantekijöitä 1 p. Hyvin harva oli huomauttanut, että myös R/I on kommutatiivinen R:n kommutatiivisuuden tähden; puutteesta ei sakotettu. Ekvivalenttien ehtojen R/I ja $I \neq R$ mainitsematta jättämisestä sakotettiin 1 p.

4. Jaa polynomi $f = x^4 + 3x^3 + x + 1$ jaottomien tekijöiden tuloksi renkaassa $\mathbb{Z}_5[x]$ osoittamalla ensin, että f:llä ei ole ensimmäisen asteen tekijöitä, ja tekemällä sitten yrite $f = (x^2 + Ax + B)(x^2 + Cx + D)$.

Ratk. Kerroinrengas $\mathbb{Z}_5$ on kunta, koska 5 on alkuluku. Täten pääpolynomilla f on tekijöiden järjestystä vaille yksikäsitteinen esitys jaottomien pääpolynomien tulona renkaassa $\mathbb{Z}_5[x]$ ja tekijäin astelukujen summa on yhtäsuuri kuin f:n asteluku 4.

Koska $f(0) = 1$, $f(1) = 1 + 3 + 1 + 1 = 6 = 1$, $f(2) = 16 + 24 + 2 + 1 = 1 + 4 + 2 + 1 = 8 = 3$, $f(3) = 81 + 81 + 3 + 1 = 1 + 1 + 3 + 1 = 6 = 1$ ja $f(4) = 256 + 192 + 4 + 1 = 1 + 2 + 4 + 1 = 8 = 3$, niin f:llä ei ole nollakohtia eikä siis ensimmäisen asteen tekijöitä.

Täten joko f on jaoton tai f:llä on kaksi toisen asteen tekijää, jotka tällöin välttämättä ovat jaottomia, sillä ei niilläkään voi olla ensimmäisen asteen tekijöitä. Tutkitaan jälkimmäistä mahdollisuutta. Voidaan vaatia, että tekijätkin ovat pääpolynomeja. Tehdään täten yrite $f = (x^2 + Ax + B)(x^2 + Cx + D)$ määritettävin kertoimin $A, B, C, D \in \mathbb{Z}_5$. Tulee vaatimus $f = x^4 + (A + C)x^3 + (B + D + AC)x^2 + (AD + BC)x + BD$ eli yhtäpitävästi seuraava $\mathbb{Z}_5$:n yhtälöryhmä:

$$\begin{cases} A + C & = 3 \quad (1) \\ B + D + AC & = 0 \quad (2) \\ AD + BC & = 1 \quad (3) \\ BD & = 1. \quad (4) \end{cases}$$

Nyt $(1) \iff (A, C) \in \{(0,3), (1,2), (2,1), (3,0), (4,4)\}$, mutta symmetrian vuoksi yhtälöiden (2)–(4) tutkimisessa voidaan rajoittua tapauksiin $(A, C) = (0,3)$, $(1,2)$ tai $(4,4)$ eli siis joko löytää ratkaisu (B, D) yhdessä näistä kolmesta tapauksesta tai osoittaa, että missään näistä kolmesta tapauksesta ei ratkaisua ole.

Kokeillaan aluksi tapausta $A = 0$ ja $C = 3$. Tällöin $(2) \iff B + D = 0$ ja $(3) \iff 3B = 1 \iff B = 3^{-1} = 2$. Nyt $(4) \iff 2D = 1 \iff D = 2^{-1} = 3$, jolloin myös ehto $(2) \iff 2 + 3 = 0$ toteutuu. Tämä riittää, sillä saatiin vaadittu esitys

$$f = \underline{(x^2 + 2)(x^2 + 3x + 3)}.$$

Ainoa toinen pääpolynomiratkaisu saadaan vaihtamalla tekijöiden järjestys. **Vaihtoehtoisesti**, koska $(4) \iff (B, D) \in \{(1,1), (2,3), (3,2), (4,4)\}$, olisi riittänyt tutkia yhtälöitä (1)–(3) oletuksella, että $(B, D) = (1,1)$, $(2,3)$ tai $(4,4)$.

Arvostelusta. Vain yksi oli maininnut kerroinrenkaan $\mathbb{Z}_5$ olevan kunnan; puutteesta ei sakotettu. Kustakin seuraavista tuli 2 p: Sen osoittaminen, että f:llä ei ole ensimmäisen asteen tekijöitä; yhtälöryhmän johtaminen yritteen kertoimille A, B, C, D; tämän yhtälöryhmän ratkaiseminen.