Algebra I, erilliskoe ti 12.5.2009/ratkaisut (J. Luukkainen), 2 sivua (sijoitettu myös kurssin kotisivulle)

1. Ajatellaan kokonaisluvut määritellyiksi luonnollisten lukujen *muodollisina* (eli merkittyinä, ei siis vielä "suoritettavina") erotuksina $m-n$, joille on asetettu identtisyysehto

$$m-n=p-q \Longleftrightarrow m+q=n+p.$$

a) Osoita, että tämä symbolilla $=$ merkitty relaatio on todellisuudessa (vain) ekvivalenssi luonnollisten lukujen muodollisten erotusten joukossa.

b) Millä kaavoilla kokonaislukujen yhteenlasku ja kertolasku nyt määritellään luonnollisten lukujen yhteen- ja kertolaskujen avulla? (Ajattele $\mathbb{Z}$:n laskusääntöjen nojalla, minkälaiset kaavojen on oltava.)

c) Osoita, että tämä kokonaislukujen yhteenlasku on hyvinmääritelty: jos yhteenlaskettavat erotukset vaihdetaan näiden kanssa identtisiin erotuksiin, niin yhteenlaskun tulokseksi saatava erotus on identtinen alkuperäisen yhteenlaskun tuloksen kanssa.

Ratk. a) Refl.: Kaikilla m,n pätee $m-n=m-n$, sillä $m+n=n+m$. Symm.: Jos $m-n=p-q$, niin $m+q=n+p$, joten $p+n=q+m$ ja siis $p-q=m-n$. Transit.: Jos $m-n=p-q$ ja $p-q=r-s$, niin $m+q=n+p$ ja $p+s=q+r$, jolloin yhteenlaskemalla $m+q+p+s=n+p+q+r$ ja tästä supistamalla $m+s=n+r$ eli $m-n=r-s$. Täten kyseinen relaatio on ekvivalenssi.

b) Laskutoimitusten määritelmät on helppo palauttaa mieleen katsomalla, miten niiden $\mathbb{Z}$:n laskusääntöjen mukaan tulisi olla: $(m-n)+(p-q)=(m+p)-(n+q)$; $(m-n)(p-q)=(mp+nq)-(mq+np)$.

c) Jos $m-n=m'-n'$ ja $p-q=p'-q'$, niin $m+n'=n+m'$ ja $p+q'=q+p'$, josta puolittain yhteenlaskemalla saadaan $m+n'+p+q'=n+m'+q+p'$ ja tästä järjestelemällä tulee $(m+p)+(n'+q')=(n+q)+(m'+p')$, jolloin $(m+p)-(n+q)=(m'+p')-(n'+q')$ eli siis $(m-n)+(p-q)=(m'-n')+(p'-q')$.

Huom. Luennoissa on ensin käytetty luonnollisten lukujen järjestettyjä pareja (m,n) ja sitten näiden ekvivalenssiluokkia $[m,n]$, kun taas yllä nämä kaksi on yhdistetty samaan muodollisten erotusten $m-n$ käsitteeseen määrittelemällä, milloin kahta muodollista erotusta pidetään identtisinä. Vertaa joskus esitettyyn tason vektoreiden (alkeis)määritelmään suuntajanoina pitämällä tällöin kahta vektoria samana, jos niillä on sama suunta ja sama pituus; varsinaisessa matemaattisessa määritelmässä (jota tuskin voitaisiin esittää ainakaan koulussa) vektorit ovat vastaavia suuntajanojen ekvivalenssiluokkia.

2. Olkoon G (multiplikatiivinen) ryhmä ja H, K sekä L ryhmän G äärellisiä aliryhmiä, joiden kertaluvut eli alkioiden lukumäärät ovat $|H|=15$, $|K|=21$ ja $|L|=35$. Osoita, että $H\cap K\cap L=\{1_G\}$.

Ratk. Aliryhmien leikkauksena $M=H\cap K\cap L$ on G:n aliryhmä ja täten myös ryhmien H, K ja L aliryhmä. Lagrangen lauseen mukaan tällöin M:n kertaluku $|M|$ on kertalukujen $|H|=15=3\cdot 5$, $|K|=21=3\cdot 7$ ja $|L|=35=5\cdot 7$ tekijä. Koska $\mathrm{syt}(15,21,35)=1$, niin täten on $|M|=1$ ja siis $M=\{1_G\}$.

Huom. Jos $G=\mathbb{Z}_3\times\mathbb{Z}_5\times\mathbb{Z}_7$, niin korvaamalla 3., 2. tai 1. tekijä aliryhmällänsä $\{0\}$ saadaan esimerkki oletukset täyttävistä aliryhmistä H, K ja L, joille vieläpä $|H\cap K|=3$, $|H\cap L|=5$ ja $|K\cap L|=7$.

3. Olkoon $G=S_{\mathbb{N}}$ luonnollisten lukujen joukon $\mathbb{N}$ permutaatioryhmä eli bijektioiden $f\colon\mathbb{N}\to\mathbb{N}$ joukko laskutoimituksena kuvausten yhdistäminen. Kutsukaamme bijektiota $f\in G$ *melkein identtiseksi*, jos jollekin luvulle $m_f\in\mathbb{N}$ pätee, että $f(n)=n$, kun $n\geq m_f$. Olkoon H melkein identtisten bijektioiden $f\in G$ joukko. Osoita, että H on G:n normaali aliryhmä.

Ratk. (i) Koska $1_G(n)=\mathrm{id}_G(n)=n$ kaikilla $n\in\mathbb{N}$, niin $1_G\in H$ ($m_{1_G}=0$ käy). (ii) Jos $f\in H$, niin $f(n)=n$ ja siis $n=f^{-1}(n)$, kun $n\geq m_f$; täten $f^{-1}\in H$ ($m_{f^{-1}}=m_f$ käy). (iii) Jos $f,g\in H$ ja $m=\max\{m_f,m_g\}\in\mathbb{N}$, niin ehdosta $n\geq m$ seuraa, että $f(n)=n$ ja $g(n)=n$, jolloin $(f\circ g)(n)=f(g(n))=f(n)=n$; täten $f\circ g\in H$ ($m_{f\circ g}=m$ käy). Näin ollen ehtojen (i)–(iii) nojalla H on määritelmän mukaan G:n aliryhmä. (**3 p**)

Osoitetaan sitten, että aliryhmä H on G:n normaali aliryhmä. Olkoon $f\in H$ ja $g\in G$. On osoitettava, että $h=g\circ f\circ g^{-1}\in H$. Huomataan, että luvulle $n\in\mathbb{N}$ pätee, että $h(n)=g(f(g^{-1}(n)))=n$, jos $f(g^{-1}(n))=g^{-1}(n)$ ja siis jos $g^{-1}(n)\geq m_f$. Etsitään luku $m\in\mathbb{N}$, jolla ehdosta $n\geq m$ seuraa, että

$g^{-1}(n) \geq m_f$, eli jolla ehdosta $g^{-1}(n) < m_f$ seuraa, että $n < m$. Olkoon $J = \{k \in \mathbb{N} \mid k < m_f\}$; tällöin kullakin $n \in \mathbb{N}$ pätee seuraava: $g^{-1}(n) < m_f \iff g^{-1}(n) \in J \iff n \in g(J)$. Nyt J on äärellinen, joten myös sen kuvajoukko $g(J)$ on äärellinen ja täten rajoitettu. Näin ollen on olemassa luku $m \in \mathbb{N}$, jolla $n < m$ kaikilla $n \in g(J)$. Tälle siis pätee, että $h(n) = n$ kaikilla $n \geq m$, jolloin $h \in H$ ($m_h = m$ käy). (**3 p**)

4. Olkoon R rengas, ja olkoon $Y_2(R)$ kaikkien R-kertoimisten 2-rivisten yläkolmiomatriisien

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \qquad (a, b, c \in R,\ 0 = 0_R)$$

joukko varustettuna matriisien tavanomaisilla yhteen- ja kertolaskuilla:

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} + \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} = \begin{pmatrix} a+a' & b+b' \\ 0 & c+c' \end{pmatrix}; \qquad \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} = \begin{pmatrix} aa' & ab'+bc' \\ 0 & cc' \end{pmatrix}.$$

Pidetään tunnettuna, että tällöin $Y_2(R)$ on rengas (tämä voidaan todistaa aivan kuten $\mathbb{R}$-kertoimisten matriisien tapauksessa; ei todellakaan tarvitse olettaa, että rengas R olisi kommutatiivinen).

Osoita nyt, että joukko $J = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \mid b \in R \right\} \subset Y_2(R)$ on renkaan $Y_2(R)$ ideaali ja että tekijärengas $Y_2(R)/J$ on isomorfinen tulorenkaan $R \times R$ kanssa; anna myös tämä isomorfismi. **Ohje.** Sovella renkaiden homomorfialausetta kuvaukseen $f\colon Y_2(R) \to R \times R$, jolla $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto (a, c)$.

Ratk. Osoitetaan ensin, että f on rengashomomorfismi ja että $\mathrm{Ker}(f) = J$. Jos $\alpha = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in Y_2(R)$ ja $\alpha' = \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} \in Y_2(R)$, niin

$$f(\alpha\alpha') = f\left(\begin{pmatrix} a+a' & b+b' \\ 0 & c+c' \end{pmatrix}\right) = (a+a', c+c') = (a,c) + (a',c') = f(\alpha) + f(\alpha') \quad \text{ja}$$
$$f(\alpha\alpha') = f\left(\begin{pmatrix} aa' & ab'+bc' \\ 0 & cc' \end{pmatrix}\right) = (aa', cc') = (a,c)(a',c') = f(\alpha)f(\alpha');$$

lisäksi $f(1_{Y_2(R)}) = f\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = (1,1) = 1_{R\times R}$. Siis f on rengashomomorfismi. Jos $\alpha = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in Y_2(R)$, niin $\alpha \in \mathrm{Ker}(f) \iff f(\alpha) = 0_{R\times R} \iff (a,c) = (0,0) \iff \alpha \in J$; siis $\mathrm{Ker}(f) = J$.
Tällöin $J = \mathrm{Ker}(f)$ on renkaan $Y_2(R)$ ideaali (tätä ei siis tarvinnut todistaa erikseen, mutta tehtävänannossa J oli mainittava ideaaliksi, jotta voitiin puhua tekijärenkaasta $Y_2(R)/J$). Jos $(a,c) \in R \times R$, niin $\alpha = \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \in Y_2(R)$ ja $f(\alpha) = (a,c)$, joten f on surjektio. Täten renkaiden homomorfialauseen perusteella f indusoi rengasisomorfismin $\overline{f}\colon Y_2(R)/J \to R \times R$, $\alpha + J \mapsto f(\alpha)$.

5. Esitä polynomi $f = x^4 - 5x^3 + x^2 - 2x - 15$ renkaassa $\mathbb{Q}[x]$ jaottomien polynomien tulona.

Ratk. Kerroinrengas $\mathbb{Q}$ on kunta, ja f on pääpolynomi (johtava kerroin = 1). Siis f:llä on tekijöiden järjestystä vaille yksikäsitteinen esitys jaottomien pääpolynomien tulona, ja tulossa tekijäin asteiden summa on sama kuin f:n aste 4. Jos $c \in \mathbb{Q}$ on f:n nollakohta, niin $c \in \mathbb{Z}$ ja $c|(-15)$ eli $c = \pm 1, \pm 3, \pm 5$ tai ± 15 (ks. kevään 2009 ht 11:4). Nyt $f(1) = -20$, $f(-1) = -6$, $f(3) = -66, f(-3) = 216$, $f(5) = 0$, $f(-5) = 1270$, $f(15) = 33930$ ja $f(-15) = 67740$. Täten $\{c \in \mathbb{Q} \mid f(c) = 0\} = \{5\}$. Siis $(x-5)|f$, ja $x - 5$ on jaoton 1. asteen polynomina. Jakokulmassa jakamalla saadaan, että $f = (x-5)(x^3+x+3)$. Tarkastellaan polynomia $g = x^3 + x + 3 \in \mathbb{Q}[x]$. Jos $c \in \mathbb{Q}$ ja $g(c) = 0$, niin myös $f(c) = (c-5)g(c) = 0$, joten $c = 5$. Mutta $g(5) = 133$, joten g:llä ei ole nollakohtia. Koska $\deg(g) = 3$, tästä seuraa, että g on jaoton (sillä muuten g:llä olisi välttämättä 1. asteen tekijä ja siis nollakohta). Täten $f = \underline{(x-5)(x^3+x+3)}$ on vaadittu esitys. (**Vaihtoehtoisesti** voi heti huomata, että $f = x^3(x-5) + (x+3)(x-5) = (x^3+x+3)(x-5)$ ja että polynomilla $g = x^3+x+3$ ei ole nollakohtaa $c \in \mathbb{Q}$, koska vakiokertoimen 3 tekijöille on $g(1) = 5$, $g(-1) = 1$, $g(3) = 33$ ja $g(-3) = -27$.)