Algebra I/Ylimääräinen harjoitus 12, 20.–24.4.2009/ratk. (JL), 2 sivua

1. Olkoot H ja K äärellisen ryhmän G aliryhmiä niin, että $\operatorname{syt}(|H|,|K|)=1$. Osoita, että $|H\cap K|=1$.

Ratk. Olkoon $h=|H|$, $k=|K|$ ja $n=|H\cap K|$. Koska $H\cap K\le H$ ja $H\cap K\le K$, niin $n|h$ ja $n|k$ Lagrangen lauseen mukaan, joten $n|\operatorname{syt}(h,k)$ eli $n|1$ ja siis $n=1$.

2. Olkoon G (multiplikatiivinen) ryhmä, $H\le G$ aliryhmä ja $N\trianglelefteq G$ normaali aliryhmä.

a) Harjoitustehtävässä 8:2 osoitettiin, että HN on G:n aliryhmä. Osoita, että $HN=\langle H\cup N\rangle$.

b) Oletetaan, että $H\cap N=\{1_G\}$ ja $\langle H\cup N\rangle=G$. Osoita, että tekijäryhmä G/N on isomorfinen H:n kanssa.

Ratk. a) Siis $\langle H\cup N\rangle$ on osajoukon $H\cup N\subset G$ virittämä G:n aliryhmä, ja $HN=\{hn\mid h\in H,\,n\in N\}$. Nyt $H=H\{1\}\subset HN$ ja $N=\{1\}N\subset HN$, joten $H\cup N\subset HN$ ja siis $\langle H\cup N\rangle\subset HN$. Toisaalta $H\subset H\cup N\subset\langle H\cup N\rangle$ ja $N\subset H\cup N\subset\langle H\cup N\rangle$, joten $HN\subset\langle H\cup N\rangle$. Siis $HN=\langle H\cup N\rangle$.

b) Kanonisen surjektion $p\colon G\to G/N$ rajoittuma $f=p|H\colon H\to G/N$ on ryhmähomomorfismi; osoitetaan, että f on bijektio. Jos $a\in H$ ja $f(a)=1_{G/N}$, niin $aN=N$ ja siis $a\in N$, joten $a\in H\cap N=\{1_G\}$. Täten $\operatorname{Ker}(f)=\{1_G\}$, ja f on injektio. Jos $x\in G/N$, niin $x=p(a)=aN$ jollain $a\in G$; koska $G=HN$, niin $a=hn$ joillain $h\in H$, $n\in N$, ja tällöin $f(h)=hN=hnN=aN=x$. Siis f on surjektio. Täten f on ryhmäisomorfismi $H\xrightarrow{\sim}G/N$.

II tod. ryhmähomomorfialauseen avulla. Konstruoidaan surjektiivinen ryhmähomomorfismi $g_0\colon G\to H$, jolla $\operatorname{Ker}(g_0)=N$; tällöin ryhmähomomorfialauseen perusteella g_0 indusoi ryhmäisomorfismin $g\colon G/N\xrightarrow{\sim}H$.

Huomataan, että jos $h_1,h_2\in H$, $n_1,n_2\in N$ ja $h_1n_1=h_2n_2$, niin $h_2^{-1}h_1=n_2n_1^{-1}\in H\cap N=\{1_G\}$, ja siis $h_1=h_2$ (sekä $n_1=n_2$); koska $G=HN$, voidaan siis määritellä kuvaus $g_0\colon G\to H$ asettamalla $g_0(hn)=h$, kun $h\in H$ ja $n\in N$. Osoitetaan, että g_0 on ryhmähomomorfismi. Olkoon $a_1,a_2\in G$; tällöin on olemassa $h_1,h_2\in H$ ja $n_1,n_2\in N$, joilla $a_1=h_1n_1$ ja $a_2=h_2n_2$; koska N on normaali aliryhmä, niin $a_1a_2=(h_1n_1)(h_2n_2)=(h_1h_2)(n_1'n_2)$ jollain $n_1'\in N$, joten $g_0(a_1a_2)=h_1h_2=g_0(a_1)g_0(a_2)$, kuten haluttiin. Jos $h\in H$, niin $g_0(h)=g_0(h1_G)=h$; siis g_0 on surjektio. Osoitetaan lopuksi, että $\operatorname{Ker}(g_0)=N$. Jos $n\in N$, niin $g_0(n)=g(1_Gn)=1_G$; kääntäen, jos $h\in H$, $n\in N$ ja $h=g_0(hn)=1_G$, niin $hn=n\in N$.

Huom. Isomorfismit f ja g ovat toistensa käänteiskuvaukset, sillä $g(f(h))=g(hN)=g_0(h)=h$, kun $h\in H$.

3. Olkoon $(A,+)$ Abelin ryhmä. Alkio $a\in A$ on *torsioalkio*, jos $\operatorname{ord}(a)<\infty$, ts. $na=0$ jollain $n\in\mathbb{N}_+$. Osoita, että $T(A)=\{a\in A\mid a\text{ on torsioalkio}\}$ on A:n aliryhmä. Osoita vielä, että tekijäryhmässä $A/T(A)$ vain neutraalialkio on torsioalkio.

Ratk. Koska $1\cdot 0=0$, niin $0\in T(A)$ ja siis $T(A)\ne\emptyset$. Jos $a,b\in T(A)$, niin $ma=0$ ja $nb=0$ joillakin $m,n\in\mathbb{N}_+$, jolloin $(mn)(a-b)=(mn)a-(mn)b=n(ma)-m(nb)=n\cdot 0-m\cdot 0=0-0=0$ ja siis $a-b\in T(A)$. Aliryhmäkriteerion nojalla $T(A)$ on täten A:n aliryhmä.

Koska A on kommutatiivinen, niin $T(A)$ on A:n normaali aliryhmä ja tekijäryhmä $A/T(A)$ on Abelin ryhmä. Olkoon $x\in T(A/T(A))$. Tällöin on olemassa $a\in A$ ja $n\in\mathbb{N}_+$, joilla $x=a+T(A)$ ja $nx=0_{A/T(A)}$. Silloin $na+T(A)=nx=T(A)$ ja siis $na\in T(A)$, joten on olemassa $m\in\mathbb{N}_+$, jolla $m(na)=0$. Nyt $(mn)a=m(na)=0$, joten $a\in T(A)$ ja siis $x=a+T(A)=T(A)=0_{A/T(A)}$. (Täten $T(A/T(A))=\{T(A)\}$.)

4. Osoita, että renkaan R *keskus* $C(R)=\{a\in R\mid ab=ba\text{ kaikilla }b\in R\}$ on R:n alirengas.

Ratk. Koska $1b=b=b1$ kaikilla $b\in R$, niin $1\in C(R)$. Jos $a,a'\in C(R)$, niin $(a-a')b=ab-a'b=ba-ba'=b(a-a')$ ja $(aa')b=a(a'b)=a(ba')=(ab)a'=(ba)a'=b(aa')$ kaikilla $b\in R$, joten $a-a'\in C(R)$ ja $aa'\in C(R)$. Siis alirenkaan määritelmän mukaan $C(R)$ on R:n alirengas.

5. Olkoon R kommutatiivinen rengas. Kerrataan harjoitustehtävästä 9:5, että alkiota $a\in R$ sanotaan nilpotentiksi, jos $a^n=0$ jollain $n\in\mathbb{N}_+$, ja harjoitustehtävästä 9:6, että $N(R)=\{a\in R\mid a\text{ on nilpotentti}\}$ on R:n ideaali. Määritä $N\big(R/N(R)\big)$.

Ratk. Myös tekijärengas $R/N(R)$ on kommutatiivinen. Tietysti renkaan $R/N(R)$ nolla-alkio 0 on nilpotentti renkaassa $R/N(R)$. Olkoon kääntäen x renkaan $R/N(R)$ nilpotentti alkio. Tällöin on olemassa $a\in R$ ja $m\in\mathbb{N}_+$, joilla $x=a+N(R)$ ja $x^m=0$. Silloin $a^m+N(R)=x^m=N(R)$ ja siis $a^m\in N(R)$, joten löytyy

$n \in \mathbb{N}_+$, jolla $(a^m)^n = 0$. Nyt $a^{mn} = (a^m)^n = 0$, joten $a \in N(R)$ ja siis $x = N(R) = 0$. Täten $N(R/N(R)) = \{0\}$.

6. Määritä renkaassa $\mathbb{Z}_7[x]$ polynomien $f = x^3 + 2x^2 + x + 1$ ja $g = x^2 + 5$ (jokin) suurin yhteinen tekijä ja esitä se muodossa $uf + vg$ joillain $u, v \in \mathbb{Z}_7[x]$.

Ratk. Huomataan, että $\mathbb{Z}_7$ on kunta. Koska (jakokulmassa jakaen saadaan ja on myös helppo tarkastaa, että) $f = (x+2)g+(3x+5)$ ja $g = (5x+1)(3x+5)$, niin $3x+5 = \mathrm{syt}(f, g)$ ja $3x+5 = f-(x+2)g = f+(6x+5)g$.

Koska $3^{-1} = 5$ kunnassa $\mathbb{Z}_7$, niin pääpolynomiratkaisu on $\mathrm{syt}(f, g) = 5(3x + 5) = x + 4$, ja tälle on $x + 4 = 5(f + (6x + 5)g) = 5f + (2x + 4)g$.

7. Jaa alkutekijöihin polynomi $x^3 + 5x^2 + 5$ renkaassa $\mathbb{Z}_{11}[x]$ ja polynomi $x^4 + 1$ renkaassa $\mathbb{Z}_2[x]$.

Ratk. Koska 11 ja 2 ovat alkulukuja, niin molemmat kerroinrenkaat $\mathbb{Z}_{11}$ ja $\mathbb{Z}_2$ ovat kuntia.

Olkoon $f = x^3 + 5x^2 + 5 \in \mathbb{Z}_{11}[x]$. Tällöin $f(1) = 1 + 5 + 5 = 11 = 0$, $f(2) = 8 + 20 + 5 = 33 = 0$ ja $f(3) = 27 + 45 + 5 = 77 = 0$, joten $(x - 1)(x - 2)(x - 3)|f$; koska f:n johtava kerroin on $= 1$ ja $\deg(f) = 3$, niin täten on $f = (x - 1)(x - 2)(x - 3)$, jaottomien polynomien tulo.

Olkoon $g = x^4 + 1 \in \mathbb{Z}_2[x]$. Tällöin $g = x^4 + 1 = x^4 + 2x^2 + 1 = (x^2 + 1)^2 = (x^2 + 2x^2 + 1)^2 = ((x + 1)^2)^2 = (x + 1)^4$ on haluttu g:n esitys $\mathbb{Z}_2[x]$:ssä jaottomien polynomien tulona.

8. Olkoon I polynomin $x^3 + x^2 + 1$ virittämä renkaan $\mathbb{Z}_2[x]$ ideaali. Osoita, että tekijärengas $\mathbb{Z}_2[x]/I$ on 8-alkioinen kunta. Tutki sen struktuuria.

Ratk. Olkoon $f = x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$. Tällöin $f(0) = 1$ ja $f(1) = 3 = 1$, joten f:llä ei ole nollakohtia; koska $\deg(f) = 3$, niin täten f on jaoton. Siis, kun $I = \langle f \rangle$, niin tekijärengas $L = \mathbb{Z}_2[x]/I$ on kunta, joka on kunnan $\mathbb{Z}_2$ laajennus ja jonka kertaluku on $|\mathbb{Z}_2|^{\deg(f)} = 2^3 = 8$.

Olkoon $\omega = x + I \in L$. Tällöin, kun f ajatellaan L-kertoimiseksi polynomiksi, niin ω on f:n nollakohta L:ssä: $f(\omega) = 0$ eli $\omega^3 = -\omega^2 - 1$ eli siis

$$\omega^3 = \omega^2 + 1.$$

Kunnan L alkioilla on yksikäsitteinen esitys muotoa $a + b\omega + c\omega^2 \quad (a, b, c \in \mathbb{Z}_2)$. Yhteenlasku L:ssä saa muodon

$$(a + b\omega + c\omega^2) + (a' + b'\omega + c'\omega^2) = (a + a') + (b + b')\omega + (c + c')\omega^2,$$

kun $a, b, c, a', b', c' \in \mathbb{Z}_2$. Huomataan, että

$$\omega^4 = \omega\omega^3 = \omega(\omega^2 + 1) = \omega^3 + \omega = \omega^2 + \omega + 1.$$

Kertolasku L:ssä saa täten muodon (lopuksi on yritetty sieventää ω^0:n, ω^1:n ja ω^2:n kertoimia)

$$\begin{aligned}
&(a + b\omega + c\omega^2)(a' + b'\omega + c'\omega^2) \\
&\quad = aa' + (ab' + a'b)\omega + (ac' + a'c + bb')\omega^2 + (bc' + b'c)\omega^3 + cc'\omega^4 \\
&\quad = aa' + (ab' + a'b)\omega + (ac' + a'c + bb')\omega^2 + (bc' + b'c)(\omega^2 + 1) + cc'(\omega^2 + \omega + 1) \\
&\quad = (aa' + bc' + b'c + cc') + (ab' + a'b + cc')\omega + (ac' + a'c + bb' + bc' + b'c + cc')\omega^2 \\
&\quad = (aa' + bb' + (b + c)(b' + c')) + (ab' + a'b + cc')\omega + (ac' + a'c + (b + c)(b' + c'))\omega^2,
\end{aligned}$$

kun $a, b, c, a', b', c' \in \mathbb{Z}_2$.