Matematiikan ja tilastotieteen laitos
Algebra I (Kevät 2009)
Harjoitus 9
Ratkaisuja (Jussi Martin)

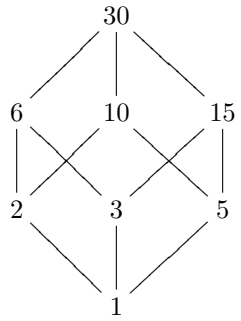
1. a) Etsi syklisen ryhmän $\mathbb{Z}_{30}$ kaikki aliryhmät (riittää ilmoittaa kunkin virittäjä) ja piirrä kaavio niiden sisältyvyyksistä toisiinsa. Jos H ja K ovat $\mathbb{Z}_{30}$:n aliryhmiä, joilla on $H \lneqq K$ eli yhtäpitävästi $H < K$, mutta joilla $H < L < K$ ei päde yhdelläkään $\mathbb{Z}_{30}$:n aliryhmällä L, niin sijoita piirroksessa K ylemmäksi kuin H ja yhdistä ne viivalla. *Ohje.* Etsi ensin luvun 30 positiiviset tekijät ja piirrä vastaava kaavio niiden jaollisuudesta toisillaan.

b) Määritä syklisen ryhmän $\mathbb{Z}_{18}$ kaikkien alkioiden kertaluvut. *Ohje.* Valmiilla kaavalla määrittämättä alkioiden virittämiä aliryhmiä.

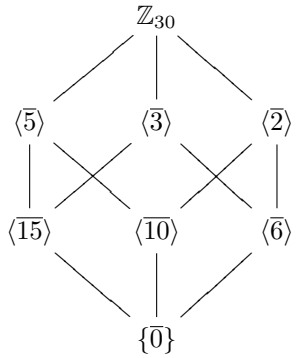
Ratkaisu:

a)-kohta:

Luvun 30 positiivisten tekijöiden jaollisuuskaavio:



Vastaavaa kertalukua olevien aliryhmien sisältyvyyskaavio:



b)-kohta:
Sovelletaan luentomonisteen sivun 75 lausetta 7. Koska ryhmässä $\mathbb{Z}_{18}$ on laskutoimituksena yhteenlasku, pätee lause tässä tapauksessa muodossa:

$$a \in \mathbb{Z}_{18}, \quad \operatorname{ord}(a) = n \in \mathbb{N}_+ \quad \Rightarrow \quad \operatorname{ord}(ma) = \frac{n}{\operatorname{syt}(n,m)}.$$

Nyt tiedon $\operatorname{ord}(\overline{1}) = 18$ avulla saadaan laskettua kaikkien alkioiden kertaluvut.

Jos $\text{syt}(18,m)=1$ eli m on jokin luvuista $1,5,7,11,13,17$, on tällöin

$$\text{ord}(\overline{m}) = \text{ord}(m\overline{1}) = \frac{18}{\text{syt}(18,m)} = \frac{18}{1} = 18.$$

Jos $\text{syt}(18,m)=2$ eli m on jokin luvuista $2,4,8,10,14,16$, on tällöin

$$\text{ord}(\overline{m}) = \frac{18}{\text{syt}(18,m)} = \frac{18}{2} = 9.$$

Jos $\text{syt}(18,m)=3$ eli m on joko 3 tai 15, on tällöin

$$\text{ord}(\overline{m}) = \frac{18}{\text{syt}(18,m)} = \frac{18}{3} = 6.$$

Jos $\text{syt}(18,m)=6$ eli m on joko 6 tai 12, on tällöin

$$\text{ord}(\overline{m}) = \frac{18}{\text{syt}(18,m)} = \frac{18}{6} = 3.$$

Jos $\text{syt}(18,m)=9$ eli $m=9$, on tällöin

$$\text{ord}(\overline{9}) = \frac{18}{\text{syt}(18,9)} = \frac{18}{9} = 2.$$

Jos $\text{syt}(18,m)=18$ eli $m=18$, on tällöin

$$\text{ord}(\overline{1}) = \frac{18}{\text{syt}(18,18)} = \frac{18}{18} = 1.$$

Koska luvun 18 kaikki tekijät ovat $1,2,3,6,9,18$, on kaikki mahdolliset tapaukset käyty läpi.

2. Olkoon $n \in \mathbb{N}_+$. Osoita, että joukko $\mathbb{Z}[\sqrt{n}] = \{a + b\sqrt{n} \mid a,b \in \mathbb{Z}\}$ on renkaan $\mathbb{R}$ alirengas.

Ratkaisu:
Olkoon $r_1 = a_1 + b_1\sqrt{n}$, $r_2 = a_2 + b_2\sqrt{n}$, missä $a_1,b_1,a_2,b_2 \in \mathbb{Z}$. Tällöin

$$r_1 - r_2 = a_1 - a_2 + (b_1 - b_2)\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$$

ja

$$\begin{aligned} r_1 r_2 &= (a_1 + b_1\sqrt{n})(a_2 + b_2\sqrt{n}) = a_1a_2 + a_1b_2\sqrt{n} + b_1a_2\sqrt{n} + b_1b_2(\sqrt{n})^2 \\ &= (a_1a_2 + b_1b_2n) + (a_1b_2 + b_1a_2)\sqrt{n} \in \mathbb{Z}[\sqrt{n}]. \end{aligned}$$

Lisäksi $1 = 1 + 0\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$.

Edellä olleet kolme kohtaa osoittavat, että $\mathbb{Z}[\sqrt{n}]$ on $\mathbb{R}$:n alirengas.

3. Oletetaan tunnetuksi, että jos $n \in \mathbb{N}_+$, niin $\sqrt{n}$ on irrationaalinen jos ja vain jos n ei ole minkään kokonaisluvun neliö. Ovatko renkaat $\mathbb{Z}[\sqrt{2}]$ ja $\mathbb{Z}[\sqrt{3}]$ isomorfiset? Etsi kaikki rengasisomorfismit $\mathbb{Z}[\sqrt{5}] \to \mathbb{Z}[\sqrt{5}]$.

Ratkaisu:
Olkoon $f : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{3}]$ rengashomomorfismi. Tällöin

$$\begin{aligned} f(\sqrt{2})^2 = f(\sqrt{2}^2) = f(2) = f(1+1) \\ = f(1) + f(1) = 1 + 1 = 2 \Leftrightarrow f(\sqrt{2}) = \pm\sqrt{2}. \end{aligned}$$

Nyt $f(\sqrt{2}) \notin \mathbb{Z}[\sqrt{3}]$, sillä jos joillakin $a,b \in \mathbb{Z}$ pätisi $f(\sqrt{2}) = a + b\sqrt{3}$, niin tällöin

$$2 = (a + b\sqrt{3})^2 = a^2 + 3b^2 + 2ab\sqrt{3}.$$

Koska aina $a^2 + 3b^2 \leq 1$ tai $a^2 + 3b^2 \geq 3$, niin $ab \neq 0$, joten

$$\sqrt{3} = \frac{2 - a^2 - 3b^2}{2ab} \in \mathbb{Q},$$

mikä on ristiriita.

Kyseistä rengashomomorfismia ei siis voi olla olemassa, eivätkä renkaat $\mathbb{Z}[\sqrt{2}]$ ja $\mathbb{Z}[\sqrt{3}]$ voi siten myöskään olla isomorfiset keskenään.

Olkoon nyt sitten $f : \mathbb{Z}[\sqrt{5}] \to \mathbb{Z}[\sqrt{5}]$ rengasisomorfismi. Tällöin

$$f(k) = kf(1) = k \cdot 1 = k, \quad \text{kaikilla} \quad k \in \mathbb{Z}$$

ja

$$f(n\sqrt{5}) = f(n)f(\sqrt{5}) = nf(\sqrt{5}), \quad \text{kaikilla} \quad n \in \mathbb{Z}.$$

Toisaalta

$$f(\sqrt{5})^2 = f(\sqrt{5}^2) = f(5) = 5,$$

joten

$$f(\sqrt{5}) = \pm\sqrt{5}.$$

Mahdolliset isomorfismit ovat siis: identtinen kuvaus ja kuvaus

$$f : \mathbb{Z}[\sqrt{5}] \to \mathbb{Z}[\sqrt{5}], \quad k + n\sqrt{5} \mapsto k - n\sqrt{5},$$

joka nähdään rengashomomorfismiksi seuraavasti:

$$f(a_1 + b_1\sqrt{5}) + f(a_2 + b_2\sqrt{5}) = a_1 - b_2\sqrt{5} + a_2 - b_2\sqrt{5}$$
$$= (a_1 + a_2) - (b_1 + b_2)\sqrt{5} = f((a_1 + a_2) + (b_1 + b_2)\sqrt{5})$$

ja

$$f(a_1 + b_1\sqrt{5})f(a_2 + b_2\sqrt{5}) = (a_1 - b_1\sqrt{5})(a_2 - b_2\sqrt{5})$$
$$= a_1a_2 - a_1b_2\sqrt{5} - b_1a_2\sqrt{5} + (-b_1\sqrt{5})(-b_2\sqrt{5})$$
$$= a_1a_2 + 5b_1b_2 - (a_1b_2 + b_1a_2)\sqrt{5}$$
$$= f(a_1a_2 + 5b_1b_2 + (a_1b_2 + b_1a_2)\sqrt{5}) = f((a_1 + b_1\sqrt{5})(a_2 + b_2\sqrt{5})),$$

kun $a_1, b_1, a_2, b_2 \in \mathbb{Z}$. Näiden lisäksi

$$f(1) = f(1 + 0\sqrt{5}) = 1 - 0\sqrt{5} = 1,$$

joten f on rengashomomorfismi. Isomorfisuus puolestaan seuraa siitä, että

$$f^2(a + b\sqrt{5}) = f(f(a + b\sqrt{5}) = a + (-1)^2b\sqrt{5} = a + b\sqrt{5}, \quad \text{kaikilla} \quad a, b \in \mathbb{Z},$$

joten f on oma käänteiskuvauksensa ja siten myös automorfismi renkaalta $\mathbb{Z}[\sqrt{5}]$ sille itselleen.

4. Osoita, että renkaan $\mathbb{Z}[\sqrt{5}]$ kääntyvien alkioiden eli yksiköiden ryhmä on

$$\mathbb{Z}[\sqrt{5}]^* = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z},\ a^2 - 5b^2 = \pm 1\}.$$

Anna myös kummassakin tapauksessa $a^2 - 5b^2 = 1$ ja $a^2 - 5b^2 = -1$ esimerkki yksiköstä $a + b\sqrt{5}$, jolla $b \neq 0$.

Ratkaisu:
Oletetaan, että $a + b\sqrt{5}$ on kääntyvä. Merkitään $s = a^2 - 5b^2$. Nyt $s \neq 0$, sillä jos $s = a^2 - 5b^2 = 0$, niin $b = 0$, sillä muutoin $5 = (a/b)^2$, mikä olisi ristiriita; joten myös $a = 0$ ja siis $0 = a + b\sqrt{5}$ on kääntyvä, mikä jälleen olisi ristiriita.

Olkoon $c + d\sqrt{5} = 1/(a + b\sqrt{5})$. Tällöin

$$c + d\sqrt{5} = \frac{1}{a + b\sqrt{5}} = \frac{a - b\sqrt{5}}{a^2 - 5b^2} = \frac{a - b\sqrt{5}}{s},$$

joten $a = sc$ ja $b = -sd$; nyt $s = a^2 - 5b^2 = s^2(c^2 - 5d^2)$ ja siis $1 = s(c^2 - 5d^2)$, joten $|s| = 1$.

Toisaalta, jos $|s| = 1$, niin $a + b\sqrt{5}$ on kääntyvä. Nimittäin, jos $s = 1$, on

$$(a + b\sqrt{5})(a - b\sqrt{5}) = a^2 - (b\sqrt{5})^2 = a^2 - 5b^2 = s = 1$$

ja kommutatiivisuuden nojalla myös $(a-b\sqrt{5})(a+b\sqrt{5})=1$ eli $1/(a+b\sqrt{5}) = a-b\sqrt{5}$. Jos taas $s=-1$, on

$$(a+b\sqrt{5})(-a+b\sqrt{5}) = (b\sqrt{5})^2 - a^2 = 5b^2 - a^2 = -s = 1$$

ja taas kommutatiivisuudesta seuraa, että myös $(-a+b\sqrt{5})(a+b\sqrt{5}) = 1$ eli $1/(a+b\sqrt{5}) = -a+b\sqrt{5}$.

Esimerkki yksiköstä $a+b\sqrt{5}$, jolla $a^2-5b^2=1$:

$$9+4\sqrt{5}.$$

Esimerkki yksiköstä $a+b\sqrt{5}$, jolla $a^2-5b^2=-1$:

$$2+\sqrt{5}.$$

5. Olkoon R rengas. Alkio $a \in R$ on *nilpotentti*, jos $a^n = 0$ jollain $n \in \mathbb{N}_+$. Osoita, että jos $a \in R$ on nilpotentti, niin $1+a$ on kääntyvä. *Ohje.* Arvaa, minkä äärellisen "geometrisen" sarjan summa $(1+a)^{-1}$ olisi.

Ratkaisu:
(Tehtävässä oli oikean kaavan $n \in \mathbb{N}_+$ tilalla alunperin virheellinen kaava $a \in \mathbb{N}_+$.) Olkoon a nilpotentti ja $n \in \mathbb{N}_+$ se luku jolla $a^n = 0$. Tällöin

$$\begin{aligned}(1+a)\Big(\sum_{k=0}^{n-1}(-1)^k a^k\Big) &= \sum_{k=0}^{n-1}(-1)^k a^k + \sum_{k=0}^{n-1}(-1)^k a^{k+1} \\ &\overset{l=k+1}{=} 1 + \sum_{k=1}^{n-1}(-1)^k a^k + \sum_{l=1}^{n}(-1)^{l-1} a^l \\ &= 1 + \sum_{k=1}^{n-1}(-1)^k a^k + \sum_{k=1}^{n-1}(-1)^{k-1} a^k + (-1)^{n-1}a^n \\ &= 1 + (-1)^{n-1}a^n = 1 + 0 = 1.\end{aligned}$$

Vastaavalla laskulla nähdään, että myös $\big(\sum_{k=0}^{n-1}(-1)^k a^k\big)(1+a) = 1$. Näin ollen $1+a$ on siis kääntyvä.

6. Olkoon R kommutatiivinen rengas ja $\mathrm{Nil}(R) = \{a \in R \mid a \text{ on nilpotentti}\}$. Osoita, että $\mathrm{Nil}(R)$ on R:n ideaali.

Ratkaisu:
Ensinnäkin huomataan, että $\mathrm{Nil}(R) \neq \emptyset$, sillä $0^1 = 0$ ja näin ollen $0 \in \mathrm{Nil}(R)$.

Nyt jos $a, b \in \mathrm{Nil}(R)$, niin $a^n = 0$ ja $b^m = 0$, joillakin $n, m \in \mathbb{Z}_+$. Tällöin

$$\begin{aligned}(a-b)^{n+m} &= \sum_{k=0}^{n+m}\binom{n+m}{k} a^{n+m-k}b^k \\ &= 0 + \ldots + 0 = 0 \quad \Rightarrow \quad a-b \in \mathrm{Nil}(R),\end{aligned}$$

sillä jos $0 \le k \le m$, niin $m-k \ge 0$, joten $a^{n+m-k} = a^{m-k}a^n = a^{m-k}0 = 0$, ja jos taas $m \le k \le m+n$, niin $k-m \ge 0$, joten $b^k = b^{k-m}b^m = b^{k-m}0 = 0$.

Tässä käytettiin *binomikaavaa*

$$(x+y)^n = \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k, \quad \binom{n}{k} = \frac{n!}{k!(n-k)!}, \quad n \in \mathbb{N}_+;$$

mikä oli oikeutettua, koska R oletettiin kommutatiiviseksi renkaaksi.

Lisäksi kommutatiivisuudesta seuraa nyt, että

$$x \in R \quad \Rightarrow \quad (xa)^n = x^n a^n = a^n x^n = 0 \cdot x^n = 0 \quad \Rightarrow \quad xa = ax \in \mathrm{Nil}(R),$$

kun $a \in \mathrm{Nil}(R)$ ja $n \in \mathbb{N}_+$ on luku jolla $a^n = 0$.

Edellä olevat kohdat ja se, että $\mathrm{Nil}(R)$ on epätyhjä, yhdessä osoittavat, että $\mathrm{Nil}(R)$ on R:n ideaali.