LUKUTEORIAA

1 Jakajat ja jäännökset

Luonnollisten lukujen joukko

$$\mathbb{N} \;=\; \{\, 0, 1, 2, 3, \ldots \,\}$$

on *hyvinjärjestetty*, eli jokaisessa epätyhjässä joukossa $J \subseteq \mathbb{N}$ on pienin alkio. Otetaan käyttöön merkintä

$$\mathbb{Z}_+ = \{1, 2, 3, \ldots\},$$

jolla siis viitataan *positiivisten kokonaislukujen* joukkoon. (Joukko

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

on *kokonaislukujen* joukko.)

Lause 1.1 (Jakoyhtälö)**.** *Olkoon $d \in \mathbb{Z}_+$ positiivinen kokonaisluku. Jokaisella $x \in \mathbb{Z}$ on olemassa yksikäsitteiset $q, r \in \mathbb{Z}$ siten, että*

$$x = qd + r,$$

missä $0 \leq r < d$.

Todistus. Käsitellään luennolla. □

Määritelmä 1.2. Oletetaan, että $x \in \mathbb{Z}$ ja $d \in \mathbb{Z}_+$, ja että

$$x = qd + r,$$

missä $q \in \mathbb{Z}$ ja $0 \leq r < d$. Tällöin sanomme, että r on x:n *jakojäännös* jaettaessa d:llä. Otetaan käyttöön merkintä $r = [x]_d$. Jos d on selvä asiayhteydestä, voimme käyttää myös merkintää $r = [x]$.

Esimerkki. Tarkastellaan lukua 2807. Tämä luku voidaan esittää muodossa

$$2807 \;=\; 2 \cdot 10^3 + 8 \cdot 10^2 + 0 \cdot 10^1 + 7 \cdot 10^0,$$

eli luvun 10 potenssien summana. Luvun 2807 esitys *kymmenjärjestelmässä*, eli desimaalijärjestelmässä, perustuu esitykseen luvun 10 potenssien summana.

Esitetään seuraavaksi luku 2807 vastaavalla tavalla luvun 8 potenssien summana.

$$2807 = 5 \cdot 8^3 + 3 \cdot 8^2 + 6 \cdot 8^1 + 7 \cdot 8^0,$$

eli luku 2807 esitettynä 8-järjestelmässä on 5367. □

Esimerkki. Esitetään luku 2807 luvun 16 potenssien summana.

$$2807 = 10 \cdot 16^2 + 15 \cdot 16^1 + 7 \cdot 16^0.$$

Merkitään $A = 10,\ B = 11,\ C = 12,\ D = 13,\ E = 14,\ F = 15$. Luvun 2807 esitys 16-järjestelmässä on nyt $AF7$. □

Esimerkki. Esitetään luku 53 binäärijärjestelmässä. Esimerkki käsitellään luennolla. □

Esimerkki. Lasketaan 8-järjestelmän lukujen 312 ja 702 summa. Käsitellään luennolla. □

Lause 1.3. *Olkoon $b \in \mathbb{N} \setminus \{0, 1\}$ ja $x \in \mathbb{Z}_+$. Tällöin on olemassa sellaiset yksikäsitteiset luvut $d_0, d_1, ..., d_k \in \mathbb{N}$, että*

$$x = d_k b^k + d_{k-1} b^{k-1} + ... + d_0 b^0,$$

missä $d_k \neq 0$ ja $0 \leq d_i < b_i$ kaikilla $i \in \{0, ..., k\}$.

Todistus. Käsitellään luennolla. □

Lauseen 1.3 esitys

$$x = d_k b^k + d_{k-1} b^{k-1} + ... + d_0 b^0$$

antaa jonon $(d_k, d_{k-1}, ..., d_0)$, joka vastaa luvun x esitystä b-järjestelmässä; huomaa kuitenkin, että esim. luvun 2807 esitys 16-järjestelmässä on $AF7$, missä $A = 10$ ja $F = 15$, ja tätä vastaava jono on $(10, 15, 7)$, mutta luku 10157 *ei ole* luvun 2807 esitys 16-järjestelmässä.

Määritelmä 1.4. Olkoot $a, b, c \in \mathbb{Z}$ lukuja siten, että $a = bc$. Tällöin luku b on luvun a *jakaja* (tai *tekijä*). Sanotaan, että luku b *jakaa* luvun a. Merkitään $b \,|\, a$ (lue: b jakaa a:n).

- $1 \,|\, a,\ -1 \,|\, a,\ a \,|\, a,\ -a \,|\, a$.
- $0 \,|\, a \ \Leftrightarrow\ a = 0$.
- $bc \,|\, a \ \Rightarrow\ b \,|\, a$.

- $(a \mid b$ ja $b \mid c) \;\Rightarrow\; a \mid c$.
- $(a \mid b$ ja $a \mid c) \;\Rightarrow\; \forall \lambda, \mu \in \mathbb{Z}\big(\; a \mid \lambda b + \mu c \;\big)$.
- $(a \mid b$ ja $b \mid a) \;\Rightarrow\; a = \pm b$.
- $(a \mid b$ ja $a \mid b + 1) \;\Rightarrow\; a = \pm 1$.

2 Kongruenssit ja jäännösluokat

Määritelmä 2.1 (Gauss)**.** Olkoon $d \in \mathbb{Z}_+$ ja $a, b \in \mathbb{Z}$. Jos $d|b - a$, niin sanomme, että a ja b ovat *kongruentteja modulo* d. Merkitään $a \equiv b \; (mod\; d)$. Mikäli d on tunnettu asiayhteydestä, voimme käyttää myös merkintää $a \equiv b$.

Esimerkki

- $5 \mid 23 - 3$, joten $3 \equiv 23 \pmod 5$.
- $7 \mid 56 - 28$, joten $28 \equiv 56 \pmod 7$.
- $4 \mid 8 + 20$, joten $-20 \equiv 8 \pmod 4$.

Lause 2.2. *Relaatio* $\equiv \; (mod\; d)$ *on ekvivalenssirelaatio, toisin sanoen*

1. $a \equiv a$,
2. $a \equiv b \;\Rightarrow b \equiv a$,
3. $(a \equiv b \; ja \; b \equiv c) \;\Rightarrow\; b \equiv c$.

Todistus. Käsitellään luennolla. □

Mikä on luvun $a \in \mathbb{Z}$ ekvivalenssiluokka relaation $\equiv \pmod d$ suhteen, eli mitkä luvut $b \in \mathbb{Z}$ toteuttavat ehdon $a \equiv b \pmod d$?

$$\begin{aligned} x \equiv a \; (mod\; d) \;&\Leftrightarrow\; d \mid x - a \\ &\Leftrightarrow\; x - a = kd \text{ jollakin } k \in \mathbb{Z} \\ &\Leftrightarrow\; x = a + kd \text{ jollakin } k \in \mathbb{Z}, \end{aligned}$$

joten a:n ekvivalenssiluokka on joukko

$$\{x \in \mathbb{Z} \mid x = a + kd \text{ jollakin } k \in \mathbb{Z} \;\} = a + k\mathbb{Z}.$$

Esimerkiksi luvun 5 ekvivalenssiluokka modulo 12 on joukko

$$\{\; ..., -7, 5, 17, 39, ... \;\} = 5 + 12\mathbb{Z}.$$

Lause 2.3. *Olkoon $d \in \mathbb{Z}_+$. Tällöin*

$$a \equiv b \ (mod\ d) \ \Leftrightarrow \ [a]_d = [b]_d.$$

Todistus. Käsitellään luennolla. □

Jos $a \in \mathbb{Z}$, niin $[a]_{10}$ on sama kuin a:n viimeinen numero. Täten

$$a \equiv b \ mod\ 10 \ \Leftrightarrow \ a\text{:n ja } b\text{:n viimeiset numerot ovat samat.}$$

Jos $a \in \mathbb{Z}$ ja $d \in \mathbb{Z}_+$, niin

$$a + d\mathbb{Z} \ = \ \{\ x \in \mathbb{Z} \mid [x]_d = [a]_d\ \}.$$

Tätä ekvivalenssiluokkaa sanotaan luvun *a jäännösluokaksi* modulo d.

Korollaari 2.4. *Olkoon $d \in \mathbb{Z}_+$. Tällöin*

1. $a \equiv [a]_d \ (mod\ d)$.
2. *Mikäli* $0 \leq a \leq b < d$, *niin* $a \equiv b \ (mod\ d) \Leftrightarrow a = b$.

Todistus. Käsitellään luennolla. □

Lause 2.5. *Olkoon $d \in \mathbb{Z}_+$. Oletetaan, että $x_1 \equiv x_2 \ (mod\ d)$ ja $y_1 \equiv y_2$ $(mod\ d)$. Tällöin*

1. $x_1 + y_1 \equiv x_2 + y_2 \ (mod\ d)$,
2. $x_1 y_1 \equiv x_2 y_2 \ (mod\ d)$.

Todistus. Käsitellään luennolla. □

Korollaari 2.6. *Olkoon $d \in \mathbb{Z}_+$ positiivinen kokonaisluku. Jos $x, y \in \mathbb{Z}$, niin*

1. $[x + y]_d = [[x]_d + [y]_d]_d$,
2. $[xy]_d = [[x]_d [y]_d]_d$.

Todistus. Käsitellään luennolla. □

Esimerkki. $[13^{2011}]_4 = [[13]_4^{2011}]_4 = [1^{2011}]_4 = 1$.

Esimerkki (Toistuva neliöinti)**.** Lasketaan "tehokkaasti" $[12^{11}]_{21}$. Esimerkki käsitellään luennolla.

3 Suurin yhteinen tekijä

Luvun 24 positiiviset tekijät ovat $1, 2, 3, 4, 6, 8, 12, 24$. Luvun 36 positiiviset tekijät ovat $1, 2, 3, 4, 6, 9, 12, 18, 36$. Lukujen 24 ja 36 yhteiset positiiviset tekijät ovat $1, 2, 3, 6, 12$. Suurin yhteinen positiivinen tekijä on 12. Kaikki positiiviset yhteiset tekijät ovat luvun 12 tekijöitä.

Määritelmä 3.1. Olkoon $m, n \in \mathbb{Z}$ kokonaislukuja. Luku $d \in \mathbb{N}$ on lukujen m ja n *suurin yhteinen tekijä*, jos

1. $d \,|\, m$ ja $d \,|\, n$,
2. $(p \,|\, m$ ja $p \,|\, n) \;\Rightarrow\; p \,|\, d$.

Näiden ehtojen pätiessä merkitään $d = syt(m, n)$.

Jos lisäksi $d' = syt(m, n)$, niin kohdan 1 nojalla

$$d \,|\, m,\; d \,|\, n,\; d' | \, m, \text{ ja } d' \,|\, n.$$

Kohdan 2 nojalla siis

$$d \,|\, d' \text{ ja } d' \,|\, d.$$

Täten $d' = \pm d$ (HT), joten $d = d'$, sillä $d, d' \in \mathbb{N}$. Täten $syt(m, n)$ on *yksikäsitteinen.*

Esimerkki. Jos $m \in \mathbb{N}$, niin $syt(m, 0) = m$:

1. $m \,|\, m$ ja $m \,|\, 0$,
2. $(p \,|\, m$ ja $p \,|\, 0) \Rightarrow\; p \,|\, m$.

Entä *syt*:n olemassaolo? Olkoot $m, n \in \mathbb{Z}$ kokonaislukuja. Havaitsemme, että

$$(p \,|\, m \text{ ja } p \,|\, n) \;\Leftrightarrow\; (p \,|\, |m| \text{ ja } p \,|\, |n|).$$

Nyt jos $syt(|m|, |n|)$ on olemassa, myös $syt(m, n)$ on olemassa, ja

$$syt(m, n) \;=\; syt(|m|, |n|).$$

Täten *syt*:n olemassaolo seuraa seuraavasta lauseesta:

Lause 3.2 (Eukleideen algoritmi)**.** *Olkoot $m, n \in \mathbb{Z}_+$ positiivisia kokonaislukuja siten, että $m \geq n$. Suoritetaan jakolaskut*

$$\begin{aligned}
m &= q_0 n + r_1 \ (0 \leq r_1 < n),\\
n &= q_1 r_1 + r_2 \ (0 \leq r_2 < r_1),\\
r_1 &= q_2 r_2 + r_3 \ (0 \leq r_3 < r_2),\\
r_2 &= q_3 r_3 + r_4 \ (0 \leq r_4 < r_3),\\
&\cdot\\
&\cdot\\
&\cdot\\
r_{k-2} &= q_{k-1} r_{k-1} + r_k \ (0 \leq r_k < r_{k-1}),\\
r_{k-1} &= q_k r_k.
\end{aligned}$$

Tällöin $syt(m, n)$ on viimeinen nollasta eroava jakojäännös r_k. Algoritmi päättyy, koska $n > r_1 > r_2 > ... \geq 0$.

Todistus. Käsitellään luennolla. □

Esimerkki. Etsitään $syt(326, 78)$. Esimerkki käsitellään luennolla.

Lause 3.3. *Olkoot $m, n \in \mathbb{Z}$ kokonaislukuja. Tällöin on olemassa sellaiset $\lambda, \mu \in \mathbb{Z}$, että*

$$syt(m, n) = \lambda m + \mu n.$$

Todistus. Käsitellään luennolla. □

Havaitsemme, että kertoimet λ ja μ *eivät ole* yksikäsitteisiä, sillä

$$\lambda m + \mu n = (\lambda + kn)m + (\mu - km)n$$

pätee kaikilla $k \in \mathbb{Z}$.

Määritelmä 3.4. Luvut $a, b \in \mathbb{Z}$ ovat *keskenään jaottomia*, mikäli pätee, että $syt(a, b) = 1$.

Lause 3.5. *Olkoot $a, b \in \mathbb{Z}$ kokonaislukuja. Oletetaan, että $a \mid bc$. Jos a ja b ovat keskenään jaottomia, niin $a \mid c$.*

Todistus. Käsitellään luennolla. □

Ratkaistaan *Diofantoksen yhtälö* $ax + by = c$, missä $a, b \in \mathbb{Z} \setminus \{0\}$ ja $c \in \mathbb{Z}$. Tehtävänä on löytää sellaiset $x, y \in \mathbb{Z}$, että $ax + by = c$.

1.) Oletetaan aluksi, että (x_0, y_0) on ratkaisu yhtälölle. Täten siis

$$ax_0 + by_0 = c.$$

Tällöin, jos $d = syt(a, b)$, niin $d \,|\, a$ ja $d \,|\, b$. Täten

$$d \,|\, ax_0 + by_0 = c,$$

eli

$$syt(a, b) = d \,|\, c.$$

2.) Oletetaan, että $syt(a, b) = d \,|\, c$. Huomaa, että $d \neq 0$, sillä $a \neq 0$ ja $b \neq 0$. Nyt

$$d \,|\, c = c'd \text{ jollakin } c' \in \mathbb{Z}.$$

Lauseen 3.3 nojalla on olemassa sellaiset $\lambda, \mu \in \mathbb{Z}$, että

$$\lambda a + \mu b = d.$$

Täten

$$c'\lambda a + c'\mu b = c'd = c,$$

joten

$$\begin{cases} x = \lambda c' \\ y = \mu c' \end{cases}$$

on eräs ratkaisu Diofantoksen yhtälölle $ax + by = c$.

Olemme siis osoittaneet, että Diofantoksen yhtälöllä $ax + by = c$ on ratkaisu jos ja vain jos $syt(a, b) \,|\, c$. Tämä seuraa kohdista 1 ja 2.

Olkoon (x, y) mielivaltainen ratkaisu yhtälöllemme $ax + by = c$, missä $a, b \in \mathbb{Z} \setminus \{0\}$, $c \in \mathbb{Z}$. Tällöin

$$\begin{cases} ax + by = c \\ ax_0 + by_0 = c, \text{ missä } x_0 = \lambda c' \text{ ja } y_0 = \mu c', \end{cases}$$

joten

$$a(x - x_0) + b(y - y_0) = 0,$$

Näin ollen, jakamalla luvulla $d \neq 0$, päätellään, että

$$a'(x - x_0) + b'(y - y_0) = 0, \text{ missä } a' = \frac{a}{d} \text{ ja } b' = \frac{b}{d}.$$

Tässä siis $d = syt(a, b)$. Luvut a' ja b' ovat keskenään jaottomia (Harjoituskerta 2, harjoitus 8), eli $syt(a', b') = 1$. Täten

$$\begin{aligned}
&a'(x - x_0) + b'(y - y_0) = 0 \\
\Rightarrow\ &a'(x - x_0) = -b'(y - y_0) \\
\Rightarrow\ &b' \mid a'(x - x_0) \\
\Rightarrow\ &b' \mid (x - x_0) \quad \text{(Lause 3.5)} \\
\Rightarrow\ &x - x_0 = b'm \text{ jollain } m \in \mathbb{Z} \\
\Rightarrow\ &x = x_0 + mb' \text{ jollain } m \in \mathbb{Z}.
\end{aligned}$$

Samoin osoitetaan, että $y = y_0 + na'$ jollakin $n \in \mathbb{Z}$.

Olemme siis osoittaneet, että jokainen ratkaisu yhtälöllemme $ax + by = c$ on muotoa

$$\begin{cases} x = x_0 + m\frac{b}{d} \\ y = y_0 + n\frac{a}{d}, \end{cases}$$

missä $m, n \in \mathbb{Z}$.

Mitkä muotoa

$$\begin{cases} x = x_0 + m\frac{b}{d} \\ y = y_0 + n\frac{a}{d} \end{cases}$$

olevat luvut x ja y, missä $m, n \in \mathbb{Z}$, ovat sitten ratkaisuja yhtälöllemme $ax + by = c$? Kiinnitetään jotkin luvut $m, n \in \mathbb{Z}$, ja oletetaan, että

$$\begin{cases} x = x_0 + m\frac{b}{d} \\ y = y_0 + n\frac{a}{d}. \end{cases}$$

Nyt pätee

$$\begin{aligned}
ax + by &= a(x_0 + mb') + b(y_0 + na') \\
&= ax_0 + by_0 + amb' + bna' \\
&= c + amb' + bna' \\
&= c + a'dmb' + b'dna' \\
&= c + (m + n)a'b'd.
\end{aligned}$$

Havaitsemme, että

$$
\begin{aligned}
&(x, y) \text{ on ratkaisu yhtälölle} \\
\Leftrightarrow\ &ax + by = c \\
\Leftrightarrow\ &c + (m+n)a'b'd = c \\
\Leftrightarrow\ &(m+n)a'b'd = 0 \\
\Leftrightarrow\ &n = -m \text{ (huomaa, että } a \neq 0 \text{ ja } b \neq 0, \text{ joten } a' \neq 0 \text{ ja } b' \neq 0).
\end{aligned}
$$

Täten Diofantoksen yhtälön $ax+by = c$ (missä siis $a, b \in \mathbb{Z}\setminus\{0\}$ ja $c \in \mathbb{Z}$) ratkaisuja ovat täsmälleen kaikki luvut x ja y siten, että

$$
\begin{cases}
x = x_0 + m\frac{b}{d} \\
y = y_0 - m\frac{a}{d}
\end{cases}
$$

jollekin $m \in \mathbb{Z}$. Tässä $x_0 = \lambda c'$ ja $y_0 = \mu c'$. Luvut λ ja μ ovat vakioita siten, että

$$d = syt(a, b) = \lambda a + \mu b.$$

Esimerkki. Ratkaistaan Diofantoksen yhtälö $36x + 28y = 16$. Käytetään yllä olevia merkintöjä parametreille $a, b, c, d = syt(a, b), \lambda, \mu$ ja $c' = \frac{c}{d}$. Nyt siis $a = 36$, $b = 28$ ja $c = 16$. Etsitään ensiksi *yksittäisratkaisu* Eukleideen algoritmin avulla.

$$
\begin{aligned}
36 &= 1 \cdot 28 + 8, \\
28 &= 3 \cdot 8 + 4, \\
8 &= 2 \cdot 4.
\end{aligned}
$$

Täten $d = syt(36, 28) = 4$. Käsittelemällä saatua yhtälöryhmää takaperin, saamme

$$
\begin{aligned}
4 &= 28 - 3 \cdot 8 \\
&= 28 - 3 \cdot (36 - 1 \cdot 28) \\
&= 4 \cdot 28 - 3 \cdot 36 \\
&= \mu b + \lambda a.
\end{aligned}
$$

Näin saadaan yksittäisratkaisu

$$\begin{cases} x = \lambda c' = -3 \cdot c' = -3 \cdot \frac{c}{d} = -3 \cdot \frac{16}{4} = -12 \\ y = \mu c' = 4 \cdot c' = 4 \cdot \frac{c}{d} = 4 \cdot \frac{16}{4} = 16, \end{cases}$$

eli

$$\begin{cases} x = -12 \\ y = 16. \end{cases}$$

Olemme siis löytäneet *yksittäisratkaisun* $x = -12$ ja $y = 16$. Joskus yksittäisratkaisun voi helposti löytää suoraankin, esimerkiksi yhtälömme $36x + 28y = 16$ tapauksessa havaitaan helpohkosti, että myös $x = 2$ ja $y = -2$ on yksittäisratkaisu yhtälöllemme.

Kun olemme löytäneet yksittäisratkaisun yhtälöllemme, saamme yleisen ratkaisun seuraavasti.

$$\begin{cases} x = -12 + \frac{b}{d}m \\ y = 16 - \frac{a}{d}m, \qquad m \in \mathbb{Z}, \end{cases}$$

eli

$$\begin{cases} x = -12 + 7m \\ y = 16 - 9m, \qquad m \in \mathbb{Z}. \end{cases}$$

Tämä on yleinen ratkaisu yhtälölle $36x + 28y = 16$. Vaihtoehtoisesti, lähtemällä liikkeelle yksittäisratkaisusta

$$\begin{cases} x = 2 \\ y = -2, \end{cases}$$

päädytään yleiseen ratkaisuun

$$\begin{cases} x = 2 + 7m \\ y = -2 - 9m, \qquad m \in \mathbb{Z}. \end{cases}$$

On helppo nähdä, että muotoilemamme yleiset ratkaisut ovat (totta kai) samat.

4 Alkuluvut

Määritelmä 4.1. Kokonaisluku $p > 1$ on *alkuluku*, jos

$$\forall d \in \mathbb{N}\big(\, d \,|\, p \;\Rightarrow\; d \in \{1, p\}\big).$$

Esimerkki. 2,3,5,7 ja 11 ovat alkulukuja. Toisaalta, $6 = 2 \cdot 3$, joten 6 ei ole alkuluku.

Esimerkki. Ongelma: etsi välin $[0, n]$ alkuluvut. Tehtävä voidaan suorittaa *Erastotheneen seulan* avulla. Erastotheneen seulan käyttö käsitellään luennolla.

23.8.2008 suurin tunnettu alkuluku oli $2^{43112609} - 1$. Luvussa on noin 13 miljoonaa numeroa.

Lemma 4.2. *Jokainen luku $n \in \mathbb{N} \setminus \{0, 1\}$ on joko alkuluku tai voidaan esittää alkulukujen tulona.*

Todistus. Käsitellään luennolla. □

Lause 4.3 (Eukleides)**.** *Alkulukuja on äärettömän monta.*

Todistus. Käsitellään luennolla. □

Lause 4.4 (Eukleideen Lemma)**.** *Olkoot $a, b \in \mathbb{Z}$ kokonaislukuja ja olkoon p alkuluku. Jos $p \mid ab$, niin $p \mid a$ tai $p \mid b$.*

Todistus. Käsitellään luennolla. □

Lause 4.5 (Aritmetiikan peruslause)**.** *Jokainen luku $n \in \mathbb{N} \setminus \{0, 1\}$ voidaan esittää järjestystä vaille yksikäsitteisesti alkulukujen tulona.*

Todistus. Käsitellään luennolla. □

Suurin yhteinen tekijä - uusi näkökulma

Lause 4.6. *Olkoot $p_1, ..., p_r$ eri alkulukuja. Olkoot $j_1, ..., j_k \in \mathbb{N}$ luonnollisia lukuja. Tällöin*

$$d \mid p_1^{j_1} \cdot ... \cdot p_r^{j_r} \;\Leftrightarrow\; d = p_1^{k_1} \cdot ... \cdot p_r^{k^r},$$

missä $0 \leq k_i \leq j_i$ aina, kun $i \in \{1, ..., r\}$.

Todistus. Käsitellään luennolla. □

Olkoot $m, n \in \mathbb{N}$. Kirjoitetaan

$$m = p_1^{t_1} \cdot ... \cdot p_r^{t_r} \text{ ja } n = p_1^{s_1} \cdot ... \cdot p_r^{s_r}$$

missä $p_1, ..., p_r$ ovat eri alkulukuja ja $t_1, ..., t_r, s_1, ..., s_r \in \mathbb{N}$ sekä $r \in \mathbb{N}$. Lauseen 4.6 perusteella

$$(a \mid m \text{ ja } a \mid n) \;\Leftrightarrow\; a = p_1^{k_1} \cdot ... \cdot p_r^{k_r},$$

missä $0 \leq k_i \leq t_i$ ja $0 \leq k_i \leq s_i$ pätee kaikilla $i \in \{1, ..., r\}$. Toisin sanoen, $0 \leq k_i \leq min\{t_i, s_i\}$ kaikilla $i \in \{1, ..., r\}$. Tällä perusteella voidaan päätellä, että seuraava lause pätee.

Lause 4.7. $syt(m,n) = p^{min\{t_1,s_1\}} \cdot ... \cdot p^{min\{t_r,s_r\}}$. □

Määritellään, että lukujen m ja n *pienin yhteinen jaettava*

$$pyj(m,n) = p^{max\{t_1,s_1\}} \cdot ... \cdot p^{max\{t_r,s_r\}}.$$

Vaihtoehtoisesti voitaisiin määritellä, että $e = pyj(m,n)$ jos

1. $m \mid e$ ja $n \mid e$,
2. $(m \mid l$ ja $n \mid l) \Rightarrow e \mid l$.

Esimerkki. Etsitään $syt(280,600)$ ja $pyj(280,600)$. Luvun 280 *alkulukuhajotelma* on $2^3 \cdot 5 \cdot 7$. Luvun 600 alkulukuhajotelma on $2^3 \cdot 3 \cdot 5^2$. Täten

1. $280 = 2^3 \cdot 3^0 \cdot 5^1 \cdot 7^1$,
2. $600 = 2^3 \cdot 3^1 \cdot 5^2 \cdot 7^0$.

Täten

1. $syt(280,60) = 2^3 \cdot 3^0 \cdot 5^1 \cdot 7^0 = 40$,
2. $pyj(280,60) = 2^3 \cdot 3^1 \cdot 5^2 \cdot 7^1 = 4200$.

Lause 4.8 (Fermat'n pieni lause)**.** *Olkoon p alkuluku. Tällöin, jos $a \in \mathbb{Z}$ on kokonaisluku siten että $syt(a,p) = 1$, niin $a^{p-1} \equiv 1 \ (mod\ p)$.*

Todistus. Käsitellään luennolla. □

Esimerkki. Etsi $[100^{88}]_{89}$. Esimerkki käsitellään luennolla.

Lause 4.9. *Jos p on alkuluku, niin kaikilla $a \in \mathbb{Z}$ pätee $a^p \equiv a \ (mod\ p)$.*

Todistus. Käsitellään luennolla. □

Esimerkki. RSA-salaus perustuu yllä käsiteltyihin määritelmiin ja lauseisiin. Käsittelemme RSA-salauksen teoriaa luennolla.

RYHMÄTEORIAA

Kertausta

Olkoot A ja B joukkoja. Tulojoukon

$$A \times B \;=\; \{\,(x,y) \mid x \in A,\, y \in B\,\}$$

osajoukot ovat *relaatioita*.

Kuvaus eli *funktio* $f : A \to B$ on relaatio siten, että jokaiselle $x \in A$ on olemassa täsmälleen yksi alkio $y \in B$ siten että $(x,y) \in f$. Tätä merkitään kirjoittamalla $f(x) = y$.

Kuvaus f on *injektio*, mikäli kaikki joukon A alkiot kuvautuvat eri alkioille, eli ehto

$$x \neq y \Rightarrow f(x) \neq f(y)$$

pätee kaikilla $x, y \in A$.

Kuvaus $f : A \to B$ on *surjektio*, jos jokaisella $y \in B$ on olemassa jokin $x \in A$ siten, että $f(x) = y$.

Kuvaus f on *bijektio* jos se on sekä injektio että surjektio. Jos f on bijektio, sillä on olemassa käänteiskuvaus f^{-1} siten, että kaikilla $y \in B$ pätee $f^{-1}(y) = x$, missä $f(x) = y$.

5 Permutaatiot

Määritelmä 5.1. Olkoon X joukko. Bijektiota $f : X \to X$ sanotaan joukon X *permutaatioksi*.

Käytetään merkintää

$$S_X = \{\, f \mid f : X \to X \text{ on } X\text{:n permutaatio}\,\}.$$

Jos $X = \{1, 2, ..., n\}$, käytetään merkintää $S_n = S_X$. Lisäksi, jokaiselle $\alpha \in S_n$, käytetään merkintää

$$\alpha \;=\; \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha(1) & \alpha(2) & \dots & \alpha(n) \end{pmatrix}.$$

Havaitsemme, että funktioiden yhdiste-operaation $\circ$ on laskutoimitus permutaatioille: jos $f, g \in S_X$, niin $f \circ h$ on permutaatio siten, että

$$(f \circ h)(x) = f(h(x)).$$

On helppo osoittaa, että esimerkiksi $(f \circ h)^{-1} = h^{-1} \circ f^{-1}$, (HT).

Esimerkki. Jos

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

ja

$$\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

ovat permutaatioita joukossa S_3, niin

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

ja

$$\beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Havaitsemme, että permutaatiot $f, g, h \in S_X$ toteuttavat laskusäännöt

1. $f \circ id_X = id_X \circ f = f$,
2. $f \circ f^{-1} = f^{-1} \circ f = id_X$,
3. $f \circ (g \circ h) = (f \circ g) \circ h$,

missä id_X on identiteettifunktio, eli $id_X(y) = y$ kaikilla $y \in X$. Laskusääntöjen todistaminen jätetään harjoitustehtäväksi.

Määritelmä 5.2. Permutaatio $\alpha \in S_n$ on *k-sykli*, jos on olemassa sellaiset eri luvut $i_1, ..., i_k \in \{1, ..., n\}$, että

$$\alpha(i_1) = i_2,\ \alpha(i_2) = i_3, ..., \alpha(i_{k-1}) = i_k \text{ ja } \alpha(i_k) = i_1,$$

eli toisin ilmaisten,

$$i_1 \mapsto i_2 \mapsto i_3 \ ... \ i_{k-1} \mapsto i_k \ \text{ ja } \ i_k \mapsto i_1,$$

ja lisäksi $\alpha(j) = j$ aina, kun $j \notin \{i_1, ..., i_k\}$. Tällöin merkitään $\alpha = (i_1\, i_2 \ldots i_k)$.

Esimerkiksi

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\,3\,2) = (3\,2\,1) = (2\,1\,3).$$

Tällaista kuvausta kutsutaan 3-sykliksi. Huomaa, että

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \neq (3\,1\,2) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Erilliset syklit, eli syklit joissa ei ole samoja alkioita, kommutoivat. Esimerkiksi

$$(1\,3\,2) \circ (4\,5) = (4\,5) \circ (1\,3\,2).$$

Esimerkki. Jokainen $\alpha \in S_n$ on yhdistetty kuvaus erillisistä sykleistä. Esimerkki käsitellään luennolla.

2-syklejä sanotaan *transpositioiksi*. Transpositio on siis permutaatio $(k\,l)$, joka kuvaa kaksi alkiota toisikseen ja jättää muut alkiot itsekseen.

Esimerkki. Olkoon $(3\,7\,8\,9) \in S_9$ permutaatio. Nyt

$$(3\,7\,8\,9) \;=\; (3\,7) \circ (7\,8) \circ (8\,9).$$

Esimerkki. Yleisesti, jokainen permutaatio $\alpha \in S_n$ voidaan esittää yhdistettynä kuvauksena transpositioista. Tämä perustuu siihen, että jokainen $\alpha \in S_n$ voidaan edeltävän esimerkin nojalla esittää yhdistettynä kuvauksena erillisistä sykleistä, ja toisaalta jokainen sykli taas voidaan esittää yhdistettynä kuvauksena transpositioista säännön

$$(i_1 \ldots i_k) \;=\; (i_1\,i_2) \circ (i_2\,i_3) \circ \;\ldots\; \circ (i_{k-1}\,i_k)$$

mukaisesti, mikä osoitetaan luennolla.

Määritelmä 5.3 (Permutaation merkki)**.** Olkoon $\alpha \in S_n$. Sanotaan, että pari (i, j) on α:n *vaihto*, jos $i < j$, mutta $\alpha(j) < \alpha(i)$. Jos k on α:n vaihtojen lukumäärä, niin α:n *merkki* on

$$\varepsilon(\alpha) = (-1)^k.$$

Esimerkki. Jos

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

niin α:n vaihdot ovat $\{(1,3),(2,3)\}$. Tällöin

$$\varepsilon(\alpha) = (-1)^2 = 1.$$

Esimerkki. Jos

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix},$$

niin α:n vaihdot ovat $\{(1,2),(1,3),(2,3),(4,5)\}$. Tällöin

$$\varepsilon(\alpha) = (-1)^4 = 1$$

Lause 5.4. *Jos $\alpha \in S_n$, niin*

$$\varepsilon(\alpha) = \prod_{i<j} \frac{\alpha(j) - \alpha(i)}{j - i}.$$

Todistus. Havaitsemme aluksi, että kaksioiden $\{i, j\} \subseteq \{1, ..., n\}$ joukko

$$\{\{i, j\} \mid i, j \in \{1, ..., n\},\ i \neq j\ \}$$

voidaan yhtä hyvin kirjoittaa muotoon

$$\{\{i, j\} \mid i, j \in \{1, ..., n\},\ i < j\}.$$

Jokainen kaksio $\{i, j\} \subseteq \{1, ..., n\}$ esiintyy tulossa

$$x = \prod_{i<j} j - i$$

terminä $j - i$ täsmälleen kerran: tulo x onkin havainnollista kirjoittaa muotoon

$$x = \prod_{\{i,j\} \subseteq \{1,...,n\},\ i<j} j - i.$$

Koska funktio $\alpha : \{1, ..., n\} \to \{1, ..., n\}$ on bijektio, havaitsemme, että kaksioiden $\{\alpha(i), \alpha(j)\} \subseteq \{1, ..., n\}$ joukko on täsmälleen sama kuin kaksioiden $\{i, j\} \subseteq \{1, ..., n\}$ joukko. Täten joko

$$x \ = \prod_{\{\alpha(i),\alpha(j)\} \subseteq \{1,...,n\},\ i<j} \alpha(j) - \alpha(i) \ = \prod_{i<j} \alpha(j) - \alpha(i)$$

tai

$$-x \ = \prod_{\{\alpha(i),\alpha(j)\} \subseteq \{1,...,n\},\ i<j} \alpha(j) - \alpha(i) \ = \prod_{i<j} \alpha(j) - \alpha(i).$$

Tulon

$$x = \prod_{i<j} j - i$$

termit $j - i$ ovat aina positiivisia; tulon

$$\prod_{i<j} \alpha(j) - \alpha(i)$$

termi $\alpha(j) - \alpha(i)$ on negatiivinen joss (i, j) on α:n vaihto. Näin ollen havaitsemme, että

$$\prod_{i<j} \alpha(j) - \alpha(i) = \varepsilon(\alpha) \prod_{i<j} j - i.$$

Täten

$$\varepsilon(\alpha) = \prod_{i<j} \frac{\alpha(j) - \alpha(i)}{j - i}.$$

□

Lause 5.5. *Jos* $\alpha, \beta \in S_n$, *niin* $\varepsilon(\alpha \circ \beta) = \varepsilon(\alpha)\varepsilon(\beta)$.

Todistus. Lauseen 5.4 perusteella

$$\begin{aligned}
\varepsilon(\alpha \circ \beta) &= \prod_{i<j} \frac{\alpha(\beta(j)) - \alpha(\beta(i))}{j - i} \\
&= \prod_{i<j} \frac{\alpha(\beta(j)) - \alpha(\beta(i))}{\beta(j) - \beta(i)} \frac{\beta(j) - \beta(i)}{j - i} \\
&= \prod_{i<j} \frac{\alpha(\beta(j)) - \alpha(\beta(i))}{\beta(j) - \beta(i)} \prod_{i<j} \frac{\beta(j) - \beta(i)}{j - i} \\
&= \prod_{i<j} \frac{\alpha(\beta(j)) - \alpha(\beta(i))}{\beta(j) - \beta(i)} \varepsilon(\beta).
\end{aligned}$$

Riittää siis todistaa, että

$$\prod_{i<j} \frac{\alpha(\beta(j)) - \alpha(\beta(i))}{\beta(j) - \beta(i)} = \prod_{i<j} \frac{\alpha(j) - \alpha(i)}{j - i}.$$

Havaitsemme aluksi, että kaikilla permutaatioiden α ja β määrittelyjoukkoon $\{1, ..., n\}$ kuuluvilla alkioilla x, y pätee

$$\frac{\alpha(x) - \alpha(y)}{x - y} = \frac{\alpha(y) - \alpha(x)}{y - x},$$

joten kaikilla $i, j \in \{1, ..., n\}$ pätee

$$\frac{\alpha(\beta(i)) - \alpha(\beta(j))}{\beta(i) - \beta(j)} = \frac{\alpha(\beta(j)) - \alpha(\beta(i))}{\beta(j) - \beta(i)}.$$

Koska β on bijektio, kaksioiden $\{\beta(i), \beta(j)\}$ joukko on täsmälleen sama kuin kaksioiden $\{i, j\}$ joukko. Näin ollen (vertaa Lauseen 5.4 todistus) havaitsemme, että

$$\prod_{i<j} \frac{\alpha(\beta(j)) - \alpha(\beta(i))}{\beta(j) - \beta(i)} = \prod_{i<j} \frac{\alpha(j) - \alpha(i)}{j - i}.$$

□

Lause 5.6. *Jos* $\tau = (k\,l) \in S_n$, *niin* $\varepsilon(\tau) = -1$.

Todistus. Käsitellään luennolla. □

Lause 5.7. *Jos* $\alpha \in S_n$ *ja* $\alpha = \tau_1 \circ ... \circ \tau_r$, *missä* $\tau_1, ..., \tau_r$ *ovat transpositioita, niin*

$$\varepsilon(\alpha) = (-1)^r.$$

Todistus. Seuraa suoraan lauseista 5.5 ja 5.6. □

Jos $\varepsilon(\alpha) = 1$, niin sanomme, että α on *parillinen*. Jos $\varepsilon(\alpha) = -1$, niin sanomme, että α on *pariton*. Esimerkiksi jos $\alpha = (2\,1\,3) \in S_3$, niin $\alpha = (2\,1) \circ (1\,3)$. Yleisesti, jos $\alpha \in S_n$ on k-sykli, niin

$$\varepsilon(\alpha) = (-1)^{k-1},$$

koska

$$(i_1 ... i_k) = (i_1\,i_2) \circ (i_2\,i_3) \circ ... \circ (i_{k-1}\,i_k).$$

Huomioi, että parittoman pituiset syklit ovat parillisia.

6 Ryhmän määritelmä

Olkoon G joukko. Sanomme, että kuvaus $* : G \times G \to G$ on (kaksipaikkainen) *laskutoimitus* joukossa G. Käytetään merkintää $*(g,h) = g*h$, kun $g,h \in G$.

Määritelmä 6.1. Olkoon G joukko ja $*$ laskutoimitus joukossa G. Tällöin pari $(G,*)$ on *ryhmä*, jos seuraavat ehdot pätevät.

1. Laskutoimitus $*$ on *liitännäinen*, eli kaikille $r,s,t \in G$ pätee
$$r*(s*t) = (r*s)*t.$$
2. On olemassa sellainen alkio $e \in G$, että kaikille $s \in G$ pätee
$$e*s = s*e = s.$$
Tällöin sanomme, että e on *neutraalialkio*.
3. Jokaisella alkiolla $s \in G$ on olemassa sellainen alkio $t \in G$, että
$$s*t = t*s = e.$$
Sanomme, että t on alkion s *käänteisalkio*. □

Jos lisäksi pätee, että laskutoimitus $*$ on *vaihdannainen*, eli kaikilla $s,t \in G$ pätee
$$s*t = t*s,$$
niin G on *Abelin ryhmä* (Niels Henrik Abel 1802 - 1829). Vaihdannaisuutta kutsutaan myös *kommutatiivisuudeksi*.

Mikäli S on joukko, merkintä $|S|$ tarkoittaa joukon S alkioiden lukumäärää. Esim. $|\{1,2,6\}| = 3$. Jos $(G,*)$ on ryhmä, niin lukua $|G|$ kutsutaa ryhmän $(G,*)$ *kertaluvuksi*. Mikäli laskutoimitus $*$ on asiayhteyden perusteella tunnettu, voimme puhua myös ryhmästä G, millä tietenkin tarkoitetaan ryhmää $(G,*)$.

Esimerkki. $(\mathbb{Z},+)$ on ryhmä, missä

1. 0 on neutraalialkio.
2. $-x$ on alkion x käänteisalkio.
3. Liitännäisyys pätee.

Lisäksi $x+y = y+x$ pätee kaikilla $x,y \in \mathbb{Z}$, joten $(\mathbb{Z},+)$ on Abelin ryhmä.

Esimerkki. Olkoon $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$. Havaitsemme, että $(\mathbb{Q}^*, \cdot)$ on ryhmä.

1. 1 on ryhmän neutraalialkio.
2. $\frac{1}{x}$ on alkion x käänteisalkio.
3. Liitännäisyys pätee.

Lisäksi $x \cdot y = y \cdot x$ pätee kaikilla $x, y \in \mathbb{Q}^*$, joten $(\mathbb{Q}^*, \cdot)$ on Abelin ryhmä. Ryhmää kutsutaan rationaalilukujen *multiplikatiiviseksi ryhmäksi*. Olio $(\mathbb{Q}, +)$ on rationaalilukujen *additiivinen* ryhmä.

Esimerkki. Olkoon X joukko. $(S_X, \circ)$ on ryhmä. Ryhmää kutsutaan joukon X *symmetriaryhmäksi*.

1. Identiteetikuvaus $id_X : X \to X$ on ryhmän neutraalialkio.
2. Kuvauksen f käänteisalkio on käänteiskuvaus f^{-1}.
3. Liitännäisyys pätee.

Esimerkki Tutkitaan ryhmää S_3 ja konstruoidaan ryhmän kertotaulu. Esimerkki käsitellään luennolla.

Lause 6.2. *Olkoon $(G, *)$ ryhmä. Tälloin,*

1. *neutraalialkio e on yksikäsitteinen,*
2. *jokaisen alkion $s \in G$ käänteisalkio on yksikäsitteinen.*

Todistus. Käsitellään luennolla. □

Määritelmä 6.3. Ryhmän $(G, *)$ alkion $x \in G$ käänteisalkiolle käytetään merkintää x^{-1}.

Lause 6.4. *Olkoon $(G, *)$ ryhmä. Tällöin kaikilla $x, y \in G$ pätee*

$$(x * y)^{-1} = y^{-1} * x^{-1}.$$

Todistus. Käsitellään luennolla. □

Ryhmässä $(G, *)$ on voimassa *supistussääntö*: kaikilla $x, y, z \in G$ pätee implikaatiot

$$x * z = y * z \;\Rightarrow\; x = y,$$

$$z * x = z * y \;\Rightarrow\; x = y.$$

Tämä nähdään helposti:

$$\begin{aligned} & x * z = y * z \\ \Rightarrow\ & (x * z) * z^{-1} = (y * z) * z^{-1} \\ \Rightarrow\ & x * (z * z^{-1}) = y * (z * z^{-1}) \\ \Rightarrow\ & x * e = y * e \\ \Rightarrow\ & x = y. \end{aligned}$$

Toinen supistussääntö todistetaa vastaavasti.

Lause 6.5. *Olkoon $(G, *)$ ryhmä. Olkoon $g \in G$ ryhmän alkio. Tällöin kuvaus $\varphi : G \to G$, $x \mapsto g*x$, on bijektio. Vastaavasti, kuvaus $\varphi' : G \to G$, $x \mapsto x*g$, on bijektio.*

Todistus. Käsitellään luennolla. □

Tästä lauseesta seuraa suoraan, että jokainen joukon G alkio esiintyy ryhmän $(G, *)$ kertotaulun jokaisella rivillä täsmälleen kerran. Sama koskee sarakkeita: jokainen joukon G alkio esiintyy ryhmän $(G, *)$ kertotaulun jokaisessa sarakkeessa täsmälleen kerran.

Esimerkki. Selvitetään kokoa $|G| = 2$ ja kokoa $|G| = 3$ olevien ryhmien rakenne ja kertotaulut. Esimerkki käsitellään luennolla.

Määritelmä 6.6 (Alkioiden tulot)**.** Olkoon $(G, *)$ ryhmä ja $x_1, x_2..., x_n \in G$ ryhmän alkioita. Merkintä $x_1 * x_2 * ... * x_n$ viittaa laskutoimitukseen, joka lasketaan seuraavasti.

1. Aluksi lasketaan $x_1 * x_2$.
2. Kun on määritetty $x_1 * x_2 * ... * x_{k-1}$, niin voidaan määrittää

$$x_1 * x_2 * ... * x_k = (x_1 * x_2 * ... * x_{k-1}) * x_k.$$

Laskutoimitukseen $x_1 * x_2 * ... * x_n$ viitataan termillä *tulo*.

Huom, ryhmäteoriassa puhutaan toisinaan alkioiden tuloista, vaikka tarkasteltaisiinkin esim. additiivista ryhmää $(\mathbb{Z}, +)$.

Määritelmä 6.7 (Positiivinen potenssi)**.** Olkoon $(G, *)$ ryhmä ja $x \in G$ ryhmän alkio. Määritellään

1. $x^0 = e$,
2. $x^{n+1} = x^n * x$.

On mahdollista osoittaa, että $x^{m+n} = x^m * x^n$ ja $(x^m)^n = x^{mn}$. Tämä jätetään haasteeksi motivoituneille lukijoille. Vinkki: todista ensin ensimmänen laki käyttäen sopivaan induktio-oletukseen perustuvaa induktiota ja Määritelmää 6.7. Todista tämän jälkeen toinen laki käyttäen sopivaan induktio-oletukseen perustuvaa induktiota, ensimmäistä lakia ja Määritelmää 6.7.

7 Ryhmät ja kongruenssi

Olkoon $d \in \mathbb{Z}_+$ positiivinen kokonaisluku. Luvun $a \in \mathbb{Z}$ ekvivalenssiluokka on

$$\begin{aligned}\{\ x \in \mathbb{Z} \mid x \equiv a\ (mod\ d)\ \} &= \{\ x \in \mathbb{Z} \mid x = a + kd,\ k \in \mathbb{Z}\ \} \\ &= a + d\mathbb{Z} \\ &= a\text{:n jäännösluokka} \\ &= \{\ x \in \mathbb{Z} \mid [x]_d = [a]_d\ \}.\end{aligned}$$

Otetaan käyttöön merkintä

$$\overline{a} = \overline{a}_d = a + d\mathbb{Z}.$$

Kaikilla $a, b \in \mathbb{Z}$ siis pätee, että

$$\overline{a} = \overline{b} \Leftrightarrow a \equiv b\ (mod\ d) \Leftrightarrow d \,|\, b - a.$$

Lause 7.1. *Jäännösluokat mod d ovat* $\overline{0}, \overline{1}, ..., \overline{d-1}$. □

Otetaan käyttöön merkintä $\mathbb{Z}_d = \{\overline{0}, \overline{1}, ..., \overline{d-1}\}$. Esimerkiksi

$$\mathbb{Z}_{12} = \{\overline{0}, \overline{1}, ..., \overline{11}\},$$

missä

$$\begin{aligned}\overline{0} &= \{..., -12, 0, 12, 24, ...\} \\ \overline{1} &= \{..., -11, 1, 13, 25, ...\} \\ &\vdots \\ \overline{11} &= \{..., -1, 11, 23, 35, ...\}\end{aligned}$$

Määritellään yhteenlasku joukossa $\mathbb{Z}_d$ asettamalla

$$\overline{a} + \overline{b} = \overline{a + b}.$$

Tämä laskutoimitus on siis kuvaus $+ : \mathbb{Z}_d \times \mathbb{Z}_d \to \mathbb{Z}_d$, $(\overline{x}, \overline{y}) \mapsto \overline{x+y}$. Tarkastetaan, onko laskutoimitus $+$ *hyvin määritelty*, eli toisin sanoen, päteekö, että jokaisella $(\overline{a}, \overline{b}) \in \mathbb{Z}_d \times \mathbb{Z}_d$ on olemassa täsmälleen yksi $\overline{c} \in \mathbb{Z}_d$ siten, että $\overline{a} + \overline{b} = \overline{c}$. Riittää osoittaa, että

$$(\overline{a}, \overline{b}) = (\overline{a'}, \overline{b'}) \Rightarrow \overline{a+b} = \overline{a'+b'}.$$

Oletetaan, että $(\overline{a}, \overline{b}) = (\overline{a'}, \overline{b'})$. Täten $\overline{a} = \overline{a'}$ ja $\overline{b} = \overline{b'}$. Näin ollen

$$a \equiv a' \ (mod\ d) \text{ ja } b \equiv b' \ (mod\ d).$$

Lauseen 2.5 nojalla näin ollen

$$a + b \equiv a' + b' \ (mod\ d),$$

joten

$$\overline{a+b} = \overline{a'+b'}.$$

Näin ollen yhteenlasku on hyvin määritelty operaatio.

Lause 7.2. *Olio $(\mathbb{Z}_d, +)$ on Abelin ryhmä.*

Todistus. Todistimme edellä, että laskutoimitus $+$ on hyvin määritelty joukossa $\mathbb{Z}_d$. Riittää siis todistaa, että $(\mathbb{Z}_d, +)$ toteuttaa ryhmän määritelmän vaativat lait sekä lisäksi vaihdannaisuuslain.

1.) Liitännäisyys pätee, sillä kaikilla $a, b, c \in \mathbb{Z}$,

$$\begin{aligned}
\overline{a} + (\overline{b} + \overline{c}) &= \overline{a} + \overline{b+c} \\
&= \overline{a + (b+c)} \\
&= \overline{(a+b) + c} \\
&= \overline{a+b} + \overline{c} \\
&= (\overline{a} + \overline{b}) + \overline{c}.
\end{aligned}$$

2.) Neutraalialkio on $\overline{0}$: kaikilla $a \in \mathbb{Z}$ pätee

$$\begin{aligned}
\overline{a} + \overline{0} &= \overline{a+0} \\
&= \overline{a} \quad \text{ja} \\
\overline{0} + \overline{a} &= \overline{0+a} \\
&= \overline{a}.
\end{aligned}$$

3.) Alkion $\overline{a} \in \mathbb{Z}_d$ vasta-alkio on $\overline{-a}$, koska

$$\begin{aligned}
\overline{a} + \overline{-a} &= \overline{a + (-a)} = \overline{0} \text{ ja} \\
\overline{-a} + \overline{a} &= \overline{-a + a} = \overline{0}.
\end{aligned}$$

4.) Vaihdannaisuus pätee:

$$\overline{a} + \overline{b} = \overline{a+b} = \overline{b+a} = \overline{b} + \overline{a}.$$

□

Vähemmälläkin työllä olisi selvitty: esimerkiksi olisimme voineet todistaa vaihdannaisuuden ensiksi ja sitten vasta käsitellä kohdat 2 ja 3.

Määritellään sitten myös kertolasku joukossa $\mathbb{Z}_d$ siten, että

$$\overline{a} \cdot \overline{b} = \overline{ab}.$$

Osoitetaan, että kertolasku $\cdot$ on hyvin määritelty. Oletetaan siis, että $(\overline{a}, \overline{b}) = (\overline{a'}, \overline{b'})$. Täten $\overline{a} = \overline{a'}$ ja $\overline{b} = \overline{b'}$. Näin ollen

$$a \equiv a' \ (mod\ d) \text{ ja } b \equiv b' \ (mod\ d).$$

Lauseen 2.5 nojalla näin ollen

$$ab \equiv a'b' \ (mod\ d),$$

joten

$$\overline{a} \cdot \overline{b} = \overline{ab} = \overline{a'b'} = \overline{a'} \cdot \overline{b'}$$

Näin ollen kertolasku on hyvin määritelty operaatio.

Havaitaan, että

$$\overline{a} \cdot \overline{b} = \overline{ab} = \overline{ba} = \overline{b} \cdot \overline{a},$$

joten joukon $\mathbb{Z}_d$ kertolasku on vaihdannainen. Onko $(\mathbb{Z}_d, \cdot)$ ryhmä?

1.) Liitännäisyys: kaikilla $a, b, c \in \mathbb{Z}$ pätee

$$\begin{aligned} \overline{a} \cdot (\overline{b} \cdot \overline{c}) &= \overline{a} \cdot \overline{bc} \\ &= \overline{a(bc)} \\ &= \overline{(ab)c} \\ &= \overline{ab} \cdot \overline{c} \\ &= (\overline{a} \cdot \overline{b}) \cdot \overline{c}. \end{aligned}$$

2.) Alkio $\overline{1}$ on neutraalialkio: kaikilla $a \in \mathbb{Z}$ pätee

$$\begin{aligned} \overline{a} \cdot \overline{1} &= \overline{a1} \\ &= \overline{a} \quad \text{ja} \\ \overline{1} \cdot \overline{a} &= \overline{1a} \\ &= \overline{a}. \end{aligned}$$

3.) Käänteisalkiot: Havaitaan että joukossa $\mathbb{Z}_4$ pätee

$$\overline{2} \cdot \overline{2} = \overline{4} = \overline{0}.$$

Oletetaan, että alkiolla $\overline{2}$ on olemassa käänteisalkio $\overline{n} = \overline{2}^{-1}$. Täten

$$\begin{aligned} \overline{2} \cdot \overline{2} = \ \overline{0} \ &\Rightarrow \ \overline{2}^{-1} \cdot (\overline{2} \cdot \overline{2}) = \ \overline{2}^{-1} \cdot \overline{0} \\ &\Rightarrow \ (\overline{2}^{-1} \cdot \overline{2}) \cdot \overline{2} = \ \overline{0} \\ &\Rightarrow \ \overline{1} \cdot \overline{2} = \ \overline{0} \\ &\Rightarrow \ \overline{2} = \ \overline{0}, \end{aligned}$$

joten päädymme ristiriitaan. Näin ollen alkiolla $\overline{2}$ ei siis ole käänteisalkiota joukossa $\mathbb{Z}_4$. Olio $(\mathbb{Z}_4, \cdot)$ ei ole ryhmä.

Lause 7.3. *Jos $\overline{a} \in \mathbb{Z}_d$, niin yhtälöllä $\overline{a} \cdot \overline{x} = \overline{1}$ on olemassa ratkaisu $\overline{x} \in \mathbb{Z}_d$ joss $syt(a, d) = 1$.*

Todistus. Käsitellään luennolla. □

Jos $syt(a, d) = 1$, sanotaan, että $\overline{a} \in \mathbb{Z}_d$ on *alkuluokka*. Otetaan käyttöön merkintä

$$\mathbb{Z}_d^* = \{ \ \overline{a} \in \mathbb{Z}_d \mid syt(a, d) = 1 \ \}.$$

Tarkastetaan vielä, että alkuluokan käsite on hyvin määritelty. Oletetaan siis, että $\overline{a} = \overline{b}$, ja tehdään vastaoletus, että a määrää alkuluokan, eli $syt(a, d) = 1$, mutta b ei määrää alkuluokkaa, eli $syt(b, d) \neq 1$. Koska $\overline{a} = \overline{b}$, niin $b = a + kd$ jollain $k \in \mathbb{Z}$. Täten (harjoitus 2, tehtävä 4)

$$syt(b, d) = syt(a + kd, d) = syt(a, d),$$

mikä on ristiriita.

Lause 7.4. *Olio $(\mathbb{Z}_d^*, \cdot)$ on Abelin ryhmä*

Todistus. Osoitetaan aluksi, että olion $(\mathbb{Z}_d^*, \cdot)$ laskutoimitus on hyvin määritelty. Tällä kertaa riittää olettaa, että $\overline{a}, \overline{b} \in \mathbb{Z}_d^*$, ja näin ollen osoittaa, että $\overline{a} \cdot \overline{b} \in \mathbb{Z}_d^*$. (Olemme aikaisemmin osoittaneet, että jos $(\overline{a}, \overline{b}) = (\overline{a'}, \overline{b'})$, niin $\overline{a} \cdot \overline{b} = \overline{a'} \cdot \overline{b'}$).

Koska $\overline{a}, \overline{b} \in \mathbb{Z}_d^*$, Lauseen 7.3 nojalla $\overline{a} \cdot \overline{x} = \overline{1}$ ja $\overline{b} \cdot \overline{y} = \overline{1}$ joillekin $x, y \in \mathbb{Z}$. Täten

$$\overline{a} \cdot \overline{x} \cdot \overline{b} \cdot \overline{y} = \overline{1} \cdot \overline{1}.$$

Näin ollen

$$\overline{a \cdot x \cdot b \cdot y} = \overline{1}.$$

Merkitään $z = xy$. Täten

$$\overline{(ab)z} = \overline{1},$$

joten

$$\overline{ab} \cdot \overline{z} = \overline{1}.$$

Näin ollen Lauseen 7.3 nojalla päättelemme, että $syt(ab, d) = 1$. Täten $\overline{ab} \in \mathbb{Z}_d^*$, joten olion $(\mathbb{Z}_d^*, \cdot)$ laskutoimitus on hyvin määritelty.

Liitännäisyys, neutraalialkion olemassa olo ja vaihdannaisuus on käsitelty edellä. Käänteisalkioiden olemassa olo seuraa suoraan Lauseesta 7.3. □

8 Aliryhmät

Määritelmä 8.1. Olkoon $(G, *)$ ryhmä ja $H \subseteq G$. Sanomme, että H on G:n *aliryhmä*, jos

$e \in H$,

$x \in H \Rightarrow x^{-1} \in H$,

$x, y \in H \Rightarrow x * y \in H$. □

Esimerkki. Tarkastellaan luennolla tarkasteltua ryhmää $S_3 = \{e, \rho, \delta, \tau, \alpha, \beta\}$ Esim. $\{e\}$, $\{e, \rho\}$ ja $\{e, \alpha, \beta\}$ ovat S_3:n aliryhmiä.

Esimerkki. Mikäli $d \in \mathbb{N}$, niin $d\mathbb{Z} = \{\ dx \mid x \in \mathbb{Z}\ \}$ on ryhmän $(\mathbb{Z}, +)$ aliryhmä.

Esimerkki. Ryhmän G *triviaalit aliryhmät* ovat $\{e\}$ ja G.

Lause 8.2. *Olkoon G ryhmä ja $H \subseteq G$* aliryhmä. *Tällöin H on ryhmä.*

Todistus. Triviaali aliryhmän määritelmän nojalla. □

Aliryhmän H laskutoimitus on G:n laskutoimitus $*$ rajoitettuna joukkoon H. Eli H:n laskutoimitus on funktio $*' : H \times H \to H$ siten, että kaikille $x, y \in H$ pätee $x *' y = z$ joss $x * y = z$. Yleensä kuitenkin viittaamme laskutoimitukseen $*'$ samalla symbolilla $*$ kuin ryhmän G laskutoimitukseen. Voimme siis puhua myös ryhmän $(G, *)$ aliryhmästä $(H, *)$. Tarkasti ottaen ryhmän $(G, *)$ aliryhmä on kuitenkin $(H, *')$. Kun G:n laskutoimitus on asiayhteydestä selvä, puhumme G:n aliryhmästä H.

Esimerkki. Olemme määritelleet, että parillinen permutaatio on permutaatio, jonka merkki on 1. Otetaan käyttöön merkintä

$$A_n = \{\text{parilliset permutaatiot} \in S_n\}, \text{ eli}$$

$$A_n = \{\, \alpha \in S_n \mid \varepsilon(\alpha) = 1 \,\}.$$

Tällöin A_n on S_n:n aliryhmä, ns. *alternoiva aliryhmä*:

1. Koska $\varepsilon(id) = 1$, niin $id \in A_n$.
2. Jos $\alpha, \beta \in A_n$, niin lauseen 5.5 nojalla $\varepsilon(\alpha \circ \beta) = \varepsilon(\alpha)\varepsilon(\beta) = 1 \cdot 1 = 1$. Näin ollen $\alpha \circ \beta \in A_n$.
3. Oletetaan, että $\alpha \in A_n$. Täten $\varepsilon(\alpha) = 1$. Koska $\alpha \circ \alpha^{-1} = id$, niin $1 = \varepsilon(\alpha \circ \alpha^{-1}) = \varepsilon(\alpha)\varepsilon(\alpha^{-1})$. Täten $\varepsilon(\alpha^{-1}) = 1$, joten $\alpha^{-1} \in A_n$.

Lause 8.3. *Jos $H \subseteq \mathbb{Z}$ on $(\mathbb{Z}, +)$:n aliryhmä, niin on olemassa täsmälleen yksi $d \in \mathbb{N}$ siten, että $H = d\mathbb{Z} = \{\, nd \mid n \in \mathbb{Z} \,\}$.*

Todistus. Todistetaan ensiksi luvun d yksikäsitteisyys. Oletetaan siis, että $H = d\mathbb{Z} = d'\mathbb{Z}$ joillekin $d, d' \in \mathbb{N}$. Koska $d' \in d\mathbb{Z}$, niin $d \mid d'$. Koska $d \in d'\mathbb{Z}$, niin $d' \mid d$. Täten $d' = \pm d$. Koska $d, d' \in \mathbb{N}$, niin $d = d'$.

Todistetaan sitten d:n olemassaolo. Mikäli $H = \{0\}$, niin valitaan $d = 0$. Voimme siis olettaa, että $H \neq \{0\}$. Koska joukko $\mathbb{N}$ on *hyvinjärjestetty* (eli jokaisessa joukon $\mathbb{N}$ epätyhjässä osajoukossa S, jokin alkio on joukon S pienin alkio), niin joukossa

$$T = \{\, k \in H \mid k > 0 \,\}$$

on pienin luku d. Osoitetaan, että $H = d\mathbb{Z}$.

Osoitetaan ensiksi, että $H \subseteq d\mathbb{Z}$. Olkoon $m \in H$ jokin luku. Jakoyhtälön nojalla on olemassa sellaiset $q, r \in \mathbb{Z}$, että

$$m = qd + r,$$

missä $0 \leq r < d$. Koska H on ryhmä, niin

$$\begin{aligned} d \in H &\Rightarrow -qd = -(d + d + \ldots + d) \in H \\ &\Rightarrow m - qd \in H \\ &\Rightarrow r \in H. \end{aligned}$$

Siis $r \in H$. Mutta koska $0 \leq r < d$, niin on pädettävä, että $r = 0$, sillä d on joukon T pienin positiivinen alkio. Täten $m = qd \in d\mathbb{Z}$.

Osoitetaan sitten, että $d\mathbb{Z} \subseteq H$. Koska H on aliryhmä, niin mikäli $x \in H$, niin tällöin

$$x^{-1} = -x \in H \quad \text{ja} \quad x + x \in H.$$

Koska $d \in H$, niin myös $-d \in H$. Koska $2d = d + d \in H$, niin myös $-(2d) \in H$. Koska $3d = (d+d)+d \in H$, niin myös $-(3d) \in H$. Tätä voidaan jatkaa ilman rajoitusta, joten havaitsemme, että $nd \in H$ pätee kaikilla $n \in \mathbb{Z}$. Näin ollen $d\mathbb{Z} \subseteq H$. □

Kerrataan ryhmän potenssin määritelmä:

1. $x^0 = e$,
2. $x^{n+1} = x^n * x$.

Laajennetaan tätä määritelmää asettamalla, että kaikille $n \in \mathbb{Z}_+$ pätee

$$x^{-n} = (x^n)^{-1}.$$

Yleiselle potenssille (positiivinen, nolla ja negatiivinen potenssi) on mahdollista osoittaa, että $x^{m+n} = x^m * x^n$ ja $(x^m)^n = x^{mn}$. Tämä jätetään harjoitustehtäväksi motivoituneille lukijoille.

Määritelmä 8.4. Jos G on ryhmä ja $g \in G$, niin *alkion g virittämä ryhmä* on

$$\langle g \rangle := \{ g^n \mid n \in \mathbb{Z} \} = \{..., g^{-2}, g^{-1}, e, g, g^2, ...\}.$$

Alkion g *kertaluku* on

$$ord(g) := |\langle g \rangle|.$$

Mikäli $G = \langle g \rangle$ jollakin $g \in G$, niin sanotaan, että G on *syklinen* ryhmä, ja g on G:n virittäjä.

Lause 8.5. *Jos G on ryhmä ja $g \in G$, niin $\langle g \rangle$ on suppein ryhmän G aliryhmä, joka sisältää alkion g. Tämä tarkoittaa, että jos $H \subseteq G$ on aliryhmä siten, että $g \in H$, niin $\langle g \rangle \subseteq H$.*

Todistus. Todistetaan aluksi, että $\langle g \rangle$ on aliryhmä.

1. $e = g^0 \in \langle g \rangle$.
2. $(g^n)^{-1} = g^{-n} \in \langle g \rangle$ aina, kun $n \in \mathbb{Z}$.
3. $g^n * g^m = g^{n+m} \in \langle g \rangle$ aina, kun $n, m \in \mathbb{Z}$.

Todistetaan sitten, että $\langle g \rangle$ on suppein ryhmän G aliryhmä, joka sisältää alkion g. Olkoon $H \subseteq G$ on sellainen aliryhmä, että $g \in H$. Koska H on ryhmä ja $g \in H$, niin $g^n \in H$ aina, kun $n \in \mathbb{Z}$. Täten $\langle g \rangle \subseteq H$. □

Esimerkki. Tarkastellaan ryhmää S_3. Käytetään samoja merkintöjä, kuin luennolla esitetyssä esimerkissä, jossa konstruoitiin ryhmän S_3 kertotaulu.

Kuten kertotaulun avulla on helppo nähdä, ryhmässä pätee

$$\begin{aligned}
&\alpha^2 = \beta,\\
&\alpha^3 = \beta \circ \alpha = e,\\
&\alpha^4 = e \circ \alpha = \alpha,\\
&\alpha^5 = \alpha \circ \alpha = \beta = \alpha^2\\
&\text{ja}\\
&\alpha^{-1} = \beta,\\
&\alpha^{-2} = (\alpha^2)^{-1} = \beta^{-1} = \alpha,\\
&\alpha^{-3} = (\alpha^3)^{-1} = e^{-1} = e.
\end{aligned}$$

Täten $\langle \alpha \rangle = \{ e, \alpha, \beta \}$ ja $ord(\alpha) = 3$.

Esimerkki. Tarkastellaan ryhmää $(\mathbb{Z}, +)$. Olkoon $d \in \mathbb{N}$ luonnollinen luku. Tällöin $\langle d \rangle = d\mathbb{Z}$. Jos $d = 1$, niin $\langle d \rangle = \mathbb{Z}$, joten $(\mathbb{Z}, +)$ on syklinen ryhmä.

Esimerkki. Tarkastellaan ryhmää $\mathbb{Z}_d$, $(d \in \mathbb{Z}_+)$, eli jäännösluokkien ryhmää, jossa laskutoimituksena on jäännösluokkien yhteenlasku $\overline{a} + \overline{b} = \overline{a+b}$. Otetaan *virittäjäksi* alkio $\overline{1}$. Jos $n \in \mathbb{N}$, niin

$$\overline{1}^{\,n} = \overline{1} + \overline{1} + ... + \overline{1} = \overline{1 + 1 + ...1} = \overline{n}.$$

Lisäksi

$$\overline{1}^{\,-n} = (\overline{1}^{\,n})^{-1} = \overline{n}^{\,-1} = \overline{-n}.$$

Täten

$$\langle \overline{1} \rangle = \{ \overline{n} \mid n \in \mathbb{Z} \} = \mathbb{Z}_d.$$

Täten $\mathbb{Z}_d$ on syklinen ryhmä ja $ord(\overline{1}) = d$.

Lause 8.6. *Olkoon G ryhmä ja $g \in G$ alkio. Jos $ord(g) \in \mathbb{N}$, niin*

1. *$ord(g) = min\{ n \in \mathbb{Z}_+ \mid g^n = e \}$,*
2. *kaikilla $n \in \mathbb{Z}$ pätee $g^n = e \Leftrightarrow ord(g) \mid n$.*

Todistus. Merkitään

$$d = min\{ n \in \mathbb{Z}_+ \mid g^n = e \}.$$

Jakoyhtälön perusteella mielivaltaisella luvulla $n \in \mathbb{Z}$ on olemassa $q, r \in \mathbb{Z}$ siten, että $n = qd + r$, missä $0 \leq r < d$. Tällöin $g^n = g^{qd+r} = (g^d)^q * g^r = g^r$. Näin ollen, koska $0 \leq r < d$, päättelemme, että

$$\langle g \rangle \subseteq \{e, g, ..., g^{d-1}\}.$$

Täten

$$\langle g \rangle = \{e, g, ..., g^{d-1}\}.$$

Näin ollen $ord(g) = |\langle g \rangle| \leq d$. Jos $e, g, g^2, ..., g^{d-1}$ ovat eri alkioita, niin $ord(g) = d$. Alkiot $e, g, g^2, ..., g^{d-1}$ ovat eri alkioita, sillä muuten pätisi $g^i = g^j$ s.e. $0 \leq i < j < d$, jolloin pätisi $g^{j-i} = e$, mikä on ristiriidassa luvun d määritelmän kanssa, sillä $0 < j - i < d$. Täten kohta 1 on todistettu.

Todistetaan sitten kohta 2. Oletetaan ensin, että $g^n = e$ jollakin $n \in \mathbb{Z}$. Jakoyhtälön nojalla on olemassa sellaiset $q, r \in \mathbb{Z}$, että $n = qd + r$, missä $0 \leq r < d = ord(g)$. Täten

$$e = g^n = g^{qd+r} = g^{qd} * g^r = (g^d)^q * g^r = e^q * g^r = g^r.$$

Näin ollen, koska $0 \leq r < d$ ja d on pienin positiivinen kokonaisluku siten, että $g^d = e$, on pädettävä että $r = 0$. Täten $d \,|\, n$.

Oletetaan sitten, että $d = ord(g) \,|\, n$. Täten $n = n' \cdot d$ jollain $n' \in \mathbb{Z}$. Näin ollen päättelemme, käyttäen hyväksi kohtaa 1, että

$$g^n = g^{n'd} = (g^d)^{n'} = e^{n'} = e.$$

□

Esimerkki. Olkoon G ryhmä ja $g \in G$. Tiedetään, että $g^{101} = e$. Mitä on $ord(g)$, jos $g \neq e$? Havaitaan, että 101 on alkuluku. Lauseen 8.6 nojalla $ord(g) \,|\, 101$. Toisaalta $g \neq e$, joten $ord(g) > 1$. Siispä $ord(g) = 101$.

Lause 8.7. *Syklisen ryhmän jokainen aliryhmä on syklinen.*

Todistus. Olkoon $G = \langle g \rangle$, missä $g \in G$. Olkoon $H \subseteq G$ aliryhmä. Jos $H = \{e\}$, niin $H = \langle e \rangle$. Oletetaan siis, että $H \neq \{e\}$. Tarkastellaan joukkoa

$$S = \{ n \in \mathbb{Z}_+ \mid g^n \in H \} \neq \emptyset.$$

(Joukko S ei ole tyhjä, sillä jos $g^n \in H$, missä $n < 0$, niin $(g^n)^{-1} = g^{-n} \in H$.) Koska $\mathbb{N}$ on hyvinjärjestetty, niin joukolla S on pienin alkio d. Osoitetaan, että $H = \langle g^d \rangle$.

Olkoon $g^n \in H$, $n \in \mathbb{Z}$, jokin alkio. Jakoyhtälön nojalla on olemassa sellaiset $q, r \in \mathbb{Z}$, että $n = qd + r$, missä $0 \leq r < d$. Nyt

$$g^n = g^{qd+r} = g^{qd} * g^r,$$

joten

$$g^r = (g^{qd})^{-1} g^n = ((g^d)^q)^{-1} g^n = ((g^d)^{-q} g^n) \in H \quad (g^d, g^n \in H).$$

Koska siis $g^r \in H$, niin $r = 0$, sillä d on pienin positiivinen kokonaisluku k siten, että $g^k \in H$. Näin ollen $g^n = g^{qd} = (g^d)^q \in \langle g^d \rangle$. □

Esimerkki. Tarkastellaan *diedriryhmää* D_4. Esimerkki ja siihen liittyvä taustamatematiikka käsitellään luennoilla.

9 Isomorfismit ja homomorfismit

Tarkastellaan ryhmiä $\mathbb{Z}_3$ ja $\{e, \alpha, \beta\} \subseteq S_3$. Ryhmä $\{e, \alpha, \beta\}$ on siis symmetriaryhmän S_3 aliryhmä. Piirretään ryhmien kertotaulut (luennolla). Havaitsemme, että kertotaulut ovat (alkioiden nimeämistä vaille) täsmälleen samat.

Kahta alkioiden nimiä vaille samaa ryhmää kutsutaan *isomorfisiksi*. Määrittelemme seuraavaksi isomorfisuuden käsitteen täsmällisesti.

Määritelmä 9.1. Olkoot $G = (G, *)$ ja $G' = (G', *')$ ryhmiä. Mikäli on olemassa bijektio $f : G \to G'$ siten, että kaikilla $x, y \in G$ pätee

$$f(xy) = f(x)f(y), \text{ eli}$$

$$f(x * y) = f(x) *' f(y),$$

niin sanomme, että f on *ryhmäisomorfismi*, tai yksinkertaisesti *isomorfismi*. Ryhmät G ja G' ovat *isomorfiset*. Merkintä $G \cong G'$ tarkoittaa, että ryhmät G ja G' ovat isomorfiset.

Ryhmien G ja G' isomorfisuus tarkoittaa, että ryhmät ovat oleellisesti samat: isomorfismin f voidaan ajatella vain nimeävän ryhmän G jokaisen alkion x uudelleen $f(x)$:ksi, ryhmän laskutoimituksen pysyessä ennallaan. Ryhmien G ja G' matemaattinen rakenne on sama.

Esimerkki. Käytetään merkintää

$$\mathbb{R}_+ = \{\ x \in \mathbb{R} \mid x > 0\ \}.$$

Ryhmä $(\mathbb{R}_+, \cdot)$ on ryhmän $(\mathbb{R} \setminus \{0\}, \cdot)$ aliryhmä. Osoitamme seuraavaksi, että $(\mathbb{R}_+, \cdot)$ ja $(\mathbb{R}, +)$ ovat isomorfiset.

Olkoon e Neperin luku. Kuvaus $f : \mathbb{R} \to \mathbb{R}_+$, $x \mapsto e^x$, on isomorfismi ryhmien $(\mathbb{R}, +)$ ja $(\mathbb{R}_+, \cdot)$ välillä, sillä

$$f(x + y) = e^{x+y} = e^x e^y = f(x)f(y),$$

ja lisäksi f on bijektio. □

Esimerkki. Olkoon $D_2 = (\{id, R, S, F\}, \circ)$, missä

1. $id : \mathbb{R}^2 \to \mathbb{R}^2$ on identiteettifunktio,
2. $R : \mathbb{R}^2 \to \mathbb{R}^2$ on kierto kulman π verran,
3. $S : \mathbb{R}^2 \to \mathbb{R}^2$ on peilaus x-akselin suhteen,
4. $F : \mathbb{R}^2 \to \mathbb{R}^2$ on peilaus y-akselin suhteen,

5. $\circ$ on meille tässä vaiheesssa jo erittäin tuttu funktioiden yhdiste. Siis, jos Y ja X ovat funktioita siten, että funktion X kuvajoukko on funktion Y määrittelyjoukon osajoukko, niin $Y \circ X$ on funktio, jonka määrittelyjoukko on sama kuin funktion X, ja lisäksi $(Y \circ X)(x) = Y(X(x))$ kaikille funktion X määrittelyjoukon alkioille x.

Piirtämällä ryhmien D_2 ja $\mathbb{Z}_8^*$ kertotaulut havaitaan, että kuvaus

$$f : \{id, R, S, F\} \to \mathbb{Z}_8^*$$

siten, että

1. $id \mapsto \overline{1}$,
2. $R \mapsto \overline{3}$,
3. $S \mapsto \overline{5}$,
4. $F \mapsto \overline{7}$,

on isomorfismi. Kertotaulut ovat nimeämistä vaille samat. Ryhmät D_2 ja $\mathbb{Z}_8^*$ ovat *Kleinin neliryhmiä*. Täsmälleen kaikki näiden ryhmien kanssa isomorfiset ryhmät ovat Kleinin neliryhmiä. Kleinin neliryhmien kokoelma on *isomorfialuokka*. Se sisältää täsmälleen kaikki ryhmän D_2 kanssa isomorfiset ryhmät. Intuition tasolla algebrassa on yleensä tapana samaistaa ryhmä oman isomorfialuokkansa kanssa: isomorfiset ryhmät ovat oleellisesti samat, joten epämuodollisella intuition tasolla kahta isomorfista ryhmää ei edes yleensä ajatella eri ryhminä. □

Määritelmä 9.2. Olkoot G ja G' ryhmiä. Kuvaus $f : G \to G'$ on *ryhmähomomorfismi*, tai yksinkertaisesti *homomorfismi*, mikäli ehto

$$f(xy) = f(x)f(y)$$

pätee kaikilla $x, y \in G$.

Havaitsemme, että isomorfismi on bijektiivinen homomorfismi.

Esimerkki. Tarkastellaan kuvausta $f : \mathbb{Z} \to \mathbb{Z}_d$ siten, että $x \mapsto \overline{x}$. Kuvaus f on homomorfismi olioiden $(\mathbb{Z}, +)$ ja $(\mathbb{Z}_d, +)$ välillä, sillä

$$f(x + y) = \overline{x + y} = \overline{x} + \overline{y} = f(x) + f(y)$$

pätee kaikilla $x, y \in \mathbb{Z}$.

Lause 9.3. *Olkoon G ja G' ryhmiä ja $f : G \to G'$ ryhmähomomorfismi. Tällöin*

1. $f(e) = e'$,
2. $f(x^{-1}) = (f(x))^{-1}$.

Todistus. Havaitaan, että

$$f(e) = f(e \cdot e) = f(e)f(e).$$

Kerrotaan puolittain alkiolla $(f(e))^{-1}$. Täten $e' = f(e)$.

Käsitellään sitten kohta 2. Havaitaan, että

$$f(x)f(x^{-1}) = f(x \cdot x^{-1}) = f(e)$$

ja

$$f(x^{-1})f(x) = f(x^{-1} \cdot x) = f(e).$$

Käänteisalkion yksikäsitteisyyden nojalla $(f(x))^{-1} = f(x^{-1})$. □

Määritelmä 9.4. Olkoot G ja G' ryhmiä ja $f : G \to G'$ homomorfismi. Tällöin

1. f:n *ydin* on $ker(f) := \{\ x \in G \mid f(x) = e'\ \}$,
2. f:n *kuva* on $im(f) := \{\ x \in G' \mid x = f(z)$ jollain $z \in G\ \}$.

Tässä "ker" tulee sanasta *kernel* ja "im" sanasta *image*. Ydin sisältää neutraalialkiolle kuvautuvat alkiot ja kuva ne alkiot, joilla on alkukuva joukossa G.

Esimerkki. Tarkastellaan ryhmiä $(\mathbb{Z}, +)$ ja $(\mathbb{Z}_d, +)$ ja niiden välistä homomorfismia $f : \mathbb{Z} \to \mathbb{Z}_d$ siten, että $x \mapsto \overline{x}$. Havaitaan, että

$$f(x) = \overline{0} \ \Leftrightarrow\ \overline{x} = \overline{0} \ \Leftrightarrow\ x \in d\mathbb{Z}.$$

Täten $ker(f) = d\mathbb{Z}$. Kaikilla $\mathbb{Z}_d$:n alkioilla on alkukuva, joten $im(f) = \mathbb{Z}$.

Lause 9.5. *Olkoot G ja G' ryhmiä ja $f : G \to G'$ homomorfismi. Tällöin $ker(f)$ on ryhmän G aliryhmä ja $im(f)$ on ryhmän G' aliryhmä.*

Todistus. Ensimmäinen väite jätetään harjoitustehtäväksi. Todistetaan toinen väite.

Lauseen nojalla 9.3 $f(e) = e'$, joten $e' \in im(f)$.

Oletetaan, että $x, y \in im(f)$. Tällöin on olemassa sellaiset $a, b \in G$, että $f(a) = x$ ja $f(b) = y$. Täten

$$xy = f(a)f(b) = f(ab),$$

joten $xy \in im(f)$.

Oletetaan, että $z \in im(f)$. Tällöin on olemassa jokin $c \in G$ siten, että $f(c) = z$. Täten, käyttäen hyväksi lausetta 9.3, päätellään, että

$$z^{-1} = (f(c))^{-1} = f(c^{-1}),$$

joten $z^{-1} \in im(f)$. □

Lause 9.6. *Olkoot G ja G' ryhmiä ja $f : G \to G'$ homomorfismi. Tällöin f on injektio jos ja vain jos $ker(f) = \{e\}$.*

Todistus. Oletetaan ensin, että f on injektio. Lauseen 9.3 nojalla $f(e) = e'$. Näin ollen

$$x \in ker(f) \;\Leftrightarrow\; f(x) = f(e) \;\Leftrightarrow\; x = e.$$

Oletetaan sitten, että $ker(f) = \{e\}$. Oletetaan, että $x, y \in G$ ja $f(x) = f(y)$. Täten, kertomalla puolittain $(f(y))^{-1}$:llä, nähdään, että

$$f(x)(f(y))^{-1} = e'.$$

Lauseen 9.3 nojalla

$$f(x)f(y^{-1}) = e'.$$

Edelleen, koska f on homomorfismi, niin

$$f(xy^{-1}) = e'.$$

Täten

$$xy^{-1} \in ker(f) = \{e\},$$

joten

$$xy^{-1} = e.$$

Kertomalla puolittain y:llä, päättelemme, että $x = y$. □

Injektiivistä homomorfismia $f : G \to G'$ kutsutaan *upotukseksi*. Jos f on upotus, ja jos lisäksi rajataan f:n maalijoukko joukoksi $im(f)$, saadaan bijektio $f' : G \to im(f)$, $x \mapsto f(x)$, joka on tällöin isomorfismi ryhmältä G ryhmälle $im(f)$.

Esimerkki. Kuvaus $f : \mathbb{R} \to \mathbb{C}$, $x \mapsto x$ (muodollisemmin, $x \mapsto (x, 0)$), on ryhmän $(\mathbb{R}, +)$ upotus ryhmään $(\mathbb{C}, +)$.

10 Tekijäryhmät

Esittelemme seuraavaksi jäännösluokan käsitteen yleistyksen, joka koskee ryhmiä. Tarkastellaan aluksi additiivista ryhmää $(\mathbb{Z}, +)$. Olkoon $d \in \mathbb{Z}_+$ positiivinen kokonaisluku. Jos $n \in \mathbb{Z}$, niin

$$\overline{n} = \overline{n}_d = n + d\mathbb{Z}.$$

Joukko $d\mathbb{Z}$ on struktuurin $(\mathbb{Z}, +)$ aliryhmä. Kun merkitään $d\mathbb{Z} = H$ ja käytetään merkin $+$ sijasta abstraktia laskutoimitusmerkkiä $*$, voidaan yllä oleva yhtälö kirjoittaa muotoon

$$\overline{n} = n * H.$$

Määritelmä 10.1. Olkoon G ryhmä ja $H \subseteq G$ ryhmän G aliryhmä. Olkoon $g \in G$ ryhmän G alkio. Joukko

$$g * H = gH := \{\ x \in G \mid x = gh \text{ jollain } h \in H\ \}$$

on aliryhmän H *vasen sivuluokka.* (Tarkemmin, gH on alkion g määräämä, aliryhmän H vasen sivuluokka.)

Otetaan käyttöön merkintä

$$G/H\ :=\ \{\ gH \mid g \in G\ \}.$$

Esimerkki. Tarkastellaan additiivista ryhmää $\mathbb{Z} = (\mathbb{Z}, +)$. Tällöin

$$\mathbb{Z}/d\mathbb{Z} = \{\ n * d\mathbb{Z} \mid n \in \mathbb{Z}\ \} = \{\ n + d\mathbb{Z} \mid n \in \mathbb{Z}\ \} = \{\ \overline{n} \mid n \in \mathbb{Z}\ \} = \mathbb{Z}_d.$$

Esimerkki. Tarkastellaan kolmiulotteisen euklidisen avaruuden additiivista ryhmää $(\mathbb{R}^3, +)$. Tässä ryhmässä siis

$$(x_1, x_2, x_3) + (y_1, y_2, y_3) = (x_1 + y_1, x_2 + y_2, x_3 + y_3).$$

Olkoon $H \subseteq \mathbb{R}^3$ aliryhmä

$$H\ :=\ \{\ (x, y, z) \in \mathbb{R}^3 \mid z = 0\ \},$$

eli xy-taso. Olkoon $r = (r_1, r_2.r_3) \in \mathbb{R}^3$ jokin vektori. Tällöin

$$\begin{aligned} r + H\ &:= \{\ (x, y, z) \in \mathbb{R} \mid (x, y, z) = r + (u, v, w) \text{ jollain } (u, v, w) \in H\ \} \\ &= \{\ (x, y, z) \in \mathbb{R} \mid (x, y, z) = (r_1 + u, r_2 + v, r_3 + 0) \text{ jollain } u, v \in \mathbb{R}\} \\ &= \{\ (x, y, z) \in \mathbb{R} \mid z = r_3\ \}. \end{aligned}$$

Vasen sivuluokka $r + H$ on siis xy-tason suuntainen, korkeudella r_3 oleva taso. Täten $\mathbb{R}^3/H$ on xy-tason suuntaisten tasojen joukko. $\square$

Määritellään seuraavaksi yleistys kongruenssirelaatiolle $\equiv$. Olkoon G ryhmä ja H ryhmän G aliryhmä. Määritellään relaatio $\sim \subseteq G \times G$ siten, että

$$x \sim y \;\Leftrightarrow\; x = yh \text{ jollain } h \in H.$$

Tällöin $gH = \{\, x \in G \mid x \sim g \,\}$.

Havaitsemme, että $\sim$ todella on kongruenssirelaation $\equiv$ yleistys, sillä

$$\begin{aligned} & a \equiv b \ (mod\ d) \\ \Leftrightarrow\ & d \,|\, a - b \\ \Leftrightarrow\ & a = b + kd, \text{ missä } kd \in d\mathbb{Z} \\ \Leftrightarrow\ & a = b * h \text{ jollain } h \in H = d\mathbb{Z}. \end{aligned}$$

Lause 10.2. *Relaatio $\sim$ on ekvivalenssirelaatio.*

Todistus. Käsitellään luennolla. $\square$

Edellisen lauseen nojalla sivuluokat xH, missä $x \in G$, ovat ekvivalenssiluokkia. Ekvivalenssiluokat osittavat joukon G, joten seuraava lause pätee.

Lause 10.3. *1.* $G = \bigcup_{x \in G} xH$.

2. $xH \cap yH = \emptyset \;\Leftrightarrow\; xH \neq yH$.

3. $xH = yH \;\Leftrightarrow\; y = xh$ *jollakin* $h \in H \;\Leftrightarrow\; x^{-1}y \in H$. $\square$

Otetaan käyttöön merkintä

$$G : H \;:=\; \text{sivuluokkien lukumäärä} \;=\; |\, G/H \,|.$$

Lause 10.4 (Lagrange)**.** *Olkoon G äärellinen ryhmä ja $H \subseteq G$ ryhmän G aliryhmä. Tällöin*

$$|G| \;=\; (G : H)|H|.$$

Todistus. Käsitellään luennolla. $\square$

Esimerkki. Todistetaan seuraava moderni variantti Fermat'n pienestä lauseesta: jos G on äärellinen ryhmä, niin $g^{|G|} = e$ kaikilla $g \in G$. Olkoon $d = ord(g) = |\langle g \rangle|$. Lauseen 8.6 nojalla $g^d = e$. Lagrangen lauseen nojalla $d \,|\, |G|$, joten $|G| = nd$ jollain $n \in \mathbb{N}$. Täten

$$g^{|G|} \;=\; (g^d)^n \;=\; e,$$

mikä olikin osoitettava.

Havaitsemme, että Fermat'n pieni lause seuraa suoraan tästä lauseesta. Nimittäin jos p on alkuluku, niin

$$\begin{aligned} syt(a,p) = 1 &\Rightarrow \overline{a} \in \mathbb{Z}_p^* \ \text{ (missä } \mathbb{Z}_p^* = (\mathbb{Z}_p^*, \cdot) \text{ on alkuluokkaryhmä)} \\ &\Rightarrow \overline{a}^{p-1} = \overline{1} \ \text{ (uuden lauseemme nojalla)} \\ &\Rightarrow a^{p-1} \equiv 1 \ (mod\ p). \end{aligned}$$

Jos määritellään kertolasku

$$(xH) \cdot (yH) \ = \ (xy)H$$

joukossa G/H, saadaanko ryhmä? Tarkistetaan aluksi, onko näin määritelty kertolasku hyvin määritelty. Riittäisi osoittaa, että

$$\big(xH = x'H \ \text{ ja } \ yH = y'H\big) \ \Rightarrow \ (xy)H = (x'y')H.$$

Tämä ei kuitenkaan välttämättä päde. (HT: etsi jokin esimerkkitapaus, jossa ehto ei toteudu, ja osoita, että ehto ei todella toteudu.)

Määritelmä 10.5. Ryhmän G aliryhmä H on *normaali*, mikäli $xH = Hx$ kaikilla $x \in G$.

Osoitetaan seuraavaksi, että jos H on normaali, on kertolasku

$$(xH) \cdot (yH) = (xy)H$$

joukossa G/H hyvin määritelty. Oletetaan, että

$$xH = x'H \ \text{ ja } \ yH = y'H.$$

Täten $x' = xh$ ja $y' = yk$ joillain $h, k \in H$. Näin ollen $x'y' = xhyk$. Koska H on normaali, niin $hy \in Hy = yH$, joten $hy = yl$ jollain $l \in H$. Täten $x'y' = xylk$ ja $xy = x'y'k^{-1}l^{-1}$. Päätellään sitten, että $(x'y')H = (xy)H$. Jos $a \in (x'y')H$, niin $a = x'y's = xylks$ jollain $s \in H$. Koska $lks \in H$, niin $a \in xyH$. Jos $b \in (xy)H$, niin $b = xyt = x'y'k^{-1}l^{-1}t$ jollain $t \in H$. Koska $k^{-1}l^{-1}t \in H$, niin $b \in x'y'H$.

Lause 10.6. *Olkoon G on ryhmä ja H ryhmän G normaali aliryhmä. Tällöin G/H on ryhmä. Ryhmän kertolasku on määritelty siten, että $(xH) \cdot (yH) = (xy)H$.*

Todistus. Käsitellään luennolla. □

Ryhmä $(G/H, \cdot)$, missä siis $(xH) \cdot (yH) = (xy)H$, on ryhmän G *tekijäryhmä.*

Milloin aliryhmä on normaali?

Esimerkki. Jos G on Abelin ryhmä, niin jokainen aliryhmä $H \subseteq G$ on normaali.

Esimerkki. Symmetriaryhmän S_3 aliryhmä $\{id, (1\,2)\}$ ei ole normaali, sillä

$$(1\,2\,3)H \;=\; \{\,(1\,2\,3),\,(1\,2\,3)(1\,2)\,\} \;=\; \{\,(1\,2\,3),\,(1\,3)\,\}$$

ja

$$H(1\,2\,3) \;=\; \{\,(1\,2\,3),\,(1\,2)(1\,2\,3)\,\} \;=\; \{\,(1\,2\,3),\,(2\,3)\,\}.$$

Lause 10.7. *Olkoon G ryhmä ja H sen aliryhmä. H on normaali jos ja vain jos $xHx^{-1} \subseteq H$ pätee kaikilla $x \in G$.*

Todistus. Käsitellään luennolla. □

11 Isomorfialause

Lause 11.1. *Jos $f : G \to G'$ on ryhmähomomorfismi, niin*

$$ker(f) = \{\ x \in G \mid f(x) = e'\ \}$$

on ryhmän G normaali aliryhmä.

Todistus. Lauseen 9.5 nojalla $ker(f)$ on G:n aliryhmä. Lauseen 10.7 nojalla riittää osoittaa, että

$$h \in ker(f) \ \Rightarrow\ xhx^{-1} \in ker(f)$$

pätee kaikilla $x \in G$.

Olkoon $h \in ker(f)$ ja $x \in G$. Tällöin

$$\begin{aligned} f(xhx^{-1}) =& f(x)f(h)f(x^{-1}) \\ =& f(x)e'f(x^{-1}) \quad (h \in ker(f)) \\ =& f(x)f(x^{-1}) \\ =& f(x)f(x)^{-1} \\ =& e'. \end{aligned}$$

Täten $xhx^{-1} \in ker(f)$. □

Jos A ja B ovat joukkoja ja $f : A \to B$ on kuvaus ja $a \in A$, niin joukko

$$\{\ x \in A \mid f(x) = f(a)\ \}$$

on kuvauksen f *säie*. Alkion $a \in A$ ja funktion $f : A \to B$ määräämään säikeeseen on kätevä viitata merkinnällä

$$f^{-1}(\{f(a)\}) := \{\ x \in A \mid f(x) = f(a)\ \}.$$

(Tätä merkintää käytettäessä on syytä kuitenkin huomata, että funktiolla f ei välttämättä ole olemassa varsinaista käänteisfunktiota f^{-1}. Käänteisrelaatio kuitenkin on.)

Millaisia ovat $ker(f)$:n sivuluokat?

Lause 11.2. *Jos $f : G \to G'$ on ryhmähomomorfismi, niin*

$$x \cdot ker(f) = f^{-1}(\{f(x)\})$$

kaikilla $x \in G$.

Todistus.

$$\begin{aligned} y \in f^{-1}(\{f(x)\}) &\Leftrightarrow f(y) = f(x) \\ &\Leftrightarrow (f(x))^{-1} f(y) = e' \\ &\Leftrightarrow f(x^{-1}) f(y) = e' \\ &\Leftrightarrow f(x^{-1}y) = e' \\ &\Leftrightarrow x^{-1}y \in ker(f) \\ &\Leftrightarrow y \in x \cdot ker(f). \end{aligned}$$

□

Homomorfismin $f : G \to G'$ ydin $ker(f) = e \cdot ker(f)$ sisältää täsmälleen ne alkiot, jotka kuvautuvat alkiolle $e' = f(e)$; vastaavasti sivuluokka $x \cdot ker(f)$ sisältää täsmälleen ne alkiot, jotka kuvautuvat alkiolle $f(x)$.

Esimerkki. Tarkastellaan homomorfismia $f : \mathbb{Z} \to \mathbb{Z}_d$, $x \mapsto \overline{x}$, ryhmältä $(\mathbb{Z}, +)$ ryhmälle $(\mathbb{Z}_d, +)$. Tällöin

$$\begin{aligned} y \in f^{-1}(\{f(x)\}) &\Leftrightarrow f(y) = f(x) \\ &\Leftrightarrow \overline{y} = \overline{x} \\ &\Leftrightarrow d \,|\, y - x \\ &\Leftrightarrow y \in x + d\mathbb{Z}. \end{aligned}$$

Täten f:n säikeet ovat muotoa $x + d\mathbb{Z}$.

Olkoon G ryhmä ja $H \subseteq G$ ryhmän G normaali aliryhmä. Tarkastellaan nk. *kanonista surjektiota*

$$\pi : G \to G/H,\ x \mapsto xH,$$

ryhmältä G tekijäryhmälle $(G/H, \cdot)$. Tässä siis $\cdot$ on tekijäryhmän kertolasku, eli $(xH) \cdot yH = (xy)H$. Kuvaus π on triviaalisti surjektio, sillä G/H on kaikkien sivuluokkien joukko. Kuvaus on homomorfismi, sillä

$$\pi(xy) = (xy)H = (xH)(yH) = \pi(x)\pi(y).$$

Millainen $ker(\pi)$ on?

$$\begin{aligned} x \in ker(\pi) &\Leftrightarrow \pi(x) = eH \\ &\Leftrightarrow xH = eH \\ &\Leftrightarrow x = eh \text{ jollain } h \in H \\ &\Leftrightarrow x \in H. \end{aligned}$$

Siis $ker(\pi) = H$.

Lause 11.3. *Olkoon G ryhmä ja $H \subseteq G$ aliryhmä. Tällöin H on normaali jos ja vain jos on olemassa sellainen homomorfismi f, että $H = ker(f)$.*

Todistus. Suunta "$\Rightarrow$" käsiteltiin edellä: jos H on normaali, niin $\pi : G \to G/H$, $x \mapsto xH$, on homomorfismi siten, että $ker(f) = H$. Ekvivalenssin toinen suunta seuraa suoraan lauseesta 11.1. □

Lause 11.4 (Ensimmäinen isomorfialause)**.** *Olkoon $f : G \to G'$ homomorfismi. Kuvaus*

$$\overline{f} : G/ker(f) \to im(f),\ (x \cdot ker(f)) \mapsto f(x),$$

on isomorfismi.

Todistus. Käsitellään luennolla. □

Isomorfialause on kätevä, jos pitää todistaa isomorfismismi

$$G/H \cong J,$$

missä $J \subseteq G'$. Tällöin riittää identifioida sellainen homomorfismi $f : G \to G'$, että $ker(f) = H$ ja $im(f) = J$. Isomorfisuus seuraa suoraan isomorfialauseesta.

Esimerkki. Tarkastellaan reaalilukujen additiivista ryhmää $(\mathbb{R}, +)$ ja sen normaalia aliryhmää $(2\pi\mathbb{Z}, +)$. Tässä siis

$$2\pi\mathbb{Z} \ = \ \{\ 2\pi n \mid n \in \mathbb{Z}\ \}.$$

Sivuluokkakokoelmasta

$$\mathbb{R}/(2\pi\mathbb{Z}) \ = \ \{\ \varphi + 2\pi\mathbb{Z} \mid \varphi \in \mathbb{R}\ \}$$

saadaan *kulmien* muodostama tekijäryhmä $(\mathbb{R}/(2\pi\mathbb{Z}), +)$. Tämä ryhmä on siis tekijäryhmä, joten määritelmän mukaan ryhmäoperaatio toteuttaa ehdon

$$(\varphi + 2\pi\mathbb{Z}) + (\psi + 2\pi\mathbb{Z}) = (\varphi + \psi) + 2\pi\mathbb{Z}.$$

Olkoon $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ ja

$$S \ := \ \{\ z \in \mathbb{C}^* \mid |z| = 1\ \} = \text{yksikköympyrä}.$$

Tarkastellaan ryhmiä $(\mathbb{R}/(2\pi\mathbb{Z}), +)$ ja $(S, \cdot)$. Ryhmä $(S, \cdot)$ on ryhmän $(\mathbb{C}^*, \cdot)$ aliryhmä. Osoitetetaan, että $\mathbb{R}/(2\pi\mathbb{Z}) \cong S$, käyttäen hyväksi ensimmäistä isomorfialausetta.

Tarkastellaan kuvausta $f : \mathbb{R} \to \mathbb{C}^*$, $x \mapsto e^{ix}$. Tämä on homomorfismi $(\mathbb{R}, +)$:lta $(\mathbb{C}^*, \cdot)$:lle, sillä jos $x, y \in \mathbb{R}$, niin

$$f(x+y) = e^{i(x+y)} = e^{ix}e^{iy} = f(x)f(y).$$

Homomorfismille f pätee

$$ker(f) \ = \ \{ \ x \in \mathbb{R} \mid e^{ix} = 1 \ \} = 2\pi\mathbb{Z}$$

ja

$$\begin{aligned} im(f) \ &= \{ \ z \in \mathbb{C}^* \mid z = e^{ix} \text{ jollain } x \in \mathbb{R} \ \} \\ &= \{ \ z \in \mathbb{C}^* \mid |z| = 1 \ \} \\ &= S. \end{aligned}$$

Ensimmäisen isomorfialauseen perusteella siis $\mathbb{R}/(2\pi\mathbb{Z}) \cong S$. $\square$

Lause 11.5. *Jos G on äärellinen syklinen ryhmä, niin $(\mathbb{Z}_d, +) \cong G$ jollain $d \in \mathbb{Z}_+$. Jos G on ääretön syklinen ryhmä, niin $(\mathbb{Z}, +) \cong G$.*

Todistus. Oletetaan, että $d \in \mathbb{Z}_+$. Tiedämme, että $\mathbb{Z}/(d\mathbb{Z}) = \mathbb{Z}_d$: tämä osoitettiin yhdessä luvun 10 esimerkeistä. Yhteys pätee, koska

$$n + d\mathbb{Z} \ = \ \overline{n}.$$

Lisäksi $(\mathbb{Z}/d\mathbb{Z}, +) = (\mathbb{Z}_d, +)$, sillä tekijäryhmän ryhmäoperaation määritelmän ja jäännösluokkien summaoperaation määritelmän nojalla pätee

$$(n + d\mathbb{Z}) + (m + d\mathbb{Z}) = (n+m) + d\mathbb{Z} = \overline{n+m} = \overline{n} + \overline{m}.$$

Olkoon $G = \langle g \rangle$ syklinen ryhmä. Tarkastellaan kuvausta $f : \mathbb{Z} \to G$, $n \mapsto g^n$.

1.) Kaikilla $m, n \in \mathbb{Z}$ pätee

$$f(m+n) = g^{m+n} = g^m g^n = f(m)f(n),$$

joten f on homomorfismi.

2.) Selvästi $im(f) = G$, sillä G on syklinen ryhmä $G = \langle g \rangle$.

3 a) Jos $G = \langle g \rangle$ on äärellinen syklinen ryhmä siten, että $d = |G|$, niin

$$\begin{aligned} n \in ker(f) \ &\Leftrightarrow f(n) = e \\ &\Leftrightarrow g^n = e \\ &\Leftrightarrow d \mid n \text{ (Lause 8.6)} \\ &\Leftrightarrow n \in d\mathbb{Z}. \end{aligned}$$

Täten $ker(f) = d\mathbb{Z}$, joten ensimmäisen isomorfialauseen nojalla

$$(\mathbb{Z}_d, +) = (\mathbb{Z}/d\mathbb{Z}, +) \cong G.$$

3 b) Tarkastellaan tapausta, jossa G on ääretön syklinen ryhmä. Osoitetaan aluksi, että $ker(f) = \{0\}$. Tällöin isomorfialauseen nojalla $(\mathbb{Z}/\{0\}, +) \cong G$, mistä väite $(\mathbb{Z}, +) \cong G$ seuraa lyhyellä päättelyllä, joka on muotoiltu alla.

Osoitetaan siis ensiksi, että $ker(f) = \{0\}$. Tehdään vastaoletus, että $ker(f) \neq \{0\}$. Täten on olemassa $n \in ker(f)$, missä $n \neq 0$. Koska $ker(f)$ on ryhmä, on olemassa $m \in \{n, -n\}$ siten, että $m > 0$ ja $m \in ker(f)$. Täten $f(m) = g^m = e$. Näin ollen on helppo päätellä (HT), että $G = \{g^0, ..., g^{m-1}\}$. Täten G on äärellinen, mikä on ristiriita.

Nyt riittää osoittaa, että $(\mathbb{Z}, +) \cong (\mathbb{Z}/\{0\}, +)$, ja että kahden isomorfismin p ja q kompositio $p \circ q$ on isomorfismi.

Osoitetaan, että $(\mathbb{Z}, +) \cong (\mathbb{Z}/\{0\}, +)$; isomorfismien kompositio-ominaisuus käsitellään laskuharjoitusten yhteydessä. (Lisäksi laskuharjoitusten yhteydessä osoitetaan myöhemmin isomorfialauseen avulla, että yleisesti kaikille ryhmille X pätee $X/\{e\} \cong X$.)

Määritellään $g : \mathbb{Z} \to \mathbb{Z}/\{0\}$ siten, että $x \mapsto x + \{0\}$. Koska

$$\mathbb{Z}/\{0\} = \{\ \{x\} \mid x \in \mathbb{Z}\ \}$$

ja $g(x) = \{x\}$ kaikilla $x \in \mathbb{Z}$, niin g on selvästi hyvin määritelty bijektio. Lisäksi

$$g(x + y) = (x + y) + \{0\} = (x + \{0\}) + (y + \{0\}) = g(x) + g(y),$$

missä ensimmäinen ja viimeinen yhtälö seuraavat kuvauksen g määritelmästä, ja keskimmäinen yhtälö seuraa tekijästruktuurin ryhmäoperaation määritelmästä. Täten $(\mathbb{Z}, +) \cong (\mathbb{Z}/\{0\}, +)$. □

RENGASTEORIAA

12 Renkaan määritelmä

Olkoon $d \in \mathbb{Z}_+$. Joukossa

$$\mathbb{Z}_d \;=\; \{\, \overline{0}, \overline{1}, ..., \overline{d-1} \,\}$$

on määritelty yhteenlasku $\overline{x}+\overline{y} = \overline{x+y}$ ja kertolasku $\overline{x}\cdot\overline{y} = \overline{x\cdot y}$. Kumpikin laskutoimitus on vaihdannainen ja liitännäinen. Myös osittelulaki pätee:

$$\begin{aligned}
\overline{x}\cdot(\overline{y}+\overline{z}) &= \overline{x}\cdot\overline{y+z} \\
&= \overline{x\cdot(y+z)} \\
&= \overline{xy+xz} \\
&= \overline{xy}+\overline{xz} \\
&= \overline{x}\cdot\overline{y} \;+\; \overline{x}\cdot\overline{z}.
\end{aligned}$$

Lisäksi tiedämme, että $(\mathbb{Z}_d, +)$ on Abelin ryhmä. Olio $(\mathbb{Z}_d, +, \cdot)$ on esimerkki *renkaasta*.

Määritelmä 12.1. Olkoon $(R, +)$ Abelin ryhmä. Mikäli $\cdot$ on sellainen kuvaus $\cdot : R \times R \to R$, että

1. $(xy)z = x(yz)$ kaikilla $x, y, z \in R$,
2. on olemassa nk. *ykkösalkio* $u \in R$ siten, että $ux = xu = x$ kaikilla $x \in R$,
3. $x(y+z) = xy \;+\; xz$ ja $(x+y)z = xz \;+\; yz$ kaikilla $x, y, z \in R$,

niin olio $(R, +, \cdot)$ on *rengas*.

Yllä olevan ehdon 1 mukaan siis $\cdot$ on *liitännäinen*. Ehto 2 sanoo, että renkaasta R löytyy nk. *ykkösalkio* u. Tästä eteenpäin ykkösalkioehdon toteuttavaan alkioon viitataan symbolilla 1 symbolin u sijasta. On kuitenkin tärkeää huomata, että ykkösalkion ei tarvitse olla kokonaisluku $1 \in \mathbb{Z}$, vaikka ykkösalkioon viitataankin samalla symbolilla. Abelin ryhmän $(R, +)$ neutraalialkioon viitataan symbolilla 0. Tässäkin tapauksessa on mahdollista että neutraalialkio *ei* ole kokonaisluku $0 \in \mathbb{Z}$. Renkaan $(R, +, \cdot)$ Abelin ryhmän $(R, +)$ alkion $x \in R$ käänteisalkioon viitataan merkinnällä $-x$. Rengasteoreettisessa yhteydessä alkiota $-x$ kutsutaan alkion x *vasta-alkioksi*.

Ehto 3 sanoo, että laskutoimitukset $\cdot$ ja $+$ toteuttavat *osittelulait*. Kuten yllä on tehty, renkaan kertolasku $\cdot$ jätetään usein merkitsemättä, eli kirjoitetaan xy sen sijaan, että kirjoitettaisiin $x \cdot y$. Lisäksi, kertolasku suoritetaan ennen yhteenlaskua, kuten alkeisaritmetiikassakin, eli esimerkiksi

$$xy \ + \ xz \ = \ (x \cdot y) + (x \cdot z).$$

Usein on tapana puhua renkaasta R, sen sijaan, että puhuttaisiin renkaasta $(R, +, \cdot)$.

Esimerkki. Jos R on rengas, niin $x \cdot 0 = 0 = 0 \cdot x$ kaikilla $x \in R$:

$$0 \cdot x \ = \ (0 + 0) \cdot x \ = \ 0 \cdot x \ + \ 0 \cdot x,$$

joten lisäämällä $-(0 \cdot x)$ yhtälön molemmin puolin, saadaan

$$0 \ = \ 0 \cdot x.$$

Yhtälö $x \cdot 0 = 0$ todistetaan vastaavasti.

Esimerkki. Jos $0 = 1$ renkaassa R, niin $R = \{0\}$, koska tällöin

$$x = x \cdot 1 = x \cdot 0 = 0.$$

Esimerkki. Renkaan R ykkösalkio on yksikäsitteinen, eli on olemassa täsmälleen yksi alkio $u \in R$ siten, että $ux = xu = x$ pätee kaikilla $x \in R$:

$$1 = 1' \cdot 1 = 1'.$$

Mikäli $xy = yx$ pätee kaikilla $x, y \in R$, sanotaan, että rengas R on *kommutatiivinen*.

Esimerkki. $(\mathbb{Z}_d, +, \cdot)$ on kommutatiivinen rengas kaikilla $d \in \mathbb{Z}_+$. Lisäksi $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ ja $(\mathbb{C}, +, \cdot)$ ovat kommutatiivisia renkaita.

Määritelmä 12.2. Olkoon R rengas. Joukko $S \subseteq R$ on renkaan R *alirengas*, mikäli

1. S on ryhmän $(R, +)$ aliryhmä,
2. $1 \in S$, missä 1 on renkaan R ykkösalkio,
3. $x, y \in S \ \Rightarrow \ xy \in S$.

Alirengas on rengas (HT).

Esimerkki. *Gaussin kokonaisluvut* $\{\ a+ib \mid a,b \in \mathbb{Z}\ \}$ muodostavat kompleksilukujen $\mathbb{C}$ renkaan alirenkaan.

Määritelmä 12.3. Olkoon R rengas ja $x \in R$. Jos on olemassa sellainen $y \in R$, että $xy = yx = 1$, niin x on renkaan R *yksikkö* (tai, vaihtoehtosesti, x on *kääntyvä* renkaassa R).

Otetaan käyttöön merkintä

$$R^* \ := \ \{\, x \in R \mid x \text{ on } R\text{:n yksikkö } \}.$$

Esimerkki. $\mathbb{Z}^* = \{\, 1, -1 \,\}$, $\mathbb{Q}^* \ = \ \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* \ = \ \mathbb{R} \setminus \{0\}$, $\mathbb{C}^* \ = \ \mathbb{C} \setminus \{0\}$.

Esimerkki. Aikaisemmin määrittelemämme alkuluokkien joukko

$$\mathbb{Z}_d^* = \{\ \overline{a} \in \mathbb{Z}_d \mid \mathit{syt}(a,d) = 1\ \}$$

on renkaan $(\mathbb{Z}_d, +, \cdot)$ yksiköiden joukko Lauseen 7.3 nojalla.

Lause 12.4. *Olkoon R rengas. Tällöin $(R^*, \cdot)$ on ryhmä.*

Todistus. Käsitellään luennolla. □

13 Rengashomomorfismi

Määritelmä 13.1. Olkoot R ja R' renkaita. Kuvaus $f : R \to R'$ on rengashomomorfismi, mikäli

1. $f(x+y) = f(x) + f(y)$ kaikilla $x, y \in R$, eli f on ryhmähomomorfismi ryhmältä $(R, +)$ ryhmälle $(R', +)$,
2. $f(xy) = f(x)f(y)$ kaikilla $x, y \in R$,
3. $f(1) = 1'$.

Rengasisomorfismi on bijektiivinen rengashomomorfismi.

Esimerkki. Kuvaus $f : \mathbb{R} \to \mathbb{C}$, $x \mapsto (x, 0)$, on rengashomomorfismi, sillä jos $x, y \in \mathbb{R}$, niin

1. $f(x+y) = (x+y, 0) = (x, 0) + (y, 0) = f(x) + f(y)$,
2. $f(xy) = (xy, 0) = (x, 0)(y, 0) = f(x)f(y)$,
3. $f(1) = (1, 0)$.

Itse asiassa kyseessä injektiivinen homomorfismi, eli upotus.

Lause 13.2. *Jos $f : R \to R'$ on rengashomomorfismi, niin sen* kuva, *eli joukko*

$$im(f) := \{ y \in R \mid y = f(x) \text{ jollain } x \in R \},$$

on renkaan R' alirengas.

Todistus. Harjoitustehtävä □

14 Kunnat ja kokonaisalueet

Määritelmä 14.1. Olkoon R rengas ja $x \in R$, $x \neq 0$. Jos on olemassa $y \in R \setminus \{0\}$ siten, että $xy = 0$ tai $yx = 0$, niin x on *nollantekijä*.

Esimerkki. $\overline{2}$ on nollantekijä renkaassa $\mathbb{Z}_4$, sillä $\overline{2} \cdot \overline{2} = \overline{0}$.

Lause 14.2 (Supistussääntö)**.** *Jos R on rengas ja $a \in R \setminus \{0\}$ ei ole nollantekijä, niin kaikilla $x, y \in R$ pätee*

$$ax = ay \ \Rightarrow x = y.$$

Todistus. Käsitellään luennolla. □

Määritelmä 14.3. Jos R on kommutatiivinen rengas, jossa ei ole nollantekijöitä, niin R on *kokonaisalue*.

Havaitsemme, että kommutatiivinen rengas R on kokonaisalue jos ja vain jos kaikilla $x, y \in R$,

$$xy = 0 \ \Rightarrow \ (x = 0 \text{ tai } y = 0).$$

Esimerkki. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ja $\mathbb{C}$ ovat kokonaisalueita.

Määritelmä 14.4. Kommutatiivinen rengas K on *kunta*, jos jokaisella $x \in K \setminus \{0\}$ on *käänteisalkio* x^{-1} siten, että $xx^{-1} = 1$.

Toisin sanoen, kommutatiivinen rengas K on kunta, jos $K^* = K \setminus \{0\}$.

Kunnassa K alkion $x \in K$ käänteisalkio on alkio x^{-1} siten, että $xx^{-1} = 1$, kun taas alkion x vasta-alkio $-x$ on alkio siten, että $x + (-x) = 0$.

Esimerkki. $\mathbb{Q}$, $\mathbb{R}$ ja $\mathbb{C}$ ovat kuntia. $\mathbb{Z}$ ei ole kunta.

Lause 14.5. *Jos K on kunta, niin se on kokonaisalue.*

Todistus. Käsitellään luennolla. □

Lause 14.6. *Olkoon $d \in \mathbb{N} \setminus \{0\}$ luku. Seuraavat ehdot ovat yhtäpitäviä.*

1. *$\mathbb{Z}_d$ on kokonaisalue.*
2. *d on alkuluku.*
3. *$\mathbb{Z}_d$ on kunta.*

Todistus. Käsitellään luennolla. □

Olkoon $(R, +, \cdot)$ rengas ja $a \in R$. Määritellään merkintä a^n, missä $n \in \mathbb{N}$.

1. $a^0 = 1$ (missä $0 \in \mathbb{N}$ ja $1 \in R$),
2. $a^{n+1} = a^n \cdot a$.

Renkaissa potenssi a^n siis viittaa kertolaskuun. Määritellään lisäksi renkaan yhteenlaskuun viittaava uusi merkintä na, missä $n \in \mathbb{N}$ ja $a \in R$:

1. $0a = 0 \in R$ (missä ensimmäinen 0 kuuluu joukkoon $\mathbb{N}$ ja toinen renkaaseen R),
2. $(n+1)a = a + (na)$.

Merkintä na siis viittaa summaan $a + a + ... + a$, missä a esiintyy n kertaa. Lisäksi, jos $n \in \mathbb{N}$ ja $a \in R$, niin määritellään, että

$$(-n)a = -(na).$$

Muista, että renkaan $(R, +, \cdot)$ määräämä olio $(R, +)$ on ryhmä, ja vertaa nyt määrittelemiämme yhteenlaskuun liittyviä merkintöjä na ja $(-n)a$ ryhmäteorian yhteydessä annettuun potenssimerkintään g^n, missä $g \in G$ ryhmällä G. Merkintä na on siis vanha tuttu ryhmän potenssimerkintä, mutta uusi merkintä na on tarpeellinen, sillä merkintä a^n viittaa renkaan kertolaskuun.

Toisin sanoen, kun n on positiivinen, merkintä a^n viittaa alkioon $a \cdot a \cdot ... \cdot a$, missä a esiintyy n kertaa, ja merkintä na viittaa alkioon $a + a + ... + a$, missä a esiintyy n kertaa.

Luvuissa 15, 16 ja 17 renkaalla tarkoitetaan aina kommutatiivista rengasta, jossa $0 \neq 1$. (Tentissä ja harjoitustehtävissä ilmoitetaan aina selvästi, tehdäänkö tämä oletus vai ei.)

15 Polynomirenkaat

Olkoon R rengas. *Polynomifunktio* on kuvaus $f : R \to R$ siten, että

$$x \mapsto a_n x^n + a_{n-1}x^{n-1} + ... + a_2 x^2 + a_1 x + a_0,$$

missä $a_0, a_1, ..., a_n \in R$ on *äärellinen* joukko alkioita.

Esimerkki. Tarkastellaan rengasta $(\mathbb{Z}_3, +, \cdot)$. Kuvaus $f : \mathbb{Z}_3 \to \mathbb{Z}_3$,

$$x \mapsto \overline{2}\, x^3 + \overline{2}\, x^2 + \overline{0}\, x + \overline{1},$$

on polynomifunktio. (HT: Laske $f(\overline{2})$.) Myös kuvaus $g : \mathbb{Z}_3 \to \mathbb{Z}_3$,

$$x \mapsto x^8 + \overline{2}\, x^3,$$

on polynomifunktio. (HT: Laske $f(\overline{2})$.) Edelleen, myös kuvaus $h : \mathbb{Z}_3 \to \mathbb{Z}_3$,

$$x \mapsto \overline{1},$$

on polynomifunktio.□

Esimerkki. Tarkastellaan rengasta $(\mathbb{Z}, +, \cdot)$. Kuvaus $f : \mathbb{Z} \to \mathbb{Z}$,

$$x \mapsto 9\, x^3 + 40\, x^2 + 2\, x,$$

on polynomifunktio. Myös kuvaus $g : \mathbb{Z} \to \mathbb{Z}$,

$$x \mapsto x$$

on polynomifunktio, kuten on kuvaus $k : \mathbb{Z} \to \mathbb{Z}$,

$$x \mapsto 0.$$

Tarkastellaan sitten rengasta $(\mathbb{R}, +, \cdot)$. Kuvaus $h : \mathbb{R} \to \mathbb{R}$,

$$x \mapsto 6,987x^6 + \pi x,$$

on polynomifunktio.□

Otetaan käyttöön merkintä $\sum_{i \in \mathbb{N}} a_i x^i$,

$$\sum_{i \in \mathbb{N}} a_i x^i = a_0 + a_1 x + a_2 x^2 + ...$$

missä alkiot a_i ovat jonkin renkaan alkioita. Huomaa, että $\sum_{i\in\mathbb{N}} a_i x^i$ identifioi polynomifunktion, mikäli on olemassa sellainen $j \in \mathbb{N}$, että kaikilla $k \geq j$ pätee $a_k = 0$. Eli jostakin alkiosta a_j alkaen, kertoimet a_i ovat nollia.

Olkoon R rengas ja $p : R \to R$ ja $q : R \to R$ polynomifunktioita. Määritellään, että $p + q$ on funktio siten, että

$$(p + q)(x) = p(x) + q(x)$$

kaikilla $x \in R$. Toisin sanoen, jos

$$p(x) = \sum_{i\in\mathbb{N}} a_i x^i$$

ja

$$q(x) = \sum_{i\in\mathbb{N}} b_i x^i,$$

niin $p + q$ on funktio siten, että

$$(p + q)(x) = \Big(\sum_{i\in\mathbb{N}} a_i x^i\Big) + \Big(\sum_{i\in\mathbb{N}} b_i x^i\Big) \;=\; \sum_{i\in\mathbb{N}} (a_i + b_i)x^i.$$

Selvästi nähdään, että $(p + q)$ on polynomifunktio.

Samaan tapaan, määritellään, että pq on funktio siten, että

$$(pq)(x) = p(x)q(x)$$

kaikilla $x \in R$. Toisin sanoen, pq funktio siten, että

$$(pq)(x) = \Big(\sum_{i\in\mathbb{N}} a_i x^i\Big)\Big(\sum_{i\in\mathbb{N}} b_i x^i\Big) \;=\; \sum_{j\in\mathbb{N}} \Big(\sum_{i=0}^{j} a_i b_{j-i}\Big) x^j,$$

koska

$$\begin{aligned}
\Big(\sum_{i\in\mathbb{N}} a_i x^i\Big)\Big(\sum_{i\in\mathbb{N}} b_i x^i\Big) \;&=\; (a_0 + a_1 x + ... + a_n x^n)(b_0 + b_1 x + ... + b_m x^m) \\
&=\; a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + ... \\
&\quad ... + (a_n b_m)x^{n+m} \\
&=\; \sum_{j\in\mathbb{N}} \Big(\sum_{i=0}^{j} a_i b_{j-i}\Big) x^j.
\end{aligned}$$

("a:n ja b:n alaindeksit summautuvat x:n eksponenttiin.")

Selvästi nähdään, että funktio pq on polynomifunktio.

Eli, polynomifunktioilla voidaan siis laskea, kun määritellään yhteenlaskuoperaatio ja kertolaskuoperaatio siten, että

$$(p+q)(x) = p(x) + q(x)$$

ja

$$(pq)(x) = p(x)q(x)$$

kaikilla $x \in R$. Tällöin $p+q$ ja pq ovat polynomifunktioita.

Esimerkki. Olkoon X joukko ja R rengas. Määritellään olio $(F(X,R),+,\cdot)$, missä

1. $F(X,R) := \{\ f \mid f \text{ on funktio } X \to R\ \}$,
2. kaikille $f,g \in F(X,R)$ pätee, että $(f+g)$ on funktio $X \to R$ siten, että $(f+g)(x) = f(x) + g(x)$ kaikille $x \in R$,
3. kaikille $f,g \in F(X,R)$ pätee, että (fg) on funktio $X \to R$ siten, että $(fg)(x) = f(x)g(x)$ kaikille $x \in R$.

Laskuharjoitusten yhteydessä osoitetaan, että struktuuri $(F(X,R),+,\cdot)$ on rengas.[1]

Tarkastellaan rengasta $(F(R,R),+,\cdot)$. Osoitetaan, että polynomifunktioiden $R \to R$ kokoelma P muodostaa struktuurin $(F(R,R),+,\cdot)$ alirenkaan.

1. Osoitetaan, että $(P,+)$ on ryhmän $(F(R,R),+)$ aliryhmä.
   (a) Nollafunktio $x \mapsto 0$ on ryhmän $(F(R,R),+)$ neutraalialkio. Selvästi nollafunktio 0 on myös polynomifunktio. Ryhmän $(F(R,R),+)$ neutraalialkio, eli nollafunktio 0, siis kuuluu joukkoon P.
   (b) Oletetaan, että $p \in P$. On osoitettava, että $-p \in P$. Mikä on $-p \in F(R,R)$? $-p$ on funktio siten, että $((-p)+p) = (p+(-p)) = 0$ (nollafunktio). Olkoon $p(x) = \sum_{i \in \mathbb{N}} a_i x^i$. Määritellään funktio $q : R \to R$ siten, että
   $$q(x) = \sum_{i \in \mathbb{N}} -(a_i x^i).$$

[1] Kyseisissä laskuharjoituksissa ei oleteta, että rengas on aina kommutatiivinen rengas, jossa $0 \neq 1$. Laskuharjoitusten todistusta laajentamalla on kuitenkin triviaali osoittaa, että jos R on kommutatiivinen rengas jossa $0 \neq 1$, niin tällöin $(F(X,R),+,\cdot)$ on kommutatiivinen rengas, jossa $0 \neq 1$.

Nyt $q + p = p + q = 0$, joten riittää osoittaa, että q on polynomifunktio. Koska renkaissa $-(uv) = (-u)v$ (laskuharjoitukset), niin

$$q(x) = \sum_{i \in \mathbb{N}} (-a_i) x^i.$$

Täten $q = -p$ on polynomifunktio. Siis $-p \in P$.

(c) Oletetaan, että $p, q \in P$. On osoitettava, että $(p + q) \in P$. Tämä tehdiin jo edellä: jos $p(x) = \sum_{i \in \mathbb{N}} a_i x^i$ ja $q(x) = \sum_{i \in \mathbb{N}} b_i x^i$, niin tällöin

$$(p + q)(x) = \Big(\sum_{i \in \mathbb{N}} b_i x^i\Big) + \Big(\sum_{i \in \mathbb{N}} b_i x^i\Big) = \sum_{i \in \mathbb{N}} (a_i + b_i) x^i,$$

mistä nähdään helposti, että $(p + q)$ on polynomifunktio.

2. Osoitetaan, että renkaan $F(R, R)$ ykkösalkio kuuluu joukkoon P. Ykkösalkio on vakiofunktio $f = 1$, eli funktio $f : R \to R$ siten, että $f(x) = 1$ kaikilla $x \in R$. Selvästi $f = 1$ on polynomifunktio.

3. Osoitetaan, että jos $p, q \in P$, niin $(pq) \in P$. Tämäkin nähtiin jo edellä.□

Polynomifunktioihin liittyy ongelma, joka on kiusallinen eräiden matemaattisten tarkastelujen kannalta. Nimittäin, kaksi eri merkkijonoa

$$a_n x^n + ... + a_0 \text{ ja } b_m x^m + ... + b_0$$

määrittelevät joissakin tapauksissa *saman* polynomifunktion. Tarkastellaan esimerkiksi polynomifunktiota $f : \mathbb{Z}_3 \to \mathbb{Z}_3$, $x \mapsto x^3 + \overline{2}x$. Havaitaan, että

$$f(\overline{0}) = f(\overline{1}) = f(\overline{2}) = \overline{0},$$

joten f on nollakuvaus. Täten eri merkkijonot

$$x^3 + \overline{2}x \text{ ja } \overline{0}$$

määrittelevät saman polynomifunktion. Samaan tapaan, eri merkkijonot

$$x \text{ ja } x^2$$

määrittelevät yhden ja saman polynomifunktion renkaassa $\mathbb{Z}_2$. Seuraavaksi kehitellään tapa välttää tämä ilmiö.

Määritelmä 15.1. Jos R on rengas, niin *R-kertoiminen polynomi* on kuvaus

$$p : \mathbb{N} \to R$$

siten, että jollain $j \in \mathbb{N}$ pätee, että $p(k) = 0$ kaikilla $k \geq j$. Toisin sanoen, jostakin syötteestä j alkaen, kaikki p:n arvot ovat nollia.

Polynomi $p : \mathbb{N} \to R$ samaistetaan jonon

$$p = (a_0, a_1, a_2, ..., a_n, 0, 0, 0, 0, 0, 0, ...)$$

kanssa, missä $a_i = p(i)$ kaikilla $i \in \mathbb{N}$.

Esimerkki. Tarkastellaan rengasta $(\mathbb{Z}, +, \cdot)$. Jono

$$p = (1, 2, 3, 0, 6, 0, 0, 0, 0, 0, 0, ...)$$

on $\mathbb{Z}$-kertoiminen polynomi. Tämä polynomi p vastaa intuition tasolla merkkijonoa

$$6x^4 + 3x^2 + 2x + 1.$$

Jono

$$(0, 19, 0, 2, 10, 0, 0, 0, 0, 0, 0, ...)$$

taas vastaa merkkijonoa

$$10x^4 + 2x^3 + 19x.$$

Merkkijonoa

$$x^6 + x^3 + 2x^2 + 8$$

vastaa polynomi

$$(8, 0, 2, 1, 0, 0, 1, 0, 0, 0, 0, 0, ...).$$

Tarkastellaan sitten rengasta $(\mathbb{Z}_8, +, \cdot)$. Polynomi

$$(\overline{7}, \overline{1}, \overline{2}, \overline{6}, \overline{0}, \overline{1}, \overline{0}, \overline{0}, \overline{0}, \overline{0}, \overline{0}, \overline{0}, ...)$$

vastaa merkkijonoa

$$x^5 + \overline{6}x^3 + \overline{2}x^2 + x + \overline{7}. \quad \square$$

Otetaan käyttöön merkintä

$$R[X] := \{\ p \mid p \text{ on } R\text{-kertoiminen polynomi }\}.$$

On tärkeää huomata, että polynomi ei ole sama asia kuin polynomifunktio.

Olkoot $p, q \in R[X]$ polynomeja. Määritellään summa $p+q$ ja tulo pq siten, että $p+q$ on polynomi joukossa $R[x]$, jolle pätee

$$(p+q)(j) = p(j) + q(j)$$

kaikilla $j \in \mathbb{N}$, ja pq on polynomi joukossa $R[X]$, jolle pätee

$$(pq)(j) = \sum_{i=0}^{j} p(i)q(j-i)$$

kaikilla $j \in \mathbb{N}$. Kerroin $(pq)(j)$ on siis summa kaikista tuloista $p(l)q(k)$, missä $l+k=j$. Vertaa tulon määritelmää aikaisemmin suorittamaamme (polynomifunktioita koskevaan) tarkasteluun, jossa totesimme, että

$$\begin{aligned}\Big(\sum_{i\in\mathbb{N}} a_i x^i\Big)\Big(\sum_{i\in\mathbb{N}} b_i x^i\Big) &= (a_0 + a_1 x + ... + a_n x^n)(b_0 + b_1 x + ... + b_m x^m) \\ &= a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + ... \\ &\quad ... + (a_n b_m)x^{n+m} \\ &= \sum_{j\in\mathbb{N}} \Big(\sum_{i=0}^{j} a_i b_{j-i}\Big) x^j.\end{aligned}$$

Eli, polynomien summa ja kertolasku määritellään siten, että

$$(a_0, a_1, a_2, ...) + (b_0, b_1, b_2, ...) = (a_0 + b_0,\ a_1 + b_1,\ a_2 + b_2, ...)$$

ja

$$(a_0, a_1, a_2, ...) \cdot (b_0, b_1, b_2, ...) = (a_0 b_0,\ a_0 b_1 + a_1 b_0,\ a_0 b_2 + a_1 b_1 + a_2 b_0, ...).$$

Kertolaskussa siis "tulotermien alaindeksit summautuvat vastaavan koordinaattiposition järjestyslukuun". Esimerkiksi koordinaattiposition 2 tulotermit ovat $a_0 b_2$, $a_1 b_1$ ja $a_2 b_0$. Vasemmanpuoleisin koordinaattipositio on koordinaattipositio 0.

Esimerkki. Summaillaan ja kerrotaan konkreettisia polynomeja

$$(a, b, c, 0, 0, 0, ...).$$

Esimerkki käsitellään luennolla.

Jos $a \in R$, niin jono

$$(a, 0, 0, 0, ...)$$

on *vakiopolynomi* $p_a \in R[X]$.

Kuvaus $f : R \to R[X]$, $a \mapsto p_a$, on injektio siten, että

$$f(a + b) = p_{a+b} = p_a + p_b = f(a) + f(b)$$

ja

$$f(ab) = p_{ab} = p_a p_b = f(a)f(b).$$

Lisäksi

$$f(1) = p_1 = (1, 0, 0, 0, ...).$$

Täten f on rengashomomorfismi, kunhan vielä osoitetaan, että $R[X]$ on rengas, jonka ykkösalkio on p_1. Näin ollen f on upotus, eli injektiivinen homomorfismi $R \to R[X]$. Intuition tasolla täten rengas $R[X]$ sisältää kopion renkaasta R. Vakiopolynomit p_a muodostavat kyseessä olevan kopion. Merkitään jatkossa epämuodollisesti

$$p_a = a,$$

jolloin R " $\subseteq$ " $R[X]$.

Lemma 15.2. *Jos $a \in R$ ja $p \in R[X]$, niin*

$$(a\,p)(i) = a\,p(i) \text{ kaikilla } i \in \mathbb{N}.$$

Tässä ensimmäinen a on $p_a \in R[X]$ ja toinen a on alkio joukossa R.

Todistus. Käsitellään luennolla. □

Lemma 15.2 sanoo yksinkertaisesti, että

$$a(a_0, a_1, a_2, ...) = (aa_0, aa_1, aa_2, ...).$$

Lause 15.3. *Jos R on rengas, niin samoin on $R[X]$ (nk.* polynomirengas*).*

Todistus. Laskuharjoitusten yhteydessä osoitetaan, että $(F(X, R), +)$ on rengas.[2] Laskuharjoitusten argumentin nojalla on helppo nähdä, että $(R[X], +)$ on ryhmän $(F(\mathbb{N}, R), +)$ aliryhmä, ja edelleen näin ollen selvästi Abelin ryhmä.

[2]Ks. laskuharjoituksissa ei oleteta, että rengas tarkoittaa kommutatiivista rengasta, jossa $0 \neq 1$. Tällä ei ole merkitystä todistuksemme kannalta.

1.) Ykkösalkio joukossa $R[X]$ on vakiopolynomi $p_1 = 1$, sillä Lemman 15.2 nojalla

$$(1 \cdot p)(i) = 1 \cdot p(i) = p(i)$$

kaikilla $p \in R[X]$; myös

$$(p \cdot 1)(i) = p(i),$$

mikä seuraa lopulta siitä, että $R[X]$ osoitetaan kommutatiiviseksi (ks. alla).

2.) Olkoot $p, q, r \in R[X]$. Nyt

$$\begin{aligned}
[(pq)r](i) &= \sum_{j+k=i} (pq)(j)\ r(k) \\
&= \sum_{j+k=i} \Big(\sum_{m+l=j} p(m)q(l) \Big) r(k) \\
&= \sum_{m+l+k=i} p(m)q(l)r(k) \\
&= \sum_{j+m=i} p(m) \Big(\sum_{l+k=j} q(l)r(k) \Big) \\
&= \sum_{j+m=i} p(m)(qr)(j) \\
&= [p(qr)](i).
\end{aligned}$$

3.) Koska tässä luvussa renkaalla tarkoitetaan kommutatiivista rengasta, osoitetaan, että $R[X]$ on kommutatiivinen. Tämä seuraa R:n kommutatiivisuudesta.

$$\begin{aligned}
(pq)(i) &= \sum_{j+k=i} p(j)q(k) \\
&= \sum_{j+k=i} q(k)p(j) \\
&= (qp)(i).
\end{aligned}$$

4.) Koska $R[X]$ on osoitettu kommutatiiviseksi, osittelulakien osoittami-

seksi riittää käsitellä toinen osittelulaki.

$$\begin{aligned}
[p(q+r)](i) &= \sum_{j+k=i} p(j)\ (q+r)(k) \\
&= \sum_{j+k=i} p(j)\ (q(k)+r(k)) \\
&= \sum_{j+k=i} \big(p(j)q(k)+p(j)r(k)\big) \\
&= \sum_{j+k=i} p(j)q(k)\ +\ \sum_{j+k=i} p(j)r(k) \\
&= (pq)(i)+(pr)(i) \\
&= (pq+pr)(i).
\end{aligned}$$

Koska $0 \in R$ ja $1 \in R$ ovat eri alkiot, niin selvästi ykkösalkio p_1 ei ole Abelin ryhmän $(R[X],+)$ nolla-alkio p_0. Täten $R[X]$ on rengas. □

Määritellään *muuttuja* $X \in R[X]$ asettamalla

$$X(i) = \begin{cases} 1, \text{ kun } i = 1 \\ 0, \text{ kun } i \neq 1. \end{cases}$$

Toisin sanoen,

$$X := (0,1,0,0,0,...).$$

Lemma 15.4. *Jos $n \in \mathbb{N}$, niin*

$$X^n(i) = \begin{cases} 1, \ \textit{kun } i = n \\ 0, \ \textit{kun } i \neq n. \end{cases}$$

Toisin sanoen,

$$X^n = (...,0,0,0,1,0,0,0,...),$$

missä 1 on koordinaattiposition n kohdalla. (Huomaa, että

$$X^0 = 1 = (1,0,0,0,...)$$

potenssin määritelmän nojalla.)

Todistus. Käsitellään luennolla. □

Lause 15.5. *Jokaiselle $p \in R[X]$ on olemassa yksikäsitteinen esitys*

$$p = \sum_{i \in \mathbb{N}} a_i X^i,$$

missä $a_i = p_{a_i} \in R[X]$ jokaisella $i \in \mathbb{N}$, ja lisäksi on olemassa jokin $k \in \mathbb{N}$ siten, että kaikilla $j \geq k$ pätee $a_j = 0 = p_0$. Toisin sanoen, jostakin luvusta k lähtien kaikki kertoimet a_i ovat nollia.

Todistus. Käsitellään luennolla. □

Esimerkki. Tarkastellaan polynomirengasta $\mathbb{Z}[X]$. Esimerkiksi

$$(0, 6, 0, 8, 0, 0, 0, ...) = 8X^3 + 6X,$$

missä termien 6 ja 8 jälkimmäisille esiintymille pätee

$$6 = p_6 = (6, 0, 0, 0, 0, ...) \in \mathbb{Z}[X],$$
$$8 = p_8 = (8, 0, 0, 0, 0, ...) \in \mathbb{Z}[X].$$

Lisäksi tietenkin

$$X = (0, 1, 0, 0, 0, ...) \in \mathbb{Z}[X].$$

Tarkastellaan mielivaltaista polynomirengasta $R[X]$. Kiinnitetään jotkin alkiot $a, b, c, d \in R[X] \setminus \{0\}$. Lauseen 15.5 nojalla polynomien summaesitykset ovat yksikäsitteisiä, joten esimerkiksi

$$aX^2 + bX \neq cX^3 + d$$

pätee polynomirenkaassa $R[X]$. □

Määritelmä 15.6. Olkoon R rengas ja $p \in R[X] \setminus \{0\}$ polynomi. Mikäli

$$p = a_n X^n + a_{n-1} X^{n-1} + ... + a_0,$$

missä $a_n \neq 0$, niin a_n on polynomin p *johtava kerroin*. Lisäksi, n on polynomin *aste*. Otetaan käyttöön merkintä $deg(p) = n$. Lisäksi sovitaan, että polynomille $0 \in R[X]$ pätee $deg(0) = -\infty$.

Nollapolynomin $0 \in R[X]$ aste on siis $-\infty$. Määritellään, että kaikille $k \in \mathbb{N} \cup \{-\infty\}$ pätee

$$-\infty + k = k + -\infty = -\infty, \ -\infty \leq k \text{ ja } \ -\infty < 0.$$

Lause 15.7. *Jos R on kokonaisalue, niin samoin on $R[X]$. Tällöin*

$$deg(pq) = deg(p) + deg(q)$$

kaikilla $p, q \in R[X]$.

Todistus. Käsitellään luennolla. □

Olkoon R on rengas, $p \in R[X]$ on polynomi,

$$p = \sum_{i \in \mathbb{N}} a_i X^i,$$

ja $c \in R$ renkaan R alkio. Tällöin merkintä $p(c)$ tarkoittaa renkaan R alkiota

$$p(c) \ := \ \sum_{i \in \mathbb{N}} a_i c^i.$$

Eli $p(c)$ on se renkaan R alkio, joka saadaan "sijoittamalla" c polynomiin p.

Lause 15.8. *Jos R on rengas ja $c \in R$, niin kuvaus*

$$s_c : R[X] \to R, \ f \mapsto f(c),$$

on homomorfismi (*nk.* sijoitushomomorfismi).

Todistus. HT. □

Määritelmä 15.9. Olkoon R rengas ja $p \in R[X]$. Jos $a \in R$ ja $p(a) = 0$, niin a on p:n juuri.

Kuten jo edellä totesimme, jatkossa merkitsemme usein epämuodollisesti

$$p_a = a.$$

Jatkossa vakiopolynomit $p_a \in R[X]$ ja vakiot $a \in R$ samaistetaan usein ilman erillistä varoitusta. Voimme esimerkiksi määritellä, että $a \in R$, ja tämän jälkeen todeta, että $a + X \in R[X]$. Virallisesti termi $a + X$ viittaa tällöin tietenkin termiin $p_a + X$.

Olkoot c, d renkaan R alkioita. Merkintä $c - d$ tarkoitaa alkiota $c + (-d)$.

16 Jakoyhtälö

Olkoon K kunta ja $a, b \in K$, $b \neq 0$. Tällöin $\frac{a}{b}$ tarkoittaa alkiota ab^{-1}. Tässä luvussa merkki K tarkoittaa aina kuntaa. Lukuja 15, 16 ja 17 koskevan oletuksemme nojalla renkaat ovat kommutatiivisia renkaita joissa $0 \neq 1$. Kunnat ovat renkaita, joten $0 \neq 1$ pätee kunnissa.

Lause 16.1 (Jakoyhtälö.)**.** *Olkoon K kunta ja $f \in K[X]$ polynomi. Jos $0 \neq g \in K[X]$, niin on olemassa yksikäsitteiset polynomit $q, r \in K[X]$ siten, että*

$$f = q \cdot g + r$$

ja $deg(r) < deg(g)$.

Todistus. 1.) Olemassaolo:

Jos $f = qg$ jollain $q \in K[X]$, niin olemassaolo on selvä. Oletetaan siis, että näin ei ole. Tarkastellaan joukkoa

$$M := \{ n \in \mathbb{N} \mid n = deg(f - qg) \text{ jollain } q \in K[X] \}.$$

Koska luonnollisten lukujen joukko on hyvinjärjestetty, niin joukolla M on olemassa pienin alkio $min(M)$. Täten

$$min(M) = deg(f - qg)$$

jollain $q \in K[X]$. Merkitään $r := f - qg$. Osoitetaan, että

$$deg(r) = min(M) < deg(g).$$

Merkitään

$$p := min(M) \text{ ja } m := deg(g).$$

Vastaoletus: $p \geq m$. Olkoot

$$r = a_p X^p + a_{p-1} X^{p-1} + ... + a_0$$

ja

$$g = b_m X^m + b_{m-1} X^{m-1} + ... + b_0,$$

ja olkoon

$$h = r - \frac{a_p}{b_m} X^{p-m} g.$$

Tällöin

$$\begin{aligned} h &= r - \frac{a_p}{b_m} X^{p-m} g \\ &= r - \Big(\frac{a_p}{b_m} b_m X^p + \frac{a_p}{b_m} b_{m-1} X^{p-1} + ... \Big) \\ &= \big(a_p - \frac{a_p}{b_m} b_m\big) X^p + \big(a_{p-1} - \frac{a_p}{b_m} b_{m-1}\big) X^{p-1} + ... \ , \end{aligned}$$

missä termin X^p kerroin on

$$a_p - \frac{a_p}{b_m} b_m = 0,$$

joten $deg(h) < p$. Mutta

$$\begin{aligned} h &= r - \frac{a_p}{b_m} X^{p-m} g \\ &= f - gq - \frac{a_p}{b_m} X^{p-m} g \\ &= f - \big(q + \frac{a_p}{b_m} X^{p-m}\big) g, \end{aligned}$$

joten $deg(h) \in M$. Tämä on ristiriita.

2.) Yksikäsitteisyys:

Oletetaan, että on olemassa jotkin $q, r, q', r' \in K[X]$ siten, että

$$f = qg + r = q'g + r',$$

missä $deg(r) < deg(g)$ ja $deg(r') < deg(g)$. Tehdään vastaoletus, että $q' \neq q$. Täten

$$r - r' = q'g - qg = (q' - q)g.$$

Jos pätisi, että $q' \neq q$, niin Lauseen 15.7 nojalla pätisi

$$deg\big((q' - q)g\big) = deg(q' - q) + deg(g) \geq deg(g).$$

Tämä on mahdotonta, sillä

$$deg\big((q' - q)g\big) = deg(r - r') \leq max\{deg(r), deg(r')\} < deg(g).$$

Näin ollen $q = q'$. Täten

$$r - r' = (q' - q)g = 0 \cdot g = 0,$$

joten myös $r = r'$. □

Lause 16.2. *Olkoon $f \in K[X]$ polynomi. Jos $a \in K$, niin tällöin $f(a) = 0$ jos ja vain jos jollain $g \in K[X]$ pätee $f = (X - a)g$.*

Todistus. Oletetaan, että $f(a) = 0$. Jakoyhtälön nojalla on olemassa jotkin $q, r \in K[X]$ siten, että

$$f = (X - a)q + r,$$

missä $deg(r) < deg(X - a) = 1$. Merkitään $g := q$, eli

$$f = (X - a)g + r$$

ja $deg(r) < 1$. Koska $deg(r) \leq 0$, niin $r \in K$, eli r on vakio. Havaitsemme, että Lauseen 15.8 perusteella mielivaltaisille polynomeille $p, p' \in K[X]$ pätee

$$\begin{aligned}(p + p')(a) &= s_a(p + p') \text{ (s_a on sijoitushomom.)}\\ &= s_a(p) + s_a(p')\\ &= p(a) + p'(a)\end{aligned}$$

ja

$$\begin{aligned}(pp')(a) &= s_a(pp')\\ &= s_a(p)\, s_a(p')\\ &= p(a)\, p'(a).\end{aligned}$$

Täten

$$\begin{aligned}0 &= f(a)\\ &= \big((X - a)g + r\big)(a)\\ &= \big(\big(X - a\big)\, g\big)(a) + r(a)\\ &= \big(X - a\big)(a)\, g(a) + r(a)\\ &= 0 \cdot g(a) + r(a)\\ &= r(a)\\ &= r \text{ (koska r on vakio).}\end{aligned}$$

Näin ollen $f = (X - a)g$. Todistettavana olevan implikaation ensimmäinen suunta on siis käsitelty.

Oletetaan sitten, että $f = (X - a)g$ jollain $g \in K[X]$. Täten

$$\begin{aligned}f(a) &= \big((X - a)g\big)(a)\\ &= \big(X - a\big)(a)\, g(a)\\ &= 0 \cdot g(a)\\ &= 0.\end{aligned}$$

□

Lause 16.3. *Oletetaan, että n-asteisella polynomilla $f \in K[X]$ on johtava kerroin c ja vähintään n eri juurta $a_1, ..., a_n$. Tällöin*

$$f = c(X - a_1) \cdot (X - a_2) \cdot \ ... \ \cdot (X - a_n).$$

Todistus. Todistetaan väite induktiolla luvun n suhteen. Kun $n = 0$, niin $f = c$.

Olkoon $n > 0$. Oletetaan, että f:llä on eri juuret $a_1, ..., a_n$. Lauseen 16.2 nojalla on olemassa sellainen $g \in K[X]$, että $f = (X - a_n)g$. Selvästi g:n johtava kerroin on c. Koska

$$deg(fg) = deg(f) + deg(g)$$

(Lause 15.7), niin $deg(g) = n - 1$. Oletuksemme perusteella jokaiselle $i \in \{1, ..., n\}$ pätee

$$0 = f(a_i) = (a_i - a_n)\ g(a_i).$$

Täten, koska

1. K on kuntana kokonaisalue ja näin ollen siinä ei ole nollantekijöitä, ja
2. alkiot $a_1, ..., a_n$ ovat eri alkioita, joten $a_i - a_n = 0 \ \Rightarrow \ i = n$,

niin jokainen alkioista $a_1, ..., a_{n-1}$ on g:n juuri. Induktio-oletuksen nojalla

$$g = c(X - a_1) \cdot (X - a_2) \cdot \ ... \ \cdot (X - a_{n-1}),$$

joten

$$f = c(X - a_1) \cdot (X - a_2) \cdot \ ... \ \cdot (X - a_{n-1}) \cdot (X - a_n).$$

□

Lause 16.4. *Jos $f \in K[X] \setminus \{0\}$ on n-asteinen polynomi, niin sillä on korkeintaan n juurta.*

Todistus. Tehdään vasta-oletus, että f:llä on eri juuret $a_1, ..., a_{n+1}$. Täten myös joukko $a_1, ...a_n$ on kokoelma f:n eri juuria. Lauseen 16.3 nojalla

$$f = c(X - a_1) \cdot \ ... \ \cdot \ (X - a_n),$$

missä $c \in K$, $c \neq 0$. Täten

$$f(a_{n+1}) = c(a_{n+1} - a_1) \cdot \ ... \ \cdot (a_{n+1} - a_n).$$

Koska mikään termeistä $(a_{n+1} - a_i)$ ei ole nolla kun $i \in \{1, ..., n\}$, ja koska kunnassa K ei ole nollantekijöitä, niin $f(a_{n+1}) \neq 0$. Täten a_{n+1} ei ole f:n juuri, mikä on ristiriita. □

Lause 16.5. *Olkoon K ääretön kunta ja $f \in K[X]$ polynomi. Tällöin, mikäli $f(a) = 0$ kaikilla $a \in K$, niin $f = 0$.*

Todistus. Oletetaan, että $f(a) = 0$ kaikilla $a \in K$. Tehdään vastaoletus, että $f \neq 0$. Lauseen 16.4 nojalla f:llä on enintään $deg(f)$ juurta. Se, että $deg(f)$ on äärellinen, mutta toisaalta f:llä on äärettömän monta juurta, on ristiriita. □

17 Ideaalit ja tekijärenkaat

Tässä luvussa selvitämme, millaisia ovat rengashomomorfismin $f : R \to R'$ ytimet

$$ker(f) = \{\ x \in R \mid f(x) = 0'\ \}.$$

Tämän kertoo Lause 17.4. (Katso myös Lause 13.2.)

Esimerkki. Tarkastellaan rengasta $\mathbb{R}$ ja sijoitushomomorfismia

$$\varphi : \mathbb{R}[X] \to \mathbb{R}$$

siten, että kaikille $f \in \mathbb{R}[X]$ pätee $\varphi(f) = f(2)$. Tällöin Lauseen 16.2 nojalla

$$\begin{aligned} ker(\varphi) &= \{\ f \in \mathbb{R}[X] \mid 2 \text{ on } f\text{:n juuri }\} \\ &= \{\ (X-2)g \mid g \in \mathbb{R}[X]\ \}. \ \square \end{aligned}$$

Olkoot R ja R' renkaita, $f : R \to R'$ rengashomomorfismi ja $a \in R$ renkaan R alkio. Havaitsemme, että

$$\big(a \in R \text{ ja } x \in ker(f)\big) \ \Rightarrow\ ax \in ker(f),$$

sillä

$$f(x) = 0' \ \Rightarrow\ f(ax) = f(a)f(x) = 0'.$$

Eli, jos mikä tahansa alkio kerrotaan jollain joukon $ker(f)$ alkiolla, kuuluu näin saatu tulo myös joukkoon $ker(f)$. Tämä joukon $ker(f)$ ominaisuus on tärkeä. Määrittelemme seuraavaksi tähän ominaisuuteen liittyvän käsitteen.

Määritelmä 17.1. Jos R on rengas, niin $I \subseteq R$ on sen *ideaali*, mikäli

1. I on ryhmän $(R, +)$ aliryhmä,
2. $\big(a \in R \text{ ja } x \in I\big) \ \Rightarrow\ ax \in I.$

Intuition tasolla ideaali I voidaan nähdä eräänlaisena nollan käsitteen yleistyksenä. Yleisesti pätee $a0 \in \{0\}$, ja toisaalta vastaavasti $ax \in I$ pätee kaikilla $x \in I$. Lisäksi $\{0\}$ on aina aliryhmä.

Lause 17.2. *Jos R on rengas ja $I \subseteq R$, niin I on ideaali jos ja vain jos*

1. $I \neq \emptyset$,
2. $\big(a_1, ..., a_n \in R \text{ ja } x_1, ..., x_n \in I\big) \Rightarrow a_1x_1 + ... + a_nx_n \in I$.

Todistus. Käsitellään luennolla. □

Jos R on rengas ja $x \in R$, niin x:n virittämä *pääideaali* on

$$\langle x \rangle := \{ ax \mid a \in R \}.$$

Tämä on ideaali Lauseen 17.2 nojalla, sillä tällöin

1. $x = 1 \cdot x \in \langle x \rangle$, joten $\langle x \rangle \neq \emptyset$,
2. jos $b_1, ..., b_n \in R$ ja $a_1x, ..., a_nx \in \langle x \rangle$, niin

$$b_1(a_1x) + ... + b_n(a_nx) = (b_1a_1 + ... + b_na_n)x \in \langle x \rangle.$$

Huomaa, että ideaali $\langle x \rangle$ ei tarkoita samaa kuin syklinen aliryhmä $\langle x \rangle$. Sen kumpaa oliota tarkoitetaan, tulee selvitä asiayhteydestä.

Esimerkki. Edellä määrittelimme kuvauksen $\varphi : \mathbb{R}[X] \to \mathbb{R}$, $f \mapsto f(2)$. Havaitsimme, että Lauseen 16.2 nojalla tälle kuvaukselle pätee

$$ker(f) = \{ (X-2)g \mid g \in \mathbb{R} \}.$$

Nyt havaitsemme, että $ker(f) = \langle X - 2 \rangle$.

Jos jokainen renkaan R ideaali on pääideaali, niin sanotaan, että R on *pääideaalirengas*.

Esimerkki. Lauseen 8.3 avulla on helppo nähdä, että struktuurin $(\mathbb{Z}, +)$ aliryhmät ovat täsmälleen tyyppiä $d\mathbb{Z}$ olevat joukot. Tässä $d \in \mathbb{N}$. Myös renkaan $(\mathbb{Z}, +, \cdot)$ ideaalit ovat täsmälleen joukot $d\mathbb{Z}$, (HT). Täten $\mathbb{Z}$ on pääideaalirengas.

Esimerkki. Jos R on rengas ja $x_1, ..., x_n \in R$, niin alkiot $x_1, ..., x_n$ *virittävät* ideaalin

$$\langle x_1, ..., x_n \rangle := \{ a_1x_1 + ... + a_nx_n \mid a_1, ..., a_n \in R \},$$

jolloin

1. $\langle x_1, ..., x_n \rangle$ on todella ideaali (HT),

2. jos $I \subseteq R$ on ideaali siten, että $x_1, ..., x_n \in I$, niin Lauseen 17.2 nojalla $\langle x_1, ..., x_n \rangle \subseteq I$.

Näin ollen $\langle x_1, ..., x_n \rangle$ on suppein ideaali, joka sisältää alkiot $x_1, ..., x_n$. Eli jos J on jokin ideaali siten, että $x_1, ..., x_n \in J$, niin tällöin $\langle x_1, ..., x_n \rangle \subseteq J$.

Esimerkki. Osoitetaan, että jos $a, b \in \mathbb{Z}$, niin

$$\langle a, b \rangle = \langle syt(a, b) \rangle.$$

Esimerkki käsitellään luennolla.

Esimerkki. Renkaan R *triviaalit ideaalit* ovat $\{0\}$ ja $R = \langle 1 \rangle$.

Esimerkki. Olkoon R rengas. Tällöin

$$\begin{aligned} \langle X, X^2 + 1 \rangle &= \{\ fX + g(X^2 + 1) \mid f, g \in R[X]\ \} \\ &= \{\ X(f + gX) + g \mid f, g \in R[X]\ \} \\ &= \{\ hX + g \mid h, g \in R[X]\ \} \\ &= R[X]. \end{aligned}$$

Olkoon R rengas ja $I \subseteq R$ ideaali. Ideaali I on Abelin ryhmän $(R, +)$ aliryhmä, joten se on normaali aliryhmä. Voidaan siis määritellä tekijäryhmä

$$R/I = \{\ x + I \mid x \in R\ \}.$$

Huomaa, että Lauseen 10.3 nojalla

$$x + I = y + I \ \Leftrightarrow\ x - y \in I.$$

Tekijäryhmässä R/I on voimassa tekijäryhmän määritelmän mukainen yhteenlasku

$$(x + I) + (y + I) = (x + y) + I.$$

Määritellään kertolasku joukossa R/I siten, että

$$(x + I)(y + I) = xy + I.$$

Kertolasku on hyvinmääritelty, sillä

$$\begin{cases} x+I = x'+I \\ y+I = y'+I \end{cases} \Rightarrow \begin{cases} x-x' \in I \\ y-y' \in I \end{cases} \quad \text{(Lause 10.3)}$$

$$\Rightarrow \begin{cases} (x-x')y \in I \\ x'(y-y') \in I \end{cases} \quad (I \text{ on ideaali})$$

$$\Rightarrow \quad xy - x'y' = (x-x')y + x'(y-y') \ \in \ I \ (I \text{ on aliryhmä})$$

$$\Rightarrow \quad x'y' + I \ = \ xy + I \text{ (Lause 10.3).}$$

Lause 17.3. *Olkoon R rengas ja $I \subseteq R$ ideaali, $I \neq R$. Tällöin R/I on rengas.*[3]

Todistus. Käsitellään luennolla. □

Olkoon R rengas ja $I \subseteq R$ ideaali, $I \neq R$. Tarkastellaan kanonista surjektiota

$$\pi : R \to R/I, \ x \mapsto x + I.$$

Tiedämme, että π on ryhmähomomorfismi. Kuvaus π on myös rengashomomorfismi, sillä

1. $\pi(1) = 1 + I$,
2. jos $x, y \in R$, niin

$$\pi(xy) = xy + I = (x+I)(y+I) = \pi(x)\pi(y).$$

Seuraava lause karakterisoi ideaalin käsitteen.

Lause 17.4. *Olkoon R rengas ja $I \subseteq R$ joukko, $I \neq R$. Tällöin I on ideaali jos ja vain jos on olemassa sellainen rengashomomorfismi $\varphi : R \to R'$ jollekin renkaalle R', että $ker(\varphi) = I$.*

Todistus. Käsitellään luennolla. □

[3] Mikäli $I = R$, niin R/I on yhden alkion rengas (eli $0 = 1$), sillä R/R sisältää täsmälleen yhden sivuluokan. Muistamme luvusta 12, että $0 = 1$ renkaassa R joss $R = \{0\}$.

Lause 17.5 (Renkaiden isomorfialause)**.** *Olkoon $f : R \to R'$ rengashomomorfismi. Kuvaus*

$$\overline{f} : R/ker(f) \to im(f), \ \ missä \ \ x + ker(f) \mapsto f(x),$$

on rengasisomorfismi.

Todistus. Käsitellään luennolla. □

Polynomien jaollisuus

Jatkossa K tarkoittaa aina kuntaa. Lukuja 15, 16 ja 17 koskevan oletuksemme nojalla renkaat ovat kommutatiivisia renkaita joissa $0 \neq 1$. Kunnat ovat renkaita, joten $0 \neq 1$ pätee kunnissa.

Määritelmä 17.6. Olkoon $f, g \in K[X]$ polynomeja. Jos on olemassa sellainen $h \in K[X]$, että $f = gh$, niin sanomme, että g jakaa f:n. Merkintä $g \,|\, f$ tarkoittaa, että g jakaa f:n.

Esimerkki. Renkaassa $\mathbb{Z}_2[X]$ pätee

$$X + 1 \,|\, X^2 + 1,$$

sillä

$$X^2 + 1 = X^2 + 2X + 1 = (X + 1)(X + 1).$$

Tässä käytimme jäännösluokille $\overline{n}$ merkintää n, eli jätimme ylleviivausmerkin kirjoittamatta. Jatkossa voimme käyttää tälläista merkintäkonventiota, kunhan asiayhteydestä on selvää, missä struktuurissa yhteenlasku ja kertolasku tapahtuvat.

Esimerkki. Olkoon K jokin kunta. Tarkastellaan tilannetta, jossa $f \,|\, g$ ja $g \,|\, f$, missä $f, g \in K[X]$.

$$\begin{aligned}
\big(f \,|\, g \text{ ja } g \,|\, f\big) \ &\Rightarrow \big(g = fg' \text{ jollain } g' \in K[X] \\
&\quad \text{ja } f = gf' \text{ jollain } f' \in K[X]\big) \\
&\Rightarrow f = fg'f' \text{ joillain } f', g' \in K[X] \\
&\Rightarrow 1 = g'f' \text{ jollain } g' \in K[X] \text{ (supistussääntö, Lause 14.2)} \\
&\Rightarrow 0 = deg(1) = deg(g'f') = deg(g') + deg(f') \text{ (Lause 15.7)} \\
&\Rightarrow deg(g') = deg(f') = 0 \\
&\Rightarrow f', g' \text{ ovat vakiopolynomeja.}
\end{aligned}$$

Havaitsemme, että $f', g' \in K[X]^*$, eli f' ja g' kuuluvat renkaan $K[X]$ yksiköiden joukkoon, ks. määritelmä 12.3.

Lause 17.7. *Olkoon K kunta. Rengas $K[X]$ on pääideaalirengas.*

Todistus. Käsitellään luennolla. □

Määritelmä 17.8. Olkoot $f, g \in K[X]$ polynomeja. Polynomi $p \in K[X]$ on f:n ja g:n *suurin yhteinen tekijä*, jos

1. $p \mid f$ ja $p \mid g$,
2. $(q \mid f$ ja $q \mid g) \;\Rightarrow\; q \mid p$.

Merkitsemme $p = syt(f, g)$, kun p on f:n ja g:n suurin yhteinen tekijä.

Huomaa, että kun $a \in K[X]^*$ on yksikkö, niin

$$p = syt(f, g) \;\Rightarrow\; ap = syt(f, g),$$

joten polynomien tapauksessa $syt(f, g)$ ei ole välttämättä yksikäsitteinen.

Lause 17.9. *Olkoon K kunta. Olkoot $f, g \in K[X]$ polynomeja. Tällöin on olemassa jokin $syt(f, g)$. Lisäksi on olemassa sellaiset polynomit $A, B \in K[X]$, että*

$$syt(f, g) = Af + Bg.$$

Todistus. Käsitellään luennolla. □

Esimerkki. Eukleideen algoritmi toimii myös struktuurissa $K[X]$. Soveltamalla jakoyhtälöä, saamme esitykset

$$\begin{aligned}
f &= q_0 g + r_1 \quad \big(deg(r_1) < deg(g)\big),\\
g &= q_1 r_1 + r_2 \quad \big(deg(r_2) < deg(r_1)\big),\\
r_1 &= q_2 r_2 + r_3 \quad \big(deg(r_3) < deg(r_2)\big),\\
r_2 &= q_3 r_3 + r_4 \quad \big(deg(r_4) < deg(r_3)\big),\\
&\;\;\vdots\\
r_{n-2} &= q_{n-1} r_{n-1} + r_n,\\
r_{n-1} &= q_n r_n.
\end{aligned}$$

Algoritmi päättyy, sillä

$$deg(r_1) > deg(r_2) > \;\ldots\;.$$

Tällöin r_n on $syt(f, g)$. Tämä todistetaan samoin, kuin vastaava kokonaislukuja koskeva väite.

Etsitään $syt(7X^3 + 2X, 3X^2 + X)$ struktuurissa $\mathbb{Z}_{11}[X]$. Esimerkki käsitellään loppuun luennolla.

Jaottomat Polynomit

Olkoon K kunta. Luvusta 14 muistamme, että triviaalisti $K^* = K \setminus \{0\}$. Entä millainen on joukko $K[X]^*$? Selvästi $K^* \subseteq K[X]$, eli vakiopolynomit $a \in K^*$ ovat joukossa $K[X]^*$. Toisaalta, selvästi nollapolynomi ei ole joukossa $K[X]^*$. Olkoon $f \in K[X]$ jokin polynomi siten, että $deg(f) \geq 1$. Tehdään oletus, että $f \in K[X]^*$. Täten $fg = 1$ jollain $g \in K[X]$. Tällöin Lauseen 15.7 nojalla

$$deg(f) + deg(g) = deg(fg) = deg(1) = 0.$$

Tämä on mahdotonta, sillä $deg(f) \geq 1$. Näin ollen $K[X]^* = K^* = K \setminus \{0\}$.

Määritelmä 17.10. Olkoon K kunta. Polynomi $f \in K[X]$ on jaoton, mikäli

1. $deg(f) \geq 1$,
2. jos $f = gh$ joillakin $g, h \in K[X]$, niin tällöin $g \in K^*$ tai $h \in K^*$.

Esimerkki. Osoitetaan, että polynomi $f = X^2 + 1 \in \mathbb{R}[X]$ on jaoton. Tehdään vastaoletus, että $X^2 + 1 = gh$, missä $g, h \notin K^*$. Selvästi $g \neq 0 \neq h$. Koska $X^2 + 1 = gh$, niin

$$deg(X^2 + 1) = deg(gh).$$

Lauseen 15.7 nojalla täten

$$2 = deg(g) + deg(h).$$

Nyt jos $deg(g) = 0$, niin $g \in K^*$, joten $deg(g) \neq 0$. Samoin $deg(h) \neq 0$. Täten

$$deg(g) = deg(h) = 1.$$

Täten $g = aX + b$, missä $a, b \in \mathbb{R}$. Tässä $a \neq 0$. Nyt

$$aX + b = a(X + \frac{b}{a}),$$

joten $g(-\frac{b}{a}) = 0$. Koska $f = gh$, niin $f(-\frac{b}{a}) = 0$. Tämä on ristiriita, sillä polynomilla $f = X^2 + 1$ ei ole reaalijuuria $\mathbb{R}$:ssä. $\square$

Olkoon K kunta ja $f \in K[X]$ polynomi. Viritetyn ideaalin $\langle f \rangle$ määritelmän mukaan

$$\langle f \rangle \;=\; \{\; hf \mid h \in K[X] \;\}.$$

Otetaan joukon $K[X]/\langle f \rangle$ sivuluokille käyttöön merkintä

$$\overline{g} \;:=\; g + \langle f \rangle$$

kaikille $g \in K[X]$. Täten sivuluokan $g + \langle f \rangle$ määritelmän nojalla

$$\overline{g} = g + \langle f \rangle = \{\; g + p \mid p \in \langle f \rangle \;\} = \{\; g + p \mid p = hf \text{ jollain } h \in K[X] \;\},$$

joten

$$\overline{g} \;=\; \{\; g + hf \mid h \in K[X] \;\}.$$

Havaitsemme, että

$$\overline{0} \;=\; \{0 + hf \mid h \in K[X] \;\} \;=\; \{\; hf \mid h \in K[X] \;\} = \langle f \rangle.$$

Toisaalta

$$\overline{f} = \{\; f + hf \mid h \in K[X] \;\},$$

joten $f \in \overline{f}$ (koska $0 \in K[X]$). Täten $f \in \overline{f}$ ja $f \in \langle f \rangle = \overline{0}$, joten $\overline{f} = \overline{0} = \langle f \rangle$.

Millainen olio $K[X]/\langle f \rangle$ on?

Lause 17.11. *Olkoon K kunta ja $f \in K[X] \setminus K$ polynomi. Seuraavat ehdot ovat yhtäpitäviä:*

1. *$K[X]/\langle f \rangle$ on kokonaisalue,*
2. *f on jaoton,*
3. *$K[X]/\langle f \rangle$ on kunta.*

Todistus. Käsitellään luennolla. □

Olkoon K kunta ja f jaoton polynomi. Osoitamme seuraavaksi, että kuvaus

$$\varphi : K \to K[X]/\langle f \rangle, \quad a \mapsto \overline{a},$$

on upotus, eli injektiivinen homomorfismi. Kuvaus φ siis kuvaa kunnan K alkion a vakiopolynomin $p_a = a$ määräämäksi sivuluokaksi

$$\overline{a} = a + \langle f \rangle.$$

Osoitetaan aluksi, että homomorfisuusehdot pätevät.

$$\begin{aligned}\varphi(a+b) &= \overline{a+b} \\ &= (a+b)+\langle f\rangle \\ &= (a+\langle f\rangle)+(b+\langle f\rangle) \\ &= \overline{a}+\overline{b} \\ &= \varphi(a)+\varphi(b)\end{aligned}$$

$$\begin{aligned}\varphi(ab) &= \overline{p_{ab}} \\ &= \overline{p_a \cdot p_b} \quad (p_a \text{ ja } p_b \text{ ovat vakiopolynomeja}) \\ &= (p_a \cdot p_b)+\langle f\rangle \\ &= (p_a+\langle f\rangle)(p_b+\langle f\rangle) \\ &= \overline{p_a}\cdot\overline{p_b} \\ &= \varphi(a)\varphi(b)\end{aligned}$$

Lisäksi, kuvauksen φ määritelmän nojalla

$$\varphi(1) = \overline{1}.$$

Osoitetaan vielä, että φ on injektiivinen. Oletetaan, että $a \in ker(\varphi)$. Täten

$$\varphi(a) = \overline{a} = \overline{0},$$

eli $a+\langle f\rangle = 0+\langle f\rangle$. Täten $a = a-0 \in \langle f\rangle$ (Lause 10.3), joten $a = hf$ jollekin $h \in K[X]$. Jos $hf = a \neq 0$, niin $h \neq 0$, ja saamme Lauseen 15.7 nojalla ristiriidan

$$0 = deg(a) = deg(hf) = deg(h)+deg(f) \geq 1,$$

sillä f on jaoton ja siksi $deg(f) \geq 1$. Täten $a = 0$. Olemme siis osoittaneet, että $ker(\varphi) = \{0\}$, joten φ on injektiivinen.

Koska φ on injektiivinen homomorfismi eli upotus, niin struktuuri $K[X]/\langle f\rangle$ sisältää isomorfisen kopion struktuurista K. Epäformaalisti, K " $\subseteq$ " $K[X]/\langle f\rangle$.