Algebra I

Kevät 2004

Pentti Haukkanen

Sisällys

1 Lukuteoriaa

Lukuteoria on karkeasti sanottuna matematiikan osa-alue, joka käsittelee kokonaislukujen ominaisuuksia. Tässä monisteessa paneudutaan varsinkin jaollisuuden problematiikkaan.

Kokonaislukujen joukkoa merkitsemme symbolilla $\mathbf{Z}$. Kaikki tämän pykälän luvut ovat kokonaislukuja ellei toisin mainita.

1.1 Jaollisuus

Määritelmä Luku a on luvun b *tekijä* (eli luku b on *jaollinen* luvulla a eli luku a jakaa luvun b), jos on olemassa sellainen $c \in \mathbf{Z}$, että $b = ac$.

Merkintä Jos luku a on luvun b tekijä, niin merkitään $a \mid b$. Muussa tapauksessa $a \nmid b$.

Esimerkki 1.1.1 On helppo todeta, että $3 \mid 6$ ja $3 \nmid 7$. Mitkä ovat lukujen 6 ja 7 kaikki tekijät?

Esimerkki 1.1.2 Todista, että $n \mid \sum_{i=1}^{n} i$ aina, kun n on pariton kokonaisluku.

Esimerkki 1.1.3 Todista, että $a \mid 0$ ja $1 \mid a$ aina, kun $a \in \mathbf{Z}$.

Lause 1.1.1 *Oletetaan, että a, b, $c \in \mathbf{Z}$. Silloin*

1) $a \mid b,\ a \mid c \Rightarrow a \mid b + c$,

2) $a \mid b,\ a \mid c \Rightarrow a \mid b - c$,

3) $a \mid b,\ c \mid d \Rightarrow ac \mid bd$,

4) $a \mid b \Rightarrow a \mid bd$.

Todistus 1) Oletetaan, että $a \mid b$ ja $a \mid c$. Silloin on olemassa sellaiset e ja f, että $b = ae$ ja $c = af$. Näin ollen $b + c = ae + af = a(e + f)$. Siis $a \mid b + c$.
2-4) Harjoitustehtävä. □

Lause 1.1.2 *Oletetaan, että a, b, $c \in \mathbf{Z}^+$. Silloin*

1) $a \mid a$,

2) $a \mid b,\ b \mid a \Rightarrow a = b$,

3) $a \mid b,\ b \mid c \Rightarrow a \mid c$.

Todistus Harjoitustehtävä.

Huomautus Lauseen 1.1.2 mukaan jaollisuusrelaatio $\mid$ on osittainen järjestysrelaatio joukossa $\mathbf{Z}^+$.

Huomautus Lauseen 1.1.2 kaavaa 2 voi käyttää lukuteoreettisten yhtälöiden todistamiseen. (Vrt. joukko-opissa $A = B \Leftrightarrow A \subseteq B, B \subseteq A$ ja logiikassa $(p \Leftrightarrow q) \Leftrightarrow (p \Rightarrow q, q \Rightarrow p)$.

Esimerkki 1.1.4 Todista, että

1) $a \mid b,\ a \mid c \Rightarrow a \mid xb + yc$ aina, kun $x,\ y \in \mathbf{Z}$,

2) $a \mid b,\ c \mid d \not\Rightarrow a + c \mid b + d$,

3) $a \mid b,\ a \nmid c \Rightarrow a \nmid b + c$,

4) $a \mid (-a)$.

1.2 Suurin yhteinen tekijä

Määritelmä Olkoot a ja b kokonaislukuja, joista ainakin toinen on $\neq 0$. Silloin c on lukujen a ja b *suurin yhteinen tekijä* (syt), jos

1) $c \mid a,\ c \mid b$ ja

2) $d \mid a,\ d \mid b \Rightarrow d \leq c$.

Merkintä Lukujen a ja b suurinta yhteistä tekijää merkitään symbolilla (a, b), $\text{syt}(a, b)$ tai $\gcd(a, b)$. Huom. $(a, b) = (b, a)$.

Huomautus Lukujen suurin yhteinen tekijä (syt) on aina olemassa ja on yksikäsitteinen.

Huomautus 1) Syt:n määritelmän mukaan $(a, b)|a$ ja $(a, b)|b$.
2) Kohdan 1 ja lauseen 1.1.2 kohdan 3 perusteella $c|(a, b) \Rightarrow c|a, c|b$. (Lauseen 1.3.5 seurauksen 1 mukaan edellinen kaava on voimassa käänteisestikin.)

Esimerkki 1.2.1 On helppo todeta, että $(6, 9) = 3$. Mikä on $(6, 16)$?

Esimerkki 1.2.2 On helppo todeta, että $(0, a) = |a|$ $(a \neq 0)$ ja $(1, a) = 1$ aina, kun $a \in \mathbf{Z}$.

Esimerkki 1.2.3 Todista, että $(a, a+1) = 1$ aina, kun $a \in \mathbf{Z}$.

Huomautus Pykälissä 1.3 ja 1.7 esittelemme menetelmiä, joilla syt voidaan määrittää mekaanisesti.

Määritelmä Luvut a ja b ovat *suhteellisia alkulukuja*, jos $(a, b) = 1$. Käytetään myös sanontaa *keskenään jaottomia*.

Lause 1.2.1 Oletetaan, että $a, b > 0$. Jos $(a, b) = c$, niin a/c ja b/c ovat keskenään jaottomia.

Todistus Harjoitustehtävä.

1.3 Jakoalgoritmi

Lause 1.3.1 (Jakoalgoritmi) *Jokaista lukua a ja b ($\neq 0$) kohti on olemassa sellaiset yksikäsitteiset luvut q ja r, että*

$$a = bq + r, \ \textit{missä}\ 0 \leq r < |b|.$$

Huomautus Lukua a sanotaan *jaettavaksi*, lukua b *jakajaksi*, lukua q *osamääräksi* ja lukua r *jakojäännökseksi*. Usein merkitään $r = a \bmod b$ (vrt. § 1.9).

Lauseen 1.3.1 todistus Olkoot a ja b sellaisia kokonaislukuja, että $b > 0$. (Tapaus $b < 0$ käsitellään vastaavasti.) Todistetaan ensiksi, että lauseen 1.3.1 mukaiset luvut q ja r ovat olemassa. Merkitään

$$q = \left[\frac{a}{b}\right],$$

missä $[a/b]$ on suurin kokonaisluku, joka on $\leq a/b$, ja merkitään

$$r = a - bq.$$

Koska

$$\frac{a}{b} - 1 < \left[\frac{a}{b}\right] = q \leq \frac{a}{b},$$

niin

$$a - b < bq \leq a.$$

Täten

$$0 \leq a - bq = r < b.$$

Näin olemme todistaneet, että lauseen 1.3.1 luvut q ja r ovat olemassa.

Todistamme toiseksi, että luvut q ja r ovat yksikäsitteiset. Oletamme, että

$$a = bq' + r', \quad 0 \leq r' < b.$$

Silloin

$$0 = b(q - q') + (r - r').$$

Näin ollen $b \mid (r - r')$. Koska $0 \leq r < b$ ja $0 \leq r' < b$, niin $-b < r - r' < b$ eli $|r - r'| < b$. Siis $r = r'$. Koska $b \neq 0$, niin $q = q'$. Näin olemme todistaneet lukujen q ja r yksikäsitteisyyden. Siis lause 1.3.1 on voimassa. □

Esimerkki 1.3.1 Selvästi $7 = 2 \cdot 3 + 1$. Kirjoita jakoalgoritmi, kun $a = -7$ ja $b = 3$.

Lause 1.3.2 *Olkoon $b \geq 2$. Jokainen luku $a \in \mathbf{Z}^+$ voidaan esittää yksikäsitteisesti muodossa*

$$a = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_1 b + a_0,$$

missä $0 \leq a_i < b$, $i = 0, 1, \ldots, m$.

Todistus Harjoitustehtävä. Vihje. Sovelletaan jakoalgoritmia.

Huomautus Lauseen 1.3.2 esitystä merkitään myös niin, että $a = (a_m a_{m-1} \ldots a_1 a_0)_b$. Jos $b = 10$, niin kyseessä on kymmenjärjestelmän esitys.

Esimerkki 1.3.2 Kymmenjärjestelmässä esitetty luku $(93)_{10}$ on 8-järjestelmässä esitettynä $(135)_8$. Nimittäin

$$93 = 8 \cdot 11 + 5 = 8(8 \cdot 1 + 3) + 5 = 1 \cdot 8^2 + 3 \cdot 8 + 5.$$

Lause 1.3.3 *Jos $a = bq + r$, niin $(a, b) = (b, r)$.*

Todistus Merkitään $(a, b) = c$. Todistetaan, että $(b, r) = c$ eli että $(b, a - bq) = c$.

Osa 1. Todistetaan, että c on lukujen b ja $a - bq$ *yhteinen* tekijä. Koska $c \mid a$, $c \mid b$, niin $c \mid (-bq)$. Näin ollen lauseen 1.1.1 nojalla, $c \mid (a - bq)$. Siis $c \mid b$ ja $c \mid (a - bq)$. Näin osa 1 on todistettu.

Osa 2. Todistetaan, että c on lukujen b ja $a - bq$ *suurin* yhteinen tekijä. Oletetaan, että $d \mid b$ ja $d \mid (a - bq)$. Voidaan todeta, että $d \mid a$ ja $d \mid b$. Näin ollen syt:n määritelmän nojalla $d \leq c$. Siis osa 2 on todistettu. □

Huomautus Lauseesta 1.3.3 seuraa, että jaettavan ja jakajan syt on yhtäsuuri kuin jakajan ja jakojäännöksen syt.

Lause 1.3.4 (Eukleideen algoritmi) *Olkoot a ja b sellaisia positiivisia kokonaislukuja, että $b \nmid a$. Silloin voidaan kirjoittaa*

$$\begin{aligned}
a &= bq_1 + r_1, \quad 0 < r_1 < b, \\
b &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1, \\
r_1 &= r_2 q_3 + r_3, \quad 0 < r_3 < r_2, \\
&\vdots \\
r_{k-2} &= r_{k-1} q_k + r_k, \quad 0 < r_k < r_{k-1}, \\
r_{k-1} &= r_k q_{k+1},
\end{aligned}$$

ts. prosessi päättyy niin, että jokin jakojäännös r_{k+1} ($k \geq 1$) on $= 0$. Viimeinen nollasta poikkeava jakojäännös r_k on $= (a, b)$. (Jos $b \mid a$, niin $r_1 = 0$ ja $(a, b) = b$.)

Todistus 1) Koska jakojäännöksien jono $r_1, r_2, r_3, \ldots$ on aidosti vähenevä jono ei-negatiivisia kokonaislukuja, niin on olemassa sellainen k, että $r_{k+1} = 0$.
2) Lauseen 1.3.3 nojalla

$$(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_k, 0) = r_k.$$

Näin olemme todistaneet lauseen 1.3.4. □

Esimerkki 1.3.3 Sovella Eukleideen algoritmia lukuihin 86 ja 8. Totea, että $(86, 8) = 2$.

Lause 1.3.5 *Olkoot a ja b kokonaislukuja. Silloin*

$$\exists x, y \in \mathbf{Z}\colon (a, b) = ax + by.$$

Todistus Eukleideen algoritmissa kaikki jakojäännökset ovat muotoa $ax + by$. Siis myös r_k eli (a, b) on tätä muotoa. Lisäksi jos $b|a$, niin $(a, b) = a \cdot 0 + b \cdot 1$. □

Esimerkki 1.3.4 Luku $(64, 6)$ voidaan kirjoittaa muodossa $(64, 6) = 64 \cdot (-1) + 6 \cdot 11$.

Seuraus 1 Jos $c \mid a$ ja $c \mid b$, niin $c \mid (a, b)$.

Todistus Lauseen 1.3.5 mukaan

$$(a, b) = ax + by.$$

Koska $c \mid a$ ja $c \mid b$, niin $c \mid (ax + by)$ eli $c \mid (a, b)$. □

Seuraus 2 Jos $a \mid bc$ ja $(a, b) = 1$, niin $a \mid c$.

Todistus Lauseen 1.3.5 mukaan

$$1 = ax + by.$$

Siis

$$c = axc + byc.$$

Koska $a \mid axc$ ja $a \mid byc$, niin $a \mid (axc + ayc)$ eli $a \mid c$. □

Seuraus 3 Jos $a \mid c$, $b \mid c$ ja $(a, b) = 1$, niin $ab \mid c$.

Todistus Olettamusten ja lauseen 1.3.5 nojalla $c = ad$, $c = be$ ja $1 = ax + by$, joten

$$c = axc + byc = axbe + byad = ab(xe + yd).$$

Näin ollen $ab \mid c$. □

1.4 Lineaarinen Diofantoksen yhtälö

Määritelmä *Diofantoksen yhtälö* on yhden tai usean muuttujan yhtälö, jolle etsitään kokonaislukuratkaisuja. Kahden muuttujan *lineaarinen Diofantoksen yhtälö* on muotoa

$$ax + by = c, \tag{1}$$

missä a, b, $c \in \mathbf{Z}$.

Lause 1.4.1 *Diofantoksen yhtälö $ax + by = c$ on ratkeava, jos ja vain jos $(a, b) \mid c$.*

Todistus Merkitään $(a, b) = d$. Oletetaan, että $ax + by = c$ on ratkeava. Koska $d \mid a$ ja $d \mid b$, niin $d \mid ax + by$ eli $d \mid c$. Siis $(a, b) \mid c$.
Oletetaan käänteisesti, että $(a, b) \mid c$ eli $d \mid c$. Lauseen 1.3.5 mukaan on olemassa sellaiset kokonaisluvut u ja v, että

$$d = au + bv.$$

Toisaalta on olemassa sellainen e, että

$$de = c.$$

Näin ollen

$$a(ue) + b(ve) = c,$$

joten yhtälö $ax + by = c$ on ratkeava. □

Huomautus Yllä lause 1.4.1 antaa menetelmän, jolla voidaan tarkistaa, onko yhtälö $ax + by = c$ ratkeava.

Huomautus Alla lause 1.4.2 antaa menetelmän, jolla ratkaisut saadaan.

Lause 1.4.2 *Olkoot a, b ja c kokonaislukuja. Merkitään $(a, b) = d$. Jos yhtälö $ax + by = c$ on ratkeava (ts. jos $d \mid c$), niin yhtälön kaikki ratkaisut ovat*

$$\begin{cases} x &= x_0 + bt/d, \\ y &= y_0 - at/d, \end{cases} \quad t \in \mathbf{Z}, \tag{2}$$

missä x_0, y_0 on yksi ratkaisu.

Huomautus Vielä puuttuu menetelmä yksittäisen ratkaisun etsimiseksi. Yksittäinen ratkaisu saadaan esimerkiksi keksimällä tai Eukleideen algoritmilla.

Huomautus Kaava (2) on luonteeltaan suoran parametriesityksen kaltainen.

Lauseen 1.4.2 todistus 1) Kyseessä olevat parit ovat ratkaisuja, sillä

$$a(x_0 + bt/d) + b(y_0 - at/d) = ax_0 + by_0 = c.$$

2) Todistetaan, että näin saadaan kaikki ratkaisut. Olkoon x, y mielivaltainen ratkaisu. Silloin

$$ax + by = c = ax_0 + by_0,$$

joten

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

Kun jaetaan puolittain luvulla d, saadaan

$$\frac{a}{d}(x - x_0) + \frac{b}{d}(y - y_0) = 0$$

eli

$$\frac{a}{d}(x - x_0) = -\frac{b}{d}(y - y_0). \tag{3}$$

Näin ollen

$$\frac{b}{d} \mid \frac{a}{d}(x - x_0).$$

Lauseen 1.2.1 ja lauseen 1.3.5 seurauksen 2 nojalla

$$\frac{b}{d} \mid x - x_0.$$

Siis

$$x - x_0 = \frac{b}{d}t$$

eli

$$x = x_0 + \frac{b}{d}t.$$

Nyt yhtälön (3) nojalla

$$\frac{a}{d}\frac{b}{d}t = \frac{b}{d}(y - y_0),$$

joten

$$y = y_0 - at/d.$$

Siis kaava (2) on voimassa. □

Diofantoksen yhtälön $ax + by = c$ ratkaisualgoritmi

1. Tutkitaan, onko $(a, b) \mid c$ ts. onko yhtälö ratkeava (ks. lause 1.4.1).
2. Etsitään jokin yksittäinen ratkaisu x_0, y_0

2.1. keksimällä (tai tietokoneella) tai

2.2. Eukleideen algoritmin avulla $[(a,b) = au + bv \quad | \cdot \frac{c}{(a,b)} \in \mathbf{Z}]$.

3. Yleinen ratkaisu on

$$\begin{cases} x &= x_0 + bt/(a,b), \\ y &= y_0 - at/(a,b), \end{cases} \quad t \in \mathbf{Z},$$

(ks. lause 1.4.2).

Esimerkki 1.4.1 Ratkaistaan yhtälö $19x + 94y = 1994$ yllä olevalla algoritmilla.

1. Koska $(19, 94) \mid 1994$, niin yhtälö on ratkeava.

2.1. Yksittäinen ratkaisu $x_0 = 100$, $y_0 = 1$ löydetään keksimällä.

3. Yleinen ratkaisu on

$$\begin{cases} x &= 100 + 94t, \\ y &= 1 - 19t, \end{cases} \quad t \in \mathbf{Z}.$$

Esimerkki 1.4.2 Ratkaistaan yhtälö $15x + 6y = 199$.

1. Koska $(15, 6) \not| \, 199$, niin yhtälö ei ole ratkeava.

Esimerkki 1.4.3 Ratkaistaan yhtälö $52x + 62y = 6$.

1. Tutkitaan, onko relaatio $(52, 62) \mid 6$ voimassa. Eukleideen algoritmilla saadaan

$$\begin{aligned} 62 &= 52 \cdot 1 + 10, \\ 52 &= 10 \cdot 5 + 2, \\ 10 &= 2 \cdot 5. \end{aligned}$$

Siis $\text{syt}(52, 62) = 2$. Koska $2 \mid 6$, niin yhtälö on ratkeava.

2.2. Etsitään yksittäinen ratkaisu Eukleideen algoritmilla. Kohdan 1 nojalla saadaan

$$\begin{aligned} 2 &= 52 - 10 \cdot 5 = 52 - (62 - 52) \cdot 5 \\ &= 52 \cdot 6 + 62 \cdot (-5). \end{aligned}$$

Kun kerrotaan puolittain luvulla 3 (eli luvulla $c/(a,b)$), saadaan

$$6 = 52 \cdot 18 + 62 \cdot (-15).$$

Siis yksittäinen ratkaisu on $x_0 = 18$, $y_0 = -15$.

3. Kaikki ratkaisut ovat

$$\begin{cases} x &= x_0 + bt/(a,b) = 18 + 31t, \\ y &= y_0 - at/(a,b) = -15 - 26t, \end{cases} \quad t \in \mathbf{Z}.$$

Esimerkki 1.4.4 Olkoot käytössä kahden kupin vaaka ja punnukset, jotka painavat a ja b kiloa, missä a, $b \in \mathbf{Z}^+$. Punnitaan esine, jonka paino w kiloa on tuntematon. Punnitus on mahdollista silloin ja vain silloin, kun

$$\exists x, y \in \mathbf{Z}\colon w = ax + by$$

eli silloin ja vain silloin, kun

$$(a, b) \mid w.$$

Kaikki painot w ($\in \mathbf{Z}^+$) on mahdollista punnita silloin ja vain silloin, kun $(a, b) = 1$.

1.5 Alkuluvuista

Määritelmä Luku p (> 1) on *alkuluku*, jos sen ainoat positiiviset tekijät ovat 1 ja p.

Merkintä Alkulukujen joukkoa merkitään symbolilla $\mathbf{P}$.

Määritelmä Luku a (> 1) on *yhdistetty* luku, jos se ei ole alkuluku (ts. $a = bc$, missä $1 < b$, $c < a$).

Esimerkki 1.5.1 Luvut 2, 3 ja 5 ovat alkulukuja. Luvut 4 ja 6 ovat yhdistettyjä lukuja. Lukua 20 pienemmät alkuluvut ovat 2, 3, 5, 7, 11, 13, 17 ja 19. Mikä on seuraava alkuluku?

Esimerkki 1.5.2 Luku 2 on ainoa parillinen alkuluku.

Esimerkki 1.5.3 Todista, että $a^4 + 4$ on yhdistetty luku aina, kun $a > 1$.

Ratkaisu Kirjoitetaan $a^4 + 4$ muodossa

$$\begin{aligned} a^4 + 4 &= a^4 + 4a^2 + 4 - 4a^2 \\ &= (a^2 + 2)^2 - (2a)^2 \\ &= (a^2 + 2 - 2a)(a^2 + 2 + 2a). \end{aligned}$$

Koska $a > 1$, niin $a^2 + 2 - 2a > 1$ ja $a^2 + 2 + 2a > 1$. Siis $a^4 + 4$ on yhdistetty luku.

Esimerkki 1.5.4 Milloin $a^3 - 1$ on yhdistetty luku?

Esimerkki 1.5.5 Todista, että $(a, a + p)$ voi saada vain arvot 1 ja p, kun $p \in \mathbf{P}$.

Lause 1.5.1 *Jokainen luku a (> 1) on alkulukujen tulo (jossa voi olla yksi tai useampia tekijöitä).*

Todistus Sovelletaan induktiota luvun a suhteen. Jos $a = 2$, niin a on alkuluku ja väite on oikein. Oletetaan, että väite on oikein, kun $a < k$ ($k > 2$). Silloin jos k on alkuluku, niin väite on oikein. Jos taas k on yhdistetty luku, niin $k = bc$, missä $1 < b, c < k$. Näin ollen induktio-olettamuksen nojalla b ja c ovat alkulukujen tuloja, joten bc eli k on alkulukujen tulo. □

Lause 1.5.2 (Eukleides) *Alkulukuja on ääretön määrä.*

Todistus Tehdään vastaoletus, jonka mukaan alkulukuja on äärellinen määrä. Olkoot ne $p_1, p_2, \ldots, p_n$. Merkitään $N = 1 + p_1 p_2 \cdots p_n$. Lauseen 1.5.1 mukaan on olemassa sellainen $i = 1, 2, \ldots, n$, että $p_i \mid N$. Koska lisäksi $p_i \mid p_1 p_2 \cdots p_n$, niin $p_i \mid N - p_1 p_2 \cdots p_n$ eli $p_i \mid 1$. Tämä on mahdotonta, joten vastaoletus on väärin ja siis väite on oikein. □

1.6 Aritmetiikan peruslause

Esitämme aluksi apulauseita (eli lemmoja) aritmetiikan peruslauseen todistamista varten.

Lemma 1.6.1 *Jos p on alkuluku ja $p \mid ab$, niin $p \mid a$ tai $p \mid b$.*

Todistus Jos $p \mid a$, niin silloin ei ole mitään todistettavaa. Oletetaan, että $p \nmid a$. Silloin $(p, a) = 1$, sillä luvun p ainoat tekijät ovat 1 ja p. Nyt lauseen 1.3.5 seurauksen 2 nojalla $p \mid b$. □

Lemma 1.6.2 *Jos p on alkuluku ja $p \mid a_1 a_2 \cdots a_n$, niin on olemassa sellainen $i = 1, 2, \ldots, n$, että $p \mid a_i$.*

Todistus Induktiolla luvun n suhteen.

Lemma 1.6.3 *Jos $p_1, p_2, \ldots, p_n$ ovat alkulukuja ja $p \mid p_1 p_2 \cdots p_n$, niin on olemassa sellainen $i = 1, 2, \ldots, n$, että $p = p_i$.*

Todistus Lemman 1.6.2 nojalla on olemassa sellainen $i = 1, 2, \ldots, n$, että $p \mid p_i$. Koska $p > 1$ ja luvun p_i ainoat tekijät ovat 1 ja p, niin $p = p_i$. □

Nyt olemme valmiit todistamaan *aritmetiikan peruslauseen.*

Lause 1.6.1 *Jokainen kokonaisluku a (≥ 2) voidaan esittää alkulukujen tulona ja tämä tulo on yksikäsitteinen tekijöitten järjestystä lukuunottamatta.*

Todistus Sovelletaan induktiota luvun a suhteen. Jos $a = 2$, niin lause on oikein. Oletetaan, että lause on oikein, kun $2 \leq a < k$. Todistetaan, että se on oikein, kun $a = k$. Jos k on alkuluku, niin silloin ei ole mitään todistettavaa. Oletetaan, että k on yhdistetty luku ja että luvulla k on kaksi alkutuloesitystä, sanokaamme

$$k = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t. \tag{1}$$

Todistamme, että $s = t$ ja että jokainen p on yhtäsuuri kuin jokin q. Koska $p_1 \mid q_1 q_2 \cdots q_t$, niin lemman 1.6.3 mukaan $p_1 = q_i$, missä $i = 1, 2, \ldots, n$. Muutetaan lukujen q numerointia niin, että $p_1 = q_1$. Näin ollen

$$k/p_1 = p_2 p_3 \cdots p_s = q_2 q_3 \cdots q_t.$$

Jos $s \geq 2$ tai $t \geq 2$, niin $1 < k/p_1 < k$. Induktio-olettamuksen mukaan luvun k/p_1 tuloesitykset ovat samat, joten $s = t$ ja luvun k esitykset yhtälössä (1) ovat samat. □

Esimerkki 1.6.1 Luvun 8750 esitys alkulukujen tulona on $8750 = 2 \cdot 5 \cdot 5 \cdot 5 \cdot 5 \cdot 7$. Tämä voidaan kirjoittaa muodossa

$$8750 = 2 \cdot 5^4 \cdot 7$$

tai

$$8750 = \prod_{p \in \mathbf{P}} p^{a(p)},$$

missä $a(2) = 1$, $a(3) = 0$, $a(5) = 4$, $a(7) = 1$, $a(p) = 0$ $(p \geq 11)$.

Esimerkki 1.6.2 Luku 600 voidaan kirjoittaa muodossa

$$600 = 2^3 \cdot 3 \cdot 5^2$$

tai

$$600 = \prod_{p \in \mathbf{P}} p^{a(p)},$$

missä $a(2) = 3$, $a(3) = 1$, $a(5) = 2$, $a(p) = 0$ $(p \geq 7)$.

Määritelmä Luvun a (> 1) *kanoninen alkutekijäesitys* on muotoa

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, \tag{2}$$

missä $p_1, p_2, \ldots, p_n$ $(p_1 < p_2 < \cdots < p_n)$ ovat luvun a alkutekijät (eli alkulukutekijät) ja $a_1, a_2, \ldots, a_n > 0$. Kanoniseksi alkutekijäesitykseksi sanotaan myös esitystä

$$a = \prod_{p \in \mathbf{P}} p^{a(p)}, \tag{3}$$

missä p käy läpi kaikki alkuluvut ja $a(p) \geq 0$. Usein (3) kirjoitetaan lyhyesti $a = \prod_p p^{a(p)}$ eli merkintä $\in \mathbf{P}$ jätetään pois.

Huomautus Kaavassa (3) $a(p) > 0$, jos ja vain jos $p \mid a$, ts. p on luvun a alkutekijä. Edelleen kaavassa (3) tulo on äärellinen, ts. $a(p) > 0$ vain äärellisellä määrällä alkulukuja p. Kaava (3) on hyödyllinen monissa teoreettisissa tarkasteluissa.

Huomautus Kanonista alkutekijäesitystä sanotaan usein lyhyesti *kanoniseksi esitykseksi*.

Esimerkki 1.6.3 Esimerkeissä 1.6.1 ja 1.6.2 on lukujen 8750 ja 600 kanoniset esitykset.

Esimerkki 1.6.4 Luku a on parillinen, jos ja vain jos $a(2)$ on > 0 sen kanonisessa esityksessä.

1.7 Aritmetiikan peruslauseen sovelluksia

Aritmetiikan peruslause on erittäin käyttökelpoinen työväline monissa sellaisissa tehtävissä, jotka käsittelevät luvun tekijöitä, lukujen syt:tä ja lukujen tuloja. Esitämme tässä joitakin esimerkkejä. Koko *tässä pykälässä tarkastelemme positiivisia kokonaislukuja* ja merkitsemme

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, \quad a_1, a_2, \ldots, a_n > 0 \tag{1}$$

tai

$$a = \prod_p p^{a(p)}, \quad a(p) \geq 0. \tag{2}$$

Lause 1.7.1 *Luku d on luvun a tekijä (eli $d \mid a$), jos ja vain jos d on muotoa*

$$d = \prod_p p^{d(p)}, \tag{3}$$

missä $0 \leq d(p) \leq a(p)$, $p \in \mathbf{P}$.

Todistus Oletetaan, että $d \mid a$. Silloin $a = db$, missä $b \in \mathbf{Z}^+$. Merkitään $b = \prod_p p^{b(p)}$, missä $b(p) \geq 0$. Silloin

$$a(p) = d(p) + b(p), \quad p \in \mathbf{P},$$

missä $a(p)$, $d(p)$, $b(p) \geq 0$, $p \in \mathbf{P}$. Näin ollen $0 \leq d(p) \leq a(p)$, $p \in \mathbf{P}$, eli d on muotoa (3).

Oletetaan käänteisesti, että d on muotoa (3). Merkitään $b = \prod_p p^{a(p)-d(p)}$. Silloin $a(p) - d(p) \geq 0$, $p \in \mathbf{P}$, joten $b \in \mathbf{Z}^+$. Siis $a = bd$, missä $b \in \mathbf{Z}^+$, eli $d \mid a$. □

Seuraus Luvun a tekijöitten lukumäärä on

$$\prod_p (a(p)+1)$$

eli

$$\prod_{i=1}^{n}(a_i+1).$$

Esimerkki 1.7.1 Luvun 200 kanoninen esitys on $2^3 \cdot 5^2$. Siis luvun 200 tekijät ovat

$$\begin{array}{lll} 1, & 5, & 5^2, \\ 2, & 2\cdot 5, & 2\cdot 5^2, \\ 2^2, & 2^2\cdot 5, & 2^2\cdot 5^2, \\ 2^3, & 2^3\cdot 5, & 2^3\cdot 5^2. \end{array}$$

Luvun 200 tekijöitten lukumäärä on $(3+1)(2+1)$ eli 12.

Lause 1.7.2 *Lukujen a ja b* syt *on*

$$(a,b) = \prod_p p^{c(p)},$$

missä $c(p) = \min\{a(p), b(p)\}$.

Todistus Merkitään kirjaimella c yhtälön oikean puolen lukua, ts. $c = \prod_p p^{c(p)}$, missä $c(p) = \min\{a(p), b(p)\}$. Silloin $c(p) \le a(p)$ ja $c(p) \le b(p)$, joten lauseen 1.7.1 nojalla

$$c \mid a, \quad c \mid b. \tag{4}$$

Oletetaan, että $d \mid a$, $d \mid b$. Silloin lauseen 1.7.1 mukaan $d(p) \le a(p)$ ja $d(p) \le b(p)$, joten $d(p) \le \min\{a(p), b(p)\}$ eli $d(p) \le c(p)$. Näin ollen $d \mid c$. Siis

$$d \le c. \tag{5}$$

Kaavoja (4) ja (5) nojalla $c = (a,b)$. □

Esimerkki 1.7.2 Lauseen 1.7.2 nojalla saadaan

$$(60, 18) = (2^2 \cdot 3 \cdot 5, 2 \cdot 3^2) = 2^1 \cdot 3^1 \cdot 5^0 = 6.$$

Esimerkki 1.7.3 Todista, että $(ac, bc) = (a,b)c$.

Ratkaisu Sovelletaan aritmetiikan peruslausetta ja kaavaa

$$\min\{a(p)+c(p), b(p)+c(p)\} = \min\{a(p), b(p)\} + c(p).$$

Määritelmä Luku c on lukujen a ja b *pienin yhteinen monikerta* (pym), jos

1) $c > 0$,

2) $a \mid c$, $b \mid c$,

3) $a \mid d$, $b \mid d$, $d > 0 \Rightarrow c \leq d$.

Merkintä Lukujen a ja b *pienintä yhteistä monikertaa* merkitään symbolilla $[a, b]$, pym$[a, b]$ tai lcm$[a, b]$.

Huomautus Lukujen pienin yhteinen monikerta (pym) on aina olemassa ja on yksikäsitteinen.

Esimerkki 1.7.4 Selvästi $[6, 9] = 18$.

Lause 1.7.3 *Lukujen a ja b* pym *on*

$$[a, b] = \prod_p p^{c(p)},$$

missä $c(p) = \max\{a(p), b(p)\}$.

Todistus Harjoitustehtävä. (vrt. lauseen 1.7.2 todistus)

Esimerkki 1.7.5 Lauseen 1.7.3 nojalla

$$[60, 18] = [2^2 \cdot 3 \cdot 5, 2 \cdot 3^2] = 2^2 \cdot 3^2 \cdot 5 = 180.$$

Lause 1.7.4 *Lukujen a ja b* syt *ja* pym *toteuttavat yhtälön*

$$(a, b)[a, b] = ab.$$

Todistus Sovelletaan aritmetiikan peruslausetta ja kaavaa

$$\min\{a(p), b(p)\} + \max\{a(p), b(p)\} = a(p) + b(p). \ \square$$

Esimerkki 1.7.6 Aikaisemmin on todettu, että $(a, a + 1) = 1$. Näin ollen lauseen 1.7.4 perusteella

$$[a, a + 1] = a(a + 1).$$

1.8 Kongruenssi

Määritelmä Olkoon $m \in \mathbf{Z}^+$. Silloin sanotaan, että luku a on *kongruentti* luvun b kanssa *modulo* m, jos

$$m \mid (a - b).$$

Merkintä Jos luku a on kongruentti luvun b kanssa modulo m, niin merkitään

$$a \equiv b \pmod{m}.$$

Esimerkki 1.8.1 Selvästi $5 \equiv 7 \pmod{2}$, mutta $6 \not\equiv 7 \pmod{2}$.

Lause 1.8.1 $a \equiv b \pmod{m}$, *jos ja vain jos*

$$\exists k \in \mathbf{Z}\colon a = b + km.$$

Todistus Lause seuraa suoraan määritelmästä. □

Lause 1.8.2 *Kongruenssi* $\equiv$ *on ekvivalenssirelaatio, ts.*

1) $a \equiv a \pmod{m}$,

2) $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$,

3) $a \equiv b \pmod{m}$, $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$.

Todistus 1) Kohta 1) seuraa relaatiosta $m \mid 0$.
2) Oletetaan, että $a \equiv b \pmod{m}$. Silloin $m \mid (a - b)$, joten $m \mid (b - a)$. Siis $b \equiv a \pmod{m}$.
3) Harjoitustehtävä. □

Lause 1.8.3 *Oletetaan, että* $a \equiv b \pmod{m}$ *ja* $c \equiv d \pmod{m}$. *Silloin*

1) $ax + cy \equiv bx + dy \pmod{m}$ *aina, kun* $x, y \in \mathbf{Z}$,

2) $ac \equiv bd \pmod{m}$,

3) $a^n \equiv b^n \pmod{m}$ *aina, kun* $n \in \mathbf{Z}^+ \cup \{0\}$,

4) $f(a) \equiv f(b)$ *aina, kun* f *on kokonaislukukertoiminen polynomi.*

Todistus 1) Koska $m \mid (a-b)$ ja $m \mid (c-d)$, niin

$$m \mid (a-b)x + (c-d)y$$

eli

$$m \mid (ax+cy) - (bx+dy).$$

Näin ollen kohta 1) pitää paikkansa.

2) Harjoitustehtävä.

3) Sovelletaan induktiota luvun n suhteen ja kohtaa 2).

4) Sovelletaan induktiota polynomin asteen suhteen. □

Esimerkki 1.8.2 Olkoon luvun a esitys 10-järjestelmässä $a = (a_n a_{n-1} \dots a_1 a_0)_{10}$. Silloin

$$3 \mid a \Leftrightarrow 3 \mid a_n + a_{n-1} + \cdots + a_1 + a_0.$$

Todistus Merkitään $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Koska $10 \equiv 1 \pmod 3$, niin $f(10) \equiv f(1) \pmod 3$ eli

$$a \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \pmod 3.$$

Näin ollen lauseen 1.8.2 nojalla

$$\begin{aligned} 3 \mid a &\Leftrightarrow a \equiv 0 \pmod 3 \\ &\Leftrightarrow a_n + a_{n-1} + \cdots + a_1 + a_0 \equiv 0 \pmod 3 \\ &\Leftrightarrow 3 \mid a_n + a_{n-1} + \cdots + a_1 + a_0. \ \square \end{aligned}$$

Huomautus Edellinen esimerkki pitää paikkansa, kun luku 3 korvataan luvulla 9.

Esimerkki 1.8.3 Relaatio $9 \mid 819$ on voimassa, koska $9 \mid (8+1+9)$.

Lause 1.8.4 *Merkitään $(a, m) = d$. Silloin*

$$ab \equiv ac \pmod m \Leftrightarrow b \equiv c \pmod{m/d}.$$

Todistus Selvästi

$$\begin{aligned} ab \equiv ac \pmod m &\Leftrightarrow m \mid a(b-c) \\ &\Leftrightarrow \frac{m}{d} \Big| \frac{a}{d}(b-c) \\ &\Leftrightarrow \frac{m}{d} \Big| b-c \quad \text{(lauseen 1.3.5 seuraus 2)} \\ &\Leftrightarrow b \equiv c \pmod{m/d}. \end{aligned}$$

Näin lause 1.8.4 on todistettu. □

Esimerkki 1.8.4 Lauseen 1.8.4 avulla saadaan

$$4x \equiv 20 \pmod 6 \Leftrightarrow x \equiv 5 \pmod 3.$$

Siis $x \equiv 2 \pmod 3$.

Huomautus Jos $a \equiv b \pmod m$, niin $(a, m) = (b, m)$. (Harjoitustehtävä.)

1.9 Jäännös ja kongruenssi

Kun luku a jaetaan jakoalgoritmin mukaisesti luvulla m (> 0), niin saadaan

$$a = qm + r, \tag{1}$$

missä $0 \leq r < m$. Lukua r sanotaan *jäännökseksi*. Tässä yhteydessä puhutaan tarkemmin *jäännöksestä modulo* m ja merkitään $r = a \,\mathbf{mod}\, m$. Jäännöksellä on selkeä yhteys kongruenssiin, joka todetaan tässä pykälässä.

Lause 1.9.1 1) *Jos* $r = a \,\mathbf{mod}\, m$, *niin* $a \equiv r \pmod m$.
2) *Jos* $a \equiv r \pmod m$ *ja* $0 \leq r < m$, *niin* $r = a \,\mathbf{mod}\, m$.

Todistus Seuraa jakoalgoritmin (1) ja lauseen 1.8.1 avulla.

Seuraus Jokaista kokonaislukua a kohti on olemassa yksikäsitteinen $r \in \{0, 1, \ldots, m-1\}$ niin, että $a \equiv r \pmod m$. Tämä yksikäsitteinen r on luvun a jäännös modulo m.

Huomautus Lauseista 1.8.2 ja 1.8.3 seuraa, että kun tuloja ja summia sisältävässä kokonaislukulausekkeessa jokin yhteenlaskettava tai tulontekijä korvataan sen kanssa kongruentin luvun kanssa $\pmod m$, niin saatu uusi lauseke on kongruentti alkuperäisen lausekkeen kanssa $\pmod m$.

Esimerkki 1.9.1 Määritä $32^{2001} \,\mathbf{mod}\, 3$ eli luvun 32^{2001} jäännös modulo 3.

Ratkaisu Etsitään sellainen $r \in \{0, 1, 2\}$, että $32^{2001} \equiv r \pmod 3$. Huomautuksen periaatteella saadaan

$$32^{2001} \equiv (-1)^{2001} = -1 \equiv 2 \pmod 3$$

eli jäännös on 2.

Esimerkki 1.9.2 Määritä luvun $2^{71} + 17 \cdot 6^{833}$ jäännös modulo 5.

Ratkaisu Huomautuksen periaatteella saadaan

$$\begin{aligned} 2^{71} + 17 \cdot 6^{833} &= 4^{35} \cdot 2 + 17 \cdot 6^{833} \\ &\equiv (-1)^{35} \cdot 2 + 17 \cdot 1^{833} = -2 + 17 \\ &= 15 \equiv 0 \pmod 5. \end{aligned}$$

Näin ollen $5 \mid 2^{71} + 17 \cdot 6^{833}$ eli jäännös on 0.

Esimerkki 1.9.3 Määritä lukujen 7835714 ja $\sum_{i=1}^{100} i!$ jäännökset modulo 4.

Ratkaisu Huomautuksen periaatteella saadaan

$$\begin{aligned} 7835714 &= 78357 \cdot 100 + 14 \\ &\equiv 78357 \cdot 0 + 14 \equiv 2 \pmod 4 \end{aligned}$$

ja

$$\begin{aligned} \sum_{i=1}^{100} i! &= 1! + 2! + 3! + 4! + \cdots + 100! \\ &\equiv 1 + 2 + 2 + 0 + \cdots + 0 \equiv 1 \pmod 4. \end{aligned}$$

Siis jäännökset ovat 2 ja 1.

Lause 1.9.2 *$a \equiv b \pmod m$, jos ja vain jos $a \bmod m = b \bmod m$.*

Todistus Oletetaan, että $a \equiv b \pmod m$. Todistetaan, että $a \bmod m = b \bmod m$. Kirjoitetaan

$$a = qm + r, \quad 0 \leq r < m. \tag{2}$$

Silloin

$$r = a \bmod m. \tag{3}$$

Oletuksen ja lauseen 1.8.1 mukaan on olemassa sellainen k, että

$$a = b + km. \tag{4}$$

Kaavojen (2) ja (4) perusteella

$$b + km = qm + r, \quad 0 \leq r < m$$

eli

$$b = (q - k)m + r, \quad 0 \leq r < m.$$

Näin ollen

$$b \,\mathbf{mod}\, m = r. \tag{5}$$

Kaavojen (3) ja (5) perusteella $a \,\mathbf{mod}\, m = b \,\mathbf{mod}\, m$.

Oletetaan käänteisesti, että $a \,\mathbf{mod}\, m = b \,\mathbf{mod}\, m$. Todistetaan, että $a \equiv b \pmod{m}$. Kirjoitetaan

$$\begin{aligned} a &= qm + r, \quad 0 \leq r < m, \\ b &= q'm + r', \quad 0 \leq r' < m. \end{aligned}$$

Oletuksen mukaan $r = r'$. Näin ollen

$$a - b = (q - q')m,$$

joten

$$m \mid a - b.$$

Siis

$$a \equiv b \pmod{m}. \ \square$$

1.10 Jäännösluokat

Olkoon $m \in \mathbf{Z}^+$ kiinteä. Lauseessa 1.8.2 on todistettu, että kongruenssi $\equiv \pmod{m}$ on ekvivalenssirelaatio joukossa $\mathbf{Z}$. Tämä antaa oikeutuksen seuraavalle määritelmälle.

Määritelmä Olkoon $m \in \mathbf{Z}^+$ kiinteä. Silloin ekvivalenssirelaation $\equiv \pmod{m}$ ekvivalenssiluokkia sanotaan *jäännösluokiksi* modulo m.

Merkintä Merkitään lyhyesti $\overline{a} = (a/ \equiv (\mathrm{mod}\, m))$ (ks. §1.14), ts.

$$\overline{a} = \{x \in \mathbf{Z} |\ x \equiv a \pmod{m}\}.$$

Siis $\overline{a}$ on luvun a jäännösluokka modulo m.

Huomautus Jäännösluokka $\overline{a}$ riippuu luvusta m, vaikka se ei merkinnästä $\overline{a}$ ilmenekään. Jos modulo m ei selviä asiayhteydestä, niin se on syytä mainita erikseen. Termin jäännösluokka luontevuus tulee selväksi alla olevista ominaisuuksista.

Merkintä Merkitään lyhyesti

$$\mathbf{Z}_m = (\mathbf{Z}/ \equiv (\mathrm{mod}\, m))$$

(ks. §1.14), ts.

$$\mathbf{Z}_m = \{\overline{a} |\ a \in \mathbf{Z}\}.$$

Siis $\mathbf{Z}_m$ on kaikkien jäännösluokkien joukko modulo m.

Lause 1.10.1 *Kokoelma* $\overline{0}$, $\overline{1}$, $\overline{2}$, $\ldots$, $\overline{m-1}$ *käsittää kaikki jäännösluokat modulo* m *täsmälleen kerran, ts.*

$$\mathbf{Z}_m = \left\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\right\}, \tag{1}$$

missä jäännösluokat $\overline{0}$, $\overline{1}$, $\overline{2}$, $\ldots$, $\overline{m-1}$ *ovat erisuuret.*

Todistus Todistetaan ensiksi kaava (1). Selvästi $\left\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\right\} \subseteq \mathbf{Z}_m$. Todistetaan, että $\mathbf{Z}_m \subseteq \left\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\right\}$. Olkoon $\overline{a} \in \mathbf{Z}_m$ mielivaltainen jäännösluokka. Merkitään $r = a \,\mathbf{mod}\, m$. Silloin $a \equiv r \pmod{m}$ ja $0 \leq r < m$. Ekvivalenssirelaation ominaisuuksien nojalla $\overline{a} = \overline{r}$ ja $0 \leq r < m$. Siis $\overline{a} \in \left\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\right\}$.

Todistetaan toiseksi, että jäännösluokat $\overline{0}$, $\overline{1}$, $\overline{2}$, $\ldots$, $\overline{m-1}$ ovat erisuuret. Oletetaan, että $\overline{u} = \overline{v}$, missä $0 \leq u, v < m$. Silloin ekvivalenssiluokkien yleisten ominaisuuksien nojalla

$$u \equiv v \pmod{m},$$

joten

$$m \mid u - v.$$

Koska $0 \leq |u - v| < m$, niin $u - v = 0$ eli $u = v$. □

Lause 1.10.2 *Joukko* $\mathbf{Z}_m$ *muodostaa joukon* $\mathbf{Z}$ *osituksen, ts. sen alkiot ovat erilliset ja niiden unioni on* $\mathbf{Z}$.

Todistus Lause 1.10.2 seuraa suoraan ekvivalenssiluokkien ominaisuuksista. □

Huomautus Seuraavat ominaisuudet ovat voimassa jäännösluokille:

1) $\overline{r} = \{x \in \mathbf{Z} |\ x \,\mathbf{mod}\, m = r\}$, kun $0 \leq r < m$,

2) $\overline{a} = \overline{r}$, missä $r = a \,\mathbf{mod}\, m$,

3) x ja y kuuluvat samaan jäännösluokkaan $\Leftrightarrow x \equiv y \pmod{m} \Leftrightarrow x \,\mathbf{mod}\, m = y \,\mathbf{mod}\, m$,

4) $\overline{a} = \overline{b} \Leftrightarrow a \equiv b \pmod{m} \Leftrightarrow a \,\mathbf{mod}\, m = b \,\mathbf{mod}\, m$,

5) $\overline{a} = \{x \in \mathbf{Z} |\ x \,\mathbf{mod}\, m = a \,\mathbf{mod}\, m\}$,

6) $r \in \overline{a}$, missä $r = a \,\mathbf{mod}\, m$.

Todistetaan ominaisuus 1). Oletetaan, että $x \in \overline{r}$. Silloin $x \equiv r \pmod{m}$, joten lauseen 1.9.1 2) mukaan $r = x \,\mathbf{mod}\, m$. Käänteisesti, jos $x \,\mathbf{mod}\, m = r$, niin lauseen 1.9.1 1) mukaan $x \equiv r \pmod{m}$ eli $x \in \overline{r}$. □

1.11 Lineaarinen kongruenssi

Polynomikongruenssit muistuttavat jossakin määrin tavallisia algebran polynomiyhtälöitä. Tässä tarkastelemme vain lineaarista kongruenssia $ax \equiv b \pmod{m}$.

Lause 1.11.1 *Kongruenssi*

$$ax \equiv b \pmod{m} \tag{1}$$

on ratkeava silloin ja vain silloin, kun $(a, m) \mid b$.

Todistus Kongruenssi (1) on ratkeava, jos ja vain jos on olemassa sellainen x, että $m \mid (ax - b)$, ts. jos ja vain jos on olemassa sellaiset x ja y, että

$$ax - my = b. \tag{2}$$

Yhtälö (2) on Diofantoksen yhtälö, joka on ratkeava, jos ja vain jos $(a, m) \mid b$. □

Huomautus Kongruenssin (1) ratkaiseminen voidaan palauttaa Diofantoksen yhtälön (2) ratkaisemiseen.

Lause 1.11.2 *Oletetaan, että* $(a, m) \mid b$. *Silloin kongruenssin* (1) *kaikki ratkaisut ovat*

$$x \equiv x_0 \pmod{m/(a, m)}, \tag{3}$$

missä x_0 *on yksi ratkaisu.*

Todistus Lauseen 1.11.1 mukaan kongruenssi (1) on ratkeava. Lauseen 1.4.2 mukaan yhtälön (2) kaikki ratkaisut ovat

$$\begin{cases} x &= x_0 + mt/(a, m), \\ y &= y_0 - mt/(a, m), \end{cases} \quad t \in \mathbf{Z},$$

missä x_0, y_0 on yhtälön (2) yksi ratkaisu. Siis kongruenssin (1) ratkaisut ovat

$$x = x_0 + mt/(a, m), \quad t \in \mathbf{Z},$$

eli kongruenssi (3) pitää paikkansa. □

Huomautus Kongruenssilla (1) on täsmälleen yksi ratkaisu kokonaislukuvälillä $[0, m/(a, m))$. Erisuuria ratkaisuja modulo m on (a, m) kappaletta. Jos $(a, m) = 1$, niin kongruenssilla (1) on yksikäsitteinen ratkaisu $\pmod{m}$.

Kongruenssin $ax \equiv b \pmod{m}$ **ratkaisualgoritmi**

Vaihe 1. Tutkitaan, onko $(a, m) \mid b$ ts. onko kongruenssi ratkeava (ks. lause 1.11.1).

Vaihe 2. Etsitään jokin yksittäinen ratkaisu x_0

2.1. keksimällä,

2.2. käymällä läpi luvut 0, 1, 2, ..., $m/(a,m) - 1$ (tai mitkä tahansa $m/(a,m)$ peräkkäistä lukua),

2.3. Eukleideen algoritmilla (ratkaise Diofantoksen yhtälö $ax - my = b$).

Vaihe 3. Yleinen ratkaisu on $x \equiv x_0 \pmod{m/(a,m)}$ (ks. lause 1.11.2).

Esimerkki 1.11.1 Ratkaistaan kongruenssi $139x \equiv 8 \pmod 3$.

1. Koska $(139, 3) \mid 8$, niin kongruenssi on ratkeava.

2.(2.) Etsitään yksittäinen ratkaisu käymällä läpi luvut 0, 1, 2. On helppo laskea, että 0 ja 1 eivät ole ratkaisuja, mutta 2 on ratkaisu.

3. Yleinen ratkaisu on $x \equiv 2 \pmod 3$.

Esimerkki 1.11.2 Ratkaistaan kongruenssi $16x \equiv 3 \pmod 8$.

1. Koska $(16, 8) \nmid 3$, niin kongruenssi ei ole ratkeava.

Esimerkki 1.11.3 Ratkaistaan kongruenssi $15x \equiv 9 \pmod{152}$.

1. Koska $(15, 152) \mid 9$, niin kongruenssi on ratkeava.

2.(3.) Etsitään yksittäinen ratkaisu x_0 Eukleideen algoritmilla. Selvästi

$$15x \equiv 9 \pmod{152} \Leftrightarrow \exists y\colon 15x - 152y = 9.$$

Ratkaistaan yllä oleva Diofantoksen yhtälö Eukleideen algoritmilla:

$$\begin{aligned} 152 &= 15 \cdot 10 + 2, \\ 15 &= 2 \cdot 7 + 1, \\ 2 &= 1 \cdot 2. \end{aligned}$$

Siis

$$\begin{aligned} 1 &= 15 - 2 \cdot 7 = 15 - (152 - 15 \cdot 10) \cdot 7 \\ &= 15 \cdot 71 - 152 \cdot 7. \end{aligned}$$

Kun kerrotaan viimeisin yhtälö puolittain luvulla 9, saadaan

$$9 = 15 \cdot \underbrace{639}_{x_0} - 152 \cdot 63.$$

3. Yleinen ratkaisu on $x \equiv 639 \equiv 31 \pmod{152}$.

Esimerkki 1.11.4 Ratkaistaan kongruenssi $18x \equiv 3 \pmod{15}$.

1. Koska $(8, 15) \mid 3$, niin kongruenssi on ratkeava.
2.(1.) Yksittäinen ratkaisu $x_0 = 1$ löydetään keksimällä.
3. Yleinen ratkaisu on $x \equiv 1 \pmod{5}$.

Huomautus kongruenssi $ax \equiv b \pmod{m}$ voidaan myös ratkaista manipuloimalla kongruenssia yhtäpitävästi lauseilla 1.8.2 ja 1.8.4.

Esimerkki 1.11.5 Ratkaistaan kongruenssi $22x \equiv 4 \pmod{30}$. Saadaan

$$\begin{aligned}
22x &\equiv 4 \pmod{30} \quad \mid :2 \\
11x &\equiv 2 \pmod{15} \quad [11 \equiv -4 \pmod{15}] \\
-4x &\equiv 2 \pmod{15} \quad \mid :(-2) \\
2x &\equiv -1 \pmod{15} \quad [-1 \equiv 14 \pmod{15}] \\
2x &\equiv 14 \pmod{15} \quad \mid :2 \\
x &\equiv 7 \pmod{15}.
\end{aligned}$$

Harjoitus Mitkä ovat yllä olevien kongruenssien erisuuret ratkaisut modulo m?

Huomautus Kun $(a, m) = 1$, niin kongruenssin $ax \equiv b \pmod{m}$ ratkaisua x_0 varten on olemassa eksplisiittinen kaava

$$x_0 = ba^{\varphi(m)-1},$$

missä $\varphi(m)$ on Eulerin phi-funktio. Funktiolle φ on muun muassa kaava

$$\varphi(m) = m \prod_{p \mid m} \left(1 - \frac{1}{p}\right).$$

(Todistukset sivuutetaan.) Voiko tätä periaatetta soveltaa yleiseen tapaukseen $(a, m) \mid b$, kun $(a, m) \geq 1$?

1.12 Esimerkki kryptologiasta

Kryptologia on salakirjoituksen teoriaa. Se tutkii systeemejä, joiden avulla muunnetaan kaikkien osapuolten ymmärtämä sanoma sellaiseen muotoon, jonka ymmärtävät vain ne, jotka pystyvät purkamaan salakirjoituksen.

Terminologiaa:

$$\text{selväteksti} \overset{\text{kryptaaminen}}{\longrightarrow} \text{kryptoteksti} \overset{\text{dekryptaaminen}}{\longrightarrow} \text{selväteksti}$$

Sovelluksia:

- tietojenkäsittelysysteemien tietosuoja (internet, matkaviestintä)

- kauppa-, sotilas- ja diplomatiaviestintä

Kryptologia jakautuu

- kryptografiaan, joka kehittää kryptosysteemejä

- kryptoanalyysiin, joka pyrkii purkamaan nämä systeemit

Tässä käsitellään aihetta lyhyesti yhden esimerkkisysteemin avulla. Esimerkki on luonteeltaan historiallinen kuriositeetti.

Caesarin systeemi

Selväteksti koostuu kirjainjonoista, jotka aluksi muutetaan lukujonoiksi niin, että jokainen kirjain (A, ..., Z) muutetaan luvuksi: A $\leftarrow 0$, ..., Z $\leftarrow 25$.

Olkoon nyt p jokin selvätekstin luku (väliltä 0 – 25). Merkitään vastaavaa kryptotekstin lukua symbolilla $f(p)$. (Symboli p tulee termistä "plain text" eikä siis tarkoita alkulukua.)

Kryptaaminen Caesarin systeemissä kryptoteksti muodostetaan kirjaimittain kaavalla

$$f(p) = (p + 3) \bmod 26$$

eli kaavalla

$$f(p) \equiv p + 3 \pmod{26} \quad \text{ja} \quad f(p) \in \{0, 1, \ldots, 25\}.$$

Esimerkki 1.12.1 Kryptataan END.

$$\text{END} \rightarrow 4\ 13\ 3 \rightarrow 7\ 16\ 6 \rightarrow \text{HQG}.$$

Dekryptaaminen Kryptoteksti puretaan kaavalla

$$p \equiv f(p) - 3 \pmod{26} \quad \text{ja} \quad p \in \{0, 1, \ldots, 25\}$$

eli kaavalla

$$p = (f(p) - 3) \bmod 26.$$

Esimerkki 1.12.2 Dekryptataan EBH.

$$\text{EBH} \leftarrow 4\ 1\ 7 \leftarrow 1\ 24\ 4 \leftarrow \text{BYE}.$$

1.13 Mathematica-ohjelmistosta

Mathematica-ohjelmistossa on useita lukuteoreettisia komentoja. Esimerkiksi `FactorInteger[n]` muodostaa luvun n kanonisen alkutekijäesityksen ja `GCD[m,n]` laskee lukujen m ja n suurimman yhteisen tekijän. Kongruenssiyhtälö $ax \equiv b \pmod{m}$ voidaan ratkaista komennolla `Solve[ax==b && Modulus==m,x]`. Lukuteoriaa varten on myös omia "pakkauksia", joissa tosin on enimmäkseen sellaisia aiheita, joita ei tällä kurssilla käsitellä.

1.14 Appendix (ekvivalenssirelaatio)

Tässä pykälässä esitetään ekvivalenssirelaation määritelmä ja perusominaisuuksia. Asiat esitetään lyhyesti luettelomaisesti, koska lukijan oletetaan tutustuneen aiemmin tähän käsitteeseen.

Määritelmä Olkoon A ei-tyhjä joukko. Karteesisen joukon $A \times A$ osajoukkoa R sanotaan *relaatioksi* joukossa A. Jos $(a, b) \in R$, niin merkitään $a \sim b$. Usein puhutaan relaation R sijasta relaatiosta $\sim$.

Määritelmä Relaatio $\sim$ joukossa A on *ekvivalenssi*, jos

1) $a \sim a$ (refleksiivisyys),

2) $a \sim b \Rightarrow b \sim a$ (symmetrisyys),

3) $a \sim b$, $b \sim c \Rightarrow a \sim c$ (transitiivisuus).

Määritelmä Olkoon $\sim$ joukon A ekvivalenssirelaatio. Silloin joukkoa $a/\!\sim$, missä

$$a/\!\sim = \{x \in A |\ x \sim a\},$$

sanotaan alkion a määräämäksi *ekvivalenssiluokaksi* ja alkiota a tämän luokan *edustajaksi*.

Lause 1.14.1 $a \sim b \Leftrightarrow a/\!\sim = b/\!\sim$.

Määritelmä Perhe $\{A_i\}$ joukon A ei-tyhjiä osajoukkoja muodostaa joukon A *osituksen*, jos joukon A jokainen alkio kuuluu yhteen ja vain yhteen joukoista A_i, ts. jos

1) $A = \bigcup_i A_i$,

2) $A_i \cap A_j = \emptyset$, kun $i \neq j$.

Määritelmä Olkoon $\sim$ joukon A ekvivalenssirelaatio. Kaikkien ekvivalenssiluokkien joukkoa (tai perhettä) sanotaan *tekijäjoukoksi* tai *osamääräjoukoksi* ja merkitään symbolilla $A/\sim$. Siis

$$A/\sim = \{a/\sim \mid a \in A\}\,.$$

Lause 1.14.2 *Jos $\sim$ on joukon A ekvivalenssi, niin kaikkien ekvivalenssiluokkien joukko $A/\sim$ muodostaa joukon A osituksen, ts.*

1) $A = \bigcup_a (a/\sim)$,

2) $(a/\sim) \cap (b/\sim) = \emptyset$, *kun* $a/\sim \neq b/\sim$.

Harjoitus Esitä osittaisen järjestysrelaation määritelmä.

2 Yhden laskutoimituksen struktuureja

Tässä luvussa tarkastellaan yhden laskutoimituksen algebrallisia struktuureja, ts. (yleisiä) joukkoja, jotka on varustettu yhdellä (yleisellä) laskutoimituksella ja joissa laskutoimitusta säätelee aksioomat. Erilaisia algebrallisia struktuureja saadaan sen mukaan, millaisia aksioomat ovat. Tärkein yhden laskutoimituksen algebrallinen struktuuri on ryhmä. Tässä monisteessa tutkitaan potenssia ja supistamista ryhmässä, ryhmän alistruktuureja ja ryhmien isomorfiaa (samankaltaisuutta). Konkreettiset esimerkit otetaan pääasiassa lukuteoriasta.

2.1 Laskutoimitus

Määritelmä Olkoon A ei-tyhjä joukko. Silloin kuvausta $A \times A \to A$ sanotaan *laskutoimitukseksi* joukossa A (tai *binäärioperaatioksi* joukossa A).

Huomautus Laskutoimitus siis *liittää jokaiseen pariin* $(a, b) \in A \times A$ *täsmälleen yhden joukon* A *alkion.* Tätä joukon A alkiota merkitään symbolilla $a \star b$. Usein käytetään myös merkintöjä $a \circ b$, $a \cdot b$, ab, $a + b$. Laskutoimitukselta siis vaaditaan, että

1) $a \star b$ on olemassa aina, kun $a, b \in A$ (olemassaolo),

2) $a \star b$ on yksikäsitteinen eli hyvin määritelty ja

3) $a \star b \in A$ aina, kun $a, b \in A$ (sulkeutuvuus).

Esimerkki 2.1.1 Sääntö

1) $a \star b = ab$ määrittelee laskutoimituksen joukossa $\mathbf{R}$,

2) $a \star b = a + b$ määrittelee laskutoimituksen joukossa $\mathbf{R}$,

3) $a \star b = a/b$ ei määrittele laskutoimitusta joukossa $\mathbf{R}$,

4) $a \star b = a - b$ määrittelee laskutoimituksen joukossa $\mathbf{R}$,

5) $a \star b = a - b$ ei määrittele laskutoimitusta joukossa $\mathbf{Z}^+$.

Esimerkki 2.1.2 Olkoon E joukko ja 2^E sen kaikkien osajoukkojen joukko. (Ts. 2^E on joukon E potenssijoukko. Sitä merkitään myös $\mathcal{P}(E)$). Silloin

1) $A \star B = A \cap B$,

2) $A \star B = A \cup B$

määrittelee laskutoimituksen joukossa 2^E.

Esimerkki 2.1.3 Olkoon $M_{m\times n}$ reaalielementtisten $m \times n$–matriisien joukko. Silloin

1) $A \star B = A + B$ määrittelee laskutoimituksen joukossa $M_{m\times n}$,

2) $A \star B = AB$ määrittelee laskutoimituksen joukossa $M_{m\times n}$, kun $m = n$.

Esimerkki 2.1.4 Sääntö

1) $a \star b = a + 2b$ määrittelee laskutoimituksen joukossa $\mathbf{R}$,

2) $a \star b = a$ määrittelee laskutoimituksen joukossa $\mathbf{R}$,

3) $a \star b = \frac{1}{2}ab$ määrittelee laskutoimituksen joukossa $\mathbf{R}$,

4) $a \star b = a + b + ab$ määrittelee laskutoimituksen joukossa $\mathbf{R}$,

5) $a \star b = \max\{a, b\}$ määrittelee laskutoimituksen joukossa $\mathbf{R}$.

Esimerkki 2.1.5 Sääntö

1) $(a/b) \star (c/d) = (a + c)/(b + d)$ ei määrittele laskutoimitusta joukossa $\mathbf{Q}^+$,

2) $\overline{a} \star \overline{b} = \overline{(ab) \bmod 3}$ ei määrittele laskutoimitusta joukossa $\mathbf{Z}_2$.

Määritelmä Paria $(A, \star)$, missä A on ei-tyhjä joukko ja $\star$ sen laskutoimitus, sanotaan (yhden laskutoimituksen) *algebralliseksi struktuuriksi*.

2.2 Laskulakeja

Assosiatiivisuus ja kommutatiivisuus

Määritelmä Joukon A laskutoimitusta $\star$ sanotaan *assosiatiiviseksi* (eli *liitännäiseksi*), jos

$$(a \star b) \star c = a \star (b \star c)$$

aina, kun $a, b, c \in A$, ja *kommutatiiviseksi* (eli *vaihdannaiseksi*), jos

$$a \star b = b \star a$$

aina, kun a, $b \in A$.

Esimerkki 2.2.1 Esimerkin 2.1.4 1) laskutoimitus ei ole assosiatiivinen eikä kommutatiivinen. Todistetaan väitteet vastaesimerkeillä. Yleisesti

$$(a \star b) \star c = (a + 2b) \star c = (a + 2b) + 2c = a + 2b + 2c$$

ja

$$a \star (b \star c) = a \star (b + 2c) = a + 2(b + 2c) = a + 2b + 4c.$$

Erikoisesti, $(0 \star 0) \star 1 = 2$ ja $0 \star (0 \star 1) = 4$, joten assosiatiivisuus ei ole voimassa. Edelleen

$$a \star b = a + 2b \quad \text{ja} \quad b \star a = b + 2a.$$

Erikoisesti, $0 \star 1 = 2$ ja $1 \star 0 = 1$, joten kommutatiivisuus ei ole voimassa.

Esimerkki 2.2.2 Esimerkin 2.1.4 2) laskutoimitus on assosiatiivinen, sillä

$$(a \star b) \star c = a \star c = a$$

ja

$$a \star (b \star c) = a \star b = a$$

aina, kun a, b, $c \in \mathbf{R}$. Sen sijaan kyseessä oleva laskutoimitus ei ole kommutatiivinen. (Totea!)

Esimerkki 2.2.3 Esimerkkien 2.1.4 3) ja 4) laskutoimitukset ovat sekä assosiatiivisia että kommutatiivisia. (Totea!)

Harjoitus Konstruoitava laskutoimitus, joka on kommutatiivinen mutta ei ole assosiatiivinen.

Neutraalialkio

Määritelmä Alkio $e \in A$ on algebrallisen struktuurin $(A, \star)$ *neutraalialkio*, jos

$$a \star e = e \star a = a$$

aina, kun $a \in A$.

Lause 2.2.1 *Jos parilla $(A, \star)$ on neutraalialkio, niin se on yksikäsitteinen.*

Todistus Olkoot e ja e' neutraalialkioita. Silloin

$$(e \star a =) a \star e = a \quad \forall a \in A$$

ja

$$e' \star b (= b \star e') = b \quad \forall b \in A.$$

Valitaan $a = e'$ ja $b = e$, jolloin saadaan

$$e' = e' \star e = e. \ \square$$

Esimerkki 2.2.4 Algebrallisen struktuurin $(\mathbf{R}, \star)$, missä $a \star b = ab$, neutraalialkio on reaaliluku 1, ja algebrallisen struktuurin $(\mathbf{R}, \star)$, missä $a \star b = a + b$, neutraalialkio on reaaliluku 0.

Esimerkki 2.2.5 Algebrallisen struktuurin $(\mathbf{R}, \star)$, missä $a \star b = \frac{1}{2}ab$, neutraalialkio on reaaliluku 2, sillä

$$a \star 2 = \frac{1}{2}a2 = a \quad \text{ja} \quad 2 \star a = \frac{1}{2}2a = a \quad \forall a \in A.$$

Algebrallisen struktuurin $(\mathbf{R}, \star)$, missä $a \star b = a + b + ab$, neutraalialkio on reaaliluku 0, sillä

$$a \star 0 = a + 0 + a0 = a \quad \text{ja} \quad 0 \star a = 0 + a + 0a = a \quad \forall a \in A.$$

Vrt. esimerkit 2.1.4 3) ja 4).

Esimerkki 2.2.6 Algebrallisella struktuurilla $(\mathbf{R}, \star)$, missä $a \star b = \max\{a, b\}$, ei ole neutraalialkiota. (Huomaa, että $-\infty \notin \mathbf{R}$.) Myöskään algebrallisen struktuurilla $(\mathbf{R}^+, \star)$, missä $a \star b = a^2b^2$, ei ole neutraalialkiota. Tehdään vastaoletus, että e on neutraalialkio. Silloin

$$a \star e = a^2e^2 = a \quad \forall a \in \mathbf{R}^+,$$

joten $e = 1/\sqrt{a}$ $\forall a \in \mathbf{R}^+$. Kun $a = 1$, niin $e = 1$, ja kun $a = 4$, niin $e = 1/2$. Lauseen 2.2.1 mukaan e on yksikäsitteinen, jolloin päädytään ristiriitaan. Siis algebrallisella struktuurilla $(\mathbf{R}^+, \star)$, missä $a \star b = a^2b^2$, ei ole neutraalialkiota

Harjoitus Onko algebrallisella struktuurilla $(\mathbf{R}, \star)$, missä $a \star b = ab + a$, neutraalialkio?

Huomautus Kun laskutoimitus on yhteenlaskunkaltainen, neutraalialkiota kutsutaan usein *nolla-alkioksi*. Vastaavasti kun laskutoimitus on kertolaskunkaltainen, neutraalialkiota kutsutaan *ykkösalkioksi*.

2.3 Ryhmä

Puoliryhmä

Määritelmä Algebrallinen struktuuri $(A, \star)$, jonka laskutoimitus on assosiatiivinen, on *puoliryhmä*.

Määritelmä Puoliryhmää $(A, \star)$, jolla on neutraalialkio, sanotaan *monoidiksi*.

Esimerkki 2.3.1 Pari $(\mathbf{R}, \star)$, missä $a \star b = \max\{a, b\}$, on puoliryhmä, mutta ei monoidi.

Esimerkki 2.3.2 Pari $(\mathbf{Z}^+, \star)$, missä $a \star b = \max\{a, b\}$, on monoidi (ja siis myös puoliryhmä).

Huomautus Jos puoliryhmän (vastaavasti monoidin) laskutoimitus on kommutatiivinen, niin puoliryhmää (vastaavasti monoidia) sanotaan kommutatiiviseksi.

Käänteisalkio

Määritelmä Olkoon $(A, \star)$ on monoidi ja merkitään sen neutraalialkiota kirjaimella e. Alkion $a \in A$ sanotaan olevan *yksikkö* (tai *kääntyvä*), jos on olemassa sellainen $a' \in A$, että

$$a \star a' = a' \star a = e.$$

Alkiota a' sanotaan alkion a *käänteisalkioksi*, ja merkitään $a' = a^{-1}$.

Lause 2.3.1 *Olkoon $(A, \star)$ on monoidi. Silloin kääntyvän alkion a käänteisalkio on yksikäsitteinen.*

Todistus Olkoot x ja y alkion a käänteisalkioita. Silloin

$$a \star x = x \star a = e$$

ja

$$a \star y = y \star a = e.$$

Koska $(A, \star)$ on monoidi, voidaan kirjoittaa

$$x = e \star x = (y \star a) \star x = y \star (a \star x) = y \star e = y.$$

Siis

$$x = y.$$

Näin lause 2.3.1 on todistettu. □

Esimerkki 2.3.3 Monoidissa $(\mathbf{R}, \cdot)$ alkion a $(\neq 0)$ käänteisalkio on $1/a$. Monoidissa $(\mathbf{R}, +)$ alkion a käänteisalkio on $-a$.

Huomautus Kun laskutoimitus on yhteenlaskunkaltainen, on käänteisalkion sijasta syytä puhua *vasta-alkiosta*.

Esimerkki 2.3.4 Monoidissa $(M_{n\times n}, \cdot)$ alkiolla A on käänteisalkio, jos ja vain jos $\det A \neq 0$.

Esimerkki 2.3.5 Monoidissa $(\mathbf{Z}^+, \star)$, missä $a \star b = \max\{a, b\}$, vain alkiolla 1 on käänteisalkio. Nimittäin, neutraalialkio on 1, ja $\max\{a, 1\} = 1$, jos ja vain jos $a = 1$.

Esimerkki 2.3.6 Monoidissa $(\mathbf{R}, \star)$, missä $a \star b = \frac{1}{2}ab$, alkion a $(\neq 0)$ käänteisalkio on $4/a$. Nimittäin neutraalialkio on 2 ja $a \star 4/a = \frac{1}{2}a4/a = 2$. Vrt. esimerkki 2.2.5.

Esimerkki 2.3.7 Algebrallisen struktuurin $(\mathbf{R}, \star)$, missä $a \star b = a + b + ab$, alkion a $(\neq -1)$ käänteisalkio on $-a/(a+1)$. (Totea!) Vrt. esimerkki 2.2.5.

Lause 2.3.2 *Jos monoidin alkiot a ja b ovat kääntyviä, niin alkiot $a \star b$ ja a^{-1} ovat kääntyviä ja*

$$\begin{aligned} (a \star b)^{-1} &= b^{-1} \star a^{-1}, \\ (a^{-1})^{-1} &= a. \end{aligned}$$

Todistus Selvästi

$$\begin{aligned} (a \star b) \star (b^{-1} \star a^{-1}) &= a \star (b \star b^{-1}) \star a^{-1} = a \star e \star a^{-1} \\ &= a \star a^{-1} = e. \end{aligned}$$

Samoin $(b^{-1} \star a^{-1}) \star (a \star b) = e$. Siis $a \star b$ on kääntyvä ja sen käänteisalkio on $b^{-1} \star a^{-1}$. Kaava $(a^{-1})^{-1} = a$ jätetään harjoitustehtäväksi. □

Ryhmä

Määritelmä Monoidi $(A, \star)$ on *ryhmä*, jos jokaisella alkiolla $a \in A$ on käänteisalkio.

Huomautus Ryhmästä käytetään yleensä kirjallisuudessa merkintää $(G, \star)$. Näin toimitaan jatkossa myös tässä esityksessä.

Lause 2.3.3 *Pari $(G, \star)$ on ryhmä, jos ja vain jos*

1) *pari $(G, \star)$ on algebrallinen struktuuri,*
2) *laskutoimitus $\star$ on assosiatiivinen,*
3) *joukossa G on neutraalialkio laskutoimituksen $\star$ suhteen,*
4) *jokaisella alkiolla $a \in G$ on käänteisalkio.*

Todistus Lause 2.3.3 seuraa suoraan monoidin ja ryhmän määritelmistä. □

Määritelmä Ryhmä $(G, \star)$ on *Abelin ryhmä*, jos laskutoimitus $\star$ on vaihdannainen.

Esimerkki 2.3.8 Parit $(\mathbf{R}, +)$ ja $(\mathbf{R}^*, \cdot)$ ovat Abelin ryhmiä, missä $\mathbf{R}^* = \mathbf{R} \setminus \{0\}$.

Esimerkki 2.3.9 Pari $(\mathbf{R}^*, \star)$ on Abelin ryhmä, missä $a \star b = \frac{1}{2}ab$.

Esimerkki 2.3.10 Pari $(M^*_{n\times n}, \cdot)$ on ryhmä, missä $M^*_{n\times n}$ on sellaisten $n\times n$–matriisien A joukko, että $\det A \neq 0$. Tämä ryhmä ei ole Abelin ryhmä.

Esimerkki 2.3.11 Pari $(\mathbf{Z}^+, \star)$, missä $a \star b = \max\{a, b\}$, ei ole ryhmä.

Esimerkki 2.3.12 Jos $(G, \star)$ on ryhmä ja $(a \star b)^{-1} = a^{-1} \star b^{-1}$ aina, kun a, $b \in G$, niin $(G, \star)$ on Abelin ryhmä.
Todistus Ehdon $(a \star b)^{-1} = a^{-1} \star b^{-1}$ nojalla

$$(a \star b) \star (a^{-1} \star b^{-1}) = e.$$

Kun tämä yhtälö kerrotaan puolittain oikealta alkioilla b ja a, niin saadaan

$$a \star b = b \star a.$$

(Millä perusteella yhtälö voidaan kertoa puolittain?) Siis ryhmä on Abelin ryhmä. □

2.4 Potenssi

Määritelmä Olkoon $(G, \star)$ ryhmä ja $a \in G$. Silloin alkion a potenssi a^k $(k \in \mathbf{Z}^+)$ määritellään kaavoilla

$$\begin{aligned} a^1 &= a, \quad a^n = a^{n-1} \star a, \quad n \geq 2. \\ a^0 &= e, \\ a^{-n} &= (a^n)^{-1}, \quad n > 0. \end{aligned}$$

Huomautus Assosiatiivisuuden nojalla positiivinen potenssi voidaan kirjoittaa

$$a^n = a \star a \star \cdots \star a.$$

Lauseen 2.3.2 nojalla negatiivinen potenssi voidaan kirjoittaa

$$a^{-n} = (a^n)^{-1} = a^{-1} \star a^{-1} \star \cdots \star a^{-1} = (a^{-1})^n.$$

Huomautus Assosiatiivisuuden takia positiivisen potenssin käsite on mielekäs jo puoliryhmässä. Ei-negatiivinen potenssi voidaan määritellä monoidissa ja yleinen kokonaislukupotenssi ryhmässä.

Huomautus Jos ryhmän laskutoimitus on yhteenlaskunkaltainen, on syytä puhua potenssin sijasta *monikerrasta*. Silloin merkitään na, $0a$ ja $(-n)a$. Esimerkiksi ryhmässä $(\mathbf{R}^*, \cdot)$ puhutaan potenssista, kun taas ryhmässä $(\mathbf{R}, +)$ puhutaan monikerrasta.

Esimerkki 2.4.1 Positiivinen potenssi ei ole mielekäs algebrallisessa struktuurissa $(\mathbf{R}^*, \div)$, sillä esimerkiksi $(2/2)/2 = 1/2$, mutta $2/(2/2) = 2$.

Esimerkki 2.4.2 Olkoon $(G, \star)$ sellainen ryhmä, jossa $a^2 = e$ aina, kun $a \in G$. Silloin $(G, \star)$ on Abelin ryhmä.
Todistus Koska $a^2 = e$, niin $a^{-1} = a$ aina, kun $a \in G$. Näin ollen

$$a \star b = (a \star b)^{-1} = b^{-1} \star a^{-1} = b \star a$$

aina, kun a, $b \in G$.

Lause 2.4.1 *Jos $(G, \star)$ on ryhmä ja $a \in G$, niin*

$$\begin{aligned} a^m \star a^n &= a^{m+n}, \\ (a^m)^n &= a^{mn} \end{aligned}$$

aina, kun m, $n \in \mathbf{Z}$.

Todistus Harjoitustehtävä.

Lause 2.4.2 *Jos $(G, \star)$ on Abelin ryhmä ja a, $b \in G$, niin*

$$(a \star b)^n = a^n \star b^n$$

aina, kun $n \in \mathbf{Z}$.

Todistus Harjoitustehtävä.

Harjoitus Olkoon $(G, \star)$ sellainen ryhmä, jossa $(a \star b)^2 = a^2 \star b^2$ aina, kun a, $b \in G$. Todista, että $(G, \star)$ on Abelin ryhmä.

2.5 Supistamislait

Lause 2.5.1 (Supistamislait) *Olkoon $(G, \star)$ ryhmä. Silloin*

$$\begin{aligned} a \star b = a \star c &\Rightarrow b = c, \\ a \star c = b \star c &\Rightarrow a = b. \end{aligned}$$

Todistus Oletetaan, että $a \star b = a \star c$. Silloin $a^{-1} \star (a \star b) = a^{-1} \star (a \star c)$, joten $(a^{-1} \star a) \star b = (a^{-1} \star a) \star c$ eli $e \star b = e \star c$. Näin ollen $b = c$. (Millä perusteella edelliset päättelyt voidaan tehdä?) Toinen ominaisuus todistetaan samalla tavalla. □

Huomautus Käänteiset ominaisuudet

$$\begin{aligned} b = c &\Rightarrow a \star b = a \star c, \\ a = b &\Rightarrow a \star c = b \star c \end{aligned}$$

ovat voimassa aina, kun $\star$ on laskutoimitus. Jos $\star$ ei ole laskutoimitus, niin yllä olevat ominaisuudet eivät välttämättä pidä paikkaansa. Vastaesimerkki löytyy esimerkiksi tarkastelemalla sääntöä $(a/b) \oplus (c/d) = (a+c)/(b+d)$ joukossa $\mathbf{Q}$.

Huomautus Supistamislait eivät ole aina voimassa monoidissa. Esimerkiksi parit $(M_{n\times n}, \cdot)$ ja $(\mathbf{Z}^+, \star)$, missä $a \star b = \max\{a, b\}$, ovat monoideja, ja on helppo todeta, että supistuslait eivät ole voimassa. Esimerkiksi $2 \star 1 = 2 \star 2 (= 2)$, mutta $1 \neq 2$. Valinta A on nollamatriisi on triviaali esimerkki monoidissa $(M_{n\times n}, \cdot)$. Etsi jokin muu vastaesimerkki.

Huomautus Yhtälöiden

$$a \star x = b \quad \text{ja} \quad y \star a = b$$

ratkaisemisessa toimitaan samalla tavalla kuin supistamislakien todistuksessa. Voidaan todistaa, että ryhmässä kyseessä olevilla yhtälöillä on yksikäsitteiset ratkaisut

$$x = a^{-1} \star b \quad \text{ja} \quad y = b \star a^{-1}.$$

Monoidissa yksikäsitteisiä ratkaisuja ei aina ole. (Totea!)

Esimerkki 2.5.1 Ratkaistaan yhtälöt $2 \oplus x = 7$ ja $2x = 7$ Abelin ryhmässä $(\mathbf{R}, \oplus)$, missä $a \oplus b = a + b + 1$.
Ratkaisu Yhtälö $2 \oplus x = 7$ tarkoittaa, että $2 + x + 1 = 7$ eli $x = 4$. Yhtälö $2x = 7$ tarkoittaa, että $x \oplus x = 7$ eli $x + x + 1 = 7$. Siis $x = 3$.

Huomautus Abelin ryhmässä $a^{-1} \star b = b \star a^{-1}$, joten silloin on mielekästä määritellä osamäärä (additiivisin termein erotus).

Esimerkki 2.5.2 Kääntyville (eli ei-singulaarisille) matriiseille ei ole mielekästä määritellä osamäärää, sillä yleensä $A^{-1}B \neq BA^{-1}$. Sen sijaan $m \times n$–matriisien joukossa on mielekäs erotus $B - A = (-A) + B = B + (-A)$.

2.6 Permutaatioryhmät

Määritelmä Joukon X bijektiota itselleen sanotaan joukon X *permutaatioksi*.

Esimerkki 2.6.1 Kuvaus $f\colon \mathbf{R} \to \mathbf{R}$, $f(x) = x^3$, on joukon $\mathbf{R}$ permutaatio.

Esimerkki 2.6.2 Olkoon $X = \{1, 2, 3\}$ ja $\pi\colon X \to X$ sellainen kuvaus, että $\pi(1) = 2$, $\pi(2) = 1$, $\pi(3) = 3$. Silloin π on joukon X permutaatio. Permutaatiota π merkitään usein myös

$$(2, 1, 3)$$

ja

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Joukon X permutaatioita on kaikkiaan 3! kappaletta. Yleisemmin, n–alkioisen joukon permutaatioiden lukumäärä on $n!$.

Merkintä Joukon X kaikkien permutaatioiden joukkoa merkitään symbolilla S_X. Jos $X = \{1, 2, \ldots, n\}$, niin merkitään $S_X = S_n$.

Määritelmä Olkoot $f\colon A \to B$ ja $g\colon B \to C$ kuvauksia. Silloin *yhdistetty kuvaus* $g \circ f$ on kuvaus $g \circ f\colon A \to C$, $(g \circ f)(x) = g(f(x))$.

Esimerkki 2.6.3 Joukossa S_3 on voimassa

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

Lause 2.6.1 *Pari* $(S_X, \circ)$ *on ryhmä.*

Todistus 1) Kuvausten yhdistäminen $\circ$ on laskutoimitus.

2) Kuvausten yhdistäminen $\circ$ on assosiatiivinen.

3) Neutraalialkio on identtinen kuvaus $I\colon X \to X$, $I(a) = a$.

4) Alkion $\pi \in S_X$ käänteisalkio on käänteiskuvaus π^{-1}, sillä se toteuttaa ehdot

$$\pi^{-1} \circ \pi = I \quad \text{ja} \quad \pi \circ \pi^{-1} = I.$$

(Kohtien 1–4 yksityiskohtainen todistaminen sivuutetaan.) □

Esimerkki 2.6.4 Ryhmässä $(S_3, \circ)$ permutaation $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ käänteispermutaatio on $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$. (Totea!)

Määritelmä Ryhmää $(S_X, \circ)$ sanotaan *symmetriseksi ryhmäksi*. Sen aliryhmiä (ks. §2.9) *permutaatioryhmiksi*. (Permutaatioryhmiä ei tässä esityksessä tarkastella yksityiskohtaisemmin.)

2.7 Jäännösluokkaryhmä

Olkoon $m \in \mathbf{Z}^+$ kiinteä. Merkitään symbolilla $\mathbf{Z}_m$ kaikkien jäännösluokkien joukkoa (mod m). Siis

$$\mathbf{Z}_m = \left\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\right\}.$$

Määritellään yhteenlasku joukossa $\mathbf{Z}_m$ niin, että

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

aina, kun $\overline{a}$, $\overline{b} \in \mathbf{Z}_m$. Yhtälön oikealla puolella viivan alla oleva yhteenlasku $a + b$ on kokonaislukujen tavallinen yhteenlasku. Vasemman puolen yhteenlasku on määriteltävänä oleva yhteenlasku joukossa $\mathbf{Z}_m$. Tätä yhteenlaskua kutsutaan usein yhteenlaskuksi (mod m).

Esimerkki 2.7.1 Yhteenlaskun joukossa $\mathbf{Z}_2$ antaa taulu

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

.

Esimerkki 2.7.2 Yhteenlaskun joukossa $\mathbf{Z}_3$ antaa taulu

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

.

Esimerkiksi $\overline{2} + \overline{2} = \overline{4} = \overline{1}$.

Lause 2.7.1 *Pari* $(\mathbf{Z}_m, +)$ *on Abelin ryhmä.*

Todistus 1) Yhteenlasku (mod m) on laskutoimitus joukossa $\mathbf{Z}_m$. (Totea!)
2) Yhteenlasku (mod m) on assosiatiivinen, sillä

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

Kolmas yhtälö seuraa tavallisen yhteenlaskun assosiatiivisuudesta. Muut yhtälöt seuraavat yhteenlaskun (mod m) määritelmästä.

3) Struktuurin neutraalialkio (eli tässä nolla-alkio) on jäännösluokka $\overline{0}$. (Totea!)

4) Jäännösluokan $\overline{a} \in \mathbf{Z}_m$ käänteisalkio (eli tässä vasta-alkio) on luvun a vastaluvun $-a$ määräämä jäännösluokka $\overline{(-a)}$. (Totea!)

5) Yhteenlasku $\pmod m$ on kommutatiivinen, sillä

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

(Mihin yllä olevat yhtälöt perustuvat?) $\square$

Määritelmä Abelin ryhmää $(\mathbf{Z}_m, +)$ sanotaan *jäännösluokkaryhmäksi* $\pmod m$ tai *additiiviseksi jäännösluokkaryhmäksi* $\pmod m$.

Esimerkki 2.7.3 Mitkä ovat alkioiden $\overline{1}$ ja $\overline{2}$ vasta-alkiot ryhmässä $(\mathbf{Z}_3, +)$?
Ratkaisu Lauseen 2.7.1 todistuksen mukaan $-(\overline{1}) = \overline{-1} = \overline{2}$ ja $-(\overline{2}) = \overline{-2} = \overline{1}$. Huomaa, että $\overline{1} + \overline{2} = \overline{3} = \overline{0}$.

Esimerkki 2.7.4 Mitkä ovat alkioiden $\overline{1}$ ja $\overline{2}$ vasta-alkiot ryhmässä $(\mathbf{Z}_4, +)$?
Ratkaisu Nyt $-(\overline{1}) = \overline{-1} = \overline{3}$ ja $-(\overline{2}) = \overline{-2} = \overline{2}$. Huomaa, että $\overline{1} + \overline{3} = \overline{4} = \overline{0}$ ja $\overline{2} + \overline{2} = \overline{4} = \overline{0}$.

Esimerkki 2.7.5 Ratkaise yhtälöt

a) $\overline{2} + \overline{x} = \overline{1}$,

b) $2\overline{x} = \overline{1}$

ryhmässä $(\mathbf{Z}_4, +)$.
Ratkaisu Kokeilemalla voidaan todeta, että a) $\overline{x} = \overline{3}$, b) yhtälöllä ei ole ratkaisua.

2.8 Alkuluokkaryhmä

Olkoon $m \in \mathbf{Z}^+$ kiinteä. Määritellään kertolasku joukossa $\mathbf{Z}_m$ kaavalla

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

aina, kun $\overline{a}$, $\overline{b} \in \mathbf{Z}_m$. Yhtälön oikealla puolella viivan alla tulo ab on tavallinen kokonaislukujen tulo. Vasemman puolen tulo on määriteltävänä oleva kertolasku joukossa $\mathbf{Z}_m$ eli kertolasku $\pmod m$.

Esimerkki 2.8.1 Kertolaskun joukossa $\mathbf{Z}_2$ antaa taulu

$\cdot$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

.

Esimerkki 2.8.2 Kertolaskun joukossa $\mathbf{Z}_4$ antaa taulu

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

.

Lause 2.8.1 *Pari* $(\mathbf{Z}_m, \cdot)$ *on kommutatiivinen monoidi.*

Todistus Harjoitustehtävä. (Esimerkiksi neutraalialkio (eli tässä ykkösalkio) on jäännösluokka $\overline{1}$.) □

Pari $(\mathbf{Z}_m, \cdot)$ ei ole aina ryhmä, sillä jäännösluokilla ei ole välttämättä käänteisalkiota. Esimerkiksi alkiolla $\overline{2}$ ei ole käänteisalkiota monoidissa $(\mathbf{Z}_4, \cdot)$, ts. ei ole olemassa sellaista alkiota $\overline{a}$, että $\overline{2} \cdot \overline{a} = \overline{1}$. (Totea!)

Seuraavassa lauseessa annamme välttämättömän ja riittävän ehdon sille, että alkiolla $\overline{a} \in \mathbf{Z}_m$ on käänteisalkio.

Lause 2.8.2 *Alkiolla* $\overline{a}$ *on käänteisalkio monoidissa* $(\mathbf{Z}_m, \cdot)$*, jos ja vain jos* $(a, m) = 1$*.*

Todistus Alkiolla $\overline{a}$ on käänteisalkio silloin ja vain silloin, kun yhtälö $\overline{a} \cdot \overline{x} = \overline{1}$ on ratkeava. Yhtälö $\overline{a} \cdot \overline{x} = \overline{1}$ voidaan kirjoittaa $\overline{ax} = \overline{1}$ eli $ax \equiv 1 \pmod{m}$, joka on ratkeava, jos ja vain jos $(a, m) \mid 1$ eli $(a, m) = 1$. □

Merkintä Merkitään symbolilla $\mathbf{Z}_m^*$ niiden monoidin $(\mathbf{Z}_m, \cdot)$ alkioiden joukkoa, joilla on käänteisalkio, ts.

$$\mathbf{Z}_m^* = \{\overline{a} \in \mathbf{Z}_m |\ (a, m) = 1\}\,.$$

Huomautus Ehdon $(a, m) = 1$ toteutuminen ei riipu jäännösluokan $\overline{a}$ edustajan valinnasta. Nimittäin jos $b \in \overline{a}$, niin $a \equiv b \pmod{m}$ ja siis $(a, m) = (b, m)$.

Määritelmä Joukon $\mathbf{Z}_m^*$ alkioita sanotaan *alkuluokiksi* modulo m.

Esimerkki 2.8.3 $\mathbf{Z}_9^* = \left\{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\right\}$.

Esimerkki 2.8.4 Jos p on alkuluku, niin $\mathbf{Z}_p^* = \left\{\overline{1}, \overline{2}, \ldots, \overline{p-1}\right\}$.

Esimerkki 2.8.5 Mikä on alkion $\overline{2}$ käänteisalkio monoidissa $(\mathbf{Z}_9, \cdot)$?

Ratkaisu Käänteisalkio on sellainen $\overline{x}$, että $\overline{2}\overline{x} = \overline{1}$. On helppo todeta, että $\overline{x} = \overline{5}$. Siis $\overline{2}^{-1} = \overline{5}$.

Lause 2.8.3 *Pari* $(\mathbf{Z}_m^*, \cdot)$ *on Abelin ryhmä.*

Todistus Todistetaan, että 1) kertolasku on laskutoimitus, 2) ykkösalkio kuuluu joukkoon $\mathbf{Z}_m^*$ ja 3) jokaisen alkion käänteisalkio kuuluu joukkooon $\mathbf{Z}_m^*$. Muut vaatimukset on jo todettu.

1) Olkoot $\overline{a}$, $\overline{b} \in \mathbf{Z}_m^*$. Silloin $\overline{a} \cdot \overline{b}$ on olemassa ja on hyvin määritelty. (Itse asiassa $\overline{a} \cdot \overline{b} = \overline{ab}$.) Lisäksi kertolasku on sulkeutuva eli $\overline{a} \cdot \overline{b} \in \mathbf{Z}_m^*$. Nimittäin, koska $(a, m) = (b, m) = 1$, niin $(ab, m) = 1$. Näin ollen $\overline{ab} \in \mathbf{Z}_m^*$ eli $\overline{a} \cdot \overline{b} \in \mathbf{Z}_m^*$.

2) Ykkösalkio on $\overline{1}$, sillä $\overline{a} \cdot \overline{1} = \overline{a1} = \overline{a}$ aina, kun $\overline{a} \in \mathbf{Z}_m^*$. Edelleen $\overline{1} \in \mathbf{Z}_m^*$, sillä $(1, m) = 1$.

3) Olkoon $\overline{a} \in \mathbf{Z}_m^*$ ja $\overline{a}^{-1} = \overline{x}$. Silloin yhtälö $\overline{a} \cdot \overline{x} = \overline{1}$ on ratkeava alkion $\overline{x}$ suhteen. Toisaalta yhtälö on myös ratkeava alkion $\overline{a}$ suhteen. Siis lauseen 2.8.2 mukaan $(x, m) = 1$, joten $\overline{x} \in \mathbf{Z}_m^*$. □

Määritelmä Ryhmää $(\mathbf{Z}_m^*, \cdot)$ sanotaan alkuluokkaryhmäksi $\pmod m$.

Esimerkki 2.8.6 Ratkaise yhtälöt a) $\overline{3}\overline{x} = \overline{1}$, b) $(\overline{x})^3 = \overline{1}$, c) $(\overline{x})^2 = \overline{3}$ ryhmässä $(\mathbf{Z}_4^*, \cdot)$.

Ratkaisu a) $\overline{x} = \overline{3}$, b) $\overline{x} = \overline{1}$, c) ei ratkaisua.

2.9 Aliryhmä

Määritelmä Olkoon $(G, \star)$ ryhmä ja H joukon G ei-tyhjä osajoukko. Silloin $(H, \star)$ on ryhmän $(G, \star)$ *aliryhmä*, jos $(H, \star)$ on ryhmä.

Merkintä Jos $(H, \star)$ on ryhmän $(G, \star)$ aliryhmä, niin merkitään $(H, \star) \leq (G, \star)$ tai lyhyesti $H \leq G$.

Lause 2.9.1 (Aliryhmäkriteeri) *Olkoon $(G, \star)$ ryhmä ja H joukon G ei-tyhjä osajoukko. Silloin $H \leq G$, jos ja vain jos*

$$\forall a, b \in H \colon a \star b^{-1} \in H. \tag{1}$$

Todistus Sivuutetaan.

Esimerkki 2.9.1 Selvästi $(\mathbf{Z}, +) \leq (\mathbf{R}, +)$.

Esimerkki 2.9.2 Merkitään $m\mathbf{Z} = \{mk \colon k \in \mathbf{Z}\}$. Silloin $(m\mathbf{Z}, +) \leq (\mathbf{Z}, +)$.

Esimerkki 2.9.3 Olkoot $(A, \star)$ ja $(B, \star)$ ryhmän $(G, \star)$ aliryhmiä. Todista, että $(A \cap B, \star)$ on ryhmän $(G, \star)$ aliryhmä.

Todistus Olkoot a, $b \in A \cap B$ mielivaltaisia. Silloin a, $b \in A$ ja a, $b \in B$. Koska A, $B \leq G$, niin lauseen 2.9.1 perusteella $a \star b^{-1} \in A$ ja $a \star b^{-1} \in B$. Siis $a \star b^{-1} \in A \cap B$. Lisäksi $A \cap B \neq \emptyset$, sillä ainakin $e \in A \cap B$, missä e on ryhmän neutraalialkio, ja $A \cap B \subseteq G$, sillä $A \subseteq G$ ja $B \subseteq G$. Näin ollen lauseen 2.9.1 perusteella $A \cap B \leq G$. □

Määritelmä Ryhmää $(G, \star)$ sanotaan *äärelliseksi*, jos joukossa G on äärellinen määrä alkioita.

Lause 2.9.2 (Aliryhmäkriteeri äärellisille ryhmille) *Olkoon $(G, \star)$ äärellinen ryhmä ja H joukon G ei-tyhjä osajoukko. Silloin $H \leq G$, jos ja vain jos*

$$\forall a, b \in H \colon a \star b \in H. \tag{2}$$

Todistus Sivuutetaan.

Esimerkki 2.9.4 $(\{\overline{0}, \overline{3}\}, +) \leq (\mathbf{Z}_6, +)$. (Totea!)

Esimerkki 2.9.5 $(\{\overline{0}, \overline{4}\}, +) \not\leq (\mathbf{Z}_6, +)$. (Totea!)

3 Kahden laskutoimituksen struktuureja

Luvussa 2 tutkittiin yhden laskutoimituksen struktuureja $(A, \star)$, joista ryhmä on keskeisin. Monissa joukoissa on kuitenkin useita mielekkäitä laskutoimituksia, esimerkiksi lukujoukoissa **Z**, **Q** ja **R** tavallinen yhteen- ja kertolasku.

Tässä luvussa tarkastellaan yleisiä kahden laskutoimituksen struktuureja $(R, +, \cdot)$, siis joukkoa R, kahta laskutoimitusta $+$ ja $\cdot$ sekä niiden keskinäisiä suhteita. Laskutoimitukset $+$ ja $\cdot$ ovat yleisiä, mutta $+$ on yleensä tavallisen yhteenlaskun kaltainen laskutoimitus ja $\cdot$ tavallisen kertolaskun kaltainen laskutoimitus.

Laskutoimituksista $+$ ja $\cdot$ käytetään kuitenkin nimityksiä yhteenlasku ja kertolasku. Jos on vaarana sekaannus tavanomaisiin yhteen- ja kertolaskuihin, voi käyttää esimerkiksi merkintöjä $\oplus$ ja $\odot$.

Kahden laskutoimituksen struktuurien tutkimisen aloitamme renkaan käsitteestä. Muita tarkasteltavia struktuureja ovat kokonaisalue ja kunta.

3.1 Renkaan määritelmä

Määritelmä Kolmikko $(R, +, \cdot)$ on *rengas*, jos

1) $(R, +)$ on Abelin ryhmä,

2) $(R, \cdot)$ on puoliryhmä,

3) $a(b + c) = ab + ac \quad \forall a,\, b,\, c \in R,$
$(a + b)c = ac + bc \quad \forall a,\, b,\, c \in R$
eli osittelulait ovat voimassa.

Huomautus Kertolaskun symboli $\cdot$ jätetään usein merkitsemättä.

Huomautus Ehto 3) antaa yhteyden struktuurien $(R, +)$ ja $(R, \cdot)$ välille. Ilman sitä struktuurit $(R, +)$ ja $(R, \cdot)$ olisivat toisistaan riippumattomia.

Määritelmä Rengasta $(R, +, \cdot)$ sanotaan *kommutatiiviseksi*, jos kertolasku $\cdot$ on kommutatiivinen.

Määritelmä Jos puoliryhmä $(R, \cdot)$ on monoidi, niin rengas on 1–rengas (eli *ykkösrengas*). Monoidin $(R, \cdot)$ neutraalialkiota sanotaan *ykkösalkioksi* ja sitä merkitään symbolilla 1.

Määritelmä Ryhmän $(R, +)$ neutraalialkiota sanotaan *nolla-alkioksi* ja merkitään symbolilla 0.

Esimerkki 3.1.1 Joukot **Z**, **Q**, **R** ja **C** varustettuina tavallisilla yhteen- ja kertolaskuilla ovat kommutatiivisia 1–renkaita.

Esimerkki 3.1.2 Kolmikko $(\mathbf{Z}_m, +, \cdot)$ on kommutatiivinen 1–rengas. (Totea!)

Esimerkki 3.1.3 Kolmikko $(M_{n\times n}, +, \cdot)$ on 1–rengas.

Esimerkki 3.1.4 Olkoon $(G, +)$ Abelin ryhmä. Merkitään

$$\mathrm{Hom}(G, G) = \{f|\ f\colon G \to G \text{ on homomorfismi}\}.$$

Silloin $(\mathrm{Hom}(G, G), +, \circ)$ on 1–rengas. (Totea!)

Esimerkki 3.1.5 Tutkitaan algebrallista struktuuria $(\mathbf{R}, \oplus, \odot)$, missä $a \oplus b = a+b+1$ ja $a \odot b = a + b + ab$. Osittelulait ovat voimassa, sillä

$$\begin{aligned} a \odot (b \oplus c) &= a \odot (b + c + 1) = a + (b + c + 1) + a(b + c + 1) \\ &= (a + b + ab) + (a + c + ac) + 1 = (a + b + ab) \oplus (a + c + ac) \\ &= (a \odot b) \oplus (a \odot c) \end{aligned}$$

ja

$$\begin{aligned} (a \oplus b) \odot c &= (a + b + 1) \odot c = (a + b + 1) + c + (a + b + 1)c \\ &= (a + c + ac) + (b + c + bc) + 1 = (a + c + ac) \oplus (b + c + bc) \\ &= (a \odot c) \oplus (b \odot c) \end{aligned}$$

aina, kun $a, b, c \in \mathbf{R}$. Algebrallisen struktuurin $(\mathbf{R}, \oplus, \odot)$ nolla-alkio on reaaliluku -1, sillä

$$a \oplus (-1) = a + (-1) + 1 = a \quad \text{ja} \quad (-1) \oplus a = (-1) + a + 1 = a$$

aina, kun $a \in \mathbf{R}$. Edelleen algebrallisen struktuurin $(\mathbf{R}, \oplus, \odot)$ ykkösalkio on reaaliluku 0, sillä

$$a \odot 0 = a + 0 + a0 = a \quad \text{ja} \quad 0 \odot a = 0 + a + 0a = a$$

aina, kun $a \in \mathbf{R}$. Alkion $a \in \mathbf{R}$ vasta-alkio on $-a - 2$, sillä

$$a \oplus (-a - 2) = a + (-a - 2) + 1 = -1 \quad \text{ja} \quad (-a - 2) \oplus a = (-a - 2) + a + 1 = -1,$$

missä -1 on siis struktuurin nolla-alkio.

3.2 Renkaan perusominaisuuksia

Laskulakeja

Lause 3.2.1 *Olkoon $(R, +, \cdot)$ rengas ja olkoot a, b, $c \in R$. Silloin*

1) $0a = a0 = 0$,

2) $a(-b) = (-a)b = -(ab)$,

3) $-(-a) = a$,

4) $(-a)(-b) = ab$,

5) $a(b-c) = ab - ac$, $(a-b)c = ac - bc$,
missä $a - b = a + (-b)$.

Todistus 1) Osittelulain ja nolla-alkion määritelmän nojalla

$$0a + 0a = (0+0)a = 0a = 0 + 0a,$$

joten ryhmän $(R, +)$ supistussäännön perusteella $0a = 0$. Yhtälö $a0 = 0$ todistetaan samalla tavalla. (Totea!)
2) Osittelulain, vasta-alkion määritelmän ja kohdan 1) nojalla

$$a(-b) + ab = a\,[(-b) + b] = a0 = 0.$$

Siis $a(-b) + ab = 0$, joten $a(-b)$ on alkion ab vasta-alkio eli $a(-b) = -(ab)$. Yhtälö $(-a)b = -(ab)$ todistetaan samalla tavalla.
3) Kaava on voimassa yleisesti ryhmässä (huomaa additiivinen merkintä).
4) Seuraa kohdista 2) ja 3). (Totea!)
5) Seuraa osittelulaista ja kohdasta 2). □

Seuraus Jos $(R, +, \cdot)$ on 1–rengas ja $|R| \geq 2$, niin $0 \neq 1$.

Todistus Tehdään vastaoletus: $0 = 1$. Silloin $1a = 0a$ aina, kun $a \in R$. Siis ykkösalkion määritelmän ja lauseen 3.2.1 kohdan 1) nojalla $a = 0$ aina, kun $a \in R$, joten $R = \{0\}$. Näin ollen $|R| = 1 < 2$. Täten vastaoletus $0 = 1$ on väärin ja väite $0 \neq 1$ on oikein. □

Seuraus Olkoon $(R, +, \cdot)$ rengas, jossa

$$a + b = a \cdot b \quad \forall a, b \in R. \tag{1}$$

Silloin $R = \{0\}$.

Todistus Olkoon $a \in R$ mielivaltainen ja asetetaan b nolla-alkioksi 0. Silloin oletuksen (1) mukaan $a + 0 = a0$. Nyt nolla-alkion määritelmän ja lauseen 3.2.1 nojalla $a = 0$. Siis $R = \{0\}$. □

Monikerta ja potenssi

Monikerralla renkaassa $(R, +, \cdot)$ tarkoitetaan monikertaa ryhmässä $(R, +)$. Pykälän 2.4 mukaan monikerta na, $n \in \mathbf{Z}$, on mielekäs ryhmässä. Huomaa, että tässä käytetään additiivista terminologiaa, kun taas pykälässä 2.4 käytetään multiplikatiivista terminologiaa. Pykälän 2.4 lauseet ovat voimassa renkaan monikerralle.

Potenssilla renkaassa $(R, +, \cdot)$ tarkoitetaan potenssia puoliryhmässä $(R, \cdot)$. Renkaan potenssi a^n on mielekäs, kun $n \in \mathbf{Z}^+$. Pykälän 2.4 lauseet ovat rajoitetusti voimassa renkaan potenssille.

Esitetään tässä esimerkki, jossa tarkastellaan samanaikaisesti monikertaa ja potenssia.

Esimerkki 3.2.1 Olkoon $(R, +, \cdot)$ rengas. Silloin

$$(a+b)^2 = a^2 + 2(ab) + b^2 \quad \forall a, b \in R, \tag{2}$$

jos ja vain jos R on kommutatiivinen rengas.

Todistus "$\Leftarrow$" Oletetaan, että R on kommutatiivinen rengas. Silloin potenssin määritelmän ja osittelulakien nojalla

$$\begin{aligned}(a+b)^2 &= (a+b)(a+b) = a(a+b) + b(a+b) \\ &= a^2 + ab + ba + b^2.\end{aligned}$$

Kun viimeisimpään lausekkeeseen sovelletaan renkaan kommutatiivisuutta ja monikerran määritelmää, niin saadaan

$$(a+b)^2 = a^2 + ab + ab + b^2 = a^2 + 2(ab) + b^2.$$

Siis suunta "$\Leftarrow$" on todistettu. Suunta "$\Rightarrow$" jätetään harjoitustehtäväksi. $\square$

Supistussäännöistä

Todistetaan, että renkaassa on voimassa

1) $ab = ac \not\Rightarrow b = c$,

2) $ab = ac$, $a \neq 0 \not\Rightarrow b = c$,

3) $a + b = a + c \Rightarrow b = c$.

Kohta 1 Esimerkiksi renkaassa $(\mathbf{Z}, +, \cdot)$ $0 \cdot 1 = 0 \cdot 2$ mutta $1 \neq 2$.

Kohta 2 Esimerkiksi renkaassa $(M_{2\times 2}, +, \cdot)$

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

ja $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ ei ole nollamatriisi, mutta

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

Kohta 3 Renkaassa $(R, +, \cdot)$ voidaan supistaa yhteenlaskun suhteen, sillä $(R, +)$ on ryhmä ja ryhmässä supistussääntö on voimassa.

3.3 Alirengas

Määritelmä Kolmikko $(S, +, \cdot)$ on renkaan $(R, +, \cdot)$ *alirengas*, jos $\emptyset \neq S \subseteq R$ ja $(S, +, \cdot)$ on rengas.

Huomautus Yllä alirenkaan $(S, +, \cdot)$ laskutoimitukset ovat samat kuin renkaan $(R, +, \cdot)$ laskutoimitukset.

Esimerkki 3.3.1 Rengas $(\mathbf{Z}_3, +, \cdot)$ ei ole renkaan $(\mathbf{Z}_4, +, \cdot)$ alirengas. (Miksi?)

Lause 3.3.1 (Alirengaskriteeri) *Olkoon $(R, +, \cdot)$ rengas ja S joukon R ei-tyhjä osajoukko. Silloin $(S, +, \cdot)$ on renkaan $(R, +, \cdot)$ alirengas, jos ja vain jos*

1) *S on sulkeutuva vähennyslaskun suhteen,*

2) *S on sulkeutuva kertolaskun suhteen.*

Todistus Harjoitustehtävä.

Esimerkki 3.3.2 Rengas $(\mathbf{Z}, +, \cdot)$ on renkaan $(\mathbf{R}, +, \cdot)$ alirengas.

Esimerkki 3.3.3 Kolmikko $(M^*_{n\times n}, +, \cdot)$ ei ole renkaan $(M_{n\times n}, +, \cdot)$ alirengas. (Miksi?)

Esimerkki 3.3.4 Kolmikko $(M'_{n\times n}, +, \cdot)$ on renkaan $(M_{n\times n}, +, \cdot)$ alirengas, missä $M'_{n\times n}$ on $n \times n$–diagonaalimatriisien joukko.

Esimerkki 3.3.5 Merkitään $\mathbf{Z}(i) = \{a + bi |\ a, b \in \mathbf{Z}\}$. (Tämä on niin sanottujen *Gaussin kokonaislukujen* joukko.) Silloin $(\mathbf{Z}(i), +, \cdot)$ on renkaan $(\mathbf{C}, +, \cdot)$ alirengas. (Totea!)

3.4 Renkaan nollanjakajat

Määritelmä Olkoon $(R, +, \cdot)$ rengas. Silloin $a \in R$ on *nollanjakaja*, jos

1) $a \neq 0$ ja

2) $\exists b \in R \setminus \{0\} : ab = 0$ tai $ba = 0$.

Huomautus Yllä olevassa määritelmässä myös alkio b on nollanjakaja.

Esimerkki 3.4.1 Lukurenkaissa ei ole nollanjakajia, kun laskutoimituksina ovat tavalliset yhteen- ja kertolasku. (Miksi yhteenlaskulla on merkitystä nollanjakajien olemassaoloon?)

Esimerkki 3.4.2 Renkaassa $(M_{2\times 2}, +, \cdot)$ on nollanjakajia. Esimerkiksi

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Esimerkki 3.4.3 Renkaan $(\mathbf{Z}_4, +, \cdot)$ ainoa nollanjakaja on $\overline{2}$. (Totea!)

Esimerkki 3.4.4 Renkaassa $(\mathbf{Z}_3, +, \cdot)$ ei ole nollanjakajia. (Totea!)

Lause 3.4.1 *Alkio $\overline{a}$ $(\neq \overline{0})$ on renkaan $(\mathbf{Z}_m, +, \cdot)$ nollanjakaja, jos ja vain jos $(a, m) > 1$.*

Todistus Olkoon $\overline{a} \neq \overline{0}$. Silloin $\overline{a}$ on nollanjakaja, jos ja vain jos yhtälöllä $\overline{a}\,\overline{x} = \overline{0}$ on ratkaisu $\overline{x} \neq \overline{0}$ eli kongruenssiyhtälöllä $ax \equiv 0 \pmod{m}$ on ratkaisu $x \not\equiv 0 \pmod{m}$. Yhtälön $ax \equiv 0 \pmod{m}$ kaikki ratkaisut ovat $x \equiv 0 \pmod{m/(a, m)}$. Siis ratkaisu $x \not\equiv 0 \pmod{m}$ löytyy, jos ja vain jos $(a, m) > 1$. □

Seuraus Renkaassa $(\mathbf{Z}_p, +, \cdot)$ ei ole nollanjakajia, kun p on alkuluku.

Esimerkki 3.4.5 Renkaan $(\mathbf{Z}_9, +, \cdot)$ nollanjakajat ovat $\overline{3}$ ja $\overline{6}$. (Totea!)

Lause 3.4.2 *Olkoon $(R, +, \cdot)$ 1–rengas. Jos $a \in R$ on kääntyvä (kertolaskun suhteen), niin a ei ole nollanjakaja.*

Todistus Olkoon $ab = 0$. Silloin $a^{-1}(ab) = a^{-1}0$. Tästä saadaan helposti, että $b = 0$. (Totea!) Samalla tavalla todistetaan, että jos $ba = 0$, niin $b = 0$. Siis a ei ole nollanjakaja. □

Esimerkki 3.4.6 Renkaan $(M_{n\times n}, +, \cdot)$ matriisit, joiden determinantti on $\neq 0$, eivät ole nollanjakajia.

Huomautus Lause 3.4.2 ei pidä paikkaansa käänteisesti (vaikka oletettaisiin, että $a \neq 0$). Esimerkiksi renkaassa $(\mathbf{Z}, +, \cdot)$ luvut a $(\neq 0, \pm 1)$ eivät ole nollanjakajia eivätkä kääntyviä.

3.5 Kokonaisalue

Määritelmä Kommutatiivista 1–rengasta, jossa ei ole nollanjakajia, sanotaan *kokonaisalueeksi*. Kokonaisaluetta merkitään usein kolmikolla $(D, +, \cdot)$.

Esimerkki 3.5.1 Lukurenkaat $(\mathbf{Z}, +, \cdot)$, $(\mathbf{Q}, +, \cdot)$, $(\mathbf{R}, +, \cdot)$ ja $(\mathbf{C}, +, \cdot)$ ovat kokonaisalueita.

Esimerkki 3.5.2 Rengas $(M_{n\times n}, +, \cdot)$ ei ole kokonaisalue, kun $n > 1$. (Miksi?)

Lause 3.5.1 *Rengas* $(\mathbf{Z}_m, +, \cdot)$ *on kokonaisalue, jos ja vain jos* m *on alkuluku.*

Todistus "$\Leftarrow$" On jo itse asiassa todistettu. (Miksi?)
"$\Rightarrow$" Oletetaan, että rengas $(\mathbf{Z}_m, +, \cdot)$ on kokonaisalue. Silloin siinä ei ole nollanjakajia. Siis lauseen 3.4.1 mukaan $(a, m) = 1$ aina, kun $\overline{a} \neq \overline{0}$ eli aina, kun $a = 1, 2, \ldots, m-1$. Näin ollen m on alkuluku. □

Supistussäännöistä

Todistetaan, että kokonaisalueessa on voimassa

1) $ab = ac \not\Rightarrow b = c$,

2) $ab = ac$, $a \neq 0 \Rightarrow b = c$,

3) $a + b = a + c \Rightarrow b = c$.

Kohta 1 Esimerkiksi kokonaisalueessa $(\mathbf{Z}, +, \cdot)$ $0 \cdot 1 = 0 \cdot 2$ mutta $1 \neq 2$.

Kohta 2 Harjoitustehtävä.

Kohta 3 Kokonaisalueessa $(D, +, \cdot)$ voidaan supistaa yhteenlaskun suhteen, sillä $(D, +)$ on ryhmä ja supistamissääntö on voimassa ryhmässä.

Huomautus Kohdassa 2) alkiolla a ei välttämättä ole käänteisalkiota. Siitä huolimatta se voidaan supistaa pois.

Harjoitus Todista, että kokonaisalueessa

1) yhtälöllä $ax = b$ voi olla ääretön määrä ratkaisuja,

2) yhtälöllä $ax = b$, $a \neq 0$, on korkeintaan 1 ratkaisu,

3) yhtälöllä $a + x = b$ on täsmälleen 1 ratkaisu.

3.6 Kunta

Määritelmä Kommutatiivinen 1–rengas $(F, +, \cdot)$ on *kunta*, jos jokaisella joukon $F \setminus \{0\}$ alkiolla on käänteisalkio.

Esimerkki 3.6.1 Lukurenkaat $(\mathbf{Q}, +, \cdot)$, $(\mathbf{R}, +, \cdot)$ ja $(\mathbf{C}, +, \cdot)$ ovat kuntia. Lukurengas $(\mathbf{Z}, +, \cdot)$ ei ole kunta.

Esimerkki 3.6.2 Kunta $(\mathbf{Q}, +, \cdot)$ on suppein lukukunta ($\neq \{0\}$). (Totea!)

Lause 3.6.1 *Olkoon* $|F| \geq 2$. *Silloin* $(F, +, \cdot)$ *on kunta, jos ja vain jos*

1) $(F, +)$ *on Abelin ryhmä,*

2) $(F \setminus \{0\}, \cdot)$ *on Abelin ryhmä,*

3) *osittelulait ovat voimassa.*

Todistus Harjoitustehtävä.

Lause 3.6.2 *Jokainen kunta on kokonaisalue.*

Todistus Seuraa lauseesta 3.4.2. □

Lause 3.6.3 *Jokainen äärellinen kokonaisalue on kunta.*

Todistus Olkoon $(F, +, \cdot)$ äärellinen kokonaisalue ja merkitään $F = \{0, k_1, k_2, \ldots, k_n\}$. Todistetaan, että $(F, +, \cdot)$ on kunta. Kokonaisalueen ja kunnan määritelmien nojalla riittää todistaa, että alkiolla x on käänteisalkio aina, kun $x \neq 0$, ts. että jokin tuloista xk_i ($i = 1, 2, \ldots, n$) on $= 1$. Tuloilla xk_i on seuraavat kaksi ominaisuutta.

1) Kaikki tulot xk_i ovat $\neq 0$, sillä kokonaisalueessa ei ole nollanjakajia.

2) Kaikki tulot xk_i ovat erisuuria. Nimittäin jos $xk_s = xk_r$, niin $x(k_s - k_r) = 0$. Koska tässä $x \neq 0$, niin $k_s - k_r = 0$ eli $k_s = k_r$.

Kohtien 1) ja 2) nojalla tulot xk_i ($i = 1, 2, \ldots, n$) käyvät läpi kaikki joukon F nollasta poikkeavat alkiot, siis myös alkion 1. Näin ollen on olemassa sellainen t, että $xk_t = 1$. Koska rengas on kommutatiivinen, niin myös $k_t x = 1$. Täten alkiolla x on käänteisalkio k_t. Näin olemme todistaneet, että $(F, +, \cdot)$ on kunta. □

Lause 3.6.4 *Kolmikko* $(\mathbf{Z}_m, +, \cdot)$ *on kunta, jos ja vain jos* m *on alkuluku.*

Todistus Seuraa lauseista 3.5.1, 3.6.2 ja 3.6.3. □

Huomautus Jos F on äärellinen kunta, niin $|F| = p^n$, $p \in \mathbf{P}$. Todistus ei kuulu tämän monisteen alueeseen.

3.7 Osamäärä kunnassa

Määritelmä Olkoon $(F, +, \cdot)$ kunta ja olkoot a, $b \in F$, $b \neq 0$. Silloin *osamäärä* a/b määritellään kaavalla

$$\frac{a}{b} = ab^{-1}.$$

Huomautus 1) Koska $b \neq 0$, niin yllä olevassa määritelmässä käänteisalkio b^{-1} on olemassa.

2) Koska kertolasku on kommutatiivinen, niin $ab^{-1} = b^{-1}a$.

Näin ollen osamäärän määritelmä on mielekäs.

Lause 3.7.1 *Oletetaan, että* b, $d \neq 0$. *Silloin*

1) $\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc$,

2) $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$,

3) $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$,

4) $\frac{-a}{-b} = \frac{a}{b}$.

Todistus Todistetaan kohta 3) ja jätetään muut kohdat harjoitustehtäviksi. Ilmeisesti

$$\begin{aligned} \frac{a}{b} + \frac{c}{d} &= ab^{-1} + cd^{-1} = ab^{-1}dd^{-1} + cd^{-1}bb^{-1} \\ &= ad(bd)^{-1} + bc(bd)^{-1} \\ &= (ad + bc)(bd)^{-1} \\ &= \frac{ad + bc}{bd}. \end{aligned}$$

(Millä perusteella mikin vaihe on voimassa?) □

Esimerkki 3.7.1 Oletetaan, että $(F, +, \cdot)$ on kunta, $a, b, c \in F$ ja $n \in \mathbf{Z}$. Todista, että

1) $\frac{na}{b} = n\frac{a}{b}$,

2) $\frac{ca}{b} = c\frac{a}{b}$.

Ratkaisu 1) Todistetaan kohta 1), kun $n \in \mathbf{Z}^+$. Tapaus $n \notin \mathbf{Z}^+$ jätetään harjoitustehtäväksi. Ilmeisesti

$$\begin{aligned} \frac{na}{b} &= (na)b^{-1} = (a + a + \cdots + a)b^{-1} \\ &= ab^{-1} + ab^{-1} + \cdots + ab^{-1} = n(ab^{-1}) \\ &= n\frac{a}{b}. \end{aligned}$$

(Millä perusteella mikin vaihe on voimassa?)

2) Osamäärän määritelmän ja kertolaskun assosiatiivisuuden nojalla

$$\frac{ca}{b} = (ca)b^{-1} = c(ab^{-1}) = c\frac{a}{b}.$$