802354A Lukuteoria ja ryhmät

Luentorunko

Kevät 2014

Työryhmä: Markku Niemenmaa, Kari Myllylä,
Juha-Matti Tirilä, Antti Torvikoski, Topi Törmä

Sisältö

1 Ekvivalenssirelaatio

Määritelmä 1.1. Olkoon A ei-tyhjä joukko. Tällöin joukkoa

$$A \times A = \{(a_1, a_2) \mid a_1, a_2 \in A\}$$

kutsutaan *joukon A karteesiseksi tuloksi itsensä kanssa.*

Määritelmä 1.2. Joukon $A \times A$ osajoukkoa R sanotaan *binääriseksi relaatioksi* joukossa A. Jos pari $(x, y) \in R$, niin merkitään $x\,R\,y$ ja sanotaan, että alkio x on relaatiossa R alkion y kanssa.

Määritelmä 1.3. Joukon A binäärinen relaatio R on *ekvivalenssirelaatio*, mikäli

1. $x\,R\,x$ aina, kun $x \in A$ (refleksiivisyys);
2. $x\,R\,y \Rightarrow y\,R\,x$ aina, kun $x, y \in A$ (symmetrisyys);
3. $x\,R\,y$ ja $y\,R\,z \Rightarrow x\,R\,z$ aina, kun $x, y, z \in A$ (transitiivisuus).

Jos R on ekvivalenssirelaatio ja $a \in A$, niin joukkoa

$$[a] = \{x \in A \mid x\,R\,a\}$$

sanotaan *alkion a määräämäksi ekvivalenssiluokaksi.*

Lause 1.4. *Jos R on ekvivalenssirelaatio ja $a\,R\,b$, niin $[a] = [b]$.*

Todistus. Luennolla.

Huomautus. Jos $[a] = [b]$, niin $a\,R\,b$.

Lause 1.5. *Jos R on joukon A ekvivalenssirelaatio, niin kaikkien ekvivalenssiluokkien yhdiste (unioni) on koko joukko A. Lisäksi, jos $[a] \neq [b]$, niin $[a] \cap [b] = \emptyset$.*

Todistus. Luennolla.

Huomautus. Joukon A alkioiden lukumäärää merkitään $|A|$.

2 Lukuteoriaa

Merkintöjä lukujoukoille:

- *Luonnolliset luvut* (natural numbers):

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

- *Kokonaisluvut* (integers):

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$$

- *Positiiviset kokonaisluvut* (positive integers):

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

2.1 Lukuteorian alkeita

Määritelmä 2.1. Joukko S on *hyvin järjestetty* (well-ordered), jos ja vain jos sen jokaisessa epätyhjässä osajoukossa on pienin alkio.

Huomautus. Joukko $\mathbb{N}$ on hyvin järjestetty.

Lause 2.2. *Jos $a, b \in \mathbb{Z}$ ja $b \neq 0$, niin on olemassa sellaiset yksikäsitteisesti määrätyt kokonaisluvut q ja r, että $a = qb + r$, missä $0 \leq r < |b|$.*

Todistus. Luennolla.

Huomautus. Yhtälöä $a = qb + r$, missä $0 \leq r < |b|$, sanotaan *jakoyhtälöksi* (jakoalgoritmi, division algorithm). Edelleen, ko. yhtälössä a on *jaettava*, b *jakaja*, q *osamäärä* ja r *jakojäännös*.

Lukujärjestelmät

1. Kymmenjärjestelmä (positive integers expressed in base 10); kantaluku 10 ja numerot 0,1,2,. . . ,9.

Esim.
$$478_{10} = 4 \cdot 10^2 + 7 \cdot 10^1 + 8 \cdot 10^0.$$

2. Binäärijärjestelmä; kantaluku 2 ja numerot 0 ja 1.
   Esim.
$$17_{10} = 10001_2.$$

3. 8-järjestelmä; kantaluku 8 ja numerot $0, 1, 2, \ldots, 7$.
   Esim.
$$17_{10} = 21_8.$$

Määritelmä 2.3. Jos $a, b \in \mathbb{Z}$ ja on olemassa sellainen luku $k \in \mathbb{Z}$, että $b = ka$, niin *a jakaa luvun b*. Tästä käytetään merkintää $a \mid b$. Jos a ei jaa lukua b, niin merkitään $a \nmid b$. Edelleen, jos $a \mid b$, niin lukua a kutsutaan luvun b *tekijäksi*.

Lause 2.4. *Olkoon $a, b, c \in \mathbb{Z}$. Tällöin*

1. $\pm 1 \mid a$ *ja* $\pm a \mid a$,
2. $a \mid 0$,
3. *jos* $0 \mid a$, *niin* $a = 0$,
4. *jos* $a \mid 1$, *niin* $a = \pm 1$,
5. *jos* $a \mid b$ *ja* $b \mid a$, *niin* $a = \pm b$,
6. *jos* $a \mid b$ *ja* $b \mid c$, *niin* $a \mid c$,
7. *jos* $a \mid b$ *ja* $a \mid c$, *niin* $a \mid (b + c)$ *ja* $a \mid (b - c)$,
8. *jos* $a \mid b$ *ja* $a \mid c$, *niin* $a \mid (mb + nc)$ *kaikilla* $m, n \in \mathbb{Z}$,
9. *jos* $a \mid b$ *ja* $a \mid c$, *niin* $a^2 \mid bc$,
10. *jos* $a \mid b$, *niin* $a \mid b^n$ *ja* $a^n \mid b^n$ *kaikilla* $n \in \mathbb{Z}_+$,
11. *jos* $a \mid b$ *ja* $a \mid (b + c)$, *niin* $a \mid c$,
12. *jos* $a \mid b$, *niin* $ma \mid mb$ *kaikilla* $m \in \mathbb{Z}$,
13. *jos* $m \in \mathbb{Z} \setminus \{0\}$ *ja* $ma \mid mb$, *niin* $a \mid b$.

Todistus. Luennolla.

Määritelmä 2.5. Jos $n \in \mathbb{Z}$ ja luvun n ainoat tekijät ovat ± 1 ja $\pm n$, niin n on *jaoton* luku.

Määritelmä 2.6. Jos $p \in \mathbb{N}$, $p \geq 2$ ja luvulla p ei ole muita tekijöitä kuin ± 1 ja $\pm p$, niin lukua p sanotaan *alkuluvuksi* (prime number). Jos luku $n \in \mathbb{Z}$ voidaan esittää muodossa $n = ab$, missä $a, b \in \mathbb{Z}$ ja $|a|, |b| \geq 2$, niin sanotaan, että n on *yhdistetty luku* (composite number).

Lause 2.7. *Jos $a \in \mathbb{N}$, $a \geq 2$, niin a voidaan esittää alkulukujen tulona.*

Todistus. Luennolla.

Huomautus.

- Alkulukuja on äärettömän monta. Tämä todistetaan esim. vastaoletuksen avulla.
- Lauseen 2.2 nojalla jokainen kokonaisluku on jotain seuraavista muodoista:
$$4q \qquad 4q+1 \qquad 4q+2 \qquad 4q+3,$$
missä $q \in \mathbb{Z}$. Koska $4q$ ja $4q+2$ ovat parillisia, niin parittomat alkuluvut ovat tämän nojalla muotoa $4k+1$ $(5, 13, 17, \ldots)$ tai muotoa $4k+3$ $(3, 7, 11, 19, \ldots)$.
- Alkulukua, joka on muotoa $2^{2^n}+1$, $n = 0, 1, 2, \ldots$, sanotaan *Fermat'n alkuluvuksi* (Fermat prime; Pierre de Fermat 1601 – 1665).
- Alkulukua, joka on muotoa $2^n - 1$, $n = 0, 1, 2, \ldots$ sanotaan *Mersennen alkuluvuksi* (Mersenne prime; Marim Mersenne 1588 – 1648). Tämän tyyppisiin lukuihin liittyy seuraava tulos: jos $2^n - 1$ on alkuluku, niin myös n on alkuluku (todistus harjoitustehtävänä). Käänteinen väite ei kuitenkaan pidä paikkaansa!
- Eräs lukuteorian avoimista ongelmista on ns. *Goldbachin väittämä* (Christian Goldbach 1690 – 1764): Jos $n \geq 4$ on parillinen luku, niin se voidaan esittää kahden alkuluvun summana.

2.2 Suurin yhteinen tekijä

Määritelmä 2.8. Olkoot a ja b kokonaislukuja ja ainakin toinen nollasta poikkeava. Jos positiivinen kokonaisluku t toteuttaa seuraavat ehdot:

1. $t \mid a \quad \text{ja} \quad t \mid b$;
2. Jos $\quad c \mid a \quad \text{ja} \quad c \mid b, \quad \text{niin} \quad c \mid t,$

niin sanotaan, että t on lukujen a ja b *suurin yhteinen tekijä* (greatest common divisor); merkitään $t = \text{syt}(a, b)$ tai $t = (a, b)$.

Lause 2.9. *Jos $a, b \in \mathbb{Z}$ ja luvuista ainakin toinen $\neq 0$, niin* $\text{syt}(a, b)$ *on olemassa. Lisäksi on olemassa sellaiset kokonaisluvut x ja y, että*

$$ax + by = \text{syt}(a, b).$$

Todistus. Luennolla.

Huomautus. Suurin yhteinen tekijä on yksikäsitteinen; tämä todistetaan luennolla.

Määritelmä 2.10. Jos $a, b \in \mathbb{Z}$ ja $\text{syt}(a, b) = 1$, niin sanotaan, että a ja b ovat *keskenään jaottomia* (mutually indivisible) lukuja eli *suhteellisia alkulukuja* (relatively prime). Tällöin merkitään $a \perp b$.

Eukleideen algoritmi

Jos on annettu kaksi kokonaislukua a ja b, niin $\text{syt}(a, b)$ löydetään ns. *Eukleideen algoritmin* avulla: Olkoot $a, b \in \mathbb{Z},\ a \neq 0,\ b \neq 0$. Tällöin lauseen 2.2

nojalla

$$\begin{aligned}
a &= q_1 b + r_1, \text{ missä } 0 < r_1 < |b| \\
b &= q_2 r_1 + r_2, \text{ missä } 0 < r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3, \text{ missä } 0 < r_3 < r_2 \\
&\vdots \\
r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1}, \text{ missä } 0 < r_{n-1} < r_{n-2} \\
r_{n-2} &= q_n r_{n-1} + r_n, \text{ missä } 0 < r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} r_n
\end{aligned}$$

Menettely todella päättyy ja viimeisen rivin mukainen muoto löytyy, sillä jono $r_1, r_2, \ldots$ on aidosti vähenevä ja alhaalta rajoitettu. Edelleen havaitaan, että

1. $r_n \mid r_{n-1} \Rightarrow r_n \mid r_{n-2} \Rightarrow \ldots \Rightarrow r_n \mid b \Rightarrow r_n \mid a$, ts. r_n jakaa sekä luvun a että luvun b;
2. $c \mid a$ ja $c \mid b \Rightarrow c \mid r_1 \Rightarrow c \mid r_2 \Rightarrow \ldots \Rightarrow c \mid r_n$.

Näin ollen r_n on määritelmän 2.8 mukaisesti lukujen a ja b suurin yhteinen tekijä $\text{syt}(a, b)$.

Aputulos 2.11. *Olkoon* $\text{syt}(a, b) = d$. *Tällöin* $\text{syt}(\frac{a}{d}, \frac{b}{d}) = 1$.

Todistus. Harjoitustehtävä.

Aputulos 2.12. *Olkoon* $a, b \in \mathbb{Z}$ *ja* $m \in \mathbb{Z}_+$. *Tällöin*

$$\text{syt}(ma, mb) = m \,\text{syt}(a, b).$$

Todistus. Harjoitustehtävä.

Aputulos 2.13. *Jos* $\text{syt}(a, b) = 1$ *ja* $a \mid bc$, *niin* $a \mid c$.

Todistus. Luennolla.

Aputulos 2.14. *Jos* $\text{syt}(a, b) = 1$ *ja* $a \mid c$ *sekä* $b \mid c$, *niin* $ab \mid c$.

Todistus. Luennolla.

Aputulos 2.15. *Jos p on alkuluku ja $p \mid ab$, niin $p \mid a$ tai $p \mid b$. Jos erityisesti a ja b ovat alkulukuja, niin $p = a$ tai $p = b$.*

Todistus. Luennolla.

Seuraus 2.16. *Induktiolla edellinen tulos voidaan yleistää muotoon:*

Jos p on alkuluku ja $p \mid a_1 a_2 \cdots a_n$, niin p jakaa jonkun luvuista $a_1, a_2, \ldots, a_n$. Jos erityisesti $a_1, a_2, \ldots, a_n$ ovat kaikki alkulukuja, niin p on jokin luvuista $a_1, a_2, \ldots, a_n$.

Lause 2.17 (Aritmetiikan peruslause)**.** *Jokainen kokonaisluku $n \geq 2$ voidaan esittää yksikäsitteisesti muodossa*

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},$$

missä $p_1 < p_2 < \ldots < p_k$ ovat alkulukuja ja eksponentit $a_1, a_2, \ldots, a_k$ positiivisia kokonaislukuja.

Todistus. Lauseen 2.7 nojalla esitys $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ on olemassa. Onko esitys yksikäsitteinen? Tehdään vastaoletus: väite ei ole tosi, eli esitys ei aina ole yksikäsitteinen. Tällöin on olemassa pienin positiivinen kokonaisluku $m \geq 2$, joka ei toteuta väitettä. Siis luvulla m on esitykset

$$m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},$$

ja

$$m = q_1^{b_1} q_2^{b_2} \cdots q_l^{b_l},$$

missä $p_1 < p_2 < \ldots < p_k$ ja $q_1 < q_2 < \ldots < q_l$ ovat alkulukuja ja kaikki eksponentit positiivisia kokonaislukuja. Koska $p_1 \mid m$ ja $m = q_1^{b_1} \cdots q_l^{b_l}$, niin aputuloksen 2.15 nojalla $p_1 \mid q_i^{b_i}$ jollakin $i \in \{1, \ldots, l\}$. Koska p_1 ja q_i ovat alkulukuja, niin täytyy olla $p_1 = q_i$.

Toisaalta $q_1 \mid m$, missä $m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, joten q_1 jakaa jonkin luvuista $p_j^{a_j}$ jollakin $j \in \{1, \ldots, k\}$. Koska q_1 ja p_j ovat alkulukuja, niin täytyy olla $q_1 = p_j$. Nyt

$$p_1 \leq p_j = q_1 \leq q_i = p_1,$$

joten on oltava $p_1 = q_1$. Koska $\frac{m}{p_1} < m$, niin luvulla $\frac{m}{p_1} = p_1^{a_1 - 1} p_2^{a_2} \cdots p_k^{a_k} = q_1^{b_1 - 1} q_2^{b_2} \cdots q_l^{b_l}$ on yksikäsitteinen väitteen mukainen esitys. Siis

$$k = l, p_2 = q_2, \ldots, p_k = q_k$$

ja

$$a_1 - 1 = b_1 - 1, a_2 = b_2, \ldots, a_k = b_k.$$

Mutta tällöin myös $a_1 = b_1$ ja luvulla m on yksikäsitteinen väitteen mukainen esitys, mikä on ristiriidassa vastaoletuksen kanssa. Siis vastaoletus on väärä ja väite tosi. □

Määritelmä 2.18. Olkoot $a, b \in \mathbb{Z}$. Pienintä sellaista positiivista kokonaislukua t, jonka sekä a että b jakavat, sanotaan lukujen a ja b *pienimmäksi yhteiseksi jaettavaksi* (lowest common multiple) ja siitä käytetään lyhennysmerkintää $\text{pyj}(a, b)$.

Formaalisti $t = \text{pyj}(a, b)$, jos se toteuttaa seuraavat ehdot:

1. $a \mid t \quad \text{ja} \quad b \mid t$;
2. Jos $\quad a \mid c \quad \text{ja} \quad b \mid c, \quad \text{niin} \quad t \mid c.$

Huomautus. Kahden kokonaisluvun pienimmän yhteisen jaettavan etsimiseen voidaan käyttää lauseen 2.17 mukaista kokonaisluvun esitystä alkulukujen tulona. Tästä esimerkkejä luennolla.

Lause 2.19. *Olkoot $a, b \in \mathbb{Z}$. Tällöin*

$$\text{pyj}(a, b) = \frac{a \cdot b}{\text{syt}(a, b)}.$$

Todistus. Merkitään $d = \text{syt}(a, b)$. Tällöin on olemassa sellaiset $x, y \in \mathbb{Z}$, että $a = xd$ ja $b = yd$, jolloin

$$\frac{ab}{d} = xyd = ay = bx \in \mathbb{Z}.$$

Siispä

$$a \mid \frac{ab}{d} \text{ ja } b \mid \frac{ab}{d}.$$

Olkoon $c \in \mathbb{Z}$ ja oletetaan, että $a \mid c$ ja $b \mid c$. Tällöin on olemassa sellaiset $k, l \in \mathbb{Z}$, että $c = ka = lb$. Lauseen 2.9 nojalla on olemassa sellaiset $m, n \in \mathbb{Z}$,

että $d = na + mb$. Tällöin

$$\begin{aligned} & cd = cna + cmb \\ \Leftrightarrow \quad & cd = lbna + kamb \\ \Leftrightarrow \quad & cd = ab(ln + km) \\ \Leftrightarrow \quad & c = \frac{ab}{d}(ln + km). \end{aligned}$$

Siispä $\frac{ab}{d} \mid c$, joten määritelmän 2.18 nojalla

$$\text{pyj}(a, b) = \frac{ab}{d} = \frac{a \cdot b}{\text{syt}(a, b)}.$$

2.3 Kongruenssiin liittyviä perustuloksia

Oletetaan, että $m \in \mathbb{Z}_+$ ja $a, b \in \mathbb{Z}$. Jos $m \mid a - b$, niin sanotaan, että *luku a on kongruentti luvun b kanssa modulo m*. Merkitään

$$\begin{aligned} & a \equiv b \pmod{m} \quad \text{tai} \\ & a \equiv b \quad (m). \end{aligned}$$

Lause 2.20. *Kongruenssi on ekvivalenssirelaatio joukossa $\mathbb{Z}$. Toisin sanoen jos $m \in \mathbb{Z}_+$, niin kaikilla $a, b, c \in \mathbb{Z}$ pätee*

1. $a \equiv a \pmod{m}$,
2. *jos* $a \equiv b \pmod{m}$, *niin* $b \equiv a \pmod{m}$,
3. *jos* $a \equiv b \pmod{m}$ *ja* $b \equiv c \pmod{m}$, *niin* $a \equiv c \pmod{m}$.

Todistus. Luennolla.

Lause 2.21. *Olkoon $a, b, c, d \in \mathbb{Z}$, $a \equiv b \pmod{m}$ ja $c \equiv d \pmod{m}$. Tällöin*

1. $ax + cy \equiv bx + dy \pmod{m}$ *kaikilla* $x, y \in \mathbb{Z}$,
2. $ac \equiv bd \pmod{m}$,
3. $a^n \equiv b^n \pmod{m}$ *kaikilla* $n \in \mathbb{N}$,

4. $p(a) \equiv p(b) \pmod{m}$ *kaikilla kokonaislukukertoimisilla polynomeilla* $p(n)$.

Todistus. Luennolla.

Huomautus. Lauseen 2.21 kohdasta 1 saadaan, että $a + c \equiv b + d \pmod{m}$ aina, kun $a \equiv b \pmod{m}$ ja $c \equiv d \pmod{m}$. Lisäksi kohdasta 2 saadaan, että jos $a \equiv b \pmod{m}$ ja $c \in \mathbb{Z}$, niin $ac \equiv bc \pmod{m}$.

Lause 2.22. *Olkoon* $a, b \in \mathbb{Z}$ *ja* $c \in \mathbb{Z}_+$. *Tällöin* $a \equiv b \pmod{m}$ *jos ja vain jos* $ac \equiv bc \pmod{mc}$.

Todistus. Luennolla.

Lause 2.23. *Olkoon* $a, b \in \mathbb{Z}$ *ja* $c \in \mathbb{Z}_+$. *Jos* $ac \equiv bc \pmod{m}$ *ja* $d = \text{syt}(m, c)$, *niin* $a \equiv b \pmod{\frac{m}{d}}$.

Todistus. Luennolla.

Huomautus. Lauseesta 2.23 saadaan erikoistapauksena, että jos $ac \equiv bc \pmod{m}$ ja $\text{syt}(c, m) = 1$, niin $a \equiv b \pmod{m}$. Ts. tässä tapauksessa c voidaan "supistaa".

Lause 2.24. *Olkoon* $a, b \in \mathbb{Z}$, $d \in \mathbb{Z}_+$ *ja* $a \equiv b \pmod{m}$. *Jos* $d \mid m$ *ja* $d \mid a$, *niin* $d \mid b$.

Todistus. Luennolla.

Lause 2.25. *Olkoon* $a, b \in \mathbb{Z}$ *ja* $a \equiv b \pmod{m}$. *Tällöin* $\text{syt}(a, m) = \text{syt}(b, m)$.

Todistus. Luennolla.

Lause 2.26. *Olkoon* $a, b \in \mathbb{Z}$ *ja* $a \equiv b \pmod{m}$. *Jos* $0 \leq |b - a| < m$, *niin* $a = b$.

Todistus. Luennolla.

Lause 2.27. *Olkoon* $a, b \in \mathbb{Z}$. *Tällöin* $a \equiv b \pmod{m}$ *jos ja vain jos luvuilla* a *ja* b *on sama jakojäännös jaettaessa luvulla* m.

Todistus. Luennolla.

Huomautus. Lauseen 2.27 seurauksena saadaan

1. jos $a \in \mathbb{Z}$, niin $m \mid a$ jos ja vain jos $a \equiv 0 \ (m)$,
2. jos $a \equiv b \pmod{m}$, niin $m \mid a$ jos ja vain jos $m \mid b$.

Lause 2.28. *Olkoon $a, b \in \mathbb{Z}$. Jos $a \equiv b \pmod{m}$ ja $a \equiv b \pmod{n}$, missä $\text{syt}(m, n) = 1$, niin $a \equiv b \pmod{mn}$.*

Todistus. Luennolla.

Huomautus. Olkoon $a, b, c, d \in \mathbb{Z}$. Tällöin

1. jos $a \equiv b \ (m)$, niin

$$a + km \equiv b \ (m) \text{ aina, kun } k \in \mathbb{Z},$$
$$a \equiv b + km \ (m) \text{ aina, kun } k \in \mathbb{Z},$$

2. $a \equiv a + km \ (m)$ aina, kun $k \in \mathbb{Z}$,
3. $a + b \equiv c + d \ (m) \quad \Leftrightarrow \quad a + b - d \equiv c \ (m) \quad \Leftrightarrow \quad a \equiv c + d - b \ (m)$.

Lause 2.29 (Jaollisuussääntöjä)**.**

1. *Kolmen jaollisuussääntö: Luku on jaollinen kolmella jos ja vain jos sen numeroiden summa on jaollinen kolmella.*
2. *Yhdeksän jaollisuussääntö: Luku on jaollinen yhdeksällä jos ja vain jos sen numeroiden summa on jaollinen yhdeksällä.*
3. *Seitsemän jaollisuussääntö: Luku*

$$L = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_1 \cdot 10^1 + a_0$$

on jaollinen seitsemällä, jos ja vain jos luku

$$a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} + \ldots + a_1 - 2 \cdot a_0$$

on jaollinen seitsemällä.

4. Yhdentoista jaollisuussääntö: Luku

$$L = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_1 \cdot 10^1 + a_0$$

on jaollinen luvulla 11*, jos ja vain jos luku*

$$a_n - a_{n-1} + a_{n-2} - a_{n-3} + \ldots + (-1)^n a_0$$

on jaollinen luvulla 11*.*

Todistus.

1. Luennolla.

2. Olkoon $L = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_1 \cdot 10 + a_0$, missä $0 \leq a_i \leq 9$ kaikilla $i = 0, 1, \ldots, n$. Koska $10 \equiv 1 \pmod 9$, niin

$$\begin{aligned} L &= a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_1 \cdot 10 + a_0 \\ &\equiv a_n + a_{n-1} + \ldots + a_1 + a_0 \pmod 9. \end{aligned}$$

   Lauseen 2.27 huomautuksen nojalla $9 \mid L$ jos ja vain jos

$$9 \mid a_n + a_{n-1} + \ldots + a_1 + a_0.$$

3. Harjoitustehtävä.

4. Olkoon $L = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_1 \cdot 10 + a_0$, missä $0 \leq a_i \leq 9$ kaikilla $i = 0, 1, \ldots, n$. Koska $10 \equiv -1 \pmod{11}$, niin

$$\begin{aligned} L &= a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_1 \cdot 10 + a_0 \\ &\equiv a_n \cdot (-1)^n + a_{n-1} \cdot (-1)^{n-1} + \ldots + a_1 \cdot (-1) + a_0 \pmod{11}. \end{aligned}$$

   Lauseen 2.27 huomautuksen nojalla $11 \mid L$ jos ja vain jos

$$11 \mid a_n \cdot (-1)^n + a_{n-1} \cdot (-1)^{n-1} + \ldots + a_1 \cdot (-1) + a_0.$$

   Koska jaollisuus säilyy, kun luku

$$a_n \cdot (-1)^n + a_{n-1} \cdot (-1)^{n-1} + \ldots + a_1 \cdot (-1) + a_0$$

   kerrotaan luvulla $(-1)^n$, niin

$$\begin{aligned} & 11 \mid a_n \cdot (-1)^n + a_{n-1} \cdot (-1)^{n-1} + \ldots + a_1 \cdot (-1) + a_0 \\ \Leftrightarrow \quad & 11 \mid a_n - a_{n-1} + a_{n-2} - \ldots + (-1)^{n-1} a_1 + (-1)^n a_0. \end{aligned}$$

Lause 2.30. *Kongruenssiyhtälö*

$$ax \equiv b(m)$$

on ratkeava, mikäli $\text{syt}(a, m) = 1$. *Jos* x_0 *on jokin tämän kongruenssin ratkaisu, niin kaikki ratkaisut ovat muotoa* $x \equiv x_0 \ (m)$.

Todistus. Luennolla.

Seuraus 2.31. *Olkoon* $\text{syt}(a, m) = d > 1$. *Kongruenssiyhtälöllä* $ax \equiv b \ (m)$ *on ratkaisu täsmälleen silloin, kun* $d \mid b$. *Jos* x_0 *on jokin ratkaisu, niin kaikki ratkaisut ovat muotoa* $x \equiv x_0 \ (\frac{m}{d})$.

Todistus. Luennolla.

Huomautus. Ratkaistaessa lauseen 2.30 oletukset täyttävää kongruenssia etsitään ensin yksi ratkaisu Eukleideen algoritmin avulla ja käytetään sitten kaikkien ratkaisujen muotoilemiseen lauseen jälkimmäistä osaa. Tästä esimerkkejä luennolla.

3 Jäännösluokat ja Eulerin φ-funktio

Määritelmä 3.1. Kokonaislukujen joukossa $\mathbb{Z}$ määritellyn ekvivalenssirelaation

$$x \, R \, y \Leftrightarrow x \equiv y \pmod{m}$$

ekvivalenssiluokkia kutsutaan *jäännösluokiksi modulo* m. Alkion y määräämästä jäännösluokasta *modulo* m käytetään merkintää

$$[y] = \{x \in \mathbb{Z} \mid x \equiv y \ (m)\}.$$

Kaikki jäännösluokat (mod m) ovat $\{[0], [1], [2], \ldots, [m-1]\}$ (perustelu luennolla). Tästä joukosta käytetään merkintää $\mathbb{Z}_m$.
Siis $\mathbb{Z}_m = \{[0], [1], [2], \ldots, [m-1]\}$ ja $|\mathbb{Z}_m| = m$.

Huomautus. Luvun $y \in \mathbb{Z}$ määräämä jäännösluokka *modulo* m on siis

$$[y] = \{x \in \mathbb{Z} \mid x \equiv y \pmod{m}\} = \{x \in \mathbb{Z} \mid x = y + km\} = [y + km].$$

Määritelmä 3.2. Jäännösluokkaa $[a]$ (*mod* m) sanotaan *alkuluokaksi* (mod m), mikäli $\text{syt}(a, m) = 1$. Alkuluokkien joukkoa merkitään $\mathbb{Z}_m^*$. Siis

$$\mathbb{Z}_m^* = \{[a] \in \mathbb{Z}_m \mid \text{syt}(a, m) = 1\}.$$

Huomautus. Jos p on alkuluku, niin

$$\mathbb{Z}_p^* = \{[1], [2], \ldots, [p-1]\}.$$

Määritelmä 3.3. Funktio $\varphi : \mathbb{Z}_+ \to \mathbb{Z}_+$, $\varphi(m) = |\mathbb{Z}_m^*|$ on *Eulerin φ-funktio.*
Siis $\varphi(m)$ kertoo alkioiden lukumäärän joukossa

$$\{x \mid x \in \mathbb{N}, \ x < m \text{ ja } \text{syt}(x, m) = 1\}.$$

Huomautus. Jos p on alkuluku, niin $\varphi(p) = p - 1$.

Lause 3.4. *Jos p on alkuluku ja $k \in \mathbb{N}$, niin $\varphi(p^k) = p^{k-1}(p-1)$.*

Todistus. Luennolla.

Lause 3.5. *Jos* $\text{syt}(m,n)=1$, *niin* $\varphi(mn)=\varphi(m)\varphi(n)$.

Todistus. Huomataan ensin, että $\text{syt}(mn,a)=1 \Leftrightarrow \text{syt}(m,a)=1$ ja $\text{syt}(n,a)=1$. Muodostetaan luvuista $0,1,\ldots,mn-1$ seuraava taulukko (taulukossa on n pystyriviä ja m vaakariviä).

$$\begin{array}{ccccc}
0 & 1 & 2 & \ldots & n-1 \\
n & n+1 & n+2 & \ldots & 2n-1 \\
2n & 2n+1 & 2n+2 & \ldots & 3n-1 \\
\vdots & & & & \vdots \\
(m-1)n & (m-1)n+1 & (m-1)n+2 & \ldots & mn-1 \\
\hline
\uparrow & \uparrow & \uparrow & & \uparrow \\
\equiv 0\ (n) & \equiv 1\ (n) & \equiv 2\ (n) & & \equiv n-1\ (n) \\
\in [0] & \in [1] & \in [2] & \ldots & \in [n-1]
\end{array}$$

Nyt kullakin pystyrivillä on tarkalleen yhden jäännösluokan alkioita $\bmod n$. Pystyriveistä $\varphi(n)$ kappaletta sisältyy alkuluokkiin $\bmod n$, toisin sanoen näiden pystyrivien alkioiden suurin yhteinen tekijä luvun n kanssa on 1.

Tarkastellaan sitten yhtä alkuluokkaan $\bmod n$ liittyvää pystyriviä $\bmod m$ suhteen. Olkoon tämä pystyrivi

$$\begin{array}{c}
k \\
n+k \\
2n+k \\
\vdots \\
(m-1)n+k
\end{array}$$

Jos $[dn+k]=[tn+k] \pmod m$, missä $0 \le d,t < m$, niin $dn+k \equiv tn+k\ (m)$ eli $dn \equiv tn\ (m)$ eli

$$d \equiv t \quad (m),$$

koska $\text{syt}(m,n)=1$. Nyt $m \mid d-t$ ja siten $d=t$, koska $d,t<m$. Näin ollen pystyrivin kaikki alkiot sisältyvät eri jäännösluokkaan $\bmod m$, eli pystyrivillä on edustajat kaikista jäännösluokista $\bmod m$. Tällöin tämän pystyrivin luvuista $\varphi(m)$ kappaletta on sellaisia, että ne ovat alkuluokassa $\bmod m$, eli suurin yhteinen tekijä luvun m kanssa on 1. Täten lukuja, joiden suurin yhteinen tekijä luvun mn kanssa on 1, on $\varphi(n)\cdot\varphi(m)$ kappaletta. Siis $\varphi(mn)=\varphi(m)\varphi(n)$. □

Lause 3.6 (Seuraus)**.** *Jos $m \in \mathbb{Z}_+$ ja luvulla m on esitys $m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ eri alkulukujen potenssien tulona, niin*

$$\begin{aligned}\varphi(m) &= \varphi(p_1^{a_1})\varphi(p_2^{a_2}) \cdots \varphi(p_r^{a_r}) \\ &= p_1^{a_1-1}(p_1 - 1) \cdots p_r^{a_r-1}(p_r - 1) \\ &= \prod_{i=1}^{r} p_i^{a_i-1}(p_i - 1).\end{aligned}$$

Todistus. Lauseet 3.4 ja 3.5

Lause 3.7. *(Eulerin teoreema) Olkoot $a, m \in \mathbb{Z}_+$. Jos $\mathrm{syt}(a, m) = 1$, niin*

$$a^{\varphi(m)} \equiv 1 \quad (m).$$

Todistus. Todistus ryhmäteoria-osassa.

Lause 3.8. *(Fermat'n pieni lause.) Olkoon p alkuluku ja $a \in \mathbb{Z}_+$. Jos $p \nmid a$ eli $a \not\equiv 0$ (p), niin*

$$a^{p-1} \equiv 1 \quad (p).$$

Todistus. Väite seuraa havainnosta $\varphi(p) = p - 1$ sekä lauseesta 3.7

Lause 3.9. *(Seurauslause) Olkoon p alkuluku ja $a \in \mathbb{Z}_+$. Tällöin*

$$a^p \equiv a \quad (p).$$

Todistus. Luennolla

4 Ryhmät

4.1 Ryhmäteorian alkeita

Määritelmä 4.1.1. Olkoon S ei-tyhjä joukko. Kuvaus $* : S \times S \to S$, $(a, b) \mapsto a * b$ on joukon S *binäärinen operaatio* (eli $a * b \in S$ aina, kun $a, b \in S$ ja $a * b$ on yksikäsitteinen).

Lisäksi binäärinen operaatio $(*)$ on

- *kommutatiivinen* (vaihdannainen) joukossa S, jos $a * b = b * a$ aina, kun $a \in S$ ja $b \in S$;
- *assosiatiivinen* (liitännäinen), jos $a * (b * c) = (a * b) * c$ aina, kun $a, b, c \in S$.

Huomautus. Yhteenlasku joukossa $\mathbb{Z}$ on kommutatiivinen ja assosiatiivinen. Sen sijaan vähennyslasku ei ole kumpaakaan.

Määritelmä 4.1.2. Jos $S \neq \emptyset$ ja $(*)$ on joukon S assosiatiivinen binäärinen operaatio, niin paria $(S, *)$ sanotaan *puoliryhmäksi* (semigroup).

Määritelmä 4.1.3. Olkoot $G \neq \emptyset$ ja $(*)$ joukon G operaatio. Pari $(G, *)$ on *ryhmä* (group), mikäli seuraavat ehdot toteutuvat:

1. $(*)$ on binäärinen joukossa G eli
$$a * b \in G$$
aina, kun $a, b \in G$.
2. $(*)$ on assosiatiivinen joukossa G eli
$$(a * b) * c = a * (b * c)$$
aina, kun $a, b, c \in G$;
3. Joukossa G on sellainen alkio e, että
$$a * e = e * a = a$$
aina, kun $a \in G$. Alkiota e kutsutaan *neutraali- tai ykkösalkioksi* (identity/neutral element);

4. Aina, kun $a \in G$, on olemassa sellainen alkio $a^{-1} \in G$, että

$$a * a^{-1} = a^{-1} * a = e.$$

   Alkiota a^{-1} kutsutaan *alkion a käänteisalkioksi* (inverse element).

Jos lisäksi

5. $(*)$ on kommutatiivinen joukossa G eli

$$a * b = b * a$$

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

niin kyseessä on *Abelin ryhmä* eli kommutatiivinen ryhmä.

Jatkossa ryhmästä $(G, *)$ käytetään merkintää G, mikäli operaatiosta $(*)$ ei ole epäselvyyttä. Tällöin operaatiota $a * b$ merkitään ab.

Lause 4.1.4. *Olkoot G ryhmä sekä $a, b \in G$. Tällöin*

1. *neutraalialkio on yksikäsitteinen;*
2. *kunkin alkion käänteisalkio on yksikäsitteinen;*
3. *yhtälöllä $ax = b$ on yksikäsitteinen ratkaisu $x \in G$;*
4. *yhtälöllä $ya = b$ on yksikäsitteinen ratkaisu $y \in G$.*

Todistus. Luennolla.

Lause 4.1.5. *Ryhmässä G ovat voimassa seuraavat lait:*

1. $ab = ac \Rightarrow b = c$;
2. $ba = ca \Rightarrow b = c$;
3. $(ab)^{-1} = b^{-1}a^{-1}$;
4. $(a^{-1})^{-1} = a$.

Todistus. Luennolla.

Ryhmän G *kertaluku* (the order of G) tarkoittaa joukon G alkioiden lukumäärää; merkitään $|G|$.

Huomautus. Äärettömässä ryhmässä (infinite group) on ääretön määrä alkioita. Äärellisessä ryhmässä (finite group) on äärellinen määrä alkioita ja siis myös ryhmäoperaation tuloksia. Siispä äärellisessä tapauksessa voidaan kirjoittaa *ryhmätaulu* (group table), johon merkitään kaikkien ryhmäoperaatioiden tulokset omiin soluihinsa; yksityiskohdat esitetään luennolla.

$*$	*alkiot*
a	
l	alkioiden
k	väliset
i	operaatiot
o	
t	

Huomautus. Ryhmätaulun jokaisella vaaka- ja pystyrivillä esiintyy kukin ryhmän G alkio tarkalleen kerran.

4.2 Jäännösluokkaryhmät

Luennolla nähtiin, että joukon $\mathbb{Z}$ ekvivalenssirelaatio $x\,Ry \Leftrightarrow x \equiv y(m)$ johtaa ekvivalenssiluokkiin $\mathbb{Z}_m = \{[0], [1], [2], \ldots, [m-1]\}$, missä $m \in \mathbb{Z}_+$. Näitä ekvivalenssiluokkia kutsutaan *jäännösluokiksi* $\pmod m$.

Miten jäännösluokilla lasketaan?

Jos $x \equiv a \ (m)$ ja $y \equiv b \ (m)$, niin $x + y \equiv a + b \ (m)$ ja $xy \equiv ab \ (m)$. Siis

$$[a] + [b] = [a + b] \quad \text{ja}$$
$$[a]\,[b] = [ab]$$

Huomautus. Yhteenlasku $\pmod m$ ja kertolasku $\pmod m$ eivät riipu jäännösluokkien edustajien a ja b valinnasta.

Lause 4.2.1. *Pari $(\mathbb{Z}_m, +)$ on Abelin ryhmä.*

Todistus. Luennolla.

Huomautus. $|(\mathbb{Z}_m, +)| = m$.

Tarkastellaan seuraavaksi joukkoa $\mathbb{Z}_m$ varustettuna kertolaskulla $\pmod m$. Selvästi kyseessä on binäärinen ja assosiatiivinen operaatio ja jäännösluokka $[1]$ on ykkösalkio.

Ongelma. Milloin jäännösluokalla $[a]$ on käänteisalkio kertolaskun $\pmod m$ suhteen eli milloin on olemassa sellainen $[x]$, että $[a] \cdot [x] = [1]$?

Ratkaisu: $[a] \cdot [x] = [1] \Leftrightarrow [ax] = [1] \Leftrightarrow ax \equiv 1(m)$. Tällä kongruenssilla on ratkaisu täsmälleen silloin, kun $\text{syt}(a, m) = 1$ (ks. lause 2.30).

Jäännösluokkaa $[a]$ $\pmod m$ sanotaan alkuluokaksi $\pmod m$, mikäli $\text{syt}(a, m) = 1$. Alkuluokkien joukkoa merkitään $\mathbb{Z}_m^*$.

Lause 4.2.2. *Pari $(\mathbb{Z}_m^*, \cdot)$ on Abelin ryhmä.*

Todistus. Luennolla.

Ongelma. Olkoon $m \in \mathbb{Z}_+$. Helposti nähdään, että ryhmän $(\mathbb{Z}_m, +)$ kertaluku $|(\mathbb{Z}_m, +)| = m$. Mutta miten lasketaan ryhmän $(\mathbb{Z}_m^*, \cdot)$ kertaluku $|(\mathbb{Z}_m^*, \cdot)|$?

Määritelmä 4.1. Funktio $\varphi : \mathbb{Z}_+ \to \mathbb{Z}_+$, $\varphi(m) = |\mathbb{Z}_m^*|$ on *Eulerin φ-funktio.* Siis $\varphi(m)$ kertoo alkioiden määrän joukossa

$$\{x \mid x \in \mathbb{N},\ x < m \text{ ja } \operatorname{syt}(x, m) = 1\}.$$

Huomautus. Jos p on alkuluku, niin $\varphi(p) = |\mathbb{Z}_p^*| = p - 1$.

Seuraavat lauseet on esitetty aiemmin luvussa 3.

Lause 4.2. *Jos p on alkuluku ja $k \in \mathbb{N}$, niin $\varphi(p^k) = |\mathbb{Z}_{p^k}^*| = p^{k-1}(p-1)$.*

Lause 4.3. *Jos $\operatorname{syt}(m, n) = 1$, niin $\varphi(mn) = \varphi(m)\varphi(n)$.*

Lause 4.4 (Seuraus)**.** *Jos $m \in \mathbb{Z}_+$ ja luvulla m on esitys $m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ eri alkulukujen potenssien tulona, niin*

$$\begin{aligned} \varphi(m) = |\mathbb{Z}_m^*| &= \varphi(p_1^{a_1})\varphi(p_2^{a_2}) \cdots \varphi(p_r^{a_r}) \\ &= p_1^{a_1-1}(p_1 - 1) \cdots p_r^{a_r-1}(p_r - 1) \\ &= \prod_{i=1}^{r} p_i^{a_i-1}(p_i - 1). \end{aligned}$$

4.3 Aliryhmä

Määritelmä 4.3.1. Olkoon $(G, *)$ ryhmä ja $H \subseteq G,\ H \neq \emptyset$. Jos $(H, *)$ on ryhmä, sitä sanotaan *ryhmän* $(G, *)$ *aliryhmäksi* (subgroup); merkitään $(H, *) \leq (G, *)$ tai lyhyemmin $H \leq G$.

Huomautus. Jos $H \leq G$, niin aina ryhmän G neutraalialkio $e_G \in H$.

Lause 4.3.2 (Aliryhmäkriteeri)**.** *Olkoot G ryhmä ja $H \subseteq G,\ H \neq \emptyset$. Nyt $H \leq G$ jos ja vain jos seuraavat ehdot toteutuvat:*

1. $a, b \in H \Rightarrow ab \in H$;
2. $a \in H \Rightarrow a^{-1} \in H$.

Todistus. Luennolla.

Seuraus 4.3.3. *Olkoot G ryhmä ja $H \subseteq G,\ H \neq \emptyset$. Tällöin $H \leq G$ jos ja vain jos ehto*

3. $a, b \in H \Rightarrow ab^{-1} \in H$

on voimassa.

Todistus. " $\Rightarrow$ " Jos $H \leq G$, niin ehto 3. toteutuu, sillä H on ryhmä.

" $\Leftarrow$ " Oletetaan, että ehto 3. on voimassa. Jos $a \in H$, niin ehdon 3. nojalla $aa^{-1} = e \in H$. Edelleen $ea^{-1} = a^{-1} \in H$, joten lauseen 4.3.2 ehto 2. toteutuu.

Jos $a, b \in H$, niin edellisen nojalla $b^{-1} \in H$ ja ehdon 3. nojalla

$$ab = a(b^{-1})^{-1} \in H.$$

Siispä myös lauseen 4.3.2 ehto 1. toteutuu. Näin ollen lauseen 4.3.2 nojalla $H \leq G$.

Huomautus. Jos $(G, *)$ on ryhmä, $a \in G$ ja $n \in \mathbb{Z}_+$, niin

$$a^n = \underbrace{a * a * \ldots * a}_{n \text{ kpl}}$$

Seuraus 4.3.4. *Jos G on ryhmä ja H on ryhmän G äärellinen ei-tyhjä osajoukko, niin $H \leq G$ jos ja vain jos $ab \in H$ aina, kun $a, b \in H$.*

Todistus. Luennolla.

Huomautus. Äärellisessä tapauksessa siis riittää, että ryhmän G ryhmäoperaatio on binäärinen joukossa H. Äärettömässä tapauksessa tämä ei vielä takaa sitä, että H olisi ryhmän G aliryhmä.

Huomautus. Jos G on ryhmä, niin aina $G \leq G$ ja $\{e_G\} \leq G$. Näitä ryhmiä sanotaan ryhmän G *triviaaleiksi* aliryhmiksi.

Määritelmä 4.3.5. Olkoon $(H, *) \leq (G, *)$ ja $a \in G$. Joukkoa $aH = a * H = \{a * h \mid h \in H\}$ sanotaan *alkion a määräämäksi aliryhmän H vasemmaksi sivuluokaksi* (left coset).

Huomautus.

- Additiivisessa ryhmässä vasen sivuluokka on

$$aH = a + H = \{a + h \mid h \in H\}.$$

- Koska $eH = H$, niin H itse on eräs vasen sivuluokka.
- Kuvaus $f : H \to aH,\ f(h) = ah$ on bijektio, joten sivuluokassa aH on yhtä monta alkiota kuin aliryhmässä H.
- Vasenta sivuluokkaa vastaavalla tavalla voidaan määritellä myös ryhmän G *alkion a määräämä aliryhmän H oikea sivuluokka*

$$Ha = \{ha \mid h \in H\}, \qquad \text{missä } a \in G.$$

  Oikeilla sivuluokilla on voimassa samat ominaisuudet kuin vasemmilla sivuluokilla.

Lause 4.3.6. *Olkoon G ryhmä ja $H \leq G$. Tällöin joukossa G määritelty relaatio*

$$a \, R \, b \Leftrightarrow b^{-1}a \in H$$

on ekvivalenssirelaatio. Jos $a \in G$, niin alkion a määräämä ekvivalenssiluokka $[a]$ on alkion a määräämä aliryhmän H vasen sivuluokka aH.

Todistus. Luennolla.

Seuraus 4.3.7. *Olkoon G ryhmä, $H \leq G$ ja $a_1H, a_2H, \ldots$ aliryhmän H vasemmat sivuluokat ryhmässä G.*

Tällöin

$$G = \bigcup_i a_i H$$

ja aina joko $a_iH \bigcap a_jH = \emptyset$ tai $a_iH = a_jH$.

Lisäksi, jos $b \in aH$, niin $bH = aH$.

Todistus. Tulos seuraa lauseista 1.4 ja 1.5.

Lause 4.3.8 (Lagrangen lause)**.** *Olkoot G äärellinen ryhmä, $H \leq G$ ja n aliryhmän H vasempien sivuluokkien lukumäärä ryhmässä G. Tällöin*

$$|G| = n\,|H|\,,$$

ts. äärellisessä ryhmässä aliryhmän kertaluku jakaa ryhmän kertaluvun.

Todistus. Luennolla.

Seuraus 4.3.9. *Jos äärellisen ryhmän G kertaluku on alkuluku, niin sen ainoat mahdolliset aliryhmät ovat $\{e\}$ ja G (nk. triviaalit aliryhmät).*

Todistus. Luennolla.

4.4 Syklinen ryhmä

Olkoon $(G, *)$ ryhmä ja $a \in G$. Kun $n \in \mathbb{Z}_+$, niin

$$a^n = \underbrace{a * a * \ldots * a}_{n \text{ kpl}} \quad \text{ja} \quad a^{-n} = \underbrace{a^{-1} * a^{-1} * \ldots * a^{-1}}_{n \text{ kpl}}.$$

Lisäksi asetetaan $a^0 = e$. Tällöin joukko $H = \{a^k \mid k \in \mathbb{Z}\}$ on joukon G osajoukko.

Jos $x, y \in H$, niin $x = a^m$ ja $y = a^n$ eräillä $m, n \in \mathbb{Z}$ sekä

$$xy^{-1} = a^m a^{-n} = a^{m-n} \in H.$$

Näin ollen osajoukko H on seurauksen 4.3.3 nojalla ryhmän G aliryhmä.

Määritelmä 4.4.1. Yllä määriteltyä ryhmää $H = \{a^k \mid k \in \mathbb{Z}\}$ sanotaan *alkion a generoimaksi sykliseksi ryhmäksi* (cyclic group); merkitään $H = \langle a \rangle$. Alkio a on *generoija* (generator).

Lause 4.4.2. *Jos ryhmän kertaluku on alkuluku, niin ryhmä on syklinen.*

Todistus. Luennolla.

Huomautus. Ryhmä $(\mathbb{Z}_m, +)$ on syklinen. Sen sijaan ryhmä $(\mathbb{Z}_m^*, \cdot)$ ei välttämättä ole syklinen.

Lause 4.4.3. *Olkoot G ryhmä ja $a \in G$ sekä n pienin sellainen positiivinen kokonaisluku, että $a^n = e$. Tällöin $|\langle a \rangle| = n$ ja*

$$\langle a \rangle = \{a^0 = e, a^1 = a, a^2, a^3, \ldots, a^{n-1}\}.$$

Todistus. Luennolla.

Lause 4.4.4. *Jos G on äärellinen ryhmä, niin $a^{|G|} = e$ kaikilla $a \in G$.*

Todistus. Luennolla.

Huomautus. Lauseen 4.4.3 mukaista lukua n sanotaan alkion *a kertaluvuksi*; alkion kertaluvusta käytetään merkintää $|\langle a \rangle|$, $|a|$ tai $ord(a)$.

Lause 4.4.5 (Eulerin teoreema)**.** *Jos* $a, m \in \mathbb{Z}_+$ *ja* $\text{syt}(a, m) = 1$*, niin*

$$a^{\varphi(m)} \equiv 1(m).$$

Todistus. Luennolla.

Seuraus 4.4.6 (Fermat'n pieni lause)**.** *Jos* p *on alkuluku ja* $\text{syt}(a, p) = 1$*, niin* $a^{p-1} \equiv 1(p)$*.*

Todistus. Luennolla.

Lause 4.4.7. *Syklisen ryhmän jokainen aliryhmä on syklinen.*

Todistus. Olkoon $G = \langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$ ja $H \leq G$. Nyt jokainen aliryhmän H alkio on alkion a potenssi. Jos $H = \{e\}$, niin $H = \langle e \rangle$ on syklinen. Jos $H \neq \{e\}$, niin on olemassa sellainen $m \in \mathbb{Z}_+$, että $a^m \in H$. Olkoon sitten

$$n = \min\{m \mid a^m \in H, m \in \mathbb{Z}_+\}.$$

Väitetään, että $H = \langle a^n \rangle$.

Olkoon $b \in H$ mielivaltainen. Siis on olemassa sellainen $l \in \mathbb{Z}$, että $b = a^l$. Nyt jakoalgoritmin (Lause 2.2) nojalla $l = qn+r$, missä $q, r \in \mathbb{Z}$ ja $0 \leq r < n$. Siis

$$b = a^l = a^{qn+r} = (a^n)^q a^r.$$

Täten $a^r = [(a^n)^q]^{-1} b \in H$. Luvun n valinnasta johtuen täytyy olla $r = 0$. Siis $l = qn$ ja

$$b = a^l = a^{qn} = (a^n)^q.$$

Täten $H = \langle a^n \rangle$ on syklinen.

Huomautus. Syklinen ryhmä on aina Abelin ryhmä.

4.5 Normaali aliryhmä ja tekijäryhmä

Määritelmä 4.5.1. Olkoon $N \leq G$. Aliryhmää N sanotaan *normaaliksi*, mikäli $aN = Na$ aina, kun $a \in G$. Tällöin merkitään $N \trianglelefteq G$.

Huomautus.

- $\{e\} \trianglelefteq G \qquad$ ja $\qquad G \trianglelefteq G$.
- Jos G on Abelin ryhmä ja $N \leq G$, niin kaikilla $a \in G$ pätee

$$\begin{aligned} aN &= \{an \mid n \in N\} \\ &= \{na \mid n \in N\} \\ &= Na. \end{aligned}$$

  Siis Abelin ryhmän jokainen aliryhmä on normaali.

Lause 4.5.2. *Ryhmän G aliryhmä N on normaali jos ja vain jos*

$$aNa^{-1} \subseteq N \quad \textit{aina, kun} \quad a \in G.$$

Todistus. Luennolla.

Huomautus. Kun todistetaan, että $N \trianglelefteq G$, niin pitää osoittaa, että

1. $N \leq G$;
2. $ana^{-1} \in N$ aina, kun $a \in G$ ja $n \in N$ (aliryhmän normaalisuuskriteeri).

Olkoon nyt $N \trianglelefteq G$. Sivuluokkien joukossa $\{aN \mid a \in G\}$ voidaan määritellä operaatio $(\cdot)$ seuraavasti:

$$aN \cdot bN = ab\,N.$$

Näin saatu operaatio on *hyvin määritelty* (well-defined) eli se ei ole riippuvainen sivuluokkien aN ja bN edustajista. Lisäksi sivuluokkien joukko $\{aN \mid a \in G\}$ yhdessä kyseisen operaation kanssa on ryhmä. Näiden väitteiden paikkansapitävyys todistetaan luennolla.

Lause 4.5.3. *Olkoon G ryhmä ja $N \trianglelefteq G$. Tällöin $(\{aN \mid a \in G\}, \cdot)$ on ryhmä.*

Todistus. Luennolla.

Määritelmä 4.5.4. Edellä esiteltyä paria $(\{aN \mid a \in G\}, \cdot)$ kutsutaan *ryhmän G tekijäryhmäksi normaalin aliryhmän N suhteen* (factor group/quotient group of G by N). Kyseisestä ryhmästä käytetään merkintää G/N.

Huomautus.

$$|G/N| = \frac{|G|}{|N|},$$

mikäli ryhmä G on äärellinen.

4.6 Permutaatioryhmistä

Määritelmä 4.6.1. Olkoon $X \neq \emptyset$. Bijektiota $f : X \to X$ sanotaan joukon X *permutaatioksi* (permutation).

Huomautus. Kuvaus $f : X \to X$ on *bijektio* jos ja vain jos se on

1. *injektio* eli ehdosta $f(a) = f(b)$ seuraa, että $a = b$ aina, kun $a, b \in X$,
2. *surjektio* eli jokaiselle $b \in X$ on olemassa sellainen $a \in X$, että $f(a) = b$.

Huomautus. Jos X on äärellinen joukko, niin mikä tahansa sen permutaatio voidaan esittää nk. *permutaatiomatriisin* avulla (esimerkkejä luennolla).

Lause 4.6.2. *Olkoon S_X joukon X kaikkien permutaatioiden joukko. Jos $(\circ)$ on kuvausten yhdistämisoperaatio, niin $(S_X, \circ)$ on ryhmä.*

Todistus. Luennolla.

Huomautus. Yleensä $(\circ)$ ei ole kommutatiivinen operaatio, eli $(S_X, \circ)$ ei yleensä ole Abelin ryhmä.

Yleisesti, jos $|X| = n$, niin merkitään $S_X = S_n$. Näin saadaan *astetta n oleva symmetrinen ryhmä* (symmetric group of order n) ja $|S_n| = n!$.

Permutaatioryhmillä on käyttöä esim. kappaleiden (kiteiden ja molekyylien) symmetriatarkasteluiden yhteydessä. Permutaatioryhmiä ja niiden sovelluksia tarkastellaan tarkemmin kurssilla *Permutaatiot, kunnat ja Galois'n teoria.*

Huomautus. Symmetrisen ryhmän $(S_n, \cdot)$ aliryhmiä nimitetään permutaatioryhmiksi.

4.7 Ryhmähomomorfismi

Määritelmä 4.7.1. Olkoot $(G, \cdot)$ ja $(H, *)$ ryhmiä. Kuvausta $f : G \to H$ sanotaan *ryhmähomomorfismiksi* ryhmältä G ryhmälle H, mikäli

$$f(a \cdot b) = f(a) * f(b)$$

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

Lause 4.7.2. *Olkoon $f : G \to H$ ryhmähomomorfismi ja olkoot e_G ja e_H ryhmien G ja H neutraalialkiot. Tällöin*

$$f(e_G) = e_H \qquad ja \qquad f(a^{-1}) = (f(a))^{-1}$$

aina, kun $a \in G$.

Todistus. Luennolla.

Määritelmä 4.7.3. Olkoon $f : G \to H$ ryhmähomomorfismi ja $D \leq G$. Tällöin $f(D) = \{f(x) \mid x \in D\}$ on aliryhmän D *kuva* (image) ryhmässä H.

Määritelmä 4.7.4. Olkoon $f : G \to H$ ryhmähomomorfismi ja $T \leq H$. Tällöin $f^{-1}(T) = \{x \in G \mid f(x) \in T\}$ on aliryhmän T *alkukuva* (pre-image) ryhmässä G.

Lause 4.7.5. *Olkoon $f : (G, \cdot) \to (H, *)$ ryhmähomomorfismi.*

1. *Jos $D \leq G$, niin $f(D) \leq H$.*
2. *Jos $T \leq H$, niin $f^{-1}(T) \leq G$.*

   Todistus. Oletetaan, että $f : (G, \cdot) \to (H, *)$ on ryhmähomomorfismi. Todistetaan väitteet erikseen.

1. Olkoon $D \leq G$. Selvästi $f(D) \subseteq H$ ja $f(D) \neq \emptyset$, sillä $e_G \in D$ ja siten $f(e_G) = e_H \in f(D)$.

   Onko $f(D) \leq H$?

   Olkoon $c, d \in f(D)$. Tällöin on olemassa sellaiset alkiot $a, b \in D$, että $f(a) = c$ ja $f(b) = d$. Koska $D \leq G$, niin aliryhmäkriteerin nojalla

$a \cdot b^{-1} \in D$ ja siten $f(a \cdot b^{-1}) \in f(D)$. Koska f on homomorfismi, niin myös

$$\begin{aligned} & f(a) * f(b^{-1}) \in f(D), \\ \text{eli } & f(a) * f(b)^{-1} \in f(D), \\ \text{eli } & c * d^{-1} \in f(D). \end{aligned}$$

Näin ollen aliryhmäkriteerin nojalla $f(D) \leq H$.

2. Olkoon $T \leq H$.

   Selvästi $f^{-1}(T) \subseteq G$ ja $f^{-1}(T) \neq \emptyset$, sillä $e_H \in T$, ja siten $e_G \in f^{-1}(T)$.

   Onko $f^{-1}(T) \leq G$?

   Olkoon $a, b \in f^{-1}(T)$. Näin ollen $f(a), f(b) \in T$.

   Koska $T \leq H$, niin aliryhmäkriteerin nojalla

$$\begin{aligned} & f(a) * f(b)^{-1} \in T \\ \text{eli } & f(a) * f(b^{-1}) \in T \\ \text{eli } & f(a \cdot b^{-1}) \in T \\ \text{eli } & a \cdot b^{-1} \in f^{-1}(T). \end{aligned}$$

   Näin ollen aliryhmäkriteerin nojalla $f^{-1}(T) \leq G$.

□

Huomautus. Lauseen sisältö voidaan muotoilla seuraavasti: homomorfisessa kuvauksessa aliryhmät kuvautuvat aliryhmiksi ja aliryhmien alkukuvat ovat aliryhmiä.

Edellä esitetty johtaa luontevasti kysymykseen siitä, mitä normaaleille aliryhmille tapahtuu homomorfismeissa.

Lause 4.7.6. *Olkoon $f : (G, \cdot) \to (H, *)$ ryhmähomomorfismi.*

1. *Jos $N \trianglelefteq G$ ja f on surjektio, niin $f(N) \trianglelefteq H$.*
2. *Jos $M \trianglelefteq H$, niin $f^{-1}(M) \trianglelefteq G$.*

Todistus. Oletetaan, että $f : (G, \cdot) \to (H, *)$ on ryhmähomomorfismi. Todistetaan väitteet erikseen.

1. Oletetaan, että $N \trianglelefteq G$ ja f on surjektio $G \to H$. Tällöin Lauseen 4.7.5 nojalla $f(N) \leq H$.

   Onko $f(N) \trianglelefteq H$?

   Olkoon $z \in f(N)$ ja $d \in H$. Siten on olemassa sellainen $x \in N$, että $z = f(x)$, ja koska f on surjektio, on myös olemassa sellainen $a \in G$, että $d = f(a)$.

   Koska $N \trianglelefteq G$, niin $a \cdot x \cdot a^{-1} \in N$ (Lause 4.5.2)

   $$\begin{aligned} &\text{eli} \quad f(a \cdot x \cdot a^{-1}) \in f(N) \\ &\text{eli} \quad f(a) * f(x) * f(a^{-1}) \in f(N) \\ &\text{eli} \quad f(a) * f(x) * f(a)^{-1} \in f(N) \\ &\text{eli} \quad d * z * d^{-1} \in f(N). \end{aligned}$$

   Täten normaalisuuskriteerin nojalla $f(N) \trianglelefteq H$.

2. Oletetaan, että $M \trianglelefteq H$.

   Lauseen 4.7.5 nojalla $f^{-1}(M) \leq G$.

   Onko $f^{-1}(M) \trianglelefteq G$?

   Olkoon $x \in f^{-1}(M)$ ja $a \in G$. Nyt $f(x) \in M$ ja $f(a) \in H$.
   Koska $M \trianglelefteq H$, niin Lauseen 4.5.2 nojalla

   $$\begin{aligned} &\quad f(a) * f(x) * f(a)^{-1} \in M \\ &\text{eli} \quad f(a) * f(x) * f(a^{-1}) \in M \\ &\text{eli} \quad f(a \cdot x \cdot a^{-1}) \in M \\ &\text{eli} \quad a \cdot x \cdot a^{-1} \in f^{-1}(M). \end{aligned}$$

   Täten normaalisuuskriteerin nojalla $f^{-1}(M) \trianglelefteq G$.

□

Määritelmä 4.7.7. Olkoon $f : G \to H$ homomorfismi. Joukkoa

$$Im(f) = f(G) = \{f(x) \mid x \in G\}$$

sanotaan homomorfismin f *kuvaksi* (the image of f) ja joukkoa

$$Ker(f) = \{x \in G \mid f(x) = e_H\} = f^{-1}(\{e_H\})$$

sanotaan homomormismin f *ytimeksi* (the kernel of f).

Lause 4.7.8. *Olkoon $f : G \to H$ ryhmähomomorfismi. Tällöin $Im(f) \leq H$ ja $Ker(f) \trianglelefteq G$.*

Todistus. Seuraa suoraan lauseista 4.7.5 ja 4.7.6.

Huomautus. Jos G on ryhmä ja $N \trianglelefteq G$, niin kuvaus

$$f : G \to G/N, \ f(a) = aN$$

on surjektiivinen homomorfismi, jonka ydin on N. Kyseessä on ns. *luonnollinen homomorfismi* $G \to G/N$.

Määritelmä 4.7.9. Ryhmät $(G, \cdot)$ ja $(H, *)$ ovat *isomorfiset* eli rakenneyhtäläiset (G and H are isomorphic), mikäli on olemassa bijektio $f : G \to H$, joka toteuttaa ehdon $f(a \cdot b) = f(a) * f(b)$ aina, kun $a, b \in G$ (eli f on bijektiivinen homomorfismi). Tällöin merkitään $G \cong H$ ja sanotaan, että f on *ryhmäisomorfismi* (a group isomorphism).

Huomautus. Jos G on äärellinen ryhmä ja $G \cong H$, niin $|G| = |H|$.

Huomautus. Jos $G \cong H$ ja $H \cong N$, niin $G \cong N$.

Lause 4.7.10 (Homomorfismien peruslause)**.** *Olkoon $f : (G, \cdot) \to (H, *)$ homomorfismi. Tällöin*

$$G/Ker(f) \cong Im(f).$$

Todistus. Merkitään $Ker(f) = K$ ja määritellään kuvaus

$$F : G/K \to Im(f), \quad F(aK) = f(a).$$

1. Onko kuvaus F hyvinmääritelty (ts. onko kuvaus F riippumaton sivuluokan määrääjän valinnasta)?

   Olkoon $a'K = aK$. Tällöin $a' \in aK$ eli $a' = a \cdot k$ jollakin $k \in K$. Näin ollen

   $$F(a'K) = f(a') = f(a \cdot k) = f(a) * f(k) = f(a) * e_H = f(a) = F(aK).$$

   Siispä F on hyvinmääritelty.

2. Onko kuvaus F surjektio?

   Olkoon $f(b) \in Im(f)$. Tällöin $bK \in G/K$ ja $F(bK) = f(b)$, joten F on surjektio.

3. Onko kuvaus F injektio?

   Olkoon $F(aK) = F(bK)$, jolloin $f(a) = f(b)$. Tällöin $f(b)^{-1} * f(a) = e_H$, joten

   $$e_H = f(b)^{-1} * f(a) = f(b^{-1}) * f(a) = f(b^{-1} \cdot a).$$

   Näin ollen ytimen määritelmän nojalla $b^{-1} \cdot a \in K$ eli

   $$K = (b^{-1} \cdot a)K = b^{-1}K \cdot aK.$$

   Operoimalla yhtälöä puolittain vasemmalta sivuluokalla bK saadaan

   $$\begin{aligned} & bK * e_G K = bK \cdot b^{-1}K \cdot aK \\ \Leftrightarrow \quad & bK = aK. \end{aligned}$$

   Siispä F on injektio.

   Kohtien 2. ja 3. nojalla kuvaus F on bijektio $G/K \to Im(f)$.

4. Onko kuvaus F ryhmähomomorfismi?

   Olkoon $aK, bK \in G/K$. Tällöin

   $$F(aK \cdot bK) = F((a \cdot b)K) = f(a \cdot b) = f(a) * f(b) = F(aK) * F(bK),$$

   joten F on ryhmähomomorfismi.

Kohtien 1.-4. nojalla kuvaus F on ryhmäisomorfismi $G/Ker(f) \to Im(f)$ eli

$$G/Ker(f) \cong Im(f).$$

Lause 4.7.11. *Samaa kertalukua olevat sykliset ryhmät ovat isomorfiset.*

Todistus. Luennolla.

Lause 4.7.12. *Olkoon G ryhmä. Tällöin on olemassa sellainen permutaatioryhmä, joka on isomorfinen ryhmän G kanssa.*

Todistus. *Ryhmäteoria*-kurssilla.

Lause 4.7.13. *Olkoon G ryhmä, $N \trianglelefteq G$ ja $\{eN\} < H \triangleleft G/N$.*

Tällöin on olemassa sellainen $M \leq G$, että

$$N \triangleleft M \triangleleft G.$$

Todistus. Olkoon $f : G \to G/N$, $f(a) = aN$ (luonnollinen homomorfismi).

Merkitään $M = f^{-1}(H) = \{a \in G \mid f(a) \in H\}$.

Lauseen 4.7.6 nojalla

$$M = f^{-1}(H) \trianglelefteq G.$$

Lisäksi, jos $x \in N$, niin $f(x) = xN = eN \in H$. Siten

$$\begin{aligned} & x \in f^{-1}(H) = M \\ \text{eli} \quad & N \leq M. \end{aligned}$$

Koska $N \trianglelefteq G$, niin $N \trianglelefteq M$. Näin ollen $N \trianglelefteq M \trianglelefteq G$.

Koska $H \triangleleft G/N$, niin on olemassa sellainen $xN \in G/N$, että $xN \notin H$.

Siis

$$\begin{aligned} & f(x) = xN \notin H \\ \text{eli} \quad & x \notin f^{-1}(H) = M \quad \text{ja} \quad x \in G \\ \text{eli} \quad & M \triangleleft G. \end{aligned}$$

Vastaavasti, koska $\{eN\} < H$, niin on olemassa sellainen $yN \in H$, että $yN \neq eN$. Siis $y \notin eN = N$.

Toisaalta

$$\begin{aligned} & f(y) = yN \in H \\ \text{eli} \quad & y \in f^{-1}(H) = M. \end{aligned}$$

Siten $N \triangleleft M$.

Näin ollen $N \triangleleft M \triangleleft G$. □

Edellisessä lauseessa itse asiassa toteutuu, että $H = M/N$.

Lause 4.7.14. *Olkoon G ryhmä, $N \trianglelefteq G$, $M \trianglelefteq G$ ja $N < M \triangleleft G$.*

Tällöin

$$\{eN\} < M/N \triangleleft G/N.$$

Todistus. Olkoon $f : G \to G/N$, $f(a) = aN$ (luonnollinen homomorfismi).

Koska $N \trianglelefteq G$ ja $N < M$, niin $N \triangleleft M$, eli M/N on olemassa.

Nyt $f(M) = \{f(x) \mid x \in M\} = \{xN \mid x \in M\} = M/N$.

Koska $M \triangleleft G$, niin Lauseen 4.7.6 nojalla $M/N = f(M) \trianglelefteq G/N$ (koska f on surjektiivinen homomorfismi).

Selvästi $\{eN\} \leq M/N$. Koska $N < M$, niin on olemassa sellainen $x \in M$, että $x \notin N$.

Tällöin $xN \in M/N$ ja $xN \neq eN = N$. Siis $\{eN\} < M/N$.

Vastaavasti, koska $M \triangleleft G$, niin on olemassa sellainen $y \in G$, että $y \notin M$.

Tällöin $yN \in G/N$ ja $yN \notin M/N$. Siis $M/N \triangleleft G/N$.

Näin ollen

$$\{eN\} < M/N \triangleleft G/N.$$

□