800333A Algebra I

Luentorunko

Kevät 2010

Työryhmä: Markku Niemenmaa, Kari Myllylä,
Juha-Matti Tirilä

Sisältö

1 Lukuteorian alkeita

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):

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

Joukko $\mathbb{N}$ on *hyvin järjestetty* (well-ordered), sillä jos

$$A \neq \emptyset \qquad \text{ja} \qquad A \subseteq \mathbb{N},$$

niin joukossa A on pienin alkio.

Lause 1.1. *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 1.2. Jos $a, b \in \mathbb{Z}$, $a \neq 0$ 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*.

Määritelmä 1.3. 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 voidaan esittää muodossa $n = ab$, missä $|a|, |b| \geq 2$, niin sanotaan, että n on *yhdistetty luku* (composite number).

Lause 1.4. *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 1.1 nojalla jokainen luonnollinen luku on jotain seuraavista muodoista:
  $$4q \qquad 4q+1 \qquad 4q+2 \qquad 4q+3.$$
  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 $2^{2^n}+1$, sanotaan *Fermat'n alkuluvuksi* (Fermat prime; Pierre de Fermat 1601 – 1665).
- Alkulukua, joka on muotoa $2^n - 1$, 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.

Määritelmä 1.5. 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. $c \mid a \quad \text{ja} \quad c \mid b \Rightarrow c \mid t$,

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 1.6. *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.

Huomautus. 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).

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 1.1

nojalla

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

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 1.5 mukaisesti lukujen a ja b suurin yhteinen tekijä.

Aputulos 1.7. *Jos* $\text{syt}(a, b) = 1$ *ja* $a \mid bc$*, niin* $a \mid c$*.*

Todistus. Harjoitustehtävänä. Käytä lausetta 1.6.

Aputulos 1.8. *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* $p = b$*.*

Huomautus. 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 1.9 (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. Luennolla.

Määritelmä 1.10. 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* ja siitä käytetään lyhennysmerkintää $\text{pyj}(a, b)$.

Formaalisti $t = \text{pyj}(a, b)$, jos

1. $a \mid t$ ja $b \mid t$ ja
2. jos $a \mid c$ ja $b \mid c$, niin $t \mid c$.

Huomautus. Kahden kokonaisluvun pienimmän yhteisen jaettavan etsimiseen voidaan käyttää lauseen 1.9 mukaista kokonaisluvun esitystä alkulukujen tulona. Tästä esimerkkejä luennolla.

Huomautus. Olkoot $a, b \in \mathbb{Z}$. Tällöin $\text{pyj}(a, b) = \frac{a \cdot b}{\text{syt}(a,b)}$.

1.1 Kongruenssiin liittyviä perustuloksia

Oletetaan, että $m \in \mathbb{N} \setminus \{0\}$ ja $a, b \in \mathbb{Z}$. Jos $m \mid a - b$, niin sanotaan, että *luku a on kongruentti luvun b kanssa modulo m*. Merkitään

$$a \equiv b \pmod{m} \quad \text{tai}$$
$$a \equiv b \quad (m).$$

Lause 1.11.

1. *Olkoon $a \equiv b$ (m) sekä $c \equiv d$ (m). Tällöin $a + c \equiv b + d$ (m) ja $ac \equiv bd$ (m).*
2. *Jos $ac \equiv bc$ (m) ja $\text{syt}(c, m) = 1$, niin $a \equiv b$ (m) (ts. c voidaan "supistaa").*

Todistus. Luennolla.

Seuraus 1.12.

1. *Jos* $a \equiv b \ (m)$ *ja* $n \in \mathbb{N}$, *niin* $a^n \equiv b^n \ (m)$;
2. $ac \equiv bc \ (mc) \Leftrightarrow a \equiv b \ (m)$.

Todistus. Luennolla.

Lause 1.13.

1. *Jos* $a \equiv b \ (m)$ *ja* $b \equiv c \ (m)$, *niin* $a \equiv c \ (m)$;
2. *Aina* $a \equiv a \ (m)$;
3. *Jos* $a \equiv b \ (m)$ *ja* $c \in \mathbb{Z}$, *niin* $ac \equiv bc \ (m)$;
4. *Jos* $a \equiv b \ (m)$, *niin* $b \equiv a \ (m)$;
5. $m \mid a \Leftrightarrow a \equiv 0 \ (m)$;
6. *Olkoon* $a \equiv b \ (m)$. *Tällöin*
$$a + km \equiv b \ (m) \quad \text{aina, kun} \quad k \in \mathbb{Z};$$
7. $a \equiv a + km \ (m)$ *aina, kun* $k \in \mathbb{Z}$;
8. *Olkoon* $a \equiv b \ (m)$. *Tällöin*
$$m \mid a \quad \text{jos ja vain jos} \quad m \mid b.$$

Kongruenssien avulla saadaan jaollisuussääntöjä (todistukset luennolla):

1. Kolmen jaollisuussääntö: Jos luvun numeroiden summa on kolmella jaollinen, niin itse luku on kolmella jaollinen.
2. Yhdeksän jaollisuussääntö: Jos luvun numeroiden summa on jaollinen yhdeksällä, niin luku 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 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 luku

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

on jaollinen luvulla 11.

Lause 1.14. *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* $x \equiv x_0 \ (m)$.

Todistus. Luennolla.

Seuraus 1.15. *Olkoon* $\text{syt}(a, m) = d > 1$. *Kongruenssiyhtälöllä* $ax \equiv b \ (m)$ *on ratkaisuja täsmälleen silloin, kun* $d \mid b$. *Jos* x_0 *on jokin ratkaisu, niin kaikki ratkaisut ovat* $x \equiv x_0 \ (\frac{m}{d})$.

Todistus. Luennolla.

Huomautus. Ratkaistaessa lauseen 1.14 oletukset täyttävää kongruenssia etsitään ensin yksi ratkaisu Eukleideen algoritmin avulla ja käytetään sitten kaikkien ratkaisujen muotoilemiseen lauseen jälkimmäistä osaa. Tästä esimerkkejä luennolla.

2 Ekvivalenssirelaatio

Määritelmä 2.1. 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 2.2. 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 2.3. Joukon A binäärinen relaatio R on *ekvivalenssirelaatio*, mikäli

1. $x\,R\,x$ aina, kun $x \in A$;
2. $x\,R\,y \Rightarrow y\,R\,x$ aina, kun $x, y \in A$;
3. $x\,R\,y$ ja $y\,R\,z \Rightarrow x\,R\,z$ aina, kun $x, y, z \in A$.

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

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

sanotaan *alkion a määräämäksi ekvivalenssiluokaksi.*

Lause 2.4. *Jos R on ekvivalenssirelaatio ja $a\,R\,b$, niin $[a] = [b]$.*

Todistus. Luennolla.

Lause 2.5. *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.

Luennolla tarkastellaan kokonaislukujoukossa määriteltävää relaatiota

$$x\,R\,y \Leftrightarrow x \equiv y \pmod{m}, \quad \text{missä } x, y \in \mathbb{Z} \text{ ja } m \in \mathbb{Z}_+.$$

Tämä relaatio on ekvivalenssirelaatio, jonka määräämiä ekvivalenssiluokkia kutsutaan *jäännösluokiksi modulo* m. Alkion y määräämästä jäännösluokasta *modulo* m käytetään merkintää

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

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

3 Ryhmät

3.1 Ryhmäteorian alkeita

Määritelmä 3.1.1. 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 $a, b \in S$).

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

Määritelmä 3.1.3. Olkoot $G \neq \emptyset$ ja $(*)$ joukon G binäärinen operaatio. Pari $(G, *)$ on *ryhmä* (group), mikäli seuraavat kolme ehtoa toteutuvat:

1. $(*)$ on assosiatiivinen eli

   $$(a * b) * c = a * (b * c)$$

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

2. Joukossa G on sellainen alkio e, että

   $$a * e = e * a = a$$

   aina, kun $a \in G$. Alkiota e kutsutaan *ykkös- tai neutraalialkioksi* (identity/neutral element);

3. 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 $(G, *)$ toteuttaa ehdon

4. $a * b = b * a$ aina, kun $a, b \in G$ eli $(*)$ on kommutatiivinen,

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

1. *ykkösalkio 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 3.1.5. *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. Äärellisessä ryhmässä (finite group) on äärellinen määrä alkioita ja siis myös ryhmäoperaation tuloksia. Siispä tällaisessa tapauksessa voidaan kirjoittaa *ryhmätaulu* (group table), johon merkitään kaikkien ryhmäoperaatioiden tulokset omiin soluihinsa; yksityiskohdat esitetään luennolla.

3.2 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 3.2.1. *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 1.14).

Määritelmä 3.2.2. Jäännösluokkaa $[a]$ *(mod* m*)* sanotaan *alkuluokaksi* $\pmod m$, mikäli $\text{syt}(a, m) = 1$. Alkuluokkien joukkoa merkitään $\mathbb{Z}_m^*$.

Huomautus. Jos p on alkuluku, niin

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

Lause 3.2.3. *Pari* $(\mathbb{Z}_m^*, \cdot)$ *on Abelin ryhmä.*

Todistus. Luennolla.

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

Määritelmä 3.2.4. Funktio $\varphi : \mathbb{Z}_+ \to \mathbb{Z}_+$, $\varphi(m) = |\mathbb{Z}_m^*|$ on *Eulerin φ-funktio*. Siis $\varphi(m)$ kertoo alkioiden määrän joukossa

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

Lause 3.2.5. *Jos p on alkuluku ja $k \in \mathbb{N}$, niin $\varphi(p^k) = p^{k-1}(p-1)$.*

Todistus. Luennolla.

Lause 3.2.6. *Jos* $\operatorname{syt}(m, n) = 1$, *niin $\varphi(mn) = \varphi(m)\varphi(n)$.*

Todistus. Luennolla.

Lause 3.2.7 (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. Luennolla.

3.3 Aliryhmä

Määritelmä 3.3.1. 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 $H \leq G$.

Lause 3.3.2 (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 3.3.3. *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.

Seuraus 3.3.4. *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 $a, b \in H$.*

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

Määritelmä 3.3.5. Olkoon $H \leq G$ ja $a \in G$. Joukkoa $aH = \{ah \mid h \in H\}$ 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 $eH = H$ (additiivisessa tapauksessa $e + H = H$), 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

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

Lause 3.3.6. *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 on aH.

Todistus. Luennolla.

Lause 3.3.7 (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.

Huomautus. Lauseesta 3.3.7 seuraa, että jos äärellisen ryhmän G kertaluku on alkuluku, niin sen ainoat mahdolliset aliryhmät ovat $\{e\}$ ja G (nk. triviaalit aliryhmät).

3.4 Syklinen ryhmä

Olkoon G ryhmä ja $a \in G$. Nyt 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

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

Siis H on seurauksen 3.3.3 nojalla ryhmän G aliryhmä.

Määritelmä 3.4.1. Yllä määriteltyä ryhmää H sanotaan *alkion a generoimaksi sykliseksi ryhmäksi* (cyclic group); merkitään $H = \langle a \rangle$. Alkio a on *generoija* (generator).

Lause 3.4.2. *Jos ryhmän kertaluku on alkuluku, niin ryhmä on syklinen.*

Todistus. Luennolla.

Huomautus. Ryhmä $(\mathbb{Z}_m^*, \cdot)$ ei välttämättä ole syklinen; vrt. edellinen lause.

Lause 3.4.3. *Olkoot G ryhmä ja $a \in G$ sekä n pienin sellainen positiivinen kokonaisluku, että $a^n = e$. Tällöin $|\langle a \rangle| = n$. Jos G on äärellinen ryhmä, niin $a^{|G|} = e$.*

Todistus. Luennolla.

Huomautus. Lauseen 3.4.3 mukaista lukua n sanotaan alkion a *kertaluvuksi*; alkion kertaluvusta käytetään merkintää $|\langle a \rangle|$, $|a|$ tai $ord(a)$.

Lause 3.4.4. *Jos $a, m \in \mathbb{Z}_+$ ja $\text{syt}(a, m) = 1$, niin*

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

Todistus. Luennolla.

Seuraus 3.4.5 (Fermat'n pieni lause)**.** *Jos p on alkuluku ja $\text{syt}(a, p) = 1$, niin $a^{p-1} \equiv 1(p)$.*

Lause 3.4.6. *Syklisen ryhmän jokainen aliryhmä on syklinen.*

Todistus. Luennolla.

Huomautus. Syklinen ryhmä on aina Abelin ryhmä.

3.5 Normaali aliryhmä ja tekijäryhmä

Määritelmä 3.5.1. Olkoon $N \leq G$. Aliryhmää N sanotaan *normaaliksi*, mikäli $aN = Na$ aina, kun $a \in G$. Tällöin merkitään $N \trianglelefteq G$.

Huomautus.

- $\{e\} \trianglelefteq G$ ja $G \trianglelefteq G$.
- Jos G on Abelin ryhmä ja $N \leq G$, niin

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

  Siis Abelin ryhmän jokainen aliryhmä on normaali.

Lause 3.5.2. *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 tulo $(\cdot)$ seuraavasti:

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

Näin saatu tulo 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 tulon kanssa on ryhmä. Näiden väitteiden paikkansapitävyys todistetaan luennolla.

Lause 3.5.3. *Olkoon G ryhmä ja $N \trianglelefteq G$. Tällöin $(\{aN \mid a \in G\}, \cdot)$ on ryhmä.*

Todistus. Luennolla.

Määritelmä 3.5.4. 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.

3.6 Ryhmähomomorfismi

Määritelmä 3.6.1. 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 3.6.2. *Olkoon $f : G \to H$ homomorfismi 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.

Lause 3.6.3. *Olkoon $f : G \to H$ homomorfismi. Jos $D \leq G$, niin $f(D) \leq H$, ja jos $T \leq H$, niin $f^{-1}(T) \leq G$.*

Todistus. Luennolla.

Huomautus.

- $f(D) = \{f(x) \mid x \in D\}$ on aliryhmän $D \leq G$ *kuva* (image) ryhmässä H.
- $f^{-1}(T) = \{x \in G \mid f(x) \in T\}$ on aliryhmän $T \leq H$ *alkukuva* (pre-image) ryhmässä G.
- 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 3.6.4. *Olkoon $f : G \to H$ ryhmähomomorfismi. Jos $N \trianglelefteq G$ ja f on surjektio, niin $f(N) \trianglelefteq H$. Jos $M \trianglelefteq H$, niin $f^{-1}(M) \trianglelefteq G$.*

Todistus. Luennolla.

Määritelmä 3.6.5. 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

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

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

Huomautus.

- Lauseiden 3.6.3 ja 3.6.4 nojalla $Im(f) \leq H$ ja $Ker(f) \trianglelefteq G$.
- 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 3.6.6. 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).

Lause 3.6.7 (Homomorfismien peruslause). *Olkoon $f : G \to H$ homomorfismi. Tällöin*

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

Todistus. Luennolla.

Huomautus. Samaa kertalukua olevat sykliset ryhmät ovat isomorfiset.

3.7 Permutaatioryhmistä

Määritelmä 3.7.1. Olkoon $X \neq \emptyset$. Bijektiota $f : X \to X$ sanotaan joukon X *permutaatioksi* (permutation).

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

Lause 3.7.2. *Olkoon S_X joukon X kaikkien permutaatioiden joukko. Jos $(\circ)$ on kuvausten yhdistämisoperaatio, niin $(S_X, \circ)$ on ryhmä.*

Todistus. Luennolla.

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. Permutaatioryhmistä ja niiden sovelluksista tarkemmin kurssilla *Algebra II*.

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

Lause 3.7.3. *Olkoon G ryhmä. Tällöin on olemassa sellainen permutaatioryhmä, joka on isomorfinen ryhmän G kanssa.*

Todistus. *Ryhmäteoria*-kurssilla.

4 Renkaat ja kunnat

4.1 Renkaiden teoriaa

Määritelmä 4.1.1. Kolmikko $(R, +, \cdot)$ on *rengas* (ring), mikäli

1. $(R, +)$ on Abelin ryhmä.
2. $(R, \cdot)$ on puoliryhmä (eli $(\cdot)$ on assosiatiivinen binäärinen operaatio joukossa R), jossa on ykkösalkio $\mathbf{1}$.
3. Seuraavat distributiivisuus- eli osittelulait ovat voimassa:

$$a \cdot (b + c) = a \cdot b + a \cdot c \qquad \text{ja}$$
$$(a + b) \cdot c = a \cdot c + b \cdot c$$

aina, kun $a, b, c \in R$.

Lisäksi rengasta sanotaan *kommutatiiviseksi*, mikäli se on kommutatiivinen tulo-operaationsa suhteen, ts. jos $a \cdot b = b \cdot a$ aina, kun $a, b \in R$.

Jatkossa tulosta $a \cdot b$ käytetään lyhyempää merkintää ab.

Lause 4.1.2. *Olkoot R rengas, a, b ja c joukon R alkioita sekä $\mathbf{0}$ summaoperaation nolla-alkio renkaassa R. Tällöin*

1. $\mathbf{0}a = a\mathbf{0} = \mathbf{0}$;
2. $a(-b) = (-a)b = -(ab)$;
3. $(-a)(-b) = ab$;
4. $a(b - c) = ab - ac \qquad ja \qquad (a - b)c = ac - bc.$

Todistus. Luennolla.

Määritelmä 4.1.3. Olkoot $(R, +, \cdot)$ rengas ja $\emptyset \neq S \subseteq R$. Jos $(S, +, \cdot)$ on rengas, jolla on sama ykkösalkio kuin renkaalla R, niin sitä sanotaan renkaan R *alirenkaaksi* (subring).

Huomautus. Renkaan $(R, +, \cdot)$ ei-tyhjä osajoukko S on renkaan R alirengas jos ja vain jos

1. $a, b \in S \Rightarrow a - b \in S$;
2. $a, b \in S \Rightarrow ab \in S$;
3. $\mathbf{1}_R \in S$.

Määritelmä 4.1.4. Renkaan $(R, +, \cdot)$ ei-tyhjä osajoukko I on *ideaali* (ideal), mikäli

1. $(I, +) \leq (R, +)$;
2. $ra \in I$ ja $ar \in I$ aina, kun $a \in I$ ja $r \in R$.

Huomautus. Jos I on renkaan R ideaali ja $\mathbf{1} \in I$, niin $I = R$.

Määritelmä 4.1.5. Jos $(R, +, \cdot)$ on rengas ja $a \in R$, niin suppeinta ideaalia, joka sisältää alkion a, sanotaan alkion a generoimaksi *pääideaaliksi* (principal ideal). Kyseisestä ideaalista käytetään merkintää (a).

Lause 4.1.6. *Jos $(R, +, \cdot)$ on kommutatiivinen rengas ja $a \in R$, niin*

$$(a) = Ra = \{ra \mid r \in R\}.$$

Todistus. Luennolla.

Lause 4.1.7. *Renkaan $(\mathbb{Z}, +, \cdot)$ jokainen ideaali on pääideaali.*

Todistus. Luennolla.

Huomautus. Jos renkaan $(R, +, \cdot)$ jokainen ideaali on pääideaali, niin R on *pääideaalirengas* (principal ideal ring).

Määritelmä 4.1.8. Renkaan $(R, +, \cdot)$ ideaali M on *maksimaalinen*, mikäli

1. $M \neq R$;
2. jos I on renkaan R ideaali ja $M \subset I \subseteq R$, niin $I = R$.

(Siis M on laajin mahdollinen renkaan R aito ideaali.)

Ongelma. Tiedetään, että renkaan $(\mathbb{Z}, +, \cdot)$ kaikki ideaalit ovat pääideaaleja. Millaiset pääideaalit ovat maksimaalisia ideaaleja?

Lause 4.1.9. *Renkaan $(\mathbb{Z}, +, \cdot)$ maksimaalisia ideaaleja ovat tarkalleen ne pääideaalit (p), missä p on alkuluku.*

Todistus. Luennolla.

Jos I on renkaan $(R, +, \cdot)$ ideaali, niin $(R/I, +)$ on tekijäryhmä, jonka alkioina ovat sivuluokat $r + I = \{r + x \mid x \in I\}$, $r \in R$. Kun määritellään

$$(a + I) \cdot (b + I) = ab + I,$$

niin saadaan rengas $(R/I, +, \cdot)$, jota kutsutaan renkaan $(R, +, \cdot)$ tekijärenkaaksi ideaalin I suhteen. (Tarkempi tarkastelu luennolla.)

Määritelmä 4.1.10. Renkaan $(R, +, \cdot)$ nolla-alkiosta eroava alkio a on renkaan R *nollanjakaja*, jos renkaassa R on sellainen nolla-alkiosta eroava alkio b, että $\quad ab = \mathbf{0} \quad$ tai $\quad ba = \mathbf{0}$.

Määritelmä 4.1.11. Kommutatiivista rengasta, jossa ei ole nollanjakajia, sanotaan *kokonaisalueeksi*.

Esimerkki.

- Rengas $(\mathbb{Z}, +, \cdot)$ on kokonaisalue.
- Rengas $(\mathbb{Z}_4, +, \cdot)$ ei ole kokonaisalue.

Lause 4.1.12. *Olkoon* $(R, +, \cdot)$ *kokonaisalue ja* $a \in R$, $a \neq \mathbf{0}$. *Tällöin*

$$ab = ac \Rightarrow b = c \quad ja$$
$$ba = ca \Rightarrow b = c.$$

4.2 Kuntien teoriaa

Määritelmä 4.2.1. Kommutatiivista rengasta $(K, +, \cdot)$ sanotaan *kunnaksi* (field), mikäli $(K \setminus \{\mathbf{0}\}, \cdot)$ on Abelin ryhmä. Ryhmä $(K \setminus \{\mathbf{0}\}, \cdot)$ on kunnan *multiplikatiivinen ryhmä* ja ryhmä $(K, +)$ on kunnan *additiivinen ryhmä*.

Lause 4.2.2. *Jäännösluokkarengas $(\mathbb{Z}_n, +, \cdot)$ on kunta tarkalleen silloin, kun n on alkuluku.*

Todistus. Luennolla.

Määritelmä 4.2.3. Äärellisen kunnan $(K, +, \cdot)$ ykkösalkion $\mathbf{1}$ additiivista kertalukua sanotaan kunnan *karakteristikaksi*, merk. char K. Siis char K on pienin positiivinen kokonaisluku n, joka toteuttaa ehdon $n\mathbf{1} = \mathbf{0}$ (char K on siis alkion $\mathbf{1}$ kertaluku ryhmässä $(K, +)$).

Huomautus.

- Äärellisen kunnan karakteristika on välttämättä alkuluku; todistus luennolla.
- Jos kunnan $(K, +, \cdot)$ karakteristika on alkuluku p ja $a \in K$, niin $pa = \mathbf{0}$; todistus luennolla.
- Kunta $(K, +, \cdot)$ on kokonaisalue.

Yleisesti voidaan todistaa, että jokaisen äärellisen kunnan $(K, +, \cdot)$ kertaluku on p^n, missä p on alkuluku ja $n \geq 1$. Tällöin char $K = p$. Samoin voidaan osoittaa, että samaa kertalukua olevat kunnat ovat keskenään isomorfisia.

Jos kunnan kertaluku on p^n, missä p on alkuluku ja $n \in \mathbb{Z}_+$, niin kyseisestä kunnasta käytetään merkintää $GF(p^n)$ ja sitä kutsutaan *Galois'n kunnaksi kertalukua* p^n (Galois field of order p^n). Voidaan myös todistaa, että muita äärellisiä kuntia ei ole olemassa.

Tutkitaan lopuksi hieman renkaiden ja kuntien välistä suhdetta.

Huomautus. Kunnan $(K, +, \cdot)$ ainoat ideaalit ovat $(\mathbf{0})$ ja K.

Lause 4.2.4. *Olkoon $(R, +, \cdot)$ kommutatiivinen rengas, jonka ainoat ideaalit ovat $(\mathbf{0})$ ja R (triviaalit ideaalit). Tällöin $(R, +, \cdot)$ on kunta.*

Todistus. Luennolla.

Lause 4.2.5. *Olkoon $(R, +, \cdot)$ kommutatiivinen rengas ja M renkaan R maksimaalinen ideaali. Tällöin tekijärengas R/M on kunta.*

Todistus. Luennolla tai kurssilla *Algebra II*.

4.3 Polynomirengas

Määritelmä 4.3.1. Olkoon $(K, +, \cdot)$ kunta. Merkitään

$$K[x] = \{a_n x^n + \ldots + a_1 x + a_0 \mid a_i \in K, n \geq 0\}.$$

Tämän joukon alkioita kutsutaan K-kertoimisiksi polynomeiksi ja koko joukkoa $K[x]$ varustettuna polynomien yhteen- ja kertolaskulla *polynomirenkaaksi kunnan K suhteen* (the ring of polynomials in x over K); merkitään $(K[x], +, \cdot)$.

Määritelmä 4.3.2. Olkoon K kunta. Jos

$$f(x) = a_n x^n + \ldots + a_1 x + a_0 \in K[x] \qquad \text{ja} \qquad a_n \neq \mathbf{0},$$

niin kyseisen polynomin *aste* on n; merkitään $\deg\ f(x) = n$. Edelleen, jos $a \neq \mathbf{0}$, niin vakiopolynomin $f(x) = a$ aste on nolla, ts. $\deg\ a = 0$. Sovitaan lisäksi, että $\deg\ \mathbf{0} = -\infty$.

Lause 4.3.3. *Jos $f(x), g(x) \in K[x]$, niin*

$$\deg\ (f(x) \cdot g(x)) = \deg\ f(x) + \deg\ g(x).$$

Todistus. Luennolla

Lause 4.3.4 (Jakoalgoritmi polynomeille)**.** *Mikäli $f(x), g(x) \in K[x]$ sekä $g(x) \neq \mathbf{0}$ (nollapolynomi), niin*

$$f(x) = q(x)g(x) + r(x),$$

missä $q(x), r(x) \in K[x]$ ovat yksikäsitteiset ja $\deg\ r(x) < \deg\ g(x)$.

Todistus. Luennolla

Määritelmä 4.3.5. Jos $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in K[x]$ ja $\alpha \in K$ sekä

$$f(\alpha) = a_n \alpha^n + \ldots + a_1 \alpha + a_0 = \mathbf{0},$$

niin α on polynomin $f(x)$ *nollakohta* (tai yhtälön $f(x) = \mathbf{0}$ juuri).

Määritelmä 4.3.6. Jos $f(x), g(x) \in K[x]$ ja

$$f(x) = q(x)g(x) \text{ eräällä } q(x) \in K[x],$$

niin sanotaan, että $g(x)$ *jakaa polynomin* $f(x)$. Merkitään $g(x) \mid f(x)$.

Lause 4.3.7. *Olkoot $f(x) \in K[x]$ ja $\alpha \in K$. Tällöin*

$$f(\alpha) = \mathbf{0} \Leftrightarrow (x - \alpha) \mid f(x).$$

Todistus. Luennolla

Määritelmä 4.3.8. Polynomi $f(x) \in K[x]$ on *jaoton* (irreducible) polynomirenkaassa $K[x]$, mikäli deg $f(x) \geq 1$ ja polynomia f ei voida esittää kahden positiivista astetta olevan polynomin tulona polynomirenkaassa $K[x]$.

Lause 4.3.9. *Olkoon $f(x) \in K[x]$ ja* deg $f(x) = 2$ *tai* deg $f(x) = 3$. *Tällöin $f(x)$ on jaoton jos ja vain jos sillä ei ole nollakohtaa kunnassa K.*

Todistus. Luennolla

Luennolla annetaan esimerkki neljännen asteen reaalipolynomista, joka on jaollinen, mutta jolla ei ole reaalisia nollakohtia.

Lause 4.3.10. *Olkoon $f(x) \in K[x]$. Jos* deg $f(x) = n$, *niin polynomilla $f(x)$ on korkeintaan n nollakohtaa kunnassa K.*

Todistus. Luennolla

Lause 4.3.11. *Olkoon K kunta. Polynomirenkaan $K[x]$ jokainen ideaali on pääideaali.*

Todistus. Luennolla.

Lause 4.3.12. *Jos $p(x) \in K[x]$ on jaoton polynomi, niin $(p(x))$ on renkaan $K[x]$ maksimaalinen ideaali.*

Todistus. Luennolla.

Seuraus 4.3.13. *Jos K on kunta ja $p(x)$ on polynomirenkaan $K[x]$ jaoton polynomi, niin tekijärengas*

$$K[x]/(p(x)) \quad \text{on kunta.}$$

Yllä esitetty seuraus antaa menetelmän kuntalaajennuksen konstruointiin (esimerkkejä luennolla).

4.4 Osamääräkunta

Tarkennetaan hieman rationaalilukujen ja rationaalifunktioiden käsitteitä ja sitä kautta niillä operointia.

Määritelmä 4.4.1. Olkoon D kokonaisalue ja $a, b, c, d \in D$, $b \neq \mathbf{0}$, $d \neq \mathbf{0}$. Asetetaan relaatio

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

Lause 4.4.2. *Relaatio $\sim$ on ekvivalenssirelaatio joukossa*

$$D \times (D \setminus \{\mathbf{0}\}) = \mathcal{D}.$$

Määritelmä 4.4.3. Ekvivalenssiluokille

$$[a, b] = \{(c, d) \in \mathcal{D} \mid (c, d) \sim (a, b)\}$$

sovitaan yhteenlasku

$$[a_1, b_1] + [a_2, b_2] = [a_1 b_2 + a_2 b_1, b_1 b_2]$$

ja kertolasku

$$[a_1, b_1]\,[a_2, b_2] = [a_1 a_2, b_1 b_2]$$

aina, kun $(a_1, b_1), (a_2, b_2) \in \mathcal{D}$.

Merkitään vielä

$$a/b = \frac{a}{b} = [a, b] \quad \text{ja} \quad Q(D) = \{a/b \mid (a, b) \in \mathcal{D}\}.$$

Voidaan todistaa, että

Lause 4.4.4. *Kolmikko $(Q(D), +, \cdot)$ on kunta.*

Sanotaan, että $Q(D)$ on kokonaisalueen D *osamääräkunta* (quotient field, field of fractions).

Tällöin pätee rengasisomorfiatulos

$$\{[a, \mathbf{1}] \mid a \in D\} = \left\{\frac{a}{\mathbf{1}} \mid a \in D\right\} \cong D,$$

jonka nojalla voidaan merkitä $a = a/\mathbf{1}$. Edelleen,

$$ab^{-1} = \frac{a}{\mathbf{1}}\left(\frac{b}{\mathbf{1}}\right)^{-1} = \frac{a}{\mathbf{1}}\frac{\mathbf{1}}{b} = \frac{a}{b}.$$

Lisäksi suoraan määritelmästä seuraa, että supistamis- ja laventamislait

$$\frac{ac}{bc} = \frac{a}{b} \qquad \text{ja} \qquad \frac{a}{b} = \frac{da}{db}$$

ovat voimassa.

Määritelmä 4.4.5. Rationaalilukujen kunta $\mathbb{Q} = Q(\mathbb{Z})$.

Määritelmä 4.4.6. Rationaalifunktioiden kunta $K(x) = Q(K[x])$.

Tällöin pätevät yllä esitetyt supistamis- ja laventamissäännöt, jolloin esimerkiksi

$$\frac{(x^2-1)\,x}{(x-1)\,x^2} = \frac{x+1}{x} = 1 + \frac{1}{x}.$$