Algebra II

Syksy 2004

Pentti Haukkanen

Sisällys

1 Ryhmäteoriaa **3**
1.1 Ryhmän määritelmä . . . 3
1.2 Aliryhmä . . . 3
1.3 Sivuluokat . . . 4
1.4 Sykliset ryhmät . . . 7
1.5 Ryhmäisomorfismi . . . 11

2 Polynomeista **14**
2.1 Renkaan määritelmä . . . 14
2.2 Polynomirengas . . . 14
2.3 Polynomien jaollisuus . . . 18

3 Tekijästruktuureista **21**
3.1 Tekijäjoukko ja luonnollinen projektio . . . 21
3.2 Laskutoimituksen ja ekvivalenssin yhteensopivuus . . . 22
3.3 Normaali aliryhmä . . . 24
3.4 Tekijäryhmä . . . 25
3.5 Johdatusta homomorfialauseeseen . . . 27
3.6 Homomorfialause . . . 29
3.7 Renkaan ihanne . . . 31
3.8 Tekijärengas . . . 34

1 Ryhmäteoriaa

1.1 Ryhmän määritelmä

Määritelmä Olkoon $(G, \star)$ algebrallinen struktuuri. Silloin $(G, \star)$ on ryhmä, jos

1) laskutoimitus $\star$ on assosiatiivinen,

2) joukossa G on neutraalialkio laskutoimituksen $\star$ suhteen,

3) jokaisella alkiolla $a \in G$ on käänteisalkio.

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

1.2 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 1.2.1 (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 Harjoitustehtävä.

Esimerkki 1.2.1 Selvästi $(\mathbf{Z}, +) \leq (\mathbf{R}, +)$.

Esimerkki 1.2.2 Merkitään $m\mathbf{Z} = \{mk \colon k \in \mathbf{Z}\}$. Silloin $(m\mathbf{Z}, +) \leq (\mathbf{Z}, +)$.

Esimerkki 1.2.3 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 1.2.1 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 1.2.1 perusteella $A \cap B \leq G$. □

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

Lause 1.2.2 (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 "$\Rightarrow$" (Totea!) "$\Leftarrow$" Olkoot a, $b \in H$ mielivaltaisia. Kaavan (2) nojalla jonon $a \star b$, $a \star b^2$, $a \star b^3$, ... kaikki jäsenet ovat joukon H alkioita. Koska H on äärellinen, niin on olemassa sellaiset m ja n, että

$$a \star b^m = a \star b^n,$$

missä $m < n$. Silloin

$$a \star b^{-1} = a \star b^{n-m-1}.$$

Koska $n - m - 1 \geq 0$, niin $a \star b^{n-m-1} \in H$ eli $a \star b^{-1} \in H$. Täten lauseen 1.2.1 perusteella $H \leq G$. $\square$

Esimerkki 1.2.4 $(\{\overline{0}, \overline{3}\}, +) \leq (\mathbf{Z}_6, +)$. (Totea!)

Esimerkki 1.2.5 $(\{\overline{0}, \overline{4}\}, +) \not\leq (\mathbf{Z}_6, +)$. (Totea!)

1.3 Sivuluokat

Määritelmä Olkoon $(G, \star)$ ryhmä ja $(H, \star)$ sen aliryhmä. Silloin alkion $a \in G$ määräämä *vasen sivuluokka* modulo H on

$$a \star H = \{a \star h |\ h \in H\}.$$

Vastaavasti *oikea sivuluokka* modulo H on

$$H \star a = \{h \star a |\ h \in H\}.$$

Kaikki vasemmat ja oikeat sivuluokat saadaan, kun a käy läpi joukon G.

Huomautus On helppo todeta, että

1) $e \star H = H$,

2) $a \in a \star H$ ja $a \in H \star a$ aina, kun $a \in G$,

3) jos G on Abelin ryhmä, niin $a \star H = H \star a$ aina, kun $a \in G$,

4) jos G ei ole Abelin ryhmä, niin yleensä $a \star H \neq H \star a$. Konstruoi esimerkki tällaisesta tilanteesta.

Esimerkki 1.3.1 Kun $(G, \star) = (\mathbf{Z}, +)$ ja $H = m\mathbf{Z}$ $(m \geq 2)$, niin vasemmat sivuluokat modulo $m\mathbf{Z}$ ovat muotoa $a + m\mathbf{Z}$, missä

$$\begin{aligned} a + m\mathbf{Z} &= \{a + h |\ h \in m\mathbf{Z}\} \\ &= \{a + mk |\ k \in \mathbf{Z}\} \\ &= \{x |\ x \equiv a \pmod{m}\} \\ &= \overline{a}. \end{aligned}$$

Siis ryhmän $(\mathbf{Z}, +)$ vasemmat sivuluokat modulo $m\mathbf{Z}$ ovat samat kuin jäännösluokat modulo m. Koska $(\mathbf{Z}, +)$ on Abelin ryhmä, niin oikeat sivuluokat ovat samat kuin vasemmat.

Määritelmä Olkoon $(G, \star)$ ryhmä ja $H \leq G$. Silloin sanotaan, että alkiot a, $b \in G$ ovat *vasemmanpuoleisesti kongruentteja* modulo H, jos

$$a \in b \star H.$$

Silloin merkitään

$$a \equiv_L b \pmod{H}.$$

Vastaavasti määritellään $a \equiv_R b \pmod{H}$, jos $a \in H \star b$.

Huomautus Jos $(G, \star)$ on Abelin ryhmä, niin relaatiot $\equiv_L$ ja $\equiv_R \pmod{H}$ ovat samat. Nimittäin silloin $b \star H = H \star b$ aina, kun $b \in G$.

Esimerkki 1.3.2 Ryhmässä $(\mathbf{Z}, +)$ relaatiot $\equiv_L$ ja $\equiv_R \pmod{m\mathbf{Z}}$ ovat samat kuin kongruenssirelaatio $\equiv \pmod{m}$.

Lause 1.3.1 *Relaatiot* $\equiv_L$ *ja* $\equiv_R \pmod{H}$ *ovat ekvivalenssirelaatioita joukossa* G.

Todistus Todistetaan väite relaatiolle $\equiv_L \pmod{H}$.

1) Koska $e \in H$, niin $a \in a \star H$ eli $a \equiv_L a \pmod{H}$ aina, kun $a \in G$.

2) Oletetaan, että $a \equiv_L b \pmod{H}$. Silloin $a = b \star h$, missä $h \in H$. Koska $(H, \star)$ on ryhmä, niin $h^{-1} \in H$. Näin ollen $b = a \star h^{-1}$, missä $h^{-1} \in H$. Siis $b \equiv_L a \pmod{H}$.

3) Oletetaan, että $a \equiv_L b \pmod{H}$ ja $b \equiv_L c \pmod{H}$. Silloin $a = b \star h_1$ ja $b = c \star h_2$, missä h_1, $h_2 \in H$. Näin ollen $a = (c \star h_1) \star h_2 = c \star (h_1 \star h_2)$. Koska $h_1 \star h_2 \in H$, niin $a \equiv_L c \pmod{H}$. $\square$

Lause 1.3.2 *Ekvivalenssirelaation* $\equiv_L \pmod{H}$ *ekvivalenssiluokat ovat vasemmat sivuluokat modulo* H. *Vastaavasti ekvivalenssirelaation* $\equiv_R \pmod{H}$ *ekvivalenssiluokat ovat oikeat sivuluokat modulo* H.

Todistus Harjoitustehtävä.

Esimerkki 1.3.3 Kun $(G, \star) = (\mathbf{Z}, +)$ ja $H = m\mathbf{Z}$ $(m \geq 2)$, niin vasemmat sivuluokat modulo $m\mathbf{Z}$ ovat samat kuin jäännösluokat modulo m.

Huomautus Koska vasemmat sivuluokat ovat ekvivalenssiluokkia, niin

1) kaksi vasenta sivuluokkaa ovat joko samat tai erilliset,

2) $a \star H = b \star H \Leftrightarrow a \equiv_L b \pmod{H} \Leftrightarrow a \in b \star H \Leftrightarrow b \in a \star H$,

3) vasemmat sivuluokat muodostavat joukon G osituksen,

4) Kohdat 1-3 ovat voimassa myös oikeille sivuluokille.

Lause 1.3.3 *Jokaisella sivuluokalla (sekä vasemmalla että oikealla) modulo H on sama kardinaaliluku. Erikoisesti jos H on äärellinen, niin sivuluokkien modulo H alkioiden lukumäärät ovat samat.*

Todistus Kuvaukset $f\colon H \to a \star H$, $f(h) = a \star h$, ja $g\colon H \to H \star a$, $g(h) = h \star a$, ovat bijektioita aina, kun $a \in G$. (Totea!) $\square$

Esimerkki 1.3.4 Jokainen jäännösluokka modulo m on numeroituvasti ääretön.

Merkintä Merkitään lyhyesti

$$G/H = (G/ \equiv_L \pmod{H}).$$

Siis lauseen 1.3.2 perusteella G/H on ryhmän $(G, \star)$ vasempien sivuluokkien joukko modulo H, ts.

$$G/H = \{a \star H |\ a \in G\}.$$

Lisäksi merkitään lyhyesti

$$H\backslash G = (G/ \equiv_R \pmod{H}).$$

Siis $H\backslash G$ on ryhmän $(G, \star)$ oikeiden sivuluokkien joukko modulo H.

Esimerkki 1.3.5 Esimerkin 1.3.3 ja Algebra I:n perusteella $\mathbf{Z}/m\mathbf{Z} = \mathbf{Z}_m = \left\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\right\}$.

Merkintä Joukon A alkioiden lukumäärää merkitään symbolilla $|A|$.

Lause 1.3.4 *Olkoon $(G, \star)$ äärellinen ryhmä ja $H \leq G$. Olkoon $|G/H| = k$. Silloin*

$$|G| = k|H|.$$

Todistus Olkoot $a_1 \star H$, $a_2 \star H$, $\ldots$, $a_k \star H$ ryhmän $(G, \star)$ erisuuret sivuluokat modulo H. Silloin ne muodostavat joukon G osituksen ja lauseen 1.3.3 mukaan jokaisen sivuluokan alkioiden lukumäärä on $|H|$. Siis

$$|G| = \sum_{i=1}^{k} |a_i \star H| = \sum_{i=1}^{k} |H| = k|H|.$$

Näin olemme todistaneet lauseen 1.3.4. □

Seuraus (Lagrangen lause) Jos $(G, \star)$ on äärellinen ryhmä ja $H \leq G$, niin joukon H alkioitten lukumäärä on joukon G alkioitten lukumäärän tekijä, ts.

$$|H| \Big| |G|.$$

Esimerkki 1.3.6 Jos $|G|$ on alkuluku, niin ryhmällä $(G, \star)$ on vain triviaalit aliryhmät $(\{e\}, \star)$ ja $(G, \star)$. (Miksi?)

1.4 Sykliset ryhmät

Olkoon $(G, \star)$ ryhmä ja $a \in G$. Merkitään alkion a potenssien joukkoa symbolilla $\langle a \rangle$, ts.

$$\langle a \rangle = \left\{ a^k |\ k \in \mathbf{Z} \right\}.$$

Koska $(G, \star)$ on ryhmä, niin $\langle a \rangle \subseteq G$. Lauseissa 1.4.1 ja 1.4.2 tutkimme alkion a potenssien joukon $\langle a \rangle$ ominaisuuksia tarkemmin. Sen jälkeen määrittelemme syklisen ryhmän käsitteen. (Jos ryhmän laskutoimitus on yhteenlaskunkaltainen, niin potenssien joukon sijasta on syytä käyttää termiä monikertojen joukko.)

Lause 1.4.1 *Olkoon $(G, \star)$ ryhmä ja $a \in G$. Silloin $\langle a \rangle$ on ryhmän G suppein aliryhmä, joka sisältää alkion a.*

Todistus 1) Kun asetetaan $k = 1$, saadaan $a \in \langle a \rangle$. Siis $\langle a \rangle$ *sisältää* alkion a.

2) Olkoot b, $c \in \langle a \rangle$ mielivaltaisesti valittuja. Silloin $b = a^k$, $c = a^l$, missä k, $l \in \mathbf{Z}$. Voidaan todeta, että $c^{-1} = a^{-l}$. Näin ollen $b \star c^{-1} = a^k \star a^{-l} = a^{k-l}$, missä $k - l \in \mathbf{Z}$, joten $b \star c^{-1} \in \langle a \rangle$. Täten aliryhmäkriteerin (lause 1.2.1) perusteella $\langle a \rangle$ on ryhmän G *aliryhmä.*

3) Todistetaan vielä, että $\langle a \rangle$ on *suppein* aliryhmä, joka sisältää alkion a. Oletetaan, että $H \leq G$ ja $a \in H$. Koska H on ryhmä, niin $a^k \in H$ aina, kun $k \in \mathbf{Z}$. Siis $H \supseteq \langle a \rangle$. Näin ollen $\langle a \rangle$ on suppein aliryhmä, joka sisältää alkion a. □

Huomautus Aliryhmää $\langle a \rangle$ sanotaan alkion a generoimaksi aliryhmäksi.

Huomautus Jos G on äärellinen ryhmä, niin lauseiden 1.4.1 ja 1.3.4 perusteella

$$|\langle a \rangle| \Big| |G|.$$

Lause 1.4.2 *Olkoon $(G, \star)$ ryhmä ja $a \in G$.*

i) *Jos $\langle a \rangle$ on ääretön, niin kaikki potenssit a^k, $k \in \mathbf{Z}$, ovat erisuuria.*

ii) *Jos $\langle a \rangle$ on äärellinen ja merkitään $|\langle a \rangle| = m$, niin*

$$\langle a \rangle = \left\{ e, a, a^2, \ldots, a^{m-1} \right\}, \tag{1}$$

missä $a^m = e$. Edelleen

$$a^k = e \Leftrightarrow m \mid k \tag{2}$$

ja yleisemmin

$$a^k = a^h \Leftrightarrow k \equiv h \pmod{m}. \tag{3}$$

Todistus Jos kaikki potenssit ovat erisuuria, niin lause on voimassa. Oletetaan, että kaikki potenssit eivät ole erisuuria. Todistetaan, että silloin kohta ii) on voimassa. Olettamuksen mukaan on olemassa sellaiset r, $s \in \mathbf{Z}$, että $a^r = a^s$ ja $r \neq s$, sanokaamme $r > s$. Silloin $a^{r-s} = e$, missä $r - s > 0$. Siis on olemassa positiivinen potenssi, joka on $= e$. Olkoon m pienin sellainen positiivinen kokonaisluku, että $a^m = e$.

1) Todistetaan, että kaava (1) on voimassa. Suunta " $\supseteq$ " on triviaali. Todistetaan, suunta " $\subseteq$ ". Oletetaan, että $a^k \in \langle a \rangle$. Silloin jakoalgoritmin mukaan $k = qm + r$, missä $0 \leq r < m$. Näin ollen

$$a^k = a^{qm+r} = (a^m)^q \star a^r = e^q \star a^r = e \star a^r = a^r.$$

Koska $0 \leq r < m$, niin $a^k \in \{e, a, a^2, \ldots, a^{m-1}\}$. Siis kaava (1) on voimassa.

2) Todistetaan, että kaava (2) on voimassa. Merkitään $k = qm + r$, missä $0 \leq r < m$. Silloin $a^k = a^r$. Koska m on pienin sellainen positiivinen kokonaisluku, että $a^m = e$, niin

$$a^k = e \Leftrightarrow a^r = e \Leftrightarrow r = 0.$$

Ehto $r = 0$ on yhtäpitävä ehdon $m \mid k$ kanssa.

3) Kohdan 2 nojalla saadaan

$$a^k = a^h \Leftrightarrow a^{k-h} = e \Leftrightarrow m \mid k - h \Leftrightarrow k \equiv h \pmod{m}.$$

Näin olemme todistaneet lauseen 1.4.2. □

Esimerkki 1.4.1 Tarkastellaan ryhmää $(\mathbf{Z}_{10}^*, \cdot)$. Mikä on a) $\langle \overline{9} \rangle$, b) $\langle \overline{3} \rangle$?

Ratkaisu Selvästi $\mathbf{Z}_{10}^* = \left\{ \overline{1}, \overline{3}, \overline{7}, \overline{9} \right\}$. Näin ollen joukot $\langle \overline{3} \rangle$ ja $\langle \overline{9} \rangle$ ovat äärellisiä ja siis lauseen 1.4.2 muotoa (1).

a) Lauseen 1.4.2 perusteella

$$\begin{aligned}\langle\overline{9}\rangle &= \left\{\overline{9}^k |\ k \in \mathbf{Z}\right\} = \left\{\overline{1}, \overline{9}, \overline{9}^2, \ldots\right\} \\ &= \left\{\overline{1}, \overline{9}, \overline{1}, \ldots\right\} \\ &= \left\{\overline{1}, \overline{9}\right\}.\end{aligned}$$

b) Lauseen 1.4.1 huomautuksen perusteella

$$\begin{aligned}\langle\overline{3}\rangle &= \left\{\overline{3}^k |\ k \in \mathbf{Z}\right\} = \left\{\overline{1}, \overline{3}, \overline{3}^2, \ldots\right\} \\ &= \left\{\overline{1}, \overline{3}, \overline{9}, \ldots\right\} \\ &= \mathbf{Z}_{10}^*.\end{aligned}$$

Esimerkki 1.4.2 Tarkastellaan ryhmää $(\mathbf{Z}_4, +)$. Mikä on a) $\langle\overline{2}\rangle$, b) $\langle\overline{3}\rangle$?
Ratkaisu a) Lauseen 1.4.2 perusteella

$$\begin{aligned}\langle\overline{2}\rangle &= \left\{k\,\overline{2} |\ k \in \mathbf{Z}\right\} = \left\{\overline{0}, \overline{2}, 2\,\overline{2}, \ldots\right\} \\ &= \left\{\overline{0}, \overline{2}, \overline{0}, \ldots\right\} = \left\{\overline{0}, \overline{2}\right\}.\end{aligned}$$

b) Lauseen 1.4.1 huomautuksen perusteella

$$\langle\overline{3}\rangle = \left\{\overline{0}, \overline{3}, \overline{2}, \ldots\right\} = \mathbf{Z}_4.$$

Määritelmä Ryhmä $(G, \star)$ on *syklinen*, jos on olemassa sellainen $a \in G$, että $G = \langle a\rangle$. Alkiota a sanotaan syklisen ryhmän *generaattoriksi*.

Esimerkki 1.4.3 Ryhmä $(\mathbf{Z}_{10}^*, \cdot)$ on syklinen. Alkion $\overline{3}$ on sen generaattori (ks. esimerkki 1.4.1). Myös alkio $\overline{7}$ on sen generaattori. Sen sijaan alkiot $\overline{1}$ ja $\overline{9}$ eivät ole generaattoreita. (Totea!)

Esimerkki 1.4.4 Ryhmä $(\mathbf{Z}_4, +)$ on syklinen. Alkion $\overline{3}$ on sen generaattori (ks. esimerkki 1.4.2). Myös alkio $\overline{1}$ on sen generaattori. Sen sijaan alkiot $\overline{0}$ ja $\overline{2}$ eivät ole generaattoreita. (Totea!)

Esimerkki 1.4.5 Ryhmä $(\mathbf{Z}_8^*, \cdot)$ ei ole syklinen, sillä $\mathbf{Z}_8^* = \left\{\overline{1}, \overline{3}, \overline{5}, \overline{7}\right\}$ ja $\left\langle\overline{1}\right\rangle = \left\{\overline{1}\right\}$, $\langle\overline{3}\rangle = \left\{\overline{1}, \overline{3}\right\}$, $\langle\overline{5}\rangle = \left\{\overline{1}, \overline{5}\right\}$ ja $\langle\overline{7}\rangle = \left\{\overline{1}, \overline{7}\right\}$. (Totea!)

Esimerkki 1.4.6 Ryhmä $(\mathbf{Z}, +)$ on syklinen. Sen generaattorit ovat 1 ja -1. Huomaa, että yleisesti $\langle m\rangle = m\mathbf{Z}$. (Totea!)

Esimerkki 1.4.7 Ryhmä $(\mathbf{Z}_m, +)$ on syklinen. Alkio $\overline{1}$ on sen generaattori. Kaikki generaattorit saadaan lauseen 1.4.3 seurauksena.

Lause 1.4.3 *Olkoon $(G, \star)$ äärellinen syklinen ryhmä. Olkoon $|G| = m$ ja $a \in G$ ryhmän generaattori. Silloin a^n on generaattori, jos ja vain jos $(m, n) = 1$, ts. $\langle a^n \rangle = G$, jos ja vain jos $(m, n) = 1$.*

Todistus Oletetaan, että $(m, n) = 1$. Todistetaan, että $\langle a^n \rangle = G$ eli että $\langle a^n \rangle = \langle a \rangle$. Selvästi $\langle a^n \rangle \subseteq \langle a \rangle$. Todistetaan, että $\langle a^n \rangle \supseteq \langle a \rangle$. Valitaan $a^k \in \langle a \rangle$. Nyt $(m, n) \mid k$, joten yhtälö $nx \equiv k \pmod{m}$ on ratkeava (ks. Algebra I). Näin ollen, lauseen 1.4.2 kaavan (3) nojalla, on olemassa sellainen x, että $a^{nx} = a^k$. Täten $a^k \in \langle a^n \rangle$ ja siis $\langle a^n \rangle \supseteq \langle a \rangle$.
Käänteisen puolen todistus jätetään harjoitustehtäväksi. □

Seuraus Alkio $\overline{a}$ on syklisen ryhmän $(\mathbf{Z}_m, +)$ generaattori, jos ja vain jos $(a, m) = 1$.

Esimerkki 1.4.8 Jos p on alkuluku, niin syklisen ryhmän $(\mathbf{Z}_p, +)$ generaattorit ovat $\overline{1}, \overline{2}, \ldots, \overline{p-1}$. (Miksi?)

Esimerkki 1.4.9 Syklisen ryhmän $(\mathbf{Z}_8, +)$ generaattorit ovat $\overline{1}$, $\overline{3}$, $\overline{5}$, $\overline{7}$.

Esimerkki 1.4.10 Ryhmä $(\mathbf{Z}_{10}^*, \cdot)$ on syklinen ryhmä, jonka alkioiden lukumäärä on neljä ja jonka generaattori on $\overline{3}$. Koska $|\mathbf{Z}_{10}^*| = 4$, niin kaikki generaattorit ovat $\overline{3}^1$ ja $\overline{3}^3$ eli $\overline{3}$ ja $\overline{7}$ (vrt. esimerkit 1.4.1 ja 1.4.3).

Lause 1.4.4 *Jokainen syklinen ryhmä on Abelin ryhmä.*

Todistus Olkoon $(G, \star)$ syklinen ryhmä. Silloin G on muotoa

$$G = \left\{ a^k |\ k \in G \right\},$$

missä $a \in G$. Olkoot b, $c \in G$. Silloin b ja c ovat muotoa $b = a^k$, $c = a^l$, missä k, $l \in \mathbf{Z}$. Siis

$$b \star c = a^k \star a^l = a^{k+l} = a^{l+k} = a^l \star a^k = c \star b.$$

Täten $(G, \star)$ on Abelin ryhmä. □

Esimerkki 1.4.11 Ryhmät $(M_{m\times m}^*, \cdot)$ ja $(S_n, \circ)$ eivät ole syklisiä, koska ne eivät ole Abelin ryhmiä. (Luvuille m ja n on asetettava rajoitukset $m \geq 2$, $n \geq 3$. Miksi?)

Huomautus Jokainen Abelin ryhmä ei ole syklinen. Esimerkiksi $(\mathbf{Z}_8^*, \cdot)$ on Abelin ryhmä, mutta ei ole syklinen (ks. esimerkki 1.4.5).

1.5 Ryhmäisomorfismi

Määritelmä Olkoot $(G, \star)$ ja $(G', \bullet)$ ryhmiä. Kuvaus $f\colon G \to G'$ on *homomorfismi* (tai lyhyesti *morfismi*), jos

$$f(a \star b) = f(a) \bullet f(b)$$

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

Esimerkki 1.5.1 Tarkastellaan ryhmiä $(\mathbf{Z}, +)$ ja $(\mathbf{Z}_m, +)$. Määritellään $f\colon \mathbf{Z} \to \mathbf{Z}_m$, $f(a) = \overline{a}$. Silloin

$$f(a+b) = \overline{a+b} = \overline{a} + \overline{b} = f(a) + f(b)$$

aina, kun a, $b \in \mathbf{Z}$. Näin ollen f on morfismi.

Lause 1.5.1 *Olkoot $(G, \star)$ ja $(G', \bullet)$ ryhmiä ja olkoon $f\colon G \to G'$ morfismi. Silloin*

1) $f(e) = e'$,

2) $f(a^{-1}) = f(a)^{-1} \quad \forall a \in G$,

missä e ja e' ovat ryhmien $(G, \star)$ ja $(G', \bullet)$ neutraalialkiot.

Todistus 1) Ensiksi $f(e) = f(e \star e) = f(e) \bullet f(e)$. Kun supistetaan $f(e)$, niin saadaan $f(e) = e'$. 2) Toiseksi $f(a) \bullet f(a^{-1}) = f(a \star a^{-1}) = f(e) = e'$ ja samoin $f(a^{-1}) \bullet f(a) = e'$, joten $f(a^{-1}) = f(a)^{-1}$. □

Määritelmä Olkoot $(G, \star)$ ja $(G', \bullet)$ ryhmiä. Kuvaus $f\colon G \to G'$ on *isomorfismi*, jos se on bijektio ja morfismi.

Merkintä Jos yllä oleva f on olemassa, niin sanotaan, että G ja G' ovat isomorfiset ja merkitään

$$G \simeq G'$$

tai täsmällisemmin $(G, \star) \simeq (G', \bullet)$.

Huomautus Jos $G \simeq G'$, niin isomorfismi f antaa joukkojen G ja G' välille 1–1-vastaavuuden ja säilyttää ryhmien $(G, \star)$ ja $(G', \bullet)$ laskutoimituksen. Näin ollen $(G, \star)$ ja $(G', \bullet)$ ovat ryhmäteoreettisesti olennaisesti samat.

Lause 1.5.2 *Relaatio $\simeq$ on ekvivalenssi.*

Todistus 1) (Refleksiivisyys) Jokainen ryhmä $(G, \star)$ on isomorfinen itsensä kanssa. Isomorfismiksi kelpaa kuvaus $f\colon G \to G$, $f(a) = a$.

2) (Symmetrisyys) Oletetaan, että $(G, \star) \simeq (G', \bullet)$. Olkoon $f\colon G \to G'$ isomorfismi. Silloin f on bijektio ja $f(a \star b) = f(a) \bullet f(b)$ aina, kun a, $b \in G$. On tunnettua, että

f^{-1} on olemassa ja on bijektio $G' \to G$. Todistetaan, että f^{-1} on morfismi $G' \to G$. Olkoot a', $b' \in G'$ mielivaltaisesti valittuja. Olkoot a, $b \in G$ sellaiset, että $f(a) = a'$ ja $f(b) = b'$. Silloin

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

Näin ollen f^{-1} on morfismi. Koska f^{-1} on lisäksi bijektio, niin f^{-1} on isomorfismi. Siis $(G', \bullet) \simeq (G, \star)$.

3) (Transitiivisuus) Harjoitustehtävä. □

Esimerkki 1.5.2 Ryhmät $(\mathbf{R}, +)$ ja $(\mathbf{R}^+, \cdot)$ ovat isomorfiset. Kuvaus $f\colon \mathbf{R} \to \mathbf{R}^+$, $f(x) = e^x$, on isomorfismi. (Totea!)

Esimerkki 1.5.3 Kaikki 2–alkioiset ryhmät ovat keskenään isomorfisia. (Totea!)

Esimerkki 1.5.4 Ryhmät $(\mathbf{Z}, +)$ ja $(2\mathbf{Z}, +)$ ovat isomorfiset. Kuvaus $f\colon \mathbf{Z} \to 2\mathbf{Z}$, $f(k) = 2k$, on isomorfismi. (Totea!)

Esimerkki 1.5.5 Ryhmät $(\mathbf{Z}, +)$ ja $(\mathbf{R}, +)$ eivät ole isomorfiset, sillä $\mathbf{Z}$ on numeroituva ja $\mathbf{R}$ on ylinumeroituva.

Esimerkki 1.5.6 Ryhmät $(\mathbf{Z}_3, +)$ ja $(\mathbf{Z}_5^*, \cdot)$ eivät ole isomorfiset, sillä $|\mathbf{Z}_3| \neq |\mathbf{Z}_5^*|$.

Esimerkki 1.5.7 Ryhmät $(\mathbf{Q}, +)$ ja $(\mathbf{Q}^*, \cdot)$ eivät ole isomorfiset.

Todistus Tehdään vastaoletus: ryhmät ovat isomorfiset. Olkoon $f\colon \mathbf{Q} \to \mathbf{Q}^*$ isomorfismi. Olkoon $a \in \mathbf{Q}$ sellainen luku, että $f(a) = 3$. On selvää, että $a/2 + a/2 = a$ ryhmässä $(\mathbf{Q}, +)$. Näin ollen $f(a/2)f(a/2) = 3$ ryhmässä $(\mathbf{Q}^*, \cdot)$. Mutta yhtälöllä $x^2 = 3$ ei ole ratkaisua ryhmässä $(\mathbf{Q}^*, \cdot)$. Näin olemme päätyneet ristiriitaan. Siis vastaoletus on väärin ja väitös on oikein. □

Huomautus Jos $(G, \star)$ on Abelin ryhmä ja $(G, \star) \simeq (G', \bullet)$, niin $(G', \bullet)$ on Abelin ryhmä. (Totea!)

Lause 1.5.3 *Jos $(G, \star)$ on syklinen ryhmä ja $(G, \star) \simeq (G', \bullet)$, niin $(G', \bullet)$ on syklinen ryhmä.*

Todistus Olkoon $G = \langle a \rangle$ ja $f: G \to G'$ isomorfismi. Todistetaan, että $G' = \langle f(a) \rangle$. On selvää, että $G' \supseteq \langle f(a) \rangle$, joten riittää todistaa, että $G' \subseteq \langle f(a) \rangle$. Olkoon $a' \in G'$ mielivaltainen. Silloin $f^{-1}(a') \in G$. Siis $f^{-1}(a') = a^k$, $k \in \mathbf{Z}$, eli $a' = f(a^k)$. Koska f on homomorfismi, niin $a' = f(a)^k$ eli $a' \in \langle f(a) \rangle$. Näin ollen $G' \subseteq \langle f(a) \rangle$. Siis $G' = \langle f(a) \rangle$. □

Seuraus Jos $(G, \star)$ on syklinen ryhmä ja $(G', \bullet)$ ei ole syklinen ryhmä, niin $(G, \star) \not\simeq (G', \bullet)$.

Esimerkki 1.5.8 Ryhmä $(\mathbf{Z}_4, +)$ on syklinen, mutta ryhmä $(\mathbf{Z}_8^*, \cdot)$ ei ole syklinen. Siis $(\mathbf{Z}_4, +) \not\simeq (\mathbf{Z}_8^*, \cdot)$.

Lause 1.5.4 *Samaa kardinaalilukua olevat sykliset ryhmät ovat isomorfisia.*

Todistus 1) Jos $(\langle a \rangle, \star)$ on numeroituvasti ääretön syklinen ryhmä, niin $(\mathbf{Z}, +) \simeq (\langle a \rangle, \star)$. Kuvaus $f: \mathbf{Z} \to \langle a \rangle$, $f(k) = a^k$, on isomorfismi. (Totea!)
2) Jos $(\langle a \rangle, \star)$ on äärellinen syklinen ryhmä ja $|\langle a \rangle| = m$, niin $(\mathbf{Z}_m, +) \simeq (\langle a \rangle, \star)$. Kuvaus $f: \mathbf{Z}_m \to \langle a \rangle$, $f(\overline{k}) = a^k$, on isomorfismi. (Totea!) □

Esimerkki 1.5.9 Lauseen 1.5.4 perusteella $(\mathbf{Z}_4, +) \simeq (\mathbf{Z}_{10}^*, \cdot)$.

Apulause 1.5.1 *Jos ryhmän alkioiden lukumäärä on alkuluku, niin ryhmä on syklinen.*

Todistus Harjoitustehtävä. Vihje: Sovella Lagrangen lausetta.

Lause 1.5.5 *Kaikki p–alkioiset ryhmät ovat keskenään isomorfiset, kun p on alkuluku.*

Todistus Lause 1.5.5 seuraa lauseesta 1.5.4 ja apulauseesta 1.5.1. □

Lause 1.5.6 *Nelialkioisia ryhmiä on kaksi kappaletta (kun isomorfisia ryhmiä pidetään samoina).*

Todistus 1) Jos $(G, \star)$ on syklinen, niin $(G, \star) \simeq (\mathbf{Z}_4, +)$.
2) Oletetaan, että $(G, \star)$ ei ole syklinen. Tällainen ryhmä on tosiaan olemassa (esimerkiksi $(\mathbf{Z}_8^*, \cdot)$). Merkitään $G = \{e, a, b, c\}$. Silloin Lagrangen lauseen nojalla $|\langle e \rangle| = 1$, $|\langle a \rangle| = |\langle b \rangle| = |\langle c \rangle| = 2$. Siis $a^2 = b^2 = c^2 = e$. Nämä ehdot määräävät ryhmän G kaikki tulot yksikäsitteisesti. (Totea!) Siis $(G, \star) \simeq (\mathbf{Z}_8^*, \cdot)$. □

Huomautus Nelialkioista ei-syklistä ryhmää sanotaan *Kleinin neliryhmäksi*.

2 Polynomeista

2.1 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.

2.2 Polynomirengas

Polynomi

Analyysissä polynomi määritellään kuvauksena

$$f\colon \mathbf{R} \to \mathbf{R},\ \ f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n,$$

missä $a_0,\ a_1,\ a_2,\ \ldots,\ a_n \in \mathbf{R}$ ovat polynomin kertoimia. Algebrassa polynomit määritellään toisin. Polynomi on (kerrointen) jono $(a_0, a_1, a_2, \ldots, a_n)$, jonka elementit kuuluvat johonkin renkaaseen, ns. kerroinrenkaaseen. Jonon tutkimista helpotetaan usein jatkamalla jono $(a_0, a_1, a_2, \ldots, a_n)$ äärettömäksi jonoksi $(a_0, a_1, a_2, \ldots, a_n, 0, 0, \ldots)$ lisäämällä loppuun nolla-alkioita.

Määritelmä Olkoon $(R, +, \cdot)$ rengas. Renkaan R *polynomi* on ääretön jono

$$(a_0, a_1, a_2, \ldots)$$

joukon R alkioita, joista vain äärellinen määrä on nollasta poikkeavia (tarkemmin sanoen, nolla-alkiosta poikkeavia). Alkioita $a_0,\ a_1,\ a_2,\ \ldots$ sanotaan polynomin *kertoimiksi*. Jos kaikki kertoimet $a_0,\ a_1,\ a_2,\ \ldots$ ovat nollia, polynomia sanotaan *nollapolynomiksi*.

Huomautus Jos polynomin kaikki kertoimet eivät ole nollia ja jos a_n $(n \geq 0)$ on viimeinen nollasta poikkeava kerroin, niin

$$(a_0, a_1, a_2, \ldots) = (a_0, a_1, a_2, \ldots, a_n, 0, 0, \ldots).$$

Kerrointa a_n sanotaan polynomin *johtavaksi* kertoimeksi.

Merkintä Usein merkitään muodollisesti

$$(a_0, a_1, a_2, \ldots) = \sum_{k=0}^{\infty} a_k x^k = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n, \tag{1}$$

missä symboli x ei ole muuttuja vaan symbolin x potenssit x^k ilmaisevat kertoimensa a_k paikan jonossa $(a_0, a_1, a_2, \ldots)$. Jos kertoimia a_k ei tarvita, voidaan merkitä lyhyesti

$$A(x) = \sum_{k=0}^{\infty} a_k x^k.$$

Lausekkeita $A(x)$, $\sum a_k x^k$ ja $a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ on joskus miellyttävämpi käsitellä kuin listaa $(a_0, a_1, a_2, \ldots)$.

Huomautus Jos $a_k = 0$, niin termi $a_k x^k$ jätetään usein merkitsemättä. Jos $(R, +, \cdot)$ on 1–rengas ja $a_k = 1$, niin merkitään $a_k x^k = 1x^k = x^k$.

Esimerkki 2.2.1 Jos $R = \mathbf{Z}$, niin

$$(1, 0, 1, 0, 0, \ldots) = 1 + x^2.$$

Huomautus Polynomit $A(x)$ ja $B(x)$ ovat samat, jos ja vain jos $a_k = b_k$ aina, kun $k = 0,\ 1,\ 2,\ \ldots$

Merkintä Renkaan $(R, +, \cdot)$ kaikkien polynomien joukkoa merkitään symbolilla $R\,[x]$.

Polynomien summa ja tulo

Määritelmä Polynomien yhteenlasku $+$ ja kertolasku $\cdot$ määritellään kaavoilla

$$\begin{aligned} A(x) + B(x) &= \sum_{k=0}^{\infty} (a_k + b_k) x^k, \\ A(x)B(x) &= \sum_{k=0}^{\infty} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) x^k. \end{aligned}$$

Esimerkki 2.2.2 Olkoot polynomit $A(x) = \overline{1} + \overline{2}x + x^3$ ja $B(x) = \overline{2} + \overline{2}x$ joukon $\mathbf{Z}_3\,[x]$ alkioita. Silloin

$$\begin{aligned} A(x) + B(x) &= x + x^3, \\ A(x)B(x) &= \overline{2} + x^2 + \overline{2}x^3 + \overline{2}x^4. \end{aligned}$$

(Totea!)

Määritelmä Jos $A(x) = a_0 + a_1 x + \cdots + a_n x^n$, missä $a_n \neq 0$, niin polynomin $A(x)$ *aste* on n. Silloin merkitään $\deg A(x) = n$. Lisäksi nollapolynomin asteeksi määritellään $-\infty$.

Lause 2.2.1 *Summan ja tulon asteille on voimassa*

$$\deg(A(x)+B(x)) \begin{cases} = & \max\{\deg A(x), \deg B(x)\}, \ \textit{jos} \ \deg A(x) \neq \deg B(x), \\ \leq & \deg A(x), \ \textit{jos} \ \deg A(x) = \deg B(x), \end{cases}$$

$$\deg(A(x)B(x)) \leq \deg A(x) + \deg B(x).$$

Todistus Harjoitustehtävä.

Huomautus Jos polynomien $A(x)$ ja $B(x)$ johtavat kertoimet eivät ole nollanjakajia, niin tulon asteen kaavassa on yhtäsuuruus voimassa. Esimerkiksi kokonaisalueessa se on aina voimassa.

Esimerkki 2.2.3 Olkoon $A(x) = \overline{1} + \overline{2}x \in \mathbf{Z}_4[x]$. Silloin $\deg A(x) = 1$, $\deg(A(x) + A(x)) = 0$ ja $\deg(A(x)A(x)) = 0$. (Totea!)

Lause 2.2.2 *Jos* $(R, +, \cdot)$ *on rengas, niin* $(R[x], +, \cdot)$ *on rengas.*

Todistus 1) Yhteenlaskun määritelmän ja lauseen 2.2.1 nojalla yhteenlasku on laskutoimitus joukossa $R[x]$.

2) Yhteenlasku on assosiatiivinen joukossa $R[x]$. (Totea!)

3) Nolla-alkio on nollapolynomi.

4) Polynomin $(a_0, a_1, \ldots)$ vastapolynomi on $(-a_0, -a_1, \ldots)$.

5) Yhteenlasku on kommutatiivinen joukossa $R[x]$. (Totea!)

Kohtien 1–5 nojalla $(R[x], +)$ on Abelin ryhmä.

6) Kertolaskun määritelmän ja lauseen 2.2.1 nojalla kertolasku on laskutoimitus joukossa $R[x]$.

7) Kertolasku on assosiatiivinen. (Harjoitustehtävä.)

Kohtien 6 ja 7 nojalla $(R[x], \cdot)$ on puoliryhmä.

8) Osittelulait ovat voimassa. (Harjoitustehtävä.) □

Polynomin määräämä kuvaus

Määritelmä Olkoon $(R, +, \cdot)$ rengas ja $A(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$. Silloin kuvausta

$$A\colon R \to R, \ A(t) = a_0 + a_1t + \cdots + a_nt^n, \tag{1}$$

sanotaan *polynomin* $A(x)$ *määräämäksi kuvaukseksi* (tai *polynomikuvaukseksi*). Kaavassa (1) yhteen- ja kertolaskut ovat renkaan $(R, +, \cdot)$ laskutoimituksia. (Huomaa, että tosiaan $A(t) \in R$ aina, kun $t \in R$.)

Esimerkki 2.2.4 Olkoon $A(x) = \overline{1} + x \in \mathbf{Z}_3[x]$. Silloin $A(x)$ on polynomi, joka voidaan kirjoittaa myös muodossa

$$A(x) = \overline{1} + \overline{1}\,x + \overline{0}\,x^2 + \overline{0}\,x^3 + \overline{0}\,x^4 + \cdots = (\overline{1}, \overline{1}, \overline{0}, \overline{0}, \overline{0}, \ldots).$$

Sen määräämä kuvaus on

$$A\colon \mathbf{Z}_3 \to \mathbf{Z}_3, \quad A(t) = \overline{1} + t,$$

ts. $A(\overline{0}) = \overline{1}, \quad A(\overline{1}) = \overline{2}, \quad A(\overline{2}) = \overline{0}$.

Esimerkki 2.2.5 Olkoon $B(x) = \overline{1} + x^3 \in \mathbf{Z}_3[x]$. Silloin

$$B(x) = (\overline{1}, \overline{0}, \overline{0}, \overline{1}, \overline{0}, \overline{0}, \overline{0}, \ldots).$$

Sen määräämä kuvaus on

$$B\colon \mathbf{Z}_3 \to \mathbf{Z}_3, \ B(t) = \overline{1} + t^3,$$

ts. $B(\overline{0}) = \overline{1}, \quad B(\overline{1}) = \overline{2}, \quad B(\overline{2}) = \overline{1} + \overline{8} = \overline{9} = \overline{0}$. Näin ollen polynomi $B(x)$ ja esimerkin 2.2.4 polynomi $A(x)$ ovat erisuuret, mutta niiden määräämät kuvaukset ovat samat.

Huomautus Renkaassa $(\mathbf{R}[x], +, \cdot)$ ei ole mahdollista, että eri polynomit määräävät samat polynomikuvaukset. (Huomaa, että tässä kerroinrengas on reaalilukujen rengas.)

Kunnan polynomirengas

Tarkastellaan polynomirenkaita $(F[x], +, \cdot)$, joissa kerroinrenkaana on kokonaisalue $(D, +, \cdot)$ tai kunta $(F, +, \cdot)$.

Lause 2.2.3 *Jos $(D, +, \cdot)$ on kokonaisalue, niin $(D[x], +, \cdot)$ on kokonaisalue.*

Todistus 1) Lauseessa 2.2.2 on todistettu, että $(D[x], +, \cdot)$ on rengas.

2) Polynomien kertolasku on kommutatiivinen. (Totea!)

3) Polynomi $(1, 0, 0, \ldots)$ on ykkösalkio.

4) Todistetaan, että renkaassa $(D[x], +, \cdot)$ ei ole nollanjakajia. Tehdään vastaoletus: On olemassa polynomit $A(x)$ ja $B(x)$, jotka eivät ole nollapolynomeja mutta joiden tulo on nollapolynomi. Merkitään $A(x) = a_0 + a_1x + \cdots + a_nx^n$ ja $B(x) = b_0 + b_1x + \cdots + b_mx^m$, missä a_n, $b_m \neq 0$, n, $m \geq 0$. Silloin tulon $A(x)B(x)$ johtava kerroin on a_nb_m. Koska $A(x)B(x)$ on nollapolynomi, niin $a_nb_m = 0$. Näin ollen a_n ja b_m ovat nollanjakajia, mikä on mahdotonta, koska $(D, +, \cdot)$ on kokonaisalue. □

Huomautus Polynomirengas $(F[x], +, \cdot)$ ei ole välttämättä kunta, vaikka kerroinrengas $(F, +, \cdot)$ olisi kunta. Esimerkiksi renkaan $(\mathbf{R}, +, \cdot)$ polynomilla $1 + x$ ei ole käänteisalkiota. Nimittäin jos $A(x)$ olisi käänteisalkio, niin $(1 + x)A(x) = 1$. Tällöin

$$\underbrace{\deg(1 + x)}_{=1} + \underbrace{\deg A(x)}_{\geq 0} = 0,$$

mikä on mahdotonta.

2.3 Polynomien jaollisuus

Polynomien jaollisuudella on paljon yhteistä kokonaislukujen jaollisuuden kanssa varsinkin silloin, kun polynomien kerroinrengas on kunta. Tässä pykälässä esitämme joitakin yksittäisiä polynomien jaollisuuden ominaisuuksia. Oletamme yleisesti, että kerroinrengas on kunta.

Määritelmä Olkoon $(F, +, \cdot)$ kunta ja $A(x)$, $B(x) \in F[x]$. Jos on olemassa sellainen $C(x) \in F[x]$, että

$$A(x) = B(x)C(x),$$

niin sanotaan, että polynomi $B(x)$ *jakaa* polynomin $A(x)$ tai että polynomi $B(x)$ on polynomin $A(x)$ *tekijä*. Silloin merkitään

$$B(x) \mid A(x).$$

Esimerkki 2.3.1 Renkaassa $(\mathbf{Z}_5[x], +, \cdot)$ voidaan kirjoittaa

$$x^2 + \overline{4} = (x - \overline{1})(x + \overline{1}),$$

joten

$$x - \overline{1} \mid x^2 + \overline{4} \quad \text{ja} \quad x + \overline{1} \mid x^2 + \overline{4}.$$

Huomautus Jos $B(x) \mid A(x)$ ja $c \neq 0$, niin $cB(x) \mid A(x)$, missä $cB(x) = cb_0 + cb_1x + cb_2x^2 + \cdots$ (Totea!)

Lause 2.3.1 (Jakoalgoritmi) *Oletetaan, että $A(x)$, $B(x) \in F[x]$, missä* $\deg B(x) \geq 0$. *Silloin $A(x)$ voidaan kirjoittaa yksikäsitteisesti muodossa*

$$A(x) = Q(x)B(x) + R(x),$$

missä $Q(x)$, $R(x) \in F[x]$ ja $\deg R(x) < \deg B(x)$.

Todistus Sivuutetaan.

Esimerkki 2.3.2 Voidaan laskea (esimerkiksi Mathematica-ohjelmistolla), että jos $A(x) = \overline{3}x^4 + x^3 + \overline{2}x^2 + \overline{1} \in \mathbf{Z}_5[x]$ ja $B(x) = x^2 + \overline{4}x + \overline{2} \in \mathbf{Z}_5[x]$, niin $Q(x) = \overline{3}x^2 + \overline{4}x$ ja $R(x) = \overline{2}x + \overline{1}$.

(Vihje: `<< Algebra'PolynomialMod'; ?PolynomialQuotientMod; ?PolynomialRemainderMod`)

Määritelmä Kunnan K alkio α on polynomin $A(x) \in K[x]$ *nollakohta*, jos se on polynomin $A(x)$ määräämän kuvauksen nollakohta (ts. jos $A(\alpha) = 0$).

Esimerkki 2.3.3 Polynomin $x^2 + \overline{2} \in \mathbf{Z}_3[x]$ nollakohdat ovat $\overline{1}$ ja $\overline{2}$. Sen sijaan $\overline{0}$ ei ole nollakohta. (Totea!)

Esimerkki 2.3.4 Polynomilla $x^2 + \overline{2} \in \mathbf{Z}_5[x]$ ei ole nollakohtia. (Totea!)

Lause 2.3.2 *Olkoon $A(x) \in K[x]$ ja $\alpha \in K$. Silloin*

$$A(\alpha) = 0 \Leftrightarrow x - \alpha \mid A(x).$$

Todistus "$\Leftarrow$" Oletetaan, että $x - \alpha \mid A(x)$. Silloin $A(x)$ on muotoa $A(x) = (x - \alpha)B(x)$, joten $A(\alpha) = (\alpha - \alpha)B(\alpha) = 0B(\alpha) = 0$.
"$\Rightarrow$" Oletetaan, että $A(\alpha) = 0$. Jakoalgoritmin (lause 2.3.1) perusteella

$$A(x) = Q(x)(x - \alpha) + r,$$

missä $r \in K$. Koska $A(\alpha) = 0$, niin $Q(\alpha)(\alpha - \alpha) + r = 0$ eli $r = 0$. Näin ollen $x - \alpha \mid A(x)$. □

Esimerkki 2.3.5 Renkaassa $(\mathbf{Z}_3[x], +, \cdot)$ polynomit $x - \overline{1}$ ja $x - \overline{2}$ jakavat polynomin $x^2 + \overline{2}$, mutta renkaassa $(\mathbf{Z}_5[x], +, \cdot)$ mikään 1. asteen polynomi ei jaa polynomia $x^2 + \overline{2}$ (ks. esimerkit 2.3.3 ja 2.3.4).

Määritelmä Polynomi $A(x)$ on *jaoton* (engl. irreducible) renkaassa $(F[x], +, \cdot)$, jos $\deg A(x) > 0$ ja polynomia $A(x)$ ei voida kirjoittaa kahden positiivista astetta olevan polynomin tulona. Muussa tapauksessa $A(x)$ on *jaollinen* (engl. reducible).

Esimerkki 2.3.6 Polynomi $x^2 + 1$ on jaoton renkaassa $(\mathbf{R}[x], +, \cdot)$ mutta jaollinen renkaassa $(\mathbf{C}[x], +, \cdot)$.

Lause 2.3.3 *Olkoon $A(x) \in F[x]$.*

1) *Jos $\deg A(x) = 1$, niin $A(x)$ on jaoton.*

2) *Jos $\deg A(x) \geq 2$ ja polynomilla $A(x)$ on nollakohta, niin $A(x)$ on jaollinen.*

3) *Olkoon $\deg A(x) = 2$ tai 3. Silloin $A(x)$ on jaollinen, jos ja vain jos sillä on nollakohta.*

3') *Olkoon $\deg A(x) = 2$ tai 3. Silloin $A(x)$ on jaoton, jos ja vain jos sillä ei ole nollakohtaa.*

Todistus 1) Seuraa lauseen 2.2.1 huomautuksen avulla. (Totea!)

2) Seuraa lauseen 2.2.1 huomautuksen ja lauseen 2.3.2 avulla. (Totea!)

3) Seuraa lauseen 2.2.1 huomautuksen ja lauseen 2.3.2 avulla. (Totea!)

3') Väite 3') on ekvivalentti väitteen 3) kanssa. □

Esimerkki 2.3.7 Polynomi $x - \overline{1} \in \mathbf{Z}_3[x]$ on jaoton. Polynomi $x^2 + \overline{2} \in \mathbf{Z}_3[x]$ on jaollinen mutta polynomi $x^2 + \overline{2} \in \mathbf{Z}_5[x]$ on jaoton. Polynomi $x^4 - 1 \in \mathbf{R}[x]$ on jaollinen. (Perustelut?)

Huomautus Lauseen 2.3.3 kohta 2) ei ole voimassa käänteisesti. Esimerkiksi $(x^2 + 1)^2 \in \mathbf{R}[x]$ on jaollinen vaikka sillä ei ole nollakohtaa.

Huomautus Jaottomat polynomit vastaavat kokonaislukujen jaollisuusteorian alkulukuja. Esimerkiksi voidaan todistaa, että kunnan K polynomirenkaan $K[x]$ polynomi $A(x)$ $(\neq 0)$ voidaan esittää jaottomien polynomien tulona ja että esitys on yksikäsitteinen (tekijöitten järjestystä ja 0. asteen polynomeja lukuunottamatta). Tätä teoriaa ei tässä esityksessä tarkastella.

3 Tekijästruktuureista

Tässä luvussa tarkastellaan joukkoja A, joissa on määritelty sekä laskutoimitus että ekvivalenssirelaatio $\sim$. Tekijästruktuuri saadaan, kun ekvivalenssiluokkien joukkoon $A/\sim$ määritellään laskutoimitus. Aiemmin pykälissä 2.7 ja 2.8 oli konkreettinen esimerkki tällaisesta tilanteesta. Silloin joukkona oli kokonaislukujen joukko $\mathbf{Z}$, ekvivalenssirelaationa kongruenssi $\equiv \pmod{m}$, ekvivalenssiluokkina jäännösluokat ja laskutoimituksena yhteenlasku tai kertolasku. Tässä pykälässä tämä konkreettinen jäännösluokkien teoria abstrahoidaan tekijästruktuurien teoriaksi.

Kunnat $(\mathbf{Z}_p, +, \cdot)$ ovat esimerkkejä äärellisistä kunnista. Kaikki äärelliset kunnat saadaan tekijästruktuurien ja polynomien teorian avulla. Tässä luvussa konstruoimme lopuksi esimerkin äärellisestä kunnasta, jonka alkioiden lukumäärä ei ole alkuluku. Äärelliset kunnat ovat tärkeitä sovelletussa matematiikassa.

Merkitsemme tässä luvussa yleistä laskutoimitusta merkin $\star$ sijasta lyhyemmin merkillä $\cdot$. Yleensä $\cdot$ siis tarkoittaa yleistä laskutoimitusta, mutta joskus se tarkoittaa kertolaskua. Oletamme tässä vaiheessa lukijan jo niin kokeneeksi, että sekaannuksen vaaraa ei ole.

3.1 Tekijäjoukko ja luonnollinen projektio

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

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

missä $a/\sim$ on alkion $a \in A$ määräämä ekvivalenssiluokka.

Esimerkki 3.1.1 Kokonaislukujen joukossa määritelty kongruenssi $\equiv \pmod{m}$ on ekvivalenssi ja

$$(\mathbf{Z}/\equiv \pmod{m}) = \mathbf{Z}_m = \left\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\right\},$$

missä $\overline{a}$ on alkion $a \in \mathbf{Z}$ määräämä jäännösluokka.

Määritelmä Olkoon $\sim$ joukon A ekvivalenssi. Kuvausta

$$p\colon A \to A/\sim,\ p(a) = a/\sim,$$

sanotaan *luonnolliseksi* tai *kanoniseksi projektioksi*.

Huomautus Luonnollinen projektio on surjektio mutta ei yleensä injektio.

Esimerkki 3.1.2 Kun ekvivalenssirelaationa on ryhmässä G määritelty $\equiv_L \pmod{H}$, niin luonnollinen projektio on

$$p\colon G \to G/H,\ p(a) = aH.$$

Esimerkki 3.1.3 Kun ekvivalenssirelaationa on joukossa $\mathbf{Z}$ määritelty kongruenssi $\equiv \pmod{m}$, niin luonnollinen projektio on

$$p\colon \mathbf{Z} \to \mathbf{Z}_m,\ p(a) = \overline{a}.$$

3.2 Laskutoimituksen ja ekvivalenssin yhteensopivuus

Olkoon A ei-tyhjä joukko, $\cdot$ joukon A laskutoimitus ja $\sim$ joukon A ekvivalenssi. Silloin $(A, \cdot)$ on algebrallinen struktuuri ja $A/\!\sim$ on tekijäjoukko. Tutkimme, voidaanko joukon A laskutoimitus $\cdot$ siirtää joukkoon $A/\!\sim$ luonnollisen projektion $p\colon A \to A/\!\sim$ avulla. Tarkemmin sanoen, voidaanko joukossa $A/\!\sim$ määritellä laskutoimitus $\cdot$ niin, että $p\colon A \to A/\!\sim$ on homomorfismi.

Huomautus Joukon A laskutoimitusta ja ekvivalenssiluokkien joukon $A/\!\sim$ laskutoimitusta merkitään samalla symbolilla, vaikka kyseessä on eri laskutoimitukset (vrt. kokonaislukujen tavallinen yhteenlasku ja yhteenlasku $\pmod{m}$). Operandit eli laskutoimitusten kohteet kertovat, onko kyseessä joukon A vai joukon $A/\!\sim$ laskutoimitus. Kun symbolina on $\cdot$, jätetään se yleensä merkitsemättä. Siis $a \cdot b = ab$ ja $(a/\!\sim) \cdot (b/\!\sim) = (a/\!\sim)(b/\!\sim)$.
Oletamme nyt, että luonnollinen projektio $p\colon A \to A/\!\sim$ on homomorfismi. Silloin välttämättä

1) $(a/\!\sim)(b/\!\sim) = p(a)\,p(b) = p(ab) = (ab)/\!\sim$ eli

$$(a/\!\sim)(b/\!\sim) = (ab)/\!\sim\ . \tag{1}$$

(Perustelut!) Huomaa, että $(a/\!\sim)(b/\!\sim)$ tarkoittaa ekvivalenssiluokkien $a/\!\sim$ ja $b/\!\sim$ tuloa, kun taas $(ab)/\!\sim$ tarkoittaa tulon ab ekvivalenssiluokkaa.

2) jos $a \sim a'$ ja $b \sim b'$, niin

$$(a'b')/\!\sim = (a'/\!\sim)(b'/\!\sim) = (a/\!\sim)(b/\!\sim) = (ab)/\!\sim,$$

joten

$$ab \sim a'b'. \tag{2}$$

(Perustelut!)

Siis ehdot (1) ja (2) ovat välttämättömät sille, että joukossa $A/\sim$ voidaan määritellä laskutoimitus $\cdot$ niin, että $p\colon A \to A/\sim$ on homomorfismi. Asetamme laskutoimituksen ja kongruenssin yhteensopivuuden määritelmän kohdan 2) pohjalta.

Määritelmä Olkoon A ei-tyhjä joukko, $\cdot$ joukon A laskutoimitus ja $\sim$ joukon A ekvivalenssi. Sanomme, että $\cdot$ ja $\sim$ ovat *yhteensopivat*, jos

$$a \sim a',\ b \sim b' \Rightarrow ab \sim a'b'.$$

Seuraava lause osoittaa, että yhteensopivuus on paitsi välttämätön myös riittävä ehto haluamallemme laskutoimituksen $\cdot$ olemassaololle joukossa $A/\sim$.

Lause 3.2.1 *Olkoon $(A, \cdot)$ algebrallinen struktuuri, ja olkoon $\sim$ laskutoimituksen $\cdot$ kanssa yhteensopiva joukon A ekvivalenssi. Silloin kaavan* (1) *määrittelemä sääntö $\cdot$ on laskutoimitus joukossa $A/\sim$, ts. $(A/\sim, \cdot)$ on algebrallinen struktuuri. Lisäksi luonnollinen projektio $p\colon A \to A/\sim$ on homomorfismi.*

Todistus 1) Todistetaan, että $\cdot$ on laskutoimitus joukossa $A/\sim$. Selvästi $(a/\sim)(b/\sim)$ on aina olemassa ja $\in A/\sim$. Todistetaan, että $\cdot$ on hyvin määritelty. Oletetaan, että $a'/\sim = a/\sim$ ja $b'/\sim = b/\sim$. Silloin $a' \sim a$ ja $b' \sim b$, joten yhteensopivuuden nojalla $a'b' \sim ab$. Siis $(a'b')/\sim = (ab)/\sim$ eli $(a'/\sim)(b'/\sim) = (a/\sim)(b/\sim)$.

2) Luonnollinen projektio p on homomorfismi, sillä

$$p(ab) = (ab)/\sim = (a/\sim)(b/\sim) = p(a)\,p(b).$$

Näin lause 3.2.1 on todistettu. □

Esimerkki 3.2.1 Aikaisemmin on sovittu merkinnästä $\mathbf{Z}_m = (\mathbf{Z}/\equiv \pmod m)$ ja todistettu, että yhteenlasku ja kertolasku voidaan määritellä joukossa $\mathbf{Z}_m$ kaavoilla

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

ja

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

Lause 3.2.1 antaa abstraktimman selityksen näille kaavoille ja perustelun sille, että parit $(\mathbf{Z}_m, +)$ ja $(\mathbf{Z}_m, \cdot)$ ovat algebrallisia struktuureja. Tässä tapauksessa lausetta 3.2.1 sovelletaan niin, että algebrallisena struktuurina $(A, \cdot)$ ovat $(\mathbf{Z}, +)$ ja $(\mathbf{Z}, \cdot)$ ja ekvivalenssirelaationa $\sim$ on kongruenssi $\equiv \pmod m$, joka on yhteensopiva sekä yhteenlaskun että kertolaskun suhteen joukossa $\mathbf{Z}$.

Huomautus Olkoon $(G, \cdot)$ ryhmä ja $\sim$ joukon G ekvivalenssi. Oletetaan, että $\cdot$ ja $\sim$ ovat yhteensopivat. Silloin $(G/\sim, \cdot)$ on ryhmä.

Todistus Harjoitustehtävä.

3.3 Normaali aliryhmä

Määritelmä Ryhmän $(G, \cdot)$ aliryhmää N sanotaan *normaaliksi* aliryhmäksi, jos

$$aN = Na \tag{1}$$

aina, kun $a \in G$. Silloin merkitään $N \trianglelefteq G$.

Esimerkki 3.3.1 Abelin ryhmän jokainen aliryhmä on normaali. (Totea!)

Esimerkki 3.3.2 Symmetrisen ryhmän $(S_3, \circ)$ aliryhmä $H = \{(1,2,3), (1,3,2)\}$ ei ole normaali, sillä

$$(2,3,1) \circ H \neq H \circ (2,3,1).$$

(Totea!)

Esimerkki 3.3.3 $(m\mathbf{Z}, +) \trianglelefteq (\mathbf{Z}, +)$. (Perustelu?)

Lause 3.3.1 (Normaalisuuskriteeri) *Ryhmän $(G, \cdot)$ aliryhmä N on normaali, jos ja vain jos*

$$ana^{-1} \in N \tag{2}$$

aina, kun $a \in G$, $n \in N$.

Todistus 1) Oletetaan, että $N \trianglelefteq G$ ja että $a \in G$, $n \in N$. Silloin $an \in aN$, joten olettamuksen $N \trianglelefteq G$ nojalla $an \in Na$. Näin ollen on olemassa sellainen $n' \in N$, että $an = n'a$ eli $ana^{-1} = n'$. Siis $ana^{-1} \in N$, joten (2) on voimassa.

2) Oletetaan käänteisesti, että (2) on voimassa ja osoitetaan, että $aN = Na$ aina, kun $a \in G$. Olkoon $a \in G$. Oletetaan, että $x \in aN$. Siis on olemassa sellainen $n \in N$, että

$$x = an = an(a^{-1}a) = (ana^{-1})a,$$

joten kaavan (2) nojalla $x \in Na$. Siis $aN \subseteq Na$. Oletetaan, että $y \in Na$. Silloin y on muotoa

$$y = na = (aa^{-1})na = a(a^{-1}n(a^{-1})^{-1}).$$

Koska $a^{-1} \in G$, niin kaavan (2) nojalla $a^{-1}n(a^{-1})^{-1} \in N$, joten $y \in aN$. Siis $Na \subseteq Na$. Näin olemme todistaneet, että $aN = Na$ aina, kun $a \in G$, eli että $N \trianglelefteq G$. □

Esimerkki 3.3.4 Sovelletaan lausetta 3.3.1 esimerkkiin 3.3.1. Jos $(G, \cdot)$ on Abelin ryhmä, niin $ana^{-1} = (aa^{-1})n = n \in N$. Siis kaavan (2) nojalla jokainen Abelin ryhmän aliryhmä on normaali.

Esimerkki 3.3.5 Jos M, $N \trianglelefteq G$, niin $M \cap N \trianglelefteq G$, sillä

1) M, $N \leq G \Rightarrow M \cap N \leq G$, (ks. aliryhmät)

2) $a \in G$, $n \in M \cap N \Rightarrow a \in G$, $n \in M$, $n \in N \Rightarrow ana^{-1} \in M$, $ana^{-1} \in N \Rightarrow ana^{-1} \in M \cap N$. (Implikaatioiden perustelut?)

3.4 Tekijäryhmä

Olkoon $(G, \cdot)$ ryhmä ja N sen normaali aliryhmä. Silloin ekvivalenssirelaatiot $\equiv_L$ ja $\equiv_R \pmod N$ ovat samat, joten voidaan kirjoittaa lyhyesti $\equiv \pmod N$. Vasemmat ja oikeat sivuluokat ovat samat, joten ekvivalenssirelaation $\equiv \pmod N$ ekvivalenssiluokkia voidaan kutsua lyhyesti sivuluokiksi. Sivuluokkien joukolle $G/\equiv \pmod N$ käytetään merkintää G/N. Siis

$$G/N = \{aN |\ a \in G\}$$

(vrt. §2.10).

Lauseessa 3.4.1 todistamme, että joukon G laskutoimitus $\cdot$ ja ekvivalenssirelaatio $\equiv \pmod N$ ovat yhteensopivat. Näin ollen $(G/N, \cdot)$ on algebrallinen struktuuri. Lisäksi lauseessa 3.4.2 todistamme, että tämä algebrallinen struktuuri on jopa ryhmä, ns. *tekijäryhmä* $\pmod N$.

Lause 3.4.1 *Olkoon $N \trianglelefteq G$. Silloin kaava*

$$(aN)(bN) = (ab)N \tag{1}$$

määrittelee laskutoimituksen joukossa G/N.

Todistus Lauseen 3.2.1 nojalla riittää todistaa, että ryhmän G laskutoimitus $\cdot$ ja ekvivalenssirelaatio $\equiv \pmod N$ ovat yhteensopivat. Olkoon

$$a \equiv b \pmod N, \quad c \equiv d \pmod N.$$

Silloin $a \in bN$ ja $c \in dN$, ts. on olemassa sellaiset n, $n' \in N$, että $a = bn$ ja $c = dn'$. Siis

$$ac = bndn'.$$

Koska N on normaali, niin $nd = dn''$, missä $n'' \in N$. Siis

$$ac = bd(n''n) \in bdN,$$

joten

$$ac \equiv bd \pmod N. \ \square$$

Lause 3.4.2 *Pari $(G/N, \cdot)$ on ryhmä.*

Todistus 1) Lauseen 3.4.1 mukaan pari $(G/N, \cdot)$ on algebrallinen struktuuri.

2) Kertolasku on assosiatiivinen, sillä

$$\begin{aligned}(aNbN)cN &= (ab)NcN = ((ab)c)N \\ &= (a(bc))N = aN(bc)N \\ &= aN(bNcN).\end{aligned}$$

(Perustele yhtälöt!)

3) Neutraalialkio on N eli $1N$, sillä

$$(aN)(1N) = (a1)N = aN \text{ ja } (1N)(aN) = (1a)N = aN$$

aina, kun $a \in G$.

4) Sivuluokan aN käänteisalkio on $a^{-1}N$. (Totea!) □

Huomautus Lause 3.4.2 voidaan perustella myös pykälän 3.2 lopun huomautuksen ja lauseen 3.4.1 avulla.

Esimerkki 3.4.1 Pari $(\mathbf{Z}, +)$ on ryhmä ja $m\mathbf{Z} \trianglelefteq \mathbf{Z}$. Silloin

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

ja tekijäjoukon laskutoimitus on jäännösluokkien yhteenlasku $\overline{a} + \overline{b} = \overline{a+b}$. Lauseen 3.4.2 mukaan pari $(\mathbf{Z}_m, +)$ on ryhmä, se on jopa Abelin ryhmä. Tämä on todistettu aikaisemmin lauseessa 2.7.1.

Huomautus Jos G on äärellinen, niin Lagrangen lauseen mukaan

$$|G/N| = |G|/|N|.$$

Esimerkki 3.4.2 Ryhmä $(\mathbf{Z}_6, +)$ on Abelin ryhmä, joten sen jokainen aliryhmä on normaali. Olkoon

$$N = \left\langle \overline{2} \right\rangle = \left\{\overline{0}, \overline{2}, \overline{4}\right\}.$$

Silloin $\mathbf{Z}_6/\left\langle \overline{2} \right\rangle = \left\{\left\langle \overline{2} \right\rangle, \overline{1} + \left\langle \overline{2} \right\rangle\right\}$. (Totea!) Kirjoita ryhmän $\left(\mathbf{Z}_6/\left\langle \overline{2} \right\rangle, +\right)$ ryhmätaulu. Esimerkiksi

$$\left(\overline{1} + \left\langle \overline{2} \right\rangle\right) + \left(\overline{1} + \left\langle \overline{2} \right\rangle\right) = \left(\overline{1} + \overline{1}\right) + \left\langle \overline{2} \right\rangle = \left\langle \overline{2} \right\rangle.$$

Esimerkki 3.4.3 Ryhmä $(\mathbf{Z}_7^*, \cdot)$ on Abelin ryhmä, joten sen jokainen aliryhmä on normaali. Olkoon

$$N = \left\langle \overline{6} \right\rangle = \left\{\overline{1}, \overline{6}\right\}.$$

Silloin

$$\begin{aligned}\mathbf{Z}_7^*/\left\langle\overline{6}\right\rangle &= \left\{\left\langle\overline{6}\right\rangle, \overline{2}\left\langle\overline{6}\right\rangle, \overline{3}\left\langle\overline{6}\right\rangle\right\} \\ &= \left\{\left\{\overline{1},\overline{6}\right\}, \left\{\overline{2},\overline{5}\right\}, \left\{\overline{3},\overline{4}\right\}\right\}.\end{aligned}$$

(Totea!) Kirjoita ryhmän $\left(\mathbf{Z}_7^*/\left\langle\overline{6}\right\rangle, \cdot\right)$ ryhmätaulu. Esimerkiksi

$$\left(\overline{2}\left\langle\overline{6}\right\rangle\right)\cdot\left(\overline{2}\left\langle\overline{6}\right\rangle\right) = \overline{4}\left\langle\overline{6}\right\rangle = \left\{\overline{3},\overline{4}\right\} = \overline{3}\left\langle\overline{6}\right\rangle.$$

3.5 Johdatusta homomorfialauseeseen

Kuvauksen indusoima ekvivalenssi

Määritelmä *Kuvauksen $f\colon A \to B$ joukkoon A indusoima ekvivalenssi* määritellään kaavalla

$$a \sim b \Leftrightarrow f(a) = f(b),$$

missä a, $b \in A$.

Esimerkki 3.5.1 Olkoon $f\colon \mathbf{R}^* \to \mathbf{R}^*$, $f(a) = |a|$. Silloin $a \sim b \Leftrightarrow |a| = |b|$. Lisäksi $\mathbf{R}/\!\sim = \{\{\pm a\} \mid a > 0\}$.

Lause 3.5.1 *Olkoon $\sim$ kuvauksen $f\colon A \to B$ indusoima ekvivalenssi ja $p\colon A \to A/\!\sim$, $p(a) = a/\!\sim$, vastaava luonnollinen projektio. Silloin on olemassa täsmälleen yksi sellainen kuvaus $F\colon A/\!\sim \to B$, että*

$$f = F \circ p.$$

Kuvaus F on injektio.

Todistus Määritellään $F\colon A/\!\sim \to B$, $F(a/\!\sim) = f(a)$. Tämä on todellakin kuvaus. (Totea!) Lisäksi $F \circ p = f$, sillä

$$(F \circ p)(a) = F(p(a)) = F(a/\!\sim) = f(a)$$

aina, kun $a \in A$.

Todistetaan seuraavaksi yksikäsitteisyys. Olkoon F' sellainen kuvaus, että $F' \circ p = f$. Silloin

$$F'(a/\!\sim) = F'(p(a)) = (F' \circ p)(a) = f(a)$$

aina, kun $a/\!\sim \in A/\!\sim$. Siis $F' = F$.

Todistetaan lopuksi injektiivisyys. Oletetaan, että $F(a/\sim) = F(b/\sim)$. Silloin $F(p(a)) = F(p(b))$ eli $f(a) = f(b)$, joten $a \sim b$. Näin ollen $a/\!\sim = b/\!\sim$. □

Huomautus Jos f on surjektio, niin F on surjektio. (Totea!)

Esimerkki 3.5.2 Esimerkissä 3.5.1 on voimassa, että $f(a) = |a|$, $p(a) = \{\pm a\}$, $F(\{\pm a\}) = |a|$. Siis $f = F \circ p$.

Esimerkki 3.5.3 Olkoot $(A, \cdot)$ ja $(B, \cdot)$ algebrallisia struktuureja ja $f\colon A \to B$ homomorfismi. Olkoon $\sim$ kuvauksen f joukkoon A indusoima ekvivalenssi, ts.

$$a \sim a' \Leftrightarrow f(a) = f(a').$$

Osoitamme, että $\cdot$ ja $\sim$ ovat yhteensopivat. Olkoon $a \sim a'$ ja $b \sim b'$, missä a, a', b, $b' \in A$. Silloin $f(a) = f(a')$ ja $f(b) = f(b')$. Koska f on homomorfismi, niin $f(ab) = f(a'b')$, joten $ab \sim a'b'$. Siis $\cdot$ ja $\sim$ ovat yhteensopivat. Silloin $(A/\sim, \cdot)$ on algebrallinen struktuuri. Lisäksi voidaan todistaa, että lauseen 3.5.1 kuvaus F on homomorfismi $(A/\sim, \cdot) \to (B, \cdot)$. Koska kuvaus F on injektio, niin saadaan siitä maalijoukkoa rajoittamalla isomorfismi.

Kuva ja ydin

Määritelmä Ryhmähomomorfismin $f\colon G \to G'$ *kuva* on

$$\operatorname{Im} f = \{f(a) |\ a \in G\} \ \ (= f(G))$$

ja *ydin* on

$$\operatorname{Ker} f = \{a \in G |\ f(a) = 1'\} \ \ \left(= f^{-1}(\{1'\})\right),$$

missä $1'$ on ryhmän G' ykkösalkio.

Huomautus Selvästi $\operatorname{Im} f \subseteq G'$ ja $\operatorname{Ker} f \subseteq G$.

Esimerkki 3.5.4 Esimerkin 3.5.1 kuvaus on homomorfismi ja $\operatorname{Im} f = \mathbf{R}^+$ ja $\operatorname{Ker} f = \{\pm 1\}$.

Esimerkki 3.5.5 Olkoon $f\colon \mathbf{Z} \to \mathbf{R}^*$, $f(a) = (-1)^a$. Silloin f on homomorfismi ja $\operatorname{Im} f = \{\pm 1\}$ ja $\operatorname{Ker} f = 2\mathbf{Z}$.

Esimerkki 3.5.6 Olkoon $f\colon 5\mathbf{Z} \to \mathbf{Z}_4$, $f(5k) = \overline{k}$. Silloin f on homomorfismi ja

$$\begin{aligned} \operatorname{Im} f &= \mathbf{Z}_4, \\ \operatorname{Ker} f &= 20\,\mathbf{Z}. \end{aligned}$$

(Totea!) $(f(5k) = \overline{0} \Leftrightarrow \overline{k} = \overline{0} \Leftrightarrow 4 \mid k \Leftrightarrow 20 \mid 5k \Leftrightarrow 5k \in 20\,\mathbf{Z}.)$

Lause 3.5.2 *Olkoon $f\colon G \to G'$ ryhmähomomorfismi. Silloin*

1) $\operatorname{Im} f \leq G'$,

2) $\operatorname{Ker} f \trianglelefteq G$.

Todistus 1) Selvästi $\emptyset \neq \operatorname{Im} f \subseteq G'$. Sovelletaan nyt aliryhmäkriteeriä (lause 2.9.2). Olkoot c, $d \in \operatorname{Im} f$. Silloin on olemassa sellaiset a, $b \in G$, että $f(a) = c$, $f(b) = d$. Siis lauseen 2.12.1 ja homomorfismin määritelmän nojalla

$$cd^{-1} = f(a)f(b)^{-1} = f(a)f(b^{-1}) = f(ab^{-1}),$$

joten on olemassa alkio, jonka f kuvaa alkiolle cd^{-1}. Siis $cd^{-1} \in \operatorname{Im} f$ eli $\operatorname{Im} f \leq G'$.

2) Osoitetaan ensiksi, että $\operatorname{Ker} f \leq G$. On helppo todeta, että $\emptyset \neq \operatorname{Ker} f \subseteq G$. Sovelletaan nyt aliryhmäkriteeriä (lause 2.9.2). Olkoot a, $b \in \operatorname{Ker} f$. Silloin $f(a) = f(b) = 1'$, joten

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = 1'(1')^{-1} = 1'.$$

Näin ollen $ab^{-1} \in \operatorname{Ker} f$ eli $\operatorname{Ker} f \leq G$.

Osoitetaan toiseksi, että $\operatorname{Ker} f \trianglelefteq G$. Sovelletaan normaalisuuskriteeriä (lause 3.3.1). Olkoon $a \in G$ ja $n \in \operatorname{Ker} f$. Silloin homomorfisuuden ja lauseen 2.12.1 perusteella

$$\begin{aligned} f(ana^{-1}) &= f(a)f(n)f(a)^{-1} = f(a)\,1'\,f(a)^{-1} \\ &= f(a)f(a)^{-1} = 1', \end{aligned}$$

joten $ana^{-1} \in \operatorname{Ker} f$ eli $\operatorname{Ker} f \trianglelefteq G$. □

3.6 Homomorfialause

Lause 3.6.1 (Homomorfialause) *Olkoon $f\colon G \to G'$ ryhmähomomorfismi. Silloin*

$$G/\operatorname{Ker} f \simeq \operatorname{Im} f.$$

Todistus Kuvauksen f joukkoon G indusoima ekvivalenssirelaatio $\sim$ on sama kuin joukon G ekvivalenssirelaatio $\equiv \pmod{\operatorname{Ker} f}$, sillä

$$\begin{aligned} f(a) = f(b) &\Leftrightarrow f(ab^{-1}) = 1' \Leftrightarrow ab^{-1} \in \operatorname{Ker} f \\ &\Leftrightarrow a \in b\operatorname{Ker} f \Leftrightarrow a \equiv b \pmod{\operatorname{Ker} f}. \end{aligned}$$

(Perustele yksityiskohdat!) Näin ollen $G/\sim = G/\operatorname{Ker} f$. Lauseen 3.5.1 nojalla on olemassa injektio

$$F\colon G/\operatorname{Ker} f \to G',\ F(a\operatorname{Ker} f) = f(a). \tag{1}$$

Todistetaan, että sääntö

$$F\colon G/\operatorname{Ker} f \to \operatorname{Im} f,\ F(a\operatorname{Ker} f) = f(a), \tag{2}$$

on isomorfismi. Lauseen 3.5.1 nojalla arvot $F(a \operatorname{Ker} f)$ ovat olemassa ja ovat yksikäsitteisesti määriteltyjä. Koska $F(a \operatorname{Ker} f) = f(a) \in \operatorname{Im} f$, niin F on sulkeutuva. Siis kaavan (2) sääntö F on kuvaus. Lauseen 3.5.1 mukaan se on injektio. Siis riittää todistaa, että se on surjektio ja homomorfismi.

Todistetaan ensiksi, että kaavan (2) F on surjektio. Olkoon $b \in \operatorname{Im} f$. On olemassa sellainen $a \in G$, että $f(a) = b$. Silloin $F(a \operatorname{Ker} f) = f(a) = b$.

Todistetaan toiseksi, että F on homomorfismi. Koska $f\colon G \to G'$ on homomorfismi, saadaan

$$\begin{aligned} F((a \operatorname{Ker} f)(b \operatorname{Ker} f)) &= F((ab) \operatorname{Ker} f) = f(ab) \\ &= f(a)f(b) = F(a \operatorname{Ker} f)F(b \operatorname{Ker} f). \end{aligned}$$

Siis kaavan (2) sääntö on bijektiivinen homomorfismi eli isomorfismi (vrt. esimerkki 3.5.3). Täten lauseen 3.6.1 isomorfia on voimassa. □

Esimerkki 3.6.1 Esimerkin 3.5.4 ja lauseen 3.6.1 nojalla

$$\mathbf{R}^*/\{\pm 1\} \simeq \mathbf{R}^+.$$

Esimerkki 3.6.2 Esimerkin 3.5.5 ja lauseen 3.6.1 nojalla

$$\mathbf{Z}/2\mathbf{Z} \simeq \{\pm 1\}.$$

Esimerkki 3.6.3 Esimerkin 3.5.6 ja lauseen 3.6.1 nojalla

$$5\mathbf{Z}/20\,\mathbf{Z} \simeq \mathbf{Z}_4.$$

Esimerkki 3.6.4 Tarkastellaan ryhmiä $(M^*_{n\times n}, \cdot)$ ja $(\mathbf{R}^*, \cdot)$. Kuvaus $f\colon M^*_{n\times n} \to \mathbf{R}^*$, $f(A) = \det A$, on homomorfismi. Selvästi

$$\operatorname{Ker} f = \left\{A \in M^*_{n\times n} \colon \det A = 1\right\}.$$

Lisäksi

$$\operatorname{Im} f = \mathbf{R}^*,$$

koska jokaista $x \in \mathbf{R}^*$ kohti $\operatorname{diag}(x, 1, \ldots, 1) \in M^*_{n\times n}$ ja $f(\operatorname{diag}(x, 1, \ldots, 1)) = x$.
Lauseen 3.5.2 mukaan $\operatorname{Ker} f \trianglelefteq M^*_{n\times n}$ ja lauseen 3.6.1 mukaan

$$M^*_{n\times n}/\left\{A \in M^*_{n\times n} \colon \det A = 1\right\} \simeq \mathbf{R}^*.$$

Huomautus Lausetta 3.6.1 sanotaan usein myös 1. isomorfialauseeksi. Kirjallisuudessa esitetään usein lisäksi 2. ja 3. isomorfialause, jotka esitellään lyhyesti esimerkeissä 3.6.5 ja 3.6.6.

Esimerkki 3.6.5 Olkoon $H \leq G$ ja $N \trianglelefteq G$. Merkitään

$$HN = \{hn \,|\, h \in H, n \in N\}.$$

Voidaan todistaa, että $HN \leq G$, $N \trianglelefteq HN$ ja $(HN)/N = \{hN \,|\, h \in H\}$ (Totea!). Edelleen voidaan todistaa, että kuvaus $f : H \to (HN)/N, f(h) = hN$, on homomorfismi ja että $\operatorname{Ker} f = H \cap N$, $\operatorname{Im} f = (HN)/N$ (Totea!). Näin ollen lauseen 3.6.1 nojalla $H/\operatorname{Ker} f \simeq \operatorname{Im} f$ eli

$$H/(H \cap N) \simeq (HN)/N.$$

Tulosta kutsutaan usein 2. isomorfialauseeksi ja suunnikassäännöksi.

Esimerkki 3.6.6 Olkoon $N \trianglelefteq G$, $M \trianglelefteq G$ ja $N \subseteq M$. Voidaan todistaa, että $N \trianglelefteq M$. Edelleen voidaan todistaa, että $f : G/N \to G/M, f(aN) = f(aM)$, on kuvaus ja homomorfismi ja että $\operatorname{Ker} f = M/N$, $\operatorname{Im} f = G/M$ (Totea!). Näin ollen lauseen 3.6.1 nojalla $(G/N)/\operatorname{Ker} f \simeq \operatorname{Im} f$ eli

$$(G/N)/(M/N) \simeq G/M.$$

Tulosta kutsutaan usein 3. isomorfialauseeksi.

3.7 Renkaan ihanne

Määritelmä Renkaan $(R, +, \cdot)$ alirengas I on *ihanne* (tai *ideaali*), jos

$$ra, ar \in I$$

aina, kun $r \in R$ ja $a \in I$.

Lause 3.7.1 (Ihannekriteeri) *Joukon R ei-tyhjä osajoukko I muodostaa renkaan $(R, +, \cdot)$ ihanteen, jos ja vain jos*

1) *$a - b \in I$ aina, kun a, $b \in I$,*

2) *ra, $ar \in I$ aina, kun $r \in R$, $a \in I$.*

Todistus Harjoitustehtävä.

Esimerkki 3.7.1 Renkaan R ns. triviaalit ihanteet ovat $\{0\}$ ja R.

Esimerkki 3.7.2 Alirengas $m\,\mathbf{Z}$ on renkaan $(\mathbf{Z}, +, \cdot)$ ihanne. (Totea!)

Esimerkki 3.7.3 $n \times n$–diagonaalimatriisit eivät muodosta $n \times n$–matriisien renkaan ihannetta, sillä $n \times n$–diagonaalimatriisin ja $n \times n$–matriisin tulo ei ole aina $n \times n$–diagonaalimatriisi. (Kirjoita esimerkki.)

Lause 3.7.2 *Olkoon R 1–rengas ja I sen ihanne, joka sisältää kääntyvän alkion. Silloin $I = R$.*

Todistus Olkoon $r \in R$ mielivaltaisesti valittu. Silloin

$$r = r \cdot 1 = r(u^{-1}u) = (ru^{-1})u,$$

missä u on ihanteen I kääntyvä alkio. Silloin $ru^{-1} \in R$ ja $u \in I$, joten $(ru^{-1})u \in I$ eli $r \in I$. Näin ollen $R \subseteq I$. Käänteisesti, koska I on renkaan R ihanne, niin $I \subseteq R$. Täten $I = R$. □

Seuraus Jos R on 1–rengas ja I sen ihanne, joka sisältää ykkösalkion, niin $I = R$.

Todistus Ykkösalkio on kääntyvä. □

Lause 3.7.3 *Jos I ja J ovat renkaan R ihanteita, niin $I \cap J$ on renkaan R ihanne.*

Todistus Sovelletaan ihannekriteeriä (lause 3.7.1). (Harjoitustehtävä.)

Määritelmä Olkoon R rengas ja S sen osajoukko. Silloin joukon S *virittämä ihanne* $\langle S \rangle$ on suppein ihanne, joka sisältää joukon S. Jos $S = \{a\}$, niin merkitään $\langle S \rangle = \langle a \rangle$ ja sanotaan, että $\langle a \rangle$ on alkion a virittämä ihanne. Yhden alkion virittämää ihannetta sanotaan *pääihanteeksi*.

Huomautus Joukon S virittämä ihanne on olemassa ja on yksikäsitteinen. Se on kaikkien joukon S sisältävien ihanteiden leikkaus.

Lause 3.7.4 *Olkoon R kommutatiivinen rengas ja $a \in R$. Silloin*

$$\langle a \rangle = \{x \in R |\ x = ra + na, \quad r \in R, n \in \mathbf{Z}\}.$$

Todistus Merkitään $A = \{x \in R |\ x = ra + na, \quad r \in R, n \in \mathbf{Z}\}$. Todistetaan, että A on suppein ihanne, joka sisältää alkion a, ts. että $A = \langle a \rangle$. Kun asetetaan $r = 0$ ja $n = 1$, saadaan $a \in A$, ts. A *sisältää* alkion a. Ihannekriteerin (lause 3.7.1) avulla voidaan todistaa, että A on *ihanne*. (Harjoitustehtävä.) Todistetaan, että A on *suppein* ihanne, joka sisältää alkion a. Olkoon I jokin ihanne, joka sisältää alkion a. Todistetaan, että $A \subseteq I$. Olkoon $x \in A$. Silloin $x = ra + na$, missä $r \in R$ ja $n \in \mathbf{Z}$. Ihannekriteerin kohdan 2) nojalla $ra \in I$ ja kohdan 1) nojalla $na \in I$. Edelleen kohdan 1) nojalla $ra + na \in I$ eli $x \in I$. Täten $A \subseteq I$. □

Seuraus Jos R on kommutatiivinen 1–rengas, niin

$$\langle a \rangle = \{ra |\ r \in R\}\ \ (= Ra = aR).$$

Todistus Tarkastellaan lauseketta $x = ra + na$. Jos $n \in \mathbf{Z}^+$, niin

$$na = \underbrace{a + a + \cdots + a}_{n \text{ kpl}} = 1 \cdot a + 1 \cdot a + \cdots + 1 \cdot a = (1 + 1 + \cdots + 1)a = r'a,$$

missä $1 \in R$ ja $r' = 1 + 1 + \cdots + 1 \in R$. Näin ollen

$$x = ra + na = ra + r'a = (r + r')a = r''a,$$

missä $r'' \in R$. Siis x on haluttua muotoa. Tapaukset $n = 0$ ja $n \in \mathbf{Z}^-$ käsitellään vastaavalla tavalla. □

Esimerkki 3.7.4 Tarkastellaan rengasta $(\mathbf{Z}, +, \cdot)$. Silloin

$$\langle m \rangle = m\mathbf{Z}.$$

Määritelmä Renkaan R ihanne M on *maksimaalinen ihanne*, jos

1) $M \neq R$ ja

2) ei ole olemassa sellaista ihannetta I, että $M \subset I \subset R$.

(Tässä merkintä $A \subset B$ tarkoittaa, että $A \subseteq B$ ja $A \neq B$.)

Huomautus Renkaalla voi olla useita maksimaalisia ihanteita.

Lause 3.7.5 *Ihanne $m\mathbf{Z}$ on renkaan $(\mathbf{Z}, +, \cdot)$ maksimaalinen ihanne, jos ja vain jos m on alkuluku.*

Todistus 1) Jos $m = 0$, niin $m\mathbf{Z} = 0\mathbf{Z} \subset 2\mathbf{Z} \subset \mathbf{Z}$. Näin ollen maksimaalisen ihanteen määritelmän kohdan 2) nojalla $0\mathbf{Z}$ eli $\{0\}$ ei ole maksimaalinen ihanne.

2) Jos $m = 1$, niin $m\mathbf{Z} = 1\mathbf{Z} = \mathbf{Z}$. Näin ollen maksimaalisen ihanteen määritelmän kohdan 1) nojalla $1\mathbf{Z}$ ei ole maksimaalinen ihanne.

3) Oletetaan, että m on yhdistetty luku. Merkitään $m = ab$, missä $1 < a,\ b < m$. Silloin

$$m\mathbf{Z} \subset a\mathbf{Z} \subset \mathbf{Z}.$$

(Harjoitustehtävä.) Näin ollen maksimaalisen ihanteen määritelmän kohdan 2) nojalla $m\mathbf{Z}$ ei ole maksimaalinen ihanne.

4) Oletetaan, että m on alkuluku. Merkitään $m = p$. Silloin $m\mathbf{Z} = p\mathbf{Z} \neq \mathbf{Z}$, joten maksimaalisen ihanteen määritelmän kohta 1) on voimassa. Todistetaan, että myös kohta 2) on voimassa. Olkoon I sellainen ihanne, että $p\mathbf{Z} \subset I \subseteq \mathbf{Z}$. Todistetaan, että $I = \mathbf{Z}$. Olkoon $n \in \mathbf{Z}$ mielivaltaisesti valittu. Todistetaan, että $n \in I$. Koska $I \neq p\mathbf{Z}$, niin on olemassa sellainen $k \in I$, että $k \notin p\mathbf{Z}$ ts. $p \nmid k$. Näin ollen yhtälö

$$px \equiv n \pmod{k}$$

on ratkeava. Olkoon $px_0 \equiv n \pmod{k}$. Silloin on olemassa sellainen $y_0 \in \mathbf{Z}$, että

$$px_0 + ky_0 = n.$$

Koska $p\mathbf{Z} \subseteq I$, niin $px_0 \in I$. Koska $k \in I$, niin $ky_0 \in I$. Täten $px_0 + ky_0 \in I$ eli $n \in I$. Siis $I = \mathbf{Z}$ ja maksimaalisen ihanteen määritelmän kohta 2) on voimassa. Näin ollen $p\mathbf{Z}$ on maksimaalinen ihanne. □

Huomautus Lauseen 3.7.5 kohta 4) olisi selvästi helpompi todistaa, jos käytettäisiin tulosta, jonka mukaan renkaan $(\mathbf{Z}, +, \cdot)$ kaikki ihanteet ovat $m\mathbf{Z}$, missä $m = 0, 1, 2, \ldots$ (Tulosta ei ole tässä monisteessa todistettu.)

3.8 Tekijärengas

Olkoon $(R, +, \cdot)$ rengas ja I sen ihanne. Silloin I on renkaan R alirengas. Näin ollen

$$(I, +) \leq (R, +).$$

Koska yhteenlasku alirenkaassa on kommutatiivinen, niin

$$(I, +) \trianglelefteq (R, +).$$

Aliryhmän I määräämä ekvivalenssirelaatio $\equiv \pmod{I}$ joukossa R on muotoa

$$a \equiv b \pmod{I} \Leftrightarrow a \in b + I. \tag{1}$$

Ekvivalenssirelaation $\equiv \pmod{I}$ ekvivalenssiluokkien (eli tässä sivuluokkien) joukko on

$$R/I = \{a + I |\ a \in R\}.$$

Lauseissa 3.4.1 ja 3.4.2 olemme todistaneet, että ekvivalenssirelaatio $\equiv \pmod{I}$ ja laskutoimitus $+$ ovat yhteensopivat ja että pari $(R/I, +)$ on ryhmä, missä yhteenlasku määritellään kaavalla

$$(a + I) + (b + I) = (a + b) + I.$$

Lauseessa 3.8.1 todistamme, että kertolasku $\cdot$ ja ekvivalenssirelaatio $\equiv \pmod{I}$ ovat yhteensopivat, ja lauseessa 3.8.2 todistamme, että $(R/I, +, \cdot)$ on rengas.

Lause 3.8.1 *Olkoon $(R, +, \cdot)$ rengas ja I sen ihanne. Silloin pari $(R/I, \cdot)$ on algebrallinen struktuuri, missä $\cdot$ määritellään kaavalla*

$$(a + I)(b + I) = ab + I.$$

Todistus Lauseen 3.2.1 nojalla riittää todistaa, että renkaan R kertolasku $\cdot$ ja kaavan (1) määrittelemä ekvivalenssirelaatio $\equiv \pmod{I}$ ovat yhteensopivat. Olkoon $a \equiv a' \pmod{I}$ ja $b \equiv b' \pmod{I}$. Silloin

$$a \in a' + I, \quad b \in b' + I$$

eli on olemassa sellaiset i_1, $i_2 \in I$, että

$$a = a' + i_1, \quad b = b' + i_2,$$

joten osittelulakien perusteella

$$ab = a'b' + a'i_2 + i_1b' + i_1i_2.$$

Koska I on ihanne, niin $a'i_2 + i_1b' + i_1i_2 \in I$. Näin ollen

$$ab \in a'b' + I$$

eli

$$ab \equiv a'b' \pmod{I}.$$

Täten kertolasku $\cdot$ ja ekvivalenssirelaatio $\equiv \pmod{I}$ ovat yhteensopivat. □

Lause 3.8.2 *Olkoon $(R, +, \cdot)$ rengas ja I sen ihanne. Silloin $(R/I, +, \cdot)$ on rengas, ns. tekijärengas.*

Todistus 1) Olemme aikaisemmin todenneet, että $(R/I, +)$ on ryhmä. Koska yhteenlasku renkaassa R on kommutatiivinen, niin yhteenlasku ryhmässä R/I on kommutatiivinen. (Totea!) Siis $(R/I, +)$ on Abelin ryhmä.

2) Lauseen 3.8.1 mukaan $(R/I, \cdot)$ on algebrallinen struktuuri. Koska kertolasku renkaassa R on assosiatiivinen, niin kertolasku algebrallisessa struktuurissa $(R/I, \cdot)$ on assosiatiivinen. (Totea!) Siis $(R/I, \cdot)$ on puoliryhmä.

3) Osittelulait tekijäjoukossa R/I seuraavat renkaan R osittelulaeista. (Totea!) □

Esimerkki 3.8.1 Renkaan $(\mathbf{Z}, +, \cdot)$ alirenkaat $m\mathbf{Z}$ ovat ihanteita. Siis

$$(\mathbf{Z}/m\mathbf{Z}, +, \cdot)$$

on rengas. Kyseessä on sama rengas kuin

$$(\mathbf{Z}_m, +, \cdot)$$

(ks. esimerkki 3.1.2).

Seuraavaksi tutkimme, milloin tekijärengas on kunta.

Lause 3.8.3 *Olkoon I kommutatiivisen 1–renkaan R ihanne. Silloin $(R/I, +, \cdot)$ on kunta, jos ja vain jos I on maksimaalinen ihanne.*

Todistus 1) Oletetaan, että $(R/I, +, \cdot)$ on kunta. Todistetaan, että I on maksimaalinen ihanne. Olkoon J sellainen ihanne, että $I \subset J \subseteq R$. Pitää todistaa, että $J = R$. Koska $I \subset J$, niin on olemassa sellainen $a \in J$, että $a \notin I$. Koska $a \notin I$, niin $a + I \neq I$ toisin sanoen $a + I$ ei ole kunnan R/I nolla-alkio. Täten alkiolla $a + I \in R/I$ on käänteisalkio, ts. on olemassa sellainen $b + I \in R/I$, että

$$(a + I)(b + I) = 1 + I$$

eli

$$ab + I = 1 + I.$$

Koska $0 \in I$, niin on olemassa sellainen $i \in I$, että

$$ab + i = 1.$$

Koska $a \in J$ ja $b \in R$, niin $ab \in J$. Koska lisäksi $i \in I \subseteq J$, niin $ab + i \in J$ eli $1 \in J$. Täten lauseen 3.7.2 seurauksen mukaan $J = R$.

2) Oletetaan, että I on maksimaalinen ihanne. Todistetaan, että $(R/I, +, \cdot)$ on kunta. Koska R on kommutatiivinen 1–rengas, niin on helppo todistaa, että R/I on kommutatiivinen 1–rengas. (Totea!) Vielä pitää todistaa, että alkiolla $a + I$ $(\neq I)$ on käänteisalkio, missä $a + I \in R/I$. Koska $a + I \neq I$, niin $a \notin I$. Tarkastellaan joukkoa $J = \{ar + b |\ r \in R, b \in I\}$. Silloin J on renkaan R ihanne ja $I \subset J \subseteq R$. (Harjoitustehtävä.) Koska I on maksimaalinen ihanne, niin $J = R$. Näin ollen $1 \in J$, joten 1 on muotoa

$$1 = ar + b, \quad \text{missä } r \in R, b \in I.$$

Silloin

$$1 + I = (ar + b) + I = (ar + I) + (b + I).$$

Koska $b \in I$, niin $b + I = I$ eli $b + I$ on renkaan R/I nolla-alkio. Näin ollen

$$1 + I = ar + I = (a + I)(r + I).$$

Koska R/I on kommutatiivinen, niin tämä todistaa, että $r + I$ on alkion $a + I$ käänteisalkio. □

Esimerkki 3.8.2 Renkaan $(\mathbf{Z}, +, \cdot)$ ihanne $m\mathbf{Z}$ on maksimaalinen, jos ja vain jos m on alkuluku (ks. lause 3.7.5). Näin ollen rengas $(\mathbf{Z}/m\mathbf{Z}, +, \cdot)$ on kunta, jos ja vain jos m on alkuluku. Tämä tulos on sama kuin lause 3.6.4.

Huomautus Jos $P(x)$ on renkaan $(F[x], +, \cdot)$ jaoton polynomi, missä F on kunta, niin polynomin $P(x)$ virittämä ihanne $\langle P(x) \rangle$ on maksimaalinen ihanne. (Todistus sivuutetaan.) Koska rengas $F[x]$ on kommutatiivinen 1–rengas, niin lauseen 3.8.3 mukaan tekijärengas $F[x]/\langle P(x) \rangle$ on kunta.

Esimerkki 3.8.3 Rengas $\mathbf{Z}_5$ on kunta ja polynomi $x^3 + \overline{3}x + \overline{2}$ on jaoton polynomirenkaassa $\mathbf{Z}_5[x]$. (Totea!) Näin ollen tekijärengas

$$\mathbf{Z}_5[x]/\langle x^3 + \overline{3}x + \overline{2} \rangle$$

on kunta. Sen alkiot ovat muotoa

$$A(x) + \langle x^3 + \overline{3}x + \overline{2} \rangle, \quad \text{missä } A(x) \in \mathbf{Z}_5[x].$$

Jaetaan polynomi $A(x)$ jakoalgoritmin avulla polynomilla $x^3 + \overline{3}x + \overline{2}$. Silloin saadaan

$$A(x) = Q(x)(x^3 + \overline{3}x + \overline{2}) + R(x), \quad \text{missä } \deg R(x) < 3.$$

Lauseen 3.7.4 seurauksen perusteella $Q(x)(x^3 + \overline{3}x + \overline{2}) \in \langle x^3 + \overline{3}x + \overline{2} \rangle$, joten

$$A(x) + \langle x^3 + \overline{3}x + \overline{2} \rangle = R(x) + \langle x^3 + \overline{3}x + \overline{2} \rangle, \quad \text{missä } \deg R(x) < 3.$$

Kun $A(x)$ käy läpi joukon $\mathbf{Z}_5[x]$, niin $R(x)$ käy läpi kaikki joukon $\mathbf{Z}_5$ polynomit, joiden aste on < 3. Näin ollen tekijärenkaan $\mathbf{Z}_5[x]/\langle x^3 + \overline{3}x + \overline{2} \rangle$ alkioiden lukumäärä on 5^3. Tämä on siis esimerkki äärellisestä kunnasta. Huomaa, että alkioiden lukumäärä on muotoa p^n, missä p on alkuluku.