Sisältö

Luku 0. Kuvausten hajottaminen 1
0.1. Kuvausten yleiset hajotelmat 1
Ongelman asettelu 1
Yksikäsitteisyys 2
Olemassaolo 2
0.2. Kuvausten kanoniset hajotelmat 3

Luku 1. Algebralliset struktuurit 5
1.1. Laskutoimitukset 5
Homomorfismit 6
Liitännäisyys 6
Vakaat osajoukot 8
Vaihdannaisuus 9
Tekijämagmat 10
1.2. Neutraalialkiot ja käänteisalkiot 11
Kääntyvät alkiot 13
Jakomonoidi 15
1.3. Ryhmät 20
Homomorfismit 20
Aliryhmät 20
Tekijäryhmät 21
Homomorfismien hajotelmat 23
Isomorfialauseet 24
Tulot 27
1.4. Toiminnat 28
Homomorfismit 30
Vakaat osajoukot 30
Radat 31
Homogeeniset joukot 32
1.5. Ratkeavat ja nilpotentit ryhmät 36
Jordanin-Hölderin lause 37
Ratkeavat ryhmät 38
p-ryhmät 40
Sylowin aliryhmät 40
Nilpotentit ryhmät 42
1.6. Vapaat vaihdannaiset ryhmät ja monoidit 44
Konstruktio 45

Virittäjät 45
Universaaliominaisuus 46
1.7. Renkaat 48
Homomorfismit 48
Alirenkaat 49
Ideaalit 49
Tekijärenkaat 50
Jakorenkaat 51
1.8. Kunnat 54

Luku 2. Lineaarialgebraa 57
2.1. Modulit 57
Lineaariset yhdistelmät 58
Lineaarikuvaukset 58
Alimodulit 59
Tekijämodulit 60
Modulien tulot 61
Modulien suorat summat 62
Vapaat perheet ja kannat 64
2.2. Tensoritulot 68
Bilineaariset kuvaukset 68
Tensoritulon konstruktio 70
Tensoritulon ominaisuuksia 75
2.3. Algebrat 80
Homomorfismit 81
Alialgebrat, ideaalit ja tekijäalgebrat 81
Ykköselliset algebrat 82
Algebrojen kannat 83
Magma-, monoidi- ja ryhmäalgebrat 85
2.4. Polynomialgebrat 87
Polynomialgebran konstruktio 88
Universaaliominaisuus 89
2.5. Derivaattakuvaukset 92

Luku 3. Jaollisuus 97
3.1. Jaollisuusrelaatio 97
Liittoalkiot 98
Jaottomat alkiot 99
3.2. Faktoriaaliset renkaat 100
Eukleideen renkaat 105
3.3. Polynomien jaollisuus 108
Eisensteinin kriteerio 112

Luku 4. Vaihdannaiset kunnat 115
4.1. Laajennukset 115
Aste 116

Adjunktio 118
4.2. Algebralliset laajennukset 119
Algebrallisuuden transitiivisuus 124
Sovellus: Geometriset konstruktiot 125
4.3. Algebrallisesti suljetut laajennukset 128
Upotuslause 130
Juurikunnat 131
Kunnan algebrallinen sulkeuma 135
4.4. Konjugaatit ja normaalit laajennukset 137
Normaalilaajennusten virittäjäjoukot 142
4.5. Separoituvat algebralliset laajennukset 143
Separoituvat polynomit 143
Homomorfismien lineaarinen riippumattomuus 145
Laajennuksen separoituva aste 146
Separoituvat algebralliset alkiot 147
Separoituvat algebralliset laajennukset 148
4.6. Galois'n laajennukset 149
Galois'n ryhmä 151
Artinin lause 153
Galois'n teorian peruslause 155
4.7. Abelin laajennukset 158
Ykkösenjuuret 159
Ykkösenjuurikunnat 162
Äärelliset eli Galois'n kunnat 164
Sykliset laajennukset 165
Yhtälöiden algebrallinen ratkeavuus 168

Liite A. Zornin lemma 175
A.1. Järjestetyt joukot 175
Maksimaaliset alkiot ja ylärajat 177
A.2. Valintakuvaukset 177
A.3. Rekursio 179
A.4. Ketjulause ja Zornin lemma 181
A.5. Rekursiolauseen todistus 182

Liite B. Permutaatiot 185
B.1. Syklit 185
Permutaation esitys sykleillä 186
Vaihdokset 187
B.2. Permutaation merkki 188

Kirjallisuutta 191

Merkinnät 193

Hakemisto 195

LIITE A

Zornin lemma

Matemaattisissa todistuksissa on usein suoritettava valintoja. Se ei ole ongelmallista, jos on valittava vain yksi alkio kerrallaan ja tiedetään, että valittavien alkioiden joukko ei ole tyhjä.

Asia ei kuitenkaan ole yhtä selvä, kun on tehtävä useita – tavallisesti ääretön määrä – toisistaan riippuvia valintoja samanaikaisesti. Tyypillinen esimerkki algebran alalta on Krullin lause renkaan maksimaalisista ideaaleista (lause 1.7.7). Sen todistamiseksi on osoitettava, että renkaasta voidaan valita alkiot, joiden joukko on annetun ideaalin sisältävä aito ideaali, vieläpä niin, että ainoa laajempi ideaali on koko rengas.

Mutkikkaat valintatehtävät ratkaistaan tavallisesti seuraavaan tapaan: Aluksi tarkastellaan toivottujen ratkaisujen ohella myös "osittaisia ratkaisuja" eli sellaisia ratkaisuehdokkaita, jotka toteuttavat vain osan vaadituista ehdoista. Sitten vertaillaan ehdokkaita eli täsmällisemmin sanottuna määritellään niiden joukossa järjestys, jota voi ajatella "paremmuusjärjestykseksi." Lopuksi etsitään parhaat mahdolliset ehdokkaat ja osoitetaan, että ne ovat toivottuja ratkaisuja.

Esimerkiksi Krullin lauseen tapauksessa ehdokkaita ovat kaikki annetun ideaalin sisältävät aidot ideaalit. Järjestys niiden joukossa on tavallinen sisältymisrelaatio: mitä suurempi ideaali, sitä parempi osittainen ratkaisu. Parhaat mahdolliset eli maksimaaliset ehdokkaat ovatkin tehtävän ratkaisuja.

Yllä esitetyn tarkastelun keskeiseksi kysymykseksi jää maksimaalisten alkioiden olemassaolo osittaisten ratkaisujen muodostamassa järjestetyssä joukossa. Tärkein apukeino tällaisten ongelmien ratkaisuun on Zornin lemma.

A.1. Järjestetyt joukot

Ennen Zornin lemman käsittelyä on syytä kerrata järjestysrelaatioita koskevat peruskäsitteet. Olkoon E joukko.

MÄÄRITELMÄ A.1.1. Relaatio $x \leq y$ joukossa E on *järjestys*, kun kaikilla x, y, $z \in E$ pätee

i) $x \leq x$;
ii) jos $x \leq y$ ja $y \leq x$, niin $x = y$;
iii) jos $x \leq y$ ja $y \leq z$, niin $x \leq z$.

Järjestyksellä varustettuna joukko E on *järjestetty joukko*.

Määritelmän ehdot merkitsevät, että järjestysrelaatio on refleksiivinen (i), transitiivinen (iii) ja *antisymmetrinen* (ii). Jos lisäksi kaikilla x, $y \in E$ on voimassa ehto

iv) $x \leq y$ tai $y \leq x$,

niin sanotaan, että E on *täysin järjestetty* joukko ja että sen järjestys on *täysi järjestys*.

Huomautus. Toisinaan sanotaan, että ehdot i) - iii) täyttävä relaatio on *osittainen järjestys*, ja järjestykseltä vaaditaan myös ehto iv). Koska useimmat järjestetyt joukot eivät ole täysin järjestettyjä, on käytännöllisempää jättää pois viittaus osittaisuuteen.

Esimerkkejä. 1) Olkoon X joukko ja $E = \mathcal{P}(X)$ sen potenssijoukko. Tällöin *sisältymisrelaatio* $A \subset B$ on järjestys E:ssä. Se on täysi järjestys vain, jos joukossa X on enintään yksi alkio.

2) Olkoon A järjestetyn joukon E osajoukko. Tällöin relaatio

$$x \in A,\ y \in A \text{ ja } x \leq y$$

on järjestys A:ssa, ns. *indusoitu järjestys*. Tällä varustettuna A on E:n *järjestetty osajoukko*. Jos A on täysin järjestetty, niin sitä sanotaan E:n *ketjuksi*.

3) Jos E on järjestetty joukko, niin relaatio

$$x \leq' y \ \Leftrightarrow\ y \leq x$$

on myös järjestys E:ssä, ns. *käänteinen järjestys*. Tavallisesti sille käytetään merkintää $x \geq y$.

4) Olkoot X ja Y kaksi joukkoa sekä E joukko, jonka muodostavat kaikki parit (A, f), missä $A \subset X$ ja $f\colon A \to Y$ on kuvaus. Tällöin relaatio

$$(A, f) \leq (B, g) \ \Leftrightarrow\ A \subset B \text{ ja } f = g|A$$

on järjestys E:ssä. (Tällainen järjestys tarvitaan usein todistuksissa, joissa käytetään Zornin lemmaa, kuten esim. lauseessa 4.3.4.)

5) Olkoon X joukko ja E sellaisten X:n alkioperheiden $(x_i)_{i\in I}$ muodostama joukko, joiden indeksijoukko I on erään joukon A osajoukko. Kun perheet tulkitaan kuvauksiksi kuten edellisessä esimerkissä, saadaan joukon E järjestysrelaatio

$$(x_i)_{i\in I} \leq (y_j)_{j\in J} \ \Leftrightarrow\ I \subset J \text{ ja } x_i = y_i, \text{ kun } i \in I.$$

Jos $x \leq y$ on järjestys joukossa E, niin E:ssä määritellään relaatio $x < y$ ehdolla

$$x \leq y \text{ ja } x \neq y.$$

Tällöin kaikilla alkioilla x, y, $z \in E$ ovat voimassa seuraavat tulokset:

$$x \leq y \ \Leftrightarrow\ x < y \text{ tai } x = y,$$

$$x \leq y \text{ ja } y < z \ \Rightarrow\ x < z,$$

$$x < y \text{ ja } y \leq z \ \Rightarrow\ x < z.$$

Maksimaaliset alkiot ja ylärajat.

MÄÄRITELMÄ A.1.2. Järjestetyn joukon E alkio a on sen *maksimaalinen alkio*, kun ehdoista $x \in E$, $x \geq a$ seuraa $x = a$.

Alkio a on joukon E *suurin alkio*, kun $x \leq a$ kaikilla $x \in E$.

Jos joukossa on suurin alkio, niin se on yksikäsitteinen ja samalla ainoa joukon maksimaalinen alkio. Jos suurinta alkiota ei ole, maksimaalisia alkioita voi olla useita.

Kun tarkastellaan joukon käänteistä järjestystä, saadaan vastaavasti *minimaalisen alkion* ja *pienimmän alkion* määritelmät.

MÄÄRITELMÄ A.1.3. Olkoon E järjestetty joukko ja A sen osajoukko. Alkio $a \in E$ on joukon A *yläraja*, kun $x \leq a$ kaikilla $x \in A$. Alkio $a \in E$ on A:n *pienin yläraja* joukossa E, kun se on A:n kaikkien ylärajojen joukon pienin alkio.

Käänteistä järjestystä tarkastelemalla saadaan taas osajoukon *alarajan* ja *suurimman alarajan* määritelmät.

Jos järjestetyn joukon E osajoukon A pienin yläraja (tai suurin alaraja) joukossa E on olemassa, niin se on yksikäsitteinen ja sille käytetään merkintää

$$\sup_E A \text{ tai } \sup A \qquad (\text{ja } \inf_E A = \inf A).$$

Jos joukossa A on suurin (tai pienin) alkio, niin se on myös pienin yläraja $\sup A$ (tai vastaavasti suurin alaraja $\inf A$).

Esimerkki 6) Olkoon E joukon X potenssijoukko $\mathcal{P}(X)$ ja

$$A = \{Y_i \mid i \in I\}, \quad Y_i \subset X \, (i \in I),$$

jokin E:n epätyhjä osajoukko. Tällöin on E:ssä aina olemassa pienin yläraja ja suurin alaraja

$$\sup A = \bigcup_{i \in I} Y_i \,, \quad \inf A = \bigcap_{i \in I} Y_i \,.$$

(Jos $A = \emptyset$, niin $\sup A = \emptyset$ ja $\inf A = X$; muulloin $\inf A \subset \sup A$.)

A.2. Valintakuvaukset

Olkoon E järjestetty joukko. Tavoitteena on löytää maksimaalisia alkioita joukosta E. Jos sellaisia ylimalkaan on olemassa, niitä voi olla useita, ja siksi maksimaalisen alkion tavoittamiseen tarvitaan yleensä valintoja. Ei voida odottaa, että olisi olemassa jokin yleinen menetelmä, jolla maksimaalinen alkio voitaisiin suoraan määrittää. Eräs tapa tehdä valintoja on seuraava.

Valitaan aluksi jokin E:n alkio x_0. Jotta valinta olisi mahdollinen, on tietenkin oletettava, että E ei ole tyhjä. Tarkastellaan sitten joukkoa

$$A_0 =]x_0, \rightarrow[\, = \{x \in E \mid x_0 < x\},$$

jonka muodostavat alkiota x_0 aidosti suuremmat E:n alkiot.

Jos $A_0 = \emptyset$, niin x_0 on E:n maksimaalinen alkio ja tavoite on saavutettu. Muussa tapauksessa A_0 on E:n aito epätyhjä osajoukko. Lisäksi A_0 sisältää kaikki mitä tahansa alkiotaan x suuremmat E:n alkiot. Tästä seuraa, että x on maksimaalinen A_0:ssa, jos ja vain jos se on maksimaalinen E:ssä, ja siten jatkossa on riittävää etsiä maksimaalinen alkio osajoukosta A_0.

Toistetaan sama menettely: Valitaan alkio $x_1 \in A_0$ ja tarkastellaan A_0:n aitoa osajoukkoa

$$A_1 =]x_1, \rightarrow[\,.$$

Jos nyt A_1 on tyhjä, niin x_1 on maksimaalinen. Muuten jatketaan samaan tapaan, kunnes saadaan joko maksimaalinen alkio tai päättymätön aidosti kasvava jono E:n alkioita

$$x_0 < x_1 < x_2 < \cdots < x_n < \cdots\,.$$

Siirretään myöhemmäksi kysymys siitä, miten tästä eteenpäin olisi jatkettava. Sen sijaan selvitetään ensin, kuinka edellä hahmoteltu menettely voitaisiin muotoilla täsmällisesti. Ennen kaikkea miten siinä tehdyt valinnat olisi mahdollista perustella.

Ensi näkemältä vaikuttaa siltä, että alkioiden x_n löytämiseksi joudutaan suorittamaan ääretön määrä toisistaan riippuvia valintoja. Lähempi tarkastelu osoittaa kuitenkin, että näin ei ole asian laita. Vaikka yllä valinnat kuvattiin peräkkäisinä, ne ovat kuitenkin oleellisesti toisistaan riippumattomia.

Jokaiseen alkioon $x \in E$ liittyy E:n osajoukko

$$A_x =]x, \rightarrow[\,.$$

Olkoon S niiden alkioiden x joukko, joilla A_x ei ole tyhjä. Jos $x \in S$, niin A_x:stä voidaan valita alkio $p(x)$. Tällainen valinta voidaan tehdä kaikilla alkioilla $x \in S$ toisistaan riippumatta. Näin saadaan kuvaus

$$p\colon S \to E,$$

joka kaikilla $x \in S$ toteuttaa ehdon

$$p(x) \in A_x.$$

Tällaista kuvausta sanotaan *valintakuvaukseksi*.

Yllä esitetty periaate, jonka mukaan mielivaltainen määrä valintoja voidaan tehdä samanaikaisesti, kun ne ovat riippumattomia toisistaan, tunnetaan nimellä *valinta-aksiooma*. Se voidaan yleisesti muotoilla seuraavasti.

Olkoon $(X_i)_{i\in I}$ perhe epätyhjiä joukkoja. Tällöin on olemassa valintakuvaus

$$p\colon I \to \bigcup_{i\in I} X_i,$$

joka kaikilla $i \in I$ toteuttaa ehdon $p(i) \in X_i$.

Huomautus. Kun tulkitaan valintakuvaukset p alkioperheiksi $(x_i)_{i\in I}$, missä $x_i = p(i) \in X_i$, valinta-aksiooma saa lyhyen ja helposti ymmärrettävän muodon

$$\prod_{i\in I} X_i \neq \emptyset.$$

A.3. Rekursio

Valintakuvausta käyttäen voidaan palata yllä esitettyyn menettelyyn jonoa (x_n) valittaessa. Joukon E järjestystä ei tällöin tarvita. Tulos saadaan suoraan seuraavasta lauseesta.

LAUSE A.3.1. *Olkoon E joukko, S sen osajoukko, $p\colon S \to E$ kuvaus ja a jokin E:n alkio. On olemassa yksikäsitteinen $r \in \mathbf{N} \cup \{\infty\}$ ja jono $(x_n)_{n\in\mathbf{N},n\leq r}$, joka toteuttaa ehdot*

i) $x_0 = a$;
ii) $x_n \in S$ *ja* $x_{n+1} = p(x_n)$, *kun* $n < r$;
iii) $x_r \notin S$, *jos* $r \neq \infty$.

Todistus. Tarkastellaan äärellisiä jonoja $(x_n)_{0\leq n\leq r}$, jotka toteuttavat ehdot i) ja ii). Niiden joukko $\mathcal{M}$ ei ole tyhjä, koska se sisältää ainakin jonon, jossa on vain yksi alkio $x_0 = a$.

Olkoot $(x_n)_{0\leq n\leq r}$ ja $(y_n)_{0\leq n\leq s}$ kaksi joukkoon $\mathcal{M}$ kuuluvaa jonoa. Osoitetaan induktiolla, että $x_n = y_n$, kun $n \leq \min(r, s)$. Ehdon i) nojalla tämä pätee, kun $n = 0$.

Oletetaan sitten, että $x_n = y_n$ jollakin $n < \min(r, s)$. Ehdosta ii) seuraa silloin $x_n = y_n \in S$ ja $x_{n+1} = p(x_n) = p(y_n) = y_{n+1}$. Väite pitää siten paikkansa.

Yllä on nähty, että jonot $(x_n) \in \mathcal{M}$ eroavat toisistaan vain pituutensa puolesta; muuten niissä on samat alkiot. Jokaista lukua $r \in \mathbf{N}$ kohti on siis enintään yksi ehdot i) ja ii) täyttävä jono.

Tällöin on kaksi mahdollisuutta: joko $\mathcal{M}$:ssä on mielivaltaisen pitkiä jonoja tai sitten niiden joukossa yksi on pisin. Jälkimmäisessä tapauksessa ehto iii) on välttämättä voimassa, koska muuten jonoa olisi mahdollista vielä jatkaa; edellisessä voidaan taas kaikki $\mathcal{M}$:n jonot yhdistää äärettömäksi jonoksi, jota ehto iii) ei koske. Kummassakin tapauksessa jono on yksikäsitteinen. □

Kun E on epätyhjä järjestetty joukko, S on sen maksimaalisten alkioiden joukon komplementti ja $p\colon S \to E$ täyttää ehdon $x < p(x)$ kaikilla $x \in S$, lauseesta seuraa, että E:ssä on maksimaalinen alkio $m = x_r \notin S$ tai ääretön kasvava alkiojono $(x_n)_{n\in\mathbf{N}}$. (Siinä voi myös olla sekä maksimaalinen alkio että kasvava jono.)

Tarkastellaan nyt lähemmin sitä tapausta, jossa joukosta E on löydetty aidosti kasvava jono

$$x_0 < x_1 < x_2 < \cdots < x_n < \cdots .$$

Tällöin on kaksi mahdollisuutta: joko alkioiden x_n joukolla on yläraja $x \in E$ tai sitten niillä ei ole ylärajaa E:ssä. Jos ylärajaa ei ole, syynä voi olla, ettei E:ssä ole yhtään maksimaalista alkiota. Monesti voidaan kuitenkin osoittaa, että jonolla (x_n) on yläraja E:ssä. Tällöin valintamenettelyä voidaan jatkaa.

Oletetaan, että jonolla on yläraja E:ssä, ja valitaan niistä yksi, x_ω, joka siis täyttää ehdon

$$x_0 < x_1 < x_2 < \cdots < x_n < \cdots < x_\omega.$$

Indeksi ω merkitsee ensimmäistä ääretöntä järjestyslukua. Jos x_ω ei ole maksimaalinen E:ssä, voidaan valita sitä suurempi alkio $x_{\omega+1}$ ja valintoja voidaan jatkaa, kunnes kohdataan maksimaalinen alkio tai saadaan uusi ääretön kasvava E:n alkiojono

$$x_\omega < x_{\omega+1} < x_{\omega+2} < \cdots < x_{\omega+n} < \cdots .$$

Jos tällaisella jonolla on yläraja E:ssä, voidaan taas valita niistä yksi, $x_{\omega+\omega}$. Näin on ilmeisesti mahdollista jatkaa valintoja niin kauan kuin muodostuville jonoille löytyy ylärajoja E:ssä.

Kun halutaan täsmentää viimeksi kuvattua menettelyä havaitaan yksinkertaisen jonon (x_n) etsimiseen verrattuna kaksi eroa. Ensinnäkin yksittäisten epämaksimaalisten alkioiden x_n, $x_{\omega+n}$, ... joukossa määritellyn valintakuvauksen ohella tarvitaan kuvaus, joka valitsee kokonaiselle jonolle ylärajan. Ja toiseksi luonnollisten lukujen lisäksi indekseinä esiintyy äärettömiä järjestyslukuja.

Tarkastellaan nyt kumpaakin kohtaa lähemmin. Ehdon $x < p(x)$ täyttävää valintakuvausta p käytetään, kun päättyvää jonon alkuosaa

$$(x_\nu)_{\nu\leq\alpha} \qquad (\alpha = n, \omega + n, \ldots)$$

halutaan jatkaa alkiolla $x_{\alpha+1} = p(x_\alpha)$, joka toteuttaa ehdon

$$x_\nu < x_{\alpha+1} \qquad (\nu \leq \alpha).$$

Niiden alkioiden x_α kiinnittämiseen, joilla ei ole välitöntä edeltäjää ($\alpha = \omega, \omega+\omega, \ldots$), tarvitaan taas kaikista edeltäjistä riippuva valinta:

$$x_\nu < x_\alpha \qquad (\nu < \alpha).$$

Kun $\nu \leq \alpha$ kirjoitetaan muotoon $\nu < \alpha + 1$, nähdään, että ehdot ovat oleellisesti samat. Tarvitaan siis vain yksi valintakuvaus p, joka liittää jokaiseen osajoukkoon

$$U_\alpha = \{x_\nu \mid \nu < \alpha\}$$

ylärajan, joka ei kuulu joukkoon, eli *aidon ylärajan* $x_\alpha = p(U_\alpha)$.

Myös äärettömät järjestysluvut voidaan unohtaa, sillä indeksejä on edellä käytetty vain alkioiden järjestämiseen. Kun koko joukko on jo järjestetty, ei indeksejä tarvita. Esimerkiksi U_α on sama kuin kaikkien alkioiden x_ν muodostaman joukon U osajoukko

$$U_x = \{y \in U \mid y < x\},$$

missä $x = x_\alpha$. Tällaiset joukot $V = U_x$ toteuttavat ehdon

$$\text{jos } x \in V,\ y \in U \text{ ja } y \leq x, \text{ niin } y \in V,$$

ja niitä sanotaan U:n *alkuosiksi*. Palautetaan myös mieleen, että järjestetyn joukon täysin järjestettyjä osajoukkoja sanotaan ketjuiksi. Näiden huomioiden jälkeen voidaan edellinen lause yleistää seuraavasti.

LAUSE A.3.2. *Olkoon E järjestetty joukko, $\mathcal{S}$ joukko sen osajoukkoja ja $p\colon \mathcal{S} \to E$ kuvaus, joka jokaiseen joukkoon $U \in \mathcal{S}$ liittää jonkin sen aidon ylärajan $p(U) \in E$.*

Tällöin on olemassa E:n ketjuja U, jotka toteuttavat ehdon

(R) *Jos V on U:n alkuosa ja $V \neq U$, niin $V \in \mathcal{S}$, $x = p(V) \in U$ ja $V = U_x = \{y \in U \mid y < x\}$.*

Niiden joukossa on suurin F, ja se ei kuulu joukkoon $\mathcal{S}$.

Lauseen todistus on oleellisesti sama kuin edellisellä lauseella ja sivuutetaan toistaiseksi.

Huomautus. Ehto (R) vastaa lauseen A.3.1 ehtoja i) ja ii). Rekursion alkuehtoa i) ei erikseen tarvita, koska $V = \emptyset$ on jokaisen U:n alkuosa ja $x_0 = p(\emptyset)$ on U:n pienin alkio, kun $\emptyset \in \mathcal{S}$. (Jos $\emptyset \notin \mathcal{S}$, niin $F = \emptyset$.)

A.4. Ketjulause ja Zornin lemma

Edellä on nähty, miten ketjuja voidaan jatkaa ylöspäin niin kauan kuin niillä on aito eli joukkoon kuulumaton yläraja. Näin saadaan seuraava yleinen tulos yksin valinta-aksioomaa käyttäen.

LAUSE A.4.1. *Jokaisessa järjestetyssä joukossa on ketju, jolla ei ole aitoa ylärajaa.*

Todistus. Olkoon E järjestetty joukko ja $\mathcal{S}$ niiden E:n ketjujen joukko, joilla on aito yläraja E:ssä. Valinta-aksiooman nojalla on olemassa kuvaus $p\colon \mathcal{S} \to E$, joka kaikilla joukoilla $U \in \mathcal{S}$ toteuttaa ehdon

$$p(U) \in E \setminus U \text{ on } U\text{:n yläraja.}$$

Rekursiolauseen A.3.2 mukaan on tällöin olemassa E:n ketju F, joka ei kuulu joukkoon $\mathcal{S}$ ja jolla siten ei ole aitoa ylärajaa E:ssä, □

KOROLLAARI A.4.2 (Zornin lemma). *Jos järjestetyn joukon E jokaisella ketjulla on yläraja E:ssä, niin E:ssä on maksimaalinen alkio.*

Todistus. Lauseen nojalla E:ssä on ketju F, jolla ei ole aitoa ylärajaa E:ssä. Toisaalta oletuksen mukaan F:llä on kuitenkin yläraja m. Koska se ei ole aito, se kuuluu ketjuun F. Se on silloin F:n suurin alkio ja siten myös sen pienin yläraja.

Olkoon nyt x jokin E:n alkio, joka täyttää ehdon $m \leq x$. Koska m on F:n pienin yläraja, x on myös F:n yläraja. Koska F:llä ei ole aitoa ylärajaa, x kuuluu ketjuun F ja täyttää siten ehdon $x \leq m$. Antisymmetrisyyden nojalla pätee tällöin $x = m$. Alkio m on siis maksimaalinen E:ssä. □

Esimerkki 1) Olkoon K kunta, ja olkoot E ja Ω kaksi sen laajennusta. Tarkastellaan pareja (E', u), missä E' on E:n alilaajennus ja $u\colon E' \to \Omega$ on K-homomorfismi. Upotuslauseen 4.3.4 todistamiseksi tarvitaan maksimaalinen tällainen pari. Sellaisen olemassaolo seuraa Zornin lemmasta.

Oletetaan, että (E_i, u_i) $(i \in I)$ on perhe, jonka alkiot muodostavat ketjun. Tämä merkitsee, että kaikilla $i, j \in I$ joko $E_i \subset E_j$ ja $u_i = u_j|E_i$ tai $E_j \subset E_i$ ja $u_j = u_i|E_j$. Jos nyt x ja y ovat yhdisteen

$$E' = \bigcup_{i \in I} E_i$$

alkioita, niin $x \in E_i$ ja $y \in E_j$ joillakin i, $j \in I$. Silloin x ja y kuuluvat kumpikin suurempaan laajennuksista E_i, E_j, ja se sisältää myös alkiot $x + y$, xy sekä x^{-1}, kun $x \neq 0$. Tämä merkitsee, että E' on myös E:n alilaajennus.

Koska homomorfismit u_i saavat samat arvot kaikilla niillä alkioilla $x \in E'$, joilla ne ovat määritellyt, ne voidaan yhdistää K-homomorfismismiksi $u\colon E' \to \Omega$. Tällöin (E', u) on ketjun $\{(E_i, u_i) \mid i \in I\}$ yläraja. Zornin lemman ehto on siten voimassa ja maksimaalinen pari on olemassa.

Huomautus. Zornin lemman ehdon toteutumiseksi on esimerkissä ratkaisevaa, että ehdot, jotka määrittävät alilaajennukset ja homomorfismit, riippuvat vain *äärellisestä* määrästä alkioita kerrallaan (itse asiassa kahdesta). Tämä on tyypillistä algebrassa ja siksi Zornin lemmaa voidaan käyttää yleensä aina, kun maksimaalisuutta tarvitaan.

Harjoitustehtäviä

1) Olkoon A rengas, E A-moduli ja F E:n alimoduli. Osoitettava, että on olemassa maksimaalinen E:n alimoduli G, joka täyttää ehdon $F \cap G = \{0\}$.

2) Olkoon A rengas ja E A-moduli. Osoitettava, että on olemassa maksimaalinen vapaa E:n alkioperhe $(a_i)_{i \in I}$. (Merkintöjen yksinkertaistamiseksi voidaan tarkastella perheiden asemasta niihin liittyviä joukkoja $H = \{a_i \mid i \in I\}$.)

3) Osoitettava, että valinta-aksiooma seuraa Zornin lemmasta.

A.5. Rekursiolauseen todistus

Palataan lopuksi lauseen A.3.2 todistukseen. Oletetaan, että E on järjestetty joukko, $\mathcal{S}$ on joukko sen osajoukkoja ja $p\colon \mathcal{S} \to E$ on kuvaus, joka kaikilla joukoilla $U \in \mathcal{S}$ täyttää ehdon

$$p(U) \in E \setminus U \text{ on } U\text{:n yläraja.}$$

Olkoon $\mathcal{M}$ joukko, jonka muodostavat kaikki ehdon (R) toteuttavat E:n ketjut U. Se sisältää ainakin joukon $U = \emptyset$.

LEMMA A.5.1. *Jos U, $U' \in \mathcal{M}$, niin U on U':n alkuosa tai U' on U:n alkuosa.*

Todistus. Jokaiseen alkioon $x \in U$ liittyy U:n alkuosa

$$U_x = \{y \in U \mid y < x\}.$$

Olkoon V niiden alkioiden $x \in U \cap U'$ joukko, jotka täyttävät ehdon $U_x = U'_x$. Osoitetaan, että V on U:n ja U':n yhteinen alkuosa.

Olkoon $x \in V$. Jos $y \in U$ ja $y < x$, niin y kuuluu joukkoon U_x ja alkuosa U_y on sama kuin U_x:n alkuosa $(U_x)_y$. Toisaalta $U_x = U'_x$. Siten y kuuluu myös joukkoon U' ja $(U_x)_y = (U'_x)_y$. Tämä merkitsee, että $U_y = U'_y$ ja siksi $y \in V$. Siis V on U:n alkuosa. Symmetrian vuoksi se on myös U':n alkuosa.

Lopuksi on riittävää osoittaa, että $V = U$ tai $V = U'$. Jos $V \neq U$, niin ehdon (R) nojalla $V \in \mathcal{S}$, $x = p(V) \in U$ ja $V = U_x$. Jos tällöin olisi $V \neq U'$, niin vastaavasti $x \in U'$ ja $V = U'_x$, joten x kuuluisi joukkoon V. Tämä on kuitenkin mahdotonta, koska $p(V) \notin V$. Siis täytyy olla $V = U'$. □

Erityisesti nähdään, että joukko $\mathcal{M}$ sisältymisrelaatiolla varustettuna on täysin järjestetty joukko. Olkoon F kaikkien siihen kuuluvien joukkojen yhdiste

$$F = \bigcup_{U \in \mathcal{M}} U.$$

LEMMA A.5.2. *Joukko F on täysin järjestetty ja toteuttaa ehdon* (R).

Todistus. Jokainen F:n alkio x kuuluu johonkin joukkoon $U \in \mathcal{M}$. Jos y on toinen F:n alkio ja $y \in U'$, $U' \in \mathcal{M}$, niin edellisen lemman nojalla x ja y kumpikin kuuluvat suurempaan joukoista U ja U'. Koska tämä on ketju, on voimassa $x \leq y$ tai $y \leq x$. Siten F on täysin järjestetty.

Samoin nähdään, että jokainen $U \in \mathcal{M}$ on F:n alkuosa. Jos näet $x \in U$, $y \in F$ ja $y \leq x$, niin y kuuluu johonkin joukkoon $U' \in \mathcal{M}$. Jos $U' \subset U$, niin $y \in U$; muuten U on U':n alkuosa ja siksi taas $y \in U$. Siis joka tapauksessa y on U:ssa.

Osoitetaan sitten, että ehto (R) on voimassa. Olkoon V jokin F:n alkuosa, joka ei ole koko F. Silloin on olemassa alkio $x \in F \setminus V$. Tällöin jokainen $y \in V$ toteuttaa ehdon $y < x$, koska muuten epäyhtälöstä $x \leq y$ seuraisi, että myös x kuuluisi alkuosaan V. Siten $V \subset F_x$ ja V on myös F_x:n alkuosa.

Toisaalta x kuuluu johonkin joukkoon $U \in \mathcal{M}$. Koska U on F:n alkuosa, on $F_x = U_x$, ja siten V on myös U_x:n ja edelleen U:n alkuosa. Lisäksi $V \neq U$, koska $x \in U \setminus V$, joten ehdon (R) nojalla $V \in \mathcal{S}$, $y = p(V) \in U \subset F$ ja $V = U_y = F_y$. Myös ketju F toteuttaa siis ehdon (R). □

Tulos osoittaa, että F kuuluu myös joukkoon $\mathcal{M}$ ja on siten sen suurin alkio. Jos nyt F olisi joukossa $\mathcal{S}$, niin $a = p(F) \notin F$ olisi F:n aito yläraja E:ssä Tällöin $F' = F \cup \{a\}$ olisi myös ketju ja lisäksi se toteuttaisi ehdon (R).

Jos näet V on jokin F':n alkuosa ja $V \neq F'$, niin joko $V = F$ tai $V \subset F$, $V \neq F$. Edellisessä tapauksessa $V = F \in \mathcal{S}$, $p(V) = p(F) = a \in F'$ ja $F'_a = F = V$. Jälkimmäisessä taas $V \in \mathcal{S}$, $x = p(V) \in F \subset F'$ ja $F'_x = F_x = V$, koska (R) pätee F:ssä. Siten F' kuuluisi myös joukkoon $\mathcal{M}$, mikä on mahdotonta, koska F on siinä suurin.

Siis nähdään, että F ei voi olla joukossa $\mathcal{S}$. Tämä päättää lauseen A.3.2 todistuksen.

Huomautus. Joukko F ei ole vain täysin järjestetty vaan toteuttaa seuraavan ehdon:

> *Jokaisessa F:n epätyhjässä osajoukossa on pienin alkio.*

Tämä merkitsee, että F on *hyvin järjestetty* eli F:ssä on *hyvä järjestys*. Kun ehtoa sovelletaan kahden alkion osajoukkoon $\{x, y\}$, nähdään, että jokainen hyvin järjestetty joukko on myös täysin järjestetty.

Todistus. Olkoon A jokin F:n osajoukko. Sen aitojen alarajojen joukko F:ssä

$$V = \{x \in F \mid x < y \text{ kaikilla } y \in A\}$$

on F:n alkuosa. Lisäksi $V \neq F$, kun $A \neq \emptyset$, koska $V \cap A = \emptyset$. Ehdosta (R) seuraa silloin $V \in \mathcal{S}$, $x = p(V) \in F$ ja $V = F_x$.

Osoitetaan, että x on joukon A pienin alkio. Ensinnäkin x on A:n alaraja, koska $A \subset F \setminus V = F \setminus F_x$, ja siten $x \leq y$ kaikilla $y \in A$. Lisäksi x on joukossa A, koska muuten olisi $x < y$ kaikilla $y \in A$, jolloin $x = p(V)$ kuuluisi joukkoon V. Siis x on pienin alkio joukossa A. $\square$

LIITE B

Permutaatiot

Olkoon E joukko. Sen bijektiivisiä kuvauksia $\sigma\colon E \to E$ itselleen sanotaan joukon E *permutaatioiksi*. Laskutoimituksella

$$(\sigma, \tau) \mapsto \sigma\tau = \sigma \circ \tau$$

varustettuna kaikkien E:n permutaatioiden joukko $\mathfrak{S}_E$ on ryhmä, joukon E *symmetrinen ryhmä*. Sillä on joukossa E *kanoninen toiminta*

$$(\sigma, x) \mapsto \sigma(x).$$

Kun E on väli $[1, n] \subset \mathbf{N}$, vastaavalle symmetriselle ryhmälle käytetään merkintää $\mathfrak{S}_n$. Jokaisen n-alkioisen joukon symmetrinen ryhmä on isomorfinen $\mathfrak{S}_n$:n kanssa.

Symmetrisen ryhmän $\mathfrak{S}_E$ aliryhmiä sanotaan E:n *permutaatioryhmiksi*; koko ryhmä $\mathfrak{S}_E$ on E:n *täysi permutaatioryhmä*. Jokainen E:n permutaatioryhmä G toimii myös E:ssä kanonisen inkluusion $G \hookrightarrow \mathfrak{S}_E$ välityksellä.

Esimerkki 1) Jokainen permutaatio σ virittää permutaatioryhmän. Sen muodostavat σ:n potenssit ja sille käytetään jatkossa merkintää

$$\bar{\sigma} = \{\sigma^k \mid k \in \mathbf{Z}\}.$$

Jos σ^k ei ole identtinen permutaatio, kun $k \neq 0$, niin $\bar{\sigma}$ on isomorfinen $\mathbf{Z}$:n kanssa. Muussa tapauksessa $\bar{\sigma}$ on äärellinen syklinen ryhmä. Tällöin $\bar{\sigma} = \{\sigma^k \mid 0 \leq k < m\}$, missä m on σ:n kertaluku ryhmässä $\mathfrak{S}_E$. Näin käy aina, kun E on äärellinen.

Tästä lähtien oletetaan, että E on äärellinen joukko.

B.1. Syklit

Olkoon σ joukon E permutaatio. Tarkastellaan alkioita x, $\sigma(x)$, $\sigma^2(x)$, ..., jotka saadaan soveltamalla toistuvasti kuvausta σ johonkin E:n alkioon x. Niiden lukumäärä on pienin luku $n > 0$, joka täyttää ehdon $\sigma^n(x) = x$, ja niiden joukko on sama kuin x:n rata σ:n virittämän aliryhmän $\bar{\sigma}$ toiminnassa:

$$\bar{\sigma}x = \{\sigma^k(x) \mid 0 \leq k < n\}.$$

Luku n on alkion x kiinnittäjän $\bar{\sigma}_x$ indeksi syklisessä ryhmässä $\bar{\sigma}$ ja σ:n kertaluvun m tekijä (kor. 1.4.8). Rata sisältää yksin alkion x, jos ja vain jos $\bar{\sigma}$ kiinnittää x:n eli yhtäpitävästi $\sigma(x) = x$.

MÄÄRITELMÄ B.1.1. Äärellisen joukon E permutaatio ζ on *sykli*, jos E:ssä on sen virittämän aliryhmän $\bar{\zeta}$ toiminnassa yksi ja vain yksi rata, joka ei ole yksiö. Tämä rata on syklin ζ *kantaja*.

Olkoon ζ joukon E sykli. Sen kantaja S on niiden alkioiden $x \in E$ joukko, joilla $\zeta(x) \neq x$. Jos x on jokin S:n alkio, niin sen muut alkiot ovat $\zeta^k(x)$ $(1 \leq k < n)$, missä $n = \mathrm{Card}(S)$, ja $\zeta^n(x) = x$. Tällöin

$$\zeta^n(\zeta^k(x)) = \zeta^k(\zeta^n(x)) = \zeta^k(x),$$

kun $1 \leq k < n$, joten ζ^n on identtinen kuvaus. Siis ζ:n kertaluku ryhmässä $\mathfrak{S}_E$ on n, ja sanotaan, että ζ on *n-sykli*.

Jono $(x, \zeta(x), \zeta^2(x), \ldots, \zeta^{n-1}(x))$ määrää syklin ζ yksikäsitteisesti, ja usein käytetään merkintää

$$\zeta = (x_1\, x_2 \ldots x_n),$$

missä $x_k = \zeta^{k-1}(x)$ $(1 \leq k \leq n)$. Merkintä ei ole yksikäsitteinen vaan riippuu alkion $x = x_1$ valinnasta. Sama sykli voidaan myös merkitä

$$\zeta = (x_2\, x_3 \ldots x_n\, x_1) = (x_3\, x_4 \ldots x_n\, x_1\, x_2) = \ldots.$$

Esimerkki 1) Olkoon σ joukon E permutaatio ja x jokin E:n alkio. Jos $\sigma(x) \neq x$, niin x:n rata S ryhmän $\bar{\sigma}$ toiminnassa sisältää $n > 1$ alkiota $x_k = \sigma^{k-1}(x)$ $(1 \leq k < n)$. Tällöin $\zeta = (x_1\, x_2 \ldots x_n)$ on sykli, jonka kantaja on S ja joka toteuttaa ehdot $\zeta(y) = \sigma(y)$, kun $y \in S$, ja $\zeta(y) = y$, kun $y \in E \setminus S$.

Permutaation esitys sykleillä. Olkoon σ jokin E:n permutaatio. Tarkastellaan sen virittämän permutaatioryhmän $\bar{\sigma}$ toimintaa E:ssä. Olkoon $\mathcal{S}$ niiden ratojen joukko, jotka eivät supistu yksiöiksi. Jokaista rataa $S \in \mathcal{S}$ kohti olkoon ζ_S se E:n sykli, jonka määrittelevät ehdot $\zeta_S(x) = \sigma(x)$, kun $x \in S$, ja $\zeta_S(x) = x$, kun $x \in E \setminus S$ (ks. esim. B.1.1). Tällöin syklien ζ_S kantajat $S \in \mathcal{S}$ ovat erilliset, koska radat muodostavat E:n osituksen.

LEMMA B.1.2. *Jos kahden syklin ζ ja ζ' kantajat ovat erilliset, niin ne kommutoivat keskenään: $\zeta\zeta' = \zeta'\zeta$.*

Todistus. Olkoot syklien ζ ja ζ' kantajat S ja S' erilliset. Jos $x \in S$, niin $\zeta'(x) = x$ ja $\zeta(x) \in S$, joten $\zeta\zeta'(x) = \zeta(x) = \zeta'\zeta(x)$. Samoin, jos $x \in S'$, niin $\zeta'\zeta(x) = \zeta'(x) = \zeta\zeta'(x)$. Lopuksi, jos $x \notin S \cup S'$, niin $\zeta\zeta'(x) = x = \zeta'\zeta(x)$. □

Olkoon nyt $(\zeta_i)_{i \in I}$ mikä tahansa perhe E:n syklejä, joiden kantajat S_i ovat parittain erilliset. Tällöin syklit ζ_i kommutoivat keskenään, joten tulo $\sigma = \prod_{i \in I} \zeta_i$ on hyvin määritelty ryhmässä $\mathfrak{S}_E$. Olkoon $\bar{\sigma}$ sen virittämä aliryhmä.

LEMMA B.1.3. *Tulo $\sigma = \prod_{i \in I} \zeta_i$ toteuttaa ehdon*

$$\sigma(x) = \begin{cases} \zeta_i(x) & , \text{ kun } x \in S_i, i \in I, \\ x & , \text{ kun } x \notin \bigcup_{i \in I} S_i. \end{cases}$$

Lisäksi ne $\bar{\sigma}$-radat, jotka eivät ole yksiöitä, ovat joukot S_i $(i \in I)$.

Todistus. Jos x kuuluu johonkin joukoista S_i, niin $\zeta_j(x) = x$, kun $j \neq i$, ja siten tulon arvo on $\zeta_i(x)$. Jokainen joukko S_i on $\bar{\sigma}$-rata, koska se on ζ_i-rata ja σ yhtyy siinä sykliin ζ_i. Muut radat ovat yksiöitä, koska $\sigma(x) = x$, kun $x \notin \bigcup_{i\in I} S_i$. □

LAUSE B.1.4. *Olkoon E äärellinen joukko ja σ sen permutaatio. On olemassa yksikäsitteinen äärellinen E:n syklijoukko C, joka toteuttaa seuraavat ehdot:*

i) *joukon C syklien kantajat ovat parittain erilliset;*
ii) $\sigma = \prod_{\zeta\in C} \zeta$.

Todistus. Olkoon $\bar{\sigma}$ permutaation σ virittämä aliryhmä ja olkoon $\mathcal{S}$ niiden $\bar{\sigma}$-ratojen joukko, jotka eivät ole yksiöitä. Jokaista rataa $S \in \mathcal{S}$ kohti olkoon $\zeta_S(x) = \sigma(x)$, kun $x \in S$, ja $\zeta_S(x) = x$, kun $x \notin S$. Tällöin ζ_S on sykli, jonka kantaja on S, ja $\sigma = \prod_{S\in\mathcal{S}} \zeta_S$, koska radat S ovat parittain erilliset (lemma B.1.3). Syklien ζ_S joukko toteuttaa siten vaaditut ehdot.

Olkoon toisaalta C syklijoukko, joka täyttää ehdot. Silloin syklien $\zeta \in C$ kantajat ovat $\bar{\sigma}$-radat $S \in \mathcal{S}$ ja lisäksi $\zeta(x) = \sigma(x)$, kun x kuuluu ζ:n kantajaan (lemma B.1.3). Siis C on syklien ζ_S joukko. □

Joukon C syklejä sanotaan permutaation σ *komponenteiksi.*

Esimerkki 2) Olkoon σ välin $[1, 6] \subset \mathbf{N}$ permutaatio

$$(1, 2, 3, 4, 5, 6) \mapsto (4, 6, 1, 3, 5, 2).$$

Tällöin $[1, 6]$ jakautuu kolmeen $\bar{\sigma}$-rataan $\{1, 4, 3\}$, $\{2, 6\}$ ja $\{5\}$, joista saadaan σ:n komponenteiksi $(1\,4\,3)$ ja $(2\,6)$.

Vaihdokset. Olkoon τ sykli, jonka kantajassa on kaksi alkiota x ja y. Silloin $\tau(x) = y$ ja $\tau(y) = x$, eli τ vaihtaa alkiot x ja y keskenään.

MÄÄRITELMÄ B.1.5. Sykli, jonka kertaluku on 2 on *vaihdos* eli *transpositio.*

Olkoot x ja y joukon E kaksi eri alkiota. Tällöin on olemassa yksikäsitteinen vaihdos $\tau_{x,y}$, jonka kantaja on $\{x, y\}$.

LAUSE B.1.6. *Olkoon E äärellinen joukko. Sen symmetrinen ryhmä $\mathfrak{S}_E$ on vaihdosten virittämä.*

Todistus. Jokaista permutaatiota σ kohti olkoon S_σ niiden alkioiden $x \in E$ joukko, joilla $\sigma(x) \neq x$. Osoitetaan induktiolla sen mahtavuuden suhteen, että σ on vaihdosten virittämässä aliryhmässä. Jos $S_\sigma = \emptyset$, niin σ on identtinen permutaatio ja siksi jokaisessa aliryhmässä.

Oletetaan sitten, että $\mathrm{Card}(S_\sigma) = n > 0$ ja että jokainen permutaatio σ', jolla $\mathrm{Card}(S_{\sigma'}) < n$, on tulo vaihdoksista. Olkoon $x \in S_\sigma$ ja $y = \sigma(x)$. Tällöin $y \neq x$ ja $y \in S_\sigma$. Tarkastellaan permutaatiota $\sigma' = \tau_{x,y}\sigma$. Jos $z \in E \setminus S_\sigma$, niin $\sigma'(z) = z$. joten $S_{\sigma'} \subset S_\sigma$. Lisäksi

$\sigma'(x) = \tau(y) = x$ ja siksi $S_{\sigma'} \neq S_\sigma$. Induktio-oletuksen nojalla σ' on vaihdosten tulo; siis myös $\sigma = \tau_{x,y}\sigma'$ on vaihdosten tulo. □

Huomautus. Kun permutaatio esitettään tulona vaihdoksista, näiden kantajat eivät välttämättä ole erillisiä. Tulo voi siten riippua järjestyksestä. Esitys ei myöskään ole yleensä yksikäsitteinen.

Esimerkki 3) Olkoot x_1, x_2, …, x_n joukon E eri alkioita, ja olkoon τ_i vaihdos $\tau_{x_i,x_{i+1}}$ $(1 \leq i < n)$. Tällöin tulo $\tau_1\tau_2 \cdots \tau_{n-1}$ on sykli

$$\zeta = (x_1\, x_2 \ldots x_n).$$

Vastakkaisessa järjestyksessä saadaan taas käänteinen sykli

$$\tau_{n-1}\tau_{n-2} \cdots \tau_1 = (x_n\, x_{n-1} \ldots x_1) = \zeta^{-1}.$$

Harjoitustehtäviä

1) Olkoon σ joukon E permutaatio, ζ sykli ja S sen kantaja. Osoitettava, että $\sigma\zeta\sigma^{-1}$ on sykli, jonka kantaja on $\sigma(S)$.

2) Olkoon $n \geq 2$. Osoitettava, että kaikki ryhmän $\mathfrak{S}_E$ n-syklit ovat toistensa konjugaatteja.

3) Osoitettava, että vaihdokset $\tau_{i,i+1}$ $(1 \leq i < n)$ virittävät $\mathfrak{S}_n$:n. ($\tau_{i,j+1} = \tau_{j,j+1}\tau_{i,j}\tau_{j,j+1}$, kun $1 \leq i < j < n$.)

4) Osoitettava, että $\tau = (1\,2)$ ja $\zeta = (1\,2 \ldots n)$ virittävät $\mathfrak{S}_n$:n. (Tarkastellaan τ:n konjugaatteja $\zeta^k\tau\zeta^{-k}$.)

5) Osoitettava, että permutaation $\sigma \in \mathfrak{S}_E$ kertaluku on sen komponenttien kertalukujen pienin yhteinen kerrannainen.

B.2. Permutaation merkki

Permutaatioiden esitykset komponenttisyklien avulla (lause B.1.4) antavat hyvän kuvan niiden rakenteesta, mutta niistä on vain vähän hyötyä, kun yhdistetään permutaatioita. Jopa kahden syklin tulo voi olla mutkikas, jos syklien kantajat eivät ole erilliset.

Toinen tapa käsitellä permutaatioita on esittää ne vaihdosten tuloina (lause B.1.6). Tällaiset esitykset eivät ole yksikäsitteisiä eivätkä edes vaihdosten lukumäärät ole niissä samat, ellei vaihdoksia jotenkin rajoiteta. Näin voidaan tehdä ryhmässä $\mathfrak{S}_n$ (ks. teht. B.1.3) ja yleisemmin täysin järjestetyn joukon symmetrisessä ryhmässä.

Jos $\sigma \in \mathfrak{S}_n$, niin välin $[1, n]$ lukuparia (i, j) sanotaan σ:n *inversioksi*, kun $i < j$ ja $\sigma(i) > \sigma(j)$. Inversioiden lukumäärää $\nu(\sigma)$ voidaan pitää yhtenä permutaation σ mutkikkuuden mittana. Se on 0 vain, kun σ on identtinen permutaatio, ja 1 jos ja vain jos σ on jokin vaihdoksista $\tau_{i,i+1}$ $(1 \leq i < n)$. Ei ole vaikea nähdä, että jokainen permutaatio σ voidaan esittää tällaisten vaihdosten tulona, jossa on $\nu(\sigma)$ tekijää.

Huomautus. Funktio ν toteuttaa (kolmio)epäyhtälön

$$\nu(\sigma\sigma') \leq \nu(\sigma) + \nu(\sigma').$$

Tästä seuraa, että $d(\sigma, \sigma') = \nu(\sigma^{-1}\sigma')$ on metriikka $\mathfrak{S}_n$:ssä. Erityisesti $\nu(\sigma)$ on σ:n etäisyys identtisestä permutaatiosta.

LEMMA B.2.1. *Jos* σ, $\sigma' \in \mathfrak{S}_n$, *niin* $\nu(\sigma\sigma') \equiv \nu(\sigma) + \nu(\sigma') \pmod 2$.

Todistus. Määritelmän nojalla negatiivisten erotusten $\sigma(j) - \sigma(i)$ $(1 \leq i < j \leq n)$ lukumäärä on $\nu(\sigma)$, joten tulon

$$p_\sigma = \prod_{i<j} (\sigma(j) - \sigma(i)) \in \mathbf{Z}$$

etumerkki on $(-1)^{\nu(\sigma)}$. Lisäksi sen itseisarvo on $p_1 = \prod_{i<j}(j-i)$, koska jokainen tekijä $j-i$ esiintyy siinä kerran joko sellaisenaan tai muodossa $i-j$, ja siten

$$(-1)^{\nu(\sigma)} = \frac{p_\sigma}{p_1} = \prod_{i<j} \frac{\sigma(j) - \sigma(i)}{j-i}.$$

Koska oikean puolen osamäärät säilyvät,vaikka i ja j vaihtaisivat paikkaa, tulo voidaan myös kirjoittaa muotoon

$$\prod_{i<j} \frac{\sigma(\sigma'(j)) - \sigma(\sigma'(i))}{\sigma'(j) - \sigma'(i)} = \frac{p_{\sigma\sigma'}}{p_{\sigma'}}.$$

Näin saadaan

$$p_{\sigma\sigma'} = (-1)^{\nu(\sigma)} p_{\sigma'} = (-1)^{\nu(\sigma)}(-1)^{\nu(\sigma')} p_1,$$

ja väite seuraa yhtälöstä $p_{\sigma\sigma'} = (-1)^{\nu(\sigma\sigma')} p_1$. □

LAUSE B.2.2. *Olkoon* E *äärellinen joukko. On olemassa yksi ja vain yksi homomorfismi* $\varepsilon\colon \mathfrak{S}_E \to \{-1, +1\}$ *, jolla pätee* $\varepsilon(\tau) = -1$ *aina kun* τ *on vaihdos.*

Todistus. Koska vaihdokset virittävät ryhmän $\mathfrak{S}_E$ (lause B.1.6), homomorfismi ε on yksikäsitteinen, kun sen arvot vaihdoksilla ovat annetut. Olemassaolon todistamiseksi on riittävää tarkastella ryhmää $\mathfrak{S}_n$, koska $\mathfrak{S}_E$ on isomorfinen sen kanssa, kun $n = \mathrm{Card}(E)$.

Olkoon $\varepsilon(\sigma) = (-1)^{\nu(\sigma)}$, kun $\sigma \in \mathfrak{S}_n$. Lemman B.2.1 nojalla ε on homomorfismi. Jokainen vaihdos τ on sykli $(i\,j)$, missä $1 \leq i < j \leq n$, ja sen inversiot ovat (i,k) ja (k,j) $(i < k < j)$ sekä (i,j). Koska niiden lukumäärä on pariton, ehto $\varepsilon(\tau) = -1$ on voimassa. □

MÄÄRITELMÄ B.2.3. Lauseen B.2.2 merkinnöin $\varepsilon(\sigma)$ on permutaation σ *merkki*. Homomorfismin ε ydin on joukon E *alternoiva ryhmä*.

Jos $\varepsilon(\sigma) = +1$, niin jokaisessa σ:n esityksessä vaihdosten tulona on parillinen määrä tekijöitä; tällöin sanotaan, että permutaatio σ on *parillinen*. Vastaavasti σ on *pariton*, jos $\varepsilon(\sigma) = -1$. Alternoiva ryhmä koostuu parillisista permutaatioista. Se on $\mathfrak{S}_E$:n normaali aliryhmä, ja

sille käytetään merkintää $\mathfrak{A}_E$ (tai $\mathfrak{A}_n$, kun $E = [1, n]$). Sen kertaluku on $n!/2$, kun $n \geq 2$.

1) Jokainen n-sykli ζ on $n-1$:n vaihdoksen tulo (esim. B.1.3), ja siten

$$\varepsilon(\zeta) = (-1)^{n-1}.$$

Erityisesti ζ on parillinen, jos ja vain jos n on pariton.

2) Ryhmän $\mathfrak{A}_3$ kertaluku on 3. Se sisältää identtisen permutaation lisäksi 3-syklit $(1\,2\,3)$ ja $(1\,3\,2)$. Se on syklinen ja siten vaihdannainen.

3) Ryhmän $\mathfrak{A}_4$ kertaluku on 12. Se sisältää 8 3-sykliä sekä tulot $(1\,2)(3\,4)$, $(1\,3)(2\,4)$, $(1\,4)(2\,3)$, jotka yhdessä identtisen permutaation kanssa muodostavat vaihdannaisen normaalin aliryhmän.

Harjoitustehtäviä

1) Osoitettava, että $(1\,2)(3\,4)$, $(1\,2\,3)$, $(1\,2\,3\,4\,5)$, $(1\,2\,3\,5\,4)$ ja identtinen permutaatio muodostavat ryhmän $\mathfrak{A}_5$ alkioiden konjugaattiluokkien edustajiston ja että vastaavissa luokissa on alkioita 15, 20, 12, 12 ja 1. Pääteltävä, että ryhmä $\mathfrak{A}_5$ on yksinkertainen. (Normaali aliryhmä on yhdiste konjugaattiluokista.)

Kirjallisuutta

[1] Thomas W. Hungerford, *Algebra*, Graduate Texts in Mathematics 73, Springer-Verlag, 1974.

[2] Serge Lang, *Algebra*, third ed., Addison-Wesley, 1993.

[3] Serge Lang, *Algebra*, revised third ed., Graduate Texts in Mathematics 211, Springer-Verlag, 2002.

[4] Joseph J. Rotman, *Advanced Modern Algebra*, Prentice Hall, 2002.

Merkinnät

X/R : s. 3
$x \equiv x' \pmod{R}$: s. 3
$\mathbf{M}_n(\mathbf{R})$: s. 5
$x \top y$: s. 6
$\overset{n}{\underset{i=1}{\top}} x_i$, $\underset{1\le i\le n}{\top} x_i$, $\underset{i\in I}{\top} x_i$: s. 7
$\overset{n}{\top} x$: s. 7
$\prod_{i\in I} x_i$: s. 9
$\sum_{i\in I} x_i$: s. 9
$\underset{i\in\emptyset}{\top} x_i$: s. 12
$\overset{0}{\top} x$: s. 12
A^* : s. 14
$\mathfrak{S}_X$: s. 14
E_S : s. 16
a/p, $a-p$: s. 16
X^{-1} : s. 21
G/H : s. 22
$x \equiv y \pmod{H}$: s. 22
$\mathrm{Ker}(f)$: s. 23
$\mathrm{Im}(f)$: s. 23
AB : s. 24
$A+B$, $A \top B$: s. 24
$\mathfrak{S}_n$, $\mathfrak{A}_n$: s. 25
$\prod_{i\in I} E_i$: s. 27
$\prod_{i\in I} G_i$: s. 27
$\bigoplus_{i\in I} G_i$: s. 27
M^o : s. 30
M_A : s. 31
M_a, G_a : s. 31
E^M : s. 31
E/G, $E\backslash G$: s. 32
$(G:H)$: s. 35
G_p : s. 41
$\mathbf{Z}^{(X)}$: s. 45
δ_x : s. 45
$\mathbf{N}^{(X)}$: s. 46
$\mathrm{End}(G)$: s. 48
$\prod_{i\in I} A_i$: s. 48
$x \equiv y \ (\mathfrak{a})$: s. 50
$A/\mathfrak{a}$: s. 50
$A[S^{-1}]$: s. 52
$\mathrm{char}(K)$: s. 54
A^o : s. 57
$\mathbf{M}_n(\mathbf{R})$: s. 58
$\mathrm{Hom}_A(E,F)$: s. 59
E/M : s. 60
$\prod_{i\in I} E_i$: s. 61
E^I : s. 61
$\bigoplus_{i\in I} E_i$: s. 62
$E^{(I)}$: s. 63
$A^{(I)}$: s. 64
δ_{ij} : s. 64
$\mathrm{End}_A(E)$: s. 67
E^* : s. 67
$\mathbf{M}_{m,n}(A)$: s. 69
$\mathcal{L}_2(E,F;G)$: s. 69
$E \otimes_A F$: s. 71
$x \otimes y$: s. 72
$\overset{n}{\underset{i=1}{\bigotimes}} E_i$, $\underset{1\le i\le n}{\bigotimes} E_i$: s. 79
$E^{\otimes n}$: s. 79
$\mathbf{M}_n(A)$: s. 80
$\mathrm{Hom}_{A-\mathrm{alg}}(E,E')$: s. 81
$E/\mathfrak{a}$: s. 81

$Z(E)$: s. 82
$\mathbf{H}$: s. 83
$A^{(S)}$, e_s : s. 85
e^s : s. 85
$P_A(I)$: s. 88
X^ν : s. 88
X_i : s. 89
$|\nu|$: s. 89
$\deg(u)$: s. 89
$u((x_i)_{i\in I})$: s. 90
$A[(x_i)_{i\in I}]$: s. 90
$A[(X_i)_{i\in I}]$: s. 91
$A[X_1, X_2, \ldots, X_n]$: s. 91
$u \circ v$: s. 92
$A[\varepsilon]$: s. 93
D_i, $\frac{\partial}{\partial X_i}$: s. 95
$x \mid y$: s. 97
$\operatorname{div}(x)$: s. 98
(E, u) : s. 115
$\dim_K(A)$: s. 116
$[A : K]$: s. 116
$K((x_i)_{i\in I})$: s. 118
$K(A)$, $K[A]$: s. 118
$K(x_1, x_2, \ldots, x_n)$: s. 118
$[E : K]_s$: s. 146
$\operatorname{Gal}(N/K)$: s. 151
$\mu_n(K)$: s. 160
$\mu_\infty(K)$: s. 160
$\mathbf{F}_q$: s. 165

Hakemisto

Abel, 172
  ∼in laajennus, 158
  ∼in yhtälö, 172
additiivinen
  merkintä, 7
adjunktio, 118
alaraja, 177
  suurin, 177
algebra, 80
  magman, monoidin, ryhmän, 85
  äärellinen, 116
algebrallinen, 120
  laajennus, 122
  relaatio, 119
  sulkeuma, 135
    laajennuksessa, 124
algebrallisesti suljettu
  alikunta, 124
  kunta, 130
algebralliset luvut, 124
algebran peruslause, 130
alialgebra, 81
aliavaruus, 59
alikunta, 54
alilaajennus, 115
  alkioperheen virittämä, 118
alimagma, 8
alimoduli, 59
alimonoidi, 12
alirengas, 49
aliryhmä, 20
  normaali, 22
  Sylowin, 40
alkio
  maksimaalinen, 177
  minimaalinen, 177
  pienin, 177
  suurin, 177
alkualkio, 100
alkukunta, 54
alkuosa, 181
alternoiva
  ryhmä, 25
Artin
  ∼in lause, 153
arvo
  polynomin, 90
assosiatiivinen, 6
aste
  algebrallisen alkion, 120
  algebran, 116
  laajennuksen, 116
  modulin, 66
  monomin, 89
  polynomin, 89
  separoituva, 146
  vapaan ryhmän, 47
automorfismi
  sisäinen, 35

Bezout
  ∼'n kaava, 73
biadditiivinen, 69
bilineaarinen, 68

Cardano, 172
  ∼n kaavat, 173
Cayley
  ∼n lause, 35

Dedekind
  ∼in lause, 145
derivaattakuvaus, 93
differentti, 172
dimensio
  vektoriavaruuden, 66
diskriminantti, 172
divisori, 98
duaali, 67
dyaditulo, 75

Eisenstein
  ∼in kriteerio, 112

eksponenttimerkintä, 47
ekvivalenssi
  kuvaukseen liittyvä, 4
endomorfismi, 6
endomorfismirengas, 48
erotusmonoidi, 16
esitys
  ryhmän, 86
Eukleides
  ∼en lemma, 107
  ∼en rengas, 105
Euler, 127

faktoriaalinen, 104
Fermat
  ∼n alkuluku, 127
Ferrari, 172

Galois, 172
  ∼n kunta, 164
  ∼n laajennus, 151
  ∼n lause, 170
  ∼n ryhmä, 151
  ∼n vastaavuus, 155
  polynomin ∼n ryhmä, 152
Gauss, 127, 130
  ∼in kokonaisluvut, 105
  ∼in lemma, 109
geometrinen konstruktio, 125

hajotelma
  homomorfismin, 10
  homomorfismin kanoninen, 23
  kanoninen, 4
hajotuslause
  kuvausten, 2
  modulihomomorfismien, 60
  rengashomomorfismien, 51
  ryhmähomomorfismien, 23
homogeeninen
  joukko, 32
homomorfialause
  modulien, 60
  renkaiden, 51
homomorfismi
  M-joukkojen, 30
  algebrojen, 81
  järjestettyjen ryhmien, 101
  kanoninen
    alimodulien summan, 63
  magmojen, 6
  modulien, 58
  projektio∼, 27
  renkaiden, 48
  ryhmä∼, 20
  ykkösellinen, 11

ideaali, 49
  algebran, 81
  kaksipuolinen, 49
  maksimaalinen, 49
  oikeanpuolinen, 49
  vasemmanpuolinen, 49
idempotentti, 54
indeksi
  aliryhmän, 34, 35
indusoitu
  järjestys, 176
  laskutoimitus, 8
  toiminta, 30
isomorfialause
  ryhmäteorian 1., 24
  ryhmäteorian 2., 26
isomorfismi, 6

jakokunta, 52
jakomonoidi, 16
jakorengas, 52
  täysi, 52
jaollinen, 97
jaoton, 99
Jordanin-Hölderin
  jono, 37
  lause, 38
joukko
  M-∼, 29
juurikunta, 131
juurros, 168
juurroslaajennus, 168
  iteroitu, 168
järjestetty
  hyvin ∼ joukko, 184
  joukko, 175
  osajoukko, 176
  ryhmä, 98
järjestys, 175
  hyvä, 184
  indusoitu, 176
  käänteinen, 176
  täysi, 176

kanoninen
  hajotelma, 4
    rengashomomorfismin, 51
  homomorfismi
    jakomonoidin, 17

tekijämagman, 10
homomorfismin ∼ hajotelma, 23
injektio, 3
suoraan summaan, 62
injektiohomomorfismi, 27
kuvaus
tensorituloon, 72
surjektio, 3
kanta, 65
algebran, 83
duaalinen, 67
kantaja
monoidin alkioperheen, 12
karakteristika
kunnan, 54
kerrannainen, 7, 97
kertolasku
algebran, 80
kertotaulu, 83
keskeinen
renkaan alkio, 54
keskittäjä, 35
keskus
renkaan, 82
ryhmän, 35
ketju, 176
kiinnittäjä, 31
kiintokunta, 153
kommutaattori, 43
kommutatiivinen, 9
kommutoiva, 9
komponentti
homomorfismin, 61
kompositiojono, 36
tekijät, 36
kongruenssi, 10
modulo $\mathfrak{a}$, 50
konjugaatti, 138
ryhmässä, 32
konjugaattiluokka, 32
konjugointi
ryhmän alkiolla, 32
ryhmässä, 35
Kroneckerin funktio, 45
Krull
∼in lause, 50
kunta, 54
kuva
ryhmähomomorfismin, 23
kuvausmoduli, 61
käänteisalkio, 13
oikeanpuolinen, 13
vasemmanpuolinen, 13
kääntyvä, 13
oikealta, 13
vasemmalta, 13

laajennus, 115
Abelin, 158
adjungoimalla saatu, 118
algbrallinen, 122
Galois'n, 151
normaali, 141
separoituva, 148
syklinen, 165
transkendenttinen, 122
äärellistyyppinen, 118
Lagrange
∼n resolventti, 167
laskutoimitus, 5
indusoitu, 8
liitännäinen, 6
vaihdannainen, 9
vastakkainen, 6
yhteensopiva, 10
lause
Cayleyn, 35
Krullin, 50
Sylowin, 41
Leibniz
∼in sääntö, 93
liittoalkio, 98
liitännäinen, 6
liitäntälaki, 6
yleistetty, 7
lineaarikuvaus, 58
perheen määräämä, 65
lineaarinen
relaatio, 65
lineaarinen yhdistelmä, 58
luokkayhtälö, 35

magma, 6
liitännäinen, 6
tekijä∼, 10
tulo∼, 27
vaihdannainen, 9
ykkösellinen, 11
maksimaalinen alkio, 177
minimaalinen alkio, 177
minimaalipolynomi, 120
moduli, 57
vapaa, 65
monoidi, 11
erotus∼, 16

jako∼, 16
osamäärä∼, 16
tulo∼, 27
vapaa vaihdannainen, 46
monoidihomomorfismi, 11
monomi, 89
multiplikatiivinen
merkintä, 7
renkaan ∼ monoidi, 12
muodollinen
A-kertoiminen yhdistelmä, 71
$\mathbf{Z}$-kertoiminen yhdistelmä, 46
murtolauseke, 110

neutraalialkio, 11
Newton
∼in kaavat, 172
nilpotentti
ryhmä, 43
nolla-alkio, 11
nollarengas, 48
normaali, 141
aliryhmä, 22
normaalisuuskriteeri, 22

osamäärämonoidi, 16
ositteleva
kertolasku, 48

p-ryhmä, 40
perfekti
kunta, 149
permutaatioryhmä
täysi, 14
polynomi, 89
yleinen asteen n, 152
polynomialgebra, 91
polynomirelaatio, 91
potenssi, 7
eksponentilla 0, 12
negatiivinen, 14
potenssilait, 7
primitiivinen
juuri, 164
polynomi, 109
ykkösenjuuri, 161
projektiohomomorfismi, 27

rakennevakiot, 83
rata, 32
ratkeava
algebrallisesti ∼ yhtälö, 169
ryhmä, 38
relaatio
algebrallinen, 119
lineaarinen, 65
rengas, 48
Eukleideen, 105
resolventti
Lagrangen, 167
retraktio, 13
ryhmä, 13
alternoiva, 25
Galois'n, 151
järjestetty, 98
nilpotentti, 43
polynomin Galois'n, 152
ratkeava, 38
renkaan kääntyvien alkioiden, 14
symmetrinen, 14
vapaa vaihdannainen, 46
yksinkertainen, 36

sektio, 13
separoituva
alkio, 147
aste, 146
laajennus, 148
polynomi, 144
sidottu
perhe, 65
sijoitushomomorfismi, 90
sisäinen
automorfismi, 35
skalaarikertolasku, 57
sopeutuva
ekvivalenssiin ∼ kuvaus, 3
struktuurihomomorfismi
algebran, 83
summa
alimodulien, 64
suora, 27
suora summa
alimodulien, 64
modulien, 62
supistussääntö
kuvausten, 2
supistuva, 16
syklinen
laajennus, 165
Sylow
∼in aliryhmä, 40
∼in lause, 41
symmetrinen
ryhmä, 14

tekijä, 97

epäaito, 99
kompositiojonon, 36
suora, 36
tekijäalgebra, 81
tekijäavaruus, 60
tekijämagma, 10
tekijämoduli, 60
tekijämonoidi, 12
tekijärengas, 51
tekijäryhmä, 22
tensoripotenssi, 79
tensoritulo, 71
alkioiden, 72
toiminta, 29
indusoitu, 30
kanoninen, 30
oikealta, 30
transitiivinen, 32
vasemmalta, 29
vastamonoidin, 30
torsioalkio, 67
torsioton, 67
transitiivinen
toiminta, 32
transkendenttiluku, 125
transkendenttinen
alkio, 119
laajennus, 122
puhtaasti $\sim$ laajennus, 128
tulo
karteesinen, 27
laskutoimitusten, 27
rajoitettu, 27
renkaiden, 48
ryhmien, 27
tulomagma, 27
tulomoduli, 61
tulomonoidi, 27

universaaliominaisuus
jakomonoidin, 17
jakorenkaan, 53
magma-algebran, 86
modulin $A^{(I)}$, 65
polynomialgebran, 89
suoran summan, 63
tensoritulon, 72
tulon, 61
vapaan modulin, 66
vapaan vaihdannaisen monoidin, 46
upotuslause, 130

vaihdannainen, 9
rengas, 48
vakaa
laskutoimituksen suhteen, 8
toiminnan suhteen, 30
vakauttaja, 31
vakiopolynomi, 89
valinta-aksiooma, 178
valintakuvaus, 178
vapaa
moduli, 65
perhe, 65
vaihdannainen ryhmä, 46
virittäjäjoukko, 45
vasta-alkio, 14
vastamagma, 6
vektori, 57
vektoriavaruus, 57
vinokunta, 54
virittäjäjoukko, 8
alikunnan, 55
alirenkaan, 49
aliryhmän, 21
Galois'n laajennuksen, 151
ideaalin, 49
laajennuksen, 118
modulin, 60
normaalin laajennuksen, 142
vapaa, 45
virittäjäperhe, 60
alialgebran, 90
alilaajennuksen, 118

ydin
ryhmähomomorfismin, 23
yhdistelmä
lineaarinen, 49, 58
muodollisesti ääretön, 13
äärellisen alkiojonon, 7
äärellisen alkioperheen, 9
yhteensopiva
laskutoimitus, 10
ykkösalkio, 11
ykkösellinen
homomorfismi, 11
magma, 11
ykkösenjuuri, 159
$\sim$kunta, 162
primitiivinen, 161
yksikkö, 98
yksinkertainen
ryhmä, 36
yleinen
asteen n polynomi, 152

ylikunta, 54
yläraja, 177
  pienin, 177

äärellinen
  algebra, 116
äärellistyyppinen, 60
  laajennus, 118