Algebra - matematiikan osa-alue, joka tutkii *algebrallisia struktuureja* eli **laskutoimituksilla** *varustettuja* joukkoja.

Tällä kurssilla tutkitaan **lineaarialgebraa**. Lineaarialgebra on algebran osa-alue, joka tutkii *moduleita* ja erityisesti *vektoriavaruuksia* (jotka ovat modulien erikoistapaus).

Lineaarialgebrassa käytetään *työkaluna* myös yleisimpiä algebrallisia olentoja (ryhmiä, renkaita, kuntia), jotka sinänsä eivät ole moduleita, mutta silti niiden ymmärtäminen algebran näkökulmasta on hyödyllinen lineaarialgebran ymmärtämisen kannalta. Esimerkiksi kääntyvät $(n \times n)$-matriisit muodostavat luonnollisella tavalla *ryhmän*, $(n \times n)$-kokoiset neliömatriisit yleisemmin muodostavat *renkaan*. Luvussa 3 tutkimme lineaarisia operaattoreita polynomien muodostaman renkaan avulla jne. Lisäksi koko vektoriavaruuden käsitteen määritelmässä esiintyvät *kunnat*.

Laskutoimituksista

Yleisesti ottaen *laskutoimitus* on (mikä tahansa) tapa liittää olioihin x, y tämän laskutoimituksen tuloksen z.

Havainnollisesti - x ja y *lasketaan yhteen* (*kerrotaan* jne.) jolloin saadaan z.

Esimerkkejä laskutoimituksista:

- Reaalilukujen laskutoimitukset - yhteenlasku, kertolasku, vähennyslasku, jakolasku.
- Kuvausten yhdistäminen $(f, g) \mapsto g \circ f$.
- Matriisien kertolasku.
- Skalaarikertolasku vektoriavaruudessa - vektori kerrotaan reaaliluvulla.
- Sisätulo $\mathbb{R}^n$:ssä.
- Ristitulo $\mathbb{R}^3$:ssä.

Emme anna mitään mahdollisimman yleistä formaalia määritelmä laskutoimitukselle, olemme kiinnostuneita vain kahdesta erikoistapauksesta:

- Joukossa X määritelty laskutoimitus. Tästä puhutaan tässä osiossa.
- Skalaarikertolaskun tyyppinen laskutoimitus. Tästä puhutaan vektoriavaruuksien yhteydessä.

Laskutoimitus joukossa X:

Algebrallinen operaatio tai **laskutoimitus** joukossa X on (mikä tahansa) kuvaus $f\colon X \times X \to X$.

Tärkeitä algebrallisten operaatioiden ominaisuuksia ovat - *liitännäisyys, vaihdannaisuus, neutraalialkion olemassaolo, käänteisalkioiden olemassaolo.* Kahden laskutoimituksen tapauksessa esille nousevat myös *osittelulait.*

Liitännäisyys.
Laskutoimitusta $\cdot$ joukossa X sanotaan *liitännäiseksi* jos kaikilla $a, b, c \in X$ pätee

$$(ab)c = a(bc)$$

Additiivisella merkinnällä $(x + y) + z = x + (y + z)$.

Kommutatiivisuus/Vaihdannaisuus.
Joukon X laskutoimitus $\cdot$ on *kommutatiivinen* eli *vaihdannainen* jos kaikilla $a, b \in X$ pätee

$$ab = ba.$$

Additiivisella merkintätavalla $a + b = b + a$.

Neutraalialkio.
Olkoon $\cdot$ joukon X laskutoimitus. Alkiota $e \in X$ sanotaan tämän laskutoimituksen *neutraalialkioksi* jos kaikilla $x \in X$ pätee

$$ex = x = xe.$$

Neutraalialkion on yksikäsitteinen (jos olemassa).
Kun laskutoimitusta $\cdot$ merkitään *multiplikatiivisesti*, neutraalialkiolle usein käytetään merkintää 1. Tällöin tätä alkiota sanotaan myös laskutoimituksen *ykkösalkioksi.*
Kun laskutoimitusta merkitään additiivisesti symbolilla $+$, neutraalialkiota merkitään tavallisesti symbolilla 0 ja sitä sanotaan *nollaksi* tai nolla-alkioksi.

Käänteisalkio/Vasta-alkio.
Olkoon $\cdot$ laskutoimitus joukossa X, *jolla on neutraalialkio* e. Alkiota $y \in X$ sanotaan alkion $x \in X$ *käänteisalkioksi* jos pätee

$$xy = e = yx.$$

Jos laskutoimitus on liitännäinen käänteisalkio on yksikäsitteinen (jos olemassa).

Kun laskutoimitus $\cdot$ on liitännäinen, alkion x känteisalkiota merkitään, jos se on olemassa, symbolilla x^{-1}. Sanomme tällöin, että x on *kääntyvä* laskutoimituksen $\cdot$ suhteen.

Jos laskutoimituksen symbolina käytetään $+$ merkkiä, käänteisalkion sijaan puhutaan x:n *vasta-alkiosta.* Vasta-alkio merkitään symbolilla $-x$. Tällöin

$$x + (-x) = (-x) + x = 0.$$

Käänteisalkioiden olemassaolo liittyy *lineaaristen yhtälöiden* ratkaisemiseen (Lemma 1.8).

Potenssit

Määritellään induktiivisesti jos laskutoimitus $\cdot$ joukossa X on liitännäinen, tässä $n = 1, 2, 3, \ldots$ pos. kokonaisluku,

$$x^1 = x,$$

$$x^{n+1} = x^n \cdot x = \underbrace{x \cdot x \cdot \ldots \cdot x}_{n \text{ kertaa}}.$$

Jos laskutoimituksella $\cdot$ on neutraalialkio e, voidaan määritellä nollaspotenssi $x^0 = e$. Jos lisäksi alkiolla x on käänteisalkio x^{-1}, voidaan määritellä negatiiviset potenssit kaavalla

$$x^{-n} = (x^{-1})^n.$$

Potenssilait (voimassa aina kun kaikki kaavoissa esiintyvät potenssit ovat määriteltyjä):

$$x^n \cdot x^m = x^{n+m},$$

$$(x^n)^m = x^{nm}.$$

Additiivisessa tapauksessa puhutaan *monikerrasta*

$$nx = \underbrace{x + x + \ldots + x}_{n \text{ kertaa}}.$$

Puhtaasti algebralliset (ei lineaarialgebralliset) struktuurit, joiden tuntemisesta on meille hyötyä:

- Ryhmät
- Renkaat
- Kunnat

Ryhmät
Olkoon $\cdot$ joukossa G määritelty laskutoimitus. Paria $(G, \cdot)$ sanotaan *ryhmäksi* jos laskutoimitus $\cdot$ on liitännäinen, sillä on neutraalialkio e ja jokaisella joukon G alkiolla $g \in G$ on käänteisalkio g^{-1} laskutoimituksen $\cdot$ suhteen.

Jos ryhmän G laskutoimitus on vaihdannainen, ryhmää sanotaan **Abelin ryhmäksi**. Abelin ryhmän laskutoimitusta on tapana merkitä yleisesti additiivisesti eli symbolilla $+$, paitsi tietysti silloin kun laskutoimitukselle on jostakin syystä sovittu toinen merkintätapa.

Addiivisen merkintätavan tapauksessa Abelin ryhmässä voidaan määritellä *vähennyslaskutoimitus*. Olkoon $(G, +)$ Abelin ryhmä ja olkoot $x, y \in G$. Tällöin asetetaan

$$x - y = x + (-y),$$

missä $-y$ on alkion y vasta-alkio Abelin ryhmässä G.

Ryhmässä $(G, \cdot)$ jokaisella *lineaarisella yhtälöllä* $ax = b$ ($xa = b$) on *yksikäsitteinen ratkaisu* $x = a^{-1}b$ ($x = ba^{-1}$). Tämä on olellisesti (yksi) syy siihen, miksi ryhmät ovat matematiikassa niin tärkeitä.

Renkaat.
Olkoon R joukko, jossa on määritelty kaksi laskutoimitusta,
yhteenlasku $+$ ja kertolasku $\cdot$. Kolmikko $(R, +, \cdot)$ on *rengas*, jos

- $(R, +)$ on Abelin ryhmä.
- Kertolasku $\cdot$ on liitännäinen ja sillä on neutraalialkio $1 = 1_R$.
- Kaikilla $x, y, z \in R$ pätee (vasemmanpuoleinen osittelulaki)

$$x \cdot (y + z) = x \cdot y + x \cdot z.$$

- Kaikilla $x, y, z \in R$ pätee (oikeanpuoleinen osittelulaki)

$$(x + y) \cdot z = x \cdot z + y \cdot z.$$

Abelin ryhmän $(R, +)$ neutraalkiota merkitään $0 = 0_R$ ja sanotaan renkaan nollaalkioksi.
Kertolaskun $\cdot$ neutraalkiota merkitään $1 = 1_R$ ja sanotaan renkaan ykkösalkioksi.

Jos renkaan kertolasku on vaihdannainen, rengasta sanotaan *vaihdannaiseksi*.

Kunnat

Kunta K on epätriviaali vaihdannainen rengas, jossa jokaisella nollasta eroavalla alkiolla $x \in K$, $x \neq 0_K$, on olemassa *käänteisalkio* (kertolaskun suhteen) x^{-1}.

Kunta on tällä kurssilla ehkä *tärkein* algebrallinen struktuuri, koska vektoriavaruuksissa käytetään skalaareina nimenomaan kunnan alkioita.

Kunnassa on luonnollista puhua *jakolaskusta* ja *murtoluvusta*. Nämä määritellään seuraavasti - olkoot $a, b \in K$, missä K on kunta. Oletetaan, että $b \neq 0_K$. Tällöin asetetaan

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

Mielivaltaisen kunnan murtolausekkeille pätevät samat laskusäännöt kuin tavalliselle murtolausekkeille reaailuvuilla. Olkoon $(K, +, \cdot)$ kunta ja olkoot $a, b, c, d \in K$, $b, d \neq 0_K$. Tällöin

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

Kompleksilukujen kunta

Kompleksiluku on muotoa $a + bi$ oleva luku, missä $a, b \in \mathbb{R}$ ja i on *imäginääriyksikkö*, jolle pätee $i^2 = -1$. Kompleksilukuja voidaan laskea yhteen ja kertoa keskenään käyttämällä "tavallisia laskusääntöjä" (eli renkaan aksioomeja).

Formaalisti kompleksiluku on järjestetty pari $(a, b) \in \mathbb{R}^2$. Kompleksilukujen yhteen- ja kertolasku määritellään kaavoilla

$$(a, b) + (c, d) = (a + c, b + d),$$

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

Näillä laskutoimituksilla varustettuna kompleksilukujen joukko $\mathbb{C}$ on tärkeä esimerkki *kunnasta*

Kuvaukset algebrassa

Olkoon $\cdot$ joukon X laskutoimitus ja $\cdot'$ joukon Y laskutoimitus. Olkoon $f\colon X \to Y$ kuvaus. Tällöin f on *yhteensopiva* laskutoimitusten $\cdot$ ja $\cdot'$ kanssa, jos kaikilla $x, x' \in X$ pätee

$$f(x \cdot x') = f(x) \cdot' f(x').$$

Myös sanontaa "*laskutoimitukset säilyttävä kuvaus*" käytetään.

Homomorfismit

Yleisesti ottaen homomorfismi algebrallisesta struktuurista toiseen samantyyppiseen alg. struktuuriin on kuvaus, joka säilyttää kaikki laskutoimitukset sekä struktuurin algebrallisia ominaisuuksia.

Ryhmien tapaus.

Määritelmä 1. *Olkoot $(G, \cdot)$ ja $(G', \cdot')$ molemmat ryhmiä. Sanomme, että kuvaus $f\colon G \to G'$ on* ryhmien välinen homomorfismi*, jos se on yhteensopiva ryhmien G ja G' laskutoimitusten kanssa, eli jos ja vain jos kaikilla $g, h \in G$ pätee*

$$f(gh) = f(g)f(h). \tag{2}$$

Renkaiden tapaus.

Määritelmä 3. *Olkoot $(R, +, \cdot)$ ja $(R', +, \cdot)$ renkaita. Kuvausta $f\colon R \to R'$ sanotaan* rengashomomorfismiksi*, jos f on yhteensopiva sekä yhteenlaskun, että kertolaskun suhteen, eli jos kaikilla $x, y \in R$ pätee*

$$f(x + y) = f(x) + f(y) \text{ ja } f(xy) = f(x)f(y), \tag{4}$$

ja lisäksi f säilyttää kertolaskun neutraalialkiot, eli pätee yhtälö

$$f(1_R) = 1_{R'}. \tag{5}$$

Kuntien tapaus
Olkoot $(K, +, \cdot)$ ja $(K', +, \cdot)$ kuntia. Koska kunta on erikoistapaus renkaasta, määritelemme yksinkertaisesti, että kuvaus $f\colon K \to K'$ on *kuntahomomorfismi*, jos ja vain jos se on rengashomomorfismi renkaiden $(K, +, \cdot)$ ja $(K', +, \cdot)$ välillä.

Isomorfismit
Isomorfismi on **bijektiivinen** homomorfismi $f\colon X \to Y$. Jos kahden algebrallisilla struktuureilla varustetun joukon X ja Y välillä on olemassa jokin isomorfismi $f\colon X \to Y$, sanomme, että X ja Y ovat *isomorfisia*. Tällöin merkitään $X \cong Y$. Jos halutaan korostaa, että kuvaus f on isomorfismi, käytetään sille merkintää $f\colon X \xrightarrow{\cong} Y$.

Alistruktuureista

Olkoon $\cdot$ laskutoimitus joukossa X ja olkoon $Y \subset X$. Sanomme, että Y on *vakaa* (*suljettu*) laskutoimituksen $\cdot$ suhteen jos kaikilla $x, y \in Y$ pätee $xy \in Y$.
On selvää, että jos Y on vakaa, niin X:n laskutoimituksen $\cdot$ *rajoittuma* karteesiseen tuloon $Y \times Y$ määrittelee luonnollisella tavalla kuvauksen $\cdot\colon Y \times Y \to Y$, joka on laskutoimitus joukossa Y. Tällöin voimme puhua algebrallisesta struktuurista $(Y, \cdot)$.

Olkoon X jollakin algebrallisella struktuurilla varustettu joukko ja olkoon $Y \subset X$. Tällöin Y sanotaan struktuurin X *alistruktuuriksi* jos se on vakaa jokaisen X:n laskutoimituksen suhteen ja lisäksi" toteuttaa samat mahdolliset lisäehdot, jotka X toteuttaa". Tällöin merkitään myös $Y \leq X$.

Aliryhmät.
Olkoon $(G, \cdot)$ ryhmä ja $H \subset G$. Tällöin osajoukkoa H sanotaan ryhmän G *aliryhmäksi* jos seuraavat ehdot toteutuvat.

- $xy \in H$ kaikilla $x, y \in H$, eli H on vakaa laskutoimituksen $\cdot$ suhteen.
- $e \in H$, missä e on ryhmän G neutraalialkio.
- H on suljettu käänteisalkioiden suhteen, eli $x^{-1} \in H$ kaikilla $x \in H$. Tässä x^{-1} on alkion x käänteisalkio ryhmässä G.

Kun H on ryhmän $(G, \cdot)$ ryhmä, pari $(H, \cdot)$ muodostaa itse ryhmän. Jos ryhmä G on vaihdannainen eli Abelin ryhmä, myös H on vaihdannainen.

Renkaiden tapaus
Olkoon $(R, +, \cdot)$ rengas ja olkoon $R' \subset R$. Tällöin R' on renkaan R *alirengas* jos seuraavat ehdot toteutuvat

- $(R', +)$ on Abelin ryhmän $(R, +)$ aliryhmä.
- R' on vakaa kertolaskun suhteen.
- $1_R \in R'$. Tässä 1_R on renkaan R neutraalialkio kertolaskun suhteen.

Jos R' on renkaan R alirengas, kolmikko $(R', +, \cdot)$ on rengas.

Kuntien tapaus
Olkoon $(K, +, \cdot)$ kunta ja olkoon $K' \subset K$. Tällöin K' on kunnan R *alikunta* jos seuraavat ehdot toteutuvat

- $(K', +, \cdot)$ on renkaan $(K, +, \cdot)$ alirengas.
- K' on suljettu kertolaskun käänteisalkioiden suhteen eli kaikilla $k \in K', k \neq 0$ pätee $k^{-1} \in K'$. Tässä k^{-1} on alkion k käänteisalkio kunnassa K.

Jos K' on kunnan K alikunta, kolmikko $(K', +, \cdot)$ on kunta.

Alistruktuurien ja homomorfismien yhteys

Olkoon $\cdot$ joukon X laskutoimitus ja $\cdot'$ joukon Y laskutoimitus. Olkoon $f\colon X \to Y$ kuvaus, joka on yhteensopiva näiden laskutoimitusten kanssa. Oletetaan, että $A \subset X$ on vakaa laskutoimituksen $\cdot$ suhteen ja $B \subset Y$ on vakaa laskutoimituksen $\cdot'$ suhteen. Tällöin *kuvajoukko* $f(A) \subset Y$ on vakaa laskutoimituksen $\cdot'$ suhteen ja *alkukuva* $f^{-1}(B) \subset X$ on on vakaa laskutoimituksen $\cdot$ suhteen.

Jos joukolla Y on laskutoimituksen $\cdot'$ suhteen olemassa neutraalialkio $e' \in Y$, voidaan puhua kuvauksen f *ytimestä*

$$\operatorname{Ker} f = \{x \in X \mid f(x) = e'\},$$

joka on tällöin on joukon X vakaa osajoukko.

Ryhmien tapaus.

Olkoot $(G, \cdot)$ ja $(G', \cdot')$ ryhmiä ja olkoon $f\colon G \to G'$ ryhmähomomorfismi. Olkoon $H \subset G$ ryhmän G aliryhmä ja $H' \subset G'$ vastaavasti ryhmän G' aliryhmä. Tällöin *kuvajoukko* $f(H) \subset G'$ on ryhmän G' aliryhmä ja *alkukuva* $f^{-1}(H') \subset G$ on ryhmän G aliryhmä.

Olkoot $f\colon G \to G'$ ryhmien välinen homomorfismi. Tällöin

- f on injektio jos ja vain jos $\operatorname{Ker} f = \{e\}$ on triviaali (eli sisältää vain neutraalialkion).
- f on surjektio jos ja vain jos $\operatorname{Im} f = G'$.
- f on isomorfismi jos ja vai jos $\operatorname{Im} f = G'$ ja $\operatorname{Ker} f = \{e\}$.

Olkoon G *ryhmä* ja olkoon $N < G$ sen aliryhmä. Sanomme, että N on **normaali** aliryhmä jos kaikilla $x \in G$ ja $n \in N$ pätee $xnx^{-1} \in N$. Jos $N < G$ on normaali aliryhmä, merkitään $N \triangleleft G$.

Normaalien aliryhmien yhteys homomorfismeihin on seuraava. Olkoon $f\colon (G, \cdot) \to (G', \cdot')$ ryhmähomomorfismi. Tällöin sen ydin $N = \operatorname{Ker} f$ on ryhmän G normaali aliryhmä.

Kääntäen mikä tahansa ryhmän normaali aliryhmä on jonkun ryhmähomomorfismin ydin. Normaaleilla aliryhmillä on tärkeä rooli *tekijäryhmien teoriassa*.

Renkaiden/Kuntien tapaus.

Olkoot $(R, +, \cdot)$ ja $(R', +', \cdot')$ renkaita ja olkoon $f\colon R \to R'$ rengashomomorfismi. Olkoon $P \subset R$ renkaan R alirengas ja $P' \subset R'$ vastaavasti renkaan R' alirengas. Tällöin *kuvajoukko* $f(P) \subset R'$ on renkaan R' alirengas ja *alkukuva* $f^{-1}(P') \subset R$ on renkaan R alirengas.

Olkoot $(K, +, \cdot)$ ja $(K', +', \cdot')$ kuntia ja olkoon $f\colon K \to K'$ kuntahomomorfismi. Olkoon $Q \subset K$ kunnan K alikunta ja $Q' \subset K'$ vastaavasti kunnan K' alikunta. Tällöin *kuvajoukko* $f(K) \subset K'$ on kunnan K' alikunta ja *alkukuva* $f^{-1}(Q') \subset K$ on kunnan K alikunta.

Olkoot $f\colon R \to R'$ renkkaiden välinen homomorfismi. Tällöin

- f on injektio jos ja vain jos $\operatorname{Ker} f = \{0_R\}$ on triviaali.
- f on surjektio jos ja vain jos $\operatorname{Im} f = R'$.
- f on isomorfismi jos ja vai jos $\operatorname{Im} f = R'$ ja $\operatorname{Ker} f = \{0_R\}$.

Kuntien välinen homomorfismi on *aina injektiivinen.*

Olkoon $(R, +, \cdot)$ *rengas* ja olkoon $I \subset R$ sen osajoukko. Sanomme, että I on renkaan R **ideaali** jos seuraavat ehdot toteuttuvat.

(1) $(I, +)$ on Abelin ryhmän $(R, +)$ aliryhmä.

(2) Kaikilla $x \in I$ ja $a \in R$ pätee $xa \in I$ ja $ax \in I$.

Ideaaleilla on renkkaiden maailmassa sama rooli kuin normaaleilla aliryhmäillä ryhmien maailmassa.
Nolla-alkion muodostama yksiö $\{0_R\}$ on aina renkaan R ideaali, niin sanottu *triviaali ideaali.* Myös koko rengas eli R on itsensä ideaali. Jos $R = K$ on kunta, niin nämä ovat ainoat kunnan ideaalit.

Olkoon $f\colon (R, +, \cdot) \to (R', +', \cdot')$ rengashomomorfismi. Tällöin sen ydin

$$I = \operatorname{Ker} f = \{r \in R \mid f(r) = 0_R\}$$

on renkaan R ideaali.

Esimerkki Kokonaislukujen renkaan $(\mathbb{Z}, +, \cdot)$ kaikki ideaalit ovat muotoa $n\mathbb{Z}$ jollakin $n \in \mathbb{Z}$.

Tekijästrukruurit

Eivät ole tällä kurssilla niin tärkeitä, mutta perusperiaatteiden ymmärtäminen on hyödyllistä. Lisäksi tekijärengas $\mathbb{Z}_n$ ja sen ominaisuuksien on oltava tuttuja.

Relaatio joukossa X on mikä tahansa $R \subset X \times X$ eli kokoelma pareja (x, y), $x, y \in X$. Tällöin $(x, y) \in R$ merkitään myös xRy.

Määritelmä 6. *Joukossa X määriteltyä relaatiota $\sim \subset X \times X$ sanotaan* ekvivalenssirelaatioksi*, jos*

(i) $\sim$ *on* refleksiivinen*, eli $x \sim x$ kaikilla $x \in X$,*

(ii) $\sim$ *on* symmetrinen*, eli jos $x \sim y$ joillakin $x, y \in X$, niin myös $y \sim x$,*

(iii) $\sim$ *on* transitiivinen*, eli jos $x \sim y$ ja $y \sim z$, niin tällöin aina $x \sim z$.*

Intuitiivisesti - jos $x \sim y$, niin x ja y "samastetaan samaksi alkioksi".

Teknisesesti - määritellään jokaisella $x \in X$ sen *ekvivalenssiluokka*

$$\bar{x} = \{y \in X \mid x \sim y\}.$$

Ekvivalenssiluokat muodostavat joukon X *osituksen*. Tarkemmin sanottuna jokainen $x \in X$ kuuluu *tasan yhteen* ekvivalenssiluokkaan A, jolloin $A = \bar{x}$. Jos $x, y \in X$, niin

$$\bar{x} \cap \bar{y} \neq \emptyset$$

pätee jos ja vain jos $x \sim y$, jolloin $\bar{x} = \bar{y}$.

Ekvivalenssiluokkien muodostamaa joukkoa

$$X/\sim = \{\bar{x} \mid x \in X\}$$

sanotaan *tekijäjoukoksi* (relaation $\sim$ suhteen).

Kanoninen projektio on kuvaus $p\colon X \to X/\sim$, $p(x) = \bar{x}$.

Kokonaisluvut modulo n

Olkoon $n \in \mathbb{N}_+ = \{1, 2, 3, \ldots\}$. Määritellään kokonaislukujen joukossa $\mathbb{Z}$ relaatio $\equiv_n$ ehdolla $x \equiv_n y$ jos ja vain jos erotus $(x - y)$ on jaollinen luvulla n, toisin sanoen jos ja vain jos on olemassa $k \in \mathbb{N}$ siten, että $x - y = kn$. Tällöin $\equiv_n$ on ekvivalenssirelaatio joukossa $\mathbb{Z}$.

Ekvivalenssiluokat: jokaisella $x \in \mathbb{Z}$ pätee

$$\bar{x} = \{x + kn \ \ | k \in \mathbb{Z}\} = x + n\mathbb{Z} = x_n.$$

Tästä seuraa, että $x_n = r_n$, missä $r = 0, 1, \ldots, n-1$ on *jakojäännös*, joka saadaan kun x jaetaan luvulla n. Johtopäätös: Tekijäjoukko

$$\mathbb{Z}/\sim_n = \mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, \bar{n-1}\}$$

on *äärellinen* ja siinä on tasan n alkiota.
Tämän joukon alkioita sanotaan *kokonaisluvuiksi modulo* n.

Ekvivalenssirelaatiot algebrassa

Olkoon $\cdot$ laskutoimitus joukossa X. Olkoon $\sim$ joukon X ekvivalenssirelaatio. Sanomme, että $\sim$ on *yhteensopiva* laskutoimituksen $\cdot$ kanssa, jos ehdoista $x \sim x', y \sim y'$ aina seuraa, että $xy \sim x'y'$.

Jos ekvivalenssirelaatio $\sim$ on yhteensopiva laskutoimituksen $\cdot$ kanssa, tekijäjoukossa $X/\sim$ voidaan määritellä *indusoitu* laskutoimitus $\cdot'$ kaavalla

$$\bar{x} \cdot' \bar{y} = \overline{x \cdot y}.$$

Kanoninen projektio $p\colon (X, \cdot) \to (X/\sim, \cdot')$ on tällöin *laskutoimitukset säilyttävä surjektio.*

Ryhmien tapaus

Olkoon $(G, \cdot)$ ryhmä ja olkoon $\sim$ joukon G ekvivalenssirelaatio, joka on yhteensopiva laskutoimituksen $\cdot$ kanssa. Tällöin tekijäjoukko $G/\sim$ indusoidulla laskutoimituksella $\cdot'$ varustettuna on ryhmä $(G/\sim, \cdot')$. Sanomme tätä ryhmää ryhmän G *tekijäryhmäksi.* Kanoninen kuvaus $p\colon G \to G/\sim$ on tällöin ryhmähomomorfismi.

Jos $(G, \cdot)$ on Abelin ryhmä, myös tekijäryhmä $(G/\sim, \cdot')$ on Abelin ryhmä.

Tekijäryhmä voidaan aina esittää kanonisessa muodossa G/N, missä N on jokin *normaali* aliryhmä. Täsmällisemmin - olkoon $\sim$ ryhmän G ekvivalenssirelaatio, joka on yhteensopiva laskutoimituksen $\cdot$ kanssa. Tällöin neutraalialkion e ekvivalenssiluokka $\bar{e}$ on kanonisen projektion $p\colon G \to G/\sim$ *ydin* $N = \operatorname{Ker} p$, joka on, näin ollen ryhmän G eräs *normaali aliryhmä.* Lisäksi relaatio $\sim$ voidaan tällöin lausua aliryhmän N avulla, sillä $x \sim y$ on yhtäpitävä ehdon $xy^{-1} \in N$ kanssa.

Kääntäen, olkoon N ryhmän G *normaali* aliryhmä. Määritellään joukossa G relaatio $\sim_N$ ehdolla $x \sim_N y$ jos ja vain jos $xy^{-1} \in N$. Tällöin

(i) Relaatio $\sim_N$ on ekvivalenssirelaatio.

(ii) Relaatio $\sim_N$ on yhteensopiva laskutoimituksen $\cdot$ kanssa.

(iii) $N = \bar{e}$ on neutraalialkion e ekvivalenssiluokka relaation $\sim_N$ suhteen.

(iv) Alkion $x \in G$ ekvivalenssiluokka on

$$\bar{x} = xN = Nx,$$

missä

$$xN = \{xn \mid n \in N\}$$

ja vastaavasti

$$Nx = \{nx \mid n \in N\}.$$

Näin ollen kaikki ryhmän G tekijäryhmät ovat täsmälleen muotoa $G/\sim_N$, missä N on jokin ryhmän G *normaali* aliryhmä ja $\sim_N$ on ehdolla $xy^{-1} \in N$ määritelty relaatio. Tekijäryhmää $G/\sim_N$ on tapana merkitä yksinkertaisesti G/N. Tekijäryhmän G/N neutraalialkio on ekvivalenssiluokka $\bar{e} = N$. Yleisemmin mielivaltaisen alkion $x \in G$ ekvivalenssiluokka on sivuluokka

$$xN = \{xn \mid n \in N\}.$$

Tällä merkintätavalla tekijäryhmässä G/N lasketaan seuraavaksi:

$$xN \cdot' yN = (xy)N,$$

$$(xN)^{-1} = x^{-1}N.$$

Jos G on vaihdannainen ryhmä, jokainen sen aliryhmä on normaali ja tekijäryhmä G/N voidaan muodostaa minkä tahansa aliryhmän N suhteen.

Renkaiden tapaus

Olkoon $(R, +, \cdot)$ rengas ja olkoon $\sim$ joukon R ekvivalenssirelaatio, joka on yhteensopiva sekä laskutoimituksen $+$, että laskutoimituksen $\cdot$ kanssa. Tällöin tekijäjoukko $R/\sim$ indusoiduilla laskutoimituksilla $+'$ ja $\cdot'$ varustettuna on rengas $(R/\sim, +', \cdot')$. Sanomme tätä rengasta renkaan R *tekijärenkaaksi*. Kanoninen kuvaus $p\colon G \to G/\sim$ on tällöin ryhmähomomorfismi.

Jos rengas R on kommutatiivinen, myös tekijärengas $R/\sim$ on kommutatiivinen rengas.

Esimerkki

Relaatio $\equiv_n$ kokonaislukujen $\mathbb{Z}$ joukossa on yhteensopiva kokonaislukujen sekä yhteen-, että kertolaskun kanssa. Koska $(\mathbb{Z}, +, \cdot)$ on kommutatiivinen rengas, kokonaislukujen modulo n muodostama joukko $\mathbb{Z}_n$ muodostaa tämän nojalla *kommutatiivisen renkaan* $(\mathbb{Z}_n, +, \cdot)$. Tämä on tärkeä esimerkki äärellisestä renkaasta, jossa on n alkiota.

Rengas $\mathbb{Z}_n$ on kunta jos ja vain jos n on alkuluku.

Tekijärengas voidaan aina esittää kanonisessa muodossa R/I, missä I on eräs renkaan R *ideaali*. Tarkemmin - olkoon R rengas ja olkoon $\sim$ joukon R ekvivalenssirelaatio, joka on yhteensopiva sekä renkaan yhteenlaskun, että renkaan kertolaskun suhteen. Tällöin nolla-alkion 0_R ekvivalenssiluokka $\bar{0_R}$ on kanoisen projektion *ydin* $\operatorname{Ker} p$, joten se on eräs *ideaali*

$$I = \operatorname{Ker} p = p^{-1}(\overline{0_R}).$$

Relaatio $\sim$ voidaan tällöin lausua joukon I avulla, sillä osoittautuu, että $x \sim y$ jos ja vain jos $x - y \in I$.

Kääntäen, olkoon I renkaan R *ideaali*. Määritellään joukossa R relaatio $\sim_I$ ehdolla $x \sim_I y$ jos ja vain jos $x - y \in I$. Tällöin

(i) Relaatio $\sim_I$ on ekvivalenssirelaatio.

(ii) Relaatio $\sim_I$ on yhteensopiva renkaan laskutoimitusten $+$ ja $\cdot$ kanssa.

(iii) $I = \overline{0_R}$ on nolla-alkion 0_R ekvivalenssiluokka relaation $\sim_I$ suhteen.

(iv) Alkion $x \in R$ ekvivalenssiluokka on

$$\bar{x} = x + I = I + x.$$

Näin ollen kaikki renkaan R tekijärenkaat ovat täsmälleen muotoa $R/\sim_I$, missä I on jokin renkaan R *ideaali* ja $\sim_I$ on ehdolla $x - y \in I$ määritelty relaatio. Alkion $x \in R$ ekvivalenssiluokka on

$$x + I = \{x + a \mid a \in I\}.$$

Tekijärenkaassa R/I laskutoimitukset ovat määritelty seuraavasti:

$$(x + I) + (y + I) = (x + y) + I,$$

$$(x + I) \cdot (y + I) = (xy) + I,$$

Kertolaksun ykkösalkio tekijärenkaassa R/I on renkaan R ykkösalkion 1_R ekvivalenssiluokka $1_R + I$.

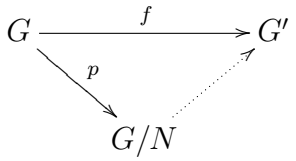
Tärkeä Esimerkki: Osajoukko $n\mathbb{Z} \subset \mathbb{Z}$ on renkaan $(\mathbb{Z}, +, \cdot)$ ideaali jokaisella $n \in \mathbb{Z}$. Tekijärengas $\mathbb{Z}/n\mathbb{Z}$ on kokonaislukujen modulo n rengas $\mathbb{Z}_n$.

Hajotelma- ja Isomorfialauseet

Tekijästruktuurien tärkeimpiä sovelluksia ovat niin sanotut *isomorfialauseet* ja, yleisemmin, *hajoitelmalauseet*.

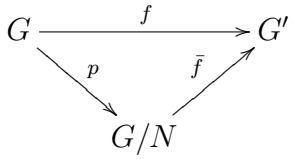
Ryhmien tapaus

Olkoot $(G, \cdot)$ ja $(G', \cdot')$ ryhmiä. Olkoon $f\colon G \to G'$ ryhmähomomorfismi. Olkoon $N \lhd G$ ryhmän G normaali aliryhmä ja olkoon $p\colon G \to G/N$ kanoninen projektio tekijäryhmälle. Tällöin kuvaukset f ja p muodostavat diagramin



Ryhmähomomorfismien hajotelmalause:

Tilanteessa yllä on olemassa indusoidu ryhmähomomorfismi $\bar{f}\colon G/N \to G'$ jolle pätee $f = \bar{f} \circ p$,



jos ja vain jos $N \subset \operatorname{Ker} f$.

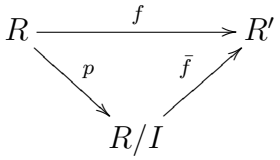
Jos tällainen kuvaus $\bar{f}$ on olemassa, niin se on yksikäsitteinen. Lisäksi pätee $\operatorname{Im} \bar{f} = \operatorname{Im} f$. Erityisesti $\bar{f}$ on surjektio jos ja vain jos f on surjektio. Lisäksi $\bar{f}$ on injektio jos ja vain jos $N = \operatorname{Ker} f$.

Tapauksessa $N = \operatorname{Ker} f$, saadaan hajoitelmalauseen seurauksena niin sanottu *(ensimmäinen) isomorfialause*, joka on Algebran tärkeämpiä perustuloksia:

Ryhmien Isomorfialause Olkoot G, G' ryhmiä ja olkoon $f\colon G \to G'$ ryhmähomomorfismi. Tällöin indusoitu kuvaus $\bar{f}\colon G/\operatorname{Ker} f \to \operatorname{Im} f$, joka on määritelty ehdolla $\bar{f}(\bar{x}) = f(x)$, on **ryhmäisomorfismi**.

Renkkaiden tapaus
Renkaille pätevät täysin analogiset hajotelma- ja isomorfismilauseet, kuten ryhmien teoriassa.

Rengashomomorfismien hajotelmalause
Olkoot $(R, +, \cdot)$ ja $(R', +', \cdot')$ renkaita. Olkoon $f\colon R \to R'$ rengashomomorfismi. Olkoon I renkaan R ideaali ja olkoon $p\colon R \to R/I$ kanoninen projektio tekijärenkaalle. Tällöin on olemassa indusoidu rengashomomorfismi $\bar{f}\colon R/I \to R'$ jolle pätee $f = \bar{f} \circ p$,



jos ja vain jos $I \subset \operatorname{Ker} f$.
Jos tällainen kuvaus $\bar{f}$ on olemassa, niin se on yksikäsitteinen. Lisäksi pätee $\operatorname{Im} \bar{f} = \operatorname{Im} f$. Erityisesti $\bar{f}$ on surjektio jos ja vain jos f on surjektio.

Lisäksi $\bar{f}$ on injektio jos ja vain jos $I = \operatorname{Ker} f$.

Renkaiden Isomorfialause Olkoot R, R' renkaita ja olkoon $f\colon R \to R'$ rengashomomorfismi. Tällöin indusoitu kuvaus $\bar{f}\colon R/\operatorname{Ker} f \to \operatorname{Im} f$, joka on määritelty ehdolla $\bar{f}(\bar{x}) = f(x)$, on **rengasisomorfismi**.

Renkaan kokonaisluvut ja karakteristika
Olkoon $(R, +, \cdot)$ rengas. Tällöin $(R, +)$ on Abelin ryhmä, joten voimme muodostaa renkaan ykkösalkion $1_R \in R$ *monikerrat* $m \cdot 1_R$ jokaisella kokonaisluvulla $m \in \mathbb{Z}$. Määritellään kuvaus $\phi\colon \mathbb{Z} \to R$ kaavalla $\phi(m) = m \cdot 1$. Tällöin ϕ on renkaiden välinen homomorfismi. Tämän kuvaksen kuvajoukko

$$\mathbb{Z}1_R = \{m1_R \mid m \in \mathbb{Z}\}$$

on kaikkien ykkösten monikertojen muodostama joukko ja ydin $\operatorname{Ker} \phi$ on jokin renkaan $\mathbb{Z}$ ideaali, eli muotoa $n\mathbb{Z}$ jollakin $n \in \mathbb{Z}$, $n \geq 0$. Renkaiden isomorfialauseesta seuraa, että on olemassa indusoidu **isomorfismi** tekijärenkaasta $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ renkaan R alirenkaalle $\mathbb{Z}1_R$. Tämän renkaan $\mathbb{Z}1_R$ alkiota sanotaan *renkaan kokonaisluvuiksi*. Luonnollista lukua $n \in \mathbb{N}$ sanotaan renkaan R **karakteristikaksi**.

Vaihtoehto 1: Renkaan R karakteristikka on 0. Tällöin $\operatorname{Ker} \phi = 0\mathbb{Z} = 0$, joten ϕ on injektio, joten

$$\mathbb{Z}1_R \cong \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\{0\} \cong \mathbb{Z}$$

Renkaan R ykkösalkiolle pätee $n1_R = 0_R$ jos ja vain jos $n = 0$.

Vaihtoehto 2: Yllä $n > 0$ eli renkaan R karakteristikka n on positiivinen kokonaisluku. Tällöin $\operatorname{Ker} \phi = n\mathbb{Z}$, jotens

$$\mathbb{Z}1_R \cong \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$$

eli renkaan kokonaislukujen alirengas on isomorfinen äärellisen renkaan $\mathbb{Z}_n$ kanssa. Renkaan ykkösalkiolle pätee

$$n1_R = \underbrace{1 + 1 + \ldots + 1}_{n \text{ kertaa}} = 0_R$$

ja renkaan karakteristikka n on itse asiassa *pienin* positiivinen kokonaisluku k jolla on ominaisuus $k1_R = 0_R$.

Voidaan osoittaa, että kunnan karakteristikka on aina joko nolla tai alkuluku.