802355A Renkaat, kunnat ja polynomit

Luentorunko

Syksy 2013

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

Sisältö

1 Kertausta kurssilta Lukuteoria ja ryhmät

(Näitä asioita kerrataan vain tarpeen mukaan.)

Määritelmä 1.1. Kokonaislukujen joukossa $\mathbb{Z}$ määritellyn ekvivalenssirelaation

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

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

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

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

Määritelmä 1.2. Jäännösluokkaa $[a] \pmod{m}$ sanotaan *alkuluokaksi* (mod m), mikäli $\text{syt}(a, m) = 1$. Alkuluokkien joukkoa merkitään $\mathbb{Z}_m^*$.

Miten jäännösluokilla lasketaan?

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

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

Määritelmä 1.3. Olkoot $G \neq \emptyset$ ja $(*)$ joukon G binäärinen operaatio eli $a * b \in G$ aina, kun $a, b \in G$. Pari $(G, *)$ on *ryhmä* (group), mikäli seuraavat kolme ehtoa toteutuvat:

1. $(*)$ on assosiatiivinen eli

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

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

2. Joukossa G on sellainen alkio e, että

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

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

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

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

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

Jos lisäksi $(G, *)$ toteuttaa ehdon

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

niin kyseessä on *Abelin ryhmä* eli kommutatiivinen ryhmä.

Lause 1.4.

1. *Pari* $(\mathbb{Z}_m, +)$ *on Abelin ryhmä.*
2. *Pari* $(\mathbb{Z}_m^*, \cdot)$ *on Abelin ryhmä.*

Määritelmä 1.5. Olkoon $(G, *)$ ryhmä ja $H \subseteq G,\ H \neq \emptyset$. Jos $(H, *)$ on ryhmä, sitä sanotaan *ryhmän* $(G, *)$ *aliryhmäksi* (subgroup); merkitään $(H, *) \leq (G, *)$ tai lyhyemmin $H \leq G$.

Lause 1.6 (Aliryhmäkriteeri)**.** *Olkoot* $(G, *)$ *ryhmä ja* $H \subseteq G,\ H \neq \emptyset$. *Nyt* $H \leq G$ *jos ja vain jos seuraavat ehdot toteutuvat:*

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

Seuraus 1.7. *Olkoot* $(G, *)$ *ryhmä ja* $H \subseteq G,\ H \neq \emptyset$. *Tällöin* $H \leq G$ *jos ja vain jos ehto*

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

on voimassa.

Määritelmä 1.8. Olkoon $(H, *) \leq (G, *)$ ja $a \in G$. Joukkoa
$aH = a * H = \{a * h \mid h \in H\}$ sanotaan *alkion a määräämäksi aliryhmän H vasemmaksi sivuluokaksi* (left coset).
Joukkoa $Ha = H * a = \{h * a \mid h \in H\}$ sanotaan *alkion a määräämäksi aliryhmän H oikeaksi sivuluokaksi* (right coset). Oikeilla sivuluokilla on voimassa samat ominaisuudet kuin vasemmilla sivuluokilla.

Lause 1.9. *Olkoon G ryhmä, $H \leq G$ ja $a_1H, a_2H, \ldots$ aliryhmän H vasemmat sivuluokat ryhmässä G.*

Tällöin

$$G = \bigcup_i a_i H$$

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

Lisäksi, jos $b \in aH$, niin $bH = aH$. Siten $hH = eH = H$ kaikilla $h \in H$.

Lause 1.10 (Lagrangen lause)**.** *Olkoot G äärellinen ryhmä, $H \leq G$ ja n aliryhmän H vasempien sivuluokkien lukumäärä ryhmässä G. Tällöin*

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

ts. äärellisessä ryhmässä aliryhmän kertaluku jakaa ryhmän kertaluvun.

Määritelmä 1.11. Olkoon G ryhmä ja $a \in G$. Tällöin joukko

$$H = \{a^k \mid k \in \mathbb{Z}\}$$

on *alkion a generoima syklinen ryhmä* (cyclic group); merkitään $H = \langle a \rangle$. Alkio a on *generoija* (generator).

Lause 1.12. *Olkoot G ryhmä ja $a \in G$ sekä n pienin sellainen positiivinen kokonaisluku, että $a^n = e$. Tällöin $|\langle a \rangle| = n$.*

Lause 1.13. *Jos G on äärellinen ryhmä, niin $a^{|G|} = e$ kaikilla $a \in G$.*

Määritelmä 1.14. Olkoon $N \leq G$. Aliryhmää N sanotaan *normaaliksi*, mikäli $aN = Na$ aina, kun $a \in G$. Tällöin merkitään $N \trianglelefteq G$.

Lause 1.15. *Ryhmän G aliryhmä N on normaali jos ja vain jos*

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

Huomautus. Abelin ryhmän jokainen aliryhmä on normaali.

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

$$aN \cdot bN = (a * b)\, N.$$

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

Lause 1.16. *Olkoon G ryhmä ja $N \trianglelefteq G$. Tällöin $(\{aN \mid a \in G\}, \cdot)$ on ryhmä.*

Määritelmä 1.17. Edellä esiteltyä paria $(\{aN \mid a \in G\}, \cdot)$ kutsutaan *ryhmän G tekijäryhmäksi normaalin aliryhmän N suhteen* (factor group/quotient group of G by N). Kyseisestä ryhmästä käytetään merkintää G/N.

Määritelmä 1.18. Olkoot $(G, \cdot)$ ja $(H, *)$ ryhmiä. Kuvausta $f : G \to H$ sanotaan *ryhmähomomorfismiksi* ryhmältä G ryhmälle H, mikäli

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

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

Lause 1.19. *Olkoon $f : G \to H$ ryhmähomomorfismi ja olkoot e_G ja e_H ryhmien G ja H neutraalialkiot. Tällöin*

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

aina, kun $a \in G$.

Määritelmä 1.20. Olkoon $f : G \to H$ kuvaus, $S \subseteq G$ ja $T \subseteq H$. Joukon *S kuva* kuvauksessa f on joukko $f(S) = \{f(s) \mid s \in S\}$.
Joukon *T alkukuva* kuvauksessa f on joukko $f^{-1}(T) = \{g \in G \mid f(g) \in T\}$.

Määritelmä 1.21. Olkoon $f : G \to H$ homomorfismi. Joukkoa

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

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

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

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

Lause 1.22.

1. $Ker(f) \trianglelefteq G$, *ja*
2. $Im(f) \leq H$.

Määritelmä 1.23. Ryhmät $(G, \cdot)$ ja $(H, *)$ ovat *isomorfiset* eli rakenneyhtäläiset (G and H are isomorphic), mikäli on olemassa bijektio $f : G \to H$, joka toteuttaa ehdon $f(a \cdot b) = f(a) * f(b)$ aina, kun $a, b \in G$ (eli f on bijektiivinen homomorfismi). Tällöin merkitään $G \cong H$ ja sanotaan, että f on *ryhmäisomorfismi* (a group isomorphism).

Lause 1.24 (Homomorfismien peruslause)**.** *Olkoon $f : G \to H$ homomorfismi. Tällöin*

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

2 Renkaat

2.1 Renkaiden teoriaa

Määritelmä 2.1.1. Kolmikko $(R, +, \cdot)$ on *rengas* (ring), mikäli

1. $(R, +)$ on Abelin ryhmä (ns. *additiivinen ryhmä*):
   - $(+)$ on binäärinen operaatio joukossa R eli $a + b \in R$ kaikilla $a, b \in R$.
   - $(+)$ on assosiatiivinen operaatio eli $a+(b+c) = (a+b)+c$ kaikilla $a, b, c \in R$.
   - Joukossa R on neutraalialkio operaation $(+)$ suhteen eli on olemassa sellainen alkio $\mathbf{0} \in R$, että $a+\mathbf{0} = \mathbf{0}+a = a$ kaikilla $a \in R$. Tätä alkiota nimitetään renkaan R *nolla-alkioksi*.
   - Jokaisella joukon R alkiolla on olemassa käänteisalkio joukossa R operaation $(+)$ suhteen eli jokaiselle $a \in R$ on olemassa sellainen alkio $-a \in R$, että $a + (-a) = -a + a = \mathbf{0}$. Tätä käänteisalkiota nimitetään alkion a *vasta-alkioksi*.
   - $(+)$ on kommutatiivinen operaatio eli $a+b = b+a$ kaikilla $a, b \in R$.
2. $(R, \cdot)$ on monoidi:
   - $(\cdot)$ on binäärinen operaatio joukossa R eli $a \cdot b \in R$ kaikilla $a, b \in R$.
   - $(\cdot)$ on assosiatiivinen operaatio eli $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ kaikilla $a, b, c \in R$.
   - Joukossa R on neutraalialkio operaation $(\cdot)$ suhteen eli on olemassa sellainen alkio $\mathbf{1} \in R$, että $a \cdot \mathbf{1} = \mathbf{1} \cdot a = a$ kaikilla $a \in R$. Tätä alkiota nimitetään renkaan R *ykkösalkioksi*.
3. Seuraavat distributiivisuus- eli osittelulait ovat voimassa:

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

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

Lisäksi rengasta sanotaan *kommutatiiviseksi*, mikäli se on kommutatiivinen operaation $(\cdot)$ suhteen eli jos $a \cdot b = b \cdot a$ aina, kun $a, b \in R$.

Huomautus. Renkaan ykkösalkio on yksikäsitteinen.

Jatkossa operaation $(\cdot)$ tuloksesta $a \cdot b$ käytetään lyhyempää merkintää ab.

Esimerkki. Esimerkiksi $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Z}_m, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ ja $(\mathbb{C}, +, \cdot)$ ovat renkaita.

Lause 2.1.2. *Olkoot R rengas, a, b ja c joukon R alkioita sekä $\mathbf{0}$ renkaan R nolla-alkio. Tällöin*

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

Huomautus: merkinnällä $b - c$ tarkoitetaan yhteenlaskua $b + (-c)$.

Todistus. Luennolla.

Määritelmä 2.1.3. Olkoot $(R, +, \cdot)$ rengas ja $\emptyset \neq S \subseteq R$. Jos $(S, +, \cdot)$ on rengas, jolla on sama ykkösalkio kuin renkaalla R, niin sitä sanotaan renkaan R *alirenkaaksi* (subring).

Lause 2.1.4 (Alirengaskriteeri)**.** *Renkaan $(R, +, \cdot)$ ei-tyhjä osajoukko S on renkaan R alirengas jos ja vain jos*

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

Todistus. Luennolla.

Huomautus. $|S| \mid |R|$

2.2 Ideaali

Määritelmä 2.2.1. Renkaan $(R, +, \cdot)$ ei-tyhjä osajoukko I on *ideaali* (ideal), mikäli

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

Huomautus.

- Renkaalla on aina *triviaalit ideaalit* R ja $\{\mathbf{0}\}$
- $|I| \mid |R|$

Lause 2.2.2. *Jos I on renkaan R ideaali ja $\mathbf{1}_R \in I$, niin $I = R$.*

Todistus. Luennolla

Lause 2.2.3. *Jos I ja J ovat renkaan R ideaaleja, niin tällöin myös niiden leikkaus $I \cap J$ ja summa*

$$I + J = \{a + b \mid a \in I, b \in J\}$$

ovat ideaaleja.

Todistus. Luennolla.

Huomautus. Edellinen tulos voidaan yleistää useammalle ideaalille, leikkauksen tapauksessa jopa äärettömän monelle.

Määritelmä 2.2.4. Jos $(R, +, \cdot)$ on rengas ja $a \in R$, niin suppeinta ideaalia, joka sisältää alkion a, sanotaan alkion a generoimaksi *pääideaaliksi* (principal ideal) ja siitä käytetään merkintää (a). Toisin sanoen alkion a generoima pääideaali on sellainen ideaali, joka sisältää alkion a ja sisältyy kaikkiin muihin alkion a sisältäviin renkaan R ideaaleihin.

Huomautus. Ykkösalkion määräämä pääideaali on koko rengas R.
Nolla-alkion määräämä pääideaali on $\{\mathbf{0}\}$.

Lause 2.2.5. *Jos $(R, +, \cdot)$ on kommutatiivinen rengas ja $a \in R$, niin*

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

Todistus. Luennolla.

Lause 2.2.6. *Renkaan $(\mathbb{Z}, +, \cdot)$ jokainen ideaali on pääideaali.*

Todistus. Luennolla.

Määritelmä 2.2.7. Rengas $(R, +, \cdot)$ on *pääideaalirengas* (principal ideal ring), jos sen jokainen ideaali on pääideaali.

Määritelmä 2.2.8. Renkaan $(R, +, \cdot)$ ideaali M on *maksimaalinen*, mikäli

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

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

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

Lause 2.2.9. *Renkaan $(\mathbb{Z}, +, \cdot)$ maksimaalisia ideaaleja ovat tarkalleen ne pääideaalit (p), missä p on alkuluku.*

Todistus. Luennolla.

2.3 Tekijärengas

Samalla tavoin kuin ryhmälle määriteltiin tekijäryhmä, voidaan renkaalle määritellä tekijärengas. Tekijäryhmät muodostettiin normaalien aliryhmien suhteen, jolloin sivuluokkien joukossa oli mahdollista määritellä laskutoimitus. Tekijärenkaan tapauksessa on pystyttävä määrittelemään kaksi laskutoimitusta, yhteen- ja kertolasku.

Olkoon I renkaan $(R, +, \cdot)$ ideaali, jolloin $(I, +) \leq (R, +)$. Nyt $(R, +)$ on Abelin ryhmä, joten $(I, +) \trianglelefteq (R, +)$. Siten tekijäryhmä $(R/I, +)$ on olemassa. Tekijäryhmän alkioina ovat sivuluokat $r + I = \{r + x \mid x \in I\}$, missä $r \in R$, ja sivuluokkien yhteenlasku määritellään siten, että

$$(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I$$

aina, kun $r_1, r_2 \in R$. Tällöin ryhmän $(R/K, +)$ nolla-alkio on $\mathbf{0} + I = I$ ja alkion $a + I \in R/K$ vasta-alkio on $(-a) + I$.

Määritellään sivuluokkien välinen kertolasku $(\cdot)$ siten, että

$$(r_1 + I) \cdot (r_2 + I) = (r_1 r_2) + I$$

aina, kun $r_1, r_2 \in R$. Osoitetaan, että näin määritelty kertolasku on hyvinmääritelty. Jos $a_1 + I = b_1 + I$ ja $a_2 + I = b_2 + I$, niin $a_1 \in b_1 + I$ ja $a_2 \in b_2 + I$, joten $a_1 = b_1 + i_1$ ja $a_2 = b_2 + i_2$ joillakin $i_1, i_2 \in I$. Tällöin

$$\begin{aligned}(a_1 + I) \cdot (a_2 + I) &= a_1 a_2 + I = (b_1 + i_1)(b_2 + i_2) + I \\ &= (b_1 b_2 + b_1 i_2 + i_1 b_2 + i_1 i_2) + I \\ &= (b_1 b_2 + I) + (b_1 i_2 + I) + (i_1 b_2 + I) + (i_1 i_2 + I) \\ &= (b_1 b_2 + I) + (\mathbf{0} + I) + (\mathbf{0} + I) + (\mathbf{0} + I) \\ &= b_1 b_2 + I = (b_1 + I) \cdot (b_2 + I),\end{aligned}$$

sillä $b_1 i_2,\ i_1 b_2,\ i_1 i_2 \in I$, koska I on ideaali. Tulo on siis riippumaton sivuluokkien edustajista.

Lause 2.3.1. *Olkoon I renkaan $(R, +, \cdot)$ ideaali ja $R/I = \{r + I \mid r \in R\}$, missä $r + I = \{r + x \mid x \in I\}$. Tällöin $(R/I, +, \cdot)$ on rengas, missä $(+)$ ja $(\cdot)$ ovat edellä määritellyt sivuluokkien yhteen- ja kertolasku.*

Todistus. Osoitetaan, että määritelmän 2.1.1 ehdot toteutuvat.

1. (a) Olkoon $a + I,\ b + I \in R/I$. Tällöin

$$(a + I) + (b + I) = (a + b) + I \in R/I.$$

(b) Olkoon $a+I,\ b+I,\ c+I \in R/I$. Tällöin

$$\begin{aligned}(a+I)+((b+I)+(c+I)) &= (a+I)((b+c)+I)\\ &= (a+(b+c))+I\\ &= ((a+b)+c)+I\\ &= ((a+b)+I)+(c+I)\\ &= ((a+I)+(b+I))+(c+I).\end{aligned}$$

(c) Nyt $\mathbf{0}+I = I \in R/I$ ja

$$(\mathbf{0}+I)+(a+I) = (a+I) = (a+I)+(\mathbf{0}+I)$$

kaikilla $a+I \in R/I$, joten $\mathbf{0}+I = I$ on nolla-alkio joukossa R/I.

(d) Olkoon $a+I \in R/I$. Tällöin $(-a)+I = -a+I \in R/I$ ja

$$(a+I)+(-a+I) = (a-a)+I = \mathbf{0}+I = (-a+I)+(a+I),$$

joten $-a+I$ on alkion $a+I$ vasta-alkio joukossa R/I.

(e) Olkoon $a+I,\ b+I \in R/I$. Tällöin

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

Kohtien (a)–(e) nojalla $(R/I,+)$ on Abelin ryhmä.

2. (a) Olkoon $a+I,\ b+I \in R/I$. Tällöin $(a+I)\cdot(b+I) = ab+I \in R/I$.

(b) Olkoon $a+I,\ b+I,\ c+I \in R/I$. Tällöin

$$\begin{aligned}(a+I)\cdot((b+I)\cdot(c+I)) &= (a+I)\cdot(bc+I)\\ &= a(bc)+I = (ab)c+I\\ &= (ab+I)\cdot(c+I)\\ &= ((a+I)\cdot(b+I))\cdot(c+I).\end{aligned}$$

(c) Nyt $\mathbf{1}+I \in R/I$ ja

$$(\mathbf{1}+I)\cdot(a+I) = (a+I) = (a+I)\cdot(\mathbf{1}+I)$$

kaikilla $a+I \in R/I$, joten $\mathbf{1}+I$ on ykkösalkio joukossa R/I.

Kohtien (a)–(c) nojalla $(R/I,\cdot)$ on monoidi.

3. Olkoon $a+I,\ b+I,\ c+I \in R/I$. Tällöin

$$\begin{aligned}(a+I)\cdot((b+I)+(c+I)) &= (a+I)\cdot((b+c)+I)\\ &= a(b+c)+I = (ab+ac)+I\\ &= (ab+I)+(ac+I)\\ &= (a+I)\cdot(b+I)+(a+I)\cdot(c+I)\end{aligned}$$

ja

$$\begin{aligned}((a+I)+(b+I))\cdot(c+I) &= ((a+b)+I)\cdot(c+I)\\ &= (a+b)c+I = (ac+bc)+I\\ &= (ac+I)+(bc+I)\\ &= (a+I)\cdot(c+I)+(b+I)\cdot(c+I).\end{aligned}$$

Kohtien 1–3 nojalla $(R/I,+,\cdot)$ on rengas.

Huomautus. Jos $(R,+,\cdot)$ on kommutatiivinen rengas, niin myös tekijärengas $(R/I,+,\cdot)$ on kommutatiivinen rengas, sillä tällöin

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

kaikilla $a+I,\ b+I \in R/K$.

2.4 Rengashomomorfismi

Määritelmä 2.4.1. Olkoon $(R, +, \cdot)$ ja $(R', \oplus, \odot)$ renkaita. Tällöin kuvausta $f : R \to R'$ sanotaan *rengashomomorfismiksi* (ring homomorphism), jos se täyttää seuraavat ehdot:

1. $f(a + b) = f(a) \oplus f(b)$ kaikilla $a, b \in R$,
2. $f(ab) = f(a) \odot f(b)$ kaikilla $a, b \in R$,
3. $f(\mathbf{1}_R) = \mathbf{1}_{R'}$.

Huomautus. Jos f on rengashomomorfismi, niin määritelmän kohdan 1 nojalla f on myös ryhmähomomorfismi $(R, +) \to (R', \oplus)$. Täten kurssilla Lukuteoria ja ryhmät todistetun lauseen nojalla pätee

$$f(\mathbf{0}_R) = \mathbf{0}_{R'} \text{ ja}$$
$$f(-a) = -f(a) \text{ kaikilla } a \in R.$$

Lisäksi, kohdista 2 ja 3 seuraa, että jos a^{-1} on olemassa, niin

$$f(a^{-1}) = f(a)^{-1} \text{ kaikilla } a \in R.$$

Määritelmä 2.4.2. Olkoon $f : R \to R'$ kuvaus, $S \subseteq R$ ja $S' \subseteq R'$. Joukon S *kuva* (image) kuvauksessa f on joukko $f(S) = \{f(s) \mid s \in S\}$.
Lisäksi joukon S' *alkukuva* (inverse image/preimage) kuvauksessa f on joukko $f^{-1}(S') = \{r \in R \mid f(r) \in S'\}$.

Lause 2.4.3. *Olkoon $f : (R, +, \cdot) \to (R', \oplus, \odot)$ rengashomomorfismi. Tällöin seuraavat väitteet pätevät.*

1. *Jos S on renkaan R alirengas, niin $f(S)$ on renkaan R' alirengas.*
2. *Jos S' on renkaan R' alirengas, niin $f^{-1}(S')$ on renkaan R alirengas.*
3. *Jos I on renkaan R ideaali, niin $f(I)$ on renkaan $f(R)$ ideaali.*
4. *Jos I' on renkaan R' ideaali, niin $f^{-1}(I')$ on renkaan R ideaali.*

Todistus.

1. Olkoon S renkaan $(R, +, \cdot)$ alirengas. Selvästi $f(S) \subseteq R'$, ja $f(S) \neq \emptyset$, sillä $\mathbf{0}_R \in S$, joten $f(\mathbf{0}_R) \in f(S)$. Olkoon $c, d \in f(S)$. Tällöin on olemassa sellaiset $a, b \in S$, että $c = f(a)$ ja $d = f(b)$.

(a) Koska S on renkaan R alirengas, niin $a - b \in S$. Tällöin

$$f(a - b) = f(a + (-b)) \in f(S).$$

Kuvaus f on rengashomomorfismi, joten

$$c \oplus (-d) = f(a) \oplus (-f(b)) = f(a) \oplus f(-b) = f(a + (-b)) \in f(S).$$

(b) Koska S on renkaan alirengas, niin $a \cdot b \in S$. Siispä $f(a \cdot b) \in f(S)$. Koska f on rengashomomorfismi, niin

$$c \odot d = f(a) \odot f(b) = f(a \cdot b) \in f(S).$$

(c) Koska S on renkaan R alirengas, niin $\mathbf{1}_R \in S$. Koska f on rengashomomorfismi, niin

$$\mathbf{1}_{R'} = f(\mathbf{1}_R) \in f(S).$$

Nyt kohtien (a)–(c) ja alirengaskriteerin nojalla $f(S)$ on renkaan R' alirengas.

2. Olkoon S' renkaan R' alirengas. Selvästi $f^{-1}(S') \subseteq R$. Nyt f on rengashomomorfismi ja S' on renkaan R' alirengas, joten $f(\mathbf{0}_R) = \mathbf{0}_{R'} \in S'$. Näin ollen $\mathbf{0}_R \in f^{-1}(S')$, joten $f^{-1}(S') \neq \emptyset$. Olkoot $a, b \in f^{-1}(S')$, jolloin $f(a), f(b) \in S'$.

   (a) Koska S' on renkaan R' alirengas, niin $f(a) \oplus (-f(b)) \in S'$. Koska f on rengashomomorfismi, niin

   $$f(a - b) = f(a + (-b)) = f(a) \oplus f(-b) = f(a) \oplus (-f(b)) \in S'.$$

   Näin ollen $a - b \in f^{-1}(S')$.

   (b) Koska S' on renkaan R' alirengas, niin $f(a) \odot f(b) \in S'$. Koska f on rengashomomorfismi, niin

   $$f(a \cdot b) = f(a) \odot f(b) \in S'.$$

   Näin ollen $a \cdot b \in f^{-1}(S')$.

   (c) Koska S' on renkaan R' alirengas, niin $\mathbf{1}_{R'} \in S'$. Koska f on rengashomomorfismi, niin

   $$f(\mathbf{1}_R) = \mathbf{1}_{R'} \in S'.$$

   Näin ollen $\mathbf{1}_R \in f^{-1}(S')$.

Nyt kohtien (a)–(c) ja alirengaskriteerin nojalla $f^{-1}(S')$ on renkaan R alirengas.

3. Olkoon I renkaan R ideaali. Tällöin $\mathbf{0}_R \in I$, joten $\emptyset \neq I \subseteq R$. Näin ollen $\emptyset \neq f(I) \subseteq f(R)$. Koska R on renkaan R alirengas, niin edellä todistetun kohdan 1. nojalla $f(R)$ on renkaan R' alirengas. Siispä $f(R)$ on rengas.

   (a) Olkoon $c, d \in f(I)$. Tällöin on olemassa sellaiset $a, b \in I$, että $c = f(a)$ ja $d = f(b)$. Koska I on renkaan R ideaali, niin $a - b \in I$ eli $f(a - b) \in f(I)$. Koska f on rengashomomorfismi, niin

   $$c \oplus (-d) = f(a) \oplus (-f(b)) = f(a) \oplus f(-b) = f(a - b) \in f(I).$$

   Siispä $(f(I), \oplus) \leq (f(R), \oplus)$.

   (b) Olkoon $x \in f(I)$ ja $s \in f(R)$. Tällöin on olemassa sellaiset $a \in I$ ja $r \in R$, että $x = f(a)$ ja $s = f(r)$. Koska I on renkaan R ideaali, niin $a \cdot r,\ r \cdot a \in I$, jolloin $f(a \cdot r),\ f(r \cdot a) \in f(I)$. Koska f on rengashomomorfismi, niin

   $$x \odot s = f(a) \odot f(r) = f(a \cdot r) \in f(I)$$

   ja

   $$s \odot x = f(r) \odot f(a) = f(r \cdot a) \in f(I).$$

   Kohtien (a) ja (b) nojalla $f(I)$ on renkaan $f(R)$ ideaali.

4. Olkoon I' renkaan R' ideaali. Tällöin $\mathbf{0}_{R'} \in I'$, joten koska $f(\mathbf{0}_R) = \mathbf{0}_{R'}$, niin $\mathbf{0}_R \in f^{-1}(I')$. Siispä $\emptyset \neq f^{-1}(I') \subseteq R$.

   (a) Olkoon $a, b \in f^{-1}(I')$. Tällöin $f(a), f(b) \in I'$. Koska I' on renkaan R' ideaali, niin $f(a) \oplus (-f(b)) \in I'$. Koska f on rengashomomorfismi, niin

   $$f(a - b) = f(a + (-b)) = f(a) \oplus f(-b) = f(a) \oplus (-f(b)) \in I'.$$

   Näin ollen $a - b \in f^{-1}(I')$. Siispä $(f^{-1}(I'), +) \leq (R, +)$.

   (b) Olkoon $a \in f^{-1}(I')$ ja $r \in R$. Tällöin $f(a) \in I'$ ja $f(r) \in R'$. Koska I' on renkaan R' ideaali, niin $f(a) \odot f(r) \in I'$ ja $f(r) \odot f(a) \in I'$. Koska f on rengashomomorfismi, niin

   $$f(a \cdot r) = f(a) \odot f(r) \in I'$$

   ja

   $$f(r \cdot a) = f(r) \odot f(a) \in I'.$$

   Siispä $a \cdot r,\ r \cdot a \in f^{-1}(I')$.

Kohtien (a) ja (b) nojalla $f^{-1}(I')$ on renkaan R ideaali.

Määritelmä 2.4.4. Rengashomomorfismia $f : R \to R'$ sanotaan *rengasisomorfismiksi* (ring isomorphism), jos f on bijektio. Rengasta R sanotaan *isomorfiseksi* renkaan R' kanssa, jos on olemassa jokin isomorfismi $R \to R'$. Tällöin merkitään $R \cong R'$.

Huomautus. Erikoistapauksissa homomorfismeilla on omat nimensä:

- *monomorfismi* = injektiivinen homomorfismi,
- *epimorfismi* = surjektiivinen homomorfismi,
- *endomorfismi* = homomorfismi joukolta itselleen,
- *automorfismi* = isomorfismi joukolta itselleen.

Määritelmä 2.4.5. Olkoon $f : R \to R'$ rengashomomorfismi. Homomorfismin f *ydin* (kernel) on joukko

$$Ker(f) = \{r \in R \mid f(r) = \mathbf{0}_{R'}\}.$$

Homomorfismin f *kuva* (image) on joukko

$$Im(f) = \{f(r) \mid r \in R\}.$$

Lause 2.4.6. *Jos $f : R \to R'$ on rengashomomorfismi, niin*

1. *$Ker(f)$ on renkaan R ideaali,*
2. *$Im(f)$ on renkaan R' alirengas.*

Todistus.

1. Koska $Ker(f) = f^{-1}(\{\mathbf{0}_{R'}\})$ ja $\{\mathbf{0}_{R'}\}$ on renkaan R' ideaali, niin lauseen 2.4.3 kohdan 4 nojalla $Ker(f)$ on renkaan R ideaali.
2. Koska $Im(f) = f(R)$ ja R on renkaan R alirengas, niin lauseen 2.4.3 kohdan 1 nojalla $Im(f)$ on renkaan R' alirengas.

Lause 2.4.7 (Renkaiden homomorfismilause)**.** *Jos $f : (R, +, \cdot) \to (R', \oplus, \odot)$ on rengashomomorfismi, niin*

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

Todistus. Olkoon $f : (R, +, \cdot) \to (R', \oplus, \odot)$ rengashomomorfismi ja merkitään $K = Ker(f)$. Määritellään kuvaus $F : R/K \to Im(f)$ siten, että

$$F(a + K) = f(a)$$

kaikilla $a \in R$. Osoitetaan, että kuvaus on hyvinmääritelty. Olkoon $a, b \in R$ ja $a + K = b + K$. Tällöin $b \in a + K$ eli $b = a + k$ jollakin $k \in K$. Koska f on ryhmähomomorfismi ja $k \in K = Ker(f)$, niin

$$F(b+K) = f(b) = f(a+k) = f(a) \oplus f(k) = f(a) \oplus \mathbf{0}_{R'} = f(a) = F(a+K).$$

Siis jos $a+K = b+K$, niin $F(a+K) = F(b+K)$, joten F on hyvinmääritelty.

1. Olkoon $x \in Im(f)$. Tällöin on olemassa sellainen $a \in R$, että $x = f(a)$. Nyt
$$x = f(a) = F(a + K),$$
missä $a + K \in R/K$, joten $F : R/K \to Im(f)$ on surjektio.

2. Olkoon $a+K, b+K \in R/K$ ja $F(a+K) = F(b+K)$. Tällöin kuvauksen F määritelmän mukaan $f(a) = f(b)$, joten koska f on rengashomomorfismi, niin
$$\mathbf{0}_{R'} = f(a) \oplus (-f(b)) = f(a) \oplus f(-b) = f(a - b).$$
Siispä $a - b \in K$. Näin ollen $(a - b) + K = K$, josta saadaan lisäämällä puolittain $b + K$, että
$$(b + K) + ((a - b) + K) = b + K$$
eli $a + K = b + K$. Näin ollen F on injektio.

3. (a) Olkoon $a + K, b + K \in R/K$. Koska f on rengashomomorfismi, niin
$$\begin{aligned} F((a + K) + (b + K)) &= F((a + b) + K) = f(a + b) = f(a) \oplus f(b) \\ &= F(a + K) \oplus F(b + K). \end{aligned}$$

   (b) Olkoon $a + K, b + K \in R/K$. Koska f on rengashomomorfismi, niin
$$\begin{aligned} F((a + K)(b + K)) &= F((ab) + K) = f(ab) = f(a) \odot f(b) \\ &= F(a + K) \odot F(b + K). \end{aligned}$$

(c) Nyt $\mathbf{1}_R + K$ on tekijärenkaan R/K ykkösalkio, ja $\mathbf{1}_{R'}$ on myös renkaan R' alirenkaan $Im(f)$ ykkösalkio. Koska f on rengashomomorfisimi, niin

$$F(\mathbf{1}_R + K) = f(\mathbf{1}_R) = \mathbf{1}_{R'}$$

Kohtien (a)–(c) nojalla F on rengashomomorfismi $R/K \to Im(f)$.

Kohtien 1–3 nojalla F on rengasisomorfismi $R/K \to Im(f)$ ja näin ollen $R/Ker(f) \cong Im(f)$.

Määritelmä 2.4.8. Olkoon $(R, +, \cdot)$ rengas ja $a \in R$. Kun n on positiivinen kokonaisluku, niin merkintä na on lyhennysmerkintä summalle $a + \ldots + a$, missä alkioita a on n kappaletta. Alkio na on renkaan alkion a n. *monikerta*. Ykkösalkiota käyttäen voidaan alkio na esittää renkaan operaationa, nimittäin $na = (n\mathbf{1}) \cdot a = (\mathbf{1} + \ldots + \mathbf{1}) \cdot a$. Negatiivisilla kokonaisluvun n arvoilla alkio na on alkion $|n|a$ vasta-alkio eli $na = -a + (-a) + (-a) + \ldots + (-a)$, missä alkioita $-a$ on n kappaletta.

Lause 2.4.9. *Olkoot m ja n kokonaislukuja. Tällöin renkaan $(R, +, \cdot)$ alkiot toteuttavat seuravat laskulait:*

1. $(m + n)a = ma + na$,
2. $(mn)a = m(na)$,
3. $n(a + b) = na + nb$,
4. $n(a \cdot b) = (na) \cdot b = a \cdot (nb)$,
5. $(na) \cdot (mb) = (nm)(a \cdot b)$,

aina, kun $m, n \in \mathbb{Z}$ ja $a, b \in R$.

Todistus. Harjoitustehtävä.

2.5 Kokonaisalue

Määritelmä 2.5.1. Renkaan $(R, +, \cdot)$ nolla-alkiosta eroava alkio a on renkaan R *nollanjakaja*, jos renkaassa R on sellainen nolla-alkiosta eroava alkio b, että $\quad ab = \mathbf{0} \quad$ tai $\quad ba = \mathbf{0}$.

Määritelmä 2.5.2. Kommutatiivista rengasta, jossa ei ole nollanjakajia, sanotaan *kokonaisalueeksi*.

Esimerkki.

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

Lause 2.5.3. *Olkoon $(R, +, \cdot)$ kokonaisalue ja $a \in R$, $a \neq \mathbf{0}$. Tällöin*

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

Todistus. Luennolla.

3 Kuntien teoriaa

Määritelmä 3.1. Kommutatiivista rengasta $(K, +, \cdot)$ sanotaan *kunnaksi* (field), mikäli $(K \setminus \{\mathbf{0}\}, \cdot)$ on Abelin ryhmä. Ryhmä $(K \setminus \{\mathbf{0}\}, \cdot)$ on kunnan *multiplikatiivinen ryhmä* ja ryhmä $(K, +)$ on kunnan *additiivinen ryhmä*.

Toisin sanoen $(K, +, \cdot)$ on kunta, jos seuraavat ehdot toteutuvat.

1. $(K, +)$ on Abelin ryhmä:
   - $(+)$ on binäärinen operaatio joukossa K eli $a + b \in K$ kaikilla $a, b \in K$.
   - $(+)$ on assosiatiivinen operaatio eli $a+(b+c) = (a+b)+c$ kaikilla $a, b, c \in K$.
   - On olemassa nolla-alkio $\mathbf{0} \in K$, jolle $\mathbf{0} + a = a + \mathbf{0} = a$ kaikilla $a \in K$.
   - Jokaiselle $a \in K$ on olemassa vasta-alkio $-a \in K$, jolle pätee $a + (-a) = -a + a = \mathbf{0}$.
   - $(+)$ on kommutatiivinen operaatio eli $a+b = b+a$ kaikilla $a, b \in K$.
2. Operaatiolle $(\cdot)$ pätevät seuraavat ehdot:
   - $(\cdot)$ on binäärinen operaatio joukossa K eli $a \cdot b \in K$ kaikilla $a, b \in K$.
   - $(\cdot)$ on assosiatiivinen operaatio eli $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ kaikilla $a, b, c \in K$.
   - On olemassa ykkösalkio $\mathbf{1} \in K$, jolle $\mathbf{1} \cdot a = a \cdot \mathbf{1} = a$ kaikilla $a \in K$.
   - Jokaiselle $a \in K \setminus \{\mathbf{0}\}$ on olemassa käänteisalkio $a^{-1} \in K \setminus \{\mathbf{0}\}$, jolle pätee $a \cdot a^{-1} = a^{-1} \cdot a = \mathbf{1}$.
   - $(\cdot)$ on kommutatiivinen operaatio eli $a \cdot b = b \cdot a$ kaikilla $a, b \in K$.
3. Osittelulait pätevät:
   - $a \cdot (b + c) = a \cdot b + a \cdot c$ kaikilla $a, b, c \in K$.
   - $(a + b) \cdot c = a \cdot c + b \cdot c$ kaikilla $a, b, c \in K$.

Huomautus. Olkoon $(K, +, \cdot)$ kommutatiivinen rengas. Mikäli tällöin jokaiselle $a \in K \setminus \{\mathbf{0}\}$ on olemassa käänteisalkio $a^{-1} \in K \setminus \{\mathbf{0}\}$, niin tällöin $(\cdot)$ on binäärinen operaatio joukossa $K \setminus \{\mathbf{0}\}$.

Lause 3.2. *Jäännösluokkarengas $(\mathbb{Z}_n, +, \cdot)$ on kunta tarkalleen silloin, kun n on alkuluku.*

Todistus. Luennolla.

Määritelmä 3.3. Kunnan $(K, +, \cdot)$ osajoukko $F \neq \emptyset$ on kunnan K *alikunta*, jos $(F, +, \cdot)$ on kunta.

Lause 3.4 (Alikuntakriteeri)**.** *Kunnan $(K, +, \cdot)$ osajoukko $F \neq \emptyset$ on kunnan K alikunta jos ja vain jos seuraavat ehdot pätevät:*

1. *Osajoukossa F on vähintään kaksi alkiota,*
2. *$a - b = a + (-b) \in F$ kaikilla $a, b \in F$ ja*
3. *$\frac{a}{b} = a \cdot b^{-1} \in F$ kaikilla $a, b \in F, b \neq \mathbf{0}$.*

Todistus. Luennolla.

Määritelmä 3.5. Jos $(K, +, \cdot)$ ja $(K', \oplus, \odot)$ ovat kuntia, niin rengashomomorfismia $f : K \to K'$ sanotaan *kuntahomomorfismiksi*. Rengasisomorfismia $f : K \to K'$ sanotaan *kuntaisomorfismiksi*.

Määritelmä 3.6. Äärellisen kunnan $(K, +, \cdot)$ ykkösalkion $\mathbf{1}$ additiivista kertalukua sanotaan kunnan *karakteristikaksi*, merkitään $\operatorname{char} K$. Siis $\operatorname{char} K$ on pienin positiivinen kokonaisluku n, joka toteuttaa ehdon $n\mathbf{1} = \mathbf{0}$ ($\operatorname{char} K$ on siis alkion $\mathbf{1}$ kertaluku ryhmässä $(K, +)$).

Huomautus. Karakteristika voidaan määritellä näin jo kokonaisalueen tapauksessa.

Lause 3.7.

1. *Äärellisen kunnan karakteristika on välttämättä alkuluku.*
2. *Jos kunnan $(K, +, \cdot)$ karakteristika on alkuluku p ja $a \in K$, niin $pa = \mathbf{0}$.*

Todistus. Luennolla.

Lause 3.8. *Jokaisen äärellisen kunnan $(K, +, \cdot)$ kertaluku on p^n, missä p on alkuluku ja $n \geq 1$. Tällöin* char $K = p$. *Lisäksi samaa kertalukua olevat kunnat ovat keskenään isomorfisia.*

Todistus. Todistus kurssilla *Permutaatiot, kunnat ja Galois'n teoria.*

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

Tutkitaan lopuksi hieman renkaiden ja kuntien välistä suhdetta.

Lause 3.9. *Kunnan $(K, +, \cdot)$ ainoat ideaalit ovat $(\mathbf{0})$ ja K.*

Todistus. Luennolla.

Lause 3.10. *Olkoon $(R, +, \cdot)$ kommutatiivinen rengas, jonka ainoat ideaalit ovat $(\mathbf{0})$ ja R (triviaalit ideaalit). Tällöin $(R, +, \cdot)$ on kunta.*

Todistus. Luennolla.

Kommutatiivisesta renkaasta voidaan aina laajentaa kunta sen maksimaalisen ideaalin avulla seuraavalla tavalla:

Lause 3.11 (Kuntalaajennuslause)**.** *Olkoon $(R, +, \cdot)$ kommutatiivinen rengas ja M renkaan R maksimaalinen ideaali. Tällöin tekijärengas R/M on kunta.*

Todistus. Koska R on kommutatiivinen rengas, niin R/M on myös kommutatiivinen rengas. Osoitetaan, että $(R/M \setminus \{\mathbf{0} + M\}, \cdot)$ on Abelin ryhmä. Koska R/M on kommutatiivinen rengas, riittää osoittaa, että jokaiselle tekijärenkaan nolla-alkiosta eroavalle alkiolle on olemassa käänteisalkio joukossa $R/M \setminus \{\mathbf{0} + M\}$.

Olkoon $a + M \in R/M$ ja $a + M \neq \mathbf{0} + M$. Tällöin $a \notin \mathbf{0} + M = M$, joten $(a) \neq M$. Lauseen 2.2.3 nojalla $M + (a)$ on renkaan R ideaali ja $M \subset M + (a)$.

Koska M on renkaan R maksimaalinen ideaali, niin $M + (a) = R$, ja edelleen lauseen 2.2.5 nojalla $R = M + Ra$.

Nyt $\mathbf{1} \in R$ eli $\mathbf{1} \in M + Ra$, joten $\mathbf{1} = m + ra$ joillakin $m \in M$ ja $r \in R$. Tällöin tekijärenkaan R/M ykkösalkio

$$\begin{aligned}\mathbf{1} + M &= (m + ra) + M = (m + M) + (ra + M) = (\mathbf{0} + M) + (ra + M) \\ &= ra + M = (r + M) \cdot (a + M).\end{aligned}$$

Koska tekijärengas R/M on kommutatiivinen, niin myös

$$(a + M) \cdot (r + M) = \mathbf{1} + M.$$

Näin ollen $r+M$ on alkion $a+M$ käänteisalkio ja luonnollisesti $r+M \neq \mathbf{0}+M$.

Käänteisalkion olemassaolon seurauksena sivuluokkien tulo on binäärinen operaatio joukossa $R/M \setminus \{\mathbf{0} + M\}$ ja näin ollen $(R/M \setminus \{\mathbf{0} + M\}, \cdot)$ on Abelin ryhmä. Siispä tekijärengas $(R/M, +, \cdot)$ on kunta.

Huomautus. Kunta $(K, +, \cdot)$ on aina kokonaisalue.

4 Polynomirengas

4.1 Polynomirenkaan teoriaa

Määritelmä 4.1.1. Olkoon $(K, +, \cdot)$ kunta. Merkitään

$$K[x] = \left\{ a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \mid a_i \in K, n \geq 0 \right\}.$$

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

Huomautus. Polynomirengas $(K[x], +, \cdot)$ on rakenteeltaan kommutatiivinen rengas.

- Nolla-alkio on nollapolynomi $f(x) = \mathbf{0}$, $\mathbf{0} \in K$.
- Ykkösalkio on vakiopolynomi $g(x) = \mathbf{1}$, $\mathbf{1} \in K$.

Määritelmä 4.1.2. Olkoon K kunta. Jos

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \in K[x]$$

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

Määritelmä 4.1.3. Olkoon $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0$ polynomirenkaan $K[x]$ polynomi ja $a_n \neq \mathbf{0}$. Tällöin kerroin a_n on polynomin $f(x)$ *johtava kerroin.*
Polynomia $f(x)$ sanotaan *pääpolynomiksi* (principal polynomial), jos sen johtava kerroin on kunnan $(K, +, \cdot)$ ykkösalkio.

Lause 4.1.4. *Jos $f(x), g(x) \in K[x]$, niin*

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

Todistus. Luennolla

Lause 4.1.5 (Jakoalgoritmi polynomeille)**.** *Mikäli* $f(x), g(x) \in K[x]$ *sekä* $g(x) \neq \mathbf{0}$ *(nollapolynomi), niin on olemassa sellaiset yksikäsitteiset polynomit* $q(x), r(x) \in K[x]$*, että*

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

ja $\deg\ r(x) < \deg\ g(x)$.

Todistus. Olkoon $f(x), g(x) \in K[x]$ ja $g(x) \neq \mathbf{0}$.

1. Olemassaolo. Tarkastellaan joukkoa

   $$S = \{f(x) - s(x)g(x) \mid s(x) \in K[x]\}.$$

   Selvästi $\emptyset \neq S \subseteq K[x]$. Olkoon $r(x) \in S$ polynomi, jonka aste on mahdollisimman pieni. Nyt $r(x) = f(x) - q(x)g(x)$ jollakin $q(x) \in K[x]$ eli $f(x) = q(x)g(x) + r(x)$. Osoitetaan, että $\deg\ r(x) < \deg\ g(x)$.

   Vastaoletus: $\deg\ r(x) \geq \deg\ g(x)$. Merkitään $r(x) = r_n x^n + \ldots + r_0$ ja $g(x) = b_m x^m + \ldots + b_0$, missä $r_n \neq \mathbf{0}$ ja $b_m \neq \mathbf{0}$. Vastaoletuksen nojalla $n \geq m$. Tällöin $k(x) = b_m^{-1} r_n x^{n-m} \in K[x]$. Olkoon

   $$\begin{aligned} t(x) &= r(x) - k(x)g(x) \\ &= r_n x^n + \ldots + r_0 - b_m^{-1} r_n x^{n-m}(b_m x^m + \ldots + b_0) \\ &= r_n x^n + \ldots + r_0 - (r_n x^n + \ldots + b_m^{-1} r_n b_0 x^{n-m}). \end{aligned}$$

   Siis $\deg\ t(x) < n$ eli $\deg\ t(x) < \deg\ r(x)$. Toisaalta

   $$\begin{aligned} t(x) &= r(x) - k(x)g(x) = f(x) - q(x)g(x) - k(x)g(x) \\ &= f(x) - [q(x) + k(x)]g(x) \in S, \end{aligned}$$

   mikä on ristiriita polynomin $r(x)$ valinnan kanssa. Siispä vastaoletus on väärä, joten $\deg\ r(x) < \deg\ g(x)$.

2. Yksikäsitteisyys. Oletetaan, että $f(x) = q(x)g(x) + r(x)$ voidaan esittää myös muodossa $f(x) = q'(x)g(x) + r'(x)$, missä $q'(x), r'(x) \in K[x]$ ja $\deg\ r'(x) < \deg\ g(x)$. Selvästi $\deg\ (r(x) - r'(x)) < \deg\ g(x)$. Toisaalta

   $$\begin{aligned} r(x) - r'(x) &= (f(x) - q(x)g(x)) - (f(x) - q'(x)g(x)) \\ &= [q'(x) - q(x)]g(x). \end{aligned}$$

   Siten $\deg\ (r(x) - r'(x)) = \deg\ (q'(x) - q(x)) + \deg\ g(x)$. Tämä on mahdollista vain, kun $\deg\ (q'(x) - q(x)) = -\infty$, joten $q'(x) - q(x) = \mathbf{0}$ eli $q'(x) = q(x)$. Tällöin myös $r(x) - r'(x) = \mathbf{0} \cdot g(x) = \mathbf{0}$ eli $r(x) = r'(x)$.

Määritelmä 4.1.6. Jos $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in K[x]$ ja $\alpha \in K$ sekä

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

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

Huomautus. Polynomirenkaan $K[x]$ 1. asteen polynomilla on aina nollakohta kunnassa K.

Määritelmä 4.1.7. Jos $f(x), g(x) \in K[x]$ ja

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

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

Lause 4.1.8. *Olkoot $f(x) \in K[x]$ ja $\alpha \in K$. Tällöin*

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

Todistus. Luennolla

Määritelmä 4.1.9. Polynomi $f(x) \in K[x]$ on *jaoton* (irreducible) polynomirenkaassa $K[x]$, mikäli deg $f(x) \geq 1$ ja polynomia f ei voida esittää kahden positiivista astetta olevan polynomin tulona polynomirenkaassa $K[x]$.

Lause 4.1.10. *Olkoon $f(x) \in K[x]$ ja* deg $f(x) = 2$ *tai* deg $f(x) = 3$. *Tällöin $f(x)$ on jaoton jos ja vain jos sillä ei ole nollakohtaa kunnassa K.*

Todistus. Luennolla

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

Lause 4.1.11. *Olkoon $f(x) \in K[x]$. Jos* deg $f(x) = n$, *niin polynomilla $f(x)$ on korkeintaan n nollakohtaa kunnassa K.*

Todistus. Luennolla

Huomautus. Olkoon $(K, +, \cdot)$ kunta. Tällöin $K[x]$ on kommutatiivinen rengas. Jos $f(x) \in K[x]$, niin Lauseen 2.2.5 nojalla

$$(f(x)) = K[x] \cdot f(x) = \{k(x) \cdot f(x) \mid k(x) \in K[x]\}.$$

Lause 4.1.12. *Olkoon K kunta. Polynomirenkaan $K[x]$ jokainen ideaali on pääideaali.*

Todistus. Luennolla.

Huomautus. Jos I on polynomirenkaan $(K[x], +, \cdot)$ ideaali, niin $I = (f(x))$, missä $f(x)$ on jokin pääpolynomi.

Lause 4.1.13. *Jos $p(x) \in K[x]$ on jaoton polynomi, niin $(p(x))$ on renkaan $K[x]$ maksimaalinen ideaali.*

Todistus. Luennolla.

Seuraus 4.1.14. *Jos K on kunta ja $p(x)$ on polynomirenkaan $K[x]$ jaoton polynomi, niin tekijärengas $K[x]/(p(x))$ on kunta.*

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

4.2 Polynomien suurin yhteinen tekijä

Määritelmä 4.2.1. Olkoon $f(x), g(x) \in K[x]$ polynomeja, joista ainakin toinen on nolla-alkiosta eroava. Polynomien $f(x)$ ja $g(x)$ *suurin yhteinen tekijä* (greatest common divisor) $\text{syt}(f(x), g(x))$ on polynomi $d(x) \in K[x]$, joka toteuttaa seuraavat ehdot:

1. $d(x)$ on pääpolynomi.
2. $d(x) \mid f(x)$ ja $d(x) \mid g(x)$.
3. Jos $h(x) \mid f(x)$ ja $h(x) \mid g(x)$, niin $h(x) \mid d(x)$.

Lause 4.2.2. *Jos $f(x), g(x) \in K[x]$, $f(x) \neq \mathbf{0}$ ja $g(x) \neq \mathbf{0}$, niin suurin yhteinen tekijä $\text{syt}(f(x), g(x)) = d(x) \in K[x]$ on olemassa ja se on yksikäsitteinen. Lisäksi tällöin on olemassa sellaiset polynomit $a(x), b(x) \in K[x]$, että $d(x) = \text{syt}(f(x), g(x)) = a(x)f(x) + b(x)g(x)$.*

Todistus. Olkoon $f(x), g(x) \in K[x]$, $f(x) \neq \mathbf{0}$, $g(x) \neq \mathbf{0}$ ja

$$I = \{r(x)f(x) + s(x)g(x) \mid r(x), s(x) \in K[x]\}.$$

Selvästi I on polynomirenkaan $K[x]$ epätyhjä osajoukko. Osoitetaan, että I on renkaan $K[x]$ ideaali.

1. Olkoon $i_1(x), i_2(x) \in I$, jolloin

$$i_1(x) = r_1(x)f(x) + s_1(x)g(x)$$

ja

$$i_2(x) = r_2(x)f(x) + s_2(x)g(x)$$

joillakin $r_1(x), r_2(x), s_1(x), s_2(x) \in K[x]$. Tällöin

$$i_1(x) - i_2(x) = [r_1(x) - r_2(x)]f(x) + [s_1(x) - s_2(x)]g(x) \in I,$$

joten $(I, +) \leq (K[x], +)$.

2. Olkoon $i(x) \in I$ ja $k(x) \in K[x]$. Nyt $i(x) = r(x)f(x)+s(x)g(x)$ joillakin $r(x), s(x) \in K[x]$, jolloin

$$k(x)i(x) = [k(x)r(x)]f(x) + [k(x)s(x)]g(x) \in I.$$

Lisäksi $i(x)k(x) = k(x)i(x) \in I$, sillä $K[x]$ on kommutatiivinen rengas.

Kohtien 1 ja 2 nojalla I on polynomirenkaan $K[x]$ ideaali.

Lauseen 4.1.12 ja sen huomautuksen nojalla on olemassa sellainen pääpolynomi $d(x) \in K[x]$, että $I = (d(x))$. Koska

$$f(x), g(x) \in I = (d(x)) = K[x] \cdot d(x),$$

niin $d(x) \mid f(x)$ ja $d(x) \mid g(x)$. Polynomi $d(x)$ on siis polynomien $f(x)$ ja $g(x)$ yhteinen tekijä. Koska $d(x) \in I$, niin on olemassa sellaiset $a(x), b(x) \in K[x]$, että

$$d(x) = a(x)f(x) + b(x)g(x).$$

Jos $h(x) \mid f(x)$ ja $h(x) \mid g(x)$, niin $h(x) \mid a(x)f(x)$ ja $h(x) \mid b(x)g(x)$, ja siten

$$h(x) \mid a(x)f(x) + b(x)g(x)$$

eli $h(x) \mid d(x)$. Näin ollen $d(x) = \text{syt}(f(x), g(x))$.

Osoitetaan vielä suurimman yhteisen tekijän yksikäsitteisyys. Olkoon siis $d(x) = \text{syt}(f(x), g(x))$ ja $d'(x) = \text{syt}(f(x), g(x))$. Koska $d(x)$ on syt, niin määritelmän 4.2.1 nojalla $d'(x) \mid d(x)$. Toisaalta, koska $d'(x)$ on syt, niin $d(x) \mid d'(x)$. Koska sekä $d(x)$ että $d'(x)$ ovat pääpolynomeja, niin $d(x) = d'(x)$.

Polynomien $f(x)$ ja $g(x)$ suurin yhteinen tekijä saadaan määrättyä käyttämällä samanlaista menettelyä kuin kokonaislukujen tapauksessa. Prosessi tunnetaan **Eukleideen algoritmina**. Menetelmässä sovelletaan jakoalgoritmia toistuvasti.

Oletetaan, että $f(x) \neq \mathbf{0}$ ja $g(x) \neq \mathbf{0}$. Nyt

$$
\begin{aligned}
&g(x) = q_0(x) \cdot f(x) + r_1(x), \text{ missä } 0 \leq \deg r_1(x) < \deg f(x)\\
&f(x) = q_1(x) \cdot r_1(x) + r_2(x), \text{ missä } 0 \leq \deg r_2(x) < \deg r_1(x)\\
&r_1(x) = q_2(x) \cdot r_2(x) + r_3(x), \text{ missä } 0 \leq \deg r_3(x) < \deg r_2(x)\\
&r_2(x) = q_3(x) \cdot r_3(x) + r_4(x), \text{ missä } 0 \leq \deg r_4(x) < \deg r_3(x)\\
&\vdots\\
&r_k(x) = q_{k+1}(x) \cdot r_{k+1}(x) + r_{k+2}(x), \text{ missä } 0 \leq \deg r_{k+2}(x) < \deg r_{k+1}(x)\\
&r_{k+1}(x) = q_{k+2}(x) \cdot r_{k+2}(x).
\end{aligned}
$$

Tällöin viimeinen jakaja $r_{k+2}(x)$ on polynomien $f(x)$ ja $g(x)$ suurin yhteinen tekijä. Edellistä yhtälöryhmää takautuvasti käyttämällä polynomien $f(x)$ ja $g(x)$ suurin yhteinen tekijä $d(x) = r_{k+2}(x)$ voidaan kirjoittaa muodossa $d(x) = a(x)f(x) + b(x)g(x)$.

Määritelmä 4.2.3. Jos polynomien $f(x)$ ja $g(x) \in K[x]$ suurin yhteinen tekijä on $\mathbf{1}$, niin sanotaan, että $f(x)$ ja $g(x)$ ovat *keskenään jaottomia polynomeja* (relatively prime polynomials).

Lause 4.2.4. *Jos $f(x), g(x) \in K[x]$ ovat keskenään jaottomia polynomeja, niin $a(x)f(x) + b(x)g(x) = \mathbf{1}$ joillakin $a(x), b(x) \in K[x]$.*
Kääntäen, jos $a(x)f(x) + b(x)g(x) = \mathbf{1}$ joillakin $a(x), b(x) \in K[x]$, niin $f(x)$ ja $g(x)$ ovat keskenään jaottomia.

Todistus. Luennolla.

Lause 4.2.5. *Jos $q(x)$ ja $f(x)$ ovat keskenään jaottomia polynomeja, ja $q(x) \mid f(x)g(x)$, niin tällöin $q(x) \mid g(x)$.*

Todistus. Luennolla.

5 Osamääräkunta

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

Määritelmä 5.1. Olkoon $(D, +, \cdot)$ kokonaisalue ja $a, b, c, d \in D$, $b \neq \mathbf{0}$, $d \neq \mathbf{0}$. Asetetaan relaatio

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

Lause 5.2. *Relaatio $\sim$ on ekvivalenssirelaatio joukossa*

$$\mathcal{D} = D \times (D \setminus \{\mathbf{0}\}) = \{(a, b) \mid a \in D, b \in D \setminus \{\mathbf{0}\}\}.$$

Todistus. Olkoon $a, c, e \in D$ ja $b, d, f \in D \setminus \{\mathbf{0}\}$.

1. Nyt $(a, b) \sim (a, b)$, sillä $ab = ba$, koska D on kommutatiivinen rengas.
2. Olkoon $(a, b) \sim (c, d)$ eli $ad = bc$. Tällöin $cb = da$, joten $(c, d) \sim (a, b)$.
3. Olkoon $(a, b) \sim (c, d)$ ja $(c, d) \sim (e, f)$ eli $ad = bc$ ja $cf = de$. Tällöin $adcf = bcde$ eli $afdc = bedc$, joten lauseen 2.5.3 nojalla $af = be$. Siispä $(a, b) \sim (e, f)$.

Määritelmä 5.3. Ekvivalenssiluokille

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

sovitaan yhteenlasku

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

ja kertolasku

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

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

Merkitään vielä

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

Tällöin laskutoimitukset voidaan kirjoittaa muodossa

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2}$$

ja

$$\frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2}$$

kaikilla $\frac{a_1}{b_1}, \frac{a_2}{b_2} \in Q(D)$.

Lisäksi suoraan määritelmästä seuraa, että supistamis- ja laventamislait

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

ovat voimassa.

Lause 5.4. *Kolmikko* $(Q(D), +, \cdot)$ *on kunta.*

Todistus. Osoitetaan, että määritelmän 3.1 ehdot toteutuvat.

1. (a) Olkoon $\frac{a}{b}, \frac{c}{d} \in Q(D)$. Tällöin

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd} \in Q(D).$$

   (b) Olkoon $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in Q(D)$. Tällöin

$$\begin{aligned} \frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right) &= \frac{a}{b} + \left(\frac{cf + ed}{df}\right) = \frac{a(df) + (cf + ed)b}{b(df)} \\ &= \frac{(ad + cb)f + e(bd)}{(bd)f} = \left(\frac{ad + cb}{bd}\right) + \frac{e}{f} \\ &= \left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f}. \end{aligned}$$

   (c) Nyt $\frac{\mathbf{0}}{\mathbf{1}} \in Q(D)$ ja

$$\frac{\mathbf{0}}{\mathbf{1}} + \frac{a}{b} = \frac{\mathbf{0}b + a\mathbf{1}}{\mathbf{1}b} = \frac{a}{b} \quad \text{sekä} \quad \frac{a}{b} + \frac{\mathbf{0}}{\mathbf{1}} = \frac{a\mathbf{1} + \mathbf{0}b}{b\mathbf{1}} = \frac{a}{b}$$

   kaikilla $\frac{a}{b} \in Q(D)$, joten nolla-alkio on $\frac{\mathbf{0}}{\mathbf{1}}$. Lisäksi

$$\frac{\mathbf{0}}{\mathbf{1}} = [\mathbf{0}, \mathbf{1}] = [\mathbf{0}, a] = \frac{\mathbf{0}}{a}$$

   kaikilla $a \in D \setminus \{\mathbf{0}\}$, sillä $\mathbf{0}a = \mathbf{0} = \mathbf{0} \cdot \mathbf{1}$ eli $(\mathbf{0}, a) \sim (\mathbf{0}, \mathbf{1})$ kaikilla $a \in D \setminus \{\mathbf{0}\}$.

(d) Olkoon $\frac{a}{b} \in Q(D)$. Tällöin $\frac{-a}{b} \in Q(D)$ ja

$$\frac{a}{b} + \frac{-a}{b} = \frac{ab + (-a)b}{b^2} = \frac{ab - ab}{b^2} = \frac{\mathbf{0}}{b^2} = \frac{\mathbf{0}}{\mathbf{1}}$$

sekä

$$\frac{-a}{b} + \frac{a}{b} = \frac{(-a)b + ab}{b^2} = \frac{-ab + ab}{b^2} = \frac{\mathbf{0}}{b^2} = \frac{\mathbf{0}}{\mathbf{1}},$$

joten alkion $\frac{a}{b} = [a, b]$ vasta-alkio on

$$-\frac{a}{b} = \frac{-a}{b} \quad \text{eli} \quad -[a, b] = [-a, b].$$

(e) Olkoon $\frac{a}{b}, \frac{c}{d} \in Q(D)$. Tällöin

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd} = \frac{cb + ad}{db} = \frac{c}{d} + \frac{a}{b}.$$

2. (a) Olkoon $\frac{a}{b}, \frac{c}{d} \in Q(D)$. Tällöin

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \in Q(D).$$

(b) Olkoon $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in Q(D)$. Tällöin

$$\begin{aligned} \frac{a}{b} \cdot \left(\frac{c}{d} \cdot \frac{e}{f}\right) = \frac{a}{b} \cdot \left(\frac{ce}{df}\right) = \frac{a(ce)}{b(df)} = \frac{(ac)e}{(bd)f} \\ = \left(\frac{ac}{bd}\right) \cdot \frac{e}{f} = \left(\frac{a}{b} \cdot \frac{c}{d}\right) \cdot \frac{e}{f}. \end{aligned}$$

(c) Nyt $\frac{\mathbf{1}}{\mathbf{1}} \in Q(D)$ ja

$$\frac{\mathbf{1}}{\mathbf{1}} \cdot \frac{a}{b} = \frac{\mathbf{1}a}{\mathbf{1}b} = \frac{a}{b} \quad \text{sekä} \quad \frac{a}{b} \cdot \frac{\mathbf{1}}{\mathbf{1}} = \frac{a\mathbf{1}}{b\mathbf{1}} = \frac{a}{b}$$

kaikilla $\frac{a}{b} \in Q(D)$, joten ykkösalkio on $\frac{\mathbf{1}}{\mathbf{1}}$. Lisäksi

$$\frac{\mathbf{1}}{\mathbf{1}} = [\mathbf{1}, \mathbf{1}] = [a, a] = \frac{a}{a}$$

kaikilla $a \in D \setminus \{\mathbf{0}\}$, sillä $\mathbf{1}a = a = a\mathbf{1}$ eli $(a, a) \sim (\mathbf{1}, \mathbf{1})$ kaikilla $a \in D \setminus \{\mathbf{0}\}$.

(d) Olkoon $\frac{a}{b} \in Q(D) \setminus \left\{\frac{\mathbf{0}}{\mathbf{1}}\right\}$. Tällöin $\frac{b}{a} \in Q(D) \setminus \left\{\frac{\mathbf{0}}{\mathbf{1}}\right\}$ ja

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{ab}{ab} = \frac{\mathbf{1}}{\mathbf{1}} \text{ sekä } \frac{b}{a} \cdot \frac{a}{b} = \frac{ba}{ab} = \frac{ba}{ba} = \frac{\mathbf{1}}{\mathbf{1}},$$

joten alkion $\frac{a}{b} = [a, b]$ käänteisalkio on

$$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a} \text{ eli } [a, b]^{-1} = [b, a].$$

(e) Olkoon $\frac{a}{b}, \frac{c}{d} \in Q(D)$. Tällöin

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} = \frac{ca}{db} = \frac{c}{d} \cdot \frac{a}{b}.$$

3. Olkoon $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in Q(D)$. Tällöin

$$\begin{aligned}\frac{a}{b} \cdot \left(\frac{c}{d} + \frac{e}{f}\right) &= \frac{a}{b} \cdot \left(\frac{cf + ed}{df}\right) = \frac{a(cf + ed)}{b(df)} = \frac{acf + aed}{bdf} \\ &= \frac{(ac)(bf) + (ae)(bd)}{(bd)(bf)} = \frac{ac}{bd} + \frac{ae}{bf} = \frac{a}{b} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{e}{f}\end{aligned}$$

ja

$$\begin{aligned}\left(\frac{a}{b} + \frac{c}{d}\right) \cdot \frac{e}{f} &= \left(\frac{ad + cb}{bd}\right) \cdot \frac{e}{f} = \frac{(ad + cb)e}{(bd)f} = \frac{ade + cbe}{bdf} \\ &= \frac{(ae)(df) + (ce)(bf)}{(bf)(df)} = \frac{ae}{bf} + \frac{ce}{df} = \frac{a}{b} \cdot \frac{e}{f} + \frac{c}{d} \cdot \frac{e}{f}.\end{aligned}$$

Kohtien 1-3 nojalla $(Q(D), +, \cdot)$ on kunta.

Määritelmä 5.5. Olkoon $(D, +, \cdot)$ kokonaisalue. Tällöin kunta $Q(D)$ on kokonaisalueen D *osamääräkunta* (quotient field, field of fractions).

Lause 5.6. *Olkoon $(D, +, \cdot)$ kokonaisalue. Tällöin*

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

Todistus. Merkitään $A = \{[a, \mathbf{1}] \mid a \in D\}$ ja osoitetaan ensin, että A on renkaan $Q(D)$ alirengas.

1. Olkoon $[a, \mathbf{1}], [b, \mathbf{1}] \in A$. Tällöin

$$[a, \mathbf{1}] - [b, \mathbf{1}] = [a, \mathbf{1}] + [-b, \mathbf{1}] = [(a - b), \mathbf{1}] \in A.$$

2. Olkoon $[a, \mathbf{1}], [b, \mathbf{1}] \in A$. Tällöin $[a, \mathbf{1}] \cdot [b, \mathbf{1}] = [(a \cdot b), \mathbf{1}] \in A$.

3. Renkaan $Q(D)$ ykkösalkio on $[\mathbf{1}, \mathbf{1}]$ ja $[\mathbf{1}, \mathbf{1}] \in A$.

Kohtien 1–3 ja alirengaskriteerin nojalla A on renkaan $Q(D)$ alirengas. Erityisesti siis $(A, +, \cdot)$ on rengas.

Määritellään kuvaus $f : (A, +, \cdot) \to (D, +, \cdot)$ siten, että $f([a, \mathbf{1}]) = a$ kaikilla $a \in D$. Osoitetaan, että f on rengasisomorfismi $A \to D$.

1. Olkoon $x \in D$. Tällöin $[x, \mathbf{1}] \in A$ ja $f([x, \mathbf{1}]) = x$, joten f on surjektio.

2. Olkoon $[a, \mathbf{1}], [b, \mathbf{1}] \in A$ ja $f([a, \mathbf{1}]) = f([b, \mathbf{1}])$. Tällöin $a = b$, joten $[a, \mathbf{1}] = [b, \mathbf{1}]$. Siispä f on injektio.

3. (a) Olkoon $[a, \mathbf{1}], [b, \mathbf{1}] \in A$. Tällöin

$$f([a, \mathbf{1}] + [b, \mathbf{1}]) = f([(a + b), \mathbf{1}]) = a + b = f([a, \mathbf{1}]) + f([b, \mathbf{1}]).$$

   (b) Olkoon $[a, \mathbf{1}], [b, \mathbf{1}] \in A$. Tällöin

$$f([a, \mathbf{1}] \cdot [b, \mathbf{1}]) = f([(a \cdot b), \mathbf{1}]) = a \cdot b = f([a, \mathbf{1}]) \cdot f([b, \mathbf{1}]).$$

   (c) Renkaan $(A, +, \cdot)$ ykkösalkio on $[\mathbf{1}, \mathbf{1}]$, missä $\mathbf{1} \in D$ on renkaan $(D, +, \cdot)$ ykkösalkio. Nyt $f([\mathbf{1}, \mathbf{1}]) = \mathbf{1}$.

   Kohtien (a)–(c) nojalla f on rengashomomorfismi.

Kohtien 1–3 nojalla f on rengasisomorfismi $A \to D$, joten

$$A = \{[a, \mathbf{1}] \mid a \in D\} \cong D.$$

Edellisen lauseen nojalla voidaan tehdä samaistus $a = a/\mathbf{1}$. Jos $a, b \in D$ ja b^{-1} on olemassa, niin

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

Määritelmä 5.7. Rationaalilukujen kunta $\mathbb{Q} = Q(\mathbb{Z})$.

Määritelmä 5.8. K-kertoimisten rationaalifunktioiden kunta $K(x) = Q(K[x])$.

Huomautus. Rationaalifunktiot ovat muotoa $f(x) = \dfrac{p(x)}{q(x)}$, missä $p(x)$ ja $q(x)$ ovat polynomeja.

Tällöin pätevät yllä esitetyt supistamis- ja laventamissäännöt, jolloin esimerkiksi

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