Rengashomomorfismi $\phi\colon R \to R'$ on erityisesti ryhmähomomorfismi $\phi\colon (R,+) \to (R',+)$ additiivisten ryhmien välillä. Rengashomomorfismin ydin määritellään tämän ryhmähomomorfismin ϕ ytimen avulla:

Määritelmä 11.1. Rengashomomorfismin $\psi\colon R \to R'$ *ydin* on

$$\ker\psi = \psi^{-1}(0) = \{x \in R : \psi(x) = 0\}.$$

Proposition 5.6 nojalla ryhmähomomorfismin $\phi\colon G \to G'$ ydin on ryhmän G normaali aliryhmä, joten rengashomomorfismin ψ ydin on additiivisen ryhmän $(R,+)$ normaali aliryhmä. Kertolaskun suhteen homomorfisuus antaa ytimelle lisää rakennetta, jota tarkastelemme seuraavaksi.

Määritelmä 11.2. Olkoon R rengas ja olkoon $\mathscr{I} \subset R$ siten, että $(\mathscr{I},+)$ on ryhmän $(R,+)$ aliryhmä.

(1) $\mathscr{I}$ on *vasen ideaali*, jos $xa \in \mathscr{I}$ kaikilla $x \in R$ ja $a \in \mathscr{I}$.
(2) $\mathscr{I}$ on *oikea ideaali*, jos $ay \in \mathscr{I}$ kaikilla $y \in R$ ja $a \in \mathscr{I}$.
(3) $\mathscr{I}$ on *kaksipuolinen ideaali*, jos $xay \in \mathscr{I}$ kaikilla $x, y \in R$ ja $a \in \mathscr{I}$.

Jos R on kommutatiivinen rengas, niin Määritelmän 11.2 kohdissa (1)–(3) määritellyt käsitteet ovat kaikki samoja. Tällöin käytetään yleensä yksinkertaisempaa terminologiaa ja sanotaan, että $\mathscr{I}$ on *ideaali.*

Lemma 11.3. *(1) $\mathscr{I}$ on vasen ideaali, jos ja vain jos $xa+x'a' \in \mathscr{I}$ kaikilla $x, x' \in R$ ja $a, a' \in \mathscr{I}$.*

(2) $\mathscr{I}$ on oikea ideaali, jos ja vain jos $ay + a'y' \in \mathscr{I}$ kaikilla $y, y' \in R$ ja $a, a' \in \mathscr{I}$.

(3) $\mathscr{I}$ on kaksipuolinen ideaali, jos ja vain jos se on vasen ideaali ja oikea ideaali.

Todistus. Harjoitustehtävä 116. □

Esimerkki 11.4. (a) R ja $\{0\}$ ovat renkaan R kaksipuolisia ideaaleja.

(b) $q\mathbb{Z}$ on renkaan $\mathbb{Z}$ ideaali jokaisella $q \in \mathbb{Z}$.

(c) Olkoot $\Omega \neq \emptyset$, $\emptyset \neq A \subset \Omega$, ja R rengas. Olkoon

$$N(A) = \{f \in \mathscr{F}(\Omega, R) : f(a) = 0 \text{ kaikilla } a \in A\}.$$

Tällöin $N(A)$ on funktiorenkaan $\mathscr{F}(\Omega, R)$ kaksipuolinen ideaali. Jos nimittäin $g_1, g_2 \in \mathscr{F}(\Omega, R)$ ja $h_1, h_2 \in N(A)$ ja $a \in A$, niin

$$(g_1h_1)(a) = g_1(a)h_1(a) = g_1(a) \cdot 0 = 0,$$

joten $gh \in N(A)$. Vastaavasti nähdään, että $g_2h_2 \in N(A)$, joten

$$(g_1h_1 + g_2h_2)(a) = 0.$$

Siis $g_1h_1 + g_2h_2 \in N(A)$, joten $N(A)$ on vasen ideaali. Samalla tavalla tarkastetaan, että $N(A)$ on oikea ideaali, joten se on kaksipuolinen ideaali.

Sama konstruktio antaa kaksipuolisia ideaaleja monille renkaan $\mathscr{F}(\Omega, R)$ alirenkaille, esimerkiksi

$$\{f \in C^\infty(\mathbb{R}) : f(0) = 0\}$$

on renkaan $C^\infty(\mathbb{R})$ ideaali.

Propositio 11.5. *Olkoon $\phi\colon R \to S$ rengashomomorfismi. Tällöin*

(1) Jos $\mathscr{I} \subset R$ on vasen (vastaavasti oikea tai kaksipuolinen) ideaali, niin $\phi(\mathscr{I})$ on renkaan $\phi(S)$ vasen (vastaavasti oikea tai kaksipuolinen) ideaali.

(2) Jos $\mathscr{I} \subset S$ on vasen (oikea tai kaksipuolinen) ideaali, niin $\phi^{-1}(\mathscr{I})$ on renkaan R vasen (oikea tai kaksipuolinen) ideaali.

Todistus. (1) Harjoitustehtävä 117.

(2) Tarkastelemme vain tapausta, jossa $\mathscr{I}$ on vasen ideaali, oikean ideaalin tapaus todistetaan samalla tavalla ja kaksipuolista ideaalia koskeva väite seuraa yhdistämällä nämä kaksi tulosta. Proposition 5.6 nojalla $(\phi^{-1}(\mathscr{I}), +) \leq (R, +)$. Olkoot $a \in \phi^{-1}(\mathscr{I})$ ja $r \in R$. Tällöin $\phi(ra) = \phi(r)\phi(a) \in \mathscr{I}$, koska $\phi(a) \in \mathscr{I}$ ja $\mathscr{I}$ on vasen ideaali. Siis $ra \in \phi^{-1}(\mathscr{I})$. □

Seuraus 11.6. *Rengashomomorfismin ydin on määrittelyrenkaansa kaksipuolinen ideaali.*

Todistus. Väite seuraa Propositiosta 11.5(2) koska $\{0\}$ on kaksipuolinen ideaali. □

Esimerkki 11.7. Luonnollinen kuvaus $\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$ on surjektiivinen rengashomomorfismi, joten renkaan $\mathbb{Z}/q\mathbb{Z}$ ideaalit ovat täsmälleen renkaan $\mathbb{Z}$ ideaalien kuvat luonnollisessa homomorfismissa. Erityisesti jokainen renkaan $\mathbb{Z}/q\mathbb{Z}$ aliryhmä on jonkin ideaalin additiivinen ryhmä.

Propositio 11.8. *Jos renkaan R vasen, oikea tai kaksipuolinen ideaali $\mathscr{I}$ on alirengas, niin $\mathscr{I} = R$.*

Todistus. Tarkastelemme ainoastaan vasempia ideaaleja. Oikeat ideaalit tarkastellaan samalla tavalla. Jos $\mathscr{I}$ on renkaan R vasen ideaali ja $1 = 1_R \in \mathscr{I}$, niin kaikilla $x \in R$ pätee $x = x1 \in \mathscr{I}$, joten $\mathscr{I} = R$. □

Propositio 11.9. *Olkoon R jakorengas, ja olkoon $\mathscr{I}$ sen vasen, oikea tai kaksipuolinen ideaali. Silloin $\mathscr{I} = R$ tai $\mathscr{I} = \{0\}$. Erityisesti, jos R on kunta, niin sen ainoat ideaalit ovat $\{0\}$ ja R.*

Todistus. Jos $a \in R^\times$, niin sillä on käänteisalkio a^{-1}. Jos $\mathscr{I}$ on vasen ideaali, jolle $a \in \mathscr{I}$, niin $1 = a^{-1}a \in \mathscr{I}$. Väite seuraa Propositiosta 11.8. □

Kaksipuolinen ideaali vastaa Proposition 11.5 mukaan rengasteoriassa ryhmäteorian normaalia aliryhmää. Renkaan additiivinen ryhmä on kommutatiivinen, joten ideaali ajateltuna kommutatiivisena additiivisena ryhmänä on siis renkaan additiivisen ryhmän normaali aliryhmä. Käyttämällä samaa ekvivalenssirelaatiota kuin luvussa 4 muodostamme renkaan R ideaalia $\mathscr{I}$ vastaavan tekijäjoukon $R/\mathscr{I}$. Seuraavan tuloksen mukaan tämä tekijäjoukko voidaan varustaa kahdella laskutoimituksella.

Propositio 11.10. *Olkoon R rengas ja olkoon $I \subset R$ kaksipuolinen ideaali. Renkaan R yhteenlasku ja kertolasku ovat yhteensopivia ideaalin I määräämän ekvivalenssirelaation kanssa*

Todistus. Yhteenlaskun yhteensopivuus seuraa tekijäryhmien vastaavasta tuloksesta. Tarkastelemme siis vain kertolaskua: Olkoot $a, a', b, b' \in R$, $a \sim a'$ ja $b \sim b'$. Nyt $a - a' \in \mathscr{I}$ ja $b - b' \in \mathscr{I}$, joten

$$ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + (a - a')b' \in \mathscr{I},$$

koska $\mathscr{I}$ on kaksipuolinen ideaali. □

Proposition 11.10 mukaan renkaan R molemmat laskutoimitukset määrittelevät tekijälaskutoimituksen tekijäjoukossa $R/\mathscr{I}$. Ideaalia $\mathscr{I}$ vastaaville sivuluokille käytetään additiivista merkintää $x + I$, jolloin laskutoimitukset ovat siis

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

ja

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

kaikille $x, y \in R$.

Propositio 11.11. *Olkoon R rengas, ja olkoon $\mathscr{I}$ sen kaksipuolinen ideaali. Tällöin tekijäjoukko $R/\mathscr{I}$ on rengas.*

Todistus. Harjoitustehtävä 126. □

Esimerkki 11.12. Luvun $q \geq 2$ monikerrat muodostavat renkaan $\mathbb{Z}$ ideaalin $q\mathbb{Z}$. Tätä ideaalia vastaa tuttu tekijärengas $\mathbb{Z}/q\mathbb{Z}$.

Propositiot 3.7 ja 3.8 antavat seurauksena

Propositio 11.13. *(1) Tekijärengas on kommutatiivinen, jos alkuperäinen rengas on kommutatiivinen.*
(2) Luonnollinen kuvaus $R \to R/\mathscr{I}$ on rengashomomorfismi. □

Lause 11.14 (Renkaiden isomorfismilause)**.** *Olkoon $\psi\colon R \to S$ rengashomomorfismi. Tällöin tekijärengas $R/\ker\psi$ on isomorfinen renkaan $\psi(R)$ kanssa.*

Todistus. Lause todistetaan kuten ryhmien isomorfismilause (Lause 7.23). Harjoitustehtävä 127. □

Esimerkki 11.15. (a) $R/R \cong \{0\}$, joten tekijärengas $R/\mathscr{I}$ voi olla kommutatiivinen vaikka R ei olisikaan. Toinen ääriesimerkki tekijärenkaasta on $R/\{0\} \cong R$.
(b) Olkoon R rengas, $\Omega \neq \emptyset$ ja $c \in \Omega$. Kuvaus $E_c\colon \mathscr{F}(\Omega, R) \to R$, $E_c(f) = f(c)$ on surjektiivinen rengashomomorfismi, jonka ydin on

$$N(a) = \{f \in \mathscr{F}(\Omega, R) : f(c) = 0\}.$$

Renkaiden isomorfismilauseen nojalla $\mathscr{F}(\Omega, R)/N(a)$ on rengasisomorfinen renkaan R kanssa.
(c) Reaaliluvut konstruoidaan kurssilla Lukualueet rationaalilukujen Cauchyn jonojen renkaan nollaan suppenevien jonojen ideaalia vastaavana tekijärenkaana.

Propositio 11.16. *Olkoot L ja M renkaan R vasempia (vastaavasti oikeita tai kaksipuolisia) ideaaleja. Tällöin niiden* summa

$$L + M = \{x_1 + x_2 : x_1 \in L, x_2 \in M\}$$

ja tulo

$$LM = \{x_1y_1 + x_2y_2 + \cdots + x_ny_n : x_i \in L, y_i \in M, n \in \mathbb{N}\},$$

ovat renkaan R vasempia (vastaavasti oikeita tai kaksipuolisia) ideaaleja.

Todistus. Harjoitustehtävä 119. □

Propositio 11.17. *Olkoot $\mathscr{I}_i$, $i \in I$, renkaan R vasempia (vastaavasti oikeita tai kaksipuolisia) ideaaleja. Tällöin*

$$\bigcap_{i \in I} \mathscr{I}_i$$

on renkaan R vasen (vastaavasti oikea tai kaksipuolinen) ideaali.

Todistus. Harjoitustehtävä 124. □

Määritelmä 11.18. Jos $S \subset R$, $S \neq \emptyset$, niin *joukon S virittämä vasen (vastaavasti oikea tai kaksipuolinen) ideaali* on joukon S sisältävien (vastaavasti oikeiden tai kaksipuolisten) ideaalien leikkaus.

Lemma 11.19. *Olkoon R rengas. Äärellisen joukon $A = \{x_1, x_2, \ldots, x_n\} \subset R$ virittämä vasen ideaali on*

$$RA = \left\{ \sum_{i=1}^{n} r_i x_i : r_1, r_2, \ldots, r_n \in R \right\},$$

niiden virittämä oikea ideaali on

$$AR = \left\{ \sum_{i=1}^{n} x_i r_i : r_1, r_2, \dots, r_n \in R \right\}$$

ja niiden virittämä kaksipuolinen ideaali on

$$RAR = \left\{ \sum_{i=1}^{n} s_i x_i r_i : s_1, r_1, s_2 r_2, \dots, s_n, r_n \in R \right\}.$$

Todistus. Harjoitustehtävä 118. □

Erityisesti yhden alkion x virittämä vasen ideaali on $Rx = \{rx : r \in R\}$ ja sen virittämä oikea ideaali on xR. Jos rengas K on kommutatiivinen, niin $xK = Kx$ ja tätä ideaalia merkitään usein (x) ja sanotaan *pääideaaliksi*. Vastaavasti alkioiden $x_1, x_2, \dots, x_m$ virittämää ideaalia kommutatiivisessa renkaassa merkitään usein $(x_1, x_2, \dots, x_m)$. Kokonaisalue, jonka kaikki ideaalit ovat pääideaaleja on *pääideaalialue*.

Lause 11.20. *Olkoon K kunta. Tällöin polynomirengas $K[X]$ on pääideaalialue.*

Todistus. Olkoon $\mathscr{I}$ nollasta poikkeava ideaali renkaassa $K[X]$ ja olkoon $P_0(X) \in \mathscr{I} \setminus \{0\}$ polynomi, jolla on minimaalinen aste: $\deg P_0(X) \le \deg P(X)$ kaikille $P(X) \in \mathscr{I} \setminus \{0\}$. Olkoon $A(X) \in \mathscr{I}$. Jakoyhtälön (Seuraus 10.13) mukaan on $Q(X), J(X) \in K[X]$, joille pätee

$$A(X) = Q(X)P_0(X) + J(X)$$

ja $\deg J(X) < \deg P_0(X)$. Erityisesti

$$J(X) = A(X) - Q(X)P_0(X) \in \mathscr{I}.$$

Koska $\deg P_0(X)$ on minimaalinen nollasta poikkeaville ideaalin $\mathscr{I}$ polynomeille, pätee $J(X) = 0$, joten $A(X) \in (P_0(X))$. □

Esimerkki 11.21. Olkoon $\psi \colon \mathbb{R}[X] \to \mathbb{C}$ kuvaus, joka määritellään asettamalla $\psi(Q(X)) = Q(i)$ kaikille $\mathbb{R}$-kertoimisille polynomeille $Q(X)$. Tällöin ψ on surjektiivinen rengashomomorfismi, jonka ydin on jaottoman polynomin X^2+1 virittämä pääideaali (X^2+1). Renkaiden isomorfismilauseen mukaan tekijärengas $\mathbb{R}[X]/(X^2+1)$ on rengasisomorfinen kompleksilukujen kunnan $\mathbb{C}$ kanssa.

Määritelmä 11.22. Olkoon K kunta. Jos polynomi $D(X) \in K[X]$ on polynomien $P(X), Q(X) \in K[X]$ yhteinen tekijä, joka on jaollinen jokaisella polynomien $P(X)$ ja $Q(X)$ yhteisellä tekijällä, niin $D(X)$ on polynomien $P(X)$ ja $Q(X)$ *suurin yhteinen tekijä*. Tällöin käytetään merkintää $D(X) = \mathrm{syt}(P(X), Q(X))$.

Lause 11.23. *Olkoon K kunta. Polynomeilla $P(X), Q(X) \in K[X]$ on suurin yhteinen tekijä. Jos $D(X) = \mathrm{syt}(P(X), Q(X))$, niin on polynomit $R(X), S(X) \in K[X]$, joille pätee*

$$D(X) = R(X)P(X) + S(X)Q(X). \tag{18}$$

Todistus. Harjoitustehtävä 129. □

Yhtälö (18) on polynomien *Bezout'n yhtälö*. Jos $u \in K$, $u \neq 0$, ja $D(X) = \mathrm{syt}(P(X), Q(X)$, niin $uD(X) = \mathrm{syt}(P(X), Q(X))$: Polynomi $uD(X)$ on polynomin $D(X)$ tekijä koska u on yksikkö. Siis $uD(X)$ on polynomien $P(X)$ ja $Q(X)$ yhteinen tekijä. Toisaalta $D(X) \mid uD(X)$, joten jokainen polynomien $P(X)$ ja $Q(X)$ yhteinen tekijä jakaa polynomin $uD(X)$. Jos polynomien $P(X)$ ja $Q(X)$ suurin yhteinen tekijä on nollannen asteen polynomi, pätee siis erityisesti $1 = \mathrm{syt}(P(X), Q(X))$.

Lause 11.24. *Olkoon K kunta ja olkoon $P(X) \in K[X]$ polynomi, jonka aste on d.*

(1) Jos kunnassa K on q alkiota, niin renkaassa $K[X]/(P(X))$ on q^d alkiota.

(2) Jos $P[X]$ on jaoton, niin $K[X]/(P(X))$ on kunta.

Todistus. Käytämme todistuksessa merkintää $\mathscr{I} = (P(X))$.

(1) Kuntakertoimisten polynomien jakoyhtälön (Seuraus 10.13) nojalla jokaisella ekvivalenssiluokalla $Q(X) + (P(X)) \in K[X]/\mathscr{I}$ on edustaja $\bar{Q}(X)$, jolle pätee $\deg \bar{Q}(X) < \deg P(X) = d$:

$$Q(X) = T(X)P(X) + \bar{Q}(X)$$

yksikäsitteiselle $T(X) \in K[X]$.

Tällaisia polynomeja on q^d kappaletta ja mitkään kaksi eivät ole ekvivalentteja.

(2) Olkoon $\bar{Q}(X) \neq 0$ kuten kohdassa (1). Tällöin $P(X)$ ei ole polynomin $\bar{Q}(X)$ tekijä koska $\deg \bar{Q}(X) < \deg P(X)$. Toisaalta, jos $\bar{Q}(X) \mid P(X)$, niin $\bar{Q}(X)$ on vakio ja siis yksikkö koska oletimme, että $P(X)$ on jaoton. Siis $1 = \mathrm{syt}(P(X), \bar{Q}(X))$ ja polynomien Bezout'n yhtälön mukaan on $R(X), S(X) \in K[X]$, joille pätee

$$1 = R(X)P(X) + S(X)\bar{Q}(X),$$

joten $S(X)\bar{Q}(X) \in 1 + \mathscr{I}$. Siis

$$\big(S(X) + \mathscr{I}\big)\,\big(\bar{Q}(X) + \mathscr{I}\big) = 1 + \mathscr{I},$$

joten polynomin $\bar{Q}(X)$ luokka tekijärenkaassa $K[X]/\mathscr{I}$ on yksikkö. □

Esimerkki 11.25. Polynomi $P(X) = X^2 + X + 1$ on jaoton toisen asteen polynomi polynomirenkaassa $(\mathbb{Z}/2\mathbb{Z})[X]$. Lauseen 11.24 nojalla $(\mathbb{Z}/2\mathbb{Z})[X]/(P[X])$ on neljän alkion kunta.

Ennen Esimerkkiä 11.25 olemme tavanneet äärellisistä kunnista ainoastaan kunnat $\mathbb{Z}/p\mathbb{Z}$, missä p on alkuluku, erityisesti siis näiden kuntien alkioiden lukumäärä on alkuluku. Esimerkin 11.25 tulos yleistyy kaikille alkulukupotensseille p^q. Emme kuitenkaan todista seuraavaa tulosta tällä kurssilla.

Lause 11.26. *Jokaiselle luonnolliselle luvulle $q \geq 1$ ja alkuluvulle p on äärellinen kunta, jossa on p^q alkiota. Toisaalta jokaisessa äärellisessä kunnassa on p^q alkiota joillain tällaisilla p ja q.* □

Harjoitustehtäviä.

Tehtävä 116. Olkoon R rengas, ja olkoon $\mathscr{I} \subset R$. Osoita, että

(1) $\mathscr{I}$ on vasen ideaali, jos ja vain jos $xa + x'a' \in \mathscr{I}$ kaikilla $x, x' \in R$ ja $a, a' \in \mathscr{I}$.

(2) $\mathscr{I}$ on kaksipuolinen ideaali, jos ja vain jos se on vasen ideaali ja oikea ideaali.

Tehtävä 117. Olkoon $\psi : R \to S$ rengashomomorfismi. Olkoon $\mathscr{I}$ renkaan R vasen ideaali. Osoita, että $\psi(\mathscr{I})$ on renkaan $\psi(R)$ vasen ideaali.

Tehtävä 118. Olkoon R rengas. Olkoot $a_1, a_2, \dots a_n \in R$. Osoita, että

$$\{x_1 a_1 + x_2 a_2 + \cdots + x_n a_n : x_1, x_2, \dots, x_n \in R\}$$

on renkaan R vasen ideaali.

Tehtävä 119. Olkoot L ja M renkaan R vasempia ideaaleja. Olkoot

$$LM = \{x_1y_1 + x_2y_2 + \cdots + x_ny_n : x_i \in L, y_i \in M, n \in \mathbb{N}\},$$

ja

$$L + M = \{x + y : x \in L, y \in M\},$$

Osoita, että LM ja $L + M$ ovat renkaan R vasempia ideaaleja.

Tehtävä 120. Olkoon R rengas. Alkion $r \in R$ *vasen annihilaattori* on

$$\{a \in R : ar = 0\}.$$

Osoita, että vasen annihilaattori on vasen ideaali.

Tehtävä 121. Olkoon R kommutatiivinen rengas. Osoita, että renkaassa R pätee *binomikaava*

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

kaikille $a, b \in R$.

Tehtävä 122. Olkoon R kommutatiivinen rengas. Alkio $x \in R$ on *nilpotentti*, jos $x^n = 0$ jollain $n \in \mathbb{N}$. Osoita, että renkaan R nilpotentit alkiot muodostavat ideaalin.

Tehtävä 123. Sievennä lauseke $(a + b)^p$ kunnassa $\mathbb{Z}/p\mathbb{Z}$.

Tehtävä 124. Olkoot $\mathscr{I}_i$, $i \in I$ on renkaan R vasempia ideaaleja. Osoita, että $\bigcap_{i \in I} \mathscr{I}_i$ on renkaan R vasen ideaali.

Tehtävä 125. Olkoot L ja M renkaan R vasempia ideaaleja. Osoita, että $LM \subset L \cap M$, jos R on kommutatiivinen

Tehtävä 126. Olkoon R rengas, ja olkoon $\mathscr{I}$ sen kaksipuolinen ideaali. Osoita, että $R/\mathscr{I}$ on rengas.

Tehtävä 127. Todista renkaiden isomorfismilause.

Tehtävä 128. Olkoot K ja K' kuntia. Olkoon $\phi\colon K \to K'$ kuntahomomorfismi. Osoita, että ϕ on injektio.

Tehtävä 129. Olkoon K kunta. Osoita, että polynomeilla $P(X), Q(X) \in K[X]$ on suurin yhteinen tekijä. Jos $D(X) = \mathrm{syt}(P(X), Q(X))$, osoita, että on polynomit $R(X), S(X) \in K[X]$, joille pätee

$$D(X) = R(X)P(X) + S(X)Q(X).$$

Lukemista

Tämä kurssi antaa perustietoja algebrasta. Kiinnostunut lukija voi kurssin tietojen pohjalta tutustua algebraan laajemmin esimerkiksi seuraavan luettelon kirjojen avulla.

(1) N. Bourbaki: Algebra I, Springer-Verlag, 1989
(2) D. Dummit ja R. Foote: Abstract algebra, John Wiley & Sons, 2004.
(3) R. Godement: Algebra, Hermann, 1968
(4) A. Hillman ja G. Alexanderson : A first undergraduate course in abstract algebra, Wadsworth, 1983.

[122]Vihje: Huomaa, että potenssi n voi riippua alkiosta x. Käytä tehtävän 121 binomikaavaa.

[129]Vihje: Tarkastele polynomien $P(X)$ ja $Q(X)$ virittämää ideaalia.

(5) S. Lang: Undergraduate algebra, Springer-Verlag, 1987.
(6) C. Pinter: A book of abstract algebra, Dover, 2010.