

1. Tutki, onko joukko  $\{1, -1, i, -i\}$  ryhmä, kun laskutoimituksena on kompleksilukujen kertolasku.

2. Ratkaise yhtälö  $x^2 - 5x + 6 = 0$

(a)  $\mathbf{Z}_7$ :ssä,

(b)  $\mathbf{Z}_{10}$ :ssä.

(Ohje: Jos merkitään  $P(x) = x^2 - 5x + 6$ , niin yhtälö  $P(x) = 0$  ratkaistaan renkaassa  $\mathbf{Z}_n$  helpoimmin kokeilemalla millä  $x \in \{0, 1, \dots, n-1\}$  pätee  $P(x) \equiv 0 \pmod{n}$ .)

3. Osoita, että rengas  $R$  on kommutatiivinen, jos ja vain jos

$$(x + y)^2 = x^2 + y^2 + 2xy \text{ kaikilla } x, y \in R.$$

4. Renkaan  $R$  aitoa ideaalia  $P$  sanotaan *alkuideaaliksi*, jos  $P$  täyttää ehdon  $a, b \in R$ ,  $ab \in P \Rightarrow a \in P$  tai  $b \in P$ . Todista, että kommutatiivisen renkaan maksimaalinen ideaali on alkuideaali. (Ohje: Tarkastele jäännösluokkarengasta (tekijärengasta)  $R/P$ . Muista, että kunta on kokonaisalue.)

5. Olkoon  $f(x) \in \mathbf{R}[x]$  ja  $a \in \mathbf{R}$ . Palautetaan mieleen, että

$$(x - a) \text{ jakaa polynomin } f(x) \Leftrightarrow f(a) = 0.$$

Todista, että

$$(x - a)^2 \text{ jakaa polynomin } f(x) \Leftrightarrow f(a) = 0 \text{ ja } f'(a) = 0.$$

(Merkintä  $f'(a)$  tarkoittaa  $f(x)$ :n derivaattaa pisteessä  $a$ . Palautetaan mieleen tulon derivoimiskaava  $(fg)' = fg' + f'g$ .)

Algebra I  
Loppukoe  
24.1. 2008

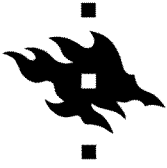
1. Etsi lukujen 901 ja 257 suurin yhteinen tekijä Eukleideen algoritmilla.
2. Ratkaise yhtälö  $a \circ x \circ b = c$  joukon  $\{1, 2, 3, 4\}$  määräämässä permutaatio-ryhmässä  $S_4$ , kun

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, c = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}.$$

3. (*teoria*) Määrittele ryhmän  $(G, \cdot)$  normaali aliryhmä  $H$ , sekä tekijäryhmä  $G/H$  ja sen laskutoimitus. Perustele miksi tekijäryhmän laskutoimitus on hyvin määritelty (ts. ei riipu edustajien valinnasta).

4. Ratkaise yhtälö  $1 + x + x^2 + x^3 = 0$  jäännösluokkarenkaissa  $(\mathbf{Z}_5, +, \cdot)$  ja  $(\mathbf{Z}_7, +, \cdot)$ . [*Muistutus.* Jos  $P(x) = 1 + x + x^2 + x^3$ , niin renkaassa  $\mathbf{Z}_p$  ratkaistaan yhtälö  $P(x) = 0$  helpoiten kokeilemalla millä arvoilla  $a \in \{0, \dots, p-1\}$  pätee  $P(a) \equiv 0 \pmod{p}$ .]

5. Osoita, että lukurenkaat  $\mathbf{Z}[\sqrt{2}] = \{m + n\sqrt{2} : m, n \in \mathbf{Z}\}$  ja  $\mathbf{Z}[\sqrt{3}] = \{m + n\sqrt{3} : m, n \in \mathbf{Z}\}$  eivät ole isomorfiset, kun laskutoimitukset ovat reaalilukujen indusoima yhteenlasku ja tulo. [*Vihje:* Tee vastaoletus, että on olemassa rengashomomorfismi  $f : (\mathbf{Z}[\sqrt{2}], +, \cdot) \rightarrow (\mathbf{Z}[\sqrt{3}], +, \cdot)$ . Kirjoita  $f(\sqrt{2}) = m + n\sqrt{3}$  sopivilla  $m, n \in \mathbf{Z}$ , ja tutki alkioita  $f(2)$ . Tehtävässä saa pitää tunnettuna, että  $\sqrt{2}$  ja  $\sqrt{3}$  ovat irrationaalilukuja.]

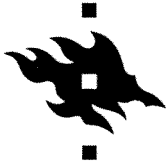


1. Onko olemassa sellaisia kokonaislukuja  $x$  ja  $y$ , että  $341103x + 251062y = 1$ ?
2. Määrittelemme joukossa  $\mathbb{R}^3 = \{(x_1, x_2, x_3) \mid x_1, x_2, x_3 \in \mathbb{R}\}$  relaation  $\sim$  asettamalla  $(x_1, x_2, x_3) \sim (y_1, y_2, y_3)$  täsmälleen silloin, kun on olemassa joukon  $\{1, 2, 3\}$  permutaatio  $\varphi$  (siis  $\varphi \in S_3$ ), jolla  $y_k = x_{\varphi(k)}$  kaikilla  $k \in \{1, 2, 3\}$ . Osoita, että  $\sim$  on ekvivalenssirelaatio. Määritä  $\mathbb{R}^3$ :n alkioiden  $(0, 0, 1)$  ja  $(0, 1, 2)$  ekvivalenssiluokat.
3. Olkoon  $X = \{2, 3, 5, 7, 11, 13\}$ . Kun  $p, q \in X$ , olkoon

$$p \top q = \text{luvun } p + q - 2 \text{ suurin alkutekijä.}$$

Taulukoi luvut  $p \top q$  kaikilla  $p, q \in X$  ja totea näin, että  $\top$  on laskutoimitus joukossa  $X$ . Osoita, että  $X$ :ssä on  $\top$ :n suhteen neutraalialkio ja jokaisella  $X$ :n alkiolla on käänteisalkio. Onko  $(X, \top)$  ryhmä?

4. Osoita, että renkaan  $R$  keskus  $C(R) = \{a \in R \mid ab = ba \text{ kaikilla } b \in R\}$  on  $R$ :n alirengas.
5. Olkoon  $I$  polynomin  $x^2 - 3$  virittämä polynomirenkaan  $\mathbb{Q}[x]$  ideaali ja  $f = x - 1 \in \mathbb{Q}[x]$ . Osoita, että  $f + I$  on kääntyvä jäännösluokkarenkaassa  $\mathbb{Q}[x]/I$ , ja määritä sen käänteisalkio.



1. Olkoon  $A = \{1, 2, 3, 4, 5\}$  ja  $f : A \rightarrow A$  se kuvaus, jolla  $f(1) = f(3) = 2$ ,  $f(2) = f(4) = 4$  ja  $f(5) = 1$ . Olkoon edelleen  $A_0 = \{4\} \subset A$  ja  $A_n = f^{-1}(A_{n-1})$  kaikilla  $n \in \mathbb{N}$ ,  $n \geq 1$ . Luettele joukon  $A_n$  alkioit jokaisella  $n \geq 1$ .
2. Selvitä, onko luku  $2008^{2008} + 2006$  jaollinen luvulla 13.
3. Olkoot  $H$  ja  $K$  multiplikatiivisen ryhmän  $G$  aliryhmiä. Osoita: Jos on olemassa sellaiset  $a, b \in G$ , että  $aH = bK$ , niin  $H = K$ .
4. Osoita, että  $R = \{m/5^n \mid m \in \mathbb{Z}, n \in \mathbb{N}\}$  on rationaalilukujen renkaan  $\mathbb{Q}$  alirengas. Mitkä alkioit ovat kääntyviä (eli yksiköitä) renkaassa  $R$ ?
5. Etsi polynomirenkaan  $\mathbb{Z}_2[x]$  kaikki jaottomat alkioit, joiden aste on korkeintaan kolme (niitä löytynee 5 kpl). Tutki, onko neljännen asteen polynomi  $x^4 + x^2 + 1 \in \mathbb{Z}_2[x]$  jaoton.



1. Osoita, että reaalilukujen joukon  $\mathbb{R}$  relaatio  $E$ ,

$$xEy \iff y = ax \text{ jollakin } a > 0,$$

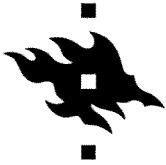
on ekvivalenssi. Kuinka monta eri ekvivalenssiluokkaa tällä relaatiolla on?

2. Joukon  $A$  laskutoimituksella  $\top$  on neutraalialkio, ja

$$a \top (b \top c) = (a \top c) \top b \quad \text{kaikilla } a, b, c \in A.$$

Osoita, että  $\top$  on liitännäinen ja vaihdannainen.

3. Olkoon  $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$  kaavan  $f(m, n) = 3m - 2n$  määrittelemä kuvaus. Osoita, että  $f$  on additiivisten ryhmien surjektiivinen homomorfismi, jonka ydin  $\text{Ker}(f)$  on alkion  $(2, 3)$  virittämä  $\mathbb{Z} \times \mathbb{Z}$ :n syklinen aliryhmä.
4. Osoita, että  $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$  on  $\mathbb{R}$ :n alikunta.
5. Etsi polynomirenkaan  $\mathbb{Z}_2[x]$  kaikki jaottomat alkio, joiden aste on korkeintaan kolme (niitä löytyy 5 kpl). Tutki, onko neljännen asteen polynomi  $x^4 + x^2 + 1 \in \mathbb{Z}_2[x]$  jaoton.



1. Olkoot  $f : A \rightarrow B$  ja  $g : B \rightarrow C$  kuvauksia, ja  $g \circ f$  injektio. Osoita, että  $f$  on injektio. Onko  $g$  välttämättä injektio? (Esitä jälkimmäiseen kysymykseen todistus tai vastaesimerkki.)
2. Osoita, että kaava  $a * b = |a - b|$  määrittelee joukossa  $\{0, 1, 2, \dots, 10\}$  laskutoimituksen  $*$ . Tutki, onko  $*$  a) vaihdannainen, b) liitännäinen, ja c) onko sillä neutraalialkiota.
3. Olkoon  $G$  multiplikatiivinen ryhmä. Kun  $g \in G$ , määrittelemme kuvauksen  $c_g : G \rightarrow G$  asettamalla  $c_g(a) = gag^{-1}$  kaikilla  $a \in G$ . Todista, että  $c_{1_G} = \text{id}_G$ ,  $c_{g_1 g_2} = c_{g_1} \circ c_{g_2}$  kaikilla  $g_1, g_2 \in G$ , ja  $c_g$  on  $G$ :n automorfismi (so. isomorfismi  $G \rightarrow G$ ) kaikilla  $g \in G$ .
4. Tarkastellaan funktiorengaan  $\mathbb{R}^{[0,1]}$  alirengasta

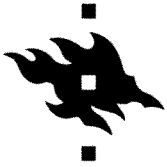
$$C([0, 1], \mathbb{R}) = \{f \in \mathbb{R}^{[0,1]} \mid f \text{ on jatkuva}\}.$$

Todista, että

$$I = \{f \in C([0, 1], \mathbb{R}) \mid f(0) = f(1) = 0\}$$

on  $C([0, 1], \mathbb{R})$ :n ideaali ja tekijärengas  $C([0, 1], \mathbb{R})/I$  on isomorfinen tulorengaan  $\mathbb{R} \times \mathbb{R}$  kanssa. Ohje: Tutki kuvausta  $f \rightarrow (f(0), f(1))$ .

5. Jaa alkutekijöihin polynomi  $x^3 - x + 1$  renkaissa  $\mathbb{Z}_3[x]$  ja  $\mathbb{Z}_5[x]$ .



HELSINGIN YLIOPISTO  
HELSINGFORS UNIVERSITET  
UNIVERSITY OF HELSINKI

Matematiikan ja tilastotieteen laitos  
Algebra I  
Erilliskoe, 22.1.2009

1. Olkoon  $A = \{1, 2, 3, 4, 5\}$  ja  $f : A \rightarrow A$  se kuvaus, jolla  $f(1) = f(3) = 2$ ,  $f(2) = f(4) = 4$  ja  $f(5) = 1$ . Olkoon edelleen  $A_0 = \{4\} \subset A$  ja  $A_n = f^{-1}(A_{n-1})$  kaikilla  $n \in \mathbb{N}$ ,  $n \geq 1$ . Luettele joukon  $A_n$  alkioit jokaisella  $n \geq 1$ .
2. Selvitä, onko luku  $2009^{2009} + 2005$  jaollinen luvulla 13.
3. Olkoot  $H$  ja  $K$  multiplikatiivisen ryhmän  $G$  aliryhmiä. Osoita: Jos on olemassa sellaiset  $a, b \in G$ , että  $aH = bK$ , niin  $H = K$ .
4. Osoita, että  $R = \{m/7^n \mid m \in \mathbb{Z}, n \in \mathbb{N}\}$  on rationaalilukujen renkaan  $\mathbb{Q}$  alirengas. Mitkä alkioit ovat kääntyviä (eli yksiköitä) renkaassa  $R$ ?
5. Etsi polynomirenkaan  $\mathbb{Z}_2[x]$  kaikki jaottomat alkioit, joiden aste on korkeintaan kolme (niitä löytynee 5 kpl). Tutki, onko neljännen asteen polynomi  $x^4 + x^2 + 1 \in \mathbb{Z}_2[x]$  jaoton.

1. Ajatellaan kokonaisluvut määritellyiksi luonnollisten lukujen *muodollisina* (eli merkityinä, ei siis vielä "suoritettavina") erotuksina  $m - n$ , joille on asetettu identtisyysehto

$$m - n = p - q \iff m + q = n + p.$$

a) Osoita, että tämä symbolilla  $=$  merkitty relaatio on todellisuudessa (vain) ekvivalenssi luonnollisten lukujen muodollisten erotusten joukossa.

b) Millä kaavoilla kokonaislukujen yhteenlasku ja kertolasku nyt määritellään luonnollisten lukujen yhteen- ja kertolaskujen avulla? (Ajattele  $\mathbb{Z}$ :n laskusääntöjen nojalla, minkälaiset kaavojen on oltava.)

c) Osoita, että tämä kokonaislukujen yhteenlasku on hyvinmääritelty: jos yhteenlaskettavat erotukset vaihdetaan näiden kanssa identtisiin erotuksiin, niin yhteenlaskun tulokseksi saatava erotus on identtinen alkuperäisen yhteenlaskun tuloksen kanssa.

2. Olkoon  $G$  (multiplikatiivinen) ryhmä ja  $H$ ,  $K$  sekä  $L$  ryhmän  $G$  äärellisiä aliryhmiä, joiden kertaluvut eli alkioiden lukumäärät ovat  $|H| = 15$ ,  $|K| = 21$  ja  $|L| = 35$ . Osoita, että  $H \cap K \cap L = \{1_G\}$ .

3. Olkoon  $G = S_{\mathbb{N}}$  luonnollisten lukujen joukon  $\mathbb{N}$  permutaatioryhmä eli bijektioiden  $f: \mathbb{N} \rightarrow \mathbb{N}$  joukko laskutoimituksena kuvausten yhdistäminen. Kutsukaamme bijektiota  $f \in G$  *melkein identtiseksi*, jos jollekin luvulle  $m_f \in \mathbb{N}$  pätee, että  $f(n) = n$ , kun  $n \geq m_f$ . Olkoon  $H$  melkein identtisten bijektioiden  $f \in G$  joukko. Osoita, että  $H$  on  $G$ :n normaali aliryhmä.

4. Olkoon  $R$  rengas, ja olkoon  $Y_2(R)$  kaikkien  $R$ -kertoimisten 2-rivisten yläkolmiomatriisien  $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$  ( $a, b, c \in R$ ,  $0 = 0_R$ ) joukko varustettuna matriisien tavanomaisilla yhteen- ja kertolaskuilla:

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} + \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} = \begin{pmatrix} a + a' & b + b' \\ 0 & c + c' \end{pmatrix}; \quad \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} = \begin{pmatrix} aa' & ab' + bc' \\ 0 & cc' \end{pmatrix}.$$

Pidetään tunnettuna, että tällöin  $Y_2(R)$  on rengas (tämä voidaan todistaa aivan kuten  $\mathbb{R}$ -kertoimisten matriisien tapauksessa; ei todellakaan tarvitse olettaa, että rengas  $R$  olisi kommutatiivinen). Osoita nyt, että joukko  $J = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \mid b \in R \right\} \subset Y_2(R)$  on renkaan  $Y_2(R)$  ideaali ja että tekijärenkas  $Y_2(R)/J$  on isomorfinen tulorenkaan  $R \times R$  kanssa; anna myös tämä isomorfismi. **Ohje.** Sovella renkaiden homomorfialausetta kuvaukseen  $f: Y_2(R) \rightarrow R \times R$ , jolla  $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto (a, c)$ .

5. Esitä polynomi  $f = x^4 - 5x^3 + x^2 - 2x - 15$  renkaassa  $\mathbb{Q}[x]$  jaottomien polynomien tulona.



1. Määritellään kuvaus  $f: \mathbb{N} \rightarrow \mathbb{N}$  asettamalla  $f(0) = 1$  sekä kullakin  $n \in \mathbb{N}$  rekursiivisesti

$$f(n+1) = \begin{cases} f(n)/2, & \text{jos } f(n) \text{ on parillinen;} \\ 5f(n) + 1, & \text{jos } f(n) \text{ on pariton.} \end{cases}$$

Osoita, että  $f(n+7) = f(n)$  kaikilla  $n \in \mathbb{N}$ , ja määritä  $f$ :n kuvajoukko  $f(\mathbb{N})$ .

2. Käyttämällä Eukleideen algoritmia **a)** osoita, että luvut 725 ja 147 ovat keskenään jaottomat, ja **b)** etsi kokonaisluvut  $x$  ja  $y$ , joilla  $725x + 147y = 1$ .

3. Olkoon  $G$  multiplikatiivinen ryhmä. Määritä ne parit  $(a, b) \in G \times G$ , joilla kuvaus  $f: G \rightarrow G$ , jolla  $f(x) = axb$  kaikilla  $x \in G$ , on ryhmähomomorfismi.

4. Olkoon  $R$  rengas. Määritä ne parit  $(a, b) \in R \times R$ , joilla kuvaus  $f: R \rightarrow R$ , jolla  $f(x) = axb$  kaikilla  $x \in R$ , on rengashomomorfismi. **Vihje ja varoitus.** Tulos on samantapainen kuin ryhmille tehtävässä 3, mutta todistus on juonikkaampi.

5. Palautetaan mieleen, että jos  $n \in \mathbb{N}_+$ , niin kokonaislukujen jäännösluokkien modulo  $n$  joukko  $\mathbb{Z}_n$  on rengas luonnollisten laskutoimitustensa suhteen.

**a)** Määritä renkaan  $\mathbb{Z}_9$  kääntyvien alkioiden multiplikatiivisen ryhmän  $G = \mathbb{Z}_9^*$  alkioita ja kertotaulukko.

**b)** Osoita, että  $G$  on syklinen ryhmä, ja anna sopivalla  $n \in \mathbb{N}_+$  jokin ryhmäisomorfismi additiiviselta ryhmältä  $\mathbb{Z}_n$  ryhmälle  $G$ .

**c)** Määritä  $G$ :n kunkin alkion virittämä  $G$ :n aliryhmä.