Algebran ja lukuteorian harjoitustehtäviä

Versio 1.0 (27.1.2006)
Turun yliopisto

Lukuteoria

1. Tutki, ovatko seuraavat relaatiot ekvivalenssirelaatioita joukon $\mathbb{N}$ kaikkien osajoukkojen joukolla:

a) $C \sim D \iff$ on olemassa bijektio $f : C \to D$,

b) $C \sim D \iff$ on olemassa injektio $f : C \to D$.

Vastaus: **a)** Kyllä. **b)** Ei.

2. Olkoon joukon $\mathbb{R} \times \mathbb{R}$ relaatio ρ määritelty ehdolla

$$(a, b)\, \rho (c, d) \qquad \text{joss} \qquad a = d \text{ ja } b = c.$$

Onko tämä relaatio

a) refleksiivinen,

b) symmetrinen,

c) transitiivinen?

Vastaus: **a)** Ei. **b)** On. **c)** Ei.

3. Etsi jokin edustajisto seuraaville annetun joukon A ekvivalenssirelaatioille $\sim$:

a) $A = \mathbb{Z} \times \mathbb{Z}$, $(a, b) \sim (c, d)$, joss $a - c$ ja $b - d$ ovat molemmat parillisia.

b) $A = \mathcal{M}_{2\times 2}(\mathbb{R})$, $P \sim Q$, joss $\det P = \det Q$.

4. Olkoon $a \in \mathbb{Z}$. Osoita, että luku $a^2 + 1$ ei ole neljällä jaollinen.

5. Etsi kaikki sellaiset positiiviset kokonaisluvut n, että luvuista n, $n+2$ ja $n+4$ jokainen on alkuluku.

Vastaus: Ainoa ratkaisu on $n = 3$.

6. Laske $\text{syt}(242963, 702191)$ ja esitä se muodossa $242963u + 702191v$, missä $u, v \in \mathbb{Z}$.

Vastaus: $\text{syt}(242963, 702191) = 7 = 242963 \cdot (-6286) + 702191 \cdot 2175$.

7. Osoita, että $\text{syt}(8a + 3, 5a + 2) = 1$, aina kun $a \in \mathbb{Z}$

Vihje: Tutki erikseen tapaukset $a > 0$, $a = 0$ ja $a < 0$.

8. Olkoon n jokin luonnollinen luku, $n > 1$. Merkitään $N = n! + 1$. Osoita, että

a) luvun N kaikki alkutekijät p toteuttavat ehdon $p > n$,

b) luvuista $N + 1$, $N + 2$, ..., $N + n - 1$ ei yksikään ole alkuluku.

9. Etsi kussakin kohdassa kaikki sellaiset positiiviset kokonaisluvut m, että annettu kongruenssi on voimassa:

a) $27 \equiv 4 \pmod{m}$

b) $1000 \equiv 1 \pmod{m}$

c) $1331 \equiv 0 \pmod{m}$

Vihje: Tutki lukujen $27 - 4$, $1000 - 1$ ja 1331 alkutekijähajotelmia.

Vastaus: **a)** 23. **b)** 3, 9, 27, 37, 111, 333, 999. **c)** 11, 121, 1331.

10. Laske luvun $n = 1! + 2! + 3! + \cdots + 100!$ pienin ei-negatiivinen jäännös

a) modulo 5,

b) modulo 7,

c) modulo 48.

Vihje: Kuinka pitkälle kyseisen luvun kertomatermejä on laskettava?

Vastaus: **a)** 3, **b)** 5, **c)** 9.

11. Osoita, että Diofantoksen yhtälöllä $5x^2 - 3y^2 = 7$ ei ole yhtään kokonaislukuratkaisua.

12. Etsi luvun $2 \cdot 4^n + 3 \cdot 9^n$ pienin alkutekijä kun n on positiivinen kokonaisluku.

Vihje: Tarkastele aluksi kyseistä lukua arvoilla $n = 1, 2, 3, \ldots$ ja yritä havaita jokin kaava pienimmälle alkutekijälle.

Vastaus: 5.

13. Lukuja $F_n = 2^{2^n} + 1$, $n \in \mathbb{Z}_{\geq 0}$, sanotaan *Fermat'n luvuiksi*. Osoita, että Fermat'n luvut ovat pareittain suhteellisia alkulukuja, tai siis kahden erisuuren Fermat'n luvun F_m ja F_n suurin yhteinen tekijä on 1.

Vihje: Osoita ensin, että $F_n = (F_{n-i} - 1)^{2^i} + 1$ kaikilla $0 \leq i \leq n$.

14. Todista: Olkoot a, c ja $m > 0$ kokonaislukuja ja d lukujen a ja m suurin yhteinen tekijä. Kongruenssiyhtälö

$$ax \equiv c \pmod{m}$$

on ratkeava, jos ja vain jos d jakaa luvun c. Jos yhtälö on ratkeava, sillä on täsmälleen d erisuurta ratkaisua välillä $0 \leq x \leq m - 1$.

15. Etsi kokeilemalla kongruenssiyhtälöiden $4x \equiv 6 \pmod{10}$ ja $3x \equiv 7 \pmod{10}$ kaikki ratkaisut $0 \leq x \leq 9$.

Vastaus: 4 ja 9; 9.

16. Osoita, ettei luku $2^{32} + 1$ ole alkuluku.

Vihje 1: Kyseinen luku on jaollinen luvulla 641.

Vihje 2: Kongruenssiyhtälöistä $5 \cdot 2^7 \equiv -1 \pmod{641}$ ja $5^4 \equiv -2^4 \pmod{641}$ voi olla apua.

17. Mikä on luvun 1234^{1234} jakojäännös, kun sitä jaetaan luvulla 7?

Vihje: Tutki ensin luvun 1234 jakojäännöstä.

Vastaus: 2.

18. Osoita, ettei yhtälöllä $x^3 = 3 + 6y^3$ ole kokonaislukuratkaisuja.

Vihje: Tutki yhtälöä modulo 7.

Ryhmät

19. Osoita, että parillisten kokonaislukujen joukko $2\mathbb{Z}$ muodostaa ryhmän kokonaislukujen yhteenlaskun suhteen.

20. Olkoon G ryhmä. Todista seuraavat väitteet:

a) Jos G on kommutatiivinen ryhmä, niin $(ab)^2 = a^2b^2$ kaikilla $a, b \in G$.

b) Jos $(ab)^2 = a^2b^2$ kaikilla $a, b \in G$, niin G on kommutatiivinen.

c) Jos $a^2 = 1$ kaikilla $a \in G$, niin G on kommutatiivinen.

21. Laadi ryhmän $\mathbb{Z}_9^*$ ryhmätaulu ja ratkaise sen avulla ryhmässä yhtälö $\overline{7}x = \overline{5}$.

Vastaus: $x = \overline{2}$.

22. Olkoon $S_n = \{\alpha \mid \alpha : \mathbb{N}_n \to \mathbb{N}_n \text{ on bijektio}\}$, missä $\mathbb{N}_n = \{1, 2, \ldots, n\}$. Olkoon $G = (S_n, \circ)$, missä $(\alpha \circ \beta)(x) = \alpha(\beta(x))$, kaikilla $\alpha, \beta \in S_n$ ja $x \in \mathbb{N}_n$.

a) Osoita, että G on ryhmä.

b) Onko $H = \{\alpha \in S_n \mid \alpha(1) = 1\}$ ryhmän G aliryhmä?

c) Onko $K = \{\alpha \in S_n \mid \alpha(1) \neq 1\}$ ryhmän G aliryhmä?

Vastaus: **b)** On. **c)** Ei ole.

23. Mistä alkioista ryhmän $\mathbb{R}^*$ aliryhmä $< S >$ koostuu, kun

a) $S = \{-1\}$,

b) $S = \{3\}$,

c) $S = 2\mathbb{Z}$?

Vastaus: **a)** $< S > = \{\pm 1\}$. **b)** $< S > = \{3^n \mid n \in \mathbb{Z}\}$. **c)** $< S > = \mathbb{Q}^*$.

24. Olkoon G ryhmä, $a \in G$ ja luvut $m, n \in \mathbb{Z}$ suhteellisia alkulukuja. Oletetaan, että $a^m = 1$. Osoita, että on olemassa sellainen $b \in G$, että $a = b^n$.

25. Tutki, ovatko seuraavat ryhmät syklisiä:

a) $\mathbb{Z}_2 \times \mathbb{Z}_3$,

b) $\mathbb{Z}_2 \times \mathbb{Z}_4$.

Vastaus: **a)** On. **b)** Ei ole.

26. Olkoon G ryhmä, joka ei ole kommutatiivinen. Osoita, että ryhmällä G on ainakin kolme eri aliryhmää.

Vihje: Ajattele ryhmän generoivaa joukkoa.

27. Osoita, että joukko

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\}$$

muodostaa ryhmän matriisikertolaskun suhteen.

28. Osoita, että neliöt

$$QR_m = \{\overline{a}^2 \mid \overline{a} \in \mathbb{Z}_m^*\}$$

muodostavat ryhmän $\mathbb{Z}_m^*$ aliryhmän. Luettele ryhmien QR_7, QR_8 ja QR_{11} alkiot.

Vastaus: $QR_7 = \{\overline{1}, \overline{-3}, \overline{2}\}$, $QR_8 = \{\overline{1}\}$, $QR_{11} = \{\overline{1}, \overline{4}, \overline{-2}, \overline{5}, \overline{3}\}$.

29. Osoita, ettei ryhmä $G = Z_{12}^*$ ole syklinen. Etsi jotkin kaksi alkiota, jotka generoivat koko ryhmän G.

30.

a) Montako alkiota on ryhmässä $\mathbb{Z}_{17}^*$?

b) Osoita, että $\overline{3}^2 \not\equiv \overline{1}$, $\overline{3}^4 \not\equiv \overline{1}$ ja $\overline{3}^8 \not\equiv \overline{1}$ ryhmässä $\mathbb{Z}_{17}^*$.

c) Osoita a- ja b-kohtien avulla, että Z_{17}^* on syklinen ryhmä.

Vastaus: a) 16.

31. Olkoon $G = \mathbb{Z}_{109}^*$ ja H alkion $\overline{23}$ generoima ryhmän G aliryhmä. Tutki, mitkä ryhmän G alkiot kuuluvat aliryhmään H.

Vihje 1: Ryhmän G alkiot $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{108}$ voi olla mukavampaa ajatella muodossa

$$\overline{-54}, \overline{-53}, \ldots, \overline{-1}, \overline{0}, \overline{1}, \ldots, \overline{54}.$$

Vihje 2: Ratkaise ensin ord($\overline{23}$).

Vihje 3: Yritä löytää jokin pieni positiivinen luku n, jolla $< \overline{n} > = < \overline{23} >$.

32. Olkoon G joukko, $\mathcal{O}$ joukko siinä määriteltyjä binäärioperaatioita (paria $(G, \mathcal{O})$ kutsutaan *algebraksi*, ryhmä on siis eräs erikoistapaus algebrasta) ja $\sim$ ekvivalenssirelaatio joukossa G. Relaatiota $\sim$ sanotaan *kongruenssiksi*, jos se täyttää ehdon

$$\text{jos } a \sim b \text{ ja } c \sim d, \qquad \text{niin} \qquad (a * c) \sim (b * d),$$

kaikilla joukon $\mathcal{O}$ operaatioilla $*$ ja joukon G alkioilla a, b, c ja d (vertaa lukukongruenssiin).

a) Osoita, että ehdolla

$$[a] * [b] = [a * b]$$

määritelty joukon $G/\sim$ binäärioperaatio on hyvin määritelty eli ehdoista $[a] = [b]$ ja $[c] = [d]$ seuraa $[a] * [c] = [b] * [d]$, jos $\sim$ on kongruenssi. (Tämä merkitsee, että $(G/\sim, \mathcal{O})$ on algebra, jos $\sim$ on kongruenssi.)

b) Olkoon nyt $\mathcal{O} = \{*\}$ ja $(G, *)$ (kommutatiivinen) ryhmä, jonka neutraalialkio on e. Osoita, että myös $G/\sim$ on (kommutatiivinen) ryhmä, ts. kaikki (kommutatiivisen) ryhmän ehdot periytyvät ryhmältä G algebralle $G/\sim$, jos $\sim$ on kongruenssi.

c) Osoita, että jos H on ryhmän G normaali aliryhmä ja $\sim$ ehdolla

$$b \sim a, \text{ jos ja vain jos } b \in a * H$$

määritelty ekvivalenssirelaatio, niin $\sim$ on kongruenssi.

d) Osoita, että $[e]$ on ryhmän G normaali aliryhmä, jos $\sim$ on kongruenssi.

33. Määrää ryhmän $G = \mathbb{Z}_{15}^*$ aliryhmän $A = \{\overline{1}, \overline{4}\}$ kaikki sivuluokat.

34. Tutkitaan ryhmää $G = \mathbb{Z}_2 \times \mathbb{Z}_6$, missä $(a, b) + (c, d) = (a + c, b + d)$, aina kun $(a, b), (c, d) \in G$. Olkoon H alkion $(\overline{1}, \overline{3})$ generoima ryhmän G aliryhmä.

a) Miksi H on välttämättä normaali aliryhmä?

b) Kuinka monta alkiota aliryhmässä H on?

c) Jaa koko ryhmä G aliryhmän H (vasempiin) sivuluokkiin, ja etsi jokin sivuluokkien edustajisto.

d) Kirjoita edustajiston avulla ryhmän G/H ryhmätaulu.

e) Onko G/H syklinen ryhmä?

Vastaus: **a)** Koska G on Abelin ryhmä. **b)** 2.
c) $G = \big((\overline{0}, \overline{0}) + H\big) \cup \big((\overline{0}, \overline{1}) + H\big) \cup \big((\overline{0}, \overline{2}) + H\big) \cup \big((\overline{0}, \overline{3}) + H\big) \cup \big((\overline{0}, \overline{4}) + H\big) \cup \big((\overline{0}, \overline{5}) + H\big)$.
d)

$+$	$(\overline{0}, \overline{0}) + H$	$(\overline{0}, \overline{1}) + H$	$(\overline{0}, \overline{2}) + H$	$(\overline{0}, \overline{3}) + H$	$(\overline{0}, \overline{4}) + H$	$(\overline{0}, \overline{5}) + H$
$(\overline{0}, \overline{0}) + H$	$(\overline{0}, \overline{0}) + H$	$(\overline{0}, \overline{1}) + H$	$(\overline{0}, \overline{2}) + H$	$(\overline{0}, \overline{3}) + H$	$(\overline{0}, \overline{4}) + H$	$(\overline{0}, \overline{5}) + H$
$(\overline{0}, \overline{1}) + H$	$(\overline{0}, \overline{1}) + H$	$(\overline{0}, \overline{2}) + H$	$(\overline{0}, \overline{3}) + H$	$(\overline{0}, \overline{4}) + H$	$(\overline{0}, \overline{5}) + H$	$(\overline{0}, \overline{0}) + H$
$(\overline{0}, \overline{2}) + H$	$(\overline{0}, \overline{2}) + H$	$(\overline{0}, \overline{3}) + H$	$(\overline{0}, \overline{4}) + H$	$(\overline{0}, \overline{5}) + H$	$(\overline{0}, \overline{0}) + H$	$(\overline{0}, \overline{1}) + H$
$(\overline{0}, \overline{3}) + H$	$(\overline{0}, \overline{3}) + H$	$(\overline{0}, \overline{4}) + H$	$(\overline{0}, \overline{5}) + H$	$(\overline{0}, \overline{0}) + H$	$(\overline{0}, \overline{1}) + H$	$(\overline{0}, \overline{2}) + H$
$(\overline{0}, \overline{4}) + H$	$(\overline{0}, \overline{4}) + H$	$(\overline{0}, \overline{5}) + H$	$(\overline{0}, \overline{0}) + H$	$(\overline{0}, \overline{1}) + H$	$(\overline{0}, \overline{2}) + H$	$(\overline{0}, \overline{3}) + H$
$(\overline{0}, \overline{5}) + H$	$(\overline{0}, \overline{5}) + H$	$(\overline{0}, \overline{0}) + H$	$(\overline{0}, \overline{1}) + H$	$(\overline{0}, \overline{2}) + H$	$(\overline{0}, \overline{3}) + H$	$(\overline{0}, \overline{4}) + H$

e) On.

35. Tutki, mitkä seuraavista kuvauksista ovat homomorfismeja:

a) $f : \mathbb{R} \to \mathbb{R}^*$, $f(x) = 2^x$,

b) $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = x + 1$,

c) $f : \mathbb{R}^* \to \mathbb{R}^*$, $f(x) = |x|$.

Vastaus: **a)** On. **b)** Ei ole. **c)** On.

36. Oletetaan, että ryhmät G ja G_1 ovat isomorfiset. Todista seuraavat väitteet:

a) Jos G on Abelin ryhmä, myös G_1 on Abelin ryhmä.

b) Jos G on syklinen ryhmä, myös G_1 on syklinen.

37. Tutki, ovatko seuraavat ryhmät isomorfiset:

a) $(\mathbb{R}^2, +)$ ja $(\mathbb{C}, +)$,

b) $\mathbb{Z}$ ja $\mathbb{Z} \times \mathbb{Z}$.

Vihje: Voivatko alkioista $(1,0)$ ja $(1,1)$ molemmat kuulua homomorfismin $f : \mathbb{Z} \to \mathbb{Z}\times\mathbb{Z}$ kuvaan $\mathrm{Im}(f)$?

Vastaus: **a)** Ovat. **b)** Eivät ole.

38.

a) Olkoot G ja G' ryhmiä, $f : G \to G'$ isomorfismi ja $c \in G$. Osoita, että

$$\mathrm{ord}(c) = \mathrm{ord}(f(c)).$$

b) Olkoon G ryhmä ja $a, b \in G$. Millainen kaava saadaan a-kohdan tuloksesta, kun tarkastellaan isomorfismia $f : G \to G$, $f(x) = axa^{-1}$ ja valitaan $c = ba$.

Vastaus: **b)** $\mathrm{ord}(ba) = \mathrm{ord}(ab)$.

39. Etsi ryhmästä $\mathbb{Z}_{17}^*$ jokin kertalukua 16 oleva alkio. Konstruoi sitten isomorfismi ryhmien $\mathbb{Z}_{17}^*$ ja $\mathbb{Z}_{16}$ välille.

Vihje: Mitä vaihtoehtoja ryhmän $\mathbb{Z}_{17}^*$ alkioiden kertaluvuilla on?

40. Osoita, että funktiot

$$f(x) = \begin{pmatrix} \cos x & \sin x \\ -\sin x & \cos x \end{pmatrix} \qquad \text{ja} \qquad g(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

ovat homomorfismeja ryhmältä $(\mathbb{R}, +)$ ryhmään $GL_2(\mathbb{R})$. Mitkä ovat niiden ytimet?

Vihje: Tarvitset trigonometrian kaavoja

$$\sin(x+y) = \sin x \cos y + \cos x \sin y \quad \text{ja} \quad \cos(x+y) = \cos x \cos y - \sin x \sin y$$

eli sinin ja kosinin summakaavoja. Jälkimmäisen näistä saa todistettua huomaamalla, että yksikköympyrän pisteiden $\big(\cos(x+y), \sin(x+y)\big)$ ja $(\cos 0, \sin 0) = (1,0)$ välimatka toisiinsa on täsmälleen sama kuin $-y$ asteen verran kierrettyjen pisteiden $(\cos x, \sin x)$ ja $\big(\cos(-y), \sin(-y)\big) = (\cos y, -\sin y)$ välimatka, eli

$$\big(\cos(x+y) - 1\big)^2 + \big(\sin(x+y) - 0\big)^2 = (\cos x - \cos y)^2 + (\sin x + \sin y)^2.$$

Haluttu kaava saadaan tästä sieventämällä, kun muistetaan, että $\sin^2 x + \cos^2 x = 1$ (kateettien neliöiden summa on hypotenuusan neliö, joka yksikköympyrän tapauksessa on yksi).

Tämän jälkeen saadaan todistettua kaavat $\cos(\pi/2 - x) = \sin x$ ja $\sin(\pi/2 - x) = \cos x$ tässä järjestyksessä. Näiden kahden ja kosinin summakaavan avulla saadaan lopulta sinin summakaava.

41. On olemassa homomorfismi $f : \mathbb{Z}_{12} \to \mathbb{Z}_{20}$, joka määräytyy ehdosta $f(\overline{1}) = \overline{5}$. Luettele muiden alkioiden kuvat. Määrää tämän homomorfismin ydin ja kuva.

42. Luettele ryhmän $G = \mathbb{Z}_{18}^*$ alkiot. Osoita, että G on syklinen. Etsi sitten sen kaikki aliryhmät.

Vihje: Kuinka suuri kertaluku ryhmällä G on? Minkä additiivisen ryhmän kanssa G on silloin isomorfinen?

Renkaat

43. Anna esimerkki joukoista A ja R, $A \subset R$, sekä joukossa R määritellyistä binäärioperaatioista $+$ ja $\cdot$, joilla

a) $(A, +, \cdot)$ ja $(R, +, \cdot)$ ovat renkaita, mutta $(A, +, \cdot)$ ei ole renkaan $(R, +, \cdot)$ alirengas,

b) lisäksi $(A, +, \cdot)$ ei ole nollarengas,

c) lisäksi A on ääretön joukko.

44. Seuraavassa esitetään joitakin rationaalilukujen joukon $\mathbb{Q}$ osajoukkoja, joiden määritelmissä murtoluku $\frac{m}{n}$ tarkoittaa aina supistettua murtolukua, jossa siis osoittajan m ja nimittäjän n suurin yhteinen tekijä on yksi ($m, n \in \mathbb{Z}$, $n > 0$). Mitkä näistä osajoukoista ovat rationaalilukujen renkaan alirenkaita?

a) $R_1 = \{\frac{m}{n} \mid n \text{ on pariton}\}$,

b) $R_2 = \{\frac{m}{n} \mid m \text{ on pariton}\}$,

c) $R_3 = \{\frac{m}{n} \mid n \text{ on kakkosen potenssi}\}$.

d) Määritä vielä löytämiesi renkaiden yksikköryhmät.

45. Olkoon $\mathbb{R}_{>0}$ positiivisten reaalilukujen joukko. Määritellään siinä uudet yhteenlasku- ($\oplus$) ja kertolaskuoperaatiot ($*$) säännöillä

$$x \oplus y = x \cdot y \qquad \text{ja} \qquad x * y = x^{\lg y},$$

missä $\lg y$ tarkoittaa luvun y kymmenkantaista logaritmia. Osoita, että $(\mathbb{R}_{>0}, \oplus, *)$ on kommutatiivinen rengas.

46. Tutki, muodostavatko seuraavat matriisijoukot renkaan $\mathcal{M}_3(\mathbb{R})$ alirenkaan:

a) $S_1 = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{R} \right\}$,

b) $S_2 = \left\{ \begin{pmatrix} a & 0 & b \\ 0 & 0 & 0 \\ 0 & 0 & c \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{R} \right\}$,

c) $S_3 = \left\{ \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} \;\middle|\; a, b, c, d, e, f \in \mathbb{R} \right\}$.

Vastaus: **a)** Ei, **b)** ei, **c)** kyllä.

47. Olkoon $(\mathbb{H}, +, \cdot)$, $\mathbb{H} = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mid a, b, c, d \in \mathbb{R}\}$, ns. *kvaternionirengas*, jonka nolla- ja ykkösalkiot ovat $0_{\mathbb{H}} = 0$ ja $1_{\mathbb{H}} = 1$, jonka operaatiot $+$ ja $\cdot$ rajoitettuna reaaliluvuille $\mathbb{R}$ ovat reaalilukujen tavanomaiset yhteen- ja kertolaskut ja jossa pätee laskusäännöt:

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1, \quad \mathbf{ij} = \mathbf{k}, \quad \mathbf{jk} = \mathbf{i}, \quad \mathbf{ki} = \mathbf{j}$$

ja

$$a\mathbf{i} = \mathbf{i}a, \quad a\mathbf{j} = \mathbf{j}a, \quad a\mathbf{k} = \mathbf{k}a,$$

aina kun $a \in \mathbb{R}$.

a) Laske **ji**, **kj** ja **ik**.

b) Olkoon kvaternionin $q = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ *konjugaattikvaternioni* alkio $\overline{q} = a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}$. Laske $q\overline{q}$.

c) Osoita, että renkaan $\mathbb{H}$ yksikköryhmä on $\mathbb{H}^* = \mathbb{H} \setminus \{0_{\mathbb{H}}\}$.

d) Merkitään $M(z_1, z_2) = \left(\begin{smallmatrix} z_1 & z_2 \\ -\overline{z_2} & \overline{z_1} \end{smallmatrix}\right)$ kaikilla $z_1, z_2 \in \mathbb{C}$. Osoita, että joukko

$$\mathbb{H}' = \{M(z_1, z_2) \mid z_1, z_2 \in \mathbb{C}\}$$

muodostaa renkaan $\mathcal{M}_2(\mathbb{C})$ alirenkaan.

e) Osoita, että renkaat $\mathbb{H}$ ja $\mathbb{H}'$ ovat isomorfiset.

48. Osoita, että renkaan

$$\mathbb{Z}[\mathrm{i}] = \{a + b\mathrm{i} \mid a, b \in \mathbb{Z}\}$$

kaikki yksiköt ovat 1, i, -1 ja $-\mathrm{i}$.

Vihje: Jos $z = a + b\mathrm{i}$, niin $z\overline{z} = a^2 + b^2$. Jos $z_1 z_2 = 1$, niin $z_1 z_2 \overline{z_1 z_2} = 1$.

49. Olkoon R rengas. Alkioiden $a, b \in R$ sanotaan *kommutoivan*, jos $ab = ba$ (kommutatiivisessa renkaassa siis kaikki alkiot kommutoivat toistensa kanssa). Osoita, että a ja b kommutoivat, jos ja vain jos kaikilla kokonaisluvuilla $n > 1$ pätee yhtälö

$$(a - b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + ab^{n-2} + b^{n-1}) = a^n - b^n.$$

50. Renkaan R alkiota a sanotaan *nilpotentiksi*, jos $a^n = 0$, jollakin kokonaisluvulla $n > 0$.

a) Mitä nilpotentteja alkioita on renkaassa $\mathbb{Z}_{16}$?

b) Entä renkaassa $\mathbb{Z}_{15}$?

c) Osoita, että jos $a \in R$ on nilpotentti, niin $1 - a \in R^*$.

Vastaus: **a)** $\overline{0}$, $\overline{\pm 2}$, $\overline{\pm 4}$, $\overline{\pm 6}$ ja $\overline{8}$. **b)** $\overline{0}$.

51. Olkoon R joukko, $\mathcal{O}$ joukko siinä määriteltyjä binäärioperaatioita (paria $(R, \mathcal{O})$ kutsutaan *algebraksi*, rengas on siis eräs erikoistapaus algebrasta) ja $\sim$ ekvivalenssirelaatio joukossa R. Relaatiota $\sim$ sanotaan *kongruenssiksi*, jos se täyttää ehdon

$$\text{jos } a \sim b \text{ ja } c \sim d, \qquad \text{niin} \qquad (a * c) \sim (b * d),$$

kaikilla joukon $\mathcal{O}$ operaatioilla $*$ ja joukon R alkioilla a, b, c ja d (vertaa lukukongruenssiin).

a) Osoita, että ehdolla

$$[a] * [b] = [a * b]$$

määritelty joukon $R/\sim$ binäärioperaatio on hyvin määritelty eli ehdoista $[a] = [b]$ ja $[c] = [d]$ seuraa $[a] * [c] = [b] * [d]$, jos $\sim$ on kongruenssi. (Tämä merkitsee, että $(R/\sim, \mathcal{O})$ on algebra, jos $\sim$ on kongruenssi.)

b) Olkoon nyt $\mathcal{O} = \{+, \cdot\}$ ja $(R, +, \cdot)$ (kommutatiivinen) rengas. Osoita, että myös $R/\sim$ on (kommutatiivinen) rengas, ts. kaikki (kommutatiivisen) renkaan ehdot periytyvät renkaalta R algebralle $R/\sim$, jos $\sim$ on kongruenssi.

c) Osoita, että jos I on renkaan R ihanne ja $\sim$ ehdolla

$$b \sim a, \text{ jos ja vain jos } b \in a + I$$

määritelty ekvivalenssirelaatio, niin $\sim$ on kongruenssi.

d) Osoita, että $[0_R]$ on renkaan R ihanne, jos $\sim$ on kongruenssi.

52.

Osoita, että matriisirenkaalla $R = \mathcal{M}_2(\mathbb{R})$ ei ole kuin triviaalit ihanteet $\{0\}$ ja R.

Vihje 1: Oleta, että I on jokin mielivaltaisesti valittu, nollasta eroava, renkaan R ihanne ja $\alpha \in I$ nollamatriisista eroava matriisi. Osoita ensin, että ihanteessa I on tällöin sellainen matriisi, jossa on tasan yksi nollasta eroava alkio.

Vihje 2: Jatka sitten osoittamalla, että ihanteessa I on sellaisia matriiseja, joissa on tasan yksi nollasta eroava alkio määrätyssä paikassa (vasemmassa yläkulmassa, oikeassa yläkulmassa, jne.)

Vihje 3: Kolmanneksi näytä, että ihanteessa I on ainakin yksi säännöllinen matriisi.

Vihje 4: Ensimmäisen vihjeen osoittamiseksi tutki matriisin α kertomista eri puolilta matriiseilla $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) \in R$. Toisessa vihjeessä voit puolestaan käyttää matriisia $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \in R$.

53.

a) Luettele kaikki ryhmähomomorfismit $f : \mathbb{Z}_6 \to \mathbb{Z}_2$.

b) Mitkä näistä homomorfismeista ovat myös rengashomomorfismeja?

c) Miten tilanne muuttuu, kun edellä $\mathbb{Z}_6$ ja $\mathbb{Z}_2$ vaihtavat paikkaa?

54.

a) Osoita, että yläkolmiomatriisit

$$U_2(\mathbb{R}) = \left\{ \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \;\middle|\; a, b, d \in \mathbb{R} \right\}$$

muodostavat renkaan.

b) Osoita, että $(\mathbb{R}^2, +, \cdot)$ on rengas, kun binäärioperaatiot määritetään ehdoilla

$$(a, b) + (c, d) = (a + c, b + d), \quad (a, b) \cdot (c, d) = (a \cdot c, b \cdot d).$$

c) Osoita, että ehto

$$f : \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \mapsto (a, d)$$

määrittelee rengashomomorfismin $f : U_2(\mathbb{R}) \to \mathbb{R}^2$.

d) Määritä $\mathrm{Ker}(f)$ ja $\mathrm{Im}(f)$.

e) Minkälaisen isomorfian renkaiden homomorfialause antaa d-kohdan tilanteessa?

f) Onko renkaalla $U_2(\mathbb{R})$ sellaista alirengasta, joka olisi isomorfinen renkaan $\mathbb{R}^2$ kanssa?

Vastaus: **d)** $\mathrm{Ker}(f) = \left\{ \left(\begin{smallmatrix} 0 & b \\ 0 & 0 \end{smallmatrix}\right) \mid b \in \mathbb{R} \right\} =: \left(\begin{smallmatrix} 0 & \mathbb{R} \\ 0 & 0 \end{smallmatrix}\right)$ ja $\mathrm{Im}(f) = \mathbb{R}^2$.
f) On: $\left\{ \left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right) \mid a, d \in \mathbb{R} \right\}$.

55. Oletetaan, että R ja S ovat renkaita, $h : R \to S$ rengashomomorfismi ja I renkaan R ihanne. Tällöin $h(R)$ on renkaan S alirengas ja $h(I)$ renkaan $h(R)$ ihanne. Onko kuitenkin mahdollista, että $h(I)$ ei olisikaan renkaan S ihanne?

Vastaus: On.

56. Oletetaan, että R on rengas, jonka karakteristika on neljä (sama karakteristikan määritelmä toimii myös yleisemmin mille tahansa renkaalle, mutta tällöin karakteristika ei välttämättä ole pelkästään alkuluku tai nolla).

a) Osoita, että kaikille $a, b \in R$ on voimassa $(a+b)^4 = a^4 + 2a^2b^2 + b^4$ ja $(a+b)^8 = a^8 + 2a^4b^4 + b^8$.

b) Miten tätä voisi yleistää?

57. Etsi yhtälön $x^2 + \overline{8}x = \overline{1}$ ratkaisut x

a) renkaassa $\mathbb{Z}_8$,

b) kokonaisalueessa $\mathbb{Z}_{17}$.

Vastaus: **a)** $\overline{\pm 1}$ ja $\overline{\pm 3}$. **b)** $\overline{-4}$.

58. Olkoon $I = 5\mathbb{Z}[\mathrm{i}]$ kokonaisluvun 5 generoima Gaussin kokonaislukujen renkaan ihanne.

a) Onko jäännösluokkarengas $\mathbb{Z}[\mathrm{i}]/I$ kokonaisalue?

b) Onko jäännösluokka $1 + i + I$ renkaan $\mathbb{Z}[\mathrm{i}]/I$ yksikkö?

Vastaus: **a)** Ei ole. **b)** On.

Kunnat

59. Oletetaan, että p on alkuluku ja $(R, +, \cdot)$ rengas, jossa on p alkiota. Osoita, että R on kunta.

60. Oletetaan, että $(D, +, \cdot)$ on äärellinen kokonaisalue, jossa on q alkiota. Osoita, että jokainen $x \in D$ toteuttaa yhtälön

$$x^q = x.$$

61. Osoita, että kokonaisalueen

$$\mathbb{Z}[\mathrm{i}] = \{a + b\mathrm{i} \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$$

osamääräkunta $Q(\mathbb{Z}[\mathrm{i}])$ on isomorfinen kunnan

$$\mathbb{Q}[\mathrm{i}] = \{a + b\mathrm{i} \in \mathbb{C} \mid a, b \in \mathbb{Q}\}$$

kanssa.

62.

a) Mitkä joukoista

$$S_1 = \left\{ \frac{m}{n} \;\middle|\; m, n \in \mathbb{Z}, 5|m, n \neq 0 \right\},$$
$$S_2 = \left\{ \frac{m}{n} \;\middle|\; m, n \in \mathbb{Z}, 5|m, 5 \nmid n \right\},$$
$$S_3 = \left\{ \frac{m}{n} \;\middle|\; m, n \in \mathbb{Z}, 5 \nmid n \right\},$$
$$S_4 = \left\{ \frac{m}{5^n} \;\middle|\; m, n \in \mathbb{Z}, n \geq 0 \right\}$$

ovat rationaalilukujen kunnan $\mathbb{Q}$ alirenkaita, mitkä alikuntia?

b) Kommutatiivista rengasta R sanotaan *lokaaliksi renkaaksi*, jos sen epäyksiköt muodostavat ihanteen, eli joukko

$$E_R = \{a \in R \mid a \text{ ei ole renkaan } R \text{ yksikkö}\} = R \setminus R^*$$

on renkaan R ihanne. Mitkä joukoista S_1, S_2, S_3 ja S_4 ovat lokaaleja renkaita?

c) Osoita, että lokaalin renkaan R epäyksikköjen joukko E_R on maksimaalinen ihanne.

Vastaus:
a) S_1 on alikunta, S_3 ja S_4 ovat alirenkaita, mutta eivät alikuntia, ja S_2 ei ole edes alirengas.
b) S_1 ja S_3.

Polynomirenkaat

63. Olkoon R rengas, joka ei ole nollarengas.

a) Osoita, ettei mikään renkaan R alkioista voi samanaikaisesti sekä kuulua yksikköryhmään R^* että olla nollanjakaja.

b) Olkoon $I = < x^3 - 1 >$ polynomirenkaan $R[x]$ ihanne. Onko alkio $x + I$ jäännösluokkarenkaan $R[x]/I$ yksikkö?

c) Entä $x - 1 + I$?

Vastaus: **b)** On. **c)** Ei ole.

64. Generoiko polynomi x maksimaalisen ihanteen renkaassa

a) $\mathbb{R}[x]$,

b) $\mathbb{Z}[x]$?

Vihje: Onko olemassa homomorfismia, joka kuvaa ko. renkaan kunnaksi ja jonka ydin on kyseinen ihanne?

Vastaus: **a)** Kyllä. **b)** Ei.

65. Olkoon $I = \{p(x) \in \mathbb{Z}[x] \mid p(0) \text{ on parillinen luku}\}$.

a) Osoita, että I on renkaan $\mathbb{Z}[x]$ ihanne.

b) Osoita, että polynomit x ja 2 generoivat ihanteen I.

c) Osoita, ettei $\mathbb{Z}[x]$ ole pääihannerengas.

Vihje: Voit todistaa c-kohdan osoittamalla, ettei I ole pääihanne. Tämän puolestaan saa osoitettua lähtemällä liikkeelle siitä vastaoletuksesta, että I olisi yhden polynomin generoima, jolloin syntyy ongelmia ihanteeseen kuuluvien polynomien x ja 2 kanssa.

66. Jos K on kunta ja $p(x) = a_0 + a_1x + \cdots + a_nx^n \in K[n]$ on astetta n oleva polynomi, niin sen *resiprookkipolynomi* on $\tilde{p}(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n = x^np(1/x)$.

a) Osoita, että polynomi $x^5 + x^2 + 1$ on jaoton renkaassa $\mathbb{Z}_2[x]$.

b) Osoita, että jos $p(c) = 0$, jollakin alkiolla $c \in K \setminus \{0\}$, niin $\tilde{p}(c^{-1}) = 0$.

c) Osoita, että $\widetilde{pq}(x) = \tilde{p}(x)\tilde{q}(x)$ eli polynomien tulon resiprookkipolynomi on resiprookkipolynomien tulo.

d) Osoita, että myös polynomi $x^5 + x^3 + 1$ on jaoton renkaassa $\mathbb{Z}_2[x]$.

67. Oletetaan, että $p(x) \in \mathbb{Z}_2[x]$ on k-asteinen polynomi. Osoita, että on olemassa sellainen binomi $q(x) = x^m + x^n \in \mathbb{Z}_2[x]$, että $p(x)|q(x)$, missä $0 \leq m < n \leq 2^k$.

Vihje 1: Tarkastele eri monomien x^n jakojäännöksiä $r_n(x)$ modulo $p(x)$. Onko olemassa kokonaisluvut $0 \leq m < n$, joilla $r_m(x) = r_n(x)$?

Vihje 2: Kuinka monta erilaista jakojäännöspolynomia $r_n(x)$ voi enintään olla?

68.

a) Osoita, että polynomi $p(x) = x^4 + x + 1 \in \mathbb{Z}_2[x]$ on jaoton.

Olkoon ihanne $I = < p(x) >$, kunta $K = \mathbb{Z}_2[x]/I$ ja jäännösluokka $\alpha = x + I \in K$. Merkitään vielä kunnassa K: $1 = 1 + I$ ja $0 = 0 + I$.

b) Etsi alkioille α^5 ja α^{10} esitys sellaisina alkion α polynomeina, joiden aste on enintään kolme.

c) Osoita, että joukko $A = \{0, 1, \alpha^5, \alpha^{10}\}$ on kunnan K alikunta.

69. Onko polynomin x jäännösluokka yksikkö renkaassa

a) $R_1 = \mathbb{R}[x]/< x^2 + 3 >$,

b) $R_2 = \mathbb{Z}_7[x]/< x^2 + 3 >$ tai

c) $R_3 = \mathbb{Z}_{11}[x]/< x^{251} >$?

Vastaus: **a)** Kyllä. **b)** Kyllä. **c)** Ei.