Algebran ja lukuteorian harjoitustehtävien ratkaisut

Versio 1.0 (27.1.2006)
Turun yliopisto

Lukuteoria

1.

a) Tarkistetaan ekvivalenssirelaation ehdot. $\sim$ on refleksiivinen, sillä identiteettikuvaus, $id : C \to C$, $id(x) = x$, on bijektio. Relaatio on symmetrinen, koska jos kuvaus $f : C \to D$ on bijektio, samoin on kuvaus $f^{-1} : D \to C$. Oletetaan sitten, että $C \sim D$ ja $D \sim E$, eli on olemassa bijektiot $f : C \to D$ ja $g : D \to E$. Silloin myös kuvaus $g \circ f : C \to E$ on bijektio, eli $C \sim E$.

b) Samaan tapaan kuin edellä havaitaan, että $\sim$ on refleksiivinen ja transitiivinen, mutta entäpä symmetrinen? Joukkojen $C = \{0\}$ ja $D = \{0, 1\}$ avulla havaitaan, että relaatio ei ole symmetrinen. Nimittäin $C \sim D$, koska kuvaus $id : C \to D$, $id(0) = 0$, on injektio, mutta ei ole olemassa injektiota joukolta D joukolle C, eli $D \not\sim C$.

2.

a) $(a, b)\, \rho(a, b)$, joss $a = b$. Esimerkiksi $(0, 1)$ ei ole relaatiossa itsensä kanssa.

b) Jos $(a, b)\, \rho(c, d)$, niin $a = d$ ja $b = c$. Tällöin tietenkin $c = b$ ja $d = a$, eli $(c, d)\, \rho(a, b)$.

c) $(0, 1)\, \rho(1, 0)$ ja $(1, 0)\, \rho(0, 1)$, mutta $(0, 1)\, \rho(0, 1)$ ei päde.

3.

a) $a-c$ on parillinen, jos ja vain jos a ja c ovat joko molemmat parillisia tai molemmat parittomia. Yksittäisessä luokassa siis kaikkien parien ensimmäisten elementtien pariteetti on sama. Samoin toisten elementtien. Siispä luokkia on kaikkiaan neljä ja niiden edustajiksi kelpaavat vaikkapa parit $(0, 0)$, $(0, 1)$, $(1, 0)$ ja $(1, 1)$.

b) Determinantti voi tietenkin olla mikä tahansa kokonaisluku. Niinpä luokkia on ”yhtä paljon” kuin reaalilukujakin. Determinantti on helpointa laskea lävistäjämatriisista, joten edustajistoksi kannattaa valita vaikkapa joukko $\left\{ \left(\begin{smallmatrix} 1 & 0 \\ 0 & x \end{smallmatrix} \right) \;\middle|\; x \in \mathbb{R} \right\}$.

4. Jos $a = 2n$, jollakin $n \in \mathbb{Z}$, niin $a^2 + 1$ on pariton, eikä siis ole neljällä jaollinen. Jos taas $a = 2n + 1$, niin $a^2 + 1 = 4n^2 + 4n + 2$. Jos nyt $a^2 + 1$ olisi neljällä jaollinen samoin olisi luku $a^2 + 1 - 4(n^2 + n) = 2$.

5. Luku 2 on ainoa parillinen alkuluku, joten luvun n on oltava pariton, koska jos n on parillinen, samoin ovat luvut $n + 2$ ja $n + 4$. Jos n on kolmella jaollinen, samoin on luku $n + 6$, eli joka kolmas pariton luku on kolmella jaollinen. Jos siis luku n on lukua 3 suurempi pariton luku, on korkeintaan kaksi luvuista n, $n + 2$ ja $n + 4$ alkulukuja. Siispä ainoaksi ratkaisuksi kelpaa $n = 3$, jolloin myös $n + 2 = 5$ ja $n + 4 = 7$ ovat alkulukuja.

6. Sovelletaan Eukeleideen algoritmia:

$$\begin{aligned}
702191 &= 2 \cdot 242963 + 216265 \\
242963 &= 1 \cdot 216265 + 26698 \\
216265 &= 8 \cdot 26698 + 2681 \\
26698 &= 9 \cdot 2681 + 2569 \\
2681 &= 1 \cdot 2569 + 112 \\
2569 &= 22 \cdot 112 + 105 \\
112 &= 1 \cdot 105 + 7 \\
105 &= 15 \cdot 7,
\end{aligned}$$

eli $\text{syt}(242963, 702191) = 7$. Yhtälöketjua alhaalta ylöspäin laskettaessa saadaan:

$$\begin{aligned}
7 &= 112 - 105 = 112 - (2569 - 22 \cdot 112) \\
&= 23 \cdot 112 - 2569 = 23(2681 - 2569) - 2569 \\
&= 23 \cdot 2681 - 24 \cdot 2569 = 23 \cdot 2681 - 24(26698 - 9 \cdot 2681) \\
&= 239 \cdot 2681 - 24 \cdot 26698 = 239(216265 - 8 \cdot 26698) - 24 \cdot 26698 \\
&= 239 \cdot 216265 - 1936 \cdot 26698 = 239 \cdot 216265 - 1936(242963 - 216265) \\
&= 2175 \cdot 216265 - 1936 \cdot 242963 = 2175(702191 - 2 \cdot 242963) - 1936 \cdot 242963 \\
&= 2175 \cdot 702191 - 6286 \cdot 242963.
\end{aligned}$$

7. Jos $a = 0$, niin $\text{syt}(8a + 3, 5a + 2) = \text{syt}(3, 2) = 1$. Jos $a > 0$, niin Eukleideen algoritmilla saadaan

$$\begin{aligned}
8a + 3 &= (5a + 2) + (3a + 1) \\
5a + 2 &= (3a + 1) + (2a + 1) \\
3a + 1 &= (2a + 1) + a \\
2a + 1 &= \begin{cases} 3a & \text{jos } a = 1, \text{ jolloin } \text{syt}(8a + 3, 5a + 2) = a = 1 \\ 2 \cdot a + 1 & \text{jos } a > 1, \text{ jolloin jatketaan laskentaa...} \end{cases} \\
a &= a \cdot 1,
\end{aligned}$$

eli $\text{syt}(8a + 3, 5a + 2) = 1$. Jos $a < 0$, niin merkitään $b = -a$, jolloin $\text{syt}(8a + 3, 5a + 2) = \text{syt}(8b - 3, 5b - 2)$ ja jälleen saadaan Eukleideen algoritmilla

$$\begin{aligned}
8b - 3 &= (5b - 2) + (3b - 1) \\
5b - 2 &= (3b - 1) + (2b - 1) \\
3b - 1 &= \begin{cases} 2(2b - 1) & \text{jos } b = 1, \text{ jolloin } \text{syt}(8b - 3, 5b - 2) = 2b - 1 = 1 \\ (2b - 1) + b & \text{jos } b > 1, \text{ jolloin jatketaan laskentaa...} \end{cases} \\
2b - 1 &= b + (b - 1) \\
b &= (b - 1) + 1 \\
b - 1 &= (b - 1) \cdot 1,
\end{aligned}$$

eli $\text{syt}(8b - 3, 5b - 2) = 1$.

8.

a) Jos alkuluku p on enintään luvun n suuruinen, niin p jakaa luvun $n!$. Jos nyt p jakaisi luvun N, jakaisi se myös luvun $N - n! = 1$, mikä on mahdotonta. Siispä luvun N kaikki alkutekijät ovat väistämättä suurempia kuin luku n.

b) Oletetaan, että $1 \leq i \leq n-1$. Silloin luku $i+1$ jakaa luvun $n!$ ja siis edelleen luvun $N + i = n! + i + 1$. Toisaalta $i + 1 < N + i$, eli $N + i$ ei voi olla alkuluku.

10.

a) Kaikilla $k \geq 5$ luku 5 jakaa luvun $k!$, joten $n \equiv 1 + 2 + 3! + 4! \equiv 1 + 2 + 1 + 4 \equiv 3 \pmod 5$.

b) $n \equiv 1 + 2 + 3! + 4! + 5! + 6! \equiv 1 + 2 - 1 - 4 + 1 - 1 \equiv -2 \equiv 5 \pmod 7$.

c) $48 = 2^4 \cdot 3$, joten $6! = 2^4 \cdot 3^2 \cdot 5$ on jaollinen luvulla 48, eli $k! \equiv 0 \pmod{48}$, kaikilla $k \geq 6$. Siispä $n \equiv 1! + 2! + 3! + 4! + 5! \equiv 1 + 2 + 6 + 24 + 24 \equiv 9 \pmod{48}$.

11. Jos yllä olevalla yhtälöllä olisi kokonaislukuratkaisu (x, y), seuraisi siitä, että luku $5x^2 - 7$ olisi kolmella jaollinen, tai siis $5x^2 - 7 \equiv -x^2 - 1 \equiv 0 \pmod 3$. Kuitenkin

$$-x^2 - 1 \equiv \begin{cases} 2 \pmod 3 & \text{jos } x \equiv 0 \pmod 3, \\ 1 \pmod 3 & \text{jos } x \equiv \pm 1 \pmod 3. \end{cases}$$

12. Ensinnäkin $4^n \equiv (-1)^n \equiv 9^n \pmod 5$. Luku $2 \cdot 4^n + 3 \cdot 9^n$ ei ole kahdella jaollinen, koska silloin myös luku $2 \cdot 4^n + 3 \cdot 9^n - 2 \cdot 4^n = 3^{2n+1}$ olisi. Samaten $2 \cdot 4^n + 3 \cdot 9^n$ ei ole myöskään kolmella jaollinen. Sen sijaan $2 \cdot 4^n + 3 \cdot 9^n \equiv 5(-1)^n \equiv 0 \pmod 5$, eli $2 \cdot 4^n + 3 \cdot 9^n$ on viidellä jaollinen.

13.

$$F_n - 1 = 2^{2^n} = 2^{2^{n-i} \cdot 2^i} = \left(2^{2^{n-i}}\right)^{2^i} = (F_{n-i} - 1)^{2^i}.$$

Olkoon nyt $0 \leq m < n$ ja oletetaan, että alkuluku p jakaa luvun F_m. Näytetään, kongruenssin avulla, ettei p jaa lukua F_n:

$$F_n = (F_m - 1)^{2^{n-m}} + 1 \equiv (-1)^{2^{n-m}} + 1 = 2 \pmod p.$$

Tästä seuraa, että jos alkuluku q jakaa luvun F_n, niin se ei jaa lukua F_m. Siispä lukujen F_m ja F_n suurin yhteinen tekijä on 1.

14. Olkoot a' ja m' ne luvut, joilla $a = da'$, $m = dm'$ ja $\text{syt}(a', m') = 1$.

Oletetaan ensin, että $ax \equiv c \pmod m$ on ratkeava. Silloin on olemassa sellainen luku x_0, että m ja edelleen d jakaa luvun $ax_0 - c$. Koska d jakaa myös luvun ax_0, jakaa se siis myös luvun $ax_0 - (ax_0 - c) = c$.

Oletetaan toiseksi, että d jakaa luvun c, eli on olemassa luku c', jolla $c = dc'$. Koska $\text{syt}(a', m') = 1$, on yhtälöllä $a'x \equiv c' \pmod{m'}$ ratkaisu x_0, eli $a'x_0 = c' + km'$, jollakin luvulla k. Silloin

$$ax_0 = da'x_0 = d(c' + km') = c + km \equiv c \pmod m.$$

Edellä nähtiin, että jos x_0 on yhtälön $a'x \equiv c' \pmod{m'}$ ratkaisu, on se myös alkuperäisen yhtälön $ax \equiv c \pmod{m}$ ratkaisu. Tämä pätee myös kääntäen. Jos nimittäin $ax_0 - c = km$, eli $d(a'x_0 - c') = dkm'$, niin jakamalla puolittain luvulla d nähdään, että $a'x_0 \equiv c' \pmod{m'}$. Yhtälöillä on siis samat ratkaisut. Yhtälöllä $a'x \equiv c' \pmod{m'}$ on yksikäsitteinen ratkaisu x_0 välillä $0 \leq x_0 \leq m'-1$, joten yhtälöiden kaikki ratkaisut muodostavat joukon $\{x_0+km' \mid k \in \mathbb{Z}\}$. Näistä ratkaisuista osuvat välille $[0, m-1]$ luvut $x_0, x_0+m', x_0+2m', \ldots, x_0+(d-1)m'$, joita on d kappaletta.

16. Suoraan laskemalla saadaan $5 \cdot 2^7 = 640 \equiv -1 \pmod{641}$ ja korottamalla puolittain neljänteen potenssiin $5^4 \cdot 2^{28} \equiv 1 \pmod{641}$. Edelleen: $5^4 = 625 \equiv -16 = -2^4 \pmod{641}$. Nyt saadaan $2^{32} = -(-2^4) \cdot 2^{28} \equiv -5^4 \cdot 2^{28} \equiv -1 \pmod{641}$, jolloin $2^{32}+1 \equiv -1+1 = 0 \pmod{641}$ ja siis $2^{32}+1$ on jaollinen luvulla 641 eikä voi olla alkuluku.

17. Ensinnäkin $1234 = 176 \cdot 7 + 2 \equiv 2 \pmod{7}$. Toiseksi $2^3 = 8 \equiv 1 = 2^0 \pmod{7}$, jolloin $2^n \equiv 2^m \pmod{7}$, aina kun $n \equiv m \pmod{3}$. Kolmanneksi $1234 = 411 \cdot 3 + 1 \equiv 1 \pmod{3}$. Siis $1234^{1234} \equiv 2^{1234} \equiv 2^1 = 2 \pmod{7}$.

18. Jos yhtälöllä olisi ratkaisu (x_0, y_0), niin saataisiin kongruenssi

$$x_0^3 + y_0^3 \equiv 3 \pmod{7}.$$

Kuitenkin $0^3 \equiv 0$, $(\pm 1)^3 \equiv \pm 1$, $(\pm 2)^3 \equiv \pm 1$ ja $(\pm 3)^3 \equiv \mp 1$ modulo 7. Tästä seuraa, että valittiinpa kokonaisluvut r ja s miten tahansa, niin $r^3 + s^3 \equiv t \pmod{7}$, missä $t \in \{0, \pm 1, \pm 2\}$.

Ryhmät

19. On tarkistettava ryhmän ehdot. Selvästi $2\mathbb{Z}$ on suljettu yhteenlaskun suhteen, eli kahden parillisen luvun summakin on aina parillinen. Assosiatiivisuus seuraa ryhmän $(\mathbb{Z}, +)$ assosiatiivisuudesta. Ryhmän $2\mathbb{Z}$ neutraalialkio on 0 ja luvun n käänteisalkio on $-n$, joka on parillinen, jos n on. Itse asiassa $2\mathbb{Z}$ on myös kommutatiivinen, mikä on assosiatiivisuuden tapaan seurausta ryhmän $\mathbb{Z}$ kommutatiivisuudesta.

20.

a) Kommutatiivisuusehdosta saadaan $(ab)^2 = abab = aabb = a^2b^2$.

b) Kerrotaan yhtälöä $(ab)^2 = a^2b^2$ vasemmalta alkion a käänteisalkiolla ja oikealta alkion b käänteisalkiolla, jolloin saadaan

$$(ab)^2 = a^2b^2 \Longrightarrow a^{-1}ababb^{-1} = a^{-1}aabbb^{-1} \Longrightarrow ba = ab.$$

c) Nyt saadaan $(ab)^2 = 1 = a^2b^2$ aina, kun $a, b \in G$, mistä b)-kohdan mukaan seuraa ryhmän G kommutatiivisuus.

21. Ryhmätaulu on

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{5}$	$\overline{7}$	$\overline{8}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{5}$	$\overline{7}$	$\overline{8}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{8}$	$\overline{1}$	$\overline{5}$	$\overline{7}$
$\overline{4}$	$\overline{4}$	$\overline{8}$	$\overline{7}$	$\overline{2}$	$\overline{1}$	$\overline{5}$
$\overline{5}$	$\overline{5}$	$\overline{1}$	$\overline{2}$	$\overline{7}$	$\overline{8}$	$\overline{4}$
$\overline{7}$	$\overline{7}$	$\overline{5}$	$\overline{1}$	$\overline{8}$	$\overline{4}$	$\overline{2}$
$\overline{8}$	$\overline{8}$	$\overline{7}$	$\overline{5}$	$\overline{4}$	$\overline{2}$	$\overline{1}$

,

josta voidaan laskea $\overline{7} \cdot \overline{2} = \overline{5}$. Huomaa, että koska ryhmä $\mathbb{Z}_9^*$ on kommutatiivinen, niin sen ryhmätaulu on symmetrinen päälävistäjänsä suhteen.

22.

a) Selvästi $\circ$ on joukossa S_n määritelty. Lasku

$$(\alpha \circ (\beta \circ \gamma))(x) = \alpha((\beta \circ \gamma)(x)) = \alpha(\beta(\gamma(x))) = (\alpha \circ \beta)(\gamma(x)) = ((\alpha \circ \beta) \circ \gamma)(x)$$

osoittaa assosiatiivisuuden. Neutraalialkio on identiteettikuvaus, $id : \mathbb{N}_n \to \mathbb{N}_n$, $id(x) = x$. Alkion α käänteisalkio on käänteiskuvaus α^{-1}.

b) Joukko H on epätyhjä ja selvästi $(\alpha \circ \beta^{-1})(1) = 1$, jos $\alpha(1) = \beta(1) = 1$, eli $\alpha \circ \beta^{-1} \in H$, jos $\alpha, \beta \in H$. Niinpä aliryhmäkriteerin perusteella H on aliryhmä.

c) Identiteettikuvaus ei kuulu joukkoon K, joten se ei ole aliryhmä.

23.

a) $1 \in < S >$ ja $(-1)^{-1} = -1 \in < S >$. Toisaalta $\{\pm 1\}$ on ryhmä, joten $< S > = \{\pm 1\}$.

b) $< S > = \{a_1 a_2 \cdots a_m \mid m \geq 1, a_i \in \{3, 3^{-1}\}$, kaikilla $1 \leq i \leq m\} = \{3^n \mid n \in \mathbb{Z}\}$.

c) 2^{-1} kuuluu ryhmään $< S >$, joten myös $n = 2n/2$ ja edelleen n^{-1} kuuluu siihen, kaikilla $n \in \mathbb{Z}$. Silloin myös $\mathbb{Q}^* \subseteq < S >$. Toisaalta $\mathbb{Q}^*$ on ryhmä, joten $< S > = \mathbb{Q}^*$.

24. Koska $\text{syt}(m, n) = 1$, on olemassa sellaiset luvut $u, v \in \mathbb{Z}$, että $mu + nv = 1$. Silloin

$$a = a^1 = a^{mu+nv} = (a^m)^u a^{nv} = 1^u a^{nv} = a^{nv} = (a^v)^n,$$

eli $b = a^v$.

25.

a) $\sharp(\mathbb{Z}_2 \times \mathbb{Z}_3) = 6$. Huomataan, että $2(\overline{1}, \overline{1}) = (\overline{0}, \overline{2})$, $3(\overline{1}, \overline{1}) = (\overline{1}, \overline{0})$, $4(\overline{1}, \overline{1}) = (\overline{0}, \overline{1})$ ja $5(\overline{1}, \overline{1}) = (\overline{1}, \overline{2})$, jolloin $\text{ord}(\overline{1}, \overline{1}) = 6$. Siispä $\mathbb{Z}_2 \times \mathbb{Z}_3 = < (\overline{1}, \overline{1}) >$.

b) $\sharp(\mathbb{Z}_2 \times \mathbb{Z}_4) = 8$, mutta

$$\text{ord}(a, b) = \begin{cases} 1 & \text{jos } a = b = \overline{0}, \\ 2 & \text{jos } (a = \overline{1} \text{ ja } b = \overline{0}) \text{ tai } b = \overline{2}, \\ 4 & \text{jos } b = \overline{\pm 1}, \end{cases}$$

eli $\mathbb{Z}_2 \times \mathbb{Z}_4 \neq < (a, b) >$, valittiinpa alkio (a, b) miten tahansa.

26. Oletetaan kääntäen, että ryhmällä G olisi korkeintaan kaksi eri aliryhmää. Näiden täytyisi silloin olla G itse ja $\{1\}$ (jotka voivat olla samoja, jos G on triviaali ryhmä). Silloin

$$< a > = \begin{cases} G & \text{jos } a \neq 1, \\ \{1\} & \text{jos } a = 1, \end{cases}$$

eli G on syklinen, jolloin se on myös kommutatiivinen.

Huomaa, että käänteinen väite ei pidä paikkaansa: ryhmä voi olla kommutatiivinen, vaikka sillä olisikin vähintään kolme eri aliryhmää. Ajattele vaikkapa ryhmää $\mathbb{Z}_4$, jolla on aliryhmä $\{\overline{0}, \overline{2}\}$.

27. Osoitetaan, että $G = < \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) >$. Lasketaan

$$\begin{aligned} \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)^2 &= \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right), \\ \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)^3 &= \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right), \\ \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)^4 &= \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right). \end{aligned}$$

Symmetrian nojalla saadaan myös $G = < \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) >$.

28. Riittää tarkistaa aliryhmäkriteeri äärellisten ryhmien tapauksessa. Eli oletetaan, että $\overline{a}^2, \overline{b}^2 \in QR_m$. Silloin $\overline{a}^2 \cdot \overline{b}^2 = \overline{ab}^2 \in QR_m$.

Laskettaessa esimerkiksi ryhmää QR_7 kannattaa ryhmän $\mathbb{Z}_7^*$ alkiot ajatella muodossa $\mathbb{Z}_7^* = \{\overline{\pm 1}, \overline{\pm 2}, \overline{\pm 3}\}$, jolloin

$$QR_7 = \{\overline{1}^2, \overline{2}^2, \overline{3}^2\} = \{\overline{1}, \overline{-3}, \overline{2}\}.$$

Muut ryhmät lasketaan samaan tapaan.

29. Ryhmä $G = \{\overline{\pm 1}, \overline{\pm 5}\}$. Ryhmän kaikki alkiot ovat itsensä käänteisalkioita, koska

$$(\pm 5)^2 = 25 \equiv 1 = (\pm 1)^2 \pmod{12}.$$

Siispä muiden kuin alkion $\overline{1}$ kertaluku on 2. Selvästi

$$G = < \overline{-1}, \overline{5} > = < \overline{-1}, \overline{-5} >,$$

mutta myös $G = < \overline{-5}, \overline{5} >$. Siispä tämän ryhmän generoivat mitkä tahansa kaksi erisuurta, alkiosta $\overline{1}$ poikkeavaa, alkiota.

30.

a) $\text{syt}(a, 17) = 1$, kaikilla $1 \leq a \leq 16$, joten $\sharp\mathbb{Z}_{17}^* = 16$.

b) $\overline{3}^2 = \overline{-8}$, $\overline{3}^4 = \overline{-8}^2 = \overline{-4}$ ja $\overline{3}^8 = \overline{-4}^2 = \overline{-1}$.

c) Lagrangen lauseesta seuraa, että $\text{ord}(\overline{3})$ jakaa luvun $\sharp\mathbb{Z}_{17}^* = 16$, joten alkion $\overline{3}$ kertaluku on jokin luvuista 2, 4, 8 tai 16. Kohta b) rajaa näistä luvuista kolme pienintä pois, joten $\text{ord}(\overline{3}) = 16$, eli $\mathbb{Z}_{17}^* = < \overline{3} >$.

31. Koska 109 on alkuluku, on $\sharp\mathbb{Z}_{109}^* = 108 = 2^2 \cdot 3^3$, joten Lagrangen lauseen mukaan alkion $\overline{23}$ kertaluku $\text{ord}(\overline{23}) \in \{2, 3, 4, 6, 9, 12, 18, 27, 36, 54, 108\}$. Kertaluvun määrittämiseksi lasketaan

aluksi

$$\overline{23}^2 = \overline{-16}$$
$$\overline{23}^3 = \overline{-16} \cdot \overline{23} = \overline{-41}$$
$$\overline{23}^4 = (\overline{23}^2)^2 = \overline{-16}^2 = \overline{38}$$
$$\overline{23}^6 = (\overline{23}^3)^2 = \overline{-41}^2 = \overline{46}.$$

Sitten ei jatketakaan tämän pidemmälle, koska huomataan, että $\overline{23}^6 = \overline{23} \cdot \overline{23}^5 = \overline{23} \cdot \overline{2}$, mistä seuraa supistussäännön avulla (tai siis kertomalla yhtälö puolittain vasemmalta alkiolla $(\overline{2})^{-1}$)

$$\overline{23}^5 = \overline{2}.$$

Seuraavaksi havaitaan, että

$$\overline{-1} \cdot \overline{23}^2 = \overline{16} = \overline{2}^4 = (\overline{23}^5)^4 = \overline{23}^{20}.$$

Kun tässä supistetaan oikealta alkiolla $\overline{23}^2$, saadaan $\overline{23}^{18} = \overline{-1}$, eli $\overline{23}^{36} = \overline{1}$. Siispä alkion $\overline{23}$ kertaluku ei voi olla ainakaan suurempi kuin 36. Osoitetaan, ettei se ole myöskään pienempi. $\overline{23}^{18} = (\overline{23}^9)^2 \neq \overline{1}$, joten $\overline{23}^9 \neq \overline{\pm 1}$. Tästä seuraa, että

$$\overline{23}^{27} = \overline{23}^{18} \cdot \overline{23}^9 = \overline{-1} \cdot \overline{23}^9 \neq \overline{1}.$$

Suoraan laskemalla saadaan

$$\overline{23}^{12} = \overline{46}^2 = \overline{45} \neq \overline{1}.$$

Saadaan siis $\operatorname{ord}(\overline{23}) = 36$.

Nyt $\overline{2}^n = \overline{23}^{5n} = \overline{1}$, jos ja vain jos luku 36 jakaa luvun $5n$, jos ja vain jos luku 36 jakaa luvun n. Siispä myös $\operatorname{ord}(\overline{2}) = 36$, eli $H = <\overline{23}> = <\overline{2}>$. Koska $\overline{-1} \in H$, niin

$$\overline{n} \in H, \qquad \text{jos ja vain jos} \qquad \overline{-n} \in H,$$

kaikilla luvuilla $n \in \mathbb{Z}$. Saadaan $H = \{\overline{\pm n} \mid n \in A\}$, missä

$$\begin{aligned} A &= \{n \in \mathbb{Z} \mid -54 \leq n \leq 54 \text{ ja } \exists m \in \mathbb{Z} : (0 \leq m \leq 17 \text{ ja } 2^m \equiv n \pmod{109})\} \\ &= \{1, 2, 4, 8, 16, 32, -45, 19, 38, -33, 43, -23, -46, 17, 34, -41, 27, 54\}. \end{aligned}$$

32.

a) Kongruenssiehdosta saadaan suoraan laskemalla $[a] * [b] = [a * b] = [c * d] = [c] * [d]$.

b) Ryhmäehtojen osoittamiseksi oletetaan, että alkiot $a, b, c \in G$ on valittu mielivaltaisesti. Suoraan laskemalla saadaan

$$[a] * ([b] * [c]) = [a] * [b * c] = [a * (b * c)] = [(a * b) * c] = [a * b] * [c] = ([a] * [b]) * [c],$$
$$[a] * [e] = [a * e] = [a] = [e * a] = [e] * [a],$$
$$[a] * [a^{-1}] = [a * a^{-1}] = [e] = [a^{-1} * a] = [a^{-1}] * [a]$$

sekä kommutatiivisen ryhmän tapauksessa vielä

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

Koska alkiot a, b ja c oli valittu mielivaltaisesti, toimivat yllä olevat ehdot tietenkin kaikille ryhmän G alkioille ja siis kaikille ryhmän $G/\!\sim$ luokille. Siispä ryhmän $G/\!\sim$ neutraaliluokka on $[e]$ ja luokan $[a]$ käänteisluokka $[a]^{-1} = [a^{-1}]$. Huomaa, että kaikki laskut ryhmässä $G/\!\sim$ palautuvat laskuiksi ryhmässä G.

c) Olkoon a, b, c ja d mielivaltaisesti valittuja ryhmän G alkioita ja oletetaan, että $a \sim b$ ja $c \sim d$. Silloin $a = b * h_1$ ja $c = d * h_2$, joillakin ryhmän H alkioilla h_1 ja h_2. Koska H on normaali aliryhmä, on $h_1 * d = h_3 * d$, jollakin alkiolla $h_3 \in H$. Nyt saadaan

$$a * c = b * h_1 * d * h_2 = b * d * h_3 * h_2 \in bd * H,$$

eli $a * c \sim b * d$. Koska kongruenssiehto toimii mielivaltaisesti valituille alkioille, toimii se silloin kaikille ryhmän G alkioille. Siispä $\sim$ on kongruenssi.

d) Osoitetaan ensin aliryhmäkriteerin avulla, että $[e]$ on ryhmän G aliryhmä. Luonnollisesti $[e]$ on epätyhjä, koska ainakin $e \in [e]$. Oletetaan sitten, että $a \in [e]$ ja $b \in [e]$. Silloin relaation $\sim$ refleksiivisyydestä ja kongruenssiehdosta saadaan

$$a * b^{-1} = a * b^{-1} * e \sim a * b^{-1} * b = a \sim e,$$

eli $a * b^{-1} \in [e]$. Siispä ainakin $[e]$ on ryhmän G aliryhmä.
Osoitetaan vielä normaalius. Olkoon $a \in G$ ja $h \in [e]$ mielivaltaisesti valittuja alkioita. Koska $\sim$ on ekvivalenssirelaatio on $a \sim a$ ja $a^{-1} \sim a^{-1}$. Silloin kongruenssiehdon avulla saadaan ensin $a*h \sim a*e = a$ ja sitten $a*h*a^{-1} \sim a*a^{-1} = e$, eli $a*h*a^{-1} \in [e]$. Jälleen tämä päättely toimii yhtä hyvin kaikilla alkioilla $a \in G$ ja $h \in H$, jolloin aliryhmän normaalisuuskriteerin perusteella $[e]$ on ryhmän G normaali aliryhmä.

33. Ryhmän G kertaluku on $\sharp G = 8$ ja $\sharp A = 2$. Lagrangen lauseen mukaan sivuluokkien määrä $[G{:}A] = \sharp G/\sharp A = 4$. A itse on yksi sivuluokista. Samoin on $\overline{-1}A = \{\overline{-1}, \overline{-4}\}$. $\overline{2}A = \{\overline{2}, \overline{-7}\}$ ja $\overline{-2}A = \{\overline{-2}, \overline{7}\}$. Näin on löydetty 4 eri sivuluokkaa, eli kaikki sivuluokat ja etsintä voidaan lopettaa.

34.

a) Ryhmät $\mathbb{Z}_2$ ja Z_6 ovat Abelin ryhmiä, joten samoin on niiden karteesinen tulo G. Nimittäin

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

kaikilla alkioilla $(a, b), (c, d) \in G$. Toisaalta kaikki Abelin ryhmän aliryhmät ovat normaaleja.

b) $H = \{(\overline{0}, \overline{0}), (\overline{1}, \overline{3})\}$, koska $2(\overline{1}, \overline{3}) = (\overline{2}, \overline{6}) = (\overline{0}, \overline{0})$.

c) Huomaa aluksi, että

$$(\overline{0}, \overline{n}) + H = \{(\overline{0}, \overline{n}), (\overline{1}, \overline{n+3})\} = (\overline{1}, \overline{n+3}) + H,$$

kaikilla luvuilla $n \in \mathbb{Z}$. Niinpä edustajistoksi D voidaan valita joukko $\{(\overline{0}, \overline{n}) \mid 0 \leq n \leq 5\}$.

d) Valitun edustajiston D ansiosta laskeminen ryhmässä G/H on nyt helppoa. Nimittäin

$$\big((\overline{0}, \overline{m}) + H\big) + \big((\overline{0}, \overline{n}) + H\big) = \big((\overline{0}, \overline{m+n}) + H\big),$$

kaikilla $m, n \in \mathbb{Z}$.

e) Kohdasta d) nähdään välittömästi, että ryhmä G/H on isomorfinen ryhmän $\mathbb{Z}_6$ kanssa, joten G/H on syklinen.

35.

a) $f(x + y) = 2^{x+y} = 2^x 2^y = f(x)f(y)$.

b) $f(0) \neq 0$, eli f ei kuvaa neutraalialkiota neutraalialkioksi, joten f ei ole homomorfismi.

c) $f(xy) = |xy| = |x||y| = f(x)f(y)$.

36. Voidaan olettaa, että kyseinen isomorfismi on $f : G \to G_1$.

a) Olkoon alkiot $a_1, b_1 \in G_1$ valittu mielivaltaisesti. Koska f on surjektio, on olemassa jotkin alkiot $a, b \in G$, jotka ovat alkioiden a_1 ja b_1 alkukuvia, eli $a_1 = f(a)$ ja $b_1 = f(b)$. Silloin

$$a_1 b_1 = f(a)f(b) = f(ab) = f(ba) = f(b)f(a) = b_1 a_1.$$

Edellä oleva pätee kaikille alkioille $a_1, b_1 \in G_1$, koska se pätee mielivaltaisesti valituillekin. Siispä G_1 on kommutatiivinen.

b) Olkoon $G = < a >$ ja $a_1 = f(a)$. Osoitetaan, että $G_1 = < a_1 >$. Olkoon siis $b_1 \in G_1$ valittu mielivaltaisesti. Silloin on olemassa alkio $b \in G$, jonka kuva b_1 on. Nyt on olemassa jokin luku $n \in \mathbb{Z}$, jolla $b = a^n$. Saadaan

$$b_1 = f(b) = f(a^n) = f(a)^n = a_1^n,$$

eli $b_1 \in < a_1 >$. Jälleen edellä sanottu pätee kaikille alkioille $b_1 \in G_1$, joten G_1 on syklinen.

37.

a) Luonnollisesti isomorfismiksi kelpaa $f : \mathbb{R}^2 \to \mathbb{C}$, $f(x, y) = x + y\mathrm{i}$. Varmistetaan vielä homomorfisuus (injektiivisyys ja surjektiivisuus ovat triviaaleja):

$$\begin{aligned} f((x_1, y_1) + (x_2, y_2)) &= f(x_1 + x_2, y_1 + y_2) = x_1 + x_2 + (y_1 + y_2)\mathrm{i} \\ &= x_1 + y_1\mathrm{i} + x_2 + y_2\mathrm{i} = f(x_1, y_1) + f(x_2, y_2), \end{aligned}$$

kaikilla $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$.

b) Olkoon $f : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ homomorfismi. Näytetään, että se ei ole surjektio. Ryhmä $\mathbb{Z}$ on syklinen. Nimittäin $\mathbb{Z} = < 1 >$. Oletetaan, että $f(1) = (a, b)$. Jos $b = 0$, niin homomorfismin kuva $\mathrm{Im}(f) = \{(na, 0) \mid n \in \mathbb{Z}\}$, eikä alkio $(1, 1)$ kuulu siihen. Jos taas $b \neq 0$, niin kuva $\mathrm{Im}(f) = \{(na, nb) \mid n \in \mathbb{Z}\}$, eikä tällä kertaa $(1, 0)$ kuulu siihen.

38.

a) $1 = f(1)$ ja $f(c)^n = f(c^n)$, kaikilla $n \in \mathbb{Z}$. Silloin $f(c)^n = 1$, jos ja vain jos $c^n = 1$. Siispä $\mathrm{ord}(c) = \mathrm{ord}(f(c))$.

b) $\mathrm{ord}(ba) = \mathrm{ord}(f(ba)) = \mathrm{ord}(abaa^{-1}) = \mathrm{ord}(ab)$.

39. Ensinnäkin $\sharp\mathbb{Z}_{17}^* = 16$, joten minkä tahansa ykkösalkiosta eroavan alkion kertaluku on jokin luvuista 2, 4, 8 tai 16. Tämä helpottaa tutkimusta. Saadaan

$$\begin{aligned} 3^2 &= 9 \equiv -8 \pmod{17}, \\ 3^4 &= (-8)^2 = 64 \equiv -4 \pmod{17}, \\ 3^8 &= (-4)^2 = 16 \equiv -1 \pmod{17}, \end{aligned}$$

eli alkion $\overline{3}$ kertaluku ei voi olla mikään luvuista 2, 4 eikä 8, joten sen täytyy olla 16. Niinpä $\mathbb{Z}_{17}^* = < \overline{3} >$. Nyt saadaan helposti isomorfismi $h : \mathbb{Z}_{16} \to \mathbb{Z}_{17}^*, h(\overline{x}) = \overline{3}^x$.

40. Selvästi

$$\det\begin{pmatrix} \cos x & \sin x \\ -\sin x & \cos x \end{pmatrix} = \cos^2 x + \sin^2 x = 1 = \det\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix},$$

joten ainakin f ja g ovat funktioita joukolta $\mathbb{R}$ joukkoon $GL_2(\mathbb{R})$. Tarkistetaan sitten funktion f homomorfisuus:

$$\begin{aligned} f(x+y) &= \begin{pmatrix} \cos(x+y) & \sin(x+y) \\ -\sin(x+y) & \cos(x+y) \end{pmatrix} = \begin{pmatrix} \cos x\cos y - \sin x \sin y & \sin x \cos y + \cos x \sin y \\ -\sin x \cos y - \cos x \sin y & \cos x \cos y - \sin x \sin y \end{pmatrix} \\ &= \begin{pmatrix} \cos x & \sin x \\ -\sin x & \cos x \end{pmatrix}\begin{pmatrix} \cos y & \sin y \\ -\sin y & \cos y \end{pmatrix} = f(x)f(y). \end{aligned}$$

Lopuksi funktion g homomorfisuus nähdään näin:

$$g(x)g(y) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix} = g(x+y).$$

Huomaa, että funktion g homomorfisuus todennettiin "eri suuntaan" kuin funktion f homomorfisuus. Suunnan valinnalla ei ole lopputuloksen kannalta merkitystä, joten tämäntyyppisissä laskuissa kannattaa valita se tapa, joka tuntuu helpoimmalta.

Funktion f ydin on joukko $\{n2\pi \mid n \in \mathbb{Z}\}$. Funktion g ydin muodostuu pelkästään alkiosta 0, joten g on injektio.

41. Koska $\mathbb{Z}_{12} = <\overline{1}>$, saadaan muiden alkioiden kuvat homomorfismiehdosta:

$$f(\overline{n}) = f(n\overline{1}) = nf(\overline{1}) = n\overline{5},$$

eli

x	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$
$f(x)$	$\overline{0}$	$\overline{5}$	$\overline{10}$	$\overline{15}$	$\overline{0}$	$\overline{5}$	$\overline{10}$	$\overline{15}$	$\overline{0}$	$\overline{5}$	$\overline{10}$	$\overline{15}$

.

Tästä taulukosta nähdään, että $\ker f = \{\overline{0}, \overline{4}, \overline{8}\}$ ja $\operatorname{Im} f = \{\overline{0}, \overline{5}, \overline{10}, \overline{15}\}$

42. Välillä $0 < x < 18$ on 9 lukua x, jotka eivät ole kahdella jaollisia. Näistä luvuista joka kolmas on kolmella jaollinen. Siispä välillä $0 < x < 18$ on täsmälleen kuusi lukua x jotka ovat jaottomia sekä kahdella että kolmella. Niinpä $\sharp G = 6$ ja

$$G = \{\overline{\pm 1}, \overline{\pm 5}, \overline{\pm 7}\}.$$

Minkä tahansa ryhmän G alkion kertaluku jakaa luvun 6, eli kertaluku on 1 (ainoastaan alkiolla $\overline{1}$), 2, 3 tai 6. Nyt $5^2 \equiv 7 \pmod{18}$ ja $5^3 \equiv 5 \cdot 7 \equiv -1 \pmod{18}$, joten alkion $\overline{5}$ kertaluku ei ole mikään luvuista 1, 2 tai 3, eli sen täytyy olla 6. Siispä $G = <\overline{5}>$.

Selvästi kuvaus $h : \mathbb{Z}_6 \to G, h(\overline{n}) = \overline{5}^n$ on isomorfismi. Ryhmän $\mathbb{Z}_6$ aliryhmät ovat $\{\overline{0}\}$, $\{\overline{0}, \overline{3}\}$, $\{\overline{0}, \overline{\pm 2}\}$ ja $\mathbb{Z}_6$ itse. Ryhmän G aliryhmät ovat silloin täsmälleen ryhmän $\mathbb{Z}_6$ aliryhmien h-kuvat: $\{\overline{1}\}$, $\{\overline{5}^0, \overline{5}^3\} = \{\overline{\pm 1}\}$, $\{\overline{5}^0, \overline{5}^2, \overline{5}^4\} = \{\overline{1}, \overline{7}, \overline{-5}\}$ ja G.

Renkaat

43.

a) Alirenkaan määritelmästä nähdään, että on löydettävä sellainen rengas $(R, +, \cdot)$, jolla on yhtälön $a^2 = a$ toteuttava alkio $a \neq 1_R$, joka toimii renkaan $(A, +, \cdot)$ ykkösalkiona 1_A. Itse asiassa tällöin voidaan valita $A = \{a\}$, eli $(A, +, \cdot)$ on nollarengas. Tässä ei kannata mennä merta edemmäs kalaan, eli riittää valita $R = \{0_R = 0, 1_R = 1, a, b = 1 + a\}$. Oletetaan vielä, että $1 + 1 = 0$ ja $a \cdot a = a$. Näistä yhtälöistä saadaan yhteenlaskun kommutatiivisuuden ja distributiivilain avulla $(c_0 + c_1 a) + (d_0 + d_1 a) = (c_0 + d_0) + (c_1 + d_1)a$ ja $(c_0 + c_1 a)(d_0 + d_1 a) = c_0 d_0 + (c_0 d_1 + c_1 d_0 + c_1 d_1)a$, $c_i, d_i \in \{0, 1\}$, $i = 0, 1$. Alla on yhteen- ja kertolaskutaulut:

$+$	0	1	a	$1+a$
0	0	1	a	$1+a$
1	1	0	$1+a$	a
a	a	$1+a$	0	1
$1+a$	$1+a$	a	1	0

$\cdot$	1	a	$1+a$
1	1	a	$1+a$
a	a	a	0
$1+a$	$1+a$	0	$1+a$

.

Osoitetaan vielä kertolaskun assosiatiivisuus. Oletetaan, että $x = c_0 + c_1 a$, $y = d_0 + d_1 a$ ja $z = e_0 + e_1 a$, $c_i, d_i, e_i \in \{0, 1\}$, $i = 0, 1$. Saadaan

$$\begin{aligned}(xy)z &= (c_0 d_0 + (c_0 d_1 + c_1 d_0 + c_1 d_1)a)(e_0 + e_1 a) \\ &= (c_0 d_0)e_0 + (c_0 d_0 e_1 + (c_0 d_1 + c_1 d_0 + c_1 d_1)e_0 + (c_0 d_1 + c_1 d_0 + c_1 d_1)e_1)a \\ &= c_0(d_0 e_0) + (c_0(d_0 e_1 + d_1 e_0 + d_1 e_1) + c_1(d_0 e_0) + c_1(d_0 e_1 + d_1 e_0 + d_1 e_1))a \\ &= (c_0 + c_1 a)(d_0 e_0 + (d_0 e_1 + d_1 e_0 + d_1 e_1)a) = x(yz).\end{aligned}$$

Distributiivisuus voidaan osoittaa samaan tapaan ja yhteenlaskun assosiatiivisuus ja kommutatiivisuus ovat triviaaleja.

b) Nyt on puolestaan löydettävä sellainen rengas $(R, +, \cdot)$, jolla on yhtälöt $a^2 = a$ ja $ab = b = ba$ toteuttavat alkiot $a \neq 1_R$ ja b. Nyt voidaan valita $R = \{0, 1, a, b, a+b, 1+a, 1+b, 1+a+b\} = \{c_0 + c_1 a + c_2 b \mid c_i \in \{0,1\}, i = 0,1,2\}$, jossa $1 + 1 = 0$, $a \cdot a = a$ ja $b \cdot b = b = ab = ba$. Näistä yhtälöistä saadaan

$$(c_0 + c_1 a + c_2 b) + (d_0 + d_1 a + d_2 b) = (c_0 + d_0) + (c_1 + d_1)a + (c_2 + d_2)b$$

ja

$$(c_0 + c_1 a + c_2 b)(d_0 + d_1 a + d_2 b) = c_0 d_0 + (c_0 d_1 + c_1 d_0 + c_1 d_1)a + (c_0 d_2 + c_1 d_2 + c_2 d_0 + c_2 d_1 + c_2 d_2)b,$$

$c_i, d_i \in \{0,1\}$, $i = 0,1,2$. Yhteenlaskutaulu on

$+$	0	1	a	b	$a+b$	$1+a$	$1+b$	$1+a+b$
0	0	1	a	b	$a+b$	$1+a$	$1+b$	$1+a+b$
1	1	0	$1+a$	$1+b$	$1+a+b$	a	b	$a+b$
a	a	$1+a$	0	$a+b$	b	1	$1+a+b$	$1+b$
b	b	$1+b$	$a+b$	0	a	$1+a+b$	1	$1+a$
$a+b$	$a+b$	$1+a+b$	b	a	0	$1+b$	$1+a$	1
$1+a$	$1+a$	a	1	$1+a+b$	$1+b$	0	$a+b$	b
$1+b$	$1+b$	b	$1+a+b$	1	$1+a$	$a+b$	0	a
$1+a+b$	$1+a+b$	$a+b$	$1+b$	$1+a$	1	b	a	0

ja kertolaskutaulu

$\cdot$	1	a	b	$a+b$	$1+a$	$1+b$	$1+a+b$
1	1	a	b	$a+b$	$1+a$	$1+b$	$1+a+b$
a	a	a	b	$a+b$	0	$a+b$	b
b	b	b	b	0	0	0	b
$a+b$	$a+b$	$a+b$	0	$a+b$	0	$a+b$	0
$1+a$	$1+a$	0	0	0	$1+a$	$1+a$	$1+a$
$1+b$	$1+b$	$a+b$	0	$a+b$	$1+a$	$1+b$	$1+a$
$1+a+b$	$1+a+b$	b	b	0	$1+a$	$1+a$	$1+a+b$.

Distributiivisuus ja operaatioiden assosiatiivisuudet voidaan todistaa samaan tapaan kuin a)-kohdassa. Saadaan $A = \{0, a, b, a+b\}$, missä $1_A = a$.

c) Yleistetään edellä saadut tulokset. Olkoon $R = \{\sum_{i=0}^{n} c_i a^i \mid n \in \mathbb{N}_0, c_i \in \{0,1\}, i = 0,1,2,\dots\}$, missä $a^0 = 1$, $1+1=0$, $a^i \neq a^j$, jos $i \neq j$, ja $a^i a^j = a^{\max\{i,j\}}$. Oletetaan, että $x = \sum_{i=0}^{\alpha} c_i a^i$, $y = \sum_{i=0}^{\beta} d_i a^i$ ja $z = \sum_{i=0}^{\gamma} e_i a^i$. Tässä voidaan olettaa, että $\alpha = \beta = \gamma = n$ lisäämällä alkioiden perään tarvittaessa nollatermejä. Nyt yhteen- ja kertolasku näyttävät seuraavanlaisilta:

$$x + y = \sum_{i=0}^{n} (c_i + d_i) a^i \qquad \text{ja} \qquad xy = \sum_{i=0}^{n} \Big(\sum_{\max\{j,k\}=i} c_j d_k \Big) a^i.$$

Nähdään, että

$$\begin{aligned}
(xy)z &= \Big(\sum_{i=0}^{n} \Big(\sum_{\max\{j,k\}=i} c_j d_k \Big) a^i \Big) z = \sum_{i=0}^{n} \Big(\sum_{\max\{m,l\}=i} \Big(\sum_{\max\{j,k\}=m} c_j d_k \Big) e_l \Big) a^i \\
&= \sum_{i=0}^{n} \Big(\sum_{\max\{j,k,l\}=i} c_j d_k e_l \Big) a^i = \sum_{i=0}^{n} \Big(\sum_{\max\{j,m\}=i} c_j \Big(\sum_{\max\{k,l\}=m} d_k e_l \Big) \Big) a^i \\
&= x \Big(\sum_{i=0}^{n} \Big(\sum_{\max\{k,l\}=i} d_k e_l \Big) a^i \Big) = x(yz).
\end{aligned}$$

Muiden ehtojen todistaminen on suoraviivaista. Huomataan, että $a^i \big(\sum_{j=i}^{n} c_j a^j \big) = \sum_{j=i}^{n} c_j a^j = \big(\sum_{j=i}^{n} c_j a^j \big) a^i$, Joten $(A_i, +, \cdot)$, missä $A_i = \{\sum_{j=i}^{n} c_j a^j \mid n \geq i, c_j \in \{0,1\}, j = i, i+1, i+2, \dots\}$, on rengas ja $1_{A_i} = a^i$.

44.

a) Käytetään alirengaskriteeriä. $1_{\mathbb{Q}} = 1 = 1/1 \in R_1$. Kaikilla luvuilla $m_1/n_1, m_2/n_2 \in R_1$ on $m_1/n_1 - m_2/n_2 = (m_1 n_2 - m_2 n_1)/n_1 n_2$. Tämä luku ei välttämättä ole supistettu, mutta sen nimittäjä $n_1 n_2$ on pariton, joten vastaavan supistetun muodonkin nimittäjä on pariton. Siispä kyseinen erotus kuuluu joukkoon R_1. Lopuksi nähdään, että $m_1/n_1 \cdot m_2/n_2 = m_1 m_2 / n_1 n_2 \in R_1$. Siispä R_1 on renkaan $\mathbb{Q}$ alirengas.

b) Joukko R_2 ei ole alirengas, sillä $0_{\mathbb{Q}} = 0 = 0/1 \notin R_2$.

c) Joukko R_3 on alirengas, mikä nähdään jälleen alirengaskriteerin avulla a)-kohdan tapaan. Huomaa nimittäin, että luku 1 on myös kakkosen potenssi, $1 = 2^0$.

d) Renkaan R_1 yksikköryhmä on joukko $R_1^* = \{m/n \mid m \text{ ja } n \text{ ovat molemmat parittomia}\}$, koska $(m/n)^{-1} = n/m$. Renkaan R_3 yksikköryhmä on $R_3^* = \{2^n \mid n \in \mathbb{Z}\}$, koska luku m on käänteisalkionsa $m^{-1} = 1/m$ nimittäjä.

45. Ensinnäkin $(\mathbb{R}_{>0}, \oplus)$ on kommutatiivinen ryhmä, koska se on kommutatiivisen ryhmän $(\mathbb{R}^*, \cdot)$ aliryhmä. Selvästi $*$ on joukossa $\mathbb{R}_{>0}$ määritelty binäärioperaatio. Loppujen ehtojen tarkistamiseksi oletetaan, että luvut $x, y, z \in \mathbb{R}_{>0}$ on valittu mielivaltaisesti. Tarkistetaan kolmanneksi liitäntälaki:

$$x * (y * z) = x^{\lg y^{\lg z}} = x^{\lg z \lg y} = (x^{\lg y})^{\lg z} = (x * y) * z.$$

Ykkösalkioksi kelpaa nyt luku $1_{\mathbb{R}_{>0}} = 10$ (nolla-alkio on luku $0_{\mathbb{R}_{>0}} = 1$). Nimittäin

$$10 * x = 10^{\lg x} = x = x^1 = x^{\lg 10} = x * 10.$$

Viidenneksi tarkistetaan distributiivisuus. Saadaan

$$x * (y \oplus z) = x^{\lg(yz)} = x^{\lg y + \lg z} = x^{\lg y} x^{\lg z} = x * y \oplus x * z \quad \text{ja}$$
$$(x \oplus y) * z = (xy)^{\lg z} = x^{\lg z} y^{\lg z} = x * z \oplus y * z.$$

Lopuksi vielä operaation $*$ kommutatiivisuus:

$$x * y = x^{\lg y} = 10^{\lg x \lg y} = y^{\lg x} = y * x.$$

46. Lasketaan ensin kahden mielivaltaisesti valitun yläkolmiomatriisin $M = \left(\begin{smallmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{smallmatrix}\right) \in \mathcal{M}_3(\mathbb{R})$ ja $M' = \left(\begin{smallmatrix} a' & b' & c' \\ 0 & d' & e' \\ 0 & 0 & f' \end{smallmatrix}\right) \in \mathcal{M}_3(\mathbb{R})$ tulo:

$$\begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix}\begin{pmatrix} a' & b' & c' \\ 0 & d' & e' \\ 0 & 0 & f' \end{pmatrix} = \begin{pmatrix} aa' & ab'+bd' & ac'+be'+cf' \\ 0 & dd' & de'+ef' \\ 0 & 0 & ff' \end{pmatrix}.$$

Huomataan, että yläkolmiomatriisien tulo säilyy yläkolmiomatriisina. Itse asiassa kaikki joukot S_1, S_2 sekä S_3 ovat suljettuja kertolaskun suhteen. S_1 ei kuitenkaan ole suljettu yhteenlaskun suhteen, koska esimerkiksi $I_3 + I_3 \notin S_1$. Niinpä S_1 ei ole alirengas. S_2 ei myöskään ole, sillä renkaan $\mathcal{M}_3(\mathbb{R})$ ykkösalkio $1_{\mathcal{M}_3(\mathbb{R})} = I_3$ ei kuulu siihen. Sen sijaan S_3 on kertolaskun lisäksi suljettu yhteenlaskun suhteen, sisältää kaikkien alkioidensa M vasta-alkiot $-M$ ja myös identiteettimatriisi kuuluu siihen. Niinpä alirengaskriteeristä seuraa, että S_3 on alirengas.

47.

a)

$$\mathbf{ji} = \mathbf{ki}^2 = -\mathbf{k}, \quad \mathbf{kj} = \mathbf{ij}^2 = -\mathbf{i}, \quad \mathbf{ik} = \mathbf{jk}^2 = -\mathbf{j}.$$

b) Distributiivilaista ja a-kohdasta seuraa

$$\begin{aligned} q\overline{q} &= (a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})(a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}) \\ &= a^2 - b^2\mathbf{i}^2 - c^2\mathbf{j}^2 - d^2\mathbf{k}^2 + ab(\mathbf{i} - \mathbf{i}) + ac(\mathbf{j} - \mathbf{j}) + ad(\mathbf{k} - \mathbf{k}) - bc(\mathbf{ij} + \mathbf{ji}) - bd(\mathbf{ik} + \mathbf{ki}) - cd(\mathbf{jk} + \mathbf{kj}) \\ &= a^2 + b^2 + c^2 + d^2, \end{aligned}$$

aina kun $q = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \in \mathbb{H}$.

c) b-kohdan mukaan $q\overline{q} \in \mathbb{R} \setminus \{0\}$, kaikilla $q \in \mathbb{H} \setminus \{0\}$. Niinpä alkion $q \in \mathbb{H} \setminus \{0\}$ käänteisalkio on $q^{-1} = (q\overline{q})^{-1}\overline{q}$.

d) Käytetään alirengaskriteeriä. Ensinnäkin ykkösalkio eli identiteettimatriisi $I_2 = M(1, 0)$ kuuluu triviaalisti joukkoon $\mathbb{H}'$. Oletetaan, että matriisit $M(z_1, z_2), M(z_1', z_2') \in \mathbb{H}'$ on valittu mielivaltaisesti. Silloin

$$\begin{aligned} M(z_1, z_2) - M(z_1', z_2') &= \begin{pmatrix} z_1 & z_2 \\ -\overline{z_2} & \overline{z_1} \end{pmatrix} - \begin{pmatrix} z_1' & z_2' \\ -\overline{z_2'} & \overline{z_1'} \end{pmatrix} = \begin{pmatrix} z_1 - z_1' & z_2 - z_2' \\ -\overline{z_2} + \overline{z_2'} & \overline{z_1} - \overline{z_1'} \end{pmatrix} \\ &= \begin{pmatrix} z_1 - z_1' & z_2 - z_2' \\ -\overline{z_2 - z_2'} & \overline{z_1 - z_1'} \end{pmatrix} = M(z_1 - z_1', z_2 - z_2') \in \mathbb{H}'. \end{aligned}$$

Kolmanneksi

$$\begin{aligned} M(z_1, z_2)M(z_1', z_2') &= \begin{pmatrix} z_1 & z_2 \\ -\overline{z_2} & \overline{z_1} \end{pmatrix}\begin{pmatrix} z_1' & z_2' \\ -\overline{z_2'} & \overline{z_1'} \end{pmatrix} = \begin{pmatrix} z_1 z_1' - z_2\overline{z_2'} & z_1 z_2' + z_2\overline{z_1'} \\ -\overline{z_2} z_1' - \overline{z_1} z_2' & -\overline{z_2} z_2' + \overline{z_1} z_1' \end{pmatrix} \\ &= \begin{pmatrix} z_1 z_1' - z_2\overline{z_2'} & z_1 z_2' + z_2\overline{z_1'} \\ -\overline{z_1 z_2' + z_2\overline{z_1'}} & \overline{z_1 z_1' - z_2\overline{z_2'}} \end{pmatrix} = M(z_1 z_1' - z_2\overline{z_2'}, z_1 z_2' + z_2\overline{z_1'}) \in \mathbb{H}'. \end{aligned}$$

e) Olkoon kuvaus $h : \mathbb{H} \to \mathbb{H}'$, $h(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) = M(a + b\mathrm{i}, c + d\mathrm{i})$. Selvästi h on bijektio. Näytetään, että se on homomorfismi, eli isomorfismi. Oletetaan, että alkiot $q = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$, $q' = a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k} \in \mathbb{H}$ on valittu mielivaltaisesti. Silloin ensinnäkin

$$\begin{aligned} h(q+q') &= h\big((a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) + (a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k})\big) = h\big(a + a' + (b + b')\mathbf{i} + (c + c')\mathbf{j} + (d + d')\mathbf{k}\big) \\ &= M\big(a + a' + (b + b')\mathrm{i}, c + c' + (d + d')\mathrm{i}\big) = M(a + b\mathrm{i}, c + d\mathrm{i}) + M(a' + b'\mathrm{i}, c' + d'\mathrm{i}) \\ &= h(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) + h(a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k}) = h(q) + h(q'). \end{aligned}$$

Toiseksi d-kohdan avulla saadaan

$$\begin{aligned} h(qq') &= h\big((a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})(a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k})\big) \\ &= h\big(aa' - bb' - cc' - dd' + (ab' + ba' + cd' - dc')\mathbf{i} \\ &+ (ac' + ca' - bd' + db')\mathbf{j} + (ad' + da' + bc' - cb')\mathbf{k}\big) \\ &= M\big(aa' - bb' - cc' - dd' + (ab' + ba' + cd' - dc')\mathrm{i}, \\ &\quad ac' + ca' - bd' + db' + (ad' + da' + bc' - cb')\mathrm{i}\big) \\ &= M\big((a + b\mathrm{i})(a' + b'\mathrm{i}) - (c + d\mathrm{i})(c' - d'\mathrm{i}) \ , \ (a + b\mathrm{i})(c' + d'\mathrm{i}) + (c + d\mathrm{i})(a' - b'\mathrm{i})\big) \\ &= M\big((a + b\mathrm{i})(a' + b'\mathrm{i}) - (c + d\mathrm{i})\overline{(c' + d'\mathrm{i})} \ , \ (a + b\mathrm{i})(c' + d'\mathrm{i}) + (c + d\mathrm{i})\overline{(a' + b'\mathrm{i})}\big) \\ &= M(a + b\mathrm{i}, c + d\mathrm{i})M(a' + b'\mathrm{i}, c' + d'\mathrm{i}) = h(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})h(a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k}) = h(q)h(q'). \end{aligned}$$

Kolmanneksi

$$h(1_{\mathbb{H}}) = h(1) = M(1, 0) = I_2 = 1_{\mathbb{H}'}.$$

48. Selvästi luvut 1, i, -1 ja $-\mathrm{i}$ ovat yksikköjä, sillä $(\pm 1)^2 = -\mathrm{i}^2 = 1$. Olkoon sitten $z = a + b\mathrm{i} \in \mathbb{Z}[\mathrm{i}]$. Silloin $z\overline{z} = a^2 + b^2$. Siispä $z\overline{z}$ on aina positiivinen kokonaisluku, kun $z \neq 0$. Jos nyt z on yksikkö, eli on olemassa käänteislukuluku $z^{-1} \neq 0$, jolla $zz^{-1} = 1$, niin

$$(a^2 + b^2)z^{-1}\overline{z^{-1}} = z\overline{z}z^{-1}\overline{z^{-1}} = zz^{-1}\overline{zz^{-1}} = 1^2 = 1.$$

Tästä seuraa $a^2 + b^2 = 1$, eli $(a, b) \in \{(\pm 1, 0), (0, \pm 1)\}$, eli $z \in \{\pm 1, \pm\mathrm{i}\}$.

49. Oletetaan ensin, että a ja b kommutoivat ja n on yhtä suurempi kokonaisluku. Silloin

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

Oletetaan sitten, että kyseinen yhtälö pätee alkioilla a ja b sekä kaikilla kokonaisluvuilla $n > 1$. Silloin se pätee erityisesti kokonaisluvulla $n = 2$, eli

$$a^2 + ab - ba - b^2 = (a - b)(a + b) = a^2 - b^2.$$

Vähentämällä puolittain $a^2 - b^2$ saadaan $ab - ba = 0$, eli $ab = ba$. Siispä a ja b kommutoivat.

50.

a) $\overline{a}^n = \overline{0}$, jos ja vain jos $a^n \equiv 0 \pmod{16}$, jos ja vain jos 16 jakaa luvun a^n. Siispä $\overline{a}$ on nilpotentti, jos ja vain jos a on parillinen.

b) Tällä kertaa $\overline{a}$ on nilpotentti, jos ja vain jos sekä kolme että viisi jakavat luvun a. Välillä $-7 \leq a \leq 7$ vain luku 0 täyttää tämän ehdon.

c) Oletetaan, että $a^n = 0$, jollakin kokonaisluvulla $n > 0$. Silloin

$$(1-a)(1+a+a^2+\dots a^{n-1}) = 1+a+\dots+a^{n-1}-(a+a^2+\dots+a^n) = 1-a^n = 1-0 = 1,$$

eli $1+a+\dots a^{n-1}$ on alkion $1-a$ käänteisalkio. Siispä $1-a \in R^*$.

51.

a) Kongruenssiehdosta saadaan suoraan laskemalla $[a]*[b] = [a*b] = [c*d] = [c]*[d]$.

b) Kohdasta a) seuraa, että operaatiot $+$ ja $\cdot$ ovat hyvinmääritellyt myös joukolle $R/\!\sim$. Renkaan $R/\!\sim$ laskulait palautuvat renkaan R laeiksi. Renkaassa $R/\!\sim$ on $0_{R/\sim} = [0_R]$ ja $1_{R/\sim} = [1_R]$ sekä luokan $[a]$ käänteisluokka $-[a] = [-a]$. Näytetään esimerkiksi distributiivilaki. Oletetaan, että alkiot $a, b, c \in G$ on valittu mielivaltaisesti. Saadaan

$$\begin{aligned}
&[a]([b]+[c]) = [a][b+c] = [a(b+c)] = [ab+ac] = [ab]+[ac] = [a][b]+[a][c] \quad \text{ja}\\
&([a]+[b])[c] = [a+b][c] = [(a+b)c] = [ac+bc] = [ac]+[bc] = [a][c]+[b][c].
\end{aligned}$$

Koska alkiot a, b ja c oli valittu mielivaltaisesti, toimivat yllä olevat ehdot tietenkin kaikille renkaan R alkioille ja siis kaikille renkaan $R/\!\sim$ luokille.

c) Olkoon a, b, c ja d mielivaltaisesti valittuja renkaan R alkioita ja oletetaan, että $a \sim b$ ja $c \sim d$. Silloin $a = b + i_1$ ja $c = d + i_2$, joillakin ihanteen I alkioilla i_1 ja i_2. Koska $(R, +)$ on kommutatiivinen ryhmä saadaan

$$a + c = b + i_1 + d + i_2 = b + d + i_1 + i_2 \in b + d + I,$$

eli $a + c \sim b + d$. Koska I on ihanne, niin $i_1 d, b i_2 \in I$. Nyt saadaan

$$ac = (b + i_1)(d + i_2) = bd + i_1 d + b i_2 + i_1 i_2 \in bd + I,$$

eli $ac \sim bd$. Koska kongruenssiehto toimii mielivaltaisesti valituille alkioille, toimii se silloin kaikille renkaan R alkioille. Siispä $\sim$ on kongruenssi.

d) Osoitetaan väite Ihannekriteerin avulla. Luonnollisesti $[0_R]$ on epätyhjä, koska ainakin $0 \in [0_R]$. Oletetaan sitten, että $a, b \in [0_R]$ ja $r \in R$. Silloin relaation $\sim$ refleksiivisyydestä ja kongruenssiehdosta saadaan

$$\begin{aligned}
a - b = a - b + 0_R \sim a - b + b = a \sim 0_R \quad &\text{ja}\\
ra \sim r0_R = 0_R = 0_R r \sim ar,&
\end{aligned}$$

eli $a - b, ra, ar \in [0_R]$. Siispä $[0_R]$ on renkaan R ihanne.

52. Olkoon I jokin mielivaltaisesti valittu, nollasta eroava, renkaan R ihanne ja $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in I$ nollamatriisista eroava matriisi. Määritetään aluksi neljä ihanteesta I löytyvää matriisia:

$$\begin{aligned}
M_{vy} &= \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)\alpha\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & 0 \\ 0 & 0 \end{smallmatrix}\right),\\
M_{oy} &= \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)\alpha\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & b \\ 0 & 0 \end{smallmatrix}\right),\\
M_{va} &= \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)\alpha\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ c & 0 \end{smallmatrix}\right),\\
M_{oa} &= \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)\alpha\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & d \end{smallmatrix}\right).
\end{aligned}$$

Nyt huomataan, että esimerkiksi $a = 0$, jos ja vain jos M_{vy} on nollamatriisi. Samoin $b = 0$, jos ja vain jos $M_{oy} = 0$, jne. Niinpä ainakin yksi näistä neljästä matriisista $M_{vy}, \dots, M_{oa}$

eroaa nollamatriisista. Oletetaan nyt esimerkiksi, että $M_{va} = \left(\begin{smallmatrix} 0 & 0 \\ c & 0 \end{smallmatrix}\right)$ poikkeaa nollamatriisista (muut tapaukset käsitellään vastaavasti). On helppo havaita, että jos jotakin matriisia kerrotaan vasemmalta matriisilla $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, vaihtavat sen vaakarivit paikkoja. Vastaavasti oikealta kertomalla vaihtavat pystysarakkeet paikkoja. Niinpä löydetään kaksi uutta ihanteen I matriisia:

$$N_1 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) M_{va} = \left(\begin{smallmatrix} c & 0 \\ 0 & 0 \end{smallmatrix}\right) \quad \text{ja}$$
$$N_2 = M_{va} \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & c \end{smallmatrix}\right).$$

Nyt säännöllinen diagonaalimatriisi $\left(\begin{smallmatrix} c & 0 \\ 0 & c \end{smallmatrix}\right) = N_1 + N_2$ kuuluu ihanteeseen I, jolloin myös identiteettimatriisi, eli renkaan R ykkösalkio, $1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} c^{-1} & 0 \\ 0 & c^{-1} \end{smallmatrix}\right)\left(\begin{smallmatrix} c & 0 \\ 0 & c \end{smallmatrix}\right) \in I$. Silloin $R = R \cdot 1 \subseteq I$, eli $I = R$. Koska I, ja samalla α, oli valittu mielivaltaisesti, ei renkaassa R ole muita ihanteita triviaalien ihanteiden $\{0\}$ ja R lisäksi.

53.

a) Aluksi kannattaa pistää merkille, että olipa f mikä tahansa ryhmähomomorfismi ja n mikä tahansa kokonaisluku, niin $f(\overline{2n}) = 2f(\overline{n}) = \overline{0}$. Edelleen $f(\overline{2n+1}) = f(\overline{2n}) + f(\overline{1}) = f(\overline{1})$. Niinpä on olemassa vain kaksi erisuurta ryhmähomomorfismia f_0 ja f_1, missä $f_0(\overline{n}) = \overline{0}$, kaikilla $n \in \mathbb{Z}$, ja $f_1(\overline{0}) = f_1(\overline{2}) = f_1(\overline{4}) = \overline{0}$ sekä $f_1(\overline{1}) = f_1(\overline{3}) = f_1(\overline{5}) = \overline{1}$.

b) Ainoastaan f_1 kuvaa ykkösalkion ykkösalkioksi. Myöskin

$$f_1(\overline{m \cdot n}) = \begin{cases} \overline{1} & \text{jos } m \text{ ja } n \text{ ovat kumpikin parittomia,} \\ \overline{0} & \text{muuten,} \end{cases}$$

eli $f_1(\overline{m} \cdot \overline{n}) = f_1(\overline{m}) f(\overline{n})$. Siispä ainoastaan f_1 on rengashomomorfismi.

c) Oletetaan, että $f : \mathbb{Z}_2 \to \mathbb{Z}_6$ on jokin ryhmähomomorfismi. Silloin

$$2f(\overline{1}) = f(\overline{2}) = f(\overline{0}) = \overline{0},$$

joten $f(\overline{1})$ on joko $\overline{0}$ tai $\overline{3}$. Näin ryhmähomomorfismeja on jälleen vain kaksi kappaletta. Kumpikaan ei kuvaa ykkösalkiota ykkösalkioksi, eikä siis ole rengashomomorfismi.

54.

a) Näytetään alirengaskriteerillä, että $U_2(\mathbb{R})$ on renkaan $\mathcal{M}_2(\mathbb{R})$ alirengas. Ensinnäkin $1_{\mathcal{M}_2(\mathbb{R})} = I_2$ kuuluu joukkoon $U_2(\mathbb{R})$. Toiseksi yläkolmiomatriisien erotus on triviaalisti edelleen yläkolmiomatriisi. Lasketaan vielä yläkolmiomatriisien tulo:

$$\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)\left(\begin{smallmatrix} a' & b' \\ 0 & d' \end{smallmatrix}\right) = \left(\begin{smallmatrix} aa' & ab'+bd' \\ 0 & dd' \end{smallmatrix}\right) \in U_2(\mathbb{R}).$$

b) Nolla-alkiona toimii $(0,0)$ ja ykkösalkiona $(1,1)$. Kaikki rengaspostulaattien todistukset ovat suoraviivaisia laskuja. Näytetään esimerkkinä ensimmäinen distributiivilaeista:

$$\begin{aligned}(a_1,a_2)\big((b_1,b_2)+(c_1,c_2)\big) &= (a_1,a_2)(b_1+c_1,b_2+c_2) = \big(a_1(b_1+c_1), a_2(b_2+c_2)\big) \\ &= (a_1b_1+a_1c_1, a_2b_2+a_2c_2) = (a_1b_1,a_2b_2)+(a_1c_1,a_2c_2) \\ &= (a_1,a_2)(b_1,b_2)+(a_1,a_2)(c_1,c_2).\end{aligned}$$

c) Oletetaan, että $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right), \left(\begin{smallmatrix} a' & b' \\ 0 & d' \end{smallmatrix}\right) \in U_2(\mathbb{R})$. Silloin

$$f\left(\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) + \left(\begin{smallmatrix} a' & b' \\ 0 & d' \end{smallmatrix}\right)\right) = f\left(\begin{smallmatrix} a+a' & b+b' \\ 0 & d+d' \end{smallmatrix}\right) = (a+a', d+d') = (a,d) + (a',d') = f\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) + f\left(\begin{smallmatrix} a' & b' \\ 0 & d' \end{smallmatrix}\right)$$

ja

$$f\left(\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)\left(\begin{smallmatrix} a' & b' \\ 0 & d' \end{smallmatrix}\right)\right) = f\left(\begin{smallmatrix} aa' & ab'+bd' \\ 0 & dd' \end{smallmatrix}\right) = (aa', dd') = (a,d)(a',d') = f\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) f\left(\begin{smallmatrix} a' & b' \\ 0 & d' \end{smallmatrix}\right).$$

Lisäksi renkaan $U_2(\mathbb{R})$ identiteettialkio I_2 kuvautuu alkioksi $(1,1) = 1_{\mathbb{R}^2}$.

d) Matriisi $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ kuuluu ytimeen $\mathrm{Ker}(f)$, jos ja vain jos $f\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) = 0_{\mathbb{R}^2} = (0,0)$, jos ja vain jos $a = d = 0$. Siispä ytimeksi saadaan $\mathrm{Ker}(f) = \left\{\left(\begin{smallmatrix} 0 & b \\ 0 & 0 \end{smallmatrix}\right) \mid b \in \mathbb{R}\right\}$. Kuvaus f on selvästi surjektio, eli kuvaksi $\mathrm{Im}(f)$ saadaan koko rengas $\mathbb{R}^2$.

e) Renkaiden homomorfialauseesta saadaan nyt isomorfismi

$$F : U_2(\mathbb{R})/\mathrm{Ker}(f) \to \mathbb{R}^2, F\left(\begin{smallmatrix} a & b+\mathbb{R} \\ 0 & d \end{smallmatrix}\right) = (a,d),$$

missä $\left(\begin{smallmatrix} a & b+\mathbb{R} \\ 0 & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) + \mathrm{Ker}(f) = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) + \left\{\left(\begin{smallmatrix} 0 & x \\ 0 & 0 \end{smallmatrix}\right) \mid x \in \mathbb{R}\right\}$.

f) Joukko $A = \left\{\left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right) \mid a, d \in \mathbb{R}\right\}$ on triviaalisti renkaan $U_2(\mathbb{R})$ alirengas (alirengaskriteeri). Kuvaus f rajoitettuna tähän alirenkaaseen on selvästi injektio ja surjektio, eli siis isomorfismi.

55. Oletetaan esimerkiksi, että R on reaalilukujen rengas $\mathbb{R}$ ja S puolestaan kompleksilukujen rengas $\mathbb{C}$. Oletetaan, että h on niin sanottu inkluusiokuvaus, eli $h(x) = x$. Tämä on triviaalisti rengashomomorfismi. Nyt $\mathbb{R}$ itse on renkaan $\mathbb{R}$ ihanne ja myös renkaan $\mathbb{C}$ alirengas. $\mathbb{R}$ ei kuitenkaan ole renkaan $\mathbb{C}$ ihanne, koska luku yksi kuuluu joukkoon $\mathbb{R}$ ja ainoa renkaan $\mathbb{C}$ ihanne, johon ykkösalkio voi kuulua, on $\mathbb{C}$ itse.

56.

a) Lasketaan

$$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4 = a^4 + 2a^2b^2 + b^4$$

ja

$$\begin{aligned}(a+b)^8 &= ((a+b)^4)^2 = (a^4 + 2a^2b^2 + b^4)^2 \\ &= (a^4)^2 + (2a^2b^2)^2 + (b^4)^2 + 2(a^4 2a^2b^2 + a^4b^4 + 2a^2b^2b^4) = a^8 + 2a^4b^4 + b^8.\end{aligned}$$

b) Oletetaan, että

$$(a+b)^{2^k} = a^{2^k} + 2a^{2^{k-1}}b^{2^{k-1}} + b^{2^k},$$

jollakin $k \in \mathbb{Z}_{>0}$. Silloin

$$\begin{aligned}(a+b)^{2^{k+1}} &= ((a+b)^{2^k})^2 = (a^{2^k} + 2a^{2^{k-1}}b^{2^{k-1}} + b^{2^k})^2 \\ &= (a^{2^k})^2 + (2a^{2^{k-1}}b^{2^{k-1}})^2 + (b^{2^k})^2 + 2(a^{2^k}2a^{2^{k-1}}b^{2^{k-1}} + a^{2^k}b^{2^k} + 2a^{2^{k-1}}b^{2^{k-1}}b^{2^k}) \\ &= a^{2^{k+1}} + 2a^{2^k}b^{2^k} + b^{2^{k+1}}.\end{aligned}$$

Siispä induktiivisesti nähdään, että b-kohdan alussa mainittu kaava pätee kaikilla kokonaisluvun k positiivisilla arvoilla.

57.

a) Renkaassa $\mathbb{Z}_8$ kyseinen yhtälö muuntuu muotoon $x^2 = \overline{1}$. Toisin sanoen on etsittävä ne alkiot, jotka ovat itsensä käänteisalkioita. Tämä rajaa heti pois muotoa $\overline{2n}$ olevat alkiot, koska $\mathrm{syt}(2n, 8) > 1$. Toisaalta kaikki muut alkiot käyvät, sillä $\overline{\pm 1}^2 = \overline{1}$ ja $\overline{\pm 3}^2 = \overline{9} = \overline{1}$.

b) Selvästikään $\overline{0}$ ei ole ratkaisu. Distributiivilain avulla saadaan yhtälö muunnettua muotoon $x(x+\overline{8}) = \overline{1}$. Ratkaisuksi kelpaavat siis täsmälleen kaikkia ne alkiot x, joilla on käänteisalkiona $x^{-1} = x + \overline{8} = x - \overline{9}$. Kun halutaan löytää alkion $\overline{n}$, $1 \leq |n| \leq 8$, käänteisalkio, niin kannattaa yrittää löytää luku m, jolla $nm \in \{-16, 18, 35\}$. Nimittäin $\overline{-16} = \overline{18} = \overline{35} = \overline{1}$ kokonaisalueessa $\mathbb{Z}_{17}$. Helposti saadaan

x	$\overline{\pm 1}$	$\overline{\pm 2}$	$\overline{\pm 3}$	$\overline{\pm 4}$	$\overline{\pm 5}$	$\overline{\pm 6}$	$\overline{\pm 7}$	$\overline{\pm 8}$
x^{-1}	$\overline{\pm 1}$	$\overline{\mp 8}$	$\overline{\pm 6}$	$\overline{\mp 4}$	$\overline{\pm 7}$	$\overline{\pm 3}$	$\overline{\pm 5}$	$\overline{\mp 2}$

.

Huomataan, että ainoastaan alkio $\overline{-4}$ toteuttaa yhtälön $x^{-1} = x + \overline{8}$.

58.

a) Ihanne

$$I = \{5a + 5b\mathrm{i} \mid a, b \in \mathbb{Z}\},$$

joten voidaan merkitä

$$\mathbb{Z}[\mathrm{i}]/I = \{a + b\mathrm{i} + I \mid -2 \leq a, b \leq 2\}.$$

Huomataan, että $2 + \mathrm{i} + I$ on nollanjakaja, eikä siis voi olla yksikkö. Nimittäin

$$(2 + \mathrm{i} + I)(2 - \mathrm{i} + I) = (2 + \mathrm{i})(2 - \mathrm{i}) + I = 2^2 + 1^2 + I = 5 + I = 0 + I.$$

Siispä $\mathbb{Z}[\mathrm{i}]/I$ ei ole kokonaisalue.

b) Jäännösluokan $1 + \mathrm{i} + I$ käänteisalkioksi kelpaa $-2 + 2\mathrm{i} + I$. Nimittäin

$$(1 + \mathrm{i} + I)(-2 + 2\mathrm{i} + I) = -2(1 + \mathrm{i})(1 - \mathrm{i}) + I = -4 + I = 1 + I.$$

Kunnat

59. On osoitettava, että R on kommutatiivinen ja että sen kaikilla nollasta eroavilla alkioilla on käänteisalkio. Oletetaan siksi, että alkiot $a, b \in R$ on valittu sattumanvaraisesti ja $a \neq 0_R$.

Alkion a kertaluku additiivisessa ryhmässä $(R, +)$ on suurempi kuin yksi, joten sen täytyy olla p, koska Lagrangen lauseen seurauslauseen mukaan tämä kertaluku jakaa ryhmän $(R, +)$ kertaluvun p, joka oletettiin alkuluvuksi. Tämä merkitsee sitä, että a generoi ryhmän $(R, +)$. Silloin on olemassa positiivinen kokonaisluku m, jolla $b = ma$. Tällöin renkaan $(R, +, \cdot)$ distributiivisuudesta seuraa

$$ab = a(ma) = m(a^2) = (ma)a = ba,$$

eli R on kommutatiivinen rengas.

Koska a generoi ryhmän $(R, +)$, on olemassa positiivinen kokonaisluku n, jolla renkaan R ykkösalkio on $1_R = na$. Toisaalta renkaan R distributiivisuuden vuoksi

$$(n1_R)a = na = a(n1_R),$$

joten alkion a käänteisalkio on $n1_R$. Koska a valittiin mielivaltaisesti, on siis jokaisella renkaan R nollasta eroavalla alkiolla käänteisalkio.

60. Yhtälö pätee triviaalisti nolla-alkiolla, joten oletetaan jatkossa, että $x \neq 0_D$. D on äärellisenä kokonaisalueena kunta, joten $(D \setminus \{0_D\}, \cdot)$ on multiplikatiivinen ryhmä, jossa on $q - 1$ alkiota. Silloin Lagrangen lauseen toisen seurauslauseen mukaan $x^{q-1} = 1_D$, eli $x^q = x$.

61. Ensinnäkin osamääräkunta $Q(\mathbb{Z}[\mathrm{i}])$ on isomorfinen kompleksilukujen kunnan $\mathbb{C}$ alikunnan $\mathbb{C}_{\mathbb{Z}[\mathrm{i}]}$ kanssa. Selvästi kokonaisalue $\mathbb{Z}[\mathrm{i}]$ sisältyy kuntaan $\mathbb{Q}[\mathrm{i}]$, joten $\mathbb{C}_{\mathbb{Z}[\mathrm{i}]} \subseteq \mathbb{Q}[\mathrm{i}]$. Toisaalta

$$\mathbb{Q}[\mathrm{i}] = \left\{ \tfrac{a+b\mathrm{i}}{c} \;\middle|\; a, b, c \in \mathbb{Z} \right\} \subseteq \mathbb{C}_{\mathbb{Z}[\mathrm{i}]}.$$

Siispä $\mathbb{C}_{\mathbb{Z}[\mathrm{i}]} = \mathbb{Q}[\mathrm{i}]$.

62.

a) S_1 on itse asiassa rationaalilukujen kunta $\mathbb{Q}$ itse, sillä

$$\mathbb{Q} = \left\{ \frac{5m}{5n} \;\middle|\; m, n \in \mathbb{Z}, n \neq 0 \right\} \subseteq S_1.$$

S_2 ei voi olla alirengas, sillä kunnan $\mathbb{Q}$ ykkösalkio, eli luku 1, ei kuulu siihen. Joukkoihin S_3 ja S_4 luku 1 sen sijaan kuuluu. Lisäksi

$$\frac{m}{n} - \frac{m'}{n'} = \frac{mn' - m'n}{nn'} \in S_i \quad \text{ja}$$
$$\frac{m}{n}\frac{m'}{n'} = \frac{mm'}{nn'} \in S_i,$$

aina kun $\frac{m}{n}, \frac{m'}{n'} \in S_i$, $i = 3, 4$. Niinpä S_3 ja S_4 ovat molemmat alirenkaita. Ne eivät kuitenkaan kumpikaan ole alikuntia, koska luvun 5 käänteisluku $1/5$ ei kuulu renkaaseen S_3 ja luvun $2 = \frac{2}{5^0}$ käänteisluku $1/2$ ei puolestaan kuulu renkaaseen S_4.

b) S_1 on kuntana triviaalisti myös lokaali rengas, sillä ainoa epäyksikkö nolla muodostaa yksinään nollaihanteen. Renkaan S_3 osalta havaitaan, että

$$E_{S_3} = \left\{ \frac{m}{n} \in S_3 \;\middle|\; 5 | m \right\} = S_2.$$

S_2 on ihannekriteerin mukaan ihanne, sillä se on epätyhjä sekä

$$\frac{5m}{n} - \frac{5m'}{n'} = \frac{5(mn' - m'n)}{nn'} \in S_2 \quad \text{ja}$$
$$\frac{h}{k}\frac{5m}{n} = \frac{5hm}{kn} \in S_2,$$

aina kun $\frac{5m}{n}, \frac{5m'}{n'} \in S_2$ ja $\frac{h}{k} \in S_3$. Siispä S_3 on myös lokaali rengas.
Sen sijaan S_4 ei ole lokaali rengas, koska esimerkiksi luvut 3 ja 2 ovat epäyksikköjä, eli kuuluvat joukkoon E_{S_4}, mutta niiden erotus 1 onkin yksikkö. Jos nimittäin E_{S_4} olisi ihanne, pitäisi myös tämän erotuksen kuulua siihen.

c) E_R on maksimaalinen, jos ja vain jos jäännösluokkarengas R/E_R on kunta. Riittää siis näyttää, että mielivaltaisesti valitulla alkiolla $a + E_R \in R/E_R \setminus \{0 + E_R\}$ on käänteisalkio. Koska $a + E_R$ eroaa nolla-alkiosta, niin a ei kuulu ihanteeseen E_R, eli alkiolla a on käänteisalkio a^{-1} renkaassa R. Silloin alkion $a + E_R$ käänteisalkio jäännösluokkarenkaassa R/E_R on luonnollisesti $a^{-1} + E_R$.

Polynomirenkaat

63.

a) Tehdään sellainen vastaoletus, että on olemassa alkiot $a \in R^* \setminus \{0\}$ ja $b \in R \setminus \{0\}$, joilla $ab = 0$. Silloin

$$b = 1b = a^{-1}ab = a^{-1}0 = 0,$$

mikä on ristiriita. Samaan tulokseen päädytään symmetrian nojalla lähtötilanteesta $ba = 0$.

b) $x^2 + I$ on alkion $x + I$ käänteisalkio, mikä nähdään laskemalla

$$(x + I)(x^2 + I) = x^3 + I = x^3 - (x^3 - 1) + I = 1 + I.$$

c) $x - 1 + I$ ei ole yksikkö, koska se on nollanjakaja. Nimittäin

$$(x - 1 + I)(x^2 + x + 1 + I) = x^3 - 1 + I = 0 + I.$$

$x^2+x+1+I$ ei ole nolla-alkio, eli x^2+x+1 ei kuulu ihanteeseen I, koska kaikkien nollapolynomista eroavien ihanteen I polynomien aste on vähintään kolme (ks. sivua "Ihanteen generointi ja pääihannerengas").

64.

a) Olkoon kuvaus $\rho : \mathbb{R}[x] \to \mathbb{R}$, $\rho(f(x)) = f(0)$. Tämä kuvaus on selvästi homomorfismi, koska renkaan ykkösalkio, vakiopolynomi 1, kuvautuu luvuksi 1 sekä kahden polynomin summan ja tulon arvot pisteessä nolla ovat vastaavien polynomien nollapisteiden arvojen summa ja tulo.
Kuvauksen ytimen muodostavat ne polynomit, jotka saavat arvoksi nollan pisteessä nolla. Nämä ovat täsmälleen ne polynomit, joiden vakiotermi on nolla, eli jotka ovat jaollisia polynomilla x. Siis ydin on polynomin x generoima ihanne.
Kuvaus ρ on selvästi surjektio, eli kuvaksi saadaan kunta. Tämä tarkoittaa sitä, että $< x >$ on maksimaalinen ihanne.
Saman olisi voinut päätellä suoraankin. Oletetaan, että $I = < x > \subset J$ ja $f(x) \in J$. Silloin polynomin $f(x)$ vakiotermi k eroaa nollasta. Nyt $k - f(x) \in I \subset J$, joten $k = f(x) + (k - f(x)) \in J$. Edelleen $1 = k^{-1}k \in J$, joten $J = \mathbb{R}[x]$.

b) Olkoon $\sigma = \rho|_{\mathbb{Z}[x]}$ sama kuin a-kohdan kuvaus ρ, mutta rajoitettuna renkaaseen $\mathbb{Z}[x]$. Silloin σ on myös homomorfismi, jonka ydin on polynomin x generoima ihanne. Tällä kertaa kyseinen ihanne ei kuitenkaan ole maksimaalinen, sillä kuva $\mathrm{Im}(\sigma) = \mathbb{Z}$ ei nyt olekaan kunta. Esimerkiksi $< x > \subseteq < x, 2 > = J$, missä ihanne J sisältää kaikki sellaiset polynomit, joiden vakiotermi on parillinen.

65.

a) Oletetaan, että polynomit $p(x), q(x) \in I$ ja $r(x) \in \mathbb{Z}[x]$ on valittu mielivaltaisesti. Silloin $p(0) = 2m$ ja $q(0) = 2n$, joillakin kokonaisluvuilla m ja n. Tästä seuraa, että

$$\begin{aligned}(p - q)(0) = p(0) - q(0) = 2(m - n) \quad &\text{ja} \\ rp(0) = r(0)p(0) = 2mr(0) = pr(0),&\end{aligned}$$

eli $(p-q)(x), rp(x), pr(x) \in I$. Selvästi $2 \in I$, joten I ei ole tyhjä. Siispä ihannekriteerin mukaan I on ihanne.

b) Näytetään ensin, että $I \subseteq < x, 2 >$. Oletetaan siis, että $p(x) \in I$. Silloin

$$p(x) = 2a_0 + a_1x + \cdots + a_nx^n = (a_1 + a_2x + \dots a_nx^{n-1})x + a_0 2 \in < x, 2 >,$$

joillakin kokonaisluvuilla $a_0, \dots, a_n$.
Näytetään toiseksi, että $< x, 2 > \subseteq I$. Oletetaan, että $q(x), r(x) \in \mathbb{Z}[x]$ ja $p(x) = q(x)x + r(x)2 \in < x, 2 >$. Silloin $p(0) = q(0)0 + r(0)2 = 2r(0)$ on parillinen luku, eli $p(x) \in I$. Siispä $I = < x, 2 >$.

c) Näytetään, ettei I ole pääihanne. Tehdään sellainen vastaoletus, että $I = < b(x) >$. Nyt

$$\deg r(x)b(x) = \deg r(x) + \deg b(x) \geq b(x),$$

joten $\deg b(x) = 0$, eli $b(x) = b$ on vakiopolynomi, koska vakiopolynomi 2 kuluu ihanteeseen I. Toisaalta myös polynomi x kuuluu ihanteeseen I, eli on olemassa polynomi $s(x)$, jolla $x = s(x)b(x)$. Tällöin polynomin $b(x)$ johtavan kertoimen b itseisarvon on oltava yksi. Siispä $b(x) \in \{\pm 1\}$. Mutta silloin myös vakiopolynomi 1 kuuluu ihanteeseen I, mikä on ristiriita. Siispä I ei ole pääihanne, eikä $\mathbb{Z}[x]$ pääihannerengas.

66.

a) Tehdään sellainen vastaoletus, että $x^5 + x^2 + 1 = p(x)q(x)$, missä $1 \leq \deg p(x) \leq 2$. Ensimmäisen asteen tekijöitä ei polynomilla ole, koska sillä ei ole nollakohtia kunnassa $\mathbb{Z}_2$. Niinpä polynomin $p(x)$ aste on kaksi. Molempien polynomien $p(x)$ ja $q(x)$ vakiokertoimien täytyy olla yksi, koska polynomin $x^5 + x^2 + 1$ vakiokerroinkin on yksi. Saadaan

$$\begin{aligned} x^5 + x^2 + 1 = p(x)q(x) &= (x^2 + ax + 1)(x^3 + bx^2 + cx + 1) \\ &= x^5 + (a + b)x^4 + (c + ab + 1)x^3 + (b + ac + 1)x^2 + (a + c)x + 1, \end{aligned}$$

joillakin alkioilla $a, b, c \in \mathbb{Z}_2$. Vertaamalla termien kertoimia saadaan neljän yhtälön yhtälöryhmä

$$\begin{cases} a + b = 0 \\ c + ab + 1 = 0 \\ b + ac + 1 = 1 \\ a + c = 0. \end{cases}$$

Ensimmäisestä ja viimeisestä yhtälöstä seuraa $a = b = c$. Silloin toinen yhtälö johtaa umpikujaan, koska sen vasemmaksi puoleksi kunnassa $\mathbb{Z}_2$ saadaan aina

$$c + ab + 1 = a + a^2 + 1 = 2a + 1 = 1.$$

Niinpä polynomin $x^5 + x^2 + 1$ täytyy olla jaoton.

b) Suoraan laskemalla saadaan

$$\tilde{p}(c^{-1}) = c^{-n}p\big((c^{-1})^{-1}\big) = c^{-n}p(c) = 0.$$

c) Oletetaan, että $\deg p(x) = m$ ja $\deg q(x) = n$, joillakin ei-negatiivisilla kokonaisluvuilla m ja n. Silloin $\deg pq(x) = m + n$ ja

$$\widetilde{pg}(x) = x^{m+n}pq(1/x) = x^m p(1/x)x^n q(1/x) = \tilde{p}(x)\tilde{q}(x).$$

d) Tehdään vastaoletus, että $x^5 + x^3 + 1 = p(x)q(x)$, joillakin positiiviasteisilla polynomeilla $p(x), q(x) \in \mathbb{Z}_2[x]$. Polynomi $x^5 + x^2 + 1$ on polynomin $x^5 + x^3 + 1$ resiprookkipolynomi, joten c-kohdan mukaan polynomi $x^5 + x^2 + 1 = \tilde{p}(x)\tilde{q}(x)$ ei olisikaan jaoton. Tämä on kuitenkin ristiriidassa a-kohdan kanssa.

67. Polynomien jakoalgoritmin mukaan jokaista monomia x^n kohti on olemassa yksikäsitteiset polynomit $s_n(x), r_n(x) \in \mathbb{Z}_2[x]$, $\deg r_n(x) \leq k-1$, joilla $x^n = s_n(x)p(x)+r_n(x)$. Koska jakojäännöspolynomien $r_n(x)$ aste on enintään $k-1$ ja termien kertoimilla on vain kaksi vaihtoehtoa, 0 tai 1, niin näitä polynomeja on enintään 2^k erilaista. Siispä on olemassa kaksi lukua välillä $0 \leq m < n \leq 2^k$, joilla $r_m(x) = r_n(x)$. Silloin

$$\begin{aligned} x^m + x^n &= s_m(x)p(x) + r_m(x) + s_n(x)p(x) + r_n(x) \\ &= \big(s_m(x) + s_n(x)\big)p(x) + r_m(x) + r_n(x) = \big(s_m(x) + s_n(x)\big)p(x), \end{aligned}$$

eli $p(x)$ jakaa polynomin $x^m + x^n$.

68.

a) 0 ja 1 eivät kumpikaan ole polynomin $p(x)$ nollakohtia, eli sillä ei ole nollakohtia kunnassa $\mathbb{Z}_2$. Niinpä sillä ei ole ensimmäisen eikä kolmannen asteen polynomitekijää. Se voisi kuitenkin jakaantua kahdeksi toisen asteen polynomiksi $q_1(x) = x^2 + ax + 1$ ja $q_2(x) = x^2 + bx + 1$, jolloin

$$p(x) = q_1(x)q_2(x) = (x^2 + ax + 1)(x^2 + bx + 1) = x^4 + (a + b)x^3 + abx^2 + (a + b)x + 1.$$

Tällöin kuitenkin huomataan, että polynomin $p(x)$ kolmannen ja ensimmäisen asteiden termien kertoimien pitäisi olla yhtäsuuret, mikä ei pidä paikkaansa. Niinpä polynomin $p(x)$ on oltava jaoton.

b) Koska $\alpha^4 = x^4 + I = x + 1 + (x^4 + x + 1) + I = x + 1 + I = \alpha + 1$, on

$$\begin{aligned} \alpha^5 &= \alpha(\alpha + 1) = \alpha^2 + \alpha \quad \text{ja} \\ \alpha^{10} &= (\alpha^2 + \alpha)^2 = \alpha^4 + \alpha^2 = \alpha^2 + \alpha + 1. \end{aligned}$$

c) Huomataan, että

$$\alpha^{15} = \alpha^5\alpha^{10} = (\alpha^2 + \alpha)(\alpha^2 + \alpha + 1) = \alpha^4 + 2\alpha^3 + 2\alpha^2 + \alpha = \alpha + 1 + \alpha = 1,$$

joten α^5 ja α^{10} ovat toistensa käänteisalkioita ja $(\alpha^{10})^2 = \alpha^5$. Kunnan K jokainen alkio on itsensä vasta-alkio, koska kunnan $\mathbb{Z}_2$ karakteristika on kaksi. Saadaan $\alpha^5 + \alpha^{10} = 1$, $\alpha^5 + 1 = \alpha^{10}$ ja $\alpha^{10} + 1 = \alpha^5$. Siispä joukko A on kunnan K alikunta.

69.

a) Polynomilla $p(x) = x^2 + 3$ ei ole nollakohtaa reaalilukujen kunnassa, joten R_1 on kunta, jonka jokaisella nollasta eroavalla alkiolla on käänteisalkio.

b) Polynomi $p(x) = x^2 - 4 = (x + 2)(x - 2)$ ei ole jaoton yli kunnan $\mathbb{Z}_7$, joten R_2 ei ole kunta. Merkitään $I = < p(x) >$. Kuitenkin alkio $2x + I$ on alkion $x + I$ käänteisalkio renkaassa R_2. Nimittäin

$$(x + I)(2x + I) = 2x^2 + I = -6 + 2(x^2 + 3) + I = -6 + I = 1 + I.$$

c) Merkitään $J = < x^{251} >$. Alkio $x + J$ on nollanjakaja renkaassa R_3, sillä

$$(x + J)(x^{250} + J) = x^{251} + J = 0 + J,$$

joten alkiolla $x + J$ ei voi olla käänteisalkiota renkaassa R_3. Jos nimittäin olisi vaikkapa $\alpha = (x + J)^{-1}$, niin saataisiin

$$x^{250} + J = (x^{250} + J)(1 + J) = (x^{250} + J)(x + J)\alpha = (0 + J)\alpha = 0 + J,$$

mikä on mahdotonta, koska ihanteeseen J kuuluvat nollapolynomin lisäksi täsmälleen kaikki ne polynomit, joiden aste on vähintään 251.