Algebralliset rakenteet I
Helsingin yliopisto, matematiikan ja tilastotieteen laitos
Kevät 2017
Harjoitus 4 - Ratkaisuehdotuksia tähdettömiin tehtäviin

Tehtäväsarja I

1.* Jos et ole varma, miksi $(\mathbb{Z}, +)$ on ryhmän $(\mathbb{R}, +)$ normaali aliryhmä, tarkista se ennen kuin luet eteenpäin. Tutkitaan tekijäryhmää $\mathbb{R}/\mathbb{Z} = (\mathbb{R}, +)/(\mathbb{Z}, +)$. Osoita vasta-alkion ja tekijäryhmän laskutoimituksen määritelmien perusteella, että alkiolla $2/3 + \mathbb{Z}$ on tekijäryhmässä vasta-alkiot $-2/3+\mathbb{Z}$ ja $7/3+\mathbb{Z}$. Miksei tämä ole ristiriidassa sen kanssa, että ryhmän alkiolla voi olla vain yksi käänteisalkio?

2. Olkoon $S^1 = (S^1, \cdot)$ kompleksilukujen yksikköympyrä varustettuna kompleksilukujen kertolaskulla. Kuten aiemmin ollaan todettu, se on ryhmä. Yksikköympyrän alkiot ovat muotoa e^{ix} ja niiden laskutoimitus toteuttaa $e^{ix}e^{iy} = e^{i(x+y)}$. Osoita, että tämä ryhmä on isomorfinen ryhmän $\mathbb{R}/\mathbb{Z}$ kanssa (ks. edellinen tehtävä). Kompleksilukujen käsittelyyn löydät lisäapua kirjan liitteestä.

   Ratkaisuehdotus: Määritellään kuvaus $f\colon S^1 \to \mathbb{R}/\mathbb{Z}$, $f(e^{ix}) = x/(2\pi) + \mathbb{Z}$. Tarkistetaan, että kyseessä on kuvaus osoittamalla kuva-alkioiden yksikäsitteisyys. Oletetaan, että $e^{ix}, e^{iy} \in S^1$ ja $e^{ix} = e^{iy}$. Tällöin kompleksilukujen ominaisuuksien perusteella tiedetään, että $x = y + 2n\pi$ jollakin $n \in \mathbb{Z}$. Nyt

$$\begin{aligned} f(e^{ix}) &= \frac{x}{2\pi} + \mathbb{Z} = \frac{y + 2n\pi}{2\pi} + \mathbb{Z} = \left(\frac{y}{2\pi} + n\right) + \mathbb{Z} \\ &= \left(\frac{y}{2\pi} + \mathbb{Z}\right) + (n + \mathbb{Z}) = \frac{y}{2\pi} + \mathbb{Z} = f(e^{iy}). \end{aligned}$$

   Alkioiden kuva-alkiot eivät siis riipu valittavasta alkion esitystavasta, joten kyseessä on kuvaus.

   Osoitetaan kuvaus f isomorfismiksi. Oletetaan, että $x + \mathbb{Z} \in \mathbb{R}/\mathbb{Z}$. Tällöin $x \in \mathbb{R}$, joten myös $2\pi x \in \mathbb{R}$. On siis olemassa alkio $e^{i2\pi x} \in S^1$, jolla $f(e^{i2\pi x}) = (2\pi x)/(2\pi)+\mathbb{Z} = x+\mathbb{Z}$. Näin ollen f on surjektio.

   Olkoot $e^{ix}, e^{iy} \in S^1$ ja $f(e^{ix}) = f(e^{iy})$. Nyt siis $x/(2\pi) + \mathbb{Z} = y/(2\pi) + \mathbb{Z}$, joten lauseen 11.6 nojalla $x/(2\pi) \in y/(2\pi) + \mathbb{Z}$. Tällöin $x/(2\pi) \in y/(2\pi) + k$ jollakin $k \in \mathbb{Z}$, eli $x = y + 2\pi k$. Näin ollen $e^{ix} = e^{i(y+2\pi k)} = e^{iy}e^{i2\pi k} = e^{iy} \cdot 1 = e^{iy}$, joten f on myös injektio. Kuvaus f on siis bijektio.

   Tarkistetaan vielä isomorfismin määritelmän toinen ehto. Oletetaan, että $e^{ix}, e^{iy} \in S^1$. Tällöin

$$f(e^{ix}e^{iy}) = f(e^{i(x+y)}) = \frac{x+y}{2\pi} + \mathbb{Z} = \left(\frac{x}{2\pi} + \mathbb{Z}\right) + \left(\frac{y}{2\pi} + \mathbb{Z}\right) = f(e^{ix}) + f(e^{iy}).$$

   Kuvaus f on siis isomorfismi, joten $S^1 \cong \mathbb{R}/\mathbb{Z}$.

   (Ryhmien S^1 ja $\mathbb{R}/\mathbb{Z}$ välinen isomorfia voidaan osoittaa myös homomorfialauseen avulla. Tämä on tehty kurssikirjan esimerkissä 21.4.)

3. Oletetaan, että G on vaihdannainen ryhmä, jolla on normaali aliryhmä N. Osoita, että myös tekijäryhmä G/N on vaihdannainen.

   Ratkaisuehdotus: Oletetaan, että $x, y \in G/N$. Nyt $x = aN$ ja $y = bN$ joillakin $a, b, \in G$. Nähdään, että

   $$xy = aNbN = abN = baN = bNaN = yx.$$

   Tässä käytettiin ryhmän G vaihdannaisuutta.

   Siten ryhmä G/N on vaihdannainen.

4. Olkoon G ryhmä ja N sen normaali aliryhmä. Osoita, että tekijäryhmän G/N alkiolle gN pätee $(gN)^k = g^kN$ kaikilla $k \in \mathbb{Z}$.

   Ratkaisuehdotus: Osoitetaan ensin induktiolla, että väite pätee kaikilla $k \in \mathbb{N}$.

   - *Alkuaskel:* Potenssin määritelmän nojalla $(gN)^0 = N = eN = g^0N$, joten väite pätee luvulla 0.
   - *Induktioaskel:* Oletetaan, että $k \in \mathbb{N}$ on sellainen, jolla $(gN)^k = g^kN$. Nyt potenssin määritelmän nojalla

     $$(gN)^{k+1} = (gN)^k(gN) = (g^kN)(gN) = g^kgN = g^{k+1}N,$$

     joten väite pätee myös luvulla $k + 1$.

   Siis induktioperiaatteen nojalla $(gN)^k = g^kN$ kaikilla $k \in \mathbb{N}$. Oletetaan sitten, että $k \in \mathbb{Z}$, $k < 0$. Tällöin $-k \in \mathbb{N}$, joten äskeisen nojalla

   $$(gN)^k = ((gN)^{-k})^{-1} = (g^{-k}N)^{-1} = (g^{-k})^{-1}N = g^kN.$$

   (Alkion $hN \in G/N$ käänteisalkio on $h^{-1}N$, koska $(hN)(h^{-1}N) = (hh^{-1})N = eN$ ja toisin päin.) Näin ollen $(gN)^k = g^kN$ kaikilla $k \in \mathbb{Z}$.

Tehtäväsarja II

5. Luettele kaikki polynomirenkaan $\mathbb{Z}_2[X]$ astetta kolme olevat alkiot.

   Ratkaisuehdotus: Polynomirenkaan $\mathbb{Z}_2[X]$ kaikki kolmannen asteen polynomit ovat $X^3, X^3+1, X^3+X, X^3+X^2, X^3+X+1, X^3+X^2+1, X^3+X^2+X$ ja X^3+X^2+X+1.

6.* Korollaarin 22.8 mukaan, polynomirengas on kokonaisalue, jos sen kerroinrengas on kokonaisalue. Osoita, että käänteinen pätee myös: jos rengas $R = (R, +, \cdot)$ *ei* ole kokonaisalue, niin ei myöskään $R[X]$ ole.

Tehtäväsarja III

7. Määritä polynomin $X^2 - X - 1 \in \mathbb{Z}_5[X]$ juuret.

Ratkaisuehdotus: Merkitään $P = X^2 - X - 1$. Määritelmän mukaisesti jokin kerroinrenkaan $\mathbb{Z}_5$:n alkio c on juuri, mikäli $P(c) = 0_R$. Etsitään P:n juuret käymällä $\mathbb{Z}_5$:n alkiot läpi.

$$\begin{aligned}
P([0]_5) &= [0]_5^2 - [0]_5 - [1]_5 = -[1]_5 = [4]_5 \\
P([1]_5) &= [1]_5^2 - [1]_5 - [1]_5 = [1]_5 - [1]_5 - [1]_5 = -[1]_5 = [4]_5 \\
P([2]_5) &= [2]_5^2 - [2]_5 - [1]_5 = [4]_5 - [2]_5 - [1]_5 = [1]_5 \\
P([3]_5) &= [3]_5^2 - [3]_5 - [1]_5 = [9]_5 - [3]_5 - [1]_5 = [5]_5 = [0]_5 \\
P([4]_5) &= [4]_5^2 - [4]_5 - [1]_5 = [16]_5 - [4]_5 - [1]_5 = [11]_5 = [1]_5
\end{aligned}$$

Tuloksista nähdään, että polynomilla P on vain yksi juuri ja se on $[3]_5$.

8. Etsi jokin ensimmäistä astetta oleva polynomi, joka jakaa edellisen tehtävän polynomin.

   Ratkaisuehdotus: Koska kerroinrengas $\mathbb{Z}_5$ on kunta, lauseen 23.9 nojalla polynomi $X^2 - X - 1$ on jaollinen ensimmäisen asteen polynomilla $X - 3$; itse asiassa $X^2 - X - 1 = (X - 3)(X - 3)$, kuten laskemalla huomataan.

9. Tässä tehtävässä tarkasteltavat polynomit ovat $\mathbb{Z}_5$-kertoimisia. Osoita, että vakiopolynomi 4 jakaa polynomin $-2X^3 - 3X + 1$.

   Ratkaisuehdotus: Koska $[-2]_5 = [3]_5$ ja $[-3]_5 = [2]_5$, niin polynomirenkaassa $\mathbb{Z}_5[X]$ pätee $-2X^3 - 3X + 1 = 3X^3 + 2X + 1$. Nyt huomataan, että

   $$4 \cdot \Big(2X^3 + 3X + 4\Big) = 8X^3 + 12X + 16 = 3x^3 + 2X + 1 = -2X^3 - 3X + 1.$$

   Näin ollen vakiopolynomi 4 jakaa polynomin $-2X^3 - 3X + 1$.

10. Onko polynomi $X^4 + 2X^2 + 1 \in \mathbb{Z}_3[X]$ jaoton?

    Ratkaisuehdotus: Polynomi ei ole jaoton, koska $X^4 + 2X^2 + 1 = (X^2 + 1)(X^2 + 1)$. (Jos tarkistaa polynomin juuret, huomaa, että niitä ei ole. Tästä nähdään, että vaikka polynomilla ei olisi lainkaan juuria, se ei silti välttämättä ole jaoton.)

Tehtäväsarja IV

11. Mitkä näistä ovat homomorfismejä?

    Ratkaisuehdotus: Olkoot $n, m \in \mathbb{Z}$. Tällöin

    $$\begin{aligned}
    f(n+m) &= 5(n+m) = 5n + 5m = f(n) + f(m), \\
    g(n+m) &= 0 = 0 + 0 = g(n) + g(m) \quad \text{ja} \\
    k(n+m) &= -(n+m) = -n - m = k(n) + k(m).
    \end{aligned}$$

    Näin ollen f,g ja k ovat homomorfismeja. Osoitetaan, ettei h ole homomorfismi vastaesimerkillä. Esimerkiksi

    $$h(2+2) = h(4) = 2^4 = 16 \neq 8 = 4 + 4 = 2^2 + 2^2 = h(2) + h(2).$$

    Täten h ei ole homomorfismi $\mathbb{Z} \to \mathbb{Z}$.

12. Olkoon $l\colon \mathbb{Z} \to \mathbb{Z}_7$ määritelty kaavalla $l(n) = [n]_7$. Osoita, että tämä on homomorfismi, mutta ei isomorfismi.

    Ratkaisuehdotus: Oletetaan, että $a, b \in \mathbb{Z}$. Tällöin

    $$l(n+m) = [n+m]_7 = [n]_7 + [m]_7 = l(n) + l(m).$$

    Näin ollen l on homomorfismi.

    Kuvaus l ei ole isomorfismi, sillä se ei ole injektio. Esimerkiksi $l(0) = [0]_7$ ja $l(7) = [7]_7 = [0]_7$, mutta $0 \neq 7$. Tällöin l ei voi olla bijektiivinen.

13. Määritä niiden yllä olevien kuvausten ytimet, jotka ovat ryhmähomomorfismejä.

    Ratkaisuehdotus: Ytimen määritelmän mukaan

    $$\begin{aligned}\operatorname{Ker} f &= \{m \in \mathbb{Z} \mid f(m) = 0\} \\ &= \{m \in \mathbb{Z} \mid 5m = 0\}.\end{aligned}$$

    Ainoa kokonaisluku m, jolla pätee $5m = 0$, on 0, joten $\operatorname{Ker} f = 0$.

    Koska $g(m) = 0$ kaikilla $m \in \mathbb{Z}$, pätee $\operatorname{Ker} g = \mathbb{Z}$.

    Kuten kuvauksella f, on kuvauksen h ydin $\operatorname{Ker} h = \{m \in \mathbb{Z} \mid h(m) = -m = 0\} = \{0\}$.

    Kuvauksen l ytimeksi saadaan

    $$\begin{aligned}\operatorname{Ker} l &= \{m \in \mathbb{Z} \mid l(m) = [m]_7 = [0]_7\} \\ &= \{m \in \mathbb{Z} \mid m = 7k \text{ jollakin } k \in \mathbb{Z}\} \\ &= \{7k \mid k \in \mathbb{Z}\} = 7\mathbb{Z}.\end{aligned}$$

14. Anna esimerkki kahdesta ryhmästä ja niiden välisestä ryhmähomomorfismista, jossa jokaisen alkion alkukuva sisältää täsmälleen kaksi alkiota, eli $f\colon G \to H$ ja kaikilla $h \in H$ on olemassa täsmälleen kaksi $g_1, g_2 \in G$ joille pätee $f(g_1) = f(g_2) = h$ (ja $g_1 \neq g_2$).

    Ratkaisuehdotus: Määritellään kuvaus $f\colon \mathbb{Z}_4 \to \mathbb{Z}_2$ kaavalla $f([a]_4) = [a]_2$. Osoitetaan, että kyseessä on ryhmähomomorfismi. Olkoot $[a]_4, [b]_4 \in \mathbb{Z}_4$, jolloin

    $$f([a]_4 + [b]_4) = f([a+b]_4) = [a+b]_2 = [a]_2 + [b]_2 = f([a]_4) + f([b]_4).$$

    Kuvaus f on siis homomorfismi.

    Lisäksi käymällä ryhmän $\mathbb{Z}_4$ alkiot läpi nähdään, että $f([0]_4) = [0]_2 = [2]_2 = f([2]_4)$ ja $f([1]_4) = [1]_2 = [3]_2 = f([3]_4)$. Jokaisen ryhmän $\mathbb{Z}_2$ alkion alkukuvassa on siis täsmälleen kaksi ryhmän $\mathbb{Z}_4$ alkiota.

15.* Olkoon $X = (\{f\colon \mathbb{R} \to \mathbb{R}\}, +)$ kaikkien funktioiden muodostama ryhmä, joiden lähtö- ja maalijoukko on reaaliluvut. Laskutoimitus on määritelty pisteittäin: kaikilla $f, g \in X$ $f + g = h$, missä $h(x) = f(x) + g(x)$. Osoita, että kuvaus $F\colon X \to \mathbb{R}$ joka on määritelty kaavalla $F(f) = f(0)$ on ryhmähomomorfismi ryhmään $(\mathbb{R}, +)$.

Ylimääräisiä tehtäviä

16. Oletetaan, että R on ääretön kunta. Osoita, että kaksi eri polynomirenkaan $R[X]$ polynomia ei voi määrittää samaa polynomikuvausta. Polynomit voidaan siis samastaa polynomikuvausten kanssa, jos kerroinkunta on ääretön.

    Ratkaisuehdotus: Oletetaan, että polynomeja $P \in R[X]$ ja $Q \in R[X]$ vastaa sama polynomikuvaus. Silloin $P(r) = Q(r)$ kaikilla kunnan alkioilla $r \in R$. Yhtäpitävästi $P(r) - Q(r) = 0$ ja edelleen lemman 22.8 nojalla $(P - Q)(r) = 0$. Siten jokainen renkaan R alkio on polynomin $P - Q$ juuri, eli tällä polynomilla on äärettömän monta juurta. Mutta lauseen 22.12 perusteella nollasta poikkeavalla polynomilla on juuria korkeintaan sen asteen verran, eli erityisesti aina äärellinen määrä. Niinpä polynomin $P - Q$ on oltava nollapolynomi! Toisin sanoen $P = Q$ ja väite pätee. Huomaa, että oletimme kerroinrenkaan olevan kunta; tätä tarvitaan lauseessa 22.12.

17. Oletetaan, että R on ääretön kunta. Osoita, että kaksi eri polynomirenkaan $R[X]$ polynomia ei voi määrittää samaa polynomikuvausta. Polynomit voidaan siis samastaa polynomikuvausten kanssa, jos kerroinkunta on ääretön.

    Ratkaisuehdotus: ks. edellinen (sama) tehtävä.

18. Anna esimerkki kahdesta ryhmästä, joiden kertaluku on 42 ja jotka eivät ole isomorfisia keskenään. (Muista perustella, että ryhmät eivät ole isomorfisia.)

    Ratkaisuehdotus: Ratkaisun idea: Otetaan ryhmät $\mathbb{Z}_{42}$ ja $S_3 \times \mathbb{Z}_7$. Kummankin kertaluku on 42. Havaitaan kuitenkin, että $\mathbb{Z}_{42}$ on vaihdannainen mutta koska S_3 ei ole vaidannainen niin myöskään ryhmä $S_3 \times \mathbb{Z}_7$ ei ole vaihdannainne. Näin ollen harjoituksen 5 tehtävän 15 nojalla nämä ryhmät eivät voi olla keskenään isomorfisia.

    Toinen esimerkki epäisomorfisista ryhmistä joiden kertaluku on 42 voisivat olla ryhmä $\mathbb{Z}_{42}$ ja 21-kulmion symmetriaryhmä D_{21}. Ryhmä D_{21} ei nimittäin ole vaihdannainen. Tämän näkee, kun koittaa suorittaa peilauksen ja kierron eri järjestyksissä.