Algebralliset rakenteet I
Helsingin yliopisto, matematiikan ja tilastotieteen laitos
Kevät 2017
Harjoitus 6 - Ratkaisuehdotuksia tähdettömiin tehtäviin

Tehtäväsarja I

1. Totta vai tarua?

   (a) Jokainen sivuluokka on aliryhmä.
   (b) Jokainen aliryhmä on sivuluokka.
   (c) Jokainen jäännösluokka on sivuluokka.

   Ratkaisuehdotus:

   (a) Tämä väite on tarua. Esimerkiksi ryhmällä S_3 on aliryhmä $B = \{(1), (13)\}$. Tarkastellaan sivuluokkaa $(12)B = \{(12), (132)\}$. Jotta kyseessä olisi S_3:n aliryhmä, neutraalialkion (1) tulisi kuulua joukkoon $(12)B$, mikä ei kuitenkaan pidä paikkansa. Siis kaikki sivuluokat eivät ole aliryhmiä.
   (b) Tämä väite on totta. Oletetaan, että G on jokin ryhmä ja H sen jokin aliryhmä. Nyt $e_G H = H$ on H:n sivuluokka, joten jokaisen aliryhmän voidaan ajatella olevan myös sivuluokka.
   (c) Tämä väite on totta. Jokainen jäännösluokka $[k]_n$, $k \in \mathbb{Z}, n \in \mathbb{N}$ voidaan kirjoittaa muodossa $\{k + an \mid a \in \mathbb{Z}\} = k + n\mathbb{Z}$. Näin ollen jokainen jäännösluokka on myös sivuluokka.

2. Olkoon $f\colon \mathbb{Z} \to S_3$ määritelty kaavalla $f(n) = (123)^n$. Merkitään $A_3 = \{(1), (123), (321)\}$. Totta vai tarua?

   (a) Joukko S_3 on f:n maalijoukko.
   (b) Joukko S_3 on f:n arvojoukko.
   (c) Joukko A_3 on f:n maalijoukko.
   (d) Joukko A_3 on f:n arvojoukko.
   (e) f on surjektio.
   (f) f on injektio.
   (g) f:n ydin on $\{0\}$.

   Ratkaisuehdotus:

   (a) Väite on totta. Kuvaus f on määritelty $\mathbb{Z} \to S_3$, joten S_3 on sen maalijoukko.
   (b) Väite on tarua. Esimerkiksi $(12) \in S_3$, mutta ei ole sellaista $n \in \mathbb{Z}$, että $f(n) = (123)^n = (12)$, sillä $(123)^n \in A_3$ kaikilla $n \in \mathbb{Z}$. Ryhmässä S_4 on siis alkio, jolle ei kuvaudu mitään kokonaislukua, joten S_4 ei voi olla arvojoukko.
   (c) Väite on tarua. Kuvauksen f maalijoukoksi on annettu S_4.
   (d) Väite on totta. Koska $(123)^3 = (1)$, lemman 8.6 mukaan

   $$\langle (123) \rangle = \{(1), (123), (123)^2\} = \{(1), (123), (321)\} = A_3.$$

   A_3 on siis (123):n virittämä aliryhmä, joten $f(n) = (123)^n \in A_3$ kaikilla $n \in \mathbb{Z}$.

(e) Väite on tarua. Kuvaus on surjektio vain, jos sen arvojoukko on koko maalijoukko. Koska $A_3 \neq S_3$, f ei siis ole surjektio.

(f) Väite on tarua. Esimerkiksi $f(4) = (123)^4 = (123) = f(1)$, joten f ei ole injektio.

(g) Väite on tarua. Ydin koostuu kaikista niistä lähtöjoukon $\mathbb{Z}$ alkioista, jotka kuvautuvat maalijoukon S_4 neutraalialkiolle. Koska $f(3) = (123)^3 = (1)$, niin $3 \in \operatorname{Ker} f$, eli ydin ei ole $\{0\}$.

3. Olkoon N ryhmän G normaali aliryhmä. Pitääkö tällöin paikkansa, että N on vaihdannainen? Perustele vastauksesi.

Ratkaisuehdotus: Ei pidä. Käytetään vastaesimerkkinä harjoituksen 5 tehtävissä 2 ja 3 esiintynyttä ryhmän $GL_2(\mathbb{R})$ normaalia aliryhmää $S = \{a \in GL_2(\mathbb{R}) \mid \det(a) = 1\}$. Valitsemalla

$$a = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \quad \text{ja} \quad b = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix},$$

niin $a, b \in S$, sillä $\det(a) = \det(b) = 1$. Tällöin $ab \neq ba$, joten S ei ole vaihdannainen.

Tehtäväsarja II

4. Miten ryhmähomomorfismismin ydin ja kuva liittyvät kuvauksen injektiivisyyteen ja surjektiivisuuteen? Selitä omin sanoin, mistä yhteydet näiden käsitteiden välilä johtuvat.

Ratkaisuehdotus: Ryhmähomomorfismi f on injektiivinen täsmälleen silloin, kun sen ydin koostuu pelkästään lähtöjoukon neutraalialkiosta. Määritelmänsä nojalla $\operatorname{Ker} f$ koostuu niistä alkioista, jotka kuvautuvat maalijoukon neutraalialkiolle. Nyt tiedetään, että ainakin lähtöjoukon neutraalialkiolle edellinen pätee. Jos f on injektio, niin mikään muu lähtöjoukon alkio ei voi tuottaa tätä samaa alkiota, joten ytimen on pakko koostua pelkästään neutraalialkiosta.

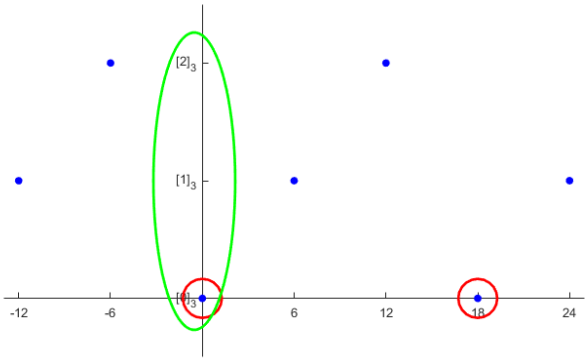
Vastaavasti, jos ytimessä on pelkästään neutraalialkio, niin kuvaus on injektio. Tämän selittäminen onkin hankalampaa ja sen voi tehdä monella eri tavalla. Tässä eräs tapa. Kuvauksen ydin jaottelee lähtöjoukon alkiot sivuluokkiin. Lisäksi kunkin sivuluokan alkiot kuvautuvat keskenään samalle alkiolle, eivätkä eri sivuluokkien alkiot kuvaudu samoille alkioille. Sivuluokat muodostuvat siis itse asiassa sen mukaan, mikä kuva alkioilla on kuvauksessa. Jos ytimessä on pelkkä neutraalialkio, on kaikissa sivuluokissakin vain yksi alkio. Siten jokainen lähtöjoukon alkio kuvautuu eri alkiolle kuin muut alkiot, eli kuvaus on injektio.

Ryhmähomomorfismi f on surjektiivinen täsmälleen silloin, kun sen kuva $\operatorname{Im} f$ on koko maalijoukko. Väite seuraa suoraan surjektiivisuuden määritelmästä. Kun kuvaus on surjektio, niin jokaiselle maalijoukon alkiolle kuvauutuu ainakin yksi lähtöjoukon alkio. Tällöin siis kuvauksen kuvan on pakko olla koko maalijoukko. Jos taas kuva on koko maalijoukko, kuvautuu jokaiselle maalijoukon alkiolle jotain ja kuvaus on siten surjektio.

Huomaa, että surjektiivisuuden tapauksessa ei käytetä mitenkään hyväksi kuvauksen homomorfisuutta. Mikä tahansa kuvaus on surjektio, jos ja vain jos sen kuvajoukko on sama kuin maalijoukko. Merkintää $\operatorname{Im} f$ ja termiä ”kuva” käytetään kuitenkin yleensä vain homomorfismien tapauksessa.

5. Tutkitaan homomorfismia $f\colon 6\mathbb{Z} \to \mathbb{Z}_3$, $f(a) = [a/6]_3$. Havainnollista kuvausta f piirtämällä sen kuvaaja. Merkitse kuvaan aliryhmät $\operatorname{Ker} f$ ja $\operatorname{Im} f$.

   Ratkaisuehdotus:



   Ytimen $\operatorname{Ker} f$ alkiot on merkitty punaisella, vihreällä on kuva $\operatorname{Im} f$, joka on siis koko ryhmä $\mathbb{Z}_3$.

6.* Jatkoa edelliseen tehtävään. Määritä isomorfismi, joka saadaan homomorfismista f ryhmien homomorfialauseen avulla.

7. Osoita ryhmien homomorfialauseen avulla, että tekijäryhmä $(\mathbb{Z} \times \mathbb{Z})/(\mathbb{Z} \times \{0\})$ on isomorfinen ryhmän $\mathbb{Z}$ kanssa.

   Neuvo: Kuvauksesta $f\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $f(a, b) = b$ on apua.

   Ratkaisuehdotus: Tarkistetaan ensin, että annettu kuvaus f on ryhmähomomorfismi. Oletetaan, että $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}$. Tällöin

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

   eli f on homomorfismi.

   Osoitetaan sitten, että homomorfismin f ydin on $\operatorname{Ker} f = \mathbb{Z} \times \{0\}$.

   - "$\subset$": Olkoon $(a, b) \in \operatorname{Ker} f$. Tällöin $f(a, b) = 0$ ja toisaalta $f(a, b) = b$, joten on oltava $b = 0$. Siis $(a, b) = (a, 0) \in \mathbb{Z} \times \{0\}$.
   - "$\supset$": Olkoon $(a, b) \in \mathbb{Z} \times \{0\}$. Tällöin $b = 0$, joten $f(a, b) = f(a, 0) = 0$. Siis $(a, b) \in \operatorname{Ker} f$.

   Havaitaan vielä, että f on surjektio, sillä jos $b \in \mathbb{Z}$, niin esimerkiksi $f(0, b) = b$. Näin ollen $\operatorname{Im} f = \mathbb{Z}$, joten homomorfialause antaa isomorfismin

$$\bar{f}\colon \mathbb{Z} \times \mathbb{Z}/\operatorname{Ker} f \cong \operatorname{Im} f \quad \text{eli}$$
$$\bar{f}\colon \frac{\mathbb{Z} \times \mathbb{Z}}{\mathbb{Z} \times \{0\}} \cong \mathbb{Z}.$$

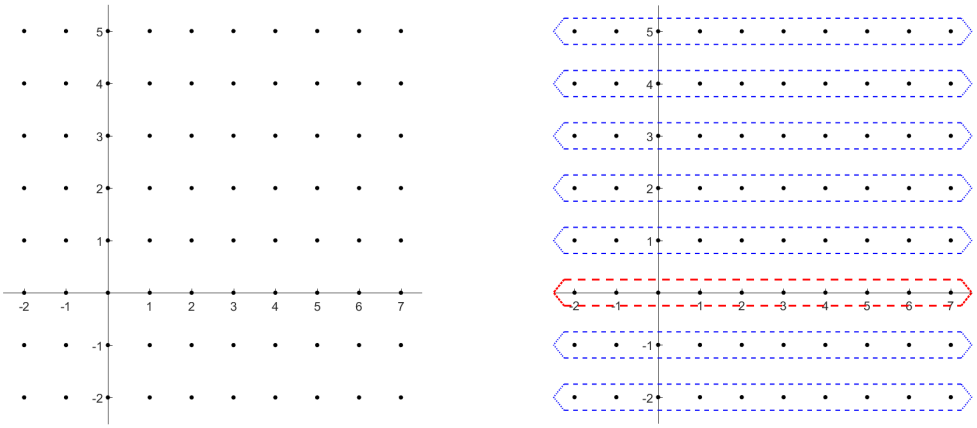
   (Tässä on tekijäryhmää merkitty selvyyden vuoksi vaakaviivan avulla, niin kuin toisinaan tehdään). Lisäksi pätee

$$\bar{f}((a, b) + \mathbb{Z} \times \{0\}) = f(a, b) = b$$

   kaikilla $(a, b) + \mathbb{Z} \times \{0\} \in (\mathbb{Z} \times \mathbb{Z})/(\mathbb{Z} \times \{0\})$.

8. Piirrä ensin kuva ryhmästä $\mathbb{Z} \times \mathbb{Z}$ ja sitten ryhmästä $(\mathbb{Z} \times \mathbb{Z})/(\mathbb{Z} \times \{0\})$. Kuinka jälkimmäisestä kuvasta näkyy, että ryhmät $(\mathbb{Z} \times \mathbb{Z})/(\mathbb{Z} \times \{0\})$ ja $\mathbb{Z}$ ovat isomorfisia?

   Ratkaisuehdotus:



   Vasemmalla on esitetty $\mathbb{Z} \times \mathbb{Z}$, joka koostuu siis kokonaislukupistepareista. Oikealla on merkitty tekijäryhmän $(\mathbb{Z} \times \mathbb{Z})/(\mathbb{Z} \times \{0\})$ sivuluokat. Näitä miettiessä lienee helpointa lähteä liikkeelle itse aliryhmästä $\mathbb{Z} \times \{0\}$, joka on yksi sivuluokista. Se on merkitty kuvaan punaisella. Tämän jälkeen voi miettiä esimerkiksi, millainen joukko on sivuluokka $(1, 1) + \mathbb{Z} \times \{0\}$.

   Tekijäryhmän $(\mathbb{Z} \times \mathbb{Z})/(\mathbb{Z} \times \{0\})$ isomorfisuus $\mathbb{Z}$:n kanssa näkyy siinä, että kuvassa jokaista pystyakselin kokonaislukua vastaa tasan yksi sivuluokka. Pystyakselilla olevat kokonaisluvut ja tekijäryhmän alkiot vastaavat siis yksi yhteen toisiaan.

9.* Olkoon $f\colon G \to H$ ryhmähomomorfismi. Tutkitaan ytimen $\operatorname{Ker} f$ sivuluokkia. Osoita, että samassa sivuluokissa olevilla alkioilla on sama kuva-alkio kuvauksessa f.

Tehtäväsarja III

10. Anna esimerkki kahdesta renkaan $\mathbb{Z}_3[X]$ eri polynomista, joita vastaava polynomikuvaus on vakiokuvaus

$$f\colon \mathbb{Z}_3 \to \mathbb{Z}_3, \quad f(x) = 1$$

    Vinkki: Varo, ettet vahingossa anna samaa polynomia kahdella eri tavalla kirjoitettuna! Toisen polynomin asteeksi kannattaa valita kolme.

    Ratkaisuehdotus: Valitaan polynomit $P = 1$ ja $Q = X^3 + 2X + 1$.

    Olkoon $f_P\colon \mathbb{Z}_3 \to \mathbb{Z}_3$ polynomia P vastaava polynomikuvaus ja $f_Q\colon \mathbb{Z}_3 \to \mathbb{Z}_3$ polynomia Q vastaava polynomikuvaus.

    Selvästikin $f_P(c) = 1$ kaikilla $c \in \mathbb{Z}_3$. Lasketaan myös f_Q:n arvot:

    - $c = [0]_3$: $f_Q(c) = [0]_3^3 + 2 \cdot [0]_3 + [1]_3 = [1]_3 = 1$
    - $c = [1]_3$: $f_Q(c) = [1]_3^3 + 2 \cdot [1]_3 + [1]_3 = [1]_3 + [2]_3 + [1]_3 = [1]_3 = 1$

- $c = [2]_3$: $f_Q(c) = [2]_3^3 + 2 \cdot [2]_3 + [1]_3 = [8]_3 + [4]_3 + [1]_3 = [2]_3 + [1]_3 + [1]_3 = [1]_3 = 1$

Koska kuvaukset f_P ja f_Q saavat samat arvot kaikilla lähtöjoukon alkioilla, ovat ne samat.

11. Onko renkaan $\mathbb{Z}_3[X]$ polynomi $X^3 + 2X + 2$ jaoton?

Ratkaisuehdotus: Polynomi on jaoton. Sillä ei ole juuria, mutta tämä ei vielä todista väitettä.

Tehdään vastaoletus, että polynomi voitaisiin kirjoittaa kahden positiivista astetta olevan polynomin P ja Q tulona. Koska $\mathbb{Z}_3$ on kokonaisalue, niin lauseen 21.6 nojalla $\deg(PQ) = \deg(P) + \deg(Q)$. Toisaalta $\deg(PQ) = \deg(X^3 + 2X + 2) = 3$, joten toisen polynomeista P ja Q on oltava astetta 1. Olkoon se P, toisin sanoen $P = aX + b$ joillain $a, b \in \mathbb{Z}_3$, $a \neq 0$. Koska $a \neq 0$ ja $\mathbb{Z}_3$ on kunta, niin P:llä on juuri $-a^{-1}b$ (ensimmäisen asteen polynomilla on aina juuri). Mutta nyt lemman 22.8 nojalla

$$(PQ)(-a^{-1}b) = P(-a^{-1}b) \cdot Q(-a^{-1}b) = 0 \cdot Q(-a^{-1}b) = 0,$$

joten tämä on myös alkuperäisen polynomin juuri. Sillä ei kuitenkaan ole juuria, joten syntyy ristiriita.

12.* Onko polynomirenkaan $\mathbb{Z}_5[X]$ alkio $3X^2 - 1$ yksikkö?

Tehtäväsarja IV

13. Tutkitaan ryhmää $\mathbb{Z}_8$ ja sen aliryhmää $I = \langle [4]_8 \rangle$. Tekijäryhmässä $\mathbb{Z}_8/I$ voidaan määritellä kertolasku kaavalla

$$(a + I) \cdot (b + I) = ab + I.$$

Tällöin joukko $\mathbb{Z}_8/I$ on rengas.

(a) Määritä renkaan $\mathbb{Z}_8/I$ yhteenlasku- sekä kertotaulu.
(b) Mikä on renkaan nolla-alkio? Entä ykkösalkio?
(c) Onko alkiolla $[2]_8 + I$ käänteisalkiota?

Ratkaisuehdotus:

(a) Selvitetään ensin, mitkä ovat I:n alkiot.Koska $2 \cdot [4]_8 = [0]_8$, niin lemman 8.6 mukaan $I = \{[0]_8, 1 \cdot [4]_8\} = \{[0]_8, [4]_8\}$.
Määritetään sitten sivuluokat. Lagrangen lauseen nojalla nähdään, että sivuluokkien lukumäärä on: $|\mathbb{Z}_8|/|I| = 8/2 = 4$. Sivuluokiksi saadaan:

$$\begin{aligned} I &= \{[0]_8, [4]_8\} \\ [1]_8 + I &= \{[1]_8, [5]_8\} \\ [2]_8 + I &= \{[2]_8, [6]_8\} \\ [3]_8 + I &= \{[3]_8, [7]_8\}. \end{aligned}$$

Koska löydettiin neljä eri sivuluokkaa, on kaikki sivuluokat löydetty.

Muodostetaan nyt joukon $\mathbb{Z}_8/I$ laskutoimitustaulut.

$+$	I	$[1]_8+I$	$[2]_8+I$	$[3]_8+I$
I	I	$[1]_8+I$	$[2]_8+I$	$[3]_8+I$
$[1]_8+I$	$[1]_8+I$	$[2]_8+I$	$[3]_8+I$	I
$[2]_8+I$	$[2]_8+I$	$[3]_8+I$	I	$[1]_8+I$
$[3]_8+I$	$[3]_8+I$	I	$[1]_8+I$	$[2]_8+I$

$\cdot$	I	$[1]_8+I$	$[2]_8+I$	$[3]_8+I$
I	I	I	I	I
$[1]_8+I$	I	$[1]_8+I$	$[2]_8+I$	$[3]_8+I$
$[2]_8+I$	I	$[2]_8+I$	I	$[2]_8+I$
$[3]_8+I$	I	$[3]_8+I$	$[2]_8+I$	$[1]_8+I$

Huomaa, että taulukoissa on lemmaa 11.6 hyödyntäen sievennetty sivuluokkia. Esimerkiksi $([2]_8+I)\cdot([3]_8+I)=[6]_8+I=[2]_8+I$, koska $[6]_8\in[2]_8+I$.

(b) Yhteenlaskutaulun perusteella nähdään, että renkaan $\mathbb{Z}_8/I$ nolla-alkio on I. Samoin kertotaulusta nähdään, että ykkösalkiona toimii sivuluokka $[1]_8+I$.

(c) Kertotaulun perusteella ei ole sellaista renkaan $\mathbb{Z}_8/I$ alkiota $c+I$, että pätisi $([2]_8+I)(c+I)=[1]_8+I$. Näin ollen alkiolla $[2]_8+I$ ei ole käänteisalkiota renkaassa $\mathbb{Z}_8/I$.

14. Jatkoa edelliseen tehtävään. Onko rengas $\mathbb{Z}_8/I$ kokonaisalue?

Ratkaisuehdotus: Rengas $\mathbb{Z}_8/I$ ei ole kokonaisalue, sillä $([2]_8+I)\cdot([2]_8+I)=[0]_8+I=I$, vaikka $[2]_8+I\neq I$. Renkaasta $\mathbb{Z}_8/I$ löytyy siis nollanjakaja, joten se ei ole kokonaisalue.

15. Osoita, että $I=\langle[4]_8\rangle$ on renkaan $\mathbb{Z}_8$ ideaali. Miten tämä liittyy siihen, että sivuluokkien joukossa voidaan määritellä kertolasku?

Ratkaisuehdotus: Jotta I olisi ideaali, parin $(I,+)$ tulisi olla parin $(\mathbb{Z}_8,+)$ aliryhmä sekä kaikilla $r\in\mathbb{Z}_8, a\in I$ tulisi päteä $ra\in I$ ja $ar\in I$. Edellisen tehtävän nojalla $I=\{[0]_8,[4]_8\}$.

Ensiksi nähdään suoraan, että $(I,+)$ on $(\mathbb{Z}_8,+)$:n aliryhmä, sillä I on alkion $[4]_8$ virittämä aliryhmä.

Tarkastetaan nyt ideaalin määritelmän toinen ehto. Oletetaan, että $r\in\mathbb{Z}_8$ ja $s\in I$. Havaitaan, että rengas $\mathbb{Z}_8$ on vaihdannainen, joten riittää tarkastaa, että $rs\in I$. Nyt $r=[a]_8, s=[b]_8$, joillakin $a\in\{0,1,2,3,4,5,6,7\}\subset\mathbb{Z}$ ja $b\in\{0,4\}\subset\mathbb{Z}$. Saadaan $rs=[a]_8\cdot[b]_8=[ab]_8$. Nyt jos $b=0$, niin $rs=[0]_8$, ja jos $b=4$, niin $rs=[0]_8$ tai $rs=[4]_8$. (Tämä nähdään käymällä läpi eri vaihtoehdot alkiolle a.) Erityisesti $rs\in I$. Näin saatiin siis, että ehdot täyttyvät ja näin ollen $I=\langle[4]_8\rangle$ on renkaan $\mathbb{Z}_8$ ideaali.

Ideaali vastaa renkaiden tapauksessa käsitteenä vastaanlaista rakennetta kuin normaali aliryhmä ryhmien tapauksessa. Kuten ryhmillä voitiin sivuluokkien joukossa määritellä yhteenlasku aliryhmän ollessa normaali, niin myös renkailla voidaan sivuluokkien joukossa määritellä kertolasku aliryhmän ollessa ideaali.

Ylimääräisiä tehtäviä

16. Laadi käsitekartta kurssilla käsitellyistä asioista. Selitä kartassasi käsitteiden väliset yhteydet. Merkitse karttaan jollakin tavalla kaikkein keskeisimmät käsitteet.

17. Oletetaan, että $G = \langle g \rangle$ on äärellinen syklinen ryhmä, jossa on n alkiota. Osoita ryhmien homomorfialauseen avulla, että $\mathbb{Z}_n \cong G$.

    Ratkaisuehdotus: Esimerkin 11.2 nojalla $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. Homomorfialausetta varten tarvitaan siis surjektiivinen homomorfismi $f\colon \mathbb{Z} \to G$, jonka ydin on $n\mathbb{Z}$. Määritellään f asettamalla

    $$f(k) = g^k \quad \text{kaikilla } k \in \mathbb{Z}.$$

    Jos $k, l \in \mathbb{Z}$, niin

    $$f(k+l) = g^{k+l} = g^k g^l = f(k)f(l),$$

    joten f on homomorfismi.

    "$n\mathbb{Z} \subset \operatorname{Ker} f$": Olkoon $nk \in n\mathbb{Z}$. Lauseen 8.8 nojalla $g^n = e$, joten saadaan $f(nk) = g^{nk} = (g^n)^k = e^k = e$ eli $nk \in \operatorname{Ker} f$.

    "$n\mathbb{Z} \supset \operatorname{Ker} f$": Olkoon $k \in \operatorname{Ker} f$ eli $f(k) = g^k = e$. Lemman 8.11 nojalla alkion g kertaluku n jakaa luvun k. Siten $k \in n\mathbb{Z}$.

    Siispä $\operatorname{Ker} f = n\mathbb{Z}$ ja lisäksi huomataan, että $\operatorname{Im} f = G$ (lause 6.2). Homomorfialauseen nojalla on siis olemassa isomorfismi

    $$\bar{f}\colon \mathbb{Z}_n \to G.$$

18. Oletetaan, että G on ryhmä. Tutkitaan ryhmää S_G, joka koostuu kaikista ryhmän G alkioiden permutaatiosta.

    (a) Oletetaan, että $g \in G$. Osoita, että kuvaus $f_g\colon G \to G$, $f_g(x) = gx$ on bijektio. Toisin sanoen $f_g \in S_G$.
    (b) Edellisen kohdan nojalla voidaan määritellä kuvaus $\varphi\colon G \to S_G$ kaavalla $\varphi(g) = f_g$. Osoita, että φ on ryhmähomomorfismi.
    (c) Osoita, että φ on injektio. Päättele tämän avulla, että ryhmällä S_G on aliryhmä, joka on isomorfinen ryhmän G kanssa.

    Ratkaisuehdotus:

    (a) Jos $x, y \in G$ ovat sellaiset, että $f_g(x) = f_g(y)$, niin $gx = gy$, joten $x = y$. Siis f_g on injektio. Toisaalta jos $y \in G$, niin $g^{-1}y \in G$ ja $f_g(g^{-1}y) = gg^{-1}y = y$, joten f_g on myös surjektio. Siis f_g on bijektio.

    Vaihtoehtoisesti voisi osoittaa, että kuvauksen f_g käänteiskuvaus on $f_{g^{-1}}$.

    (b) Olkoot $g, h \in G$. On osoitettava, että $\varphi(gh) = \varphi(g)\varphi(h)$ eli että $f_{gh} = f_g \circ f_h$. Olkoon siis $x \in G$. Nyt

    $$(f_g \circ f_h)(x) = f_g(f_h(x)) = f_g(hx) = g(hx) = (gh)x = f_{gh}(x),$$

    mistä väite seuraa.

(c) Olkoon $g \in G$ sellainen, että $\varphi(g) = e_{S_G}$. Koska $e_{S_G} = \mathrm{id}_G$, niin nyt $f_g = \mathrm{id}_G$. Siis $gx = x$ kaikilla $x \in G$. Erityisesti $ge_G = e_G$, joten $g = e_G$. Siispä homomorfismin φ ydin on triviaali, ja lauseen 19.12 nojalla φ on injektio.

Kuvaus φ ei välttämättä ole surjektio, mutta siitä saadaan surjektio maalijoukkoa pienentämällä: kuvaus

$$\hat{\varphi}\colon G \to \operatorname{Im}\varphi, \quad \hat{\varphi}(g) = \varphi(g)$$

on surjektio. Se on siis bijektio ja edelleen ryhmäisomorfismi.

Lauseen 18.7 nojalla $\operatorname{Im}\varphi \leq S_G$ on aliryhmä. Nyt on siis osoitettu, että

$$G \cong \operatorname{Im}\varphi \leq S_G.$$

Tämä todistaa väitteen.

Kohdat a) ja b) voi myös tehdä toisessa järjestyksessä. Ensin siis osoitetaan, että jos $g, h \in G$, niin $f_{gh} = f_g \circ f_h$. Lisäksi huomataan, että $f_e(x) = ex = x$ kaikilla $x \in G$, joten $f_e = \mathrm{id}_G$. Tästä saadaan

$$\begin{aligned} f_g \circ f_{g^{-1}} &= f_{gg^{-1}} = f_e = \mathrm{id}_G \quad \text{ja} \\ f_{g^{-1}} \circ f_g &= f_{g^{-1}g} = f_e = \mathrm{id}_G, \end{aligned}$$

joten f_g on bijektio. Nyt φ voidaan määritellä ja se on jo osoitettu homomorfismiksi, joten voidaan siirtyä kohtaan c).