Matematiikan ja tilastotieteen laitos
Algebra I
Ratkaisuehdoituksia harjoituksiin 8, 23.–27.3.2009
5 sivua
ℝami Luisto

1. Osoita, että kullakin $n \in \mathbb{N}_+$ lukujen n^5 ja n viimeiset numerot kymmenkantaisessa järjestelmässä ovat samat. *Ohje.* Avuksi Fermat.

Todistus: Tehtävän väite on yhtäpitävää sen kanssa, että $n^5 - n$ on jaollinen kymmenellä kaikilla $n \in \mathbb{N}_+$.

Fermat'n pieni lause sanoo meille, että kaikilla kokonaisluvuilla a ja alkuluvuilla p pätee, että $a^p \equiv a \pmod{p}$. Täten siis erityisesti tehtävän tilanteessa mielivaltaiselle $n \in \mathbb{N}_+$ pätee, että $n^5 \equiv n \pmod{5}$, joten luku $n^5 - n$ on siis jaollinen viidellä.

Seuraavaksi huomataan, että

$$\begin{aligned} n^5 - n &= n(n^4 - 1) = n(n^2 - 1)(n^2 + 1) \\ &= \underbrace{n(n-1)}_{\text{Aina parillinen}} (n+1)(n^2 - 1), \end{aligned}$$

joten $n^5 - n$ on parillinen kaikilla $n \in N_+$.

Luku $n^5 - n$ on siis aina jaollinen sekä kahdella että viidellä, joten se on erityisesti jaollinen kymmenellä. Täten väite pätee.

2. Olkoon G (multiplikatiivinen) ryhmä, $H \leq G$ aliryhmä ja $N \trianglelefteq G$ normaali aliryhmä. Osoita, että joukko

$$HN = \{hn \mid h \in H,\, n \in N\}$$

on G:n aliryhmä.

Todistus: Todistetaan väite aliryhmän ehto kerrallaan. Selvästi $HN \subset G$, sillä ryhmä G on vakaa laskutoimituksensa suhteen.
(i): Väite: $1_G \in HN$. Koska H ja N ovat ryhmän G aliryhmiä, niin $1_G \in H$ ja $1_G \in N$, joten $1_G = 1_G 1_G \in HN$.
(ii): Väite: Jos $a, b \in HN$, niin $ab \in HN$. Olkoot siis $a, b \in HN$, eli $a = hn$ ja $b = km$, missä $h, k \in H$ ja $n, m \in N$. Nyt koska oletimme, että N on ryhmän G normaali aliryhmä, niin $Nk = kN$, eli erityisesti $nk = kn'$ jollakin $n' \in N$. Täten

$$ab = (hn)(km) = h(nk)m = h(kn')m = (hk)(n'm) \in HN,$$

sillä $hk \in H$ ja $n'm \in N$, koska aliryhmät H ja N ovat vakaita laskutoimituksen suhteen.
(iii): Väite: Jos $a \in HN$, niin $a^{-1} \in HN$. Huomataan, että jos $a = hn \in HN$, jossa $h \in H$ ja $n \in N$, niin myös $h^{-1} \in H$ ja $n^{-1} \in N$, sillä H ja N ovat ryhmän G aliryhmiä. Nyt

$$a^{-1} = (hn)^{-1} = n^{-1}h^{-1} \in Nh^{-1} = h^{-1}N \subset HN,$$

sillä N oli normaali. Täten siis $a^{-1} \in HN$, kuten haluttiin.

Joukko HN on siis ryhmän G aliryhmä.

3. Osoita, että (multiplikatiivisen) ryhmän G *keskus*

$$Z(G) = \{a \in G \mid ax = xa \text{ kaikilla } x \in G\}$$

on G:n normaali aliryhmä ja että G:n sisäisten automorfismien ryhmä on isomorfinen tekijäryhmän $G/Z(G)$ kanssa.

Huomautus: Ryhmän G sisäisten automorfismien ryhmä, merkitään $\mathrm{Inn}(G)$, on kuvausjoukko

$$\left\{c_g \colon G \to G \mid c_g(x) = gxg^{-1} \text{ kaikilla } x \in G, \text{ kiinteällä } g \in G\right\}.$$

Olemme todistaneet harjoituksien 7 tehtävässä 6, että jokainen muotoa c_g oleva kuvaus on automorfismi, joten $\mathrm{Inn}(G) \subset \mathrm{Aut}(G)$. Harjoituksen tuloksista seuraa peräti, että $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$.

Todistus: Todistetaan väite osissa.
(i): Väite: $Z(G)$ on ryhmän G aliryhmä. Todistetaan aliryhmän ehto kerrallaan.

Koska neutraalialkio kommutoi jokaisen ryhmän alkion kanssa, eli $1_G a = a 1_G = a$ kaikilla $a \in G$, niin $1_G \in Z(G)$. Jos taas $a, b \in Z(G)$ ja $x \in G$ on mielivaltainen, niin koska määritelmän mukaan alkiot a ja b kommutoivat kaikkien ryhmän G alkioiden kanssa, niin $abx = axb = xab$, eli myöskin $ab \in Z(G)$. Nyt jos $a \in Z(G)$, niin tällöin $a^{-1}x = a^{-1}xaa^{-1} = a^{-1}axa^{-1} = xa^{-1}$, eli $a^{-1} \in Z(G)$.

(ii): Väite: $Z(G)$ on normaali aliryhmä, eli $kZ(G) = Z(G)k$ kaikilla $k \in G$. Olkoon $x \in kZ(G)$, eli $x = ka$ jollakin $a \in Z(G)$. Koska keskuksen määritelmän mukaan a tällöin kommutoi kaikkien ryhmän G alkioiden kanssa, niin erityisesti se kommutoi alkion k kanssa. Toisin sanoen $x = ka = ak$, eli $x \in Z(G)k$. Täten $kZ(G) \subset Z(G)k$, ja väite saadaan identtisellä päättelyllä toiseen suuntaan, joten $kZ(G) = Z(G)k$.

(iii): Väite: $G/Z(G) \cong \mathrm{Inn}(G)$.

Harjoitusten 7 tehtävässä 6 olemme todistaneet, että kuvaus $g \overset{h}{\mapsto} c_g$ on homomorfismi ryhmien G ja $\mathrm{Aut}(G)$ välillä. Tarkastelmalla kuvauksen h määrittelyä sekä joukon $\mathrm{Inn}(G)$ määritelmää huomaamme, että $\mathrm{Im}(h) = \mathrm{Inn}(G)$. Ryhmien homomorfialause kertoo meille, että nyt ryhmä $G/\operatorname{Ker}(h)$ on isomorfinen kuvauksen h kuvan, eli sisäisten automorfismien ryhmän kanssa. Riittää siis osoittaa, että $\operatorname{Ker}(h) = Z(G)$.

Olkoon siis $g \in Z(G)$. (Keskus on aina epätyhjä sillä neutraalialkio kommutoi kaikkien ryhmän alkioiden kanssa.) Saamme seuraavan päättelyketjun:

$$\begin{aligned} & g \in Z(G) \Leftrightarrow gx = xg \text{ kaikilla } x \in G \\ & \overset{(1)}{\Leftrightarrow} gxg^{-1} = x \text{ kaikilla } x \in G \Leftrightarrow c_g(x) = x \text{ kaikilla } x \in G \\ & \Leftrightarrow c_g = id \Leftrightarrow g \in \operatorname{Ker}(h). \end{aligned}$$

(1): Kerrotaan yhtälö puolittain oikealta alkiolla g^{-1} (tai alkiolla g liikuttaessa päättelyketjua toiseen suuntaan).

Olemme siis näyttäneet, että $\mathrm{Ker}(h) = Z(G)$, kuten haluttiin. Täten $G/\mathrm{Ker}(h) \cong \mathrm{Inn}(G)$.

Huomautus: Kohdan (iii) todistus antaisi meille toisen tavan osoittaa, että ryhmän keskus on aina normaali aliryhmä, sillä kurssin lauseiden mukaan homomorfismin ydin on aina ryhmän normaali aliryhmä.

4. Etsi ryhmän S_3 kaikki aliryhmät. Mitkä aliryhmistä ovat normaaleja? *Ohje ensimmäiseen kohtaan.* Jos $\{\mathrm{id}\} < H < S_3$, niin Lagrangen lauseen nojalla on $|H| = 2$ tai 3, joten H on syklinen.

Todistus: Symmetrinen ryhmä S_3 vastaa tasasivuisen kolmion symmetriaryhmää. Ryhmä on siis

$$S_3 = \{\underbrace{\mathrm{id}, (123), (132)}_{\text{Kierrot}}, \underbrace{(12), (13) \text{ sekä } (23)}_{\text{Peilaukset}}\}.$$

Ryhmässä S_3 on siis kuusi alkiota. Noudattamalla tehtävänannon ohjetta muistamme, että Lagrangen lauseen mukaan aliryhmän kertaluku jakaa ryhmän kertaluvun. Mahdollisten aliryhmien kertaluvut ovat siis 1, 6, 2 tai 3. Näistä kaksi ensimmäistä vastaavat triviaaleja aliryhmiä, joista tiedämme, että koko ryhmä on itsensä normaali aliryhmä, sillä ryhmä on vakaa laskutoimituksen suhteen ja että yhden alkion aliryhmä on aina normaali, sillä neutraalialkio kommutoi kaikkien ryhmän alkioiden kanssa. Jälkimmäiset luvut edustavat mahdollisten epätriviaalien aliryhmien kertalukuja.

Noudattamalla jälleen tehtävänannon ohjetta huomaamme, että kertalukua kaksi tai kolme olevat ryhmät ovat aina syklisiä, joten kaikki epätriviaalit aliryhmät löytyvät, kun tarkastelemme ryhmän eri alkioiden virittämiä aliryhmiä.

(i) Peilaukset: Jokainen peilaus virittää kahden alkion aliryhmän, koska jokainen peilaus on itsensä käänteisalkio. Saamme peilausten avulla siis aikaan aliryhmät

$$\langle(12)\rangle = \{\mathrm{id}, (12)\}, \langle(23)\rangle = \{\mathrm{id}, (23)\}, \langle(13)\rangle = \{\mathrm{id}, (13)\}.$$

Näistä ei yksikään ole normaali aliryhmä, sillä jotta kahden alkion ryhmä olisi normaali aliryhmä, pitäisi sen neutraalialkiosta poikkeavan alkion kommutoida kaikkien ryhmän alkioiden kanssa. Yksikään peilaus ei kuitenkaan kommutoi kummankaan epätriviaalin kierron kanssa, joten ryhmistä yksikään ei ole normaali.

(ii) Kierrot: Identtinen kuvaus virittää tietenkin triviaalin aliryhmän, mutta kaksi muuta kiertoa virittävät saman kolmen alkion aliryhmän:

$$\langle(\mathrm{id})\rangle = \{\mathrm{id}\}, \langle(123)\rangle = \langle(132)\rangle = \{\mathrm{id}, (123), (132)\}.$$

Triviaali yhden alkion ryhmä on normaali, kuten aikaisemmin totesimme. Myös toinen kolmen alkion aliryhmä on normaali, sillä kierrot

kommutoivat keskenään, ja peilaus yhdistettynä kiertoon vastaa 'käänteiskiertoa' yhdistettynä samaan peilaukseen.

Luentojen huomioiden avulla epätriviaalin kierron virittämän kolmen alkion aliryhmän K näkisi normaaliksi myös siitä, että sen indeksi on 2, ($|S_3 \colon K| = 6/3 = 2$) sillä tällöin välttämättä vasemmat K-sivuluokat yhtyvät pareittain oikeiden K-sivuluokkien kanssa.

5. Olkoon G (multiplikatiivinen) Abelin ryhmä, $|G| = 6$, $a \in G$ ja $\mathrm{ord}(a) = 3$. Osoita, että G on syklinen ryhmä. *Ohje.* Huomaa, että $G/\langle a\rangle \cong \mathbb{Z}_2$.

Todistus: Noudatetaan ohjetta ja huomataan, että Lagrangen lauseen mukaan (normaalin) aliryhmän $\langle a\rangle$ sivuluokkien lukumäärä on

$$|G|/|\langle a\rangle| = 6/3 = 2,$$

eli tekijäryhmän $G/\langle a\rangle$ kertaluku on 2. Kahden alkion ryhmiä on olemassa isomorfiaa vaille täsmälleen yksi, joten $G/\langle a\rangle \cong \mathbb{Z}_2$.

Valitaan nyt alkio b alkion a virittämän kolmialkioisen ryhmän komplementista, eli olkoon $b \in G\backslash\langle a\rangle$. Nyt koska alkio b valittiin alkion a virittämän ryhmän komplementista, niin $bH \neq H$. Kuitenkin, koska totesimme että tekijäryhmä on isomorfinen ryhmän $\mathbb{Z}_2$ kanssa, on oltava $bH \cdot bH = b^2H = H$. Erityisesti siis $b^2 \in H = \{1_G, a, a^2\}$. Etsitään virittäjä kussakin tapauksessa.

Tätä ennen kumminkin huomataan, että alkiot $\{1_G, a, a^2, b, ab, a^2b\}$ ovat kaikki keskenään eri. Tämä huomataan siitä, että alkion a kertaluku on tasan kolme, ja siitä, että b valittiin alkion a virittämän aliryhmän komplementista, eli erityisesti se ei ole neutraalialkio, a tai a^2.

(i): Tapaus $b^2 = 1$. Nyt

$$\langle ab\rangle = \{ab, (ab)^2, (ab)^3, (ab)^4, (ab)^5, (ab)^6\} = \{ab, a^2, b, a, a^2b, 1\},$$

eli alkion ab kertaluku on 6 ja se virittää koko ryhmän.

(ii): Tapaus $b^2 = a$. Nyt

$$\langle b\rangle = \{b, (b)^2, (b)^3, (b)^4, (b)^5, (b)^6\} = \{b, a, ab, a^2, a^2b, 1_G\},$$

eli alkion b kertaluku on 6 ja se virittää koko ryhmän.

(iii): Tapaus $b^2 = a^2$. Nyt

$$\langle b\rangle = \{b, (b)^2, (b)^3, (b)^4, (b)^5, (b)^6\} = \{b, a^2, a^2b, a, ab, 1_G\},$$

eli alkion b kertaluku on 6 ja se virittää koko ryhmän.

Olemme käyneet läpi kaikki mahdolliset tapaukset, ja huomaamme että ryhmä G on välttämättä syklinen.

6. Osoita, että additiiviset ryhmät $\mathbb{Z}_2 \times \mathbb{Z}_4$ ja $\mathbb{Q}$ eivät ole syklisiä.

Todistus: Tutkitaan ryhmiä erikseen.

(i): Ryhmä $(\mathbb{Z}_2 \times \mathbb{Z}_4, +)$.

Olkoon nyt $(a,b) \in \mathbb{Z}_2 \times \mathbb{Z}_4$. Jos $a = \overline{0}$, niin

$$\langle (a,b) \rangle \leq \{\overline{0}\} \times \mathbb{Z}_4 \neq \mathbb{Z}_2 \times \mathbb{Z}_4.$$

Olkoon siis $a \neq \overline{0}$, eli $a = \overline{1}$.

Huomataan, että

$$\begin{aligned}
\langle (\overline{1},\overline{0}) \rangle &= \mathbb{Z}_2 \times \{\overline{0}\} \neq \mathbb{Z}_2 \times \mathbb{Z}_4 \\
\langle (\overline{1},\overline{1}) \rangle &= \{(\overline{1},\overline{1}), (\overline{0},\overline{2}), (\overline{1},\overline{3}), (\overline{0},\overline{0})\} \neq \mathbb{Z}_2 \times \mathbb{Z}_4 \\
\langle (\overline{1},\overline{2}) \rangle &= \{(\overline{1},\overline{2}), (\overline{0},\overline{0})\} \neq \mathbb{Z}_2 \times \mathbb{Z}_4 \\
\langle (\overline{1},\overline{3}) \rangle &= \{(\overline{1},\overline{3}), (\overline{0},\overline{2}), (\overline{1},\overline{1}), (\overline{0},\overline{0})\} \neq \mathbb{Z}_2 \times \mathbb{Z}_4,
\end{aligned}$$

joten yksikään ryhmän alkio ei viritä koko ryhmää, joten $\mathbb{Z}_2 \times \mathbb{Z}_4$ ei ole syklinen ryhmä. (Tehtävässä voisi tarkistaa myös kaikkien alkioiden (a,b) kertaluvut, joista yksikään ei ole kahdeksan.)

HUOMAUTUS: Voidaan peräti todistaa, että additiivinen ryhmä

$$\mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_n}$$

on syklinen täsmälleen silloin kun luvut $p_1, \ldots, p_n$ ovat keskenään jaottomia.

(ii): Ryhmä $(\mathbb{Q}, +)$.

Olkoon $q \in \mathbb{Q}$. Väite: $\mathbb{Q} \neq \langle q \rangle$.

Jos $q = 0$, niin väite on selvä, sillä $\langle 0 \rangle = \{0\}$. Jos taas $q \neq 0$, niin väitänkin, että $\frac{1}{2}q \notin \langle q \rangle$. Nimittäin nyt jos merkitsemme $q = a/b$, missä $a, b \neq 0$, niin jotta $\frac{1}{2}q \in \langle q \rangle$, pitäisi jollakin kertoimella $n \in \mathbb{Z}$ päteä, että

$$\frac{a}{2b} = \frac{na}{b},$$

josta ristiinkertomalla saamme yhtäpitävästi $ab = 2nab$, eli $1 = 2n$, sillä oletimme, että $a, b \neq 0$. Pitäisi siis olla $n = 1/2 \in \mathbb{Z}$, joka tuottaa ristiriidan.