Insinöörimatematiikka: Diskreetti matematiikka

Älä käytä demotehtävissä tekoälyä, vaan omaasi

Demonstraatio 3, 12.3.2026

1. Millaisen aliryhmän alkio $(13) \in S_3$ generoi? onko se normaali aliryhmä? Ohje: Selvitä normaalius tarkistamalla onko $gH = Hg$ aina, kun $g \in S_3$. Käytä edellisen demokerran kertolaskutaulua

   Mallivastaus: Koska $(13)(13) = (1)$, on alkion (13) generoima aliryhmä kahden alkion syklinen ryhmä $H = \{(1), (13)\}$. Koska esim. $(12)H = \{(12), (132)\}$, mutta $H(12) = \{(12), (123)\}$, ei aliryhmä H ole normaali

2. Olkoon $H = \langle(13)\rangle$ edellisen tehtävän aliryhmä. Selvitä montako sivuluokkaa aliryhmällä H on.

   Mallivastaus: Lagrangen lauseen mukaan sivuluokkia on $|S_3| \,/\, |H| = 6/2 = 3$.

3. Olkoon H kuten edellä. Määritellään ryhmässä S_3 relaatio $a \equiv b$ ehdolla $a^{-1}b \in H$. Onko tämä relaatio ekvivalenssirelaatio? Entä kongruenssi?

   Mallivastaus: Luennolla todetun mukaan tämä relaatio on ekvivalenssi, vaikka aliryhmä ei olekaan normaali. Toisaalta $(132) \equiv (12)$, koska $(132)^{-1}(12) = (123)(12) = (13) \in H$, ja $(123) \equiv (23)$, koska $(123)^{-1}(23) = (132)(23) = (13) \in H$, mutta $(132)(123) = (1)$, kun taas $(12)(23) = (123) \neq (1)$. Relaatio ei siksi ole kongruenssi.

4. Olkoon H kuten aiemmin. Esitä esimerkki tilanteesta (mikäli sellainen on olemassa), jossa sivuluokkien aH ja bH tulo ei ole riippumaton edustajan valinnasta.

   Mallivastaus: Esimerkki saadaan suoraan edellisestä tehtävästä: $(132)H = (12)H$ ja $(123)H = (23)H$, mutta $(132)H \cdot (123)H = (132)(123)H = (1)H = H$, kun taas $(12)H \cdot (23)H = (12)(23)H = (123)H \neq H$.

5. Osoita, että permutaatioryhmän S_3 aliryhmä $A_3 = \{(1), (123), (132)\}$ on normaali. Ohje: Käytä edellisen demokerran kertolaskutaulua.

   Mallivastaus: Jokaiselle $g \in A_3$ on triviaalisti $gA_3 = A_3g = A_3$, joten tarkastellaan sivuluokkia $(12)A_3 = \{(12), (23), (13)\} = A_3(12)$, $(13)A_3 = \{(13), (12), (23)\} = A_3(13)$ ja $(23)A_3 = \{(23), (13), (12) = A_3(23)\}$, joten aliryhmä A_3 on normaali.

6. Millainen on tekijäryhmä S_3/A_3? Ohje: Selvitä aluksi Lagrangen lauseen avulla kuinka monta alkiota tekijäryhmässä on. Tekijäryhmän alkiot ovat sivuluokkia gA_3, missä $s \in S_3$. Näiden kertolasku määritellään $g_1A_3 \cdot g_2A_3 = g_1g_2A_3$. Jos $g \in A_3$, on $gA_3 = A_3$. Laske ainakin joitain tuloja $g_1A_3 \cdot g_2A_3$. Voit käyttää edellisen demokerran kertolaskutaulua.

   Mallivastaus: Lagrangen lauseen perusteella tekijäryhmässä on $|S_3| \,/\, |A_3| = 6/3 = 2$ alkiota, ja edellinen tehtävä vahvistaa tämän. Esimerkiksi $A_3 \cdot (12)A_3 = (12)A_3 = \{(12), (23), (13)\}$, $(12)A_3 \cdot (13)A_3 = (12)(13)A_3 = (132)A_3 = A_3$.

7. Totea, että $\overline{2} \in \mathbb{F}_{11}$ generoi kunnan $\mathbb{F}_{11}$ multiplikatiivisen ryhmän. Ohje: Totea, että kaikki kunnan $\mathbb{F}_{11}$ nollasta eroavat alkiot saadaan luokan $\overline{2}$ potensseina $\overline{2}^0$, $\overline{2}^1$, $\overline{2}^2$, jne.

   Mallivastaus: $\overline{2}^2 = \overline{4}$, $\overline{2}^3 = \overline{8}$, $\overline{2}^4 = \overline{16} = \overline{5}$, $\overline{2}^5 = \overline{5} \cdot \overline{2} = \overline{10}$, $\overline{2}^6 = \overline{2} \cdot \overline{10} = \overline{20} = \overline{9}$, $\overline{2}^7 = \overline{2} \cdot \overline{9} = \overline{18} = \overline{7}$, $\overline{2}^8 = \overline{2} \cdot \overline{7} = \overline{14} = \overline{3}$, ja $\overline{2}^9 = \overline{2} \cdot \overline{3} = \overline{6}$.

8. Olkoon γ syklisen ryhmän C generaattori. Kuinka monta ryhmäoperaatiota (ryhmän kertolaskua) riittää γ^{2026} laskemiseksi? Ohje: Käytä luennolla esiteltyä peräkkäisten neliöimisten menetelmää.

   Mallivastaus: $2026 = 2^{10} + 2^9 + 2^8 + 2^7 + 2^6 + 2^5 + 2^3 + 2^1$, joten

$$\gamma^{2026} = \gamma^{2^{10}} \cdot \gamma^{2^9} \cdot \gamma^{2^8} \cdot \gamma^{2^7} \cdot \gamma^{2^6} \cdot \gamma^{2^5} \cdot \gamma^{2^3} \cdot \gamma^{2}.$$

   Tässä tarvitaan 7 ryhmäoperaatiota, ja alkioiden $\gamma^2 = \gamma \cdot \gamma$, $\gamma^{2^2} = \gamma^2 \cdot \gamma^2$, $\gamma^{2^3} = \gamma 2^2 \cdot \gamma 2^2$, $\ldots$ $\gamma^{2^{10}} = \gamma^{2^9} \cdot \gamma^{2^9}$ laskemiseen tarvitaan lisäksi 10 ryhmäoperaatiota. Yhteismäärä on siis 17 operaatiota.

9. Selvitä onko polynomi $x^2 + x + 1 \in \mathbb{F}_2[x]$ jaoton. Ohje: Mieti mitä astetta tekijät voisivat olla ja mitä jaollisuus tarkoittaisi nollakohtien osalta.

   Mallivastaus: Polynomin epätriviaalit tekijät voivat olla vain ensimmäistä astetta. Tekijähajotelmasta $x^2 + x + 1 = (x + a)(x + b)$ kuitenkin seuraisi, että polynomilla olisi kunnassa $\mathbb{F}_2$ nollakohta $x = -a$. Mutta kunnassa $\mathbb{F}_2$ on $0^2 + 0 + 1 = 1$ ja $1^1 + 1 + 1 = 1$, joten polynomilla ei ole nollakohtia. Näin ollen sillä ei myöskään ole ensimmäisen asteen tekijöitä ja siksi se on jaoton kunnassa $\mathbb{F}_2$.