Algebrallinen lukuteoria: VI Binääriset neliömuodot

1. Esittääkö neliömuoto $f = 5x^2 - 7y^2$ nollaa rationaalilukujen kunnan yli?

2. Tarkastellaan neliömuotoa $(1, 0, 1)$. Esittääkö tämä muoto lukua 2? Jos, niin millä x, y:n arvoilla. Milloin muoto esittää alkulukua p?

3. Anna esimerkki kahdesta neliömuodosta, joilla on sama diskriminantti, mutta jotka eivät ole ekvivalentteja.

4. Osoita, että jos $f = (a, b, c)$ on surkastettu/redusoitu muoto ja sen diskriminantti on $-D$, silloin $|b| \leq \sqrt{D/3}$.

5. Osoita, että lukuunottamatta ekvivalensseja $(a, b, a) \sim (a, -b, a)$ ja $(a, a, c) \sim (a, -a, c)$ mitkään kaksi redusoitua muotoa eivät voi olla ekvivalentteja.

6. Päätä, mitkä seuraavista muodoista ovat ekvivalentteja
$$(6, 12, 7), \quad (3, 6, 5), \quad (5, 14, 11).$$

7. Osoita, että 2×2 matriisit, joiden determinantti on 1 renkaan $\mathbb{Z}$ yli muodostavat ryhmän. Merkitään tätä ryhmää $\mathrm{SL}_2(\mathbb{Z})$. Tässä tehtävässä tarkastelemme tätä lukuteoriassa tärkeää modulaariryhmää tarkemmin. Huomaa, että tämä ryhmä ei ole kommutatiivinen!

   Olkoon
$$S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$
   ja
$$T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$
   Laske kertaluvut alkioille T ja $P = T^3 S$. Etsi ja kirjoita todistus sille, että nämä kaksi alkiota vapaasti virittävät ryhmän $\mathrm{SL}_2(\mathbb{Z})$, eli osoita, että kaikki ryhmän $\mathrm{SL}_2(\mathbb{Z})$ alkiot
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$
   voidaan kirjoittaa alkioiden
$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

ja

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

eripituisina tuloina.

Sanotaan, että ryhmä G toimii joukossa S, jos on olemassa binäärifunktio $G \times S \longrightarrow S$, missä $(g, s) \mapsto g * s$ ja joka toteuttaa ehdot

(i) $1 * s = s$ kaikille $s \in S$

(ii) $(gh) * s = g * (h * s)$ kaikille $g, h \in G$ ja $s \in S$.

Olkoon $\mathcal{H} := \{z = x+iy \in \mathbb{C} : y > 0\}$ kompleksitason ylempi puolitaso. Määritellään $\mathrm{SL}_2(\mathbb{Z})$ toimimaan $\mathcal{H}$:ssa, seuraavalla tavalla. Jos $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ silloin

$$M * z \mapsto \frac{az + b}{cz + d}.$$

Osoita, että tämä täyttää toiminnan ehdot.

8. Alkion $s \in S$ vakauttajaksi sanotaan ryhmää $G_s := \{g \in G : g*s = s\}$. Etsi vakauttajat alkioille i ja $\omega = e^{2\pi i/3}$ ryhmän $\mathrm{SL}_2(\mathbb{Z})$:n yllä olevassa toiminnassa.

   Olkoon G ryhmä, joka toimii joukossa S kuvaamalla sen injektiivisesti itseensä. Fundamentaalialue F on joukon S osajoukko siten, että jokainen $s \in S$ voidaan kuvata jonkun $g \in G$ avulla joksikin pisteeksi $f \in F$. Lisäksi, mitään kahta F:n pistettä ei voi kuvata G:n alkioilla toisiinsa.

   Fundamentaalialue ryhmälle $\mathrm{SL}_2(\mathbb{Z})$ on joukko

$$\begin{aligned} F := &\{z \in \mathcal{H} : |z| > 1, -1/2 < \Re(z) < 1/2\} \cup \\ &\{z \in \mathcal{H} : |z| \geq 1, \Re(z) = -1/2\} \cup \\ &\{z \in \mathcal{H} : |z| = 1, \Re(z) \leq 0\} \end{aligned}$$

   Piirrä kuva! Ylläolevaa todistusta hieman muokkaamalla nähdään, että tämä on fundamentaalialue.

9. Osoita, että redusoidun binäärisen neliömuodon pääjuuri sijaitsee fundamentaalin alueen sulkeumassa. Voit käyttää todistuksessa edellistä tehtävää hyödyksesi.