Algebra, syksy 1999, kotitehtävät 10, ratkaisuja

1. a) injektiivisyys: oletetaan, että $g(a) = g(b)$ joillekin $a, b \in \mathbf{R}_+$. Siis $\sqrt{a} = \sqrt{b}$. Korottamalla neliöön saadaan $a = b$.
b) surjektiivisuus: olkoon $y \in \mathbf{R}_+$. Silloin $y^2 \in \mathbf{R}_+$ kuvautuu luvulle y, sillä $g(y^2) = \sqrt{y^2} = y$.
2. Homomorfismi on esimerkiksi f, jolle $f(1) = f(6) = 0$, $f(2) = f(5) = 1$ ja $f(3) = f(4) = 2$.

	1	6	2	5	3	4
1	1	6	2	5	3	4
6	6	1	5	2	4	3
2	2	5	4	3	6	1
5	5	2	3	4	1	6
3	3	4	6	1	2	5
4	4	3	1	6	5	2

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

3. a) Sääntö f, $f(x) := 2x$, on todella funktio $\mathbf{R}_+ \to \mathbf{R}_+$. Edelleen $f(ab) = 2ab$, mutta $f(a)f(b) = 2a2b = 4ab$: esimerkiksi, kun $a = 1$ ja $b = 1$, on $f(ab) \neq f(a)f(b)$. Siis ei homomorfismi, ei isomorfismi, eikä täten automorfismikaan.
b) Samoin f, $f(x) := \sqrt{x}$, on funktio $\mathbf{R}_+ \to \mathbf{R}_+$. Tehtävän 1 mukaan se on bijektio. Se on myös homomorfismi, sillä positiiviluvuilla on $f(ab) = \sqrt{ab} = \sqrt{a}\sqrt{b} = f(a)f(b)$.
Kyseessä on siis isomorfismi joukolta itselleen, ja siten automorfismi.
4. ($\Rightarrow$) Oletetaan, että f on injektio, ts. on voimassa: $f(x) = f(y)$ vain kun $x = y$. Tiedämme, että $f(e) = e'$, joten ainakin $e \in \ker f$ eli $\{e\} \subseteq \ker f$. Jos taas $a \in \ker f$, niin $f(a) = e'$. Mutta silloin $f(a) = f(e)$, ja injektiivisyyden perusteella $a = e$. Näin myös $\ker f \subseteq \{e\}$ ja $\ker f = \{e\}$.
($\Leftarrow$) Oletetaan, että $\ker f = \{e\}$. Olkoot $a, b \in G$ ja $f(a) = f(b)$. Näytetään, että $a = b$ eli $ab^{-1} = e$. Käyttämällä homomorfisuutta kahdesti saadaan

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(b)f(b^{-1}) = f(bb^{-1}) = f(e) = e'.$$

Koska ydin sisältää vain alkion e, on siis $ab^{-1} = e$ eli $a = b$. Siis injektio.
5. Olkoon $y \in G$ mielivaltainen. Koska f on surjektio, on $y = f(x)$ jollekin $x \in G$.
Koska G on syklinen, on $G = \langle h \rangle$ jollekin $h \in G$. Tällöin $x = h^i$ jollekin $i \in \mathbf{Z}$. Silloin

$$y = f(x) = f(h^i) = f(hh \cdots h) = f(h)f(h) \cdots f(h) = f(h)^i.$$

Niinpä $f(h)$ virittää ryhmän G'.
Tuli siis osoitetuksi enemmänkin, virittäjä kuvautuu virittäjälle!
6. a) Sääntö f, $f(x) := 4x \bmod 12$, on selvästi funktio $\mathbf{Z}_{12} \to \mathbf{Z}_{12}$. Käytetään ”modien supistussääntöjä” (Lause 5.4), esim. $(x \bmod n + y \bmod n) \bmod n = (x + y) \bmod n$:

$$\begin{aligned} f(a +_{12} b) &= \big(4(a +_{12} b)\big) \bmod 12 = \big((4 \bmod 12)((a+b) \bmod 12)\big) \bmod 12 = (4(a+b)) \bmod 12, \\ f(a) +_{12} f(b) &= (4a) \bmod 12 +_{12} (4b) \bmod 12 = (4a + 4b) \bmod 12 = \big(4(a+b)\big) \bmod 12. \end{aligned}$$

Kuvajoukko on $\{0, 4, 8\}$ ja ydin $\{0, 3, 6, 9\}$.
7. Molemmissa joukoissa on 10 alkiota ja laskemalla nähdään, että $f(0) = 1$, $f(1) = 6$, $f(2) = 3$, $f(3) = 7$, $f(4) = 9$, $f(5) = 10$, $f(6) = 5$, $f(7) = 8$, $f(8) = 4$, $f(9) = 2$ (ja $f(10) = 1$). Kaikki kuvautuvat eri alkioille ja kaikille kuvautuu jotain; siis bijektio.
8. Edellisestä nähdään, että luvun 6 kertaluku ryhmässä $(\mathbf{Z}_{11} \setminus \{0\}, *_{11})$ on 10, nimittäin

$$6^k \bmod 11 = (6 \cdot 6 \cdots 6) \bmod 11 = 6 *_{11} 6 *_{11} \cdots *_{11} 6 \quad (k \text{ kpl})$$

ja vasta $6^{10} \bmod 11 = 1$. Täten

$$\begin{aligned} f(k +_{10} l) &= 6^{(k+l) \bmod 10} \bmod 11 = 6^{k+l} \bmod 11 = (6^k 6^l) \bmod 11 = \big((6^k \bmod 11)(6^l \bmod 11)\big) \bmod 11 \\ &= \big(f(k)f(l)\big) \bmod 11 = f(k) *_{11} f(l). \end{aligned}$$