Algebra, syksy 1999, kotitehtävien 8 ratkaisut lyhyesti (+ tehtävä 7/7)

1. Syklisenä $G = \{g^k \mid k \in \mathbf{Z}\}$. Sen mielivaltaisille alkioille $a := g^m$ ja $b := g^n$ on siis

$$ab = g^m g^n = g^{m+n} = g^{n+m} = g^n g^m = ba.$$

Siis kyseessä on Abelin ryhmä.
2. Käytetään Aliryhmätestiä 6.2: Määrittelynsä mukaan $H \subseteq G$. Ilmeisestikin e on ryhmän G neutraalialkio.
(i) $\circ$ suljettu joukossa H: jos a, $b \in H$, liitännäisyyden ja vaihdannaisuuden nojalla

$$(a \circ b)^2 = (a \circ b) \circ (a \circ b) = a \circ (b \circ a) \circ b = a \circ (a \circ b) \circ b = (a \circ a) \circ (b \circ b).$$

Siis $(a \circ b)^2 = e \circ e = e$, ja $a \circ b \in H$
(ii) neutraalialkio: aina $e^2 = e$, joten $e \in H$
(iii) käänteisalkiot: jos $a \in H$, on $aa = e$ eli $a^{-1} = a$. Siis $(a^{-1})^2 = a^2 = e$, ja siten $a^{-1} \in H$
3. Laskettava läpi vaikkapa Aliryhmätestin avulla!
4. (i) Fermat'n pienen lauseen mukaan $5^6 \equiv 1 \pmod 7$. Silloin $5^{1001} = 5^{6 \cdot 166 + 5} = 5^5 \cdot 1 \pmod 7$, ja edelleen $5^5 = 25 \cdot 25 \cdot 5 \equiv 4 \cdot 4 \cdot 5 \equiv 16 \cdot 5 \equiv 2 \cdot 5 \equiv 3 \pmod 7$.
(ii) Taas Fermat'n mukaan $3^{16} \equiv 1 \pmod{17}$. Oletuksen mukaan $n = 16s$ jollekin $s \in \mathbf{Z}$, joten

$$3^n = 3^{16s} = (3^{16})^s \equiv 1^s \equiv 1 \pmod{17}.$$

5. Nyt $x^2 \equiv x \pmod p \;\Leftrightarrow\; p \mid (x^2 - x) \;\Leftrightarrow\; p \mid x(x-1)$. Alkulukuna $p \mid x$ tai $p \mid (x-1)$ eli $x \equiv 0 \pmod p$ tai $x \equiv 1 \pmod p$.
6. ($\Rightarrow$) Oletetaan, että $H \subseteq G$ on aliryhmä, ja olkoot a, $b \in H$. Koska myös $b^{-1} \in H$, tulo $ab^{-1} \in H$.
($\Leftarrow$) Oletetaan, että $ab^{-1} \in H$ kaikilla a, $b \in H$. Koska $H \neq \emptyset$, on olemassa $h \in H$.
(ii) neutraalialkio: $e = hh^{-1}$, joten $e \in H$.
(iii) käänteisalkiot: jos $y \in H$, niin $y^{-1} = ey^{-1} \in H$.
(i) laskutoimitus suljettu joukossa H: Olkoot x, $y \in H$. Koska edellisen mukaan $y^{-1} \in H$, oletuksen nojalla $xy = x(y^{-1})^{-1} \in H$.
7. Määrittelynsä mukaan $Z(G) \subseteq G$.
(i) suljettu: Olkoot x, $y \in Z(G)$, eli $xg = gx$ ja $yg = gy$ kaikilla $g \in G$. Silloin

$$(xy)g = x(yg) = x(gy) = (xg)y = (gx)y = g(xy),$$

eli $xy \in Z(G)$ (mitäpä tietoja laskussa tarvittiin?)
(ii) neutraalialkio: kaikilla $g \in G$ on $eg = g = ge$, joten $e \in Z(G)$.
(iii) käänteisalkiot: olkoon $x \in Z(G)$. Silloin

$$x^{-1}g = x^{-1}g(xx^{-1}) = x^{-1}(gx)x^{-1} = x^{-1}(xg)x^{-1} = (x^{-1}x)gx^{-1} = gx^{-1},$$

ja siten $x^{-1} \in Z(G)$ (lisääppä tuohon taas perustelut!).
8. Käytetään Lausetta 6.8. Olkoon alkion a kertaluku n. Oletuksen mukaan $1 \leq n \leq 12$. Koska $a^{12} = e$, Lauseen 6.8 mukaan $n \mid 12$, eli mahdolliset arvot ovat $n = 1, 2, 3, 4, 6, 12$.
9. a) Esimerkiksi $H := \{0, 3, 6, 9\}$ ja $K := \{0, 4, 8\}$ ovat ryhmän $\mathbf{Z}_{12}$ aliryhmiä mutta yhdiste ei ole. Miksi?
b) Jos $H \subseteq K$ tai $K \subseteq H$, on asia selvä (miksi?!). Jäljelle jää vaihtoehto: H:ssa on alkio h, joka ei ole K:ssa, ja K:ssa on alkio k, joka ei ole H:ssa. Silloin kuitenkin h, $k \in H \cup K$.
Väite: $hk \notin H \cup K$.
Todistus. (1) Jos olisi $hk \in H$, niin koska $h^{-1} \in H$, olisi myös $h^{-1}hk = k \in H$.
(2) Vastaava ristiriita saadaan toisesta vaihtoehdosta $hk \in K$.
Siis laskutoimitus ei ole suljettu joukossa $H \cup K$.
10. Aputulos: Ryhmässä alkioilla x ja x^{-1} on aina sama kertaluku.

Todistus. Olkoon alkion x kertaluku $n \geq 1$. Silloin

$$e = x^n = xx^{n-1} = x^2x^{n-2} = \ldots = x^{n-1}x,$$

ja siten $x^{-1} = x^{n-1}$, $x^{-2} = x^{n-2}$, $\ldots$, $x^{-n} = e$. Siis $(x^{-1})^n = x^{-n} = e$. Toisaalta mikään muu $(x^{-1})^p = x^{n-p}$ ei voi olla e, sillä muutoin x:n kertaluku olisi $n-p < n$.
Itse väite: Alkion ab kertaluku on sama kuin alkion ab.
Todistus. Jos $a = e$ tai $b = e$ tai $a^{-1} = b$, on asia selvä. Muutoin, olkoon alkion ab kertaluku n ja alkion ba kertaluku k.
Antiteesi: $k < n$. Silloin yleistetyn liitäntälain ja aputuloksen (todistuksen) mukaan

$$e = (ab)^n = (ab)\cdots(ab) = a(ba)\cdots(ba)b = a(ba)^{n-1}b = a(ba)^{n-1-k}b = (ab)^{n-k},$$

eli alkion ab kertaluku olisikin $n-k$. Ristiriita.
Myöskään epäyhtälö $n < k$ ei voi olla voimassa, miksi?
11. Oletuksen mukaan jokaiselle $g \in G$ on $g^2 = e$ ja siten $g^{-1} = g$. Olkoot a, $b \in G$. Koska $ab \in G$, on $(ab)^{-1} = ab$ ja siis $ab = (ab)^{-1} = (a^{-1}b^{-1})^{-1} = ba$ tulon käänteisalkion laskusäännön mukaan. Siis $ab = ba$ ja kyseessä on Abelin ryhmä.
12. Ehdoista $a * b \leq a + b$ ja $a * a = 0$ saa täytetyksi taulukkoa vasemmanpuoleiseen tilanteeseen saakka. Sitten jatketaan liitännäisyyden avulla, mm. $1 * 3 = 1 * (1 * 2) = (1 * 1) * 2 = 0 * 2 = 2$ jne

$*$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3					
2	2	3	0					
3	3			0				
4	4				0			
5	5					0		
6	6						0	
7	7							0

$*$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	0	1	6	7	4	5
3	3	2	1	0	7	6	5	4
4	4	5	6	7	0	1	2	3
5	5	4	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1
7	7	6	5	4	3	2	1	0

13. Ei ole ryhmä, ei neutraalialkiota.
14. (i) Ei totta: esimerkiksi $5 \mid (1^2+3^2)$ ja $5 \mid (3^2+4^2)$, mutta $1^2 - 3^2 = -8$ ei ole viidellä jaollinen.
(ii) Totta: oletuksen mukaan $a = sp$ ja $a^2+b^2 = kp$ joillekin $s, k \in \mathbf{Z}$. Silloin $a^2 = s^2p^2$ ja

$$b^2 = a^2 + b^2 - a^2 = kp - s^2p^2 = (k - s^2p)\,p.$$

Siten $p \mid b^2$ eli $p \mid bb$. Koska p oli alkuluku, on $p \mid b$.
15. Koska a ei ole parillinen, ovat $a+1$ ja $a-1$ parillisia ja jompikumpi on jaollinen myös neljällä. Koska a ei ole jaollinen kolmella, on joko $a+1$ tai $a-1$ jaollinen kolmella. Tulon $(a-1)(a+1)$ molemmilla tekijöillä on siis parillisuuden takia tekijöinä 2, ts. $a-1 = 2m$ ja $a+1 = 2n$. Koska toinen on jaollinen jopa neljällä, on edelleen $(a-1)(a+1) = 8p$. Kolmella jaollisuuden perusteella vielä $(a-1)(a+1) = 24q$, joten $24 \mid (a^2-1)$.
16. Vastaoletus: $k := \text{syt}(\frac{a}{d}, \frac{b}{d}) > 1$. On siis olemassa kokonaisluvut s ja t, joille $\frac{a}{d} = sk$ ja $\frac{b}{d} = tk$. Mutta silloin $a = dsk$ ja $b = dtk$, ja siten dk olisi lukujen a ja b yhteinen tekijä, joka on aidosti suurempi kuin k. Ristiriita.

Kotilaskujen 7 tehtävä 7.
7. Koska $S \subseteq H_1$ ja $S \subseteq H_2$, myös $S \subseteq H_1 \cap H_2$. Osoitetaan vielä leikkaus aliryhmäksi. Aliryhmien leikkauksena $H_1 \cap H_2 \subseteq G$.
(i) suljettu: jos a ja $b \in H_1 \cap H_2$, niin a, $b \in H_1$ ja a, $b \in H_2$. Koska H_1 ja H_2 ovat aliryhmiä, niin $ab \in H_1$ ja $ab \in H_2$. Siten $ab \in H_1 \cap H_2$.
(ii) Koska H_1 ja H_2 ovat aliryhmiä, neutraalialkio $e \in H_1$ ja $e \in H_2$ ja siten $e \in H_1 \cap H_2$.
(iii) Olkoon $a \in H_1 \cap H_2$. Silloin $a \in H_1$ ja $a \in H_2$, ja koska H_1 ja H_2 ovat aliryhmiä, käänteisalkiot $a^{-1} \in H_1$ ja $a^{-1} \in H_2$. Mutta silloin myös $a^{-1} \in H_1 \cap H_2$.
Leikkaus on siis aliryhmä.
Huomautus. Ryhmässä minkä tahansa aliryhmäkokoelman leikkaus on aliryhmä!