Algebra I, erilliskoe 28.1.2010, ratkaisut ja arvostelukommentit (Jouni Luukkainen), 3 s.
Nämä ratkaisut ovat myös kevään 2009 kurssin kotisivulla.

1. Osoita induktiolla, että $4^{2n}-1$ on jaollinen luvulla 15 kullakin kokonaisluvulla $n \geq 1$.

Ratk. Tapaus $n=1$: $4^{2\cdot 1}-1 = 4^2-1 = 16-1 = 15 = 15\cdot 1$, joten $15|4^{2\cdot 1}-1$.

Olkoon $n \geq 1$ sellainen kokonaisluku, jolla $15|4^{2n}-1$. Tällöin $4^{2n}-1 = 15k$ jollain kokonaisluvulla $k \geq 1$. Siis $4^{2n} = 15k+1$. Nyt

$$4^{2(n+1)}-1 = 4^{2n+2}-1 = 4^{2n}4^2-1 = (15k+1)\cdot 16-1 = 15\cdot 16k+16-1 = 15\cdot 16k+15 = 15(16k+1).$$

Täten $15|4^{2(n+1)}-1$.

Arvostelusta. Induktiolla todistettava väite on sinänsä tämän kurssin alaa, kokonaislukujen jaollisuudesta. Se olisi nopeinta todistaa $\mathbb{Z}_{15}$:ssä laskien, jolloin induktiota ei erikseen tarvita. Mutta tehtävän ydin onkin tällä kurssilla hyvin tärkeä todistusmenetelmä, induktio. Siksi sakotin yhden pisteen, jos induktioaskeleen lähtökohdan muotoilu ei ollut oikein ja täydellinen. Vaihtoehtoina yllä olevalla muotoilulle olisi "Olkoon $n \geq 1$ ja $15|4^{2n}-1$." tai "Oletetaan, että $15|4^{2n}-1$ jollain tietyllä $n \geq 1$." (Makustelkaa tuota "tietyllä"-sanaa!) Väärin ovat "Oletetaan, että $15|4^{2n}-1$ kaikilla $n \geq 1$." (joka on juuri koko induktiolla todistettava väite, tässä hassusti oletettuna) ja "Oletetaan, että $15|4^{2n}-1$ jollain $n \geq 1$." (joka tarkoittaisi "Oletetaan, että on olemassa $n \geq 1$, jolla $15|4^{2n}-1$." — me jopa tiedämme tuossa vaiheessa, että sellainen n on olemassa olettamattakin, nimittäin $n=1$ käy). Muotoilu "Oletetaan, että $15|4^{2n}-1$." on taas puutteellinen, ja juuri koska muotoilun täydentäminen voisi johtaa vikaan, tästäkin oli sakotettava.

2. Ratkaise yhtälöt $a \circ x = b$ ja $y \circ a = b$ ryhmässä S_4, kun

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}.$$

Ratk. Siis esimerkiksi $a(1)=3$, jolloin $a^{-1}(3)=1$. Täten

$$a^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} = b.$$

Nyt

$$x = (a^{-1}\circ a)\circ x = a^{-1}\circ(a\circ x) = b\circ b \qquad \text{ja} \qquad y = y\circ(a\circ a^{-1}) = (y\circ a)\circ a^{-1} = b\circ b.$$

Siis

$$x = y = b\circ b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}\circ\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 4 & 2 & 1 & 3 \\ 3 & 2 & 4 & 1 \end{pmatrix}\circ\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = a,$$

jossa permutaatiotulon ensimmäisen tekijän sarakkeiden järjestys on vaihdettu toisen tekijän toisen rivin mukaiseksi, jolloin tulo on välittömästi luettavissa.

Arvostelusta. Minun olisi ollut laadittava tehtävä toisin, sillä yhdistetyn kuvauksen $b\circ b$ saattoi nyt laskea väärällä tavalla silti oikean tuloksen saaden (määritelmän mukaan $(f\circ g)(t) = f(g(t))$, ei $(f\circ g)(t) = g(f(t))$, mutta jos $f=g$, ero ei näy). Jos tulon tekijät olivat kopiointivirheen vuoksi toisistaan eriävät, niin väärä tulonmuodostustapa saattoi tulla näkyviin, jolloin sakkoa meni 2p samoin kuin väärin muodostetusta käänteispermutaatiosta a^{-1}.

3. Määritellään kokonaislukujen joukon $\mathbb{Z}$ ja rationaalilukujen joukon $\mathbb{Q}$ tulojoukossa $G = \mathbb{Z}\times\mathbb{Q}$ laskutoimitus $\circ$ asettamalla

$$(m,q)\circ(n,r) = (m+n, 2^n q + r).$$

(a) Osoita, että G on ryhmä laskutoimituksen $\circ$ suhteen.

(b) **(i)** Onko joukko $H = \{(m,0) \in G \mid m \in \mathbb{Z}\}$ ryhmän G aliryhmä?

(ii) Onko joukko $K = \{(0,q) \in G \mid q \in \mathbb{Q}\}$ ryhmän G aliryhmä?

Ratk. (a) Laskutoimituksen $\circ$ arvot ovat todellakin joukossa G, sillä jos $m,n \in \mathbb{Z}$ ja $q,r \in \mathbb{Q}$, niin $m+n \in \mathbb{Z}$ ja $2^n q + r \in \mathbb{Q}$, koska $2^n \in \mathbb{Q}$.

(1) Laskutoimitus $\circ$ on liitännäinen: Jos $(m,q),(n,r),(p,s) \in G$, niin

$$\begin{aligned}((m,q)\circ(n,r))\circ(p,s) &= (m+n, 2^n q + r)\circ(p,s) = ((m+n)+p, 2^p(2^n q + r) + s)\\ &= (m+(n+p), 2^{n+p}q + (2^p r + s)) = (m,q)\circ(n+p, 2^p r + s)\\ &= (m,q)\circ((n,r)\circ(p,s)).\end{aligned}$$

(2) Alkio $(0,0) \in G$ on neutraalialkio: Jos $(m,q) \in G$, niin

$$(m,q)\circ(0,0) = (m+0, 2^0 q + 0) = (m,q) = (0+m, 2^m 0 + q) = (0,0)\circ(m,q).$$

(3) Alkiolla $(m,q) \in G$ on käänteisalkio $(-m, -2^{-m}q) \in G$, sillä

$$\begin{aligned}&(m,q)\circ(-m,-2^{-m}q) = (m+(-m), 2^{-m}q + (-2^{-m}q)) = (0,0) \quad \text{ja}\\ &(-m,-2^{-m}q)\circ(m,q) = ((-m)+m, 2^m(-2^{-m}q) + q) = (0, -2^0 q + q) = (0, -q+q) = (0,0).\end{aligned}$$

Täten G on ryhmä.

(b) Määritellään kuvaukset $f\colon \mathbb{Z} \to G$, $m \mapsto (m,0)$, ja $g\colon \mathbb{Q} \to G$, $q \mapsto (0,q)$. Tällöin

$$\begin{aligned}&f(m)\circ f(n) = (m,0)\circ(n,0) = (m+n, 2^n 0 + 0) = (m+n,0) = f(m+n) \quad \forall m,n \in \mathbb{Z};\\ &g(q)\circ g(r) = (0,q)\circ(0,r) = (0+0, 2^0 q + r) = (0, q+r) = g(q+r) \quad \forall q,r \in \mathbb{Q}.\end{aligned}$$

Täten f ja g ovat ryhmähomomorfismeja. Näin ollen $H = f(\mathbb{Z})$ ja $K = g(\mathbb{Q})$ ovat G:n aliryhmiä (itse asiassa $f\colon \mathbb{Z} \cong H$ ja $g\colon \mathbb{Q} \cong K$).

Vaihtoehtoinen määritelmään perustuva todistus:

(i) H on G:n aliryhmä, sillä:
(1) Jos $(m,0),(n,0) \in H$, niin $(m,0)\circ(n,0) = (m+n, 2^n 0 + 0) = (m+n,0) \in H$.
(2) $(0,0) \in H$.
(3) Jos $(m,0) \in H$, niin $(m,0)^{-1} = (-m, -2^{-m}0) = (-m,0) \in H$.

(ii) K on G:n aliryhmä, sillä:
(1) Jos $(0,q),(0,r) \in K$, niin $(0,q)\circ(0,r) = (0+0, 2^0 q + r) = (0, q+r) \in K$.
(2) $(0,0) \in K$.
(3) Jos $(0,q) \in K$, niin $(0,q)^{-1} = (-0, -2^{-0}q) = (0,-q) \in K$.

4. Olkoon $\mathbb{Q}$ rationaalilukujen kunta, X joukko ja $R = \mathbb{Q}^X$ kuvausten $f\colon X \to \mathbb{Q}$ kommutatiivinen rengas, laskutoimitukset siis pisteittäin määriteltyinä.

(a) Olkoon $A \subset X$ osajoukko ja

$$I_A = \{f \in R \mid f(x) = 0 \text{ kaikilla } x \in A\} \subset R,$$

joukossa A häviävien kuvausten $f \in R$ joukko. Osoita määritelmään nojautuen, että I_A on R:n ideaali.

(b) Osoita, että I_A on jopa R:n pääideaali eli muotoa Ra jollain $a \in R$.

(c) Osoita, että kääntäen jokainen R:n pääideaali on muotoa I_A jollain osajoukolla $A \subset X$.

Ratk. Renkaan R kertolasku on vaihdannainen, koska $\mathbb{Q}$:n kertolasku on vaihdannainen.

(a) (1) Selvästi $\overline{0} \in I_A$, kun $\overline{0} \in R$ on nollakuvaus $x \mapsto 0$. Täten $I_A \neq \emptyset$.

(2) Olkoon $f,g \in I_A$. Tällöin $(f-g)(x) = f(x) - g(x) = 0 - 0 = 0$ kaikilla $x \in A$, joten $f - g \in I_A$.

(3) Olkoon $f \in I_A$ ja $g \in R$. Tällöin $(fg)(x) = f(x)g(x) = 0 \cdot g(x) = 0$ kaikilla $x \in A$. Täten $fg \in I_A$. (Silloin myös $gf = fg \in I$.)

Ehtojen (1)–(3) nojalla I_A on R:n ideaali.

(b) Määritellään $a \in R$ asettamalla $a(x) = 0$ kaikilla $x \in A$ ja $a(x) = 1$ kaikilla $x \in X \setminus A$. Tällöin $a \in I_A$. Osoitetaan, että I_A on a:n virittämä R:n pääideaali $\langle a \rangle = Ra = \{ga \mid g \in R\}$. Ensiksikin, $\langle a \rangle \subset I_A$, koska $\langle a \rangle$ on pienin a:n sisältävistä R:n ideaaleista. Toisaalta, jos $f \in I_A$, niin on jopa $f = fa \in \langle a \rangle$, sillä $(fa)(x) = f(x)a(x) = f(x) \cdot 1 = f(x)$ kaikilla $x \in X \setminus A$ ja $(fa)(x) = 0 = f(x)$ kaikilla $x \in A$. Siis $I_A = \langle a \rangle$.

(c) Olkoon $I = \langle a \rangle$ renkaan R mielivaltainen, erään alkion $a \in R$ virittämä pääideaali. Olkoon $A = a^{-1}(\{0\}) \subset X$. Tällöin $a(x) = 0$ kaikilla $x \in A$, joten $a \in I_A$ ja siis myös $I \subset I_A$. Osoitetaan, että $I = I_A$. Huomataan, että kullakin $x \in X \setminus A$ on olemassa $1/a(x) \in \mathbb{Q}$. Jos siis $f \in I_A$, niin voidaan määritellä kuvaus $g \in R$ asettamalla $g(x) = f(x)/a(x) \in \mathbb{Q}$ kaikilla $x \in X \setminus A$ ja vaikkapa $g(x) = 0$ kaikilla $x \in A$; tällöin $(ga)(x) = g(x)a(x) = f(x)$ kaikilla $x \in X \setminus A$ ja $(ga)(x) = g(x)a(x) = 0 = f(x)$ kaikilla $x \in A$, jolloin $f = ga \in I$. Näin ollen $I_A \subset I$ ja siis $I = I_A$.

5. Määritä polynomin $f = x^2 + 14 \in \mathbb{Z}_{15}[x]$ kaikki esitykset muotoa $f = (x + a)(x + b)$ joillain $a, b \in \mathbb{Z}_{15}$.

Ratk. Jos $a, b \in \mathbb{Z}_{15}$, niin $f = (x + a)(x + b) \iff x^2 + 14 = x^2 + (a + b)x + ab \iff a + b = 0$ ja $ab = 14 \iff b = -a$ ja $-a^2 = 14 = -1 \iff a^2 = 1$ ja $b = -1$. Nyt renkaassa $\mathbb{Z}_{15}$ on $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 9$, $4^2 = 16 = 1$, $5^2 = 25 = 10$, $6^2 = 36 = 6$, $7^2 = 49 = 4$, $8^2 = 64 = 4$, $9^2 = 81 = 6$, $10^2 = 100 = 10$, $11^2 = 121 = 1$, $12^2 = 144 = 9$, $13^2 = 169 = 4$ ja $14^2 = 196 = 1$. Siis $a^2 = 1 \iff a \in \{1, 4, 11, 14\}$. Koska $-1 = 14$ ja $-4 = 11$, niin kaikki haetut esitykset tekijöiden järjestystä vaille ovat $\underline{f = (x + 1)(x + 14)}$ ja $\underline{f = (x + 4)(x + 11)}$.

Huom. Koska 15 ei ole alkuluku, niin $\mathbb{Z}_{15}$ ei ole kokonaisalue, jolloin kävi niin, että toisen asteen polynomilla f oli enemmän kuin kaksi nollakohtaa ja enemmän kuin yksi esitys (tekijöiden järjestystä vaille) jaottomien tekijöiden tuloksi. Teoriaan ei siis voinut vedota.

Arvostelusta. Teorian puuttuessa nollakohtien etsimisessä oli ilmoitettava $f(a)$:n arvo kullakin $a \in \mathbb{Z}_{15}$; ei riittänyt ilmoittaa pelkkiä nollakohtia. Sakkoa 1p.