Huom.: Jos laskutoimituksia merkitään toisin, homom. ehto muuttuu vastaavasti. Esim. $f: (G,+) \to (G',+)$ homom. $\iff$ $f(a+b) = f(a) + f(b)$ $\forall a, b \in G$.
Yleisesti $f: (G,\top) \to (G',\top')$ homom. $\iff$
$f(a \top b) = f(a) \top' f(b)$ $\forall a, b \in G$.

Lause: $f: G \to G'$ ryhmähomom. $\Rightarrow$
$f(1_G) = 1_{G'}$ ja $f(a^{-1}) = f(a)^{-1}$ $\forall a \in G$.

Tod.: $f(1) = f(1 \cdot 1) = f(1) \cdot f(1) \Rightarrow 1 = f(1) \cdot f(1)^{-1}$
$= f(1) \cdot f(1) \cdot f(1)^{-1} = f(1) \cdot 1 = f(1)$. Kun $a \in G$,
on $f(a) \cdot f(a^{-1}) = f(a \cdot a^{-1}) = f(1) = 1$ ja samoin
$f(a^{-1}) \cdot f(a) = 1$; siispä $f(a^{-1}) = f(a)^{-1}$. □

Seuraus: $f: G \to G'$ ryhmähomom., $a_1, \dots, a_k, a \in G$

$\Rightarrow$ $f(a_1 a_2 \cdots a_k) = f(a_1) \cdot f(a_2) \cdot \ldots \cdot f(a_k)$
$f(a^n) = f(a)^n$ $\forall n \in \mathbb{Z}$. □

Huom.: Jos G, G' ovat vain (multipl.) monoideja, niin ehto $f(1_G) = 1_{G'}$ ei seuraa ehdosta $f(ab) = f(a) \cdot f(b)$ $\forall a, b \in G$.

Esim.: a) $f: \mathbb{R} \setminus \{0\} \to \mathbb{R} \setminus \{0\}$, $f(x) = x^2$ $\forall x \in \mathbb{R} \setminus \{0\}$, on multipl. homom., sillä $f(xy) = (xy)^2 = x^2 y^2 = f(x) f(y)$ $\forall x, y \in \mathbb{R} \setminus \{0\}$.

b) Kuvaus $x \mapsto \ln x$ on homom. $(\mathbb{R}_+^*, \cdot) \to (\mathbb{R}, +)$, sillä $\ln(xy) = \ln x + \ln y$ $\forall x, y \in \mathbb{R}_+^*$ $(= \{x \in \mathbb{R} \mid x > 0\})$.

c) Kan. surj. $p: \mathbb{Z} \to \mathbb{Z}_n$ $(n \in \mathbb{N}_+)$ on (addit.) homom.

d) $\det: (GL_2(\mathbb{R}), \cdot) \to (\mathbb{R} \setminus \{0\}, \cdot)$ on homom.

e) Ol. G (multipl.) ryhmä ja $a \in G$. Potenssien laskusäännöt $\Rightarrow$ kuvaus $f: (\mathbb{Z}, +) \to G$, $f(n) = a^n$ $\forall n \in \mathbb{Z}$, on homom. $(a^{m+n} = a^m \cdot a^n \ \forall\, m, n \in \mathbb{Z})$.
Käänteen, jos $f: \mathbb{Z} \to G$ on homom. ja merk. $a = f(1) \in G$, niin $f(n) = f(n \cdot 1) = f(1)^n = a^n$ $\forall n \in \mathbb{Z}$.
Saadaan siis lyhyesti

$\{\text{homomorfismit } \mathbb{Z} \to G\} \xrightarrow{\sim} G$
$f \longmapsto f(1)$.

f) G_1, G_2 ryhmiä $\Rightarrow$ projektiot $pr_1 : G_1 \times G_2 \to G_1$ ja $pr_2 : G_1 \times G_2 \to G_2$ ovat homom. (ks. Lause 4).

g) Triviali homom. $f : G \to G'$, $f(a) = 1_{G'}$ $\forall a \in G$.

Lause: a) $id_G : G \to G$ on homom.
b) $f : G \to G'$, $g : G' \to G''$ homom. $\Rightarrow$
$g \circ f : G \to G''$ on homom.

Tod.: a) on triviali.
b) $a, b \in G \Rightarrow (g \circ f)(ab) = g(f(ab)) = g(f(a) \cdot f(b))$
$= g(f(a)) \cdot g(f(b)) = (g \circ f)(a) \cdot (g \circ f)(b)$. □

Alkuhuan kuva- ja alkukuvajoukko homomorfismissa on aliryhmä:

Lause 8: Ol. $f : G \to G'$ homom. Silloin

a) $H \leq G \Rightarrow f(H) \leq G'$
b) $H' \leq G' \Rightarrow f^{-1}(H') \leq G$.

Tod.: a) Ol. $H \leq G$. $1_G \in H \Rightarrow 1_{G'} = f(1_G) \in f(H)$
$\Rightarrow f(H) \neq \emptyset$. Ol. $a', b' \in f(H) \Rightarrow \exists a, b \in H$
s.e. $a' = f(a)$, $b' = f(b)$; H alir. $\Rightarrow ab^{-1} \in H$;
nyt $a' \cdot b'^{-1} = f(a) \cdot f(b)^{-1} = f(a) \cdot f(b^{-1}) = f(ab^{-1}) \in f(H)$.
Aliryhmäkrit. $\Rightarrow f(H) \leq G'$.

b) Ol. $H' \leq G'$. $f(1_G) = 1_{G'} \in H' \Rightarrow 1_G \in f^{-1}(H')$
$\Rightarrow f^{-1}(H') \neq \emptyset$. Ol. $a, b \in f^{-1}(H') \Rightarrow f(a), f(b) \in H'$
$\Rightarrow f(ab^{-1}) = f(a) \cdot f(b^{-1}) = f(a) \cdot f(b)^{-1} \in H'$ (H' alir.)
$\Rightarrow ab^{-1} \in f^{-1}(H')$. Aliryhmäkrit. $\Rightarrow f^{-1}(H') \leq G$. □

Erityisesti homomorfismin $f : G \to G'$ ydin

$$\ker(f) = \{a \in G \mid f(a) = 1_{G'}\} = f^{-1}(\{1_{G'}\})$$

on G:n aliryhmä ja kuva $\mathrm{Im}(f) = f(G)$ on G':n aliryhmä.

Esim.: a) $f: \mathbb{R}\setminus\{0\} \to \mathbb{R}\setminus\{0\}$, $f(x) = x^2$ $\forall x$
$\Rightarrow$ $\ker(f) = \{x \mid x^2 = 1\} = \{1, -1\}$, $\mathrm{Im}(f) = \mathbb{R}_+^*$.

b) $f: \mathbb{R}_+^* \to \mathbb{R}$, $f(x) = \ln x$ $\forall x$
$\Rightarrow$ $\ker(f) = \{x \in \mathbb{R}_+^* \mid \ln x = 0\} = \{1\}$, $\mathrm{Im}(f) = \mathbb{R}$.

c) $p: \mathbb{Z} \to \mathbb{Z}_n$ kan. surj. $\Rightarrow$ $\ker(p) = n\mathbb{Z}$, $\mathrm{Im}(p) = \mathbb{Z}_n$.

d) $\ker[\det: GL_2(\mathbb{R}) \to \mathbb{R}\setminus\{0\}] = SL_2(\mathbb{R})$,
$\mathrm{Im}[\quad\text{-}''\text{-}\quad] = \mathbb{R}\setminus\{0\}$.

e) $f: G \to G'$, $f(a) = 1_{G'}$ $\forall a \in G$
$\Rightarrow$ $\ker(f) = G$, $\mathrm{Im}(f) = \{1_{G'}\}$.

Lause 9: Ryhmähomom. $f: G \to G'$ on injektio
$\Leftrightarrow$ $\ker(f) = \{1_{G'}\}$.

Tod.: Jokin tapauksessa $1_G \in \ker(f)$.
$\Rightarrow$: Ol. f inj. $a \in \ker(f) \Rightarrow f(a) = 1_{G'} = f(1_G)$
$\Rightarrow a = 1_G$ (koska f inj.). $\therefore \ker(f) = \{1_G\}$.
$\Leftarrow$: Ol. $\ker(f) = \{1_G\}$. Olk. $a, b \in G$ ja $f(a) = f(b)$
$\Rightarrow$ $f(ab^{-1}) = f(a)\cdot f(b)^{-1} = f(a)\cdot f(a)^{-1} = 1_{G'}$ $\Rightarrow ab^{-1} \in \ker(f)$
$\Rightarrow$ $ab^{-1} = 1_G \Rightarrow a = b$. $\therefore f$ on inj. $\square$

Määr.: Bijektiivinen ryhmähomom. $f: G \to G'$ on (ryhmä-) isomorfismi. Isomorfismi $G \to G$ on G:n automorfismi. Ryhmät G ja G' ovat isomorfiset, merk. $G \cong G'$, jos $\exists$ isom. $G \to G'$.

Esim.: a) $f: G \to G'$ injektiivinen homom.
$\Rightarrow$ $G \cong \mathrm{Im}(f) \leq G'$.

b) $x \mapsto \ln x$ on isom. $(\mathbb{R}_+^*, \cdot) \xrightarrow{\sim} (\mathbb{R}, +)$

c) $(\mathbb{R}, +) \not\cong (\mathbb{R}\setminus\{0\}, \cdot)$
($f: \mathbb{R} \to \mathbb{R}\setminus\{0\}$ homom. $\Rightarrow f(x) = f(\frac{x}{2} + \frac{x}{2}) =$
$= f(\frac{x}{2})\cdot f(\frac{x}{2}) > 0$ $\forall x \in \mathbb{R}$ $\Rightarrow$ f ei surj. .)

d) Ol. $f: \mathbb{Z} \to \mathbb{Z}$ homom. $\Rightarrow \exists a \in \mathbb{Z}$ s.e. $f(n) = an$ $\forall n \in \mathbb{Z}$. Selvästi f on isom. $\Leftrightarrow$ $a = \pm 1$.

Lause 11: $f: G \to G'$ isom. $\Rightarrow$ myös käänteis-kuvaus $f^{-1}: G' \to G$ on isomorfismi.

Tod.: f^{-1} on bij., joten riittää os. sen homomorfisuus.
$a', b' \in G'$ $\Rightarrow$ $a' = f(a)$, $b' = f(b)$, mistä $a = f^{-1}(a')$,
$b = f^{-1}(b')$ $\Rightarrow$ $f^{-1}(a'\cdot b') = f^{-1}(f(a)\cdot f(b)) = f^{-1}(f(ab))$
$= ab = f^{-1}(a')\cdot f^{-1}(b')$. $\square$

Lisäksi selvästi id_G on isom. ja kahden isom. yhdistelmä on isom. Erityisesti ryhmän G automorfismit muodostavat permutaatioryhmän S_G aliryhmän

$$Aut(G) = \{f : G \to G \mid f \text{ on isom.}\} \leq S_G .$$

Esim. 5: Ol. G (multipl.) ryhmä. Alkiolla $g \in G$ konjugointi $c_g : G \to G$, $c_g(a) = gag^{-1}$ $\forall a \in G$, on isomorfismi, G:n ns. sisäinen automorfismi. Lisäksi $c_{1_G} = id_G$ ja $c_{g_1 g_2} = c_{g_1} \circ c_{g_2}$ $\forall g_1, g_2 \in G$, joten kuvaus $g \mapsto c_g$ on homom.

$$c : G \to Aut(G) \qquad \text{(yleisyyskohdat harj.teht.)}.$$

Esim.: Ol. G (multipl.) ryhmä. Kun $a \in G$, niin Lause 2 $\Rightarrow$ $f_a : G \to G$, $f_a(x) = ax$ $\forall x \in G$, on bijektio (mutta ei homom.), ts. $f_a \in S_G$. Näin saatu kuvaus

$$f : G \to S_G , \quad a \mapsto f_a \quad \forall a \in G,$$

on homom., sillä $a, b \in G \Rightarrow (f_a \circ f_b)(x) = f_a(f_b(x)) = f_a(bx) = a(bx) = (ab)x = f_{ab}(x)$ $\forall x \in G \Rightarrow f_a \circ f_b = f_{ab}$. Lisäksi f on inj., sillä $f_a = f_b \Rightarrow a = a \cdot 1 = f_a(1) = f_b(1) = b \cdot 1 = b$. $\therefore G \cong Im(f) \leq S_G$.

Isomorfiset ryhmät ovat ryhmäteorian kannalta "samanarvoiset", sillä ryhmäteoreettiset ominaisuudet säilyvät isomorfismeissa.

Ed. esim. $\Rightarrow$

Lause (Cayley): Jokainen ryhmä G on isomorfinen permutaatioryhmän S_G erään aliryhmän kanssa. □

III.5 Sivuluokat ja Lagrangen lause

Olkoon G (multipl.) ryhmä ja $H \leq G$ aliryhmä. Alkion $a \in G$ vasen H-sivuluokka on G:n osajoukko

$aH = \{ah \mid h \in H\} \subset G$

(additiivisessa ryhmässä G tätä merk. $a+H$). Osoittautuu, että aH = a:n ekv.luokka eräässä G:n ekvivalenssissa:

Lemma: G:n relaatio $E = E_H^{\nu}$, $aEb \Leftrightarrow a^{-1}\cdot b \in H$, on ekvivalenssi (vasen H-ekvivalenssi), jossa $E(a) = aH$ $\forall a \in G$.

Tod.: Refl. aEa, koska $a^{-1}\cdot a = 1 \in H$.
Symm.: $aEb \Rightarrow a^{-1}b \in H \Rightarrow b^{-1}a = b^{-1}\cdot(a^{-1})^{-1} =$
$= (a^{-1}b)^{-1} \in H$ (H aliryhmä) $\Rightarrow bEa$.
Transit.: aEb, $bEc \Rightarrow a^{-1}b \in H$, $b^{-1}c \in H$
$\Rightarrow a^{-1}c = (a^{-1}b)\cdot(b^{-1}c) \in H$ (H alir.) $\Rightarrow aEc$.
$\therefore$ E on ekvivalenssi.
$b \in E(a) \Leftrightarrow bEa \Leftrightarrow aEb \Leftrightarrow a^{-1}b \in H$
$\Leftrightarrow \exists h \in H$ s.e. $a^{-1}b = h \Leftrightarrow \exists h \in H$ s.e. $b = ah$
$\Leftrightarrow b \in aH$. $\therefore E(a) = aH$. □

Seuraus: G:n vasempien H-sivuluokkien joukko $G/H = \{aH \mid a \in G\}$ on G:n osittelu, ts.

$$G = \bigcup_{a \in G} aH \; ; \quad aH \cap bH \neq \emptyset \Rightarrow aH = bH.$$

Lisäksi $aH = bH \Leftrightarrow b \in aH \Leftrightarrow a^{-1}b \in H$. □

Vastaavasti alkion $a \in G$ oikea H-sivuluokka $Ha = \{ha \mid h \in H\}$ on a:n ekv.luokka G:n oikeassa H-ekvivalenssissa E_H^{o}, $aE_H^{o}b \Leftrightarrow ba^{-1} \in H$. Oikeiden H-sivuluokkien joukko $H\backslash G = \{Ha \mid a \in G\}$ on niin ikään G:n osittelu.

Huom.: a) H on itse eräs vasen ja oikea H-sivuluokka:
$H = 1\cdot H = H\cdot 1$. $aH = H = Ha \Leftrightarrow a \in H$.
b) Jos G on Abelin ryhmä, niin $aH = Ha$ $\forall a \in G$ (koska jopa $ah = ha$ $\forall a \in G$, $h \in H$).

Esim.: a) Olk. $n \in \mathbb{N}_+$. Ryhmän $(\mathbb{Z}, +)$ (vas.=oik.) $n\mathbb{Z}$-sivuluokat ovat jäännösluokat $[a]_n = a + n\mathbb{Z}$ $(a \in \mathbb{Z})$, joten $\mathbb{Z}/n\mathbb{Z} = \{a+n\mathbb{Z} \mid a \in \mathbb{Z}\} = \{a+n\mathbb{Z} \mid a = 0, 1, \ldots, n-1\}$
$= \mathbb{Z}_n$ (joukkoina).

b) Olk. X joukko ja $x_0 \in X$. Tark. alinyhmää $H = \{h \in S_X \mid h(x_0) = x_0\}$ ($\cong S_{X\setminus\{x_0\}}$, sillä $h \in H \Leftrightarrow h(X\setminus\{x_0\}) = X\setminus\{x_0\}$). Olkoon $f \in S_X$.

V. $fH = \{g \in S_X \mid g(x_0) = f(x_0)\}$
$Hf = \{g \in S_X \mid g^{-1}(x_0) = f^{-1}(x_0)\}$.

T. $g \in fH \Leftrightarrow f^{-1}g \in H \Leftrightarrow f^{-1}(g(x_0)) = x_0 \Leftrightarrow g(x_0) = f(x_0)$;
$g \in Hf \Leftrightarrow gf^{-1} \in H \Leftrightarrow g(f^{-1}(x_0)) = x_0 \Leftrightarrow g^{-1}(x_0) = f^{-1}(x_0)$. □

Kun $x \in X$, $\exists f \in S_X$ s.e. $f(x_0) = x = f^{-1}(x_0)$ (esim. $f(x_0) = x$, $f(x) = x_0$, $f(y) = y$ $\forall y \in X\setminus\{x_0\}$). Siten S_X:n eri vasemmaiset (oikeat) H-sivuklokset ovat joukot $\{g \in S_X \mid g(x_0) = x\}$, $x \in X$ ($\{g \in S_X \mid g^{-1}(x_0) = x\}$, $x \in X$). Jos X on äärellinen, on ehtyjeisiä

$$\#(S_X/H) = \#(H\backslash S_X) = \#X.$$

Huom.: Jos $\#X \geq 3$, $x \neq x_0$ ja $f(x) = f(x_0)$, $f(x_0) = f(x)$, $f(y) = y$ $\forall y \neq x_0, x$, niin $fH = \{g \in S_X \mid g(x_0) = x\}$ $\neq \{g \in S_X \mid g^{-1}(x_0) = x\} = Hf$.

Yleensä $G/H \neq H\backslash G$; nämä joukot ovat kuitenkin yhtä mahtavat:

Lause: Kaava $aH \mapsto Ha^{-1}$ määrittelee bijektion
$$G/H \xrightarrow{\sim} H\backslash G.$$

Tod.: Jotta yllämainittu säännön kuvaus $G/H \to H\backslash G$, on todettava, että $aH = bH \Rightarrow Ha^{-1} = Hb^{-1}$.
$aH = bH \Rightarrow a E_H^{\omega} b \Rightarrow a^{-1}b \in H \Rightarrow b^{-1}(a^{-1})^{-1} = (a^{-1}b)^{-1} \in H$ (H alir.) $\Rightarrow a^{-1} E_H^{\circ} b^{-1} \Rightarrow Ha^{-1} = Hb^{-1}$.
Vastaavasti $Ha^{-1} = Hb^{-1} \Rightarrow aH = bH$, ts. ko. kuvaus on injektio. Se on myös surjektio, sillä $Hc \in H\backslash G$ $\Rightarrow c^{-1}H \mapsto Hc$. □

Lisäksi jok. yksittäinen H-sivuklokka on yhtä mahtava kuin H (kuvaukset $h \mapsto ah$ ja $h \mapsto ha$ ovat bijektioita $H \xrightarrow{\sim} aH$ ja $H \xrightarrow{\sim} Ha$).

Määr.: Jos joukot $G/H \cong H\backslash G$ ovat äärellisiä, niin $|G:H| = \#(G/H) = \#(H\backslash G) \in \mathbb{N}_+$ (luetaan $[G:H]$)

on aliryhmän H indeksi G:ssä. Muussa tapauksessa merk. $|G:H| = \infty$.

Lause 12 (Lagrange): Jos G on äärell. ryhmä ja $H \leq G$, niin $|G| = |G:H| \cdot |H|$. Erityisesti $|H| \mid |G|$ kaikilla $H \leq G$.

Tod.: Olkoon $D \subset G$ vas. H-sivuklsoluiden edustajista; $D = \{a_1, \dots, a_n\}$, $n = \#D = |G:H| \Rightarrow$
$G = a_1H \cup a_2H \cup \dots \cup a_nH$, erillinen yhdiste. Siten
$|G| = \#(a_1H) + \#(a_2H) + \dots + \#(a_nH) = n \cdot \#H$
$= |G:H| \cdot |H|$, koska $a_kH \cong H \ \forall k$. $\square$

Esim.: $|G| = 7 \Rightarrow$ G:n ainoat aliryhmät ovat $\{1_G\}$ ja G (7:n ainoat pos. tekijät ovat 1 ja 7).

Lause: $|S_n| = n! \quad \forall n \in \mathbb{N}_+$.

Tod.: Ol. $n \geq 2$. Merk. $H = \{h \in S_n \mid h(n) = n\} \leq S_n$.
Aiemmin on todettu, että $H \cong S_{n-1}$ ja $|S_n:H| = n$.
Lagrange $\Rightarrow$ $|S_n| = |S_n:H| \cdot |H| = n \cdot |S_{n-1}|$.
Väite seuraa induktiolla. $\square$

Lagrangen lauseen seurauksia:

Seuraus 1: G äärell. ryhmä, $a \in G$
$\Rightarrow$ $\operatorname{ord}(a) \mid |G|$.

Tod.: $\operatorname{ord}(a) = |\langle a \rangle|$, $|G| = |G:\langle a \rangle| \cdot |\langle a \rangle|$. $\square$

Seuraus 2: $|G| = n \in \mathbb{N}_+ \Rightarrow a^n = 1_G \quad \forall a \in G$.

Tod.: Merk. $h = \operatorname{ord}(a) = |\langle a \rangle| \Rightarrow a^h = 1_G$ (sykl. ryhmässä $\langle a \rangle$). Seur. 1 $\Rightarrow h \mid n \Rightarrow n = h \cdot k$ eräälle $k \in \mathbb{N}_+ \Rightarrow a^n = a^{hk} = (a^h)^k = 1^k = 1$. $\square$

Esim. 6: Tark. multipl. ryhmää $\mathbb{Z}_n^*$ ($n \in \mathbb{N}_+$); $|\mathbb{Z}_n^*| = \varphi(n)$. Seur. 2 $\Rightarrow \bar{a}^{\varphi(n)} = \bar{1} \quad \forall \bar{a} \in \mathbb{Z}_n^*$, eli

$$a^{\varphi(n)} \equiv 1 \pmod{n}, \text{ kun } \operatorname{syt}(a,n) = 1 \quad \text{(Eulerin lause)}.$$

Kun $n = p$ on alkuluku, $\varphi(p) = p-1$ ja saadaan

$$a^{p-1} \equiv 1 \pmod p, \text{ kun } p \nmid a \qquad \text{(Fermat)}.$$

Tästä seuraa, että $a^p \equiv a \pmod p$ $\forall a \in \mathbb{Z}$.

Esim. $7^{103} \equiv (7^{10})^{10} \cdot 7^3 \equiv 1^{10} \cdot 7^3$
$= 7^3 = 49 \cdot 7 \equiv 5 \cdot 7 = 35 \equiv 2 \pmod{11}$.

Seuraus 3: $|G| = p$ alkuluku $\Rightarrow$ G on syklinen, $G \cong \mathbb{Z}_p$.

Tod.: Val. $a \in G$, $a \neq 1_G$ $\Rightarrow$ $|\langle a\rangle| > 1$ ja $|\langle a\rangle| \mid p$. p alkuluku $\Rightarrow$ $|\langle a\rangle| = p = |G|$
$\Rightarrow$ $G = \langle a\rangle$ syklinen. Kuvaus $[k]_p \mapsto a^k$ määrittelee kom. $\mathbb{Z}_p \xrightarrow{\sim} G$. □

Esim.: Neljännen kertaluvun ryhmät. Or. G multipl. ryhmä, $|G| = 4$. 2 vaihtoehtoa:

1) G syklinen; $G = \langle a\rangle = \{1_G, a, a^2, a^3\} \cong (\mathbb{Z}_4, +)$ eräälle $a \in G$ $(a^4 = 1)$.

2) G ei syklinen. Olk. $G = \{1_G, a, b, c\}$.
Lagrange $\Rightarrow$ $\operatorname{ord}(a) = \operatorname{ord}(b) = \operatorname{ord}(c) = 2$ (koska ei ole $\langle a\rangle = G$ jne.) $\Rightarrow$ $a^2 = b^2 = c^2 = 1_G$.
$b \neq a^{-1} = a$ $\Rightarrow$ $ab \neq 1_G$; $b \neq 1_G$ $\Rightarrow$ $ab \neq a$;
$a \neq 1_G$ $\Rightarrow$ $ab \neq b$. Siis $ab = c$, ja samoin $ba = c$.
Muut tulot määräytyvät tästä, esim. $a \cdot c = aab = b$.

$\therefore$ $G \cong (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$; $1_G \leftrightarrow (\bar 0, \bar 0)$, $a \leftrightarrow (\bar 1, 0)$,
$b \leftrightarrow (\bar 0, \bar 1)$, $c \leftrightarrow (\bar 1, \bar 1)$.

Huom.: $|G| = 4$ $\Rightarrow$ G on kommut..