III.2 Peruslaskutoimituksia

Olk. G (multipl.) ryhmä. Aiemmin on määr. potenssit a^n (monoidissa G), kun $a \in G$, $n \in \mathbb{N}$.
Lisäksi on tod., että $(ab)^{-1} = b^{-1}a^{-1}$, kun $a, b \in G$.
Induktio $\Rightarrow$ $(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} \cdots a_2^{-1} \cdot a_1^{-1}$, $a_1, \ldots, a_n \in G$.
Val. $a_1 = \ldots = a_n = a \in G$ $\Rightarrow$

$$(a^n)^{-1} = (a^{-1})^n \quad \forall n \in \mathbb{N} \qquad \text{(myös arvolla } n = 0\text{)}.$$

Määr. alkion $a \in G$ negat. potenssit:

$$a^{-n} = (a^{-1})^n = (a^n)^{-1}, \text{ kun } n \in \mathbb{N}.$$

Näin siis a^n on määr. ryhmässä G $\forall a \in G$, $\forall n \in \mathbb{Z}$.

Lause: Olk. $a, b \in G$.
i) $a^{m+n} = a^m \cdot a^n$, $a^{mn} = (a^m)^n$ $\forall m, n \in \mathbb{Z}$
ii) Jos $ab = ba$, niin $(ab)^n = a^n b^n$ $\forall n \in \mathbb{Z}$.

Tod.: i) on tod., kun $m \geq 0$, $n \geq 0$. Tämän lisäksi käsiteltävä eräitä muita tap.: Kun $m, n \in \mathbb{N}$, on ensim.
$(a^m)^{-n} = ((a^m)^n)^{-1} = (a^{mn})^{-1} = a^{-mn} = a^{m(-n)}$.
Kun $m, n \in \mathbb{N}$, $m = n + p \geq n$ $(p \in \mathbb{N})$ on
$a^m \cdot a^{-n} = a^{n+p} \cdot a^{-n} = a^{p+n} \cdot a^{-n} = a^p \cdot a^n \cdot a^{-n}$
$= a^p \cdot a^n \cdot (a^n)^{-1} = a^p = a^{m-n}$.

ii) Ensiksi induktio $\Rightarrow$ $ab^n = b^n a$ $\forall n \in \mathbb{N}$;
sitten induktio $\Rightarrow$ $(ab)^n = a^n b^n$ $\forall n \in \mathbb{N}$;
lopuksi $(ab)^{-n} = (ba)^{-n} = ((ba)^n)^{-1} = (b^n a^n)^{-1}$
$= (a^n)^{-1}(b^n)^{-1} = a^{-n} b^{-n}$ $\forall n \in \mathbb{N}$. □

Huom.: Addit. ryhmässä G pätevät vast. kaavat monikerroille; ensim. $(-n)a = n(-a) = -(na)$ $\forall n \in \mathbb{N}$, ja $n(a+b) = na + nb$ $\forall n \in \mathbb{Z}$, jos $a + b = b + a$ (merkinnässä na on $n \in \mathbb{Z}$, $a \in G$; yl. $n \notin G$).

Lause 2: G (multipl.) ryhmä, $a, b \in G$
$\Rightarrow$ yhtälöillä $ax = b$ ja $ya = b$ on 1-käs. ratkaisut $x, y \in G$, nim. $x = a^{-1}b$, $y = ba^{-1}$.

Tod.: olem.olo: $a(a^{-1}b) = (aa^{-1})b = 1\cdot b = b$,
$(ba^{-1})a = b(a^{-1}a) = b\cdot 1 = b$.

1-käs.: $ax = b = ax' \Rightarrow x = (a^{-1}a)x = a^{-1}(ax) =$
$= a^{-1}(ax') = (a^{-1}a)x' = x'$; vastaavasti
$ya = b = y'a \Rightarrow y = y'$. □

Ehk. ryhmässä G pätevät supistussäännöt $ax = ax' \Rightarrow x = x'$ ja $ya = y'a \Rightarrow y = y'$. Lisäksi Lause 2 $\Rightarrow$ kuvaukset $x \mapsto ax$ ja $y \mapsto ya$ ovat bijektioita $G \xrightarrow{\sim} G$. Siten äärell. ryhmän "kertotaulun" jok. vaaka- ja pystyrivillä esiintyy jokainen G:n alkio täsm. yhden kerran.

Esim. 1: Ol. $G = \{1, a, b\}$ multipl. ryhmä, $\#G = 3$,
1 = neutr. alkio

$\cdot$	1	a	b
1	1	a	b
a	a	b	1
b	b	1	a

$a\cdot a \in \{1, b\}$, $a\cdot b \in \{1, b\}$.
$a\cdot b = b = 1\cdot b \Rightarrow a = 1$, RR;
siis täytyy olla $a\cdot b = 1$, $a\cdot a = b$.
2. pystyrivi $\Rightarrow b\cdot a = 1$. Vielä $b\cdot b = a$.
$\therefore G = \{1, a, a^2\}$.
Tällainen ryhmä on olem., nimittäin $(\mathbb{Z}_3, +)$.

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

Lause 4: (Multipl.) ryhmien G_1 ja G_2 kart.tulosta $G_1 \times G_2$ tulee ryhmä, kun määr.

$$(a_1, a_2)\cdot(b_1, b_2) = (a_1 \cdot b_1,\ a_2 \cdot b_2) \qquad (a_i, b_i \in G_i)$$

(G_1:n laskut.) (G_2:n laskutoim.)

(Vastaavan pätee myös ryhmien $G_1, \dots, G_n$ kart.tulolle.)

Tod. on helppo. Ehk. $1_{G_1\times G_2} = (1_{G_1}, 1_{G_2})$ ja $(a_1, a_2)^{-1} = (a_1^{-1}, a_2^{-1})$. □

Esim. 7: $\mathbb{R}^n = \mathbb{R}\times\dots\times\mathbb{R}$ $(n \in \mathbb{N}_+)$ on Abelin ryhmä, kun määr. $(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1+y_1, \dots, x_n+y_n)$.

Määr.: (Multipl.) ryhmän G osajoukko H on G:n aliryhmä, merk. $H \leq G$, jos

i) H on valeaa G:n laskutoim. suhteen,
tls. $a, b \in H \Rightarrow ab \in H$,
ii) $1_G \in H$, ja
iii) H on valeaa G:n operation $x \mapsto x^{-1}$ suhteen,
tls. $a \in H \Rightarrow a^{-1} \in H$.

(jos G on additiivinen ryhmä, nämä ehdot saavat muodon
i) $a, b \in H \Rightarrow a+b \in H$,
ii) $0_G \in H$,
iii) $a \in H \Rightarrow -a \in H$.)

jos $H \leq G$, mutta $H \neq G$, merk. $H < G$ (aito alіryhmä).

Huom.: Ol. $H \leq G$. i) $\Rightarrow$ G:n laskutoim. $(x,y) \mapsto xy$ $(x,y \in G)$ aiheuttaa vast. määr. H:lla (indusoitu) laskutoim. asettamalla $(a,b) \mapsto ab$ $\forall a, b \in H$. Tällöin H:sta tulee ryhmä: $x(yz) = (xy)z$ $\forall x,y,z \in G \Rightarrow$ $a(bc) = (ab)c$ $\forall a,b,c \in H$; $1_G \in H$ (ii) ja $1_G \cdot x = x = x \cdot 1_G$ $\forall x \in G \Rightarrow 1_G \cdot a = a = a \cdot 1_G$ $\forall a \in H$; $a \in H \Rightarrow \exists a^{-1} \in G$ ja iii) $\Rightarrow a^{-1} \in H$ koska a:n käänt. alkiot H:ssa.

Ellei toisin mainita, alіryhmä $H \leq G$ varustetaan aina tällä ryhmärakenteella.

Esim. a) $\{1_G\} \leq G$, $G \leq G$ triviaalit alіryhmät.
b) $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$ (additiiv.);
$\{1,-1\} < \mathbb{Q}\setminus\{0\} < \mathbb{R}\setminus\{0\} < \mathbb{C}\setminus\{0\}$ (multipl.).
c) $n \in \mathbb{N}) \Rightarrow n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} \leq \mathbb{Z}$ (erit. $0\mathbb{Z} = \{0\}$).
$(nk_1 + nk_2 = n(k_1+k_2)$; $0 = n \cdot 0$; $-(nk) = n \cdot (-k)$.)

d) Ol. Σ joukko ja $x_0 \in \Sigma$.
V. $H = \{f \in S_\Sigma \mid f(x_0) = x_0\}$ on S_Σ:n alіryhmä.
T. i) $f, g \in H \Rightarrow (f \circ g)(x_0) = f(g(x_0)) = f(x_0) = x_0$
$\Rightarrow f \circ g \in H$;
ii) $id_\Sigma(x_0) = x_0 \Rightarrow id_\Sigma \in H$;
iii) $f \in H \Rightarrow x_0 = f(x_0) \Rightarrow f^{-1}(x_0) = f^{-1}(f(x_0)) = x_0$
$\Rightarrow f^{-1} \in H$. □

e) $SL_2(\mathbb{R}) = \{A \in GL_2(\mathbb{R}) \mid \det(A) = 1\} \leq GL_2(\mathbb{R})$
$(A, B \in SL_2(\mathbb{R}) \Rightarrow \det(AB) = \det(A) \cdot \det(B) = 1 \cdot 1 = 1$
$\Rightarrow AB \in SL_2(\mathbb{R})$;

$\det(I_2) = \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} = 1 \Rightarrow I_2 \in SL_2(\mathbb{R})$;
$A \in SL_2(\mathbb{R}) \Rightarrow \det(A^{-1}) = 1/\det(A) = 1/1 = 1$
$\Rightarrow A^{-1} \in SL_2(\mathbb{R})$.)

f) Kun $\theta \in \mathbb{R}$, merk. $R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \in GL_2(\mathbb{R})$;
vastaava lin. kuvaus $\mathbb{R}^2 \to \mathbb{R}^2$ on
$(x_1, x_2) \mapsto (x_1\cos\theta - x_2\sin\theta,\ x_1\sin\theta + x_2\cos\theta)$,
kierto origon ympäri vastapäivään kulmalla θ.
Nyt $SO_2(\mathbb{R}) = \{R_\theta \mid \theta \in \mathbb{R}\} \leq GL_2(\mathbb{R})$
($R_{\theta_1} \cdot R_{\theta_2} = R_{\theta_1+\theta_2}$; $I_2 = R_0$; $(R_\theta)^{-1} = R_{-\theta}$).

Itse asiassa $SO_2(\mathbb{R}) < SL_2(\mathbb{R}) < GL_2(\mathbb{R})$.

Huom.: $H \leq G$, $a_1, \dots, a_k, a \in H$
$\Rightarrow a_1 \cdots a_k \in H$ ja $a^n \in H$ $\forall n \in \mathbb{Z}$.

Lause 3 (Alityhmäkriteeri): Ol. G ryhmä, $H \subset G$ epätyhjä.
Silloin $H \leq G \iff H \neq \emptyset$ ja $ab^{-1} \in H$ aina, kun $a, b \in H$.

Tod.: $\Rightarrow$. Ol. $H \leq G$. ii) $\Rightarrow 1_G \in H \Rightarrow H \neq \emptyset$.
Ol. $a, b \in H$. iii) $\Rightarrow$ myös $b^{-1} \in H$; i) $\Rightarrow ab^{-1} \in H$.
$\Leftarrow$: Ol. H tod. aik. pred. ehdot. Tod. alir. ehdot i)–iii).
ii) $H \neq \emptyset \Rightarrow \exists a \in H$; ol. $\Rightarrow 1_G = a \cdot a^{-1} \in H$.
iii) Olk. $a \in H$. Tiedetään jo, että $1_G \in H$;
ol. $\Rightarrow a^{-1} = 1_G \cdot a^{-1} \in H$.
i) Olk. $a, b \in H$. Yo. nojalla myös $b^{-1} \in H$, joten
$ab = a \cdot (b^{-1})^{-1} \in H$. □

Jos G on äärellinen, riittää (käytännössä) vähempikin:

Lause 5: Ol. G äärell. ryhmä ja $H \subset G$ epätyhjä.
Jos $H \neq \emptyset$ ja $ab \in H$ aina, kun $a, b \in H$, niin $H \leq G$.

Tod.: Ol. $\Rightarrow$ alir. ehto i) on voimassa.
Olk. $a \in H$ ($H \neq \emptyset \Rightarrow$ tällaista alkiota on). Ol. $\Rightarrow$
$a^n = a \cdots a \in H$ kaikilla $n = 1, 2, 3, \dots$.
G äärell. $\Rightarrow$ a^n:t eivät kaikki ole alkioita
$\Rightarrow \exists k, l \in \mathbb{N}_+$, $k > l$, s.e. $a^k = a^l$.
Tällöin $a^{k-l} \cdot a^l = a^l \Rightarrow 1_G = a^{k-l} \in H$ $(k-l \in \mathbb{N}_+)$

ja $a \cdot a^{k-l-1} = a^{k-l-1} \cdot a = 1_G \Rightarrow a^{-1} = a^{k-l-1} \in H$. □

Alirymien leikkaus ainä alirymä:

Lemma: $\mathcal{A} \neq \emptyset$ kokoelma G:n alirymiä ($\forall H \leq G \ \forall H \in \mathcal{A}$)
$\Rightarrow \bigcap \mathcal{A} = \{x \in G \mid x \in H \ \forall H \in \mathcal{A}\}$ on G:n alirymä.

Tod.: $1_G \in H \ \forall H \in \mathcal{A}$ (H alir.) $\Rightarrow 1_G \in \bigcap \mathcal{A} \Rightarrow \bigcap \mathcal{A} \neq \emptyset$.
$a, b \in \bigcap \mathcal{A} \Rightarrow a, b \in H \ \forall H \in \mathcal{A} \Rightarrow ab^{-1} \in H \ \forall H \in \mathcal{A}$
(H alir.) $\Rightarrow ab^{-1} \in \bigcap \mathcal{A}$.
Alirymäkrit. $\Rightarrow \bigcap \mathcal{A} \leq G$. □

III.3 Ryhmien virittäjät

Ol. G (multipl.) ryhmä ja $S \subset G$ osajoukko. Merk.
$\mathcal{A}_S = \{H \leq G \mid S \subset H\}$. Ainakin $G \in \mathcal{A}_S \Rightarrow \mathcal{A}_S \neq \emptyset$.
Määr.

$$\langle S \rangle = \bigcap \mathcal{A}_S \quad \left(= \bigcap_{H \in \mathcal{A}_S} H \right).$$

Ed. lemma $\Rightarrow \langle S \rangle \leq G$; $S \subset H \ \forall H \in \mathcal{A}_S \Rightarrow S \subset \langle S \rangle$;
jos $H_0 \in \mathcal{A}_S$, niin $\langle S \rangle = \bigcap_{H \in \mathcal{A}_S} H \subset H_0$.

$\therefore \langle S \rangle \in \mathcal{A}_S$ on $\mathcal{A}_S$:n pienin alkio alkuk. järjestyksen $\subset$ suhteen, ts. pienin G:n alirymä, jotka sisältää kaikki S:n alkiot.

Sanomme, että $\langle S \rangle$ on osajoukon $S \subset G$ virittämä G:n alirymä. Jos $S = \{a_1, \ldots, a_m\}$ on äärell., merk. $\langle S \rangle = \langle a_1, \ldots, a_m \rangle$.

Esim.: a) $\langle \emptyset \rangle = \langle 1_G \rangle = \{1_G\}$; $H \leq G \Rightarrow \langle H \rangle = H$.

b) Ol. $a \in G$.
V. $\langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}$.
T. Pot. laskusäännöt $\Rightarrow \{a^m \mid m \in \mathbb{Z}\} \leq G$; $a = a^1 \in \{a^m \mid m \in \mathbb{Z}\}$.
$\langle a \rangle$ pienin täll. ominaisuuksia $\Rightarrow \langle a \rangle \subset \{a^m \mid m \in \mathbb{Z}\}$.
Toisaalta $\langle a \rangle$ alir. ja $a \in \langle a \rangle \Rightarrow a^m \in \langle a \rangle \ \forall m \in \mathbb{Z}$
$\Rightarrow \{a^m \mid m \in \mathbb{Z}\} \subset \langle a \rangle$.

Yleisemmin:

Lause 6: $S \subset G \Rightarrow \langle S \rangle$:n alkiot ovat 1_G sekä kaikki tulot $a_1^{e_1} \cdot a_2^{e_2} \cdot \ldots \cdot a_m^{e_m}$, $m \in \mathbb{N}_+$, missä $a_k \in S$ ja $e_k \in \{1, -1\}$ $\forall k \in \{1, \ldots, m\}$.

(jos G on addit., $\langle S \rangle$:n alkiot ovat 0_G sekä kaikki summat $\pm a_1 \pm a_2 \pm \ldots \pm a_m$, $a_k \in S$.)

Tod.: Selvästi ko. alkiot muod. aliryhmän H (erim. $(a_1^{e_1} \cdot a_2^{e_2} \cdot \ldots \cdot a_m^{e_m})^{-1} = a_m^{-e_m} \cdot \ldots \cdot a_2^{-e_2} \cdot a_1^{-e_1}$ samaa tyyppiä), ja $S \subset H$. $\langle S \rangle$ pienin täll. alir. $\Rightarrow \langle S \rangle \subset H$.
Toisaalta $\langle S \rangle$ alir. ja $a \in \langle S \rangle$ $\forall a \in S \Rightarrow$ kaikki H:n alkiot $\in \langle S \rangle$, ts. $H \subset \langle S \rangle$. □

Huom.: jos G on äärell., niin Lauseen 5 avulla nähdään, että $\langle S \rangle = \{1_G\} \cup \{a_1 \cdot \ldots \cdot a_m \mid m \in \mathbb{N}_+, a_k \in S \ \forall k\}$.

Esim.: a) $\mathbb{Z} = \{m \mid m \in \mathbb{Z}\} = \{m \cdot 1 \mid m \in \mathbb{Z}\} = \langle 1 \rangle \ (= \langle -1 \rangle)$.
b) $\mathbb{Z}_n = \{\overline{m} \mid m \in \mathbb{Z}\} = \{m \cdot \overline{1} \mid m \in \mathbb{Z}\} = \langle \overline{1} \rangle$ $(n \in \mathbb{N}_+)$
$(= \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\})$.
c) olk. $P \subset \mathbb{N}$ alkulukujen joukko. Ryhmässä $(\mathbb{R} \setminus \{0\}, \cdot)$ on $\langle P \rangle = \mathbb{Q}^+ = \{q \in \mathbb{Q} \mid q > 0\}$ (olkoinkin alkulukujen tulojen osamäärät).

$\mathbb{Z}$ ja $\mathbb{Z}_n$ ovat (addit.) sykliisiä ryhmiä:

Määr.: Ryhmä G on sykliinen, jos se on yhden alkionsa virittämä, ts. $\exists a \in G$ s.e. $G = \langle a \rangle$.

Lause 7: Olkoon G (multipl.) sykliinen ryhmä, $G = \langle a \rangle$, $a \in G$. Silloin $G = \{a^m \mid m \in \mathbb{Z}\}$, ja
jollei G on ääretön, jolloin a^m:t ovat kaikki eri alkioita (eli $a^m \neq 1_G$ $\forall m \neq 0$)
tai G on äärellinen, $|G| = n \in \mathbb{N}_+$, jolloin $G = \{1_G, a, a^2, \ldots, a^{n-1}\}$, $a^n = 1_G$ ja $1_G, a, \ldots, a^{n-1}$ ovat kaikki eri alkioita.

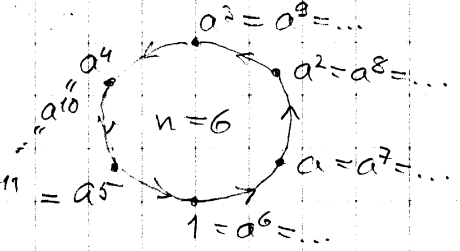
Tod.: $G = \langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}$ todettu aik.
jos: $a^m \neq a^{m'}$ aina, kun $m, m' \in \mathbb{Z}$, $m \neq m'$, ovat selvästi. Muuten $\exists m, m' \in \mathbb{Z}$ s.e. $m > m'$ ja $a^m = a^{m'}$
$\Rightarrow m - m' > 0$ ja $a^{m-m'} = 1_G$.
$\Rightarrow A = \{k \in \mathbb{N}_+ \mid a^k = 1_G\} \neq \emptyset$.

Merk. $n = \min A$, sillöin eri. $n \in \mathbb{N}_+$ ja $a^n = 1_G$.
Kun $m \in \mathbb{Z}$, jakoyht. $\Rightarrow$ $\exists\, q, r \in \mathbb{Z}$ s.e. $0 \le r < n$ ja $m = qn + r$ $\Rightarrow$

$$a^m = a^{qn+r} = (a^n)^q \cdot a^r = 1_G^q \cdot a^r = a^r .$$

Siten $G = \{a^m \mid m \in \mathbb{Z}\} = \{1, a, a^2, \dots, a^{n-1}\}$.
$1, a, \dots, a^{n-1}$ ovat eri alkioita (joten $|G| = n$), sillä $0 \le r < s < n$, $a^r = a^s$ $\Rightarrow$ $0 < s - r < n$, $a^{s-r} = 1_G$
$\Rightarrow$ $s - r \in A$, vaikka $s - r < n = \min A$, RR. □

Huom.: $G = \langle a \rangle$ syklinen, $|G| = n$
$\Rightarrow$ G:n alkiot muodostavat "n-syklisen".



Esim. 7: $\mathbb{Z}_5^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\} = \langle \bar{2} \rangle$ (multipl.),
sillä $\bar{2}^2 = \bar{4}$, $\bar{2}^3 = \bar{8} = \bar{3}$, $\bar{2}^4 = \bar{16} = \bar{1}$.
Myös $\mathbb{Z}_5^* = \langle \bar{3} \rangle$.

Määr.: Ryhmän G alkion $a \in G$ kertaluku on

$$\operatorname{ord}(a) = |a| = |\langle a \rangle| \in \mathbb{N}_+ \cup \{\infty\} .$$

Siis joko $\operatorname{ord}(a) = \infty$ tai $\operatorname{ord}(a) = \min\{n \in \mathbb{N}_+ \mid a^n = 1\}$.
Erityisesti $\operatorname{ord}(a) = 1 \iff a = 1_G$.

Esim. 8: a) $(\mathbb{R} \setminus \{0\}, \cdot)$: sill $\operatorname{ord}(1) = 1$, $\operatorname{ord}(-1) = 2$
ja $\operatorname{ord}(a) = \infty$, kun $a \neq \pm 1$.

b) Tark. multipl. ryhmää $\mathbb{Z}_{21}^*$.
$\bar{20} = (\bar{-1}) \neq \bar{1}$, $\bar{20}^2 = \bar{(-1)^2} = \bar{1}$ $\Rightarrow$ $\operatorname{ord}(\bar{20}) = 2$;
$\bar{2} \neq \bar{1}$, $\bar{2}^2 = \bar{4} \neq \bar{1}$, $\bar{2}^3 = \bar{8} \neq \bar{1}$, $\bar{2}^4 = \bar{16} \neq \bar{1}$,
$\bar{2}^5 = \bar{32} = \bar{11} \neq \bar{1}$, $\bar{2}^6 = \bar{2} \cdot \bar{11} = \bar{22} = \bar{1}$
$\Rightarrow$ $\operatorname{ord}(\bar{2}) = 6$.

II.4 Homomorfismit ja isomorfismit

Määr.: Olk. G ja G' (multipl.) ryhmiä. Kuvaus $f: G \to G'$ on (ryhmä-) homomorfismi, jos

$$f(ab) = f(a) \cdot f(b) \quad \forall a, b \in G .$$