Ryhmät 20.4.2020

$G$ ryhmä, $H \leq G$, $g \in G$

$gH = \{gh : h \in H\}$ $g$:n vasen sivuluokka

$Hg = \{hg : h \in H\}$. oikea — " —

Jos $g_1 H \cap g_2 H$, niin $\underline{g_1 H = g_2 H}$ $\Leftrightarrow$ $g_2^{-1} g_1 \in H$.

$G = \bigcup_{g \in G} gH = \bigsqcup_{gH \in G/H} gH$ – erillinen yhdiste.

$G/H$ vas. sivuluokkien joukko.

Prop. • Joukot $H$, $gH$, $Hg$ ovat yhtä mahtavia.

• Joukot $G/H$ ja $H\backslash G$ ovat yhtä mahtavia. $\longrightarrow$ Aliryhmän $H$ indeksi

$H\backslash G$: oikeat sivuluokat

$[G:H] = \#(G/H)$

$= \#(H\backslash G)$

1

**Lagrangen lause**. Jos $G$ on äärellinen ryhmä, niin $\boxed{\#G = [G:H]\,\#H}$

**Tod**. $G = \bigsqcup_{gH \in G/H} gH$ — kaikissa sama määrä alkioita $\#gH = \#H$

$$\Rightarrow \#G = \underbrace{\#(G/H)}_{[G:H]}\,\#H . \qquad \square$$

---

**Seuraus**: Jos $H \leq G$, niin $\#H \mid \#G$.

$\Rightarrow$ Jos $\#G$ on alkuluku, niin, $G$:n ainoat aliryhmät ovat $\{e\}$ ja $G$.

**Seuraus**. Jos $g \in G$ ja $G$ on äärellinen, niin $\boxed{\operatorname{ord} g \mid \#G}$.

**Tod**. $\operatorname{ord} g = \#\langle g \rangle$, $\langle g \rangle \leq G$. ed. tulos $\Rightarrow \operatorname{ord} g = \#\langle g\rangle \mid \#G$

Seuraus: Jos $\#G = p$ on alkuluku, niin $G$ on syklinen ryhmä.

Tod. $p \geq 2 \Rightarrow \exists\, g \in G - \{e\}$. $\{e\} \neq \langle g \rangle = G$, koska $G$:n aiheat aliryhmät ovat $\{e\}$ ja $G$. $\square$

Prop. 11.15 Olk. $G$ äärellinen ryhmä, $g \in G$. $g^{\#G} = e$.

Tod. Olk. $g \in G - \{e\}$. Tällöin $\operatorname{ord} g \geq 2$.

$\underbrace{\operatorname{ord} g \mid \#G}$

$\Rightarrow \exists k \in \mathbb{N}$:

$\#G = k \operatorname{ord} g$

$$g^{\#G} = g^{k \operatorname{ord} g} = (\underbrace{g^{\operatorname{ord} g}}_{e})^{k} = e. \quad \square$$

Seuraus (Fermat'n pieni lause) Jos $p$ on alkuluku, niin $a^p \equiv a \mod p$ kaikilla $a \in \mathbb{Z}$

Tod. $\#\left((\mathbb{Z}/p\mathbb{Z})^\times\right) = p-1$. Olk. $a \in \mathbb{Z} - p\mathbb{Z}$. Prop 11.15 $\Rightarrow \underbrace{(a+p\mathbb{Z})^{p-1}}_{a^{p-1}+p\mathbb{Z}\,=} = 1 + p\mathbb{Z}$

$$\Rightarrow \quad a^p + p\mathbb{Z} = a + p\mathbb{Z} \iff a^p \equiv a \mod p. \qquad \square$$

(Nollalle pätee $0^p = 0 \equiv 0 \mod p$.
Jos $a \equiv 0 \mod p$, niin $a^p \equiv 0^p = 0 \equiv 0 \mod p$ )

Esim. 11.11 $\#S_3 = 6$. Lagrange: Jos $H \leq S_3$, niin $\#H \in \{1, 2, 3, 6\}$.

$\#\langle(12)\rangle = 2$, $\#\langle(123)\rangle = 3$.

$$\begin{tikzcd}
 & & S_3 \arrow[dll, dash] \arrow[ddl, dash] \arrow[dd, dash] \arrow[ddr, dash] & \\
\langle(132)\rangle = \langle(123)\rangle \arrow[ddrr, dash] & & & \\
 & \langle(12)\rangle \arrow[dr, dash] & \langle(23)\rangle \arrow[d, dash] & \langle(13)\rangle \arrow[dl, dash] \\
 & & \{e\} &
\end{tikzcd}$$

$\boxed{S_3\text{:n aliryhmäkaavio}}$

<u>Esim.</u> $A_4$ = parilliset permutaatiot ryhmässä $S_4$

$\underline{(12)(34)}$, $(123) = \underline{(13)(12)} \in A_4$; $(123)^2 = (132) \in A_4$

$\underbrace{(123)}\cancel{(12)}(34) = \underline{\underline{(134)}} \in A_4$ $\quad (134)^2 = (143)$ $\quad \# A_4 = \frac{4!}{2} = 12$

$(13)\cancel{(12)}$

Os. että $A_4 = \langle \{(12)(34), (123)\} \rangle$.

Lagrangen lause: Jos $H \leq A_4$, niin $\# H \in \{1, 2, 3, 4, 6, 12\}$

Etsitään ryhmän $\langle (12)(34), (123) \rangle$ alkioita: id, $(12)(34)$, $(123)$, $(132)$, $(134)$, $(143)$, $(12)(34)(123) = (243)$. Siis $\# \langle (12)(34), (123) \rangle \geq 7$,

joten $\# \underbrace{\langle (12)(34), (123) \rangle}_{= A_4} = 12 = \# A_4$.

# 12 Normaalit aliryhmät (ja tekijäryhmät)

**Määr.** $H \le G$ on normaali aliryhmä, jos $gH = Hg \ \forall g \in G$.

$\rightsquigarrow$ $H \trianglelefteq G$. Jos $H < G$ ja $H \trianglelefteq G$, merk. $H \triangleleft G$.

**Esim.** • Jos $G$ on komm., niin kaikki sen alir. ovat normaaleja.

(Lemma 11.2) $$gH = \{\underbrace{gh}_{hg} : h \in H\} = Hg.$$

• Esim. 11.3: $S_3$'in aliryhmä

$H = \langle (12) \rangle$ ei ole normaali: $(123)H \neq H(123)$.

**Prop. 12.3** Jos $[G:H] = 2$, niin $H \triangleleft G$.

**Tod.** Vas. sivuluokat: $gH = H \iff g \in H$, $gH = G - H \iff g \in G - H$.

Oikeat sivuluokat: $Hg = H \iff g \in H$, $Hg = G - H \iff g \in G - H$. $\square$

Esim. $\underbrace{\#\langle(123)\rangle}_{< S_3} = 3$ , $\#S_3 = 6 \overset{\text{Lagr.}}{\Longrightarrow} [S_3 : \langle(123)\rangle] = 2$

Prop. 12.3 $\Longrightarrow \langle(123)\rangle \trianglelefteq S_3$

---

**Prop. 12.5** $H \leq G$ on normaali $\Leftrightarrow$ $ghg^{-1} \in H$ $\forall h \in H$ ja $g \in G$.

Tod. Ol. $H \trianglelefteq G$. Olk. $g \in G$, $h \in H$.

$\Longrightarrow gH = Hg \Longrightarrow gh = h'g$ jollain $h' \in H$.

$gh \in gH$

$\Rightarrow ghg^{-1} = h' \in H$.

Ol. $ghg^{-1} \in H$ $\forall h \in H$ $\forall g \in G$.
Olk. $g \in G$. Os. että $gH = Hg$. Olk. $h \in H$. $\Longrightarrow gH \subset Hg$.

$gh = (ghg^{-1})g$, $gh \in gH$, $(ghg^{-1})g \in Hg$, $ghg^{-1} \in H$

Vast. os. $Hg \subset gH$. $\square$

7

**Prop. 12.7** $\phi : G \to G'$ ryhmähomom.

1) $H \trianglelefteq G \Rightarrow \phi(H) \trianglelefteq \phi(G)$

2) $H' \trianglelefteq G' \Rightarrow \phi^{-1}(H') \trianglelefteq G$.

**Tod.** 1) Prop. 9.11 $\Rightarrow \phi(H) \leq \phi(G)$.

Olk $\underset{\phi(a),\ a \in H}{\overset{\|}{a'}} \in \phi(H)$, $\underset{\phi(g),\ g \in G}{\overset{\|}{g'}} \in \phi(G)$.

$H \trianglelefteq G$

$$\underline{\underline{g'a'(g')^{-1}}} = \phi(g)\,\phi(a)\,\underbrace{\phi(g)^{-1}}_{\phi(g^{-1})} = \phi(\overbrace{g a g^{-1}}^{\in H}) \in \phi(H). \checkmark$$

Prop. 12.5 $\Rightarrow \phi(H) \trianglelefteq \phi(G)$.

$\square$

2) Harj.