Ryhmät 13.4.2021

$S_n = \mathrm{Perm}(\{1, \dots, n\})$

$(a_1\, a_2 \cdots a_k)$ k-sykli

$a_i \mapsto a_{i+1} \mod k$

$a_k \mapsto a_1$

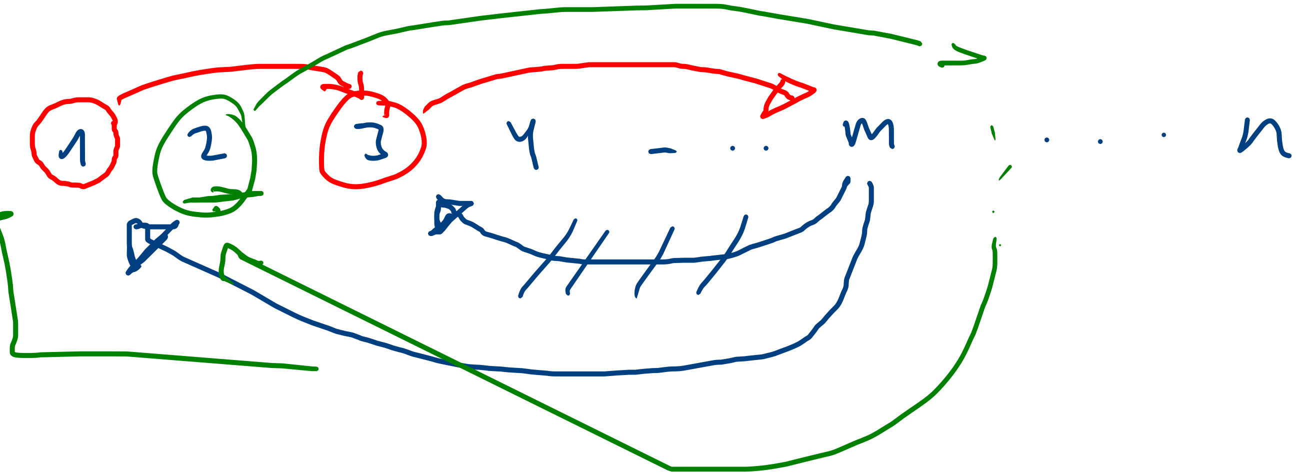
$(a_1 a_2)$ 2-sykli, vaihto

Prop. 10.17 Jos $\tau \in S_n \setminus \{id\}$, niin τ on erillisten syklien tulo.

$\tau = (a_1 \cdots a_k)(a_{k+1} \cdots a_{k+l}) \cdots (a_m \cdots a_{m+l})$

$a_1, \dots, a_{m+l} \in \{1, \dots, n\}$ eri alkioita.

Tod.



Voidaan olettaa, että $\tau(k) \neq k$ $\forall k \in \{1, \dots, n\}$.

Induktio. Jos $n = 2$, niin $\# S_n = 2$: $\tau = id$ OK.
$\tau = (12)$ sykli OK.

Ol. että väite pätee ryhmässä S_k kaikilla $k \leq n-1$.

Olk. $\tau \in S_n$. Jos τ on sykli, niin OK.

(1) Ol. että τ ei ole sykli. Tällöin $\Theta(1) = \{\tau^m(1) : m \geq 0\} \neq \{1, \dots, n\}$.

$\tau|_{O(1)}$ on sykli: $O(1)$ on äärellinen $\Rightarrow \exists\, r, q \in \mathbb{N}: r \neq q$ voe $q < r$.

$$\tau^r(1) = \tau^q(1) = \tau(\tau^{q-1}(1))$$
$$\| $$
$$\tau(\tau^{r-1}(1))$$

ol. r, q $\boxed{\text{pienimmät mahd}}$ ja $\boxed{q \neq 0}$

τ bijektio $\Rightarrow \tau^{r-1} = \tau^{q-1}$ ristiriita $\Rightarrow$ $\underline{q = 0}$

Siis on $r \in \mathbb{N}, r > 0$ s.e. $\tau^r(1) = 1$.

Ind. ol: $\tau|_{\{1,\dots,n\} - O(1)}$ on erillisten syklien tulo

$$\tau = \tau|_{O(1)}\, \tau|_{\{1,\dots,n\} - O(1)}. \quad \square$$

Seuraus. Jos $\tau \in S_n - \{id\}$ niin τ on alkeis vaihtojen tulo.

② Tod. Prop. 10.6 $\Rightarrow$ syklit ovat alkeis vaihtojen tuloja.

Seuraus Vaihdot virittävät ryhmän S_n.

Cayleyn lause. Olkoon G ryhmä, $\#G = n$. Tällöin ryhmällä S_n $\cong \mathrm{Perm}(G)$ on aliryhmä, joka on isomorfinen ryhmän G kanssa.

Huom. $\# S_n = n!$

$r_g(h) = hg$

r_g!

Määr. Ok. G ryhmä, $g \in G$. Kuvaus $l_g : G \to G$, $l_g(h) = gh$, on ~~vasen~~ oikea siirto.

Lemma Vasen siirto on bijektio.

Tod. Jos $\underset{\overset{\|}{gh}}{l_g(h)} = l_g(k) = gk$, niin supistussääntö $\Rightarrow$ $h = k$. $\square$

③

Määr. $\rho : G \to \mathrm{Perm}(G)$, $\rho(g) = l_g$.
$g \in G$, $l_g \in \mathrm{Perm}(G)$ Lemma.

Lemma. ρ on inj. homomorfismi.

Prop. $G \cong \rho(G) \leq \mathrm{Perm}(G)$.

Tod: Kuvaus $\rho : G \to \rho(G)$ on isomorfismi.

$\boxed{\text{Cayleyn lause seuraa tästä.}}$

(*) Olk. $g \in \ker \rho$.
Tällöin $l_g = id$, joten $\forall x \in G$ pätee

$$gx = l_g(x) = x = ex$$

supistussääntö: $\underline{g = e}$.

Prop. 9.14: ρ on injektio.

Lemman tod.

$$\rho(gh)(x) = l_{gh}(x) = (gh)x \overset{\text{assos}}{=} g\underbrace{(hx)}_{l_h(x)} = l_g(l_h(x)) = (l_g \circ l_h)(x)$$

$g, h, x \in G$ $\qquad \forall x \in G$

$$= (\rho(g) \circ \rho(h))(x)$$

$\Rightarrow \rho(gh) = \rho(g) \circ \rho(h)$, joten ρ on homomorfismi. (*)

Määr. $\sigma \in S_n$ on $\begin{cases} \text{parillinen} \\ \text{pariton} \end{cases}$ permutaatio, jos se on tulo $\begin{cases} \text{parillisesta} \\ \text{parittomasta} \end{cases}$ määrästä vaihtoja.

Permutaation $\overset{\sigma}{\vee}$ **merkki** on $\varepsilon(\sigma) = \begin{cases} -1, & \text{jos } \sigma \text{ on pariton} \\ +1, & \text{jos } \sigma \text{ on parillinen.} \end{cases}$

Tavoite: OS. että $\varepsilon : S_n \to \{-1, 1\}$ on hyvin määritelty.

Esim. $id \in S_n$ on parillinen: $id = (12)(12)$.

$(V,+)$ additiivinen ryhmä (yleensä $V = \mathbb{Z}$)

$X \neq \emptyset$

Määr. Kuvaus $f : X^n \to V$ on **antisymmetrinen**, jos kaikille alkeisvaihdoille $\tau \in S_n$ pätee

$$f(x_{\tau(1)}, x_{\tau(2)}, \dots, x_{\tau(n)}) = -f(x).$$

Lemma. $f : \mathbb{Z}^n \to \mathbb{Z}$, $f(x) = \prod_{1 \le i < j \le n} (x_i - x_j)$, on antisymmetrinen.

5 $\Big(n = 3,\quad f(x) = \overset{(x_2 - x_1)}{(x_1 - x_2)}\, \overset{(x_2 - x_3)}{(x_1 - x_3)}\, \overset{(x_1 - x_3)}{(x_2 - x_3)} \qquad (12),\ (23)\Big)$

Prop. 10.14. $f: X^n \to V$ antisymm, $\sigma \in S_n$ r alkeisvaihdon tulo.

$$\Rightarrow f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}) = (-1)^r f(x)$$

Tod. $\sigma = \tau \circ \omega$, missä τ alkeisvaihto
ω $r-1$ alkeisvaihdon tulo

$$f(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = f(x_{\tau\omega(1)}, \dots, x_{\tau\omega(n)}) = (-1)\underbrace{f(x_{\omega(1)}, \dots, x_{\omega(n)})}$$

$$= (-1)^{r-1} f(x) \quad \square$$

Prop. 10.16. ε on hyvin määritelty.

Tod. Jos σ on r alkeisvaihdon tulo
ja s — " —

$(-1)^s f(x)$
$\|$

ja $f: \mathbb{Z}^n \to \mathbb{Z}$ on antisymm. niin Prop 10.14: $f(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = (-1)^r f(x)$

6 $\Rightarrow (-1)^s = (-1)^r \Rightarrow s \equiv r \mod 2.$ P. 10.6. $\square$

Lause 10.17. Permutaation merkki $\varepsilon : S_n \to (\{-1,1\}, \cdot)$ on ainoa homomorfismi s.e. $\varepsilon(b) = -1$ kaikille vaihdoille $b \in S_n$.

$\{-1,1\} \cong \mathbb{Z}/2\mathbb{Z}$

Tod. Olk. $b_1, b_2 \in S_n$. Ol. että b_1 on r vaihdon tulo $\Rightarrow \varepsilon(b_1) = (-1)^r$
b_2 on s -"- . $\varepsilon(b_2) = (-1)^s$

Tällöin $b_1 b_2$ on $r+s$ vaihdon tulo.

$\Rightarrow \varepsilon(b_1 b_2) = (-1)^{r+s} = (-1)^r (-1)^s = \varepsilon(b_1)\varepsilon(b_2)$. $\Rightarrow \varepsilon$ homom.

Jos b on vaihto, niin $\varepsilon(b) = -1$ ok.
Vaihdot virittävät ryhmän S_n } Prop. 9.20 $\Rightarrow \varepsilon$ on ainoa homom. jolla on tämä omin. $\square$

Määr. $A_n = \ker(\varepsilon : S_n \to \{-1,1\}) < S_n$ on alternoiva ryhmä.

Lemma $\# A_n = \dfrac{\# S_n}{2} = \dfrac{n!}{2}$.

Tod. Olk. $\tau \in S_n$ alkeisvaihto. $\ell_\tau : A_n \to S_n$ on inj ja $\ell_\tau(A_n) \cap A_n = \emptyset$
$S_n = A_n \cup \ell_\tau(A_n)$. $\square$

Esim. $(1\,2\,3) = (1\,3)(1\,2)$ parillinen $\Rightarrow (1\,2\,3) \in A_n \;\; \forall n \geq 3$.

$(1\,2\,3\,4) = (1\,4)(1\,2\,3) = (1\,4)(1\,3)(1\,2)$ pariton $\Rightarrow (1\,2\,3\,4) \in S_n - A_n \;\; \forall n \geq 4$.