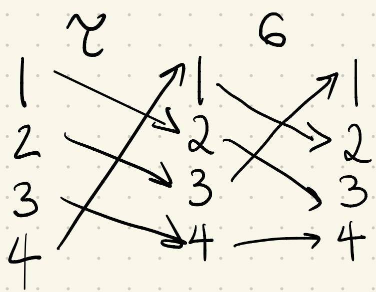
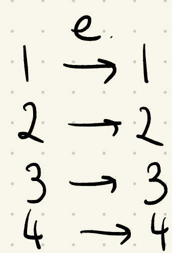
Permutations § 8 Fraleigh

Def 8.3 A permutation of a set A is a function $\sigma : A \to A$ that is bijective.

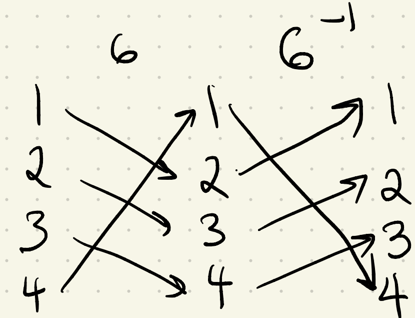
*see historical note pg 77

Ex. $A = \{1,2,3,4\}$



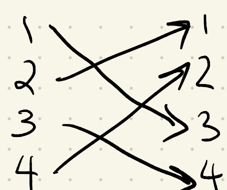


$\sigma \circ e = e \circ \sigma = \sigma$
$\forall \sigma : A \to A$ **G2**



G3 $\sigma^{-1} \circ \sigma = e = \sigma \circ \sigma^{-1}$

$\sigma \circ \tau$



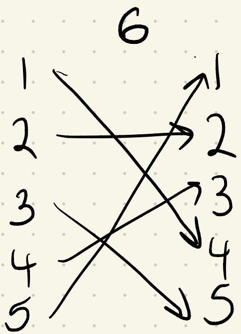
G1 Function composition is associative

$\rho \circ (\sigma \circ \tau) = (\rho \circ \sigma) \circ \tau$.

see Section 2 Fraleigh.

Thm 8.5 Let $A \neq \emptyset$ and $S_A := \{\sigma : A \to A \mid \text{bijective}\}$ the set of permutations on A. Then S_A is a group under function composition ("permutation multiplication")

Ex 8.4 "Two line notation" $A = \{1, \ldots, 5\}$.



$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}$$

write as rows instead of columns, remove arrows add parentheses.

⚠ S_A is not abelian. $(S_{\{1,2,3\}})$.

$\sigma\tau := \sigma \circ \tau \Rightarrow \sigma\tau(a) = \sigma \circ \tau(a) = \sigma(\tau(a))$.

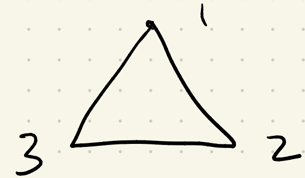
Def 8.6 Let $A = \{1, \ldots, n\}$ The group of permutations S_A is the *symmetric group* on n letters and is denoted by S_n.

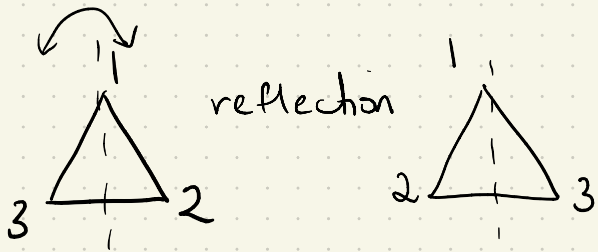
Prop $|S_n| = n! := n(n-1)(n-2) \cdots 2 \cdot 1$

Proof

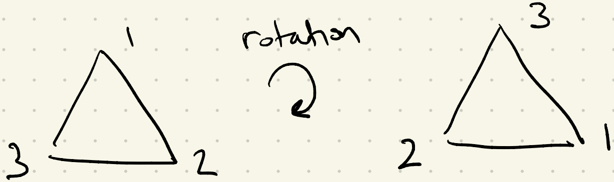
$$\begin{array}{cc} 1 & 1 \\ 2 & 2 \\ 3 & \vdots \\ \vdots & \\ n & n \end{array} \qquad n(n-1)(n-2) \cdots \cdot 1 = n!$$

Ex. 1) The shufflings of a standard deck of cards is the group S_{52}.

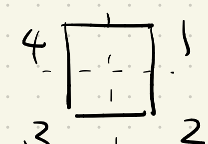
2) S_3 group of symmetries of 



$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$



$$\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

3) Dihedral group $D_4 \leq S_4$ group of symmetries of 

see Exa 8.10 and PDF "Kvadratets symmetrier" Ellingsrud.

Thm 8.16 **Cayley's Thm** Every group is isomorphic to a permutation group.

(more precisely, G a group isomorphic to subgroup of S_G)

Def 8.14 Let $f: A \to B$ be a function and $H \subseteq A$.

The image of H under f is

$$f[H] := \{ f(h) \mid h \in H \} \subseteq B.$$

Lemma 8.15 Let G and G' be groups and $\phi : G \to G'$ a one to one function such that (injective)

homomorphism property without $*, *'$

$$\phi(x * y) = \phi(x) *' \phi(y) \quad \forall\, x, y \in G. \quad ✪$$

Then $\phi[G] \leq G'$ (subgroup) and $\phi : G \to \phi[G]$ is an isomorphism.

Proof Must show 1) $\phi[G]$ is closed under $*'$, 2) $e' \in \phi[G]$

3) $\forall\, x' \in \phi[G]\ (x')^{-1} \in \phi[G]$ See details in text. $\square$

$\phi : G \to \phi[G]$ is a bijection and ✪ holds $\Rightarrow \phi$ is an isomorphism

Proof of Cayley's Thm

Will show G is isomorphic to a subgroup of S_G by applying Lemma 8.15.

For $x \in G$ <u>define</u> $\lambda_x : G \to G$ by $\lambda_x(g) := xg$.

<u>Claim</u> λ_x is bijective

- $\forall\, c \in G \quad c = x(x^{-1}c) = \lambda_x(x^{-1}c) \Rightarrow \lambda_x$ is surjective
- $\lambda_x(a) = \lambda_x(b) \Leftrightarrow \cancel{x}a = \cancel{x}b \Leftrightarrow a = b \Rightarrow \lambda_x$ is injective

Set $\phi : G \to S_G$ to be $\phi(x) = \lambda_x \in S_G$

<u>Claim</u> ϕ is injective: suppose $\lambda_x = \lambda_y : G \to G$.

In particular $\lambda_x(e) = \lambda_y(e) \iff xe = ye$
$\iff x = y$

Hence ϕ is injective.

<u>Claim</u> $\forall x,y \in G$, $\phi(xy) = \phi(x)\phi(y) \iff \lambda_{xy} = \lambda_x \circ \lambda_y$

$$\forall g \in G \quad \lambda_{xy}(g) = x(yg) \underset{\text{assoc}}{\overset{G1}{=}} \lambda_x(yg) = \lambda_x(\lambda_y(g)) = \lambda_x \circ \lambda_y(g)$$

Apply Lemma 8.15 and obtain $G \cong \phi[G] \leq S_G$ $\square$

⚠ Try replacing λ_x with $\rho_x(g) := gx$ "right mult. by x" run into problems + be forced to change $\phi: G \to S_G$.

<u>Def</u> The map $\phi: G \to S_G$ is the <u>left regular</u> <u>representation</u> of G.

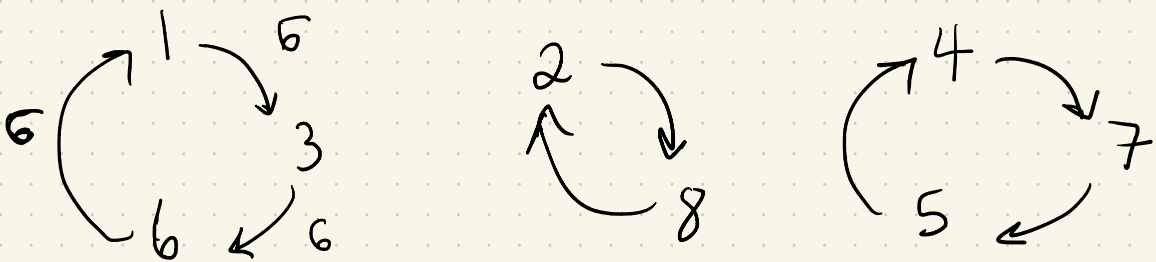
The map $\mu: G \to S_G$ by $\mu(x) := \rho_x^{-1}$ is the <u>right regular</u> <u>representation</u>

Orbits, cycles, and the alternating group §9

Ex 9.3 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix} \in S_8$

$1 \sim 3 \sim 6$

$1 \not\sim 2$



For $a, b \in A$ let $\underline{a \sim b} \iff b = \sigma^n(a)$ for some $n \in \mathbb{Z}$.

Def 9.1 Let $\sigma \in S_A$ the equivalence classes in A determined by $\sim$ are the <u>orbits</u> of A.

[σ will partition A into orbits $B_1, \ldots, B_k$].

Ex 9.3 The orbits are $\{1,3,6\}$, $\{2,8\}$, $\{4,5,7\}$

cycles of σ.

$$1 \to 3 \to 6 \to 1 \qquad \sigma_1$$

$$2 \to 8 \to 2 \qquad \sigma_2$$

$$4 \to 7 \to 5 \to 4 \qquad \sigma_3$$

Each cycle is a permutation

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 6 & 4 & 5 & 1 & 7 & 8 \end{pmatrix}$$

orbits $\{1,3,6\}$,
$\{i\}$ $i \notin \{1,3,6\}$

σ_1 is of length 3.

Def 9.6 A permutation $\sigma \in S_n$ is a cycle if it has at most 1 orbit of size larger than 1. The length of a cycle is the size of the largest orbit.

Def Two cycles σ_1, σ_2 are <u>disjoint</u> if their largest orbits are disjoint.

Ex cont

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 6 & 4 & 5 & 1 & 7 & 8 \end{pmatrix} \qquad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 8 & 3 & 4 & 5 & 6 & 7 & 2 \end{pmatrix}$$

$1 \to 3 \to 6 \to 1$ $\qquad$ $2 \to 8 \to 2$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 7 & 4 & 6 & 5 & 8 \end{pmatrix} \qquad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix}$$

$4 \to 7 \to 5 \to 4$

$$= \sigma_1 \sigma_2 \sigma_3 = \sigma_i \sigma_j \sigma_k$$

Prop disjoint cycles commute. $\sigma_1 \sigma_2 = \sigma_2 \sigma_1$. σ_1, σ_2 disjoint cycles

Proof let B_i be the largest orbit of σ_i. Then $B_1 \cap B_2 = \emptyset$

If $x \notin B_1 \cup B_2$ then $\sigma_i \sigma_j (x) = x$. If $x \in B_i$ then $\sigma_j(x) = x$ also $\sigma_i(x) \in B_i$ $\quad \sigma_j(\sigma_i(x)) = \sigma_i(x) = \sigma_i(\sigma_j(x))$ $\square$

Thm 9.8 Let A be finite. Every permutation $\sigma \in S_A$ is a product of disjoint cycles.

Proof Let $B_1, \dots, B_r$ be the orbits of σ. Then $B_i \cap B_j = \emptyset$ $i \neq j$. Define $\mu_i \in S_A$ by

$$\mu_i(x) = \begin{cases} \sigma(x) & x \in B_i \\ x & x \notin B_i \end{cases}$$

$\sigma(x) = \mu_i(x) \in B_i$

Check $\sigma(x) = \mu_1 \cdots \mu_i \cdots \mu_r(x)$. $\forall\ x \in A$. $\square$.

ordering here is not unique.

Cycle notation A cycle μ can be written as a list: $\mu = (i_0, i_1, i_2, \ldots, i_{k-1})$ μ has length k.

$$\mu(j) = \begin{cases} i_{s +_k 1} & \text{if } j = i_s \text{ for some } 0 \le s \le k-1 \\ j & \text{if } j \ne i_s \end{cases}$$

Exa Two line notation | cycle notation

1) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix}$ $\qquad \sigma = (1,3,6)(2,8)(4,7,5)$

2) $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 2 & 7 & 5 & 8 & 6 & 1 \end{pmatrix}$ $\qquad \tau = (1,4,7,6,8)(2,3)\overset{e}{\overset{\shortparallel}{\cancel{(5)}}}$

$$= (1,4,7,6,8)(2,3)$$