§2.4. Subgroups generated by elements

Def. Let G be a group.

(a) If $x \in G$, then $\langle x \rangle := \{\ldots, x^{-2}, x^{-1}, x^0, x^1, x^2, \ldots\}$
$= \{x^i \mid i \in \mathbb{Z}\} \subseteq G$.

(b) If $x_1, x_2, \ldots, x_n \in G$, then
$\langle x_1, x_2, \ldots, x_n \rangle := \{$all products whose factors belong to $\{x_1, x_2, \ldots, x_n, x_1^{-1}, x_2^{-1}, \ldots, x_n^{-1}\}\}$

$= \{y_{i_1} y_{i_2} \cdots y_{i_k} \mid k \in \mathbb{N}$, each $i \in \{x_1, \ldots, x_n, x_1^{-1}, \ldots, x_n^{-1}\}\}$

(this contains $x_2 x_3^2$ and $x_2 x_3 x_2$ and $x_1 x_2^{-5} x_3^8$ and 1 and x_5^{-1} and ...).

(c) If $S \subseteq G$, then
$\langle S \rangle := \{$all products whose factors belong to $S \cup S^{-1}\}$,

where $S^{-1} := \{s^{-1} \mid s \in S\}$.

Prop. If $x_1, x_2, \ldots, x_n \in G$, then $\langle x_1, x_2, \ldots, x_n \rangle = \langle \{x_1, x_2, \ldots, x_n\} \rangle$.

Prop. (Universal property of $\langle S \rangle$). Let G be a group. Let $S \subseteq G$.

(a) $\langle S \rangle$ is a subgroup of G.

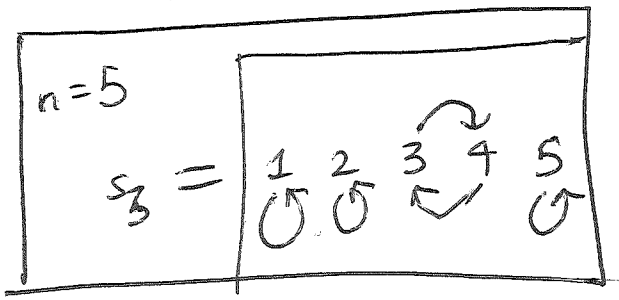
(b) If U is a subgroup of G such that $S \subseteq U$, then $\langle S \rangle \subseteq U$.

This is why $\langle S \rangle$ is called the subgroup of G generated by S.

Examples: (a) Let $G = S_n$ for some $n \in \mathbb{N}$.

For each $i \in \{1, 2, \ldots, n-1\}$, let $s_i \in S_n$ be the permutation that swaps i with $i+1$ and leaves all other numbers uncharged.

$n=5$

$s_3 =$ 

What is $\langle s_1, s_2, \ldots, s_{n-1} \rangle$?

$\langle s_1 \rangle = \{ \dots, s_1^{-2}, s_1^{-1}, s_1^0, s_1^1, s_1^2, \dots \} = \{1, s_1\}$

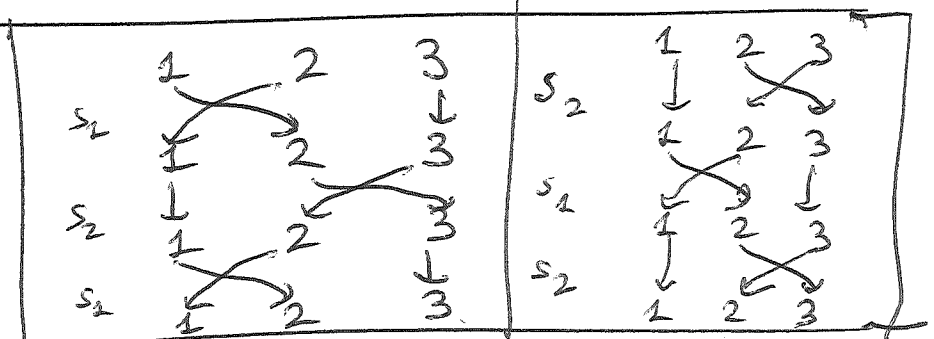
(since $s_1^2 = \mathrm{id} = 1$)

$= \{ \sigma \in S_n \mid \sigma(i) = i \ \ \forall i > 2 \}.$

$\langle s_1, s_2 \rangle = \{1, s_1, s_2, s_1^{-1}, s_2^{-1}, s_1 s_2, s_2 s_1, s_1 s_2 s_1, s_2 s_1 s_2,$

$s_1 s_2 s_1 s_2, \dots \}$

$s_2 s_1 s_2 = s_1 s_2 s_1$:



$= \{ \sigma \in S_n \mid \sigma(i) = i \ \ \forall i > 3 \}.$

More generally: For each $k < n$, we have

(1) $\langle s_1, s_2, \dots, s_k \rangle = \{ \sigma \in S_n \mid \sigma(i) = i \ \ \forall i > k+1 \}.$

[Proof of (1): The $\subseteq$ is easy.

$\supseteq$: Induction on k.

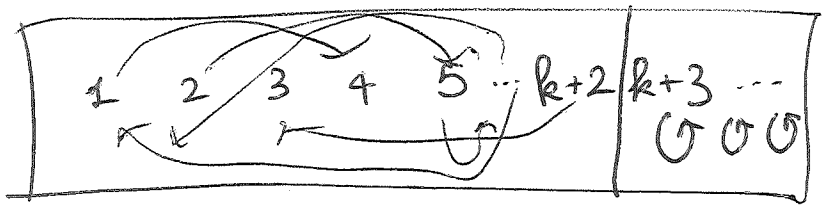
Base case ($k=0$) easy: $\langle\ \rangle = \langle\emptyset\rangle = \{1\}$, since 1 is the product of nothing (empty product).

Step ($k \to k+1$):

Assume $\langle s_1, s_2, \dots, s_k\rangle = \{\sigma \in S_n \mid \sigma(i) = i \ \ \forall i > k+1\}$, (2)

want $\langle s_1, s_2, \dots, s_{k+1}\rangle = \{\sigma \in S_n \mid \sigma(i) = i \ \ \forall i > k+2\}$.

If $\sigma \in S_n$ satisfies $\sigma(i) = i \ \ \forall i > k+2$, then we can make a permutation $\tau \in S_n$ that satisfies $\tau(i) = i \ \ \forall i > k+1$ by multiplying σ with some of the $s_1, s_2, \dots, s_{k+1}$:



If $\sigma(k+2) = j$, then $\tau := s_{k+1} \cdots s_{j+1} s_j \sigma$.

Thus, $\sigma = s_j^{-1} s_{j+1}^{-1} \cdots s_{k+1}^{-1} \tau$

$= s_j s_{j+1} \cdots s_{k+1} \tau$, with $\tau \in \langle s_1, s_2, \dots, s_k\rangle$ (by (2))

$\in \langle s_1, s_2, \dots, s_{k+1} \rangle$, qed.]

Applying (1) to $k = n-1$, we get

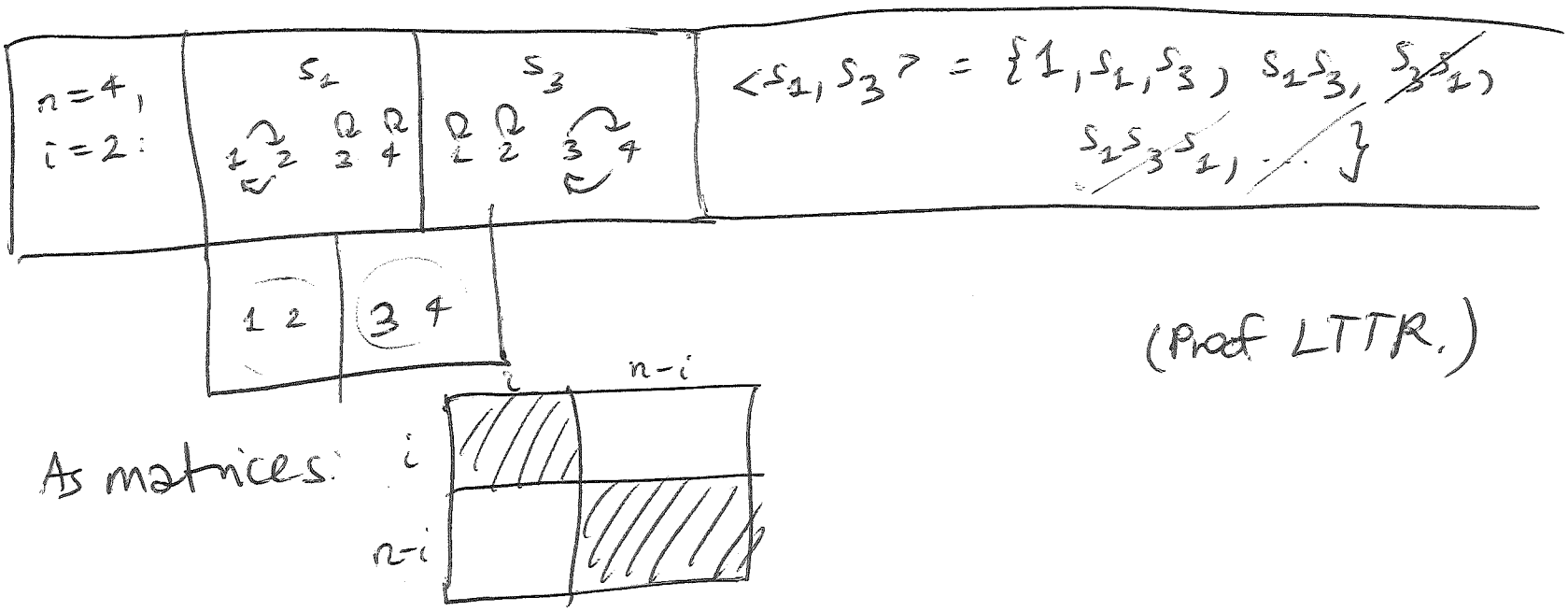
$$\langle s_1, s_2, \dots, s_{n-1} \rangle = \{\sigma \in S_n \mid \sigma(i) = i \ \forall i > n\}$$

$$= \{\sigma \in S_n\} = S_n .$$

In other words, any permutation of the list $(1, 2, \dots, n)$ can be sorted into $(1, 2, \dots, n)$ by swapping consecutive entries.

(b) Let $G = S_n$ and $i < n$.

Then $\langle s_1, s_2, \dots, s_{i-1}, s_{i+1}, s_{i+2}, \dots, s_n \rangle = \{\sigma \in S_n \mid \sigma(\{1, 2, \dots, i\}) \subseteq \{1, 2, \dots, i\}\}$



(Prof LTTR.)

(c) Let $G = \mathbb{Z}^+$.

Then $\langle 2 \rangle = \{2, 2+2, 2+2+2, \dots, 0, -2, -2-2, \dots\}$

$= 2\mathbb{Z} = \{\text{even numbers}\}$.

$\langle k \rangle = k\mathbb{Z}$ for each $k \in \mathbb{Z}$.

$\langle 3, 5 \rangle = 3\mathbb{Z} + 5\mathbb{Z} = \mathbb{Z}$.

$\langle u, v \rangle = u\mathbb{Z} + v\mathbb{Z} = \gcd(u,v)\mathbb{Z}$ for each $u, v \in \mathbb{Z}$. // $\langle \gcd(u,v) \rangle$

For each subset S of $\mathbb{Z}$: $\langle S \rangle = \underbrace{\gcd(S)}_{\text{the gcd of all elements of } S} \cdot \mathbb{Z}$.

(d) Let $G = GL_n(\mathbb{R})$.

If $S = \{\text{elementary matrices}\} = \left\{ \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & x \\ & & & 1 \end{pmatrix} \mid x \in \mathbb{R} \right\}$

$\cup \left\{ \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} \mid x \in \mathbb{R} \right\} \cup \left\{ \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 0 & \cdots & 1 \\ & & \vdots & \ddots & \\ & & 1 & \cdots & 0 \end{pmatrix} \right\}$ (transposition matrices)

$\cup \left\{ \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & x & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} \mid x \in \mathbb{R} \right\}$, then

$\langle S \rangle = GL_n(\mathbb{R})$. (because row reduction works).

Proof of Prop. (UP). (a) Closure: If $a \in \langle S \rangle$ and $b \in \langle S \rangle$, then $ab \in \langle S \rangle$. ✓

Identity: 1 is the empty product. ✓

Closure under inverses: $(y_1 y_2 \cdots y_n)^{-1} = y_n^{-1} y_{n-1}^{-1} \cdots y_1^{-1}$

and $(S^{-1})^{-1} = S$. ✓

(b) U contains all elements of S, thus also their inverses, thus also products of elements of S and their inverses. Thus, $\langle S \rangle \subseteq U$. □

How does $\langle x \rangle = \{\cdots, x^{-2}, x^{-1}, x^0, x^1, x^2, \cdots\}$ look like for $x \in G$?

Prop. 2.4.2. Let G be a group, and $x \in G$.

Let $P = \{k \in \mathbb{Z} \mid x^k = 1\}$.

(a) This P is a subgroup of $\mathbb{Z}^+$.

(b) If $r, s \in \mathbb{Z}$, then $x^r = x^s$ if & only if $r - s \in P$.

(c) If $P \neq \{0\}$, then $P = n\mathbb{Z}$ for some $n > 0$, and the elements $1, x, x^2, \cdots, x^{n-1}$ are the distinct elements of $\langle x \rangle$.

(d) If $P = \{0\}$, then all the x^i are distinct.

Proof. (a) Closure: If $a, b \in P$, then $x^a = 1$ & $x^b = 1$

$$\Rightarrow x^{a+b} = x^a \cdot x^b \quad \text{(by general associativity)}$$
$$= 1 \cdot 1 = 1.$$

Rest: easy.

(b) Let $r, s \in \mathbb{Z}$. Then

$$(x^r = x^s) \Longleftrightarrow (x^s x^{r-s} = x^s)$$

($x^r = x^s x^{r-s}$)

$$\overset{\text{cancellation}}{\Longleftrightarrow} (x^{r-s} = 1) \Longleftrightarrow (r - s \in P).$$

(c) Assume $P \neq \{0\}$. Then, Thm. 2.3.3 yields $P = n\mathbb{Z}$ for some $n \geq 0$. Thus, $n > 0$.

Thus, (b) says: If $r, s \in \mathbb{Z}$, then $x^r = x^s$ if & only if $n \mid r - s$. Thus, each $i \in \mathbb{Z}$ satisfies

$$x^i = x^{(\text{remainder of } i \text{ upon division by } n)}$$

Hence, the only elements of $\langle x \rangle$ are $1, x, x^2, \ldots, x^{n-1}$.

Remains to show that these are distinct. This again follows from (b). $\square$

Def: Let G be a group, and $x \in G$.

~~Then, let $n \in \mathbb{N}$ be as~~ Let P be as in Prop. 2.4.2.

Assume $P \neq \{0\}$. Then, the n in Prop. 2.4.2 (c) is called the order of x.

If $P = \{0\}$, then we says that the order of x is ∞.

Ex: $G = S_3$.

s_1 has order 2 (since $s_1^2 = 1$ but $s_1 \neq id$)

$s_1 s_2$ has order 3.