More about S_n:

- A <u>cycle</u> $\sigma = (a_1 a_2 \dots a_k) \in S_n$ is a permutation mapping $a_1 \mapsto a_2$, $a_2 \mapsto a_3 \dots a_k \mapsto a_1$ and all other elements to themselves.
  ↳ distinct elements of $\{1..n\}$

- <u>Prop</u>: any permutation can be expressed as a product of disjoint cycles, uniquely up to reordering the factors (disjoint cycles commute so order doesn't matter)

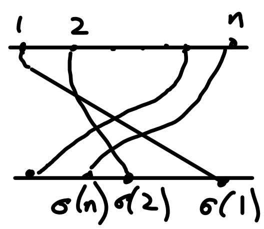
<u>Ex</u>: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 5 & 6 & 4 & 2 & 1 \end{pmatrix} = (1\,3\,6)(2\,5)$ ↳ same for other elements not in the previous cycles.
↳ successive images of 1 under σ until returns to 1

- A k-cycle can be written as a product of $(k-1)$ <u>transpositions</u> (= 2-cycles):
$$(a_1 a_2 \dots a_k) = (a_1 a_2) \circ (a_2 a_3) \circ \dots \circ (a_{k-1} a_k).$$

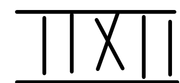
<u>So</u>: S_n is generated by transpositions. $(i\ j)$ $1 \le i < j \le n$.

In fact it is generated by $(1\,2), (2\,3), \dots, (n\text{-}1\ n)$.
Either directly (show $(i\ j)$ can be expressed in terms of these specific transpositions), or...

<u>Idea</u>: draw σ as



, slice into a stack of



$(i\ i{+}1)$.

[see also: <u>bubble sort algorithm</u>]

- Permutations are <u>odd</u> or <u>even</u> depending on length of expression of σ as a product of transpositions ($\Leftrightarrow$ parity of $\#\{(i,j) \mid 1 \le i < j \le n,\ \sigma(j) > \sigma(i)\}$)

Even permutations form a normal subgroup A_n = <u>alternating group</u> $\subset S_n$.

[this is nontrivial! proof by induction]. $\quad 1 \to A_n \to S_n \to \mathbb{Z}/2 \to 1.$

★ <u>Fact</u>: even though $A_3 \simeq \mathbb{Z}/3$, and A_4 has a normal subgroup $\simeq \mathbb{Z}/2 \times \mathbb{Z}/2$, for $n \ge 5$ A_n is <u>simple</u>!

(This fact is used to prove that there is no general formula for solving polynomial equations of degree ≥ 5! The quadratic formula has a $\pm\sqrt{\ }$, and the sign is there because over $\mathbb{C}$ there's not a consistent choice of $\sqrt{\ }$ of all complex numbers – ambiguity is in $\mathbb{Z}/2 \simeq S_2$ permuting the two roots. The Cardano formula for cubics has $\sqrt[3]{\dots + \sqrt{\dots}}$ in it. The $\mathbb{Z}/2$ & $\mathbb{Z}/3$ ambiguities in choosing these roots combine to an S_3 permuting the roots. Similarly, the formula for roots of a deg. 5 equation should have a built-in S_5 symmetry – but any expression involving $\sqrt[k]{\dots}$ will have symmetry group built from cyclic $\mathbb{Z}/k$'s. This can't be S_5 since A_5 is simple.)

Advertisement for Galois theory. (Math 123).

★ Did you know: $\mathrm{Aut}(S_n) \cong S_n$ <u>except</u> for $n=2$ ($\mathrm{Aut}(S_2) = \{id\}$) and $n=6$!

* Two constructions that help understand the extent of non-commutativity in a group:

1) • Def: ‖ the center $Z(G) = \{ z \in G \mid az = za \ \forall a \in G \}$.

Since elements of the center commute with everyone, they commute w/ each other, so $Z(G)$ is abelian! Also, $aZ(G)a^{-1} = Z(G)$, so $Z(G)$ is a normal subgroup of G.

G is abelian iff $Z(G) = G$.

2) • the commutator subgroup $C(G) = [G,G] = \{ \prod_{i=1}^{k} [a_i, b_i] \mid k \in \mathbb{N},\ a_i, b_i \in G \}$

where $[a,b] := aba^{-1}b^{-1}$ (the "commutator" of a & b, $= e$ iff $ab = ba$).

This is a normal subgroup because $g^{-1} \prod_{i=1}^{k} [a_i, b_i]\, g = \prod_{i=1}^{k} [g^{-1}a_i g,\ g^{-1} b_i g]$.

$\Rightarrow g^{-1} C(G) g = C(G). \quad \forall g \in G$.

The quotient $G/[G,G]$ is called the abelianization of G.

Since $[G,G]$ contains all commutators $[a,b]$, quotienting makes $[a,b] = e$ in the quotient group, ie. $ab = ba \quad \forall a,b \in G/[G,G]$.

Since $[G,G]$ is generated by commutators, it is the smallest subgroup of G with that property. The abelianization is the largest abelian group onto which G admits a surjective homomorphism.

---

* The free group F_n on n generators $a_1, \dots, a_n$.

Elements are all reduced words $a_{i_1}^{m_1} \cdots a_{i_k}^{m_k}$ $\quad k \geq 0$ (empty word is e)

$i_1 \dots i_k \in \{1 \dots n\} \quad i_j \neq i_{j+1}$

$m_1 \dots m_k \in \mathbb{Z} - \{0\}$

(non reduced words: reduce by:

• if $i_j = i_{j+1}$, combine $a_i^m a_i^{m'} \to a_i^{m+m'}$

• if an exponent is zero, remove a_i^0).

Repeat until word is reduced.

• This is the "largest" group with n generators, all others are $\simeq$ quotients of F_n.

If G is generated by $g_1, \dots, g_n \in G$, define a homomorphism

$F_n \twoheadrightarrow G$ by $\prod a_{i_j}^{m_j} \mapsto \prod g_{i_j}^{m_j}$. (*)

• A finitely generated group is said to be finitely presented if the kernel of (*) is the smallest normal subgroup of F_n containing some finite subset $\{r_1, \dots, r_k\} \subset F_n$, (ie. the subgroup generated by r_j's and their conjugates $x^{-1} r_j x$).

↳ words in the generators

Write $G \cong \langle \underbrace{a_1, \dots, a_n}_{\text{generators}} \mid \underbrace{r_1, \dots, r_k}_{\text{relations}} \rangle$, then $G \cong F_n / \langle \text{conj's of } r_1 \dots r_k \rangle$

Ex: $\mathbb{Z}^n \cong \langle a_1, \dots, a_n \mid a_i a_j a_i^{-1} a_j^{-1} \ \forall i,j \rangle$.

Ex: $S_3 \cong \langle t_1, t_2 \mid t_1^2, t_2^2, (t_1 t_2)^3 \rangle$

Now we move on to rings & fields on our way to vector spaces. (Artin ch. 3 / Axler ch. 1-2)
(groups will return later).

Rings and fields:

Def: A (commutative) ring is a set R with two operations $+, \times$ such that
(1) $(R,+)$ is an abelian group with identity $0 \in R$
(2) $(R, \times)$ is a (commutative) semigroup with identity $1 \in R$, namely
- $1a = a1 = a \quad \forall a \in R$
- $a(bc) = (ab)c \quad \forall a,b,c \in R$.
- ($ab = ba \quad \forall a,b \in R$ if commutative)

(3) distributive law: $a(b+c) = ab + ac \quad \forall a,b,c \in R$.

Def: A field K is a commutative ring such that $\forall a \neq 0$, $\exists b = a^{-1}$ s.t. $ab = 1$.
i.e. $(K \setminus \{0\}, \times)$ is an abelian group rather than a semigroup.

Rmk:
- the ring axioms imply $0a = a0 = 0 \ \forall a$. ($a0 = a(0+0) = a0 + a0$ + cancellation).
- the trivial ring $R = \{0\}$ is the only case where $0 = 1$. By convention this is not a field.
- most rings of interest to us are commutative. (Matrices are the main exception)
- in a field, $ab = 0 \Rightarrow a = 0$ or $b = 0$. Not necessarily true in a ring.
- hence, in a field, we have usual properties of cancellation (simplification) for both addition & multiplication.

Def: A ring/field homomorphism is a map $\varphi: R \to S$ that respects both operations:
$$\varphi(a+b) = \varphi(a) + \varphi(b)$$
(← we've seen this implies $\varphi(0) = 0$, $\varphi(-a) = -\varphi(a)$)
$$\varphi(ab) = \varphi(a)\varphi(b)$$
$$\varphi(1_R) = 1_S$$
(← this doesn't follow from $\varphi(ab) = \varphi(a)\varphi(b)$, even for fields: consider $\varphi \equiv 0$!)

Prop: IF $\varphi: R \to S$ is a field homomorphism, then φ is injective.

Pf: if $a \neq 0$ then $\exists b$ s.t. $ab = 1_R$, so $\varphi(a)\varphi(b) = \varphi(ab) = 1_S \neq 0_S$ which implies $\varphi(a) \neq 0_R$. So $\ker(\varphi) = \{0\}$, hence φ injective.
↳ as additive group homom. □

Examples:
- $\mathbb{Z}$, $\mathbb{Z}/n$ are rings.
- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields. So is $\mathbb{Z}/p$ for p prime !!
  This is denoted $\mathbb{F}_p$ when viewed as a field.

because: if $k \neq 0$ in $(\mathbb{Z}/p, +)$ then its order is p (divides p, $\neq 1$), so $\{0, k, 2k, \dots, (p-1)k\} = \mathbb{Z}/p$.
hence $\exists l \in \{0, \dots, p-1\}$ st. $lk = 1 \bmod p$. This gives the inverse!

* **Polynomials**: given a field k, the ring of polynomials in one formal variable x is $k[x] := \{a_0 + a_1 x + \dots + a_n x^n \mid a_i \in k,\ n \in \mathbb{N}\}$

Remark: x is a formal variable ie. not an element of anything, though we can evaluate a polynomial at an element of k or of any field containing k.

so: a polynomial $\Leftrightarrow$ a finite tuple of elements $(a_0, \dots, a_n, 0, 0, \dots)$ of k, with component-wise addition [but not componentwise multiplication! $x^i x^j = x^{i+j}$]

* $k[x]$ isn't a field, but it can be turned into a field by considering fractions (just like $\mathbb{Z}$ ring $\rightsquigarrow$ $\mathbb{Q}$ field): the field of rational functions is

$$k(x) = \left\{ \frac{p}{q} \;\middle|\; p, q \in k[x],\ q \neq 0 \right\} \Big/ \frac{p}{q} \sim \frac{p'}{q'} \text{ iff } pq' = qp'.$$

(This generalizes to polynomials & rational functions in any number of variables)

* **Power series**: The ring of formal power series in x is $k[[x]] = \left\{ \sum_{i=0}^{\infty} a_i x^i \;\middle|\; a_i \in k \right\}$
(add and multiply just like polynomials, term by term. check each coefficient in $(\sum a_i x^i)(\sum b_j x^j)$ is a finite expression).

Lemma: $\sum a_i x^i$ has a multiplicative inverse in $k[[x]]$ iff $a_0 \neq 0$.

Proof: We want $\sum_{i\geq 0} b_i x^i$ st. $\left(\sum_{i\geq 0} a_i x^i\right)\left(\sum_{i \geq 0} b_i x^i\right) = 1$. This gives

$$\left.\begin{aligned} a_0 b_0 &= 1 \\ a_0 b_1 + a_1 b_0 &= 0 \\ a_0 b_2 + a_1 b_1 + a_2 b_0 &= 0 \\ &\dots \end{aligned}\right\}$$

$\to$ if $a_0 = 0$, clearly no solution; if $a_0 \neq 0$, we can solve inductively: $b_0 = \frac{1}{a_0}$, $b_1 = \frac{-a_1 b_0}{a_0}, \dots$
(each step is $b_i = -(\dots)/a_0$ ✓). $\square$

$\rightsquigarrow$ since every nonzero element of $k[[x]]$ is of the form

$$\underset{\substack{\uparrow \\ \text{first nonzero coefficient}}}{a_m} x^m + a_{m+1} x^{m+1} + \dots = x^m \underbrace{(a_m + a_{m+1} x + \dots)}_{\text{invertible}},$$

to get a field we just need to allow x^{-m}.

$\rightsquigarrow$ **Def**: The field of Laurent series $k((x)) = \left\{ \sum_{i=m}^{\infty} a_i x^i \;\middle|\; m \in \mathbb{Z},\ a_i \in k \right\}$.

* Given a field k, and a polynomial $f \in k[x]$ (of degree >0), we can evaluate $f(r)$, $r \in k$, and look for roots $r \in k$ st. $f(r) = 0$.
If there are none in k, we can form a field $K \supset k$ in which f has a root.

Ex: $k = \mathbb{Q}$, $x^2 - 2$ has no roots, but we can form

$$\mathbb{Q}(\sqrt{2}) := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \text{ which is a field: } \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} \in \mathbb{Q}(\sqrt{2})$$

Ex: $k = \mathbb{R}$, $x^2 + 1 \rightsquigarrow \mathbb{R}(\underbrace{\sqrt{-1}}_{\text{usually called } i}) = \mathbb{C}$.