MATH H113: Honors Introduction to Abstract Algebra

2016-02-03

- Finish presentation of groups
- Symmetric groups
- Matrix groups
- Quaternionic group (time permitting)

Given a group presentation $\langle S | R_1, \ldots, R_m \rangle$, to find out what group G it describes:

1. Find a list of expressions in the generators (elements of S) that should cover all elements of the group
2. Find an explicit group G' such that
    a. the relations are all true in G', and
    b. each expression in the list from Step 1 is a different element of G' (this is not easy).

We did this for $\langle \{r, s\} | r^n = 1, s^2 = 1, sr = r^{-1}s \rangle$.
A trickier example:
What is $\langle \{x, y\} | x^5 = 1, y^3 = 1, yx = x^3y \rangle$?
You expect the group to have 15 elements: $x^i y^j : i = 0, 1, 2, 3, 4; j = 0, 1, 2$. In fact, these expressions cover all the elements of the group, but there are redundancies.
$yx^2 = (yx)x = x^3yx = x^3 \times x^3y = x^6y = xy$
Similarly by induction, $yx^i = x^{3i}y$ for all $i = 1, 2, 3, \ldots$
Then $y^2x^i = y \times yx^i = y \times x^{3i}y = x^{9i}y^2$
and then $y^3x = y \times y^2x = y \times x^9y^2 = x^{27}y^3$
But $y^3 = 1$, so $x = x^{27}$; $x^{26} = 1$.
But also $x^{25} = (x^5)^5 = 1^5 = 1$, so
$1 = x^{26} = x \times x^{25} = x \times 1 = x$
So $x = 1$, and therefore the group is actually $\langle \{y\} | y^3 = 1 \rangle$.
This group has 3 elements: $1, y, y^2$.

Symmetric Groups

Definition: Let Ω be a set (allow $\Omega \neq \emptyset$, but don't worry too much about that case). Then the *symmetric group on* Ω is the group S_Ω, whose elements are all of the bijections from Ω to Ω, and whose group operation is composition of functions.
Note: if $f, g \in S_\Omega$, then $f \circ g \in S_\Omega$ because $f \circ g$ maps Ω to Ω, and is bijective.
$f \circ g$ is injective: $x \neq y \implies g(x) \neq g(y) \implies f(g(x)) \neq f(g(y))\ \forall x, y \in \Omega :$

$f \circ g$ is one-to-one.
$\forall z \in \Omega. \exists y \in \Omega$ s.t. $g(y) = z$ (since g is surjective) and $\exists x \in \Omega$ s.t. $f(x) = y$ (since f is surjective). $\therefore (f \circ g)(x) = f(g(x)) = f(y) = z$ so $f \circ g$ is surjective.
Therefore $f \circ g \in S_\Omega \ \forall f, g \in S_\Omega$.
Also, composition is associative.
The *identity map*, $i : \Omega \to \Omega$, given by $i(x) = x \ \forall x \in \Omega$ is the group identity, and for all $f \in S_\Omega$, the inverse function f^{-1} is the inverse in the group. $\therefore S_\Omega$ is a group.

Definition: Let $n \in \mathbb{Z}_{>0}$ (or $n \in \mathbb{N}$). Then the *symmetric group on n letters* is the group $S_n = S_{\{1,2,\ldots,n\}}$.

Examples:

0. $S_0 = S_\emptyset$ is the trivial group (there is only one function $f : \emptyset \to \emptyset$).
1. S_1 is also the trivial group. There is only one function $f : \{1\} \to \{1\}$.
2. $S_2 = S_{\{1,2\}}$ has two elements:
   $f =$ identity function: $f(1) = 1, f(2) = 2$
   $g =$ function that switches 1 and 2: $g(1) = 2, g(2) = 1$.

$(\circ)$	f	g
f	f	g
g	g	f

Looks a lot like $\mathbb{Z}/2\mathbb{Z}$:

$(+)$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

In general, S_n has $n!$ elements $\forall n \in \mathbb{Z}_{>0}$ (or $n \in \mathbb{N}$, note that $0! = 1$).
To choose $\sigma \in S_n$:
You have n possibile choices for $\sigma(1)$
You have $n - 1$ possible choices for $\sigma(2)$
You have $n - 2$ possible choices for $\sigma(3)$
You have 1 possible choices for $\sigma(n)$

Cycles

Definition: The notation $(a_1 \ a_2 \ \ldots \ a_m)$, where $m \in \mathbb{Z}_{>0}$ and $a_1, \ldots, a_m$ are *distinct* elements of $\{1, 2, \ldots, n\}$, is the element $\sigma \in S_n$ defined by:

$\sigma(a_i) = a_{i+1},\ i = 1, \dots, m-1$
$\sigma(a_m) = a_1$
and $\sigma(x) = x\ \forall x \in \{1, 2, \dots, n\} \setminus \{a_1, a_2, \dots, a_m\}$. This is called a *cycle*, or an *m-cycle*, and its *length* is m.

Definition: Cycles $(a_1\ a_2\ \dots\ a_m)$ and $(b_1\ b_2\ \dots\ b_k)$, are *disjoint* if the sets $\{a_1, a_2, \dots, a_m\}$ and $\{b_1, b_2, \dots, b_k\}$ are disjoint.
Key Fact: Disjoint cycles commute.
Proof:
$(a_1\ a_2\ \dots\ a_m)(b_1\ b_2\ \dots\ b_k) = (b_1\ b_2\ \dots\ b_k)(a_1\ a_2\ \dots\ a_m)$
because both sides take:

- a_i to a_{i+1} $(1 \leq i < m)$
- a_m to a_1
- b_j to b_{j+1} $(1 \leq j < k)$
- b_k to b_1
- and leave all other elements of $\{1, 2, \dots, n\}$ unchanged.

Theorem: Every element of S_n can be written as a (finite) product of (pairwise) disjoint cycles.
Proof: Here's how (let $\sigma \in S_n$):

0. Start with the empty product
1. If all elements of $\{1, 2, \dots, n\}$ are already mentioned in the pairwise product so far, stop.
2. Otherwise, find the smallest $a \in \{1, 2, \dots, n\}$ not mentioned so far, and compute $\sigma(a), \sigma^2(a), \dots$ until you get $\sigma^m(a) = a$ the first time. Then, add the cycle $(a\ \sigma(a)\ \sigma^2(a)\ \dots\ \sigma^m(a))$ to the list. Go back to step 1.
3. Optional last step: cancel out all 1-cycles.