MATH H113: Honors Introduction to Abstract Algebra

2016-02-01

- Dihedral groups

	e	r	r^2	s	sr	sr^2
e	e	r	r^2	s	sr	sr^2
r	r	r^2	e	sr^2	s	sr
r^2	r^2	e	r	sr	sr^2	s
s	s	sr	sr^2	e	r	r^2
sr	sr	sr^2	s	r^2	e	r
sr^2	sr^2	s	sr	r	r^2	e

Loose Ends

1. On homework, you can use the results of earlier problems in the book without proving them.
2. If A and B are groups, then $A \times B = \{(a,b) : a \in A, b \in B\}$ is also a group, with $(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2)$.
   Note that $(a,b)^n = (a^n, b^n)$ for all $a \in A, b \in B, n \in \mathbb{Z}$ (prove by inductionfor $n > 0$, etc.).
3. Let G be a group, let $x \in G$, and assume that x has finite order n. Then (for $m \in \mathbb{Z}$), $x^m = 1 \iff n \mid m$.
   Proof:

- "$\leftarrow$" If $n \mid m$ then $nq = m$ for some $q \in \mathbb{Z}$, and $\therefore$ $x^m = x^{nq} = (x^n)^q = 1^q = 1$.
- "$\rightarrow$" Assume $x^m = 1$. Write $m = nq + r$ with $q, r \in \mathbb{Z}, 0 \le r < n$. THen $x^{nq+r} = 1$, so $1 = x^{nq}x^r = (x^n)^q x^r = 1^q x^r = x^r$, and that implies $r = 0$ (if $r \neq 0$ then $x^r = 1$ with $0 < r < n$, contradicting the definition of order of x). Then $m = nq$, so $n \mid m$.

4. When I refer to $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ or $\mathbb{Z}/n\mathbb{Z}$ as groups, the operations is *addition*. When I refer to $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$, or $(\mathbb{Z}/n\mathbb{Z})^*$ as groups, the operation is *multiplication*.

r = rotation clockwise by $\frac{2\pi}{8}$ radians s = flip about the line through vertex position 1 and the center

n	1	2	3	4	5	6	7	8
$r(n)$	2	3	4	5	6	7	8	1
$s(n)$	1	8	7	6	5	4	3	2
rs	8	7	6	5	4	3	2	1
sr^{-1}	8	7	6	5	4	3	2	1

$\therefore rs = sr^{-1}$.
Also $r^2 s = r(rs) = r(sr^{-1}) = (rs)r^{-1} = sr^{-1}r^{-1} = sr^{-2}$
Generally, $r^{n+1}s = rr^n s = rsr^{-n} = sr^{-1}r^{-n} = sr^{-(n+1)}$
$\therefore$ by induction, $r^i s = sr^{-i}$ for all $i \in \mathbb{Z}$.
$r^n = 1$ and $s^2 = 1$.
We have $D_{2n} = \{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}$, and these expressions all give different elements of D_{2n}.
Here r and s *generate* D_{2n}.

Definition: A subset S of a group G *generates* G if every element of G can be written as a (finite) product of (positive or negative) integer powers of elements of S. If S generates G, then we also say that S is a *generating set* for G.
Examples:

- $\{r, s\}$ generates $D_{2n} \forall n$
- For any group G, G generates itself.
- $S = \emptyset$ generates the trivial group (1 = empty product)

Then D_{2n} can be fully described by:

i. elements r and s generate D_{2n}, and
ii. for any two expressions in r and s, those two expressions give the same element of D_{2n} if and only if this equality can be deduced from the equalities $r^n = 1, s^2 = 1, rs = sr^{-1}$ (these are called *relations*).

(i) and (ii) (collectively) are an example of a presentation of a group.

Definition: A *presentation* of a group G is an expression $G = \langle S | R_1, R_2, \ldots, R_m \rangle$, where S is a generating set for G, and each R_i is an equation in the elements of $S \cup \{1\}$ such that any (true) equation from the elements of S can be deduced from $R_1, \ldots, R_m$.
Example:

- $\mathbb{Q}^\times = \langle \{2, 3, \ldots, -1\} | (-1)^2 = 1, pq = qp \forall p, q \in S \rangle$
- trivial group $= \langle \emptyset | \rangle$

The R_i are called *relations*, and the presentation of G is also called a *description of G using generators and relations*.

Elements of S are called *generators*.
Caution: Referring to an element of G as a generator is only valid if it is understood what the set S is.

How do you work with these?
To check whether a given group is described by a given presentation $\langle S | R_1, \ldots, R_m \rangle$:
1. Check that S generates G and that $R_1, \ldots, R_m$ are true in G. 2. Check that you have enough relations; in other words, that every equation in the elements of $S \cup \{1\}$ can be deduced from $R_1, \ldots, R_m$ (to do this it may help to find, for each element of G an expression in the elements of S that equals that element and then show that all other such expressions are equal to one of the chosen expressions).

Example: $D_{2n} = \{1, r, r^2, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}\}$ (using $rs = sr^{-1}$).