MATH H113: Honors Introduction to Abstract Algebra

2016-01-29

- Groups
- Dihedral Groups

Homework due 2016-02-05:

- Sect 1.1: 6, 12, 18, 30
- Sect 1.2: 4, 10, 14, 15

Definition: A group $(G, \star)$ is:

a. *finite* if G is a finite set;
b. *infinite* if G is an infinite set;
c. *abelian* (or *commutative*) if $\star$ is commutative

Two more examples of groups:

- the *trivial group* $G = \{e\}$, $e \star e = e$
- For any $n \in \mathbb{Z}_{>0}$, $GL_n(\mathbb{R})$ is the group of invertible $n \times n$ matrices with entries in $\mathbb{R}$. The inverse in G is the matrix inverse, and the identity in G is the identity matrix I_n. This group is non-abelian (unless $n = 1$).

A word on notation: people usually don't write $\star$ for the group operation. There are two choices of notation:

a. *Multiplicative notation*: Write ab instead of $a \star b$, a^{-1} for the inverse of a and 1 or e for the identity element.
b. *Additive notation*: Write $a + b$ instead of $a \star b$, $-a$ for the inverse of a and 0 for the identity element.
   Also define $a - b = a + (-b)$

Additive notation is *only used* for abelian groups. Multiplicative notation can be used for any group.

Basic Properties of Groups

(see book for omitted proofs)

a. A group can have only one identity element (proved already)
b. Every $a \in G$ has only one inverse and $ab = e$ *or* $ba = e \implies b = a^{-1}$.
c. $(a^{-1})^{-1} = a$
d. $(ab)^{-1} = b^{-1}a^{-1}$
   $(ab)b^{-1}a^{-1} = abb^{-1}a^{-1} = aea^{-1} = aa^{-1} = e$
e. $e^{-1} = e$
   $e^{-1} = e^{-1}e = e$
f. Generalized associative law:
   in a product of n elements ($n \in \mathbb{Z}$), you get the same answer no matter what order the operations are performed in.
   example: $(ab)(cd) = ((ab)c)d = (a(bc))d$
   The proof is by strong induction on n.

Proposition: Let G be a group, and let $a, b, c \in G$.

a. (Cancellation law): if $ac = bc$ then $a = b$.
b. (Another cancellation law): if $ca = cb$ then $a = b$.
c. The equation $ax = b$ has a unique solution $x \in G.\, x = a^{-1}b$.
d. Same for the equation $xa = b$, $x = ba^{-1}$ (not necessarily the same solution).

Proof:

a. $ac = bc \implies acc^{-1} = bcc^{-1} \implies ae = be \implies a = b$
b. Similar
c. $ax = b \iff a^{-1}ax = a^{-1}b \iff ex = a^{-1}b \iff x = a^{-1}b$
   Check by pluggin in: $a(a^{-1}b) = b$
d. Similar (be careful about lack of commutativity)

Definition: For a group G, an element $x \in G$, and $n \in \mathbb{Z}$
$$x^n = \begin{cases} xx\dots x \text{ (n times)} & n > 0 \\ e & n = 0 \\ (x^{-1})^{-n} & n < 0 \end{cases}$$
In additive notation, this is written nx.
The usual rules for exponentials are satisfied:

- $x^n x^m = x^{n+m} \forall n, m \in \mathbb{Z}$
- $(x^n)^m = x^{nm} \forall n, m \in \mathbb{Z}$

Definition: The order of an element $x \in G$ is the smallest positive integer n such that $x^n = e$, or ∞ if there is no such n. It is written $|x|$.

Examples:

- In any group, $|x| = 1 \iff x = e$
- In $\mathbb{R}$, all non-zero elements have infinite order
- In $(\mathbb{Z}/5\mathbb{Z})^\times$ $|4| = 2$ because $4^2 = 16 \equiv 1 \pmod 5$, but $|3| = 4$ because $3^2 = 9 \in \bar{4}, 3^3 = 27 \in \bar{2}, 3^4 = 81 \in \bar{1}$.

Definition: The cardinality of a set A is the number of elements of A if A is finite, or ∞ if A is infinite. (In this class, we won't distinguish between countably infinite and uncountable cardinalities). This is written $|A|$ or, sometimes, $\#A$

Definition: The *order* of a group G is the cardinality of its set of elements, also written $|G|$ (or $\#G$).

With a group, you can write its *multiplication table*. For example:

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$\mathbb{Z}/4\mathbb{Z}$ is abelian

Dihedral Groups

Definition: Let $n \in \mathbb{Z}, n \geq 3$. The *dihedral group* of order $2n$ is thg group D_{2n} (som authors write it as D_n) is the set of symmetries of a regular n-gon. This is the set of permutations (= bijections) of the set of vertices of the n-gon that can be obtained by rigid motion of $\mathbb{R}^3$.

See figure 1 on paper D_{16} has 16 elements

We can think of two elements:
r = rotation clockwise by $\frac{2\pi}{n}$ radians s = flip about the line through vertex position 1 and the center

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

headers are numbers on blackboard, below are numbers on the cardboard (if the cardboard starts in "standard position")