Abstract Algebra
Lecture 2
Monday, 9/6/2010

1 Subgroups

Defn: Subgroup
A nonempty subset H of a group G is a subgroup if $(H, *)$ is itself a group. (Recall that $G = (G, *)$.) We notate this as $H \leq G$.

Theorem: A nonempty subset H of a group G is a subgroup if and only if
1. H is closed under $*$ (i.e. $a, b \in H \Rightarrow a * b \in H$)
2. H is closed under inverses (i.e. $a \in H \Rightarrow a^{-1} \in H$)

Proof:
($\Rightarrow$) Clear (because H is already a group).
($\Leftarrow$) (See first homework.)

■

Ex:
- $G = (\mathbb{R}, +), H = \mathbb{Z}$
- $2\mathbb{Z} \leq Z$

Theorem: Let $H \subseteq G$ be nonempty. Then H is a subgroup of G if and only if for all x and y in H, xy^{-1} is in H. In other words,

$$H \leq G \Leftrightarrow \forall x, y \in H, xy^{-1} \in H$$

Proof:
($\Rightarrow$) $H \leq G$. Let $x, y \in H$. H is closed under inverses, so $y^{-1} \in H$, and H is closed under the binary operation, so $x \cdot y^{-1} \in H$.
($\Leftarrow$) $H \neq \emptyset$, so $\exists x \in H$. Thus, $x, x \in H$. Therefore $xx^{-1} \in H$, i.e. $e \in H$. Now, let $x = e$, so we have $e, y \in H \Rightarrow ey^{-1} \in H$, so H is closed under inverses. Let $x, y \in H$, then $y^{-1} \in H$. Consider $x, y^{-1} \in H \Rightarrow x(y^{-1})^{-1} \in H$, i.e. $xy \in H$, so H is closed under the binary operation. Then, by the theorem above, H is a subgroup of G.

■

Theorem: Let H be a nonempty subset of a finite group G. Then $H \leq G$ if and only if H is closed under the operation of G.

Proof:

($\Rightarrow$) By definition.

($\Leftarrow$) $H \subseteq G$, and $H \neq \emptyset$, so we know that $x, y \in H \Rightarrow xy \in H$. Let $x \in H$. Then $x^2 \in H$. In fact, $\{x^n | n \in \mathbb{Z}^+\} \subseteq H$. However, since H is finite, there must be $m > n \in \mathbb{N}$ such that $x^m = x^n$. Therefore $x^m(x^n)^{-1} = x^m x^{-n} = x^{m-n} = e \in H$. So now we want to show that $x \in H \Rightarrow x^{-1} \in H$. But $x^i \in H$ for all i, so $X^{m-n-1} \in H$. And $x(x^{m-n-1} = e$. Therefore the identity is in H, therefore the inverse of any element is in H, therefore we have that $xy^{-1} \in H$ for arbitrary x and y, which shows that H is a subgroup by the previous theorem.

■

2 Generators & Relations

Defn: Diherdral Groups

The Dihedral Group D_n is the group of (rigid) symmetries of the regular n-polygon in the plane.

Ex:

1. $n = 1$. Uh.....
2. $n = 2$. A line. Can be reflected across its midpoint, to swap points A and B. One symmetry. The group of symmetries is {Identity, Flip}, and the binary operation is $*$ = composition of symmetries, i.e. flip it, then leave it alone, then flip it twice, etc. $I * I = I$, $I * F = F * I = F$, $F * F = I$. (It seems like there is only one group of order two... we've seen this multiplication table before... hooray for isomorphisms!)
3. $n = 3$. An equilateral triangle. Can be reflected along any of its three bisectors (L_0, L_1, L_2), or rotated in either direction. Let σ_k be reflection across L_k. Let ρ_k be rotation about the center of $\frac{2\pi k}{n}$. Then we have $D_3 = \{\rho_0, \rho_1, \rho_2, \sigma_1, \sigma_2, \sigma_3\}$. In this group, ρ_0 is the identity.

In general, $D_n = \{\rho_0, \ldots, \rho_{n-1}, \sigma_1, \ldots, \sigma_n\}$.

Remark:

$$\rho_i \rho_j = \rho_{i+j}$$
$$\rho_i \sigma_j = \sigma_{i+j}$$
$$\sigma_i \sigma_j = \rho_{i-j}$$
$$\sigma_i \rho_j = \sigma_{i-j}$$

Defn: Generators

A subset $S \subseteq G$ of a group $(G, *)$ is a set of generators if and only if every element of G can be written as a product of elements in S and their inverses. We notate this as $G = \langle S \rangle$.

Ex: $\mathbb{Z} = \langle 1 \rangle$ under addition.
$D_n = \langle \rho_0, \ldots, \rho_{n-1}, \sigma_1, \ldots, \sigma_n \rangle$

Defn: Relations
Any eqations satisfied by generators of G are called relations.

Defn: Presentation
A presentation of G is a set of generators and relations such that any other relations can be derived from those given. The notation we use is $G = \langle S|R \rangle$, using a vertical bar to separate the generators, S, and the relations, R.

Ex: $\mathcal{D}_{2n} = \langle r, s | r^n = s^2 = 1, rs = sr^{-1} \rangle$.

Question for next time: How does D_n compare to $\mathcal{D}_{2n}$?