M7210 Lecture 16 Friday September 28, 2012

Homomorphisms and their kernels

Definition. Let G and H be groups. A function $\phi : G \to H$ is called a *homomorphism* if it preserves the group structure, in the sense that:
$i)$ $\phi(e_G) = e_H$,
$ii)$ for all $g \in G$, $\phi(g^{-1}) = \big(\phi(g)\big)^{-1}$.
$iii)$ for all $f, g \in G$, $\phi(fg) = \phi(f)\phi(g)$.

Fact. Any function $\phi : G \to H$ that satisfies $iii)$ also satisfies $i)$ and $ii)$.
Proof. $iii) \Rightarrow i)$: $\phi(e_G) = \phi(e_G e_G) = \phi(e_G)\phi(e_G)$. Multiplying by $\big(\phi(e_G)\big)^{-1}$, we get $e_H = \phi(e_G)$.
$iii) \Rightarrow ii)$: $e_H = \phi(e_G) = \phi(g)\phi(g^{-1})$. Now multiply on the left by $(\phi(g))^{-1}$ and simplify to get $(\phi(g))^{-1} = \phi(g^{-1})$.

Definition. If $\phi : G \to H$ is a homomorphism, the *kernel of* ϕ, denoted $\ker\phi$, is the set $\{ g \in G \mid \phi(g) = e_H \}$.

Fact. $\phi(f) = \phi(g) \;\Leftrightarrow\; \phi(f)^{-1}\phi(g) = e_H \;\Leftrightarrow\; \phi(f^{-1}g) = e_H \;\Leftrightarrow\; f^{-1}g \in \ker\phi$.

Fact. $\ker\phi$ is a subgroup of G. If $g \in \ker\phi$ and $f \in G$, then $f^{-1}gf \in \ker\phi$.
Proof. Exercise.

Definition. A subgroup $N \subseteq G$ is said to be *normal* if $f^{-1}nf \in N$ whenever $n \in N$ and $f \in G$.

Note that the kernel of any homomorphism $\phi : G \to H$ is a normal subgroup of G.

Quotients of groups

Let G be a group. We seek to determine the equivalence relations $\sim$ on G that are compatible with the group structure, in the sense that the equivalence class of a product depends only on the classes of factors. We require, in other words, that

$$\text{if } f \sim f' \text{ and } g \sim g', \text{ then } fg \sim f'g'. \tag{$*$}$$

If this is true, then for all $f, g \in G$:
$i)$ if $e \sim g$, then $g^{-1} \sim gg^{-1} = e$
$ii)$ if $f \sim e$ and $g \sim e$ then $fg \sim e$.
$iii)$ if $g \sim e$, then $gf \sim f$ and $f^{-1}gf \sim f^{-1}f = e_G$.
$iv)$ if $g \sim f$ if and only if $f^{-1}g \sim e$.

This shows the first half of:

Proposition. *(a) If $\sim$ is any equivalence relation on a group G that is compatible with the group structure in the sense that $(*)$ is satisfied, then the set of elements that are equivalent to e forms a normal subgroup $N_\sim$. Moreover, $\sim$ is completely determined by $N_\sim$ in the sense that $f \sim g \Leftrightarrow f^{-1}g \in N_\sim$. (b) Conversely, if N is any normal subgroup, then the relation $\sim_N$ defined by $f \sim_N g \Leftrightarrow f^{-1}g \in N$ is an equivalence relation that satisfies $(*)$, and hence defines a group structure on the set of equivalence classes.*

Proof. We have already proved (a). The proof of (b) is left as an exercise. /////

What do the equivalence classes of $\sim_N$ look like? Fix $f \in G$. Then, for any $g \in G$:

$$f \sim_N g \;\Leftrightarrow\; f^{-1}g \in N \;\Leftrightarrow\; \exists n \in N,\, f^{-1}g = n \;\Leftrightarrow\; \exists n \in N,\, g = fn \;\Leftrightarrow\; g \in fN$$

Thus,

$$[f]_N = \{\, g \in G \mid f \sim_N g \,\} = fN$$

$fN = \{\, fn \mid n \in N \,\}$ is called a *left coset of* N. The set of all left cosets is denoted G/N. Our discussion has shown the following:

Proposition. *$(gN)(hN) = (gh)N$ is a well-defined group operation on G/N. In G/N, $(gN)^{-1} = g^{-1}N$ and $e_{G/N} = eN = N$. Moreover, $g \mapsto gN$ is a surjective group homomorphism from G onto G/N and that its kernel is N.*

N does double duty. On the one hand, it is a *normal subgroup of* G. On the other, it is an *element of* G/N.

Zeroth Isomorphism Theorem. *Let $\phi : G \to H$ be any homomorphism of groups, let K be its kernel and let $\pi_K : G \to G/K; g \mapsto gK$. Then $\phi = \overline{\phi}\,\pi_K$, where $\overline{\phi} : G/K \to H; gK \mapsto \phi(g)$.*

Remark. If K is merely contained in $\ker\phi$, the same conclusion can be made.

Cosets

So far, we have not made any use of cosets other than to note that the cosets of a normal subgroup are equivalence classes of a group-compatible equivalence relation. But cosets of subgroups that are *not* normal have a very important role in group theory.

Let H be a subgroup of G. The left coset gH is $\{\, gh \mid h \in H \,\}$, and the set of all left cosets is denoted G/H.

Note the following:

i) The cardinality of gH is the same as the cardinality of H.

ii) $g \in H$ if and only if $gH = H$.

iii) $f^{-1}g \in H \;\Leftrightarrow\; g \in fH \;\Leftrightarrow\; gH = fH$.

Lemma. *Two left cosets of H in G are either equal or disjoint.*

Proof 1. Suppose $x \in fH \cap gH$. Then there are $h_1, h_2 \in H$ such that $fh_1 = x = gh_2$. Then $f^{-1}g = h_1h_2^{-1} \in H$, so $fH = gH$. /////

Proof 2. The relation $\sim_H$ defined by $f \sim_H g :\Leftrightarrow f^{-1}g \in H$ is reflexive (because $e \in H$), symmetric (because H is closed under inversion, and $(f^{-1}g)^{-1} = g^{-1}f$) and transitive (because H is closed under the group operation, so $f^{-1}g, g^{-1}k \in H \;\Rightarrow\; f^{-1}k \in H$); *iii*) shows that the equivalence class of f is fH. /////

Theorem. *(Lagrange) If G is finite and H is a subgroup of G, then*

$$|G| = |G/H| \cdot |H|.$$

(Here, $|S|$ denotes the cardinality of S. The cardinality of a group is called its order*.)*

The *order* of $g \in G$ is the smallest cardinal number k so that $g^k = e$. (This is equal to the order of $\langle g \rangle :=$ the subgroup of G generated by g.)

Corollary. *If G is finite, the order of any element of G divides $|G|$.*

Proof. Consider the subgroup $\langle g \rangle = \{\, g^i \mid i \in \mathbb{Z} \,\}$.

Corollary. *A group of prime order has no proper subgroups.*