MATH H113: Honors Introduction to Abstract Algebra

2016-02-29

- Cosets and Normal Subgroups
- Lagrange's Theorem

Cosets and Normal Subgroups Continued

Remark on cosets: In additive notation cosets are written $a + H$ (or $H + a$) instead of aH (or Ha). Of course, if you're using additive notation, then the group is abelian, so $a + H = H + a$.
Note also: $m\mathbb{Z} = \{nm : n \in \mathbb{Z}\}$ is not a coset. It's a *subgroup*. Also $\mathbb{Z}/m\mathbb{Z}$ is just $\mathbb{Z}/N$ with $N = m\mathbb{Z}$.

Proposition: If $N \trianglelefteq G$, then the operation $\star$ on the set of left cosets of N defined by $(uN) \star (vN) = (uv)N$ is well defined.
Proof If $u'N = uN$ and $v'N = vN$, then $u' \in uN$ and $v' \in vN$, so $u'v' \in (uN)(vN) = u(Nv)N = u(vN)N = (uv)(NN) \subseteq (uv)N$, where $(uN)(vN)$ is defined as $\{xy : x \in uN, y \in vN\}$. $\therefore (u'v')N = (uv)N$.
Note: The converse was shown earlier.
Corollary: If $N \trianglelefteq G$, then the set of (left) cosets of N in G is a group, and $\pi : G \to$ (this group) is a surjective homomorphism, whose kernel is N. Furthermore the group *is* G/N (defined using π $(\{X_u : u \in \text{image of } \pi\}, X_u = \pi^{-1}(u), X_u X_v = X_{uv})$).
Proof: $\star$ (on set of cosets) is associative because
$(uN \star vN) \star wN = (uv)N \star wN = ((uv)w)N = (u(vw))N = \ldots = uN \star (vN \star wN)$.
Similarly $1N$ is an identity element, and $u^{-1}N$ is an inverse of uN. $\therefore$ this set is a group. Call it H. Then $\pi : G \to H$ is a homomorphism by definition, and is onto by definition.
Also, $u \in \ker \pi \iff uN = 1N = N \iff u \in N$, $\therefore \ker \pi = N$. This group *is* G/N, because for all cosets $a = uN$, $g \in X_a \iff \pi(g) = a \iff gN = uN \iff g \in uN$, so $X_a = uN$. $\therefore$ the set of H = set of $G/N = \{X_a : a \in H\}$ and $\star$ is the same: if $a = uN$ and $b = vN$
$X_a \star_{\text{old}} X_b = X_{ab} = X_{(uN)(vN)} = X_{(uv)N} = (uv)N$
and $uN \star vN = (uv)N$.
So from now on, for *any* subgroup H in G, define $G/H = \{aH : a \in G\}$ = set of left cosets. If H is normal, then G/H is a group.
Definition: π (as above) is called the natural projection.

Proposition: Let $\phi : G \to H$ be a surjective homomorphism, and let $N = \ker \phi$. Then, $\forall a \in H.\, X_a = \phi^{-1}(a) = uN$ for some $u \in G$.
Proof: $X_a \neq \emptyset$, so pick $a \in X_a$.
Then $v \in X_a \iff \phi(v) = a = \phi(u) \iff \phi(u^{-1}v) \in N$, because $\phi(u^{-1}v) =$

$\phi(u)^{-1}\phi(v) = a^{-1}a = 1$.
$\therefore X_a = uN$.

Proposition: A subgroup N of a group G is the kernel of some homomorphism from G if and only if $N \trianglelefteq G$.
Proof:

- $\implies$: $\phi : G \to H$ be a homomorphism and let $N = \ker\phi$. Then, for all $g \in G$, $gNg^{-1} \subseteq N$ because $x \in gNg^{-1} \implies x = gng^{-1}$ for some $n \in N$, and $\therefore \phi(x) = \phi(gng^{-1}) = \phi(g)\phi(n)\phi(g^{-1}) = \phi(g) \cdot 1 \cdot \phi(g)^{-1} = 1$. $\therefore x \in N$. $\therefore N \trianglelefteq G$.
- $\impliedby$: Suppose $N \trianglelefteq G$. Let $\pi : G \to G/N$ be the natural projection. Then π is a homomorphism and $N = \ker\pi$.

This answers question (1): which subgroups are kernels of homomorphisms?
(2) images of homomorphisms are $\cong G/N, N \trianglelefteq G$.
(3) if $N = \ker\phi$ then the image of ϕ is $\cong G/N$.

Lagrange's Theorem

This comes from: if $H \leq G$ and $u \in G$, then $|uH| = |H|$, because the map $f : H \to uH$ given by $f(h) = uh$ is bijective (onto by definition and 1-1 by cancelation: $ux = uy \implies x = y$).

Theorem (Lagrange's Theorem): If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.
Proof: Let $|G : H| = |G/H|$. Then $|G| = |G/H||H|$ because there are $|G/H|$ left cosets of H in G, and each of them has $|H|$ elements, and each element of G is in exactly one such coset.
Definition: $|G/H|$ is written $|G : H|$ or $(G : H)$. This is called the *index* of H in G.

Remark: The set of right cosets of H in G is written $H\backslash G : \{Hu : u \in G\}$. Also $|H\backslash G| = |G/H|$ (Ex. 3.2.12).

Corollary 1: If G is a finite group and $x \in G$, then $|x|$ divides $|G|$.
Proof: $|x| = |\langle x\rangle|$, an $\langle x\rangle$ is a subgroup of G, so $|\langle x\rangle|$ divides $|G|$.

Corollary 2: If G is a finite group and $n = |G|$, then $x^n = 1\ \forall x \in G$.
Proof: $x^{|x|} = 1$ and $|x|$ divides n, so $x^n = 1$.

Corollary 3: If G is a group of order p with p prime, then G is cyclic, so $G \cong \mathbb{Z}/p\mathbb{Z}$.
Proof: Let $x \in G$, $x \neq 1$. Then $|x| > 1$ and $|x|$ divides p, so $|x| = p$, $\therefore \langle x\rangle = G$ because they have the same (*finite*) number of elements, so G is cyclic.

Corollary 4: Let G be a group and H a subgroup. If $|G : H| = p$ is prime, then there are no subgroups between G and H (other than G and H themselves).

Proof: Let $K \leq G$ such that $K \supseteq H$. By Ex. 3.2.11, $p = |G : H| = |G : K||K : H|$. So since $|G : H|$ is prime, $|G : K| = 1$ or $|K : H| = 1$, so $\therefore K = G$ or $K = H$.
Note: $|G : K| = 1 \implies$ only one right coset of K in G, so $uK = 1K = K \forall u \in G$. $\therefore u \in K \; \forall u \in G$. $\therefore K = G$ (because $K \subseteq G$).