# MATH H113: Honors Introduction to Abstract Algebra

## 2016-02-26

- Subgroups and quotient groups

Homework due 2016-03-04:

- 2.5: 5, 10
- 3.1: 22, 24, 31, 39
- 3.2: 9, 12, 20

For groups $G$

1. What groups can $G$ map *onto*?
2. Which subgroups of $G$ can be kernels of homomorphisms?
3. How is the image of a homomorphism $G \to H$ related to its kernel?

Example of question (1).
For $G = \mathbb{Z}$, we know that $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ can occur as images of homomorphisms from $\mathbb{Z}$ and *no other groups* ($\mathbb{Z}$ is cyclic, so $\phi(\mathbb{Z})$ must also be cyclic) can (up to isomorphism).
Let $\phi : G \to H$ be a homomorphism. We may assume that $\phi$ is onto (otherwise replace $H$ with the image of $\phi$).
Then we can think of $\phi$ like this: (see fig 1.) For all $a \in H$, define $X_a$ to be the fiber over $a$:
$X_a = \phi^{-1}(a) = \{g \in G : \phi(g) = a\}$.
Let $K = \ker \phi =$ the kernel of $\phi = \{g \in G : \phi(g) = 1\} = X_1$

**Definition**: $G/K$ is the set $\{X_a : a \in H\}$.
Define a binary operation $\star$ on $G/K$ by $X_a \star X_b = X_{ab}$. (It's well defined because $X_a = X_b$ can only happen if $a = b$; if $\phi$ was not onto, this would not be true).
This makes $G/K$ into a group because:

1. $\star$ is associative:
   $(X_a \star X_b) \star X_c = X_a b \star X_c = X_{(ab)c} = X_{a(bc)} = X_a \star X_{bc} = X_a \star (X_b \star X_c)$.
2. $\star$ has an identity: $X_a \star X_1 = X_{a1} = X_a$, similarly for $X_1 \star X_a$.
3. $\star$ has an inverse $X_a^{-1} = X_{a^{-1}}$
   because $X_a X_{a^{-1}} = X_{aa^{-1}} = X_1$ and $X_{a^{-1}} X_a = X_{a^{-1}a} = X_1$
   $\therefore G/K$ is a group.

*Define* $\psi$: $G/K \to H$ by $\phi(X_a) = a$. Then $\psi$ is a homomorphism (by def. of $\star$), it is onto ($\psi(X_a) = a \ \forall a \in H$), and its 1-1 ($\psi(X_a) = \psi(X_b) \implies a = b \implies X_a = X_b$).
So $G/K \cong H$ (again, this assumes that $\phi$ is onto).
*Next step*: Eliminate $\phi$ from the picture. Try to do *all of this* (define $G/K$) with just $G$ and $K$.
Notice that the set $G/K$ is a collection of nonempty subsets of $G$; in fact, $G/K$ (the set) is a *partition* of $G$.
What equivalence relation on $G$ gives us this partition?
(Think of the example $\phi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, $n \mapsto \bar{n}$ (see fig 2)).

**Proposition**: Let $H$ be any subgroup of a group $G$. Let $\sim$ be the relation $u \sim v \iff u^{-1}v \in H$. Then $\sim$ is an equivalence relation on $G$:
**Proof**:

1. *reflexive*: $u^{-1}u = 1 \in H$, so $u \sim u \ \forall u \in G$
2. *symmetric*: $u \sim v \implies u^{-1}v \in H \implies v^{-1}u = (u^{-1}v)^{-1} \in H \implies v \sim u$
3. *transitive*: $u \sim v \wedge v \sim w \implies v^{-1}u, w^{-1}v \in H \implies (w^{-1}v)(v^{-1}u) \in H \implies w^{-1}u \in H \implies u \sim w$

**Proposition**: For any $u \in G$, the equivalence class of $u$ is $\bar{u} = \{uh : h \in H\}$
**Proof**: $v \in \bar{u} \iff u \sim v \iff u^{-1}v \in H \iff u^{-1}v = h$ for some $h \in H \iff v = uh$ for some $h \in H \iff v \in \{uh : h \in H\}$. $\therefore$ $\bar{u} = \{uh : h \in H\}$

**Definition**: The *left coset* $gH$ is $\{gh : h \in H\}$
The *right coset* $Hg$ is $\{hg : h \in H\}$
*Useful fact*: $uH = vH \iff \bar{u} = \bar{v} \iff u \sim v \iff v \in uH \iff u \in vH$.

Back to $G/K$ (defined using $\phi$).
I claim that $X_a = uK$ for any $u \in X_a$, because
$v \in X_a$
$\iff \phi(v) = a = \phi(u)$
$\iff \phi(u)^{-1}\phi(v) = 1$
$\iff \phi(u^{-1}v) = 1$
$\iff u^{-1}v \in K \ (K = \ker \phi)$
$\iff u \sim v \iff v \in \bar{u} = uK$.

So, for a subgroup $H$ of $K$, can we define $uH \star vH = (uv)H$? (In other words, is it well defined?)
*Check*: if $uH = u'H \implies u' = uh$ and $vH = v'H \implies v'k$, is $(uv)H = (u^{-1}v^{-1})H \ \forall h, k \in H$?
Is $uhvk \in (uv)H$?
Is $\cancel{u}hvk = (\cancel{u}v)h'$ for some $h' \in H$?
Is $v^{-1}hvk = h'$ for some $h' \in H$?
Is $v^{-1}hv = h'k^{-1}$ for some $h' \in H$?
Is $v^{-1}hv \in H$ for some $h' \in H$?

We'd need this to be true $\forall v \in G, \forall h \in H$, so (let $g = v^{-1}$): we need $ghg^{-1} \in H$ for all $h \in H$ in other words, we need $gHg^{-1} \subseteq H$ $\forall g \in G$.

**Definition**: Let $G$ be a group.

a. If $g, n \in G$ then $gng^{-1}$ is the *conjugate* of $n$ by $g$;
b. Let $N \leq G$ and $g \in G$. Then $gNg^{-1} = \{gng^{-1} : n \in N\}$ is the conjugate of $N$ by $g$;
c. Let $N \leq G$ and $g \in G$. Then g *normalizes* if $gNg^{-1} = N$.
d. A subgroup $N \leq G$ is a *normal* subgroup of $G$ if $g$ normalizes $N$ $\forall g \in G$. If this is true, we write $N \trianglelefteq G$.

**Examples**:

1. $\{1\} \trianglelefteq G$ and $G \trianglelefteq G$ for all groups $G$.
2. In an abelian group, all subgroups are normal subgroups of the group.
3. Let $G = S_3$ and $H = \langle x \rangle$, where $x = (1\ 2)$. Then $H$ is not normal in $G$, because (let $y = (1\ 3)$) $yxy^{-1} = (1\ 3)(1\ 2)(1\ 3) = (1)(2\ 3) \notin H$. So $yHy^{-1} \neq H$.

**Note**: $H$ is not normal in $G$, but $H$ is a normal subgroup of itself. In particular: if $N_1 \trianglelefteq N_2$ and $N_2 \trianglelefteq G$, it may be *false* that $N_1 \trianglelefteq G$.

**Theorem**: Let $G$ be a group and $N$ a subgroup of $G$. Then the following are equivalent:

1. $N \trianglelefteq G$;
2. $N_G(N) = G$;
3. $gN = Ng$ $\forall g \in G$;
4. $gNg^{-1} \subseteq N$ $\forall g \in G$.

**Proof**:

- (1) $\iff$ (2): $N \trianglelefteq \iff gNg^{-1} = N$ $\forall g \in G \iff g \in N_G(N)$ $\forall g \in G \iff N_G(N) = G$.
- (1) $\iff$ (4): Let $g \in G$ and $n \in N$. Want to show $n \in gNg^{-1}$. In fact since $g^{-1}N(g^{-1})^{-1} \leq N$, $g^{-1}ng \in N$, so $g(g^{-1}ng)g^{-1} = n \in gNg^{-1}$. $\therefore N \subseteq gNg^{-1}$.
- (2) $\iff$ (3): (1) $\implies gNg^{-1} = N$ $\forall g \in G \implies gNg^{-1}g = Ng$ $\forall g \in G \implies gN = Ng$ $\forall g \in G$. (3) $\implies$ (1) is similar.

**Note**: In general, if $A, B$ are subsets of $G$, $AB = \{ab : a \in A, b \in B\}$ and $gA = \{ga : a \in A\}$, $Ag = \{ag : a \in A\}$, and these are associative: $(AB)C = A(BC)$, $g(AB) = (gA)B$, etc.