MATH H113: Honors Introduction to Abstract Algebra

2016-02-08

- Homomorphisms
- Isomorphisms
- Group actions (if time permits)

For question 12 on page 45:
Assume $n \geq 6$. Also "pairs" means "unordered pairs".

More Examples of (Group) Homomorphisms:

3. If G and H are *any* groups, the constant function $\phi : G \to H$, $\phi(g) = 1\ \forall g \in G$ is a homomorphism called the *trivial* homomorphism.
4. If G is any group, the *identity map* $\phi : G \to G$, given by $\phi(g) = g$ is a homomorphism.
5. If F is any field and $a \in F$, then $\phi : (F, +) \to (F, +)$ given by $\phi(x) = ax$ is a homomorphism (by the distributive law).
   $a(x + y) = ax + ay$
   $\phi(x + y) = \phi(x) + \phi(y)$
6. If V and W are vector spaces over a field F, then V and W are abelian groups under addition, and any linear transformation $T : V \to W$ is a homomorphism of these groups: $T(\vec{v_1} + \vec{v_2}) = T(\vec{v_1}) + T(\vec{v_2})$.
7. If A and B are groups, then $p_1 : A \times B \to A$ and $p_2 : A \times B \to B$, given by $(a, b) \mapsto a$ and $(a, b) \mapsto b$, respectively are homomorphisms (called the *projection* maps).
8. If A and B are groups, then $i_1 : A \to A \times B$ given by $a \mapsto (a, 1)$ and $i_2 : B \to A \times B$ given by $b \mapsto (1, b)$ are homomorphisms.
9. If G is a group and $x \in G$, then $\phi : \mathbb{Z} \to G$ given by $n \mapsto x^n$, is a homomorphism.

Proposition: Let $\phi : G \to H$ be a group homomorphism.
Then:

a. $\phi(1_G) = 1_H$ (1_G and 1_H are the identity elements in G and H respectively)
b. $\phi(x^{-1}) = \phi(x)^{-1}\ \forall x \in G$ (inverse in H)
c. $\phi(x^n) = \phi(x)^n\ \forall x \in G, n \in \mathbb{Z}$
d. $|\phi(x)|$ divides $|x|\ \forall x \in G$ for which $|x| < \infty$

Proof:

a. $\phi(1_G) = \phi(1_G \times 1_G) = \phi(1_G)\phi(1_G)$ now cancel $\phi(1_G)$ to get (a)
b. $\phi(x)\phi(x^{-1}) = \phi(xx^{-1}) = \phi(1_G) = 1_H$, so $\phi(x^{-1})$ is the inverse of $\phi(x)$ in H
c. Consider the following cases:
    - $n = 0$ is (a)
    - $n > 0$ is by induction on n:
      $\phi(x^{n+1}) = \phi(x^n \times x) = \phi(x^n)\phi(x) = \phi(x)^n\phi(x) = \phi(x)^{n+1}$ (n = 1 case is trivial).
    - $n < 0$ is by the $n > 0$ case and (b):
      $\phi(x^n) = \phi((x^{-1})^{-n}) = \phi(x^{-1})^{-n} = (\phi(x)^{-1})^{-n} = \phi(x)^n$
d. Let $n = |x|$ (not always equal, see homework). Then $\phi(x)^n = \phi(x^n) = \phi(1_G) = 1_H$, so n is a multiple of $|\phi(x)|$.

Proposition: If $\phi : G \to H$ and $\psi : H \to N$ are homomorphisms, then so is $\psi \circ \phi : G \to N$.
Proof: $(\psi \circ \phi)(xy) = \psi(\phi(xy)) = \psi(\phi(x)\phi(y)) = \psi(\phi(x))\psi(\phi(y)) = ((\psi \circ \phi)(x))((\psi \circ \phi)(y))$

Isomorphisms

Definition: Let G and H be groups. An *isomorphism* ϕ from G to H is a homomorphism $\phi : G \to H$ that is also bijective. *Idea*: G and H are "the same" group.
Theorem: Let S be a set of groups. Define a relation $\sim$ on S by $G \sim H$ if there is an isomorphism from G to H. Then $\sim$ is an equivalence relation on S.
Proof:

- *Reflexivity*: $G \sim G \ \forall G \in S$ because the identity map from G to G is an isomorphism
- *Symmetry*: Assume $G \sim H$. Let $\phi : G \to H$ be an isomorphism. Since ϕ is bijective, it has an inverse $\phi^{-1} : H \to G$, characterized by $\phi \circ \phi^{-1} = \text{ identity on } H$, and $\phi^{-1} \circ \phi = \text{ identity on G}$.
  Need to check that ϕ^{-1} is a homomorphism.
  Let $a', b' \in H$. Let $a = \phi^{-1}(a')$, $b = \phi^{-1}(b')$, $c = ab$, and $c' = \phi(ab) = \phi(a)\phi(b) = a'b'$.
  Then $\phi^{-1}(a'b') = \phi^{-1}(c') = \phi^{-1}(\phi(ab)) = ab = \phi^{-1}(a')\phi^{-1}(b')$.
  $\therefore$ ϕ^{-1} is a homomorphism, so $H \sim G$
- *Transitivity*: Assume $G \sim H$ and $H \sim K$. Then there are isomorphisms $\phi : G \to H$ and $\psi : H \to K$. Therefore $\psi \circ \phi : G \to K$ is an isomorphism because its a homomorphism, and it's bijective. $\therefore G \sim K$.

Definition: Groups G and H are *isomorphic* if there's an isomorphism from G to H (or equivalently from H to G). This is written $G \cong H$ or $G \xrightarrow{\sim} H$ (if we're talking about the isomorphism).

Examples:

1. $S_2 \cong \mathbb{Z}/2\mathbb{Z}$.
   $(1) \mapsto \bar{0}$
   $(1\ 2) \mapsto \bar{1}$

	(1)	(1 2)
(1)	(1)	(1 2)
(1 2)	(1 2)	(1)

(+)	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

2. $S_3 \not\cong \mathbb{Z}/5\mathbb{Z}$. ($S_3$ has 6 elements, while $\mathbb{Z}/5\mathbb{Z}$ has 5 elements) so the sets can't be bijective. Any two isomorphic groups have the same number of elements.
3. $S_3 \not\cong \mathbb{Z}/6\mathbb{Z}$ (S_3 is non-abelian, $\mathbb{Z}/6\mathbb{Z}$ is abelian).
   If $\phi : S_3 \to \mathbb{Z}/6\mathbb{Z}$ is an isomorphism, then we should have $\phi((1\ 2)) + \phi((1\ 2\ 3)) \neq \phi((1\ 2\ 3)) + \phi((1\ 2))$ (in $\mathbb{Z}/6\mathbb{Z}$), because $(1\ 2)(1\ 2\ 3) \neq (1\ 2\ 3)(1\ 2)$ (in S_3), but we don't. If $G \cong H$ and G is abelian, then so is H. Any property of a group that can be stated without referring to specific elements (other than the identity) must be the same in isomorphic groups.
   $xy = yx\ \forall x, y \in G$ abelian.

Group Actions

Definition: An *action* of a group G on a set A is a function from $G \times A$ to A written $(g, a) \mapsto g \cdot a$ (or just ga), such that:

1. $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a\ \forall g_1, g_2 \in G, a \in A$;
2. $1 \cdot a = a\ \forall a \in A$

Also "G acts on A" means there's a group action of G on A.

Examples:

1. Let $n \in \mathbb{Z}_{>0}$. Then $\mathrm{GL}_n(\mathbb{R})$ acts on $\mathbb{R}^n$ by $A \cdot \vec{x} = A\vec{x}$ (matrix multiplication). Check:

1. $A \cdot (B \cdot \vec{x}) = A(B\vec{x})$ and $(AB) \cdot \vec{x} = (AB)\vec{x}$ and they're equal $\forall A, B \in \mathrm{GL}_n(\mathbb{R})$ and $\vec{x} \in \mathbb{R}^n$.
2. $I_n \cdot \vec{x} = I_n\vec{x} = \vec{x}\ \forall \vec{x} \in \mathbb{R}^n$.

Note this also works for $n = 0$, and with $\mathbb{R}$ replaced throughout by any field F: $\mathrm{GL}_n(F)$ acts on F^n the same way $\forall$ fields F and $\forall n \in \mathbb{N}$.