MATH H113: Honors Introduction to Abstract Algebra

2016-02-12

- Subgroups

No homework due next week (Study for the midterm!)

Exam on 2016-02-17:
Covers Chapters 0 and 1
Closed book: no notes, no calculators

Subgroups (continued)

$H \leq G \implies$

i. $H \subseteq G$
ii. $H \neq \emptyset$
iii. H is closed under the group operation
iv. H is closed under inversion

More Examples of Subgroups:

3. For any group G, $\{1\}$ is a subgroup, called the *trivial subgroup*
4. For any group G, $G \leq G$
5. For any group G, $\emptyset$ is *not* a subgroup
6. $\mathbb{N}$ is *not* a subgroup of $\mathbb{Z}$ (not closed under inversion).
7. If $N \leq H$ and $H \leq G$ then $N \leq G$
8. Let $\phi : G \to G'$ be a homomorphism:
    a. For all $H' \leq G'$,
    $\phi^{-1}(H') = \{g \in G : \phi(g) \in H'\}$ is a subgroup of G
    $\phi(1_G) = 1_{G'} \in H'$ so $\phi^{-1}(H') \ni 1_G$, $\phi^{-1}(H') \neq \emptyset$.
    $x, y \in \phi^{-1}(H') \implies \phi(x), \phi(y) \in H' \implies \phi(x)\phi(y) = \phi(xy) \in H' \implies xy \in \phi^{-1}(H')$ Similarly $x^{-1} \in \phi^{-1}(H')$
    In particular, $\ker \phi = \phi^{-1}(1_{G'})$ is a subgroup (take $H' =$ the trivial subgroup).
    b. If $H \leq G$, then $\phi(H) = \{\phi(x) \cdot x \in H\}$ is a subgroup of G'
    Similar proof
9. A linear subspace of a vector space is a subgroup (of its additive group)

Proposition: Let G be a group and let H be a subset of G. Then the following are equivalent (TFAE):

i. $H \leq G$ ($H \neq \emptyset$, $x, y \in H \implies xy \in H$, $x \in H \implies x^{-1} \in H$)
ii. $H \neq \emptyset$ and $xy^{-1} \in H \ \forall x, y \in H$
iii. H is a group, and the group operation on H is the restriction of the group operation on G

Proof:

- (i) $\implies$ (ii): clearly $H \neq \emptyset$. Let $x, y \in H$. Then $y^{-1} \in H$, so $xy^{-1} \in H$
- (ii) $\implies$ (i): Again $H \neq \emptyset$. Then $\exists x \in H$, so $1 = xx^{-1} \in H$. Then give $x \in H$, $1 \cdot x^{-1} \in H$, so $x^{-1} \in H$. Finally, $x, y \in H \implies x, y^{-1} \in H$, so $x(y^{-1})^{-1} = xy \in H$
- (i) $\implies$ (iii): exercise
- (iii) $\implies$ (i): Write $G = (G, \cdot)$ and $H = (H, \star)$. Then $x \star y = x \cdot y \ \forall x, y \in H$. H has an identity element, so $H \neq \emptyset$. The identity element of H = identity of G, because
  $1_H \cdot 1_H = 1_H \star 1_H = 1_H = 1_H \cdot 1_G$.
  Now cancel 1_H to get $1_H = 1_G$
  Similarly, for all $x \in H$, its inverse in H = inverse in G ($x \cdot x^{-1_H} = x \star x^{-1_H} = 1_H = 1_G$, $x \cdot x^{-1_G} = 1_G$)\$ $\therefore x \cdot x^{-1_H} = x \cdot x^{-1_G}$ now cancel x. In particular $x^{-1_G} \in H \ \forall x \in H$.
  $x \cdot y = x \star y \in H \ \forall x, y \in H$. $\therefore H$ is closed under $\cdot$.

Definition: Let G be a group and let $x \in G$. Then $\phi : \mathbb{Z} \to G$, given by $\phi(n) = x^n$, is a homomorphism, so its image is a subgroup of G. This image is called the *cyclic subgroup generated by* x, and is written (denoted) $\langle x \rangle$. (This is similar to the idea of generators and relations, except the relations come from G)

Suppose $|x| = \infty$.
Then $x^m \neq x^n \ \forall m \neq n$ because otherwise we can assume $m < n$, so $x^m = x^m \cdot x^{n-m}$, and we get $x^{n-m} = 1$, so $|x| \leq n - m$, contradiction. $\therefore \phi$ is 1-1, and its onto $\langle x \rangle$, so ϕ gives an isomorphism: $\langle x \rangle \cong \mathbb{Z}$.
(In particular, if G is finite, then all $x \in G$ have finite order since G can't contain an infinite subset $\langle x \rangle$.)
So suppose x has finite order: $|x| = n < \infty$.
Then $\langle x \rangle = \{1, x, x^2, \ldots, x^{n-1}\}$.
Clearly all of these elements are in $\langle x \rangle$, they are all different ($0 \leq i < j < n \implies x^i = x^j \implies x^{j-i} = 1$ with $0 < j - i < n$, contradiction).
Also every element of $\langle x \rangle$ lies in this set because $\forall m \in \mathbb{Z}$, write $m = qn + r, 0 \leq r < n$, then $x^m = (x^n)^q x^r = x^r \in \{1, x, x^2, \ldots x^{n-1}\}$.

So $\langle x \rangle$ is a subgroup of order n: $|\langle x \rangle| = |x|$.
Also $\phi : \mathbb{Z}/n\mathbb{Z} \to \langle x \rangle$ given by $\phi(\bar{m}) = x^m$ is an isomorphism, so $\langle x \rangle \cong \mathbb{Z}/n\mathbb{Z}$ (need to check that this is well defined: $\bar{m} = \bar{k} \implies x^m = x^k$, and this is a homomorphism $\phi(\bar{m}) \cdot \phi(\bar{k}) = x^m x^k = x^{m+k}$, $\phi(\bar{m} + \bar{k}) = \phi(\overline{m+k}) = x^{m+k}$).
Also, ϕ is 1-1, and onto (by definition).

Subgroups of S_3:
Elements of S_3: $1 = (1)$, $x = (1\ 2)$, $y = (1\ 3)$, $z = (2\ 3)$, $w = (1\ 2\ 3)$, $w^2 = w^{-1} = (3\ 2\ 1)$.
Easy subgroups (1), S_3 Nontrivial cyclic subgroups: $\langle x \rangle$, $\langle y \rangle$, $\langle z \rangle$, $\langle w \rangle$ ($\langle w^2 \rangle = \langle w \rangle$).
$\langle w \rangle = \{1, w, w^2\}$
$w^2 = w^{-1}$ has order 3 so, $\langle w^2 \rangle = \{1, w^2, w^4\} = \{1, w^2, w\} = \langle w \rangle$.
Let $H < S_3$.
Look at $|H \cap \{x, y, z\}|$.
If $|H \cap \{x, y, z\}| = 3$, then $H = S_3$, because $1 \in H$ (always), $x, y, z \in H$, and $yx = w$ is in H $(1\ 3)(1\ 2) = (1\ 2\ 3)$. $\therefore w^2 \in H$, so $S_3 \subseteq H$. If $|H \cap \{x, y, z\}| = 2$, then if
$H \cap \{x, y, z\} = \{x, y\}$ then $yx = w$ is in H, $\therefore z = wy$ is in H, contradiction.
$= \{x, y\}$ then $zx = w \ldots\ldots \therefore y = wx \ldots\ldots$
$= \{y, z\}$ then $yz = w \ldots\ldots \therefore x = wz \ldots\ldots$