MATH H113: Honors Introduction to Abstract Algebra

2016-02-19

- Cyclic groups

We are proving: **Proposition**: Any subgroup of $\mathbb{Z}$ is cyclic, and if it's nontrivial ($\neq \{0\}$), then it has a smallest positive element, which generates the subgroup.
Proof: Let $H \leq G$. If $H = \{0\}$, then it's cyclic (generated by 0).
Suppose $H \neq \{0\}$. Then it contains a nonzero element, say $n \in H, n \neq 0$. If $n < 0$ then $-n \in H$, so H contains positive elements. Therefore $H \cap \mathbb{Z}_{>0} \neq \emptyset$, so that set contains a smallest element. Call it m.
I claim that $H = \langle m \rangle$. Clearly $\langle m \rangle \subseteq H$.
To show that $H \subseteq \langle m \rangle$, let $x \in H$.
Write $x = qm + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < m$. Then $r = x - qm$; since $x \in H$ and $qm \in H$, we have $r \in H$. Then r has to be zero, because if $r > 0$, then $r \in H \cap \mathbb{Z}_{>0}$ and $r < m$, contradicting the fact that m was the smallest element of the set. So $r = 0$, $\therefore x = qm$, so $x \in \langle m \rangle$, $\therefore H = \langle m \rangle$.

Corollary: The set of subgroups of $\mathbb{Z}$ is in 1-1 corresponence (bijection) with the elements of $\mathbb{N}$, given by $m \in N \mapsto \langle m \rangle = H$.
By the above, this map is onto.
It's 1-1 because if $0 \leq a < b$, if $a = 0$ then $\langle a \rangle = \{0\}$ but $\langle b \rangle \neq \{0\} \implies \langle a \rangle \neq \langle b \rangle$.
If $a \neq 0$ then $a \in \langle a \rangle$ but $a \notin \langle b \rangle$ because if it was we'd have a is a multiple of b, so $\frac{a}{b} \in \mathbb{Z}$, but $0 < \frac{a}{b} < 1$, and there are no integer in that range.

Subgroups of $\mathbb{Z}/m\mathbb{Z}$ ($m \in \mathbb{Z}_{>0}$)

Lemma: Let $a, b \in \mathbb{Z}$, not both zero.
Then $\gcd(a, b)$ is the smallest positive integer that can be written in the form $xa + yb$ with $x, y \in \mathbb{Z}$.
Proof: Let $d = \gcd(a, b)$. Then $d > 0$ and d can be written in this form. On the other hand, suppose $d' > 0$ and $d' = xa + yb$ for some $x, y \in \mathbb{Z}$. Since $d \mid a$ and $d \mid b$, $d \mid (xa + yb)$, so $d \mid d'$. Then we can't have $d' > 0$ and $d' < d$, because then $\frac{d'}{d}$ would be an integer in the range $0 < \frac{d'}{d} < 1$.

(*Note*: $\{xa + yb : x, y \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$.)

Proposition: Let $m \in \mathbb{Z}_{>0}$, and let H be a subgroup of $\mathbb{Z}/m\mathbb{Z}$. Let d be the smallest element of $\{n \in \mathbb{Z}_{>0} : \bar{n} \in H\}$. (This is $\neq \emptyset$, because it contains m, since $\bar{m} \neq \bar{0}$ and $\bar{0} \in H$.) Then:

a. $H = \langle \bar{d} \rangle$ (so H is cyclic);

b. $d \mid m$; and
c. $|H| = \frac{m}{d}$

Proof:

a. We have a homomorphism $\pi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, given by $n \mapsto \bar{n}$, and $\pi^{-1}(H)$ is a subgroup of $\mathbb{Z}$ (because π is a homomorphism and H is a subgroup of $\mathbb{Z}/m\mathbb{Z}$). Then (from the def.) d is the smallest positive element of $\pi^{-1}(H)$, and $\pi^{-1}(H) = \langle d \rangle$.
Then $d \in \pi^{-1}(H) \implies \bar{d} \in H \implies \langle \bar{d} \rangle \subseteq H$. Conversely, if $\bar{x} \in H$, then $x \in \pi^{-1}(H)$, so $x = qd$ for some $q \in \mathbb{Z}$. Then $\bar{x} = \overline{qd} = q\bar{d}$ (proof of this is left to you as an exercise), so $\bar{x} \in \langle \bar{d} \rangle$, $\therefore H \subseteq \langle \bar{d} \rangle$. So $H = \langle \bar{d} rangle$.
b. As noted already, $m \in \pi^{-1}(H)$, so $m \in \langle d \rangle$, $\therefore m = qd$ for some $q \in \mathbb{Z}$, $\therefore d \mid m$.
c. Let $a = \frac{m}{d}$.
I claim that $H = \{\bar{0}, \bar{d}, \overline{2d}, \dots, \overline{(a-1)d}\}$
These are all in H and $0 < d < 2d < \ldots < (a-1)d < ad = m$ so they're all different.
On the other hand, any element of H can be written $\bar{x}$ with $0 \le x < m$. $\therefore$ $x \in \pi^{-1}(H)$, so $d \mid x$, $\therefore x \in \{0, d, 2d, \dots, (a-1)d\}$.
$H = \{\bar{0}, \bar{d}, \overline{2d}, \dots, \overline{(a-1)d}\}$, $\therefore |H| = a$, because the set has a elements.

Suppose we took *any* element $\bar{b} \in \mathbb{Z}/m\mathbb{Z}$ (could have $b < 0$ or $b \nmid m$), and let $H = \langle \bar{b} \rangle$. Then what is d? We'd have $\langle \bar{b} \rangle = \langle \bar{d} \rangle$ with $d > 0$ and $d \mid m$. How are b and d related?
Then $\pi^{-1}(H) = \{n \in \mathbb{Z} : \bar{n} = y\bar{b} \text{ for some } y \in \mathbb{Z}\}$
$= \{n \in \mathbb{Z} : n \equiv yb \pmod{m} \text{ for some } y \in \mathbb{Z}\}$
$= \{n \in \mathbb{Z} : n - yb = xm \text{ for some } x, y \in \mathbb{Z}\}$
\$= {xm + yb : $x, y \in \mathbb{Z}\}$\$
Since d is the smallest positive element of this set, $d = \gcd(b, m)$.

Proposition: Let $\bar{b} \in \mathbb{Z}/m\mathbb{Z}$. Then $\langle \bar{b} \rangle$ (in $\mathbb{Z}/m\mathbb{Z}$) generated by $\bar{d}$, where $d = \gcd(b, m)$ and $|\langle \bar{b} \rangle| = \frac{m}{\gcd(a,b)}$.
We also proved: if $m, b \in \mathbb{Z}$ and $m > 0$, then $\{xm + yb : x, y \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$, because it's $\pi^{-1}(\langle b \rangle)$ (this is true for any $b, m \in \mathbb{Z}$, can be proved directly).

Theorem (subgroups of $\mathbb{Z}/m\mathbb{Z}$): Let $m \in \mathbb{Z}_{>0}$. Then, for every positive divisor a of m, there is exactly one subgroup H of $\mathbb{Z}/m\mathbb{Z}$ of order a. It is equal to $\langle \bar{d} \rangle$, where $d = \frac{m}{a}$. Also, there are no subgroups of $\mathbb{Z}/m\mathbb{Z}$ of order not dividing m.
Proof: The last sentence follow from the earlier proposition.
Given $a \in \mathbb{Z}_{>0}$ with $a \mid m$, let $d = \frac{m}{a}$. Then $|\langle \bar{d} \rangle| = \frac{m}{\gcd(d,m)} = \frac{m}{d} = a$. For any other subgroup H of $\mathbb{Z}/m\mathbb{Z}$, write $H = \langle \bar{d'} \rangle$ with $d' > 0$ and $d' \mid m$. (Let $d' =$ smallest positive element of $\pi^{-1}(H)$.)
Since (by assumption) $H \neq \langle \bar{d} \rangle$, we must have $d' \neq d$, so $|H| = \frac{m}{d'} \neq a$.
$\therefore$ $\langle \bar{d} \rangle$ is the only subgroup of order a.

Therefore, the set of subgroups of $\mathbb{Z}/m\mathbb{Z}$ is in 1-1 correspondence with the set of positive divisors of m.

Next: Subgroups generated by subsets of a group.