Monday, Sept. 10

Subgroups of $U_6$ (cont'd)

$U_6 = \{1, 5, 5^2, 5^3, 5^4, 5^5\}$

We know about the trivial subgroup $\{1\}$.

Let $H$ be a nontrivial subgroup of $U_6$, and pick $a \in H$, $a \neq 1$.

$a = 5$ $\Rightarrow$ $H$ contains $1, 5, 5^2, 5^3, 5^4, 5^5$, so $H = U_6$.

$a = 5^5$ $\Rightarrow$ $H$ contains $a^5 = 1$, so again $H = U_6$.

$a = 5^2$ $\Rightarrow$ $H$ contains $1, 5^2, 5^4, 5^5$, so $H \geq U_2 = \{1, 5^2, 5^4\}$.

$a = 5^4$ $\Rightarrow$ $H$ contains $a^2 = 5^8 = 5^2$, so again $H \geq U_2$.

$a = 5^3$ $\Rightarrow$ $H$ contains $1, 5^3 = -1$, so $H \geq \{\pm 1\} = U_2$.

We're not done yet.

What if $a = 5^2$ and $H > U_2$?

Then there is a $b \in H$ such that $b \not\in U_2$.

Then $b = 5$ or $5^3$ or $5^5$.

If $b = 5^3$, then $H = U_6$.

Similarly if $a = 5^4$ and $H > U_2$ then $H = U_6$.

Also similarly if $a = 5^3$ and $H > U_2 = \{\pm 1\}$, then $H$ again must be all of $U_6$.

So all subgroups of $U_6$ are $\{1\}$, $U_2$, $U_3$, and $U_6$.

What are the subgroups of $\mathbb{Z}_6$?

Because $\mathbb{Z}_6 \cong U_6$, the subgroups correspond, and we get $\{0\}$, $\{0, 3\}$, $\{0, 2, 4\}$, and $\mathbb{Z}_6$. 
**Def:** Let $G$ be any group, written multiplicatively. For each $x \in G$ and $n \in \mathbb{Z}$, define

$$x^n = \begin{cases} \underbrace{x \cdot x \cdot \ldots \cdot x} \text{ (n times)} & \text{if } n > 0 \\ e & \text{if } n = 0 \\ (x')^{-n} & \text{if } n < 0 \\ \end{cases}$$

*(x')^{-1} = (x')^{1} = x'$

**(Notes):** $x^n \in G \ \forall \ n \in \mathbb{Z}$.
- Also, if $H \subseteq G$ and $x \in H$, then $x^n \in H \ \forall \ n \in \mathbb{Z}$.
- Applying this with $H = \{e\}$ and $x = e$ gives $e^n = e \ \forall \ n \in \mathbb{Z}$.
- $x^1 = x \ \forall \ x \in G$, so (using this definition with $n = -1$) we have $x^{-1} = (x')^{-1} = (x')^{1} = x'$, the inverse of $x$. So we can go back to writing $x^{-1}$ for the inverse of $x$.

**Thm:** Let $G$ be a group and let $x \in G$. Then

(a) $x^n \cdot x^m = x^{n+m}$  \hspace{2cm} (proved in the handout)

and (b) $(x^n)^m = x^{nm} \hspace{2cm} \forall \ n, m \in \mathbb{Z}.$

**Caution:** It's not always true that $(xy)^n = x^n y^n$.

**In additive notation:**

- $n \cdot 0 = 0$

- $n(x + m) = (n+m)x$

- $m(nx) = (km)x$

Also $n(x+y) = nx + ny$
Let $G$ be a group and let $a \in G$. Then $\{a^n : n \in \mathbb{Z}\}$ is a subgroup of $G$.

Moreover, any subgroup of $G$ that contains $a$ must also contain this subgroup.

(Recall $U_6$).

Proof: 1$^{st}$ part follows from (1) $a^n \cdot a^m = a^{n+m}$ \[ \text{and is closed under the group operation} \]

(2) $e \in \{a^n : n \in \mathbb{Z}\}$ because it's $a^0$

(3) $\{a^n : n \in \mathbb{Z}\}$ is closed under inverse because $(a^n)^{-1} = a^{-n}$

2$^{nd}$ part: If $a \in H$ (some subgroup) and $H \triangleleft G$, then $a^m \in H \forall n \in \mathbb{Z}$ as noted already.

Notation: The subgroup $\{a^n : n \in \mathbb{Z}\}$ is written $\langle a \rangle$, and is called the cyclic subgroup of $G$ generated by $a$.

Definition: A group $G$ is cyclic if $G = \langle a \rangle$ for some $a \in G$; if so, then $a$ is called a cyclic generator for $G$.

Cyclic subgroup and cyclic generator for a subgroup are defined similarly.

Examples: $\mathbb{Z}$ is cyclic, and $\mathbb{Z}_n$ is cyclic $\forall n \in \mathbb{Z}^+$

(in each case 1 is a cyclic generator).

$U_6$ is cyclic $\forall n \in \mathbb{Z}_n$ (because $U_6 \subseteq \mathbb{Z}_n$) (structural property).

(Smallest) example of a noncyclic group:

$V = \{e, a, b, c\}$,

<table>
<thead>
<tr>
<th></th>
<th>$e$</th>
<th>$a$</th>
<th>$b$</th>
<th>$c$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e$</td>
<td>$e$</td>
<td>$a$</td>
<td>$b$</td>
<td>$c$</td>
</tr>
<tr>
<td>$a$</td>
<td>$a$</td>
<td>$b$</td>
<td>$c$</td>
<td>$e$</td>
</tr>
<tr>
<td>$b$</td>
<td>$b$</td>
<td>$c$</td>
<td>$e$</td>
<td>$a$</td>
</tr>
<tr>
<td>$c$</td>
<td>$c$</td>
<td>$e$</td>
<td>$a$</td>
<td>$b$</td>
</tr>
</tbody>
</table>

$\langle e \rangle = \{e\}$

$\langle a \rangle = \{e, a\}$

$\langle b \rangle = \{e, b\}$

$\langle c \rangle = \{e, c\}$
Thm. All cyclic groups are abelian.

Proof. See book. TL; DR: $a^n \cdot a^m = a^{n+m} = a^{m+n} = a^{m} \cdot a^n$.

Let $G$ be a group and let $a \in G$. Then the order of $a$, written $|a|$, is the order of the cyclic subgroup generated by $a$: $|a| = |\langle a \rangle|$

We'll see soon that if $a^n = e$ for some $n \neq 0$, then $|a|$ is the smallest positive integer such that $a^n = e$ (which exists). Otherwise $|a| = \infty$.

**Lemma:** Let $G$ be a group and let $a \in G$.

(a). If $a$ has finite order then $\exists n_1, n_2 \in \mathbb{Z}$ such that $n_1 \neq n_2$ and $a^{n_1} = a^{n_2}$.

(b). If such $n_1$ and $n_2$ exist, then there is a positive integer $n$ such that $a^n = e$.

**Proof.** (a). Define a function $f: \mathbb{Z} \to \langle a \rangle$ by letting $f(n) = a^n$. Since $\lbrace n \rbrace$ is an infinite set, $\lbrace f(n) \rbrace$ is an infinite set.

Then, by the pigeonhole principle, $f$ is not 1-1, so there exist $n_1, n_2 \in \mathbb{Z}$ for which $f(n_1) = f(n_2)$. This means $a^{n_1} = a^{n_2}$.

(b). Let $n = \begin{cases} n_1 - n_2 & \text{if } n_1 \geq n_2 \\ n_2 - n_1 & \text{if } n_1 < n_2 \end{cases}$. Then $n > 0$, and $a^n = \begin{cases} a^{n_1 - n_2} = a^{n_1} \cdot (a^{n_2})^{-1} = e & \text{if } n_1 \geq n_2 \\ a^{n_2 - n_1} = a^{n_2} \cdot (a^{n_1})^{-1} = e & \text{if } n_1 < n_2 \end{cases}$ because $a^{n_1} = a^{n_2}$.