Math 113, Fall 2019
Lecture 7, Thursday, 9/19/2019

Topics Today:

- Cyclic groups (continued)
- Greatest common divisor
- More!!! on Cyclic groups
- Generating sets (time permitting)

1 Clicker Questions

1. How many of the following groups are cyclic?

$$U, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$$

Answer: 1, only $\mathbb{Z}$.

2. Which of the following are NOT cyclic?

$$\mathbb{Z}_3, \text{ the trivial group}, U_7, \tilde{\mathbb{Z}}_5.$$

Answer: All of the above.

2 Theorems on Cyclic Groups

Vojta notes there are three theorems regarding cyclic groups.

Theorem 2.1. Let G be a cyclic group.

(a) If G is infinite then $G \cong \mathbb{Z}$.

(b) If G is finite, then $G \cong \mathbb{Z}_n$, where $n := |G|$.

Moreover (not in the textbook), if G is finite and is generated by an element a, then n is the smallest positive integer such that $a^n = e$, and $G = \{e, a, a^2, \ldots, a^{n-1}\}$ (without repetition).
Further, $a^j = a^k \iff j \equiv k \pmod{n}$.

Proof. Let $a \in G$ be a cyclic generator. Define $f : \mathbb{Z} \to G$ by $f(m) = a^m$. By definition of cyclic generator, this is onto.
Case 1. If f is injective, then it is bijective. Also,

$$f(n+m) = a^{n+m} = a^n a^m = f(n)f(m),$$

so f has the homomorphism property and therefore defines an isomorphism between G and $\mathbb{Z}$. That is, $G \overset{f^{-1}}{\cong} \mathbb{Z}$.

Case 2. If f is NOT injective, then by the lemma from last lecture (7.1.a), there exists $n \in \mathbb{Z}^+$ with $a^n = e$.

Pick the **smallest** such n. Define $\varphi : \mathbb{Z}_n \to G$ by $\varphi(k) = a^k$. Notice this has the homomorphism property because

$$\begin{aligned}\varphi(j +_n k) &= \varphi(j + k \text{ or } j + k - n)\\ &= a^{j+k} \text{ or } a^{j+k-n}\\ &= a^j a^k \text{ or } a^j a^k \underbrace{(a^n)^{-1}}_{e}\\ &= a^j a^k \qquad \text{(in either case)}\\ &= \varphi(j)\varphi(k)\end{aligned}$$

Also, φ is injective because if $0 \le j < k < n$ and $\varphi(j) = \varphi(k)$ then $a^k = a^j$, so $a^{k-j} = e$. However, $0 < k - j < n$, and this contradicts the choice of n as the smallest such number.
Now, φ is onto because taking any $x \in \langle a \rangle = G$ equals a^m for some $m \in \mathbb{Z}$. Write $m = qn + r$ for some $q, r \in \mathbb{Z}$ and $0 \le r < n$ (via the division algorithm). Hence $r \in \mathbb{Z}_n$ (integer in the right range), and

$$a^m = a^{qn+r} = (a^n)^q a^r = e^q a^r = a^r = \varphi(r)$$

Hence x is in the image of φ, so φ is onto, one-to-one, and has the homomorphism property, so φ specifies the isomorphism $G \overset{\varphi}{\cong} \mathbb{Z}_n$.
Now we consider the two disjoint cases:
Case 1. G is infinite and $G \cong \mathbb{Z}$.
Case 2. G is finite and $G \cong \mathbb{Z}_n$.
(a) Now if G is infinite, then we fall under Case 1, so $G \cong \mathbb{Z}$.
(b) Similarly, if G is finite, then we fall under Case 2, and hence $G \cong \mathbb{Z}_n$.
The remaining parts follow from the proof of case 2.

□

Now we have our second theorem:

Theorem 2.2. A subgroup of a cyclic group is cyclic.

Proof. Let G be a cyclic group generated by a, and let $H \le G$.
Case 1. H is trivial. Then $H = \{e\} = \langle e \rangle$ is cyclic.
Case 2. H is nontrivial. Then H contains some element $x \ne e$, say $x = a^m$ for some $m \in \mathbb{Z}$. Then $m \ne 0$. If $m > 0$ then $m \in \mathbb{Z}^+$ and $a^m \in H$. On the other hand, if $m < 0$, then $-m \in \mathbb{Z}^+$ and $a^{-m} = x^{-1} \in H$. In either case, $\exists_{n \in \mathbb{Z}^+} : a^n \in H$. Pick the smallest such n.

Now we claim that $H = \langle a^n \rangle$. To see this, let $S := \{k \in \mathbb{Z} \mid a^k \in H\}$. Then $n \in S$, and also notice $jn \in S, \forall_{j \in \mathbb{Z}}$, which is because

$$a^{jn} = (a^n)^j = x^j \in H, \forall_{j \in \mathbb{Z}}.$$

Hence $S \supseteq n\mathbb{Z}$ (recall that $n\mathbb{Z} := \{nj \mid j \in \mathbb{Z}\}$).
Now suppose $S \ne n\mathbb{Z}$. Then there exists $m \in S$ with $m \notin n\mathbb{Z}$. So m is not a multiple of n.
So m is between two consecutive multiples of n:

$$jn < m < (j + 1)n.$$

Then $0 < m - jn < n$ and

$$a^{m-jn} = a^m (a^n)^{-j} = a^m x^{-j} \in H,$$

because $a^m, x \in H$. However, this contradicts the choice of n. Hence $S = n\mathbb{Z}$.
Therefore, $H \subseteq \{a^{nj} \mid j \in \mathbb{Z}\}$ because if $x \in H$, write $x = a^m$ for some $m \in \mathbb{Z}$. Then $m \in S$, so $m \in nj$, and hence

$$x \in \{a^{nj} \mid j \in \mathbb{Z}\} = \{(a^n)^j \mid j \in \mathbb{Z}\} = \langle a^n \rangle .$$

However, we also have $a^n \in G$, so that $\langle a^n \rangle \subseteq H$. Hence $H = \langle a^n \rangle$ is cyclic, completing the proof. □

If $G = \mathbb{Z}$, then we can take $a = 1$. This brings us to our corollary:

Corollary 2.2.1. The nontrivial subgroups of $\mathbb{Z}$ are exactly $n\mathbb{Z}$ for all $n \in \mathbb{Z}^+$, and these are different.

Proof. Take $G := \mathbb{Z}$ and $a = 1$, and let H be a nontrivial subgroup of $\mathbb{Z}$. Then $H = \langle n \rangle = n\mathbb{Z}$ (where n is the smallest positive element of H). Also, for all $n \in \mathbb{Z}^+$, notice $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ via our theorem. So we ave a one-to-one correspondence:

$$\mathbb{N} \cong \text{set of subgroups of } \mathbb{Z},$$

via the mapping $n \mapsto n\mathbb{Z}$. Note that 0 corresponds to the trivial subgroup. □

3 (Greatest Common) Divisors:

Definition: Divide -

Let $a, b \in \mathbb{Z}$ (we allow $a = 0$ or $b = 0$ or both). We say that a **divides** b and write

$$a \mid b,$$

if $aq = b$ for some $q \in \mathbb{Z}$. If so, then we also say that b is a "multiple" of a, or that a is a divisor of b.

Remark: Suppose $a \neq 0$. Then $a \mid b \iff \frac{b}{a} \in \mathbb{Z}$. If $a = 0$, then $0 \mid b \iff b = 0$.

Definition: Greatest common divisor (gcd) -

Let $r, s \in \mathbb{Z}$ (where one or both may be zero). Then the set

$$H := \{nr + ms \mid n, m \in \mathbb{Z}\}$$

is a **subgroup** of G, so it equals $d\mathbb{Z}$ for some **unique** $d \in \mathbb{N}$.
Then d is called the **greatest common divisor** of r and s, and we write:

$$d = \gcd(r, s).$$

Remark: Notice $r = 1 \cdot r + 0 \cdot s \in H$, so $d \mid r$. Similarly, $d \mid s$, so d is a **common divisor** of r and s. Since $d \in H$, there exist $m, n \in \mathbb{Z}$ such that $d = mr + ns$. So if $e \mid r$ and $e \mid s$, then $e \mid mr$ and $e \mid ns$, and hence $e \mid (mr + ns)$. Therefore, $e \mid d$, so $e \leq d$ (unless of course $d = 0$). So every common divisor is less than or equal to d, unless $= s = 0$.
Also, if $r \neq 0$ or $s \neq 0$, then $\gcd(r, s)$ is the smallest positive element of H. As for $r = s = 0$, then $\gcd(r, s) = \gcd(0, 0) := 0$.

4 Clicker Questions Again!!!

3. Let $H = 6\mathbb{Z} \cap 10\mathbb{Z}$. Then :
(A) H is not a subgroup of $\mathbb{Z}$
(B) H is a subgroup of $\mathbb{Z}$, but not a cyclic subgroup.
(C) $H = 2\mathbb{Z}$
(D) $H = 30\mathbb{Z}$
(E) None of the above.

4. Let $H = 6\mathbb{Z} \cup 10\mathbb{Z}$. Then :
(A) H is not a subgroup of $\mathbb{Z}$
(B) H is a subgroup of $\mathbb{Z}$, but not a cyclic subgroup.
(C) $H = 2\mathbb{Z}$
(D) $H = 30\mathbb{Z}$
(E) None of the above.

5 Subgroups of the Cyclic Groups

Example: Let $G = U_{10} = \langle \zeta \rangle$, where $\zeta = e^{\frac{2\pi i}{10}}$. We may ask what is $\left\langle \zeta^4 \right\rangle$? Let $b := \zeta^4$.
Drawing out a pentagram on the unit circle, we have that $\langle b \rangle$ has 5 elements (so we write $|b| = 5$). In fact, $\langle b \rangle = U_5 = \left\langle \zeta^2 \right\rangle$, where $\zeta^2 = e^{\frac{2\pi i}{5}}$.

5.1 Generalizing

Now in general, let G be a finite cyclic group of order n, generated by a, and let $s \in \mathbb{Z}$. What can we say about the cyclic subgroup $\langle b \rangle$, where $b := a^s$?
Let's revisit the proof of the earlier theorem, in that all subgroups of cyclic groups are cyclic. Let $H = \langle b \rangle$. We may ask, for which $m \in \mathbb{Z}$ is $a^m \in H$?
We notice:

$$\begin{aligned} a^m \in H &\iff a^m = b^j \text{ for some } j \in \mathbb{Z} \\ &\iff a^m = a^{sj} \\ &\iff m \equiv js \pmod{n} \\ &\iff m = in + js \text{ for some } i, j \in \mathbb{Z} \\ &\iff m \in \{in + js \mid i, j \in \mathbb{Z}\}, \end{aligned}$$

which is a subgroup of $\mathbb{Z}$ from earlier proof. The smallest positive such $m := \gcd(n, s)$, and H contains

$$a^d, a^{2d}, \ldots, a^{\frac{n}{d}d} = a^n = 1,$$

where all of these but the last are not equal to 1. So $H \supseteq \left\langle a^d \right\rangle$, and a^b has order $\frac{n}{d}$. To be continued.

Lecture ends here.