

# Math 113, Fall 2019

## Lecture 6, Tuesday, 9/17/2019

### 1 Clicker Questions:

1. Which of the following are cyclic groups:

- (A)  $\mathbb{Z}$ , generated by 1
- (B)  $U_n$  (with  $n \in \mathbb{Z}^+$ ), generated by  $\zeta = e^{2\pi i/n}$
- (C) Both**
- (D) Neither
- (E) Something Else

2. Applying the Division Algorithm to divide  $-53$  by  $10$  gives:

- (B)  $-53 = -6 \cdot 10 + 7$**
- (E) My clicker fell into the toilet and this was the only button that works.

### 2 Review

Last time, Vojta left us with a cliffhanger. Let  $\varphi : G \xrightarrow{\sim} G'$  be an isomorphism of groups and let  $H \leq G$ . Then

$$\varphi[G] = \{\varphi(x) : x \in H\}$$

is a subgroup of  $G'$ .

*Proof.* In the last lecture, we already did the case where  $\varphi[H] \neq \emptyset$ . Let  $a', b' \in \varphi[H]$ . Then  $\exists_{a,b \in H}$  such that  $\varphi(a) = a'$  and  $\varphi(b) = b'$ . Since  $H \leq G$ ,  $ab^{-1} \in H$ , so  $\varphi(ab^{-1}) \in \varphi[H]$ .

Additionally,

$$\varphi(ab^{-1})b' = \varphi(ab^{-1})\varphi(b) = \varphi(ab^{-1}b) = \varphi(a) = a',$$

so  $\varphi(ab^{-1})$  is a solution to  $xb' = a'$ . This implies  $\varphi(ab^{-1}) = a'(b')^{-1}$ , where  $\varphi(ab^{-1}) \in \varphi[H]$ . Hence  $a'(b')^{-1} \in \varphi[H]$ . Therefore we conclude that  $\varphi[H]$  is a subgroup of  $G'$ .

□

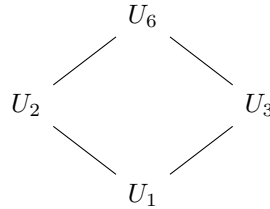
### 3 Extended Example:

Find all subgroups of  $U_6$ .

**Solution.** Recall that  $U_6 := \{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5\}$ , where  $\zeta := e^{\frac{2\pi i}{6}}$ . We already know that  $U_6$  has the trivial subgroups  $\{1\}$  and  $U_6$ . Are there any others? Let  $H$  be a nontrivial subgroup of  $U_6$ . Then  $H$  contains an element  $x \neq 1$ . If  $x = \zeta$ , then  $H$  contains  $\zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5, 1$ . Then  $H = U_6$ . If  $x = \zeta^2$ , then  $H$  contains  $\zeta^2, \zeta^4, \zeta^6 = 1$ , so  $H \supseteq \{1, \zeta^2, \zeta^4\} = U_3$ . We've found another subgroup,  $U_3 < U_6$ . If  $x = \zeta^3 = -1$ , then  $H$  contains  $\{-1, 1\} = U_2$ , so we've found yet another subgroup,  $U_2 < U_6$ . If  $x = \zeta^4$ , then  $H$  contains  $\zeta^4, \zeta^4 \cdot \zeta^4 = \zeta^3$  and 1, so  $H \supseteq \{1, \zeta^2, \zeta^4\} = U_3$ . If  $x = \zeta^5$ , then  $H$  contains  $x^{-1} = \zeta$ , hence as above,  $H = U_6$ . If  $H > U_3$ , then  $H$  contains  $\zeta$  or  $\zeta^3$  or  $\zeta^5$ . If  $H$  contains  $\zeta$  or  $\zeta^5$ , then  $H = U_6$ , as before. If  $H$  contains  $\zeta^3$ , then  $H$  also contains  $\zeta^3 \cdot \zeta^4 = \zeta$ , and so again  $H = U_6$ . Therefore there are no subgroups  $H$  with  $U_3 < H < U_6$ . If  $H > U_2$ , then  $H$  contains  $\zeta, \zeta^2, \zeta^4$ , or  $\zeta^5$ . If it's  $\zeta$  or  $\zeta^5$ , then  $H = U_6$ . If it's  $\zeta^2$  or  $\zeta^4$ , then  $H \supseteq U_3$ . Hence  $H > U_3$ . Therefore  $H = U_6$ , as before. Then in conclusion, subgroups of  $U_6$  are:

$$\{1\} = U_1, U_2, U_3, U_6.$$

We can make the diagram:



□

### 4 Group (Written Multiplicatively)

**Definition:**  $x^n$  -

Let  $G$  be a group (written multiplicatively). Let  $x \in G$ , and let  $n \in \mathbb{Z}$ . Define:

$$x^n := \begin{cases} \overbrace{x \cdot x \cdots x}^{n \text{ times}}, & n \geq 0 \\ e, & n = 0 \\ (x')^{-n}, & n < 0. \end{cases}$$

It is clear from this definition that  $x^1 = x$  for all  $x \in G$ , hence  $x^{-1} = (x')^1 = x'$ , so we go back to writing  $x^{-1}$  to denote the inverse.

In additive notation, we write  $nx$  instead of  $x^n$ . Then  $nx + mx = (n+m)x$ , and  $m(nx) = (mn)x$  (notice this is not the associative law). Also  $nx$  as defined here is  $n$  times  $x$  if  $G \leq \mathbb{C}$ . Also, we write  $(-1)x = -x$  as the additive inverse of  $x$ .

## 5 Cyclic Groups

**Theorem 5.1.** Let  $G$  be a multiplicative group, and let  $a \in G$ . Then:

- (a)  $\{a^n : n \in \mathbb{Z}\}$  is a subgroup of  $G$ ; call it  $\langle a \rangle$ .
- (b) All subgroups of  $G$  that contain  $a$  must also contain  $\langle a \rangle$ , and
- (c)  $\langle a \rangle$  is abelian (even if  $G$  isn't).

*Proof.* (a)  $\langle a \rangle$  is nonempty. Also, if  $x, y \in \langle a \rangle$ , then  $x = a^n$  and  $y = a^m$  for some  $n, m \in \mathbb{Z}$ . Then  $xy^{-1} = a^n(a^m)^{-1} = a^{n-m} \in \langle a \rangle$ . Hence  $\langle a \rangle \leq G$ .

(b) If  $H \leq G$  and  $a \in H$ , then  $a^n \in H, \forall n \in \mathbb{Z}$ .

(c) Consider:

$$a^n a^m = a^{n+m} = a^{m+n} = a^m a^n, \forall m, n \in \mathbb{Z}.$$

□

**Definition: Cyclic subgroup, Cyclic generator -**

The subgroup  $\langle a \rangle$  is called the **cyclic subgroup** of  $G$  generated by  $a$ . A group  $G$  or subgroup  $H$  is said to be **cyclic** if there is some  $a \in H$  or  $a \in G$  such that  $\langle a \rangle = G$  or  $\langle a \rangle = H$ , respectively.

If so, then we call  $a$  a **cyclic generator** of  $G$  or  $H$ , respectively.

We call it a ‘cyclic’ generator because later we will find that there are more generators we consider.

## 6 Clicker Questions:

1. Which are the cyclic generators of  $U_6$ ?

Define  $\zeta := e^{\frac{2\pi i}{6}}$ .

- (a)  $\zeta$  only
- (b)  $\zeta$  and  $\zeta^{-1}$  only
- (c)  $\zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5$ .
- (d) all elements of  $U_6$  are cyclic generators of  $U_6$
- (e) none of the above.

2. Which subgroups of  $U_6$  are cyclic subgroups?

- (a) Only  $U_6$  itself
- (b)  $U_6, U_2$  and  $U_3$  only
- (c) Only  $U_6$  and  $U_3$
- (d) all of them are
- (e) none of the above

## 7 Order of a Group

### Definition: Order -

The **order** of an element  $a \in G$  is the order of the cyclic subgroup that it generates. It is denoted  $|a|$ . So  $|a| = |\langle a \rangle|$ .

By convention, if  $\langle a \rangle$  is infinite, then we say that  $a$  has infinite order.

**Lemma 7.1.** Let  $G$  be a group and let  $a \in G$ .

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

(b) If there exists  $n_1$  and  $n_2$  as in (a) above, then  $\exists_{n \in \mathbb{Z}^+} : a^n = e$ .

*Proof.* (a) If  $|a| < \infty$ , then  $f : \mathbb{Z} \rightarrow \langle a \rangle$ , defined by  $f(n) = a^n$  maps an infinite set to a finite set, so  $f$  is NOT injective, as desired.

(b) Let  $G$  and  $a$  be as in the lemma, with  $|a| < \infty$ . Then  $a^{kn} = e \forall_{k \in \mathbb{Z}}$  because

$$a^{kn} = a^{nk} = (a^n)^k = e^k = e.$$

□

Now we may ask, are there any other integers  $m$  (other than multiples of our **order**  $n$ ) such that  $a^m = e$ ?

We claim that there aren't any such  $m$ . If there is such an  $m$ , then it's between multiples of  $n$ , so:

$$kn < m < (k+1)n.$$

Then  $0 < m - nk < n$ , and

$$a^{m-nk} = a^m (a^n)^{-k} = a^m e^{-k} = a^m = e,$$

contradicting our choice of  $n$ . So  $a^m = e \iff m$  is a multiple of  $|a|$ .

Lecture ends here.