

# Math 416 – Introduction to Abstract Algebra

## Chapter 4 – Cyclic groups

9/13 – HW #1 due: Ch 1, p. 37 # 2, 3, 12, 13, 16, 20, 22

9/18 – HW #2 due: Ch 2, p. 53 # 1, 2, 3, 6, 7, 13, 16, 22, 25, 26

9/20 - HW #3 due: Ch 3, p. 67 # 1, 2, 4, 6, 8, 9, 14, 21, 22, 28 (see p.47 example 17 and p. 45 example 9)

Online Quiz Zero – technical problems continue

10/2 – HW 4a due: Ch 4, p. 82 # 1, 3, 5, 8, 11

10/9 – HW 4b due: Ch 4, p. 82 # 13, 14, 16, 17, 23, 24, 45

Remember, sketchy definition of a group:

$G, \circ$

1. closed
2. associative
3. identity
4. inverses

Definition: A group  $G$  is *cyclic* if there is an element  $a$  in  $G$  such that

$$G = \{a^n : n \in \mathbb{Z}\} = \langle a \rangle$$

Example:  $\mathbb{Z}$  is cyclic

Example:  $\mathbb{Z}_n, +$  is cyclic, for any  $n$ , generated by 1, or by any other number relatively prime to  $n$ .

Example 3: Generators of  $\mathbb{Z}_8$  are 1, 3, 5 and 7.

Example 4:  $U_{10} = \{1, 3, 7, 9\}$  is cyclic. (operation is multiplication)  
generators are 3 and 7, not 1 or 9.

Theorem 4.1: If  $G$  is a group and  $\langle a \rangle$  a subgroup.

- a. If  $|a|$  is infinite, then all powers of  $a$  are distinct.
- b. If  $|a|$  is finite, say  $n$ , then  $\langle a \rangle = \{e, a^2, a^3, \dots, a^{n-1}\}$ , and  $a^i = a^j$  exactly when  $n$  divides  $i - j$ .

Proof plan: part a: Suppose two powers were equal, and show that the exponents are equal.

part b: First, suppose that the given elements were not distinct, and get a contradiction to the hypothesis that  $|a| = n$ . Then use the division algorithm to show that there are no other elements in  $\langle a \rangle$  by a direct proof, showing that every  $a^k$  is on the list somewhere.

Then suppose that  $a^i = a^j$ . Use the division algorithm and definition of order to show that  $n$  divides  $i - j$ . Then, finally, show directly that if  $n$  divides  $i - j$ , then  $a^i = a^j$ .

- a. distinct: suppose  $|a|$  is infinite and that  $a^i = a^j$ . Then  $a^{i-j} = e$ . Since  $|a|$  is infinite,  $i - j = 0$ , so  $i = j$ .
- b.
  1. Suppose that they were not distinct. Then some two are equal, say  $a^i = a^j$ , with  $0 \leq j < i < n$ . Then  $a^{i-j} = e$ , with  $0 < i - j < n$ . Contradicts definition of  $n$  being smallest.
  2. consider  $a^k$ , with  $k$  outside range of  $0$  to  $n-1$ , that is, suppose that  $a^k$  were apparently not on the list. Then divide  $k$  by  $n$ , to get  $k = qn + r$ , so  $a^k = a^{qn+r} = (a^n)^q a^r = e a^r = a^r$ , with  $0 \leq r < n-1$ . So  $a^k$  was on the list.
- c. Suppose  $a^i = a^j$ . write  $i - j = qn + r$ , so  $e = a^{i-j} = (a^n)^q a^r = e a^r = a^r$ , so  $r = 0$  (since  $0 \leq r < n-1$ ) so  $n \mid i - j$
- d. If  $n \mid (i - j)$  then  $i - j = nq$ , so  $a^{i-j} = e$ , so  $a^i = a^j$ .

QED.

Corollary 1:  $|a| = |\langle a \rangle|$

Corollary 2: if  $a^k = e$ , then  $|a|$  divides  $k$ .

Theorem 4.2: Let  $|a| = n$ . Then  $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$  and  $|\langle a^k \rangle| = \frac{n}{\gcd(n,k)}$

proof plan: This theorem has two parts, so we need a two-part proof.

The first part will be direct, and will use the division algorithm.

The second part will be direct and will be a calculation.

Proof: part 1: let  $d = \gcd(n,k)$ .

let  $k = dr$  (since  $d$  is a divisor of  $k$ , we can do this.)

$$a^k = a^{dr} = (a^d)^r$$

$\langle a^k \rangle$  is a subset of  $\langle a^d \rangle$

there are integers  $s$  and  $t$  such that  $d = ns + kt$  (gcd theorem 0.2)

$$a^d = a^{ns+kt} = a^{ns} a^{kt} = (a^n)^s (a^k)^t = e (a^k)^t = (a^k)^t \in \langle a^k \rangle$$

$$\text{so } \langle a^d \rangle \subseteq \langle a^k \rangle$$

recall that  $d = \gcd(n,k)$ , so we have

$$\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$$

end of part 1

part 2:

Claim:  $|a^d| = n/d$  whenever  $d$  is a divisor of  $n$ .

$$(a^d)^{n/d} = a^n = e \quad (\text{this would be wrong if } d \text{ didn't divide } n)$$

$$|a^d| \leq n/d \quad (\text{remember def'n of } |g|)$$

but suppose  $i < n/d$ . Then  $di < n$  and  $(a^d)^i = a^{di} \neq e$   
 since  $di < n$  and  $|a| = n$

So  $|a^d|$  can't be less than  $n/d$

$$\text{so } |a^d| = n/d$$

proving the claim.

Let  $d = \gcd(n,k)$ . ( $d$  divides  $n$ , so, by the claim ...)

$$|a^k| = |\langle a^k \rangle| \quad \text{by definition}$$

$$= |\langle a^{\gcd(n,k)} \rangle| \quad \text{by part 1}$$

$$= |\langle a^{\gcd(n,k)} \rangle| \quad \text{by definition}$$

$$= n/\gcd(n,k) \quad \text{by the claim.}$$

QED

Corollary 1: Let  $|a| = n$ . Then  $\langle a^i \rangle = \langle a^j \rangle$  exactly when  $\gcd(n,i) = \gcd(n,j)$

Application to drawing stars.

Corollary 2: Let  $G = \langle a \rangle$  with  $|G| = n$ . Then  $G = \langle a^k \rangle$  iff  $\gcd(n,k) = 1$

Corollary 3:  $k$  generates  $\mathbb{Z}_n$  iff  $\gcd(n,k) = 1$ .

Theorem 4.3: Fundamental theorem of cyclic groups.

Every subgroup of a cyclic group is cyclic.

If  $|\langle a \rangle| = n$ , then the order of any subgroup  $H$  of  $\langle a \rangle$  divides  $n$ .

If  $k$  is a divisor of  $n$ , then  $\langle a \rangle$  has exactly one subgroup of order  $k$ , and that subgroup is  $\langle a^{n/k} \rangle$

Trivia question:

Name another Fundamental Theorem that you should know.

Arithmetic (prime factorization)

Algebra ( $n$  roots of a polynomial of degree  $n$ )

Calculus

Still have to add the proof of Theorem 4.3.

$ZCGNQR^\circ \in \notin$