

# Math 416 – Introduction to Abstract Algebra

## Chapter 3 – Finite Groups and Subgroups

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

Remember, sketchy definition of a group:

$G, \circ$

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

Definition: The number of elements in a group is called the *order* of the group, denoted  $|G|$ . If  $G$  is not a finite group, we say it is an infinite group, even though “infinity” is not a number.

Examples:

$$|\mathbb{Z}_n| = n$$

$$|D_4| = 8$$

$|\mathbb{Z}|$  is infinite

$$|U_{10}| = 4$$

Definition: The *order* of an element  $g$  in  $G$  is the smallest positive integer  $n$ , if one exists, such that  $g^n = e$ . If no such exists, we say that  $g$  has infinite order. The order of  $g$  is denoted  $|g|$ .

Examples:

$|e| = 1$ , in any group

In  $D_4$ ,  $|R90| = 4$  and  $|f| = 2$  for any of the flips,  $D, D', H$  and  $V$ .

In  $\mathbb{Z}_{12,+}$ ,  $|2| = 6$ ,  $|3| = 4$ , and if  $a \triangleleft 1$  and  $\text{GCD}(a, 12)=1$ , then  $|a| = 12$

Definition: If  $H$  is a subset of  $G$ , and if  $H$  is a group under the same operation as  $G$ , then  $H$  is called a *subgroup* of  $G$ .

Examples:

In any group,  $G$ , both  $\{e\}$  and  $G$  itself are subgroups of  $G$ . These are called *trivial* subgroups. All other subgroups are called *proper*. A group with no proper subgroups is called *simple*.  $D_4$  is not simple, but  $\mathbb{Z}_p$  is simple exactly when  $p$  is prime.

In  $\mathbb{Z}$ ,  $+$ , the even integers form a subgroup of  $\mathbb{Z}$ .

This subgroup is denoted  $2\mathbb{Z}$ .

$3\mathbb{Z}$ ,  $4\mathbb{Z}$ , etc. are also subgroups.

$\mathbb{Z}_n$  is NOT a subgroup of  $\mathbb{Z}$ .

Its operation is different. In  $\mathbb{Z}$ ,  $(n-1) + 1 = n$ , but in  $\mathbb{Z}_n$ ,  $(n-1) + 1 = 0$ .

Theorem 3.1: One-step subgroup test:

Let  $G$  be a group and  $H$  be a (non-empty) subset of  $G$ . If  $ab^{-1}$  (or, in additive notation, if  $a - b$ ) is always in  $H$ , whenever  $a$  and  $b$  are both in  $H$ , then  $H$  is a subgroup of  $G$ .

Proof plan: To check each of the conditions in the definition of subgroup, but not necessarily in order:

0. non-empty subset
1. closed operation
2. associative
3. identity
4. inverses

Proof in five steps:

0. It is given that  $H$  is a non-empty subset.
2. The operation is the same, so it is associative.
3. If  $x$  is in  $H$ , then the condition guarantees that  $xx^{-1}$  is in  $H$  (take  $a = x$  and  $b = x$  in the condition), so  $e$  is in  $H$ .
4. Suppose  $x$  is in  $H$ . We know (from 3) that  $e$  is in  $H$ , so (take  $a = e$ ,  $b = x$ )  $ex^{-1} = x^{-1}$  is in  $H$ .
1. Suppose  $x$  and  $y$  are in  $H$ . Then (from 4)  $y^{-1}$  is in  $H$ . so (take  $a = x$ ,  $b = y^{-1}$ , and knowing that  $y^{-1-1}=y$ ),  $xy^{-1-1}=xy$  is in  $H$ .

QED

Example: Let  $G$  be an abelian group. Let  $H = \{x \in G : x^2 = e\}$ . Then  $H$  is a subgroup of  $G$ .

Note: this condition isn't really that weird. In  $D_4$ , the elements  $H$ ,  $V$ ,  $D$ ,  $D'$ ,  $e$  and  $R180$  all satisfy this property, but  $D_4$  isn't abelian, so the theorem doesn't apply here.

There are lots of abelian examples, though. In  $U_8$ , 1, 3, 5 and 7 have this property.

Proof plan: We need to show  $H$  is non-empty, and that it satisfies the  $ab^{-1}$  condition. That is, if  $a^2 = e$  and  $b^2 = e$ , then  $(ab^{-1})^2 = e$ ,

Proof.  $e \in H$  so  $H$  is non-empty.

Note, if  $x^2 = e$ , this means that  $x = x^{-1}$ .

Suppose that  $a$  and  $b$  are in  $H$ . This means that  $a^2 = e$  and  $b^2 = e$ .

$$\begin{aligned} \text{Then } (ab^{-1})^2 &= (ab)^2 && \text{(why?)} \\ &= (ab)(ab) \\ &= (aa)(bb) && \text{because } G \text{ is abelian} \\ &= e e \\ &= e \end{aligned}$$

so, by the definition of  $H$ ,  $ab^{-1}$  is in  $H$

so, by the one-step subgroup test,  $H$  is a subgroup.

QED

Theorem 3.2: Two-step subgroup test

Let  $G$  be a group and  $H$  be a nonempty subset of  $G$ . If  $ab$  is in  $H$  whenever  $a$  and  $b$  are in  $H$ , and if  $a^{-1}$  is in  $H$  whenever  $a$  is in  $H$ , then  $H$  is a subgroup of  $G$ .

Proof plan: a direct proof using theorem 3.1.

Proof: We are given that  $H$  is non-empty.

Suppose  $a$  and  $b$  are in  $H$ . Then  $b^{-1}$  is in  $H$ , by property 2. Then  $ab^{-1}$  is in  $H$  by property 1. Then  $H$  is a subgroup by theorem 3.1.

QED

Theorem 3.3: Finite subgroup test

Suppose  $H$  is a non-empty *finite* subset of  $G$ , and that  $H$  is closed under the operation of  $G$ . Then  $H$  is a subgroup of  $G$ .

Proof plan: To use a clever trick of Euler to show that  $H$  has inverses, and then to apply the two-step subgroup test.

Proof: Suppose that  $H$  is finite, non-empty and closed under the operation. Let  $a$  be any element of  $H$ . We will show that  $a^{-1}$  is in  $H$ .

Consider the sequence  $a, a^2, a^3, \dots$ . Since  $H$  is closed, all these elements must be in  $H$ .

$H$  has only finitely many elements, so eventually this sequence must repeat.

Suppose that the first repetition is that  $a^i = a^j$ , with  $i > j$ . Then  $a^{i-j} = e$ , and so  $a^{i-j-1} = a^{-1}$ , and it is in  $H$ .

So, by the two-step subgroup test,  $H$  is a subgroup.

QED

Notation: For  $a$  in  $G$ , let  $\langle a \rangle$  be the set of all elements  $a^n$ , where  $n$  is in  $\mathbb{Z}$ , including  $n=0$  giving  $e$  and  $n=-1$  giving  $a^{-1}$ .

Theorem 3.4:  $\langle a \rangle$  is a subgroup.

Let  $G$  be a group and  $a$  be any element of  $G$ . Then  $\langle a \rangle$  is a subgroup of  $G$ .

Proof plan: Direct proof using the one-step subgroup test. Two-step test would also work.

Proof: Let  $a$  be in  $G$ .  $a$  is in  $\langle a \rangle$  so  $\langle a \rangle$  is non-empty.

Suppose that  $x$  and  $y$  are in  $\langle a \rangle$ . Then for some  $m$  and  $n$ ,  $x=a^m$  and  $y=a^n$ .

Then  $y^{-1} = a^{-n}$  and  $xy^{-1} = a^{m-n}$ . That's in  $\langle a \rangle$ , so, by the one-step test,  $\langle a \rangle$  is a subgroup.

QED

Example: In  $D_n$ , let  $R$  be the smallest rotation,  $R(360/n)$ , and  $F$  be a flip. Then  $\langle R \rangle$  is a subgroup. It turns out that  $\langle R \rangle$  is all rotations, no flips.

Example: In  $\mathbb{Q}$ , take  $a = 1/2$ . Then  $\langle a \rangle$  is the set of all powers of  $2$ , (positive powers, and negative powers, which are still positive numbers.) This subgroup “behaves” just like the integers, since  $2^0$  is the identity, and when you multiply powers of  $2$  together, you just add exponents.

Definition: A group is called *cyclic* if has an element  $a$  such that  $G = \langle a \rangle$ .

Examples:  $\mathbb{Z}$  (+),  $\mathbb{Z}_n$ , and, for some values of  $n$ ,  $U_n$ .

Definition: The *Center* of a group  $G$ , denoted  $Z(G)$ , is the set of all elements of  $G$  that commute with every element of  $G$ . That is,

$$Z(G) = \{a \in G : \forall x \in G, ax = xa\}$$

Note that if  $G$  is abelian, then  $Z(G) = G$ , and conversely.  
(what does “and conversely” mean)

Theorem 3.5:  $Z(G)$  is a subgroup of  $G$ .

Proof plan: Direct proof using the two-step test. We could use the one-step test, but it is a little trickier.

Proof:  $e$  is in  $Z(G)$ , so  $Z(G)$  is nonempty. (Don't skip the "nonempty" part!)

Suppose that  $a$  and  $b$  are in  $Z(G)$ . We want to show that  $ab$  is in  $Z(G)$ .

Suppose that  $x$  is any element of  $G$ . Then

$$\begin{aligned}(ab)x &= a(bx) && \text{associativity} \\ &= a(xb) && \text{because } b \text{ is in } Z(G) \\ &= (ax)b && \text{associativity} \\ &= (xa)b && \text{because } a \text{ is in } Z(G) \\ &= x(ab) && \text{associativity.}\end{aligned}$$

So,  $ab$  is in  $Z(G)$

So, by the two-step test,  $Z(G)$  is a subgroup of  $G$ .

QED

Definition: If  $a$  is in  $G$ , then the *centralizer* of  $a$  in  $G$  is the set of all elements that commute with  $a$ , denoted  $C(a)$ . That is,

$$C(a) = \{x \in G : ax = xa\}$$

"Obviously",  $e \in C(a)$ , so  $C(a)$  is nonempty.

In fact,  $Z(G) \subseteq C(a)$ , since elements of  $Z(G)$  have to commute with everything, but elements of  $C(a)$  only have to commute with  $a$ .

$$\text{In fact, } Z(G) = \bigcap_{a \in G} C(a).$$

Theorem 3.6:  $C(a)$  is a subgroup, for each  $a$  in  $G$ .

Proof plan: to make you do it as an exercise.

ZCGNQR°