

## CONSTRUCTING GROUPS

**The “Sudoku” Rule.** If  $G$  is a finite group of order  $n$ , then every row and every column of the multiplication  $(*)$  table for  $G$  is a permutation of the  $n$  elements of the group. In particular, the row and column for multiplication by the identity element  $e$  is just the identity permutation.

**Warning:** A table satisfying the Sudoku Rules is not necessarily the multiplication table for a group. Why not?

**Lagrange’s Theorem.** The order of a subgroup divides the order of the group.

**Consequence.** The order of any element of the group divides the order of the group.

Proof: If  $a$  has order  $m$ , then  $H = \{a, a^2, a^3, \dots, a^m = e\}$  is a subgroup of  $G$ .

**Our Goal:** Find all groups of order 6.

**Homework Problem 1.** If  $G$  is a finite group whose order is even, then there exists an element  $a \in G$  of order 2, i.e.,  $a \neq e$  and  $a^2 = e$ .

**Homework Problem 2.** If every element  $a$  in  $G$  satisfies  $a^2 = e$ , then  $G$  is abelian.

Let  $G$  be a group of order 6.

Step 1. By Homework Problem 1, since 6 is even, there is an element  $a$  in  $G$  of order 2.

Step 2. What can we say about the other four elements of the group besides  $e$  and  $a$ ?

Their orders must be either 1, 2, 3, or 6 by Lagrange’s Theorem. We can rule out order 1 since the identity element is the only element whose order is 1.

Step 3. We wish to show that there is an element  $b \in G$  of order 3.

Step 4. Case (i). Suppose there is an element  $c \in G$  of order 6. Let  $b = c^2$ . Then  $b^3 = (c^2)^3 = c^6 = e$ , so  $b$  has order 3.

Step 5. Case (ii). Suppose no element in  $G$  has order 6. Then the four elements other than  $e$  and  $a$  have order 2 or 3. Suppose all four elements have order 2. At first there seems to be no reason why this couldn’t happen. After all, all non-identity elements of the Klein 4-group have order 2.

2

Step 6. Assuming that all elements of  $G$  satisfy  $g^2 = e$ , our first observation is that  $G$  must be abelian by Homework Problem 2.

Step 7. Let  $c$  be an element of  $G$  other than  $a$  whose order is 2. Consider  $H = \{e, a, c, ac\}$ . Since  $G$  is abelian,  $H$  is a subgroup. The important equation is

$$(ac)^2 = (ac)(ac) = a(ca)c = a(ac)c = (a^2) * (c^2) = e^2 = e,$$

which require that  $ca = ac$ . But this means that  $G$  has a subgroup of order 4, violating Lagrange's Theorem, since 4 does not divide 6.

Step 8. Conclusion: Not all non-identity elements of  $G$  have order 2. Since we are in the case where no element has order 6, it follows logically that some element  $b$  has order 3.

Step 9. Together steps 3 and 4 show that there exists an element  $b$  in  $G$  of order 3.

Step 10.  $G$  has the subgroup  $H = \langle b \rangle = \{e, b, b^2\}$ .

Step 11. The coset  $aH = \{a, ab, ab^2\}$  consists of 3 elements of the group distinct from the elements of  $H$ . (Cosets are either disjoint or identical and  $a$  cannot lie in  $H$ , since no element of  $H$  can have order 2 by Lagrange's Theorem.) Together  $H$  and  $aH$  must comprise all 6 elements of  $G$ .

Step 12. The group is  $G = \{e, b, b^2, a, ab, ab^2\}$  and so far the group table looks like:

	$e$	$b$	$b^2$	$a$	$ab$	$ab^2$
$e$	$e$	$b$	$b^2$	$a$	$ab$	$ab^2$
$b$	$b$	$b^2$	$e$			
$b^2$	$b^2$	$e$	$b$			
$a$	$a$			$e$		
$ab$	$ab$					
$ab^2$	$ab^2$					

Step 13. By the Sudoku Rule, there are only two choices for  $ba$ : Choice (1)  $ba = ab$  and Choice (2)  $ba = ab^2$ .

Table 1:  $ba = ab$ 

	$e$	$b$	$b^2$	$a$	$ab$	$ab^2$
$e$	$e$	$b$	$b^2$	$a$	$ab$	$ab^2$
$b$	$b$	$b^2$	$e$	$ab$		
$b^2$	$b^2$	$e$	$b$			
$a$	$a$			$e$		
$ab$	$ab$					
$ab^2$	$ab^2$					

Table 2:  $ba = ab^2$ 

	$e$	$b$	$b^2$	$a$	$ab$	$ab^2$
$e$	$e$	$b$	$b^2$	$a$	$ab$	$ab^2$
$b$	$b$	$b^2$	$e$	$ab^2$		
$b^2$	$b^2$	$e$	$b$			
$a$	$a$			$e$		
$ab$	$ab$					
$ab^2$	$ab^2$					

Complete Tables 1 and 2. Besides the Sudoku Rules, you may find it useful to use associativity. For example, in computing the multiplication  $b * (ab)$  in Table 1, since we know that  $ba = ab$ , we can deduce  $b(ab) = (ba)b = abb = ab^2$ .

Choice 1.  $ba = ab$ . To find a model for this group, let  $G = \mathbb{Z}_7^\times = \{1, 2, 3, 4, 5, 6\}$  under multiplication mod 7.

$b = 2$  has order 3, since  $2^2 = 4$  and  $2^3 = 8 \equiv 1 \pmod{7}$ .

$a = -1$  has order 2, since  $(-1)^2 = 1$ .

The group consists of the subgroup  $H = \langle 2 \rangle = \{1, 2, 4\}$  and  $(-1)H = \{-1, -2, -4\} = \{6, 5, 3\}$ .

The group is cyclic, of order 6, and has two generators: 3 and 5.

Choice 2.  $ba = ab^2$ . To find a model for this group, let  $G =$  the permutation group  $S_3$ .

$b = (1, 2, 3)$  has order 3, since  $b^2 = (1, 3, 2)$  and  $b^3 = \text{id}$ .

$a = (1, 2)$  has order 2, since  $a^2 = \text{id}$ .

The group consists of the subgroup  $H = \langle b \rangle = \{\text{id}, (1, 2, 3), (1, 3, 2)\}$  and  $aH$ . Observe that  $ab = (1, 2)(1, 2, 3) = (2, 3)$  and  $ab^2 = (1, 2)(1, 3, 2) = (1, 3)$ .

The group is non-abelian, of order 6.