

## Homework Two Solutions

Note that I have given answers in quite a bit more detail than you were expected to give on the homework. In particular, for the “find a set of generators and relations” problems, at this point in your algebra learning experience, I am happy if you write down a correct presentation without all the extra arguments I included. I give them to you to give a rigorous answer to the obvious question you almost certainly asked yourself while working the solution out— “How do I know that this is right?”

- (1.3.20) Find a set of generators and relations for  $S_3$ .

By analogy to  $D_6$  (which we mentioned in passing in class the other day is “the same” group as  $S_3$ ) we let  $r = (123)$  and  $s = (12)$ . Note that  $r^3 = s^2 = 1$ . Now  $r^2 = (132)$  and by direct computation  $rs = (123)(12) = (13)$  and  $sr^2 = (12)(132) = (13)$ , so  $rs = sr^2$ . Thus by writing  $r = (123)$  and  $s = (12)$  we have shown that the dihedral group relations with  $n = 3$  hold for  $S_3$ . By our dihedral group work, we have that this will indeed generate a group of order 6. We can check all of the multiplications:

$$\begin{array}{ll}
 1 & 1 \\
 (12) & s \\
 (13) & sr^2 = (12)(123)(123) \\
 (23) & sr = (12)(123) \\
 (123) & r \\
 (132) & r^2 = (123)(123)
 \end{array}$$

Thus our presentation would be  $\langle r, s \mid r^3 = s^2 = 1, rs = sr^2 \rangle$ . Note that this is not the only way to do it. To show you something quite different, let  $x = (12)$  and  $y = (23)$ . Note that  $xy = (123)$ ,  $yx = (132)$ , and  $xyx = (13)$ , so we can use  $x$  and  $y$  as our generators. Trying to find relations, we see at once that  $x^2 = y^2 = 1$ . Furthermore,  $(13) = xyx$ , so we include the relation  $xyx = xyx$ . Thus far we have, as a “working presentation,”  $\langle x, y \mid x^2 = y^2 = 1, xyx = xyx \rangle$ . We are able to write each element of  $S_3$  in terms of  $x$  and  $y$ , using words of length at most 3, and by the relations, the only such possible elements would be  $1, x, y, xy, yx, xyx$  since  $x^2 = y^2 = 1$  and  $xyx = xyx$ . It remains to show that these are the only possible elements, that is, if we have a word of length 4 or more in  $x$  and  $y$ , it is equivalent to one of the words already on the list. We notice that  $x^2 = y^2 = 1$  implies that the only words we need to consider are those in which  $x$  and  $y$  alternate.

We proceed by a quick induction on the length of the word, beginning with length 4. The two words under consideration are  $xyxy$  and  $yxyx$ . Using the  $xyx = xyx$  relation, we can re-express these as follows:

$$xyxy = yxyy = yx \qquad yxyx = xyxx = xy$$

so any word of length 4 is equivalent to a word of length 3 or less. Assuming now that the result holds for words of length less than  $n$ , we consider a word of length  $n$ , and again, need only consider alternating words, so our word is either  $xyxy \dots$  or  $yxyx \dots$ . As in the base case of the induction, these are equivalent to  $yx \dots$  or  $xy \dots$ ,

and by the induction hypothesis, these are equivalent to a word of length 3 or less, and so the entire group  $\langle x, y | x^2 = y^2 = 1, xyx = yxy \rangle$  consists of the six elements  $\{1, x, y, xy, yx, xyx\}$  as claimed, and by the identification above  $x = (12)$  and  $y = (23)$  our group is the same as  $S_3$ .

- (1.5.2) Write out the group tables for  $S_3, D_8$  and  $Q_8$ .

	○	1	(12)	(13)	(23)	(123)	(132)
	1	1	(12)	(13)	(23)	(123)	(132)
$S_3$ :	(12)	(12)	1	(132)	(123)	(23)	(13)
	(13)	(13)	(123)	1	(132)	(12)	(23)
	(23)	(23)	(132)	(123)	1	(13)	(12)
	(123)	(123)	(13)	(23)	(12)	(132)	1
	(132)	(132)	(23)	(12)	(13)	1	(123)

	·	1	$r$	$r^2$	$r^3$	$s$	$sr$	$sr^2$	$sr^3$
	1	1	$r$	$r^2$	$r^3$	$s$	$sr$	$sr^2$	$sr^3$
$D_8$ :	$r$	$r$	$r^2$	$r^3$	1	$sr^3$	$s$	$sr$	$sr^2$
	$r^2$	$r^2$	$r^3$	1	$r$	$sr^2$	$sr^3$	$s$	$sr$
	$r^3$	$r^3$	1	$r$	$r^2$	$sr$	$sr^2$	$sr^3$	$s$
	$s$	$s$	$sr$	$sr^2$	$sr^3$	1	$r$	$r^2$	$r^3$
	$sr$	$sr$	$sr^2$	$sr^3$	$s$	$r^3$	1	$r$	$r^2$
	$sr^2$	$sr^2$	$sr^3$	$s$	$sr$	$r^2$	$r^3$	1	$r$
	$sr^3$	$sr^3$	$s$	$sr$	$sr^2$	$r$	$r^2$	$r^3$	1

	·	1	-1	$i$	- $i$	$j$	- $j$	$k$	- $k$
	1	1	-1	$i$	- $i$	$j$	- $j$	$k$	- $k$
$Q_8$ :	-1	-1	1	- $i$	$i$	- $j$	$j$	- $k$	$k$
	$i$	$i$	- $i$	-1	1	$k$	- $k$	- $j$	$j$
	- $i$	- $i$	$i$	1	-1	- $k$	$k$	$j$	- $j$
	$j$	$j$	- $j$	- $k$	$k$	-1	1	$i$	- $i$
	- $j$	- $j$	$j$	$k$	- $k$	1	-1	- $i$	$i$
	$k$	$k$	- $k$	$j$	- $j$	$i$	- $i$	-1	1
	- $k$	- $k$	$k$	- $j$	$j$	- $i$	$i$	1	-1

- (1.5.3) Find a set of generators and relations for  $Q_8$ .

We will strive for (relative) ease of exposition, rather than trying to do it with the smallest possible number of generators and relations. We will take as generators the symbols  $i, j$  and  $-1$ . Elements of our group are then words (strings if you like) made up of the characters  $i, j$ , and  $-1$ . We impose first the relations  $i(-1) = -1i$  and  $j(-1) = -1j$ , so  $-1$  will commute with both  $i$  and  $j$ . Next we insist that  $ij = -1ji$  (of course in our heads we're identifying  $ij$  with  $k$ , but we have no such symbol to use in our words). Finally we insist that  $-1^2 = 1$  and  $i^2 = j^2 = -1$ . Thus our presentation is:

$$\langle i, j, -1 | i(-1) = -1i, j(-1) = -1j, ij = -1ji, (-1)^2 = 1, i^2 = j^2 = -1 \rangle .$$

We need to do two things, first we must establish that the elements  $i, j, -1$  and  $ij$  (which we're thinking of as  $k$ ) behave like their counterparts in  $Q_8$ . Second we must show that there are only eight elements in the group determined by our presentation (otherwise we might have a group in which  $Q_8$  is a subgroup, but not have a presentation of  $Q_8$  itself).

First we note that  $-1$  behaves as expected, and that  $ij = -1(ji)$  gives us the expected  $ij = k$  and  $ji = -k$ . Now  $i^2 = -1$  and  $(-1)^2 = 1$  together imply that  $i^4 = 1$ , and since  $i^3 = i^2i = -1i$  we have  $i^{-1} = (-1)i$  as expected. The analogous result holds for  $j$ . Considering  $k$  we have  $(ij)^2 = ijij = i[(-1)ij]j = -1iijj = (-1)(-1)(-1) = 1(-1) = -1$ . Thus we have  $k^2 = -1$  as we'd hope, and it follows that  $k^3 = -k$  and  $k^4 = 1$  as we'd hope. To finish up the correspondence with  $Q_8$  we need  $jk = i$ , and we see that " $jk$ " =  $j(ij) = (ji)j = -1(ij)j = -1i(-1) = (-1)(-1)i = i$ . Also " $kj$ " =  $ijj = i(-1) = (-1)i$  as we'd expect. Finally we need to check that  $ki = j$  and  $ik = -j$  hold. To this end, we consider " $ki$ " =  $iji = i(-1)(-1)ji = -1i[(-1)ji] = -1iij = (-1)(-1)j = j$  and " $ik$ " =  $ijj = (-1)j$ .

We have now shown that the elements  $i, j$ , and  $-1$  give us a multiplication that, with  $ij$  corresponding to  $k$ , mimics the multiplication in  $Q_8$ . It remains to show that the presentation

$$\langle i, j, -1 \mid i(-1) = -1i, j(-1) = -1j, ij = -1ji, (-1)^2 = 1, i^2 = j^2 = -1 \rangle.$$

results in a group with 8 elements. Elements of this group consist of words in  $i, j$ , and  $-1$ . We claim that any such word may be written in the form  $-1^\ell i^m j^n$ . To see this, note first that  $-1$  commutes with both  $i$  and  $j$ , so we can move all of the  $-1$  letters to the left of the word without changing its value in the group. Any time an  $i$  shows up to the right of a  $j$ , we use  $ji = (-1)(-1)ji = (-1)[(-1)ji] = (-1)ij$  to, for the price of a  $-1$ , pull the  $i$  to the left (and the  $-1$  could then be pulled all the way to the left). At this point we count the distinct strings  $-1^\ell i^m j^n$ . Since  $-1^2 = 1$  we have  $\ell = 0$  or  $1$ . We also observe that  $i^2 = -1$  and  $j^2 = -1$  imply that  $m$  and  $n$  are either 0 or 1 as well.

We can now just enumerate all possible words  $1, -1, i, j, -1i, -1j, ij, -1ij$ , corresponding to the eight possible  $(\ell, m, n)$  triples  $(0, 0, 0), (1, 0, 0), (0, 1, 0), (0, 0, 1), (1, 1, 0), (1, 0, 1), (0, 1, 1), (1, 1, 1)$ . Thus our presentation does indeed determine a group of order 8, and we have a presentation of  $Q_8$ .

- (1.6.14) Let  $G$  and  $H$  be groups and let  $\varphi : G \rightarrow H$  be a homomorphism. Define the *kernel* of  $\varphi$  to be  $\{g \in G \mid \varphi(g) = 1_H\}$  (so the kernel is the set of elements in  $G$  which map to the identity of  $H$ , i.e. the fiber over the identity of  $H$ .) Prove that the kernel of  $\varphi$  is a subgroup of  $G$ . Prove that  $\varphi$  is injective (recall this means one-to-one) if and only if the kernel of  $\varphi$  is the identity subgroup of  $G$ .

Let  $K$  denote the kernel of  $\varphi$ . As will be shown (by you) in class,  $\varphi(1_G) = 1_H$ , so  $1_G \in K$  and  $K \neq \emptyset$ . We will next show that  $K$  is closed under multiplication (i.e.  $K$  is in fact a set with a binary operation). If  $k_1, k_2 \in K$  then  $\varphi(k_1 \cdot k_2) = \varphi(k_1) \cdot \varphi(k_2) = 1_H \cdot 1_H = 1_H$  so  $k_1 \cdot k_2 \in K$  and the multiplication in  $G$  does indeed restrict to a

multiplication on  $K$  (again the fancy words are  $K$  is closed under multiplication). In showing that  $K \neq \emptyset$  we showed that  $1_G \in K$ , so  $K$  has an identity element. Finally we show that if  $k \in K$  then  $k^{-1} \in K$ , so  $K$  will have inverses, and hence be a group itself, and so a subgroup of  $G$ . Now if  $k \in K$ ,  $\varphi(k) = 1_G$ . By what you will show in class  $\varphi(k^{-1}) = \varphi(k)^{-1} = 1_G^{-1} = 1_G$ , so  $\varphi(k^{-1}) = 1_G$  and  $k^{-1} \in K$ , which was what we wanted to show. Summarizing, we have shown that  $K$  is a non-empty subset of  $G$  with a binary operation (the operation from  $G$  is in fact an operation on  $K$ , so  $K$  is closed under the operation), with the identity element and an inverse for each element. Thus  $K$  is a group, and hence a subgroup of  $G$ .  $\square$

- (1.6.20) Let  $G$  be a group and let  $Aut(G)$  be the set of all isomorphisms from  $G$  onto  $G$ . Prove that  $Aut(G)$  is a group under function composition (called the *automorphism group* of  $G$  and the elements of  $Aut(G)$  are called *automorphisms* of  $G$ ). [You can assume that function composition is associative.]

If  $f_1, f_2 : G \rightarrow G$  are isomorphisms, each is one-to-one and onto, so their composition  $f_1 \circ f_2$  will also be one-to-one and onto. Note that

$$f_1 \circ f_2(g_1 \cdot g_2) = f_1(f_2(g_1 \cdot g_2)) = f_1(f_2(g_1) \cdot f_2(g_2))$$

since  $f_2$  is a group homomorphism. Now since  $f_1$  is a group homomorphism, we also have:

$$f_1 \circ f_1(g_1 \cdot g_2) = f_1(f_2(g_1) \cdot f_2(g_2)) = f_1(f_2(g_1)) \cdot f_1(f_2(g_2)) = f_1 \circ f_2(g_1) \cdot f_1 \circ f_2(g_2)$$

and thus  $f_1 \circ f_2$  is indeed a group homomorphism, which, since it is one-to-one and onto, must be an isomorphism. We've been told to assume that function composition is associative, so function composition is indeed an associative binary operation on  $Aut(G)$ . The identity function  $id_G : G \rightarrow G$  given by  $id_G(g) = g$  for all  $g \in G$  is obviously one to one and onto, and it is clear that  $id_G(g_1 g_2) = g_1 g_2 = id_G(g_1) id_G(g_2)$ , so  $id_G$  is a homomorphism, and hence an isomorphism, and thus in  $Aut(G)$ . Now if  $f \in Aut(G)$ ,  $id_G \circ f(g) = f(g)$  and  $f \circ id_G(g) = f(g)$ , so  $id_G$  is an identity element for  $Aut(G)$ . Now if  $f$  is an automorphism, it is one-to-one and onto, and so  $f^{-1}$  is also a function from  $G$  to  $G$  (and also one-to-one and onto). We need to show that  $f^{-1}$  is a group homomorphism. Let  $g_1$  and  $g_2$  be in  $G$ , and let  $h_1$  and  $h_2$  be the unique elements such that  $f(h_1) = g_1$  and  $f(h_2) = g_2$ . Then  $f^{-1}(g_1) = h_1$  and  $f^{-1}(g_2) = h_2$ . Since  $f$  is a group homomorphism,  $f(h_1 h_2) = f(h_1) f(h_2) = g_1 g_2$ , and thus we have  $f^{-1}(g_1 g_2) = h_1 h_2 = f^{-1}(g_1) f^{-1}(g_2)$ , and  $f^{-1}$  is indeed a group homomorphism, and hence in  $Aut(G)$ . Thus  $Aut(G)$  is a set with an associative binary operation (function composition) which has an identity element  $id_G$  and each element has an inverse, and we have shown that  $Aut(G)$  is a group.