

## Assignment 2

**Notation.** I use  $D_{2n}$  to denote the dihedral group of order  $2n$ , and  $Z_n$  to denote the cyclic group on  $n$  points.

1. First, recall that if  $G/Z(G)$  is cyclic, then  $G$  is abelian. Then, remember that since  $Z(G)$  is a subgroup, we have that  $|Z(G)| = 1, p, q$ , or  $pq$ . Then if  $G$  is nonabelian, then  $|Z(G)| \neq pq$ , since that's just the trivial group (which I suppose is abelian) and  $|Z(G)| \neq p$  (or  $q$ ) since otherwise  $[G : Z(G)] = q$  (or respectively  $p$ ), which is prime, so  $G/Z(G)$  would be cyclic, and thus  $G$  abelian. Then if  $G$  is nonabelian and  $|G| = pq$ , then  $|Z(G)| = 1$  is the only option.

Then notice that if the group is of order  $p^2$ , then this permits that  $|Z(G)| = p^2$ , in other words, the group is abelian.

2. Starting off, we note that we know of two groups of order six a priori, namely  $Z_6$  and  $Z_3 \times Z_2 \cong D_6 \cong S_3$ . We claim that these two groups are all that there is. We could do this by appealing to the classification of finite abelian groups, but that is too cheaty, even for me. So let's do it from scratch:

**Claim.** *The only two groups of order 6 are  $Z_6$  and  $D_6$ .*

*Proof.* First, recall that we have an element of order 2 since the order of our group is even. Call it  $a$ .

Moreover, we necessarily also have an element of order 3. This is obvious since  $G$  has a Sylow 3-subgroup, which must be  $Z_3$ , generated by some element  $b \in G$ .

Now consider the cosets of  $\langle b \rangle$ . Namely, we get  $\{e, b, b^2\} = Z_3$  (modulo abuse of notation) and  $\{a, ab, ab^2\}$ . Then that's 6 elements, which must be distinct, so we can begin to construct our group:

$(\cdot)$	$e$	$b$	$b^2$	$a$	$ab$	$ab^2$
$e$	$e$	$b$	$b^2$	$a$	$ab$	$ab^2$
$b$	$b$	$b^2$	$e$			
$b^2$	$b^2$	$e$	$b$			
$a$	$a$	$ab$	$ab^2$	$e$	$b$	$b^2$
$ab$	$ab$	$ab^2$	$a$			
$ab^2$	$ab^2$	$a$	$ab$			

Now the only question left to answer is what happens to  $ba$ ? Well obviously  $ba \in \{a, ab, ab^2\}$ , since otherwise  $a \in \langle b \rangle$ , which can't be. So then either  $ba = ab$  or  $ba = ab^2$ .

As it happens, either option is acceptable, and a valid group table can be constructed from either, see

$(\cdot)$	$e$	$b$	$b^2$	$a$	$ab$	$ab^2$
$e$	$e$	$b$	$b^2$	$a$	$ab$	$ab^2$
$b$	$b$	$b^2$	$e$	$ab$	$ab^2$	$a$
$b^2$	$b^2$	$e$	$b$	$ab^2$	$a$	$ab$
$a$	$a$	$ab$	$ab^2$	$e$	$b$	$b^2$
$ab$	$ab$	$ab^2$	$a$	$b$	$b^2$	$e$
$ab^2$	$ab^2$	$a$	$ab$	$b^2$	$e$	$b$

$(\cdot)$	$e$	$b$	$b^2$	$a$	$ab$	$ab^2$
$e$	$e$	$b$	$b^2$	$a$	$ab$	$ab^2$
$b$	$b$	$b^2$	$e$	$ab^2$	$a$	$ab$
$b^2$	$b^2$	$e$	$b$	$ab$	$ab^2$	$a$
$a$	$a$	$ab$	$ab^2$	$e$	$b$	$b^2$
$ab$	$ab$	$ab^2$	$a$	$b$	$b^2$	$e$
$ab^2$	$ab^2$	$a$	$ab$	$b^2$	$e$	$b$

Now notice that the former case is just  $Z_3 \times Z_2$ , and in the second case  $ab$  is an element of order 6. Then, since there is nowhere else to send  $ba$ , we have the result we sought.  $\square$

- Notice that  $99 = 3^2 * 11$ . Then by the Sylow theorems, we must have a Sylow 3-subgroup and a Sylow 11-subgroup. 11 is prime, so the only group of order 11 is  $Z_{11}$ , so our group must have a subgroup of the cyclic group of order 11 (which has no subgroups). Then all that remains is to consider the Sylow 3-subgroups. Now notice that since  $9 = 3^2$  is a prime-power, our options for groups of order 9 are limited to  $Z_3 \times Z_3$  and  $Z_9$ .

So our options are either that our group of order 99 is  $Z_3 \times Z_3 \times Z_{11}$ , or it is  $Z_9 \times Z_{11}$ .

- We will show that the center of the group must be non-trivial, thus making it a non-trivial normal subgroup. Consider the class equation

$$|G| = |Z(G)| + \sum_{i=1}^n [G : C_G(g_i)]$$

$$|Z(G)| = |G| - \sum_{i=1}^n [G : C_G(g_i)]$$

But then the centralizers are subgroups, so  $[G : C_G(g_i)] = p^k$  for some  $k$ . Therefore,  $p$  divides the right hand side, so it must also divide the left hand side, and therefore it is a nontrivial normal subgroup, but when  $|Z(G)| = 1$ ,  $G \cong Z_p$ , so we're fine, and when it's the whole group, we get a similar result.

- We know that every normal subgroup is the union of conjugacy classes, and we moreover know that conjugacy classes are disjoint. Now realize that in order to truly be a subgroup, we must also include the identity of the group. Now realize that the result immediately falls out from elementary number theory.

If some union of conjugacy classes  $H$  forms a subgroup, then we must have that  $|H| \mid 60$ . But the only sums of 1, 15, 20, 12, and 12 which include 1 and divide 60 are  $1 = 1$  and  $1 + 15 + 20 + 12 + 12 = 60$  (this is easy to verify by exhaustion of all 11 nonempty combinations of the four non-unit conjugacy classes).

Therefore, the only normal subgroups are the trivial ones.

6. *Proof.* We construct the isomorphism directly. for some set  $T \in \mathcal{P}(S)$ , let  $\varphi_T$  be the morphism

$$a \mapsto \begin{cases} 1 & a \in T \\ 0 & a \notin T \end{cases}.$$

Then the isomorphism  $\varphi$  that we seek is the map

$$\begin{aligned} \varphi : \mathcal{P}(S) &\rightarrow (\mathbb{Z}/2\mathbb{Z})^S \\ T &\mapsto \varphi_T. \end{aligned}$$

Now, recall that the ring structure of  $\mathcal{P}(S)$  has that  $A +_{\mathcal{P}(S)} B = A \sqcup B (= A \cup B \setminus (A \cap B))$  and  $A \cdot_{\mathcal{P}(S)} B = A \cap B$ . Then it is quick to verify that  $\varphi$  is indeed a homomorphism. Simply realize that

$$\begin{aligned} \varphi(A + B) &= \varphi_{A+B} \\ &= \varphi_{A \sqcup B} \\ &= a \mapsto \begin{cases} 1 & a \in A \setminus B \text{ or } B \setminus A \\ 0 & \text{otherwise} \end{cases} \\ &= \varphi_A + \varphi_B \\ &= \varphi(A) + \varphi(B) \end{aligned}$$

And likewise

$$\begin{aligned} \varphi(A \cdot B) &= \varphi_{A \cdot B} \\ &= \varphi_{A \cap B} \\ &= a \mapsto \begin{cases} 1 & a \in A \cap B \\ 0 & a \notin A \cap B \end{cases} \\ &= \varphi_A \cdot \varphi_B \\ &= \varphi(A) \cdot \varphi(B). \end{aligned}$$

So  $\varphi$  is a homomorphism.  $\triangle$

And then realize that the inverse function can be given by  $\psi : (\mathbb{Z}/2\mathbb{Z})^S \rightarrow \mathcal{P}(S)$   $\varphi_T \mapsto T$ . It's worth noting at this point that every element of  $(\mathbb{Z}/2\mathbb{Z})^S$  is of the form  $\varphi_T$  since a function here can be completely characterized by the subset of  $S$  on which the function takes the value 1. Now notice that

$$\begin{aligned}
\varphi_A \cdot \varphi_B = a &\mapsto \begin{cases} 1 & a \in A \text{ and } a \in B \\ 0 & \text{otherwise} \end{cases} \\
&= a \mapsto \begin{cases} 1 & a \in A \cap B \\ 0 & \text{otherwise} \end{cases} \\
&= \varphi_{A \cap B} \\
\psi(\varphi_{A \cap B}) &= A \cap B \\
&= A \cdot B
\end{aligned}$$

And

$$\begin{aligned}
\varphi_A + \varphi_B = a &\mapsto \begin{cases} 1 & a \in A \setminus B \text{ or } B \setminus A \\ 0 & \text{otherwise} \end{cases} \\
&= a \mapsto \begin{cases} 1 & a \in A \sqcup B \\ 0 & \text{otherwise} \end{cases} \\
&= \varphi_{A \sqcup B} \\
\psi(\varphi_{A \sqcup B}) &= A \sqcup B \\
&= A + B
\end{aligned}$$

And we're done. They're isomorphic. □

7. Notice that the product of  $a_1 + b_1\mathbf{i} + c_1\mathbf{j} + d_1\mathbf{k}$  and  $a_2 + b_2\mathbf{i} + c_2\mathbf{j} + d_2\mathbf{k}$  is

$$\begin{aligned}
&a_1a_2 + a_1b_2\mathbf{i} + a_1c_2\mathbf{j} + a_1d_2\mathbf{k} \\
&+ b_1a_2\mathbf{i} + b_1b_2\mathbf{i}^2 + b_1c_2\mathbf{ij} + b_1d_2\mathbf{ik} \\
&+ c_1a_2\mathbf{j} + c_1b_2\mathbf{ji} + c_1c_2\mathbf{j}^2 + c_1d_2\mathbf{jk} \\
&+ d_1a_2\mathbf{k} + d_1b_2\mathbf{ki} + d_1c_2\mathbf{kj} + d_1d_2\mathbf{k}^2
\end{aligned}$$

Which simplifies to

$$\begin{aligned}
&a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2 \\
&+ (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)\mathbf{i} \\
&+ (a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)\mathbf{j} \\
&+ (a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)\mathbf{k}
\end{aligned}$$

Then realize that the transpose of this is precisely the shape of the hint's map, which shows that

$$\begin{bmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{bmatrix}$$

Is indeed a morphism, since the product of two such matrices will always give us a similar one back.

Likewise, the same can be verified for the other matrix representation

$$\begin{bmatrix} a + bi & c + di \\ -c + di & a - bi \end{bmatrix}$$

from the same multiplication evaluation. Hey, sorry this problem is so slapdash. This was the last problem I worked on, and something suddenly came up that I have to deal with urgently.

8. Notice that if  $J$  is an ideal of  $S$ , then  $\varphi^{-1}(J)$  is the kernel of  $R \rightarrow S \rightarrow S/J$ .
9. ( $\Rightarrow$ ) Suppose first that  $R$  is a division ring. Then consider the conjugacy class of some  $r \in R$ . Then there exists an  $r^{-1} \in R$ , and moreover, consider an ideal containing  $r$ . then  $r^{-1}rI \subseteq I$ , but then 1 is in the ideal, so the ideal must be total or trivial. Then the result follows since every such  $r$  has an inverse.
- ( $\Leftarrow$ ) We'll do the argument to show that if  $aR = R$  for all  $a \in R$ , then  $a$  has an inverse. in particular, we know that  $1 \in aR$ , so  $1 = ab$ , and likewise  $1 \in bR$ , so  $\exists c$  such that  $1 = bc$ . But then  $a = abc = c$ , so  $ab = ba = 1$ . Then the argument follows identically on the right.