MATH 701 – FALL 2023
HOMEWORK 7
DUE MONDAY, NOVEMBER 13 BY THE BEGINNING OF CLASS.

17. **Prove that A_4 does not have a subgroup of order 6.**

Assume G is a subgroup of A_4 of order 6. We expect to reach a contradiction.

Cauchy's Theorem ensures that G contains an element of order 2. The elements of A_4 of order two are

$$(12)(34), \quad (13)(24), \quad (14)(23). \tag{1}$$

Thus, G contains at least one of the elements of (1). On the other hand, G has index 2 in A_4. Thus, G must be a normal subgroup of A_4. The elements of (1) are conjugate to one another in A_4 because

$$(132)(12)(34)(123) = (13)(24) \quad \text{and} \quad (142)(12)(34)(124) = (14)(23).$$

Thus, the entire group

$$\{(1),\ (12)(34),\ (13)(24),\ (14)(23)\}$$

is contained in G. This of course is impossible, because Lagrange's Theorem guarantees that the order of a subgroup divides the order of the group and 4 does not divide 6.

18. **Let $\phi : \mathbb{Z}/4\mathbb{Z} \to \operatorname{Aut}(\mathbb{Z}/3\mathbb{Z})$ be the homomorphism with**

$$\phi(\bar{b})|_{\bar{c}} = (-1)^b\bar{c}$$

for all $\bar{b} \in \mathbb{Z}/4\mathbb{Z}$ and $\bar{c} \in \mathbb{Z}/3\mathbb{Z}$. (We say this a little more slowly: ϕ is a homomorphism from $\mathbb{Z}/4\mathbb{Z}$ to $\operatorname{Aut}(\mathbb{Z}/3\mathbb{Z})$. If $\bar{b}$ is in $\mathbb{Z}/4\mathbb{Z}$, then $\phi(\bar{b})$ is an automorphism of $\mathbb{Z}/3\mathbb{Z}$. If $\bar{b}$ is in $\mathbb{Z}/4\mathbb{Z}$ and $\bar{c} \in \mathbb{Z}/3\mathbb{Z}$, then $\phi(\bar{b})$ sends $\bar{c}$ to $(-1)^b\bar{c}$.)[1] Let T be the group $\mathbb{Z}/3\mathbb{Z} \rtimes_\phi \mathbb{Z}/4\mathbb{Z}$.

(a) **What is the order of each element of T?**

Observe that

$$\begin{aligned}
(\bar{1},\bar{2})^2 &= (\bar{2},\bar{0})\\
(\bar{1},\bar{2})^3 &= (\bar{0},\bar{2})\\
(\bar{1},\bar{2})^4 &= (\bar{1},\bar{0})\\
(\bar{1},\bar{2})^5 &= (\bar{2},\bar{2})\\
(\bar{1},\bar{2})^6 &= (\bar{0},\bar{0}).
\end{aligned}$$

[1] If n and a are integers, we write $\bar{a}$ for the class of a in $\mathbb{Z}/n\mathbb{Z}$.

Deduce

element	order
$(\bar{1}, \bar{2})$	6
$(\bar{2}, \bar{0})$	3
$(\bar{0}, \bar{2})$	2
$(\bar{1}, \bar{0})$	3
$(\bar{2}, \bar{2})$	6.

Observe that

$$(\bar{2}, \bar{1})^2 = (\bar{0}, \bar{2})$$
$$(\bar{2}, \bar{1})^3 = (\bar{2}, \bar{3})$$
$$(\bar{2}, \bar{1})^4 = (\bar{0}, \bar{0}).$$

Deduce

element	order
$(\bar{2}, \bar{1})$	4
$(\bar{0}, \bar{2})$	2
$(\bar{2}, \bar{3})$	4.

Observe that

$$(\bar{1}, \bar{3})^2 = (\bar{0}, \bar{2})$$
$$(\bar{1}, \bar{3})^3 = (\bar{1}, \bar{1})$$
$$(\bar{1}, \bar{3})^4 = (\bar{0}, \bar{0}).$$

Deduce

element	order
$(\bar{1}, \bar{3})$	4
$(\bar{0}, \bar{2})$	2
$(\bar{1}, \bar{1})$	4.

Observe that

$$(\bar{0}, \bar{1})^2 = (\bar{0}, \bar{2})$$
$$(\bar{0}, \bar{1})^3 = (\bar{0}, \bar{3})$$
$$(\bar{0}, \bar{1})^4 = (\bar{0}, \bar{0}).$$

Deduce

element	order
$(\bar{0},\bar{1})$	4
$(\bar{0},\bar{2})$	2
$(\bar{0},\bar{3})$	4.

Altogether, we conclude that

element	order
$(\bar{0},\bar{0})$	1
$(\bar{0},\bar{1})$	4
$(\bar{0},\bar{2})$	2
$(\bar{0},\bar{3})$	4
$(\bar{1},\bar{0})$	3
$(\bar{1},\bar{1})$	4
$(\bar{1},\bar{2})$	6
$(\bar{1},\bar{3})$	4
$(\bar{2},\bar{0})$	3
$(\bar{2},\bar{1})$	4
$(\bar{2},\bar{2})$	6
$(\bar{2},\bar{3})$	4.

(b) **Identify elements x and y in T with $T = \langle x, y\rangle$ $x^6 = \mathrm{id}$, $y^2 = x^3$, and $yxy^{-1} = x^5$.**

Let $x = (\bar{1},\bar{2})$ and $y = (\bar{0},\bar{1})$. We already calculated that $x^6 = (\bar{0},\bar{0})$ and that $x^3 = (\bar{0},\bar{2}) = y^2$. We calculate now that

$$yxy^{-1} = \Big((\bar{0},\bar{1})(\bar{1},\bar{2})\Big)(\bar{0},\bar{3}) = (-\bar{1},\bar{3})(0,\bar{3}) = (-\bar{1},\bar{2}) = (\bar{2},\bar{2}) = x^{-1}.$$

Observe also that $\langle x, y\rangle$ is a subgroup of T of size more than 6. The group T has size 12; the only divisor of 12 which is larger than 6 is 12. It follows from Lagrange's Theorem that $\langle x, y\rangle = T$.

(c) **Let F be the free group on the two letters X and Y; and let N be the smallest normal subgroup of F which contains X^6, Y^2X^3, $YXY^{-1}X$. Prove that F/N is isomorphic to T.**

There is a homomorphism $\phi : F \to T$, given by $\phi(X) = x$ and $\phi(Y) = y$. We showed in part (b) that X^6, Y^2X^3, and $YXY^{-1}X$ are contained in $\ker\phi$. Of course $\ker\phi$ is a normal subgroup of F. It follows that N, the smallest normal subgroup of F which contains X^6, Y^2X^3, and $YXY^{-1}X$, is contained in $\ker\phi$. Apply the first isomorphism theorem to obtain a homomorphism

$$\bar{\phi} : \frac{F}{N} \to T$$

with $\bar{\phi}(\bar{X}) = x$ and $\bar{\phi}(\bar{Y}) = y$. We showed in part (b) that $\langle x, y\rangle = T$; thus, $\bar{\phi}$ is surjective. In particular, $\frac{F}{N}$ has at least 12 elements. On the other hand, the defining elements for N can be used to show that every element of $\frac{F}{N}$ can be written in the form $\bar{X}^i\bar{Y}^j$ with $0 \le i \le 5$ and $0 \le j \le 1$. Thus, $\frac{F}{N}$ has at most 12 elements. It follows that $\frac{F}{N}$ has exactly 12 elements and $\bar{\phi}$ is an isomorphism.

19. **Let $\phi : \mathbb{Z}^4 \to \mathbb{Z}^3$ be the group homomorphism with $\phi(v) = Mv$ for all $v \in \mathbb{Z}^4$, where**

$$M = \begin{bmatrix} 3 & 5 & 5 & 6 \\ 2 & 7 & 10 & 7 \\ 3 & 8 & 11 & 9 \end{bmatrix}$$

and Mv is matrix multiplication. Let G be the Abelian group $\mathbb{Z}^3/\operatorname{im}(\phi)$. Every element in G has the form $\bar{w}$, where $w \in \mathbb{Z}^3$.

(a) **Identify elements $w_1, \dots, w_r$ in $\mathbb{Z}^3$, for some r, with $G = \mathbb{Z}\bar{w}_1 \oplus \mathbb{Z}\bar{w}_2 \oplus \cdots \oplus \mathbb{Z}\bar{w}_r$.**

(b) **What is the order of the cyclic group $\mathbb{Z}\bar{w}_i$ for each i?**

One of the two possible answers: The group G is isomorphic to $\frac{\mathbb{Z}}{6\mathbb{Z}}$. The group G is equal to the cyclic group

$$\mathbb{Z}\overline{\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}},$$

and this cyclic group has order 6. Of course, every element of the coset

$$\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} + \operatorname{im}\phi$$

is the cyclic generator of G. If your generator does not look exactly like mine, but differs from mine by an element of $\operatorname{im}\phi$, then you have the same answer.

The other possible answer: The group G is isomorphic to $\frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{3\mathbb{Z}}$; and

$$G = \mathbb{Z}\overline{\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}} \oplus \mathbb{Z}\overline{\begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}};$$

furthermore, the cyclic subgroups

$$\mathbb{Z}\overline{\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}} \quad \text{and} \quad \mathbb{Z}\overline{\begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}}$$

have order 2 and 3 respectively.

In order to find the answer I applied **COLUMN** operations on M in order to find a better generating set for im M. When one applies column operations to M, one changes the generating set for im M, but one does not change im M at all. (Notice that M is a homomorphism $\mathbb{Z}^4 \to \mathbb{Z}^3$. When one applies column operations to M one changes the basis for $\mathbb{Z}^4$. We do not care about the basis for $\mathbb{Z}^4$. On the other hand, if we were to apply row operations to M, then we would be changing the basis for $\mathbb{Z}^3$. We are required to report the answer in terms of the original basis for $\mathbb{Z}^3$. If we change to basis for $\mathbb{Z}^3$ we must undo these changes later.) After applying only column operations to M, one obtains

$$M' = \begin{bmatrix} 1 & 0 & 0 & 0 \\ -3 & 2 & 3 & 0 \\ -2 & 0 & 3 & 0 \end{bmatrix}.$$

I will show show you the intermediate steps later. At any rate $M' = MP$ for some invertible matrix P. Notice that im $M' =$ im M. This assertion is obvious; but it is so crucial we record a proof:

$$\begin{aligned} M' = MP &\implies \operatorname{im} M' \subseteq \operatorname{im} M \quad \text{and} \\ M = M'P^{-1} &\implies \operatorname{im} M \subseteq \operatorname{im} M'. \end{aligned}$$

Observe first that $\operatorname{im} M + \mathbb{Z}\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = \mathbb{Z}^3$. The inclusion $\subseteq$ is clear. We show $\supseteq$. It is clear that

$$\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \in \text{LHS}.$$

Observe that

$$\begin{bmatrix} 0 \\ 3 \\ 3 \end{bmatrix} - 3\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} - \begin{bmatrix} 0 \\ 2 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

is in LHS. Now it is clear that

$$\begin{bmatrix} 1 \\ -3 \\ -2 \end{bmatrix} + 3\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} + 2\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

is in LHS.

Now we prove that $\operatorname{im}\phi :_{\mathbb{Z}} \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = 6\mathbb{Z}$. It is clear [2] that

$$\begin{bmatrix} 0 \\ 0 \\ 6 \end{bmatrix} = 2 \begin{bmatrix} 0 \\ 3 \\ 3 \end{bmatrix} - 3 \begin{bmatrix} 0 \\ 2 \\ 0 \end{bmatrix} \in \operatorname{im}\phi.$$

Suppose

$$n \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = a \begin{bmatrix} 1 \\ -3 \\ 2 \end{bmatrix} + b \begin{bmatrix} 0 \\ 2 \\ 0 \end{bmatrix} + c \begin{bmatrix} 0 \\ 3 \\ 3 \end{bmatrix}.$$

Then $a = 0$, $n = 3c$, and $0 = 2b + 3c$. It follows that $3|n$ and $2|n$. In other words, $6|n$.

Now we examine the other legitimate answer. It is obvious that

$$\operatorname{im} M + \mathbb{Z} \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} + \mathbb{Z} \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} = \mathbb{Z}^3.$$

It is clear that

$$3 \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} \quad \text{and} \quad 2 \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

are in $\operatorname{im}\phi$. We now prove that if

$$n \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} + m \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \in \operatorname{im} M,$$

then $n \in 3\mathbb{Z}$ and $m \in 2\mathbb{Z}$. Indeed, if

$$n \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} + m \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} = a \begin{bmatrix} 1 \\ -3 \\ 2 \end{bmatrix} + b \begin{bmatrix} 0 \\ 2 \\ 0 \end{bmatrix} + c \begin{bmatrix} 0 \\ 3 \\ 3 \end{bmatrix},$$

then

$$a = 0, \quad n = 3c, \quad n + m = 2b + 3c.$$

It follows that $n \in 3\mathbb{Z}$ and $m \in 2\mathbb{Z}$, as claimed.

One might ask how the second answer gives to the first answer. That is easy. Recall that the homomorphism

$$\frac{\mathbb{Z}}{6\mathbb{Z}} \to \frac{\mathbb{Z}}{3Z} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}},$$

which is given by

$$\bar{1} \mapsto (\bar{1}, \bar{1})$$

[2]Recall that $\operatorname{im}\phi :_{\mathbb{Z}} \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = \left\{ n \in \mathbb{Z} | n \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \in \operatorname{im}\phi \right\}$.

is an isomorphism. If

$$G = \mathbb{Z}\overline{\begin{bmatrix}0\\1\\1\end{bmatrix}} \oplus \mathbb{Z}\overline{\begin{bmatrix}0\\1\\0\end{bmatrix}},$$

$\overline{\begin{bmatrix}0\\1\\1\end{bmatrix}}$ has order 3 and $\overline{\begin{bmatrix}0\\1\\0\end{bmatrix}}$ has order 2, then

$$\overline{\begin{bmatrix}0\\1\\0\end{bmatrix}} + \overline{\begin{bmatrix}0\\1\\1\end{bmatrix}} = \overline{\begin{bmatrix}0\\2\\1\end{bmatrix}}$$

generates G and has order 6. On the other hand, $\begin{bmatrix}0\\2\\0\end{bmatrix} \in \operatorname{im}\phi$; consequently,

$$\overline{\begin{bmatrix}0\\2\\1\end{bmatrix}} = \overline{\begin{bmatrix}0\\0\\1\end{bmatrix}}.$$

Here are the column operations that show that the columns of M and the columns of M' generate the same subgroup of $\mathbb{Z}^3$.

Replace column 4 by column 4 minus column 3. The matrix M has been transformed into:

$$\begin{bmatrix}3 & 5 & 5 & 1\\ 2 & 7 & 10 & -3\\ 3 & 8 & 11 & -2\end{bmatrix}$$

Replace column 1 by column 1 minus 3 times column 4.
Replace column 2 by column 2 minus 5 times column 4.
Replace column 3 by column 3 minus 5 times column 4. The matrix M has been transformed into

$$\begin{bmatrix}0 & 0 & 0 & 1\\ 11 & 22 & 25 & -3\\ 9 & 18 & 21 & -2\end{bmatrix}$$

Replace column 2 by column 2 minus 2 times column 1.
Replace column 3 by column 3 minus 2 times column 1. The matrix M has been transformed into

$$\begin{bmatrix}0 & 0 & 0 & 1\\ 11 & 0 & 3 & -3\\ 9 & 0 & 3 & -2\end{bmatrix}$$

Replace column 1 by column 1 minus 3 times column 3. The matrix M has been transformed into

$$\begin{bmatrix} 0 & 0 & 0 & 1 \\ 2 & 0 & 3 & -3 \\ 0 & 0 & 3 & -2 \end{bmatrix}.$$

Rearrange the columns to obtain

$$M' = \begin{bmatrix} 1 & 0 & 0 & 0 \\ -3 & 2 & 3 & 0 \\ -2 & 0 & 3 & 0 \end{bmatrix}.$$

In particular,

$$M' = M \underbrace{E_1 E_2 E_3 E_4 E_5 E_6}_{P},$$

where

$$E_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad E_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -3 & -5 & -5 & 1 \end{bmatrix}, \quad E_3 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

$$E_4 = \begin{bmatrix} 1 & -2 & -2 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad E_5 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ -3 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \text{and} \quad E_6 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

Suppose you have M' and it is not immediately obvious how coker M' **decomposes as a direct sum of cyclic groups. What should you do?** This is also easy. Do the row operations to transform M' into a matrix with non-zero entries only on the main diagoinal.
Replace row 2 by row 2 plus 3 times row 1.
Replace row 3 by row 3 plus 2 times row 1. The matrix M has been transformed into

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 3 & 0 \\ 0 & 0 & 3 & 0 \end{bmatrix}.$$

Replace row 2 by row 2 minus row 3. The matrix M has been transformed into

$$M'' = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 3 & 0 \end{bmatrix}.$$

Of course,

$$M'' = NMP,$$

where

$$N = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 3 & 1 & 0 \\ 2 & 0 & 1 \end{bmatrix}.$$

Furthermore, the cokernel of M'' is isomorphic to

$$\frac{\mathbb{Z}}{1\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{3\mathbb{Z}} = \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{3\mathbb{Z}},$$

$$\frac{\mathbb{Z}^3}{\operatorname{im} M''} = \mathbb{Z}\overline{\begin{bmatrix}0\\1\\0\end{bmatrix}} \oplus \mathbb{Z}\overline{\begin{bmatrix}0\\0\\1\end{bmatrix}},$$

$\overline{\begin{bmatrix}0\\1\\0\end{bmatrix}}$ has order 2, and $\overline{\begin{bmatrix}0\\0\\1\end{bmatrix}}$ has order 3. Apply the first isomorphism theorem to the composition

$$\mathbb{Z}^3 \xrightarrow{N} \mathbb{Z}^3 \xrightarrow{\text{natural quotient map}} \frac{\mathbb{Z}}{\operatorname{im}(NMP)}$$

to obtain an isomorphism

$$\frac{\mathbb{Z}}{\operatorname{im}(MP)} \xrightarrow{N} \frac{\mathbb{Z}}{\operatorname{im}(NMP)}.$$

We already saw that $\operatorname{im} MP = \operatorname{im} M$. We conclude that

$$\frac{\mathbb{Z}}{\operatorname{im} M} \xrightarrow{N} \frac{\mathbb{Z}}{\operatorname{im}(NMP)}$$

is an isomorphism. Observe that

$$N^{-1}\left(\begin{bmatrix}0\\1\\0\end{bmatrix}\right) = \begin{bmatrix}1&0&0\\-3&1&0\\-2&0&1\end{bmatrix}\begin{bmatrix}1&0&0\\0&1&1\\0&0&1\end{bmatrix}\begin{bmatrix}0\\1\\0\end{bmatrix} = \begin{bmatrix}0\\1\\0\end{bmatrix}$$

and

$$N^{-1}\begin{bmatrix}0\\0\\1\end{bmatrix} = \begin{bmatrix}0\\1\\1\end{bmatrix}.$$

This calculation yields the second of our two answers.

20. **Classify the non-Abelian groups of order eight. (This instruction means state and prove a result which says, "If G is a non-Abelian group of order 8, then G is isomorphic to exactly one of the following groups: … .")**

Theorem 0.1. *If G is a non-Abelian group of order 8, then G is isomorphic to exactly one of the groups D_4 or Q_8.*

Proof. Observe that first that some element of G has order 4. (Indeed, if every element of G squares to the identity element, then G is Abelian.) Let a be an element of G of order 4. The index of $\langle a\rangle$ in G is 2; so, $\langle a\rangle$ is a normal subgroup of G. Let b be any element of $G \setminus \langle a\rangle$. Observe that $bab^{-1} \in \langle a\rangle$ and $b^2 \in \langle a\rangle$ because $\langle a\rangle$ is a normal subgroup of G. The order of bab^{-1} is the same as the order of a; consequently, bab^{-1} can not equal id or a^2. Furthermore, if bab^{-1} were equal to a, then G would be Abelian. Thus, bab^{-1} must equal a^3. If b^2 were equal to either a or a^3, then $\langle a\rangle$ would be a proper subgroup of $\langle b\rangle$; and therefore, $\langle b\rangle$ would have to equal G (by Lagrange's Theorem) and this has been ruled out because $\langle b\rangle$ is Abelian. There are two possibilities left. If $b^2 = \mathrm{id}$, then $G \cong D_4$ (see Theorem 2.61.1) if $b^2 = a^2$, then $G \cong Q_8$ (see Exercise 2.62.1). $\square$