Moshe Mason Rubin

MATH 330 Homework #5

3 October 2016

Exercise 4.14. Let
$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \text{ and } B = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}$$
be elements in $GL_2(\mathbb{R})$.Show that A and B have finite orders but AB does not.

Proof. Notice
$$A^2 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$
and
$$\begin{aligned} A^4 = A^2 A^2 &= \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = id \end{aligned}$$
so A is of order 4. Notice
$$\begin{aligned} B^3 &= \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} \\ &= \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = id \end{aligned}$$
So B is of order 3.

Notice $AB = \left[\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right]$

Claim. $(AB)^n = \left[\begin{smallmatrix} 1 & -n \\ 0 & 1 \end{smallmatrix}\right]$ for $n \in \mathbb{N}$, so AB is of infinite order as this would imply there is no $n \in \mathbb{N}$ such that $(AB)^n = id$.

By induction:

Base case $n = 2$:
$$\begin{aligned} (AB)^2 &= \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix} \end{aligned}$$

So the hypothesis holds for $n = 2$. ✓

Inductive step Assume $(AB)^n = \left[\begin{smallmatrix} 1 & -n \\ 0 & 1 \end{smallmatrix}\right]$ for some fixed $n \in \mathbb{N}$ and show that $(AB)^{n+1} = \left[\begin{smallmatrix} 1 & -(n+1) \\ 0 & 1 \end{smallmatrix}\right]$:

$$\begin{aligned}
(AB)^{n+1} &= (AB)^n (AB) \\
&= \begin{bmatrix} 1 & -n \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 0 & 1 \end{bmatrix} \\
&= \begin{bmatrix} 1 & -1-n \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -(n+1) \\ 0 & 1 \end{bmatrix} \quad \checkmark
\end{aligned}$$

So $(AB)^n = \left[\begin{smallmatrix} 1 & -n \\ 0 & 1 \end{smallmatrix}\right]$ for $n \in \mathbb{N}$.

So AB is of infinite order as this would imply there is no $n \in \mathbb{N}$ such that $(AB)^n = id$. $\square$

Exercise 4.18. Calculate each of the following expressions.

(a) $(1+i)^{-1}$

(b) $(1+i)^6$

(c) $\left(\sqrt{3}+i\right)^5$

(d) $(-i)^{10}$

(e) $\left(\frac{1-i}{2}\right)^4$

(f) $\left(-\sqrt{2}-\sqrt{2}i\right)^{12}$

(g) $(-2+2i)^{-5}$

Proof. Recall that *Euler's Formula* that $Ae^{i\theta} = A(\cos\theta + i\sin\theta)$ for $A \in \mathbb{R}$, $\theta \in [0, 2\pi]$.

(a) $(1+i)^{-1}$ is given by $\frac{1}{2} - \frac{1}{2}i$ as $(1+i)\left(\frac{1}{2} - \frac{1}{2}i\right) = \frac{1}{2} - \frac{1}{2}i + \frac{1}{2}i + \frac{1}{2} = 1$. So $\boxed{\frac{1}{2} - \frac{1}{2}i = (1+i)^{-1}}$.

(b) By *Euler's Formula*, $1 + i = \sqrt{2}e^{\frac{i\pi}{4}}$, so

$$\begin{aligned}
(1+i)^6 &= \left(\sqrt{2}e^{\frac{i\pi}{4}}\right)^6 \\
&= \sqrt{2}^6 e^{\frac{6i\pi}{4}} \\
&= 8e^{\frac{3i\pi}{2}} \\
&= 8\left(\cos\left(\frac{3\pi}{2}\right) + i\sin\left(\frac{3\pi}{2}\right)\right) \quad \text{by } \textit{Euler's Formula} \\
&= -8i, \quad \text{as } \cos\left(\tfrac{3\pi}{2}\right) = 0 \text{ and } \sin\left(\tfrac{3\pi}{2}\right) = -1
\end{aligned}$$

So $\boxed{(1+i)^6 = -8i}$.

(c) By *Euler's Formula*, $\sqrt{3} + i = 2e^{\frac{i\pi}{6}}$, so

$$\begin{aligned}
\left(\sqrt{3}+i\right)^5 &= \left(2e^{\frac{i\pi}{6}}\right)^5 \\
&= 2^5 e^{\frac{5i\pi}{6}} \\
&= 32\left(\cos\left(\frac{5\pi}{6}\right) + i\sin\left(\frac{5\pi}{6}\right)\right) \quad \text{by } \textit{Euler's Formula} \\
&= 32\left(-\frac{\sqrt{3}}{2} + \frac{1}{2}i\right) \quad \text{as } \cos\left(\tfrac{5\pi}{6}\right) = -\tfrac{\sqrt{3}}{2} \text{ and } \sin\left(\tfrac{5\pi}{6}\right) = \tfrac{1}{2} \\
&= 16i - 16\sqrt{3}
\end{aligned}$$

So $\boxed{\left(\sqrt{3}+i\right)^5 = 16i - 16\sqrt{3}}$.

(d)

$$
\begin{aligned}
(-i)^{10} &= (-1)^{10}(i)^{10} \\
&= (-1)^{2}(i)^{2} \quad \text{as } (-1)^m = (-1)^{(m \bmod 2)} \text{ and } i^n = i^{(n \bmod 4)} \\
&= (1)(-1) \\
&= -1
\end{aligned}
$$

So $\boxed{(-i)^{10} = -1}$.

(e) By *Euler's Formula*, $\frac{1-i}{2} = \frac{1}{2} - \frac{1}{2}i = \frac{\sqrt{2}}{2}e^{\frac{7i\pi}{4}}$, so

$$
\begin{aligned}
\left(\frac{1-i}{2}\right)^4 &= \left(\frac{\sqrt{2}}{2}e^{\frac{7i\pi}{4}}\right)^4 \\
&= \left(\frac{\sqrt{2}}{2}\right)^4 e^{7i\pi} \\
&= \frac{1}{4}e^{i\pi} \quad \text{as we restrict } \theta \text{ to } 0 \le \theta \le 2\pi \\
&= \frac{1}{4}\left(\cos(\pi) + i\sin(\pi)\right) \\
&= -\frac{1}{4}
\end{aligned}
$$

So $\boxed{\left(\frac{1-i}{2}\right)^4 = -\frac{1}{4}}$.

(f) By *Euler's Formula*, $-\sqrt{2} - \sqrt{2}i = 2e^{\frac{5i\pi}{4}}$, so

$$
\begin{aligned}
\left(-\sqrt{2} - \sqrt{2}i\right)^{12} &= \left(2e^{\frac{5i\pi}{4}}\right)^{12} \\
&= 2^{12}e^{\frac{60i\pi}{4}} \\
&= 4096e^{15i\pi} \\
&= 4096e^{i\pi} \quad \text{as we restrict } \theta \text{ to } 0 \le \theta \le 2\pi \\
&= -4096 \quad \text{as } e^{i\pi} = -1 \text{ from above}
\end{aligned}
$$

So $\boxed{\left(-\sqrt{2} - \sqrt{2}i\right)^{12} = -4096}$.

(g) By *Euler's Formula*, $-2 + 2i = 2\sqrt{2}e^{\frac{3i\pi}{4}}$, so

$$
\begin{aligned}
(-2+2i)^{-5} &= \left(2\sqrt{2}e^{\frac{3i\pi}{4}}\right)^{-5} \\
&= \left(2\sqrt{2}\right)^{-5}\left(e^{\frac{3i\pi}{4}}\right)^{-5} \\
&= \frac{\sqrt{2}}{256}e^{\frac{-15i\pi}{4}} \\
&= \frac{\sqrt{2}}{256}e^{\frac{i\pi}{4}} \quad \text{as we restrict } \theta \text{ to } 0 \le \theta \le 2\pi \\
&= \frac{\sqrt{2}}{256}\left(\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i\right) \quad \text{by \textit{Euler's Formula}, as } \sin\left(\tfrac{\pi}{4}\right) = \cos\left(\tfrac{\pi}{4}\right) = \tfrac{1}{\sqrt{2}} \\
&= \frac{1}{256} + \frac{1}{256}i
\end{aligned}
$$

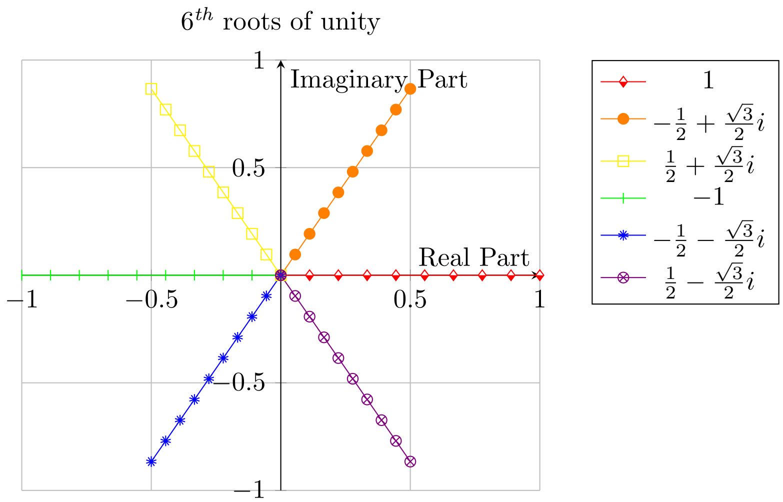
So $\boxed{(-2+2i)^{-5} = \frac{1}{256} + \frac{1}{256}i}$. ∎

Exercise 4.20. List and graph that 6^{th} roots of unity. What are the generators of this group? What are the primitive 6^{th} roots of unity?

Proof. By Theorem 4.11, the 6^{th} roots of unity are given by $z = \cos\left(\frac{k\pi}{3}\right) + i\sin\left(\frac{k\pi}{3}\right)$ for $k = 0, 1, 2, 3, 4, 5$. So the 6^{th} roots of unity are

1. $\cos(0) + i\sin(0) = 1$
2. $\cos\left(\frac{\pi}{3}\right) + i\sin\left(\frac{\pi}{3}\right) = \frac{1}{2} + \frac{\sqrt{3}}{2}i$
3. $\cos\left(\frac{2\pi}{3}\right) + i\sin\left(\frac{2\pi}{3}\right) = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$
4. $\cos(\pi) + i\sin(\pi) = -1$
5. $\cos\left(\frac{4\pi}{3}\right) + i\sin\left(\frac{4\pi}{3}\right) = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$
6. $\cos\left(\frac{5\pi}{3}\right) + i\sin\left(\frac{5\pi}{3}\right) = \frac{1}{2} - \frac{\sqrt{3}}{2}i$

Only $\frac{1}{2} + \frac{\sqrt{3}}{2}i$ and $\frac{1}{2} - \frac{\sqrt{3}}{2}i$ are primitive 6^{th} roots of unity as $1^1 = 1$, $\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)^3 = 1$, $(-1)^2 = 1$, and $\left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right)^3 = 1$ for the other roots. So $\frac{1}{2} + \frac{\sqrt{3}}{2}i$ and $\frac{1}{2} - \frac{\sqrt{3}}{2}i$ are the generators of this group. $\square$



Exercise 4.23. Let $a, b \in G$. Prove the following statements.

(a) The order of a is the same as the order of a^{-1}.

(b) For all $g \in G$, $|a| = |g^{-1}ag|$.

(c) The order of ab is the same as the order of ba.

Proof.

(a)
- Assume $a \in G$ is of finite order $k \in \mathbb{N}$. Then $a^k = 1$ by definition. Then

$$\begin{aligned}\left(a^{-1}\right)^k &= a^{-k} \quad \text{by Theorem 3.8.2}\\ &= \left(a^k\right)^{-1} \quad \text{by Theorem 3.8.2}\\ &= (1)^{-1} \quad \text{by assumption that } a \text{ is of order } k\\ &= 1\end{aligned}$$

  So $\left(a^{-1}\right)^k = 1$. So a^{-1} is of order k.

- Assume a is of infinite order. Then there does not exist $k \in \mathbb{N}$ suck that $a^k = 1$. Now, assume we wish to find $n \in \mathbb{N}$ such that $\left(a^{-1}\right)^n = 1$. Then

$$\begin{aligned}\left(a^{-1}\right)^n = 1 &\implies a^{-n} = 1 \quad \text{by Theorem 3.8.2}\\ &\implies (a^n)^{-1} = 1\\ &\implies (a^n)^{-1} = (a^n)(a^n)^{-1} \quad \text{by definition of } (a^n)^{-1}\\ &\implies 1 = a^n \quad \text{by right multiplying by } a^n\end{aligned}$$

  But $a^n \neq 1$ for all $n \in \mathbb{N}$ by assumption that $|a| = \infty$. So $\left(a^{-1}\right)^n \neq 1$ for all $n \in \mathbb{N}$, so $|a^{-1}| = \infty$.

So $|a| = |a^{-1}|$. $\square$

(b) I will show $|a|=|g^{-1}ag|$ for all $g \in G$ using the following claim:

Claim. $\left(g^{-1}ag\right)^k = g^{-1}a^kg$ for $k \in \mathbb{N}$.

By induction:

Base Case $n = 2$:

$$\begin{aligned}
\left(g^{-1}ag\right)^2 &= \left(g^{-1}ag\right)\left(g^{-1}ag\right) \\
&= \left(g^{-1}a\right)\left(gg^{-1}\right)(ag) \quad \text{by associative property} \\
&= \left(g^{-1}a\right)(ag) \quad \text{by definition of } g^{-1} \\
&= g^{-1}a^2g \quad \text{by associative property}
\end{aligned}$$

So the hypothesis holds for $n = 2$. ✓

Inductive step Assume $\left(g^{-1}ag\right)^k = g^{-1}a^kg$ for some fixed $k \in \mathbb{N}$ and show that $\left(g^{-1}ag\right)^{k+1} = g^{-1}a^{k+1}g$:

$$\begin{aligned}
\left(g^{-1}ag\right)^{k+1} &= \left(g^{-1}ag\right)^k\left(g^{-1}ag\right) \\
&= \left(g^{-1}a^kg\right)\left(g^{-1}ag\right) \quad \text{by inductive hypothesis} \\
&= \left(g^{-1}a^k\right)\left(gg^{-1}\right)(ag) \quad \text{by associative property} \\
&= \left(g^{-1}a^k\right)(ag) \quad \text{by definition of } g^{-1} \\
&= g^{-1}a^{k+1}g \quad \checkmark
\end{aligned}$$

So $\left(g^{-1}ag\right)^k = g^{-1}a^kg \implies \left(g^{-1}ag\right)^{k+1} = g^{-1}a^{k+1}g$. So $\left(g^{-1}ag\right)^k = g^{-1}a^kg$ for all $k \in \mathbb{N}$. $\square$

Now, consider that $|a|=n$ for some $n \in \mathbb{N}$. Then $a^n = 1$ by definition. Then

$$\begin{aligned}
a^n = n &\implies a^n = gg^{-1} \\
&\implies a^ng = g\left(g^{-1}g\right) \quad \text{by associative property} \\
&\implies a^ng = g, \quad \text{by definition of } g^{-1} \\
&\implies g^{-1}a^ng = g^{-1}g \\
&\implies g^{-1}a^ng = 1 \\
&\implies \left(g^{-1}ag\right)^n = 1 \quad \text{by above claim that } \left(g^{-1}ag\right)^k = g^{-1}a^kg
\end{aligned}$$

So $\left(g^{-1}ag\right)^n = 1$. So $|g^{-1}ag|=|a|$ for all $g \in G$. $\square$

(c) Notice $ab = b^{-1}(ba)b$. So

$$\begin{aligned}
|ab| &= |b^{-1}(ba)b| \\
&= |ba| \quad \text{by (b)}
\end{aligned}$$

So $|ab|=|ba|$. $\square$

Exercise 4.30. Suppose that G is a group and let $a, b \in G$. Prove that if $|a|=m$ and $|b|=n$ with $\gcd(m,n) = 1$, then $\langle a \rangle \cap \langle b \rangle = \{e\}$.

Proof. Notice $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ and $\langle b \rangle = \{e, b, b^2, \ldots, b^{m-1}\}$. We want to show e is the only element these two sets have in common.

Suppose not: Suppose $a^{n_0} = b^{m_0}$ for some $n_0, m_0 \in \mathbb{N}$ such that $0 < n_0 < n$ and $0 < m_0 < m$. Then

$$\begin{aligned} a^{n_0} = b^{m_0} &\implies (a^{n_0})^n = (b^{m_0})^n \\ &\implies a^{n_0 n} = b^{m_0 n} \quad \text{by Theorem 3.8.2} \\ &\implies e = b^{m_0 n} \quad \text{by Proposition 4.5, as } n|(m_0 n) \\ &\implies m|(m_0 n) \quad \text{by Proposition 4.5} \\ &\implies m|m_0 \quad \text{by } \textbf{Exercise 2.27} \text{ from homework 2, as } \gcd(m,n) = 1 \text{ by assumption} \end{aligned}$$

and $m|m_0$ is contradiction as we assumed $0 < m_0 < m$. So $a^{n_0} \neq b^{m_0}$ for any n_0, m_0. So $\langle a \rangle$ and $\langle b \rangle$ have no elements in common except e. So $\langle a \rangle \cap \langle b \rangle = \{e\}$. □

Exercise 5.1. Write the following permutations in cycle notation.

(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix}$ (b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3 \end{pmatrix}$ (c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 4 & 2 \end{pmatrix}$ (d) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$

Solution.

(a) (12453) (b) (14) (35) (c) (13) (25) (d) (24) □

Exercise 5.2. Compute each of the following.

(a) (1345) (234)
(b) (12) (1253)
(c) (143) (23)(24)
(d) (1423)(34)(56)(1324)
(e) (1254)(13)(25)
(f) $(1254)(13)(25)^2$

Solution.

(a) (1351)(24)
(b) (253)
(c) (14)(23)
(d) (12)(56)
(e) (1324)
(f) (13254) □

Exercise 5.3. Express the following permutations as products of transpositions and identify them as even or odd.

(a) (14356)
(b) (156)(234)
(c) (1426)(142)
(d) (17254)(1423)(154632)
(e) (142637)

Solution. Recall that

$$(a_1, a_2, \ldots, a_n) = (a_1 a_n)(a_1 a_{n-1}) \cdots (a_1 a_3)(a_1 a_2)$$

(a) (14356) = (16)(15)(13)(14) and is even.
(b) (156)(234) = (16)(15)(24)(23) and is even.
(c) (1426)(142) = (1246) = (16)(14)(12) and is odd.
(d) (17254)(1423)(154632) = (14672) = (12)(17)(16)(14) and is even.
(e) (142637) = (17)(13)(16)(12)(14) and is odd. □

Exercise 5.5. List all of the sub-groups of S_4. Find each of the following sets.

(a) $\{\sigma \in S_4 : \sigma(1) = 3\}$

(b) $\{\sigma \in S_4 : \sigma(2) = 2\}$

(c) $\{\sigma \in S_4 : \sigma(1) = 3 \text{ and } \sigma(2) = 2\}$

Proof. The elements of S_4 are given by

e	(12)	$(12)(34)$	$(123) = (13)(12)$	$(1234) = (14)(13)(12)$
	(13)	$(13)(24)$	$(132) = (12)(13)$	$(1243) = (13)(14)(12)$
	(14)	$(14)(23)$	$(124) = (14)(12)$	$(1423) = (13)(12)(14)$
	(23)		$(142) = (12)(14)$	$(1324) = (14)(12)(13)$
	(24)		$(134) = (14)(13)$	$(1432) = (12)(13)(14)$
	(34)		$(143) = (13)(14)$	$(1342) = (12)(14)(13)$
			$(234) = (24)(23)$	
			$(243) = (23)(24)$	

Then the sub-groups of S_4 are given by

1. $\langle e \rangle = \{e\}$
2. $\langle (12) \rangle = \{e, (12)\}$
3. $\langle (13) \rangle = \{e, (13)\}$
4. $\langle (14) \rangle = \{e, (14)\}$
5. $\langle (23) \rangle = \{e, (23)\}$
6. $\langle (24) \rangle = \{e, (24)\}$
7. $\langle (34) \rangle = \{e, (34)\}$
8. $\langle (12)(34) \rangle = \{e, (12)(34)\}$
9. $\langle (13)(24) \rangle = \{e, (13)(24)\}$
10. $\langle (14)(23) \rangle = \{e, (14)(23)\}$
11. $\langle (123) \rangle = \{e, (123), (132)\}$
12. $\langle (124) \rangle = \{e, (124), (142)\}$
13. $\langle (134) \rangle = \{e, (134), (143)\}$
14. $\langle (234) \rangle = \{e, (234), (243)\}$
15. $\langle (1234) \rangle = \{e, (1234), (13)(24), (1432)\}$
16. $\langle (1243) \rangle = \{e, (1243), (14)(23), (1342)\}$
17. $\langle (1423) \rangle = \{e, (1423), (12)(43), (1324)\}$
18. $\langle (12), (34) \rangle = \{e, (12), (34), (12)(34)\}$
19. $\langle (13), (24) \rangle = \{e, (13), (24), (13)(24)\}$
20. $\langle (14), (23) \rangle = \{e, (14), (23), (14)(23)\}$
21. S_4
22. I know there are more but I'm not totally sure the best way to compute "all sub-groups"

(a) $\{\sigma \in S_4 : \sigma(1) = 3\} = \{(13), (13)(24), (132), (134), (1324), (1342)\}$

(b) $\{\sigma \in S_4 : \sigma(2) = 2\} = \{e, (13), (14), (34), (134), (143)\}$

(c) $\{\sigma \in S_4 : \sigma(1) = 3 \text{ and } \sigma(2) = 2\} = \{(13), (134)\}$

$\square$