MATH 4041 HW 6

David Chen, dc3451

October 18, 2020

Problem 1

$$\begin{aligned}\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix} &= \begin{bmatrix}0-1 & 0+0\\ 0+0 & -1+0\end{bmatrix}\\ &= \begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix}\\ &= -I\end{aligned}$$

Then, we have that $A^2 = -I \implies A^3 = -(IA) = -A \neq I$ and then $A^4 = A^2A^2 = (-I)(-I) = I$, so the order of A is 4.

$$\begin{aligned}\begin{bmatrix}0 & 1\\ -1 & -1\end{bmatrix}\begin{bmatrix}0 & 1\\ -1 & -1\end{bmatrix} &= \begin{bmatrix}0-1 & 0-1\\ 0+1 & -1+1\end{bmatrix}\\ &= \begin{bmatrix}-1 & -1\\ 1 & 0\end{bmatrix}\\ \begin{bmatrix}-1 & -1\\ 1 & 0\end{bmatrix}\begin{bmatrix}0 & 1\\ -1 & -1\end{bmatrix} &= \begin{bmatrix}0+1 & -1+1\\ 0+0 & 1+0\end{bmatrix}\\ &= \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\\ &= I\end{aligned}$$

so we have that $B^3 = I$.

$$\begin{aligned}\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}\begin{bmatrix}0 & 1\\ -1 & -1\end{bmatrix} &= \begin{bmatrix}0+1 & 0+1\\ 0+0 & 1+0\end{bmatrix}\\ &= \begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}\end{aligned}$$

as desired.

Then,

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

We can show inductively that $(AB)^n = \begin{bmatrix}1 & n\\0 & 1\end{bmatrix}$. Clearly this holds for the $n = 1$ case, since we already showed that $(AB)^1 = AB = \begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}$. Then, if $(AB)^n = \begin{bmatrix}1 & n\\0 & 1\end{bmatrix}$, then

$$\begin{bmatrix}1 & n\\0 & 1\end{bmatrix}\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix} = \begin{bmatrix}1+0 & 1+n\\0+0 & 0+1\end{bmatrix}$$
$$= \begin{bmatrix}1 & n+1\\0 & 1\end{bmatrix}$$

so this holds for $n+1$, and by induction for all $n \in \mathbb{N}$. Therefore, AB cannot be of finite order, as we have that if AB has order n, $(AB)^n = I \implies \begin{bmatrix}1 & n\\0 & 1\end{bmatrix} = \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix} \implies n = 0$, and since order is defined to be a positive integer, $n > 0$. $\Rightarrow\!\Leftarrow$, so AB does not have finite order.

Problem 2

i

We can compute all of these directly:

$$([1],[1]) + ([1],[1]) = ([2],[2])$$
$$= ([0],[0])$$

So $([1],[1])$ has order 2 in $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

$$\begin{aligned}
([1],[1]) + ([1],[1]) &= ([2],[2]) \\
&= ([0],[2]) \\
([0],[2]) + ([1],[1]) &= ([1],[3]) \\
&= ([1],[0]) \\
([1],[0]) + ([1],[1]) &= ([2],[1]) \\
&= ([0],[1]) \\
([0],[1]) + ([1],[1]) &= ([1],[2]) \\
([1],[2]) + ([1],[1]) &= ([2],[3]) \\
&= ([0],[0])
\end{aligned}$$

So $([1],[1])$ has order 6 in $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$.

$$\begin{aligned}
([1],[1]) + ([1],[1]) &= ([2],[2]) \\
([2],[2]) + ([1],[1]) &= ([3],[3]) \\
([3],[3]) + ([1],[1]) &= ([4],[4]) \\
&= ([0],[4]) \\
([0],[4]) + ([1],[1]) &= ([1],[5]) \\
([1],[5]) + ([1],[1]) &= ([2],[6]) \\
([2],[6]) + ([1],[1]) &= ([3],[7]) \\
([3],[7]) + ([1],[1]) &= ([4],[8]) \\
&= ([0],[0])
\end{aligned}$$

So $([1],[1])$ has order 8 in $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z})$.

$$\begin{aligned}
([2],[4]) + ([2],[4]) &= ([4],[8]) \\
&= ([0],[0])
\end{aligned}$$

So $([2],[4])$ has order 2 in $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z})$.

ii

First, we show that in any group G, if g has order n, $g^k = 1 \iff n \mid k$.

$(\implies)$ Suppose that $n \nmid k$, such that $k = nq + r$ for some $0 \leq r \leq n-1$. Then, $1 = g^k = g^{nq+r} = g^{nq}g^r = (g^n)^q g^r = g^r = 1$. Then, we have that $g^r = 1$ for $r < n$, and so g cannot be of order n. $\Rightarrow\Leftarrow$, so $n \mid k$.

($\Longleftarrow$) We have that $n \mid k \implies k = nq$ for some $q \in \mathbb{Z}$. Then, $g^k = g^{nq} = (g^n)^q = 1^q = 1$.

The order of g, h will be $\text{lcm}(n, m)$, or the least common multiple of n and m. To see this, note that if we have $(g, h)^k = (e_G, e_H)$ where e_G, e_H are the identities of G and H respectively, we have that

$$(g, h)^k = (g^k, h^k) = (e_G, e_H) \implies g^k = e_G, h^k = e_H$$

However, from above, we have that this holds if and only if $n \mid k$ and $m \mid k$. Since the lcm of n, m is exactly the least positive integer k which satisfies $n \mid k$ and $m \mid k$ and the order is the least positive integer which satisfies the above relation, the order must be the lcm of n, m.

Problem 3

We can see that the torsion subgroup of $\mathbb{Z}/n\mathbb{Z}$ is exactly $\mathbb{Z}/n\mathbb{Z}$ itself: note that $[m] \in \mathbb{Z}/\mathbb{Z}$ satisfies that

$$n[m] = [nm] = [0]$$

so each element has order at most n, and thus has finite order.

The torsion subgroup of $\mathbb{Z}$ is exactly $\{0\}$. No other element has finite order (but 0 as the identity has order 1). To see this, $n \in \mathbb{Z}$, $n \neq 0$ alongside some $m \in \mathbb{Z}$, $m > 0$ satisfies that $n < 0 \implies nm < 0$ and $n > 0 \implies nm > 0$, so $nm \neq 0$ and n does not have finite order in $\mathbb{Z}$.

The torsion subgroup of $\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})$ is exactly all elements of the form $(0, [m])$ for $[m] \in \mathbb{Z}/n\mathbb{Z}$. To see this, we have that this has order at most n by the observation that 0 has order 1 and from above that $[m]$ has order at most n, so we have from problem 1 that $(0, m)$ has order at most $\text{lcm}(1, n) = n$. Further, we can see that for $a \neq 0$, $(a, [m])^k = (ka, k[m]) = (0, [0])$ yields that a has order k, which is impossible, so we have that $(a, [m])$ cannot have finite order for $a \neq 0$.

Problem 4

μ_∞ cannot be cyclic. Suppose that μ_∞ was in fact generated by some element μ'. In particular, since $\mu' \in \mu_\infty$, μ' must have finite order, say n. Then, we have that for any k, $(\mu'^k)^n = (\mu'^n)^k = 1^k = 1$, so every element in $\langle \mu' \rangle$ must have order at most n. However, we can very easily see that μ_∞ contains an element of order $2n$, say $e^{\pi i/n} \in \mu_{2n}$. Thus, μ' cannot generate the entirety of μ_∞.

Problem 5

i

Since we have for any $g \in G$ that $f(g) = f(g \cdot 1) = f(g) \cdot f(1)$ and $f(g) = f(1 \cdot g) = f(1) \cdot f(g)$, we have that $f(1) \cdot f(g) = f(g) = f(g) \cdot f(1)$, so $f(1)$ is an identity in G_2, as any element in G_2 can be represented as $f(g)$ for $g \in G_1$ since f is surjective. Then, since identities are unique in groups, we have that $f(1) = 1$ as *the* identity.

ii

$f(1) = 1 \implies 1 = f(g^{-1}g) = f(g^{-1})f(g), 1 = f(gg^{-1}) = f(g)f(g^{-1}) \implies f(g^{-1}) = (f(g))^{-1}$ by definition and uniqueness of inverses.

iii

$\implies$ That $f(H)$ is a subgroup of G_2 was also the last problem on the last problem set.

We need to show that $f(H)$ contains the identity, inverses, and is closed. Since H is a subgroup, it satisfies all three of those things. Then, $1 \in H \implies f(1) = 1 \in f(H)$, $g \in H \implies g^{-1} \in H$, so $f(g) \in f(H) \implies f(g^{-1}) = (f(g))^{-1} \in H$, and lastly, $g, h \in H \implies gh \in H \implies f(gh) = f(g)f(h) \in H$. Thus, $f(H)$ is a subgroup.

$\impliedby$ Applying the first part with $f^{-1} : G_2 \to G_1$, we have that $f^{-1}(f(H))$ is a subgroup of G_1; all we need to show is that $f^{-1}(f(H)) = H$ as sets to show that they are the same subgroup. To see this, note that $h \in H \implies f(h) \in f(H) \implies f^{-1}(f(h)) = h \in f^{-1}(f(H))$, and $h \in f^{-1}(f(H)) \implies \exists h = f^{-1}(h')$ for some $h' \in f(H)$, and $h' \in f(H) \implies h' = f(h'')$ for some $h'' \in H$. Then, $h = f^{-1}(f(h'')) = h'' \in H$, so we have that $H \subseteq f^{-1}(f(H))$ and $f^{-1}(f(H)) \subseteq H$, so the two sets are equal and we are done.

6

Note that a permutation of a set X is defined exactly to be a bijection from X to X.

We need to show that H_{n+1} contains the identity, inverses, and is closed. In particular, we have that $\mathrm{id} \in H_{n+1}$, as we have that $\mathrm{id}(n+1) = n+1$ as desired (in particular, $\mathrm{id} : S_{n+1} \to S_{n+1}$ takes $x \mapsto x$ for any x so it is clearly a bijection, and $f(\mathrm{id}(x)) = f(x) = \mathrm{id}(f(x))$). Further, we have that for $f, g \in S_{n+1}$, $(f \circ g)(n+1) = f(g(n+1)) = f(n+1) = n+1$, so we have that $f \circ g \in H_{n+1}$ as well (we know that $f \circ g$ as the composition of two bijections is itself a bijection).

The last thing to handle is inverses. Since $f \in H_{n+1}$ is a bijection, there is clearly some inverse $f^{-1} \in S_{n+1}$ that is bijective as well; further, since $f(n+1) = n+1$, we get that

$f^{-1}(f(n+1)) = f^{-1}(n+1) \implies n+1 = f^{-1}(n+1)$, so $f^{-1} \in H_{n+1}$ as well.

Then, an isomorphism ϕ from S_n to H_{n+1} can be given as

$$\phi(f) = g, \text{ where } g(m) = \begin{cases} f(m) & 1 \leq m \leq n \\ n+1 & m = n+1 \end{cases}$$

We need to first show that g is in fact a bijection: we have that the unique preimage of $n+1$ is $n+1$, as $1 \leq f(m) \leq n$. Then, each k where $1 \leq k \leq n$ also has a unique preimage, given by $f^{-1}(k)$, which we know exists since $f \in S_n \implies f$ is a bijection. Then, g has an inverse given by

$$g^{-1}(m) = \begin{cases} f^{-1}(m) & 1 \leq m \leq n \\ n+1 & m = n+1 \end{cases}$$

and is then a bijection, so ϕ is well-defined.

Now, we need to show that ϕ is a bijection. For $f, f' \in S_n$, $\phi(f) = \phi(f')$ implies that for every m, where $1 \leq m \leq n$, $(\phi(f))(m) = (\phi(f'))(m) \implies f(m) = f'(m)$, and since f, f' have domain $\{1, 2, \ldots, n\}$, $f = f'$ and ϕ is injective.

Similarly, every $f \in H_{n+1}$ must have a preimage: since f is a bijection with $f(n+1) = n+1$, for any m, $1 \leq m \leq n \iff 1 \leq f(m) \leq n$ (to see $\implies$, supposing otherwise gives $f(m) = n+1$, contradicting that f is injective, and to see $\impliedby$, supposing otherwise gives $m = n+1 \implies f(m) = n+1$, contradicting that $1 \leq f(m) \leq n$). Then, any m', $1 \leq m' \leq n$ must have a preimage $f^{-1}(m)$ (since f is surjective) which must satisfy $1 \leq f^{-1}(m) \leq n$ as before, and must be unique since f is surjective. Then, the restriction $f|_{\{1,2,\ldots,n\}}$ is a bijection from $\{1, 2, \ldots, n\}$ to itself, and $\phi(f|_{\{1,2,\ldots,n\}}) = f$, so ϕ is surjective.

Finally, given $f, f' \in S_n$, we have that

$$(\phi(f \circ f'))(m) = \begin{cases} f(f'(m)) & 1 \leq m \leq n \\ n+1 & m = n+1 \end{cases}$$

and

$$(\phi(f) \circ \phi(f'))(m) = \begin{cases} f((\phi(f'))(m)) & 1 \leq (\phi(f'))(m) \leq n \\ n+1 & (\phi(f'))(m) = n+1 \end{cases}$$

however, as shown above, $1 \leq (\phi(f'))(m) \leq n \iff 1 \leq m \leq n$, and $(\phi(f'))(m) = n+1 \iff m = n+1$ as $\phi(f') \in H_{n+1}$, so the conditions simplify to

$$(\phi(f) \circ \phi(f'))(m) = \begin{cases} f((\phi(f'))(m)) & 1 \leq m \leq n \\ n+1 & m = n+1 \end{cases} = \begin{cases} f(f'(m))) & 1 \leq m \leq n \\ n+1 & m = n+1 \end{cases} = (\phi(f \circ f'))(m)$$

Since $\phi(f \circ f') = \phi(f) \circ \phi(f')$, ϕ is an isomorphism and we are done.

7

Note that we have from class that there are integer solutions x, y to $ax + by = d$ if and only if $\gcd(a, b) \mid d$. Then, $n \in \langle a, b\rangle \implies n = ax + by$ for integers $x, y \implies \gcd(a, b) \mid n$, so every $n \in \langle a, b\rangle$ can be written as $k \gcd(a, b)$ for some integer k. Further, since we have that $ax + by = k \gcd(a, b)$ has solutions for every integer k, we know that $\langle a, b\rangle = \{k \gcd(a, b) \mid k \in \mathbb{Z}\}$.

Then, this is exactly $\langle \gcd(a, b)\rangle$ for positive (a, b). Then, $\langle 2, 3\rangle = \langle 1\rangle = \mathbb{Z}$, $\langle 3, 5\rangle = \langle 1\rangle = \mathbb{Z}$, and $\langle 4, 6\rangle = \langle 2\rangle$, or the even integers.

8

Notice that $9 \cdot 9 = 81$ and $16 \cdot 5 = 80 = 81 - 1$, so we have that $n = 9$, $m = -5$ satisfies $9n + 16m = 1$.

9

No: we saw in class that there are integer solutions x, y to $ax + by = d$ if and only if $\gcd(a, b) \mid d$. and since we have that $3 \nmid 2$, there are no solutions to $57x + 93y = 2$ (also note that $57x + 93y = 3(19x + 21y)$, so any solution would give that $19x + 21y = \frac{2}{3}$, where the LHS is an integer). However, since $3 \mid -6$, there are solutions to $57x + 93y = -6$. In particular, if x', y' satisfy $57x' + 93y' = 3$, then $x = -2x', y = -2y'$ satisfy $57x + 93y = -6$.