MTH 203 midterm solutions

1. Up to isomorphism, list all abelian groups of order 64.

   Solution. This is equivalent to determining all possible *admissible* tuples $T = (n_1, n_2, \ldots, n_k)$ of positive integers such that

   (a) each $n_i \geq 2$,

   (b) $n_i \leq n_{i+1}$, for $1 \leq i \leq n-1$,

   (c) $n_1 n_2 \ldots n_k = 64$, and

   (d) $\gcd(n_i, n_{i+1}) > 1$, for $1 \leq i \leq n-1$.

   By the Classification of Finitely Generated Abelian Groups, we know that each such admissible tuple $T = (n_1, n_2, \ldots, n_k)$ yields a group

   $$G_T := \prod_{i=1}^{k} \mathbb{Z}_{n_i},$$

   which is unique up to isomorphism. Finally, there are 11 admissible tuples, which are:

   1. $(2, 2, 2, 2, 2, 2)$,
   2. $(2, 2, 2, 2, 4)$
   3. $(2, 2, 2, 8)$
   4. $(2, 2, 4, 4)$
   5. $(2, 2, 16)$
   6. $(2, 4, 8)$
   7. $(4, 4, 4)$
   8. $(2, 32)$
   9. $(4, 16)$
   10. $(8, 8)$
   11. (64)

2. Using the First Isomorphism Theorem (or otherwise), establish the following isomorphisms.

   (a) $\mathbb{R}^2/\mathbb{Z}^2 \cong S^1 \times S^1$, where $S^1 = \{z \in \mathbb{C} : |z| = 1\}$.

   (b) $\mathbb{C}^\times/S^1 \cong \mathbb{R}_{>0}$, where $\mathbb{R}_{>0} = \{x \in \mathbb{R} : x > 0\}$ is a group under real multiplication.

Solution. (a) From class, we know that applying the First Isomorphism Theorem to the epimorphism

$$\varphi : \mathbb{R} \to S^1 : x \overset{\varphi}{\mapsto} e^{i2\pi x}$$

yields the isomorphism

$$\mathbb{R}/\mathbb{Z} \cong S^1.$$

Since the direct product of two groups is a group, we see that both $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ and $S^1 \times S^1$ are groups. Moreover, the map

$$\psi : \mathbb{R}^2 \to S^1 \times S^1 : (x, y) \overset{\psi}{\mapsto} (\varphi(x), \varphi(y))$$

is an epimorphism, as each of its component map are epimorphisms. Now,

$$\begin{aligned}
\operatorname{Ker}\psi &= \{(x, y) \in \mathbb{R}^2 : \psi((x, y)) = (1, 1)\} \\
&= \{(x, y) \in \mathbb{R}^2 : \varphi(x) = 1 \text{ and } \varphi(y) = 1\} \\
&= \{(x, y) \in \mathbb{R}^2 : \varphi(x) = 1 \text{ and } \varphi(y) = 1\} \\
&= \{x \in \mathbb{R} : \varphi(x) = 1\} \times \{y \in \mathbb{R} : \varphi(y) = 1\} \\
&= \operatorname{Ker}\varphi \times \operatorname{Ker}\varphi \\
&= \mathbb{Z} \times \mathbb{Z}.
\end{aligned}$$

Therefore, applying the First Isomorphism Theorem to ψ, we conclude that

$$\mathbb{R}^2/\operatorname{Ker}\psi \cong \operatorname{Im}\psi, \text{ that is, } \mathbb{R}^2/\mathbb{Z}^2 \cong S^1 \times S^1.$$

(b) Consider the map

$$m : \mathbb{C}^\times \to \mathbb{R}_{>0} : z \overset{m}{\mapsto} |z|.$$

Clearly, m is a homomorphism, for if $z, w \in \mathbb{C}^\times$, then

$$m(zw) = |zw| = |z||w| = m(z)m(w).$$

Moreover, for any $x \in \mathbb{R}_{>0}$, we see that $m(x) = |x| = x$, and so m is a surjective map. Furthermore, we have that

$$\operatorname{Ker} m = \{z \in \mathbb{C}^\times : |z| = 1\} = S^1.$$

Therefore, the First Isomorphism Theorem implies that

$$\mathbb{C}^\times/\operatorname{Ker} m \cong \operatorname{Im} m \text{ or } \mathbb{C}^\times/S^1 \cong \mathbb{R}_{>0}.$$

3. For a group G, show that $G/Z(G)$ is cyclic if, and only if, G is abelian.

Solution. First, we note that as $Z(G) \lhd G$, the quotient $G/Z(G)$ is a group. Suppose that G is abelian. Then $Z(G) = G$, and so we have that

$$G/Z(G) = G/G = \{G\} \cong \{1\},$$

which is cyclic.

Conversely, suppose that $G/Z(G)$ is cyclic. Then denoting $H = Z(G)$, we see that there exists $g \in G$ such that $G/H = \langle gH \rangle$, that is, every left coset of H in G is of the form $g^i H$, for some $i \in \mathbb{Z}$. Now consider any two distinct elements $a, b \in G$. Since the distinct cosets of H form a partition of G, there exists cosets $g^r H$ and $g^s H$ that contain the elements a and b, respectively. Further, this implies that there exists elements $h_r, h_s \in H$ such that

$$a = g^r h_r \text{ and } b = g^s h_s.$$

So, we have

$$\begin{aligned}
ab &= (g^r h_r)(g^s h_s) \\
&= g^r (h_r g^s) h_s && \text{(By associativity)} \\
&= g^r (g^s h_r) h_s && (\because h_r \in H) \\
&= (g^r g^s)(h_r h_s) && \text{(By associativity)} \\
&= (g^s g^r)(h_s h_r) && \text{(As any two powers of } g \text{ commute and } h_r, h_s \in H.) \\
&= g^s (g^r h_s) h_r && \text{(By associativity)} \\
&= g^s (h_s g^r) h_r && (\because h_s \in H) \\
&= (g^s h_s)(g^r h_r) && \text{(By associativity)} \\
&= ba
\end{aligned}$$

Therefore, as $ab = ba$, for all $a, b \in G$, the group G is abelian.

4. Let $S(\mathbb{R}^2)$ denote the group of symmetries of $\mathbb{R}^2$. Show that for every $n \geq 3$, there exists a monomorphism $\varphi_n : D_{2n} \to S(\mathbb{R}^2)$.

Solution. Let R be a rotation of $\mathbb{R}^2$ about the origin counterclockwise by $2\pi/n$ radians, and let S be a reflection of $\mathbb{R}^2$ about the X-axis. Then we see that $o(R) = n$ and $o(S) = 2$.

Now consider the complex n^{th} roots of unity $C_n = \{e^{i2\pi k/n} : 0 \leq k \leq n-1\}$. These roots correspond to the following n (pairwise equidistant) points on the unit circle S^1 in $\mathbb{R}^2$:

$$\{(\cos(2\pi k/n), \sin(2\pi k/n)) : 0 \leq k \leq n-1\}.$$

Joining each pair

$$(\cos(2\pi k/n), \sin(2\pi k/n)), (\cos(2\pi(k+1)/n), \sin(2\pi(k+1)/n)), \text{ for } 0 \leq k \leq n,$$

of equidistant points appearing in cyclical sequence in the unit circle by a line segment, yields a regular n-gon P_n. Moreover, the symmetries R and S restrict to symmetries R' and S' of P_n, where R' is a rotation of P_n by $2\pi/n$ and S' is a reflection of P_n about a bisector (or a diagonal) through the point $(1,0)$. Hence, we have that $\langle R', S' \rangle \cong D_{2n}$, and by extension $\langle R, S \rangle \cong D_{2n}$.

Finally the map $r \mapsto R, s \mapsto S$ extends to a homomorphism given by

$$\varphi : D_{2n} \to S(\mathbb{R}^2) : s^i r^j \overset{\varphi}{\mapsto} S^i R^j, \text{ for } 0 \leq i \leq 2 \text{ and } 0 \leq j \leq n-1,$$

which is clearly injective, as $\operatorname{Im} \varphi = \langle R, S \rangle (\cong D_{2n})$.

5. Let G be a nontrivial group.

   (a) Show that the set

$$\text{Aut}(G) = \{\varphi : G \to G \,|\, \varphi \text{ is an isomorphism}\}$$

   forms a group under composition.

   (b) When $G = \mathbb{Z}_n$, for $n \geq 2$, show that $\text{Aut}(\mathbb{Z}_n) \cong U_n$. [Hint: For $\varphi \in \text{Aut}(\mathbb{Z}_n)$, what is $o(\varphi([1]))$?]

   Solution. (a) Closure: Given $\phi, \psi \in \text{Aut}(G)$, we see that $\phi \circ \psi$ is bijective, and both ϕ and ψ are bijective. Moreover, given $g, h \in G$, we see that

$$\begin{aligned}(\phi \circ \psi)(gh) &= \phi(\psi(gh)) && \text{(By definition of composition.)} \\ &= \phi(\psi(g)\psi(h)) && (\psi \in \text{Aut}(G)) \\ &= \phi(\psi(g))\phi(\psi(h)) && (\phi \in \text{Aut}(G)) \\ &= (\phi \circ \psi)(g)(\phi \circ \psi)(h). && \text{(By definition of composition.)}\end{aligned}$$

   Hence, we have $\phi \circ \psi \in \text{Aut}(G)$.

   Associativity: Given $\phi, \psi, \chi \in \text{Aut}(G)$, and any $g \in G$, we see that

$$\begin{aligned}(\phi \circ (\psi \circ \chi))(g) &= \phi(\psi \circ \chi)(g)) && \text{(By definition of composition.)} \\ &= \phi(\psi(\chi(g))) && \text{(By definition of composition.)} \\ &= (\phi \circ \psi)(\chi(g)) && \text{(By definition of composition.)} \\ &= ((\phi \circ \psi) \circ \chi)(g), && \text{(By definition of composition.)}\end{aligned}$$

   from which associativity follows.

   Existence of identity: The identity isomorphism $i_G : G \to G$ is the identity element in $\text{Aut}(G)$, for given $\varphi \in \text{Aut}(G)$ and any $g \in G$, we have

$$\varphi(i_G(g)) = \varphi(g) = i_G(\varphi(g)).$$

   Existence of inverse: For any $\phi \in \text{Aut}(G)$, the inverse map ϕ^{-1} is clearly bijective. Moreover, given $g', h' \in G$, let $\varphi(g) = g'$ and $\varphi(h) = h'$, for $g, h \in G$. Then

$$\varphi^{-1}(g'h') = gh = \varphi^{-1}(g')\varphi^{-1}(h'),$$

   which shows that $\phi^{-1} \in \text{Aut}(G)$. Finally, by definition of inverse, we have

$$\varphi \circ \varphi^{-1} = i_G = \varphi^{-1} \circ \varphi.$$

   (b) Given a finite set X and a map $f : X \to X$, we know that

$$f \text{ is injective} \iff f \text{ is surjective} \iff f \text{ is bijective.} \tag{1}$$

   Moreover, we know from class (Lesson Plan 3.3 (vii)) that given a homomorphism $\varphi : G \to H$ between finite groups

$$\varphi \text{ is injective} \iff \varphi \text{ is order-preserving.} \tag{2}$$

   From (1) and (2), it follows that

$$\varphi \in \text{Aut}(G) \iff \varphi \text{ is order-preserving.} \tag{3}$$

Furthermore, given a homomorphism $\varphi : \mathbb{Z}_n \to \mathbb{Z}_n$, we have

$$\varphi([k]) = \varphi(\underbrace{[1] + \ldots + [1]}_{k}) = k\varphi([1]),$$

for any $[k] \in \mathbb{Z}_n$. So, we have that:

$$\text{Every homomorphism } \varphi : \mathbb{Z}_n \to \mathbb{Z}_n \text{ is uniquely determined by } \varphi([1]). \quad (4)$$

Therefore, an arbitrary homomorphism is of the form

$$\varphi_k : \mathbb{Z}_n \to \mathbb{Z}_n : [1] \overset{\varphi_k}{\mapsto} [k].$$

Since $\mathbb{Z}_n = \langle [1] \rangle$, we have $o([1]) = n$, and so (3) and (4) imply that

$$\varphi_k \in \mathrm{Aut}(\mathbb{Z}_n) \iff o(\varphi([1])) = n \iff \langle [k] \rangle = \mathbb{Z}_n. \quad (5)$$

Further, we know (from Quiz 1, Question 2) that

$$\langle [k] \rangle = \mathbb{Z}_n \iff \gcd(k, n) = 1. \quad (6)$$

Putting (5) and (6) together, we have

$$\begin{aligned} \varphi_k \in \mathrm{Aut}(\mathbb{Z}_n) &\iff gcd(k,n) = 1 \\ &\iff [k] \in U_n \qquad \text{(By definition of } U_n.\text{)} \end{aligned}$$

Therefore, the map

$$\alpha : \mathrm{Aut}(Z_n) = \{\varphi_k : \gcd(k,n) = 1\} \to U_n : \varphi_k \overset{\alpha}{\mapsto} [k].$$

is bijective.

It remains to show that α is a homomorphism, but this follows from the observation that given $\varphi_k, \varphi_{k'} \in \mathrm{Aut}(\mathbb{Z}_n)$, we have

$$\begin{aligned} (\varphi_k \circ \varphi_{k'})([1]) &= \varphi_k(\varphi_{k'}([1]) \\ &= \varphi_k([k']) \\ &= \varphi_k(\underbrace{[1] + \ldots + [1]}_{k'}) \\ &= \underbrace{[k] + \ldots + [k]}_{k'}) \\ &= [kk'] \\ &= [k][k'] \\ &= \varphi_k([1])\varphi_{k'}([1]). \end{aligned}$$

6. **(Bonus)** Show that $\text{Aut}(U_8) \cong D_6$.

Solution. We know from class that $U_8 = \{[1], [3], [5], [7]\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, which has three elements of order 2. Up to isomorphism, this group (the Klein 4-group) has the form

$$G = \{1, a, b, ab\}, \text{ where } o(a) = o(b) = o(ab) = 2.$$

(See the solution to HW IV - 2.3 (iv)(a).) So, this implies that

$$a = a^{-1}, b = b^{-1}, \text{ and } ab = (ab)^{-1}.$$

By assertion (3) from the solution to Question 5, we know that

$$\varphi \in \text{Aut}(G) \iff \varphi \text{ is order preserving.}$$

Moreover, since $G = \langle a, b \rangle$, it follows that any homomorphism $\varphi : G \to G$ is uniquely determined by $\varphi(a)$ and $\varphi(b)$. Consequently, there are exactly 6 choices for a $\varphi \in \text{Aut}(G)$, which are:

(i) $\varphi(a) = a$ and $\varphi(b) = b$: This would imply that $\varphi(ab) = ab$, thereby yielding the identity isomorphism, which we denote by 1.

(ii) $\varphi(a) = b$ and $\varphi(b) = a$: This would imply that

$$\varphi(ab) = ba = b^{-1}a^{-1} = (ab)^{-1} = ab.$$

This yields an isomorphism of order 2, as it swaps the two elements a and b, while fixing the remaining two group elements. We denote this isomorphism by s'.

(iii) $\varphi(a) = a$ and $\varphi(b) = ab$: This would imply that

$$\varphi(ab) = a^2 b = b.$$

This yields an isomorphism of order 2, as it swaps the two elements b and ab, while fixing the remaining two group elements. We denote this isomorphism by s''.

(iv) $\varphi(b) = b$ and $\varphi(a) = ab$: This would imply that

$$\varphi(ab) = ab^2 = a.$$

This yields an isomorphism of order 2, as it swaps the two elements a and ab, while fixing the remaining two group elements. We denote this isomorphism by s'''.

(v) $\varphi(a) = b$ and $\varphi(b) = ab$: This would imply that

$$\varphi(ab) = b(ab) = b(ab)^{-1} = b(b^{-1}a^{-1}) = (bb^{-1})a^{-1} = a^{-1} = a.$$

Since $a \to b, b \to ab, ab \to a$, this isomorphism cyclically permutes a, b, ab, and hence is of order 3. We denote this isomorphism by r'.

(vi) $\varphi(a) = ab$ and $\varphi(b) = a$: This would imply that

$$\varphi(ab) = (ab)a = (ab)^{-1}a = (b^{-1}a^{-1})a = b^{-1} = b.$$

Since $a \to ab, ab \to b, b \to a$, this isomorphism cyclically permutes a, ab, b, and hence is of order 3. We denote this isomorphism by r''.

Thus, we have

$$\mathrm{Aut}(G) = \{1, r', r'', s', s'', s'''\}.$$

Further, a direct computation yields that:

$$r' \circ r' = r'',\ s' \circ r' = s'', s' \circ (r' \circ r') = s''',\ \text{and}\ s'(r')^k = (r')^{3-k} s',\ 0 \leq k \leq 2,$$

where $(r')^k = \underbrace{r' \circ r' \circ \ldots \circ r'}_{k \text{ times}}$. Therefore, the map

$$\psi : D_6 = \langle r, s \rangle \to \mathrm{Aut}(G) = \langle r', s' \rangle : s^i r^j \overset{\psi}{\mapsto} (s')^i (r')^j,\ \text{for}\ i = 0, 1\ \text{and}\ 0 \leq j \leq 2,$$

is clearly an isomorphism, and the assertion follows.