MTH 203 Final Exam solutions

1. Show that $\mathbb{Z}_n$ has a unique element of order 2 if, and only if, $2 \mid n$.

   Solution. Suppose that $\mathbb{Z}_n$ has a unique element of order 2. Then by the Lagrange's Theorem, it follows that $2 \mid n$.

   Conversely, let us assume that $2 \mid n$. First, we note that in any group G, there is a one-to-one correspondence between the elements of order 2, and the distinct order 2 subgroups of G. By Lesson Plan 1.4 (iv), every proper subgroup of $\mathbb{Z}_n$ is of the form $\langle [n/d] \rangle$, where d is a proper divisor of n. Moreover, by Lesson Plan 1.2 (vii), we know that for any $[k] \in \mathbb{Z}_n$, $o([k]) = n/\gcd(k,n)$, so we have that

   $$o([n/d]) = 2 \iff n/\gcd(n/d, n) = 2 \iff n/(n/d) = 2 \iff d = 2.$$

   Hence, $\mathbb{Z}_n$ has a unique element of order 2, namely $[n/2]$.

2. Show that a group G is abelian if, and only if, the map

$$\varphi : G \to G : g \overset{\varphi}{\mapsto} g^{-1}, \forall g \in G$$

is an isomorphism.

Solution. Suppose that φ is an isomorphism. Then for any $a, b \in G$, we have

$$\begin{aligned} b^{-1}a^{-1} &= (ab)^{-1} && \text{(By group laws)} \\ &= \varphi(ab) && \text{(By definition)} \\ &= \varphi(a)\varphi(b) && (\because \varphi \text{ is a homomorphism}) \\ &= a^{-1}b^{-1} && \text{(By definition)} \end{aligned}$$

Hence, it follows that G is abelian.

Conversely, suppose that G is abelian. Then for any $a, b \in G$, we have

$$\begin{aligned} \varphi(ab) &= (ab)^{-1} && \text{(By definition)} \\ &= b^{-1}a^{-1} && \text{(By group laws)} \\ &= a^{-1}b^{-1} && (\because G \text{ is abelian}) \\ &= \varphi(a)\varphi(b). && \text{(By definition)} \end{aligned}$$

So, we have that φ is a homomorphism. It remains to show that φ is bijective. Since for each $g \in G$,

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

is follows that φ is surjective. Furthermore, we see that

$$\begin{aligned} \operatorname{Ker} \varphi &= \{x \in G : \varphi(x) = 1\} \\ &= \{x \in G : x^{-1} = 1\} \\ &= \{x \in G : x = 1\} \\ &= \{1\}, \end{aligned}$$

from which it follows that φ is injective, and hence an isomorphism.

3. Let $\mathbb{R}_n[x]$ be the additive group of all polynomials of degree $\leq n$ in the variable x with coefficients from $\mathbb{R}$. For $1 \leq k \leq n$, let $D_k : \mathbb{R}_n[x] \to \mathbb{R}_n[x]$ be the k^{th} derivative map defined by

$$D_k(p(x)) = \frac{d^k}{dx^k}(p(x)),\ \forall\, p(x) \in \mathbb{R}_n[x].$$

(a) Show that D_k is a homomorphism.

(b) Determine $\operatorname{Ker} D_k$ and $\operatorname{Im} D_k$.

(c) Show that $\mathbb{R}_n[x]/\mathbb{R}_{n-1}[x] \cong \mathbb{R}$.

Solution. (a) Given $f(x), g(x) \in \mathbb{R}_n[x]$, we see that

$$\begin{aligned} D_k(f(x)+g(x)) &= \tfrac{d^k}{dx^k}(f(x)+g(x)) && \text{(By definition)} \\ &= \tfrac{d^k}{dx^k}(f(x)) + \tfrac{d^k}{dx^k}(g(x)) && \text{(Derivative laws)} \\ &= D_k(f(x)) + D_k(g(x)), && \text{(By definition)} \end{aligned}$$

which shows that D_k is a homomorphism.

(b) First, we observe that given $p(x) \in \mathbb{R}_n[x]$ is a polynomial with $\deg(p(x)) = \ell$, then

$$\deg(D_k(p(x))) = \begin{cases} \ell - k, & \text{if } \ell > k, \text{ and} \\ 0, & \text{otherwise.} \end{cases} \qquad (**)$$

Therefore, we have

$$\begin{aligned} \operatorname{Ker} D_k &= \{p(x) \in \mathbb{R}_n[x] : D_k(p(x)) = 0\} && \text{(By definition)} \\ &= \{p(x) \in \mathbb{R}_n[x] : \deg(p(x)) \leq k-1\} && \text{(By (**))} \\ &= \mathbb{R}_{k-1}[x]. && \text{(By definition)} \end{aligned}$$

From (**), it is apparent that $\operatorname{Im} D_k < \mathbb{R}_{n-k}[x]$. Furthermore, given any $p(x) \in \mathbb{R}_{n-k}[x]$, let $P_k(x)$ be any k^{th} anti-derivative of $p(x)$ whose constant term is 0. More precisely, if $p(x) = \sum_{i=1}^{n-k} a_i x^i$, then $P_k(x)$ has the form

$$P_k(x) = \sum_{i=1}^{n-k-1} c_i x^i + \sum_{i=n-k}^{n} b_i x^i, \text{ where the } c_i \in \mathbb{R} \text{ are arbitrary, and } b_i = \frac{a_i}{{}^iP_k}.$$

Then by the definition of anti-derivative, we have $D_k(P_k(x)) = p(x)$, which shows that

$$\operatorname{Im} D_k = \mathbb{R}_{n-k}[x].$$

(c) Applying the First Isomorphism Theorem to the homomorphism D_n, we get

$$\mathbb{R}_n[x]/\operatorname{Ker} D_n \cong \operatorname{Im} D_n.$$

Moreover, by (b), we know that

$$\operatorname{Ker} D_n = \mathbb{R}_{n-1}[x] \text{ and } \operatorname{Im} D_n = \mathbb{R}_0[x].$$

The assertion now follows from the fact that $\mathbb{R}_0[x] = \mathbb{R}$, the additive group of all constant polynomials.

4. Consider the group $G = A_4$.

   (a) Describe the order 2 subgroups of G.

   (b) Describe the order 3 subgroups of G.

   (c) Does G have an element g with $o(g) \geq 4$? Explain why, or why not.

   (d) Show that G has a unique subgroup of order 4.

Solution. We know form Lesson Plan 6.1 (vii), that the group G is isomorphic to the group of rotational symmetries of a tetrahedron T_4 (see Lesson Plan 6.2 (vii)). To describe this isomorphism explicitly, we label the vertices of the tetrahedron with the indices 1-4, and see that each rotational symmetry $r \in \mathrm{Sym}(T_4)$ induces an even permutation σ_r of the set of vertices $\{1, 2, 3, 4\}$. Hence, the map

$$\mathrm{Sym}(T_4) \to A_4 : r \mapsto \sigma_r \tag{*}$$

is an isomorphism.

(a) The order 2 subgroups of A_4 corresponds to (and are generated by) the order 2 elements in A_4, which are induced by the order 2 (i.e π radians) rotations of T_4 under the isomorphism (*). There are precisely 3 such rotations about the 3 axes joining the mid points of opposite edges. These rotations induce permutations which are products of two disjoint transpositions. Hence, there are 3 distinct subgroups of A_4 of order 2, which are:

$$\langle(1\,2)(3\,4)\rangle,\ \langle(1\,3)(2\,4)\rangle,\ \text{and}\ \langle(1\,4)(2\,3)\rangle.$$

(b) By Lagrange's theorem, every non-trivial element in a subgroup of order 3 is of order 3. Furthermore, as every subgroup of order 3 is cyclic, it is generated by an element of order 3. Since the map (*) is an isomorphism, any element of order 3 induced by a rotation of order 3 in $\mathrm{Sym}(T_4)$. There are precisely 8 such non-trivial rotations (by $2\pi/3$ and $4\pi/3$ radians) about the 4 axes joining vertices in T_4 to the centers of opposite faces. These rotations induce 8 distinct 3-cycles in A_4 under the isomorphism (*). Finally, these 3-cycles generate 4 distinct subgroups, which are:

$$\langle(1\,2\,3)\rangle,\ \langle(2\,3\,4)\rangle, \langle(3\,4\,1)\rangle,\ \text{and}\ \langle(4\,1\,2)\rangle.$$

(c) Any element g with $o(g) \geq 4$ has to be induced by a rotation of order ≥ 4 in $\mathrm{Sym}(T_4)$ under the isomorphism (*). However, there exists no rotation in $\mathrm{Sym}(T_4)$ of order greater than 3. Hence, there exists no element $g \in A_4$ with $o(g) \geq 4$.

(d) We know from class that any group of order 4 is isomorphic either to the cyclic group $\mathbb{Z}_4$, or the Klein 4-group $\mathbb{Z}_2 \times \mathbb{Z}_2$. From (c) we know that G has no elements of order 4, so any subgroup of order 4 in A_4 (if it exists) has to be the Klein 4-group. Further, we know that the Klein 4-group has 3 non-trivial elements order 2. From (b), we know that A_4 has exactly 3 distinct elements of order 2, namely:

$$(1\,2)(3\,4),\ (1\,3)(2\,4),\ \text{and}\ (1\,4)(2\,3).$$

These three elements together generate a order 4 subgroup in A_4 given by

$$\{1,\ (1\,2)(3\,4),\ (1\,3)(2\,4),\ (1\,4)(2\,3)\},$$

which is isomorphic to the Klein 4-group.

5. (a) Is the group $\mathrm{SO}(2,\mathbb{R})$ abelian? Prove or disprove.
   (b) Describe two distinct monomorphisms $\mathrm{SO}(2,\mathbb{R}) \to \mathrm{SO}(3,\mathbb{R})$.
   (c) Show that $\mathrm{SO}(3,\mathbb{R})$ is non-abelian.

Solution. (a) From class (see Lesson Plan 6.3 (iii)), we know that $\mathrm{SO}(2,\mathbb{R}) \cong S^1$. Since S^1 is an abelian group under complex multiplication, it follows that $\mathrm{SO}(2,\mathbb{R})$ is abelian.

(b) We know from class (see Lesson Plan 6.3 (iii)), that any element in $\mathrm{SO}(2,\mathbb{R})$ is of the form

$$A_\theta := \begin{bmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{bmatrix}, \ \theta \in \mathbb{R}.$$

We consider two maps $\psi_1, \psi_2 : \mathrm{SO}(2,\mathbb{R}) \to \mathrm{SO}(3,\mathbb{R})$ defined in the following manner:

$$\psi_1(A_\theta) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos(\theta) & \sin(\theta) \\ 0 & -\sin(\theta) & \cos(\theta) \end{bmatrix}, \ \psi_2(A_\theta) = \begin{bmatrix} \cos(\theta) & \sin(\theta) & 0 \\ -\sin(\theta) & \cos(\theta) & 0 \\ 0 & 0 & 1 \end{bmatrix}, \text{ for } A_\theta \in \mathrm{SO}(2,\mathbb{R}).$$

A simple computation reveals that for $i = 1, 2$, $\psi_i(A_\theta) \in \mathrm{SO}(3,\mathbb{R})$, for each $\theta \in \mathbb{R}$. Moreover, given $\alpha, \beta \in \mathbb{R}$ with $\alpha = \beta$, we have that

$$A_\alpha = A_\beta \implies \psi_i(A_\alpha) = \psi_i(A_\beta),$$

which shows that ψ_i is well-defined for $i = 1, 2$.

We will now show that ψ_1 is a monomorphism, as the argument for ψ_2 is analogous. First, we observe that given $A_\alpha, A_\beta \in \mathrm{SO}(2,\mathbb{R})$, we have

$$A_\alpha A_\beta = \begin{bmatrix} \cos(\alpha+\beta) & \sin(\alpha+\beta) \\ -\sin(\alpha+\beta) & \cos(\alpha+\beta) \end{bmatrix} = A_{\alpha+\beta}. \tag{$\dagger$}$$

For simplicity of notation, we will write $\psi_1(A_\theta) = \begin{bmatrix} 1 & 0 \\ 0 & A_\theta \end{bmatrix}$. With this notation in place, we have

$$\begin{aligned}
\psi_1(A_\alpha)\psi_1(A_\beta) &= \begin{bmatrix} 1 & 0 \\ 0 & A_\alpha A_\beta \end{bmatrix} && \text{(By direct computation)} \\
&= \begin{bmatrix} 1 & 0 \\ 0 & A_{\alpha+\beta} \end{bmatrix} && \text{(By } (\dagger)) \\
&= \psi_1(A_{\alpha+\beta}) && \text{(By definition)} \\
&= \psi_1(A_\alpha A_\beta) && \text{(By } (\dagger)),
\end{aligned}$$

which shows that ψ_1 is a homomorphism. Furthermore, we see that

$$\begin{aligned}
\operatorname{Ker}\psi_1 &= \{A_\theta \in \mathrm{SO}(2,\mathbb{R}) : \psi_1(A_\theta) = I_3\} \\
&= \{A_\theta \in \mathrm{SO}(2,\mathbb{R}) : \begin{bmatrix} 1 & 0 \\ 0 & A_\theta \end{bmatrix} = I_3\} \\
&= \{A_\theta \in \mathrm{SO}(2,\mathbb{R}) : A_\theta = I_2\} \\
&= \{I_2\},
\end{aligned}$$

which shows that ψ_1 is injective, and hence a monomorphism.

(c) For any nontrivial $A_\theta \in \mathrm{SO}(2, \mathbb{R})$, a direct computation reveals that $\psi_1(A_\theta)\psi_2(A_\theta) \neq \psi_2(A_\theta)\psi_1(A_\theta)$, which shows that $\mathrm{SO}(3, \mathbb{R})$ is non-abelian.

6. Let G be a finite group of order n.

   (a) Show that for each $g \in Z(G)$, the conjugacy class $[g]_c = \{g\}$.

   (b) Let $g_1, \ldots, g_k$ be the the representatives of the distinct conjugacy classes in $G \setminus Z(G)$. Show that
$$n = |Z(G)| + \sum_{i=1}^{k} |[g_i]_c|.$$

   (c) Suppose that $n = p^2$, where p is prime. Assuming the fact that $p \mid |[g_i]_c|$, for each i, show that G is abelian.

Solution. (a) By definition, we know that
$$Z(G) = \{g \in G : gh = hg, \, \forall h \in G.\}$$
Therefore, for $g \in Z(G)$, we have
$$\begin{array}{rcll} [g]_c & = & \{h \in G : h \sim_c g\} & \text{(By definition of conjugacy class)} \\ & = & \{h \in G : h = xgx^{-1}, \text{for some } x \in G\} & \text{(By definition of conjugacy)} \\ & = & \{h \in G : h = gxx^{-1} = g\} & (\because g \in Z(G)) \\ & = & \{g\}. & \end{array}$$

(b) We know from class (see Lesson Plan 5.4 (ii)), we know $\sim_c$ defines an equivalence relation on G whose equivalence classes are the distinct conjugacy classes of G. Let
$$G_c = \{[g]_c : g \in G\}.$$
As the sum of the number of elements in the distinct conjugacy classes of G add up to the order of G, we have
$$\begin{array}{rcl} |G| & = & \displaystyle\sum_{[g]_c \in G_c} |[g]_c| \\ & = & \displaystyle\sum_{g \in Z(G)} |\{g\}| + \sum_{i=1}^{k} |[g_i]_c| \quad \text{(By (a))} \\ & = & |Z(G)| + \displaystyle\sum_{i=1}^{k} |[g]_c|, \end{array}$$
as required.

(c) Suppose that $|G| = p^2$, where p is prime. Then by Lagrange's Theorem, we have that $|Z(G)| = 1$ or p or p^2. If $|Z(G)| = p^2$, then we have that $Z(G) = G$, that is, G is abelian.

Suppose we assume that $|Z(G)| < p^2$. If $|Z(G)| = 1$, then by (b), we have that
$$p^2 = 1 + \sum_{i=1}^{k} |[g_i]_c|.$$
Since $p \mid |[g_i]_c|$, for each i, it follows that $p \mid \sum_{i=1}^{k} |[g_i]_c|$. Further, as $p \mid p^2$, this would imply that $p \mid 1$, which is impossible. Thus, we have that
$$Z(G) \neq \{1\}, \qquad (\kappa)$$
and so it follows that $|Z(G)| = p$. Since this implies that, $G/Z(G)$ is a group or order p, it follows that $G/Z(G)$ is cyclic. Finally, we conclude from Midterm Q.3 ($Z/Z(G)$ is cyclic $\iff$ G is abelian), that G is abelian.

7. **(Bonus)** Show that for $n \geq 2$, there exists a monomorphism $S_n \to \mathrm{GL}(n, \mathbb{R})$.

Solution. Given a matrix $M \in \mathrm{GL}(n, \mathbb{R})$, we may view it as a matrix $[M_1\, M_2 \ldots M_n]$, where for $1 \leq i \leq n$, M_i represents the i^{th} column vector of M. With this understanding, the identity matrix $I_n = [e_1\, e_2\, \ldots\, e_n]$, where for $1 \leq j \leq n$, e_j is the j^{th} unit vector in $\mathbb{R}^n$.

Consider the map

$$\varphi : S_n \to \mathrm{GL}(n, \mathbb{R}) : \sigma \overset{\varphi}{\mapsto} I_n^\sigma := [e_{\sigma(1)}\, e_{\sigma(2)}\, \ldots\, e_{\sigma(n)}],\ \forall \sigma \in S_n.$$

This map is clearly well-defined. Furthermore, we see that given $\sigma, \tau \in S_n$, we have

$$\begin{aligned} \varphi(\sigma\tau) &= [e_{(\sigma\tau)(1)}\, \ldots\, e_{(\sigma\tau)(n)}] \\ &= [e_{(\sigma(\tau(1))}\, \ldots\, e_{(\sigma(\tau(n))}] \\ &= [e_{\sigma(1)}\, \ldots\, e_{\sigma(n)}][e_{\tau(1)}\, \ldots\, e_{\tau(n)}] \text{ (see (††) below)} \\ &= \varphi(\sigma)\varphi(\tau), \end{aligned}$$

which shows that φ is a homomorphism.

Finally, we have

$$\begin{aligned} \operatorname{Ker}\varphi &= \{\sigma \in S_n : \varphi(\sigma) = I_n\} \\ &= \{\sigma \in S_n : I_n^\sigma = I_n = I_n^1\} \\ &= \{\sigma \in S_n : \sigma = 1\} \\ &= \{1\}, \end{aligned}$$

which shows that φ is injective.

(††) First, we note that for $\sigma \in S_n$, $I_n^\sigma = (a_{ij})_{n\times n}$, where

$$a_{ij} = \begin{cases} 1, & \text{if } i = \sigma(j), \text{ and} \\ 0, & \text{otherwise.} \end{cases}$$

So, for $\sigma, \tau \in S_n$, let $I_n^\sigma = (b_{ij})_{n\times n}$, $I_n^\tau = (c_{ij})_{n\times n}$, and $I_n^{\sigma\tau} = (f_{ij})_{n\times n}$. Then $I_n^\sigma I_n^\tau = (d_{ij})_{n\times n}$, where

$$\begin{aligned} d_{ij} &= \sum_{k=1}^n b_{ik}c_{kj} \\ &= \sum_{k=1}^n b_{(\sigma\tau)(\ell_i)k}c_{kj}, \text{ where } i = (\sigma\tau)(\ell_i), \forall i \\ &= \begin{cases} 1, & \text{if } k = \tau(\ell_i) \text{ and } j = \ell_i, \text{ and} \\ 0, & \text{otherwise} \end{cases} \\ &= \begin{cases} 1, & \text{if } i = (\tau\sigma)(j), \text{ and} \\ 0, & \text{otherwise,} \end{cases} \\ &= f_{ij}, \end{aligned}$$

from which the assertion follows.