2024 1013 MATH3301 Assignment 3

1. $\forall n \in \mathbb{Z},\ n = \frac{n}{1} \in \mathbb{Q}$, so $\mathbb{Z} \subseteq \mathbb{Q}$

$0 \in \mathbb{Z}$

$\forall n, m \in \mathbb{Z},\ n+m \in \mathbb{Z}$

$\forall n \in \mathbb{Z},\ -n \in \mathbb{Z}$

$\forall r \in \mathbb{Q},\quad r + \mathbb{Z} + (-r) = r + (-r) + \mathbb{Z} = \mathbb{Z}$

Hence, $\mathbb{Z} \trianglelefteq \mathbb{Q}$

(a) $\frac{1}{3} + \mathbb{Z} = \{n + \frac{1}{3} \in \mathbb{Q} : n \in \mathbb{Z}\}$

$\frac{1}{4} + \mathbb{Z} = \{n + \frac{1}{4} \in \mathbb{Q} : n \in \mathbb{Z}\}$ (Addition is commutative, so order doesn't matter)

For all $r \in \mathbb{Q}$:

$r \in (\frac{1}{3} + \mathbb{Z}) \cap (\frac{1}{4} + \mathbb{Z}) \Rightarrow \exists n_1, n_2 \in \mathbb{Z},\ r = n_1 + \frac{1}{3} = n_2 + \frac{1}{4}$

$\Rightarrow 12n_1 + 4 = 12n_2 + 3 \Rightarrow 12 \mid 12(n_2 - n_1) = 1 \Rightarrow \mathrm{F}$

Hence, $(\frac{1}{3} + \mathbb{Z}) \cap (\frac{1}{4} + \mathbb{Z}) = \emptyset$

(b) Follow the same argument in (a),

$\mathbb{N} \to (\mathbb{Q}/\mathbb{Z})$, $n \mapsto (\frac{1}{n} + \mathbb{Z})$ is an injection,

so $|\mathbb{N}| = +\infty$ implies $|\mathbb{Q}/\mathbb{Z}| = +\infty$

(c) Define $\sim$ on $\mathbb{Q}$ by $r \sim r'$ if $r \in r' + \mathbb{Z}$

$\frac{2}{3} \notin 0 + \mathbb{Z}$, $\frac{2}{3} + \mathbb{Z} \neq 0 + \mathbb{Z}$

$2 \cdot \frac{2}{3} = \frac{4}{3} \sim \frac{1}{3} \notin 0 + \mathbb{Z}$, $2 \cdot (\frac{2}{3} + \mathbb{Z}) \neq 0 + \mathbb{Z}$

$3 \cdot \frac{2}{3} = 2 \in 0 + \mathbb{Z}$, $3 \cdot (\frac{2}{3} + \mathbb{Z}) = 0 + \mathbb{Z}$

This implies $\operatorname{ord}(\frac{2}{3} + \mathbb{Z}) = 3$

(d) Follow the same argument in (a),

$(x + \mathbb{Z}) \in \mathbb{Q}/\mathbb{Z} \Rightarrow x \in \mathbb{Q} \Rightarrow \exists\, m, n \in \mathbb{Z}$ with $n \geq 1$, $x = \frac{m}{n}$

$\Rightarrow \exists\, n \in \mathbb{Z}$ with $n \geq 1$, $n \cdot (x + \mathbb{Z}) = (nx) + \mathbb{Z} = m + \mathbb{Z} = 0 + \mathbb{Z}$

(e) Define $\sigma: (\mathbb{Q}/\mathbb{Z}) \to e^{2\pi i \mathbb{Q}}$, $(\theta + \mathbb{Z}) \mapsto e^{2\pi i \theta}$ (obviously, this map is surjective)

For all $\theta_1, \theta_2 \in \mathbb{Q}$, $\theta_1 + \mathbb{Z} = \theta_2 + \mathbb{Z} \Rightarrow \exists\, n \in \mathbb{Z}, \theta_1 = \theta_2 + n \Rightarrow e^{2\pi i \theta_1} = e^{2\pi i (\theta_2 + n)} = e^{2\pi i \theta_2}$, σ is well-defined

For all $\theta_1, \theta_2 \in \mathbb{Q}$. $e^{2\pi i \theta_1} = e^{2\pi i \theta_2} \Rightarrow \exists\, n \in \mathbb{Z}, \theta_1 = \theta_2 + n \Rightarrow \theta_1 + \mathbb{Z} = (\theta_2 + n) + \mathbb{Z} = \theta_2 + \mathbb{Z}$, σ is injective

For all $\theta_1, \theta_2 \in \mathbb{Q}$, $\sigma((\theta_1 + \mathbb{Z}) + (\theta_2 + \mathbb{Z})) = \sigma((\theta_1 + \theta_2) + \mathbb{Z}) = e^{2\pi i (\theta_1 + \theta_2)} = e^{2\pi i \theta_1} e^{2\pi i \theta_2} = \sigma(\theta_1 + \mathbb{Z}) \sigma(\theta_2 + \mathbb{Z})$, σ is an isomorphism

2. Consider the group $\mathcal{P}(U)$ under $A\Delta B=\{x\in U: x\in A \text{ exclusive or } x\in B\}$

For all $A\in\mathcal{P}(U)$, $A^2=A\Delta A=\{x\in U: x\in A \text{ exclusive or } x\in A\}=\{x\in U: F\}=\phi$, $\text{ord}(A)\leq 2<+\infty$

However, take $U=\mathbb{N}$, where $|\mathbb{N}|=+\infty$, so $|\mathcal{P}(U)|=+\infty$.

Hence, every element has finite order doesn't imply the group is finite.

3.

$0(2,3)=(0,0)$, $1(2,3)=(2,3)\neq(0,0)$, $2(2,3)=(4,6)=(0,0)$, $\text{ord}((2,3))=2$

There are $[\mathbb{Z}_4\times\mathbb{Z}_6:\langle(2,3)\rangle]=|\mathbb{Z}_4\times\mathbb{Z}_6|/|\langle(2,3)\rangle|=|\mathbb{Z}_4|\times|\mathbb{Z}_6|/\text{ord}((2,3))=4\cdot 6/2=12$ cosets.

$$\left\{\begin{matrix}
(0,0)+\langle(2,3)\rangle=\{(0,0),(2,3)\}, & (0,1)+\langle(2,3)\rangle=\{(0,1),(2,4)\}, & (0,2)+\langle(2,3)\rangle=\{(0,2),(2,5)\}, \\
(1,0)+\langle(2,3)\rangle=\{(1,0),(3,3)\}, & (1,1)+\langle(2,3)\rangle=\{(1,1),(3,4)\}, & (1,2)+\langle(2,3)\rangle=\{(1,2),(3,5)\}, \\
(2,0)+\langle(2,3)\rangle=\{(2,0),(0,3)\}, & (2,1)+\langle(2,3)\rangle=\{(2,1),(0,4)\}, & (2,2)+\langle(2,3)\rangle=\{(2,2),(0,5)\}, \\
(3,0)+\langle(2,3)\rangle=\{(3,0),(1,3)\}, & (3,1)+\langle(2,3)\rangle=\{(3,1),(1,4)\}, & (3,2)+\langle(2,3)\rangle=\{(3,2),(1,5)\}
\end{matrix}\right\}$$

$$\| $$

$$(\mathbb{Z}_4\times\mathbb{Z}_6)/\langle(2,3)\rangle$$

4.(a)

$N \trianglelefteq G \Rightarrow [\forall g\in G \text{ and } n\in N,\ gng^{-1}\in N]$ and $N\le G$

$\Rightarrow [\forall h\in H \text{ and } n\in H\cap N,\ hnh^{-1}\in H\cap N]$ and $H\cap N\le H \Rightarrow H\cap N \trianglelefteq H$

Hence, the quotient group $H/(H\cap N)$ is well-defined.

$N\trianglelefteq G \Rightarrow \forall g\in G$ and $n\in N$, $gn\in Ng$ and $ng\in gN$

$\Rightarrow \forall g\in G,\ gN=Ng \Rightarrow HN=\{hN\}_{h\in H}=\{Nh\}_{h\in H}=NH\Rightarrow HN\le G$

Hence, the group HN is well-defined.

$N\trianglelefteq G$ and $N\le HN$ and $HN\le G \Rightarrow N\trianglelefteq HN$

Hence, the quotient group $(HN)/N$ is well-defined.

(b) Define $\sigma: H/(H\cap N)\to (HN)/N,\ h(H\cap N)\mapsto heN$ (obviously, this map is surjective)

For all $h_1,h_2\in H$, $h_1(H\cap N)=h_2(H\cap N)\Rightarrow \exists n\in H\cap N,\ h_1=h_2n$

$\Rightarrow \exists n\in N,\ h_1e=h_2en \Rightarrow h_1eN=h_2eN$, σ is well-defined.

For all $h_1,h_2\in H$, $h_1eN=h_2eN \Rightarrow \exists n\in N,\ h_1e=h_2en$

$\Rightarrow \exists n=h_2^{-1}h_1\in H\cap N,\ h_1=h_2n \Rightarrow h_1(H\cap N)=h_2(H\cap N)$, σ is injective.

For all $h_1,h_2\in H$, $\sigma([h_1(H\cap N)][h_2(H\cap N)])=\sigma(h_1h_2(H\cap N))=h_1h_2eN=h_1eh_2eN=(h_1eN)(h_2eN)=\sigma(h_1(H\cap N))\sigma(h_2(H\cap N))$.

This implies σ is an isomorphism, $H/(H\cap N)\cong (HN)/N$.

x Take the sequence:

(b) Another approach.

Define $\mu: H \to G/N$, $\mu(h) = hN$.

As μ is the restriction of $\pi: G \to G/N$, $\pi(g) = gN$ on the domain $H \le G$, μ is a homomorphism.

Notice that: (i) $\ker(\mu) = \{h \in H : \mu(h) = eN\} = \{h \in H : hN = eN\} = \{h \in H : h \in eN\} = H \cap N$

(ii) $\mathrm{Im}(\mu) = \{\mu(h) \in G/N : h \in H\} = \{hN \in G/N : h \in H\} = \{hnN \in G/N : h \in H \text{ and } n \in N\} = (HN)/N$

so $H/(H \cap N) = H/\ker(\mu) = \mathrm{Im}(\mu) = (HN)/N$.

5. (a) For all $gN \in G/N$ and $hN \in H/N$:

(i) $H \trianglelefteq G \Rightarrow ghg^{-1} \in H$; (ii) $(gN)(hN)(gN)^{-1} = (ghN)(g^{-1}N) = ghg^{-1}N \in H/N$;

Hence, $H/N \trianglelefteq G/N$.

(b) Define $\mu: G/N \to G/H$, $gN \mapsto gH$ (obviously, this map is surjective, $\mathrm{Im}(\mu) = G/H$)

For all $g_1, g_2 \in G$, $g_1N = g_2N \Rightarrow \exists n \in N, g_1 = g_2 n \Rightarrow \exists n \in H, g_1 = g_2 n \Rightarrow g_1H = g_2H$, μ is well-defined.

For all $g_1, g_2 \in G$, $\mu((g_1N)(g_2N)) = \mu(g_1g_2N) = g_1g_2H = (g_1H)(g_2H) = \mu(g_1N)\mu(g_2N)$, μ is a homomorphism.

Notice that $\ker(\mu) = \{gN \in G/N : \mu(gN) = eH\} = \{gN \in G/N : gH = eH\} = \{gN \in G/N : g \in eH\} = H/N$,

so $(G/N)/(H/N) = (G/N)/\ker(\mu) \cong \mathrm{Im}(\mu) = G/H$

6. (a) For all $g_1, g_2 \in G$:

$$(g_1H)(g_2H) = (g_2H)(g_1H) \Leftrightarrow g_1g_2H = g_2g_1H \Leftrightarrow \exists h \in H, g_1g_2 = g_2g_1h \Leftrightarrow [g_1, g_2] = g_1^{-1}g_2^{-1}g_1g_2 = h \in H$$

Hence:

$$G/H \text{ is abelian} \Leftrightarrow \forall g_1, g_2 \in G, (g_1H)(g_2H) = (g_2H)(g_1H) \Leftrightarrow \forall g_1, g_2 \in G, [g_1, g_2] \in H \Leftrightarrow [G,G] \leq H$$

(b) Note that $[G,G] \leq G$, and for all $g, a, b \in G$, $g[a,b]g^{-1} = [gag^{-1}, gbg^{-1}]$, $[G,G] \trianglelefteq G$.

Note that $[G,G] \leq [G,G]$, $G/[G,G]$ is Abelian, so $[G,G]$ is a valid choice.

For all valid choice H, G/N is Abelian $\Rightarrow [G,G] \leq N$, so N is greater than $[G,G]$.

Hence, $[G,G]$ is the smallest normal subgroup N of G such that G/N is Abelian.

7. Assume to the contrary that $G/Z(G)$ is cyclic, then there exists $gZ(G) \in G/Z(G)$, such that for all $xZ(G) \in G/Z(G)$, there exists $n \in \mathbb{Z}$, such that $xZ(G) = (gZ(G))^n = g^nZ(G)$.

For all $x_1, x_2 \in G$, there exist $n_1, n_2 \in \mathbb{Z}$, such that $x_1 \in g^{n_1}Z(G)$ and $x_2 \in g^{n_2}Z(G)$.

There exist $c_1, c_2 \in Z(G)$, such that $x_1 = g^{n_1}c_1$ and $x_2 = g^{n_2}c_2$, so:

$$x_1x_2 = g^{n_1}c_1g^{n_2}c_2 = g^{n_1}g^{n_2}c_1c_2 = g^{n_2}g^{n_1}c_2c_1 = g^{n_2}c_2g^{n_1}c_1 = x_2x_1, \text{ } G \text{ is Abelian.}$$

Hence, we've proven the contrapositive.

Consider the non Abelian group $\left\{\begin{pmatrix} 1 & y & z \\ 0 & 1 & x \\ 0 & 0 & 1 \end{pmatrix}\right\}$ with centre $\left\{\begin{pmatrix} 1 & 0 & z \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\right\}$. The quotient is Abelian as

$$\begin{pmatrix} 1 & y_1 & z_1 \\ 0 & 1 & x_1 \\ 0 & 0 & 1 \end{pmatrix}^{-1}\begin{pmatrix} 1 & y_2 & z_2 \\ 0 & 1 & x_2 \\ 0 & 0 & 1 \end{pmatrix}^{-1}\begin{pmatrix} 1 & y_1 & z_1 \\ 0 & 1 & x_1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & y_2 & z_2 \\ 0 & 1 & x_2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\left\{\begin{pmatrix} 1 & 0 & z \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\right\}$$

8. Take the sequence:

$$D_4=\{e,r,r^2,r^3,\sigma,r\sigma,r^2\sigma,r^3\sigma\},\ \mathbb{Z}_4=\{e,r,r^2,r^3\},\ \{e\}$$

(i) $\mathbb{Z}_4 \le D_4$ and $[D_4:\mathbb{Z}_4]=|D_4|/|\mathbb{Z}_4|=8/4=2$, so $\mathbb{Z}_4 \trianglelefteq D_4$;

(ii) $|D_4/\mathbb{Z}_4|=[D_4:\mathbb{Z}_4]=2$ is prime, so $D_4/\mathbb{Z}_4 \cong \mathbb{Z}_2$ is Abelian;

(iii) $\{e\} \trianglelefteq \mathbb{Z}_4$;

(iv) $\mathbb{Z}_4/\{e\} \cong \mathbb{Z}_4$ is Abelian. Hence, D_4 is solvable.

9.(a) $\sigma=(i,j,k)$, $\sigma^{-1}=(k,j,i)$, $\tau=(k,a,b)$, $\tau^{-1}=(b,a,k)$

$\sigma\tau\sigma^{-1}\tau^{-1}(i) = \sigma\tau\sigma^{-1}(i) = \sigma\tau(k) = \sigma(a) = a$

$\sigma\tau\sigma^{-1}\tau^{-1}(a) = \sigma\tau\sigma^{-1}(k) = \sigma\tau(j) = \sigma(j) = k$

$\sigma\tau\sigma^{-1}\tau^{-1}(k) = \sigma\tau\sigma^{-1}(b) = \sigma\tau(b) = \sigma(k) = i$

$\sigma\tau\sigma^{-1}\tau^{-1}(b) = \sigma\tau\sigma^{-1}(a) = \sigma\tau(a) = \sigma(b) = b$

$\sigma\tau\sigma^{-1}\tau^{-1}(j) = \sigma\tau\sigma^{-1}(j) = \sigma\tau(i) = \sigma(i) = j$. Hence, $\sigma\tau\sigma^{-1}\tau^{-1}=(i,a,k)$.

(b) For all $i,a,k\in G$, assume that i,a,k are distinct.

Choose $j=a$ and $b=i$, then $(i,a,k)=[(i,j,k)(k,a,b)(i,j,k)^{-1}(k,a,b)^{-1}\in[H,H]$

(c) Assume to the contrary that S_5 is solvable, that is, there exist:

$$S_5 = H_0, H_1, H_2, \cdots, H_r = \{e\},$$

such that: (i) Each $H_{i+1} \trianglelefteq H_i$; (ii) Each H_i/H_{i+1} is Abelian.

Construct: $\quad U = \{\mu \in \mathbb{Z} : H_\mu \text{ contains all 3-cycles}\}$

As $S_5 = H_0$ contains all 3-cycles, $0 \in U$, $U \neq \phi$;

As $\{e\} = H_r$ contains no 3-cycle, $r \notin U$, U has an upperbound $r-1$.

According to the Well-ordering Principle, $u = \max U$ exists.

As $u \in U$, H_u contains all 3-cycles. From question 6, $H_{u+1} \trianglelefteq H_u$ and H_u/H_{u+1} is Abelian implies $[H_u, H_u] \leq H_{u+1}$

As $u+1 \notin U$, H_{u+1} doesn't contain some 3-cycle, contradicting to $[H_u, H_u]$ contains all 3-cycles.

Hence, our assumption is false, and we've proven that S_5 is not solvable.