20241030 MATH3301 Assignment 4

1. Proof: Assume to the contrary that G is not abelian.

For some $g \in G$, the set $C(g)$ of all $h \in G$ that commutes with g is a proper subgroup of G.

Notice that the centre Z is a subgroup of $C(g)$, so $q^m = |Z| \mid |C(g)|$.

Assume that $|C(g)| = \lambda q^m$ for some $1 \le \lambda \le p$.

(i) $g \in C(g)$ and $g \notin Z$ implies $\lambda > 1$

(ii) $C(g)$ is a proper subgroup of G implies $\lambda \mid p$ and $\lambda < p$.

Now we arrive at a contradiction where no such λ exists, so G must be abelian.

2. Proof: Consider the following subset of $G \times X$:

$$Fix = \{(g, x) \in G \times X : g * x = x\}$$

▶ If we partition Fix into vertical slices,

then $Fix = \bigsqcup_{g \in G} \{Fix \text{ with the first entry } g \text{ fixed}\} = \bigsqcup_{g \in G} X_g$

$$|Fix| = \sum_{g \in G} |\{Fix \text{ with the first entry } g \text{ fixed}\}| = \sum_{g \in G} |X_g|$$

▶ If we partition Fix into horizontal slices,

then $Fix = \bigsqcup_{x \in X} \{Fix \text{ with the second entry } x \text{ fixed}\} = \bigsqcup_{x \in X} G_x$

$$|Fix| = \sum_{g \in G} |\{Fix \text{ with the second entry } x \text{ fixed}\}| = \sum_{x \in X} |G_x|$$

Hence, $\sum_{g \in G} |X_g| = \sum_{x \in X} |G_x|$.

3. Proof: Assume that G/Z has a generator gZ with order n.

As $G=\bigsqcup_{k=0}^{n-1} g^kZ$, every element of G is in the form $g^k z$.

For all $g^k z, g^{k'}z' \in G$:

$$g^k z g^{k'} z' = g^k g^{k'} z z' \quad (\text{As } z \in Z)$$
$$= g^{k'} g^k z' z \quad (\text{As } \langle g\rangle \text{ is Abelian and } z, z' \in Z)$$
$$= g^{k'} z' g^k z \quad (\text{As } z' \in Z)$$

So G is Abelian.

4.(a) Proof: Notice that $\{Gx\}_{x\in X}$ partitions X, so:

$$\sum_{y\in Gx}\frac{1}{|Gy|}=\sum_{y\in Gx}\frac{1}{|Gx|}=\frac{1}{|Gx|}\sum_{y\in Gx}1=\frac{1}{|Gx|}|Gx|=1$$

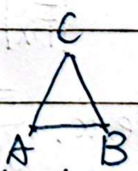
(b) Proof:

$$\#(\text{Distinct Orbit})=\sum_{\text{Distinct Orbit}}1=\sum_{\text{Distinct Orbit}}\sum_{y\in Gx}\frac{1}{|Gy|}$$
$$=\sum_{y\in\bigsqcup_{\text{Distinct Orbit}}Gx}\frac{1}{|Gy|}=\sum_{y\in X}\frac{1}{|Gy|}=\sum_{x\in X}\frac{1}{|Gx|}$$

(c) Proof:

$$\#(\text{Distinct Orbit})=\sum_{x\in X}\frac{1}{|Gx|}=\sum_{x\in X}\frac{1}{|G/G_x|}$$
$$=\sum_{x\in X}\frac{|G_x|}{|G|}=\frac{1}{|G|}\sum_{x\in X}|G_x|=\frac{1}{|G|}\sum_{g\in G}|X_g|$$

5.(a) Solution: According to the Rule of Product:



$$\#(\text{Coloring of }\triangle ABC)=\#(\text{Coloring of }AB)\cdot\#(\text{Coloring of }BC)\cdot\#(\text{Coloring of }CA)=4\cdot4\cdot4=64$$

(b) Solution: Consider the dihedral group $D_3=\{e,(A,B,C),(A,C,B),(A,B),(B,C),(A,C)\}$

$X_e=X$, $|X_e|=|X|=64$; $X_{(A,B)}=\{AC=BC\}$, $|X_{(A,B)}|=16$

$X_{(A,B,C)}=\{AB=BC=CA\}$, $|X_{(A,B,C)}|=4$; $X_{(B,C)}=\{AB=AC\}$, $|X_{(B,C)}|=16$

$X_{(A,C,B)}=\{AB=BC=CA\}$, $|X_{(A,C,B)}|=4$; $X_{(A,C)}=\{BA=BC\}$, $|X_{(A,C)}|=16$

$$\#(\text{Distinct Orbit})=\frac{1}{|D_3|}\sum_{g\in D_3}|X_g|=\frac{1}{6}(64+4+4+16+16+16)=20$$

6.(a) Proof: For $N=\{e\} \trianglelefteq G$ and $p \mid |G/N| = |G|$,

there exists $\pi(a) \in G/N$ with $ord(\pi(a)) = p$ and $\langle \pi(a) \rangle \trianglelefteq G/N$

As $\pi: G \to G/\{e\}$, $g \mapsto \{g\}$ is an isomorphism,

there exists $a \in G$ with $ord(a) = ord(\pi(a)) = p$ and $\langle a \rangle \cong \langle \pi(a) \rangle \trianglelefteq G/N \cong G$

That is, G has a normal subgroup $\langle a \rangle$ of order p.

(b) Proof: Consider the following sequence:

$$\begin{array}{ccccc} G & \xrightarrow{\pi} & G/N & \xrightarrow{\pi'} & (G/N)/N' \\ \trianglerighteq & & \trianglerighteq & & \\ N & & N' & & \end{array}$$

If we can reduce the double quotient into a single quotient, then we are done.

Note that $(G/N)/N' = Im(\pi' \circ \pi) \cong G/Ker(\pi' \circ \pi)$,

so prime $p' \mid |(G/N)/N'| \Rightarrow$ prime $p' \mid |G/Ker(\pi' \circ \pi)|$

$\Rightarrow \exists\, aKer(\pi' \circ \pi) \in G/Ker(\pi' \circ \pi)$

with $ord(aKer(\pi' \circ \pi)) = p'$ and $\langle aKer(\pi' \circ \pi) \rangle \trianglelefteq G/Ker(\pi' \circ \pi)$

$\Rightarrow \exists\, \pi' \circ \pi(a) \in (G/N)/N'$

with $ord(\pi' \circ \pi(a)) = p'$ and $\langle \pi' \circ \pi(a) \rangle \trianglelefteq (G/N)/N'$

Hence, $G' = G/N$ satisfies the property (*).

(c) Proof: We prove this by the strong form of mathematical induction.

(Basis Step) When $d=1$, it suffices to take $H = \{e\}$

(Inductive Hypothesis) For all $k \in \mathbb{N}$, when $d = 1, 2, \cdots, k$, assume the existence of H.

(Inductive Step) When $d = k+1$, note that $d \geq 2$, so d has at least one prime factor p. For this p, take a normal subgroup P of order p, then:

$|G/P| = d/p$

(i) $\frac{d}{p} \le k$; (ii) $\frac{d}{p}$ is a divisor of $|G/P|$

Apply property (*), there exists a subgroup $\tilde{H}$ of order $\frac{d}{p}$.

Now $\pi^{-1}(\tilde{H}) = \bigsqcup_{\text{Distinct Coset}} hP$, $|\pi^{-1}(\tilde{H})| = |\tilde{H}||P| = d$

So $\pi^{-1}(\tilde{H})$ is a subgroup of order d.

To conclude, for all divisor d of $|G|$, G has a subgroup of order d.

(d)(i) Proof: For Abelian group G with divisor p,

Cauchy's Theorem suggests the existence of $P \le G$, such that $|P| = p$.

As G is Abelian, $P \le G$ implies $P \trianglelefteq G$.

(ii) Proof: For p-group G, the class equation:

$$|G| = |Z(G)| + \sum_{\substack{\text{Nonsingleton Distinct} \\ \text{Conjugacy Class}}} \frac{|G|}{|G_x|}$$

suggests that $|Z(G)| \ge p$, so take a nontrivial element $c \in Z(G)$.

WLOG, assume that $ord(c) = p$, then $\langle c \rangle \trianglelefteq G$ does the job.

7.(a) Proof: According to the second isomorphism theorem:

$$\left.\begin{array}{l} \text{(i) } H \le G\times\mathbb{Z}_{30} \\ \text{(ii) } N \trianglelefteq G\times\mathbb{Z}_{30} \end{array}\right\} \Rightarrow \left\{\begin{array}{ll} \text{(i) } HN \le G\times\mathbb{Z}_{30} & \text{(iii) } N \trianglelefteq HN \\ \text{(ii) } H\cap N \trianglelefteq H & \text{(iv) } H/(H\cap N) \cong (HN)/N \end{array}\right.$$

Now it suffices to prove that $|(HN)/N| = 15$ or 30.

Note that $N = \{e\}\times\mathbb{Z}_{30}$, so $HN = K\times\mathbb{Z}_{30}$ for some $K \le G$.

Assume to the contrary that $|(HN)/N| = |K| \ne 15$ and 30, so $|K| < 15$.

As $H \le K\times\mathbb{Z}_{30}$, we have a contradiction $|H| \le |K\times\mathbb{Z}_{30}| = |K||\mathbb{Z}_{30}| < 450$.

Hence, our assumption is wrong, and it must be true that $|H/(H\cap N)| = 15$ or 30.

(b) Solution: Assume to the contrary that $A_5 \times \mathbb{Z}_{30}$ has a subgroup H,

where $|A_5| = 60$ and $|H| = 450$.

As proven in (a), if we project H to the first entry,

then the new projection subgroup K of A_5 has order 15 or 30.

Tutorial 8, Question 4(b) rejected the choice $|K| = 15 = 3*5$

The fact that A_5 is simple rejected the choice $|K| = 30 = |A_5|/2$

Hence, our assumption is wrong, and we've proven that no such H exists.

(c) Solution: Consider the group $A_5 \times \mathbb{Z}_{30}$

This group has exactly 3 prime divisors 2, 3, 5.

Notice that:

(i) $\{e\} \trianglelefteq A_5$ and $15\mathbb{Z}_{30} \trianglelefteq \mathbb{Z}_{30} \Rightarrow \{e\} \times 15\mathbb{Z}_{30} \trianglelefteq A_5 \times \mathbb{Z}_{30}$,

where $|\{e\} \times 15\mathbb{Z}_{30}| = |\{e\}||15\mathbb{Z}_{30}| = 1 \cdot 2 = 2$;

(ii) $\{e\} \trianglelefteq A_5$ and $10\mathbb{Z}_{30} \trianglelefteq \mathbb{Z}_{30} \Rightarrow \{e\} \times 10\mathbb{Z}_{30} \trianglelefteq A_5 \times \mathbb{Z}_{30}$,

where $|\{e\} \times 10\mathbb{Z}_{30}| = |\{e\}||10\mathbb{Z}_{30}| = 1 \cdot 3 = 3$;

(iii) $\{e\} \trianglelefteq A_5$ and $6\mathbb{Z}_{30} \trianglelefteq \mathbb{Z}_{30} \Rightarrow \{e\} \times 6\mathbb{Z}_{30} \trianglelefteq A_5 \times \mathbb{Z}_{30}$,

where $|\{e\} \times 6\mathbb{Z}_{30}| = |\{e\}||6\mathbb{Z}_{30}| = 1 \cdot 5 = 5$;

(iv) For some $450 \mid |A_5 \times \mathbb{Z}_{30}| = 1800$,

no subgroup of order 450 exists.

REMARK: To ensure that for all $d \mid |G|$, there exists $H \leq G$ with $|H| = d$,

it is necessary to require $\forall N \trianglelefteq G$, $\forall$ prime $p \mid |G/N|$, $\exists \pi(a) \in G/N$

with $\mathrm{ord}(\pi(a)) = p$ and $\langle \pi(a) \rangle \trianglelefteq G/N$, which is clearly stronger.

Date / /

8.(a) Solution: In the commutative ring $\mathbb{Z}_3 \times \mathbb{Z}_4$:

$(0,0)$ is neither a zero divisor nor a unit.

$(1,0)\cdot(0,2)=(0,0)$ for some $(0,2)\neq(0,0) \Rightarrow (1,0)$ is a zero divisor

$(2,0)\cdot(0,2)=(0,0)$ for some $(0,2)\neq(0,0) \Rightarrow (2,0)$ is a zero divisor

$(0,1)\cdot(1,0)=(0,0)$ for some $(1,0)\neq(0,0) \Rightarrow (0,1)$ is a zero divisor

$(1,1)\cdot(1,1)=(1,1)$ for some $(1,1)$ $\Rightarrow (1,1)$ is a unit.

$(2,1)\cdot(2,1)=(1,1)$ for some $(2,1)$ $\Rightarrow (2,1)$ is a unit.

$(0,2)\cdot(0,2)=(0,0)$ for some $(0,2)\neq(0,0) \Rightarrow (0,2)$ is a zero divisor

$(1,2)\cdot(0,2)=(0,0)$ for some $(0,2)\neq(0,0) \Rightarrow (1,2)$ is a zero divisor

$(2,2)\cdot(0,2)=(0,0)$ for some $(0,2)\neq(0,0) \Rightarrow (2,2)$ is a zero divisor

$(0,3)\cdot(1,0)=(0,0)$ for some $(1,0)\neq(0,0) \Rightarrow (0,3)$ is a zero divisor

$(1,3)\cdot(1,3)=(1,1)$ for some $(1,3)\neq(0,0) \Rightarrow (1,3)$ is a unit.

$(2,3)\cdot(2,3)=(1,1)$ for some $(2,3)\neq(0,0) \Rightarrow (2,3)$ is a unit.

(b) Solution: Take $1_1 \in R_1$ and $1_2 \in R_2$.

As R_1, R_2 are integral domains, $1_1 \neq 0_1$ and $1_2 \neq 0_2$,

so $(1_1, 0_2) \neq (0_1, 0_2)$ and $(0_1, 1_2) \neq (0_1, 0_2)$ and $(1_1, 0_2)\cdot(0_1, 1_2) = (0_1, 0_2)$

This implies $R_1 \times R_2$ has at least two zero divisors $(1_1, 0_2), (0_1, 1_2)$.

(c) Proof: We may divide our proof into two parts.

Part 1: Assume that I_1, I_2 are ideals of R_1, R_2. Define $K = I_1 \times I_2$

(i) $0_1 \in I_1$ and $0_2 \in I_2 \Rightarrow (0_1, 0_2) \in I_1 \times I_2$;

(ii) $\forall (r_1, r_2), (r_1', r_2') \in I_1 \times I_2 \Rightarrow r_1, r_1' \in I_1$ and $r_2, r_2' \in I_2$

$\Rightarrow r_1 + r_1' \in I_1$ and $r_2 + r_2' \in I_2 \Rightarrow (r_1, r_1') + (r_2, r_2') = (r_1 + r_2, r_1' + r_2') \in I_1 \times I_2$

(iii) $\forall (\lambda_1, \lambda_2) \in R_1 \times R_2$, $\forall (r_1, r_2) \in I_1 \times I_2 \Rightarrow \lambda_1 \in R_1, r_1 \in I_1$ and $\lambda_2 \in R_2, r_2 \in I_2$

$\Rightarrow \lambda_1 r_1 \in I_1$ and $\lambda_2 r_2 \in I_2 \Rightarrow (\lambda_1, \lambda_2)(r_1, r_2) = (\lambda_1 r_1, \lambda_2 r_2) \in I_1 \times I_2$.

Hence, K is an ideal of $R_1 \times R_2$.

Part 2: Assume that K is an ideal of $R_1 \times R_2$. Define $I_1 = \pi_1(K)$ and $I_2 = \pi_2(K)$.

It is clear that $K \subseteq I_1 \times I_2$. For all $(r_1, r_2) \in I_1 \times I_2$, $(r_1, r_2) = (1_1, 0_2)\cdot(r_1, r_2) + (0_1, 1_2)\cdot(r_1, r_2) \in K$

Hence, $K = I_1 \times I_2$ is in such form.