20241028 MATH3301 Tutorial 8

1.(a) Proof: We may divide our proof into three parts.

Part 1: We prove that $*$ is well-defined.

For all $g\in G$, $geg^{-1}=e$.

For all $i\in\mathbb{Z}_p$ and $(a_0,a_1,\cdots,a_{p-1})\in X$:

$$a_0a_1\cdots a_{p-1}=e \Rightarrow a_{p-1}a_0a_1\cdots a_{p-2}=a_{p-1}(a_0a_1\cdots a_{p-2}a_{p-1})a_{p-1}^{-1}=e$$
$$\Rightarrow a_{p-2}a_{p-1}a_0a_1\cdots a_{p-3}=a_{p-2}(a_{p-1}a_0a_1\cdots a_{p-3}a_{p-2})a_{p-2}^{-1}=e$$
$$\Rightarrow\cdots\Rightarrow a_ia_{i+1}\cdots a_pa_0\cdots a_{i-1}=a_i(a_{i+1}\cdots a_pa_0\cdots a_{i-1}a_i)a_i^{-1}=e$$

Hence, $*:\mathbb{Z}_p\times X\to X, (i,(a_0,a_1,\cdots,a_{p-1}))\mapsto(a_i,a_{i+1},\cdots,a_{p-1},a_0,\cdots,a_{i-1})$ is well-defined.

Part 2: We prove that $*$ is associative.

For all $i,j\in\mathbb{Z}_p$ and $(a_0,a_1,\cdots,a_{p-1})\in X$, WLOG, assume that $|i|+|j|<p$.

$$(i+j)*(a_0,a_1,\cdots,a_{p-1})=(a_{i+j},a_{i+j+1},\cdots,a_{p-1},a_0,\cdots,a_{i+j-1})$$

$$i*[j*(a_0,a_1,\cdots,a_{p-1})]=i*(a_j,a_{j+1},\cdots,a_{p-1},a_0,\cdots,a_{j-1})$$
$$=(a_{i+j},a_{i+j+1},\cdots,a_{p-1},a_0,\cdots,a_{i+j-1})$$

Part 3: We prove that $*$ has an identity $0\in\mathbb{Z}_p$.

For all $(a_0,a_1,\cdots,a_{p-1})\in X$: $0*(a_0,a_1,\cdots,a_{p-1})=(a_0,a_1,\cdots,a_{p-1})$

Combine the three parts above, we've proven that $\mathbb{Z}_p \curvearrowright X$

(b) Proof: We wish to find $\vec{a}\in X$, such that its stablizer subgroup $(\mathbb{Z}_p)_{\vec{a}}=\mathbb{Z}_p$.

For all $a\in H$ with $a^p=e$ (actually $e^p=e$, so such choice is valid):

$$aa\cdots a=a^p=e\Rightarrow(a,a,\cdots,a)\in X.$$

For all $i\in\mathbb{Z}_p$, $i*(a,a,\cdots,a)=(a,a,\cdots,a)$, so $i\in(\mathbb{Z}_p)_{(a,a,\cdots,a)}$.

This implies $\mathbb{Z}_p\subseteq(\mathbb{Z}_p)_{(a,a,\cdots,a)}(\subseteq\mathbb{Z}_p)$, so $(\mathbb{Z}_p)_{(a,a,\cdots,a)}=\mathbb{Z}_p$, $(a,a,\cdots,a)\in X^{\mathbb{Z}_p}$

Hence, $X^{\mathbb{Z}_p}\neq\emptyset$.

(c) Proof: Actually we've proven $K \subseteq X^{\mathbb{Z}_p}$, it suffices to show $X^{\mathbb{Z}_p} \subseteq K$.

For all $(a_0, a_1, \cdots, a_{p-2}, a_{p-1}) \in X^{\mathbb{Z}_p}$:

On one hand, $(a_0, a_1, \cdots, a_{p-2}, a_{p-1}) = 1 * (a_0, a_1, \cdots, a_{p-2}, a_{p-1})$

$= (a_1, a_2, \cdots, a_{p-1}, a_0)$, so $a_0 = a_1 = a_2 = \cdots = a_{p-2} = a_{p-1} = \text{some } a \in H$

On the other hand, $(a_0, a_1, \cdots, a_{p-2}, a_{p-1})$ is in the superset X of $X^{\mathbb{Z}_p}$,

so $a^p = aa \cdots aa = a_0 a_1 \cdots a_{p-2} a_{p-1} = e$

Hence, $(a_0, a_1, \cdots, a_{p-2}, a_{p-1}) \in K$, $X^{\mathbb{Z}_p} \subseteq K$ and we are done.

2. (a) Proof: Assume to the contrary that $|K| = |X^{\mathbb{Z}_p}| > 1$,

that is, K contains a nontrivial element k.

As $k^p = e$ and $k \neq e$ and p is prime, $\mathrm{ord}(k) = p \mid |H| = n$, and we are done.

(b) Proof: Every orbit $\mathbb{Z}_p \vec{a}$ has cardinality $|\mathbb{Z}_p \vec{a}| = |\mathbb{Z}_p| / |(\mathbb{Z}_p)_{\vec{a}}|$.

As $|\mathbb{Z}_p \vec{a}| > 1$ and $|\mathbb{Z}_p| = p$ is prime, it must be true that $|\mathbb{Z}_p \vec{a}| = p$.

(c) Proof: According to the orbit decomposition formula:

$$n^{p-1} = |X| = |X^{\mathbb{Z}_p}| + \sum_{\text{all distinct non-singleton orbit}} |\mathbb{Z}_p \vec{a}|$$

$$= 1 + \sum_{\text{all distinct non-singleton orbit}} \text{some multiple of } p$$

$$\equiv 1 \pmod p$$

Hence, $n^p \equiv n^{p-1} n \equiv n \pmod p$

3. (a) (i) Assume that there are n_2 2-Sylow subgroups and n_3 3-Sylow subgroups.

According to Sylow's First Theorem, $n_2 \geq 1$ and $n_3 \geq 1$.

According to Sylow's Third Theorem,

$|G| = 24 = 2^3 \cdot 3 = p^n \cdot m$, $(p, n, m) = (2, 3, 3)$

$n_2 \mid m$ and $p \mid (n_2 - 1) \Rightarrow n_2 \mid 3$ and $2 \mid (n_2 - 1) \Rightarrow n_2 \in \{1, 3\}$

$|G| = 24 = 3^1 \cdot 8 = p^n \cdot m$, $(p, n, m) = (3, 1, 8)$

$n_3 \mid m$ and $p \mid (n_3 - 1) \Rightarrow n_3 \mid 8$ and $3 \mid (n_3 - 1) \Rightarrow n_3 \in \{1, 4\}$

(iii) $S_4 = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3),$
$(1,2,3), (3,2,1), (1,2,4), (4,2,1),$
$(1,3,4), (4,3,1), (2,3,4), (4,3,2),$
$(1,2), (3,4), (1,3,2,4), (1,4,2,3),$
$(1,3), (1,2,3,4), (2,4), (1,4,3,2),$
$(1,4), (1,2,4,3), (1,3,4,2), (2,3)\}$

Step 1: Find 4 distinct 3-Sylow subgroups of S_4.

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

Step 2: Since $n_3 \in \{1, 4\}$, it must be true that $n_3 = 4$,
so we've exhausted all possibilities.

(b)(i) It suffices to prove that the surjective map $\sigma: H\times K \to HK$, $\sigma(h,k) = hk$ is injective.
For all $(h,k), (h',k') \in H\times K$, $hk = h'k' \Rightarrow h'^{-1}h = k'k^{-1} \in H\cap K = \{e\} \Rightarrow (h,k) = (h',k')$
Hence, σ is injective, thus bijective, so $|HK| = |H\times K| = |H||K|$.

(ii) Consider the Klein 4-group $K_4 = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \leq S_4$,
and the transposition group $\mathbb{Z}_2 = \{e, (1,2)\}$
As $\mathbb{Z}_2 \cap K_4 = \{e\}$, and $K_4 \trianglelefteq S_4 \Rightarrow \mathbb{Z}_2 K_4 = K_4 \mathbb{Z}_2$,
we obtain a 2-Sylow subgroup $\mathbb{Z}_2 K_4$ of S_4 as $|\mathbb{Z}_2 K_4| = |\mathbb{Z}_2||K_4| = 8$.

4. (a) (i)
$$\left.\begin{array}{l} P\cap Q \leq P \Rightarrow |P\cap Q| \mid |P| = p \\ P\cap Q \leq Q \Rightarrow |P\cap Q| \mid |Q| = q \end{array}\right\} \Rightarrow |P\cap Q| \mid xp + yq = 1 \Rightarrow |P\cap Q| = 1 \Rightarrow P\cap Q = \{e\}$$

(ii) Note that $|G| = p^1 \cdot q$ and $|P| = p^1$, so P is a p-Sylow subgroup of G.
Assume that $\#(p\text{-Sylow subgroup of } G) = r$
According to Sylow's Third Theorem, $r \mid q$ and $p \mid (r-1)$.
As $p \nmid (q-1)$, it must be true that $r = 1$, so the conjugacy class of P is $\{P\}$
This implies $P \trianglelefteq G$. Similarly, $Q \trianglelefteq G$.
Assume that $x, y \in G$ are the generators of the prime groups P, Q respectively.
$$\left.\begin{array}{l} \langle x\rangle \trianglelefteq G \Rightarrow y\langle x\rangle = \langle x\rangle y \Rightarrow \exists \mu \in \mathbb{Z},\ yx = x^{\mu+1}y \\ \langle y\rangle \trianglelefteq G \Rightarrow \langle y\rangle x = x\langle y\rangle \Rightarrow \exists \nu \in \mathbb{Z},\ yx = xy^{\nu+1} \end{array}\right\} \Rightarrow x^{\mu} = y^{\nu} \in P\cap Q = \{e\}.$$
Hence, $\mu \equiv \nu \equiv 0 \pmod p$, $xy = yx$, and every $g, g' \in G$ commute, the Abelian group $G \cong \mathbb{Z}_p\mathbb{Z}_q$

(b) Proof: Assume to the contrary that A_5 has a subgroup H of order 15.

As $15 = 5 \cdot 3$, where $p-1=4$ is not divisible by $q=3$, $H \cong \mathbb{Z}_{15}$

Take a generator h of the cyclic group H, and consider its cycle pattern.

Case 1: $h = (1,2,3,4,5)$, now $ord(h) = 5 < 15$, contradiction.

Case 2: $h = (1,2,3,4)(5)$, now $h \notin A_5$, contradiction.

Case 3: $h = (1,2,3)(4,5)$, now $h \notin A_5$, contradiction.

Case 4: $h = (1,2,3)(4)(5)$, now $ord(h) = 3 < 15$, contradiction.

Case 5: $h = (1,2)(3,4)(5)$, now $ord(h) = 2 < 15$, contradiction.

Case 6: $h = (1,2)(3)(4)(5)$, now $h \notin A_5$, contradiction.

Case 7: $h = (1)(2)(3)(4)(5)$, now $ord(h) = 1 < 15$, contradiction.

Hence, our assumption is wrong, and we've proven that such H fails to exist.

5.(a) Solution: Consider the 5-Sylow subgroup H of G.

As $|H| = 5 \in (1, 10)$, H is a nontrivial proper subgroup of G.

As $[G:H] = 2$, H is normal in G.

(b) Solution: Notice that H is closed under conjugation.

According to Cauchy's Theorem,

2 is a prime factor of $10 \Rightarrow \exists y \in G$, $ord(y) = 2$

Take a generator x of $\mathbb{Z}_5 = H$. Notice that $ord(yxy^{-1}) = ord(x) = 5$

Case 1: If $yxy^{-1} = x$, then every $g, g' \in G$ commute, the Abelian group $G \cong \mathbb{Z}_{10}$

Case 2: If $yxy^{-1} = x^{-1}$, then x can be regarded as $\frac{2\pi}{5}$ rotation and y can be regarded as reflection, the non Abelian group $G \cong D_5$.