1. Calculate the order of following group:

1(a). $GL_n(p)$

$$\prod_{i=0}^{n-1}(p^n-p^i)$$

1(b). $SL_n(p)$

Consider $SL_n(p) \xrightarrow{\text{map:}} M_i$ $\quad M_i=\{A \mid A\in GL_n(p),\ |A|=i \bmod p\}$.

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} \longrightarrow \begin{bmatrix} i a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ i a_{n1} & \cdots & a_{nn} \end{bmatrix}$$

$M_i \longrightarrow SL_n(p)$

$x \longmapsto x^{p-1}$ $\quad (i^{p-1}\equiv 1 \bmod p \quad i=1,\dots,p-1)$

$\Rightarrow \{M_i\} \xleftrightarrow{1:1} \{SL_n(p)\} \Rightarrow |SL_n(p)|=\dfrac{|GL_n(p)|}{p-1}$

2. Let $C\subset M_n(F)$ be the scalar matrix over F. Prove $C=Z(GL_n(F))$

1° $\forall x\in C,\ \forall y\in M_n(F)$ $\quad xy=yx \Rightarrow C\subset Z(GL_n(F))$

2° $\forall x\in Z(GL_nF)$

$x e_{ij}=e_{ij}x \Rightarrow x=(a)_{ij}$, $\quad$ if $i\neq j$ $a_{ij}=0$

if $i=j$ $a_{11}=\cdots=a_{nn}$.

$\Rightarrow x\in C \Rightarrow Z(GL_nF)\subset C$

3° $C=Z(GL_n(F))$

3. Prove $x^{\varphi(n)}\equiv 1 \bmod n.$ for $1\le x<n$.

Consider $N^*=\{a_1=1,\ a_2,\dots a_{\varphi(n)}\}$

$a_1, a_2\dots a_{\varphi(n)}$ are numbers coprime to n from 1 to n.

P. N^* with "$\cdot$" is a group.

binary operation ✓ associativity ✓ identity ✓ as for inverses

Consider Bezout Thm $\forall a_i \in N^*$ $\exists k_1, k_2 \in \mathbb{Z}$ s.t

$$k_1 a_i + k_2 n = 1$$

$\Rightarrow$ $k_1 a_i \equiv 1 \bmod n$ $\Rightarrow$ $\overline{k_1}$ is inverses of a_i and also $(k_1, n) = 1$

$\Rightarrow \overline{k_1} \in N^*$. ✓

3. $|N^*| = \varphi(n)$ $\Rightarrow$ $\forall x \in N^*$, $|x| \mid |N^*|$ Lengrange Thm

$\Rightarrow$ $x^{\varphi(n)} \equiv 1 \bmod n$.

4. $a, b \in G$ If $aba^{-1} = b^r$ then prove $a^i b a^{-i} = b^{r^i}$

$$aba^{-1} = b^r$$

$$\Rightarrow a^i b a^{-i} = a^{i-1} aba^{-1} a^{-i+1} = a^{i-1} b^r a^{-i+1}$$

$$= a^{i-2} a b^r a^{-1} a^{-i+2}$$

$$= a^{i-2} \underbrace{aba^{-1} \cdots aba^{-1}}_{r \text{ times}} a^{-i+2} = a^{i-2} b^{r^2} a^{-i+2} = \cdots = b^{r^i}$$

5. Let G be a group. If $\forall a, b \in G$. $(ab)^2 = a^2 b^2$ prove G abelian.

If $\exp(G) = 2$ then G abelian.

$abab = aabb \Rightarrow ba = ab \Rightarrow$ abelian.

$\exp(G) = 2$ shows $\forall a, b \in G$ $(ab)^2 = e = e \cdot e = a^2 b^2$ so G abelian.

6. Assume $|G|$ even prove $\exists\, a \neq e \in G$ s.t $a^2 = e$.

divide elements of G in pairs. if $\{g_i, g_i^{-1}\} \cap \{g_j, g_j^{-1}\} \neq \emptyset$ then they equal.

set $\{g_i, g_i^{-1}\}$ ..... (can be shown this is a partition.

since $|G|$ even. there must $\exists\, x \in G$ s.t $\{x, x^{-1}\}$ has only one elem. In other words $x = x^{-1} \Rightarrow x^2 = e$

7. Suppose $n > 2$. prove that for a finite group G. $\exists$ even number of x where $|x| = n$

Same method.

$\{g, g^{-1}\}$ appears in pairs expect of e and $|x| = 2$.

8. $a, b \in SL_2(\mathbb{Q})$ where $a = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, $b = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$

(a). $a = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ $\quad a^2 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$

$a^3 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$

$a^4 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & \\ & 1 \end{bmatrix} \Rightarrow |a| = 4$.

(b). $b = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$

$b^2 = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}$

$b^3 = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \Rightarrow |b| = 3$

(c). $ab = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ $\quad (ab)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$

$\Rightarrow |ab| = \infty$.

9. If G has only fin many subgroups. prove G is finite.

$\forall g \in G$, $\langle g \rangle$ is a subgroup.

Now consider for all elements in G

$H_1 = \langle g_1 \rangle$ $H_2 = \langle g_2 \rangle$, . . . (*)

since G has only finitely many subgroups so the sequence (*) must be finite and it shows $|G| < \infty$.