Lecture III.

Let p be a prime number, $n \geq 1$.

Consider the group $(\mathbb{Z}/p\mathbb{Z})^n$.

If $H \subset (\mathbb{Z}/p\mathbb{Z})^n$ is a subgroup

Then $H \simeq (\mathbb{Z}/p\mathbb{Z})^m$ for some

m $0 \leq m \leq n$, If $m = 0$ then $H = \langle e \rangle$

If $m = n$ then $H = (\mathbb{Z}/p\mathbb{Z})^n$

Hence we can assume $0 < m < n$.

Let $S_m = \left\{ M \subset (\mathbb{Z}/p\mathbb{Z})^n \;\middle|\; M \text{ is a subgroup and } M \simeq (\mathbb{Z}/p\mathbb{Z})^m \right\}$

$\# S_m = ?$ $\qquad$ $\# S :=$ cardinality of S.

$$\mathrm{Aut}\left((\mathbb{Z}/p\mathbb{Z})^n\right) = \left\{ f : (\mathbb{Z}/p\mathbb{Z})^n \longrightarrow (\mathbb{Z}/p\mathbb{Z})^n \;\middle|\; \begin{array}{l} f \text{ is} \\ \text{surjective homo} \end{array} \right\}$$

Is the set of Automorphisms of the group $(\mathbb{Z}/p\mathbb{Z})^n$.

$$M_n(\mathbb{Z}/p\mathbb{Z}) = \left\{ f : (\mathbb{Z}/p\mathbb{Z})^n \longrightarrow (\mathbb{Z}/p\mathbb{Z})^n \;\middle|\; \begin{array}{l} f \text{ is} \\ \text{a group} \\ \text{homo} \end{array} \right\}.$$

$$= \left\{ (a_{ij})_{1 \leq i,j \leq n} \;\middle|\; a_{ij} \in \mathbb{Z}/p\mathbb{Z} \right\}.$$

$$\mathrm{Aut}\left((\mathbb{Z}/p\mathbb{Z})^n\right) \subset M_n(\mathbb{Z}/p\mathbb{Z})$$

$$\shortparallel$$

$$GL_n(\mathbb{Z}/p\mathbb{Z}) := \left\{ (a_{ij}) \in M_n(\mathbb{Z}/p\mathbb{Z}) \;\middle|\; \underset{\neq 0}{\det(a_{ij})} \right\}$$

If $A = (a_{ij})_{1 \le i,j \le n}$ $\det(A) = \det(a_{ij})$

$$= \sum_{\sigma \in S_n} \operatorname{Sign}(\sigma)\, a_{1\sigma(1)} \cdots a_{n\sigma(n)}$$

where $S_n = \text{Bijection}\{1, 2, \ldots, n\}$
$B(\{1, 2, \ldots, n\})$.

<u>DFN</u>: An S_n is called a permutation of $\{1, \ldots, n\}$. An element $\sigma \in S_n$ is called a transposition if $\exists$ $i, j \in \{1, \ldots, n\}$ s.t. $i \neq j$

$$\sigma(k) = k \quad \forall \quad k \in \{i, j\}$$
$$\sigma(i) = j \quad \text{and} \quad \sigma(j) = i$$

<u>Fact</u>: Any permutation is product of transposition

If σ is a transposition then we define $\text{Sign}(\sigma) = -1$.

$$\text{Sign}(\text{Id}_{\{1,\dots,n\}}) = 1.$$

$$\text{Sign}(\sigma_1 \cdots \sigma_m) = \text{Sign}(\sigma_1) \cdots \text{Sign}(\sigma_m)$$

— x —

Example: $n = 2$.

$$\text{Aut}\left(\left(\mathbb{Z}/p\mathbb{Z}\right)^2\right)$$

$$\shortparallel$$

$$GL_2(\mathbb{Z}/p\mathbb{Z}) = \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \middle| \begin{array}{c} a_{11}a_{22} - a_{12}a_{21} \\ \neq 0 \end{array} \right\}$$

— x —.

$$\left(\mathbb{Z}/p\mathbb{Z}\right)^n = \underbrace{\mathbb{Z}/p\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p\mathbb{Z}}_{n\text{-copies}}.$$

$(a_1, a_2, \dots, a_n) \in (\mathbb{Z}/p\mathbb{Z})^n \qquad a_i \in \mathbb{Z}/p\mathbb{Z}.$

$$\| $$

$\sum_{i=1}^{n} a_i e_i$ where

$$e_i = (0, \dots 0, \underset{i^{th}\text{ place}}{1}, 0 \dots 0)$$

If $\varphi : (\mathbb{Z}/p\mathbb{Z})^n \longrightarrow (\mathbb{Z}/p\mathbb{Z})^n$

is a bijective homo (i.e. An Auto)

then

$$\varphi(e_i) = (a_{1i}, \dots a_{ni}) \qquad 1 \le i \le n$$

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \\ a_{n1}, & \dots, & a_{nn} \end{pmatrix} \begin{pmatrix} 0 \\ \vdots \\ 1 \text{ - } i^{th}\text{ place} \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} a_{1i} \\ \vdots \\ a_{ni} \end{pmatrix}$$

Giving "φ" is equiv. to giving the matrix $(a_{ij})_{1 \le i,j \le n} \in GL_n(\mathbb{Z}/p\mathbb{Z})$.

Note That

$GL_n(\mathbb{Z}/p\mathbb{Z})$ is a Subgroup of $B((\mathbb{Z}/p\mathbb{Z})^n)$

$$GL_n(\mathbb{Z}/p\mathbb{Z}) \subsetneq B((\mathbb{Z}/p\mathbb{Z})^n)$$

The Set $(\mathbb{Z}/p\mathbb{Z})^n$ has extra structure namely it is a group and we Can Consider Set of Bijection which preserves the group Structure.

—

If $X = \mathbb{R}^2$,

$$GL_2(\mathbb{R}) = \{ f \in B(\mathbb{R}^2) \mid f \text{ is } \mathbb{R}\text{-linear} \}$$

—x—

$\# GL_n(\mathbb{Z}/p\mathbb{Z})$.

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \in GL_n(\mathbb{Z}/p\mathbb{Z})$$

$$\Rightarrow (a_{11}, \ldots, a_{1n}) \neq (0, \ldots, 0)$$

$$\begin{array}{c} \cap \\ (\mathbb{Z}/p\mathbb{Z})^n - \{(0,\ldots,0)\} \end{array}$$

There are $(p^n - 1)$ choices are there for $(a_{11}, \ldots, a_{1n})$

$$(a_{21}, \ldots, a_{2n}) \notin \mathbb{Z}/p\mathbb{Z} \cdot \underset{\neq 0}{(a_{11}, \ldots, a_{1n})}$$

$(a_{21}, \ldots, a_{2n})$ can be chosen in $p^n - p$ ways once the choice of $(a_{11}, \ldots, a_{1n})$ is made.

$\vdots$

$(a_{i1}, \ldots, a_{in})$ can be chosen in $p^n - p^{i-1}$ ways once the choice of $(a_{11}, \ldots, a_{1n}), \ldots, (a_{i-1,1}, \ldots, a_{i-1,n})$

$(a_{n1}, \dots, a_{nn})$ can be chosen in

$p^n - p^{n-1}$ ways once the choices of

$(a_{11} \dots a_{1n}), \dots, (a_{n-1,1}, \dots, a_{n-1,n})$

are made

$$\#GL_n(\mathbb{Z}/p\mathbb{Z}) = (p^n-1)(p^n-p)\cdots(p^n-p^{n-1}).$$
$$\shortparallel$$
$$Aut((\mathbb{Z}/p\mathbb{Z})^n).$$

<u>Example</u>:

$$GL_2(\mathbb{Z}/p\mathbb{Z}) = \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \middle| \; a_{11}a_{22} - a_{12}a_{21} \neq 0 \right\}$$

$$(p^2-1)(p^2-p) = \#GL_2(\mathbb{Z}/p\mathbb{Z})$$

$$(p^3-1)(p^3-p)(p^3-p^2) = \#GL_3(\mathbb{Z}/p\mathbb{Z}).$$

$0 < m < n$

$$S_m = \{ M \subset (\mathbb{Z}/p\mathbb{Z})^n \mid M \underset{\psi}{\simeq} (\mathbb{Z}/p\mathbb{Z})^m \}.$$

Claim: The group $\mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^n)$ $(= GL_n(\mathbb{Z}/p\mathbb{Z}))$ acts on S_m.

$$GL_n(\mathbb{Z}/p\mathbb{Z}) \times S_m \longrightarrow S_m.$$

$$(A, \; M = \langle v_1, \dots, v_m \rangle) \longmapsto \langle Av_1, \dots, Av_m \rangle.$$

$$M \subset (\mathbb{Z}/p\mathbb{Z})^n \qquad M \in S_m$$

$\shortparallel$

$\langle v_1, \dots, v_m \rangle$ where $v_1 \neq 0$, $v_2 \notin \langle v_1 \rangle$

$v_3 \notin \langle v_1, v_2 \rangle, \dots, v_m \notin \langle v_1, \dots, v_{m-1} \rangle$

If $A = (a_{ij}) \in GL_n$ $\langle Av_1, \dots, Av_m \rangle \simeq (\mathbb{Z}/p\mathbb{Z})^m.$

claim: $GL_n(\mathbb{Z}/p\mathbb{Z})$ acts transitively on S_m.

If $M_1 = \langle v_1, .., v_m \rangle$

$M_2 = \langle w_1, .., w_m \rangle$.

we can find $v_{m+1}, .., v_n$

s.t. $\langle v_1, .., v_m, v_{m+1} \cdots v_n \rangle = (\mathbb{Z}/p\mathbb{Z})^n$.

$\langle w_1, .., w_m, w_{m+1}, .., w_n \rangle = (\mathbb{Z}/p\mathbb{Z})^n$

if φ is the matrix corresponding to the $v_i \longmapsto w_i$ $1 \leq i \leq n$.

Then we see $\varphi(M_1) = M_2$.

If a Group G acts on a Set X transitively then X can be identified with the coset space

$$G/G_x \quad \text{where } x \in X$$

G_x - Isotropy gp
$$G_x = \{g \in G \mid g.x = x\}$$

$$X = \underline{O(x)}$$

$$\Rightarrow \# G/G_x = \# O(x)$$

$$\# G/G_x = \frac{\# G}{\# G_x}.$$

$$S_m \simeq GL_n(\mathbb{Z}/p\mathbb{Z})/G_M \qquad MCS_m$$

If $M = \langle e_1, \ldots, e_m \rangle$.

Then we can check that

$$G_M = \left\{ A \in GL_n(\mathbb{Z}/p\mathbb{Z}) \;\middle|\; \begin{pmatrix} A_1 & C \\ 0 & B_1 \end{pmatrix} \right\}$$

where $A_1 \in GL_m(\mathbb{Z}/p\mathbb{Z})$

$B_1 \in GL_{n-m}(\mathbb{Z}/p\mathbb{Z})$

and $C \in M_{m,m-n} = \{ (c_{ij})_{\substack{1 \le i \le m \\ 1 \le j \le m-n}} \mid c_{ij} \in \mathbb{Z}/p\mathbb{Z} \}$.

$$\# M_{m,m-n} = p^{m(n-m)}$$

$$\# GL_m(\mathbb{Z}/p\mathbb{Z}) = (p^m - 1) \cdots (p^m - p^{m-1})$$

$$\# GL_{n-m}(\mathbb{Z}/p\mathbb{Z}) = (p^{m-n} - 1) \cdots (p^{m-n} - p^{m-n-1})$$

$$\therefore \; \# G_M = (p^m - 1) \cdots (p^m - p^{m-1}) (p^{m-n} - 1) \cdots (p^{m-n} - p^{m-n-1}) \times p^{m(n-m)}$$

Hence

$$\# S_m = \frac{\# GL_n(\mathbb{Z}/p\mathbb{Z})}{\# G_M}$$

$$= \frac{(p^n-1)\cdots\cdots(p^n-p^{n-1})}{p^{m(n-m)}(p^m-1)\cdots(p^m-p^{m-1})(p^{n-m}-1)\cdots(p^{n-m}-p^{n-m-1})}$$

—x——x——.