Math 541
Rongpei Wang, Xin Feng

Note: April 6, 2011

Intro question:

Question: $SL_2(\mathbb{F}_p)$={ A=$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$| a,b,c,d ∈ F_P det=ad-bc=1} and the number of elements in $\mathbb{F}_p$ is from 0 up to p-1;

Ask: count the number of element in $SL_2(\mathbb{F}_p)$

Solution: $(p+1)(p^2-p)$

Idea: $SL_2(\mathbb{F}_p) \longleftrightarrow GL_2(\mathbb{F}_p) \xrightarrow{\det\ onto} \mathbb{F}_p^*$

$\#GL_2(\mathbb{F}_p)=(p^2-1)(p^2-p)$

Proposition: *If $\varphi: G \longrightarrow G'$ is a group homomorphism (finite)*
Then the #G=#Ker(φ) · #Im(φ)

Example: $\#SL_2(\mathbb{F}_p)= \frac{(p+1)(p-1)(p^2-p)}{p-1} = (p+1)(p^2-p)$

Proof: Step1.

Claim: $[\,G: Ker(\varphi)\,] = \#Im(\varphi)$, $\#\frac{G}{N} = \#\{gN|g \in G\}$

In fact, ∃ a natural bijection, left coset $\frac{G}{Ker(\varphi)} \cong Im(\varphi)$

To describe this bijection $\frac{G}{Ker(\varphi)}$, $g \cdot Ker(\varphi) \longmapsto \varphi(g)$

Claim: This is a well-defined map, i.e. independent of the representative

If $g \cdot N = g' \cdot N$ then

$\varphi(g) = \varphi(g')$ it is a bijection.

Reformation:

$\forall g, g' \in G,\ \varphi(g) = \varphi(g') \overset{iff}{\Longleftrightarrow} g \cdot N = g' \cdot N$

proof: ⇒suppose that $\varphi(g) = \varphi(g')$

then $\varphi(g)\varphi(g') = \varphi(g^{-1} \cdot g') = 1_G$

so $g^{-1}, g' \in N$ so $g' = g \cdot n\ \ for\, n \in N$

so $g' \cdot N = (gn) \cdot N = g(nN) = g \cdot N$

$\Leftarrow$ suppose that $g \cdot N = g' \cdot N$

$\Rightarrow \quad gn = gn' \;\; \forall n, n' \in N$

$\varphi(g) = \varphi(g'n) = \varphi(g')$

$\uparrow$

$n \in \ker(\varphi)$ ■

Proof: Step2.

$\#G = \#Ker(\varphi) \cdot Im(\varphi)$

Indeed by *Lagrange Theorem*:

$\#G = [G: \ker(\varphi)] \cdot \#\ker(\varphi)$

$\|$

$\#Im(\varphi)$ proved *in Step1*. ■

Quotient Groups:

Identification (natural bijection)

$\bar{\varphi}: G/\ker(\varphi) \xrightarrow{1-to-1 \; and \; onto} Im(\varphi)$

$\uparrow$ This is a group

Examples:

(A) $GL_2(\mathbb{F}_P)/SL_2(\mathbb{F}_P) \xrightarrow{\det} \mathbb{F}_p^* = \mathbb{F}_p - \{0\}$

(B) ${}^{D_n}/_{C_n} \xrightarrow{\det} \{\pm 1\}$

$det: D_n \longrightarrow \{\pm 1\} \quad \ker(\det) = C_n$

(C) ${}^{S_n}/_{A_n} \xrightarrow{\overline{sgn}} \{\pm 1\}$

(D) ${}^{\mathbb{R}}/_{\mathbb{Z}} \xrightarrow{\overline{exp}} S'$

Note: April 8, 2011

Quotient Group

Motivation:

$\varphi: G \to G' \quad N = \ker(\varphi)$

$\frac{G}{N} \xrightarrow{\overline{\varphi}} \mathrm{im}(\varphi) \quad g \cdot n \longmapsto \varphi(g)$

Examples:

(A) $\frac{D_n}{C_n} \simeq \{\pm 1\} \quad \det D_n \to \{\pm 1\} \Rightarrow \overline{\varphi}\ \frac{D_n}{C_n} \simeq \{\pm 1\}$

(B) $\mathrm{sgn}: S_n \to \{\pm 1\}$

Notation:

onto homomorphism = epimorphism
into homomorphism = monomorphism

$\overline{\mathrm{sgn}}: \frac{S_n}{A_n} \simeq \{\pm 1\}$

(C) $\exp: \mathbb{R} \to S' \quad x \longmapsto e^{2\pi i x}$

$\ker(\exp) = \mathbb{Z} \quad \overline{\exp}: \frac{\mathbb{R}}{\mathbb{Z}} \simeq S'$

(D) $\det: O(2) \to \{\pm 1\}$

$\frac{O(2)}{SO(2)} \simeq \{\pm 1\}$

(E) $\mathbb{Z} \xrightarrow{\text{mod } n} \{0, 1, \dots\dots, n-1\}$

$\ker(\text{mod } n) = n\mathbb{Z}$

$\frac{\mathbb{Z}}{n\mathbb{Z}}$

Thereom:
If G & G′ are groups, and $\varphi: a \to a'$ *is homomorphism, then there exist a unique group structure on* $\frac{G}{ker\,(\varphi)}$ *such that the map*

$$\mathrm{Pr}: G \to \frac{G}{\ker(\varphi)}$$

$$g \longmapsto g \cdot \ker(\varphi)$$

is a homomorphism of groups. Moreover, with this group structure, the induced map

$$\bar{\varphi}: \frac{a}{\ker(\varphi)} \simeq \mathrm{Im}(\varphi)$$

is an isomorphism.

Proof:
uniqueness:
suppose we have $\cdot, *$ group structures on $\frac{G}{N}$ such that

$$\mathrm{Pr}: G \to \frac{G}{N}$$
$$g \longmapsto g \cdot \ker(\varphi)$$

Claim: $\cdot = *$

$$\begin{aligned} g \cdot N \cdot g' \cdot N &\stackrel{\text{def}}{=} \mathrm{Pr}(g) \cdot \mathrm{Pr}(g') \\ &\xRightarrow{\text{assumption}\cdot} \mathrm{Pr}(gg') \\ &\xRightarrow{\text{assumption}*} \mathrm{Pr}(g) * \mathrm{Pr}(g') \\ &= gN * g'N \end{aligned}$$

Existence:
Define:

$$gN \cdot g'N = (gg')N$$

Question:

(1) Is this definition depend on the choice of representatives?
ie. Suppose $a, b, a', b' \in G$
such that $aN = a'N$
$bN = b'N$
is true that $abN = a'b'N$

(2) Is $\left(\frac{a}{N}, \cdot, N\right)$ a group?

Definition: $H < G$
Then H acts on element of G also from the right

$$h \rhd g = h \cdot g$$

Then each orbit as $H \cdot G$ and is called right coset for H in G.
The collection of all right cosets is denoted by

$$\frac{H}{G}$$

Examples: $a = S_3 = \mathrm{Aut}(\{1,2,3\})$
$H = \{id, (1\ 2)\}$
Note, $(1\ 3)(1\ 2)(1\ 3)^{-1} = (3\ 2) \notin H$
$(1\ 3)H \neq H\,(1\ 3)$

Theorem Claim: If $N \lhd G$
Then $(\forall g \in G)$, $gN = Ng$

Corollary: If $N \lhd \dot{G}$, then
$(g * N) * (g' \cdot N) = (g \cdot g') \cdot N$