Lecture 8 Further simple groups

For each $n \in \{1, 2, 3, \dots\}$ and each commutative ring R we have the groups

$$GL_n(R) := \left\{ M = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \in M_n(R) \;\middle|\; \det(M) \in R^\times \right\},$$

$$SL_n(R) := \operatorname{Ker}\left(GL_n(R) \xrightarrow{\det} R^\times \right) \trianglelefteq GL_n(R),$$

and

$$PSL_n(R) := SL_n(R) / \{ I_n, -I_n \}.$$

Recall that every finite field F is s.t. $|F| = p^\alpha$, for some prime number p and some $\alpha \in \{1, 2, 3, \dots\}$ and, conversely, given any prime number p and a positive integer α there is (up to isomorphism) exactly one field F s.t. $|F| = p^\alpha$ which we shall denote $\mathbb{F}_{p^\alpha}$.

<u>Remark</u> In concrete terms, $\forall$ p prime and $\alpha \in \mathbb{Z}_{\geq 1}$,

$$\mathbb{F}_{p^\alpha} \cong \mathbb{F}_p[X] / \varphi(X)\mathbb{F}_p[X],$$

for some irreducible $\varphi(X) \in \mathbb{F}_p[X]$ s.t. $\deg \varphi(X) = \alpha$.

Thm The group $PSL_n(\mathbb{F}_{p^\alpha})$ is simple for each $n \in \{1, 2, \dots\}$, each prime p, and each positive integer α, except for

(i) $n = 2$ and $p^\alpha = 2$ $\quad (PSL_2(\mathbb{F}_2) \cong S_3)$

(ii) $n = 2$ and $p^\alpha = 3$ $\quad (PSL_2(\mathbb{F}_3) \cong A_4)$

Proof

[We'll address this later.]

Prop'n If F is a finite field, then the cardinality of the general linear group $GL_n(F)$ is

$$|GL_n(F)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}), \quad q := |F|$$

Proof

	# of β_i's
$\beta_1 \in F^n - \{0\}$	$q^n - 1$
$\beta_2 \in F^n - F\beta_1$	$q^n - q$
$\beta_3 \in F^n - F\beta_1 \oplus F\beta_2$	$q^n - q^2$
$\vdots$	$\vdots$
$\beta_n \in F^n - F\beta_1 \oplus \cdots \oplus F\beta_{n-1}$	$q^n - q^{n-1}$

In other words, if

$$\mathcal{S} := \{ \mathcal{B} \subseteq F^n \mid \mathcal{B} \text{ an ordered basis for } F^n \}$$

then

$$|\mathcal{S}| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}). \qquad *$$

But from linear algebra we have a bijection

$$\begin{aligned} GL_n(F) &\xrightarrow{\sim} \mathcal{S} \\ M &\longmapsto M\mathcal{B}_0 \end{aligned}$$

where $\mathcal{B}_0$ is, say, the canonical basis for F^n. This together with $(*)$ yield the propn. $\square$

Corollary For each finite field F we have

$$|SL_n(F)| = \frac{q^n - 1}{q - 1} (q^n - q) \cdots (q^n - q^{n-1}).$$

Proof

We have a short exact sequence of finite groups

$$1 \longrightarrow SL_n(F) \longrightarrow GL_n(F) \xrightarrow{\det} F^\times \longrightarrow 1.$$

Therefore

$$|GL_2(F)| = |SL_2(F)| \, |F^\times|.$$

But $|F^\times| = q - 1$, so the corollary follows $\square$

Note that

$$|PSL_2(\mathbb{F}_7)| = |GL_3(\mathbb{F}_2)| = 168.$$

It turns out that $PSL_2(\mathbb{F}_7) \simeq GL_3(\mathbb{F}_2)$. This follows from the fact that $PSL_2(\mathbb{F}_7) = \langle S, T \rangle$, where

$$S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and that

$$S \longmapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad T \longmapsto \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

extends to an isomorphism from $PSL_2(\mathbb{F}_7)$ to $GL_3(\mathbb{F}_2)$.