math 417
April 28

Growth in $SL_2(\mathbb{F}_p)$

THEOREM 6.1 (Product Theorem for $\mathrm{SL}_2(\mathbb{F}_p)$; Helfgott version). *There exists $k, \delta > 0$ such that for any p and any subset $A \subset \mathrm{SL}_2(\mathbb{F}_p)$ generating $\mathrm{SL}_2(\mathbb{F}_p)$ as a group, one of the following holds*

$$|A^{(3)}| \geqslant |A|^{1+\delta} \text{ or } (A \cup A^{-1} \cup \{\mathrm{Id}_2\})^{(k)} = \mathrm{SL}_2(\mathbb{F}_p).$$

Used Rep of $SL_2(\mathbb{F}_p)$ + Gowers.

Growth in $SL_2(\mathbb{F}_p)$

k is any finite field

THEOREM 6.2 (Product Theorem for $\mathrm{SL}_2(\mathbb{F}_p)$; approximate subgroup version). *Let $K \geqslant 2$, there exists an absolute constant $C > 0$ such that given any finite field k and any K-approximate subgroup $A \subset G = \mathrm{SL}_2(k)$ generating G, one has either*

(1) $|A| \leqslant K^C$,
(2) $|A| \geqslant |G|K^{-C}$.

By Gowers, if (2) hold $\implies A^{(3)} = SL_2(\mathbb{F}_p)$

Larsen-Pink inequalities (for subgroups)

SL_2 is an example of a linear algebraic gp.

Basics on Algebraic Geometry

Algebraic Varieties: k = field $\bar{k}$ an algebraic closure of k

$n \geq 1$ Consider the affine space $\bar{k}^n$ is equipped with the Zariski topology the closed set in this top are the sets of the shape: $\bar{I} \subset \bar{k}[X_1, \dots, X_n]$ an ideal

$$V_{\bar{I}}(\bar{k}) = \{ \underline{x} \in \bar{k}^n \text{ st } \forall P \in \bar{I} \ P(\underline{x}) = 0 \}$$

<u>Example</u>: $n=1$ $P \in \bar{k}[X]$ $\bar{I} = \bar{k}.P$

$$V_{\bar{I}}(\bar{k}) = \{ x \in \bar{k} \ P(x) = 0 \} = \mathrm{root}_P(\bar{k})$$

- $n=4$

$$\{(a,b,c,d)\in \bar{k}^n \text{ st } ad-bc=1\} = V_{\bar{k}(AD-BC)}(\bar{k})$$

in $\bar{k}[A,B,C,D]$.

- Such a closed set

$V_{\bar{I}}(\bar{k})$ is called an affine algebraic subvariety of $\bar{k}^n$.

Rmq: $I \subset \bar{k}[X_1, \dots, X_n]$ is finitely generated

$V_I(\bar{k})$ is defined as the zero set of a finite family of polynomials!

- Given $V = V_I$ some alg subvariety if the generator of I have degree $\leq D$ we say that V has degree $\leq D$

- if I is generated by at most C polynomials of degree $\leq C$ we say that V has complexity $\leq C$.

<u>Connected component of V</u>: V decomposes as a finite disjoint union of connected subvarieties: the connected component of V

and their number depend only on the complexity of V.

- <u>Irreducible components of V</u>:

V is irreducible if it is not the union of two proper subvarieties.

Any variety is a union of a unique finite set of irred subvarieties called the irred components of V.

- if V is irred: its dimension is the maximal lenght of a chain of inclusions

$$\emptyset \subsetneq V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_D = V$$

where the V_i are irred.

Ex: $\dim \bar{k}^n = n$

$\dim V_{AD-BC} = 3 = 4-1.$

- Suppose one starts from $I \subset k[X_1, \dots, X_n]$

one can define

$$V_I(k) = \{ \underline{x} \in k^n \text{ st } \forall P \in I \ P(x) = 0 \}$$

and for any $k' \supset k$

$$V_I(k') = \{ \underline{x} \in k'^n \text{ st } \forall P \in I \ P(x) = 0 \}$$

$k' = \bar{k}$

$$V_I(\bar{k}) = V_{\bar{I}}(\bar{k}) \quad \bar{I} = \bar{k}.I$$

We then say that V is defined over k and in fact one can define

$$V(K) \text{ for } K \text{ any commutative } k\text{-algebra.}$$

$$\| $$

$$\{ \underline{x} \in K^n \ \forall P \in I \ \ P(\underline{x}) = 0_K \}$$

Linear algebraic Groups

A linear algebraic gp is a subvariety of the affine space $M_n(\bar{k}) \simeq \bar{k}^{n^2}$ with is a gp for multiplication of matrices.

Ex: $SL_2(\bar{k}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\bar{k}) \text{ st } ad - bc = 1 \right\}$

$$GL_n(\bar{k}) = \{ g \in M_n(\bar{k}) \quad \det g \neq 0 \}$$

to see $GL_n(\bar{k})$ as a closed subvariety we see it in $M_n(\bar{k}) \times \bar{k} \simeq \bar{k}^{n^2+1}$

$$GL_n(\bar{k}) := \{ (g, t) \in M_n(\bar{k}) \times \bar{k} \text{ st } \det g \cdot t - 1 = 0 \}$$

$$g \in GL_n(\bar{k}) \longrightarrow (g, (\det g)^{-1}) \in M_n(\bar{k}) \times \bar{k}$$

Def: a linear algebraic gp $G(\bar{k})$ is a subvariety of $GL_n(\bar{k}) \subset M_n(\bar{k}) \times \bar{k}$ with is a subgp of $GL_n(\bar{k})$.

THEOREM 6.7 (Larsen-Pink). *Let $\overline{k}$ be algebraically closed and $\mathrm{G}(\overline{k})$ be a connected simple algebraic group.*

For any $D \geqslant 1$ there exists $C = C(D, \dim \mathrm{G}) > 0$ such that the following holds.

For any finite subgroup $A \subset \mathrm{G}(\overline{k})$, either A is contained in a proper algebraic subgroup $\mathrm{H}(\overline{k}) \subset \mathrm{G}(\overline{k})$ such that $[\mathrm{H} : \mathrm{H}^0] \leqslant C$ or for every closed algebraic subvariety $V(\overline{k}) \subset \mathrm{G}(\overline{k})$ of degree $\leqslant D$, one has

$$|A \cap V(\overline{k})| \leqslant C|A|^{\dim V / \dim G}.$$

Structure of $SL_2(\bar{k})$

Elements: Any element of $SL_2(\bar{k})$ is annihilated by

$$P_g(X) = X^2 - tr(g)X + 1$$

- $tr(g) \neq \pm 2$ g has 2 distinct eigenvalues $\lambda_1 \neq \lambda_2 \in \bar{k}$ g is conjugate to $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$

$\lambda_1 \lambda_2 = 1$

wma that conjugation is in $SL_2(\bar{k})$

if h is a conjugating matrix

$\det(h)^{-\frac{1}{2}} h \in SL_2(\bar{k})$ and conjugated

g to $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$.

- $tr(g) = \pm 2$. $g = \pm Id_2$ (g is central)

$\{\pm Id_2\} = Z_{SL_2(\bar{k})}$

- $P_g = P_{g,min} = X^2 \pm 2X + 1$

g has ± 1 as unique eigenvalue

g is conjugate $\pm\begin{pmatrix} 1 & x \\ & 1 \end{pmatrix}$ $x \in \bar{k}$

g is called regular quaisiunipotent

regular unipotent if $tr(g) = 2$

Subgroups: $g \in SL_2(\bar{k})$ $SL_2 = G$

$$\mathrm{Cent}_g(\bar{k}) = \{ h \in G(\bar{k}) \text{ st } hgh^{-1} = g \}$$

$hg - gh = 0$

algebraic subs of G

- if g is semisimple $\mathrm{Cent}_g(\bar{k})$ is conjugate to $T = \mathrm{Diag}_2(\bar{k}) = \left\{ \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} t \in \bar{k}^\times \right\}$

- The centralizer of ass elements is called a maximal torus (is conjugate) to $\mathrm{Diag}_2(SL_2)(\bar{k})$

- let T_g = maximal torus

the normalized of T_g

$$\mathrm{Nor}_{T_g}(\bar{k}) = \{ h \in SL_2(\bar{k}) \quad h T_g h^{-1} = T_g \}$$

$$\mathrm{Nor}_{T_g}(\bar{k}) = T_g \sqcup w_g T_g \quad \text{where}$$

$$w_g T_g w_g^{-1} = T_g \text{ and } w_g^2 = Id_2$$

$$T = \left\{ \begin{pmatrix} t & \\ & t^{-1} \end{pmatrix} \right\}$$

$$w_T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

- If g is regular unipotent

$$\mathrm{Cent}_g(\bar{k}) = \pm N_g$$ where N_g is a unique unipotent subgp containing g

N_g is conjugate to

$$N = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \quad x \in \bar{k} \right\}.$$

$$\mathrm{Na}_{N_g}(\bar{k}) = \{ h \in G(\bar{k}) \quad h N_g h^{-1} = N_g \}$$

$= B_g = B_{U_g} =$ is called a Borel subgroup and is conjugate to the "Standard" Borel subgp

$$B = \left\{ \begin{pmatrix} t & x \\ 0 & t^{-1} \end{pmatrix} \quad t \in \bar{k}^{\times} \quad x \in \bar{k} \right\}$$

-

Fractional Linear transformation

$\mathbb{P}^1(k) = \{ 0 \subsetneq L \subsetneq \bar{k}^2 \}$ the set of lines in $\bar{k}^2$

$L = \{ (x,y) \in \bar{k}$ st $\beta y - \alpha x = 0 \}$ for some pair $(\alpha, \beta) \neq (0,0)$

$$L \xrightarrow[\text{slope}]{} s(L) = [\alpha : \beta] = \begin{cases} \alpha/\beta & \text{if } \beta \neq 0 \\ \infty & \text{if } \beta = 0 \end{cases}$$

$SL_2(\bar{k}) \curvearrowright \mathbb{P}^1(\bar{k})$ (via the obvious action of $SL_2(\bar{k}) \curvearrowright \bar{k}^2$)

$\forall\, z = s(L) \in \bar{k} \cup \infty$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \begin{cases} \dfrac{az+b}{cz+d} & z \neq -d/c \\ \infty & z = -d/c \end{cases}$$

The kernel of the action is $\{\pm Id_2\}$

- A Borel subgp is the stabilizer of a unique point $z \in \bar{k} \cup \{\infty\}$ B_z

eg: $B_\infty = \left\{ \begin{pmatrix} t & x \\ 0 & t^{-1} \end{pmatrix} \right\}$.

- A maximal torus is the pointwise stabilizer of a pair $\{z_1, z_2\}$ $z_1 \neq z_2$

eg: $\mathrm{Diag}_2(\bar{k}) = \mathrm{Stab}_{0,\infty}$

The normalizer of a maximal torus T_{z_1,z_2} is the stabilizer of the set $\{z_1, z_2\}$

Special Cases of LP for $SL_2(\bar{k})$

Proposition 6.9 (LP for tori). *There exist a constant $C, D > 0$ such that for any finite subgroup $A \subset \mathrm{G}(\bar{k})$ satisfying $|A| \geqslant D$, one of the following holds*

- *For any maximal torus T,*
$$|T \cap A| \leqslant C|A|^{1/3}.$$
- *There is a Borel subgroup B such that*
$$|B \cap A| \geqslant C^{-1}|A|.$$

Proof: The constant C will be determined via the proof.

- Suppose $\forall$ Borel subgp $B \in G(\bar{k})$

$$|B \cap A| < C^{-1}|A|$$

let $\gamma \in G(\bar{k})$ and suppose $A \cap \gamma B \neq \emptyset$

the gp $A \cap B \curvearrowright A \cap \gamma B$ by right translations: $g \in A \cap B$ $x \in A \cap \gamma B$

$$x = a = \gamma b \text{ then}$$

$$xg \in A \qquad xg = \gamma b g \in \gamma B$$

$xg \in A \cap \gamma B$.

this action is simple transitive

$$|A\cap \gamma B| = |A\cap B| \leq C^{-1}|A|$$

Claim: $\exists g\in A$ st $g=\begin{pmatrix} a & b \\ c & d \end{pmatrix} \Rightarrow abcd \neq 0$

the set of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ st $abcd = 0$

is the union of B_∞ $B_0 = wB_\infty$ wB_∞ wB_0

If $C > 4$ and $|A|$ is sufficiently large

$$|A \cap (B_\infty \cup B_0 \cup wB_\infty \cup wB_0)| < |A|$$

so there exists some $g \in A$ with $abcd \neq 0$

- Up to conjugating T wma that

$$T = \left\{ \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \ t \in \bar{k}^{\times} \right\}$$

Let $T_A = T \cap A$.

To bound $|T_A|$ by $|A|^{1/3}$ it is sufficient to produce an injective map

$$\varphi : T_A \times T_A \times T_A \hookrightarrow A$$

$$\left(\Longrightarrow \quad |T_A|^3 = |\varphi(T_A \times T_A \times T_A)| \leq |A| \right)$$

Write $T_A = A \cap T = \left\{ \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \; t \in H_A \right\}$

$$H_A \subset \bar{k}^{\times}$$

Given $t_1, t_2, t_3 \in H_A$

$$\varphi(t_1, t_2, t_3) = \begin{pmatrix} t_1 & \\ & t_1^{-1} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} t_2 & 0 \\ 0 & t_2^{-1} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} t_3 & 0 \\ 0 & t_3^{-1} \end{pmatrix}$$

$$= \begin{pmatrix} t_1 & \\ & t_1^{-1} \end{pmatrix} \begin{pmatrix} a^2 t_2 + bc t_2^{-1} & ac t_2 + bd t_2^{-1} \\ ac t_2 + cd t_2^{-1} & bc t_2 + d^2 t_2^{-1} \end{pmatrix}$$

$$\varphi \ell = \begin{pmatrix} t_1 & \\ & t_1^{-1} \end{pmatrix} \begin{pmatrix} a^2 t_2 + bc t_2^{-1} & ac t_2 + bd t_2^{-1} \\ ac t_2 + cd t_2^{-1} & bc t_2 + d^2 t_2^{-1} \end{pmatrix} \begin{pmatrix} t_3 & 0 \\ 0 & t_3^{-1} \end{pmatrix} \in A$$

since $abcd \neq 0$ the entries of the middle matrix are zero for at most 8 values of t_2.

Given t_2 outside these 8 values

one produce $|H_A|^2$ different elements of A.

In addition the product of the diagonal entries of the matrix φ are

$$* \quad (a^2 t_2 + bc\, t_2^{-1})(bc\, t_2 + d^2 t_2^{-1})$$

$\Rightarrow$ indep of t_1, t_3.

If we vary t_2 the map:

$$t_2 \longrightarrow (d^2 t_2 + bc\, t_2^{-1})(bc\, t_2 + d^2 t_2^{-1})$$

take value in $\bar{k}$ and has fiber of size ≤ 4

One obtient $|H_A|/4$ different values for $(*)$

$$\Rightarrow |T_A| = |H_A| \leq |A|^{1/3}.$$

$\square$

Proposition 6.10. *There exist a constant $C, D > 0$ such that for any finite subgroup $A \subset \overline{G}$ satisfying $|A| \geqslant D$, one of the following holds*

- *For any unipotent subgroup N,*

$$|N \cap A| \leqslant C|A|^{1/3}.$$

- *There is a Borel subgroup B such that*

$$|B \cap A| \geqslant C^{-1}|A|.$$

Proof. Exercise. (hint: use also the inverse of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$) $\square$

LP for Conjugacy Classes

$g \in SL_2(\bar{k})$

$$\mathrm{Conj}(g) = \{ hgh^{-1} \quad h \in SL_2(\bar{k}) \}$$

We have

Proposition 6.11 (LP, large conjugacy classes). *There exist a constant $C, D > 0$ such that for any finite subgroup $A \subset \mathrm{G}(\bar{k})$ satisfying $|A| \geqslant D$, one of the following holds*

- *For any $g \in A$ regular,*

$$|\mathrm{Conj}(g) \cap A| \geqslant C^{-1}|A|^{2/3}.$$

- *There is a Borel subgroup B such that*

$$|B \cap A| \geqslant C^{-1}|A|.$$

Proof: (g semisimple)

Proposition 6.12 (LP, small conjugacy classes). *There exist a constant $C, D > 0$ such that for any finite subgroup $A \subset \mathrm{G}(\overline{k})$ satisfying $|A| \geqslant D$, one of the following holds*

- *For any $g \in \mathrm{SL}_2(\overline{k})$, regular either semisimple or unipotent*

$$|\mathrm{Conj}(g) \cap A| \leqslant C|A|^{2/3}.$$

- *There is a Borel subgroup B such that*

$$|B \cap A| \geqslant C^{-1}|A|.$$

Corollary 6.13. *There exist a constant $C, D > 0$ such that for any finite subgroup $A \subset \mathrm{G}(\overline{k})$ satisfying $|A| \geqslant D$, one of the following holds*

- *For any $g \in A$, regular semisimple contained in the maximal torus T_g we have*

$$|T_g \cap A| \geqslant C^{-1}|A|^{1/3}.$$

- *There is a Borel subgroup B such that*

$$|B \cap A| \geqslant C^{-1}|A|.$$

Corollary 6.14. *There exist a constant $C, D > 0$ such that for any finite subgroup $A \subset \mathrm{G}(\overline{k})$ satisfying $|A| \geqslant D$, one of the following holds*

- *For any $g \in A$, regular unipotent contained in the unipotent subgroup U_g we have*

$$|U_g \cap A| \geqslant C^{-1}|A|^{1/3}.$$

- *There is a Borel subgroup B such that*

$$|B \cap A| \geqslant C^{-1}|A|.$$

A Dichotomy

$A \subset SL_2(\bar{k})$ A not roughly contained in any Borel B.

Theorem 6.15 (Rough description of the finite subgroups of $\mathrm{SL}_2(\overline{k})$). *Suppose that $\overline{k} = \overline{\mathbb{F}_p}$ is the algebraic closure of a finite field k.*

There exist a constant $C, D > 0$ such that for any finite subgroup $A \subset \mathrm{G}(\overline{k})$ satisfying $|A| \geqslant D$, one of the following holds

- *There is a finite subfield $k \supset \mathbb{F}_p$ satisfying*

$$C^{-1}|A|^{1/3} \leqslant |k| \leqslant C|A|^{1/3}$$

  such that A is contained in a conjugate of $\mathrm{SL}_2(k)$ (in particular A has index $\leqslant C$ in that conjugate).
- *There is a Borel subgroup B such that*

$$|B \cap A| \geqslant C^{-1}|A|.$$

LP for AP Subgps

k = finite field $\quad K \geq 2$

$A \subset SL_2(k)$ a K-approximate Subgp

st $\langle A \rangle = SL_2(k)$.

We will prove versions of LP for A.

Lemma 6.16. *Let k, A as above. There exists an absolute constant $D \geqslant 2$ such that for any $C \geqslant 1$, one of the following holds*

- *one has* $|A| \leqslant K^{DC}$;
- *for any linear subspace* $V \subset M_2(\overline{k})$ *of dimension* $\leqslant 3$ *such that* $V \cap \mathrm{SL}_2(\overline{k})$ *is a subgroup, one has*
$$|A^{(2)} \cap V| \leqslant K^{-C}|A|.$$

Rmq:

Lemma 6.17. *There exists an absolute constant D such that for any finite field k satisfying $|k| \geqslant D$, any subspace $V \subset M_2(\overline{k})$ of dimension $d \in \{2,3\}$ such that $V \cap \mathrm{SL}_2(\overline{k})$ is a subgroup, then the group*

$$\{g \in \mathrm{SL}_2(k),\ gVg^{-1} = V\}$$

is a strict subgroup of $\mathrm{SL}_2(k)$.

Rmq: