AGRA II: Aritmética, grupos y análisis
An ICTP-CIMPA Research School

Crecimiento y expansión en SL_2

Harald Andrés Helfgott
Universität Göttingen/CNRS/Université de Paris VI/VII
helfgott@math.univ-paris-diderot.fr

UNIVERSIDAD S. ANTONIO ABAD, CUSCO, PERÚ, del 8 al 22 de Agosto de 2015

Prefacio

Ésta es una breve introducción al estudio del crecimiento en los grupos finitos, con SL_2 como ejemplo. Su énfasis cae sobre los desarrollos de la última década, provenientes en parte de la combinatoria.

El texto – basado en parte en [Hel15] – consiste, en esencia, en notas de clase para un curso en la escuela de invierno AGRA II en la Universidad San Antonio Abad, Cusco, Perú (10–21 agosto 2015), incluyendo algunos ejercicios. El curso fue la primera mitad de una unidad; la segunda mitad, sobre expansores en conexión al espacio hiperbólico, corrió a cargo de M. Belolipetsky.

El tópico tiene una intersección apreciable con varios otros textos, incluyendo el libro [Tao15] de T. Tao y las notas [Kow13] de E. Kowalski. El tratamiento en el Capítulo 3 difiere un tanto de [Hel15], en la medida que sigue un tratamiento más global (grupos algebraicos) y menos local (álgebras de Lie); en ésto puede detectarse una influencia de [Tao15] y [Kow13] (y, en última instancia, [LP11]). No parecen haber desventajas o ventajas decisivas en ésto; simplemente he tomado la oportunidad de explorar un formalismo distinto.

Sin duda, [Hel15] da más detalles que el texto presente, tanto de tipo histórico como de tipo puramente matemático; su tema también es más amplio. La meta principal aquí es dar una introducción concisa, accesible y en cierto sentido participativa al tópico.

Las brevísimas introducciones al grupo SL_2 y a la geometría algebraica en general tienen como intención hacer que el texto comprensible sea comprensible para estudiantes de distintas áreas, aparte de ser partes necesarias de la cultura general. Se pide la paciencia del los lectores para los cuales tales introducciones son innecesarias.

Capítulo 1

Introducción

Nuestra tema es el crecimiento en los grupos; nuestro ejemplo serán los grupos $\mathrm{SL}_2(K)$, K un cuerpo finito.

Qué se quiere decir aquí por *crecimiento*? Hay diferentes puntos de vista, dependiendo del área. La manera más concreta de expresar la cuestión es quizás la siguiente: tenemos un subconjunto finito A de un grupo G. Consideremos los conjuntos

$$\begin{aligned} A, & \\ A \cdot A &= \{x \cdot y : x, y \in A\}, \\ A \cdot A \cdot A &= \{x \cdot y \cdot z : x, y, z \in A\}, \\ &\dots \\ A^k &= \{x_1 x_2 \dots x_k : x_i \in A\}. \end{aligned}$$

Escribamos $|S|$ por el número de elementos de un conjunto finito S. La pregunta es: qué tan rápido crece $|A^k|$ a medida que k se incrementa?

Tales cuestión ha sido estudiado desde la perspectiva de la combinatoria aditiva (caso de G abeliano) y de la teoría de grupos geométrica (G infinito, $k \to \infty$). También hay varios conceptos relacionados, de suma importancia, provenientes de la teoría de grafos y de analogías con la geometría: *diámetros*, *expansores*, etc.

Ahora bien, porqué elegir a los grupos $\mathrm{SL}_2(K)$ como primer caso a estudiar, más allá de la necesidad, en una exposición, de comenzar por un caso concreto?

1.1 Los grupos $\mathrm{SL}_2(R)$

Sea R un anillo; por ejemplo, podemos tomar $R = \mathbb{Z}$, o $R = \mathbb{Z}/p\mathbb{Z}$. Definimos

$$\mathrm{SL}_2(R) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in R, \;\; ad - bc = 1. \right\}.$$

La letra "S" en SL viene de especial (lo que aquí quiere decir: de determinante igual a 1), mientras que "L" viene de lineal (por tratarse de un grupo de matrices). El número 2 viene del hecho que éstas son matrices 2x2.

El grupo $\mathrm{SL}_2(R)$ puede verse por lo menos de dos formas: como un grupo abstracto, y como un grupo de transformaciones geométricas. Visto de una manera o la otra, se trata de un buen caso a estudiar, pues es, por así decirlo, el objeto más sencillo en demostrar toda una gama de comportamientos complejos. Veamos cómo.

1.1.1 La estructura del grupo $\mathrm{SL}_2(R)$

Dado un grupo G, nos interesamos en sus subgrupos $H < G$, y, en particular, en sus subgrupos *normales* $H \lhd G$. Dado $H \lhd G$, podemos decir que G se descompone en H y G/H. Un grupo G sin subgrupos normales (aparte de $\{e\}$ y G) se llama *simple*.

Los grupos simples juegan un rol similar al de los primos en los enteros. Es fácil ver que, para todo grupo finito G, existen

$$\{e\} = H_0 \lhd H_1 \lhd H_2 \lhd \cdots \lhd H_k = G \tag{1.1}$$

tales que H_i/H_{i-1} es simple y no-trivial para $1 \leq i \leq k$. El teorema de Jordan-Hölder nos dice que tal decomposición es en esencia única: los factores H_{i+1}/H_i en (1.1) están determinados por G, y a lo más su orden puede cambiar.

Un grupo resoluble es un grupo que tiene una decomposición tal que H_{i+1}/H_i es abeliano para todo i. Como hemos dicho, la combinatoria aditiva ha estudiado tradicionalmente el crecimiento en los grupos abelianos. El estudio del crecimiento en los grupos resolubles esta lejos de ser trivial, o de reducirse por completo al crecimiento en los grupos abelianos. Empero, una decomposición $H \lhd G$ reduce los problemas de crecimiento (como muchos otros) al estudio de (a) los grupos H y G/H, (b) la *acción* de G/H sobre H. Por ello, en últimas cuentas, tiene sentido concentrarse en el estudio de los grupos simples, y, en particular, en el estudio del crecimiento en los grupos simples no abelianos.

Sea K un cuerpo finito. El grupo $\mathrm{SL}_2(K)$ no es ni abeliano ni resoluble. El *centro*

$$Z(G) = \{g \in G : \forall h \in G \quad hg = gh\}$$

de un grupo G es siempre un subgrupo normal de G. Ahora bien, para $G = \mathrm{SL}_2(K)$, $Z(G)$ es igual a $\{I, -I\}$; así, a menos que K sea el cuerpo $\mathbb{F}_2$ con dos elementos, $Z(G)$ no es el grupo trivial $\{e\} \neq \{I\}$, y por lo tanto $G = \mathrm{SL}_2(K)$ no es simple. Empero, el cociente

$$\mathrm{PSL}_2(K) := \mathrm{SL}_2(K)/Z(\mathrm{SL}_2(K)) = \mathrm{SL}_2(K)/\{I, -I\}$$

sí es simple, para $|K|$ finito y mayor que 3.

Comentario de índole cultural. Así, al considerar $\mathrm{SL}_2(K)$ para K variando sobre todos los cuerpos finitos, obtenemos toda un conjunto infinito de grupos finitos simples $\mathrm{PSL}_2(K)$. Se trata, por así decirlo, de la familia más sencilla de grupos finitos simples, junto con aquella dada por los grupos *alternantes* A_n. (El grupo A_n es el único subgrupo de índice 2 del *grupo simétrico* S_n, el cual, a su vez, consiste en las $n!$ permutaciones de n elementos, con la composición como operación del grupo.) En verdad, el famoso Teorema de la Clasificación de grupos simples nos dice que hay dos tipos de familias infinitas de grupos simples: las familias de grupos de matrices, como $\mathrm{PSL}_2(K)$, y la familia A_n, aparte de un número finito de grupos especiales (como el así llamado "monstruo").

Veamos la estructura de $G = \mathrm{SL}_2(K)$ en más detalle. Si bien $\mathrm{SL}_2(K)$ no tiene subgrupos normales más allá de $\{I\}$, $\{I, -I\}$ y $\mathrm{SL}_2(K)$, tiene subgrupos de varios otros tipos. Los más interesantes para nosotros son los *toros*; en $\mathrm{SL}_2(K)$, aparte del grupo trivial, todos son *toros máximos*. Recordamos que el centralizador de un elemento $g \in G$ es el grupo

$$C(g) = \{h \in G : hg = gh\}. \tag{1.2}$$

Un *toro máximo* (denotado por $T(K)$) es un grupo $C(g)$ donde g es *regular semisimple*; un elemento $g \in G$ es *regular semisimple* si tiene dos valores propios distintos. Esto es lo mismo que decir que $T(K) = \sigma D \sigma^{-1} \cap \mathrm{SL}_2(K)$, donde D es el grupo de matrices diagonales

$$D = \left\{ \begin{pmatrix} r & 0 \\ 0 & r^{-1} \end{pmatrix} : r \in \overline{K} \right\}$$

y $\sigma \in \mathrm{SL}_2(\overline{K})$. Aquí $\overline{K}$ es la compleción (clausura) algebraica de K. Nótese que σ puede o puede no estar en $\mathrm{SL}_2(K)$.

Ejemplo. Sea $K = \mathbb{R}$. Si $\sigma \in \mathrm{SL}_2(\mathbb{R})$, entonces $T(K) = \sigma D \sigma^{-1} \cap \mathrm{SL}_2(K)$ es de la forma

$$\sigma \left\{ \begin{pmatrix} r & 0 \\ 0 & r^{-1} \end{pmatrix} \sigma^{-1} : r \in \mathbb{R}^* \right\} \sigma^{-1}$$

si $\sigma \in \mathrm{SL}_2(\mathbb{R})$, y más bien de la forma

$$\tau \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} : \theta \in \mathbb{R}/\mathbb{Z} \right\} \tau^{-1} \tag{1.3}$$

(para algún $\tau \in \mathrm{SL}_2(\mathbb{R})$) si $\sigma \notin \mathrm{SL}_2(\mathbb{R})$. Está claro que, en el segundo caso, $T(K)$ es un círculo, es decir, un toro 1-dimensional (en el sentido tradicional de "toro").

1.1.2 El grupo de transformaciones $\mathrm{SL}_2(\mathbb{R})$

Uno de varios modelos equivalentes para la geometría hiperbólica en dos dimensiones es el semi-plano de Poincaré, también llamado simplemente semi-plano superior:

$$\mathbb{H} = \{(x, y) \in \mathbb{R}^2 : y > 0\}$$

con la métrica dada por

$$ds = \frac{\sqrt{dx^2 + dy^2}}{y}.$$

Las isometrías de $\mathbb{H}$ que preservan la orientación son las transformaciones lineares fraccionales

$$z \mapsto \frac{az + b}{cz + d}, \tag{1.4}$$

donde $a, b, c, d \in \mathbb{R}$ y $ad - bc \neq 0$. Es fácil ver que esto induce una biyección $\mathrm{PSL}_2(\mathbb{R})$ al conjunto de transformaciones lineares fraccionales. Escribamos gz para la imagen de z bajo una transformación (1.4) inducida por una matriz correspondiente a un elemento $g \in \mathrm{PSL}_2(\mathbb{R})$. No es nada difícil verificar que, para $g_1, g_2 \in \mathrm{PSL}_2(\mathbb{R})$,

$$g_1(g_2 z) = (g_1 g_2)z.$$

En otras palabras, tenemos un isomorfismo de $\mathrm{PSL}_2(\mathbb{R})$ al grupo (con la composición como operación) de las transformaciones lineares fraccionales.

Podemos considerar subacciones; por ejemplo, el *grupo modular (completo)* $\mathrm{SL}_2(\mathbb{Z})$ actúa sobre $\mathbb{H}$. El cociente $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ es de volúmen finito sin ser compacto. Tambien podemos considerar los *grupos modulares de congruencia*

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : a \equiv d \equiv 1 \bmod N, \quad b \equiv c \equiv 0 \bmod N \right\}$$

para $N \geq 1$. Claro está, $\Gamma(N)$ es el núcleo ("kernel") de la reducción $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, y, por lo tanto, $\Gamma(N)\backslash\mathbb{H}$ consiste de $|\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})|$ copias de $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$.

1.2 Perspectivas sobre el crecimiento en los grupos

El crecimiento en los grupos ha sido estudiado de varias perspectivas distintas. Nos concentraremos después en desarrollos relativamente recientes que toman sus herramientas en parte de algunas de estas áreas (clasificación de subgrupos, combinatoria

aditiva) y su relevancia de otras (el estudio de los diámetros y la expansión). Hay aún otras areas de suma importancia cuya relación con nuestro tema recién comienza a elucidarse (teoría de modelos, teoría de grupos geométrica). Demos una mirada a vuelo de pájaro.

Combinatoria aditiva. Éste es en verdad un nombre reciente para un campo de estudios más antiguo, con una cierta intersección con la *teoría aditiva de los números*. Se puede decir que la combinatoria aditiva se diferencia de esta última cuando considera el crecimiento de conjuntos bastante arbitrarios, y no sólamente el de conjuntos como los primos o los cuadrados. Uno de los resultados claves es el teorema de Freiman [Fre73], el cual clasifica los subconjuntos finitos $A \subset \mathbb{Z}$ tales que $A + A$ no es mucho más grande que A. Ruzsa dio una segunda prueba [Ruz91], más general y más simple, e introdujo muchos conceptos ahora claves en el área.

El uso del signo + y de la palabra *aditiva* muestran que, hasta recientemente, la combinatoria aditiva estudiaba grupos abelianos, si bien algunas de sus técnicas se generalizan a los grupos no abelianos de manera natural.

Clasificación de subgrupos. Sea A un subconjunto de un grupo G. Asumamos que A contiene la identidad $e \in G$. Entonces $|A \cdot A| = |A|$ sí y sólo sí A es un subgrupo de G; en otras palabras, clasificar los subgrupos de G equivale a clasificar los subconjuntos de G que no crecen.

Clasificar los subgrupos de un grupo es a menudo algo lejos de trivial – más aún si se desea emprender tal tarea sin utilizar la Clasificacíon de los grupos simples (una herramienta muy fuerte, cuya prueba fue inicialmente juzgada incompleta o poco satisfactoria por muchos). Resulta ser que los trabajos en este área basados sobre argumentos elementales, antes que sobre la Clasificación, son a veces robustos: pueden ser adaptados para darnos información, no sólo sobre los subgrupos de G, sino sobre los subconjuntos A de G que crecen poco.

Diámetros y tiempos de mezcla. Sea A un conjunto de generadores de un grupo G; en otras palabras, $A \subset G$ es tal que todo elemento g de G puede escribirse como un producto $g = x_1 x_2 \dots x_r$ para alguna elección de $x_i \in A$.) El *diámetro* de G con respecto a A es el k mínimo tal que todo elemento g de G puede escribirse como $g = x_1 x_2 \dots x_r$ con $x_i \in A$ y $r \leq k$. Si G es finito, el diámetro es necesariamente finito.

Por qué hablamos de "diámetro"? El *gráfo de Cayley* $\Gamma(G, A)$ es el grafo que tiene G como su conjunto de vértices y $\{(g, ag) : g \in G, a \in A\}$ como su conjunto de aristas. Podemos definir la distancia $d(g_1, g_2)$ entre $g_1, g_2 \in G$ como la longitud del camino más corto de g_1 a g_2, donde se define que la longitud de cada arista es 1. Definimos el diámetro de un grafo como definimos el de cualquier figura: será el máximo de la distancia $d(g_1, g_2)$ para toda elección posible de vertices g_1, g_2. Es

fácil verificar que $\mathrm{diam}(\Gamma(G,A))$ es igual al diámetro de G con respecto a A que acababamos de definir.

La conjetura de Babai [BS88, p. 176] postula que, si G es simple y no abeliano, entonces, para cualquier conjunto de generadores A de G,

$$\mathrm{diam}(\Gamma(G,A)) \ll (\log |G|)^{O(1)},$$

donde las constantes implícitas son absolutas.

(Un poco de notación. Sean f, g funciones de un conjunto X a $\mathbb{C}$. Como es habitual en la teoría analítica de números, para nosotros, $f(x) \ll g(x)$, $f(x) \gg g(x)$ y $f(x) = O(g(x))$ quieren decir la misma cosa: hay $C > 0$ y $X_0 \subset X$ finito ("constantes implícitas") tales que $|f(x)| \leq C \cdot g(x)$ para todo $x \in X$ fuera de X_0. (En verdad, necesitamos que $f(x)$ y $g(x)$ estén bien definidas sólo para x fuera de X_0.) Escribimos $\ll_a, \gg_a, O_a$ si X_0 y C dependen de una cantidad a (digamos). Si X_0 y C no dependen de nada, las llamamos constantes *absolutas*.)

El *tiempo de mezcla* es el k mínimo tal que, si $x_1, x_2, \dots, x_k$ son tomados al azar en A con la distribución uniforme en A, la distribución del producto $x_1 \cdots x_k$ (o, lo que es lo mismo, la distribución del resultado de una caminata aleatoria de longitud k en $\Gamma(G,A)$) esta cerca de la distribución uniforme en G. Hablamos de distintos tiempos de mezcla dependiendo de lo que se quiera decir por "cerca". El estudio de los tiempos de mezcla ha tenido no solo un fuerte color probabilístico (véanse las referencias [DSC93], [LPW09]) sino a menudo también algorítmico (e.g. en [BBS04]).

Expansores y huecos espectrales. Comenzemos dando una definición elemental de lo que es un expansor. Sea A un conjunto de generadores de un grupo finito G. Decimos que el grafo $\Gamma(G,A)$ es un ϵ-expansor (para $\epsilon > 0$ dado) si todo subconjunto $S \subset G$ con $|S| \leq |G|/2$ satisface $|S \cup AS| \geq (1+\epsilon)|S|$. Es muy simple de ver que todo ϵ expansor tiene diámetro muy pequeño ($O((\log |G|)/\epsilon)$; está claro que el diámetro de $\Gamma(G,A)$ es siempre por lo menos $O((\log |G|)/(\log |A|))$).

La alternativa (al final equivalente) es definir los grafos expansores en términos del primer valor propio no trivial λ_1 del Laplaciano discreto de un grafo de Cayley. La *matriz de adyacencia* (normalizada) $\mathcal{A}$ de un grafo es un operador linear en el espacio de funciones $f : G \to \mathbb{C}$; envía tal función a la funcíon cuyo valor en v es el promedio de $f(w)$ en los vecinos w de v. Para ser explícitos, en el caso del grafo de Cayley $\Gamma(G,A)$,

$$(\mathscr{A} f)(g) = \frac{1}{|A|} \sum_{a \in A} f(ag). \tag{1.5}$$

El *Laplaciano discreto* es simplemente $\triangle = I - \mathscr{A}$. (Muchos lectores lo reconocerán como el análogo de un Laplaciano sobre una superficie.)

Asumamos $A = A^{-1}$. Entonces $\triangle$ es un operador simétrico, así que todos sus valores propios son reales. Está claro que el valor propio más pequeño es $\lambda_0 = 0$, correspondiente a las funciones propias constantes. Podemos ordenar los valores propios:

$$0 = \lambda_0 \leq \lambda_1 \leq \lambda_2 \leq \dots .$$

A la cantidad $|\lambda_1 - \lambda_0| = \lambda_1$ se le da el nombre de *hueco espectral*.

Decimos que $\Gamma(G, A)$ es un ϵ-expansor si $\lambda_1 \geq \epsilon$. Para $|A|$ acotado, esta definición es equivalente a la primera que dimos (si bien la constante ϵ difiere en las dos definiciones). Decimos que una familia (conjunto infinito) de grafos $\Gamma(G, A)$ es una *familia de expansores*, o que es una familia con un hueco espectral, si todo grafo en la familia es un ϵ-expansor para algún $\epsilon > 0$ fijo.

Uno de los problemas centrales del área es probar que ciertas familias (si no todas las familias) del tipo

$$\{\Gamma(\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}), A_p)\}_{p \text{ primo}}, \qquad A_p \text{ genera } \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$$

son familias de expansores. Los primeros resultados atacaban el problema mediante el estudio del Laplaciano sobre las superficies $\Gamma(p)\backslash\mathbb{H}$. Un resultado clásico de Selberg [Sel65] nos dice que el Laplaciano sobre $\Gamma(p)\backslash\mathbb{H}$ tiene un hueco espectral independiente de ϵ.

Teoría de grupos geométrica. Teoría de modelos. La teoría de grupos geométrica se centra en el estudio del crecimiento de $|A^k|$ para $k \to \infty$, donde A es un subconjunto de un grupo infinito G. Por ejemplo, un teorema de Gromov [Gro81] muestra que, si A genera a G y $|A^k| \ll k^{O(1)}$, entonces G tiene que ser un grupo de un tipo muy particular (virtualmente nilpotente, para ser precisos). Los argumentos de la teoría de grupos geométrica a menudo muestran que, aún si un grupo no está dado a priori de una manera geométrica, el crecimiento de un subconjunto puede darle de manera natural una geometría que puede ser utilizada.

Si bien los problemas tratados por la teoría de grupos geométrica son muy cercanos a los nuestros, tales argumentos aún no son moneda corriente en el subárea que discutiremos en estas notas, lo cual puede decir simplemente que la manera de aplicarlos aún está por descubrirse. Por otra parte, la *teoría de modelos* – en esencia, una rama de la lógica con aplicaciones a las estructuras algebraicas – ha jugado un rol directo en el subárea. Por ejemplo, Hrushovski [Hru12] dio una nueva prueba del teorema de Gromov, expresando cuestiones del crecimiento en grupos en un lenguaje proveniente de la teoría de modelos; más allá en esta dirección, se debe mencionar a [BGT12]. Se trata de temas que parecen estar lejos de estar agotados.

1.3 Resultados

Uno de los propósitos es dar una prueba del siguiente resultado, debido al autor [Hel08] para $K = \mathbb{Z}/p\mathbb{Z}$. No será idéntica a la primera prueba que diera, sino que incluirá las ideas de varios autores posteriores, incluídas algunas que han hecho que el enunciado sea más general que el original, y otras que han hecho que la prueba sea más clara y fácil de generalizar. En cualquier forma, el enunciado deriva claramente su inspiración de la combinatoria aditiva.

Teorema 1.3.1. *Sea K un cuerpo. Sea $A \subset \mathrm{SL}_2(K)$ un conjunto que genera $\mathrm{SL}_2(K)$. Entonces, ya sea*

$$|A^3| \geq |A|^{1+\delta}$$

o $(A \cup A^{-1} \cup \{e\})^k = \mathrm{SL}_2(K)$, donde $\delta > 0$ y $k > 0$ son constantes absolutas.

Por cierto, gracias a [Gow08] y [NP11], $(A \cup A^{-1} \cup \{e\})^k = \mathrm{SL}_2(K)$ puede reemplazarse por A^3. Mostraremos por lo menos que podemos tomar $k = 3$. Las primeras generalizaciones a K de orden finito no primo se deben a [Din11] y [Var12]; hoy en día, se obtiene la forma general sin mayores complicaciones.

Veamos una consecuencia sencilla.

Ejercicio 1.3.1. *Sea $G = \mathrm{SL}_2(K)$, K un cuerpo finito. Sea $A \subset G$ un conjunto que genera G. El diámetro de $\Gamma(G, A)$ es $\ll (\log |G|)^{O(1)}$, donde las constantes implícitas son absolutas.*

Este enunciado es exactamente la conjetura de Babai para $G = \mathrm{SL}_2(K)$.

Cuándo es que $\Gamma(G, A)$ tiene diámetro $\ll \log |G|$? Yendo más lejos – cuándo es un ϵ-expansor?

Se sabía desde los años 80 (ver las referencias en [Hel15]) que la existencia de un agujero espectral para $\Gamma(p)\backslash\mathbb{H}$ (probada en [Sel65]) implica que, para

$$A_0 = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\}, \tag{1.6}$$

los gráfos $\Gamma(\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}), A_0 \bmod p)$ forman una familia de expansores (i.e., son todos ϵ-expansores para algún ϵ fijo). Empero, para, digamos,

$$A_0 = \left\{ \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix} \right\}, \tag{1.7}$$

no se tenía tal resultado, ni aún una cota razonable para el diámetro.

Ejercicio 1.3.2. *Sea $G = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$; sea A_0 como en (1.7). Pruebe que el diámetro de $\Gamma(G, A_0 \bmod p)$ es $\ll \log |G|$.*

Para resolver este ejercicio, es útil saber que A_0 genera un subgrupo libre de $\mathrm{SL}_2(\mathbb{Z})$. Decimos que un conjunto A_0 en un grupo genera un *subgrupo libre* si no existen $x_i \in A_0$, $1 \leq i \leq k$, $x_{i+1} \notin \{x_i, x_i^{-1}\}$ para $1 \leq i \leq k-1$, $x_i \neq e$ para $1 \leq i \leq k$, y $r_i \in \mathbb{Z}$, $r_i \neq 0$, tales que

$$x_1^{r_1} \cdots x_k^{r_k} = e.$$

Saber que A_0 genera un subgrupo libre es particularmente útil en los primeros pasos de la iteración; en los ultimos pasos, podemos utilisar el Teorema 1.3.1.

En verdad, la aseveración del ejercicio 1.3.2 sin la suposición que el grupo $\langle A_0 \rangle$ generado por A_0 sea libre; es suficiente (y fácil) mostrar que $\langle A_0 \rangle$ siempre tiene un subgrupo libre grande. Sí se debe asumir que $\langle A_0 \rangle$ genera un subgrupo *Zariski-denso* de SL_2, para así asegurar que $A_0 \bmod p$ en verdad genere $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, para p mayor que una constante C.

Bourgain y Gamburd [BG08] fueron netamente más lejos: probaron que, si A_0 genera un grupo Zariski-denso de SL_2, entonces

$$\{\Gamma(\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}), A_0 \bmod p)\}_{p > C,\ p \text{ primo}}$$

Nos concentraremos en dar una prueba del Teorema 1.3.1. Al final, esbozaremos el procedimiento de Bourgain y Gamburd, basado en parte sobre dicho teorema.

Queda aún mucho por hacer; por ejemplo, no sabemos si la familia de todos los grafos

$$\{\Gamma(\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}), A)\}_{p \text{ primo},\ A \text{ genera } \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})}$$

es una familia de expansores. Por otra parte, si bien hay generalizaciones del teorema 1.3.1 a otros grupos lineares ([Hel11], [GH11], y, de manera más general, [BGT11] y [PS]), aún no tenemos una prueba de la conjetura de Babai para los grupos alternantes A_n; la mejor cota conocida para el diámetro de A_n con respecto a un conjunto arbitrario de generadores es la cota dada en [HS14], la cual no es tan buena como $\ll (\log |G|)^{O(1)}$.

Capítulo 2

Herramientas elementales

2.1 Productos triples

La combinatoria aditiva, al estudiar el crecimiento, estudia los conjuntos que crecen lentamente. En los grupos abelianos, sus resultados son a menudo enunciados de tal manera que clasifican los conjuntos A tales que $|A^2|$ no es mucho más grande que $|A|$; en los grupos no-abelianos, generalmente se clasifica los conjuntos A tales que $|A^3|$ no es mucho más grande que $|A|$. Por qué?

En un grupo abeliano, si $|A^2| < K|A|$, entonces $|A^k| < K^{O(k)}|A|$ – i.e., si un conjunto no crece después de ser multiplicado por si mismo una vez, no crecera después de ser multiplicado por sí mismo muchas veces. Éste es un resultado de Plünnecke [Plü70] y Ruzsa [Ruz89]; Petridis [Pet12] dio recientemente una prueba particularmente elegante.

En un grupo no abeliano, puede haber conjuntos A que rompen esta regla.

Ejercicio 2.1.1. *Sea G un grupo. Sean $H < G$, $g \in G \setminus H$ y $A = H \cup \{g\}$. Entonces $|A^2| < 3|A|$, pero $A^3 \supset HgH$, y HgH puede ser mucho más grande que A. Dé un ejemplo con $G = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$.*

Empero, las ideas de Ruzsa sí se aplican al caso no abeliano, como fue indicado en [Hel08] y [Tao08]; en verdad, no hay que cambiar nada en [RT85], pues nunca utiliza la condición que G sea abeliano. Lo que obtendremos es que basta con que $|A^3|$ (en vez de $|A^2|$) no sea mucho más grande que $|A|$ para que $|A^k|$ crezca lentamente. Veamos como se hacen las cosas.

Lema 2.1.1 (Desigualdad triangular de Ruzsa)**.** *Sean A, B y C subconjuntos finitos*

de un grupo G. Entonces

$$|AC^{-1}||B| \leq |AB^{-1}||BC^{-1}|. \tag{2.1}$$

Demostración. Contruiremos una inyección $\iota : AC^{-1} \times B \hookrightarrow AB^{-1} \times BC^{-1}$. Para cada $d \in AC^{-1}$, escojamos $(f_1(d), f_2(d)) = (a, c) \in A \times C$ tal que $d = ac^{-1}$. Definamos $\iota(d, b) = (f_1(d)b^{-1}, b(f_2(d))^{-1})$. Podemos recuperar $d = f_1(d)(f_2(d))^{-1}$ de $\iota(d, b)$; por lo tanto, podemos recuperar $(f_1, f_2)(d) = (a, c)$, y así también b. Por lo tanto, ι es una inyección. □

Ejercicio 2.1.2. *Sea G un grupo. Pruebe que*

$$\frac{|(A \cup A^{-1} \cup \{e\})^3|}{|A|} \leq \left(3\frac{|A^3|}{|A|}\right)^3 \tag{2.2}$$

para todo conjunto finito A de G. Muestre también que, si $A = A^{-1}$ (i.e., si $g^{-1} \in A$ para todo $g \in A$), entonces

$$\frac{|A^k|}{|A|} \leq \left(\frac{|A^3|}{|A|}\right)^{k-2}. \tag{2.3}$$

para todo $k \geq 3$. Concluya que

$$\frac{|A^k|}{|A|} \leq 3^{k-2}\left(\frac{|A^3|}{|A|}\right)^{3(k-2)}$$

para todo $A \subset G$ y todo $k \geq 3$.

Esto quiere decir que, de ahora en adelante, si obtenemos que $|A^k|$ no es mucho más grande que $|A|$, podemos concluir que $|A^3|$ no es mucho más grande que $|A|$. Por cierto, gracias a (2.2), podremos suponer en varios contextos que $e \in A$ y $A = A^{-1}$ sin pérdida de generalidad.

2.1.1 El teorema de órbita-estabilizador para los conjuntos

Una de las ideas recurrentes en la investigación del crecimiento en los grupos es la siguiente: muchos enunciados acerca de los subgrupos – así como sus métodos de prueba – pueden generalizarse a los subconjuntos. Si el método de prueba es constructivo, cuantitativo o probabilístico, esto es un indicio que la prueba podría generalizarse de tal manera.

El *teorema de órbita-estabilizador* es un buen ejemplo, tanto por su simplicidad (realmente debería llamarse "lema") como por subyacer a un número sorpredente de resultados sobre el crecimiento.

Primero, un poco de lenguaje. Una *acción* $G \curvearrowright X$ es un homomorfismo de un grupo G al grupo de automorfismos de un objeto X. Estudiaremos el caso en el que X es simplemente un conjunto; su "grupo de automorfismos" es simplemente el grupo de biyecciones de X a X (con la composición como operación de grupo.) Para $A \subset G$ y $x \in X$, la *órbita* Ax ("órbita de x bajo la acción de A") es el conjunto $Ax = \{g \cdot x : g \in A\}$. El *estabilizador* $\mathrm{Estab}(x) \subset G$ está dado por $\mathrm{Estab}(x) = \{g \in G : g \cdot x = x\}$.

El enunciado que daremos es como en [HS14, §3.1].

Lema 2.1.2 (Teorema de órbita-estabilizador para conjuntos)**.** *Sea G un grupo actuando sobre un conjunto X. Sea $x \in X$, y sea $A \subseteq G$ no vacío. Entonces*

$$|(A^{-1}A) \cap \mathrm{Estab}(x)| \geq \frac{|A|}{|Ax|} \tag{2.4}$$

y, para $B \subseteq G$,

$$|BA| \geq |A \cap \mathrm{Estab}(x)||Bx|. \tag{2.5}$$

El teorema de órbita-estabilizador usual, que se enseña usualmente en un primer curso de teoría de grupos dice que, para H un subgrupo de G,

$$|H \cap \mathrm{Estab}(x)| = \frac{|H|}{|Hx|}.$$

Éste es un caso especial del lema que estamos por probar – el caso $A = B = H$.

Ejercicio 2.1.3. *Pruebe el Lema 2.1.2. Sugerencia: para (2.4), use el principio de los palomares.*

El grupo de G tiene la acción evidente "por la izquierda" sobre sí mismo: $g \in G$ actúa sobre los elementos $h \in H$ por multiplicación por la izquierda, i.e.,

$$g \mapsto (h \mapsto g \cdot h).$$

Está tambien, claro está, la acción por la derecha

$$g \mapsto (h \mapsto h \cdot g^{-1}).$$

(Por qué es que $g \mapsto (h \mapsto hg)$ no es una acción?) Ninguna de estas dos acciones son interesantes cuando se trata de aplicar directamente el Lema 2.1.2, pues los estabilizadores son triviales. Empero, tenemos también la acción *por conjugación*

$$g \mapsto (h \mapsto ghg^{-1}).$$

El estabilizador de un punto $h \in G$ no es sino su *centralizador* C(h), definido en (1.2); la órbita de un punto $h \in G$ bajo la acción de todo el grupo G es la *clase de conjugación*

$$\mathrm{Cl}(h) = \{ghg^{-1} : g \in G\}.$$

Así, tenemos el siguiente resultado, crucial en lo que sigue. Su importancia consiste en hacer que las cotas superiores (como las que derivaremos más tarde) sobre intersecciones con $\mathrm{Cl}(g)$ impliquen cotas inferiores sobre intersecciones con $C(g)$. La importancia de esto último es que siempre es útil saber que disponemos de muchos elementos dentro de un *variedad* (tal como un toro).

Lema 2.1.3. *Sea $A \subset G$ un conjunto no vacío tal que*[1] $A = A^{-1}$. *Entonces, para todo $g \in A^l$, $l \geq 1$,*

$$|A^2 \cap C(g)| \geq \frac{|A|}{|A^{l+2} \cap \mathrm{Cl}(g)|}.$$

Demostración. Sea $G \curvearrowright G$ la acción de G sobre sí mismo por conjugación. Aplique (2.4) con $x = g$; la órbita de g bajo la acción de A es un subconjunto de $A^{l+2} \cap \mathrm{Cl}(g)$. □

Es instructivo ver otras consecuencias de (2.4). La siguiente nos muestra, por así decirlo, que si obtenemos que la intersección de A con un subgrupo H de G crezca, entonces hemos mostrado que A mismo crece.

Ejercicio 2.1.4. *Sea G un grupo y H un subgrupo de G. Sea $A \subset G$ un conjunto no vacío con $A = A^{-1}$. Pruebe que, para todo $k > 0$,*

$$|A^{k+1}| \geq \frac{|A^k \cap H|}{|A^2 \cap H|}|A|.$$

(Sugerencia: considere la acción $G \curvearrowright G/H$ por multiplicación por la izquierda, es decir, $g \mapsto (aH \mapsto gaH)$.)

[1] Gracias a (2.2), podemos trabajar, en la practica, con conjuntos A tales que $A = A^{-1}$; esto simplifica más bien nuestra notación.

Capítulo 3

Intersecciones con variedades

3.1 Geometría algebraica extremadamente básica

3.1.1 Variedades

Una *variedad* (algebraica y afín) en un espacio vectorial de n dimensiones sobre un cuerpo K consiste en todos los puntos $(x_1, x_2, \ldots, x_n) \in \overline{K}^n$ que satisfacen un sistema de ecuaciones

$$P_i(x_1, \ldots, x_n) = 0, \quad 1 \leq i \leq k, \tag{3.1}$$

donde P_i son polinomios con coeficientes en K.

(Hay distintas maneras alternativas de formalizar el mismo concepto. Podríamos definir formalmente la variedad no exactamente como el sistema de ecuaciones en sí, sino como el conjunto de todas las ecuaciones polinomiales implicadas por el sistema en (3.2). También hay definiciones de apariencia mucho más abstractas, basada en la teoría de *esquemas* (Grothendieck), pero no necesitaremos entrar allí.)

Se dice generalmente que los puntos $(x_1, \ldots, x_k)$ que satisfacen (3.2) *yacen* sobre la variedad, así como hablamos de puntos que yacen sobre una curva o superficie algebraica; claro está, las curvas y las superficies son casos especiales de variedades. Dada una variedad V definida sobre K y un cuerpo L tal que $K \subset L \subset \overline{K}$, escribimos $V(L)$ por el conjunto de todos los puntos $(x_1, x_2, \ldots, x_n) \in L^n$ que yacen sobre V.

El caso trivial es el de la variedad $\mathbb{A}^n$ (*espacio afín*) definida por el sistema vacío de ecuaciones. Claramente, $\mathbb{A}^n(L) = L^n$.

Dadas dos variedades V_1, V_2,tanto $V_1 \cap V_2$ como $V_1 \cup V_2$ son variedades: la variedad $V_1 \cap V_2$ está dada por la unión de las ecuaciones que definen V_1 y aquellas que definen

V_2, mientras que, si V_1 está definida por (3.2) y V_2 está definida por

$$Q_j(x_1, \dots, x_n) = 0, \quad 1 \le j \le k', \tag{3.2}$$

donde Q_i son polinomios con coeficientes en K, entonces la variedad $V_1 \cup V_2$ está dada por las ecuaciones

$$(P_i \cdot Q_j)(x_1, \dots, x_n) = 0, \quad 1 \le i \le k, \quad 1 \le i' \le k'.$$

Consideremos ahora los grupos lineares, como $\mathrm{SL}_2(K)$. Está claro que $\mathrm{SL}_2(K)$ está contenido en

$$M_2(\overline{K}) = \left\{ \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} : x_1, x_2, x_3, x_4 \in \overline{K} \right\},$$

el cual es un espacio vectorial (de dimensión 4) sobre $\overline{K}$. Por lo tanto, tiene sentido hablar de variedades V en M_2. Por ejemplo, tenemos la variedad V de elementos que tienen una traza dada:

$$\mathrm{tr} \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} = C, \ \text{ i.e., } \ x_1 + x_4 - C = 0. \tag{3.3}$$

Nuestro grupo SL_2 es también una variedad, dada por la ecuación $x_1x_4 - x_2x_3 = 1$. Es así un ejemplo de un *grupo algebraico*. Estrictamente hablando, son los puntos $\mathrm{SL}_2(K)$ (o $\mathrm{SL}_2(L)$) del grupo algebraico SL_2 los que forman un grupo en el sentido usual del término. (Claro está, la operación de grupo $\cdot : \mathrm{SL}_2 \times \mathrm{SL}_2 \to \mathrm{SL}_2$ está bien definida como un *morfismo de variedades afines* – una aplicación de una variedad a otra dado por polinomios.)

Es fácil ver que un toro máximo $T = C(g)$ también es un grupo algebraico, puesto que la ecuación

$$hg = gh$$

es un sistema de ecuaciones polinomiales (lineares, en verdad) sobre los coeficientes de $h \in \mathrm{SL}_2$. Así, T es un subgrupo algebraico de G.

3.1.2 Dimensión, grado, intersecciones

Dada una variedad V, una *subvariedad* W es una variedad contenida en él. Una variedad V se dice irreducible si no es la unión de dos subvariedades no vacías $W, W' \subsetneq V$. Por ejemplo, SL_2 es *irreducible*; ésto es básicamente una consecuencia del hecho que el polinomio $x_1x_4 - x_2x_3 - 1$ es irreducible.

Podemos definir la *dimensión* de un variedad irreducible V como el entero d máximo tal que haya una cadena de variedades irreducibles no vacías

$$V_0 \subsetneq V_1 \subsetneq V_2 \subsetneq \ldots \subsetneq V_d = V.$$

Ésto coincide con el concepto intuitivo de *dimensión*: un plano contiene una línea, que contiene a un punto, y así un plano es de dimensión por lo menos 2; en verdad, es de dimensión exactamente 2.

Hecho. La dimensión de $\mathbb{A}^n$ es n.

En particular, la dimensión de una variedad en $\mathbb{A}^n$ es siempre finita ($\leq n$).

Ejercicio 3.1.1. *Probemos que la intersección $\cap_{i\in I} V_i$ de una colección finita o infinita de variedades $V_i \in \mathbb{A}^n$, $i \in I$, es una variedad.*

Para una colección finita, ésto es evidente. Por ende, para el caso infinito, bastará si mostramos que hay un $S \subset I$ finito tal que $\cap_{i\in I} V_i = \cap_{i\in S} V_i$. Muestre que esto se reduce a mostrar que una cadena de variedades

$$\mathbb{A}^n \supsetneq W_1 \supsetneq W_2 \supsetneq W_3 \supsetneq \ldots$$

debe ser finita. (Esta propiedad se llama *propiedad Noetheriana.*)

Reduzca esto a su vez al caso de W_1 irreducible. Concluya por inducción en la dimension de W_1.

Ejercicio 3.1.2. *(a) Sea V una variedad. Pruebe que se puede expresar V como una unión finita de variedades irreducibles $W_1, W_2, \ldots, W_k$. (Pista: use la propiedad Noetheriana.)*

(b) Sea V irreducible. Muestre que, si V es una unión finita de variedades

$$V_1, V_2, \ldots, V_k,$$

entonces existe un $1 \leq i \leq k$ tal que $V_i = V$.

(c) Sea V una variedad. Muestre que, si imponemos la condición que $W_i \not\subset W_j$ para $i \neq j$, la decomposición $V = W_1 \cup W_2 \cup \ldots \cup W_k$ en variedades irreducibles W_i es única (excepto que, claro, los W_i pueden permutarse). Las variedades W_i se llaman componentes irreducibles *de V.*

Si una variedad es una unión de variedades irreducibles todas de dimensión d, decimos que es "de dimensión pura", y podemos decir que es de dimensión d.

Dadas dos variedades irreducibles $W \subset V$, la *codimensión* $\mathrm{codim}(W)$ de W en V es simplemente $\dim(V) - \dim(W)$. Es fácil ver que, para V irreducible, o bien

$W = V$, o bien $\mathrm{codim}(W) > 0$. Si $\mathrm{codim}(W) > 0$ (o si W es una unión de variedades irreducibles de codimensión positiva), podemos pensar en los elementos de $W(\overline{K})$ como *especiales*, y en los elementos de $V(\overline{K})$ que no están en $W(\overline{K})$ como *genéricos*.

Es posible (y muy recomendable) considerar variedades más generales que las variedades afines. Por ejemplo, podemos considerar las *variedades proyectivas*, definidas por sistemas de ecuaciones polinomiales homogéneas en $n+1$. Los puntos en un variedad proyectiva viven en el *espacio proyectivo* $\mathbb{P}^n$. Los puntos del espacio proyectivo sobre un campo L son elementos de L^{n+1} (excepto $(0, 0, \dots, 0)$), donde se identifica dos elementos $x, x' \in L^{n+1}$ si x es un múltiplo escalar de x', i.e., si $x = \lambda x'$ para algún $\lambda \in L$. En otras palabras,

$$\mathbb{P}^n(L) = (L^{n+1} \setminus (0, 0, \dots, 0))\backslash \sim, \quad \text{donde } x \sim x' \text{ si } \exists \lambda \in L \text{ t.q. } x = \lambda x'.$$

La opción de trabajar con variedades proyectivas nos da mucha libertad: en particular, es posible mostrar que podemos hablar de la variedad proyectiva de todas las líneas (o todos los planos) en el espacio n-dimensional (proyectivo). El ejemplo más simple es la variedad de todas las líneas en el plano: como una línea en el plano proyectivo ($n = 2$) está dada por una ecuación linear homogénea

$$c_0 x_0 + c_1 x_1 + c_2 x_2 = 0,$$

y como dos tales ecuaciones dan la misma línea si sus triples (c_1, c_2, c_3) son múltiples el uno del otro, tenemos que las líneas en el plano proyectivo están en correspondencia uno-a-uno con $\mathbb{P}^2$ mismo. En $\mathbb{P}^n$, como en $\mathbb{A}^n$, podemos hablar de subvariedades, codimensión, elementos genéricos. Podemos hacer una inmersíon de $\mathbb{A}^n$ en $\mathbb{P}^n$:

$$(x_1, x_2, \dots, x_n) \mapsto (1, x_1, x_2, \dots, x_n).$$

El complemento es la subvariedad de $\mathbb{P}^n$ dada por $x_0 = 0$; para $n = 2$, se le llama *recta en el infinito*.

Contemplemos ahora una curva irreducible C en el plano, es decir, una subvariedad de $\mathbb{A}^2$ de dimensión 1. (En verdad, no es necesaria la irreducibilidad; la supondremos realmente sólo al trabajar con análogos en dimensiones superiores.) Consideremos también una línea ℓ en $\mathbb{A}^2$. Podría ser que ℓ fuera tangente a C, pero no es difícil demostrar que tal es el caso sólo cuando ℓ yace en una subvariedad de $\mathbb{P}^2$ (la *curva dual a* C). En otras palabras, una línea genérica (se dice también: *en posición general*) no es tangente a C. El número de puntos de intersección en $\mathbb{P}^2(\overline{K})$ de la curva C con una línea genérica ℓ resulta ser independiente de ℓ; llamamos a ese número el *grado* de C.

Resulta ser que el grado de una curva en el plano dada por una ecuación

$$P(x_1, x_2) = 0$$

(o por una ecuación $P(x_0, x_1, x_2) = 0$, P homogéneo) es simplemente el grado de P. La ventaja de la definición que dimos del grado de una curva es que es más conceptual y se generaliza de manera natural. En dimensiones superiores, la misma variedad puede ser definida por distintos sistemas de ecuaciones de grados distintos; deseamos una definición de *grado* que dependa sólo de la variedad, y no del sistema que la define.

Si V es una variedad de dimensión 2 en $\mathbb{A}^3$, definimos su grado como su número de intersecciones con una recta genérica; si V es de dimensión 1 en $\mathbb{A}^3$, definimos su grado como su número de intersecciones con un *plano* genérico. Así como hablamos de líneas y planos, podemos definir, en general, una *variedad linear* mediante ecuaciones lineares. Para V una variedad irreducible en $\mathbb{A}^n$ de dimensión d, definimos el *grado* $\deg(V)$ de V como el número de intersecciones de V con una variedad genérica de codimensión d en $\mathbb{A}^n$. La misma definición es válida cuando V es no necesariamente irreducible pero de dimensión pura e igual a d.

Si bien este grado, como decíamos, no tiene porque corresponder al grado de ninguna de las ecuaciones en un sistema de ecuaciones que defina a V, puede ser acotado por una constante que depende sólo de los grados de tales ecuaciones y su número. Ese es un caso especial de lo que estamos por discutir.

El *teorema de Bézout*, en el plano, nos dice que, para dos curvas irreducibles distintas C_1, C_2 en $\mathbb{A}^2$, el número de puntos de la intersección $(C_1 \cap C_2)(\overline{K})$ es a lo más $d_1 d_2$. (En verdad, si consideramos C_1 y C_2 genéricos, o trabajamos en $\mathbb{P}^2$ y contamos "multiplicidades", el número de puntos de intersección es *exactamente* $d_1 d_2$.)

En general, si V_1 y V_2 son variedades irreducibles, y escribimos $V_1 \cap V_2$ como una unión de variedades irreducibles $W_1, W_2, \dots, W_k$, con $W_i \not\subset W_j$ para $i \neq j$, una generalización del teorema de Bézout nos dice que

$$\sum_{i=1}^{k} \deg(W_k) \leq \deg(V_1) \deg(V_2). \tag{3.4}$$

(Véase, por ejemplo, [DS98, p.251], donde se menciona a Fulton y MacPherson en conexión a (3.4) y enunciados más generales.) Toda variedad irreducible de dimensión 0 consiste en un único punto; por ello (3.4) implica el teorema de Bézout habitual.

3.2 Escape de subvariedades

Sea G un grupo que actua por transformaciones lineares sobre el espacio n-dimensional K^n, K un cuerpo. (En otras palabras, se nos es dado un homomorfismo $\phi : G \to$

$\mathrm{GL}_n(K)$ de G al grupo de matrices invertibles $\mathrm{GL}_n(K)$.) Sea W una variedad de codimensión positiva en $\mathbb{A}^n$. Estábamos llamando a los elementos de $W(\overline{K})$ *especiales*, y a los otros elementos de $\mathbb{A}^n(\overline{K})$ *genéricos*.

Sea A un conjunto de generadores de G y x un punto de W. Muy bien podría ser que la órbita $A \cdot x$ esté contenida por entero en W. Empero, como veremos ahora, si Gx no está contenida en W, entonces siempre es posible *escapar* de W en un número acotado de pasos: no sólo que habrá (por definición) algún producto g de un número finito de elementos de A y A^{-1} tal que $g \cdot x$ está fuera de W, sino que habrá un producto (a decir verdad, muchos productos) $g \in (A \cup A^{-1})^k$, k *acotado*, tal que $g \cdot x$ está fuera de W. En otras palabras, si escapamos por lo menos una vez, eventualmente, de W, escapamos de muchas maneras de W, después de un número acotado k de pasos.

La prueba[1] procede por inducción en la dimensión, controlando el grado.

Proposición 3.2.1. *Sean dados:*

- G, *un grupo actuando por transformaciones lineares sobre* K^n, K *un cuerpo;*
- $W \subsetneq \mathbb{A}^n$, *una variedad,*
- *un conjunto de generadores* $A \subset G$*;*
- *un elemento* $x \in \mathbb{A}^n(K)$ *tal que* $G \cdot x$ *no está contenido en* W.

Entonces hay constantes k, c *que dependen sólo del número, dimensión y grado de los componentes irreducibles de* V, *tales que hay por lo menos* $\max(1, c|A|)$ *elementos* $g \in (A \cup A^{-1} \cup \{e\})^k$ *tales que* $gx \notin W(K)$.

Para aclarar el proceso de inducción, daremos primero la prueba en un caso particular. Una variedad *linear* es simplemente una línea, un espacio, etc.; en otras palabras, es una variedad definida por ecuaciones lineares.

Prueba para W linear e irreducible. Sea W linear e irreducible. Podemos asumir sin pérdida de generalidad que $A = A^{-1}$ y $e \in A$.

Procederemos por inducción en la dimensión de W. Si $\dim(W) = 0$, entonces W consiste en un sólo punto x_0, y el enunciado que queremos probar es cierto: existe un $g \in A$ tal que $gx \neq x_0$ (por qué?); si hay menos de $|A|/2$ tales elementos, escogemos un $g_0 \in A$ tal que $g_0 x \neq x$ (por qué existe?), y entonces, para cada uno de los más de $|A|/2$ elementos $g \in A$ tales que $gx = x_0$, tenemos que $gg_0 x \neq x_0$.

[1] El enunciado de la proposición es cómo en [Hel11], basado en [EMO05], pero la idea es probablemente más antigua.

Asumamos, entonces, que $\dim(W) > 0$, y que el enunciado ha sido probado para todas las variedades lineares irreducibles W' con $\dim(W') < \dim(W)$. Si $gW = W$ para todo $g \in A$, entonces ya sea (a) $gx \notin W(K)$ para todo $g \in A$, y el enunciado es inmediato, o (b) $gx \in W(K)$ para todo $g \in G$ (puesto que G está generado por A), lo cual está en contradicción con nuestras suposiciones. Podemos asumir, entonces, que $gW \neq W$ para algun $g \in A$.

Entonces $W' = gW \cap W$ es una variedad linear irreducible de dimensión $\dim(W') < \dim(W)$. Por lo tanto, por la hipótesis inductiva, hay $\geq \max(1, c'|A|)$ elementos g' de $A^{k'}$ (donde c' y k' dependen sólo de $\dim(W)$) tales que $g'x$ no yace en la variedad $W' = gW \cap W$. Entonces, para cada tal g', ya sea $g^{-1}g'x$ o $g'x$ no yace en W. Así, hemos probado la proposicion con $c = c'/2$, $k = k' + 1$. □

Ejercicio 3.2.1. *Generalize la prueba que acabamos de dar de tal manera que dé Prop. 3.2.1 para W arbitrario.* Sugerencia: *como un primer paso, generalice la prueba de tal manera que funcione para toda unión W de variedades lineares irreducibles. (Ésto ya exigirá adaptar el proceso de inducción de tal manera que se controle de alguna manera el número de componentes en cada paso. Claro está, la intersección de dos uniones W de d variedades lineares irreducibles tiene a lo más d^2 componentes.) Luego muestre que la prueba es válida para toda union W de variedades irreducibles, no necesariamente lineares, utilizando la generalización (3.4) del teorema de Bézout.*

3.3 Estimaciones dimensionales

Dado un conjunto de generadores $A \subset \mathrm{SL}_2(K)$ (o $A \subset \mathrm{SL}_n(K)$, o lo que se desee) y una subvariedad V de codimensión positiva en SL_2, sabemos que una proporción positiva de los elementos de A^k, k acotado, yacen fuera de V: éste es un caso especial de la Proposición 3.2.1 (con x igual a la identidad e).

Aunque esto desde ya implica una cota superior para el número de elementos de A^k en $V(K)$, podemos dar una cota mucho mejor. Los estimados de este tipo pueden trazarse en parte a [LP11] (caso de A un subgrupo, V general) y en parte a [Hel08] y [Hel11] (A un conjunto en general, pero V especial). Tales cotas tienen en general la forma

$$|A \cap V(K)| \ll |(A \cup A^{-1} \cup \{e\})^k|^{\frac{\dim V}{\dim G}}. \tag{3.5}$$

Se lograron cotas completamente generales del tipo (3.5) en [BGT11] y [PS] (A y V arbitrarios, G un grupo linear algebraico simple, como en [LP11]).

Como primero paso hacia la estrategia general, veamos un caso particular de manera muy concreta (aunque no lo usemos al final). La prueba es básicamente la misma que en [Hel08, §4].

Lema 3.3.1. *Sea $G = \mathrm{SL}_2$, K un cuerpo, y T un toro máximo. Sea $A \subset G(K)$ un conjunto de generadores de $G(K)$. Entonces*

$$|A \cap T(K)| \ll |(A \cup A^{-1} \cup \{e\})^k|^{1/3} \tag{3.6}$$

donde k y la constante implícita son constantes absolutas.

Demostración. Podemos suponer sin pérdida de generalidad que $|K|$ es mayor que una constante, pues, de lo contrario, la conclusión es trivial. También podemos suponer sin pérdida de generalidad que $A = A^{-1}$, $e \in A$, y que $|A|$ es mayor que una constante, reemplazando A por $(A \cup A^{-1} \cup \{e\})^c$, c constante, de ser necesario. Podemos también escribir los elementos de T como matrices diagonales, conjugando por un elemento de $\mathrm{SL}_2(\overline{K})$.

Sea

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{3.7}$$

un elemento cualquiera de SL_2 con $abcd \neq 0$. Consideremos la aplicación $\phi : T(K) \times T(K) \times T(K) \to G(K)$ dada por

$$\phi(x, y, z) = x \cdot gyg^{-1} \cdot z.$$

Queremos mostrar que esta aplicación es en algún sentido cercana a ser inyectiva. (La razón de tal estrategia? Si la aplicación fuera inyectiva, y tuvieramos $g \in A^\ell$, ℓ una constante, entonces tendríamos

$$|A \cap T(K)|^3 = |\phi(A \cap T(K), A \cap T(K), A \cap T(K))| \leq |AA^\ell AA^{-\ell} A| = |A^{2\ell+3}|,$$

lo cual implicaría inmediatamente el resultado que queremos. Simplemente estamos usando el hecho que el tamaño de la imagen $\phi(D)$ de una inyección ϕ tiene el mismo número de elementos que su dominio D.)

Multiplicando matrices, vemos que, para

$$x = \begin{pmatrix} r & 0 \\ 0 & r^{-1} \end{pmatrix}, \quad y = \begin{pmatrix} s & 0 \\ 0 & s^{-1} \end{pmatrix}, \quad z = \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix},$$

$\phi((x, y, z))$ es igual a

$$\begin{pmatrix} rt(sad - s^{-1}bc) & rt^{-1}(s^{-1} - s)ab \\ r^{-1}t(s - s^{-1})cd & r^{-1}t^{-1}(s^{-1}ad - sbc) \end{pmatrix}. \tag{3.8}$$

Sea $s \in \overline{K}$ tal que $s^{-1} - s \neq 0$ y $sad - s^{-1}bc \neq 0$. Un breve cálculo muestra que entonces $\phi^{-1}(\{\phi((x, y, z))\})$ tiene a lo más 16 elementos: tenemos que

$$rt^{-1}(s^{-1} - s)ab \cdot r^{-1}t(s - s^{-1})cd = -(s - s^{-1})^2 abcd,$$

y, como $abcd \neq 0$, hay a lo más 4 valores de s dado un valor de $-(s-s^{-1})^2 abcd$ (el producto de las esquinas superior derecha e inferior izquierda de (3.8)); para cada tal valor de s, el producto y el cociente de las esquinas superior izquierda y superior derecha de (3.8) determinan r^2 y t^2, respectivamente, y obviamente hay sólo 2 valores de r y 2 valores de t para r^2 y t^2 dados.

Ahora bien, hay a lo más 4 valores de s tales que $s^{-1} - s = 0$ o $sad - s^{-1}bc = 0$. Por lo tanto, tenemos que

$$|\phi(A \cap T(K), A \cap T(K), A \cap T(K))| \geq \frac{1}{16}|A \cap T(K)|(|A \cap T(K)| - 4)|A \cap T(K)|,$$

y, como antes, $\phi(A \cap T(K), A \cap T(K), A \cap T(K)) \subset AAAA^{-1}A = A^5$. Si $|A \cap T(K)|$ es menor que 8 (o cualquier otra constante) entonces la conclusión (3.6) es trivial. Por lo tanto, concluímos que

$$|A \cap T(K)|^3 \leq 2|A \cap T(K)|(|A \cap T(K)| - 4)|A \cap T(K)| \leq 32|A^{2\ell+3}|,$$

i.e., (3.6) es cierta.

Sólo queda verificar que existe un elemento (3.7) de A^ℓ con $abcd \neq 0$. Ahora bien, $abcd = 0$ define una subvariedad W de $\mathbb{A}^4 \sim M_2$; más aún, para $|K| > 2$, existen elementos de $G(K)$ fuera de tal variedad. Por lo tanto, las condiciones de Prop. 3.2.1 se cumplen (con x igual a la identidad e). Así, obtenemos que existe $g \in A^\ell$ (ℓ una constante) tal que $g \notin W(K)$, lo cual era lo que necesitábamos. □

Hagamos abstracción de lo que acabamos de hacer, para así poder generalizar el resultado a una variedad arbitraria V en vez de T. Trataremos el caso de V de dimensión 1, por conveniencia. La estrategia de la prueba del Lema 3.3.1 consiste en construir un morfismo $\phi : V \times V \times \cdots \times V \to G$ (r copias de V, donde $r = \dim(G)$) de la forma

$$\phi(v_1, \ldots, v_r) = v_1 g_1 v_2 g_2 \cdots v_{r-1} g_{r-1} v_r, \tag{3.9}$$

donde $g_1, g_2, \ldots, g_{r_1} \in A^\ell$, de tal manera que, para $v = (v_0, v_1, \ldots, v_{\ell-1})$ genérico (es decir, fuera de una subvariedad de $V \times \cdots \times V$ de codimensión positiva), la preimagen $\phi^{-1}(\phi(v))$ tenga dimensión 0. En verdad, como acabamos de ver, es suficiente mostrar que esto es cierto para $(g_1, g_2, \ldots, g_{r-1})$ genérico; el argumento de escape (Prop. 3.2.1) se encarga del resto.

Para hacer que el argumento marche para V general (y G general), es necesario asumir algunos fundamentos. Esencialmente, tenemos la elección de ya sea trabajar sobre el álgebra de tipo Lie o introducir un poco más de geometría algebraica. La primera elección (tomada en [Hel15], siguiendo a [Hel11]) asume que el lector tiene cierta familiaridad con los grupos y álgebras de Lie, y que sabe, o está dispuesto a

creer, que la relación entre grupos y álgebras de Lie sigue la misma si trabajamos sobre un cuerpo finito en vez de $\mathbb{R}$ o $\mathbb{C}$. La segunda elección – que tomaremos aquí – requiere saber, o estar listo a aceptar, un par de hechos básicos sobre morfismos, válidos sobre cuerpos arbitrarios.

No importa gran cosa si se sigue el uno u el otro formalismo. Los fundamentos, en uno y otro caso, se sentaron sólidamente en la primera mitad del siglo XX (Zariski, Chevalley, etc.) y son relativamente accesibles. Los lectores que sientan interés en estudiar las bases del camino que seguiremos están invitados a leer [Mum99, Ch. 1] (de por sí una excelente idea) o cualquier texto similar.

Está claro que, si $\phi : \mathbb{A}^n \to \mathbb{A}^m$ es un morfismo y $V \subset \mathbb{A}^m$ es una variedad, entonces la preimagen $\phi^{-1}(V)$ es una variedad (por qué?). Algo nada evidente que utilizaremos es el hecho que, si ϕ es como dijimos y $V \subset \mathbb{A}^n$ es una variedad, entonces $\phi(V)$ es un *conjunto construíble*, lo cual quiere decir una unión finita de términos de la forma $W \setminus W'$, donde W y $W' \subset W$ son variedades. (Por ejemplo, si $V \subset \mathbb{A}^2$ es la variedad dada por $x_1 x_2 = 1$ (una hipérbola), entonces su imagen bajo el morfismo $\phi(x_1, x_2) = x_1$ es el conjunto construíble $\mathbb{A}^1 \setminus \{0\}$.) Éste es un teorema de Chevalley [Mum99, §I.8, Cor. 2]; encapsula parte del campo clásico llamado *teoría de la eliminación*. Es fácil deducir, que, en general, para V construíble, $\phi(V)$ es construíble.

Siempre podemos expresar un conjunto construíble S como una unión $\cup_i (W_i \setminus W_i')$ con $\dim(W_i') < \dim(W_i)$. (Por qué?) La *clausura de Zariski* $\overline{S}$ del conjunto construíble S es entonces $\cup_i W_i$.

El siguiente lema es [Tao15, Prop. 1.5.30], lo cual es a su vez en esencia [LP11, Lemma 4.5]. (Murmullo de un mundo paralelo: en el formalismo que no seguimos, esto corresponde al hecho, básico pero no trivial, que el álgebra de un grupo de tipo Lie simple es simple.)

Decimos que un grupo algebraico G es *casi simple* si no tiene ningún subgrupo algebraico normal H de dimensión positiva y menor que $\dim(G)$. (Por ejemplo, SL_n es casi simple para todo $n \geq 2$.)

Lema 3.3.2. *Sea $G \subset \mathrm{SL}_n$ un grupo algebraico irreducible y casi simple definido sobre un cuerpo K. Sean $V', V \subsetneq G$ subvariedades con $\dim(V') > 0$. Entonces, para todo $g \in G(\overline{K})$ fuera de una subvariedad $W \subsetneq G$, algún componente de la clausura de Zariski $\overline{V' g V}$ tiene dimensión $> \dim(V)$.*

Más aún, el número de componentes de W y sus grados están acotados por una constante que depende sólo de n y del número y grados de los componentes de V' y V.

Demostración. Podemos suponer sin pérdida de generalidad que V_1 y V_2 son irredu-

cibles, y que $e \in V(\overline{K})$.

Sea $g \in G(\overline{K})$. Supongamos que $\overline{V'gV}$ tiene dimensión $\leq \dim(V)$. Para todo $v' \in V'(\overline{K})$, $v'gV$ es una variedad de dimensión $\dim(V)$ – uno del número finito de componentes W_i de $\overline{V'gV}$ de dimensión $\dim(V)$. Para cada tal W_i, los puntos v' tales que $v'gV = W_i$ forman una variedad V_i, al ser la intersección de variedades

$$\bigcap_{v \in V(\overline{K})} W_i v^{-1} g^{-1}.$$

Así, V es la unión de un número finito de variedades V_i; como V es irreducible, esto implica que $V = V_i$ para algún V. En particular, $gV = e \cdot gV = W_i$. Por lo tanto, $V'gV = gV$.

Ahora bien, los elementos $g \in G(\overline{K})$ tales que $V'gV = gV$ son una intersección

$$\bigcap_{\substack{v \in V \\ v' \in V'}} \phi_{v',v}^{-1}(V)$$

de variedades $\phi_{v',v}^{-1}(V)$, donde $\phi_{v',v}(g) = g^{-1}v'^{-1}gv$. Por lo tanto, tales elementos constituyen una subvariedad W de G; más aún, gracias a Bézout (3.4), su número de componentes así como el grado de estos están acotados por una constante que depende sólo de n y del número y grados de los componentes de V' y V.

Falta sólo mostrar que $W \neq G$. Supongamos que $W = G$. Entonces $V'gV = gV$ para todo $g \in G(\overline{K})$. Ahora bien, el estabilizador $\{g \in G(\overline{K}) : gV = V\}$ de V no sólo es un grupo, sino que es (el conjunto de puntos de) una variedad (nuevamente: para ver esto, expréselo como una intersección de variedades). Llamemos a tal variedad $\mathrm{Estab}(V)$. Tenemos que $g^{-1}V'g \subset \mathrm{Estab}(V)$ para todo $g \in G(\overline{K})$, y por lo tanto

$$V' \subset \bigcap_{g \in G(\overline{K})} g\,\mathrm{Estab}(V)g^{-1}.$$

Esto muestra que la variedad $\cap_{g \in G(\overline{K})} g\,\mathrm{Estab}(V)g^{-1}$ es de dimensión $\geq \dim(V') > 0$. Al mismo tiempo, dicha variedad es un subgrupo algebraico normal de G, contenido en $\mathrm{Estab}(V)$. Como $\mathrm{Estab}(V) \subsetneq G$, tenemos un subgrupo algebraico normal de G, de dimensión positiva y estrictamente contenido en G. En otras palabras, G no es un grupo algebraico casi simple. Contradicción. □

Sean G, V y V' tales que satisfagan las hipótesis del Lema 3.3.2, y sea $g \in G(\overline{K})$ como en la conclusión del Lema, i.e., fuera de la subvariedad $W \subsetneq G$. Asumamos que $\dim(V) = 1$, y consideremos el morfismo $\phi : V' \times V \to \overline{V'gV}$ dado por

$$\phi(v', v) = v'gv.$$

La dimension de la imagen de un morfismo no es mayor que la dimension de su dominio (ejercicio), así que

$$\dim(\phi(V', V)) \leq \dim(V' \times V) = \dim(V') + \dim(V) = \dim(V) + 1.$$

Al mismo tiempo, por el Lema 3.3.2, $\dim(\phi(V', V)) > \dim(V)$. Por lo tanto,

$$\phi(V', V) = \dim(V) + 1 = \dim(V' \times V).$$

Si un morfismo $\phi : X \to X'$ es tal que $\overline{\phi(X)} = X'$, decimos que ϕ es *dominante*. (Por ejemplo, el morfismo ϕ que acabamos de considerar es dominante.) Aceptemos el hecho que, si ϕ es dominante y $\dim(X') = \dim(X)$, entonces hay una subvariedad $Y \subsetneq X$ tal que, para todo $x \in X(\overline{K})$ que no yazca en $Y(\overline{X})$, la variedad $\phi^{-1}(\phi(\{x\}))$ tiene dimensión 0. (Ésta es una consecuencia inmediata del [Mum99, §1.8, Thm. 3].) Más aún, el número de componentes de Y y su grado están acotados en términos del grado de ϕ y del número, dimensión y grado de los componentes de X y X'.

(Para que lo que acabamos de llamar una consecuencia inmediata de algo en otra parte se vuelva intuitivamente claro, considere el caso $K = \mathbb{R}$. Entonces Y es la subvariedad de X definida por la condición "la determinante $D\phi(x)$ de ϕ en el punto x tiene determinante 0". Hay varias maneras de ver que Y es una subvariedad $\subsetneq X$ para K arbitrario: como dijimos, es posible definir derivadas sobre cuerpos arbitrarios, o, alternativamente, proceder como en [Mum99, §1.8, Thm. 3].)

Aplicando esto a la aplicación ϕ que teníamos, obtenemos que hay una subvariedad $Y \subsetneq V' \times V$ tal que, para todo $x \in (V' \times V)(\overline{K})$ que no yace en Y, $\phi^{-1}(\phi(x))$ tiene dimensión 0.

Dado ésto, podemos probar una generalización del Lema 3.3.1. Se trata realmente de (3.5) para toda variedad de dimensión 1.

Proposición 3.3.1. *Sea K un cuerpo y $G \subset \mathrm{SL}_n$ un grupo algebraico casi simple tal que $|G(K)| \geq c|K|^{\dim(G)}$, $c > 0$. Sea $Z \subset G$ una variedad de dimensión 1. Sea $A \subset G(K)$ un conjunto de generadores de $G(K)$. Entonces*

$$|A \cap Z(K)| \ll |(A \cup A^{-1} \cup \{e\})^k|^{1/\dim(G)} \tag{3.10}$$

donde k y la constante implícita dependen solamente de n, de c y del número y grado de los componentes irreducibles de G y Z.

Obviamente, $G = \mathrm{SL}_n$ es una elección válida, pues es casi simple y $|\mathrm{SL}_n(K)| \gg |K|^{n^2-1} = |K|^{\dim(G)}$.

Ejercicio 3.3.1. *Pruebe la Proposición 3.3.1. He aquí un esbozo:*

(a) *Muestre el siguiente lema básico: si $W \subset \mathbb{A}^N$ es una variedad de dimensión d, entonces el número de puntos $(x_1, \ldots, x_N) \in \mathbb{A}^n(K)$ que yacen en W es $\ll |K|^d$, donde la constante implícita depende sólo de N y del número y grado de componentes irreducibles de W. (Sugerencia: para $d = 0$, ésto está claro. Para $d > 0$, considere la proyección $\pi : \mathbb{A}^N \to \mathbb{A}^{N-1}$ a las primeras $N - 1$ coordenadas, o más bien dicho la restricción $\pi|W$ de π a W. Reduzca al caso de dimensión $d - 1$ – la manera de hacerlo depende de si $\pi|W$ es o no es dominante.)*

(b) *Utilizando el escape de subvariedades (Prop. 3.2.1) y el Lema 3.3.2, muestre que, dadas las condiciones del Lema 3.3.2, existe un elemento $g \in (A \cup A^{-1} \cup \{e\})^\ell$, ℓ una constante (dependiendo de esto y aquello), tal que algún componente de la clausura de Zariski $\overline{V'gV}$ tiene dimensión $> \dim(V)$. Esto es rutina, pero no olvide mostrar que hay algun punto de $G(K)$ fuera de W (usando el lema básico que acaba de probar).*

(c) *Aplicando esto (y las consecuencias discutidas inmediatamente despues del Lema 3.3.2) de manera iterada, muestre que existen $g_1, \ldots, g_{r-1} \in (A \cup A^{-1} \cup \{e\})^{\ell'}$ y una subvariedad $Y \subsetneq Z \times Z \times \ldots \times Z$ ($r = \dim(G)$ times) tales que, para todo $x \in (Z \times Z \times \ldots \times Z)(\overline{K})$ que no yace en Y, $\phi^{-1}(\phi(x))$ es de dimensión 0, donde ϕ es como en (3.9).*

(d) *Usando nuevamente un argumento que distingue si una projección (esta vez de $Z \times \ldots \times Z$ (m veces) a $Z \times \ldots \times Z$ ($m - 1$ veces)) es dominante, e iterando, muestre que hay a lo más $O(|A|^{m-1})$ elementos de $(A \times Z(K)) \times \ldots \times (A \times Z(K))$ (r veces) en Y.*

(e) *Concluya que la proposición Prop. 3.3.1 es cierta.*

En general, se puede probar (3.5) para $\dim(V)$ arbitrario siguiendo argumentos muy similares, mezclados con una inducción sobre la dimensión de la variedad V en (3.5). Ilustraremos el proceso básico haciendo las cosas en detalle para $G = \mathrm{SL}_2$ y para el tipo de variedad V que realmente necesitamos.

Se trata de la variedad V_t definida por

$$\det(g) = 1, \mathrm{tr}(g) = t \tag{3.11}$$

para $t \neq \pm 2$. Tales variedades nos interesan por el hecho que, para cualquier $g \in \mathrm{SL}_2(K)$ regular semisimple (lo cual en SL_2 quiere decir: con dos valores propios distintos), la clase de conjugacion $\mathrm{Cl}(g)$ está contenida en $V_{\mathrm{tr}(g)}$.

Proposición 3.3.2. *Sea K un cuerpo; sea $A \subset \mathrm{SL}_2(K)$ un conjunto de generadores de $\mathrm{SL}_2(K)$. Sea W_t dada por (3.11). Entonces, para todo $t \in K$ aparte de ± 2,*

$$|A \cap V_t(K)| \ll |(A \cup A^{-1} \cup \{e\})^k|^{\frac{2}{3}}, \tag{3.12}$$

donde k y la constante implícita son constantes absolutas.

Claro está, $\dim(\mathrm{SL}_2) = 3$ y $\dim(V_t) = 2$, así que este es un caso particular de (3.5).

Demostración. Consideremos la aplicación $\phi : V_t(K) \times V_t(K) \to \mathrm{SL}_2(K)$ definida por

$$\phi(y_1, y_2) = y_1 y_2^{-1}.$$

Está claro que

$$\phi(A \cap V_t(K), A \cap V_t(K)) \subset A^2.$$

Así, si ϕ fuera inyectiva, tendríamos inmediatamente que $|A \cap V_t(K)|^2 \leq |A^2|$. Ahora bien, ϕ no es inyectiva. La preimagen de $\{h\}$, $h \in \mathrm{SL}_2(K)$, es

$$\phi^{-1}(\{h\}) = \{(w, hw) : \mathrm{tr}(w) = t, tr(hw) = t\}.$$

Debemos preguntarnos, entonces, cuántos elementos de A yacen en la subvariedad $Z_{t,h}$ de G definida por

$$Z_{t,h} = \{(w, hw) : \mathrm{tr}(w) = t, tr(hw) = t\}.$$

Para $g \neq \pm e$, $\dim(Z_{t,h}) = 1$ (verificar), y el número y grado de componentes de $Z_{t,h}$ esta acotado por una constante absoluta. Así, aplicando la Proposición 3.3.1, obtenemos que, para $h \neq \pm e$,

$$|A \cap Z_{t,h}(K)| \ll |A^{k'}|^{1/3},$$

donde k' y la constante implícita son absolutas.

Ahora bien, para cada $y_1 \in W_t(K)$, hay por lo menos $|W_t(K)| - 2$ elementos $y_2 \in W_t(K)$ tales que $y_1 y_2^{-1} \neq \pm e$. Concluímos que

$$|A \cap T(K)|(|A \cap T(K)| - 2) \leq |A^2| \cdot \max_{g \neq \pm e} |A \cap Z_{t,h}(K)| \ll |A^2||A^{k'}|^{1/3}.$$

Podemos asumir que $|A \cap T(K)| \geq 3$, pues de lo contrario la conclusión deseada es trivial. Obtenemos, entonces, que

$$|A \cap T(K)| \ll |A^k|^{2/3}$$

para $k = \max(2, k')$, como queríamos. □

Pasemos a la consecuencia que nos interesa.

Corolario 3.3.1. *Sea K un cuerpo y $G = \mathrm{SL}_2$. Sea A un conjunto de generadores de $G(K)$; sea $g \in A^\ell$ ($\ell \geq 1$) regular semisimple. Entonces*

$$|A^2 \cap C(g)| \gg \frac{A}{|(A \cup A^{-1} \cup \{e\})^{k\ell}|^{2/3}}, \tag{3.13}$$

donde k y la constante implícita son absolutas.

En particular, si $|A^3| \leq |A|^{1+\delta}$, entonces

$$|A^2 \cap C(g)| \gg |A|^{1/3 - O(\delta\ell)}, \tag{3.14}$$

donde las constantes implícitas son absolutas.

Demostración. La proposición 3.2.1 y el lema 2.1.3 implican (3.13) inmediatamente. La conclusión (3.13) se deduce también inmediatamente de (2.2) y (3.13). □

Veamos ahora dos problemas cuyos resultados no utilizaremos; son esenciales, empero, si se quiere trabajar en SL_n para n arbitrario. El primer problema es relativamente ambicioso, pero ya hemos visto todos los elementos esenciales para su solución. En esencia, sólo se trata de saber organizar la recursión.

Ejercicio 3.3.2. *Generalice la Proposicion 3.3.1 a Z de dimensión arbitraria.*

En general, un elemento $g \in \mathrm{SL}_n(K)$ es *regular semisimple* si tiene n valores propios distintos. Claro está, todo elemento de $C(g)$ tiene los mismos valores propios que g. Cuando $G = \mathrm{SL}_n$, como para SL_2, los elementos de $C(g)$ son los puntos $T(K)$ de un subgrupo algebraico abeliano T de G, llamado un toro máximo. Tenemos que $\dim(T) = n - 1$ y $\dim(\overline{\mathrm{Cl}(g)}) = \dim(G) - \dim(T)$.

Ejercicio 3.3.3. *Generalice 3.3.1 a $G = \mathrm{SL}_n$, para g semisimple. En vez de (3.14), la conclusión reza como sigue:*

$$|A \cap C(g)| \gg |A|^{\frac{\dim(T)}{\dim(G)} - O(\delta)}, \tag{3.15}$$

donde las constantes implícitas dependen solo de n.

Terminemos por una breve nota con un lado anecdótico. Una versión del Corolario 3.3.1 fue probada en [Hel08], donde jugó un rol central. Luego fue generalizada a SL_n en [Hel11], dando, en esencia, (3.15).

Empero, estas versiones tenian una debilidad: daban (3.14) y (3.15) para la mayoría de los $g \in A^\ell$, y no para *todo* $g \in A^\ell$. Esto hacía que el resto del argumento –

la parte que estamos por ver – fuera más complicado y difícil de generalizar que lo es hoy en día.

La moraleja es, por supuesto, que no hay que asumir que las técnicas y argumentos que a uno le son familiares son óptimos – y que para simplificar una prueba vale la pena tratar de probar resultados intermedios más fuertes.

Capítulo 4

El crecimiento en $\mathrm{SL}_2(K)$

4.1 El caso de los subgrupos grandes

Veamos primero que pasa con $A \cdot A \cdot A$ cuando $A \subset \mathrm{SL}_2(\mathbb{F}_q)$ es grande con respecto a $G = \mathrm{SL}_2(\mathbb{F}_q)$. En verdad no es difícil mostrar que, si $|A| \geq |G|^{1-\delta}$, $\delta > 0$ suficientemente pequeño, entonces $(A \cup A^{-1} \cup \{e\})^k = G$, donde k es una constante absoluta. Probaremos algo más fuerte: $A^3 = G$. La prueba se debe a Nikolov y Pyber [NP11]; está basada sobre una idea clásica, desarrollada en este contexto por Gowers [Gow08]. Nos dará la oportunidad de revisitar el tema de los valores propios de la matriz de adyacencia $\mathscr{A}$ de $\Gamma(G, A)$. (Los comenzamos a discutir en §1.2.)

Primero, recordemos que una *representación compleja* de un grupo G es un homomorphismo $\phi : G \to \mathrm{GL}_d(\mathbb{C})$; decimos, naturalmente, que $d \geq 1$ es la *dimensión* de la representación. Una representación ϕ es *trivial* si $\phi(g) = e$ para todo $g \in G$.

El siguiente resultado se debe a Frobenius (1896), por lo menos para q primo. Se puede mostrar simplemente examinando una tabla de caracteres, como en [Sha99] (que da también análogos de esta proposición para todos los así llamados *grupos de Chevalley*).

Proposición 4.1.1. *Sea $G = \mathrm{SL}_2(\mathbb{F}_q)$, $q = p^\alpha$. Entonces toda representación compleja no trivial de G tiene dimensión $\geq (q-1)/2$.*

Ahora bien, para cada valor propio ν de $\mathscr{A}$, podemos considerar su *espacio propio* – el espacio vectorial que consiste en todas las funciones propias $f : G \to \mathbb{C}$ con valor propio ν. Como puede verse de la definición de $\mathscr{A}$ (inmediatamente después de (1.5)), tal espacio es invariante bajo la acción de G por multiplicación por la derecha. En otras palabras, es una representación de G - y puede ser trivial sólo si se trata

del espacio (uni-dimensional) que consiste de las funciones constantes, i.e., el espacio propio que corresponde al valor propio $\nu_0 = 1$. Por lo tanto, todo los otros valores propios tienen multiplicidad $\geq (q-1)/2$. Asumamos, como es nuestra costumbre, que $A = A^{-1}$, lo cual implica que todos los valores propios son reales:

$$\dots \leq \nu_2 \leq \nu_1 \leq \nu_0 = 1.$$

La idea es ahora es obtener un hueco espectral, i.e., una cota superior para ν_j, $j > 0$. Es muy común usar el hecho que la traza de una potencia $\mathscr{A}^r$ de una matriz de adyacencia puede expresarse de dos maneras: como el número (normalizado por el factor $1/|A|^r$, en nuestro caso) de ciclos de longitud r en el grafo $\Gamma(G, A)$, por una parte, y como la suma de potencias r-ésimas de los valores propios de $\mathscr{A}$, por otra. En nuestro caso, para $r = 2$, esto nos da

$$\frac{|G||A|}{|A|^2} = \sum_j \nu_j^2 \geq \frac{q-1}{2}\nu_j^2, \tag{4.1}$$

para cualquier $j \geq 1$, y, por lo tanto,

$$|\nu_j| \leq \sqrt{\frac{|G|/|A|}{(q-1)/2}}.$$

Ésta es una cota superior muy pequeña para $|A|$ grande. Esto quiere decir que unas cuantas aplicaciones de $\mathscr{A}$ bastan para hacer que una función se "uniformice", pues cualquier componente ortogonal al espacio propio de funciones constantes es multiplicado por $(1 - \lambda_j)$ en cada paso. La prueba siguiente simplemente aplica esta observación.

Proposición 4.1.2 ([NP11]). *Sea $G = \mathrm{SL}_2(\mathbb{F}_q)$, $q = p^\alpha$. Sea $A \subset G$, $A = A^{-1}$. Asumamos $|A| \geq 2|G|^{8/9}$. Entonces*

$$A^3 = G.$$

La suposicion $A = A^{-1}$ es en verdad innecesaria, gracias al trabajo adicional puesto en [Gow08] para el caso no simétrico.

Demostración. Supongamos $g \in G$ such that $g \notin A^3$. Entonces el producto escalar

$$\langle \mathscr{A} 1_A, 1_{gA} \rangle = \sum_{x \in G} (\mathscr{A} 1_A)(x) \cdot 1_{gA}(x)$$

es igual a 0. Podemos asumir que los vectores propios v_j satisfacen $\langle v_j, v_j\rangle = 1$. Entonces

$$\langle \mathscr{A} 1_A, 1_{gA}\rangle = \nu_0 \langle 1_A, v_0\rangle \langle v_0, 1_{gA^{-1}}\rangle + \sum_{j\geq 1} \nu_j \langle 1_A, v_j\rangle \langle v_j, 1_{gA^{-1}}\rangle$$

(por qué?). Por Cauchy-Schwarz, ésto es por lo menos

$$\frac{|A|^2}{|G|} - (\sqrt{\frac{2|G|/|A|}{q-1}} \sqrt{\sum_{j\geq 1} |\langle 1_A, v_j\rangle|^2} \sqrt{\sum_{j\geq 1} |\langle v_j, 1_{gA^{-1}}\rangle|^2}$$
$$\geq \frac{|A|^2}{|G|} - \sqrt{\frac{2|G|/|A|}{q-1}} |1_A|_2 |1_{gA^{-1}}|_2 = \frac{|A|^2}{|G|} - \sqrt{\frac{2|G||A|}{q-1}}.$$

Como $|G| = (q^2-q)q$, tenemos que $|A| \geq 2|G|^{8/9}$ implica que

$$\frac{|A|^2}{|G|} > \sqrt{\frac{2|G||A|}{q-1}},$$

y por lo tanto $\langle \mathscr{A} 1_A, 1_{gA^{-1}}\rangle$ es mayor que 0. Contradicción. □

4.2 El crecimiento en $\mathrm{SL}_2(K)$, K arbitrario

Probemos finalmente el teorema 1.3.1. En esta parte nos acercaremos más a tratamientos nuevos (en particular, [PS]) que al tratamiento original en [Hel08]; estos tratamientos nuevos se generalizan más fácilmente. Si bien sólo deseamos presentar una prueba para SL_2, notaremos el punto o dos en la prueba dónde hay que trabajar un poco a la hora de generalizarla para SL_n.

La primera prueba de este teorema en la literatura utilizaba el *teorema de la suma y producto*, un resultado no trivial de combinatoria aditiva. La prueba que daremos no lo utiliza, pero sí tiene algo en común con su prueba: la inducción, usada de una manera particular. En esencia, si algo es cierto para el paso n, pero no para el paso $n+1$, se trata de usar ese mismo hecho para obtener la conclusión que deseamos de otra manera (lo que se llama un "fulcro" (*pivot*) en la prueba que estamos por ver). El hecho que estemos en un grupo sin un orden natural (n, $n+1$, etc.) resulta ser irrelevante.

Prueba del Teorema 1.3.1. Gracias a (2.2), podemos asumir que $A = A^{-1}$ y $e \in A$. También podemos asumir que A es mayor que una constante absoluta, pues de lo contrario la conclusión es trivial. Escribamos $G = \mathrm{SL}_2$.

Supongamos que $|A^3| < |A|^{1+\delta}$, donde $\delta > 0$ es una pequeña constante a ser determinada más tarde. Por escape (Prop. 3.2.1), existe un elemento $g_0 \in A^c$ regular semisimple (esto es, $\mathrm{tr}(g_0) \neq \pm 2$), donde c es una constante absoluta. (A decir verdad, $c = 2$; ejercicio opcional.) Su centralizador en $G(K)$ es $C(g) = T(\overline{K}) \cap G(K)$ para algún toro maximal T.

Llamemos a $\xi \in G(K)$ un *fulcro* si la función $\phi_g : A \times C(g) \to G(K)$ definida por

$$(a, t) \mapsto a\xi t\xi^{-1} \tag{4.2}$$

es inyectiva en tanto que función de $\pm e \cdot A/\{\pm e\} \times C(g)/\{\pm e\}$ a $G(K)/\{\pm e\}$.

Caso (a): Hay un fulcro ξ en A. Por el Corolario 3.3.1, existen $\geq |A|^{1/3-O(c\delta)}$ elementos de $C(g)$ en A^2. Por lo tanto, por la inyectividad de ϕ_ξ,

$$\left|\phi_\xi(A, A^2 \cap C(g))\right| \geq \frac{1}{4}|A||A^2 \cap C(g)| \gg |A|^{\frac{4}{3}-O(c\delta)}.$$

Al mismo tiempo, $\phi_\xi(A, A^2 \cap C(g)) \subset A^5$, y por lo tanto

$$|A^5| \gg |A|^{4/3-O(c\delta)}.$$

Para $|A|$ mayor que una constante y $\delta > 0$ menor que una constante, esto nos da una contradicción con $|A^3| < |A|^{1+\delta}$ (por Ruzsa (2.3)).

Caso (b): No hay fulcros ξ en $G(K)$. Entonces, para todo $\xi \in G(K)$, hay $a_1, a_2 \in A$, $t_1, t_2 \in T(K)$, $(a_1, t_1) \neq (\pm a_2, \pm t_2)$ tales que $a_1\xi t_1\xi^{-1} = \pm e \cdot a_2\xi t_2\xi^{-1}$, lo cual da

$$a_2^{-1}a_1 = \pm e \cdot \xi t_2 t_1^{-1}\xi^{-1}.$$

En otras palabras, para cada $\xi \in G(K)$, $A^{-1}A$ tiene una intersección no trivial con el toro $\xi T\xi^{-1}$:

$$A^{-1}A \cap \xi T(K)\xi^{-1} \neq \{\pm e\}. \tag{4.3}$$

(Por cierto, esto sólo es posible si K es un cuerpo finito $\mathbb{F}_q$. Por qué?)

Escoja cualquier $g \in A^{-1}A \cap \xi T(K)\xi^{-1}$ con $g \neq \pm e$. Entonces g es regular semisimple (nota: esto es peculiar a SL_2) y su centralizador $C(g)$ es igual a $\xi T(K)\xi^{-1}$ (por qué?). Por lo tanto, el corolario 3.3.1, obtenemos que hay $\geq c|A|^{1/3-O(\delta)}$ elementos de $\xi T(K)\xi^{-1}$ en A^2, donde c y las constante implícita son absolutas.

Por lo menos $(1/2)|G(K)|/|T(K)|$ toros máximos de G son de la forma $\xi T(K)\xi^{-1}$, $\xi \in G(K)$ (mostrar!). También tenemos que todo elemento de G que no sea $\pm e$ puede estar en a lo más un toro máximo (de nuevo algo peculiar a SL_2). Por lo tanto,

$$|A^2| \geq \frac{1}{2}\frac{|G(K)|}{|T(K)|}(c|A|^{1/3-O(\delta)} - 2) \gg q^2|A|^{1/3-O(\delta)}.$$

Por lo tanto, ya sea $|A^3| \geq |A|^{1+\delta}$ (por Ruzsa (2.3)) o $|A| \geq |G|^{1-O(\delta)}$. En el segundo caso, la proposición 4.1.2 implica que $A^3 = G$.

Caso (c): Hay elementos de $G(K)$ que son fulcros y otros que no lo son. Como $\langle A \rangle = G(K)$, esto implica que existe un $\xi \in G$ que no es un fulcro y un $a \in A$ tal que $a\xi \in G$ sí es un fulcro. Como ξ no es un fulcro, (4.3) es cierto, y por lo tanto hay $|A|^{1/3-O(\delta)}$ elementos de $\xi T \xi^{-1}$ en A^k.

Al mismo tiempo, $a\xi$ es un fulcro, i.e., la aplicación $\phi_{a\xi}$ definida en (4.2) es inyectiva (considerada como una aplicación de $A/\{\pm e\} \times C(g)/\{\pm e\}$ a $G(K)/\{\pm e\}$). Por lo tanto,

$$\left|\phi_{a\xi}(A, \xi^{-1}(A^k \cap \xi T \xi^{-1})\xi)\right| \geq \frac{1}{4}|A||A^k \cap \xi T \xi^{-1}| \geq \frac{1}{4}|A|^{\frac{4}{3}-O(\delta)}.$$

Como $\phi_{a\xi}(A, \xi^{-1}(A^k \cap \xi T \xi^{-1})\xi) \subset A^{k+3}$, obtenemos que

$$|A^{k+3}| \geq \frac{1}{4}|A|^{4/3-O(\delta)}. \tag{4.4}$$

Gracias otra vez a Ruzsa (2.3), esto contradice la suposición $|A^3| \leq |A|^{1+\delta}$ para δ suficientemente pequeño. □

Apéndice A

Expansión en $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$

Daremos aquí un esbozo de cómo Bourgain y Gamburd probaron que, para $A_0 \subset \mathrm{SL}_2(\mathbb{Z})$ tal que $\langle A_0 \rangle$ es Zariski-denso, entonces

$$\{\Gamma(\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}), A_0 \bmod p)\}_{p > C,\ p \text{ primo}}$$

es una familia de expansores, i.e., tiene un hueco espectral constante.

Primero, clarifiquemos que quiere decir "Zariski-denso". Esto quiere decir simplemente que no existe ninguna subvariedad $V \subsetneq \mathrm{SL}_2(\mathbb{C})$ que contenga a $\langle A_0 \rangle$. Como dijimos en (1.3), es un hecho conocido que esto implica que $A_0 \mod p$ genera $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ para p mayor que una constante C ([Wei84], [MVW84], [Nor87] y [HP95] lo prueban para SL_2 y para muchos grupos más).

Es sencillo pasar a un subgrupo libre:

$$\Gamma(2) = \{g \in \mathrm{SL}_2(\mathbb{Z}) : g \equiv I \mod 2\}$$

es libre, y es un resultado estándar (Nielsen-Schreier) que todo subgrupo de un grupo libre es libre. Por lo tanto $\langle A_0 \rangle \cap \Gamma(2)$ es libre. El índice de $\langle A_0 \rangle \cap \Gamma(2)$ en $\langle A_0 \rangle$ es finito (por qué?), y podemos encontrar un conjunto finito que genera $\langle A_0 \rangle \cap \Gamma(2)$ (generadores de Schreier, por ejemplo). Esto es suficiente para que podamos asumir, sin pérdida de generalidad, que $\langle A_0 \rangle$ es libre.

Lo que ahora haremos es considerar la función

$$\mu(x) = \begin{cases} \frac{1}{|S|} & \text{si } x \in A_0 \bmod p, \\ 0 & \text{si } x \notin A_0 \bmod p \end{cases}$$

y sus convoluciones. La convolución $f \cdot g$ de dos funciones $f, g : G \to \mathbb{C}$ se define por

$$(f \cdot g)(x) = \sum_{y \in G} f(xy^{-1}) g(y).$$

La norma ℓ_p de una función $f : G \to \mathbb{C}$ es

$$|f|_p = \left(\sum_{y \in G} |f(y)|^p \right)^{1/p}.$$

Es fácil ver que la convolución $\mu^{(\ell)} := \mu * \mu * \ldots * \mu$ (ℓ veces) tiene norma ℓ_1 igual a 1. Empero, la norma ℓ_2 varía. Para todo f, $|f * \mu|_2 \leq |f|_2$, por Cauchy-Schwarz, con igualdad sólo si f es uniforme (ejercicio). Por lo tanto, $|\mu^{(\ell)}|_2$ decrece cuando k aumenta.

Nos interesa saber que tan rápido decrece, pues ésto nos da información sobre los valores propios de $\mathscr{A}$. Veamos por qué. El operador $\mathscr{A}$ no es sino la convolución por μ. Podemos comparar, como en (4.1), dos expresiones para la traza. Por una parte, la traza de $\mathscr{A}^{2\ell}$ es igual a la suma, para todo g, del número de maneras de ir de g a g tomando productos por A exactamente 2ℓ veces, dividido por $|A_0|^{2\ell}$; esto es

$$|G|\mu^{(2\ell)}(e) = |G| \sum_{x \in G} \mu^{(\ell)}(x^{-1})\mu^{(\ell)}(x) = |G||\mu^{(\ell)}|_2^2,$$

donde $G = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. (Como de costumbre, asumimos que $A_0 = A_0^{-1}$.) Por otra parte, la traza de $\mathscr{A}^{2\ell}$ es igual a $\sum_i \nu^{2\ell}$, donde $1 = \nu_0 > \nu_1 \geq \ldots$ son los valores propios de $\mathscr{A}$.

Como ya discutimos en §4.1, todo valor propio ν_j, $j \geq 1$, tiene multiplicidad $\geq (p-1)/2$. Por lo tanto, tenemos que, para todo $j \geq 1$,

$$\frac{p-1}{2}\nu_j^{2\ell} \leq \sum_{j \geq 0} \nu_j^{2\ell} = |G||\mu^{(\ell)}|_2^2.$$

Nuestra meta será mostrar que, para algún $\ell \leq C \log p$, C una constante suficientemente grande, la función $\mu^{(\ell)}$ es razonablemente uniforme, o "llana", por lo menos del punto de vista de su norma ℓ_2: $|\mu^{(\ell)}|_2^2 \ll 1/|G|^{1-\epsilon}$. (La distribución uniforme tiene norma ℓ_2 igual a $1/|G|$, naturalmente.) Entonces tendremos

$$\nu_j^{2\ell} \ll \frac{|G|^\epsilon}{p} \ll \frac{1}{p^{1-3\epsilon}}$$

y por lo tanto

$$\nu_j \leq e^{-\frac{(1-3\epsilon)\log p}{C \log p}} \leq 1 - \delta,$$

donde $\delta > 0$ es una constante (que, como C, puede depender de A_0). Esto es lo que deseamos.

(El uso de la multiplicidad de ν_j en este contexto particular remonta a Sarnak-Xue [SX91].)

Lo que queda es, como decíamos, mostrar que $|\mu^{(\ell)}|$ decrece rápidamente cuando ℓ aumenta. Ésto esta estrechamente ligado a mostrar que $|A_0^\ell|$ decrece (en particular, lo implica), pero no es trivialmente equivalente.

La prueba tiene dos pasos. Primero, igual que para $|A_0^\ell|$ (ver el ejercicio 1.3.2 y los comentarios que lo siguen), está el caso de lo que pasa para $\ell \leq \epsilon' \log p$, donde ϵ' es lo suficientemente pequeño como para que, para elementos $g_1, g_2, \dots, g_{2\ell} \in A_0 = A_0 \cup A_0^{-1}$ cualesquiera, tengamos que ninguno de los coeficientes de la matriz $g_1 g_2 \dots g_{2\ell} \in \mathrm{SL}_2(\mathbb{Z})$ tenga valor absoluto $\geq p-1$. Entonces, tenemos que no existen $x_i \in A_0 \bmod p$, $1 \leq i \leq k$, $x_{i+1} \notin \{x_i, x_i^{-1}\}$ para $1 \leq i \leq k-1$, $x_i \neq e$ para $1 \leq i \leq k$, y $r_i \in \mathbb{Z}$, $r_i \neq 0$, $\sum_{1 \leq i \leq k} |r_i| \leq 2\ell$, tales que

$$x_1^{r_1} \cdots x_k^{r_k} = e.$$

(Idea: si un elemento de $\mathrm{SL}_2(\mathbb{Z})$ es congruente $\bmod p$ a la identidad sin ser la identidad: entonces por lo menos uno de sus coeficientes de matriz tiene valor absoluto por lo menos $p-1$.)

Esto implica inmediatamente que los productos de elementos de $A_0 \bmod p$ de longitud ℓ son todos diferentes (excepto por las igualdades obvias del tipo $x \cdot e = x$ y $x \cdot x^{-1} = e$). Por lo tanto, $|(A \bmod p)^\ell|$ crece exponencialmente: $|(A_0 \bmod p)^\ell| \geq (|A_0| - 2)^\ell$. Ésta era la parte crucial a solución del ejercicio 1.3.2. Mostrar que $|\mu^\ell|_2$ decrece también exponencialmente no es mucho más difícil, sobre todo porque podemos asumir que A_0 es más grande que una constante. (Para A_0 más pequeño que una constante, sería un asunto más delicado: se trata de un resultado clásico de Kesten [Kes59] sobre los grupos libres.)

Queda por ver como decrece $|\mu^\ell|_2$ para $\epsilon' \log p \leq \ell \leq C \log p$. Aquí que Bourgain y Gamburd muestran que, si tuvieramos

$$|\mu^{2\ell}|_2 > |\mu^\ell|_2^{1+\delta'},$$

$\delta' > 0$, entonces existe un conjunto $A' \subset \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ tal que $|A'^3| < |A'|^{1+O(\delta')}$. (La herramienta principal es el teorema de Balog-Szemerédi [BS94], fortalecido por Gowers [Gow01] y generalizado por Tao [Tao08] al caso no conmutativo.) Muestran también que $\mu(A')$ es grande, por lo cual A' es menor que $|G|^{1-O(\delta')}$ a menos que μ ya sea tan uniforme como deseamos. Un argumento auxiliar muestra que A' genera $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. Por lo tanto, $|A'^3| < |A'|^{1+O(\delta')}$ entra en contradicción con el Teorema 1.3.1.

Esto muestra que $|\mu^{2\ell}|_2 \leq |\mu^\ell|_2^{1+\delta'}$ para $\epsilon' \log p \leq \ell \leq C \log p$, y termina la prueba. Concluimos que $\nu_1 \leq 1 - \delta$, que era lo que queríamos demostrar.

Bibliografía

[BBS04] L. Babai, R. Beals, and Á. Seress. On the diameter of the symmetric group: polynomial bounds. In *Proceedings of the Fifteenth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 1108–1112 (electronic), New York, 2004. ACM.

[BG08] J. Bourgain and A. Gamburd. Uniform expansion bounds for Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$. *Ann. of Math. (2)*, 167(2):625–642, 2008.

[BGT11] E. Breuillard, B. Green, and T. Tao. Approximate subgroups of linear groups. *Geom. Funct. Anal.*, 21(4):774–819, 2011.

[BGT12] E. Breuillard, B. Green, and T. Tao. The structure of approximate groups. *Publications mathématiques de l'IHÉS*, 116:115–221, 2012.

[BS88] L. Babai and Á. Seress. On the diameter of Cayley graphs of the symmetric group. *J. Combin. Theory Ser. A*, 49(1):175–179, 1988.

[BS94] A. Balog and E. Szemerédi. A statistical theorem of set addition. *Combinatorica*, 14(3):263–268, 1994.

[Din11] O. Dinai. Growth in SL_2 over finite fields. *J. Group Theory*, 14(2):273–297, 2011.

[DS98] V. I. Danilov and V. V. Shokurov. *Algebraic curves, algebraic manifolds and schemes.* Springer-Verlag, Berlin, 1998. Translated from the 1988 Russian original by D. Coray and V. N. Shokurov, Translation edited and with an introduction by I. R. Shafarevich, Reprint of the original English edition from the series Encyclopaedia of Mathematical Sciences [*Algebraic geometry. I*, Encyclopaedia Math. Sci., 23, Springer, Berlin, 1994; MR1287418 (95b:14001)].

[DSC93] P. Diaconis and L. Saloff-Coste. Comparison techniques for random walk on finite groups. *Ann. Probab.*, 21(4):2131–2156, 1993.

[EMO05] A. Eskin, Sh. Mozes, and H. Oh. On uniform exponential growth for linear groups. *Invent. math.*, 160(1):1–30, 2005.

[Fre73] G. A. Freĭman. *Foundations of a structural theory of set addition.* American Mathematical Society, Providence, R. I., 1973. Translated from the Russian, Translations of Mathematical Monographs, Vol 37.

[GH11] N. Gill and H. A. Helfgott. Growth of small generating sets in $\mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})$. *Int. Math. Res. Not. IMRN*, (18):4226–4251, 2011.

[Gow01] W. T. Gowers. A new proof of Szemerédi's theorem. *Geom. Funct. Anal.*, 11(3):465–588, 2001.

[Gow08] W. T. Gowers. Quasirandom groups. *Combin. Probab. Comput.*, 17(3):363–387, 2008.

[Gro81] M. Gromov. Groups of polynomial growth and expanding maps. *Inst. Hautes Études Sci. Publ. Math.*, (53):53–73, 1981.

[Hel08] H. A. Helfgott. Growth and generation in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. *Ann. of Math. (2)*, 167(2):601–623, 2008.

[Hel11] H. A. Helfgott. Growth in $\mathrm{SL}_3(\mathbb{Z}/p\mathbb{Z})$. *J. Eur. Math. Soc. (JEMS)*, 13(3):761–851, 2011.

[Hel15] H. A. Helfgott. Growth in groups: ideas and perspectives. *Bull. Amer. Math. Soc. (N.S.)*, 52(3):357–413, 2015.

[HP95] E. Hrushovski and A. Pillay. Definable subgroups of algebraic groups over finite fields. *J. Reine Angew. Math.*, 462:69–91, 1995.

[Hru12] E. Hrushovski. Stable group theory and approximate subgroups. *J. Amer. Math. Soc.*, 25(1):189–243, 2012.

[HS14] H. A. Helfgott and Á. Seress. On the diameter of permutation groups. *Ann. of Math. (2)*, 179(2):611–658, 2014.

[Kes59] H. Kesten. Symmetric random walks on groups. *Trans. Amer. Math. Soc.*, 92:336–354, 1959.

[Kow13] E. Kowalski. Explicit growth and expansion for SL_2. *Int. Math. Res. Not. IMRN*, (24):5645–5708, 2013.

[LP11] M. J. Larsen and R. Pink. Finite subgroups of algebraic groups. *J. Amer. Math. Soc.*, 24(4):1105–1158, 2011.

[LPW09] D. A. Levin, Y. Peres, and E. L. Wilmer. *Markov chains and mixing times.* American Mathematical Society, Providence, RI, 2009. With a chapter by James G. Propp and David B. Wilson.

[Mum99] D. Mumford. *The red book of varieties and schemes*, volume 1358 of *Lecture Notes in Mathematics.* Springer-Verlag, Berlin, expanded edition, 1999. Includes the Michigan lectures (1974) on curves and their Jacobians, With contributions by Enrico Arbarello.

[MVW84] C. R. Matthews, L. N. Vaserstein, and B. Weisfeiler. Congruence properties of Zariski-dense subgroups. I. *Proc. London Math. Soc. (3)*, 48(3):514–532, 1984.

[Nor87] M. V. Nori. On subgroups of $\mathrm{GL}_n(\mathbf{F}_p)$. *Invent. math.*, 88(2):257–275, 1987.

[NP11] N. Nikolov and L. Pyber. Product decompositions of quasirandom groups and a Jordan type theorem. *J. Eur. Math. Soc. (JEMS)*, 13(4):1063–1077, 2011.

[Pet12] G. Petridis. New proofs of Plünnecke-type estimates for product sets in groups. *Combinatorica*, 32(6):721–733, 2012.

[Plü70] H. Plünnecke. Eine zahlentheoretische Anwendung der Graphentheorie. *J. Reine Angew. Math.*, 243:171–183, 1970.

[PS] L. Pyber and E. Szabó. Growth in finite simple groups of Lie type. To appear in *J. Amer. Math. Soc.*

[RT85] I. Z. Ruzsa and S. Turjányi. A note on additive bases of integers. *Publ. Math. Debrecen*, 32(1-2):101–104, 1985.

[Ruz89] I. Z. Ruzsa. An application of graph theory to additive number theory. *Sci. Ser. A Math. Sci. (N.S.)*, 3:97–109, 1989.

[Ruz91] I. Z. Ruzsa. Arithmetic progressions in sumsets. *Acta Arith.*, 60(2):191–202, 1991.

[Sel65] A. Selberg. On the estimation of Fourier coefficients of modular forms. In *Proc. Sympos. Pure Math., Vol. VIII*, pages 1–15. Amer. Math. Soc., Providence, R.I., 1965.

[Sha99] Y. Shalom. Expander graphs and amenable quotients. In *Emerging applications of number theory (Minneapolis, MN, 1996)*, volume 109 of *IMA Vol. Math. Appl.*, pages 571–581. Springer, New York, 1999.

[SX91] P. Sarnak and X. X. Xue. Bounds for multiplicities of automorphic representations. *Duke Math. J.*, 64(1):207–227, 1991.

[Tao08] T. Tao. Product set estimates for non-commutative groups. *Combinatorica*, 28(5):547–594, 2008.

[Tao15] T. Tao. *Expansion in finite simple groups of Lie type*, volume 164 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2015.

[Var12] P. P. Varjú. Expansion in $\mathrm{SL}_d(\mathcal{O}_K/I)$, I square-free. *J. Eur. Math. Soc. (JEMS)*, 14(1):273–305, 2012.

[Wei84] B. Weisfeiler. Strong approximation for Zariski-dense subgroups of semi-simple algebraic groups. *Ann. of Math. (2)*, 120(2):271–315, 1984.