Chapter 1

Introducción al crecimiento

1.1 Definiciones

En esta lectura, queremos estudiar subconjuntos finitos de grupos. Sea $(G, \cdot)$ un grupo y sea A un subconjunto no vacío de G. Podemos definir

$$\begin{aligned} A^2 &= A \cdot A = \{a_1 \cdot a_2 \mid a_1, a_2 \in A\}, \\ A^3 &= A \cdot A \cdot A = \{a_1 \cdot a_2 \cdot a_3 \mid a_1, a_2, a_3 \in A\}, \end{aligned}$$

y, similarmente, tenemos $A^4, A^5, \ldots, A^k, \ldots$, para todo $k \in \mathbb{Z}^+$. En este curso queremos estudiar el *tamaño* de estos conjuntos. Entonces, estudiamos la secuencia de enteros positivos

$$|A|, |A^2|, |A^3|, |A^4|, \ldots \tag{1.1}$$

Lema 1. *La secuencia* (1.1) *es no decreciente.*

Demostración. Sea $a \in A$. El conjunto A^k contiene el conjunto

$$\{a \cdot b \mid b \in A^{k-1}\}.$$

Ahora observe que la función $\rho_a : G \to G, g \mapsto a \cdot g$ es inyectiva (tiene una inversa). □

A la luz del Lema 1, podemos decir que el conjunto A *crece* cuando es multiplicado por sí mismo. Entonces, llamamos el estudio de la secuencia (1.1) el estudio del *crecimiento* de A.

En este curso, vamos a considerar crecimiento en varios grupos. Ustedes necesitan estar familiarizados con estos grupos:

$$(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{Q}^*, \cdot), (\mathbb{R}, +), (\mathbb{R}, \cdot), (\mathbb{Z}/n\mathbb{Z}, +), (S_n, \cdot), (A_n, \cdot), \cdots$$

Hay dos casos más que son útiles considerar aunque no son exactamente grupos:

1. Si $(\mathbb{F}, +, \cdot)$ es un cuerpo, entonces $(\mathbb{F}^*, \cdot)$ es un grupo. A veces, sera útil considerar subconjuntos de $\mathbb{F}$ que contiene 0 y examinar el compartamiento de tales conjuntos con respecto a "$\cdot$". Es fácil ver que Lema 1 aplica a tales conjuntos también (Verifíquelo!).

2. Si $(R, +, \cdot)$ es un anillo y no es un cuerpo, entonces $(R, \cdot)$ es lejos de ser un grupo. En esta situación es posible encontrar conjuntos que no crecen con respecto a "$\cdot$". Por ejemplo, tome $R = \mathbb{Z}/4\mathbb{Z}$ y sea $A = \{0, 2\}$. En este caso $A \cdot A = \{0\}$ y tenemos $|A \cdot A| < |A|$. Mire Ejercicios 1 para más sobre tales conjuntos.

Necesitamos un poco más terminología: podemos escribir grupos multiplicativamente – $(G, \cdot)$ – como anteriormente o aditivamente – $(G, +)$. En el caso posterior, escribiremos

$$2A = A + A = \{a_1 + a_2 \mid a_1, a_2 \in A\},$$
$$3A = A + A + A = \{a_1 + a_2 + a_3 \mid a_1, a_2, a_3 \in A\}.$$

Es importante notar que si escribo un grupo aditivamente este grupo será siempre abeliano. Si escribo un grupo multiplicativamente este grupo puede ser abeliano o no-abeliano.

Por fin, vamos a escribir cosas como A^{-1}, $A + B$, $A - B$, $A \cdot B$ (para conjuntos A, B); $b + A$ o $b \cdot A$ (para A un conjunto y b un elemento). Espero que las definiciones sean obvias.

1.2 Primeras observaciones

Después de ahora, $(G, \cdot)$ es un grupo y $A, B \subseteq G$. Observe que

$$|A| \leq |A + A| \leq |A|^2.$$

Entonces, concluimos que el crecimiento está siempre entre una función lineal y una función cuadŕatica. Si G es abeliano, podemos mejorar estas cotas:

$$|A| \leq |A + A| \leq \frac{|A|(|A| + 1)}{2}.$$

Ejemplo 1. Sea $A = \{2, 4, 6, 8, 10\}$ y $B = \{2, 4, 8, 16, 32\}$ conjuntos de enteros. Vamos a considerar estos conjuntos como subconjuntos de varios grupos abelianos:

1. Tome $A \subset (\mathbb{Q}, +)$. Entonces $|A + A| = 9 = 2|A| - 1$.
2. Tome $B \subset (\mathbb{Q}^*, \cdot)$. Entonces $|B \cdot B| = 9 = 2|B| - 1$.
3. Tome $A \subset (\mathbb{Q}^*, \cdot)$. Entonces $|A \cdot A| = 14 > \frac{|A|}{2}$.
4. Tome $C = \{1, 2, 4, 6, 8, 9, 10\} \subset (\mathbb{Z}/11\mathbb{Z}, +, \cdot)$. Entonces $|C \cdot C| = 10$ y $|C + C| = 11$.
5. Tome $D = \{(1), (1, 2)(3, 4), (1, 4)(3, 2), (1, 3)(2, 4)\} \subset (S_4, \cdot)$. Entonces $|D \cdot D| = 4 = |D|$.

Un principio importante en el estudio de crecimiento es que “usualmente” los conjuntos crecen. Es decir, si escogemos un conjunto aleatoriamente en algún grupo, es probable que el conjunto crecerá cuadraticamente (o casi cuadraticamente).

Desde otro punto de vista, si encontramos conjuntos que no crecen, queremos probar que estos conjuntos tienen algún tipo de estructura. Tal tipo de resultado se llama un *teorema inverso*. Consideremos Ejemplo 1:

1. El conjunto A es una progresión aritmética. Ustedes probarán en ejercicios que progresiones aritméticas son los conjuntos en $(\mathbb{Q}, +)$ con crecimiento minimal.

2. El conjunto B es una progresión geométrica. Ustedes probarán en ejercicios que progresiones geométricas son los conjuntos en $(\mathbb{Q}, \cdot)$ con crecimiento minimal.

3. El conjunto C es un **gran** conjunto en el cuerpo $(\mathbb{Z}/11\mathbb{Z}, +, \cdot)$. Ya que un cuerpo es cerrado con respecto a “+” y “$\cdot$”, es claro que los grandes conjuntos no pueden crecer mucho.

4. Por fin, el conjunto D es un **subgrupo** en el grupo $(S_4, \cdot)$. Ya que los subgrupos son cerrados con respecto a la operación del grupo, luego D no puede crecer nada.

¿Qué pasa cuando tenemos el menor crecimiento? Ya se puede dar el primer teorema inverso:

Proposición 2. *Supóngase que $A \subset G$ donde $(G, +)$ es abeliano. Los siguientes son equivalentes:*

1. $|A + A| = |A|$;
2. $|A - A| = |A|$;
3. $|nA| = |A|$ *para un entero positivo* $n \neq 1$;
4. $|nA| = |A|$ *para todos enteros positivos;*
5. *Hay un subgrupo finito $H \leq G$ tal que A es un coset de H.*

Demostración. Vamos a probar (1) implica (5) y los otras se dejan ejercicios.

Escoga $g \in G$ tal que $B = g + A$ y B contiene 0. Observe que

$$|B + B| = |A + A| = |A| = |B|.$$

Además, $B + B \supset \{0\} + B = B$, entonces $B + B = B$. Por un ejercicio, concluimos que B es un subgrupo finito de G y $A = -g + B$ es un un coset de B. □

Lema 3. (Desigualdad triangular de Ruzsa) *Sean A, B y C subconjuntos finitos de un grupo $(G, \cdot)$. Entonces*

$$|A \cdot C^{-1}||B| \leq |A \cdot B^{-1}||B \cdot C^{-1}|.$$

Demostración. Construiremos una inyección $\iota : A \cdot C^{-1} \times B \to A \cdot B^{-1} \times B \cdot C^{-1}$. Para cada $d \in A \cdot C^{-1}$, escojamos $(f_1(d), f_2(d)) = (a, c) \in A \times C$ tal que $d = a \cdot c^{-1}$. Definamos $\iota(d, b) = (f_1(d) \cdot b^{-1}, b \cdot (f_2(d))^{-1})$. Podemos recuperar $d = f_1(d) \cdot (f_2(d))^{-1}$ 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. □

Corolario 4. *Sea $X = A \cup A^{-1} \cup \{0\}$.*

1. $\frac{|X^2|}{|A|} \leq 6 \left(\frac{|A^2|}{|A|}\right)^2$.
2. $\frac{|X^3|}{|A|} \leq 14 \left(\frac{|A^3|}{|A|}\right)^3$.
3. *Si $A = A^{-1}$ y $k \geq 3$, entonces* $\frac{|A^k|}{|A|} \leq \left(\frac{|A^3|}{|A|}\right)^{2k-5}$.

Demostración. Mostraremos (1) y dejamos (2) y (3) como ejercicios.

Observe que

$$X^2 = A^2 \cup (A^{-1})^2 \cup (A \cdot A^{-1}) \cup (A^{-1} \cdot A) \cup A \cup A^{-1}.$$

Para mostrar el resultado, es suficiente demostrar que $\frac{|A \cdot A^{-1}|}{|A|} \leq \left(\frac{|A \cdot A|}{|A|}\right)^2$. Por eso, tomamos $C = A$, $B = A^{-1}$ en la desigualdad triangular de Ruzsa. □

Si G es abeliano, es posible probar un resultado más fuerte que 3.[1]

[1] Este resulto puede ser probado en dos maneras: la primera demostración de Plünnecke-Ruzsa usa métodos de la teoría de grafos y es un poco complicada. Recientemente, Petridis encontró una demostración más elementaria.

Teorema 5. (Plünnecke-Ruzsa) *Si A es un subconjunto de un grupo abeliano $(G,+)$. Entonces,*

$$\frac{|kA-\ell A|}{|A|} \leq \left(\frac{|2A|}{|A|}\right)^{k+\ell}.$$

Podemos reescribir este teorema y parte (2) del Corolario 4 de la manera siguiente:

- Supóngase que A es un subconjunto de un grupo $(G,\cdot)$ con $A = A^{-1}$, y sea $K \in \mathbb{R}^+$. Si A *tiene triplicación* K, es decir, si $|A \cdot A \cdot A| \leq K|A|$, entonces $|A^k| \leq K^{2k-5}|A|$ para todo $k \geq 3$.

- Supóngase que A es un subconjunto de un grupo abeliano $(G,+)$, y sea $K \in \mathbb{R}^+$. Si A *tiene duplicación* K, es decir, si $|A+A| \leq K|A|$, entonces $|kA| \leq K^k|A|$ para todo $k \geq 1$.

Entonces, en un grupo abeliano el tamaño de $A+A$ controla la velocidad del crecimiento de A siempre, mientras que en un grupo general el tamaño de $A \cdot A \cdot A$ controla la velocidad de crecimiento de A siempre.

1.3 Ejercicios

(1) Sea A un subconjunto de $\mathbb{Z}$.
(a) Muestre que $|A+A| \geq 2|A|-1$.
(b) Muestre que si A es una progresión aritmética, entonces $|A+A| = 2|A|-1$.
(c) Muestre que si $|A+A| = 2|A|-1$, entonces A es una progresión aritmética.[2]

(2) Sea B un subconjunto de $\mathbb{Z}^+$.
(a) Muestre que $|B \cdot B| \geq 2|B|-1$.
(b) Muestre que B es una progresión geométrica si y sólo si $|B \cdot B| = 2|B|-1$.
(c) ¿Porqué la restricción a los enteros **positivos**?

(3) (a) Sea A una progresión aritmética. Encuentre una buena cota inferior para $|A \cdot A|$.
(b) Sea B una progresión geométrica. Encuentre una buena cota inferior para $|B+B|$.[3]

(4) Complete la demostración de Proposición 2. ¿Puede escribir y probar una versión no-abeliana?

(5) Sea A un conjunto en un grupo $(G, \cdot)$. Muestre que $A^2 = A$ si y sólo si A es un grupo.

(6) Sea G un grupo finito, y supóngase que A y B son subconjuntos de G tal que

$$|A| + |B| > |G|.$$

Muestre que $A \cdot B = A \cdot B^{-1} = G$. De un ejemplo de conjuntos tal que

$$|A| + |B| = |G| \text{ y } A \cdot B \neq G.$$

[2] Partes (b) y (c) juntos forman un caso especial del **teorema de Freiman**. Este teorema da una descripción completa de los subconjuntos de $\mathbb{Z}$ que satisface una cota superior lineal por duplicación. El teorema dice lo siguiente:

Para todo $C > 0$, existe $d, k \in \mathbb{Z}^+$ tal que para todo $A \subseteq \mathbb{Z}$ con $|A+A| < C|A|$, hay una progresión aritmética P de dimensión d y largo k tal que $A \subseteq P$.

En otras palabras, el teorema de Freiman dice que los todos subconjuntos de $\mathbb{Z}$ que tienen duplicación pequeña son subconjuntos de las progresiones aritméticas de dimensión a cotada y largo a cotado. Tal vez, usted no sabe lo que significa la *dimensión* de una progresión – por eso se necesita generalizar la definición de una progresión aritmética. Con esta generalización los progresiones aritméticas usuales son las progresiones aritméticas de dimensión 1. Visite wikipedia para más detalles!

[3] Los primeros dos ejercicios muestran que podemos encontrar subconjuntos de $\mathbb{Z}$ que respectan una cota superior lineal con respecto una de las operaciones disponibles: para "+", podemos tomar las progresiones aritméticas; similarmente podemos tomar las progresiones geométricas para "·".

El tercer ejercicio muestra que, en cada caso, los conjuntos que hemos encontrado no respecten una cota superior lineal con respecto a la otra operación. Una pregunta natural es encontrar subconjuntos que respectan cotas superiores con respecto a las dos operaciones simultaneamente. Una **conjetura de Erdös y Szemerédi** dice que este no es posible. La conjetura completa todavíía está abierta pero una versión más debil (con una demostración muy hermosa) es un **teorema de Solymosi**. Su resultado es el siguiente:

Para todo $\varepsilon > 0$, hay un $C > 0$ tal que, para todo finito $A \subset \mathbb{Z}$,

$$\max\{|A \cdot A|, |A+A|\} \geq C|A|^{4/3-\varepsilon}.$$

La conjetura de Erdös y Szemerédi es la misma proposición con 4/3 reemplazado con 2. En otra palabras, la conjetura dice que todos subconjuntos de $\mathbb{Z}$ crecen con respecto a "+" o "·" y, además, este crecimiento es lo mas cercana posible al crecimiento cuadrático... sin ser siempre cuadrático.

(7) (Tao-Vu, 2.3.7) Sea G un grupo abeliano, y supóngase que A y B son subconjuntos de G. Muestre que

$$|A - B| = |A|^{\frac{1}{2}}|B|^{\frac{1}{2}}$$

si y sólo si A, B son cosets de un subgrupo finito H de G.

(8) Muestre las partes 2 y 3 de Corolario 4.

(9) (Breuillard, Ejercicio 2.8) Sea G un grupo abeliano, y supóngase que A es un subconjuntos de G. Muestre que si $|AA| < \frac{3}{2}|A|$, entonces A^2 es un coset de un subgrupo de G. Dar un ejemplo de un conjunto A tal que $|AA| = \frac{3}{2}|A|$ pero A no es un coset de un subgrupo.

(10) ¿Para cuales valores de n, puede usted encontrar un subconjunto A del anillo $\mathbb{Z}/n\mathbb{Z}$ tal que $|A \cdot A| < |A|$? Escriba la mejor proposición posible sobre esta pregunta para todos los valores de $n \geq 2$.