

دراسة في المجموعات المولدة الصغرى لزمرة تبديلية

هيفاء صويص¹ د. إيمان الخوجة² د. عدنان الطيباني³

الملخص

يعدُّ البحث عن مجموعات مولدة لزمرة تبديلية، وارتباط مفهوم التوليد بمفهوم الاستقلال وتعدد أنواع الاستقلال من القضايا الهامة في نظرية الزمر، حيث تكتسب الزمرة التبديلية التي تملك مجموعة مولدة خصائصاً هامة تميزها عن الزمر التي لا تماثلها. في هذه الورقة قمنا بدراسة مفهوم المجموعات المولدة الصغرى لزمرة تبديلية ومفهوم S -استقلال وذلك في زمرة الأعداد الصحيحة بالمقاس n وفي الزمر الدوارة المنتهية، كما قمنا بإيجاد مجموعات مولدة صغرى للزمر التبديلية الحرة حيث إن هذه المجموعات لا تشكل أساساً حراً لها، فضلاً عن إيجاد مجموعات مولدة صغرى لزمرة الأعداد الصحيحة.

الكلمات المفتاحية. مجموعة مولدة صغرى، مجموعة مستقلة، مجموعة مستقلة خطياً، مجموعة S -مستقلة، الأساس، الأساس الحر.

¹ طالبة دراسات عليا في قسم الرياضيات - كلية العلوم - جامعة حمص.

² أستاذ مساعد في قسم الرياضيات - كلية العلوم - جامعة حمص.

³ مدرس في قسم العلوم الأساسية - كلية الهندسة الميكانيكية والكهربائية - جامعة حمص.

A Study of Minimal Generating Sets of an Abelian Group

Haifaa Swies¹ Dr. Eaman Al-Khouja² Dr. Adnan Al-Taybani³

Abstract

The aim of this paper is to study minimal generating sets of an abelian group and S – independent sets, in addition to examining the effect of the concept of independence, in its various forms, on the generating set of the abelian group, since an abelian group that has a generating set has important properties that distinguish it from non-isomorphic ones. We also studied minimal generating sets of $(\mathbb{Z}_n, +)$ and finite cyclic groups. Additionally, we found minimal generating sets of free abelian groups; however, these sets don't form a free basis. Finally, we determine minimal generating sets of $(\mathbb{Z}, +)$.

Key Words: Minimal generating set, Independent set, linearly Independent set, Basis, Free Basis.

¹ Graduate Student , Department of Mathematics Homs University

² Assistant Professor, Department of Mathematics Homs University.

³ .Department of Basic Sciences, Faculty of Mechanical and Electrical Engineering Homs University.

مقدمة.

تعد مسألة التعبير عن عناصر بنية جبرية بدلالة عناصر مجموعة جزئية غير خالية منها من المسائل الهامة وذات أثر كبير في الرياضيات عموماً وفي الجبر على وجه الخصوص، ويعد البحث عن أصغر المجموعات المولدة لمختلف البنى الجبرية كالزمرة والحلقة وغيرها من البنى الجبرية، والتي درست من قبل M. Hrbek و P. Ruzicka في [1] و [2] و [3] و [4]، من أبرز الدراسات وأحدثها في هذا المجال، ففي عام 2015 قام M. Hrbek و P. Ruzicka في [4] بدراسة المجموعات المولدة الصغرى لأنواع من الزمر التبديلية كزمر الفتل والزمر عديمة الفتل وذلك من خلال طرح مفهوم S -استقلال، حيث تجدر الإشارة إلى أن مفهوم الاستقلال بأنواعه وتعميماته وحالاته الخاصة تلعب دوراً هاماً في توصيف المجموعات المولدة للبنى الجبرية المختلفة، وبشكل خاص في الزمر التبديلية، وقد قمنا في هذه المقالة بدراسة ثلاثة أنواع من المجموعات وهي المجموعة المستقلة والمجموعة المستقلة خطياً بالإضافة إلى المجموعة الـ S -مستقلة، حيث بينا العلاقة بين هذه المجموعات كما قمنا بدراسة المجموعات المولدة ضمن حالات الاستقلال السابقة وبشكل خاص المجموعة المولدة الصغرى والتي تكون حسب تعريفها S -مستقلة، حيث قمنا بتوصيف طبيعة العلاقة بين عناصر مجموعة جزئية من زمرة الأعداد الصحيحة بالمقاس n لتكون مجموعة مولدة صغرى لهذه الزمرة، فضلاً عن تحديد قدرة أكبر مجموعة مولدة صغرى لها، بالإضافة إلى تعيين المجموعات المولدة الصغرى للزمرة الدوارة المنتهية والتي مرتبتها n بناءً على التماثل بين هذه الزمرة وزمرة الأعداد الصحيحة بالمقاس n ، فضلاً عن ذلك قمنا بإيجاد مجموعات مولدة صغرى للزمرة التبديلية الحرة انطلاقاً من أساس حر لها وذلك بطريقتين مختلفتين حيث إن المجموعة المولدة الصغرى في هذه الحالة لا تشكل أساساً حراً للزمرة، فضلاً عن العديد من المبرهنات والنتائج الهامة المرتبطة بمفهوم المجموعة المولدة لزمرة والمجموعات المستقلة بأنواعها.

1- تعاريف ومبرهنات أساسية.

نعرض في هذه الفقرة بعض المفاهيم الأساسية المتعلقة بالزمر والمجموعات المولدة لزمرة، والبدائية مع التعريف الآتي:

تعريف. [3].

لتكن $(G, +)$ زمرة ولنفرض أنَّ S مجموعة جزئية غير خالية من G ، عندئذ نقول عن المجموعة S إنها مولدة للزمرة G إذا كانت أصغر زمرة جزئية من G تحوي S هي G نفسها. إذا كانت المجموعة S مولدة للزمرة G فإننا نعبر ذلك بالشكل $G = \langle S \rangle$.

تعريف. [3].

لتكن $(G, +)$ زمرة، عندئذ نقول عن الزمرة G إنها منتهية التوليد إذا وجدت في G مجموعة جزئية غير خالية منتهية مولدة لها، وإلا فإن الزمرة G غير منتهية التوليد.

مبرهنة. 1.1. [3].

لتكن $(G, +)$ زمرة ولنفرض أنَّ S مجموعة جزئية غير خالية من G ، عندئذ فإنَّ $G = \langle S \rangle$ إذا وفقط إذا كان كل عنصر $x \in G$ يكتب بدلالة عناصر مجموعة جزئية منتهية من عناصر المجموعة S .

تعريف. [3].

لتكن $(G, +)$ زمرة، عندئذ نقول عن الزمرة G إنها دارة إذا وجد عنصر $a \in G$ يحقق أنَّ $G = \langle \{a\} \rangle$ ، ونقول في هذه الحالة إنَّ G زمرة دارة مولدة بالعنصر a ونكتب اختصاراً $G = \langle a \rangle$.

مبرهنة. 1.2. [3].

لتكن $(G, +)$ زمرة دارة مرتبتها n ومولدة بالعنصر a ولنفرض أنَّ $k \in \mathbb{Z}^+$ ، عندئذ فإنَّ $G = \langle a^k \rangle$ إذا وفقط إذا كان $\gcd(n, k) = 1$.

مبرهنة 1.3. [6].

لتكن G زمرة و $a \in G$ عنصر مرتبته n ، ولنفرض أن $k, r, s \in \mathbb{Z}^+$ عندئذ فإنّ
القضايا الآتية صحيحة:

$$-1 \quad \langle a^k \rangle = \langle a^{gcd(n,k)} \rangle$$

$$-2 \quad o(a^k) = \frac{n}{gcd(n,k)}$$

$$-3 \quad \langle a^r \rangle = \langle a^s \rangle \text{ عندما فقط عندما } gcd(n,r) = gcd(n,s)$$

مبرهنة 1.4. [6,3].

لتكن $\{G_i\}_{i=1}^n$ أسرة من الزمر الدوارة المنتهية، عندئذ فإنّ الشرط الازم والكافي لتكون زمرة
الجداء المباشر $G_1 \times G_2 \times \dots \times G_n$ دوارة هو أن تكون $(G_i : 1)$ و $(G_j : 1)$ أعداداً أولية فيما
بينها وذلك لأجل كل $i \neq j$ حيث $1 \leq i, j \leq n$.

مبرهنة 1.5. [3].

لتكن $(\square, +)$ زمرة الأعداد الصحيحة ولنفرض أن n_1, n_2, \dots, n_k أعداداً صحيحة موجبة
وأنّ $gcd(n_1, n_2, \dots, n_k) = d$ عندئذ فإنّ $\langle n_1, n_2, \dots, n_k \rangle = \langle d \rangle$.

مبرهنة 1.6. [6,3].

لتكن G زمرة دوارة، ولنفرض أن $G = \langle a \rangle$ ، عندئذ القضيتان الآتيتان صحيحتان:

$$-1 \quad \text{إذا كانت } G \text{ غير منتهية فإن } G \cong \mathbb{Z}$$

$$-2 \quad \text{إذا كانت } G \text{ منتهية من المرتبة } n \text{ فإن } G \cong \mathbb{Z}_n$$

مبرهنة 1.7. [6,4,3].

لتكن $(G, +)$ زمرة تبديلية، ولنفرض أن $\xi(G) = \{x \in G; o(x) \in \mathbb{N}^+\}$ ، عندئذ فإنّ
المجموعة $\xi(G)$ تشكل زمرة جزئية من الزمرة G .

تعريف. [6,4,3].

لتكن $(G, +)$ زمرة تبديلية، عندئذ تدعى الزمرة الجزئية $\langle G \rangle$ بزمرة القتل الجزئية من الزمرة G ، وإذا كانت $\langle G \rangle = G$ عندئذ نقول إنَّ G زمرة قتل، وإذا كان $\langle G \rangle = \langle e \rangle$ نقول عن الزمرة G أنها زمرة قتل حرة (عديمة القتل).

تعريف. [6,3].

لتكن $(G, +)$ زمرة تبديلية، لنفرض أن $X = \{x_i\}_{i=1}^n$ مجموعة جزئية من الزمرة G عناصرها مغايرة للصفر، عندئذ نقول عن المجموعة X إنها مستقلة إذا كان لأجل أي مجموعة جزئية $\emptyset \subsetneq \{x_i\}_{i=1}^n$ وتحقق $\sum_{i=1}^n \alpha_i x_i = 0$ ينتج أن $\alpha_i x_i = 0$ لأجل كل $1 \leq i \leq n$. ونقول عن المجموعة X إنها مرتبطة إذا لم تكن مستقلة.

تعريف. [6,3].

لتكن $(G, +)$ زمرة تبديلية، لنفرض أن X مجموعة جزئية غير خالية من الزمرة G عناصرها مغايرة للصفر، عندئذ نقول عن المجموعة X إنها مستقلة إذا كانت كل مجموعة جزئية غير خالية ومنتهية منها مستقلة. ونقول عن المجموعة X إنها مرتبطة إذا لم تكن مستقلة.

مبرهنة 1.8. [3].

لتكن $(G, +)$ زمرة تبديلية، لنفرض أن X مجموعة جزئية غير خالية من G ، عندئذ تكون المجموعة X مستقلة إذا وفقط إذا كانت $\langle X \rangle = \sum_{x \in X} \langle x \rangle$.

تعريف. [3].

لتكن $(G, +)$ زمرة تبديلية، لنفرض أن X مجموعة جزئية غير خالية ومنتهية من G عناصرها مغايرة للصفر، عندئذ نقول إنَّ X أساساً للزمرة G إذا كان $G = \langle X \rangle$ وكانت المجموعة X مستقلة.

تعريف.[3].

لتكن $(G, +)$ زمرة تبديلية، لنفرض أن $X = \{x_i\}_{i=1}^n$ مجموعة جزئية من الزمرة G عندئذ نقول إنَّ المجموعة X مستقلة خطياً إذا كان لأجل أي مجموعة جزئية $\{\alpha_i\}_{i=1}^n \subset \square$ وتحقق $\sum_{i=1}^n \alpha_i x_i = 0$ ينتج أن $\alpha_i = 0$ لأجل كل $1 \leq i \leq n$. ونقول عن المجموعة X إنها مرتبطة خطياً إذا لم تكن مستقلة خطياً.

تعريف.[3].

لتكن $(G, +)$ زمرة تبديلية، لنفرض أن X مجموعة جزئية غير خالية من G ، عندئذ نقول عن المجموعة X إنها مستقلة خطياً إذا كانت كل مجموعة جزئية غير خالية ومنتھية منها مستقلة خطياً. ونقول عن المجموعة X إنها مرتبطة خطياً إذا لم تكن مستقلة خطياً.

مبرهنة.1.9.

لتكن $(G, +)$ زمرة تبديلية عديمة القتل، ولنفرض أن X مجموعة جزئية غير خالية من G عناصرها مغايرة للصفر، عندئذ تكون المجموعة X مستقلة إذا وفقط إذا كانت مستقلة خطياً.

البرهان. واضح.

مبرهنة.1.10.

لتكن $(G, +)$ زمرة تبديلية، لنفرض أن X مجموعة جزئية غير خالية من G ، عندئذ القضايا الآتية صحيحة:

- 1- إذا كان $0 \in X$ فإنَّ المجموعة X تكون مرتبطة خطياً.
- 2- إذا كانت X مستقلة خطياً فإنها تكون مستقلة.
- 3- تكون X مرتبطة إذا وفقط إذا حوت مجموعة جزئية غير خالية ومنتھية مرتبطة.
- 4- تكون X مرتبطة خطياً إذا وفقط إذا حوت مجموعة جزئية غير خالية ومنتھية مرتبطة خطياً.

5- إذا كانت X مرتبطة فإنها تكون مرتبطة خطياً.

البرهان.

1- واضح.

2- لنفرض أن المجموعة X مستقلة خطياً عندئذ فإن عناصر المجموعة X مغايرة للصفر، من جهة أخرى أياً كانت العناصر $\{x_i\}_{i=1}^n \subset X, \{\alpha_i\}_{i=1}^n \subset \mathbb{Z}$ والتي تحقق أن $\sum_{i=1}^n \alpha_i x_i = 0$ فإن $\alpha_i = 0$ لأجل كل $1 \leq i \leq n$ وبالتالي فإن $\alpha_i v_i = 0$ لأجل كل $1 \leq i \leq n$ ، وهذا يبين أن المجموعة X مستقلة.

3- 4- واضح.

5- لنفرض أن المجموعة X مرتبطة عندئذ توجد في X مجموعة جزئية منتهية ولتكن $\{x_i\}_{i=1}^n \subset X$ مرتبطة، وبالتالي توجد العناصر $\{\alpha_i\}_{i=1}^n \subset \mathbb{Z}$ تحقق أن $\sum_{i=1}^n \alpha_i x_i = 0$ عندئذ يوجد $1 \leq i \leq n$ يحقق أن $\alpha_i v_i \neq 0$ وبالتالي فإن $\alpha_i \neq 0$ ، وهذا يبين أن المجموعة $\{x_i\}_{i=1}^n$ مرتبطة خطياً، وبالتالي فإن X مرتبطة خطياً.

نتيجة.

لتكن $(G, +)$ زمرة تبديلية، لنفرض أن X مجموعة جزئية غير خالية ومنتهية من G عناصرها مغايرة للصفر، عندئذ إذا كانت المجموعة X مستقلة فليس بالضرورة أن تكون مستقلة خطياً، وإذا كانت المجموعة X مرتبطة خطياً فليس بالضرورة أن تكون مرتبطة.

تعريف. [6,4,3].

لتكن $(G, +)$ زمرة تبديلية، عندئذ نقول عن الزمرة G إنها حرة إذا وجد في G مجموعة جزئية غير خالية X مستقلة خطياً ومولدة لها، وندعو المجموعة X في هذه الحالة أساساً حراً للزمرة G .

نتيجة.

لتكن $(G, +)$ زمرة حرة، عندئذ إذا كان X أساساً حراً للزمرة G فهو أساس لها، لكن العكس غير صحيح بالضرورة.

مبرهنة 1.11. [6,3].

لتكن $(G, +)$ زمرة تبديلية، ولنفرض أن X مجموعة جزئية غير خالية من G ، عندئذ تشكل المجموعة X أساساً حراً للزمرة G إذا وفقط إذا كان كل عنصر $x \in G$ يكتب بدلالة عناصر مجموعة جزئية منتهية من عناصر المجموعة X وبطريقة وحيدة.

مبرهنة 1.12. [6,3].

لتكن $(G, +)$ زمرة تبديلية، عندئذ تكون الزمرة G حرة إذا وفقط إذا كانت مجموعاً مباشراً لزمير جزئية دوارة غير منتهية منها.

مبرهنة 1.13. [6,3].

لتكن $(G, +)$ زمرة تبديلية حرة، ولنفرض أن X, Y أساسين حرين مختلفين لها، عندئذ فإن $card(X) = card(Y)$.

ملاحظة.

لتكن $(G, +)$ زمرة تبديلية، ولنفرض أن X, Y أساسين مختلفين لها، عندئذ ليس بالضرورة أن يكون $card(X) = card(Y)$ ، فضلاً عن ذلك إذا كان X أساساً للزمرة G ، عندئذ أيّاً كان $x \in G$ فإن x يكتب بدلالة عناصر مجموعة جزئية منتهية من عناصر المجموعة X لكن ليس بالضرورة أن تكون هذه الكتابة وحيدة.

مبرهنة 1.14.

لتكن $(G, +)$ زمرة تبديلية حرة، ولنفرض أن X أساساً حراً للزمرة G ، عندئذ أيّاً كان العنصرين $x, y \in X$ فإن $x \notin \langle y \rangle, y \notin \langle x \rangle$.

البرهان. واضح.

2- المجموعة المولدة الصغرى لزمرة تبديلية.

نعرض في هذه الفقرة مفهوم المجموعة المولدة الصغرى لزمرة تبديلية وأهم المبرهنات المتعلقة بهذا المفهوم، فضلاً عن النتائج التي تم التوصل لها، والبداية مع التعريف الآتي:

تعريف. [5,1].

لتكن $(G, +)$ زمرة تبديلية، لنفرض أن X مجموعة جزئية غير خالية من G ، عندئذ نقول عن X إنها S -مستقلة إذا كان $x \notin \langle X \setminus \{x\} \rangle$ وذلك أيًا كان $x \in X$.

مبرهنة. 2.1.

لتكن $(G, +)$ زمرة تبديلية، لنفرض أن X مجموعة جزئية غير خالية من G ، عندئذ فإن X تكون S -مستقلة إذا وفقط إذا كانت كل مجموعة جزئية غير خالية ومنتهية منها S -مستقلة.

البرهان. واضح.

مبرهنة. 2.2.

لتكن $(G, +)$ زمرة تبديلية، لنفرض أن X مجموعة جزئية غير خالية من G ، عندئذ تكون القضيتان الآتيتان متكافئتين:

1- المجموعة X هي S -مستقلة.

2- أيًا كانت $\{\alpha_i\}_{i=1}^n \subset \mathbf{Z}, \{x_i\}_{i=1}^n \subseteq X$ والتي تحقق أن $\sum_{i=1}^n \alpha_i x_i = 0$ فإن $\alpha_i \neq \pm 1$

لأجل كل $1 \leq i \leq n$.

البرهان.

(1) \Leftarrow (2). لنفرض أن X هي S -مستقلة وأن $\{x_i\}_{i=1}^n \subseteq X$ ، لتكن $\{\alpha_i\}_{i=1}^n \subset \mathbf{Z}$

تحقق أن $\sum_{i=1}^n \alpha_i x_i = 0$ ولنفرض جلاً أنه يوجد دليل $1 \leq j \leq n$ بحيث إن $\alpha_j = \pm 1$ ،

عندئذ نجد أنَّ $x_j \in \langle X \setminus \{x_j\} \rangle$ وهذا يناقض كون المجموعة X هي S -مستقلة، ومنه
الفرض الجدلي خاطئ وبالتالي $\alpha_i \neq \pm 1$ لأجل كل $1 \leq i \leq n$.
(1) \Leftrightarrow (2).

نفرض أنَّ (2) محققة، ولنفرض جدلاً أنَّ X ليست S -مستقلة وبالتالي يوجد عنصر
 $x \in X$ بحيث إنَّ $x \in \langle X \setminus \{x\} \rangle$ ومنه يوجد $\{\alpha_i\}_{i=1}^n \subset \mathbb{Z}, \{x_i\}_{i=1}^n \subseteq X$ بحيث أنَّ
 $\sum_{i=1}^n \alpha_i x_i = x$ وبالتالي:

$$\sum_{i=1}^n \alpha_i x_i + (-x) = \sum_{i=1}^n (-\alpha_i) x_i + x = 0$$

وهذا يناقض الفرض (2). ومنه الفرض الجدلي خاطئ وبالتالي المجموعة X هي S -
مستقلة.

نتيجة.

لتكن $(G, +)$ زمرة تبديلية، لنفرض أنَّ X مجموعة جزئية غير خالية من G ، عندئذ فإنَّ
 X تكون S -مستقلة إذا وفقط إذا تحقق الشرط:

أيّاً كان $x \in X$ وكانت العناصر $\{\alpha_i\}_{i=1}^n \subset \mathbb{Z}, \{x_i\}_{i=1}^n \subseteq X$ التي تحقق أنَّ
 $\sum_{i=1}^n \alpha_i x_i = x$ فإنَّ $x \in \{x_i\}_{i=1}^n$.

مبرهنة 2.3.

لتكن $(G, +)$ زمرة تبديلية، لنفرض أنَّ X مجموعة جزئية غير خالية من G ، عندئذ إذا كانت
المجموعة X مستقلة فإنها تكون S -مستقلة.

البرهان.

نفرض أنَّ المجموعة X مستقلة وبالتالي فإن جميع عناصرها مغايرة للصفر، لنفرض جدلاً
أنَّ المجموعة X ليست S -مستقلة وبالتالي يوجد $x \in X$ بحيث إنَّ $x \in \langle X \setminus \{x\} \rangle$ ومنه

يوجد $\{\alpha_i\}_{i=1}^n \subset \mathbf{Z}, \{x_i\}_{i=1}^n \subset X \setminus \{x\}$ بحيث إن $\sum_{j=1}^n \alpha_j x_j = x$ وبالتالي
 $-x + \sum_{j=1}^n \alpha_j x_j = 0$ ، بما إن المجموعة X مستقلة فإن $\alpha_j x_j = 0$ لكل $1 \leq j \leq n$ و
 $-x = 0$ ومنه $x = 0$ وهذا تناقض. ومنه الفرض الجدلي خاطئ وبالتالي المجموعة X هي
 S -مستقلة.

نتيجة.

- لتكن $(G, +)$ زمرة تبديلية، لنفرض أن X مجموعة جزئية غير خالية من G ، عندئذ فإن:
- 1- إذا كانت المجموعة X مستقلة خطياً فإنها تكون S -مستقلة.
 - 2- إذا كانت المجموعة X هي S -مستقلة فليس بالضرورة أن تكون مستقلة.
 - 3- إذا كان $0 \in X$ فإن المجموعة X ليست S -مستقلة.
 - 4- أياً كان $g \in G$ فإن المجموعة $\{g\}$ هي S -مستقلة.

تعريف. [3,2,1].

لتكن $(G, +)$ زمرة تبديلية، لنفرض أن X مجموعة جزئية غير خالية من G ، عندئذ نقول
 إن X مجموعة مولدة صغرى للزمرة G إذا كانت S -مستقلة وكان $G = \langle X \rangle$.

مبرهنة. 2.4.

لتكن $(G, +)$ زمرة تبديلية (حرة)، لنفرض أن X أساساً (أساساً حراً) للزمرة G ، عندئذ فإن
 مجموعة مولدة صغرى للزمرة G .

البرهان. ينتج مباشرة عن المبرهنة. 2.3. والنتيجة الأخيرة.

نتيجة.

- لتكن $(G, +)$ زمرة تبديلية (حرة)، لنفرض أن X مجموعة جزئية غير خالية من G ، عندئذ
 فإن:
- 1- إذا كانت X أساساً (أساساً حراً) للزمرة G فإنها تكون مولدة صغرى للزمرة G .

2- إذا كانت X مجموعة مولدة صغرى للزمرة G فليس بالضرورة أن تكون أساساً (أساساً حراً) للزمرة G .

مثال 1.

إن $(\square, +)$ زمرة حرة، وإن المجموعة $\{1\}$ تشكل أساساً حراً لها وبالتالي فهي مجموعة مولدة صغرى، من جهة أخرى نلاحظ أن المجموعة $\{6, 10, 15\}$ تشكل مجموعة مولدة صغرى ولا تشكل أساساً حراً لها، فضلاً عن ذلك نلاحظ أنه أي $x \in \square$ فإن:

$$x = (x)10 + (x)15 + (-4x)6$$

$$x = (x)10 + (-x)15 + (x)6$$

مثال 2.

نعلم أن الزمرة (U_{15}, \cdot) هي زمرة تبديلية غير دوارة، إن $\{7, 8\}$ مجموعة مولدة صغرى للزمرة U_{15} لكنها ليست أساساً لها، من جهة أخرى إن $\{7, 11\}$ تشكل أساساً للزمرة وبالتالي هي مجموعة مولدة صغرى لها.

نتيجة.

لتكن $(G, +)$ زمرة تبديلية، لنفرض أن X مجموعة مولدة صغرى للزمرة G ، عندئذ أي $x \in G$ فإن x يكتب بدلالة عناصر مجموعة جزئية منتهية من عناصر المجموعة X لكن ليس بالضرورة أن تكون هذه الكتابة وحيدة.

مبرهنة 2.5.

لتكن $(G, +)$ زمرة تبديلية، ولنفرض أن X مجموعة جزئية غير خالية من G ، عندئذ الشرط اللازم والكافي حتى تكون المجموعة X مجموعة مولدة صغرى للزمرة G هو أن تكون X مجموعة مولدة للزمرة G وأن لا تحوي مجموعة جزئية فعلية مولدة للزمرة G .

البرهان.

(\Leftarrow) لتكن X مجموعة جزئية غير خالية من G ، ولنفرض أن X مجموعة مولدة صغرى للزمرة G . لنفرض جلاً أنه توجد مجموعة جزئية $X_1 \subset X$ تحقق أن $\langle X_1 \rangle = G$ ، عندئذ

يوجد عنصر $x \in X$ بحيث إن $x \notin X_1$ ، عندئذ $x \in \langle X_1 \rangle \subseteq \langle X \setminus \{x\} \rangle$ ، أي إن $x \in \langle X \setminus \{x\} \rangle$ وهذا يبين أن المجموعة X ليست مولدة صغرى للزمرة G ، لأنها ليست S -مستقلة وهذا تناقض، وبالتالي الفرض الجدلي خاطئ، أي إن X_1 ليست مولدة للزمرة G ، وبالتالي المجموعة X لا تحوي أي مجموعة جزئية فعلية مولدة للزمرة G .

(\Rightarrow) لتكن X مجموعة جزئية غير خالية من G ، ولنفرض أن X مجموعة مولدة للزمرة G ولا تحوي أي مجموعة جزئية فعلية تولد الزمرة G ، وبالتالي أياً كان $x \in X$ فإن $x \notin \langle X \setminus \{x\} \rangle$ وبالتالي المجموعة X هي S -مستقلة، وبالتالي المجموعة X مولدة صغرى للزمرة G .

مبرهنة 2.6.

لتكن $(G, +), (\bar{G}, \cdot)$ زميرتين تبديليتين، ولنفرض أن $f: G \rightarrow \bar{G}$ تماثلاً زمرياً، عندئذ إذا كانت X مجموعة مولدة صغرى للزمرة G فإن $f(X)$ هي مجموعة مولدة صغرى للزمرة \bar{G} .

البرهان.

ليكن $f: G \rightarrow \bar{G}$ تماثلاً زمرياً من الزمرة G إلى الزمرة \bar{G} ولنفرض أن X مجموعة مولدة صغرى للزمرة G ، عندئذ بما أن $G = \langle X \rangle$ فإن $\bar{G} = \langle f(X) \rangle$.

لنفرض جدلاً أن المجموعة $f(X)$ ليست S -مستقلة عندئذ فإنه يوجد عنصر $y \in f(X)$ يحقق أن $y \in \langle f(X) \setminus \{y\} \rangle$ وبالتالي توجد عناصر α_i حيث $\{\alpha_i\}_{i=1}^n \subset \mathbb{Z}, \{y_i\}_{i=1}^n \subseteq f(X) \setminus \{y\}$ $y = \prod_{i=1}^n (y_i)^{\alpha_i}$ ، كما أنه يوجد $\{x_i\}_{i=1}^n \subseteq X, x \in X$ تحقق أن $y_i = f(x_i)$ وذلك لأجل كل $1 \leq i \leq n$ وأن $y = f(x)$ ، وبالتالي فإن:

$$y = f(x) = \prod_{i=1}^n (y_i)^{\alpha_i} = \prod_{i=1}^n (f(x_i))^{\alpha_i} = f\left(\sum_{i=1}^n \alpha_i x_i\right)$$

وهذا يكافئ أن:

$$f\left(-x + \sum_{i=1}^n \alpha_i x_i\right) = 0$$

وبما أن f تماثلاً زمرياً فإن $-x + \sum_{i=1}^n \alpha_i x_i = 0$ وبالتالي $x = \sum_{i=1}^n \alpha_i x_i$ وبما أن X هي S -مستقلة فإن $x \in \{x_i\}_{i=1}^n$ وبالتالي فإن $y \in \{y_i\}_{i=1}^n$ وهذا تناقض وبالتالي فإن الفرض الجدلي خاطئ والمجموعة $f(X)$ هي S -مستقلة، أي إن $f(X)$ مجموعة مولدة صغرى للزمرة \bar{G} .

مبرهنة 2.7.

لتكن $(G, +), (\bar{G}, \cdot)$ زمريتين تبديليتين، ولنفرض أن X مجموعة مولدة صغرى للزمرة G وأن Y مجموعة مولدة صغرى للزمرة \bar{G} ، عندئذ فإن المجموعة $Z = (X \times \{0\}) \cup (\{0\} \times Y)$ مولدة صغرى للزمرة الجداء المباشر $G \times \bar{G}$.

البرهان.

واضح أن المجموعة Z مولدة للزمرة $G \times \bar{G}$. ليكن $(x, y) \in Z$ حيث إن $x \in X, y \in Y$ عندئذ طالما أن X, Y مجموعات S -مستقلة فإن $\langle X \setminus \{x\} \rangle, y \notin \langle Y \setminus \{y\} \rangle$ وبالتالي:

$$(x, 0) \notin \langle (X \times \{0\}) \setminus \{(x, 0)\} \rangle, (0, y) \notin \langle (\{0\} \times Y) \setminus \{(0, y)\} \rangle$$

ومنه فإن $\langle Z \setminus \{(x, y)\} \rangle \neq (x, y)$ ، وبالتالي Z هي مجموعة S -مستقلة.

3- المجموعات المولدة الصغرى لبعض الزمر التبديلية الشهيرة.

في هذه الفقرة سنقوم بدراسة وجود المجموعات المولدة الصغرى لزمرة الأعداد الصحيحة بالمقاس n ضمن عدة حالات، فضلاً عن دراسة وجود مجموعات مولدة صغرى للزمر التبديلية الحرة بحيث لا تشكل أساساً حراً لها، بالإضافة لعدد من المبرهنات والنتائج الهامة، والبدائية مع المبرهنة الآتية:

مبرهنة 3.1.

ليكن p عدداً أولياً و n عدداً صحيحاً موجباً، ولنفرض أن $(Z_{p^n}, +)$ زمرة الأعداد الصحيحة بالمقاس p^n ، ولنفرض أن X مجموعة مولدة صغرى للزمرة Z_{p^n} عندئذ فإن $Card(X) = 1$.

البرهان.

ليكن $x \in Z_{p^n}$ عنصراً مغايراً للصفر وأولي مع p ، عندئذ فإن $\langle x \rangle = Z_{p^n}$ ، فضلاً عن ذلك المجموعة $\{x\}$ هي S -مستقلة وبالتالي فإن $\{x\}$ مجموعة مولدة صغرى للزمرة Z_{p^n} .
لنفرض جدلاً أن X مجموعة مولدة صغرى للزمرة Z_{p^n} وأن $Card(X) > 1$ عندئذ فإن $0 \notin X$ ، ونميز حالتين:

الحالة الأولى: إذا كان أحد عناصر المجموعة X أولي مع p وليكن x_0 عندئذ فإن $\{x_0\}$ مجموعة مولدة صغرى للزمرة Z_{p^n} وهذا يناقض كون المجموعة X مولدة صغرى للزمرة Z_{p^n} .

الحالة الثانية: كل عناصر المجموعة X ليست أولية مع p ولنفرض أن d هو القاسم المشترك الأكبر لعناصر المجموعة X ، وبالتالي فإن $\langle d \rangle = \langle X \rangle$ ، من جهة أخرى إن p يقسم d وبالتالي $\langle d \rangle \neq Z_{p^n}$ ، وهذا يتناقض مع كون المجموعة X مجموعة مولدة صغرى للزمرة Z_{p^n} .

مما سبق نجد أنه إذا كانت X مجموعة مولدة صغرى للزمرة Z_p فإن $Card(X) = 1$.

نتيجة.

ليكن p عدداً أولياً و n عدداً صحيحاً موجباً، ولنفرض أن $(Z_{p^n}, +)$ زمرة الأعداد الصحيحة بالمقاس p^n ، عندئذ تكون المجموعة $\{a\}$ مولدة صغرى للزمرة Z_{p^n} إذا وفقط إذا كان $a \in Z_{p^n}$ أولياً مع p .

مبرهنة 3.2.

ليكن p, q عدداً أوليان و n, m عدداً صحيحان موجبان، ولنفرض أن $(Z_{p^n q^m}, +)$ زمرة الأعداد الصحيحة بالمقاس $p^n q^m$ ، ولنفرض أن X مجموعة مولدة صغرى للزمرة $Z_{p^n q^m}$ عندئذ القضايا الآتية صحيحة:

$$Card(X) \leq 2 - 1$$

2- لتكن $a, b \in Z_{p^n q^m}$ ، عندئذ تكون المجموعة $\{a, b\}$ مولدة صغرى للزمرة $Z_{p^n q^m}$ إذا وفقط إذا كان a, b ليسا أوليان مع pq و $d = \gcd(a, b)$ أولي pq .

3- لتكن $a, b \in Z_{p^n q^m}$ ، ولنفرض أن $o(a) = p^n, o(b) = q^m$ عندئذ تكون المجموعة $X = \{a, b\}$ مولدة صغرى للزمرة $Z_{p^n q^m}$.

البرهان.

1- ليكن $x \in Z_{p^n q^m}$ عنصراً أولياً مع pq ، عندئذ فإن $\langle \{x\} \rangle = Z_{p^n q^m}$ ، فضلاً عن ذلك

المجموعة $\{x\}$ هي S -مستقلة وبالتالي فإن $\{x\}$ مجموعة مولدة صغرى للزمرة $Z_{p^n q^m}$.

نعلم أن $Z_{p^n q^m} \cong Z_{p^n} \times Z_{q^m}$ وبالتالي يوجد $f: Z_{p^n} \times Z_{q^m} \rightarrow Z_{p^n q^m}$ تماثلاً زمرياً من

الزمرة $Z_{p^n} \times Z_{q^m}$ إلى الزمرة $Z_{p^n q^m}$ ، ولنفرض أن X, Y مجموعات مولدة صغرى للزمر

Z_{p^n}, Z_{q^m} على الترتيب، عندئذ $Card(X) = Card(Y) = 1$ وذلك حسب المبرهنة 3.1،

كما أن $Z = (X \times \{0\}) \cup (\{0\} \times Y)$ مولدة صغرى للزمرة $Z_{p^n} \times Z_{q^m}$ وذلك حسب المبرهنة

2.6، ونلاحظ أنَّ $Card(Z) = 2$ ، ومنه حسب المبرهنة 2.5 فإنَّ المجموعة $f(Z)$ مولدة صغرى للزمرة $Z_{p^n q^m}$ ، وإنَّ $Card(f(Z)) = 2$.

لنفرض جدلاً أنَّ الزمرة $Z_{p^n q^m}$ تملك مجموعة مولدة صغرى X_1 تحقق أنَّ $Card(X_1) > 2$ وبالتالي فإنَّ الزمرة $Z_{p^n} \oplus Z_{q^m}$ تملك مجموعة مولدة صغرى Z_1 تحقق أنَّ $Card(Z_1) > 2$ وذلك لأنَّ $Z_{p^n q^m} \cong Z_{p^n} \oplus Z_{q^m}$ ، وهذا غير ممكن وبالتالي إذا كانت X_1 مجموعة مولدة صغرى للزمرة $Z_{p^n q^m}$ فإنَّ $Card(X_1) \leq 2$.

2- (\Leftarrow) لنفرض أنَّ المجموعة $\{a, b\}$ مولدة صغرى للزمرة $Z_{p^n q^m}$ ، عندئذ تكون المجموعة $\{a, b\}$ مولدة للزمرة $Z_{p^n q^m}$ وبالتالي فإنَّ $d = \gcd(a, b)$ أولي مع pq ، لنفرض جدلاً أنَّ واحد على الأقل من a, b أولي مع pq وليكن a عندئذ $\langle a \rangle = Z_{p^n q^m}$ وبالتالي المجموعة $\{a, b\}$ ليست S -مستقلة، وبالتالي a, b أوليان مع pq . (\Rightarrow) ليكن $a, b \in Z_{p^n q^m}$ ولنفرض أنَّ a, b ليسا أوليان مع pq و $d = \gcd(a, b)$ أولي pq ، عندئذ $\langle \{a, b\} \rangle = \langle d \rangle = Z_{p^n q^m}$ ، لنفرض جدلاً أنَّ المجموعة $\{a, b\}$ ليست S -مستقلة ولنفرض أنَّ $a \in \langle \{b\} \rangle$ ومنه فإنَّ:

$$\langle \{a\} \rangle \subseteq \langle \{b\} \rangle = \langle \{a, b\} \rangle = Z_{p^n q^m}$$

وهذا يعني أنَّ b أولي مع pq وهذا تناقض، ومنه فإنَّ المجموعة $\{a, b\}$ هي S -مستقلة، وهذا يبين أنَّ المجموعة $\{a, b\}$ مولدة صغرى للزمرة $Z_{p^n q^m}$.

3- لنفرض أنَّ $o(a) = p^n, o(b) = q^m$. بما أنَّ $(\langle \{a, b\} \rangle : 1)$ تقبل القسمة على كل من p^n, q^m فإنَّ $Z_{p^n q^m} = \langle \{a, b\} \rangle$. من جهة أخرى بما أنَّ $\gcd(o(a), o(b)) = 1$ فإنَّ $\langle \{a\} \rangle \cap \langle \{b\} \rangle = \{0\}$ ، وهذا يبين أنَّ $Z_{p^n q^m} = \langle \{a\} \rangle \times \langle \{b\} \rangle$ ومنه فإنَّ المجموعة $\{a, b\}$ مستقلة، وحسب المبرهنة 2.3، فإنَّ المجموعة $\{a, b\}$ هي S -مستقلة، مما سبق نجد أنَّ المجموعة $\{a, b\}$ مولدة صغرى للزمرة $Z_{p^n q^m}$.

مبرهنة 3.3.

لتكن p, q, r أعداداً أولية مختلفة و n, m, t أعداداً صحيحة موجبة، ولنفرض أن $(Z_{p^n q^m r^t}, +)$ زمرة الأعداد الصحيحة بالمقاس $p^n q^m r^t$ ، ولنفرض أن X مجموعة مولدة صغرى للزمرة $Z_{p^n q^m r^t}$ عندئذ القضايا الآتية صحيحة:

$$1- \text{Card}(X) \leq 3.$$

2- ليكن $a, b \in Z_{p^n q^m r^t}$ ، عندئذ تكون المجموعة $\{a, b\}$ مولدة صغرى للزمرة $Z_{p^n q^m r^t}$ إذا وفقط إذا كان a, b ليسا أوليان مع pqr و $d = \gcd(a, b)$ أولي pqr .

3- ليكن $a, b, c \in Z_{p^n q^m r^t}$ ، عندئذ إذا كان $o(a) = p^n, o(b) = q^m, o(c) = r^t$ فإن المجموعة $X = \{a, b, c\}$ مولدة صغرى للزمرة $Z_{p^n q^m r^t}$.

البرهان.

1- نعلم أن $Z_{p^n q^m r^t} \cong Z_{p^n q^m} \times Z_{r^t}$ وبالتالي يوجد $f: Z_{p^n q^m} \times Z_{r^t} \rightarrow Z_{p^n q^m r^t}$ تماثلاً زمرياً من الزمرة $Z_{p^n q^m} \times Z_{r^t}$ إلى الزمرة $Z_{p^n q^m r^t}$ ، ولنفرض أن X, Y مجموعات مولدة صغرى للزمر $Z_{p^n q^m}, Z_{r^t}$ على الترتيب، عندئذ $\text{Card}(Y) = 1$ وذلك حسب المبرهنة 3.1، و $\text{Card}(X) \leq 2$ وذلك حسب المبرهنة 3.2، وبالتالي فإن $\text{Card}(X_1) \leq 3$.

2- (\Leftarrow) لنفرض أن المجموعة $\{a, b\}$ مولدة صغرى للزمرة $Z_{p^n q^m r^t}$ ، عندئذ تكون المجموعة $\{a, b\}$ مولدة للزمرة $Z_{p^n q^m r^t}$ وبالتالي فإن $d = \gcd(a, b)$ أولي pqr ، لنفرض جـداً أن a, b واحد على الأقل من a, b أولي مع pqr وليكن a عندئذ $\langle a \rangle = Z_{p^n q^m r^t}$ وبالتالي $\langle b \rangle \subseteq \langle a \rangle$ والمجموعة a, b ليست S -مستقلة، وبالتالي a, b أوليان مع pqr .

(\Rightarrow) ليكن $a, b \in Z_{p^n q^m r^t}$ ولنفرض أن a, b ليسا أوليان مع pqr و $d = \gcd(a, b)$ أولي pqr ، عندئذ $\langle a, b \rangle = \langle d \rangle$ ، لنفرض جـداً أن المجموعة $\{a, b\}$ ليست S -مستقلة ولنفرض أن $a \in \langle b \rangle$ ومنه فإن:

$$\langle \{a\} \rangle \subseteq \langle \{b\} \rangle = \langle \{a, b\} \rangle = Z_{p^n q^m r^t}$$

وهذا يعني أنَّ b أولي مع pqr وهذا تناقض، ومنه فإنَّ المجموعة $\{a, b\}$ هي S -مستقلة، وبالتالي تكون المجموعة $\{a, b\}$ مجموعة مولدة صغرى للزمرة $Z_{p^n q^m r^t}$.

3- لنفرض أنَّ $o(a) = p^n, o(b) = q^m, o(c) = r^t$. بما أنَّ $(\langle \{a, b, c\} \rangle : 1)$ تقبل القسمة على كل من p^n, q^m, r^t فإنَّ $Z_{p^n q^m r^t} = \langle \{a, b, c\} \rangle$. من جهة أخرى بما أنَّ $\gcd(o(a), o(b), o(c)) = 1$ فإنَّ $\langle \{a\} \rangle \cap \langle \{b\} \rangle \cap \langle \{c\} \rangle = \{0\}$ ، وهذا يبين أنَّ $Z_{p^n q^m r^t} = \langle \{a\} \rangle \times \langle \{b\} \rangle \times \langle \{c\} \rangle$ ومنه فإنَّ المجموعة $\{a, b, c\}$ مستقلة، وحسب المبرهنة 2.3، فإنَّ المجموعة $\{a, b, c\}$ هي S -مستقلة، مما سبق نجد أنَّ المجموعة $\{a, b, c\}$ مولدة صغرى للزمرة $Z_{p^n q^m r^t}$.

مبرهنة 3.4.

لتكن $(Z_n, +)$ زمرة الأعداد الصحيحة بالمقاس n حيث إنَّ n يقبل القسمة على عددين أوليين مختلفين على الأقل، ولنفرض أنَّ X مجموعة جزئية من الزمرة Z_n . عندئذ القضايا الآتية صحيحة:

- 1- إذا كانت $X = \{x_1, x_2\}$ عندئذ تكون المجموعة X مولدة صغرى إذا وفقط إذا كان $\gcd(x_1, x_2) = d$ أولي مع n و x_1, x_2 ليست أولية مع n .
- 2- إذا كانت $X = \{x_1, x_2, \dots, x_m\}$ حيث إنَّ $m > 2$ ، ولنفرض أنَّ $x_i \in X$ حيث إنَّ $1 \leq i \leq n$ وأن $\gcd(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_m) = d_i$ ، عندئذ تكون المجموعة X مولدة صغرى إذا وفقط إذا كان $\gcd(x_1, x_2, \dots, x_m) = d$ أولي مع n و x_1, x_2, \dots, x_m ليست أولية مع n وكان d_i لا يقسم x_i لكل $1 \leq i \leq n$.

البرهان.

- 1- (\Leftarrow) لنفرض أنَّ المجموعة X مولدة صغرى للزمرة Z_n ، عندئذ تكون المجموعة $\{x_1, x_2\}$ مولدة للزمرة Z_n وبالتالي فإن $d = \gcd(x_1, x_2)$ أولي مع n ، لنفرض جدلاً أنَّ واحد على الأقل

من x_1, x_2 أولي مع n وليكن x_1 عندئذ $\langle x_1 \rangle \subseteq \langle x_2 \rangle = Z_n$ وبالتالي المجموعة $\{a, b\}$ ليست S -مستقلة، وبالتالي x_1, x_2 أوليان مع n .
(\Rightarrow) ليكن $x_1, x_2 \in Z_n$ ولنفرض أن x_1, x_2 ليسا أوليان مع n و $d = \gcd(x_1, x_2)$ أولي مع n ، عندئذ $\langle d \rangle = Z_n$ ، لنفرض جـداً أن المجموعة $\{x_1, x_2\}$ ليست S -مستقلة ولنفرض أن $x_1 \in \langle x_2 \rangle$ ومنه فإن $\langle x_1 \rangle \subseteq \langle x_2 \rangle = \langle \{x_1, x_2\} \rangle = Z_n$ وهذا يعني أن x_2 أولي مع n وهذا تناقض، ومنه فإن x_1, x_2 هي S -مستقلة، وبالتالي تكون المجموعة $\{x_1, x_2\}$ مولدة صغرى للزمرة Z_n .

2- (\Leftarrow) لنفرض أن المجموعة X مولدة صغرى للزمرة Z_n ، ولنفرض جـداً أن d ليس أولي مع n و بما أن $\langle X \rangle = \langle d \rangle = Z_n$ وهذا غير ممكن ومنه d أولي مع n ، من جهة أخرى إذا كان أحد عناصر المجموعة X وليكن x_i أولياً مع n فإن $\langle x_i \rangle = Z_n$ وهذا يناقض كون المجموعة X هي S -مستقلة.
لنفرض جـداً أن d_i يقسم x_i ومنه $x_i \in \langle d_i \rangle$ وبالتالي $x_i \in \langle X / \{x_i\} \rangle$ وهذا يناقض كون المجموعة X هي S -مستقلة و d_i لا يقسم x_i لكل $1 \leq i \leq n$.

(\Rightarrow) بما أن d أولي مع n ، فإن $\langle d \rangle = \langle X \rangle = Z_n$ ، من جهة أخرى بما أن كل عناصر المجموعة X ليست أولية مع n فإن X لا تحوي عنصراً مولداً للزمرة Z_n ، لنفرض جـداً أن المجموعة X ليست S -مستقلة أي إنه يوجد $x_i \in X$ بحيث إن $x_i \in \langle X / \{x_i\} \rangle$ ومنه فإن $x_i \in \langle d_i \rangle$ ، عندئذ يوجد $\alpha \in \mathbb{Z}$ بحيث $x_i = \alpha d_i$ وهذا يناقض كون d_i لا يقسم x_i ، وبالتالي الفرض الجدلي خاطئ، أي إن المجموعة X هي S -مستقلة وبالتالي المجموعة X مجموعة مولدة صغرى للزمرة Z_n .

من المبرهنات السابقة، نلاحظ أن المجموعات المولدة الصغرى للزمرة Z_n في حالة كان $n \geq 2$ ليست متساوية القدرة، في المبرهنة الآتية نبين أكبر قدرة ممكنة لمجموعة مولدة الصغرى للزمرة Z_n حيث $n \geq 2$:

مبرهنة 3.5.

لتكن الزمرة $(Z_n, +)$ زمرة الأعداد الصحيحة بالمقاس n و X مجموعة جزئية من الزمرة Z_n . ولنفرض أن $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$ حيث إن p_1, p_2, \dots, p_t أعداد أولية مختلفة و $\alpha_1, \alpha_2, \dots, \alpha_t$ أعداد صحيحة موجبة تماماً، عندئذ إذا كانت المجموعة X مولدة صغرى للزمرة Z_n فإن $\text{card}(X) \leq t$.

البرهان.

لنفرض أن المجموعة X مولدة صغرى للزمرة Z_n وإن $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$ حيث إن p_1, p_2, \dots, p_t أعداد أولية مختلفة و $\alpha_1, \alpha_2, \dots, \alpha_t$ أعداد صحيحة موجبة تماماً، سنورد البرهان بالاستقراء حسب t :

حسب المبرهنات 3.1، 3.2، 3.3 نجد أن المبرهنة صحيحة لأجل $t \in \{1, 2, 3\}$.

- لنفرض أن المبرهنة صحيحة لأجل $t-1$ ، أي لنفرض أنه لأجل $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_{t-1}^{\alpha_{t-1}}$ فإنه إذا كانت المجموعة X مولدة صغرى للزمرة Z_n فإن:

$$\text{card}(X) \leq t-1$$

- لأجل $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$ ، نعلم أن:

$$Z_n \cong Z_{p_1^{\alpha_1} \dots p_{t-1}^{\alpha_{t-1}}} \times Z_{p_t^{\alpha_t}}$$

وبالتالي يوجد:

$$f: Z_{p_1^{\alpha_1} \dots p_{t-1}^{\alpha_{t-1}}} \times Z_{p_t^{\alpha_t}} \rightarrow Z_n$$

تماثلاً زمرياً من الزمرة $Z_{p_1^{\alpha_1} \dots p_{t-1}^{\alpha_{t-1}}} \times Z_{p_t^{\alpha_t}}$ إلى الزمرة Z_n ، ولنفرض أن X_1, Y مجموعات مولدة صغرى للزمر $Z_{p_1^{\alpha_1} \dots p_{t-1}^{\alpha_{t-1}}}$ ، $Z_{p_t^{\alpha_t}}$ على الترتيب، عندئذ $\text{Card}(Y) = 1$ وذلك حسب المبرهنة 3.1، و $\text{Card}(X_1) \leq t-1$ وذلك حسب الفرض الاستقرائي، وبالتالي فإن $\text{Card}(X) \leq t$.

مثال 3.

لتكن $(Z_{16}, +)$ زمرة الأعداد الصحيحة بالمقاس $16 = 2^4$ ، وبالتالي أي مجموعة مولدة صغرى للزمرة Z_{16} تكون مؤلفة فقط من عنصر واحد.

مثال 4.

لتكن $(Z_{210}, +)$ زمرة الأعداد الصحيحة بالمقاس $210 = 2 \times 3 \times 5 \times 7$ ، وبالتالي أي مجموعة مولدة صغرى للزمرة Z_{210} تكون مؤلفة فقط من أربع عناصر على الأكثر، فعلى سبيل المثال، كل مجموعة من المجموعات الآتية:

$$X = \{70, 42, 30, 105\} \quad Y = \{10, 21, 35\}$$

$$Z_1 = \{105, 2\} \quad Z_2 = \{22, 33\} \quad E = \{13\}$$

تكون مجموعة مولدة صغرى للزمرة $(Z_{210}, +)$ ، ونلاحظ أنه لأجل المجموعة X أن:

$$o(70) = 3, o(42) = 5, o(30) = 7, o(105) = 2$$

أما المجموعة $\{35, 21, 15, 45\}$ فهي مولدة لكنها ليست مولدة صغرى لأن $\gcd(21, 15, 35) = 1$ يقسم 45.

مثال 5.

لتكن $(Z_{60}, +)$ زمرة الأعداد الصحيحة بالمقاس $60 = 2^2 \times 3 \times 5$. إن كل مجموعة من المجموعات:

$$Z = \{35, 21\}, Y = \{12, 5\}, X = \{15, 20, 12\}$$

هي مجموعة مولدة صغرى للزمرة Z_{60} ، ونلاحظ أنه لأجل المجموعة X أن:

$$o(15) = 4, o(20) = 3, o(12) = 5$$

مبرهنة 3.6.

لتكن G زمرة دوارة منتهية مرتبتها $n \geq 2$ مولدة بالعنصر $a \in G$ ، ولنفرض أنَّ:

$$X = \{x_1, x_2, \dots, x_m\}$$

مجموعة مولدة صغرى للزمرة Z_n ، عندئذٍ فإنَّ المجموعة $\{a^{x_1}, a^{x_2}, \dots, a^{x_m}\}$ مولدة صغرى للزمرة G .

البرهان.

بما أنَّ $(Z_n : 1) = (G : 1)$ فإنه يوجد $f : Z_n \rightarrow G$ تماثلاً زمرياً من الزمرة Z_n إلى الزمرة G ، معرفاً بالشكل $f(r) = a^r$ وذلك لكل $r \in Z_n$ ، ولنفرض أنَّ $X = \{x_1, x_2, \dots, x_m\}$ مجموعة مولدة صغرى للزمرة Z_n ، وبما أنَّ $f(\langle X \rangle) = \langle f(X) \rangle$ يكون $\langle f(x_1, x_2, \dots, x_m) \rangle = \langle a^{x_1}, a^{x_2}, \dots, a^{x_m} \rangle$ ولما كانت المجموعة X مجموعة مولدة صغرى للزمرة Z_n فإنَّ المجموعة $\{a^{x_1}, a^{x_2}, \dots, a^{x_m}\}$ مولدة صغرى للزمرة G وذلك حسب المبرهنة 2.5.

مبرهنة 3.7.

لتكن $(\square, +)$ زمرة الأعداد الصحيحة، ولتكن $X = \{x_1, x_2, \dots, x_m\}$ مجموعة من الأعداد الصحيحة الموجبة تماماً، ولنفرض أنَّ $\gcd(x_1, x_2, \dots, x_m) = 1$ وأنَّ $\gcd(x_1, x_2, \dots, x_{i-1}, x_{i+1}, \dots, x_m) = d_i \neq 1$ لأجل $x_i \in X$ حيث إنَّ $1 \leq i \leq m$ ، عندئذٍ تكون المجموعة $X = \{x_1, x_2, \dots, x_m\}$ مولدة صغرى للزمرة $(\square, +)$.

البرهان.

بما أنَّ $\gcd(x_1, x_2, \dots, x_m) = 1$ فإنَّ $Z = \langle X \rangle$ ، ولنفرض جدلاً أنَّ المجموعة X ليست S -مستقلة عندئذٍ يوجد $x_i \in X$ يحقق أنَّ $x_i \in \langle X / \{x_i\} \rangle$ حيث إنَّ $1 \leq i \leq m$ ومنه فإنَّ $x_i \in \langle d_i \rangle$ عندئذٍ يوجد $\alpha \in \mathbb{Z}$ بحيث $x_i = \alpha d_i$ بالتالي $\gcd(x_1, x_2, \dots, x_m) = d_i \neq 1$ هذا يناقض كون $d_i \neq 1$ وبالتالي الفرض الجدلي خاطئ أي

إن X هي مجموعة S -مستقلة، مما سبق نجد أن المجموعة X مجموعة مولدة صغرى للزمرة Z .

مبرهنة 3.7.

تكن G زمرة تبديلية حرة على المجموعة X وليكن p, q عددين أوليين مختلفين. عندئذ فإن $Z = pX \cup qX$ مجموعة مولدة صغرى للزمرة G .

البرهان.

بما أن p, q عددين أوليين مختلفين فإنه يوجد عددين $\alpha, \beta \in \mathbb{Z}$ بحيث إن $\alpha p + \beta q = 1$ ، وبالتالي أيًا كان $x \in X$ فإن $x = \alpha(px) + \beta(qx)$ ، ومنه نجد أن المجموعة Z مولدة للزمرة G .

أيًا كان $x_1, x_2 \in X$ فإن $px_1 \neq qx_2$ و $qx_1 \neq px_2$ وذلك لأن المجموعة X مستقلة خطياً، لنفرض جلاً أن المجموعة Z ليست S -مستقلة عندئذ فإنه يوجد عنصر $z \in Z$ يحقق أن $z \in \langle Z / \{z\} \rangle$ وبالتالي توجد مجموعات جزئية منتهية من العناصر:

$$\{\alpha_i\}_{i \in I} \subset \mathbb{Z}, \{z_i\}_{i \in I} \subseteq Z$$

حيث إن $z = \sum_{i \in I} \alpha_i z_i$ و $z \notin \{z_i\}_{i \in I}$ ، كما أنه يوجد $x \in X, x_i \in X$ بحيث إن:

$$z = \lambda x, z_i = \beta_i x_i; \forall i \in I$$

وإن $\lambda, \beta_i \in \{p, q\}; \forall i \in I$ ، بما أن $z \in \langle Z / \{z\} \rangle$ فإن $x \notin \{x_i\}_{i \in I}$ ، وبالتالي:

$$-\lambda x + \sum_{i \in I} (\alpha_i \beta_i) x_i = 0$$

وبما أن X مستقلة خطياً، فإن $\lambda = 0, \alpha_i \beta_i = 0; \forall i \in I$ وهذا يكافئ أن $p = 0$ أو $q = 0$ وهذا غير ممكن، وبالتالي فإن الفرض الجدلي خاطئ أي إن $z \notin \langle Z / \{z\} \rangle$ والمجموعة Z هي S -مستقلة. ومما سبق نجد أن المجموعة Z مجموعة مولدة صغرى للزمرة G .

مثال 6.

لأجل الزمرة $(\mathbb{Z}, +)$ نعلم أنَّ المجموعة $\{2\}$ تشكل أساساً حراً لها، لأجل العددين 2,3 فإنَّ $\{4,6\}$ هي مجموعة مولدة صغرى.

مبرهنة 3.8.

لتكن $(G, +)$ زمرة تبديلية حرة على المجموعة X . ولتكن p_1, p_2, \dots, p_k أعداد أولية فيما بينها متتى متتى. ولنفرض أنَّ $n = \prod_{i=1}^k p_i$ فإنَّ المجموعة:

$$M = \bigcup_{i=1}^k \left\{ \frac{n}{p_i} x \ ; x \in X \right\}$$

هي مجموعة مولدة صغرى للزمرة G .

البرهان.

لنفرض أنَّ $n = \prod_{i=1}^k p_i$ ولنعرّف المجموعة N بالشكل:

$$N = \left\{ n_i = \frac{n}{p_i} \right\}_{i=1}^k$$

من الواضح أنَّ $\gcd(n_1, n_2, \dots, n_k) = 1$ بالتالي يوجد $\alpha_1, \dots, \alpha_k \in \mathbb{Z}$ بحيث $\sum_{i=1}^k \alpha_i n_i = 1$.

من جهة أخرى فإنه لأجل كل $y \in G$ توجد عناصر $\{x_j\}_{j \in J} \subseteq X$ ، $\{\beta_j\}_{j \in J} \subseteq \mathbb{Z}$ تحقق

$$y = \sum_{j \in J} \beta_j x_j \quad \text{، وبالتالى:}$$

$$y = 1 \cdot y = \left[\sum_{i=1}^k \alpha_i n_i \right] y = \sum_{i=1}^k \sum_{j \in J} \alpha_i \beta_j n_i x_j$$

ومنه فإنَّ $y \in \langle M \rangle$ ، وهذا يبين أنَّ المجموعة M مولدة للزمرة التبديلية الحرة G .

نفرض جدلاً أنَّ المجموعة M ليست S -مستقلة، عندئذٍ ودون المساس بعمومية المسألة لنفرض أنه لأجل $n_1 \in N$ يوجد عنصر $z \in X$ بحيث إنَّ $\langle M \setminus \{n_1 z\} \rangle$ ، وبالتالي توجد مجموعات جزئية منتهية:

$$\{n_i x_j\}_{j \in J}^{1 \leq i \leq k} \subseteq M \setminus \{n_1 z\}, \{\alpha_{ij}\}_{j \in J}^{1 \leq i \leq k} \subset \square$$

تحقق أنَّ:

$$n_1 z = \sum_{j \in J, 1 \leq i \leq k} \alpha_{ij} (n_i x_j)$$

وهنا نميز الحالتين:

أولاً. إذا كان $z \notin \{x_j\}_{j \in J}$ ، عندئذٍ فإنَّ $-n_1 z + \sum_{j \in J, 1 \leq i \leq k} \alpha_{ij} (n_i x_j) = 0$ ، وبما أن المجموعة X مستقلة خطياً فإنَّ $n_1 = 0$ وهذا تناقض.

ثانياً. إذا كان $z \in \{x_j\}_{j \in J}$ ، عندئذٍ فإنَّ $n_1 z = \sum_{j \in J, 1 \leq i \leq k} \alpha_{ij} (n_i x_j)$ تكتب بالشكل:

$$\sum_{\substack{j \in J, 1 \leq i \leq k \\ x_j \neq z}} \alpha_{ij} (n_i x_j) + \sum_{j \in J, 1 \leq i \leq k} \alpha_{ij} (n_i z) - n_1 z = 0$$

وبالتالي:

$$\sum_{\substack{j \in J, 1 \leq i \leq k \\ x_j \neq z}} \alpha_{ij} (n_i x_j) + \left(\sum_{j \in J, 1 \leq i \leq k} [\alpha_{ij} n_i] - n_1 \right) z = 0$$

وبما أن المجموعة X مستقلة خطياً فإنَّ:

$$\sum_{j \in J, 1 \leq i \leq k} [\alpha_{ij} n_i] - n_1 = 0$$

وبالتالي فإنَّ:

$$n_1 = \sum_{j \in J, 1 \leq i \leq k} \alpha_{ij} n_i$$

ولما كان $\gcd(n_1, \dots, n_k) = 1$ فإن $\gcd(n_2, n_3, \dots, n_k) = 1 = p_1$ ، وهذا تناقض لأن p_1 عدد أولي.

مما سبق نجد أن الفرض الجدلي خاطئ وبالتالي المجموعة M هي S -مستقلة. ومما سبق نجد أن M هي مجموعة مولدة صغرى للزمرة G .

المراجع العلمية:

- [1]- M. Herbk and P. Ruzicka, "Characterization of Abelian Group With Minimal generating Set," *Quaestiones Mathematicae*, Vol. 38, no. 1, pp. 103-120, 2015.
- [2]- P. Ruzicka, "Abelian groups with a minimal generating set," *Quaestiones Mathematicae*, Vol. 33, no. 2, pp. 147-153, 2010.
- [3]- J. J. Rotman, *An Introduction to the Theory of Groups*, 4th ed., Springer- Verlag , New York, 1995.
- [4]- L. Fuchs, *Infinite Abelian Groups*, Vol. I, *Pure and Applied Mathematics*, Vol. 36, Academic Press, New York, 1970.
- [5]- G. Gratzner, *Universal Algebra*, D. Van Nostrand Company, Princeton, New Jersey, 1968.
- [6]- A. G. Kurosh, *The Theory of Groups*, Vols. I, II, AMS Chelsea Publishing, Providence, RI, 1960.