Proceedings of the 3rd International Conference on Computing Innovation and Applied Physics
DOI: 10.54254/2753-8818/9/20240736

Research on the sumsets of different types of group

Hang Yu

Shanghai International High School of Banz, Shanghai, 200000, China

8848@tzc.edu.cn

Abstract. In this article, author introduce the theories about the sums of sets. First the definition$X \cdot Y = \{ x_i \cdot y_j \mid x_i \in X, y_j \in Y \}$, that X, Y is a subset of group G. the first relative theorem is prove by Cauchy–Davenport. The beginning is the Kneser's theory, and then, in the second part, this paper introduces several types of sumsets, though most of them is based on abelian group (commutative group or additive group) and if not, the author gives out the definition. And the popular topic about this is the sum-free sets, but this paper will only introduce a few. Readers who want detailed prove need to look for proves on the reference articles and the theory author talked is a small part of them (important or interesting ones). In some of references, the "+" can be change to other operation which satisfy the group, so this paper changes them into ".".

Keywords: Sumsets, Kneser' Theory, Sum Of Sequence, Zero Sum, Unique Sum.

1. Introduction

When adding the two sets, there are some pairs of elements getting a same answer, so the questions are what is the biggest and smallest order of the new sets and when can use the adding of two sets to get the whole group (if it is finite) or when the adding of set do not have pairs of elements which get same element. As the oldest theorem of sumset is the Cauchy–Davenport theorem which is in group Z/p proved in about 300 years ago. Then about 1950s, Kneser proved his theorems.

The section 1 is about the basic theory. And in the section 2, it contains sum of sequence, zero sums, perfect sums, unique sums and comparing of sum and difference.

2. The basic theory

2.1. Kneser's theory

Kneser's theorem 1 and 2. $X, Y \in G$ (abelian group) are finite, non-empty. And the stabilizer of $X \cdot Y$ is denoted H, (stabilizer of S in group G is that : $= \{g_i \in G \mid S \cdot g_i = S\}$) [1]. Then it is satisfied that:

$$|X \cdot Y| \geq |X| + |Y| - |H| \quad (1)$$

The other theorem is that if $|X \cdot Y| < |X| + |Y|$, satisfying $|X \cdot Y| = |X \cdot H| + |Y \cdot H| - |H|$.

Besides, the condition of $|X + Y| = |X'| + |Y'| - 1$ is that $X' = \varphi G/H(X)$, and$Y' = \varphi G/H(Y)$, So then by the definition of canonical homomorphism, ($\varphi_{G/H}$ means the natural homomorphism of G onto the G/H which means quotient group, when H is a subgroup of G) [2].

Then there is a generalized **theorem 3**:

DOI: 10.54254/2753-8818/9/20240736

$$\Sigma_k(\mathbf{X}) = \{x_{i1} \cdot \cdots \cdot x_{ik} : 1 \le i_1 < \cdots < i_k \le m \text{ and } x_{ik} \in X_{ik} \; for \; every \; 1 \le j \le k\} \quad (2)$$

Let $\mathbf{X} = (x_1, ..., x_m)$ that all $x_i \in G$, let $k \le m$ and $H = stab(\Sigma_k(\boldsymbol{X}))$. If $\Sigma_k(\boldsymbol{X})$ is nonempty, then:

$$|\Sigma_k(\boldsymbol{X})| \ge |H|\,(1 - k + \sum_{Y \in \frac{G}{H}} \min\{k \mid \{i \in \{1, \ldots, m\} : X_i \cap Y \ne \emptyset\}\}) \quad (3)$$

When m=k=2, it become the Kneser's theorem [3].

2.2. Dyson e-transform and Kemperman's d-transformation

In this subsection, the abelian group is improved to be an arbitrary group. First, the definition of these two transforms [1].

Dyson e-transform. Assume that Y is commutative and identity element is in Y. Choosing randomly a $e \in X$ and define $X' = X \cup (e \cdot Y), Y' = Y \cap (e^{-1} \cdot X)$. Then the Dyson e-transform of X, Y is the X', Y' respectively.

Kemperman's Transformation. Assume that $X \cdot e \not\subset X$ for an $e \in X \cap Y$. Define $X_0 = \{x_0 \in X \mid x_0 \cdot e \notin X\}, Y_0 = \{y_0 \in Y \mid e \cdot y_0 \notin Y\}$. Put $m = |X_0|$ and $n = |Y_0|$. From definition we have $e \ne 0$, $0 \notin X_0$, $0 \notin Y_0$, and $p \ge 1$.

Define $X' = X \cup (x_0 \cdot e)$, $Y' = Y \backslash Y_0$, $if \; m \ge n$; or $Y' = Y \cup (e \cdot y_0)$, $X' = X \backslash X_0$, $if \; n > m$. And the Kemperman d-transform of X, Y is X', Y' respectively. With the using of these transformations, we can get these.

Theorem 4. G is an arbitrary group, $X, Y \in G$ and Y should be commutative. If existing a commutative $H \le G$ which is satisfy $X \cdot Y \cdot H = X \cdot H \cdot Y = X \cdot Y$ (by definition of the commutative), then $|X \cdot Y| > |X \cdot H| + |Y \cdot H| - |H|$ [1].

Theorem 5 (Kemperman theorem). $|X \cdot Y| \ge |X| + |Y| - |H|$, if $x_0 \in X$ and $y_0 \in Y$, and a $H \le G$ which satisfy $x_0 \cdot H \cdot y_0 \subseteq X \cdot Y$, then they are similar, but it has a different definition of H [4].

Theorem 6. S is the subset of X+Y, and if there is a $H \le G$ can satisfy either $H \cdot S = S$ (left coset) or $S \cdot H = S$ (right coset): $|S| \ge |X| + |Y| - |H|$. ($H \le G$ means H is a subgroup of G) [5].

3. Compare all types of sums and differences

3.1. The sums of element

3.1.1. $k \wedge X$. The definition assumes $X \subseteq G$ (G is an abelian group in this subsection), then $k \wedge X := \{\sum_{a \in Q} a, Q \subseteq X, |Q| = k\}$. Similarly, in [6] in definition as the form of $\sum_h(S) = \{x_{i1} \cdot \cdots \cdot x_{ih} \mid 1 \le i1 < \cdots < ih \le k\}$ and $S = (a_{i1}, \cdots, a_{ik})$ is a sequence of elements in G.

Theorem 7. Let $X \subseteq G$ be an additive set (commutative set), and assume $2 \le k \le |X| - 2$. And there is a restriction, it cannot happen together that $k \in \{2, |X| - 2\}$ and X is a 2-coset. Where $X \subseteq G$ call a 2-coset if X coset of $B \le G$ in which all non-identity elements have order 2 (elementary 2-subgroup) [5].

Then $|k \wedge X| \ge |X|$, Furthermore $|k \wedge X| > |X|$, unless two more condition: (i) X is an almost 2-coset which means after removing a single element, the set be a 2-coset. (ii) X is the union of two cosets of a subgroup of order 2.

For the proving, the author introduced the 2-sums and some lemma about it, because $x_1 + \cdots + x_{k-2} + 2 \wedge Y \subseteq k \wedge X$, when $Y \subseteq X$.

3.1.2. The minimum of $\Sigma(S)$. For $\Sigma(S) = \bigcup_{r=1}^{k} \sum_r(S)$, assume $|G| = n$, when $S = g_1 \cdot \ldots \cdot g_k = \prod g_i \in G$ $g^{vg(S)} = g^m T \in \mathcal{F}(G)$ which $g_i \in G$ and length $|S| \ge n$. If $\max\{v_g(S) \mid g \in G\} = h(T) \le m$ then $\sum_{\ge n-m}(T) = \sum_n(S)$.

Theorem 8. When S is a zero-sumfree sequence ($0 \notin \Sigma(S)$ and has only one element of order 2) and $|S| \geqslant 4$, $Supp(S) = \{g \in G \mid v_g(S) > 0\}$, then $\Sigma(S) \ge |S| + |Supp(S)| - 1$ [6].

And the most important theorem he proved is that [6] k be a positive integer. Let S has n + k elements of G. Set t = |Supp(S)|. Then either $0 \in \sum_n(S)$ or $|\sum_n(S)| \ge k + t - 1$ [6].

DOI: 10.54254/2753-8818/9/20240736

After theorem 8, the writer of [7] discussed a minimum of Σ(S) by |S|. Let G define as above and S ⊆ G \{0} a symmetric subset with |S| ≥ 5 and the Σ(S) is not periodic.

$$|\Sigma(S)| > \frac{(|S|\,(|S| - 2))}{4} + 5$$

Furthermore, if |G| is odd, it can be proved as: $|\Sigma(S)| > \frac{(|S|\,(|S|+2))}{4} + 2\xi'(S) - 1$. where $\xi'(S) = \begin{cases} 0 \;\; if \;\; \frac{|S'|^2+3|S'|}{2} \leq 2|<S>|+5 \\ 1 \;\; if \;\; \frac{|S'|^2+3|S'|}{2} > 2|<S>|+5 \end{cases}$, S' is a set that $|S'| = \frac{|S|}{2}$ and $S = S' \cup -S'$ and <S> means the generator of S. After this, the writer also introduces an Olson's method and prove |Σ(S)| > 2|S| when S ∩ (−S) = ∅ and |Σ(S)|>2|S|+1 under the condition $|\Sigma(S)| \leq \frac{|G|}{2}$ and |S| ≥ 4 [7].

3.1.3. Value of Σ (x1, x2, ..., xt). If $a_1, a_2, \ldots$, at is a sequence of group elements, let $\Sigma = \Sigma(x_1, \ldots, x_t)$, denote the sum set $\Sigma = \{0, x_1\} + \{0, x_2\} + \ldots + \{0, x_t\} = \bigcup_{r=1}^{k} \sum_r(S)$ and $S = (x_{i1}, \cdots, x_{it})$. Note that if G is not abelian, then Σ depends on the order in which the theorem is listed.

Theorem 9. Let S be a set of distinct non-zero (unit element) elements of G with order no less than 3 and the G can be generated by S. Then there is an arrangement $a_1, a_2, \ldots, a_s$ of the elements of S and an index $2 \leq p \leq s$ [8].

Then either $\Sigma(x_1, \ldots, x_{s-1})$, or (i)For all 2 ⩽t ⩽q, $|\Sigma(a_1, a_2, \ldots, a_t)| \geq 4 + [(s-2)(s+3) - (s-t)(s-t+5)] - \Delta(s)$, where O(s log s) = Δ(s) < s2/72. (ii) If q<s, then we can get $H = < x_{q+1}, \ldots, x_s > \subset G$ and $|H| < 2\,min\{|\Sigma|, |\bar{\Sigma}|\}$. $\Sigma = \Sigma(x_1, \ldots, x_q)$ and $\bar{\Sigma}$ is the complement of Σ in G.

Theorem 10. Let S as above, then there is an arrangement $a_1, a_2, \ldots, a_s$ of the elements of S, then $|\Sigma| > 1 + cs^2$, where $c = \frac{1}{8} - O\left(\frac{\log s}{s}\right) > \frac{1}{9}$ [8].

Theorem 11. Let S be a set of non-zero (unit element) elements from a finite group G of order n of size |S|≥cn1/2 and c⩾3 √2. (if p, the smallest divisor of n (though in the [7] writer uses smallest prime divisor, the meaning would not change), is greater than 2, then it can improved that $c \geq \left(\frac{(8p-2)}{(8p-9)}\right)^{\frac{1}{2}}$). Then S contains t distinct elements such that $\Sigma(x_1, x_2, \ldots, x_t) = H \leq G$. t⩾c|H|1/2, and every clement of H has at least two representations in $\Sigma(x_1, x_2, \ldots, x_t)$ [8].

3.1.4. The t-independent set. X has a t-independent set in abelian group G, if existing a sequence (x_1, x_2, …, x_m) that satisfying ($\lambda_1 x_1 + \lambda_2 x_2 + \ldots + \lambda_m x_m = 0$ and $|\lambda_1| + |\lambda_2| + \ldots + |\lambda_m| \leq t$. so now the coefficient of each element can be an integer rather than 0 or 1, but this is also relative to the zero-sum and author introduce after.

Define $Tor(G,h) = \{x \in G \mid h \cdot x = 0\}$ and $\sigma(G,t) = \sum_{h=1}^{t} |Tor(G,h)|$.

Theorem 12. If m ∈ Z and satisfy $|G| > \sigma(G,t) \cdot \binom{2m-2+t}{t}$, then there is a t-independent set of size m in group G [9].

Besides the writer also introduce the case when t=3 and weak t-independent in article.

3.2. Zero-sum

If $S = g_1 \cdot \ldots \cdot g_k = \prod_{g_i \in G} g^{vg\,(S)}$, then let $\sigma(S) = \sum_{i=1}^{k} g_i = \sum_{g \in G} v_g(S)\; g \in G$. The sequence S is zero-sum if the two condition is satisfied that σ(S) = 0 ∈ G and zero-sum free if 0 ∉ Σ(S).

Theorem 13. Let S be a zero-sum free subset of G. Then (i) if |S| = 1 or 2 , |Σ(S)|=2|S|−1; (ii) if |S| = 3 , |Σ(S)| ≥ 5; (iii) if |S| = 5 , |Σ(S)| ≥ 13; (iv) if |S| ≥ 4 , |Σ(S)| ≥ 2|S|; (v) if S contains no element of order 2, |Σ(S)| ≥ 6 [10].

DOI: 10.54254/2753-8818/9/20240736

Furthermore, let G finite cyclic group with odd order (like the Z/p Z). If $|S| \geq \frac{3|G|+13}{10}$, then for any g ∈ S with $v_g(S) \geq \frac{6|S|-|G|+1}{16}$.

3.3. Perfect sum

This section is introducing the situation of the sum of subset equal to the abelian group G. If X⊂ G is perfect s-basis, s equal to the smallest t to satisfy $\bigcup_{h=0}^{t} hX = G$. In the [11], the writer use isomorphism to analyze the situation of abelian group by the cyclic group. And in [12], readers can also find some theory about this, though it has one more restrict on the definition of perfect.

Theorem 14. If subset X ⊂ G is a perfect s-basis, then s = 1 and X = G\{0}, or $G \cong \mathbb{Z}_{s+1}$ (1, 2, …, s+1 mod s+1) and |X| = 1 [11].

Then the writer introduced two more definition. X is an additive base of order s, when all element in G can be written as exactly s terms. And if all s-terms sums are distinct, X can be called as Xs.

Theorem 15. If a subset Y ⊂ G is a Y_s set, then there are exactly two condition s = 1 and Y = G, or $G \cong \mathbb{Z}_{s+1}$ and |Y| = 2 [11].

Furthermore, writer introduce a special case of s=2, then only the group G which ≅ $\mathbb{Z}2$, $\mathbb{Z}4$, $\mathbb{Z}7$, $\mathbb{Z}_2^2$, $\mathbb{Z}_2^4$, $\mathbb{Z}_2^2 \times \mathbb{Z}4$, has a perfect restricted 2-basis.

3.4. The unique sum

X is a subset of commutative group G, if there is at least one c which only equal to one element of X+X (and because of commutative, $x_i + (-) x_j = x_j + (-) x_i$), then X has a unique sum (difference).

Theorem 16. p(G) is the smallest divisor of |G|, then for the X, Y ⊂ G, (i) if $p(G) > \sqrt[4]{12}^{|A|+|B|-2}$, X + Y has a unique sum, (ii) if $p(G) > 2|X| - 1$, X contains a unique difference and a unique sum [13].

Theorem 17. If Z ⊂ G has size |Z| ≤ $\log_2$ p(G), then Z is Freiman-isomorphic to a set of integers. Freiman-auto(iso, when it is bijection)morphism is a map φ: Y→Y' that if $y_1, y_2, y_3, y_4 \in Y$ and $y_1 + y_2 = y_3 + y_4$,then $\varphi(y_1) + \varphi(y_2) = \varphi(y_3) + \varphi(y_4)$ [13].

3.5. MSTD and MDTS

They are the abbreviation of “More Sums (Difference) Than Difference (More)”. And difference means $X - Y = \{ x_i \cdot y_j \mid x_i \in X, y_j \in Y \}$. First, in [14], they writer give out the estimated value bound of MSTD in group Z/p Z.

Theorem 18. Let $|MSTD(Z/p\,Z)| \sim \begin{cases} 3^{p/2} \\ p(\frac{1+\sqrt{5}}{2})^p/2 \end{cases}$. Let G(n) ∈G containing the elements of order n, so that |G(n)| = kn. Then the writer introduced the situation of that the G is a commutation group.

Theorem 19. When n is even, getting $k_n \cdot 3|Gn|^{2\left(1-|Gn|\cdot\frac{3(k_n+1)}{2}+\frac{|G_n|^2}{k_n}\right)\left(\frac{7}{9}\right)^{|Gn|}} \leq |MSTD(Gn)| \leq k_n \cdot 3|Gn|^{2\left(1+\frac{|G_n|}{k_n}\right)\left(\frac{7}{9}\right)^{|Gn|}}$. And when n is odd, $MSTD(G)| \sim (\frac{1+\sqrt{5}}{2})^{k_n} \cdot k_n$ [14].

Then, writer also give out other theory about this. Second, the writer [15] introduce the situation of dihedral group. The author used the R, F (rotation elements, flip elements) to express the X+X and X-X that X is the dihedral group.

At last, in the article [16], the writer proposed an interesting fact that when n→ ∞, most of sets in a group are balance (X is balance if X + X = X - X = G), and he use the computer to show the trend of this.

DOI: 10.54254/2753-8818/9/20240736

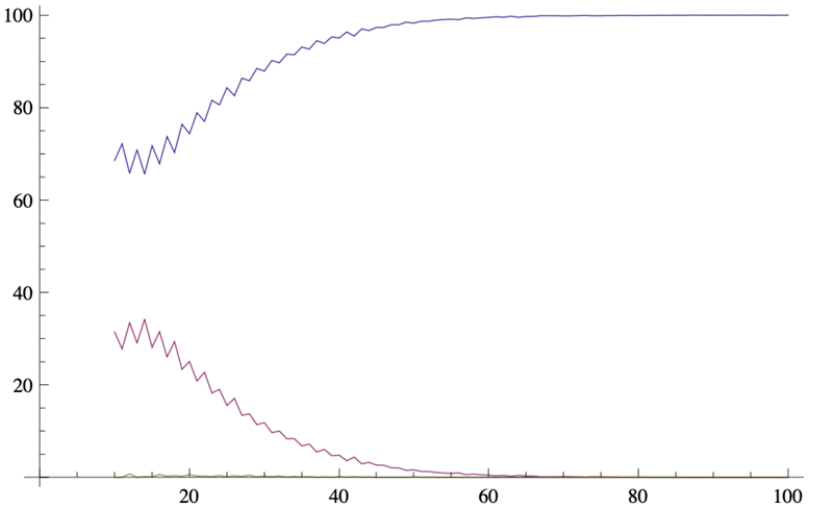

Figure 1. Simulation results [16].

As figure 1 shows, for each n (x-axis) we uniformly chose 10,000 random subsets of {1,.., n}. Top plot is the percentage of balanced, middle is the percentage of MDTS, and bottom is the percentage of MSTD [16].

4. Conclusion

In the article, readers can get the bound of each set (the theory in the section 1 give the basic bound and ones in section 2 illustrate it in different cases). Then the theory of perfect sets and unique sets answer the questions that when can use the adding of two sets to get the whole group (if it is finite) and when the adding of set do not have pairs of elements which get same element. However, the theory of free-set is popular, because it can be used on the prove of Fermat's Last Theorem. First, the definition of free-set is that if for all x, y, z $\in$ A satisfy x $\cdot$y $\neq$z, then A is a free-set.

References

[1] Diderrich G T 1973 On Kneser's addition theorem in groups. Proc. Amer. Math. Soc.
[2] Vsevolod F 2008 Critical pairs in abelian groups and Kemperman's structure theorem. International Journal of Number Theory, 3(03), 379-396.
[3] Devos M , Goddyn L , Mohar B 2009 A generalization of Kneser's Addition Theorem. Advances in Mathematics, 220(5), 1531-1548.
[4] John E 1984 Olson, On the sum of two sets in a group, Number Theory, 18, 110–120.
[5] Girard B, Griffiths S, Hamidoune Y O 2023 K-Sums in abelian groups. Working paper.
[6] Xia X, Gao W 2013 On n-sum of an abelian group of order n. Mathematics.
[7] Balandraud E, et al. 2023 Subset sums in abelian groups. Working paper.
[8] Olson J E 1975 Sums of sets of group elements. Acta Arith, 28, 147-156.
[9] Bajnok B, Ruzsa I 2015 The independence number of a subset of an abelian group. Integers.
[10] Peng J, Hui W 2017 On the structure of zero-sum free set with minimum subset sums in abelian groups. Integers.
[11] Bajnok L, et al. 2022 On perfect bases in finite Abelian group. Involve, Journal of Mathematics.
[12] Aart B, et al. 1995 Perfect sumsets in finite Abelian groups. Linear Algebra and its Applications.
[13] Bedert B 2023 On unique sums in Abelian groups. Working paper.
[14] Zhao Y 2010 Counting MSTD sets in finite abelian groups. Journal of Number Theory, 130(10).
[15] Ruben A, et al. 2022 Sum and Difference Sets in Generalized Dihedral Groups. Working paper.
[16] Vissuet K, Miller S J 2023 Most Subsets are Balanced in Finite Groups. Working paper.