BULLETIN OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 79, Number 6, November 1973

ADDITIVE GROUP THEORY—A PROGRESS REPORT

BY HENRY MANN

The first theorem in additive group theory was proved by Cauchy [2] in 1813.

THEOREM OF CAUCHY. *If A and B are residues* mod p *and* $A + B = \{x : x = a + b, a \in A, b \in B\}$ *then either* $A + B = G$ *or*

$$|A + B| \geqq |A| + |B| - 1. \tag{1}$$

(*Here* $|S|$ *denotes the cardinal of the set* S.)

This theorem was rediscovered by Davenport [5], [6] and is now known as [21] the Cauchy-Davenport theorem. Cauchy used it to show that every residue mod (p) is a sum of two squares i.e. the congruence

$$x^2 + y^2 \equiv r\,(p) \tag{2}$$

is solvable for every r. One easily obtains this result by setting $A = B = \{x : x \equiv a^2(p)\}$. We then have $|A| = |B| = (p + 1)/2$ and (2) follows from (1). Applying the C.-D. theorem to the representation of residues by sums of kth powers one may without loss of generality restrict k to divisors of $(p - 1)$. The C.-D. theorem then gives the result that every residue is a sum of not more than k kth powers. A considerable improvement is possible if one excludes the value $k = (p - 1)/2$. G. A. Vosper [30], [31], [21] refined the C.-D. theorem by completely characterizing those pairs A, B for which

$$|A + B| = |A| + |B| - 1.$$

Using Vosper's result one can show [4], [21]: If $a_1, \ldots, a_n$ are non-0 residues mod p and if $n \geqq (k + 1)/2$ then the congruence

$$a_1 x_1^k + \cdots + a_n x_n^k \equiv r\,(p) \tag{3}$$

is solvable for every r provided that $k < (p - 1)/2$.

This result was extended to finite fields of order $q = p^d$ by Tietäväinen [29] under the assumptions $k < (q - 1)/2$, $(q - 1)/k \nmid p^v - 1$ for $0 < v < d$. Tietäväinen's proof requires a result of Kempermann [13] on

---

An address delivered before the Annual Meeting of the Society in Dallas, Texas on January 26, 1973 by invitation of the Committee to Select Hour Speakers for Annual and Summer Meetings; received by the editors April 27, 1973.

AMS(MOS) subject classifications (1970). Primary 20F50, 05A05 22A99.

Key words and phrases. Elementary group theory, combinatorial mathematics, additive group theory.

Abelian groups which is analogous to Vosper's theorem on cyclic groups of prime-order.

The C.-D. theorem was generalized in various ways to Abelian groups. M. Kneser [**15**], [**21**] obtained the following result: There exists a subgroup H such that $A + B + H = A + B$ and

$$|A + B| \geqq |A + H| + |B + H| - |H|. \tag{4}$$

From this one can get an earlier result [**20**], [**21**]. If

$$|A + H| \geqq |A| + |H| - 1$$

for all subgroups H then $|A + B| \geqq |A| + |B| - 1$ for all sets B. This result implies a theorem of I. Chowla [**3**]. If A consists of 0 and residues prime to an integer m then $|A + B| \geqq |A| + |B| - 1$ where B is any set of residues mod m.

The inequality (4) implies that $A + B = G$ if $|A| + |B| > G$. This result can be obtained easily even if G is not Abelian. Although the easiest way to prove it uses the associativity of G one can obtain the theorem even for quasigroups. This was shown by W. A. McWorter [**24**]. McWorter's argument runs as follows. Let the product AB contain the element c exactly $n(c)$ times. Then the product $A\bar{B}$ must contain c exactly $|A| - n(c)$ times. But $A\bar{B}$ can contain c at most $\bar{B}$ times. Hence

$$|A| - n(c) \leqq |\bar{B}| = |G| - |B|, \qquad n(c) \geqq |A| + |B| - |G|,$$

and this implies McWorter's theorem.

In another direction Kneser [**18**] generalized his theorem to locally compact Abelian groups. If μ denotes Haar measure and μ_* interior Haar measure and if A and B are measurable sets then either

$$\mu_*(A + B) \geqq \mu(A) + \mu(B)$$

or there is an open compact subgroup H such that $A + B + H = A + B$ and

$$\mu_*(A + B) \geqq \mu(A + H) + \mu(B + H) - \mu(H).$$

Some results along these lines on noncommutative groups were obtained by Kempermann [**14**].

Let us now consider sums of n sets $C_1, \ldots, C_n$ each of which contain only two elements $C_i = \{c_i, d_i\}$. Subtracting $\sum c_i$ from $\sum C_i$ we obtain a sum $\sum A_i$ where $A_i = \{0, a_i\}$. This sum can also be described as the union of all sums over all subsequences of the sequence $\{a_1, \ldots, a_n\}$. The sum $\sum A_i$ also includes the sum over the empty set. One does not like to include this trivial representation of 0 and so we shall denote by $\sum(S)$ all elements which are equal to a sum over a nonempty subsequence of

$S = \{a_1, a_2, \ldots, a_n\}$ in symbols

$$\Sigma(S) = \{x; x = a_{i_1} + \cdots + a_{i_u}, i_1 < i_2 < \cdots < i_u, u > 0\}.$$

Let now $S = \{a_1, \ldots, a_n\}$ be a sequence of elements of G_p, the cyclic group of order p. Suppose that in S no element repeats more than k times. If $n \geqq k$ it is possible to partition the sequence into k nonempty sets $A_1, \ldots, A_k$ and the C.-D. theorem shows

$$|A_1 + \cdots + A_k| \geqq |S| - (k - 1) = n - k + 1.$$

Hence if $n \geqq p + k - 1$ then every element is a sum of exactly k elements of the sequence [22]. In particular if $k = p$ we see that every element is a sum of exactly p elements of S. If any element is repeated p times then at least 0 can be represented as a sum of p elements. Thus if $|S| = 2p - 1$ then 0 is a sum of exactly p elements of S. An easy induction carries this result over to any finite Abelian group and yields a theorem first proved by Erdös, Ginzburg and Ziv [9]: Let S be a sequence of elements of an Abelian group G and let $|S| = 2n - 1$ then 0 can be represented as a sum of exactly n elements of S. The theorem of Erdös, Ginzburg and Ziv carries over even to all solvable groups if it is permissible to arrange the summands in any order. The problem is open for nonsolvable groups. This problem can be considered also from a different point of view. Let G^* be the direct product of G and a cyclic group of order n and consider elements of the form $(s, 1)$. Let S be a set of such elements. Then the theorem of Erdös, Ginzburg and Ziv may be stated by saying that $\Sigma(S) \ni 0$ if $|S| = 2n - 1$. This leads to the following conjecture first stated by Erdös: Let $s(G)$ be the smallest integer such that $|S| = s$ implies $0 \in \Sigma(S)$ where S is a sequence of elements of G, and here and in the following all groups are Abelian. Erdös conjectured $s(G_n \times G_n) = 2n - 1$ where $|G_n| = n$. This conjecture was proved independently by D. Kruyswijk [1] and John Olson [27]. They proved: If $n_1 \mid n_2$ and $G = G_1 \times G_2$, $|G_1| = n_1$, $G_2 = n_2$ then $s(G) = n_1 + n_2 - 1$. In the proofs of Olson and Kruyswijk one first shows [26]

$$s(G) = 1 + \sum_{i=1}^{t} (n_i - 1)$$

when G is an Abelian p-group with invariants $n_1, \ldots, n_t$. This result suggests $s(G) = 1 + \sum_{i=1}^{t} (n_i - 1)$ for any Abelian group G with invariants $n_1 \mid n_2 \mid \cdots \mid n_t$. Kruyswijk [12], Baayen and van Emde Boas [11], [12] verified this conjecture in a large number of cases. However, the conjecture is false in general. The first counterexample was found by Baayen [12] in the group of type (2, 2, 2, 2, 6). Later van Emde Boas and D. Kruyswijk [12] found a counterexample in the group of type (3, 3, 3, 6). The problem is still open for groups with three generators.

If G is the class group of an algebraic number field and $s = s(G)$ then, as first pointed out by Davenport, any ideal with s or more prime factors has a factor which is a principal ideal.

An interesting special case arises if $a_1, \ldots, a_c$ are distinct and not 0. Let $c(G) = c$ denote the smallest integer such that $\Sigma(S) = G$ if $|S| = c(G)$. Erdös and Heilbronn [**10**] showed

$$\sqrt{4p + 5} - 2 < c(G_p) \leqq 2\sqrt{6p} + 1$$

and conjectured $c(G) \leqq 2\sqrt{p} + 1$. This conjecture was proved by Olson [**25**] who even improved it to $c(G) \leqq \sqrt{4p - 3} + 1$ which is within at most 2 of the best possible value.

The analogous problem for groups of type (p, p) was considered by Mann and Olson [**23**]. If G is of type (p, p) then $2p - 2 \leqq c(G) \leqq 2p - 1$. They also showed that $\Sigma(S) \ni 0$ if S has $2p - 2$ distinct non-0 elements and gave an example of a set S with $2p - 3$ elements such that $\Sigma(S) \neq G$.

It is not known for what values of p we have $c(G_p) = 2p - 2$. For $p = 3$ and $S = \{(1, 0), (0, 1), (1, 1), (1, -1)\}$ we have $\Sigma(S) \not\ni (0, -1)$. For $p = 5$ and $p = 7$ Y. S. Wou [**32**] proved $c(G_p) = 2p - 2$ and this value was also simultaneously found by Shen Lin by computer. For higher values of p the problem is still open but Wou's result makes it very likely that $c(G_p) = 2p - 2$ for $p > 3$.

The result of Mann and Olson was generalized by G. T. Diderrich. If p, q are (not necessarily distinct) primes and if $|G| = pq$ then $p + q - 2 \leqq c(G) \leqq p + q - 1$. Moreover if $q > 2p$ then $c(G) = p + q - 2$.

Another problem on which considerable progress has been made is the problem of maximal sum free sets. A set S of elements of a group G is called sum free if $(S + S) \cap S = \varnothing$. The set S is called maximal sum free if S is sum free and $|S| \geqq |S'|$ for any sum free set S'. We set $\lambda(G) = |S|$ where S is a maximal sum free set of G. The following results are due to Diananda and Yap [**7**], [**33**], [**34**].

By Kneser's theorem there is a subgroup H such that $S + S + H = S + S$ and

$$|S + S| \geqq |S + H| + |S + H| - |H|. \tag{5}$$

Now if S is sum free then $S + H$ is sum free; for suppose that $s_1 + h_1 + s_2 + h_2 = s_3 + h_3$. Then

$$s_1 + s_2 + h = s_3. \tag{6}$$

But $s_1 + s_2 + h \in S + S + H = S + S$, and so S would not be sum free. Since S is maximal $S = S + H$. Hence S consists of cosets mod H

and so $|S| = t\,|H|$ for some integer t. Moreover

$$|G| \geqq |S + S| + |S| \geqq 3\,|S| - |H|.$$

Hence $t\,|H| = |S| \leqq (|G| + |H|)/3$, and setting $|G|/|H| = d$, $t \leqq (d + 1)/3$,

$$\lambda(G) = |S| = t\frac{|G|}{d} = \frac{|G|}{d}\left[\frac{d+1}{3}\right].$$

This gives

$\lambda(G) \leqq \frac{1}{3}\,|G|\,(1 + 1/p)$ where p is the smallest prime $\equiv 2\,(3)$ which divides $|G|$,

$\leqq \frac{1}{3}\,|G|$ if $|G| \equiv 0\,(3)$ and all other prime divisors of G are $\equiv 1\,(3)$,

$\leqq \frac{1}{3}(|G| - 1)$ if all prime divisors of $|G|$ are $\equiv 1\,(3)$.

In the first two cases there are sets S such that $|S|$ equals the upper bound.

For $p \equiv 2\,(3)$ let H be a subgroup of index p and set

$$S = (H + g) \cup (H + 4g) \cup \cdots \cup (H + (p - 1)g)$$

where $g \notin H$. It is easy to see that S is sum free. In the second case we can take just one coset mod H where $|H| = |G|/3$.

In the case that all prime factors of $|G|$ are $\equiv 1\,(3)$, let m be the exponent of G and let g have order m. There exists a subgroup H of index m such that $g + H$ has order m in the factor group G/H. It is easily seen that

$$S = (H + 2g) \cup (H + 5g) \cup \cdots \cup H + (m - 2)g$$

is sum free. Since $|S| = \frac{1}{3}(m - 1)\,|G|/m$ we have

$$\tfrac{1}{3}G(1 - 1/m) \leqq \lambda(G) \leqq \tfrac{1}{3}(|G| - 1).$$

In the first case Diananda and Yap were able to characterize completely all maximal sum free sets. The third case is still open. Diananda and Yap [7] conjectured $\lambda(G) = \frac{1}{3}\,|G|\,(1 - 1/m)$ where m is the exponent of G. This conjecture is true if G is cyclic. It has been verified in a number of other cases for instance for elementary p-groups [**28**].

References

1. P. C. Baayen, *Een combinatorisch probleem voor eindige Abelse groepen*, Math. Centrum Syllabus 5, Colloquium Discrete Wiskunde Caput 3. Math. Centre Amsterdam, 1968.

2. Cauchy, *Recherche sur les nombres*, J. Ecole Polytechn. **9** (1813), 99–106.

3. I. Chowla, *A theorem in the additive theory of numbers*, Proc. Nat. Acad. Sci. U.S.A. **8** (1938), 160–164.

4. S. Chowla, H. B. Mann and E. G. Straus, *Some applications of the Cauchy-Davenport theorem*, Norske Vid. Selsk. Forh. Trondheim **32** (1959), 74–80. MR **23** #A2384.

5. H. Davenport, *On the addition of residue classes*, J. London Math. Soc. **10** (1935), 30–32.

6. ———, *A historical note*, J. London Math. Soc **22** (1947), 100–101. MR **9,** 271.

7. P. H. Diananda and H. P. Yap, *Maximal sum free sets of elements of finite groups*, Proc. Japan Acad. **45** (1969), 1–5. MR **39** #6968.

8. G. T. Diderrich, *An addition theorem for Abelian groups of order pq*, J. Number Theory (to appear).

9. P. Erdös, A. Ginzburg and A. Ziv, Bull. Res. Council Israel **10F** (1961), 41–43.

10. P. Erdös and H. Heilbronn, *On the addition of residue classes* mod *p*, Acta. Arithm. **9** (1949), 149–150.

11. Boas P. van Emde, *A combinatorial problem on finite Abelian groups*. II, Math. Centrum Amsterdam Afd. Zuivere Wisk. **1969,** ZW-007, 60 pp. MR **41** #332.

12. Boas P. van Emde and D. Kruyswijk, *A combinatorial problem on finite Abelian groups*. III, Math. Centrum Amsterdam Afd. Zuivere Wisk **1969** ZW-008.

13. J. H. B. Kempermann, *On small sum-sets in an Abelian group*, Acta. Math. **103** (1960), 63–88. MR **22** #1615.

14. ———, *On products of sets in a locally compact group*, Fund. Math. **56** (1964), 51–68. MR **34** #2772.

15. M. Kneser, *Abschäetzung der asymptotischen dichte von Summenmengen*, Math. Z. **58** (1953), 459–484. MR **15,** 104.

16. ———, *Anwendung eines Satzes von Mann auf die Geometrie der Zahlen*, Proc. Internat. Congress Math. Amsterdam, vol. 2, 1954, p. 32.

17. ———, *Ein Satz über Abelsche Gruppen mit Anwendungen auf die Geometrie der Zahlen*, Math. Z. **61** (1955), 429–434. MR **16,** 898.

18. ———, *Summenmengen in lokal kompkaten Abelschen Gruppen*, Math. Z. **66** (1956), 88–110. MR **18,** 403.

19. H. B. Mann, *On products of sets of group elements*, Canad. J. Math. **4** (1952), 64–66. MR **13,** 720.

20. ———, *An addition theorem for sets of elements of Abelian groups*, Proc. Amer. Math. Soc. **4** (1953), 423. MR **14,** 1058.

21. ———, *Addition theorems. The addition theorems of group theory and number theory*, Interscience, New York, 1965. MR **31** #5854.

22. ———, *Two addition theorems*, J. Combinatorial Theory **3** (1967), 233–235. MR **36** #1349.

23. H. B. Mann and J. E. Olson, *Sums of sets of elements in the elementary Abelian group of type* (*p*, *p*), J. Combinatorial Theory **2** (1967), 275–284. MR **35** #5506.

24. William A. McWorter, *On a theorem of Mann*, Amer. Math. Monthly **71** (1964), 285–286. MR **28** #5135.

25. John E. Olson, *An addition theorem modulo p*, J. Combinatorial Theory **5** (1968), 45–52. MR **37** #2714.

26. ———, *A combinatorial problem on finite Abelian groups*. I, J. Number Theory **1** (1969), 8–10. MR **38** #5922.

27. ———, *A combinatorial problem on finite Abelian groups*. II, J. Number Theory **1** (1969), 195–199. MR **39** #1552.

28. A. H. Rhemtulla and A. P. Street, *Maximal sum free sets in finite Abelian groups*, Bull. Austral. Math. Soc. **2** (1970), 289–297. MR **41** #8519.

29. A. Tietäväinen, *On diagonal forms over a finite field*, Ann. Univ. Turku. Ser. AI No. 118 (1968), 1–10. MR **38** #3248.

30. A. G. Vosper, *The critical pairs of subsets of a group of prime order*, J. London Math. Soc. **31** (1956), 200–205. MR **17,** 1056.

31. ———, *Addendum to "The critical pairs of subsets of a group of prime order"*, J. London Math. Soc. **31** (1956), 280–282. MR **17,** 1182.

32. Y. F. Wou, *Sums of sets in the Abelian group of type* (5, 5), J. Number Theory (to appear).

33. H. P. Yap, *Maximal sum free sets of group elements*, J. London Math. Soc. **44** (1969), 131–136. MR **38** #1167.

34. ———, *Maximal sum free sets in finite Abelian groups*. II, Bull. Austral. Math. Soc. **5** (1971), 43–54. MR **45** #3564.

Current address: Department of Mathematics, University of Arizona, Tucson, Arizona 85721