ADDITIVE PROPERTIES OF MULTIPLICATIVE SUBGROUPS
OF FINITE INDEX IN FIELDS

PEDRO BERRIZBEITIA

(Communicated by Louis J. Ratliff, Jr.)

Abstract. Gallai’s theorem, an n-dimensional generalization of Van der Waerden’s theorem on arithmetic progression, is used to prove the following theorem:

Let F be a field and \( G \subseteq F^* \) a subgroup of finite index n. There is a positive integer N, which depends only on n, so that if Char F = 0 or char F \( \geq N \), then \( G - G = F \).

Introduction

It is well known that if \( n \) is a positive integer and \( p \) is a prime number, then the equation \( x^n + y^n \equiv t \mod p \) has a solution for any \( t \) as long as \( p \) is sufficiently large. This problem can be solved by using Jacobi Sums to approximate the number of solutions of the equation. This is done in [3, Chapter 8]. The problem can be restated as follows: If \( G \) is a subgroup of \( F^*_p \) of index at most \( n \), then, for large enough values of \( p \), \( G + G \supseteq F^*_p \), with equality if and only if \(-1 \notin G\).

For the case \( n = 3 \) Leep and Shapiro [5] were able to prove the following generalization. Let \( G \) be a subgroup of index 3 in the multiplicative group \( F^* \) of a field \( F \). Then \( G + G = F \), except in the cases \( |F| = 4, 7, 13, \) or \( 16 \). They also conjectured that the conclusion holds for infinite fields if the index is 5.

In §1 of this paper we prove Theorem 1.1 which states: Let \( F \) be a field and \( G \subseteq F^* \) a subgroup of finite index \( n \). There is a positive integer \( N \), that depends only on \( n \), so that if \( \text{Char } F = 0 \) or \( \text{char } F \geq N \), then \( G - G = F \).

Fields for which the conclusion of Theorem 1.1 holds will be called uniform. It follows that if \( F \) is a uniform field, then, \( G + G = F \) if and only if \(-1 \in G\).

More generally, we show that if \( m \) is a positive integer and \( m \times G = \{g_1 + g_2 + \cdots + g_m | g_i \in G\} \) then \( m \times G = F \) if and only if \(-1 \in m - 1 \times G \) or, equivalently, if and only if \( 0 \in m \times G \) (see Corollary 1.2 below). In §2 we let \( F \) be an arbitrary field and \( G \subseteq F^* \) a subgroup of index \( n \) in \( F^* \). Let \( P \) denote the additive closure of \( G \) in \( F \). We show that if \( F \) is uniform, then
$P = m \times G$ for some $m \leq [P : G] + 1$. (See Corollary 2.2.) Finally, in §3 we let $Q$ denote the field of the rational numbers. For every odd prime $p \geq 5$, we construct a subgroup of index $n = p - 1$ in $Q^*$, such that $n + 1 \times G = Q$ but $m \times G \neq Q$ for all $m \leq n$.

1. UNIFORM FIELDS

We follow Leep and Shapiro’s notation. Let $F$ be a field. Let $G \subseteq F^*$ be a subgroup of finite index $n$. For each positive integer $m$ we denote by $m \times G$ the set of sums of $m$ elements of $G$; that is, $m \times G = \{g_1 + g_2 + \cdots + g_m | g_i \in G\}$. The additive closure of $G$ will be denoted by $\sum G$ or simply $P$. So $P = \bigcup_{i=1}^{\infty} i \times G$. $P_m$ will denote the partial union $P_m = \bigcup_{i=1}^{m} i \times G$. Finally let

$G - G = \{g_1 - g_2 | g_1, g_2 \in G\}$. We now state the main theorem of this paper.

**Theorem 1.1.** Let $F$ be a field and $G \subseteq F^*$ a subgroup of finite index $n$. There is a positive integer $N$, which depends only on $n$, so that if $\text{Char } F = 0$ or $\text{char } F \geq N$, then, $G - G = F$.

For simplicity, fields for which the conclusion of Theorem 1.1 holds will be called uniform with respect to subtraction or simply uniform fields.

**Proof of Theorem 1.1.** We make some preliminary remarks. Note first that $G - G = F$ if and only if $cG - cG = F$ for any $c \in F^*$. Also note that $cG - cG$ consists of a union of cosets of $F^*$ mod $G$ and of 0. Hence, to prove that $G - G = F$, it is enough to show that $cG - cG$ contains a complete set of representatives of $F^*$ mod $G$ for some $c \in F$.

Let $N$ be the set of nonnegative integers. For $m \in N$, $m$ positive, let

$N^m = \{(x_1, x_2, \ldots, x_m) | x_i \in N\}$. We will use the following result due to Gallai:

**Theorem G.** Let $V \subseteq N^m$ be finite. For any finite coloring of $N^m$ there is $a \in N^m$ and nonzero $d \in N$, so that all the points of $a + dV$ have the same color.

Gallai’s theorem is a result of Ramsey theory. It is derived from the Hales-Jewett theorem in [2]. To show the existence of $N(n)$ in Theorem 1.1, we will use the following apparently stronger but equivalent form of Gallai’s theorem. For $s \in N$ let $[s] = \{0, 1, 2, \ldots, s\}$.

**Theorem G’.** Let $V \subseteq N^m$ be finite. Let $m \in N$ be positive. There is a natural number $N' = N'(V, m, r)$, such that for any $N \geq N'$ and any $r$-coloring of $[N]^m$, there is $a \in [N']^m$ and a nonzero $d \in N$, $d \leq N'$, such that $a + dV$ is monochromatic.

That Theorem G’ is equivalent to Theorem G is a consequence of König’s infinity lemma. This modification was first introduced by O. Schreier for the case $m = 1$. See [6].

In our situation we assume $m = n$, the index of $G$ in $F^*$. $V \subseteq N^n$ will be the set $V = \{0, e_1, e_2, \ldots, e_n\}$, where the $e_i$ are the vectors of the canon-
ical basis for $\mathbf{R}^n$. To each one of the cosets of $F^* \mod G$ we associate a different color and to $0 \in F$ we associate another color. We will induce a $(n + 1)$-coloring on the set $\mathbb{N}^n$ as follows: Let $g_1, g_2, \ldots, g_n$ be a set of representatives of $F^* \mod G$. Paint each $(x_1, x_2, \ldots, x_n) \in \mathbb{N}^n$ with the color associated to the class of $x_1 g_1 + x_2 g_2 + \cdots + x_n g_n$. By Gallai's theorem, there is $a = (a_1, a_2, \ldots, a_n) \in \mathbb{N}^n$ and a nonzero $d \in \mathbb{N}$ such that $a + dV$ is monochromatic. It follows that if $c = a_1 g_1 + a_2 g_2 + \cdots + a_n g_n$, then $c$ and $c + d g_i$ have the same color associated. Hence $d g_i \in cG - cG$ for all $i = 1, 2, \ldots, n$. If $d \neq 0$ in $F$ the $d g_i$ run through all classes of $F^* \mod G$. In this case, by the preliminary remarks we get $G - G = F$. Clearly $d$ is nonzero in $F$ when $F$ has characteristic zero. Also, since $d \leq N' = N'(V, n, n + 1)$ given by Theorem $G'$ the same conclusion holds for fields of characteristic larger than $N'$. Since $V$ depends only on $n$ we let $N(n) = N'$. □

Remark. Following the same techniques used in [1] to derive a proof of Van der Waerden's theorem from the Hales-Jewett theorem, one can derive from Hales-Jewett a particular case of Gallai's theorem that is enough to prove Theorem 1.1. If this is done, one can show that $N(n)$ can be chosen to be no larger than $2^M$ where $M = N(n + 1, 2^n)$ is the number given in the Hales-Jewett theorem. The numbers $N(r, t)$ are defined recursively and, therefore are computable, however, they are already extremely large for small values of $t$ and $r$.

Corollary 1.2. (a) Let $F$ be a uniform field. If $m > 1$, then $m x G = F$ if and only if $-1 \in m - 1 \times G$. In particular $G + G = F$ if and only if $-1 \in G$.

(b) If $G$ has odd index in $F^*$ for some uniform field $F$, then $G + G = F$.

Proof. If $m x G = F$ then $g_1 + g_2 + \cdots + g_m = 0$ for some $g_i \in G$. Then $-1 = g_2 g_1^{-1} + g_3 g_1^{-1} + \cdots + g_m g_1^{-1} \in m - 1 \times G$. For the converse, if $-1 \in m - 1 \times G$ then $-G \subseteq m - 1 \times G$. Using Theorem 1.1 we have: $F = G - G = G + (-G) \subseteq G + m - 1 \times G = m \times G$. This proves (a). For (b) note that if $[F^* : G] = 2k + 1$ then $(-1)^{2k+1} = -1 \in G$. The result follows from (a). (The case $n = 5$ was conjectured in [5] for arbitrary finite fields.) □

Remark. Part (a) of Corollary 1.2 could have been stated in the following equivalent form: If $F$ is a uniform field, then $m x G = F$ if and only if $0 \in m x G$.

2. Inequalities concerning sets of sums of elements of $G$

Let $F$ be an arbitrary field and $G \subseteq F^*$ be a multiplicative subgroup of finite index. Lemma 1 of [5] shows that if $-1 \in P$ then $P = F$. In any case, we have the following:

Proposition 2.1. If $G$ has index $n$ in $F^*$ we have:

(a) For $i \geq 1$, $P_i \subseteq P_{i+1}$ with equality if and only if $P_i = P$.

(b) If $-1 \in P$ then $P_{n+1} = F$. If $-1 \notin P$ then $P_{(n/2)+1} = P$.

Proof. $P_i \subseteq P_{i+1}$ by definition of $P_i$. If $P_i = P$ then $P_{i+1} = P_i + G = P + G = P = P_i$, so $P_{i+1} \subseteq P_i$. Conversely, if $P_i = P_{i+1}$ then $P_i = P_r$ for all $r > i$. 

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
But \( P = \bigcup_{r=1}^{\infty} P_r = P_1 \). For (b) just note that every \( P_m \) is a union of cosets of \( F^* \) and possibly of \( \{0\} \). For simplicity \( \{0\} \) is considered to be a coset. Suppose that \(-1 \in P \) and that \( P_n \neq F \). Then, by part (a), for all \( i \leq n \), \( P_{i+1} \) contains at least one class more than \( P_i \). It follows that \( P_{n+1} \) contains all classes including \( \{0\} \). So \( P_{n+1} = F \). If \(-1 \notin P \), \( [F^*:P] \geq 2 \) then \( [P:G] \leq n/2 \) and the argument is the same as before.

**Corollary 2.2.** If \( F \) is a uniform field we have:

(a) \( i \times G \subseteq i + 1 \times G \) with equality if and only if \( i \times G = P \).

(b) If \(-1 \in P \) then \( n + 1 \times G = F \). If \(-1 \notin P \) then \( n/2 + 1 \times G = P \).

**Proof.** Using Proposition 3.1 we see that it is enough to show that \( i \times G = P \) for any \( i \). For this we note that it suffices to show that \( G \subseteq G + G \). But, since \( F \) is uniform, then \( G - G = F \). So \( G - G \supseteq G \). This means that there are elements \( g_1, g_2, g_3 \) in \( G \) such that \( g_1 - g_2 = g_3 \). So \( g_1 = g_2 + g_3 \), which implies \( G + G \subseteq G \).

**Remark.** In general it is not true that \( n + 1 \times G = P \). Let \( F = F_7 \), the finite field with 7 elements and let \( G = \{1, -1\} \). Then \( [F^*:G] = 3 \) and \( 4 \times G \neq F \).

### 3. Bounds in §2 cannot be improved

We end this paper with examples of subgroups of finite index \( n \) in \( Q^* \) for which \( n+1 \) is the minimum \( r \) such that \( Q = r \times G \). We note that subgroups of finite index in \( Q^* \) are kernels of multiplicative maps of \( Q^* \) into finite groups. These maps are determined by the image of the prime numbers and by the image of \(-1\).

Let \( q \) be an odd prime \( q \geq 5 \). We will map \( Q^* \) into \( F_q^* \) as follows: if \( p \neq q \) is a prime then let \( p \) be mapped to its class \( \mod q \). Let the prime \( q \) be mapped into 1 and let \(-1 \) be mapped to its class \( \mod q \). This way every rational number which is a unit in the field of the \( q \)-adic number is mapped into its class \( \mod q \). Hence, if \( G \) is the kernel of this map, we have, \( n \in G \) if and only if \( n = q^r u_1 \), where \( r \) is an integer and \( u_1 \) is a unit, \( u_1 \equiv 1 \mod q \). It is then easy to verify that \( q - 1 \times G = Q^* \). But \( q - 1 \) is the index of \( G \) in \( Q^* \).

**Acknowledgment**

I am grateful to Professor D. B. Shapiro for telling me about Van der Waerden's \( n \)-dimensional generalization. My original version of Theorem 1.1 used the classical one-dimensional Van der Waerden's theorem and involved only the case \( F = Q \), the field of rational numbers.

**References**


**Departamento de Matemáticas Puras y Aplicadas, Universidad Simón Bolívar, Apartado 89000, Caracas 1080-A, Venezuela**