PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 120, Number 2, February 1994

MULTIPLICATIVE SUBGROUPS OF FINITE INDEX IN A DIVISION RING

GERHARD TURNWALD

(Communicated by Maurice Auslander)

ABSTRACT. If G is a subgroup of finite index n in the multiplicative group of a division ring F then $G - G = F$ or $|F| < (n-1)^4 + 4n$. For infinite F this is derived from the Hales-Jewett theorem. If $|F| > (n-1)^2$ and -1 is a sum of elements of G then every element of F has this property; the bound $(n-1)^2$ is optimal for infinitely many n.

INTRODUCTION

It is well known that every nonzero element of a finite field F is a sum of two nonzero nth powers if $q = |F|$ is sufficiently large. Since F^* is cyclic, this is equivalent to the statement that, for every positive integer n, $G + G \supseteq F^*$ holds if G is a subgroup of index n of F^* provided $q \geq q_0(n)$. Leep and Shapiro gave a proof for $n = 3$ which also works for infinite fields; they conjectured that $G + G = F$ holds for $n = 5$ if F is an infinite field [3]. Recently, Berrizbeitia proved that $G - G = F$ if $\operatorname{char} F = 0$ or $\operatorname{char} F \geq p_0(n)$. ($G - G$ means $\{g_1 - g_2 \colon g_1, g_2 \in G\}$.) Thus, in particular, $G + G = F$ if n is odd and $\operatorname{char} F = 0$. (Note that $-1 = (-1)^n \in G$.) The proof in [1] is based on Gallai's theorem (cf. 1.2) which does not give (reasonable) bounds for $p_0(n)$. Employing the Hales-Jewett theorem, a modification of Berrizbeitia's proof allows us to prove the following result for infinite F.

Theorem 1. *Let F be a division ring and G be a subgroup of F^* with finite index n. If $|F| \geq (n-1)^4 + 4n$ then $G - G = F$; if, in addition, n is odd then $G + G = F$.*

Thus $G - G = F$ holds if $|F| \geq n^4$ and $|F| > 2$. Choosing $F = \mathbf{F}_{p^2}$ and $G = \mathbf{F}_p^*$ shows that $|F| \geq (n-1)^2$ is not sufficient if $n-1$ is a prime. A more elaborate example shows that, for infinitely many n, $|F| \geq (n+1)^2$ is not sufficient (see Proposition 1.6).

The notation of Theorem 1 will be kept throughout the paper except in Corollary 1.2. $\mathbf{N}$ denotes the set of positive integers. For every $k \in \mathbf{N}$ we put $G_k = \{g_1 + \cdots + g_k \colon g_1, \ldots, g_k \in G\}$ and $S_k = G_1 \cup \cdots \cup G_k$. Let $S = \bigcup_{k \geq 1} S_k$.

Received by the editors May 26, 1992.
1991 *Mathematics Subject Classification.* Primary 12E99; Secondary 05D10, 11T99, 12E15.
Key words and phrases. Multiplicative subgroup, field, division ring, Hales-Jewett theorem.

Theorem 2. *If* $|F| > (n-1)^2$ *and* $-1 \in S$ *then* $S = F$.

[1] Remark 2.3 shows that the bound for $|F|$ is optimal for infinitely many n. The proof is similar to the proof given by Leep and Shapiro for infinite F [3, Lemma 1]. The following theorem refines the results of §2 in [1].

Theorem 3. (i) *If* $G \subseteq G - G$ *then* $S_k = G_k$ *for all* $k \in \mathbf{N}$.
(ii) $S_k \subseteq S_{k+1}$ *for every* $k \in \mathbf{N}$; $S_k = S_{k+1}$ *iff* $S_k = S$.
(iii) $S_{n+1} = S$.
(iv) *If* $-1 \notin S$ *then* n *is even and* $S_{n/2} = S$.

The examples given in Remark 2.5 show that the bounds in (iii) and (iv) are optimal for infinitely many n.

1. Results concerning $G - G$ and $G + G$

1.1. **Theorem** (Hales-Jewett). *For all* $m, r \in \mathbf{N}$ *there exists* $N(m, r) \in \mathbf{N}$ *such that, for every* $N \in \mathbf{N}$ *with* $N \geq N(m, r)$, *every function* f *defined on* $\{0, \dots, m\}^N$ *with at most* r *values is constant on some line.*

(*A line is a set of the form* $\{(k_1, \dots, k_N) : k_j = k'_j \text{ if } j \in J_0 \text{ and } k_{j_1} = k_{j_2} \text{ if } j_1, j_2 \in J_1\}$ *for suitable disjoint* J_0, J_1 *with* $\{1, \dots, N\} = J_0 \cup J_1$, $J_1 \neq \varnothing$, *and suitable* $k'_j \in \{0, \dots, m\}$ *for* $j \in J_0$.)

For a proof we refer to [2]; note that t and 0 have to be interchanged in the definition of x_{ij}, y_{si} on p. 37 in [2].

1.2. **Corollary.** *Let* S' *be a finite subset of a commutative semigroup* S. *Then for every mapping* g *from* S *into some finite set there exist* $s \in S$ *and* $d \in \mathbf{N}$ *such that* g *is constant on* $\{s + ds' : s' \in S'\}$.

Proof. We may assume $S' = \{s_0, \dots, s_m\}$ with $m \geq 1$. The assertion follows by applying 1.1 to $f(k_1, \dots, k_N) = g(\sum_{j=1}^N s_{k_j})$ $(0 \leq k_j \leq m)$ for suitably large N.

Gallai's theorem is the special case $S = \mathbf{R}^m$ (cf. [2, p. 38]) or $S = \mathbf{N}_0^m$ (as used in [1]). Van der Waerden's theorem on arithmetic progressions is obtained for $S = \mathbf{N}$ or $S = \mathbf{N}_0$. Corollary 1.2 is not required in the sequel.

1.3. **Proposition.** *Let* F *be an infinite division ring and* G *be a subgroup of* F^* *of finite index* n. *Then for arbitrary* $x_1, \dots, x_m \in F^*$ *there exists* $c \in F^*$ *such that* $1 + cx_k \in G$ *for* $1 \leq k \leq m$.

Proof. For every $N \in \mathbf{N}$ there exist $c_1, \dots, c_N \in F$ such that $\sum_{j \in J} c_j \neq 0$ for every nonempty $J \subseteq \{1, \dots, N\}$. (Inductively, c_k can be chosen such that $\sum_{j \in J} c_j \neq 0$ for all $J \subseteq \{1, \dots, k\}$.) Now let $N = N(m, n+1)$ (according to Theorem 1.1), set $x_0 = 0$, and set $f(k_1, \dots, k_N) = (\sum_{j=1}^N c_j x_{k_j})G$ (where $cG = \{cx : x \in G\}$) for all $k_j \in \{0, \dots, m\}$. By Theorem 1.1 there exist disjoint J_0, J_1 with $\{1, \dots, N\} = J_0 \cup J_1$, $J_1 \neq \varnothing$, and $k'_j \in \{0, \dots, m\}$ such that $aG = (a + bx_k)G$ for $1 \leq k \leq m$, where $a = \sum_{j \in J_0} c_j x_{k'_j}$ and $b = \sum_{j \in J_1} c_j$. The assertion holds with $c = a^{-1}b$. (Note that $a \neq 0$ since $b \neq 0$ and $x_k \neq 0$.)

[1] Note that $-1 = p - 1 \in G_{p-1} \subseteq S$ if $p = \operatorname{char} F > 0$.

1.4. *Proof of Theorem* 1. If $-1 \notin G$ then G has index 2 in $G\langle -1\rangle$ and hence n is even. Thus it remains to show $G - G = F$. If F is infinite then applying Proposition 1.3 to any left diagonal of G yields a left diagonal $x_1, \dots, x_n$ of G such that $1 + x_k \in G$ (and hence $x_k G \subseteq G - G$) for $1 \leq k \leq n$; thus $F \subseteq G - G$. Now let F be finite. By Wedderburn's theorem [4, 2.55] we have $F = \mathbf{F}_q$ for suitable q. Thus F^* is cyclic and $G = \{x^n : x \in F^*\}$. It is well known that the number N of solutions $(x, y) \in F \times F$ of $x^n - y^n = c$ satisfies $|N - q| \leq (n-1)^2\sqrt{q}$ if $c \in F^*$ [4, 6.37]. Let $q = (n-1)^4 + d$ with $d \geq 4n$. If $n > 1$ then $(n-1)^2 + (n-1)^{-2}(d-2n) > \sqrt{q}$ and thus $N \geq q - (n-1)^2\sqrt{q} > 2n$. If $n = 1$ then $N = q \geq 4$. Since the number of solutions with $x = 0$ or $y = 0$ is at most $2n$, this shows that $c \in G - G$.

1.5. *Remark.* If $n = 2$ then $G - G = F$ unless $|F| \in \{3, 5\}$ in which case $G - G = F \backslash \{1, -1\}$. If $n = 3$ then $G - G = F$ unless $|F| \in \{4, 7, 13, 16\}$. The exceptional cases are $G - G = \{0\}$ for $|F| = 4$, $G - G = \{0, 2, -2\}$ for $|F| = 7$, and $G - G = F \backslash G$ for $|F| \in \{13, 16\}$.

By using Theorem 1 and the fact that n divides $|F| - 1$ it only remains to check three cases for $n = 2$ and six cases for $n = 3$. We omit the details. A self-contained proof of (the first part of) the assertion for $n = 3$ can be found in [3].

1.6. **Proposition.** *There are infinitely many* n *such that* $|F| = (n+1)^2$ *and* $G - G \neq F$.

Proof. Let $p > 3$ be a prime such that -3 is a square mod p. By the quadratic reciprocity law this holds for every prime $p \equiv 1 \pmod{12}$ and by Dirichlet's theorem there exist infinitely many such p. Let $F = \mathbf{F}_{p^2}$ and $G = \{x \in F : x^{p+1} = 1\}$; then G has index $n = p - 1$ in F^*. Assume that $-1 \in G - G$, i.e., there exists $x \in F^*$ with $x^{p+1} = (x-1)^{p+1} = 1$. Taking into account that $(x-1)^p = x^p - 1$ this yields $(x^{-1} - 1)(x - 1) = 1$. Hence $x^2 - x + 1 = 0$ which gives $x = (1 + a)/2$, where $a^2 = -3$. By assumption we have $a \in \mathbf{F}_p$; hence $x \in \mathbf{F}_p$ and $x^{p-1} = 1$. From $x^{p+1} = 1$ and $x^2 - x + 1 = 0$ we thus deduce $x = 2$ and $a = 3$. Clearly, this is impossible.

1.7. *Remark.* If $|F|$ is finite then in Theorem 1 one gets $G + G \supseteq F^*$. This is proved by an obvious modification of the proof of $G - G = F$. If $G + G \supseteq F^*$ then $G + G = F$ holds iff $-1 \in G$, i.e., iff $(-1)^{(|F|-1)/n} = 1$.

For infinite F the situation is different since $G = \{2^k \frac{a}{b} : k \equiv 0 \,(\mathrm{mod}\, \frac{n}{2});\ a, b \in \mathbf{N};\ a, b \text{ odd}\}$ is a subgroup of (even) index n in $\mathbf{Q}^*$ and $G + G$ is a proper subset of $\mathbf{Q}^*$ (by positivity). Hence for infinite F we cannot conclude $F^* \subseteq G + G$. We do have $G \subseteq G + G$, however, since $G \subseteq G - G$ (and hence some element of G belongs to $G + G$).

1.8. *Remark.* Let $(*)$ denote the statement $(G \cap \mathbf{Z}) - (G \cap \mathbf{Z}) = \mathbf{Z}$. The following examples show that $(*)$ holds in several cases but does not hold in general (for $F = \mathbf{Q}$).

(i) Let p be prime. Then $G = \{p^k \frac{a}{b} : k, a, b \in \mathbf{Z},\ a \equiv b \not\equiv 0 \,(\mathrm{mod}\, p)\}$ is a subgroup of finite index of $\mathbf{Q}^*$ (cf. Remark 2.5). Clearly, $x \in G \cap \mathbf{Z}$ implies $x \equiv 0, 1 \,(\mathrm{mod}\, p)$ and hence $(*)$ does not hold if $p > 3$.

(ii) $G = \{(-2)^k 9^l \frac{a}{b} : k, l \in \mathbf{Z};\ a, b \in \mathbf{N} \text{ with } (ab, 6) = 1\}$ has index 4 in $\mathbf{Q}^*$. Note that $\mathbf{Z} \subseteq \{1, -1, 3, -3\} \cdot (G \cap \mathbf{Z})$. Hence $(*)$ holds since $1 = 5 - 4$, $3 = 7 - 4$, and $4, 5, 7 \in G \cap \mathbf{Z}$.

(iii) $G = \{\prod_{p \text{ prime}} p^{k_p} : k_p \in \mathbf{Z},\ k_p = 0$ for large p, $\sum k_p$ even$\}$ has index 4 in $\mathbf{Q}^*$. For every prime p, $\{1, -1, p, -p\}$ is a diagonal of G. It is, however, easy to see that there exists no finite set $M \subseteq \mathbf{Z}$ with $\mathbf{Z} \subseteq M \cdot (G \cap \mathbf{Z})$. In order to prove $(*)$ it is sufficent to show that $(G \cap \mathbf{Z}) - (G \cap \mathbf{Z})$ contains 1 and all primes p. Now note that $1 = 10 - 9$, $2 = 6 - 4$, and $2j - 1 = j^2 - (j-1)^2$ (for $j > 1$).

(iv) Choose $m \in \mathbf{N}$ and $c_p \in \mathbf{Z}$ (for every prime p), where $c_p = 0$ for large p. Then $G = \{\pm \prod_{p \text{ primes}} p^{k_p} : k_p \in \mathbf{Z},\ k_p = 0$ for large p, $\sum c_p k_p \equiv 0 \pmod{m}\}$ has index $\leq m$. Consider nonnegative integers l_p such that $l_p = 0$ for large p. Set $k_p = m$ if $c_p \neq 0$, $l_p = 0$; set $k_p = 0$ in all other cases. It is then easy to see that $\prod p^{k_p}$ and $\prod p^{k_p} - \prod p^{l_p}$ both belong to $G \cap \mathbf{Z}$ which proves $(*)$ since $-1 \in G \cap \mathbf{Z}$.

2. Results concerning G_k, S_k, and S

2.1. **Proposition.** *$S + S \subseteq S$ and $S^* = S \setminus \{0\}$ is a group.*

Proof. Obviously, $S + S \subseteq S$ and $S \cdot S \subseteq S$. If $x \in F^*$ then $x^m \in G$ for some $m \in \mathbf{N}$ since otherwise all cosets $x^k G$ $(k \in \mathbf{Z})$ are distinct. Thus $x^{-1} = x^{m-1} x^{-m} \in S$ if $x \in S^*$.

2.2. *Proof of Theorem* 2. Let $-1 \in S$ and assume that there exists $x \in F \setminus S$. The cosets $(a + x)G$ with $a \in G \cup \{0\} \subseteq S$ are distinct since $a + x = (a_1 + x)a_2$ with $a, a_1, a_2 \in S$ yields $x(a_2 - 1) = a - a_1 a_2 \in S$ and hence (by Proposition 2.1) $a_2 - 1 = 0$, $a = a_1$. Moreover, $a + x \neq 0$ and $(a + x)G \neq G$. Hence $|G| + 2 \leq n$ and $|F| = n|G| + 1 \leq (n-1)^2$.

2.3. *Remark.* Let $F = \mathbf{F}_{q^2}$ and $G = \mathbf{F}_q^*$. Then $n = q + 1$ and $-1 \in S \subseteq \mathbf{F}_q \neq F$. Since $|F| = (n-1)^2$, this shows that the bound in Theorem 2 is optimal for infinitely many n.

2.4. *Proof of Theorem* 3. (i) Some element of G belongs to $G + G$ and thus $G \subseteq G + G$. Inductively, $S_k \subseteq G_k$ for all k and hence $S_k = G_k$.

(ii) This is evident from the definitions.

(iii) For every $k \in \mathbf{N}$, S_k is a union of cosets of G possibly together with $\{0\}$. Thus the assertion follows from (ii).

(iv) n is even since $-1 \notin G$ (cf. Proof 1.4). We have $0 \notin S$ since otherwise $0 \in G_k$ for some $k \geq 2$ and hence $-1 \in G_{k-1} \subseteq S$. Thus (by 2.1) S is a subgroup of F^*. Since $G \leq S \neq F^*$, we obtain $(S : G) \leq n/2$ and thus (ii) yields $S_{n/2} = S$ (since each S_k is a union of cosets of G).

2.5. *Remark.* It is easy to see that $G \subseteq G - G$ is equivalent to $G \subseteq G + G$. According to Theorem 1, the hypothesis $G \subseteq G - G$ may be omitted in (i) if $|F| \geq (n-1)^4 + 4n$. Choosing $G = \{1\}$ shows that some additional assumption is required in general.

Now let $F = \mathbf{Q}$ and define G as in Remark 1.8(i). Note that G has index $p - 1$ and $1, \ldots, p-1$ is a diagonal. If $1 \leq k < p$ then, putting $l = p - 1 - k$ and $G_0 = \{0\}$, we have $k = (1 - lp) + k - 1 + lp \in G + G_{k-1} + G_l = G_{p-1}$. Hence $F^* \subseteq G_{p-1}$ and $S = F$. It is easy to see that $0 \notin G_{p-1}$ and thus, since $S_k = G_k$ for all k, $S_{p-1} \neq S$. Consequently, the index $n + 1$ in (iii) is optimal if $n + 1$ is a prime (cf. [1, §3]). Since G contains negative elements (e.g., $1 - p$), the subgroup G_+ of positive elements of G has index 2 in G

and hence $(F^*: G_+) = 2(p-1)$. We have $p-1 \notin S_{p-2}$ since otherwise $0 = (p-1)+(1-p) \in S_{p-1} = G_{p-1}$. Since every positive integer is a sum of elements of any given subgroup, this shows that the index $\frac{n}{2}$ in (iv) is optimal if $n = 2(p-1)$ for some prime p.

2.6. *Remark.* In Proposition 2.1(b) of [1] it is stated that $-1 \in S$ implies $S_{n+1} = F$. (The notation $k \times G$, P_k, P in [1] corresponds to G_k, S_k, S used in this paper.) This is correct if F is infinite (cf. Theorem 2) but may fail for finite fields (cf. Remark 2.3). (In [1] a result is quoted from [3] without the hypothesis on $|F|$ made there.) Theorem 3(iv) improves the second part of Proposition 2.1(b) of [1]; thus the title of §3 in [1] is misleading.

2.7. *Remark.* Let $k > 1$. It is easy to see that $0 \in G_k$ holds iff $-1 \in G_{k-1}$. If $-1 \in G_{k-1}$ and $G - G = F$ then $F \subseteq G + G_{k-1} = G_k$ (cf. [1, 1.2]). Thus the following three statements are equivalent if $G - G = F$: $G_k = F$, $0 \in G_k$, $-1 \in G_{k-1}$; moreover, $G_k = S_k$ (by Theorem 3(i)).

Note added in proof

For infinite F Theorem 1 is a special case of the results in a recently published paper by V. Bergelson and D. B. Shapiro (*Multiplicative subgroups of finite index in a ring*, Proc. Amer. Math. Soc. **116** (1992), 885–896). Their proof is based on the amenability of abelian groups and a simple version of Ramsey's Theorem.

References

1. P. Berrizbeitia, *Additive properties of multiplicative subgroups of finite index in fields*, Proc. Amer. Math. Soc. **112** (1991), 365–369.
2. R. L. Graham, B. L. Rothschild, and J. H. Spencer, *Ramsey theory*, Wiley, New York, 1980.
3. D. B. Leep and D. B. Shapiro, *Multiplicative subgroups of index three in a field*, Proc. Amer. Math. Soc. **105** (1989), 802–807.
4. R. Lidl and H. Niederreiter, *Finite fields*, Addison-Wesley, Reading, MA, 1983.

Mathematisches Institut, Universität Tübingen, Auf der Morgenstelle 10, D-72076 Tübingen, Federal Republic of Germany

E-mail address: turnwald@mailserv.zdv.uni-tuebingen.de