PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 105, Number 4, April 1989

MULTIPLICATIVE SUBGROUPS OF INDEX THREE IN A FIELD

DAVID B. LEEP AND DANIEL B. SHAPIRO

(Communicated by Louis J. Ratliff, Jr.)

ABSTRACT. **Theorem.** If 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. The elementary methods used here provide a new proof of the classical case when F is finite.

If F is a finite field and $|F| \neq 4$ or 7, then every element $c \in F$ can be expressed as a sum of two cubes: $c = x^3+y^3$ for some x, $y \in F$. Furthermore such x, y exist with $xy \neq 0$ in F provided $|F| \neq 4$, 7, 13, 16. Versions of these results have appeared in various forms in the literature. For example, see [3 p. 95 and p. 104, 7, 8, and 9]. This theorem also follows from the known values of the cyclotomic numbers when $e = 3$, as given for example in [10, p. 35].

We present here a generalization to arbitrary fields. If F is a finite field where the multiplicative group F^* has order divisible by 3, then the nonzero cubes F^{*3} form the unique subgroup of index 3 in F^*.

Theorem. *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.*

The Theorem is proved in an elementary fashion, not using the classical results mentioned above. It is valid for fields of any cardinality and any characteristic.

1. PRELIMINARIES

Let $G \subseteq F^*$ be a subgroup of finite index n. Then $x^n \in G$ for every $x \in F^*$. Let $\sum G$ denote the additive closure of G. That is, $\sum G = \{g_1+g_2+\cdots+g_m | g_i \in G\}$. Then $P = \sum G$ satisfies $P+P \subseteq P$ and $P \cdot P \subseteq P$. Also, if $0 \neq x \in P$ then $x^{-1} \in P$, because $x^{-1} = x^{n-1}(x^{-1})^n$.

1. **Lemma.** *Suppose $-1 \in P = \sum G$. Then P is a subfield of F.*
(1) *If F is infinite then $P = F$.*

Received by the editors May 2, 1988 and, in revised form, October 17, 1988.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 12E99.

(2) *If* F *is finite with* $[F: P] = d$ *and* $|P| = q$ *then* $[F^*: P^*] = (q^d - 1)/(q - 1)$.

Proof. If $-1 \in P = \sum G$ then P is also closed under subtraction, so that P is a subfield of F. (1) Suppose $P \neq F$ and choose $\alpha \in F$ with $\alpha \notin P$. Then the cosets $(a+\alpha)P^*$ are all distinct for $a \in P$. For if $(a+\alpha)P^* = (b+\alpha)P^*$ where a, $b \in P$ then $a+\alpha = (b+\alpha)c$ for some $c \in P$. Then $a-bc = (c-1)\alpha$ implies $c = 1$ and $a = b$. Since $G \subseteq P^*$, we have $n = |F^*/G| \geq |F^*/P^*| \geq |P| \geq |G|$. This implies F^* is finite, contrary to hypothesis. (2) $|F| = q^d$ so the index is $[F^*: P^*] = |F^*|/|P^*|$. □

If $-1 \notin \sum G$ then $\sum G$ is a "torsion preordering" of the field F. These preorderings and the related "orderings of level n" have been studied extensively by E. Becker. See [1] for a survey of this theory. For our question, even the case when the index is 2 provides some difficulty.

2. **Proposition.** *Suppose* G *is a subgroup of index* 2 *in* F^* *and* $|F| \neq 3, 5$. *Then one of the following holds.*

(1) $G + G = G$ *and* G *is the positive cone of an ordering in* F.

(2) $G + G \supseteq F^*$, *with equality if and only if* $-1 \notin G$.

Furthermore, if $a \notin G$ *then* $G + aG \supseteq F^*$ *with equality if and only if* $-1 \in G$.

Proof. Suppose first that $G + G \subseteq G \cup \{0\}$. If $-1 \notin G$ then $G + G = G$ and $F^* = G \cup -G$ so that G is the positive cone of an ordering. (See [5] or other algebra texts for information on orderings.) Otherwise $-1 \in G$ and $P = \sum G = G \cup \{0\}$. By hypothesis we know that $[F^*: P^*] = [F^*: G] = 2$. But Lemma 1 states that if F is infinite then this index equals 1, and if F is finite it equals $(q^d - 1)/(q - 1)$. Both cases are impossible.

Now suppose there exists $x \in G+G$ with $x \notin G \cup \{0\}$. Then $F^* = G \cup xG$ and $xG \subseteq G + G$.

Claim. There exists $g \in G$ with $g \in G + G$. To prove this first suppose $\operatorname{char} F \neq 2$. The identity $(x^2 + 1)^2 = (x^2 - 1)^2 + (2x)^2$ shows that G meets $G+G$, provided we can choose $x \in F$ with $x^2 + 1$, $x^2 - 1$, and $2x$ nonzero. These polynomials have at most 5 roots, so since $|F| > 5$ the claim is proved. Now suppose F has characteristic 2. If F is finite then $|F^*|$ is odd contrary to the existence of G. If F is infinite we can choose $a \in F$ with $a \neq 0, 1$. Then $(1 + a)^2 = 1 + a^2 \in G + G$, as claimed.

From the Claim we conclude that $G \subseteq G + G$ and hence $F^* = G \cup xG \subseteq G + G$. To complete the proof of (2) we see that $0 \notin G + G$ if and only if $-1 \notin G$. For the last statement, note that $G + aG$ must meet (and hence contain) one of the two cosets. Scaling by a shows that $G + aG \supseteq G$ iff $G + aG \supseteq aG$. Then $G + aG \supseteq G \cup aG = F^*$. Finally we have $0 \notin G + aG$ if and only if $-1 \notin aG$ if and only if $-1 \in G$. □

Remark. There are no proper subgroups of finite index in $\mathbb{C}^*$ and no subgroups of finite index greater than 2 in $\mathbb{R}^*$, because $\mathbb{C}^*$ and $\mathbb{R}^+$ are divisible groups.

In the rational field $\mathbb{Q}$ there are many multiplicative subgroups of finite index in $\mathbb{Q}^*$, because $\mathbb{Q}^*$ is generated by the set $\mathscr{P} = \{-1\} \cup \{\text{primes in } \mathbb{Z}^+\}$. To form a subgroup of index 2, choose any partition $\mathscr{P} = A \cup B$ where B is nonempty, and define $G = G(A, B)$ to be the subgroup of index 2 with $A \subseteq G$ and $B \subseteq xG$ (where xG is the nontrivial coset). That is, G is generated by all nonzero squares, all $a \in A$ and all products $b_1 b_2$ where $b_1, b_2 \in B$. For example if $A = \{-1\}$ and $B = \{\text{all primes}\}$ then an integer n lies in $G_1 = G(A, B)$ iff $n = \pm p_1 p_2 \cdots p_k$ where the p_i are primes and k is even. Similarly if A is empty and $B = \mathscr{P}$ then an integer lies in $G_0 = G(\varnothing, \mathscr{P})$ iff $n = (-1)^k p_1 p_2 \cdots p_k$ where the p_i are primes. If $\mathscr{P}$ is partitioned into three subsets, $\mathscr{P} = A \cup B \cup C$ where $B \cup C$ is nonempty, then there is an associated subgroup $G = G(A, B, C)$ of index 3 with $A \subseteq G$ and with B lying in one of the nonidentity cosets and C in the other. Further details and generalizations are omitted.

2. Proof of the Theorem

Throughout this section we assume that G is a subgroup of index 3 in the multiplicative group F^*. This implies that $F^{*3} \subseteq G$, and in particular $-1 \in G$. We begin the proof by establishing a technical lemma which says that a given proper finite subgroup can be avoided.

3. **Lemma.** *Suppose G is a subgroup of index 3 in F^*. Let $H \subseteq G$ be a finite proper subgroup of G. Then there exists $g \in G$ with $1 - g \notin G$ and $g \notin H$.*

Proof. First we find one $g \in G$ with $g \neq 1$ and $1 - g \notin G$. If $G + G \subseteq G \cup \{0\}$ then $G \cup \{0\}$ is additively closed and Lemma 1 yields the contradiction $G = F^*$ if F is infinite. If F is finite, then using the notation from Lemma 1 we have $3 = (q^d - 1)/(q - 1)$. This implies $|F| = 4$ and $|G| = 1$ so that G has no proper subgroup, contrary to hypothesis. Therefore there exist a, $b \in G$ with $a + b \notin G \cup \{0\}$. Defining $g = -a^{-1}b$ we have $g \in G$ with $g \neq 1$ and $1 - g \notin G$. Let us fix this element g.

Suppose the conclusion of the Lemma fails, and choose any $c \in G \backslash H$. Since $c \notin H$ the hypothesis implies $1 - c \in G$. Also since $1 - g \notin G$ we have $g \in H$. Therefore $cg \notin H$, so that $1 - cg \in G$. Since $(1 - c) - (1 - cg) = -c(1 - g) \notin G$, we know that $x = (1 - cg)/(1 - c) \in G$ satisfies $1 - x \notin G$, and hence $x \in H$. Moreover $x \neq g$ since $g \neq 1$. Letting $n = |H|$, we conclude that there are at most $n - 1$ possibilities for x, and hence also for c since $c = (x - 1)/(x - g)$. Therefore $|G \backslash H| \leq n - 1$ so that $|G| \leq n + n - 1 < 2|H|$. This implies $G = H$ contrary to the hypothesis. □

Any finite subgroup of F^* is cyclic, so we are dealing with the various cyclic subgroups $H_k = \{x \in G : x^k = 1\}$. We will apply the lemma in the cases $k = 2$, 4, and 5. When $k = 5$ we have $n = |H_5|$ divides 5. Thus if $|F| > 16$ so that $|G| > 5$ then we can avoid H_5. Similarly if $|F| > 13$ we can avoid H_4 and if $|F| > 7$ we can avoid H_2.

Now we proceed with the proof of the Theorem.

4. **Lemma.** *For F and G as above suppose the 3 cosets are G, aG and a^2G. If $|F| > 7$, then $aG \cup a^2G \subseteq G + G$.*

Proof. By Lemma 3 there exists $g \in G$ with $1 - g \notin G$ and $g^2 \neq 1$. Then $1 - g$ and $1 + g$ are nonzero. We may choose the coset representative a in the Lemma to be $1 - g$. Since $a \in G + G$ we have $aG \subseteq G + G$. Suppose the claim is false so that a^2G is not in $G + G$. Then $G + G$ does not meet a^2G and $aG + aG$ does not meet G.

Since $1 + g \in G + G$ we have $1 + g \notin a^2G$. Similarly $(1 + g)(1 - g) = 1 - g^2 \notin a^2G$ and cancelling $a = 1 - g$ shows that $1 + g \notin aG$. The only possibility is $1 + g \in G$. Then also $1 - g^2 \in aG$. Next we analyze the element 2. Since $2 = 1 + 1$ we see $2 \notin a^2G$. If $2 \in aG$ we would have $1 + g = (1 - g) + 2g \in G \cap (aG + aG)$ contrary to hypothesis. Finally, if $2 = 0$ then $(1 - g)^2 = 1 + g^2 \in a^2G \cap (G + G)$, a contradiction. The only remaining possibility is $2 \in G$.

We can now analyze $1+g^2$. First we easily see $1+g^2 \notin a^2G$. If $1+g^2 \in aG$ then $1 - g^4 = (1 + g^2)(1 - g^2) \in (G + G) \cap a^2G$, a contradiction. Similarly if $1+g^2 \in G$ then $(1-g)^2 = (1+g^2) - 2g \in a^2G \cap (G+G)$. Finally if $1+g^2 = 0$ then $-2g = (1 - g)^2 \in a^2G$, another contradiction. All the possibilities for $1 + g^2$ have been eliminated. □

5. **Lemma.** *If $|F| > 16$ then $G \subseteq G + G$.*

Proof. Suppose the claim is false so that $G + G$ does not meet G. Since $|F| > 13$ there exists $g \in G$ with $1 - g \notin G$ and $g^4 \neq 1$. Then $1 - g$, $1 + g$, $1 - g^2$ and $1 + g^2$ are nonzero. Let $a = 1 - g$ so that $a \notin G$ as before. Then $1 + g \in G + G$ so that $1 + g \notin G$. Also $(1 + g)(1 - g) = 1 - g^2 \notin G$ so that $1 + g \notin a^2G$. Therefore $1 + g \in aG$. Similarly $1 + g^2 \notin G$ and since $1 - g^2 \in a^2G$ and $(1 + g^2)(1 - g^2) = 1 - g^4 \notin G$ we find $1 + g^2 \in a^2G$. Where does 2 lie? We have $2 = 1 + 1 \notin G$, $2 = (1 - g) + (1 + g) \notin aG$ and $2 = (1 + g^2) + (1 - g^2) \notin a^2G$. This is a contradiction provided $2 \neq 0$.

Suppose F has characteristic 2. Since $|F| > 16$ Lemma 3 implies that there exists $h \in G$ with $1 - h \notin G$ and $h^5 \neq 1$. Let $a = 1 + h \notin G$ with the cosets as before. Then $(1+h)(1+h+h^2+h^3) = 1+h^4 = (1+h)^4 \in aG$, and we have $1 + h + h^2 + h^3 \in G$. It follows that $1 + h^3 \neq 0$, for otherwise we would have $h(1+h) = h+h^2 \in G$, a contradiction. Now $(1+h+h^2)(1+h) = 1+h^3 \notin G$, so that $0 \neq 1 + h + h^2 \notin a^2G$. Also $1 + h + h^2 = (1 + h)^3 + h^3 \notin G$, and we have $1 + h + h^2 \in aG$. Let $x = 1 + h + h^2 + h^3 + h^4$. Then $x(1 + h) = 1 + h^5 \notin G$ so that $x \notin a^2G$. Also $x \neq 0$ since $h^5 \neq 1$. Finally note that $x = (1 + h + h^2 + h^3) + h^4 \notin G$ and $x = (1 + h) + h^2(1 + h + h^2) \notin aG$. This eliminates all possibilities for x, proving the lemma. □

Lemmas 4 and 5 show that if $|F| > 16$ then G, aG and a^2G all lie within $G + G$, and therefore $G + G = F$. Finally suppose $|F| \leq 16$. Since $|F| \equiv 1$

(mod 3) we have $|F \in \{4, 7, 13, 16\}$. Suppose $F = G + G$ for one of these fields. Listing $G = \{g_1, g_2, \dots, g_n\}$ we have $G + G = \{g_i + g_j : i \le j\}$. Then $3n + 1 = |F| = |G + G| \le n(n+1)/2$. This implies $n^2 - 5n - 2 \ge 0$, so that $n \ge 6$ and $|F| \ge 19$. Therefore the cases $q = 4$, 7, 13, and 16 must be exceptional. The proof of the theorem is now complete.

To finish our analysis of the additive structure of G we consider sums of other cosets. If $a \notin G$ then certainly $0 \notin G + aG$. Does $G + aG$ always equal F^*?

6. **Proposition.** *Suppose G has index 3 in F^* and suppose $a \in G + G$ with $a \notin G \cup \{0\}$.*

(1) *If F is finite then $G + aG = F^*$ except when $|F| = 4$ or 7.*

(2) *If F is infinite then $G \cup aG \subseteq G + aG$. There are examples where $a^2 G \nsubseteq G + aG$.*

Proof. Expressing $a = g + h$ for g, $h \in G$ we have $g = -h + a \in G + aG$, so that $G \subseteq G + aG$. If $|F| \ne 4$, 7 then Lemma 4 implies that we can write $a^2 = x + y$ where x, $y \in G$. Then $ax = a^3 - ay \in G + aG$, so that $aG \subseteq G + aG$. To complete the proof of (2) we furnish an explicit example. Let $F = \mathbb{Q}_p$ be the field of p-adic numbers with p-adic valuation v, and let $G = v^{-1}(3\mathbb{Z}) = \{p^{3k}u : k \in \mathbb{Z}$ and u is a p-adic unit$\}$. Then $F^* = G \cup pG \cup p^2 G$. There cannot be an equation $g_1 + pg_2 = p^2 g_3$ because these three quantities have unequal p-adic values.

To finish the proof of (1) we show that $a^2 G \subseteq G + aG$ when $|F| = q$ is finite. We copy the counting argument found in Lemma 1 of [6]. Let $W = \{g - 1 : 1 \ne g \in G\}$. Then $|W| = (q-4)/3$. Let $V = G \cup W \cup W^{-1}$ and note that $|V| \le q - 3$. Choose $\delta \in F^*$ with $\delta \notin V$. Then $\delta \notin G$ and since δ and $\delta^{-1} \notin W$ we have $1 + \delta$ and $1 + \delta^{-1} \notin G$. Then $1 + \delta \notin G \cup \delta G$, forcing $1 + \delta \in \delta^2 G$. Therefore $\delta^2 G \subseteq G + \delta G$. Scaling by δ^2 we also find $\delta G \subseteq G + \delta^2 G$. Since aG equals either δG or $\delta^2 G$ we conclude that $a^2 G \subseteq G + aG$. □

3. Open questions

What happens when the index of G is greater than 3? When F is finite a positive answer can be given as before.

7. **Theorem.** *Let $F = \mathbf{F}_q$ be the finite field of q elements. Suppose e is a positive divisor of $q - 1$ and let a, $b \in F^*$.*

(1) *if $q > (e-1)^4$ then every element of F is expressible as $ax^e + by^e$, for x, $y \in F$.*

(2) *If $q \ge (e-1)^4 + 4e$ then every element of F^* is expressible as $ax^e + by^e$, for x, $y \in F^*$.*

Proof. For $c \in F^*$ let $N(c)$ be the number of solutions $(x, y) \in F \times F$ of $ax^e + by^e = c$. The estimate $|N(c) - q| \le (e-1)^2 \sqrt{q}$ appears in [4 p. 57]. In

[9] this estimate was used to prove (1). Part (2) follows similarly be requiring that $N(c)$ be more than $2e$, the maximal number of trivial solutions. □

For more information on these techniques see Chapter 8 of [3]. Slightly better bounds than those in Theorem 7 were obtained in [2]. These improvements can be derived using Theorem 5 on p. 103 of [3].

With these estimates and some calculations one can list the exceptional finite fields for any given exponent e. For example here are the results when e is 4 or 5.

8. **Corollary.** *Let $F = \mathbf{F}_q$ be the finite field of q elements.*

(1) *Let $G = F^{*4}$. Then $G+G = F^*$ if $q \equiv 3, 5, 7 \pmod 8$ and $G+G = F$ otherwise, except for the cases $q = 3, 5, 9, 13, 17, 25, 29$ and 41.*

(2) *Let $G = F^{*5}$. Then $G+G = F$ except for the cases $q = 11, 16, 31, 41, 61, 71$ and 101.*

It is natural to hope that our Theorem on index 3 can be generalized to subgroups of higher index. To be concrete we make an explicit conjecture when $e = 5$. We have been unable to prove it even when F is the field of rational numbers.

9. **Conjecture.** *If F is an infinite field and G is a subgroup of index 5 in F^* then $G + G = F$.*

Acknowledgments

We are grateful to Pedro Berrizbeitia for his valuable input to this work. The original idea for proving this Theorem arose during several conversations with him. We also thank the referee for helping to clarify some of the proofs.

References

1. E. Becker, *Extended Artin-Schreier theory of fields*, Rocky Mountain J. Math. **14** (1984), 881–897.
2. A. Hurwitz, *Über die Kongruenz $ax^e + by^e + cz^e \equiv 0 \pmod p$*, J. Reine Angew. Math. **136** (1909), 272–292.
3. K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Springer-Verlag, Berlin, 1982.
4. J.-R. Joly, *Équations et variétés algébriques sur un corps fini*, Enseign. Math. **19** (1973), 1–117.
5. T.-Y. Lam, *The algebraic theory of quadratic forms*, Benjamin, Reading, Mass., 1973.
6. D. J. Lewis, *Cubic congruences*, Michigan Math. J. **4** (1957), 85–95.
7. T. Nagell, *On the solvability of some congruences*, Norski Vid. Selsk. Forh. (Trondheim) **27** (1954), 1–5.
8. E. Selmer, *The diophantine equation $ax^3 + by^3 + cz^3 = 0$*, Acta Math. **85** (1951), 203–362.
9. C. Small, *Sums of powers in large finite fields*, Proc. Amer. Math. Soc. **65** (1977), 35–36.
10. T. Storer, *Cyclotomy and difference sets*, Markham, Chicago, 1967.

Department of Mathematics, University of Kentucky, Lexington, Kentucky 40506

Department of Mathematics, Ohio State University, Columbus, Ohio 43210