DIVISIBLE MULTIPLICATIVE GROUPS OF FIELDS

GREG OMAN

Abstract. Some time ago, Laszlo Fuchs asked the following question: which abelian groups can be realized as the multiplicative group of (nonzero elements of) a field? The purpose of this note is to answer his query within the class of divisible abelian groups.

1. Introduction

In [7] (Problem 69), Laszlo Fuchs asks which abelian groups can be realized as the multiplicative group of (nonzero elements of) a field. Many decades later, this question is largely unsolved, though quite a few partial results have been obtained. We refer the reader to [1], [4]–[6], [8]–[12], [15]–[17], and [20]–[23] for a sampling of what is known on this question (and related results). As stated in the abstract, it is the purpose of this paper to solve Fuchs' problem for the class of divisible abelian groups.

We begin by recalling some definitions and results from the theory of divisible abelian groups to which we shall refer throughout the paper.

Definition 1. *An abelian group G (written additively) is divisible provided for every $g \in G$ and every positive integer n, there exists $h \in G$ with $nh = g$.*

The most natural nontrivial example of a divisible abelian group is the additive group $\mathbb{Q}$ of rational numbers. Another example is the direct limit of the cyclic groups $\mathbb{Z}/\langle p^n \rangle$ (p a prime). This group is the so-called *quasi-cyclic group of type p^∞*, denoted $C(p^\infty)$. Divisible abelian groups play a fundamental role in group theory. In particular, they are precisely the injective objects in the category of abelian groups. Moreover, their structure is well-understood:

Structure Theorem for Divisible Abelian Groups. Let G be an abelian group. Then G is divisible if and only if G is a direct sum of copies of $\mathbb{Q}$ and $C(p^\infty)$ for various primes p.

2010 Mathematics Subject Classification: 12E99, 20K99 (primary); 03C98 (secondary).

Key Words and Phrases: absolutely algebraic extension, Compactness Theorem, cyclic extension, elementary equivalence, Lós-Vaught Test, Lowenheim-Skolem Theorem, primitive pth root of unity.

Despite the relatively simple structure of divisible abelian groups, many questions involving them are quite difficult. For example, the subgroups of $\mathbb{Q}$ have been classified, yet the problem of classifying the subgroups of $\mathbb{Q} \times \mathbb{Q}$ is notoriously difficult. Even now, the subgroup structure of $\mathbb{Q} \times \mathbb{Q}$ is not well-understood.

To begin our investigation, we note that many partial results on the problem of classifying the divisible abelian groups realizable as the multiplicative group of a field are known. One of the earliest results in the direction appears in [7]. We remark that below and throughout this paper, $K^\times$ denotes the multiplicative group of (nonzero elements of) a field K.

Lemma 1 ([7], Theorem 77.1)**.** *Let K be an algebraically closed field. Then either*

(1) $K^\times \cong (\bigoplus_{i=1}^\infty C(p_i^\infty)) \oplus (\bigoplus_\kappa \mathbb{Q})$, *or*
(2) $K^\times \cong (\bigoplus_{p_i \neq p}^\infty C(p_i^\infty)) \oplus (\bigoplus_\kappa \mathbb{Q})$,

where $(p_i : i < \omega)$ is an enumeration of the primes. Moreover, (1) holds if K has characteristic 0, and (2) holds if K has characteristic p. Further, κ is a cardinal which is equal to $|K|$ except in (2) when K is algebraic over its prime subfield. In this case, $\kappa = 0$. Conversely, for any group G of the form (1) or (2), there exists an algebraically closed field K such that $K^\times \cong G$.

Notice that none of the groups appearing in Lemma 1 is torsion-free. Thus, a natural question is

Question 1. *Which nontrivial torsion-free divisible abelian groups can be realized as the multiplicative group of a field?*

Adler obtained a partial result in this direction some time ago. In particular, he shows in [1] that a countably infinite direct sum of copies of $\mathbb{Q}$ is isomorphic to the multiplicative group of some field. A complete answer to Question 1 was given by Contessa, Mott, and Nichols in [5][1]:

Lemma 2 ([5], Theorem 5.5)**.** *A nontrivial torsion-free divisible abelian group G can be realized as the multiplicative group of a field if and only if G has infinite rank.*

The purpose of this article is to extend the above classification to the class of divisible abelian groups. We refer the reader to the popular texts [3], [7], and [13]–[14] for standard results in model theory, abelian group theory, and field/Galois/elementary number theory, respectively (many of which shall be invoked throughout the paper).

2. The Characteristic Zero Case

In this section, we characterize the divisible abelian groups which are isomorphic to the multiplicative group of a field of characteristic zero. Toward this end, we shall

[1] Their result can be derived in a couple lines from Adler's paper; we conclude Section 3 with an elaboration.

make use of the following result of Contessa, Mott, and Nichols. We present a simple, self-contained proof using basic principles.

Lemma 3 ([5], Corollary 2.4)**.** *Let G be an abelian group with finite, nonzero torsion-free rank. Then G is not isomorphic to the multiplicative group of any field.*

Proof. Let F be a field for which there exists $x \in F^\times$ of infinite order. If F has characteristic 0, then F contains the infinite set $\mathcal{P}$ of prime numbers, and this set is (multiplicatively) linearly independent over $\mathbb{Z}$. Suppose now that F has characteristic p. Since x has infinite multiplicative order, it follows that x is transcendental over $\mathbb{F}_p$. Now pick an infinite set $\mathcal{S}$ of non-associate irreducible polynomials in $\mathbb{F}_p[x]$. Again, $\mathcal{S}$ is linearly independent over $\mathbb{Z}$, and the proof is complete. □

Theorem 1. *Let G be a divisible abelian group. Then G is the multiplicative group of a field of characteristic 0 if and only if $G \cong (\bigoplus_{i=1}^{\infty} C(p_i^\infty)) \oplus (\bigoplus_\kappa \mathbb{Q})$, where $(p_i : i < \omega)$ is an enumeration of the primes and κ is an infinite cardinal.*

Proof. Suppose first that $G \cong (\bigoplus_{i=1}^{\infty} C(p_i^\infty)) \oplus (\bigoplus_\kappa \mathbb{Q})$ and κ is infinite. Then Lemma 1 implies that $G \cong F^\times$, where F is an algebraically closed field of characteristic 0 and cardinality κ. Conversely, assume that $G \cong F^\times$ for some field F of characteristic 0. Since G is divisible, $G = T(G) \oplus H$ where $T(G)$ is the (divisible) torsion subgroup of G and H is a $\mathbb{Q}$-vector space. Since F has characteristic 0, it follows that there are elements of G of infinite multiplicative order. We deduce from Lemma 3 that H has infinite rank. Now, $T(G)$ is a direct sum of copies of $C(p^\infty)$ for various primes p. Since $T(F^\times)$ is locally cyclic, no $C(p^\infty)$ summand is repeated. To conclude the proof, it suffices to show that for every prime p, F possesses a primitive pth root of unity. Suppose not, and let p be least such that F has no primitive pth root of unity. Then of course $p > 2$. Fix an algebraic closure F^a of F, and let $\zeta_p \in F^a$ be a primitive pth root of unity. Then $F(\zeta_p)/F$ is a cyclic Galois extension of degree $d|p-1$. Now let $q|d$ be a prime, and let $F \subseteq K \subseteq F(\zeta_p)$ be an intermediate field such that $[K : F] = q$. Then K/F is a cyclic Galois extension of degree q. By minimality of p, F contains a primitive qth root of unity ζ_q. Thus K is a splitting field over F of a polynomial of the form $x^q - b \in F[x]$, and $K = F(u)$ for any root u of $x^q - b$ (see Theorem 7.11 of [13]). Let $u \in F^a$ be such a root. Then $u^q = b \in F$. Recall that $F^\times$ is divisible. Thus some qth root of u^q lies in F. However, F also contains a primitive qth root of unity. Therefore, *all* qth roots of u^q lie in F. In particular, $u \in F$. But since $K = F(u)$, it follows that $K = F$, contradicting that $[K : F] = q$. □

We now present two corollaries of the previous theorem.

Corollary 1. *Let F and K be fields of characteristic zero of the same cardinality. Suppose further that $F^\times$ is divisible and K is algebraically closed. Then $F^\times \cong K^\times$.*

Proof. Immediate from Theorem 1. □

Corollary 2. *Let $\mathbb{Q}^a$ be an algebraic closure of $\mathbb{Q}$. There exists a field F satisfying $\mathbb{Q} \subseteq F \subseteq \mathbb{Q}^a$ (that is, F is absolutely algebraic of characteristic 0) such that $F^+ \cong (\mathbb{Q}^a)^+$ and $F^\times \cong (\mathbb{Q}^a)^\times$, yet F is not algebraically closed.*

Proof. Let $\mathbb{Q}^r$ be a root closure of $\mathbb{Q}$ and let $\mathbb{Q}^a$ be an algebraic closure. Then note that $(\mathbb{Q}^r)^+ \cong (\mathbb{Q}^a)^+ \cong \bigoplus_{\aleph_0} \mathbb{Q}$. Further, the previous corollary implies that $(\mathbb{Q}^r)^\times \cong (\mathbb{Q}^a)^\times$. To finish the proof, let $f(x) \in \mathbb{Q}[x]$ be a polynomial that is not solvable by radicals. Then not all roots of $f(x)$ lie in $\mathbb{Q}^r$, and thus $\mathbb{Q}^r$ is not algebraically closed. □

3. The Characteristic p Case

We begin this section with a determination of the divisible abelian groups G which can be realized as the multiplicative group of an absolutely algebraic field of characteristic p. To do this, we introduce some new terminology.

Definition 2. *Let $\mathcal{S}$ be a nonempty subset of the positive integers, and let p be a prime. Let us call $\mathcal{S}$ a p-divisible system if and only if $\mathcal{S}$ satisfies the following conditions:*

(i) If $\alpha \in \mathcal{S}$, $x > 0$, and $x|\alpha$, then $x \in \mathcal{S}$.
(ii) If $\alpha, \beta \in \mathcal{S}$, then lcm$(\alpha, \beta) \in \mathcal{S}$.
(iii) If $\alpha \in \mathcal{S}$ and q is a prime such that $p^\alpha \equiv 1(mod\ q)$, then $q^i \in \mathcal{S}$ for every positive integer i.

We now present some illustrative examples.

Example 1. *$\{1\}$ is a 2-divisible system.*

Example 2. *Let k be a fixed positive integer, and let $\mathcal{S}_k := \{n \in \mathbb{Z}^+ :$ every prime divisor of n is at least $k\}$. Then $\mathcal{S}$ is a 2-divisible system*[2].

Example 3. *The set $\mathcal{S} := \{n \in \mathbb{Z}^+ : (n, p) = 1\}$ is a p-divisible system.*

More generally,

Example 4. *For any non-negative integer k, the set $\mathcal{S}_k := \{mp^i : m \in \mathbb{Z}^+, (m, p) = 1$, and $0 \leq i \leq k\}$ is a p-divisible system.*

Note that (ii) of Definition 2 implies that the product of relatively prime members of a p-divisible system $\mathcal{S}$ is also a member of $\mathcal{S}$. On the other hand, a p-divisible system need not be closed under multiplication, as Example 4 demonstrates. However, we do have the following:

[2] This general construction does not work for odd primes. Indeed, if p is an odd prime and $\mathcal{S}$ is a p-divisible system, then $p \equiv 1(\text{mod } 2)$, whence $2 \in \mathcal{S}$.

Lemma 4. *Let $\mathcal{S}$ be a p-divisible system. Then*

(1) $q^n \in \mathcal{S}$ for every prime $q < p$ and positive integer n, and
(2) $\mathcal{S} = \mathbb{Z}^+$ if and only if $p^n \in \mathcal{S}$ for arbitrarily large n.

Proof. We prove only (1), as the proof of (2) is similar. Suppose that $q^* < p$ is a prime and that $q^i \in \mathcal{S}$ for every prime $q < q^*$ and positive integer i. We will show that $(q^*)^i \in \mathcal{S}$ for every positive integer i. It suffices by (iii) to prove the existence of $\alpha \in \mathcal{S}$ such that $p^\alpha \equiv 1(\text{mod } q^*)$. If $q^* = 2$, then p is an odd prime and we may take $\alpha := 1$. Thus we assume that $q^* > 2$. Let $q^* - 1 = q_1^{n_1} \cdots q_k^{n_k}$ be the prime factorization of $q^* - 1$. By assumption, $q_i^{n_i} \in \mathcal{S}$ for $1 \leq i \leq k$. We deduce from (ii) that $q^* - 1 \in \mathcal{S}$. Fermat's Little Theorem implies that $p^{q^*-1} \equiv 1(\text{mod } q^*)$, and the proof is complete. □

We now relate the notion of a p-divisible system to the problem of determining the structure of $F^\times$ for an absolutely algebraic field F of positive characteristic with divisible multiplicative group.

Proposition 1. *Let p be a prime. Then the following hold:*

(1) If $\mathcal{S}$ is a p-divisible system, then $F := \bigcup_{\alpha \in \mathcal{S}} \mathbb{F}_{p^\alpha}$ (each $\mathbb{F}_{p^\alpha}$ is taken relative to a fixed algebraic closure of $\mathbb{F}_p$) has a divisible multiplicative group.
(2) Conversely, if F is an absolutely algebraic field of prime characteristic p such that $F^\times$ is divisible, then the set $\mathcal{S} := \{\alpha > 0 : \mathbb{F}_{p^\alpha} \subseteq F\}$ is a p-divisible system and $F = \bigcup_{\alpha \in \mathcal{S}} \mathbb{F}_{p^\alpha}$.

Proof. Let p be a prime number.

(1) Suppose that $\mathcal{S}$ is a p-divisible system, and consider $F := \bigcup_{\alpha \in \mathcal{S}} \mathbb{F}_{p^\alpha}$. We first show that F is a well-defined field. Clearly it suffices to show that for every $\alpha, \beta \in \mathcal{S}$, there exists $\gamma \in \mathcal{S}$ such that $\mathbb{F}_{p^\alpha} \cup \mathbb{F}_{p^\beta} \subseteq \mathbb{F}_{p^\gamma}$. By (ii) of Definition 2, we may take $\gamma = \text{lcm}(\alpha, \beta)$. It remains to show that the multiplicative group of F is divisible. We let q be an arbitrary prime, and show that $F^\times$ is q-divisible. We consider two cases.

Case 1: there exists some $\alpha \in \mathcal{S}$ such that $p^\alpha \equiv 1(\text{mod } q)$. Clearly

$$q \neq p \text{ and } q^i \in \mathcal{S} \text{ for every positive } i \text{ by (iii) of Definition 2.} \tag{3.1}$$

By definition of F, we have $\mathbb{F}_{p^\alpha} \subseteq F$. Since $\mathbb{F}_{p^\alpha}^\times$ has order $p^\alpha - 1$ and $q | p^\alpha - 1$, it follows that there exists an element $\zeta_q \in \mathbb{F}_{p^\alpha}^\times$ of multiplicative order q (i.e. ζ_q is a primitive qth root of unity). Let $a \in F^\times$ be arbitrary. We claim that a has a qth root in F. Choose $\beta \in \mathcal{S}$ such that $\zeta_q, a \in \mathbb{F}_{p^\beta}$, and let γ be any root of $x^q - a$. Then $\mathbb{F}_{p^\beta}(\gamma)$ is cyclic Galois over $\mathbb{F}_{p^\beta}$ of degree d for some $d|q$. If $d = 1$, then $\gamma \in \mathbb{F}_{p^\beta} \subseteq F$ and we are done. Thus assume $d = q$. Then $\mathbb{F}_{p^\beta}(\gamma) = \mathbb{F}_{p^{\beta q}}$. Recall that $\beta, q \in \mathcal{S}$. To finish this case, it suffices to show that $\beta q \in \mathcal{S}$. Write $\beta = q^i \lambda$, where $(\lambda, q) = 1$.

Since $\beta \in \mathcal{S}$, (i) of Definition 2 implies that $\lambda \in \mathcal{S}$. It follows from (3.1) above that $q^{i+1} \in \mathcal{S}$. We now conclude from (ii) of Definition 2 that $q^{i+1}\lambda = \beta q \in \mathcal{S}$.

Case 2: $q \nmid p^{\alpha} - 1$ for any $\alpha \in \mathcal{S}$. We let $a \in F^{\times}$ be arbitrary. By definition of F, we have $a \in \mathbb{F}_{p^{\beta}}$ for some $\beta \in \mathcal{S}$. Consider the function $f : \mathbb{F}_{p^{\beta}}^{\times} \to \mathbb{F}_{p^{\beta}}^{\times}$ defined by $f(x) := x^q$. We claim f is one-to-one. For suppose $x^q = y^q$. If $x \neq y$, then $\frac{x}{y}$ has multiplicative order q in $\mathbb{F}_{p^{\beta}}$. Lagrange's Theorem gives $q|p^{\beta} - 1$. But this contradicts our assumption. Hence f is one-to-one, thus onto. Therefore, a has a qth root in F and thus $F^{\times}$ is q-divisible in this case as well.

(2) Conversely, suppose that F is an absolutely algebraic field of prime characteristic p such that $F^{\times}$ is divisible, and set $\mathcal{S} := \{\alpha > 0 : \mathbb{F}_{p^{\alpha}} \subseteq F\}$. It is clear that $F = \bigcup_{\alpha \in \mathcal{S}} \mathbb{F}_{p^{\alpha}}$. We will show that $\mathcal{S}$ satisfies (i)–(iii).

(i). Suppose $\alpha \in \mathcal{S}$. Then by definition, $\mathbb{F}_{p^{\alpha}} \subseteq F$. If $x > 0$ and $x|\alpha$, then $\mathbb{F}_{p^{x}} \subseteq \mathbb{F}_{p^{\alpha}}$. Thus $x \in \mathcal{S}$.

(ii). Patent since the compositum of $\mathbb{F}_{p^{\alpha}}$ and $\mathbb{F}_{p^{\beta}}$ is $\mathbb{F}_{p^{\gamma}}$, where $\gamma = \operatorname{lcm}(\alpha, \beta)$.

(iii). We suppose that $q|p^{\alpha_1} - 1$ for some α_1 with $\mathbb{F}_{p^{\alpha_1}} \subseteq F$, and we show that $q^i \in \mathcal{S}$ for every positive integer i. There exists $x_1 \in \mathbb{F}_{p^{\alpha_1}}^{\times}$ of multiplicative order q. Since the multiplicative group of F is divisible, there exists $x_i \in F^{\times}$ of multiplicative order q^i for all $i > 0$ (recursively take qth roots of x_1). For each i, let α_i be such that $x_i \in \mathbb{F}_{p^{\alpha_i}} \subseteq F$ (note that by definition, $\alpha_i \in \mathcal{S}$). By Lagrange's Theorem, $p^{\alpha_i} \equiv 1 (\text{mod } q^i)$. We let $O(p)(\text{mod } q^i)$ denote the multiplicative order of p modulo q^i. Since $p^{\alpha_i} \equiv 1(\text{mod } q^i)$,

$$O(p)(\text{mod } q^i) \text{ divides } \alpha_i. \tag{3.2}$$

But by Lagrange's Theorem, $O(p)(\text{mod } q^i)$ divides $|\mathbb{Z}/(q^i)^{\times}| = \varphi(q^i) = q^{i-1}(q-1)$. We record this below.

$$O(p)(\text{mod } q^i) \text{ divides } q^{i-1}(q-1). \tag{3.3}$$

As $i \to \infty$, clearly $O(p)(\text{mod } q^i) \to \infty$. This fact, along with (3.2) and (3.3) above, implies that there exist arbitrarily large i such that $q^i|\alpha_i$. It now follows from (i) (established previously) that $q^i \in \mathcal{S}$ for every i. The proof is now complete. □

We are almost ready to classify the divisible abelian groups realizable as the multiplicative group of an absolutely algebraic field of positive characteristic. First, we present a final definition.

Definition 3. *Let p be a prime, and let $\mathcal{S}$ be a p-divisible system. Define the prime spectrum of $\mathcal{S}$, $P(\mathcal{S})$, by $P(\mathcal{S}) := \{q : q \text{ is prime and } O(p)(\text{mod } q) \in \mathcal{S}\}$.*

Proposition 2. *Let G be a divisible abelian group. Then G can be realized as the multiplicative group of an absolutely algebraic field of characteristic p if and only if $G \cong \bigoplus_{q \in P(\mathcal{S})} C(q^\infty)$ for some p-divisible system $\mathcal{S}$.*

Proof. Consider a fixed prime p and a p-divisible system $\mathcal{S}$. We show first that $\bigoplus_{q \in P(\mathcal{S})} C(q^\infty)$ can be realized as the (divisible) multiplicative group of an absolutely algebraic field of characteristic p. To see this, let $F := \bigcup_{\alpha \in \mathcal{S}} \mathbb{F}_{p^\alpha}$. Then Proposition 1 gives us that F is an absolutely algebraic field of characteristic p with divisible multiplicative group. It suffices to show that for each prime q, $F^\times$ has an element of multiplicative order q if and only if $q \in P(\mathcal{S})$. Thus let q be an arbitrary prime. Suppose first that F has an element x of multiplicative order q. Then $x \in \mathbb{F}_{p^\alpha}$ for some $\alpha \in \mathcal{S}$ and $x^q = 1$. It follows that $p^\alpha \equiv 1 (\text{mod } q)$. Hence $O(p)(\text{mod } q)$ divides α. By definition (i) of a p-divisible system, we deduce that $O(p)(\text{mod } q)$ is an element of $\mathcal{S}$. It follows now by definition of $P(\mathcal{S})$ that $q \in P(\mathcal{S})$. Conversely, suppose $q \in P(\mathcal{S})$. Then by defnition, $O(p)(\text{mod } q) := \alpha \in \mathcal{S}$. Hence $\mathbb{F}_{p^\alpha} \subseteq F$ and $p^\alpha \equiv 1(\text{mod } q)$. By Cauchy's Theorem, $\mathbb{F}_{p^\alpha}^\times$ has an element of multiplicative order q, whence so does $F^\times$.

Finally, consider an absolutely algebraic field F of characteristic p such that $F^\times$ is divisible. From Proposition 1, $S := \{\alpha > 0 : \mathbb{F}_{p^\alpha} \subseteq F\}$ is a p-divisible system and $F = \bigcup_{\alpha \in \mathcal{S}} \mathbb{F}_{p^\alpha}$. It now follows from our work above that $F^\times \cong \bigoplus_{q \in P(\mathcal{S})} C(p^\infty)$. □

Now that the smoke has cleared, let us pause to present an example. Recall from Example 3 that the set $\mathcal{S}$ of positive odd integers is a 2-divisible system. By Proposition 1, $F := \bigcup_{n \in \mathcal{S}} \mathbb{F}_{2^n}$ has a divisible multiplicative group. It now follows from Proposition 2 that

$$F^\times \cong C(7^\infty) \oplus C(23^\infty) \oplus C(31^\infty) \oplus C(47^\infty) \oplus \cdots .$$

Remark 1. The previous example shows that Corollary 1 fails for absolutely algebraic fields of positive characteristic. In particular, if F is the field in the above example, then Lemma 1 implies that $F^\times \ncong K^\times$ for any algebraically closed field K.

We can also show that the characteristic p analog of Corollary 2 fails.

Proposition 3. *Let $\mathbb{F}_p^a$ be an algebraic closure of $\mathbb{F}_p$, and suppose that F is a field such that $\mathbb{F}_p \subseteq F \subseteq \mathbb{F}_p^a$ and $F^\times \cong (\mathbb{F}_p^a)^\times$. Then $F \cong \mathbb{F}_p^a$.*

Proof. Let n be a positive integer, and note that $\mathbb{F}_p^a$ possesses exactly p^n elements (namely, the field $\mathbb{F}_{p^n}$) satisfying the equation $x^{p^n} = x$. But then via the isomorphism, it is clear that the same property is enjoyed by F. Thus F contains the field $\mathbb{F}_{p^n}$. Since n was arbitrary, we conclude that $F \cong \mathbb{F}_p^a$. □

As an application of Proposition 1 and Lemma 4, we have the following corollary.

Corollary 3. *Let F be an absolutely algebraic field of characteristic p. Then F is algebraically closed if and only if $F^\times$ is divisible and $\mathbb{F}_{p^{p^n}} \subseteq F$ for arbitrarily large n.*

Proof. We prove only the nontrivial direction. Assume that $F^\times$ is divisible and $\mathbb{F}_{p^{p^n}} \subseteq F$ for arbitrarily large n. Then by Proposition 1, $\mathcal{S} := \{n \in \mathbb{Z}^+ : \mathbb{F}_{p^n} \subseteq F\}$ is a p-divisible system. Lemma 4, part (2) implies that $\mathcal{S} = \mathbb{Z}^+$, whence F is algebraically closed. □

It remains to describe $F^\times$ in case F is an arbitary field of positive characteristic with divisible multiplicative group, but this is straightforward.

Theorem 2. *Let G be a divisible abelian group. Then G is the multiplicative group of a field of positive characteristic if and only if $G = H \oplus (\bigoplus_\kappa \mathbb{Q})$ for some divisible abelian group H realizable as the multiplicative group of an absolutely algebraic field of positive characteristic, and either $\kappa = 0$ or κ is infinite.*

Proof. Suppose first that $G = H \oplus (\bigoplus_\kappa \mathbb{Q})$, where H and κ are as stated. We will prove that G is the multiplicative group of a field of positive characteristic. Let F be an absolutely algebraic field of positive characteristic such that $F^\times \cong H$. If $\kappa = 0$, then $G \cong F^\times$, and we're done. So assume κ is infinite. Suppose first that $F^\times$ is trivial. Then $G = \bigoplus_\kappa \mathbb{Q}$, and Lemma 2 implies that G is the multiplicative group of some field K. It follows that K has characteristic 2 (lest -1 have order 2), and we are done in this case as well. Now suppose that $F^\times$ is nontrivial. Then since $F^\times$ is divisible, we see that that F is infinite. Suppose first that $\kappa > \aleph_0$, and let K be a field of size κ elementarily equivalent to F. Then $G \cong K^\times$. Now assume that $\kappa = \aleph_0$. Choose a field K of size $\aleph_1$ which is elementarily equivalent to F, and pick $\alpha \in K$ of infinite multiplicative order. Now let K' be a countable elementary submodel of K containing α. Lemma 3 implies that $G \cong K'^\times$, and this completes the proof of the first implication.

As for the second implication, Suppose that $G \cong K^\times$ for some field K of characteristic p. Recall that $G = T(G) \oplus H$, where $T(G)$ is the torsion subgroup of G and H is a $\mathbb{Q}$-vector space. Again, we invoke Lemma 3 to deduce that H is trivial or of infinite rank. Now, simply observe that $T(G) \cong (\mathbb{F}_p^*)^\times$, where $\mathbb{F}_p^*$ is the algebraic closure of $\mathbb{F}_p$ in K. Hence $\mathbb{F}_p^*$ is absolutely algebraic of positive characteristic, and the proof is complete. □

We conclude the section by sketching an elementary (model-theoretic) proof of Contessa, Mott, and Nichols' result that a torsion-free divisible abelian group of infinite rank is the multiplicative group of some field (Theorem 5.5 of [5]). Adler had essentially already established this result in 1978 when he showed that a torsion-free divisible abelian group of countably infinite rank is the multiplicative group of some field (now simply apply Upward Lowenheim-Skolem to obtain Theorem 5.5)). In fact, we prove the stronger result that every torsion-free divisible abelian group of infinite rank is the multiplicative group of a *pseudo-finite* field.

To begin, let $(p_i : i < \omega)$ be an enumeration of the primes, and consider the collection $\prod$ consisting of the union of the following sentences in the language of fields:

(0) the sentence φ asserting the existence of at least three objects,
(1) the schema $\mathcal{S}$ of axioms for the theory of finite fields (see [2]),
(2) for each positive integer i, the sentence $D_i := \forall x \exists y (y^{p_i} = x)$, and
(3) for each positive integer i, the sentence $TF_i := \forall x (x^{p_i} = 1 \Rightarrow x = 1)$.

We claim that every finite subset of $\prod$ has a model. Indeed, let $k > 0$ be an integer, and let $\Gamma := \{\varphi\} \cup \mathcal{S} \cup \{D_i : 1 \leq i \leq k\} \cup \{TF_i : 1 \leq i \leq k\}$. Now choose a prime number p such that $p_i < p$ for all i, $1 \leq i \leq k$. It is straighforward to check that $\mathbb{F}_{2^p}$ is a model of Γ. By the Compactness Theorem, there exists a structure F which is a model of $\prod$. Since F models (0) and (1), F is a pseudo-finite field with more than two elements. It follows from (2) that $F^\times$ is divisible; thus by (0), F is infinite. Lastly, (3) implies that $F^\times$ is torsion-free. Hence $F^\times$ is isomorphic to an infinite direct sum of copies of $\mathbb{Q}$ (this follows from Lemma 3 and The Structure Theorem for Divisible Abelian Groups). The Upward and Downward Lowenheim-Skolem Theorems apply, and we deduce that an arbitrary infinite direct sum of copies of $\mathbb{Q}$ is the multiplicative group of some pseudo-finite field.

We now obtain a short proof of the main theorem of [1] as a corollary.

Corollary 4 (Adler, 1978). *There is no set $\sum$ of sentences in the language of group theory with the property that for all groups G: G is a model of $\sum$ if and only if G is the multiplicative group of some field.*

Proof. Suppose by way of contradiction that such a set $\sum$ exists. It is well-known that the theory T of non-trivial torsion-free divisible abelian groups is complete (cf. [18] and [22]). Therefore, $\mathbb{Q}$ and $\bigoplus_{\aleph_0} \mathbb{Q}$ are elementarily equivalent. By our work above, $\bigoplus_{\aleph_0} \mathbb{Q}$ is isomorphic to the multiplicative group of a field, and therefore is a model of $\sum$. But then so is $\mathbb{Q}$, and it follows that $\mathbb{Q}$ is the multiplicative group of a field. However, this contradicts Lemma 3. □

4. An Open Question

We saw in Lemma 3 that if G is the multiplicative group of a field, then the torsion-free rank of G is either 0 or infinite. This observation leads naturally to the following question:

Problem 1. *Let G be a divisible abelian group realizable as the multiplicative group of a field. Is the torsion rank of G either* 0 *or infinite?*

At present, we have nothing deep to say about the solution to this problem, but we make some trivial observations. Let F be a field such that $F^\times$ is divisible. Since

$T(F^\times)$ is countable, $\aleph_0$ is an upper bound for $r(T(F^\times))$ (the rank of $T(F^\times)$). Moreover, $r(T(F^\times))$ cannot be 1 (in other words, for any prime p, $C(p^\infty)$ is not the multiplicative group of any field). This appears as Lemma 6 in [19]. Even the proof of this lemma employs a nontrivial result, namely Mihăilescu's Theorem (formerly Catalan's Conjecture). Recall that a *Fermat prime* is a prime number of the form 2^m+1 for some positive integer m. Let FP denote the set of Fermat primes. At present, only 5 Fermat primes are known; it is still open whether FP is infinite or not. In any case, we can use this set to obtain a somewhat crude lower bound for $r(T(F^\times))$ as follows: suppose that p is an odd prime and that F is absolutely algebraic of characteristic p with $F^\times$ divisible. Then

$$|FP| \leq r(F^\times)+1. \tag{4.1}$$

To see this, let $\mathcal{S}$ be the associated p-divisible system, and let q be a Fermat prime distinct from p. Since p is odd, $p \equiv 1 (\text{mod } 2)$. Therefore $2^i \in \mathcal{S}$ for every positive integer i by definition (iii) of a p-divisible system. Now, $2^m+1=q$ for some positive integer m. Thus $q-1 \in \mathcal{S}$. Since $p^{q-1} \equiv 1(\text{mod } q)$, we see that $O(p)(\text{mod } q)|q-1$. Since $q-1 \in \mathcal{S}$, we deduce from definition (i) of a p-divisisble system that $O(p)(\text{mod } q) \in \mathcal{S}$. Proposition 2 implies that $C(q^\infty)$ is a summand of $F^\times$.

Corollary 5. *Assume there are infinitely many Fermat primes. If F is any field not of characteristic 2 such that $F^\times$ is divisible, then $r(T(F^\times))$ is either 0 or $\aleph_0$.*

More generally, we conjecture that the answer to Problem 1 is "yes." To see how the theory of p-divisible systems is intimately connected to this problem, we close with the following proposition.

Proposition 4. *Let G be a divisible abelian group realizable as the multiplicative group of a field. Suppose further that G has finite nonzero torsion rank. Then there exists a prime number p and an infinite p-divisible system $\mathcal{S}$ such that the collection of prime divisors of members of $X := \{p^\alpha - 1 : \alpha \in \mathcal{S}\}$ is finite.*

Proof. Suppose that $F^\times$ is divisible and that $T(F^\times)$ is nontrivial of finite rank. Then Theorem 1 implies that F has characteristic p for some prime p. Moreover, $T(F^\times) \cong (\mathbb{F}_p^*)^\times$, where $\mathbb{F}_p^*$ is the algebraic closure of $\mathbb{F}_p$ in F. The set $\mathcal{S} := \{\alpha > 0 : \mathbb{F}_p^\alpha \subseteq \mathbb{F}_p^*\}$ is a p-divisible system. Moreover, Proposition 2 yields

$$(\mathbb{F}_p^*)^\times \cong \bigoplus_{q\in P(\mathcal{S})} C(q^\infty). \tag{4.2}$$

We claim that $\mathcal{S}$ is infinite. First observe that $\mathcal{S}$ contains some $\alpha > 1$. Otherwise $\mathcal{S} = \{1\}$. From this, it follows from definition (iii) of a p-divisible system that $p=2$. But then $\mathbb{F}_p^* = \mathbb{F}_2$, contradicting that $T(F^\times)$ is nontrivial. Now pick any $\alpha > 1$ in $\mathcal{S}$, and let q be a prime satisfying $p^\alpha \equiv 1(\text{mod } q)$. Then by definition (iii) of a p-divisible system, $q^i \in \mathcal{S}$ for every positive integer i; thus $\mathcal{S}$ is infinite. Finally, let $\alpha \in \mathcal{S}$, and suppose that q is any prime divisor of $p^\alpha - 1$. Then the multiplicative order of p modulo q divides α. By definition (i) of a p-divisible system, $q \in P(\mathcal{S})$. But since $\mathbb{F}_p^*$ has finite rank, we conclude from (4.2) that the set of all such q (as α ranges over $P(\mathcal{S})$) is finite. □

Acknowledgment. The author thanks the anonymous referee for a timely review and for comments which strengthened one of the results of this paper.

References

[1] A. Adler, *On the multiplicative semigroups of rings*, Comm. Algebra **6** (1978), no. 17, 1751–1753.

[2] J. Ax, *The elementary theory of finite fields*, Ann. of Math. (2) **88** (1968), 239–271.

[3] C.C. Chang and H.J. Keisler, *Model Theory*, North-Holland Publishing Company, Amsterdam, 1973.

[4] J.L. Colliot-Thèléne, R. Guralnick, and R. Wiegand, *Multiplicative groups of fields modulo products of subfields*, J. Pure Appl. Algebra **106** (1996), no. 3, 233–262.

[5] M. Contessa, J. Mott, and W. Nichols, *Multiplicative groups of fields*, Advances in Commutative Ring Theory (Fez 1997), 197–216, Lecture Notes in Pure and App. Math., 205, Dekker, New York, 1999.

[6] R.M. Dicker, *A set of independent axioms for a field and a condition for a group to be the multiplicative group of a field*, Proc. Lond. Math. Soc. **18** (1968), 114–124.

[7] L. Fuchs, *Abelian Groups*, London: Pergammon Press, 1960.

[8] A. Grisin, *The multiplicative group of a field*, Uspehi Mat. Nauk **28** (1973), no. 6(174), 201–202.

[9] R. Guralnick and R. Wiegand, *Galois groups and the multiplicative structure of field extensions*, Trans. Amer. Math. Soc. **331** (1992), 563–584.

[10] R. Guralnick and R. Wiegand, *Picard groups, cancellation, and the multiplicative structure of fields.* Zero-dimensional commutative rings (Knoxville, TN, 1994), 65–79, Lecture Notes in Pure and Appl. Math., **171**, Dekker, New York, 1995.

[11] W. Haboush, *Multiplicative groups of Galois extensions*, J. Algebra **165** (1994), 122–137.

[12] L. Hua, *On the multiplicative group of a field*, Acad. Sinica Science Record **3** (1950), 1–6.

[13] T. Hungerford, *Algebra*, Springer, New York, 1974.

[14] S. Lang, *Algebra* (second edition), Addison-Wesley Publishing Co., Advanced Book Program, Reading, 1984.

[15] W. May, *Fields with free multiplicative groups modulo torsion*, Rocky Mountain J. Math. **10** (1980), 599–604.

[16] W. May, *Multiplicative groups of fields*, Proc. Lond. Math. Soc. **24** (1972), 295–306.

[17] W. May, *Multiplicative groups under field extensions*, Can. J. Math. **31** (1979), 436–440.

[18] M. Morley, *Categoricity in power*, Trans. Amer. Math. Soc. **114** (1965), 514–538.

[19] G. Oman, *Ring semigroups whose subsemigroups form a chain*, Semigroup Forum **78** (2009), no. 2, 371–374.

[20] G. Sabbagh, *How not to characterize the multiplicative groups of fields*, J. London Math. Soc. (2) **1** (1969), 369–370.

[21] E. Schenkman, *On the multiplicative group of a field*, Arch. Math. (Basel) **15** (1964), 282–285.

[22] W. Szmielew, *Elementary properties of abelian groups*, Fund. Math. **42** (1955), 203–271.

[23] P. Van Praag, *Sur les groupes multiplicatifs des corps*, Comm. Algebra **21** (1993), no. 2, 527–534.

(Greg Oman) Department of Mathematics, The University of Colorado, Colorado Springs, CO 80918, USA

E-mail address: goman@uccs.edu