Available online at www.sciencedirect.com

ScienceDirect

Expo. Math. 34 (2016) 237–242

EXPOSITIONES MATHEMATICAE

www.elsevier.com/locate/exmath

Fields with indecomposable multiplicative groups

Sunil K. Chebolu[a,*], Keir Lockridge[b]

[a] *Department of Mathematics, Illinois State University, Normal, IL 61790, USA*
[b] *Department of Mathematics, Gettysburg College, Gettysburg, PA 17325, USA*

Received 12 February 2015; received in revised form 9 April 2015

Abstract

We classify all finite fields and all infinite fields of characteristic not equal to 2 whose multiplicative groups are direct-sum indecomposable. For finite fields, we obtain our classification using a direct argument and also as a corollary to Catalan's Conjecture. Our answer involves both Fermat and Mersenne primes. Turning to infinite fields, we use the classification of indecomposable non-torsion-free abelian groups to prove that any infinite field whose characteristic is not equal to 2 must have a decomposable multiplicative group.

MSC 2010: primary 12E20; secondary 11D41; 20K20

Keywords: Finite fields; Indecomposable groups; Mersenne primes; Fermat primes; Catalan's Conjecture

1. Introduction

More than 50 years ago, László Fuchs posed the following problem: find necessary and sufficient conditions for a group to be the multiplicative group of a field ([10, Problem 69]). Much progress has been made, but the problem remains unsolved (see, for example, [12,8,20,11]). We refer the reader to [7] for a survey of results in this area. Fuchs also

* Corresponding author.
E-mail addresses: schebol@ilstu.edu (S.K. Chebolu), klockrid@gettysburg.edu (K. Lockridge).

http://dx.doi.org/10.1016/j.exmath.2015.07.004
0723-0869/

asked whether the torsion subgroup of the multiplicative group of a field is necessarily a summand; this question was answered negatively by Cohn in [6]. In this paper, the question we ask is very much in the spirit of the aforementioned work: which fields have indecomposable multiplicative groups? (Recall that a group is said to be indecomposable if it cannot be written as direct sum of two non-trivial subgroups.) In Section 2, we classify the finite fields with indecomposable multiplicative groups. We give a direct number-theoretic argument. However, the main result may also be obtained as a corollary to Catalan's Conjecture, described in Section 3, which was proved in 2002 by Preda Mihăilescu. In Section 4, we consider infinite fields, where we show that any infinite field whose characteristic is not equal to 2 must have a decomposable multiplicative group. Throughout, we will use standard facts from number theory, algebra, and group theory which may be found in [1], [9], and [18], respectively. The structure of the group of units in a ring has been studied extensively, especially for finite rings and group rings. Examples where the unit group is saddled with a similarly strong simplifying condition include [16] and our recent work [2,5,4], where we examined the conditions under which every non-trivial unit in a ring has order p a prime.

2. Finite fields

The goal of this section is to prove Theorem 2.4 classifying the finite fields with indecomposable multiplicative groups. Our proof in this section uses elementary methods; in Section 3, we obtain this classification as a corollary to Catalan's Conjecture.

We begin by recording two basic facts about finite fields which can be found in any standard algebra textbook; see [9], for instance. First, recall that every finite field has prime power order, and for every prime p and positive integer r, there is a unique (up to isomorphism) finite field whose order is p^r. (The prime p is the characteristic of the field.) Second, recall that the multiplicative group of a finite field F, written $F^\times$, is cyclic. (In fact, the multiplicative group of any field is locally cyclic ([19, 1.3.4]); i.e., every finite subgroup is a cyclic group.) In our first proposition we make a simple observation which follows from the structure theorem for finite abelian groups. We refer to a positive integer as a prime power if it is equal to p^r for some prime p and integer $r \geq 1$.

Proposition 2.1. *If F is a finite field of order p^r, then $F^\times$ is indecomposable if and only if $p^r - 1$ is either 1 or a prime power.*

Note that $F^\times$ has order 1 if and only if $F = \mathbf{F}_2$, the finite field with two elements.

Proof. As mentioned above, the group $F^\times$ is isomorphic to C_{p^r-1}, the multiplicative cyclic group of order $p^r - 1$. From the structure theorem for finite abelian groups, a finite cyclic group is indecomposable if and only if it is trivial or has prime power order. ■

Because there is a unique finite field corresponding to each prime power p^r, determining which finite fields have an indecomposable multiplicative group is equivalent to solving the following number theoretic problem: find all pairs (p, r), where p is prime and r is a positive integer, such that $p^r - 1$ is a prime power. We begin by determining the pairs (p, r) for which $p^r - 1$ is 1 or a power of 2. Recall that a Fermat prime is a prime of the form $2^{2^n} + 1$.