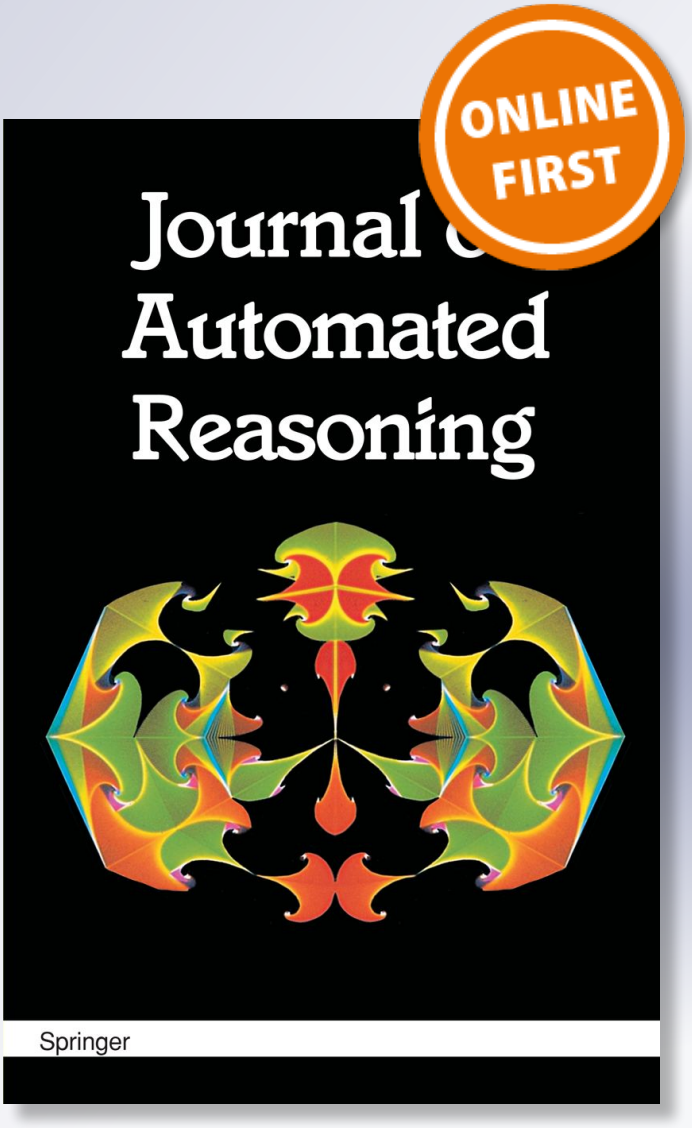
Classification of Finite Fields with Applications

Hing-Lun Chan & Michael Norrish

Journal of Automated Reasoning

ISSN 0168-7433

J Autom Reasoning
DOI 10.1007/s10817-018-9485-1



Springer

Journal of Automated Reasoning
https://doi.org/10.1007/s10817-018-9485-1

Classification of Finite Fields with Applications

Hing-Lun Chan[1] · **Michael Norrish**[1,2]

Received: 1 April 2017 / Accepted: 8 October 2018

Abstract
We present a formalisation of the theory of finite fields, from basic axioms to their classification, both existence and uniqueness, in HOL4 using the notion of subfields. The tools developed are applied to the characterisation of subfields of finite fields, and to the cyclotomic factorisation of polynomials of the form $\mathsf{X}^n - \mathbf{1}$, with coefficients over a finite fields.

Keywords Monoid · Group · Ring · Field · Finite field · Subfield · Quotient field · Extension field · Isomorphism · Minimal polynomials · Cyclotomic polynomials · Primitives · Existence · Uniqueness · Theorem proving · Formalisation · HOL4

1 Introduction

The theory of finite fields, as a branch of abstract algebra, is an appealing target for formalisation, both because of the beauty of the underlying mathematics, and because of the theory's applications in areas such as linear recurring sequences, error-correcting codes, and cryptosystems (see, e.g., Lidl and Niederreiter [34]). As with other algebraic structures, an important result in this theory is that of classification. This result states that every finite field has an underlying carrier of size equal to a prime power, and that, in fact, each prime power corresponds to exactly one unique (up to isomorphism) finite field.

In work to date, only the first half of this result has been formalised (in Coq, see next section). In this paper, we describe the proof of the whole theorem, which has been carried out in HOL4. In fact, we present two different proofs of the existence result, illustrating approaches centered on subfields and splitting fields. As a byproduct, the HOL4 algebra library has become a broader foundation on which we hope others will be able to build their own formalisations. We also believe that our formalisations are interesting proofs in their own right.

✉ Hing-Lun Chan
joseph.chan@anu.edu.au

Michael Norrish
Michael.Norrish@data61.csiro.au

[1] Australian National University, Canberra, Australia

[2] Canberra Research Laboratory, Data61, Canberra, Australia

Published online: 25 October 2018

Furthermore, to illustrate the strength of our library, we discuss two applications: subfield structures and cyclotomic factorisation of $X^n - \mathbf{1}$. These examples can be derived easily from the tools developed in the formalisation of the classification theorems, and both found use in our related work (see primality testing in Sect. 10.3).

Our aim is to give a self-contained discussion of the formalised classification of finite fields, oriented towards our two applications. We highlight the paths we have taken, discuss our formulation as appropriate, and compare with related formalisation work.

1.1 Our Work in Context

We believe the work presented here to be the first formalisation of the full classification result. The closest existing work we are aware of is the Coq formalisation [36] showing the existence half of the result, but lacking the uniqueness of finite fields [1]. That work is part of the Mathematical Components Library that was developed as part of the landmark project formalising the Odd Order Theorem [23]. Other systems, e.g., Isabelle/HOL and Mizar, have published formalisation work related to finite fields (see Sect. 10). These systems also include abstract algebra libraries supporting work in finite fields. As far as we can tell, the classification of finite fields has not been done in these systems either.

Our development stems from work done formalising the AKS algorithm. It is a mixture of techniques, drawing ideas from various sources to establish our key results, principally McEliece [37], Justesen and Høholdt [30], Ireland and Rosen [28], and Belk's very helpful course-notes [12].

1.2 Overview

We prove these classification theorems for finite fields (refer to Sect. 1.3 for HOL4 notations):

Theorem 1 Cardinality—*The order of a finite field must be a nontrivial prime power.*

$$\vdash \mathsf{FiniteField}\ \mathcal{F} \Rightarrow \exists p\ d.\ \mathsf{prime}\ p \wedge 0 < d \wedge |\mathsf{F}| = p^d$$

Here $\mathcal{F}$ denotes a field (an algebraic structure to be defined in Sect. 2) whose carrier F is finite.

Theorem 2 Existence—*For each nontrivial prime power, there exist a finite field of that order.*

$$\vdash \mathsf{prime}\ p \wedge 0 < d \Rightarrow \exists \mathcal{F}.\ \mathsf{FiniteField}\ \mathcal{F} \wedge |\mathsf{F}| = p^d$$

For a finite field $\mathcal{F}$, the unique prime p and exponent d to express its order as $|\mathsf{F}| = p^d$ are known as its characteristic $\mathsf{char}(\mathcal{F})$ and degree $\mathsf{deg}(\mathcal{F})$ respectively, see Sect. 3 and Lemma 25.

Theorem 3 Uniqueness—*Finite fields of the same order are isomorphic, i.e., structurally the same.*

$$\vdash \mathsf{FiniteField}\ \mathcal{F}_1 \wedge \mathsf{FiniteField}\ \mathcal{F}_2 \wedge |\mathsf{F}_1| = |\mathsf{F}_2| \Rightarrow \mathcal{F}_1 \cong \mathcal{F}_2$$

This completes the classification of finite fields. In addition, we discuss these applications:

[1] In this Coq script, at https://github.com/math-comp/math-comp/blob/master/mathcomp/field/finfield.v, Section FinFieldExists.

– *The classification of subfields of a finite field*
We write $\mathcal{S} \preccurlyeq \mathcal{F}$ to denote a subfield $\mathcal{S}$ of $\mathcal{F}$, with the following classification results:

Theorem 4 *All subfields have the same characteristic as the field.*

$$\vdash \mathcal{S} \preccurlyeq \mathcal{F} \Rightarrow \mathsf{char}(\mathcal{S}) = \mathsf{char}(\mathcal{F})$$

Theorem 5 *For a finite field, a subfield exists if and only if its degree divides the degree of the field.*

$$\vdash \mathsf{FiniteField}\ \mathcal{F} \Rightarrow \forall n.\ (\exists \mathcal{S}.\ \mathcal{S} \preccurlyeq \mathcal{F} \wedge \mathsf{deg}(\mathcal{S}) = n) \iff n \mid \mathsf{deg}(\mathcal{F})$$

– *The cyclotomic factorisation of polynomials of the form* $\mathsf{X}^n - \mathbf{1}$
We denote by $\boldsymbol{\Phi}_m$ the m-th cyclotomic polynomial, and F^* the nonzero elements of a field $\mathcal{F}$:

Theorem 6 *Let n be a divisor of the number of nonzero elements in a finite field. The polynomial $\mathsf{X}^n - \mathbf{1}$ is a product of cyclotomic factors $\boldsymbol{\Phi}_m$ where m divides n.*

$$\vdash \mathsf{FiniteField}\ \mathcal{F} \wedge n \mid |\mathsf{F}^*| \Rightarrow \mathsf{X}^n - \mathbf{1} = \prod \{\boldsymbol{\Phi}_m \mid m \in \mathsf{divisors}\ n\}$$

Theorem 7 *Let $\mathcal{F}$ be a finite field, n be positive, and $d = \mathsf{order}_n(|\mathsf{F}|)$ with $d > 1$. Then $\mathsf{X}^n - \mathbf{1}$ has a monic irreducible factor h of degree d, with the order of X equals to n in the quotient field $\mathcal{F}[\mathsf{X}]/\langle \mathsf{h} \rangle$.*

$$\vdash \mathsf{FiniteField}\ \mathcal{F} \wedge 0 < k \wedge 1 < \mathsf{order}_k(|\mathsf{F}|) \Rightarrow \exists z.\ \mathsf{monic}\ z \wedge \mathsf{ipoly}\ z \wedge z \mid \mathsf{X}^k - \mathbf{1} \wedge \mathsf{deg}\ z = \mathsf{order}_k(|\mathsf{F}|) \wedge \mathsf{order}_z(\mathsf{X}) = k$$

We shall define order and its notations in Sect. 2.1, and quotient fields and their notations in Sect. 4. This last result is useful for our work on the AKS algorithm (mentioned in Sect. 1.1), which is related to finite fields.

Paper Structure The rest of this paper is devoted to explaining the formalised proofs of these important results. Section 2 covers some necessary background on algebraic structures. Section 3 explores the basics of finite fields. Sections 4 and 5 describe the proofs of these classification theorems. Section 6 explains another path to obtain more general results on finite field existence. Sections 7 and 8 give the two main applications. Section 9 surveys our libraries supporting this finite field work, and Sect. 10 compares our work with others. Finally, we conclude in Sect. 11.

1.3 Notation

All statements starting with a turnstile ($\vdash$) are HOL4 theorems, automatically pretty-printed to LaTeX from the relevant theory in the HOL4 development. Generally, our notation allows an appealing combination of quantifiers ($\forall$, $\exists$), logical connectives ($\wedge$ for "and", $\vee$ for "or", $\neg$ for "not", $\Rightarrow$ for "implies", and $\iff$ for "if and only if"), and set notation ($\in$, $\cup$, $\cap$ and comprehensions such as $\{x \mid x < 6\}$).

The universal set of type α is denoted by $\mathcal{U}(:\alpha)$; the cardinality of a finite set S is written $|\mathsf{S}|$; we write $f : s \leftrightarrow t$ to mean that function f is bijective from set s to set t. The notation in HOL4 for the sum over elements of a set s is $\sum s$, and similarly for the product over elements of a set s is $\prod s$.

We write $n \mid m$ when n divides m, or, equivalently, $n \in \mathsf{divisors}\ m$. The notation $x \equiv y \pmod{n}$ means that both x and y give the same remainder after division by n.

Notation Conventions In this paper, we shall follow these conventions for notation:

- The symbols p, d, k, n, m are used to denote natural numbers, with p usually a prime.
- Generally, algebraic structures are written in calligraphic fonts, with the corresponding carrier written in sans serif fonts. For example, group $\mathcal{G}$, ring $\mathcal{R}$, and field $\mathcal{F}$, with their respective carriers G, R, and F. Typical elements in algebraic structures use the symbols a or x. Section 2 provides details on the notations used in algebraic structures.
- For monoids, an element x is invertible if its inverse x^{-1} exists. A cyclic group $\mathcal{G}$ is denoted by $\mathsf{cyclic}\ \mathcal{G}$.
- For rings and fields, the additive identity is $\mathbb{0}$ and multiplicative identity is $\mathbb{1}$.
- For a monoid $\mathcal{M}$, its invertibles form a group $\mathcal{M}^*$, with carrier M^*. This asterisk convention is extended to other cases. For example, the multiplicative group of a field $\mathcal{F}$ is denoted by $\mathcal{F}^*$, with the group carrier F^* including only the multiplicative invertibles, thus excluding $\mathbb{0}$.
- Polynomials with coefficients from a ring $\mathcal{R}$ are elements of $\mathcal{R}[\mathsf{X}]$, and polynomials with coefficients from a field $\mathcal{F}$ are elements of $\mathcal{F}[\mathsf{X}]$.
- Typical polynomials use the symbols h, f, g and t. More notations concerning polynomials are given in Sect. 2.2.

These are the basic ones. Other notations will be introduced and explained accordingly.

HOL4 Sources Our proof scripts can be found at http://bitbucket.org/jhlchan/hol/src/, in the sub-folder `algebra/finitefield`, at the tag `jar2018-ff-revised04`.

1.4 Two Approaches

Surveying the vast literature on finite fields, there seem to be two approaches to prove the key theorems. These two approaches roughly correspond to two types of textbook on finite fields.

The first one, favored by abstract algebra textbooks [2], is the *splitting-field approach*, with a bottom-up view. Starting from a field $\mathcal{F}$, we investigate the polynomials with coefficients taken from the field. For a polynomial h of degree n, with coefficients from $\mathcal{F}$, there are at most n roots in $\mathcal{F}$. If the number of roots of h in the field $\mathcal{F}$ is less than n, we find a way to extend $\mathcal{F}$ to a "bigger" field, one that will contain at least one more root for polynomial h. This is the idea of an extension field. If the number of roots of h in the extension field is still less than n, this process can be iterated to produce the so-called splitting field of the polynomial, which contains all the roots of h. By proving the existence and uniqueness of splitting fields, the existence and uniqueness of finite fields follows as a corollary: starting from the field $\mathbb{Z}_p$ with prime p, then construct the splitting field of the polynomial $\mathsf{X}^{p^n} - \mathsf{X}$ with positive n, and show that the polynomial has p^n distinct roots.

Another approach is usually found in textbooks on coding theory [3], with an introduction to finite fields as background material. This is the *subfield approach*, with a top-down view. Assuming a finite field of order p^n, for a prime p and some positive n, we study its subfields. Let a polynomial with coefficients from the subfield be called a *subfield polynomial*. Since subfield elements are field elements, a subfield polynomial can be regarded as a field polynomial. The polynomial $\mathsf{X}^{p^n} - \mathsf{X}$ is significant in this sense: it is a subfield polynomial (its coefficients are $\mathbb{1}$, $\mathbb{0}$, and $-\mathbb{1}$), but as a field polynomial, it has each field element as its

[2] Typical examples of algebra textbooks treating finite fields are Gallian [21], Herstein [24], and Judson [29].

[3] Typical examples of coding textbooks treating finite fields are McEliece [37], Garrett [22] and Pretzel [39]

root, once and only once. This leads to important factorisation patterns, and gives clues about irreducible polynomials in the subfield. The existence of finite fields then comes from the isomorphism of the smallest subfield with $\mathbb{Z}_p$, and the existence of irreducible polynomials for each degree n. The uniqueness of finite fields follows from the isomorphism between quotient fields by irreducible polynomials.

These two views are complementary, as the dual of the subfield relationship is the extension field relationship. In fact, most treatments of the subfield approach use the extension field terminology, so the distinction can be difficult to discern.

Given our desired applications, our proofs are constructed along the lines of the subfield approach. In particular, the cyclotomic polynomial results are a natural consequence of the partition of the field carrier by field elements of each order, and the fact that each field element is associated with a special monic irreducible subfield polynomial.

The splitting field approach is so common that we felt it important to also capture it in our formalisation. Fundamentally, this approach requires the iteration of a process which generates larger and larger fields with each step. Moreover, the underlying carrier sets in each field are effectively polynomials over the elements from the carrier of the previous step. This construction leads to interesting difficulties in a typed setting like HOL4's. We discuss the formalisation of extension fields and splitting fields in Sect. 6.

2 Algebraic Structures

Our formalisation of finite fields is at the top of a hierarchy of theories defining a family of algebraic structures:

- A Monoid $\mathcal{M}$ with a binary operation $*$ that is closed, associative, and an identity $\mathbf{e}$. An abelian monoid AbelianMonoid $\mathcal{M}$ has the operation also commutative.
- A Group $\mathcal{G}$ is a monoid with an inverse x^{-1} for each element x such that $x * x^{-1} = \mathbf{e}$. An abelian group AbelianGroup $\mathcal{G}$ is a commutative group.
- A Ring $\mathcal{R}$ has two components, a group $\mathcal{R}$.sum with operation + and a monoid $\mathcal{R}$.prod with operation $*$. Both share the same carrier, and:
  - $\mathcal{R}$.sum is an abelian group with identify $\mathbb{0}$;
  - $\mathcal{R}$.prod is an abelian monoid with identify $\mathbb{1}$;
  - Multiplication is distributive over addition.
- A Field $\mathcal{F}$ is a ring, with all nonzero elements having multiplicative inverses; i.e., $\mathcal{F}^*$ is a group.

The traditional mathematical presentation undergoes some drastic modifications when rendered in HOL. First, we must determine our representation for these algebraic structures. At our base, we have the α `monoid` type:

Definition 8

```
α monoid = <| carrier : α -> bool; op : α -> α -> α; id : α |>
```

A monoid ($\mathcal{M}$ `:α monoid`) is a value of the α `monoid` type, effectively a triple of three different fields. Using the HOL record machinery, we can refer to these fields with a pleasant "dot" notation; e.g., $\mathcal{M}$.op. The $\mathcal{M}$.carrier is a subset of all possible values of type α; the operation $\mathcal{M}$.op is a binary operation on those values and the identity $\mathcal{M}$.id is one of those values.

It is then straightforward to define the predicate Monoid over such values that carves out those that satisfy the axioms of a monoid. Here we annotate the definition's variables with their types, and remove the special overloading used in the rest of the paper so that uses of $\mathcal{M}$.op are explicit.

Definition 9

$$\begin{aligned}&\mathsf{Monoid}\ (\mathcal{M}\ :\alpha\ \mathtt{monoid}) \iff\\ &\quad(\forall (x:\alpha)\ (y:\alpha).\ x \in \mathcal{M}.\mathsf{carrier} \wedge y \in \mathcal{M}.\mathsf{carrier} \Rightarrow \mathcal{M}.\mathsf{op}\ x\ y \in \mathcal{M}.\mathsf{carrier}) \wedge\\ &\quad(\forall (x:\alpha)\ (y:\alpha)\ (z:\alpha).\\ &\qquad x \in \mathcal{M}.\mathsf{carrier} \wedge y \in \mathcal{M}.\mathsf{carrier} \wedge z \in \mathcal{M}.\mathsf{carrier} \Rightarrow\\ &\qquad\quad \mathcal{M}.\mathsf{op}\ (\mathcal{M}.\mathsf{op}\ x\ y)\ z = \mathcal{M}.\mathsf{op}\ x\ (\mathcal{M}.\mathsf{op}\ y\ z)) \wedge \mathcal{M}.\mathsf{id} \in \mathcal{M}.\mathsf{carrier} \wedge\\ &\quad\forall (x:\alpha).\ x \in \mathcal{M}.\mathsf{carrier} \Rightarrow \mathcal{M}.\mathsf{op}\ \mathcal{M}.\mathsf{id}\ x = x \wedge \mathcal{M}.\mathsf{op}\ x\ \mathcal{M}.\mathsf{id} = x\end{aligned}$$

A group $\mathcal{G}$ is a monoid with all its elements invertible. By hiding the underlying types, and overloading $\mathcal{G}$.carrier by G, $\mathcal{G}$.op $x\ y$ by $x*y$, and $\mathcal{G}$.id by $\mathbf{e}$, the result is better for readability:

Definition 10

$$\mathsf{Group}\ \mathcal{G} \iff \mathsf{Monoid}\ \mathcal{G} \wedge \forall x.\ x \in \mathsf{G} \Rightarrow \exists y.\ y \in \mathsf{G} \wedge y*x = \mathbf{e}$$

We can prove that such inverses are unique and are inverses on the left and right. Skolemizing, we define the inverse function, and characterise it thus

$$\vdash \mathsf{Group}\ \mathcal{G} \Rightarrow \forall x.\ x \in \mathsf{G} \Rightarrow x*x^{-1} = \mathbf{e} \wedge x^{-1}*x = \mathbf{e}$$

The ring type (omitted) consists of a combination of two monoid values: for a ring $\mathcal{R}$, its additive monoid is denoted by $\mathcal{R}$.sum and its multiplicative monoid is denoted by $\mathcal{R}$.prod. When we come to define the ring axioms, we can use prettier syntax in the description of the distributive law. In other words, $x + y$ is really $\mathcal{R}$.sum.op $x\ y$, and $x*y$ is really $\mathcal{R}$.prod.op $x\ y$. Denoting the carrier of ring $\mathcal{R}$ by R, this is the definition of a ring in HOL4:

Definition 11

$$\begin{aligned}&\mathsf{Ring}\ \mathcal{R} \iff\\ &\quad \mathsf{AbelianGroup}\ \mathcal{R}.\mathsf{sum} \wedge \mathsf{AbelianMonoid}\ \mathcal{R}.\mathsf{prod} \wedge \mathcal{R}.\mathsf{sum}.\mathsf{carrier} = \mathsf{R} \wedge\\ &\quad \mathcal{R}.\mathsf{prod}.\mathsf{carrier} = \mathsf{R} \wedge\\ &\quad \forall x\ y\ z.\ x \in \mathsf{R} \wedge y \in \mathsf{R} \wedge z \in \mathsf{R} \Rightarrow x*(y+z) = x*y + x*z\end{aligned}$$

Finally, the definition of what it is to be a field $\mathcal{F}$ can be quite terse:

Definition 12

$$\mathsf{Field}\ \mathcal{F} \iff \mathsf{Ring}\ \mathcal{F} \wedge \mathsf{Group}\ \mathcal{F}^*$$

In HOL4, definitions such as these subsequently require that all theorem statements to be qualified with assumptions such as Field $\mathcal{F}$. This is because the value $\mathcal{F}$ is just a pair of record values, and is not known to satisfy the field axioms without that explicit assumption. Though tedious, these qualifications of our theorem statements do not significantly impact the theorem-proving task. Rather, the burden lies mostly in the initial writing of the goal.

Although overloading can be used to pretty-print for readability, we keep the types barely visible through the use of different fonts. For example, a field $\mathcal{F}$ has elements in the carrier F, with the nonzero elements F* forming a group $\mathcal{F}^*$.

In the rest of the paper, overloading is used extensively to hide complicated terms such as $\mathcal{R}$. sum . op x y, but the logical assumptions (such as Field $\mathcal{F}$) always appear. Occasionally, this can make the assumption seem vacuous as the syntax for the operators no longer appears to refer back to the value (e.g., $\mathcal{F}$) at all. For example, this apparent vacuousness can be seen in the last ring axiom above.

Note that our rings are more commonly known as commutative rings with identity. We did not go all the way to non-commutative rings since our goal is about finite fields. By the same token, we do not consider skew fields. However, we do consider other algebraic structures related to finite fields, e.g., integral domains.

2.1 No Zero Divisors

In a field $\mathcal{F}$, the nonzero elements form a multiplicative group $\mathcal{F}^*$. This implies that a field has no zero divisors. A non-trivial ring, i.e., $\mathbb{1} \neq \mathbb{0}$ with no zero divisors is called an integral domain:

$$\begin{array}{l}\mathsf{IntegralDomain}\ \mathcal{F} \iff \\ \quad \mathsf{Ring}\ \mathcal{F} \wedge \mathbb{1} \neq \mathbb{0} \wedge \forall x\ y.\ x \in \mathsf{F} \wedge y \in \mathsf{F} \Rightarrow (x * y = \mathbb{0} \iff x = \mathbb{0} \vee y = \mathbb{0})\end{array}$$

For an integral domain $\mathcal{F}$, let a be a nonzero element, i.e., $a \neq \mathbb{0}$. If the integral domain is finite, the sequence $a, a^2, a^3, \ldots$ must repeat. Suppose $a^j = a^{j+k}$ for some j and $k \neq 0$. Then ring subtraction and distribution give $a^j * (a^k - \mathbb{1}) = \mathbb{0}$. The absence of zero divisors in an integral domain implies that $a^k = \mathbb{1}$. The smallest such k is the multiplicative order of a, or simply the *order* of a, denoted by $\mathsf{order}_{\mathcal{F}^*}(a)$. Note that $a^k = \mathbb{1}$ and $k \neq 0$ implies that a has a multiplicative inverse: a^{k-1}. Therefore:

Lemma 13 *A finite integral domain is always a field.*

$$\vdash \mathsf{FiniteIntegralDomain}\ \mathcal{F} \Rightarrow \mathsf{Field}\ \mathcal{F}$$

In fact, the field is finite, i.e., FiniteField $\mathcal{F}$. This allows us to conclude that a finite non-trivial ring is a finite field simply by checking that there are no zero divisors (see Sect. 4).

Order Implementation Based on our hierarchy of algebraic structures, a field element is ultimately a monoid element.[4] The notion of an order for a monoid element involves defining the exponentiation operation. This is defined in HOL4 using function iteration by FUNPOW with starting value the identity **e** and applying the monoid operation n times:

Definition 14 $x^n = \mathsf{FUNPOW}\ ((*)\ x)\ n\ \mathbf{e}$

Order for an element is defined as the least period if it exists, otherwise 0, through the optional-least operator OLEAST with case options:

Definition 15

$$\begin{array}{l}\mathsf{period}\ \mathcal{M}\ x\ k \iff 0 < k \wedge x^k = \mathbf{e} \\ \mathsf{order}_{\mathcal{M}}(x) = \mathbf{case}\ \mathsf{OLEAST}\ k.\ \mathsf{period}\ \mathcal{M}\ x\ k\ \mathbf{of}\ \mathsf{NONE} \Rightarrow 0 \mid \mathsf{SOME}\ k \Rightarrow k\end{array}$$

[4] Here we refer to an element of the multiplicative monoid, for the *multiplicative* order. Every nonzero field element has the same *additive* order, as will be discussed in Sect. 3.

Order Notation Although the order of an element x in a monoid $\mathcal{M}$ should be denoted by $\mathsf{order}_{\mathcal{M}}(x)$, the monoid subscript is usually abbreviated. For example, we write $\mathsf{order}_n(k)$ for order of k in the monoid $\mathbb{Z}_n^*$. Later in Sect. 4, we shall introduce quotient rings over rings $\mathcal{R}$ or fields $\mathcal{F}$, and write $\mathsf{order}_{\mathsf{h}}(\mathsf{X})$ for the order of polynomial X in the monoid $\mathcal{R}^*[\mathsf{X}]/(\mathsf{h})$ or $\mathcal{F}^*[\mathsf{X}]/(\mathsf{h})$ derived from a modulus polynomial h.

2.2 Polynomials

Polynomials are expressions of the form:

$$c_n\mathsf{X}^n + c_{n-1}\mathsf{X}^{n-1} + \cdots + c_1\mathsf{X} + c_0$$

where the coefficients c_j come from a ring $\mathcal{R}$. These polynomials, equipped with the usual polynomial addition and multiplication, form a polynomial ring, denoted by $\mathcal{R}[\mathsf{X}]$. In these polynomial rings, the additive identity is $\mathbf{0}$, the zero polynomial, and the multiplicative identity is $\mathbf{1}$, the constant polynomial one. When the ring $\mathcal{R}$ has further properties, e.g., without zero divisors so that it is an integral domain $\mathcal{F}$, or all nonzero elements are invertible so that it is a field $\mathcal{F}$, we shall denote the polynomial ring by $\mathcal{F}[\mathsf{X}]$.

Although a polynomial with coefficients from a ring may have more roots than its degree [5], this cannot happen when its coefficients come from a ring without zero divisors, i.e.,

Lemma 16 *A nonzero polynomial with coefficients from an integral domain has no more roots than its degree.*

$$\vdash \mathsf{IntegralDomain}\ \mathcal{F} \Rightarrow \forall \mathsf{h}.\ \mathsf{poly}\ \mathsf{h} \wedge \mathsf{h} \neq \mathbf{0} \Rightarrow |\mathsf{roots}\ \mathsf{h}| \leq \mathsf{deg}\ \mathsf{h}$$

Since a field is also an integral domain, this result holds for polynomials with coefficients from a field $\mathcal{F}$.

When defining polynomial division within the polynomial rings, whether the coefficients come from a ring or a field is of importance. For polynomials with coefficients from a ring, only those with a leading coefficient that is invertible can be taken as a divisor to carry out the division algorithm.[6] On the other hand, any nonzero polynomial $\mathsf{h} \neq \mathbf{0}$ with coefficients from a field can be taken as a divisor. This is because its leading coefficient, being a nonzero field element, is always invertible.

Clearly, a monic polynomial, regardless of whether the coefficients come from a ring or a field, can always be taken as a modulus, i.e., a divisor for polynomial division.

Polynomial Implementation In HOL4, we use the type (α `list`) to represent polynomials, i.e., as a list of coefficient from a ring or a field of type α. We introduce α `poly` as an alias for α `list`. The zero polynomial $\mathbf{0}$ is represented by `[]`. For a nonzero polynomial h with coefficients c_j, the constant c_0 is the first element of the list, and the leading c_n is the last. The leading coefficient c_n is denoted by $\mathsf{lead}\ \mathsf{h}$, and the index n is the degree, denoted by $\mathsf{deg}\ \mathsf{h}$.

Our choice of identifying $\mathbf{0}$ internally as `[]` has some advantages when defining polynomial operations. We define polynomial addition, multiplication, and scalar multiplication, inductively on lists. However, this complicates the definitions of $\mathsf{lead}\ \mathsf{h}$ and $\mathsf{deg}\ \mathsf{h}$, to cater for whether h equals $\mathbf{0}$.

[5] For example, in $\mathbb{Z}_6$, $2 * 3 = 0$. Hence in $\mathbb{Z}_6[\mathsf{X}]$, $(X-2)(X-3) = X^2 - 5X = X(X-5)$, which is an example of a degree 2 polynomial with more than 2 roots.

[6] For example, the integers $\mathbb{Z}$ form a ring. In $\mathbb{Z}[\mathsf{X}]$, $2X$ has a leading coefficient not invertible in $\mathbb{Z}$, hence cannot be taken as a modulus for polynomial division.

Our polynomials are normalized, so that a polynomial $\mathsf{h} \neq \mathbf{0}$ has $\mathsf{lead}\ \mathsf{h} \neq \mathbb{0}$. This implies that not all values of (α `list`) are considered polynomials. Those that are polynomials are qualified by $\mathsf{poly}\ \mathsf{h}$. We write $\mathsf{monic}\ \mathsf{h}$ for a monic polynomial, and $\mathsf{ipoly}\ \mathsf{h}$ for an irreducible polynomial.

Polynomial Notations Given a polynomial h with coefficients from a ring $\mathcal{R}$, $\mathsf{h}(a)$ is the value of h when X is substituted by an element $a \in \mathsf{R}$. The element a is a root of polynomial h if $\mathsf{h}(a) = \mathbb{0}$. The roots of polynomial h is the set $\mathsf{roots}\ \mathsf{h}$, or $\mathsf{roots}_{\mathcal{S}}\ \mathsf{h}$ if the underlying ring $\mathcal{S}$ needs to be specified. We extend the notion of substitution to polynomials: substituting the X in polynomial h by another polynomial g gives a polynomial $\mathsf{h}[\![\mathsf{g}]\!]$ [7]. We also extend the modulus notation for polynomials with coefficients from a field, e.g., $\mathsf{f} \equiv \mathsf{g} \pmod{\mathsf{h}}$ means that both f and g give the same remainder after division by h, or $\mathsf{h} \mid (\mathsf{f} - \mathsf{g})$. The properties for polynomial h to be a valid modulus is noted in the discussion following Lemma 16.

3 Finite Fields

A finite field $\mathcal{F}$ is a field with a finite set of elements. Therefore, any nonzero element $a \in \mathsf{F}^*$ will have an additive order, the smallest number of repeated additions of itself that is equal to $\mathbb{0}$. Due to the distributive law, and the fact that $\mathbb{1} * a = a$, all nonzero a have the same additive order as $\mathbb{1}$. Since field addition is identical to ring addition, this argument applies equally to rings. The unique additive order of $\mathbb{1}$ in a ring $\mathcal{R}$ is called its *characteristic*, denoted by $\mathsf{char}(\mathcal{R})$.

Because a field has no zero divisors, the characteristic of a finite field has no proper factor. Thus:

Lemma 17 *A finite field has prime characteristic.*

$$\vdash\ \mathsf{FiniteField}\ \mathcal{F} \Rightarrow \mathsf{prime}\ \mathsf{char}(\mathcal{F})$$

3.1 Cyclic Multiplicative Group

A finite field $\mathcal{F}$ is an integral domain, with all nonzero elements in F^* having nonzero orders. The set of elements with order equal to n is denoted by ($\mathsf{orders}\ \mathcal{F}^*\ n$). Its cardinality is related to the Euler's φ-function, $\varphi(n)$, counting the number of coprimes from 1 to n:

Lemma 18 *In a finite field $\mathcal{F}$, the number of elements with order n is $\varphi(n)$ if n divides $|\mathsf{F}^*|$, otherwise* 0.

$$\vdash\ \mathsf{FiniteField}\ \mathcal{F} \Rightarrow \forall n.\ |\mathsf{orders}\ \mathcal{F}^*\ n| = \textbf{if}\ n \mid |\mathsf{F}^*|\ \textbf{then}\ \varphi(n)\ \textbf{else}\ 0$$

The proof depends on a counting argument based on this identity about the Euler's φ-function:

Lemma 19 $\vdash n = \sum \varphi\ (\mathsf{divisors}\ n)$ or $n = \sum_{d \mid n} \varphi(d)$

This gives immediately a fundamental feature about finite fields:

[7] Viewing polynomials as functions, this is their function composition.

Theorem 20 *The multiplicative group of a finite field is cyclic.*

$\vdash$ FiniteField $\mathcal{F} \Rightarrow$ cyclic $\mathcal{F}^*$

Proof [8] Lemma 18 shows that the set (orders $\mathcal{F}^*$ $|\mathsf{F}^*|$) $\neq \emptyset$. Thus there exists a field element of order $|\mathsf{F}^*|$, i.e., a generator of $\mathcal{F}^*$, making it cyclic. □

Another proof [9] not using the Euler's φ-function (Lemma 19) is based on the properties of a finite abelian group, which is the case for $\mathcal{F}^*$ of a finite field. For a finite abelian group $\mathcal{G}$, the order of any group element must divide the maximal order:

$\vdash$ FiniteAbelianGroup $\mathcal{G} \Rightarrow \forall x.\ x \in \mathsf{G} \Rightarrow \text{order}_{\mathcal{G}}(x) \mid$ maximal_order $\mathcal{G}$

Combining this result with the fact that a nonzero polynomial with coefficients from a field has the number of its roots bounded by its degree (Lemma 16), the maximal order must be equal to the cardinality of the group carrier. Therefore, in a finite field $\mathcal{F}$, the element with the maximal order in its multiplicative group $\mathcal{F}^*$ is a generator, giving cyclic $\mathcal{F}^*$.

3.2 Primitives

The generators of the cyclic $\mathcal{F}^*$ forms the set of primitives $\pi_{\mathcal{F}}$ of the finite field $\mathcal{F}$. By Theorem 20, the set $\pi_{\mathcal{F}}$ is non-empty. Any member of this set is a *primitive* of the finite field $\mathcal{F}$, which is nonzero and has order $|\mathsf{F}^*|$:

Definition 21 $z \in \pi_{\mathcal{F}} \iff z \in \mathsf{F}^* \wedge \text{order}_{\mathcal{F}^*}(z) = |\mathsf{F}^*|$

We shall see the role played by primitives in Sect. 5.2 about isomorphic fields.

3.3 Subfields

A subfield $\mathcal{S}$ of a field $\mathcal{F}$ has its carrier $\mathsf{S} \subseteq \mathsf{F}$, and itself is a field by keeping the same field additions and multiplications. The fact that multiplication is distributive over addition gives another view of the field/subfield relationship:

Theorem 22 *A field is a vector space over its subfield.*

$\vdash \mathcal{S} \preccurlyeq \mathcal{F} \Rightarrow$ VSpace $\mathcal{S}$ $\mathcal{F}$.sum $(*)$

Proof Before we present the proof, we first define vector space. A vector space VSpace $\mathcal{S}$ $\mathcal{G}$ *op* is another algebraic structure, with three components:

- a field $\mathcal{S}$ of scalars,
- an additive group $\mathcal{G}$ of vectors, and
- a multiplication *op* taking a scalar and a vector, resulting in a vector. □

Together they must satisfy the vector space axioms, which are expressed in HOL4 as:

Definition 23

[8] This proof, based on counting field order elements, is adapted from McEliece [37], Corollary of Theorem 5.7.

[9] Such a proof is given in Justesen and Høholdt [30], Theorem 2.1.2.

$$\begin{aligned}&\mathsf{VSpace}\ \mathcal{S}\ \mathcal{G}\ op \iff \\ &\quad \mathsf{Field}\ \mathcal{S} \wedge \mathsf{AbelianGroup}\ \mathcal{G} \wedge (\forall a\ v.\ a \in \mathsf{S} \wedge v \in \mathsf{G} \Rightarrow op\ a\ v \in \mathsf{G}) \wedge \\ &\quad (\forall a\ b\ v.\ a \in \mathsf{S} \wedge b \in \mathsf{S} \wedge v \in \mathsf{G} \Rightarrow op\ a\ (op\ b\ v) = op\ (a * b)\ v) \wedge \\ &\quad (\forall v.\ v \in \mathsf{G} \Rightarrow op\ \mathbb{1}\ v = v) \wedge \\ &\quad (\forall a\ u\ v.\ a \in \mathsf{S} \wedge u \in \mathsf{G} \wedge v \in \mathsf{G} \Rightarrow op\ a\ (u * v) = op\ a\ u * op\ a\ v) \wedge \\ &\quad \forall a\ b\ v.\ a \in \mathsf{S} \wedge b \in \mathsf{S} \wedge v \in \mathsf{G} \Rightarrow op\ (a + b)\ v = op\ a\ v * op\ b\ v\end{aligned}$$

Given $\mathcal{S} \preccurlyeq \mathcal{F}$, we can:

- identify the elements of the subfield $\mathcal{S}$ as scalars.
- identity the elements of the abelian group $\mathcal{F}.\mathsf{sum}$ of field $\mathcal{F}$ as vectors.
- identify the field multiplication $*$ as the multiplication op of scalar to vector giving a vector.

Then it is a routine exercise to verify that all vector space axioms are satisfied. □

The elements given by repeated additions of $\mathbb{1}$ form a subfield. This subfield, which must be embedded in any subfield of $\mathcal{F}$, is also a field with no proper subfield. It is called its *prime field*, denoted by $\mathbf{PF}_{\mathcal{F}}$:

Lemma 24 *The prime field of a finite field is its smallest subfield.*

$$\vdash \mathsf{FiniteField}\ \mathcal{F} \wedge s \preccurlyeq \mathcal{F} \Rightarrow \mathbf{PF}_{\mathcal{F}} \preccurlyeq s$$

The order of $\mathbf{PF}_{\mathcal{F}}$ is $\mathsf{char}(\mathcal{F})$, the additive order of $\mathbb{1}$. The dimension of a finite field $\mathcal{F}$ over its prime field $\mathbf{PF}_{\mathcal{F}}$ is called its *degree*, denoted by $\mathsf{deg}(\mathcal{F})$. Treating a finite field $\mathcal{F}$ as a vector space over its prime field $\mathbf{PF}_{\mathcal{F}}$, its dimension is the number of basis vectors. Since every field element is uniquely expressed by a linear combination of basis vectors, we have:

Lemma 25 *The order of a finite field equals its characteristic raised to its degree.*

$$\vdash \mathsf{FiniteField}\ \mathcal{F} \Rightarrow |\mathsf{F}| = \mathsf{char}(\mathcal{F})^{\mathsf{deg}(\mathcal{F})}$$

With every field having its prime field as a subfield, our first key result about finite field order is immediate: **Theorem 1**

$$\vdash \mathsf{FiniteField}\ \mathcal{F} \Rightarrow \exists p\ n.\ \mathsf{prime}\ p \wedge 0 < n \wedge |\mathsf{F}| = p^n$$

Proof Take $p = \mathsf{char}(\mathcal{F})$ and $n = \mathsf{deg}(\mathcal{F})$. Since the dimension of $\mathcal{F}$ over its subfield $\mathbf{PF}_{\mathcal{F}}$ is at least 1, we have $0 < n$. Now p is prime by Lemma 17, and $|\mathsf{F}| = p^n$ by Lemma 25. □

This particular result, that all subfields of a field share its characteristic, is trivial: **Theorem 4**

$$\vdash \mathcal{S} \preccurlyeq \mathcal{F} \Rightarrow \mathsf{char}(\mathcal{S}) = \mathsf{char}(\mathcal{F})$$

Proof All subfields have the same multiplicative identity $\mathbb{1}$ of the field. □

Our formalisation of the theory of vector spaces follows the approach given in Axler [7]. The library is a standalone development consisting of basis, spanning subspace, and linear independence. The dimension of a vector space over its subspace is the minimal number of vectors in a subspace basis to span the vector space. The minimal requirement ensures that such basis vectors are linear independent.

4 Existence of Finite Fields

The integers $\mathbb{Z}$ form a ring, an infinite one. Dividing the integers by a modulus $n \neq 0$, the remainders are in the range from 0 to $(n - 1)$. These are the elements of $\mathbb{Z}_n$, a finite ring with arithmetic operations in $(\text{mod } n)$. There may be zero divisors in $\mathbb{Z}_n$, e.g.. $2 \times 3 \equiv 0 \ (\text{mod } 6)$. Thus $\mathbb{Z}_n$ cannot be a field if n is composite. However:

Theorem 26 *The ring $\mathbb{Z}_p$ for a prime p modulus is a finite field.*

$\vdash$ prime $p \Rightarrow$ FiniteField $\mathbb{Z}_p$

Proof In the finite ring $\mathbb{Z}_p$, if $a \times b \equiv 0 \ (\text{mod } p)$, then $p \mid a \times b$. Since p is prime, $p \mid a$ or $p \mid b$. This means that $a \equiv 0 \ (\text{mod } p)$ or $b \equiv 0 \ (\text{mod } p)$. Thus $\mathbb{Z}_p$ has no zero divisors for a prime p, making it a finite integral domain, or a finite field by Lemma 13. □

Polynomials with coefficients from integers or field both form Euclidean rings, which have the property that every ideal is generated by a single element. We write (a) for the ideal generated by a ring element a. Let h be a polynomial, with coefficients from a field $\mathcal{F}$. The quotient ring by the ideal (h), denoted by $\mathcal{F}[\mathsf{X}]/(\mathsf{h})$, consists of all polynomial remainders after division by h. Like $\mathbb{Z}_p$ for a prime p, we have:

Theorem 27 *For a finite field, the polynomial quotient ring generated by an irreducible is a finite field.*

$\vdash$ FiniteField $\mathcal{F} \Rightarrow \forall \mathsf{h}.$ ipoly h $\Rightarrow$ FiniteField $\mathcal{F}[\mathsf{X}]/(\mathsf{h})$

Proof [10] Note that $\mathcal{F}[\mathsf{X}]/(\mathsf{h})$ is a finite ring, as it consists of polynomials p with deg p $<$ deg h. Let f and g be two such polynomials. If $\mathsf{f} * \mathsf{g} \equiv \mathbf{0} \ (\text{mod } \mathsf{h})$, this means $\mathsf{h} \mid \mathsf{f} * \mathsf{g}$. Since h is irreducible, $\mathsf{h} \mid \mathsf{f}$ or $\mathsf{h} \mid \mathsf{g}$. Thus $\mathsf{f} \equiv \mathbf{0} \ (\text{mod } \mathsf{h})$ or $\mathsf{g} \equiv \mathbf{0} \ (\text{mod } \mathsf{h})$. Therefore $\mathcal{F}[\mathsf{X}]/(\mathsf{h})$ has no zero divisors, making it a finite integral domain, or a finite field by Lemma 13. □

Note that the order of $\mathcal{F}[\mathsf{X}]/(\mathsf{h})$ is $|\mathsf{F}|^d$, where $d =$ deg h, by counting the number of polynomial remainders, all with degree less than d. This provides a recipe to construct other finite fields, based on those of prime order, e.g., $\mathbb{Z}_p$ for prime p, if there are irreducibles of every nonzero degree d.

4.1 Counting Irreducibles

For a finite field $\mathcal{F}$, let ($\mathcal{I}_{\mathcal{F}}$ n) denote the set of monic irreducibles of degree n in $\mathcal{F}[\mathsf{X}]$. We show that:

Theorem 28 *There are monic irreducible polynomials of any positive degree.*

$\vdash$ FiniteField $\mathcal{F} \Rightarrow \forall n.\ 0 < n \Rightarrow \exists p.$ monic $p \wedge$ ipoly $p \wedge$ deg $p = n$

Proof [11] For each divisor d of $n \neq 0$, let $\Psi_d = \prod$ ($\mathcal{I}_{\mathcal{F}}$ d), the product of all monic irreducibles of degree d. Multiplying these products over all divisors of n gives a remarkable result:

[10] This proof works because polynomial rings over a field is a unique factorisation domain, in which irreducibles are primes.

[11] This proof, based on degree and divisibility of special polynomials, is adapted from Belk [12], Theorem 9.

$$\vdash \text{FiniteField } \mathcal{F} \wedge 0 < n \Rightarrow \mathsf{X}^{|\mathsf{F}|^n} - \mathsf{X} = \prod \{ \boldsymbol{\Psi}_d \mid d \in \text{divisors } n \}$$

A more pleasant typographic rendering, as one might find in textbooks, is:

$$\mathsf{X}^{|\mathsf{F}|^n} - \mathsf{X} = \prod_{d \mid n} \boldsymbol{\Psi}_d \tag{1}$$

The left-side is a polynomial of degree $|\mathsf{F}|^n$. By including more monic irreducibles on the right-side, the left polynomial becomes a divisor:

$$\left(\mathsf{X}^{|\mathsf{F}|^n} - \mathsf{X}\right) \mid \prod_{d=1}^{n} \boldsymbol{\Psi}_d$$

Now, suppose there are no monic irreducibles of degree n. Then $\mathcal{I}_{\mathcal{F}}\ n = \emptyset$, so that $\boldsymbol{\Psi}_n = \mathbf{1}$. We shall see how this leads to a contradiction, thus proving the result.

With $\boldsymbol{\Psi}_n = \mathbf{1}$, the left polynomial shall divide the product of all $\boldsymbol{\Psi}_d$, with subscript d from 1 to $n - 1$. We claim that:

$$\left(\mathsf{X}^{|\mathsf{F}|^n} - \mathsf{X}\right) \mid \prod_{d=1}^{n-1} \boldsymbol{\Psi}_d \mid \prod_{d=1}^{n-1} \left(\mathsf{X}^{|\mathsf{F}|^d} - \mathsf{X}\right)$$

This is because each $(\mathsf{X}^{|\mathsf{F}|^d} - \mathsf{X})$ has a factor $\boldsymbol{\Psi}_d$ by Equation 1, and the $\boldsymbol{\Psi}_d$'s, being the product of all monic irreducibles of degree d, are pairwise coprime. However, the degree of the polynomial product on the right-side is less than the degree of the left polynomial:

$$\sum_{d=1}^{n-1} |\mathsf{F}|^d = \frac{|\mathsf{F}|^n - 1}{|\mathsf{F}| - 1} < |\mathsf{F}|^n \qquad \text{by geometric series, and } 1 < |\mathsf{F}|.$$

This is impossible since the left-side divides the right-side, and the right-side is not the zero polynomial $\mathbf{0}$. Thus $\mathcal{I}_{\mathcal{F}}\ n \neq \emptyset$, i.e., there exists a monic irreducible polynomial of degree n. □

Most textbooks [12] arrive at Theorem 28 by another route. After deducing Equation 1, the usual method is to equate the polynomial degree on the left with the sum of counts of monic irreducibles on the right. By applying Möbius inversion, one can extract the individual monic irreducibles counts, and show that these counts are nonzero. Our proof avoids the use of Möbius inversion formula. Note that Möbius inversion had been formalised, e.g., by Asperti and Armentano [5].

With the existence of monic irreducible polynomials of any positive degree, we can deliver our second key result: the existence of finite fields with prime power order. **Theorem** 2

$$\vdash \text{prime } p \wedge 0 < n \Rightarrow \exists \mathcal{F}.\ \text{FiniteField } \mathcal{F} \wedge |\mathsf{F}| = p^n$$

Proof Note that $\mathbb{Z}_p$ is a finite field for a prime p, by Theorem 26. Applying Theorem 28, there is a monic irreducible h in $\mathbb{Z}_p[\mathsf{X}]$ with $\deg\ \mathsf{h} = n$. Then $\mathbb{Z}_p[\mathsf{X}]/(\mathsf{h})$ is a finite field by Theorem 27, with p^n elements. □

[12] See, e.g., Lidl and Niederreiter [34], Ireland and Rosen [28], and McEliece [37].

5 Uniqueness of Finite Fields

Putting $n = 1$ in Equation 1 gives $\mathsf{X}^{|\mathsf{F}|} - \mathsf{X} = \boldsymbol{\Psi}_1$. As $\boldsymbol{\Psi}_1$ is the product of linear monic irreducibles, we have:

$$\vdash \mathsf{FiniteField}\ \mathcal{F} \Rightarrow \mathsf{X}^{|\mathsf{F}|} - \mathsf{X} = \prod \{\mathsf{X} - a * \mathbf{1} \mid a \in \mathsf{F}\}$$

We use $a * \mathbf{1}$ to represent the constant polynomial given by an element $a \in \mathsf{F}$, in accordance with types. In textbooks, this is presented simply as:

$$\mathsf{X}^{|\mathsf{F}|} - \mathsf{X} = \prod_{a \in \mathsf{F}} (\mathsf{X} - a) \tag{2}$$

The polynomial on the left has coefficients $\mathbb{1}$, $\mathbb{0}$ and $-\mathbb{1}$, which are present in any subfield $\mathcal{S} \preccurlyeq \mathcal{F}$. Therefore such a polynomial is for any subfield a subfield polynomial. However, as a field polynomial, its roots are all the field elements, each contributing a single factor, i.e., there are no repeated roots.

5.1 Minimal Polynomials

Given a subfield $\mathcal{S} \preccurlyeq \mathcal{F}$, consider all the subfield polynomials, i.e., elements in $\mathcal{S}[\mathsf{X}]$. Any field element $a \in \mathsf{F}$ is then a root of some subfield polynomial, e.g., the polynomial of Equation 2. We write $\mathsf{poly}_{\mathcal{S}}\ \mathsf{h}$ to indicate a subfield polynomial with coefficients in $\mathcal{S}$. If h has no proper subfield polynomial factors, it is irreducible in the subfield, indicated by $\mathsf{ipoly}_{\mathcal{S}}\ \mathsf{h}$.

A monic subfield polynomial of the smallest degree having a as a root is called a *minimal* polynomial of a, denoted by $\mathfrak{m}_a$, with these properties (see, e.g., Belk [12]):

(1) A minimal polynomial of a finite field element a is irreducible in the subfield.

$$\vdash \mathsf{FiniteField}\ \mathcal{F} \wedge \mathcal{S} \preccurlyeq \mathcal{F} \Rightarrow \forall a.\ a \in \mathsf{F} \Rightarrow \mathsf{ipoly}_{\mathcal{S}}\ \mathfrak{m}_a$$

(2) A minimal polynomial of a finite field element a divides every subfield polynomial with root a.

$$\vdash \mathsf{FiniteField}\ \mathcal{F} \wedge \mathcal{S} \preccurlyeq \mathcal{F} \Rightarrow \forall \mathsf{h}\ a.\ \mathsf{poly}_{\mathcal{S}}\ \mathsf{h} \wedge a \in \mathsf{roots}\ \mathsf{h} \Rightarrow \mathfrak{m}_a \mid \mathsf{h}$$

From property (2), if there are two minimal polynomials of $a \in \mathsf{F}$, they will divide each other, hence equal, i.e.. $\mathfrak{m}_a$ is unique. We shall refer to $\mathfrak{m}_a$ as "the" minimal polynomial of a.

Recall from Equation 2 that all $a \in \mathsf{F}$ are roots of $\mathsf{X}^{|\mathsf{F}|} - \mathsf{X}$. By property (2), each $\mathfrak{m}_a$ divides $\mathsf{X}^{|\mathsf{F}|} - \mathsf{X}$, the dividend. Since each $\mathfrak{m}_a$ is irreducible by property (1), and irreducibles are coprime, the product of all $\mathfrak{m}_a$ also divides the dividend. Both product and dividend have identical roots, i.e., all elements in F. With all possible elements taken as roots, there can be no more roots. Thus the product and dividend differ only by a constant, which must be $\mathbf{1}$ as both are monic polynomials. Therefore:

Lemma 29 *With respect to any subfield of a finite field $\mathcal{F}$, the polynomial $\mathsf{X}^{|\mathsf{F}|} - \mathsf{X}$ is the product of distinct minimal polynomials from all the field elements.*

$$\vdash \mathsf{FiniteField}\ \mathcal{F} \wedge \mathcal{S} \preccurlyeq \mathcal{F} \Rightarrow \mathsf{X}^{|\mathsf{F}|} - \mathsf{X} = \prod \{\mathfrak{m}_a \mid a \in \mathsf{F}\}$$

Note that in our formalisation, this product is over a set, which eliminates duplicates. This result shows that if a monic irreducible divides $\mathsf{X}^{|\mathsf{F}|} - \mathsf{X}$, it is the minimal polynomial of some field element, by unique factorisation.

5.2 Isomorphic Fields

We have shown that every finite field has prime characteristic p (Lemma 17), which is also the order of its prime field. Note that the prime field operations by repeated addition of by multiplicative identity are identical to modulo arithmetic in $\mathbb{Z}_p$. Hence,

Lemma 30 *For a finite field $\mathcal{F}$, its prime field is isomorphic to $\mathbb{Z}_p$ where $p = \mathsf{char}(\mathcal{F})$.*

$$\vdash \mathsf{FiniteField}\ \mathcal{F} \Rightarrow \mathbf{PF}_{\mathcal{F}} \cong \mathbb{Z}_{\mathsf{char}(\mathcal{F})}$$

Consider two finite fields of the same order. By Theorem 1, this means equal prime powers, which happens only when both primes and powers are equal. This implies that isomorphic finite fields must have the same characteristic by Lemma 25. Therefore:

Lemma 31 *Two finite fields of the same order have isomorphic prime fields.*

$$\vdash \mathsf{FiniteField}\ \mathcal{F}_1 \wedge \mathsf{FiniteField}\ \mathcal{F}_2 \wedge |\mathsf{F}_1| = |\mathsf{F}_2| \Rightarrow \mathbf{PF}_{\mathcal{F}_1} \cong \mathbf{PF}_{\mathcal{F}_2}$$

Since the minimal polynomials $\mathfrak{m}_a$ for $a \in \mathsf{F}$ are subfield irreducibles (see property (1) in Sect. 5.1), they can be used to construct quotient fields $\mathcal{S}[\mathsf{X}]/(\mathfrak{m}_a)$. If $a \in \pi_{\mathcal{F}}$, a primitive of the finite field (see Sect. 3.2), this can be shown (e.g., see Belk [12]):

Lemma 32 *A finite field is isomorphic to the quotient field by the minimal polynomial of a primitive.*

$$\vdash \mathsf{FiniteField}\ \mathcal{F} \wedge \mathcal{S} \preccurlyeq \mathcal{F} \wedge a \in \pi_{\mathcal{F}} \Rightarrow \mathcal{F} \cong \mathcal{S}[\mathsf{X}]/(\mathfrak{m}_a)$$

These ideas lead directly to our third key result, the uniqueness of finite fields up to isomorphism: **Theorem** 3

$$\vdash \mathsf{FiniteField}\ \mathcal{F}_1 \wedge \mathsf{FiniteField}\ \mathcal{F}_2 \wedge |\mathsf{F}_1| = |\mathsf{F}_2| \Rightarrow \mathcal{F}_1 \cong \mathcal{F}_2$$

Proof [13]" Let $|\mathsf{F}_1| = |\mathsf{F}_2| = q$. Note that their primes fields are isomorphic by Lemma 31, i.e., there is an isomorphism: $\vartheta : \mathbf{PF}_{\mathcal{F}_1} \to \mathbf{PF}_{\mathcal{F}_2}$. Let $a \in \pi_{\mathcal{F}}$ be a primitive of $\mathcal{F}_1$. Its minimal polynomial $\mathfrak{m}_a$ in the prime field has coefficients in $\mathbf{PF}_{\mathcal{F}_1}$. Then $\vartheta(\mathfrak{m}_a)$, which is the polynomial whose coefficients are the ϑ-image of the corresponding coefficients of $\mathfrak{m}_a$, is a subfield polynomial of $\mathcal{F}_2[\mathsf{X}]$ with coefficients in $\mathbf{PF}_{\mathcal{F}_2}$. The isomorphism ϑ ensures that:

- Note that $\mathfrak{m}_a$ is irreducible by property (1) from Sect. 5.1. Thus $\vartheta(\mathfrak{m}_a)$ is also irreducible in $\mathcal{F}_2[\mathsf{X}]$, and it divides $\vartheta(\mathsf{X}^q - \mathsf{X}) = \vartheta(\mathsf{X})^q - \vartheta(\mathsf{X})$, a polynomial in $\mathcal{F}_2[\mathsf{X}]$ which is a product of the minimal polynomials of the elements of $\mathcal{F}_2$ (Lemma 29). Therefore $\vartheta(\mathfrak{m}_a)$ equals to some minimal polynomial $\mathfrak{m}_b$ in $\mathcal{F}_2[\mathsf{X}]$, with $b \in \mathsf{F}_2$.
- both a and b have the same order, so b is a primitive in $\mathcal{F}_2$.
- polynomial division is preserved: the quotient and remainder by a polynomial modulus will map to their respective images, giving in general, when f is the isomorphism between $\mathcal{F}_1$ and $\mathcal{F}_2$:

  $$\vdash \mathcal{F}_1 \cong_{(f)} \mathcal{F}_2 \Rightarrow \forall \mathsf{h}.\ \mathsf{ipoly}\ \mathsf{h} \Rightarrow \mathcal{F}_1[\mathsf{X}]/(\mathsf{h}) \cong_{(\mathsf{MAP}\ f)} \mathcal{F}_2[\mathsf{X}]/(f(\mathsf{h}))$$

  where $(\mathsf{MAP}\ f)$ is the isomorphism between polynomials, using f for each coefficient:

  $$(\mathsf{MAP}\ f)\left(\sum_{j=0}^{n} c_j \mathsf{X}^j\right) = \sum_{j=0}^{n} f(c_j)\mathsf{X}^j \qquad \text{where } c_j \in \mathsf{F}_1 \text{ gives } f(c_j) \in \mathsf{F}_2$$

[13] This proof, based on quotient fields by minimal polynomials of primitives, is adapted from Belk [12], Theorem 3. Similar ideas are given in Herstein [25], Theorem 6.4.2.

Using Lemma 32 and applying the last result for the isomorphic prime fields, taking $\mathsf{h} = \mathfrak{m}_a$, we have:

$$\mathcal{F}_1 \cong \mathbf{PF}_{\mathcal{F}_1}[\mathsf{X}]/(\mathfrak{m}_a) \cong \mathbf{PF}_{\mathcal{F}_2}[\mathsf{X}]/(\#(\mathfrak{m}_a)) = \mathbf{PF}_{\mathcal{F}_2}[\mathsf{X}]/(\mathfrak{m}_b) \cong \mathcal{F}_2$$

□

Our first formalisation of this result is to make an effort to construct an explicit isomorphism between two finite fields of equal order. Although the explicit isomorphic map is clumsy to express, it is essentially the chain of isomorphic maps given above.

6 Existence and Uniqueness: Maximizing Type Generality

Our Theorem 3, stating the uniqueness of fields of the same order is "doubly polymorphic" in both fields: as we can see when we redisplay the theorem with extra type annotations, the related fields may be over different underlying types α and β:

$$\vdash \mathsf{FiniteField}\ (\mathcal{F}_1 : \alpha\ \mathtt{field}) \wedge \mathsf{FiniteField}\ (\mathcal{F}_2 : \beta\ \mathtt{field}) \wedge |\mathsf{F}_1| = |\mathsf{F}_2| \Rightarrow \mathcal{F}_1 \cong \mathcal{F}_2$$

However, our "base" Theorem 2, stating the existence of finite fields of prime power order, is over fields of numeric polynomial type:

$$\vdash \mathsf{prime}\ (p : \mathtt{num}) \wedge (0 : \mathtt{num}) < (d : \mathtt{num}) \Rightarrow \exists (\mathcal{F} : \mathtt{num\ poly\ field}).\ \mathsf{FiniteField}\ \mathcal{F} \wedge |\mathsf{F}| = ((p^d) : \mathtt{num})$$

This is because we started with the finite field $\mathbb{Z}_p$ for a prime p (Theorem 26), with elements of numeric type. The resulting quotient field $\mathbb{Z}_p[\mathsf{X}]/(\mathsf{h})$ by an irreducible h of degree d (Theorem 27) will have elements of numeric polynomial type.

If desired, we can lift the existence result to an arbitrary type α, as long as that type has enough elements. Here we satisfy that cardinality constraint by requiring the universe of that type (written $\mathcal{U}(:\alpha)$) to be infinite.

The first step exploits the fact that an infinite set A has the same cardinality as the set of all possible (finite) lists of elements drawn from A:

Lemma 33 *There is a bijection between all finite lists with elements type α and the elements themselves.*

$$\vdash \mathsf{INFINITE}\ \mathcal{U}(:\alpha) \Rightarrow \exists f.\ f : \mathcal{U}(:\alpha\ \mathtt{list}) \leftrightarrow \mathcal{U}(:\alpha)$$

We instantiate this lemma with α set to num and thereby show the existence of finite fields of the desired order over the type of natural numbers. Finally, because we know that our desired destination type has an infinite cardinality, we can inject homomorphically from the natural numbers into α, giving us:

Theorem 34 *Given an infinite type and a nontrivial prime power, there exist a finite field of that type and order.*

$$\vdash \mathsf{prime}\ (p : \mathtt{num}) \wedge (0 : \mathtt{num}) < (n : \mathtt{num}) \wedge \mathsf{INFINITE}\ \mathcal{U}(:\alpha) \Rightarrow \exists (\mathcal{F} : \alpha\ \mathtt{field}).\ \mathsf{FiniteField}\ \mathcal{F} \wedge |\mathsf{F}| = ((p^n) : \mathtt{num})$$

This establishes the existence of finite fields with prime power order, for a generic type, provided its universe is infinite. As a point of interest, we can obtain the same result *via* a perhaps more traditional route: using extension fields and splitting fields.

6.1 Extension and Splitting Fields

Given a finite field $(\mathcal{F}\ :\alpha\ \texttt{field})$, consider a polynomial t in $\mathcal{F}[\mathsf{X}]$ with $\deg\ \mathsf{t}\ \neq\ 0$, i.e., not a constant polynomial. Then t has an irreducible polynomial h as its factor. We shall first concentrate on this irreducible h, then show its relationship with t.

Note that the quotient field $\mathcal{F}[\mathsf{X}]/(\mathsf{h})$ from Theorem 27 has type $(\alpha\ \texttt{poly field})$. It contains X when $\deg\ \mathsf{X}\ <\ \deg\ \mathsf{h}$, i.e. $1\ <\ \deg\ \mathsf{h}$. Because h divides itself, $\mathsf{h} = \mathsf{h}[\![\mathsf{X}]\!]\ \equiv\ \mathbf{0}\ \pmod{\mathsf{h}}$, showing that [14]:

Lemma 35 *Let* h *be a non-linear polynomial with coefficients from a field* $\mathcal{F}$. *Then* X *is a root of* h *in the quotient ring* $\mathcal{F}[\mathsf{X}]/(\mathsf{h})$.

$$\vdash\ \mathsf{Field}\ \mathcal{F}\ \wedge\ \mathsf{poly}\ \mathsf{h}\ \wedge\ 1\ <\ \deg\ \mathsf{h}\ \Rightarrow\ \mathsf{h}[\![\mathsf{X}]\!]\ \equiv\ \mathbf{0}\ \pmod{\mathsf{h}}$$

Assume that α type is infinite, i.e., $\mathsf{INFINITE}\ \mathcal{U}(:\alpha)$. The bijection between $\mathcal{U}(:\alpha\ \texttt{poly})$ and $\mathcal{U}(:\alpha)$ from Lemma 33 allows the conversion of the quotient field to an extension field $\mathcal{E}$ of type $(\alpha\ \texttt{field})$. The constant polynomials in the quotient field becomes a subfield $\mathcal{S}$ of $\mathcal{E}$, which is isomorphic to the coefficients field $\mathcal{F}$ through a bijective map f:

$$\mathcal{F}\ \cong_f\ \mathcal{S}\ \wedge\ \mathcal{S}\ \preccurlyeq\ \mathcal{E}$$

At a high level, one might hope that $\mathcal{F}$ is a subset of $\mathcal{E}$ is true if and only if $\mathcal{E}$ is an extension of $\mathcal{F}$. However, the previous discussion shows that for a typed system like HOL4 there is a subtle difference:

- A field/subfield pair $\mathcal{S}\ \preccurlyeq\ \mathcal{F}$ relates fields of the same type, with the same field operations.
- A field $\mathcal{F}$ and its extension field $\mathcal{E}$, though possibly of the same type, are related through an isomorphic subfield $\mathcal{S}$ of $\mathcal{E}$, with extended field operations in $\mathcal{E}$.

Recall that polynomial t has an irreducible factor h, i.e., h has no roots in $\mathcal{F}$. Since the coefficients of t and h are in $\mathcal{F}$, they have images $f(\mathsf{t})$ and $f(\mathsf{h})$ in $\mathcal{S}$. The root X of h in the quotient field $\mathcal{F}[\mathsf{X}]/(\mathsf{h})$ from Lemma 35 corresponds to some element in the extension field $\mathcal{E}$.

Note that any root of $f(\mathsf{h})$ is also a root of $f(\mathsf{t})$. Therefore, the extension field $\mathcal{E}$ contains a root for $f(\mathsf{t})$. The set of roots of $f(\mathsf{t})$ in $\mathcal{E}$ is denoted by $\mathsf{roots}_{\mathcal{E}}\ f(\mathsf{t})$:

$$\begin{aligned}\vdash\ &\mathsf{FiniteField}\ \mathcal{F}\ \wedge\ \mathsf{INFINITE}\ \mathcal{U}(:\alpha)\ \wedge\ \mathsf{poly}\ \mathsf{t}\ \wedge\ 0\ <\ \deg\ \mathsf{t}\ \Rightarrow\\ &\quad \exists \mathcal{S}\ \mathcal{E}\ f\ b.\ \mathcal{F}\ \cong_f\ \mathcal{S}\ \wedge\ \mathcal{S}\ \preccurlyeq\ \mathcal{E}\ \wedge\ \mathsf{FINITE}\ \mathsf{E}\ \wedge\ b\ \in\ \mathsf{roots}_{\mathcal{E}}\ f(\mathsf{t})\end{aligned}$$

Having field $\mathcal{F}$ and its extension $\mathcal{E}$ of the same type enables successive extensions until $\mathcal{E}$ reduces $f(\mathsf{t})$ into linear factors, i.e., containing all its roots. This is called a splitting field for t, denoted by $\mathsf{splitting}_{\mathcal{E}}\ f(\mathsf{t})$:

$$\begin{aligned}\vdash\ &\mathsf{FiniteField}\ \mathcal{F}\ \wedge\ \mathsf{INFINITE}\ \mathcal{U}(:\alpha)\ \wedge\ \mathsf{poly}\ \mathsf{t}\ \wedge\ 0\ <\ \deg\ \mathsf{t}\ \Rightarrow\\ &\quad \exists \mathcal{S}\ \mathcal{E}\ f.\ \mathcal{F}\ \cong_f\ \mathcal{S}\ \wedge\ \mathcal{S}\ \preccurlyeq\ \mathcal{E}\ \wedge\ \mathsf{FINITE}\ \mathsf{E}\ \wedge\ \mathsf{splitting}_{\mathcal{E}}\ f(\mathsf{t})\end{aligned}$$

The splitting field provides another proof for the existence of finite fields of an infinite type:

Proof of Theorem 34 [15] Given a prime p, a positive n, an infinite type α, one can start with a field $(\mathcal{F}\ :\alpha\ \texttt{field})$ isomorphic to $\mathbb{Z}_p$. In this field $\mathcal{F}$, with $|\mathsf{F}|\ =\ p$, consider the polynomial $\mathsf{t}\ =\ \mathsf{X}^{p^n}\ -\ \mathsf{X}$. The smallest splitting field $\mathcal{E}$ of t has all the roots of t. Note that

[14] When h is not required to be irreducible, $\mathcal{F}[\mathsf{X}]/(\mathsf{h})$ is a quotient ring, which becomes a quotient field when h is irreducible.

[15] Such proofs can be found in, e.g., Herstein [25] Theorem 6.3.3, Judson [29] Theorem 20.5, or Robinson [40] Theorem 10.3.1.

$\mathsf{char}(\mathcal{E}) = p$ by Theorem 4. Thus the formal derivative of $\mathtt{t}$ is a constant, sharing no root with $\mathtt{t}$. This shows that $\mathtt{t}$ has no multiple roots, i.e., all the p^n roots of $\mathtt{t}$ are distinct. Hence the field $(\mathcal{E}\ :\alpha\ \mathtt{field})$ has precisely p^n elements. □

We have shown that it is possible to follow what one might argue is a standard approach: making use of splitting fields to establish the existence of finite fields of order p^n for all prime p and positive n. However, the pleasant generality of the splitting field theorems is somewhat undone by the requirement to add the various INFINITE $\mathcal{U}(:\alpha)$ preconditions. It is therefore a matter of taste as to which one to prefer.

6.2 Existence of Finite Fields of Finite Type

The requirement that the universe of α be infinite guarantees that an arbitrary amount of splitting can be carried out. Of course, the final splitting field is still finite, and so one is always able to construct an isomorphic finite field over a sufficiently large finite type. For example, if one started with the two-element finite field over $\mathtt{bool}$, isomorphic to $\mathbb{Z}_2$, one could eventually carry this procedure out to construct a splitting field over a finite type of cardinality 2^n for any value of positive n. Though it is clear that this procedure can always be carried out, in HOL4 we cannot express the construction because we would need to be able to make a statement asserting the existence of a type of a specific finite cardinality.

7 Subfield Classification

Given a finite field $\mathcal{F}$, any subfield $\mathcal{S} \preccurlyeq \mathcal{F}$ is itself a finite field. Therefore its multiplicative group is cyclic by Theorem 20. This shows that $\mathcal{S}$ has a primitive, a field element of order $|\mathsf{S}| - 1$. From Lemma 25, we can express $|\mathsf{S}| = p^n$, where $p = \mathsf{char}(\mathcal{S})$ is the characteristic, and $n = \mathsf{deg}(\mathcal{S})$ is the degree. Note that $p = \mathsf{char}(\mathcal{F})$ by Theorem 4.

Therefore, if a finite field $\mathcal{F}$ has a subfield $\mathcal{S} \preccurlyeq \mathcal{F}$ with $|\mathsf{S}| = p^n$, the set $(\mathsf{orders}\ \mathcal{F}^*\ (p^n - 1))$ is non-empty. On the other hand, if this set is non-empty, all its elements, together with $\mathbb{0}$, are the only roots of the polynomial $\mathsf{X}^{p^n} - \mathsf{X}$. These roots form a subfield (see discussion below) of the finite field $\mathcal{F}$, so that:

Lemma 36 *Let a finite field have characteristic p. A subfield with degree n exists if and only if a field element of order $(p^n - 1)$ exists.*

$$\vdash \mathsf{FiniteField}\ \mathcal{F} \Rightarrow \forall n.\ (\exists \mathcal{S}.\ \mathcal{S} \preccurlyeq \mathcal{F} \wedge \mathsf{deg}(\mathcal{S}) = n) \iff \mathsf{orders}\ F^*\ (\mathsf{char}(\mathcal{F})^n - 1) \neq \emptyset$$

This result leads directly to the classification of subfields of a finite field: **Theorem 5**

$$\vdash \mathsf{FiniteField}\ \mathcal{F} \Rightarrow \forall n.\ (\exists \mathcal{S}.\ \mathcal{S} \preccurlyeq \mathcal{F} \wedge \mathsf{deg}(\mathcal{S}) = n) \iff n \mid \mathsf{deg}(\mathcal{F})$$

Proof Let $p = \mathsf{char}(\mathcal{F})$ and $d = \mathsf{deg}(\mathcal{F})$, then $|\mathsf{F}| = p^d$ from Lemma 25. Using Lemma 36, a subfield $\mathcal{S} \preccurlyeq \mathcal{F}$ with degree $\mathsf{deg}(\mathcal{S}) = n$ exists if and only if the set $(\mathsf{orders}\ \mathcal{F}^*\ (p^n - 1))$ is non-empty. The cardinality equation of Lemma 18 shows that this occurs if and only if $(p^n - 1) \mid (p^d - 1)$. Applying this numerical identity [16]:

$$\vdash \mathsf{gcd}(t^n - 1, t^m - 1) = t^{\mathsf{gcd}(n,m)} - 1 \qquad \text{for any natural numbers } t, n, m,$$

we can see that $(p^n - 1) \mid (p^d - 1)$ if and only if $n \mid d$. □

[16] Our proof of this identity follows that given in McEliece [37], Theorem 2.3.

In asserting that for the polynomial $\mathsf{h} = \mathsf{X}^{p^n} - \mathsf{X}$, its roots form a subfield of the field of coefficients (see, e.g., McEliece [37]), a key step is to show that if two field elements x and y are roots of h, then $(x - y)$ is also a root, and if $y \neq \mathbb{0}$ then $x * y^{-1}$ is also a root. The latter one is trivial by the properties of powers and exponentials, but the first depends on iterations of this basic polynomial identity for a ring with prime characteristic:

$$\vdash \mathsf{Ring}\ \mathcal{R} \wedge \mathsf{prime}\ \mathsf{char}(\mathcal{R}) \Rightarrow \forall x\ y.\ x \in \mathsf{R} \wedge y \in \mathsf{R} \Rightarrow (x + y)^{\mathsf{char}(\mathcal{R})} = x^{\mathsf{char}(\mathcal{R})} + y^{\mathsf{char}(\mathcal{R})}$$

This holds for any finite field $\mathcal{F}$, as $\mathsf{char}(\mathcal{F})$ is prime by Lemma 17. This identity with prime exponents is a variation of Fermat's Little Theorem, which had been formalised by the authors [13].

8 Cyclotomic Polynomials

In a finite field $\mathcal{F}$, each nonzero element in F^* has a nonzero order, say n. The cardinality of $(\mathsf{orders}\ \mathcal{F}^*\ n)$, the set of elements with order equal to n, is given by Lemma 18:

$$\vdash \mathsf{FiniteField}\ \mathcal{F} \Rightarrow \forall n.\ |\mathsf{orders}\ F^*\ n| = \textbf{if}\ n \mid |\mathsf{F}^*|\ \textbf{then}\ \varphi(n)\ \textbf{else}\ 0$$

The product of factors of elements of order n is called the n-th cyclotomic polynomial, denoted by $\boldsymbol{\Phi}_n$:

Definition 37 $\mathsf{Field}\ \mathcal{F} \Rightarrow \boldsymbol{\Phi}_n = \prod \{\mathsf{X} - a * \mathbf{1} \mid a \in \mathsf{F}^* \wedge \mathsf{order}_{\mathcal{F}^*}(a) = n\}$

Since $\boldsymbol{\Phi}_n$ is a product of monic monomials, its degree is given by the number of factors:

Lemma 38 $\vdash \mathsf{FiniteField}\ \mathcal{F} \Rightarrow \forall n.\ \mathsf{deg}\ \boldsymbol{\Phi}_n = \textbf{if}\ n \mid |\mathsf{F}^*|\ \textbf{then}\ \varphi(n)\ \textbf{else}\ 0$

Cyclotomic polynomials are related to the factorisation of $\mathsf{X}^n - \mathbf{1}$, our second application: **Theorem** 6

$$\vdash \mathsf{FiniteField}\ \mathcal{F} \wedge n \mid |\mathsf{F}^*| \Rightarrow \mathsf{X}^n - \mathbf{1} = \prod \{\boldsymbol{\Phi}_m \mid m \in \mathsf{divisors}\ n\}$$

Proof [17] Note that $\boldsymbol{\Phi}_m$ consists of factors of elements with order m, i.e., $x \in \mathsf{F}^*$ with $x^m = \mathbb{1}$. If $m \mid n$, then $x^n = x^{m(\frac{n}{m})} = \mathbb{1}$. Therefore x is a root of the polynomial $\mathsf{X}^n - \mathbf{1}$. The factors are pairwise coprime, and their product, $\boldsymbol{\Phi}_m$, divides $\mathsf{X}^n - \mathbf{1}$:

$$\vdash \mathsf{FiniteField}\ \mathcal{F} \Rightarrow \forall m\ n.\ m \mid n \Rightarrow \boldsymbol{\Phi}_m \mid \mathsf{X}^n - \mathbf{1}$$

Since two different cyclotomic polynomials, say $\boldsymbol{\Phi}_m$ and $\boldsymbol{\Phi}_k$, involve factors associated with elements of different orders n and k, the cyclotomic polynomials are pairwise coprime. It follows that their product over the divisors of n will divide $\mathsf{X}^n - \mathbf{1}$, or

$$\mathsf{X}^n - \mathbf{1} = \mathsf{h} \prod_{m \mid n} \boldsymbol{\Phi}_m \quad \text{for some polynomial } \mathsf{h} \tag{3}$$

Equating the polynomial degree of both sides using Lemma 38, and applying Euler's φ-function identity (Lemma 19), h must be a constant. For a product of monic polynomials giving a monic result, it must be that $\mathsf{h} = \mathbf{1}$. □

[17] This proof, based on divisibility and pairwise coprime factors, is adapted from Ireland and Rosen [28], Proposition 13.3.2.

We prove that cyclotomic polynomials have coefficients in any subfield, i.e., they are subfield polynomials:

$$\vdash \mathsf{FiniteField}\ \mathcal{F} \wedge \mathcal{S} \preccurlyeq \mathcal{F} \Rightarrow \forall n.\ \mathsf{poly}_{\mathcal{S}}\ \boldsymbol{\Phi}_n$$

Since the prime field $\mathbf{PF}_{\mathcal{F}}$ is the smallest subfield of a finite field $\mathcal{F}$ (Lemma 24), and $\mathbf{PF}_{\mathcal{F}} \cong \mathbb{Z}_{\mathsf{char}(\mathcal{F})}$ (Lemma 30), the coefficients of $\boldsymbol{\Phi}_n$ are integers. Indeed, using Equation 3 with $\mathsf{h} = \mathbf{1}$ and polynomial division, we can deduce, successively, that $\mathsf{X} - \mathbf{1} = \boldsymbol{\Phi}_1$, then $\mathsf{X}^2 - \mathbf{1} = \boldsymbol{\Phi}_1 * \boldsymbol{\Phi}_2$ giving $\boldsymbol{\Phi}_2 = \mathsf{X} + \mathbf{1}$, then $\mathsf{X}^3 - \mathbf{1} = \boldsymbol{\Phi}_1 * \boldsymbol{\Phi}_3$ giving $\boldsymbol{\Phi}_3 = \mathsf{X}^2 + \mathsf{X} + \mathbf{1}$, etc., by keeping track of the divisors of n.

8.1 Alternative Presentations of Φ_n

Our cyclotomic polynomials are defined in a finite field, so that there are elements of various orders to give the factors and form the products $\boldsymbol{\Phi}_n$. As the statement of Theorem 6 shows, Equation 3 holds in a finite field $\mathcal{F}$ with a condition: $n \mid |\mathsf{F}^*|$. This is different from usual treatments [18], where Equation 3 holds for all $0 < n$.

Some textbooks, e.g., Rotman [41] and Herstein [24], treat the cyclotomic polynomials $\boldsymbol{\Phi}_n$ as polynomials with rational coefficients, i.e., elements of $\mathbb{Q}[\mathsf{X}]$. They define $\boldsymbol{\Phi}_n$ as a product of factors from all complex n-th primitive roots of unity:

$$\boldsymbol{\Phi}_n = \prod_{k=1}^{n} \left(\mathsf{X} - e^{2\pi i \frac{k}{n}}\right) \quad \text{with } \gcd(k, n) = 1 \text{ and } i^2 = -1$$ then proving that, due to pairs of complex conjugate factors and properties of complex n-th primitive roots of unity, the resulting $\boldsymbol{\Phi}_n$'s have integer coefficients, i.e., they are indeed in $\mathbb{Z}[\mathsf{X}]$, a subring of $\mathbb{Q}[\mathsf{X}]$. Others, e.g., Herstein [25] and Garrett [22], simply define $\boldsymbol{\Phi}_n$ recursively by Equation 3 with $\mathsf{h} = \mathbf{1}$. Either approach involves a field (rationals $\mathbb{Q}$ or complex $\mathbb{C}$) which is not finite.

Within finite fields, we can prove that there is always one in which Equation 3 holds for any positive n:

Theorem 39 *For $n \neq 0$, $\mathsf{X}^n - \mathbf{1}$ is a product of cyclotomic factors of the divisors of n in some finite field.*

$$\vdash 0 < n \Rightarrow \exists \mathcal{F}.\ \mathsf{X}^n - \mathbf{1} = \prod \{\boldsymbol{\Phi}_m \mid m \in \mathsf{divisors}\ n\}$$

Proof Given n, choose a prime p not a factor of n. Then $\gcd(n, p) = 1$, and we can compute $d = \mathsf{order}_n(p)$. This is the smallest exponent $d > 0$ such that $p^d \equiv 1 \pmod{n}$, or $n \mid p^d - 1$. By Theorem 2, there exists a finite field $\mathcal{F}$ of order p^d, and $|\mathsf{F}^*| = p^d - 1$. Apply Theorem 6 with this finite field $\mathcal{F}$ to obtain the desired factorisation of $\mathsf{X}^n - \mathbf{1}$. □

8.2 A Special Factor of $\mathsf{X}^n - \mathbf{1}$

Our work on the AKS algorithm requires the following result, our final application of finite fields:

Theorem 7

$$\vdash \mathsf{FiniteField}\ \mathcal{F} \wedge 0 < k \wedge 1 < \mathsf{order}_k(|\mathsf{F}|) \Rightarrow \exists z.\ \mathsf{monic}\ z \wedge \mathsf{ipoly}\ z \wedge z \mid \mathsf{X}^k - \mathbf{1} \wedge \mathsf{deg}\ z = \mathsf{order}_k(|\mathsf{F}|) \wedge \mathsf{order}_z(\mathsf{X}) = k$$

[18] See, e.g., Bastida and Lyndon [11] Proposition 3.5.6, or Newman [38] Theorem 5.3.

Proof Let $d = \mathsf{order}_n(|\mathsf{F}|)$. This means $|\mathsf{F}|^d \equiv 1 \pmod{n}$, or $n \mid |\mathsf{F}|^d - 1$. By Theorem 28, there exists a monic irreducible polynomial z with $\mathsf{deg}\ \mathsf{z} = d$, giving a quotient field $\mathcal{F}[\mathsf{X}]/(\mathsf{z})$ of order $|\mathsf{F}|^d$.

Let $\mathcal{E} = \mathcal{F}[\mathsf{X}]/(\mathsf{z})$, the polynomial quotient field. Note that $\mathcal{E}$ has a subfield, the constant polynomials, which is isomorphic to $\mathcal{F}$. Therefore the finite field $\mathcal{E}$ can be taken as an extension field of $\mathcal{F}$ (see Sect. 6.1). In the discussion that follows, we identify the subfield of constant polynomials with $\mathcal{F}$, i.e., treating $\mathcal{F} \preccurlyeq \mathcal{E}$.

Note that $|\mathsf{E}^*| = |\mathsf{F}|^d - 1$, and $n \mid |\mathsf{E}^*|$. This fact is significant:

(a) Since Theorem 6 applies, the subfield polynomial $\mathsf{X}^n - \mathbf{1}$ is a product of cyclotomic factors. In particular, $\boldsymbol{\Phi}_n \mid (\mathsf{X}^n - \mathbf{1})$.
(b) Moreover, Lemma 18 applies, giving some nonzero element a with order equal to n, i.e., $a \in \mathsf{E}^*$ with $\mathsf{order}_{\mathcal{E}^*}(a) = n$.

Take $\mathsf{h} = \mathfrak{m}_a$, the minimal polynomial of this element a with order n. Then h is monic and irreducible in $\mathcal{F}$. Its degree is given by (see, e.g., Belk [12]):

$$\vdash \mathsf{FiniteField}\ \mathcal{E} \wedge \mathcal{F} \preccurlyeq \mathcal{E} \Rightarrow \forall a.\ a \in \mathsf{E}^* \Rightarrow \mathsf{deg}\ \mathfrak{m}_a = \mathsf{order}_{\mathsf{order}_{\mathcal{E}^*}(a)}(|\mathsf{F}|)$$

In other words, $\mathsf{deg}\ \mathsf{h} = d$. Note that $\boldsymbol{\Phi}_n$ collects all the factors from elements of order n (see Definition 37), so it is a product of all minimal polynomials of these elements:

$$\vdash \mathsf{FiniteField}\ \mathcal{E} \wedge \mathcal{F} \preccurlyeq \mathcal{E} \Rightarrow \forall n.\ \boldsymbol{\Phi}_n = \prod \{\mathfrak{m}_a \mid a \in \mathsf{orders}\ \mathcal{E}^*\ n\}$$

Thus $\mathsf{h} \mid \boldsymbol{\Phi}_n$. With $\boldsymbol{\Phi}_n \mid (\mathsf{X}^n - \mathbf{1})$, this implies $\mathsf{h} \mid (\mathsf{X}^n - \mathbf{1})$.

Now X is a root of h in the quotient field $\mathcal{F}[\mathsf{X}]/(\mathsf{h})$ (Lemma 35). Note that $\mathsf{deg}\ \mathsf{h} = \mathsf{deg}\ \mathsf{z}$, and both h and z are monic and irreducible. Their quotient fields are isomorphic by uniqueness of finite fields of the same order (Theorem 3). Let $\mathsf{Y} \in \mathsf{E}^*$ be the isomorphic element corresponding to X. Then Y is a root of h in $\mathcal{E}$, where $\mathsf{h} \mid \boldsymbol{\Phi}_n$. Therefore Y is also a root of $\boldsymbol{\Phi}_n$. Again, $\boldsymbol{\Phi}_n$ is a product of factors of elements with order equal to n (Definition 37), hence $\mathsf{order}_{\mathsf{h}}(\mathsf{Y}) = n$. Since X is the counterpart of Y, and isomorphism preserves element orders, we have $\mathsf{order}_{\mathsf{h}}(\mathsf{X}) = n$. □

Note how this proof involves all the key topics in this paper: existence and uniqueness of finite fields, subfields, extension fields, minimal polynomials, and cyclotomic polynomials.

9 Underlying Library

We have built an extensive library to support our work on finite fields, meaning that we have formalised more topics than presented so far. Some of these topics work behind the scenes to derive our key results, and they are clearly useful elements of any complete finite field library. We shall briefly survey some of these other topics.

9.1 Subfield Elements and Polynomials

Given a field/subfield pair $\mathcal{S} \preccurlyeq \mathcal{F}$, the Frobenius map takes a field element x to $x^{|\mathsf{S}|}$. A field element is in the subfield if and only if it is fixed by the Frobenius map:

$$\vdash \mathsf{FiniteField}\ \mathcal{F} \Rightarrow \forall \mathcal{S}.\ \mathcal{S} \preccurlyeq \mathcal{F} \Rightarrow \forall x.\ x \in \mathsf{F} \Rightarrow (x \in \mathsf{S} \iff x^{|\mathsf{S}|} = x)$$

This is the basis of the following check to test whether a field polynomial is a subfield polynomial:

$$\vdash \text{FiniteField } \mathcal{F} \Rightarrow \forall \mathcal{S}.\ \mathcal{S} \preccurlyeq \mathcal{F} \Rightarrow \forall \mathsf{h}.\ \text{poly } \mathsf{h} \Rightarrow (\text{poly}_{\mathcal{S}}\ \mathsf{h} \iff \mathsf{h}^{|\mathsf{S}|} = \mathsf{h}[\![\mathsf{X}^{|\mathsf{S}|}]\!])$$

We use the last criteria to establish that the cyclotomic polynomials $\boldsymbol{\Phi}_n$ have integer coefficients.

9.2 Conjugates and Minimal Polynomials

With respect to a field/subfield pair $\mathcal{S} \preccurlyeq \mathcal{F}$, the successive images of a field element under the Frobenius map are its conjugates. The set of all conjugates of a field element a is denoted by $\text{Conj}_{\mathcal{S}}\ a$:

Definition 40 $\quad \text{Conj}_{\mathcal{S}}\ a = \{a^{|\mathsf{S}|^n} \mid n \in \mathcal{U}(:\text{num})\}$

We prove that the minimal polynomial $\mathfrak{m}_a$ of the element a is a product of its conjugate factors:

$$\vdash \text{FiniteField } \mathcal{F} \wedge \mathcal{S} \preccurlyeq \mathcal{F} \Rightarrow \forall a.\ a \in \mathsf{F} \Rightarrow \mathfrak{m}_a = \prod \{\mathsf{X} - c * \mathbf{1} \mid c \in \text{Conj}_{\mathcal{S}}\ a\}$$

Many properties of the minimal polynomial of a field element, e.g., those given in Sect. 5.1, are established through this relationship.

9.3 Polynomials of Special Forms

The equations 1, 2 and 3 are not isolated results. They are deductions from a detailed study of polynomials of special forms: $\mathsf{X}^n - \mathsf{X}$ and $\mathsf{X}^n - \mathbf{1}$. For example, a polynomial of the first form with exponent $|\mathsf{F}|^d$ has all monic irreducibles of degree d as factors:

$$\vdash \text{FiniteField } \mathcal{F} \Rightarrow \forall \mathsf{h}.\ \text{monic } \mathsf{h} \wedge \text{ipoly } \mathsf{h} \Rightarrow \mathsf{h} \mid \mathsf{X}^{|\mathsf{F}|^{\deg\ \mathsf{h}}} - \mathsf{X}$$

and polynomials of the second form have an interesting divisibility condition depending only on their exponents when the coefficients come from a non-trivial ring:

$$\vdash \text{Ring } \mathcal{R} \wedge \mathbb{1} \neq \mathbb{0} \Rightarrow \forall n\ m.\ \mathsf{X}^n - \mathbf{1} \mid \mathsf{X}^m - \mathbf{1} \iff n \mid m$$

This result provides another proof [19] to establish the classification of all subfields of a finite field (Theorem 5).

9.4 Ideals, Quotient Rings and Fields

We briefly mentioned these entities in Sect. 4. We have developed a whole theory around these concepts, and established some useful results. For example, denoting a ring and ideal pair by $\mathcal{I} \prec \mathcal{R}$, the quotient ring $\mathcal{R}\ /\ \mathcal{I}$ is indeed a ring:

$$\vdash \text{Ring } \mathcal{R} \wedge \mathcal{I} \prec \mathcal{R} \Rightarrow \text{Ring } (\mathcal{R}\ /\ \mathcal{I})$$

We define EuclideanRing $\mathcal{R}\ f$ for a ring $\mathcal{R}$ equipped with a norm function f, and PrincipalIdealRing $\mathcal{R}$ where every ideal is generated by a ring element. We prove that:

$$\vdash \text{EuclideanRing } \mathcal{R}\ f \Rightarrow \text{PrincipalIdealRing } \mathcal{R}$$

Let $\mathcal{R} \simeq_f \mathcal{S}$ denote that rings $\mathcal{R}$ and $\mathcal{S}$ have a homomorphism f. Then the kernel of f is an ideal of $\mathcal{R}$:

[19] Such a proof is given in McEliece [37] Theorem 6.6, or Ireland and Rosen [28] Proposition 7.1.5.

$$\vdash \mathcal{R} \simeq_f \mathcal{S} \Rightarrow \text{kernel } f\ \mathcal{R}\ \mathcal{S} \prec \mathcal{R}$$

We also define the notion of a maximal ideal:

Definition 41 $\text{maximal } \mathcal{R}\ \mathcal{I} \iff \mathcal{I} \prec \mathcal{R} \wedge \forall \mathcal{J}.\ \mathcal{I} \prec \mathcal{J} \wedge \mathcal{J} \prec \mathcal{R} \Rightarrow \mathcal{I} = \mathcal{J} \vee \mathcal{J} = \mathcal{R}$

and prove that a quotient ring is a field if and only if the ideal is maximal:

$$\vdash \text{Ring } \mathcal{R} \Rightarrow \forall \mathcal{I}.\ \mathcal{I} \prec \mathcal{R} \wedge \text{Field } (\mathcal{R} / \mathcal{I}) \iff \mathcal{I} \neq \mathcal{R} \wedge \text{maximal } \mathcal{R}\ \mathcal{I}$$

This result provides another proof of Theorem 27: the quotient ring by an irreducible is a quotient field, by showing that the ideal by an irreducible is maximal [20].

10 Related Work

Broadly speaking, there are three streams of formalisation work related to finite fields:

- *Galois Theory*
  Since the study of finite fields arises historically from Galois theory, any formalisation work related to Galois theory will inevitably touch upon finite fields.
- *Cryptography*
  There is a great deal of formalisation work on modern cryptographic protocols, as well as the correctness of related algorithms. The theory behind these protocols, and the implementation of such algorithms, can be based on finite fields.
- *Primality Testing*
  Many primality testing algorithms are based on properties of algebraic structures, including finite fields. Hence the formalisation of such algorithms will need the support of algebra, possibly finite fields.

Our project, the formalisation of the AKS algorithm (see Sect. 1.1), falls within the last category.

In Galois Theory, the emphasis is usually on groups rather than fields. For the other streams, although they are related to fields or finite fields, the focus is usually not on their purely abstract properties, but on the application of concrete number fields to the algebraic problem at hand.

Overall, these streams have not aimed at the classification of finite fields. Naturally though, many basic results appearing in this paper *have* been covered by such formalisation work. In the rest of this section, we shall describe these various overlaps.

10.1 Galois Theory

There is a long tradition in the formalisation of abstract algebra, starting with Peter Aczel's Galois project [1]. The LEGO system was developed, from which Barthe [9] gave a formal proof of the unsolvability of the symmetric group S_n with $n \geq 5$ and Bailey [8] formalised part of Galois theory. These were pioneering efforts, with the first building from monoids to rings, and the second containing basic vector spaces.

There was another attempt to formalise the Fundamental Theorem of Galois theory by Curiel [16] in Isabelle/HOL. The work involved rings and fields, up to field automorphisms. Further progress had difficulties with adapting a polynomial library for the more advanced work.

[20] Our proof followed the approach given in Herstein [25], Theorem 4.5.11.

The work having the most overlap by far with this paper is the formalisation of the Odd Order Theorem by Gonthier et al. [23] in Coq. This was a milestone, as even the published proof was the cumulative effort by many group theory experts. In this work, a great deal of abstract algebra was developed, with Galois theory playing a vital role, and finite fields were essential ingredients. Subjects covered by this project include vector spaces, extension fields, splitting fields, minimal polynomials and cyclotomic polynomials. These became the Mathematical Components library [6] in Coq.

Interestingly, their approach seems similar to ours in that rather than using normal extensions for Galois theory, they opted for splitting fields. Their "splitting fields" are fixed, relative to a base field, with extension fields as intermediate fields in between. Our subfield approach is fundamentally the same, in a different terminology (see Sect. 1.4), but was used to dodge problems arising from a relatively impoverished type system. It is not clear to us if the same motivation was pertinent in Coq, with its more expressive dependent type theory.

The Isabelle/HOL Algebra Library [18] is another substantial library for abstract algebra work, including rings, ideals, quotient rings, fields and polynomials. Thiemann and Yamada [43] formalised algebraic numbers in Isabelle/HOL, based on polynomials and subfields of complex numbers. Their theorems were not restricted to finite fields. Ongoing work on algebraic numbers in Coq based on field theory can be found in work done by Cohen [15].

The Mizar Mathematical Library [35] has several results covered in this paper, including work on abelian groups, fields and vector spaces by Kusak et al. [31], and primitive roots of unity and cyclotomic polynomials by Arneson and Rudnicki [4]. Arneso et al. [3] formalised Witt's proof of the Wedderburn Theorem [21] using skew-fields and vector spaces over skew-fields, which are not treated in our work.

10.2 Cryptography

The applications of finite fields to cryptography include elliptic curve algorithms and polynomial factorisation algorithms. The formalisation work either treats specific finite fields, or ventures into algebraic geometry which is outside the scope of our work.

In HOL, Hurd et al. [27] formalised elliptic curve cryptography based on a group structure. They defined algebraic structures (including field, vector space, projective space, and curve) for a generic type, but their work was based on concrete instances with numeric type.

In Mizar, Futa et al. [20] formalised some theorems on elliptic curve over a prime field by enriching the Mizar Mathematical Library.

In Coq, Bartzia and Strub [10] extended the Mathematical Components library for elliptic curves based on fields and projective geometry. Affeldt et al. [2] reported on the formalisation of Reed-Solomon codes and work on LDPC codes, using polynomials with coefficients from a field.

In Isabelle/HOL, Divasón et al. [17] have formalised the Berlekamp–Zassenhaus factorization algorithm. Their work involved the fields $\mathbb{Z}_p$ where p is a prime, and polynomials over such fields.

10.3 Primality Tests

The tools developed for the classification of finite fields support our project on the formalisation of the Agrawal-Kayal-Saxena (AKS) algorithm [14]. This is a deterministic,

[21] Skew fields are fields without the commutative requirement for multiplication, and Wedderburn Theorem asserts that every finite skew field must be commutative, i.e., a field.

polynomial-time primality test. Its proof is a beautiful application of the theory of finite fields. Indeed, the last application (Theorem 7) plays a vital role in establishing the correctness of the AKS Main Theorem in its full generality.

The formalisation of Lehmer's primality criterion by Wimmer and Noschinski [42] in Isabelle/HOL was based on ideals, ring homomorphisms, module and polynomials with coefficients from a ring. Their work included a proof that the multiplicative group of a finite field is cyclic (Theorem 20) from Euler's φ-function identity (Lemma 19).

A formal verification of the Miller–Rabin probabilistic primality test was carried out by Hurd [26] in HOL. The work relied on the group structure of modulo arithmetic, both addition and multiplication, in a prime modulus. Although there was no explicit mention of fields, the two groups are the main components of the finite field $\mathbb{Z}_p$ for prime p. A proof of the cyclic nature of the multiplicative group of $\mathbb{Z}_p$ (Theorem 20) was given.

In Coq, Théry and Hanrot delivered *Primality Proving with Elliptic Curves* at TPHOL 2007 [32]. They formalised elliptic curves defined over a field, and Théry [33] proved the group structure for "addition" of rational points on elliptic curves. The proof made use of basic properties polynomials with coefficients from a ring. Their subsequent work was based on the group law, and using prime certificates to derive a checker for elliptic curve certificates—a direction different from ours.

It is worth mentioning that Pepin's test for the primality of Fermat numbers was formalized by Fujisawa et al. [19] in Mizar. Their work was purely number-theoretic, but did involve the role of order (see Sect. 2.1) for the invertibles in $\mathbb{Z}_n$.

11 Conclusion

This work is a self-contained treatment of a fundamental result in the theory of finite fields carried out in the HOL4 theorem prover. The effort of formalization clarifies our understanding of the subject, and provides sufficient generality for use by other projects building on the theory of finite fields, e.g., our work on the AKS algorithm mentioned in Sect. 10.3.

Future Work By developing a theory of Frobenius automorphisms in finite fields, we hope to complete the formalisation of the Fundamental Theorem of Galois Theory.

Acknowledgements We would like to thank our anonymous referees for their very detailed and constructive feedback.

References

1. Aczel, P.: Galois: a theory development project. Department of Computer Science and Mathematics, Manchester University, U.K. http://www.cs.man.ac.uk/~petera/galois.ps.gz (1995)
2. Affeldt, R., Garrigue, J., Saikawa, T.: Formalization of Reed–Solomon codes and progress report on formalization of LDPC codes. In: The 2016 International Symposium on Information Theory and its Applications (ISITA 2016), pp. 532–536 (2016)
3. Arneson, B., Baaz, M., Rudnicki, P.: Witt's proof of the Wedderburn theorem. J. Formaliz. Math. **12**, 69–75 (2003)
4. Arneson, B., Rudnicki, P.: Primitive roots of unity and cyclotomic polynomials. J. Formaliz. Math **12**, 59–67 (2003)
5. Asperti, A., Armentano, C.: A page in number theory. J. Formaliz. Reason. **1**(1), 1–23 (2008)
6. Assia, M., Tassi, E.: The Mathematical Components library: principles and design choices. http://ssr.msr-inria.inria.fr/doc/tutorial-itp13/slides.pdf (2013)

7. Axler, S.: Linear Algebra Done Right. Undergraduate texts in mathematics. Springer, Berlin (2015). ISBN: 9783319307657
8. Bailey, A.: The machine-checked literate formalisation of algebra in type theory. PhD thesis, Department of Computer Science, University of Manchester (1998)
9. Barthe, G.: A formal proof of the unsolvability of the symmetric group over a set with five or more elements. Department of Computer Science, University of Nijmegen, the Netherlands. ftp://ftp.cs.ru.nl/pub/CompMath.Found/sn.ps.Z (1994)
10. Bartzia, E.-I., Strub, P.-Y.: A formal library for elliptic curves in the Coq proof assistant. In: Interactive Theorem Proving: 5th International Conference, ITP 2014, Held as Part of the Vienna Summer of Logic, VSL 2014, Vienna, Austria, July 14–17, 2014. Proceedings, ITP 2014, pp. 77–92. Springer, Cham (2014)
11. Bastida, J.R., Lyndon, R.: Field Extensions and Galois Theory. Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambridge (1984). ISBN: 9781107340749
12. Belk, J.: Classification of finite fields. Number Theory Course: Math 318, Bard College. http://faculty.bard.edu/belk/math318/ClassificationFiniteFieldsRevised.pdf (2016)
13. Chan, H.L., Norrish, M.: A string of pearls: proofs of Fermat's little theorem. J. Formaliz. Reason. **6**(1), 63–87 (2013)
14. Chan, H.L., Norrish, M.: Mechanisation of AKS Algorithm: Part 1—The Main Theorem. In: Urban, C., Zhang, X. (eds), Interactive Theorem Proving, ITP 2015, number 9236 in LNCS, pp. 117–136. Springer (2015)
15. Cohen, C.: Construction of Real Algebraic Numbers in Coq. In: Beringer, L., Felty, A. (eds) Interactive Theorem Proving, ITP 2012, number 7406 in LNCS, pp. 67–82. Springer (2012)
16. Curiel, N.: Formalizing Galois Theory: I automorphism groups of fields. Master's thesis, California State University San Marcos. http://csusm-dspace.calstate.edu/handle/10211.8/107 (2011)
17. Divasón, J., Joosten, S., Thiemann, R., Yamada, A.: A Formalization of the Berlekamp–Zassenhaus Factorization Algorithm. In: Proceedings of the 6th ACM SIGPLAN Conference on Certified Programs and Proofs, CPP 2017, pp. 17–29, New York, NY, USA. ACM (2017)
18. Ballarin, C., et al.: The Isabelle/HOL Algebra Library http://isabelle.in.tum.de/library/HOL/HOL-Algebra/index.html (2016)
19. Fujisawa, Y., Fuwa, Y., Shimizu, H.: Public-key cryptography and Pepin's test for the primality of fermat numbers. J. Formaliz. Math. http://mizar.org/JFM/Vol10/pepin.html (1998)
20. Futa, Yuichi, Okazaki, Hiroyuki, Shidama, Yasunari: Formalization of definitions and theorems related to an elliptic curve over a finite prime field by using Mizar. J. Automat. Reason. **50**(2), 161–172 (2013)
21. Gallian, J.A.: Contemporary Abstract Algebra. Brooks Cole, Boston (2006). ISBN: 9780618514717
22. Garrett, P.B.: The Mathematics of Coding Theory: Information, Compression, Error Correction, and Finite Fields. Pearson Prentice Hall, Upper Saddle River (2004). ISBN: 9780131019676
23. Gonthier, G., Asperti, A., Avigad, J., Bertot, Y., Cohen, C., Garillot, F., Le Roux, S., Mahboubi, A., O'Connor, R., Biha, S., Pasca, I., Rideau, L., Solovyev, A., Tassi, E., Théry, L.: A Machine-Checked Proof of the Odd Order Theorem, pp. 163–179. Springer, Berlin (2013)
24. Herstein, I.N.: Topics in Algebra. Wiley, New York (1975). ISBN: 9780471010906
25. Herstein, I.N.: Abstract Algebra. Wiley, New York (1996). ISBN: 9780471368793
26. Hurd, J.: Verification of the Miller–Rabin Probabilistic Primality Test. Elsevier Science Inc., New York. https://doi.org/10.1016/S1567-8326(02)00065-6 (2003)
27. Hurd, J., Gordon, M., Fox, A.: Formalized elliptic curve cryptography. High Confid. Softw. Syst. https://cps-vo.org/node/1542 (2006)
28. Ireland, K., Rosen, M.: A Classical Introduction to Modern Number Theory. Graduate Texts in Mathematics, vol. 84. Springer, New York (1990). ISBN: 9781441930941
29. Judson, T.W.: Abstract Algebra: Theory and Applications. The Prindle, Weber & Schmidt Series in Advanced Mathematics. PWS Publishing Company, Boston (1994)
30. Justesen, J., Høholdt, T.: A Course in Error-Correcting Codes. EMS Textbooks in Mathematics, 2nd edn. European Mathematical Society, New York (2004)
31. Kusak, E., Leonczuk, W., Muzalewski, M.: Abelian groups, fields and vector spaces. J. Formaliz. Math. http://www.mizar.org/JFM/Vol1/vectsp_1.html (1989)
32. Laurent, T., Hanrot, G.: Primality proving with elliptic curves. In: Schneider, K., Brandt, J. (eds), TPHOL 2007, volume 4732 of LNCS, pp. 319–333. Kaiserslautern, Germany: Springer (2007)
33. Laurent, T.: Proving the group law for elliptic curves formally. Technical Report RT-0330, INRIA https://hal.inria.fr/inria-00129237/en/ (2007)
34. Lidl, R., Niederreiter, H.: Introduction to Finite Fields and Their Applications, 2nd edn. Cambridge University Press, New York (1986)
35. Mizar Mathematical Library: http://www.mizar.org/library/ (2014)

36. Mathematical Components Team: Script finfield.v in field folder of The Mathematical Components library for Coq, March. https://github.com/math-comp/math-comp/blob/master/mathcomp/field/finfield.v (2015)
37. McEliece, R.J.: Finite Fields for Computer Scientists and Engineers. The Kluwer International Series in Engineering and Computer Science. Springer, New York (1987). ISBN: 9781461291855
38. Newman, S.C.: A Classical Introduction to Galois Theory. Wiley, New York (2012). ISBN: 9781118091395
39. Pretzel, O.: Error-Correcting Codes and Finite Fields. Applied Mathematics and Computing Science Series. Clarendon Press, Oxford (1996). ISBN 9780192690678
40. Robinson, D.J.S.: An Introduction to Abstract Algebra. De Gruyter Textbook. De Gruyter, Berlin (2008). ISBN: 9783110198164
41. Rotman, J.J.: Advanced Modern Algebra: Second Edition. Graduate Studies in Mathematics. American Mathematical Society, Providence (2010). ISBN: 9781470411763
42. Wimmer, L.N.S.: A Formalisation of Lehmer's primality criterion. Arch. Formal Proofs, Isabelle (2013)
43. Thiemann, R., Yamada, A.: Algebraic Numbers in Isabelle/HOL. In: Blanchette, J.C., Merz, S. (eds), Interactive Theorem Proving: 7th International Conference, ITP 2016, Nancy, France, August 22–25, 2016, Proceedings, pp. 391–408. Cham: Springer (2016)