The existence of finite fields, again

Darij Grinberg

March 5, 2021

Contents

1. Finite fields exist: the theorem

Fix a prime p. We are going to prove the following classical fact from abstract algebra:

Theorem 1.0.1. Let n be a positive integer. Then, there exists a finite field of size p^n.

Here, we are using standard notations from abstract algebra (see, e.g., [Grinbe19a]). In particular, fields are always commutative.

Theorem 1.0.1 is well-known; various proofs can be found in [LidNie97, Theorem 2.5], [Knapp16a, Theorem 9.14], [Loehr11, Exercise 12.126], [ConradF, Theorem 2.2], [Hunger14, Corollary 11.26], [Hunger03, Chapter V, Proposition 5.6], [Stewar15, Theorem 19.3], [Escofi01, 14.5.1], [ChaLoi21, Corollary (4.5.3)], [DumFoo04, §13.5, Example after Proposition 37], [HucNeu13, Theorem 6.5], [MonAno14], [Lange18, Theorem 32], [Murphy12, Chapter 10, Theorem 9] and [Walker87, Theorem 6.2.11]. Most of these proofs use either Galois theory or the Möbius function from number theory. In this note, we will give a proof that uses only relatively basic properties of rings and fields.

We first strengthen Theorem 1.0.1 a little bit, for the convenience of our proof.

We let $\mathbb{F}_p$ denote the ring of all residue classes of integers modulo p. This is also known as $\mathbb{Z}/p\mathbb{Z}$ (in most of the literature) or as $\mathbb{Z}/\left(p\right)$ or as $\mathbb{Z}/p$ (in [Grinbe19a]) or as $\mathbb{Z}_p$ (sometimes). It is well-known that $\mathbb{F}_p$ is a field[1] of size p.

Definition 1.0.2. An $\mathbb{F}_p$-*field* will mean an $\mathbb{F}_p$-algebra that is a field (with the same addition, multiplication, zero and unity).

It is not hard to see that an $\mathbb{F}_p$-field is the same as a field of characteristic p; but we will not need this in what follows.

Now, we can strengthen Theorem 1.0.1 as follows:

Theorem 1.0.3. Let n be a positive integer. Then, there exists a finite $\mathbb{F}_p$-field of size p^n.

Of course, Theorem 1.0.3 is not that much stronger than Theorem 1.0.1. In fact, any finite field of size p^n (for n a positive integer) is an $\mathbb{F}_p$-field; this can easily be seen using some linear algebra or group theory. But since Theorem 1.0.3 will fall into our hands in this exact form, we will have no need for such arguments.

2. Ingredients of the proof

Next we shall prepare for the proof of Theorem 1.0.3 by stating several results that will end up useful.

All polynomials that appear in this note are polynomials in a single variable x. If $\mathbb{K}$ is a commutative ring, and if $\mathbf{a} = \sum\limits_{k=0}^{n} a_k x^k \in \mathbb{K}\left[x\right]$ is a nonzero polynomial of degree $n \geq 0$ (with $a_k \in \mathbb{K}$), then:

- the *leading term* of $\mathbf{a}$ is defined to be the polynomial $a_n x^n \in \mathbb{K}\left[x\right]$;
- the *leading coefficient* of $\mathbf{a}$ is defined to be the element $a_n \in \mathbb{K}$;

[1] since p is a prime

- the polynomial $\mathbf{a}$ is said to be *monic* if $a_n = 1$ (that is, its leading coefficient is 1).

Note that the leading coefficient of $\mathbf{a}$ is therefore nonzero (since $\deg \mathbf{a} = n$ and thus $a_n \neq 0$).

We use the convention that the degree of the zero polynomial 0 is $\deg 0 = -\infty$.

2.1. Adjoining a root of a polynomial

We shall use quotients of commutative rings, but we will only need the simplest case of such quotients (namely, the case when we are quotienting by a principal ideal). Let us quickly introduce shorthand notations for this kind of quotients:

Convention 2.1.1. Let $\mathbb{K}$ be a commutative ring, and $a \in \mathbb{K}$ be any element.

For each $u \in \mathbb{K}$, we let $[u]_a$ denote the residue class of u modulo a. (This is commonly denoted by $u + a\mathbb{K}$.)

We let $\mathbb{K}/a$ denote the set of all residue classes of elements of $\mathbb{K}$ modulo a. (This is commonly denoted by $\mathbb{K}/a\mathbb{K}$ or by $\mathbb{K}/(a)$.) The set $\mathbb{K}/a$ is known to be a commutative $\mathbb{K}$-algebra (with addition defined by $[u]_a + [v]_a = [u+v]_a$, and all other operations defined similarly).

Thus, for example, $\mathbb{Z}/p$ is the field $\mathbb{F}_p$, and its elements are $[0]_p, [1]_p, \ldots, [p-1]_p$.

The following theorem is the only way by which we are going to extend our fields in this note:[2]

Theorem 2.1.2. Let $\mathbb{F}$ be a field. Let $n \in \mathbb{N}$. Let $\mathbf{a} \in \mathbb{F}[x]$ be a polynomial of degree n.

Consider the $\mathbb{F}$-algebra $\mathbb{F}[x]/\mathbf{a}$.

(a) Each element of $\mathbb{F}[x]/\mathbf{a}$ can be uniquely written in the form

$$\lambda_0 \left[x^0\right]_{\mathbf{a}} + \lambda_1 \left[x^1\right]_{\mathbf{a}} + \cdots + \lambda_{n-1} \left[x^{n-1}\right]_{\mathbf{a}} \qquad \text{with } \lambda_0, \lambda_1, \ldots, \lambda_{n-1} \in \mathbb{F}.$$

(b) If $\mathbb{F}$ is finite, then $|\mathbb{F}[x]/\mathbf{a}| = |\mathbb{F}|^n$.

(c) If the polynomial $\mathbf{a}$ is irreducible, then $\mathbb{F}[x]/\mathbf{a}$ is a field.

Proof of Theorem 2.1.2. **(a)** The polynomial $\mathbf{a}$ has degree n. Thus, the coefficient of x^n in $\mathbf{a}$ is nonzero, and therefore invertible (since every nonzero element of $\mathbb{F}$ is invertible[3]). Thus, the claim of Theorem 2.1.2 **(a)** follows from [Grinbe19a, Theorem 8.1.9 **(a)**] (applied to $\mathbb{F}$, n and $\mathbf{a}$ instead of $\mathbb{K}$, m and $\mathbf{b}$).

Alternatively, it is easy to derive Theorem 2.1.2 **(a)** from the familiar fact that division with remainder works for polynomials in $\mathbb{F}[x]$.

[2] We shall tend to denote polynomials with boldface letters, for the sake of readability.

[3] since $\mathbb{F}$ is a field

(b) Assume that $\mathbb{F}$ is finite. Then, Theorem 2.1.2 **(a)** shows that each element of $\mathbb{F}[x]/\mathbf{a}$ can be uniquely written in the form

$$\lambda_0 \left[x^0\right]_{\mathbf{a}} + \lambda_1 \left[x^1\right]_{\mathbf{a}} + \cdots + \lambda_{n-1} \left[x^{n-1}\right]_{\mathbf{a}} \qquad \text{with } \lambda_0, \lambda_1, \ldots, \lambda_{n-1} \in \mathbb{F}.$$

In other words, the map

$$\begin{aligned} \mathbb{F}^n &\to \mathbb{F}[x]/\mathbf{a}, \\ (\lambda_0, \lambda_1, \ldots, \lambda_{n-1}) &\mapsto \lambda_0 \left[x^0\right]_{\mathbf{a}} + \lambda_1 \left[x^1\right]_{\mathbf{a}} + \cdots + \lambda_{n-1} \left[x^{n-1}\right]_{\mathbf{a}} \end{aligned}$$

is a bijection. Hence, there exists a bijection from $\mathbb{F}^n$ to $\mathbb{F}[x]/\mathbf{a}$ (namely, this map). Thus, $|\mathbb{F}[x]/\mathbf{a}| = |\mathbb{F}^n| = |\mathbb{F}|^n$. This proves Theorem 2.1.2 **(b)**.

(c) Theorem 2.1.2 **(c)** follows from [Grinbe19a, Theorem 8.1.17] or from [Escofi01, 4.7.2] (applied to $K = \mathbb{F}$ and $P = \mathbf{a}$).

Alternatively, it can be found in the literature under some fairly transparent guises. For instance, several sources (e.g., [Stewar15, Theorem 17.2] or [Knapp16a, proof of Theorem 9.10] or [Milne18, 1.25]) prove Theorem 2.1.2 **(c)** in the case when the polynomial $\mathbf{a}$ is monic. But the general case can easily be reduced to this case (because we can always make a nonzero polynomial $\mathbf{a} \in \mathbb{F}[x]$ monic by scaling it with the multiplicative inverse of its leading coefficient). □

2.2. Factoring polynomials into irreducibles

How do we find irreducible polynomials to apply Theorem 2.1.2 **(c)** to? The following lemma shows a simple way:

Lemma 2.2.1. Let $\mathbb{F}$ be a field. Let $\mathbf{a} \in \mathbb{F}[x]$ be a non-constant polynomial. Then, there exists a monic irreducible polynomial $\mathbf{u}$ such that $\mathbf{u} \mid \mathbf{a}$.

Proof of Lemma 2.2.1. Clearly, there exists a non-constant polynomial $\mathbf{v} \in \mathbb{F}[x]$ that satisfies $\mathbf{v} \mid \mathbf{a}$ (for example, $\mathbf{a}$ itself is such a polynomial). Choose such a $\mathbf{v}$ of the smallest possible degree, and denote it by $\mathbf{b}$. Thus, $\mathbf{b}$ is a non-constant polynomial and satisfies $\mathbf{b} \mid \mathbf{a}$.

Let κ be the leading coefficient of $\mathbf{b}$ (that is, the coefficient of $x^{\deg \mathbf{b}}$ in $\mathbf{b}$). Then, κ is a nonzero element of $\mathbb{F}$, and thus is invertible (since every nonzero element of $\mathbb{F}$ is invertible[4]). Therefore, $\kappa^{-1} \in \mathbb{F}$ is well-defined and nonzero. Thus, if we regard κ^{-1} as a polynomial in $\mathbb{F}[x]$, then κ^{-1} is a nonzero constant; hence, $\deg\left(\kappa^{-1}\right) = 0$. Now,

$$\deg\left(\kappa^{-1}\mathbf{b}\right) = \underbrace{\deg\left(\kappa^{-1}\right)}_{=0} + \deg \mathbf{b} = \deg \mathbf{b} > 0$$

(since $\mathbf{b}$ is non-constant); thus, the polynomial $\kappa^{-1}\mathbf{b}$ is non-constant. Moreover, the polynomial $\kappa^{-1}\mathbf{b}$ satisfies $\kappa^{-1}\mathbf{b} \mid \mathbf{b}$ (since $\mathbf{b} = \underbrace{1}_{=\kappa\kappa^{-1}} \mathbf{b} = \kappa\kappa^{-1}\mathbf{b} = \left(\kappa^{-1}\mathbf{b}\right) \cdot \kappa$).

[4] because $\mathbb{F}$ is a field

It is easy to see that the polynomial $\kappa^{-1}\mathbf{b}$ is irreducible.

[*Proof:* Assume the contrary. Then, we can write $\kappa^{-1}\mathbf{b}$ as $\kappa^{-1}\mathbf{b} = \mathbf{cd}$ with two polynomials $\mathbf{c}, \mathbf{d} \in \mathbb{F}[x]$ satisfying $\deg \mathbf{c} > 0$ and $\deg \mathbf{d} > 0$ (since $\kappa^{-1}\mathbf{b}$ is non-constant but not irreducible). Consider these $\mathbf{c}$ and $\mathbf{d}$. The polynomial $\mathbf{c}$ is a non-constant polynomial[5] and satisfies $\mathbf{c} \mid \mathbf{a}$ (since $\mathbf{c} \mid \mathbf{cd} = \kappa^{-1}\mathbf{b} \mid \mathbf{b} \mid \mathbf{a}$). In other words, $\mathbf{c}$ is a non-constant polynomial $\mathbf{v} \in \mathbb{F}[x]$ that satisfies $\mathbf{v} \mid \mathbf{a}$. Therefore, $\deg \mathbf{c} \geq \deg \mathbf{b}$ (because we defined $\mathbf{b}$ to be such a $\mathbf{v}$ of the smallest possible degree). However, $\deg \underbrace{\left(\kappa^{-1}\mathbf{b}\right)}_{=\mathbf{cd}} = \deg(\mathbf{cd}) = \deg \mathbf{c} + \underbrace{\deg \mathbf{d}}_{>0} > \deg \mathbf{c}$ and thus $\deg \mathbf{c} < \deg\left(\kappa^{-1}\mathbf{b}\right) = \deg \mathbf{b}$. This contradicts $\deg \mathbf{c} \geq \deg \mathbf{b}$. This contradiction shows that our assumption was false. Hence, we have shown that $\kappa^{-1}\mathbf{b}$ is irreducible.]

The leading coefficient of the polynomial $\mathbf{b}$ is κ. Hence, the leading coefficient of the polynomial $\kappa^{-1}\mathbf{b}$ is $\kappa^{-1}\kappa = 1$. In other words, the polynomial $\kappa^{-1}\mathbf{b}$ is monic. It further satisfies $\kappa^{-1}\mathbf{b} \mid \mathbf{a}$ (since $\kappa^{-1}\mathbf{b} \mid \mathbf{b} \mid \mathbf{a}$). Hence, there exists a monic irreducible polynomial $\mathbf{u}$ such that $\mathbf{u} \mid \mathbf{a}$ (namely, $\mathbf{u} = \kappa^{-1}\mathbf{b}$). This proves Lemma 2.2.1. □

Corollary 2.2.2. Let $\mathbb{F}$ be a field. Let $\mathbf{a} \in \mathbb{F}[x]$ be a nonzero polynomial. Then, $\mathbf{a}$ can be written in the form $\mathbf{a} = \lambda \mathbf{u}_1 \mathbf{u}_2 \cdots \mathbf{u}_k$, where $\lambda \in \mathbb{F}$ is a nonzero constant, and where $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k \in \mathbb{F}[x]$ are monic irreducible polynomials.

Proof of Corollary 2.2.2 (sketched). This is an analogue of the fact that every nonzero integer is a product of finitely many primes (up to sign). The proof is analogous, too: Proceed by strong induction on $\deg \mathbf{a}$, using Lemma 2.2.1 in the induction step. □

Corollary 2.2.3. Let $\mathbb{F}$ be a field. Let $\mathbf{a} \in \mathbb{F}[x]$ be a monic polynomial. Then, $\mathbf{a}$ can be written in the form $\mathbf{a} = \mathbf{u}_1 \mathbf{u}_2 \cdots \mathbf{u}_k$, where $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k \in \mathbb{F}[x]$ are monic irreducible polynomials.

Proof of Corollary 2.2.3. The polynomial $\mathbf{a}$ is monic and thus nonzero. Hence, Corollary 2.2.2 shows that $\mathbf{a}$ can be written in the form $\mathbf{a} = \lambda \mathbf{u}_1 \mathbf{u}_2 \cdots \mathbf{u}_k$, where $\lambda \in \mathbb{F}$ is a nonzero constant, and where $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k \in \mathbb{F}[x]$ are monic irreducible polynomials. Consider this λ and these $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k$.

The polynomial $\mathbf{a}$ is monic, and thus has leading coefficient 1. The polynomial $\mathbf{u}_1 \mathbf{u}_2 \cdots \mathbf{u}_k$ is monic (since it is the product of the monic polynomials $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k$), and thus has leading coefficient 1. Hence, the polynomial $\lambda \mathbf{u}_1 \mathbf{u}_2 \cdots \mathbf{u}_k$ has leading coefficient λ (since λ is nonzero). Now, recall the equality $\mathbf{a} = \lambda \mathbf{u}_1 \mathbf{u}_2 \cdots \mathbf{u}_k$. Comparing the leading coefficients on both sides of this equality, we obtain $1 = \lambda$ (because the polynomial $\mathbf{a}$ has leading coefficient 1, while the polynomial $\lambda \mathbf{u}_1 \mathbf{u}_2 \cdots \mathbf{u}_k$ has leading coefficient λ). Hence, $\lambda = 1$. Thus,

$$\mathbf{a} = \underbrace{\lambda}_{=1} \mathbf{u}_1 \mathbf{u}_2 \cdots \mathbf{u}_k = \mathbf{u}_1 \mathbf{u}_2 \cdots \mathbf{u}_k.$$

[5] since $\deg \mathbf{c} > 0$

We thus have found monic irreducible polynomials $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k \in \mathbb{F}[x]$ such that $\mathbf{a} = \mathbf{u}_1 \mathbf{u}_2 \cdots \mathbf{u}_k$. In other words, we have written $\mathbf{a}$ in the form $\mathbf{a} = \mathbf{u}_1 \mathbf{u}_2 \cdots \mathbf{u}_k$, where $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k \in \mathbb{F}[x]$ are monic irreducible polynomials. Thus, $\mathbf{a}$ can be written in this form. This proves Corollary 2.2.3. □

2.3. A lemma on maps

We shall furthermore use the following simple lemma about maps on a set:

> **Lemma 2.3.1.** Let S be a set. Let $f : S \to S$ be a map. Let a and b be two positive integers such that $f^a = \operatorname{id}$ and $f^b = \operatorname{id}$. Then, $f^{\gcd(a,b)} = \operatorname{id}$.

Here, of course, f^n (where $n \in \mathbb{N}$) stands for the map $\underbrace{f \circ f \circ \cdots \circ f}_{n \text{ times}}$.

Lemma 2.3.1 is almost obvious if you know a bit of group theory (specifically, the notion of the order of an element in a group). But in order to keep this note self-contained, I shall give an elementary proof:

Proof of Lemma 2.3.1. We have $f^a = f \circ f^{a-1}$, so that $f \circ f^{a-1} = f^a = \operatorname{id}$. Also, $f^a = f^{a-1} \circ f$, so that $f^{a-1} \circ f = f^a = \operatorname{id}$. The equalities $f \circ f^{a-1} = \operatorname{id}$ and $f^{a-1} \circ f = \operatorname{id}$ show that the maps f and f^{a-1} are mutually inverse. Hence, the map f is invertible (with inverse f^{a-1}). Thus, the powers f^n of this map f are well-defined not only for $n \in \mathbb{N}$, but also for $n \in \mathbb{Z}$. Furthermore, it is well-known that these powers satisfy the following "laws of exponents":

- We have
$$f^{n+m} = f^n \circ f^m \qquad \text{for all } n, m \in \mathbb{Z}. \tag{1}$$
(This can be proven similarly to the proof of [Grinbe19a, Proposition 4.1.20 **(h)**].)

- We have
$$f^{nm} = (f^n)^m \qquad \text{for all } n, m \in \mathbb{Z}. \tag{2}$$
(This can be proven similarly to the proof of [Grinbe19a, Proposition 4.1.20 **(l)**].)

But Bezout's theorem (see, e.g., [Grinbe19a, Theorem 2.9.12]) shows that there exist integers $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ such that $\gcd(a, b) = xa + yb$. Consider these x

and y. From $\gcd(a,b) = xa + yb = ax + by$, we obtain

$$\begin{aligned} f^{\gcd(a,b)} = f^{ax+by} &\underset{\substack{\text{(by (1), applied to } n = ax \text{ and } m = by)}}{=} \underbrace{f^{ax}}_{\substack{=(f^a)^x \\ \text{(by (2),} \\ \text{applied to } n=a \text{ and } m=x)}} \circ \underbrace{f^{by}}_{\substack{=(f^b)^y \\ \text{(by (2),} \\ \text{applied to } n=b \text{ and } m=y)}} \\ &= \Bigg(\underbrace{f^a}_{=\mathrm{id}}\Bigg)^x \circ \Bigg(\underbrace{f^b}_{=\mathrm{id}}\Bigg)^y = \underbrace{\mathrm{id}^x}_{=\mathrm{id}} \circ \underbrace{\mathrm{id}^y}_{=\mathrm{id}} = \mathrm{id} \circ \mathrm{id} = \mathrm{id}\,. \end{aligned}$$

This proves Lemma 2.3.1. □

2.4. Restriction of modules and algebras

In linear algebra, you may have learned that each $\mathbb{C}$-vector space V is (or, more precisely, becomes in a natural way) an $\mathbb{R}$-vector space: Just restrict its scaling map $\cdot : \mathbb{C} \times V \to V$ to $\mathbb{R} \times V$, and you obtain a scaling map $\cdot : \mathbb{R} \times V \to V$ that makes it into an $\mathbb{R}$-vector space. (However, the dimension of this $\mathbb{R}$-vector space V will be **double** the dimension of the original $\mathbb{C}$-vector space V.)

The simple reason why this works is that $\mathbb{R}$ is a subring of $\mathbb{C}$. More generally, if $\mathbb{K}$ is a subring of a commutative ring $\mathbb{L}$, then any $\mathbb{L}$-module V becomes a $\mathbb{K}$-module in the same way (i.e., by restricting the scaling map to $\mathbb{K} \times V$).

With a little tweak, the same construction works even more generally: We don't need $\mathbb{K}$ to be a subring of $\mathbb{L}$; we only need $\mathbb{L}$ to be a commutative $\mathbb{K}$-algebra[6]. The thing we need to do in order to turn an $\mathbb{L}$-module V into a $\mathbb{K}$-module is no longer literally restricting the scaling map $\cdot : \mathbb{L} \times V \to V$ to $\mathbb{K} \times V$, but rather a simple tweak:

Proposition 2.4.1. Let $\mathbb{K}$ be a commutative ring. Let $\mathbb{L}$ be a commutative $\mathbb{K}$-algebra. Let V be an $\mathbb{L}$-module. Consider its addition $+$, its scaling $\cdot : \mathbb{L} \times V \to V$ and its zero vector 0_V.

Define a scaling $\cdot : \mathbb{K} \times V \to V$ by setting

$$\lambda \cdot v = (\lambda \cdot 1_{\mathbb{L}}) \cdot v \qquad \text{for all } \lambda \in \mathbb{K} \text{ and } v \in V. \tag{3}$$

Here:

- the "$\cdot$" on the left hand side means the scaling $\cdot : \mathbb{K} \times V \to V$ that we are defining (written infix);
- the first "$\cdot$" on the right hand side means the scaling $\cdot : \mathbb{K} \times \mathbb{L} \to \mathbb{L}$ of the $\mathbb{K}$-algebra $\mathbb{L}$ (since $\mathbb{L}$ is a $\mathbb{K}$-algebra and thus is a $\mathbb{K}$-module, which means that it has a scaling);

[6] This case is indeed more general, because if $\mathbb{K}$ is a subring of a commutative ring $\mathbb{L}$, then $\mathbb{L}$ is clearly a commutative $\mathbb{K}$-algebra.

- the second "$\cdot$" on the right hand side means the scaling $\cdot : \mathbb{L} \times V \to V$ of the $\mathbb{L}$-module V.

Then, the set V (equipped with its addition $+$, its zero vector 0_V and the scaling $\cdot : \mathbb{K} \times V \to V$ we just defined) is a $\mathbb{K}$-module.

Roughly speaking, the definition of the scaling $\cdot : \mathbb{K} \times V \to V$ in Proposition 2.4.1 can be restated as follows: In order to scale an element $v \in V$ by an element $\lambda \in \mathbb{K}$, we first scale $1_{\mathbb{L}}$ by λ, thus obtaining some sort of "proxy element" for λ in $\mathbb{L}$, and then we scale v by this "proxy element" (which we know how to do, because V is an $\mathbb{L}$-module).

We shall prove Proposition 2.4.1 in the Appendix (Section 4.1).

Next, let us state an analogue of Proposition 2.4.1 for algebras instead of modules:

Proposition 2.4.2. Let $\mathbb{K}$ be a commutative ring. Let $\mathbb{L}$ be a commutative $\mathbb{K}$-algebra. Let V be an $\mathbb{L}$-algebra. Thus, V is a ring and an $\mathbb{L}$-module at the same time. Consider its addition $+$, its multiplication $\cdot$, its scaling $\cdot$, its zero 0_V and its unity 1_V.

Define a scaling $\cdot : \mathbb{K} \times V \to V$ as in Proposition 2.4.1.

Then, the set V (equipped with its addition $+$, its multiplication $\cdot$, its zero 0_V, its unity 1_V, and the scaling $\cdot : \mathbb{K} \times V \to V$ we just defined) is a $\mathbb{K}$-algebra.

Again, we refer to the Appendix (Section 4.1) for a proof of Proposition 2.4.2.

We can shorten Proposition 2.4.2 significantly if we omit the precise definition of the scaling $\cdot : \mathbb{K} \times V \to V$ and simply claim that such a scaling can be defined:

Proposition 2.4.3. Let $\mathbb{K}$ be a commutative ring. Let $\mathbb{L}$ be a commutative $\mathbb{K}$-algebra. Let V be an $\mathbb{L}$-algebra. Then, V becomes a $\mathbb{K}$-algebra in a natural way.

Here, "in a natural way" means "by equipping it with a scaling map $\cdot : \mathbb{K} \times V \to V$ that is defined uniquely in terms of the existing structures" (specifically, in terms of the unity $1_{\mathbb{L}}$ of $\mathbb{L}$ and the scaling maps of the $\mathbb{K}$-algebra $\mathbb{L}$ and of the $\mathbb{L}$-algebra V).

Proof of Proposition 2.4.3. Define a scaling $\cdot : \mathbb{K} \times V \to V$ as in Proposition 2.4.2. Then, Proposition 2.4.2 shows that the set V (equipped with its addition $+$, its multiplication $\cdot$, its zero 0_V, its unity 1_V, and the scaling $\cdot : \mathbb{K} \times V \to V$ we just defined) is a $\mathbb{K}$-algebra. Thus, V becomes a $\mathbb{K}$-algebra in a natural way. This proves Proposition 2.4.3. □

2.5. Fermat's little theorem for finite fields

Fermat's little theorem, in one of its forms (e.g., [Grinbe19a, Theorem 2.15.2 **(b)**]), says that $a^p \equiv a \bmod p$ for every integer a. We can transform this congruence into an equality in $\mathbb{F}_p$; then, it becomes the statement that $\alpha^p = \alpha$ for each $\alpha \in \mathbb{F}_p$. This can be generalized to finite fields other than $\mathbb{F}_p$; namely, we have the following:

Theorem 2.5.1. Let $\mathbb{F}$ be a finite field. Then, $\alpha^{|\mathbb{F}|} = \alpha$ for each $\alpha \in \mathbb{F}$.

The following proof of Theorem 2.5.1 uses the same idea as [Grinbe19a, proof of Theorem 2.15.3] (one of the standard proofs of Euler's theorem):

Proof of Theorem 2.5.1. We know that $\mathbb{F}$ is a field. In other words, $\mathbb{F}$ is a commutative skew field.

The field $\mathbb{F}$ contains at least 1 element (since it contains $0_{\mathbb{F}}$). Thus, $|\mathbb{F}| \geq 1$, so that $0^{|\mathbb{F}|} = 0$. (Here and throughout this proof, "0" means the zero of $\mathbb{F}$.)

We know that $\mathbb{F}$ is a skew field. Thus, every nonzero element of $\mathbb{F}$ is invertible, and we have $1 \neq 0$ in $\mathbb{F}$.

It is well-known that the product of any two invertible elements of $\mathbb{F}$ is invertible[7]. Thus, by induction, it is easy to see that any product of finitely many invertible elements of $\mathbb{F}$ is invertible[8].

Each $\beta \in \mathbb{F} \setminus \{0\}$ is nonzero[9] and thus invertible (since every nonzero element of $\mathbb{F}$ is invertible). Hence, $\prod\limits_{\beta \in \mathbb{F} \setminus \{0\}} \beta$ is a product of finitely many invertible elements of $\mathbb{F}$, and thus is invertible (since any product of finitely many invertible elements of $\mathbb{F}$ is invertible).

Fix $\alpha \in \mathbb{F}$. We must prove that $\alpha^{|\mathbb{F}|} = \alpha$. If $\alpha = 0$, then this is true (since $0^{|\mathbb{F}|} = 0$). Hence, we WLOG assume that $\alpha \neq 0$ for the rest of this proof. Thus, the element α of $\mathbb{F}$ is nonzero, and thus is invertible (since every nonzero element of $\mathbb{F}$ is invertible). Hence, its multiplicative inverse α^{-1} is well-defined. Moreover, $\alpha^{-1} \neq 0$ [10].

Now, each $\beta \in \mathbb{F} \setminus \{0\}$ satisfies $\alpha\beta \in \mathbb{F} \setminus \{0\}$ [11]. The same argument (applied

[7] *Proof.* Let α and β be two invertible elements of $\mathbb{F}$. We must prove that $\alpha\beta$ is invertible.

The multiplicative inverses α^{-1} and β^{-1} of α and β are well-defined (since α and β are invertible). Now, the two elements $\beta^{-1}\alpha^{-1}$ and $\alpha\beta$ of $\mathbb{F}$ satisfy

$$\left(\beta^{-1}\alpha^{-1}\right) \cdot (\alpha\beta) = \beta^{-1} \underbrace{\alpha^{-1}\alpha}_{=1} \beta = \beta^{-1}1\beta = \beta^{-1}\beta = 1 \qquad \text{and}$$
$$(\alpha\beta) \cdot \left(\beta^{-1}\alpha^{-1}\right) = \alpha \underbrace{\beta\beta^{-1}}_{=1} \alpha^{-1} = \alpha 1 \alpha^{-1} = \alpha\alpha^{-1} = 1.$$

In other words, $\beta^{-1}\alpha^{-1}$ is a multiplicative inverse of $\alpha\beta$. Thus, $\alpha\beta$ has a multiplicative inverse. In other words, $\alpha\beta$ is invertible, qed.

[8] The induction base hinges on the fact that $1 \in \mathbb{F}$ is invertible (since the empty product equals 1).

[9] since $\beta \in \mathbb{F} \setminus \{0\}$ and thus $\beta \neq 0$

[10] because otherwise, we would have $\alpha^{-1} = 0$, and thus $1 = \alpha \underbrace{\alpha^{-1}}_{=0} = \alpha 0 = 0$, which would contradict the fact that $1 \neq 0$ in $\mathbb{F}$

[11] *Proof.* Let $\beta \in \mathbb{F} \setminus \{0\}$. We must prove that $\alpha\beta \in \mathbb{F} \setminus \{0\}$. In other words, we must prove that $\alpha\beta \neq 0$ (since $\alpha\beta$ is clearly an element of $\mathbb{F}$).

to α^{-1} instead of α) shows that each $\beta \in \mathbb{F} \setminus \{0\}$ satisfies $\alpha^{-1}\beta \in \mathbb{F} \setminus \{0\}$ (since $\alpha^{-1} \neq 0$).

Consider the map

$$X : \mathbb{F} \setminus \{0\} \to \mathbb{F} \setminus \{0\}, \\ \beta \mapsto \alpha\beta$$

(this is well-defined, because each $\beta \in \mathbb{F} \setminus \{0\}$ satisfies $\alpha\beta \in \mathbb{F} \setminus \{0\}$) and the map

$$Y : \mathbb{F} \setminus \{0\} \to \mathbb{F} \setminus \{0\}, \\ \beta \mapsto \alpha^{-1}\beta$$

(this is well-defined, because each $\beta \in \mathbb{F} \setminus \{0\}$ satisfies $\alpha^{-1}\beta \in \mathbb{F} \setminus \{0\}$).

It is easy to see that these maps X and Y are mutually inverse[12]. Thus, the map $X : \mathbb{F} \setminus \{0\} \to \mathbb{F} \setminus \{0\}$ is invertible, i.e., is bijection. Hence, we can substitute $X(\beta)$ for β in the product $\prod\limits_{\beta \in \mathbb{F} \setminus \{0\}} \beta$. We thus find

$$\prod_{\beta \in \mathbb{F} \setminus \{0\}} \beta = \prod_{\beta \in \mathbb{F} \setminus \{0\}} \underbrace{X(\beta)}_{\substack{=\alpha\beta \\ \text{(by the definition} \\ \text{of } X)}} = \prod_{\beta \in \mathbb{F} \setminus \{0\}} (\alpha\beta) = \alpha^{|\mathbb{F} \setminus \{0\}|} \prod_{\beta \in \mathbb{F} \setminus \{0\}} \beta$$

(since $\mathbb{F}$ is commutative). We can divide both sides of this equality by $\prod\limits_{\beta \in \mathbb{F} \setminus \{0\}} \beta$ (since $\prod\limits_{\beta \in \mathbb{F} \setminus \{0\}} \beta$ is invertible). Thus we obtain

$$1 = \alpha^{|\mathbb{F} \setminus \{0\}|} = \alpha^{|\mathbb{F}|-1} \qquad (\text{since } |\mathbb{F} \setminus \{0\}| = |\mathbb{F}| - 1).$$

Multiplying both sides of this equality by α, we find $\alpha = \alpha^{|\mathbb{F}|-1}\alpha = \alpha^{|\mathbb{F}|}$. In other words, $\alpha^{|\mathbb{F}|} = \alpha$. This proves Theorem 2.5.1. □

Assume the contrary. Thus, $\alpha\beta = 0$. Hence, $\alpha^{-1} \underbrace{\alpha\beta}_{=0} = \alpha^{-1}0 = 0$, so that $0 = \underbrace{\alpha^{-1}\alpha}_{=1} \beta = \beta \in \mathbb{F} \setminus \{0\}$. But this entails $0 \notin \{0\}$, which is absurd. Hence, we have obtained a contradiction. This contradiction shows that our assumption was wrong. Thus, we have shown that $\alpha\beta \neq 0$. Hence, $\alpha\beta \in \mathbb{F} \setminus \{0\}$, qed.

[12] For example, $X \circ Y = \mathrm{id}$ follows from the following computation: For each $\beta \in \mathbb{F} \setminus \{0\}$, we have

$$\begin{aligned} (X \circ Y)(\beta) &= X(Y(\beta)) = \alpha \cdot \underbrace{Y(\beta)}_{\substack{=\alpha^{-1}\beta \\ \text{(by the definition} \\ \text{of } Y)}} \qquad \text{(by the definition of } X) \\ &= \underbrace{\alpha \cdot \alpha^{-1}}_{=1} \beta = 1\beta = \beta = \mathrm{id}(\beta). \end{aligned}$$

2.6. Frobenius endomorphisms

We now introduce a very special map defined on any commutative $\mathbb{F}_p$-algebra:

Definition 2.6.1. Let $\mathbb{K}$ be a commutative $\mathbb{F}_p$-algebra. The map

$$\mathbb{K} \to \mathbb{K}, \qquad a \mapsto a^p$$

will be called the *Frobenius endomorphism* of $\mathbb{K}$ and will be denoted by $F_{\mathbb{K}}$.

For example, the Frobenius endomorphism of $\mathbb{F}_p$ is the identity map (since every $a \in \mathbb{F}_p$ satisfies $a^p = a$; this is a consequence of Fermat's Little Theorem). But $\mathbb{F}_p$-algebras can be larger than $\mathbb{F}_p$, and usually their Frobenius endomorphisms will not be the identity map.

The word "endomorphism" means "homomorphism from an object (in this case, an $\mathbb{F}_p$-algebra) to itself". Thus, the name "Frobenius endomorphism" suggests that $F_{\mathbb{K}}$ is an $\mathbb{F}_p$-algebra homomorphism from $\mathbb{K}$ to $\mathbb{K}$. And this is indeed the case:

Theorem 2.6.2. Let $\mathbb{K}$ be a commutative $\mathbb{F}_p$-algebra. Then, its Frobenius endomorphism $F_{\mathbb{K}}$ is an $\mathbb{F}_p$-algebra homomorphism.

Before we prove this, let us show a simple proposition that will come useful here and later on as well:

Proposition 2.6.3. Let $\mathbb{K}$ be an $\mathbb{F}_p$-algebra.
(a) We have $pa = 0$ for each $a \in \mathbb{K}$.
(b) Assume that $\mathbb{K}$ is commutative. Then, $p\mathbf{a} = 0$ for each $\mathbf{a} \in \mathbb{K}[x]$.

Proof of Proposition 2.6.3. **(a)** Let $a \in \mathbb{K}$. Recall that $\mathbb{K}$ is an $\mathbb{F}_p$-algebra and thus satisfies the module axioms; hence, $1_{\mathbb{F}_p}a = a$ and $0_{\mathbb{F}_p}a = 0$.

The definition of $\mathbb{F}_p$ readily yields $p \cdot 1_{\mathbb{F}_p} = 0_{\mathbb{F}_p}$ [13]. Now, using $1_{\mathbb{F}_p}a = a$, we find

$$p \underbrace{a}_{=1_{\mathbb{F}_p}a} = \underbrace{p \cdot 1_{\mathbb{F}_p}}_{=0_{\mathbb{F}_p}} a = 0_{\mathbb{F}_p}a = 0.$$

This proves Proposition 2.6.3 **(a)**.

(b) There are two ways of proving this. One is the "right" way (in a philosophical sense), while another is the short way.

[13] *Proof.* Recall that $\mathbb{F}_p = \mathbb{Z}/p$ (where we are using the notations from Convention 2.1.1). Thus, the elements of $\mathbb{F}_p$ are residue classes $[u]_p$ of integers u modulo p. In particular, $1_{\mathbb{F}_p} = [1]_p$. Thus,

$$p \cdot \underbrace{1_{\mathbb{F}_p}}_{=[1]_p} = p \cdot [1]_p = [p \cdot 1]_p = [0]_p \qquad (\text{since } p \cdot 1 = p \equiv 0 \bmod p)$$
$$= 0_{\mathbb{F}_p},$$

qed.

Here is the "right" way: We know that $\mathbb{K}$ is a commutative $\mathbb{F}_p$-algebra, and we know that $\mathbb{K}[x]$ is a $\mathbb{K}$-algebra. Hence, Proposition 2.4.3 (applied to $\mathbb{F}_p$, $\mathbb{K}$ and $\mathbb{K}[x]$ instead of $\mathbb{K}$, $\mathbb{L}$ and V) shows that $\mathbb{K}[x]$ becomes an $\mathbb{F}_p$-algebra in a natural way. Thus, Proposition 2.6.3 **(a)** (applied to $\mathbb{K}[x]$ and $\mathbf{a}$ instead of $\mathbb{K}$ and a) shows that $p\mathbf{a} = 0$ for each $\mathbf{a} \in \mathbb{K}[x]$. This proves Proposition 2.6.3 **(b)**.

Here is the short way: Let $\mathbf{a} \in \mathbb{K}[x]$. Write the polynomial $\mathbf{a}$ in the form $\mathbf{a} = \sum\limits_{i=0}^{n} a_i x^i$ with $n \in \mathbb{N}$ and $a_0, a_1, \ldots, a_n \in \mathbb{K}$. Then,

$$p \underbrace{\mathbf{a}}_{= \sum\limits_{i=0}^{n} a_i x^i} = p \sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{n} \underbrace{pa_i}_{\substack{=0 \\ \text{(by Proposition 2.6.3 (a),} \\ \text{applied to } a = a_i)}} x^i = \sum_{i=0}^{n} 0x^i = 0.$$

This proves Proposition 2.6.3 **(b)** again. □

Proof of Theorem 2.6.2. Proposition 2.6.3 **(a)** (applied to $a = 1_{\mathbb{K}}$) yields $p \cdot 1_{\mathbb{K}} = 0$. Hence, $\mathbb{K}$ is a commutative ring such that $p \cdot 1_{\mathbb{K}} = 0$. Also, $F_{\mathbb{K}}$ is the map

$$\mathbb{K} \to \mathbb{K}, \qquad a \mapsto a^p.$$

Hence, [Grinbe19a, Corollary 5.11.3] (applied to $F = F_{\mathbb{K}}$) shows that $F_{\mathbb{K}}$ is a ring homomorphism.[14] Hence, $F_{\mathbb{K}}$ sends 0 to 0 and respects addition. Furthermore, we have $F_{\mathbb{K}}(\lambda a) = \lambda F_{\mathbb{K}}(a)$ for each $\lambda \in \mathbb{F}_p$ and $a \in \mathbb{K}$ [15]. Thus, $F_{\mathbb{K}}$ respects scaling (where we consider $\mathbb{K}$ as an $\mathbb{F}_p$-module). Hence, the map $F_{\mathbb{K}}$ is an $\mathbb{F}_p$-module homomorphism (since it sends 0 to 0 and respects addition and respects scaling). Thus, this map $F_{\mathbb{K}}$ is an $\mathbb{F}_p$-algebra homomorphism (since it is a ring homomorphism and an $\mathbb{F}_p$-module homomorphism). This proves Theorem 2.6.2. □

[14] Don't be fooled by the reference to [Grinbe19a]; this is not a difficult result. Here is an outline of the proof: It clearly suffices to show that $F_{\mathbb{K}}(0) = 0$ and $F_{\mathbb{K}}(1) = 1$ and $F_{\mathbb{K}}(a+b) = F_{\mathbb{K}}(a) + F_{\mathbb{K}}(b)$ and $F_{\mathbb{K}}(ab) = F_{\mathbb{K}}(a) \cdot F_{\mathbb{K}}(b)$ for all $a, b \in \mathbb{K}$. In other words, it suffices to show that $0^p = 0$ and $1^p = 1$ and $(a+b)^p = a^p + b^p$ and $(ab)^p = a^p b^p$ for all $a, b \in \mathbb{K}$ (because $F_{\mathbb{K}}(u) = u^p$ for each $u \in \mathbb{K}$). But the first two of these four equalities are obvious, whereas the fourth one follows from the commutativity of $\mathbb{K}$. It thus remains to prove the third equality, i.e., to prove that $(a+b)^p = a^p + b^p$ for all $a, b \in \mathbb{K}$. But this is the famous "Freshman's Dream", and can be shown by expanding $(a+b)^p$ using the binomial theorem and recalling that all binomial coefficients $\dbinom{p}{k}$ for $k \in \{1, 2, \ldots, p-1\}$ are divisible by p (which means that they vanish when they are used to scale elements of $\mathbb{K}$, by Proposition 2.6.3 **(a)**). Thus, all four equalities are proven, so that $F_{\mathbb{K}}$ is a ring homomorphism.

[15] *Proof.* Let $\lambda \in \mathbb{F}_p$ and $a \in \mathbb{K}$. Then, Theorem 2.5.1 (applied to $\mathbb{F} = \mathbb{F}_p$ and $\alpha = \lambda$) yields $\lambda^{|\mathbb{F}_p|} = \lambda$. In view of $|\mathbb{F}_p| = p$, this rewrites as $\lambda^p = \lambda$. But the definition of $F_{\mathbb{K}}$ yields $F_{\mathbb{K}}(a) = a^p$ and $F_{\mathbb{K}}(\lambda a) = (\lambda a)^p = \lambda^p a^p$ (by [Grinbe19a, Proposition 6.9.7 **(b)**], applied to $\mathbb{F}_p$, $\mathbb{K}$ and p instead of $\mathbb{K}$, A and k). Hence, $F_{\mathbb{K}}(\lambda a) = \underbrace{\lambda^p}_{=\lambda} \underbrace{a^p}_{=F_{\mathbb{K}}(a)} = \lambda F_{\mathbb{K}}(a)$, qed.

Professional algebraists occasionally get really lazy and shorten "the Frobenius endomorphism" to "the Frobenius".

The following property of the Frobenius endomorphism is an easy induction exercise:

Proposition 2.6.4. Let $\mathbb{K}$ be a commutative $\mathbb{F}_p$-algebra. Let $a \in \mathbb{K}$. Let F be the map $F_{\mathbb{K}} : \mathbb{K} \to \mathbb{K}$. Then,

$$F^i(a) = a^{p^i} \qquad \text{for all } i \in \mathbb{N}. \tag{4}$$

Proof of Proposition 2.6.4. We know that F is the map $F_{\mathbb{K}}$. Thus, for each $u \in \mathbb{K}$, we have

$$F(u) = F_{\mathbb{K}}(u) = u^p \tag{5}$$

(by the definition of $F_{\mathbb{K}}$).

We shall prove (4) by induction on i:

Induction base: Comparing $\underbrace{F^0}_{=\operatorname{id}}(a) = \operatorname{id}(a) = a$ with $a^{p^0} = a^1 = a$, we obtain $F^0(a) = a^{p^0}$. In other words, (4) holds for $i = 0$. This completes the induction base.

Induction step: Fix $j \in \mathbb{N}$. Assume that (4) holds for $i = j$. We must prove that (4) holds for $i = j + 1$.

We have assumed that (4) holds for $i = j$. In other words, we have $F^j(a) = a^{p^j}$. Now,

$$\begin{aligned}
\underbrace{F^{j+1}}_{=F\circ F^j}(a) &= \left(F \circ F^j\right)(a) = F\left(\underbrace{F^j(a)}_{=a^{p^j}}\right) = F\left(a^{p^j}\right) \\
&= \left(a^{p^j}\right)^p \qquad \left(\text{by (5), applied to } u = a^{p^j}\right) \\
&= a^{p^j p} = a^{p^{j+1}} \qquad \left(\text{since } p^j p = p^{j+1}\right).
\end{aligned}$$

In other words, (4) holds for $i = j + 1$. This completes the induction step. Hence, (4) is proven.

Thus, the proof of Proposition 2.6.4 is done. □

Combining Proposition 2.6.4 with Theorem 2.5.1, we obtain the following:

Corollary 2.6.5. Let $n \in \mathbb{N}$. Let $\mathbb{F}$ be a finite $\mathbb{F}_p$-field of size p^n. Let F be the map $F_{\mathbb{F}} : \mathbb{F} \to \mathbb{F}$. Then, $F^n = \operatorname{id}$.

Proof of Corollary 2.6.5. We have $|\mathbb{F}| = p^n$ (since $\mathbb{F}$ has size p^n). Moreover, $\mathbb{F}$ is an $\mathbb{F}_p$-field; in other words, $\mathbb{F}$ is an $\mathbb{F}_p$-algebra that is a field. Hence, $\mathbb{F}$ is commutative (since $\mathbb{F}$ is a field).

Let $a \in \mathbb{F}$. Then, Theorem 2.5.1 (applied to $\alpha = a$) yields $a^{|\mathbb{F}|} = a$. In view of $|\mathbb{F}| = p^n$, this rewrites as $a^{p^n} = a$. But Proposition 2.6.4 (applied to $\mathbb{K} = \mathbb{F}$ and $i = n$) yields $F^n(a) = a^{p^n} = a = \operatorname{id}(a)$.

Forget that we fixed a. We thus have shown that $F^n(a) = \operatorname{id}(a)$ for each $a \in \mathbb{F}$. In other words, $F^n = \operatorname{id}$. This proves Corollary 2.6.5. □

> **Corollary 2.6.6.** Let n be a positive integer. Let $\mathbb{F}$ be a finite $\mathbb{F}_p$-field of size p^n. Let $a \in \mathbb{F}$ and $r \in \mathbb{N}$. Then, $a^{p^{nr}} = a$.

Proof of Corollary 2.6.6. We know that $\mathbb{F}$ is an $\mathbb{F}_p$-field; in other words, $\mathbb{F}$ is an $\mathbb{F}_p$-algebra that is a field. Hence, $\mathbb{F}$ is commutative (since $\mathbb{F}$ is a field).

Let F be the map $F_{\mathbb{F}} : \mathbb{F} \to \mathbb{F}$. Then, Corollary 2.6.5 yields $F^n = \operatorname{id}$. Now, $F^{nr} = \left(\underbrace{F^n}_{=\operatorname{id}}\right)^r = \operatorname{id}^r = \operatorname{id}$. But Proposition 2.6.4 (applied to $\mathbb{K} = \mathbb{F}$ and $i = nr$) yields $F^{nr}(a) = a^{p^{nr}}$. Hence, $a^{p^{nr}} = \underbrace{F^{nr}}_{=\operatorname{id}}(a) = \operatorname{id}(a) = a$. This proves Corollary 2.6.6. □

2.7. Polynomials over fields have only so many roots

Our next ingredient is a basic property of polynomials over fields. First we define a slightly nonstandard notation:

> **Convention 2.7.1.** Let $\mathbb{K}$ be a commutative ring. Let $\mathbf{f} \in \mathbb{K}[x]$ be a polynomial. Let U be a $\mathbb{K}$-algebra. Let $u \in U$. Then, $\mathbf{f}[u]$ will denote the value of the polynomial $\mathbf{f}$ at u. (See [Grinbe19a, Definition 7.6.1] for the definition of this value. Roughly speaking, this value is obtained by substituting u for x in $\mathbf{f}$.)

I am using this notation $\mathbf{f}[u]$ in lieu of the more usual notation $\mathbf{f}(u)$, since the latter can too easily be mistaken for a product.

> **Theorem 2.7.2.** Let $\mathbb{K}$ be a field. Let $n \in \mathbb{N}$. Then, any nonzero polynomial $\mathbf{a} \in \mathbb{K}[x]$ of degree $\leq n$ has at most n roots in $\mathbb{K}$. (We are not counting the roots with multiplicity here.)

Proof of Theorem 2.7.2. This is [Grinbe19a, Theorem 7.6.11]. □

For us, the use of Theorem 2.7.2 is through the following corollary:

> **Corollary 2.7.3.** Let u be an integer such that $u > 1$. Let $\mathbb{F}$ be a field. Assume that all $a \in \mathbb{F}$ satisfy $a^u = a$. Then, $|\mathbb{F}| \leq u$. (This means, in particular, that the field $\mathbb{F}$ is finite.)

Proof of Corollary 2.7.3. Define a polynomial $\mathbf{a} \in \mathbb{F}[x]$ by $\mathbf{a} = x^u - x$. Then, the leading term of $\mathbf{a}$ is x^u (since $u > 1$). Thus, the polynomial $\mathbf{a}$ is monic of degree u; hence, $\mathbf{a}$ is nonzero. Hence, Theorem 2.7.2 (applied to $\mathbb{K} = \mathbb{F}$ and $n = u$) shows that the polynomial $\mathbf{a}$ has at most u roots in $\mathbb{F}$ (since $\mathbf{a}$ has degree u and thus has degree $\leq u$). In other words, the number of roots of $\mathbf{a}$ in $\mathbb{F}$ is $\leq u$. In other words, $|\{\text{roots of } \mathbf{a} \text{ in } \mathbb{F}\}| \leq u$.

But $\mathbb{F} \subseteq \{\text{roots of } \mathbf{a} \text{ in } \mathbb{F}\}$ [16]. Hence, $|\mathbb{F}| \leq |\{\text{roots of } \mathbf{a} \text{ in } \mathbb{F}\}| \leq u$. This proves Corollary 2.7.3. □

2.8. Factorization into distinct factors and derivatives

Another piece of our puzzle is the notion of the derivative of a polynomial. We recall its definition:

Definition 2.8.1. Let $\mathbb{K}$ be a commutative ring.

(a) For each polynomial

$$\mathbf{f} = \sum_{k \in \mathbb{N}} a_k x^k = a_0 x^0 + a_1 x^1 + a_2 x^2 + \cdots \in \mathbb{K}[x] \qquad (\text{where } a_i \in \mathbb{K}),$$

we define the *derivative* $\mathbf{f}'$ of $\mathbf{f}$ to be the polynomial

$$\sum_{k>0} k a_k x^{k-1} = 1a_1 x^0 + 2a_2 x^1 + 3a_3 x^2 + \cdots \in \mathbb{K}[x].$$

(b) Let $D : \mathbb{K}[x] \to \mathbb{K}[x]$ be the map sending each polynomial $\mathbf{f}$ to its derivative $\mathbf{f}'$.

Definition 2.8.1 **(a)** is a particular case of the definition of $\mathbf{f}'$ in [Grinbe19b, Exercise 5][17]; more precisely, the latter definition defines $\mathbf{f}'$ for every formal power series $\mathbf{f}$, whereas here we restrict ourselves to the case when $\mathbf{f}$ is a polynomial. It is almost obvious that Definition 2.8.1 **(a)** is well-defined (i.e., the infinite sum $\sum\limits_{k>0} k a_k x^{k-1}$ in this definition actually is a polynomial); see [Grinbe19b, Exercise 5 **(a)**] for the detailed proof of this fact.

The map D in Definition 2.8.1 **(b)** is a restriction of the map D in [Grinbe19b, Exercise 5]. (Indeed, the latter map is defined on formal power series, while the former map is defined on polynomials; but the two maps are defined by the same rule.) Thus, any formulas for values of D proven in [Grinbe19b] are still valid for our map D, as long as they are being applied to polynomials.

We shall need the following basic properties of derivatives:

[16] *Proof.* Let $v \in \mathbb{F}$. Then, $\mathbf{a}[v] = v^u - v$ (since $\mathbf{a} = x^u - x$). But we assumed that all $a \in \mathbb{F}$ satisfy $a^u = a$. Applying this to $a = v$, we find $v^u = v$. Hence, $\mathbf{a}[v] = v^u - v = 0$ (since $v^u = v$). In other words, v is a root of $\mathbf{a}$ in $\mathbb{F}$. In other words, $v \in \{\text{roots of } \mathbf{a} \text{ in } \mathbb{F}\}$.

Now, forget that we fixed v. We have thus shown that $v \in \{\text{roots of } \mathbf{a} \text{ in } \mathbb{F}\}$ for each $v \in \mathbb{F}$. In other words, $\mathbb{F} \subseteq \{\text{roots of } \mathbf{a} \text{ in } \mathbb{F}\}$.

[17] Note that [Grinbe19b, Exercise 5] uses the letter "f" instead of our "$\mathbf{f}$".

Proposition 2.8.2. Let $\mathbb{K}$ be a commutative ring. Let $\mathbf{f}$ and $\mathbf{g}$ be two polynomials in $\mathbb{K}[x]$.

(a) We have $(\mathbf{f}+\mathbf{g})' = \mathbf{f}' + \mathbf{g}'$.

(b) We have $(\mathbf{f}-\mathbf{g})' = \mathbf{f}' - \mathbf{g}'$.

(c) We have $(\mathbf{f}\mathbf{g})' = \mathbf{f}'\mathbf{g} + \mathbf{f}\mathbf{g}'$.

Proof of Proposition 2.8.2. In [Grinbe19b, Exercise 5 **(b)**], it is shown that the map D is $\mathbb{K}$-linear[18]. This quickly yields parts **(a)** and **(b)** of Proposition 2.8.2[19]. Proposition 2.8.2 **(c)** follows from [Grinbe19b, Exercise 5 **(c)**] (applied to $f = \mathbf{f}$ and $g = \mathbf{g}$) or from [Grinbe18, Proposition 0.2 **(c)**][20] (applied to $f = \mathbf{f}$ and $g = \mathbf{g}$). □

Proposition 2.8.2 **(c)** is known as the *Leibniz law* (or *Leibniz identity*) for derivatives of polynomials. We will need the following consequence of Proposition 2.8.2:

Corollary 2.8.3. Let $\mathbb{K}$ be a commutative ring. Let $\mathbf{f}$ and $\mathbf{g}$ be two polynomials in $\mathbb{K}[x]$. Then,

$$\left(\mathbf{f}^2\mathbf{g}\right)' = \mathbf{f} \cdot \left(2\mathbf{f}'\mathbf{g} + \mathbf{f}\mathbf{g}'\right).$$

Proof of Corollary 2.8.3. Proposition 2.8.2 **(c)** (applied to $\mathbf{f}$ instead of $\mathbf{g}$) shows that

$$(\mathbf{f}\mathbf{f})' = \underbrace{\mathbf{f}'\mathbf{f}}_{=\mathbf{f}\mathbf{f}'} + \mathbf{f}\mathbf{f}' = \mathbf{f}\mathbf{f}' + \mathbf{f}\mathbf{f}' = 2\mathbf{f}\mathbf{f}'.$$

In view of $\mathbf{f}\mathbf{f} = \mathbf{f}^2$, this rewrites as $\left(\mathbf{f}^2\right)' = 2\mathbf{f}\mathbf{f}'$. Now, Proposition 2.8.2 **(c)** (applied to $\mathbf{f}^2$ instead of $\mathbf{f}$) shows that

$$\left(\mathbf{f}^2\mathbf{g}\right)' = \underbrace{\left(\mathbf{f}^2\right)'}_{=2\mathbf{f}\mathbf{f}'}\mathbf{g} + \mathbf{f}^2\mathbf{g}' = 2\mathbf{f}\mathbf{f}'\mathbf{g} + \mathbf{f}^2\mathbf{g}' = \mathbf{f} \cdot \left(2\mathbf{f}'\mathbf{g} + \mathbf{f}\mathbf{g}'\right).$$

This proves Corollary 2.8.3. □

[18] More precisely: In [Grinbe19b, Exercise 5 **(b)**], it is shown that the map D from [Grinbe19b, Exercise 5] is $\mathbb{K}$-linear. This is not exactly our map D, but our map D is a restriction of this map; thus, it follows that our map D is $\mathbb{K}$-linear as well.

[19] In more details: The map D is $\mathbb{K}$-linear. Thus,

$$D(\mathbf{f}+\mathbf{g}) = \underbrace{D(\mathbf{f})}_{\substack{=\mathbf{f}' \\ \text{(by the definition of } D)}} + \underbrace{D(\mathbf{g})}_{\substack{=\mathbf{g}' \\ \text{(by the definition of } D)}} = \mathbf{f}' + \mathbf{g}'.$$

Comparing this with

$$D(\mathbf{f}+\mathbf{g}) = (\mathbf{f}+\mathbf{g})' \qquad \text{(by the definition of } D),$$

we obtain $(\mathbf{f}+\mathbf{g})' = \mathbf{f}' + \mathbf{g}'$. This proves Proposition 2.8.2 **(a)**. A similar argument proves Proposition 2.8.2 **(b)**.

[20] In [Grinbe18], I denote the indeterminate by t rather than x, and I use the notation $\dfrac{d}{dt}\mathbf{h}$ for the derivative $\mathbf{h}'$ of a polynomial $\mathbf{h}$.

Corollary 2.8.4. Let $\mathbb{K}$ be a field. Let $\mathbf{a} \in \mathbb{K}[x]$ be a monic polynomial such that $\deg(\mathbf{a}') = 0$ (that is, the polynomial $\mathbf{a}'$ is constant and nonzero). Then, $\mathbf{a}$ can be written in the form $\mathbf{a} = \mathbf{u}_1\mathbf{u}_2\cdots\mathbf{u}_k$, where $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k \in \mathbb{K}[x]$ are **distinct** monic irreducible polynomials.

Proof of Corollary 2.8.4. Corollary 2.2.3 (applied to $\mathbb{F} = \mathbb{K}$) shows that $\mathbf{a}$ can be written in the form $\mathbf{a} = \mathbf{u}_1\mathbf{u}_2\cdots\mathbf{u}_k$, where $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k \in \mathbb{K}[x]$ are monic irreducible polynomials. Consider these $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k$.

Next, we shall show that the polynomials $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k$ are distinct.

Indeed, assume the contrary. Thus, there exist two elements i and j of $\{1, 2, \ldots, k\}$ such that $i < j$ and $\mathbf{u}_i = \mathbf{u}_j$. Consider these i and j. Let $\mathbf{g}$ denote the polynomial $\prod\limits_{\substack{h \in \{1,2,\ldots,k\};\\ h \neq i \text{ and } h \neq j}} \mathbf{u}_h \in \mathbb{K}[x]$. (This may be an empty product, i.e., the constant polynomial 1.) Let $\mathbf{f} \in \mathbb{K}[x]$ be the polynomial $\mathbf{u}_j$. Then, $\mathbf{f} = \mathbf{u}_j$, and thus $\mathbf{f}$ is irreducible (since $\mathbf{u}_j$ is irreducible). Hence, $\deg \mathbf{f} > 0$.

Now, $\mathbf{u}_i$ and $\mathbf{u}_j$ are two distinct factors of the product $\mathbf{u}_1\mathbf{u}_2\cdots\mathbf{u}_k$ (since $i < j$). Splitting off these two factors, we obtain

$$\mathbf{u}_1\mathbf{u}_2\cdots\mathbf{u}_k = \underbrace{\mathbf{u}_i}_{=\mathbf{u}_j=\mathbf{f}} \underbrace{\mathbf{u}_j}_{=\mathbf{f}} \underbrace{\prod_{\substack{h \in \{1,2,\ldots,k\};\\ h \neq i \text{ and } h \neq j}} \mathbf{u}_h}_{\substack{=\mathbf{g} \\ \text{(by the definition of } \mathbf{g}\text{)}}} = \mathbf{f}\mathbf{f}\mathbf{g} = \mathbf{f}^2\mathbf{g}.$$

Therefore,

$$\mathbf{a} = \mathbf{u}_1\mathbf{u}_2\cdots\mathbf{u}_k = \mathbf{f}^2\mathbf{g}.$$

Taking derivatives on both sides of this equality, we find

$$\mathbf{a}' = \left(\mathbf{f}^2\mathbf{g}\right)' = \mathbf{f} \cdot \left(2\mathbf{f}'\mathbf{g} + \mathbf{f}\mathbf{g}'\right)$$

(by Corollary 2.8.3). Thus, $\mathbf{f} \cdot \left(2\mathbf{f}'\mathbf{g} + \mathbf{f}\mathbf{g}'\right) = \mathbf{a}' \neq 0$ (since $\deg(\mathbf{a}') = 0 \neq -\infty$). Hence, both polynomials $\mathbf{f}$ and $2\mathbf{f}'\mathbf{g} + \mathbf{f}\mathbf{g}'$ are nonzero. Thus,

$$\deg\left(\mathbf{f} \cdot \left(2\mathbf{f}'\mathbf{g} + \mathbf{f}\mathbf{g}'\right)\right) = \underbrace{\deg \mathbf{f}}_{>0} + \underbrace{\deg\left(2\mathbf{f}'\mathbf{g} + \mathbf{f}\mathbf{g}'\right)}_{\substack{\geq 0 \\ \text{(since } 2\mathbf{f}'\mathbf{g}+\mathbf{f}\mathbf{g}' \text{ is nonzero)}}} > 0.$$

This contradicts $\deg \underbrace{\left(\mathbf{f} \cdot \left(2\mathbf{f}'\mathbf{g} + \mathbf{f}\mathbf{g}'\right)\right)}_{=\mathbf{a}'} = \deg(\mathbf{a}') = 0$. This contradiction shows that our assumption was false. Hence, we have proven that the polynomials $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k$ are distinct.

We thus have found distinct monic irreducible polynomials $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k \in \mathbb{K}[x]$ such that $\mathbf{a} = \mathbf{u}_1\mathbf{u}_2\cdots\mathbf{u}_k$. In other words, we have written $\mathbf{a}$ in the form $\mathbf{a} = \mathbf{u}_1\mathbf{u}_2\cdots\mathbf{u}_k$, where $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k \in \mathbb{K}[x]$ are distinct monic irreducible polynomials. Thus, $\mathbf{a}$ can be written in this form. This proves Corollary 2.8.4. □

We furthermore need a formula for derivatives of monomials:

Proposition 2.8.5. Let $\mathbb{K}$ be a commutative ring. Let $m \in \mathbb{N}$. Then, in $\mathbb{K}[x]$, we have $D(x^m) = mx^{m-1}$. (Here, the expression "mx^{m-1}" is to be understood as 0 when $m = 0$.)

Proof of Proposition 2.8.5. This is proven in [Grinbe19b, Statement 8 in the solution to Exercise 5]. □

We can restate Proposition 2.8.5 as follows:

Proposition 2.8.6. Let $\mathbb{K}$ be a commutative ring. Let $m \in \mathbb{N}$. Then, in $\mathbb{K}[x]$, we have $(x^m)' = mx^{m-1}$. (Here, the expression "mx^{m-1}" is to be understood as 0 when $m = 0$.)

Proof of Proposition 2.8.6. Proposition 2.8.5 yields $D(x^m) = mx^{m-1}$. But the definition of D yields $D(x^m) = (x^m)'$. Comparing these two equalities, we find $(x^m)' = mx^{m-1}$. This proves Proposition 2.8.6. □

Corollary 2.8.7. Let $\mathbb{K}$ be a commutative $\mathbb{F}_p$-algebra. Let m be a positive integer satisfying $p \mid m$. Then, in $\mathbb{K}[x]$, we have $(x^m)' = 0$.

Proof of Corollary 2.8.7. We have $p \mid m$. Thus, there exists some integer c such that $m = pc$. Consider this c.

Proposition 2.6.3 **(b)** (applied to $\mathbf{a} = cx^{m-1}$) shows that $pcx^{m-1} = 0$. But Proposition 2.8.6 yields

$$(x^m)' = \underbrace{m}_{=pc} x^{m-1} = pcx^{m-1} = 0.$$

This proves Corollary 2.8.7. □

2.9. Factoring $x^{p^g} - x$, part I

Lemma 2.9.1. Let g be a positive integer. Let $\mathbb{K}$ be an $\mathbb{F}_p$-field. Then, the polynomial $x^{p^g} - x \in \mathbb{K}[x]$ can be written in the form $x^{p^g} - x = \mathbf{u}_1\mathbf{u}_2\cdots\mathbf{u}_k$, where $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k \in \mathbb{K}[x]$ are **distinct** monic irreducible polynomials.

Proof of Lemma 2.9.1. We know that $\mathbb{K}$ is an $\mathbb{F}_p$-field. In other words, $\mathbb{K}$ is an $\mathbb{F}_p$-algebra that is a field. Hence, $\mathbb{K}$ is commutative (since $\mathbb{K}$ is a field).

We have $g > 0$ (since g is a positive integer), hence $p^g > p^0 = 1$. Thus, the leading term of the polynomial $x^{p^g} - x$ is x^{p^g}. This shows that the polynomial $x^{p^g} - x$ is monic of degree p^g.

Proposition 2.8.6 (applied to $m = 1$) yields $\left(x^1\right)' = 1 \underbrace{x^{1-1}}_{=x^0=1} = 1$. In view of $x^1 = x$, this rewrites as $x' = 1$.

Also, g is a positive integer; hence, $g \geq 1$, so that $g - 1 \in \mathbb{N}$. Hence, p^{g-1} is an integer. Thus, $p \mid p^g$ (since $p^g = p \cdot p^{g-1}$). Hence, Corollary 2.8.7 (applied to $m = p^g$) yields $\left(x^{p^g}\right)' = 0$.

Now, Proposition 2.8.2 **(b)** (applied to x^{p^g} and x instead of $\mathbf{f}$ and $\mathbf{g}$) shows that

$$\left(x^{p^g} - x\right)' = \underbrace{\left(x^{p^g}\right)'}_{=0} - \underbrace{x'}_{=1} = 0 - 1 = -1.$$

Thus, $\deg \left(\underbrace{\left(x^{p^g} - x\right)'}_{=-1} \right) = \deg(-1) = 0$. So we know that $x^{p^g} - x$ is a monic polynomial such that $\deg\left(\left(x^{p^g} - x\right)'\right) = 0$ (that is, the polynomial $\left(x^{p^g} - x\right)'$ is constant and nonzero). Hence, Corollary 2.8.4 (applied to $\mathbf{a} = x^{p^g} - x$) shows that $x^{p^g} - x$ can be written in the form $x^{p^g} - x = \mathbf{u}_1\mathbf{u}_2 \cdots \mathbf{u}_k$, where $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k \in \mathbb{K}[x]$ are **distinct** monic irreducible polynomials. This proves Lemma 2.9.1. □

Lemma 2.9.2. Let r and m be positive integers. Let $\mathbb{K}$ be a finite $\mathbb{F}_p$-field of size p^m. Let $\mathbf{a} \in \mathbb{K}[x]$ be an irreducible polynomial such that $\mathbf{a} \mid x^{p^{mr}} - x$ in $\mathbb{K}[x]$. Then, $\deg \mathbf{a} \mid r$ in $\mathbb{Z}$.

Proof of Lemma 2.9.2. The integers m and r are positive. Hence, their product mr is positive as well.

Let $n = \deg \mathbf{a}$. Thus, $\mathbf{a}$ is a polynomial of degree n. Note that $\mathbf{a}$ is irreducible; thus, $\deg \mathbf{a} > 0$. Hence, $n = \deg \mathbf{a} > 0$. Thus, n is a positive integer. Hence, mn is a positive integer (since m is a positive integer).

We know that $\mathbb{K}$ is an $\mathbb{F}_p$-field. In other words, $\mathbb{K}$ is an $\mathbb{F}_p$-algebra that is a field. Thus, $\mathbb{K}$ is a field, so that $\mathbb{K}$ is commutative. Moreover, $\mathbb{K}$ has size p^m; thus, $|\mathbb{K}| = p^m$. Now, Theorem 2.1.2 **(b)** (applied to $\mathbb{F} = \mathbb{K}$) yields that

$$\begin{aligned} |\mathbb{K}[x]/\mathbf{a}| = |\mathbb{K}|^n &= (p^m)^n \qquad \left(\text{since } |\mathbb{K}| = p^m\right) \\ &= p^{mn}. \end{aligned}$$

Furthermore, Theorem 2.1.2 **(c)** (applied to $\mathbb{F} = \mathbb{K}$) yields that $\mathbb{K}[x]/\mathbf{a}$ is a field. Let $\mathbb{F}$ denote this field. Thus,

$$\mathbb{F} = \mathbb{K}[x]/\mathbf{a}, \qquad \text{so that} \qquad |\mathbb{F}| = |\mathbb{K}[x]/\mathbf{a}| = p^{mn}.$$

We know that $\mathbb{K}$ is a commutative $\mathbb{F}_p$-algebra. We also know that $\mathbb{K}[x]$ is a $\mathbb{K}$-algebra. Thus, Proposition 2.4.3 (applied to $\mathbb{F}_p$, $\mathbb{K}$ and $\mathbb{K}[x]$ instead of $\mathbb{K}$, $\mathbb{L}$ and V) shows that $\mathbb{K}[x]$ becomes an $\mathbb{F}_p$-algebra in a natural way.

We thus know that $\mathbb{K}[x]$ is a commutative $\mathbb{F}_p$-algebra[21]. We also know that $\mathbb{F}$ is a $\mathbb{K}[x]$-algebra (since $\mathbb{F} = \mathbb{K}[x]/\mathbf{a}$). Thus, Proposition 2.4.3 (applied to $\mathbb{F}_p$, $\mathbb{K}[x]$

[21] since $\mathbb{K}[x]$ is commutative

and $\mathbb{F}$ instead of $\mathbb{K}$, $\mathbb{L}$ and V) shows that $\mathbb{F}$ becomes an $\mathbb{F}_p$-algebra in a natural way. Thus, $\mathbb{F}$ is a commutative $\mathbb{F}_p$-algebra (since $\mathbb{F}$ is commutative). Also, $\mathbb{F}$ is an $\mathbb{F}_p$-field (since $\mathbb{F}$ is an $\mathbb{F}_p$-algebra that is also a field). Recall that $\mathbb{F}$ has size p^{mn} (since $|\mathbb{F}| = p^{mn}$).

Let F be the Frobenius endomorphism $F_{\mathbb{F}} : \mathbb{F} \to \mathbb{F}$ of $\mathbb{F}$. (See Definition 2.6.1 for the definition of a Frobenius endomorphism.)

Recall Convention 2.1.1. We have

$$\left([f]_{\mathbf{a}}\right)^k = \left[f^k\right]_{\mathbf{a}} \qquad \text{for each } f \in \mathbb{K}[x] \text{ and each } k \in \mathbb{N}. \tag{6}$$

(Indeed, this can be proven by a straightforward induction on k, using the definition of the multiplication on $\mathbb{K}[x]/\mathbf{a}$.)

The elements x and $x^{p^{mr}}$ of $\mathbb{K}[x]$ satisfy $\mathbf{a} \mid x^{p^{mr}} - x$. In other words, $x^{p^{mr}} \equiv x \operatorname{mod} \mathbf{a}$. In other words,

$$\left[x^{p^{mr}}\right]_{\mathbf{a}} = [x]_{\mathbf{a}}. \tag{7}$$

(Again, recall that we are using Convention 2.1.1.)

Proposition 2.6.4 (applied to $\mathbb{F}$, $[x]_{\mathbf{a}}$ and mr instead of $\mathbb{K}$, a and i) yields that

$$\begin{aligned} F^{mr}\left([x]_{\mathbf{a}}\right) &= \left([x]_{\mathbf{a}}\right)^{p^{mr}} = \left[x^{p^{mr}}\right]_{\mathbf{a}} \qquad \left(\text{by (6), applied to } f = x \text{ and } k = p^{mr}\right) \\ &= [x]_{\mathbf{a}} \qquad (\text{by (7)}). \end{aligned} \tag{8}$$

Also, the Frobenius endomorphism $F_{\mathbb{F}}$ is an $\mathbb{F}_p$-algebra homomorphism (by Theorem 2.6.2, applied to $\mathbb{F}$ instead of $\mathbb{K}$). In other words, F is an $\mathbb{F}_p$-algebra homomorphism (since $F = F_{\mathbb{F}}$). Hence, F^{mr} is an $\mathbb{F}_p$-algebra homomorphism as well (since any composition of $\mathbb{F}_p$-algebra homomorphisms is an $\mathbb{F}_p$-algebra homomorphism). In other words, the map F^{mr} is an $\mathbb{F}_p$-module homomorphism and a ring homomorphism at the same time.

Next, we shall show that

$$F^{mr}(u) = u \qquad \text{for each } u \in \mathbb{F}. \tag{9}$$

[*Proof of (9):* Let $u \in \mathbb{F}$. Thus, $u \in \mathbb{F} = \mathbb{K}[x]/\mathbf{a}$. But Theorem 2.1.2 **(a)** (applied to $\mathbb{K}$ instead of $\mathbb{F}$) yields that each element of $\mathbb{K}[x]/\mathbf{a}$ can be uniquely written in the form

$$\lambda_0\left[x^0\right]_{\mathbf{a}} + \lambda_1\left[x^1\right]_{\mathbf{a}} + \cdots + \lambda_{n-1}\left[x^{n-1}\right]_{\mathbf{a}} \qquad \text{with } \lambda_0, \lambda_1, \ldots, \lambda_{n-1} \in \mathbb{K}.$$

Thus, in particular, u can be written uniquely in this form (since $u \in \mathbb{K}[x]/\mathbf{a}$). In other words, there exists a unique n-tuple $(\lambda_0, \lambda_1, \ldots, \lambda_{n-1}) \in \mathbb{K}^n$ such that $u = \lambda_0\left[x^0\right]_{\mathbf{a}} + \lambda_1\left[x^1\right]_{\mathbf{a}} + \cdots + \lambda_{n-1}\left[x^{n-1}\right]_{\mathbf{a}}$. Consider this n-tuple. For each $i \in \{0, 1, \ldots, n-1\}$, we have $\lambda_i \in \mathbb{K}$ and therefore

$$(\lambda_i)^{p^{mr}} = \lambda_i \tag{10}$$

(by Corollary 2.6.6, applied to $\mathbb{K}$ and m instead of $\mathbb{F}$ and n), since $\mathbb{K}$ is a finite $\mathbb{F}_p$-field of size p^m.

But we have

$$u = \lambda_0 \left[x^0\right]_{\mathbf{a}} + \lambda_1 \left[x^1\right]_{\mathbf{a}} + \cdots + \lambda_{n-1} \left[x^{n-1}\right]_{\mathbf{a}} = \sum_{i=0}^{n-1} \lambda_i \left[x^i\right]_{\mathbf{a}}. \tag{11}$$

Applying the map F^{mr} to both sides of this equality, we obtain

$$\begin{aligned} F^{mr}(u) &= F^{mr}\left(\sum_{i=0}^{n-1} \lambda_i \left[x^i\right]_{\mathbf{a}}\right) = \sum_{i=0}^{n-1} \underbrace{F^{mr}\left(\lambda_i \left[x^i\right]_{\mathbf{a}}\right)}_{\substack{=\left(\lambda_i\left[x^i\right]_{\mathbf{a}}\right)^{p^{mr}} \\ \text{(by Proposition 2.6.4,} \\ \text{applied to } \mathbb{F},\ \lambda_i\left[x^i\right]_{\mathbf{a}} \text{ and } mr \\ \text{instead of } \mathbb{K},\ a \text{ and } i)}} \\ &\qquad \left(\text{since } F^{mr} \text{ is an } \mathbb{F}_p\text{-module homomorphism}\right) \\ &= \sum_{i=0}^{n-1} \underbrace{\left(\lambda_i \left[x^i\right]_{\mathbf{a}}\right)^{p^{mr}}}_{\substack{=(\lambda_i)^{p^{mr}}\left(\left[x^i\right]_{\mathbf{a}}\right)^{p^{mr}} \\ \text{(since } \mathbb{F} \text{ is a } \mathbb{K}\text{-algebra)}}} = \sum_{i=0}^{n-1} \underbrace{(\lambda_i)^{p^{mr}}}_{\substack{=\lambda_i \\ \text{(by (10))}}} \left(\left[x^i\right]_{\mathbf{a}}\right)^{p^{mr}} \\ &= \sum_{i=0}^{n-1} \lambda_i \left(\left[x^i\right]_{\mathbf{a}}\right)^{p^{mr}}. \end{aligned} \tag{12}$$

But for each $i \in \{0, 1, \ldots, n-1\}$, we have

$$\begin{aligned} \left(\left[x^i\right]_{\mathbf{a}}\right)^{p^{mr}} &= \left[\left(x^i\right)^{p^{mr}}\right]_{\mathbf{a}} && \left(\text{by (6), applied to } f = x^i \text{ and } k = p^{mr}\right) \\ &= \left[\left(x^{p^{mr}}\right)^i\right]_{\mathbf{a}} && \left(\text{since } \left(x^i\right)^{p^{mr}} = x^{ip^{mr}} = x^{p^{mr}i} = \left(x^{p^{mr}}\right)^i\right) \\ &= \left(\left[x^{p^{mr}}\right]_{\mathbf{a}}\right)^i && \left(\begin{array}{c} \text{since (6) (applied to } f = x^{p^{mr}} \text{ and } k = i) \\ \text{yields } \left(\left[x^{p^{mr}}\right]_{\mathbf{a}}\right)^i = \left[\left(x^{p^{mr}}\right)^i\right]_{\mathbf{a}} \end{array}\right) \\ &= \left([x]_{\mathbf{a}}\right)^i && \left(\text{since } \left[x^{p^{mr}}\right]_{\mathbf{a}} = [x]_{\mathbf{a}}\right) \\ &= \left[x^i\right]_{\mathbf{a}} && \left(\text{by (6), applied to } f = x \text{ and } k = i\right). \end{aligned} \tag{13}$$

Hence, (12) becomes

$$F^{mr}(u) = \sum_{i=0}^{n-1} \lambda_i \underbrace{\left(\left[x^i\right]_{\mathbf{a}}\right)^{p^{mr}}}_{\substack{=\left[x^i\right]_{\mathbf{a}} \\ \text{(by (13))}}} = \sum_{i=0}^{n-1} \lambda_i \left[x^i\right]_{\mathbf{a}} = u$$

(by (11)). This proves (9).]

Thus, we have shown that all $u \in \mathbb{F}$ satisfy $F^{mr}(u) = u$. Hence, all $u \in \mathbb{F}$ satisfy $F^{mr}(u) = u = \operatorname{id}(u)$. In other words, $F^{mr} = \operatorname{id}$.

On the other hand, $\mathbb{F}$ is a finite $\mathbb{F}_p$-field of size p^{mn} (since $|\mathbb{F}| = p^{mn}$). Thus, Corollary 2.6.5 (applied to mn instead of n) yields $F^{mn} = \operatorname{id}$.

Now we know that $F^{mr} = \operatorname{id}$ and $F^{mn} = \operatorname{id}$. Hence, Lemma 2.3.1 (applied to $\mathbb{F}$, F, mr and mn instead of S, f, a and b) yields that $F^{\gcd(mr,mn)} = \operatorname{id}$.

Let $i = \gcd(mr, mn)$. Thus, i is a positive integer (since mr and mn are positive integers), so that $p^i > 1$. Furthermore, from $i = \gcd(mr, mn)$, we obtain

$$F^i = F^{\gcd(mr,mn)} = \operatorname{id}.$$

Now, for each $a \in \mathbb{F}$, we have

$$F^i(a) = a^{p^i} \qquad \text{(by Proposition 2.6.4, applied to } \mathbb{F} \text{ instead of } \mathbb{K}\text{)}$$

and thus

$$a^{p^i} = \underbrace{F^i}_{=\operatorname{id}}(a) = \operatorname{id}(a) = a.$$

So we have shown that all $a \in \mathbb{F}$ satisfy $a^{p^i} = a$. Hence, Corollary 2.7.3 (applied to $u = p^i$) shows that $|\mathbb{F}| \leq p^i$ (since $p^i > 1$). In view of $|\mathbb{F}| = p^{mn}$, this rewrites as $p^{mn} \leq p^i$. Hence, $mn \leq i$ (since $p > 1$). But[22] $i = \gcd(mr, mn) \mid mn$ and thus $i \leq mn$ (since i and mn both are positive integers). Combining this with $mn \leq i$, we find $mn = i$. Thus, $mn = i = \gcd(mr, mn) \mid mr$. We can cancel m from this divisibility (since m is a nonzero integer), and thus find $n \mid r$. In view of $n = \deg \mathbf{a}$, this rewrites as $\deg \mathbf{a} \mid r$. This proves Lemma 2.9.2. □

We will say more about the factorization of the polynomial $x^{p^g} - x$ (that is, about the factors $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_k$ in Lemma 2.9.1) in Theorem 4.2.2 further below, but for now let us draw the one consequence of Lemma 2.9.2 that we will actually need for our proof of Theorem 1.0.3:

Corollary 2.9.3. Let r and m be positive integers such that r is prime. Let $\mathbb{K}$ be a finite $\mathbb{F}_p$-field of size p^m. Then, there exists a monic irreducible polynomial $\mathbf{a} \in \mathbb{K}[x]$ of degree r.

Proof of Corollary 2.9.3. Clearly, mr is a positive integer (since m and r are positive integers). Thus, $p^{mr} > 1$. Hence, the polynomial $x^{p^{mr}} - x$ is a monic polynomial of degree p^{mr}. Thus, $\deg\left(x^{p^{mr}} - x\right) = p^{mr}$.

Also, r is prime. Hence, $r > 1$. We can multiply this inequality by m (since m is positive), and thus $mr > m \cdot 1 = m$. Hence, $p^{mr} > p^m$.

Lemma 2.9.1 (applied to $g = mr$) shows that the polynomial $x^{p^{mr}} - x \in \mathbb{K}[x]$ can be written in the form $x^{p^{mr}} - x = \mathbf{u}_1\mathbf{u}_2 \cdots \mathbf{u}_k$, where $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k \in \mathbb{K}[x]$ are **distinct** monic irreducible polynomials. Consider these $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k$.

[22] From this place on, all divisibilities are understood to mean divisibilities in $\mathbb{Z}$.

Assume (for the sake of contradiction) that

$$\deg(\mathbf{u}_i) = 1 \qquad \text{for each } i \in \{1, 2, \ldots, k\}. \tag{14}$$

Thus, the polynomials $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k$ all have degree 1. Hence, $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k$ are monic polynomials of degree 1 (since we know that $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k$ are monic polynomials). Furthermore, these k monic polynomials of degree 1 are distinct (as we know). Thus, we have found k distinct monic polynomials of degree 1 (namely, $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k$). Hence,

$$(\text{the number of all monic polynomials of degree 1 in } \mathbb{K}[x]) \geq k.$$

On the other hand, each monic polynomial of degree 1 (in $\mathbb{K}[x]$) has the form $x + c$ for some unique $c \in \mathbb{K}$. Hence,

$$\begin{aligned}&(\text{the number of all monic polynomials of degree 1 in } \mathbb{K}[x]) \\ &= (\text{the number of all } c \in \mathbb{K}) = |\mathbb{K}| = p^m \qquad (\text{since } \mathbb{K} \text{ has size } p^m).\end{aligned}$$

Thus,

$$p^m = (\text{the number of all monic polynomials of degree 1 in } \mathbb{K}[x]) \geq k.$$

Recall that the degree of a product of nonzero polynomials over a field always equals the sum of their degrees. We can apply this to the polynomials $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k$ (which are nonzero because they are irreducible) and thus obtain

$$\begin{aligned}\deg(\mathbf{u}_1\mathbf{u}_2\cdots\mathbf{u}_k) &= \deg(\mathbf{u}_1) + \deg(\mathbf{u}_2) + \cdots + \deg(\mathbf{u}_k) = \sum_{i=1}^{k} \underbrace{\deg(\mathbf{u}_i)}_{\substack{=1 \\ (\text{by (14)})}} \\ &= \sum_{i=1}^{k} 1 = k \cdot 1 = k.\end{aligned}$$

Hence,

$$k = \deg \underbrace{(\mathbf{u}_1\mathbf{u}_2\cdots\mathbf{u}_k)}_{\substack{=x^{p^{mr}}-x \\ (\text{since } x^{p^{mr}}-x=\mathbf{u}_1\mathbf{u}_2\cdots\mathbf{u}_k)}} = \deg\left(x^{p^{mr}} - x\right) = p^{mr} > p^m \geq k.$$

This is clearly absurd. This contradiction shows that our assumption (that is, (14)) is false. In other words, not every $i \in \{1, 2, \ldots, k\}$ satisfies $\deg(\mathbf{u}_i) = 1$. In other words, there exists some $i \in \{1, 2, \ldots, k\}$ such that $\deg(\mathbf{u}_i) \neq 1$. Consider this i. The polynomial $\mathbf{u}_i \in \mathbb{K}[x]$ is irreducible (since $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k$ are all irreducible). Thus, its degree $\deg(\mathbf{u}_i)$ is a positive integer.

We have $\mathbf{u}_i \mid \mathbf{u}_1\mathbf{u}_2\cdots\mathbf{u}_k$ (since $\mathbf{u}_i$ is a factor of the product $\mathbf{u}_1\mathbf{u}_2\cdots\mathbf{u}_k$). Hence, $\mathbf{u}_i \mid \mathbf{u}_1\mathbf{u}_2\cdots\mathbf{u}_k = x^{p^{mr}} - x$. Thus, Lemma 2.9.2 (applied to $g = mr$ and $\mathbf{a} = \mathbf{u}_i$)

shows that $\deg(\mathbf{u}_i) \mid r$ in $\mathbb{Z}$. Hence, $\deg(\mathbf{u}_i)$ is a divisor of r, and thus is a positive divisor of r (since $\deg(\mathbf{u}_i)$ is positive). But the only positive divisors of r are 1 and r (since r is prime). Hence, $\deg(\mathbf{u}_i)$ equals either 1 or r (since $\deg(\mathbf{u}_i)$ is a positive divisor of r). Therefore, $\deg(\mathbf{u}_i) = r$ (since $\deg(\mathbf{u}_i) \neq 1$). In other words, the polynomial $\mathbf{u}_i$ has degree r. Thus, there exists a monic irreducible polynomial $\mathbf{a} \in \mathbb{K}[x]$ of degree r (namely, $\mathbf{a} = \mathbf{u}_i$). This proves Corollary 2.9.3. □

3. The proof

3.1. The case of a prime exponent

We are getting close to proving Theorem 1.0.3. The following is one of our last steps:

Lemma 3.1.1. Let r be a prime. Let m be a positive integer. Let $\mathbb{F}$ be a finite $\mathbb{F}_p$-field of size p^m. Then, there exists a finite $\mathbb{F}_p$-field of size p^{mr}.

Proof of Lemma 3.1.1. We know that $\mathbb{F}$ is an $\mathbb{F}_p$-field. In other words, $\mathbb{F}$ is an $\mathbb{F}_p$-algebra that is a field. Thus, $\mathbb{F}$ is commutative (since $\mathbb{F}$ is a field). Also, $|\mathbb{F}| = p^m$ (because $\mathbb{F}$ has size p^m).

Corollary 2.9.3 (applied to $\mathbb{K} = \mathbb{F}$) shows that there exists a monic irreducible polynomial $\mathbf{a} \in \mathbb{F}[x]$ of degree r. Consider this $\mathbf{a}$. Theorem 2.1.2 **(c)** (applied to $n = r$) yields that $\mathbb{F}[x]/\mathbf{a}$ is a field. Furthermore, Theorem 2.1.2 **(b)** (applied to $n = r$) yields that

$$\begin{aligned} |\mathbb{F}[x]/\mathbf{a}| = |\mathbb{F}|^r &= (p^m)^r \qquad\qquad (\text{since } |\mathbb{F}| = p^m) \\ &= p^{mr}. \end{aligned}$$

Thus, the field $\mathbb{F}[x]/\mathbf{a}$ is finite.

We know that $\mathbb{F}$ is a commutative $\mathbb{F}_p$-algebra. We also know that $\mathbb{F}[x]$ is an $\mathbb{F}$-algebra. Thus, Proposition 2.4.3 (applied to $\mathbb{F}_p$, $\mathbb{F}$ and $\mathbb{F}[x]$ instead of $\mathbb{K}$, $\mathbb{L}$ and V) shows that $\mathbb{F}[x]$ becomes an $\mathbb{F}_p$-algebra in a natural way. Clearly, this $\mathbb{F}[x]$ is commutative (since $\mathbb{F}$ is commutative).

We thus know that $\mathbb{F}[x]$ is a commutative $\mathbb{F}_p$-algebra. We also know that $\mathbb{F}[x]/\mathbf{a}$ is an $\mathbb{F}[x]$-algebra. Thus, Proposition 2.4.3 (applied to $\mathbb{F}_p$, $\mathbb{F}[x]$ and $\mathbb{F}[x]/\mathbf{a}$ instead of $\mathbb{K}$, $\mathbb{L}$ and V) shows that $\mathbb{F}[x]/\mathbf{a}$ becomes an $\mathbb{F}_p$-algebra in a natural way. Thus, $\mathbb{F}[x]/\mathbf{a}$ is an $\mathbb{F}_p$-field (since $\mathbb{F}[x]/\mathbf{a}$ is an $\mathbb{F}_p$-algebra that is also a field).

Thus we have shown that $\mathbb{F}[x]/\mathbf{a}$ is a finite $\mathbb{F}_p$-field of size p^{mr} (since $|\mathbb{F}[x]/\mathbf{a}| = p^{mr}$). Hence, there exists a finite $\mathbb{F}_p$-field of size p^{mr} (namely, $\mathbb{F}[x]/\mathbf{a}$). This proves Lemma 3.1.1. □

3.2. Proof of Theorem 1.0.3

Recall the following basic fact from number theory:

Lemma 3.2.1. Let $N > 1$ be an integer. Then, there exists at least one prime r such that $r \mid N$.

Lemma 3.2.1 is, for example, [Grinbe19a, Proposition 2.13.8] (with n and p renamed as N and r).

At last, we can prove Theorem 1.0.3:

Proof of Theorem 1.0.3. We shall prove Theorem 1.0.3 by strong induction on n.

Induction step: Let N be a positive integer. Assume (as the induction hypothesis) that Theorem 1.0.3 holds for all $n < N$. We must now prove that Theorem 1.0.3 holds for $n = N$. In other words, we must prove that there exists a finite $\mathbb{F}_p$-field of size p^N.

If $N = 1$, then this is obvious[23]. Thus, for the rest of this proof, we WLOG assume that $N \neq 1$. Hence, $N > 1$ (since N is a positive integer). Thus, Lemma 3.2.1 shows that there exists at least one prime r such that $r \mid N$. Consider this r. We have $r > 1$ (since r is prime), so that $r > 1 > 0$. Also, there exists an integer m such that $N = rm$ (since $r \mid N$). Consider this m. We have $N = rm$, thus $m = N/r > 0$ (since $N > 0$ and $r > 0$). Hence, we can multiply the inequality $r > 1$ by m. We thus find $rm > 1m = m$, so that $m < rm = N$. Also, m is a positive integer (since m is an integer and since $m > 0$).

Recall that Theorem 1.0.3 holds for all $n < N$ (by our induction hypothesis). Hence, Theorem 1.0.3 holds for $n = m$ (since m is a positive integer satisfying $m < N$). In other words, there exists a finite $\mathbb{F}_p$-field of size p^m. Consider such an $\mathbb{F}_p$-field, and denote it by $\mathbb{F}$. Thus, $\mathbb{F}$ is a finite $\mathbb{F}_p$-field of size p^m. Hence, Lemma 3.1.1 shows that there exists a finite $\mathbb{F}_p$-field of size p^{mr}. In other words, there exists a finite $\mathbb{F}_p$-field of size p^N (since $mr = rm = N$). In other words, Theorem 1.0.3 holds for $n = N$. This completes the induction step. Thus, Theorem 1.0.3 is proven by strong induction. □

4. Appendices

4.1. Appendix 1: Proofs of Proposition 2.4.1 and Proposition 2.4.2

We still have to prove two propositions that we used: Proposition 2.4.1 and Proposition 2.4.2. Both proofs are straightforward, but require us to recall precisely how modules and algebras were defined.

First, let us recall the definition of a $\mathbb{K}$-module. Several equivalent definitions exist; we shall use the one from [Grinbe19a, Definition 6.3.1]:

[23] *Proof.* The finite field $\mathbb{F}_p$ is clearly an $\mathbb{F}_p$-algebra, and thus is an $\mathbb{F}_p$-field (by the definition of an $\mathbb{F}_p$-field). Moreover, it has size p^1 (since $|\mathbb{F}_p| = p = p^1$). Thus, $\mathbb{F}_p$ is a finite $\mathbb{F}_p$-field of size p^1. Hence, there exists a finite $\mathbb{F}_p$-field of size p^1 (namely, $\mathbb{F}_p$). Hence, there exists a finite $\mathbb{F}_p$-field of size p^N when $N = 1$. Qed.

Definition 4.1.1. Let $\mathbb{K}$ be a commutative ring.

A $\mathbb{K}$-*module* means a set M equipped with

- a binary operation $+$ on M (called "*addition*", and not to be confused with the addition $+_{\mathbb{K}}$ of $\mathbb{K}$),
- a map $\cdot : \mathbb{K} \times M \to M$ (called "*scaling*", and not to be confused with the multiplication $\cdot_{\mathbb{K}}$ of $\mathbb{K}$), and
- an element $0_M \in M$ (called "*zero vector*" or "zero", and not to be confused with the zero of $\mathbb{K}$)

satisfying the following axioms:

- **(a)** We have $a + b = b + a$ for all $a, b \in M$.
- **(b)** We have $a + (b + c) = (a + b) + c$ for all $a, b, c \in M$.
- **(c)** We have $a + 0_M = 0_M + a = a$ for all $a \in M$.
- **(d)** Each $a \in M$ has an additive inverse (i.e., there is an $a' \in M$ such that $a + a' = a' + a = 0_M$).
- **(e)** We have $\lambda (a + b) = \lambda a + \lambda b$ for all $\lambda \in \mathbb{K}$ and $a, b \in M$. Here and in the following, we use the notation "λc" (or, equivalently, "$\lambda \cdot c$") for the image of a pair $(\lambda, c) \in \mathbb{K} \times M$ under the "scaling" map $\cdot$ (similarly to how we write ab for the image of a pair $(a, b) \in \mathbb{K} \times \mathbb{K}$ under the "multiplication" map $\cdot$).
- **(f)** We have $(\lambda + \mu) a = \lambda a + \mu a$ for all $\lambda, \mu \in \mathbb{K}$ and $a \in M$.
- **(g)** We have $0a = 0_M$ for all $a \in M$.
- **(h)** We have $(\lambda \mu) a = \lambda (\mu a)$ for all $\lambda, \mu \in \mathbb{K}$ and $a \in M$.
- **(i)** We have $1a = a$ for all $a \in M$.
- **(j)** We have $\lambda \cdot 0_M = 0_M$ for all $\lambda \in \mathbb{K}$.

These ten axioms are called the *module axioms*.

Let us also recall the definition of a $\mathbb{K}$-algebra ([Grinbe19a, Definition 6.9.1]):

Definition 4.1.2. Let $\mathbb{K}$ be a commutative ring. A $\mathbb{K}$-*algebra* is a set M endowed with two binary operations $+$ and $\cdot$ as well as a scaling map $\cdot : \mathbb{K} \times M \to M$ (not to be confused with the multiplication map, which is also denoted by $\cdot$) and two elements $0, 1 \in M$ that satisfy all the ring axioms (with $\mathbb{K}$ replaced by M) as well as all the module axioms (where the zero vector 0_M is taken to be the element $0 \in M$) and also the following axiom:

- **Scale-invariance of multiplication:** We have $\lambda(ab) = (\lambda a) \cdot b = a \cdot (\lambda b)$ for all $\lambda \in \mathbb{K}$ and $a, b \in M$.

We can now prove Proposition 2.4.1 by a fairly straightforward verification of the module axioms:

Proof of Proposition 2.4.1. We have assumed that V is an $\mathbb{L}$-module. Thus, it satisfies the module axioms. In other words, the following ten statements hold:[24]

- **(a_1)** We have $a + b = b + a$ for all $a, b \in V$.
- **(b_1)** We have $a + (b + c) = (a + b) + c$ for all $a, b, c \in V$.
- **(c_1)** We have $a + 0_V = 0_V + a = a$ for all $a \in V$.
- **(d_1)** Each $a \in V$ has an additive inverse (i.e., there is an $a' \in V$ such that $a + a' = a' + a = 0_V$).
- **(e_1)** We have $\lambda(a + b) = \lambda a + \lambda b$ for all $\lambda \in \mathbb{L}$ and $a, b \in V$.
- **(f_1)** We have $(\lambda + \mu) a = \lambda a + \mu a$ for all $\lambda, \mu \in \mathbb{L}$ and $a \in V$.
- **(g_1)** We have $0_{\mathbb{L}} a = 0_V$ for all $a \in V$.
- **(h_1)** We have $(\lambda\mu) a = \lambda(\mu a)$ for all $\lambda, \mu \in \mathbb{L}$ and $a \in V$.
- **(i_1)** We have $1_{\mathbb{L}} a = a$ for all $a \in V$.
- **(j_1)** We have $\lambda \cdot 0_V = 0_V$ for all $\lambda \in \mathbb{L}$.

We have also assumed that $\mathbb{L}$ is a $\mathbb{K}$-algebra. Thus, $\mathbb{L}$ satisfies the ring axioms, the module axioms and the "Scale-invariance of multiplication" axiom. In other words, the following 15 statements hold:

- **(a_2)** We have $a + b = b + a$ for all $a, b \in \mathbb{L}$.
- **(b_2)** We have $a + (b + c) = (a + b) + c$ for all $a, b, c \in \mathbb{L}$.
- **(c_2)** We have $a + 0_{\mathbb{L}} = 0_{\mathbb{L}} + a = a$ for all $a \in \mathbb{L}$.
- **(d_2)** Each $a \in \mathbb{L}$ has an additive inverse (i.e., there is an $a' \in \mathbb{L}$ such that $a + a' = a' + a = 0_{\mathbb{L}}$).
- **(e_2)** We have $\lambda(a + b) = \lambda a + \lambda b$ for all $\lambda \in \mathbb{K}$ and $a, b \in \mathbb{L}$.
- **(f_2)** We have $(\lambda + \mu) a = \lambda a + \mu a$ for all $\lambda, \mu \in \mathbb{K}$ and $a \in \mathbb{L}$.
- **(g_2)** We have $0_{\mathbb{K}} a = 0_{\mathbb{L}}$ for all $a \in \mathbb{L}$.
- **(h_2)** We have $(\lambda\mu) a = \lambda(\mu a)$ for all $\lambda, \mu \in \mathbb{K}$ and $a \in \mathbb{L}$.

[24] As usual, we let 0_V denote the zero vector of the $\mathbb{L}$-module V.

- **($\mathbf{i}_2$)** We have $1_{\mathbb{K}}a = a$ for all $a \in \mathbb{L}$.
- **($\mathbf{j}_2$)** We have $\lambda \cdot 0_{\mathbb{L}} = 0_{\mathbb{L}}$ for all $\lambda \in \mathbb{K}$.
- **($\mathbf{k}_2$)** We have $a(bc) = (ab)c$ for all $a, b, c \in \mathbb{L}$.
- **($\mathbf{l}_2$)** We have $a1_{\mathbb{L}} = 1_{\mathbb{L}}a = a$ for all $a \in \mathbb{L}$.
- **($\mathbf{m}_2$)** We have $a0_{\mathbb{L}} = 0_{\mathbb{L}}a = 0_{\mathbb{L}}$ for all $a \in \mathbb{L}$.
- **($\mathbf{n}_2$)** We have $a(b+c) = ab + ac$ and $(a+b)c = ac + bc$ for all $a, b, c \in \mathbb{L}$.
- **($\mathbf{o}_2$)** We have $\lambda(ab) = (\lambda a) \cdot b = a \cdot (\lambda b)$ for all $\lambda \in \mathbb{K}$ and $a, b \in \mathbb{L}$.

Now, our set V is endowed with an addition $+$, a scaling map $\cdot : \mathbb{K} \times V \to V$ (defined by (3)) and a zero vector 0_V. Our goal is to show that V is a $\mathbb{K}$-module (when equipped with this addition, this scaling map and this zero vector). In other words, our goal is to show that it satisfies the module axioms. In other words, our goal is to show that the following ten statements hold:

- **($\mathbf{a}_3$)** We have $a + b = b + a$ for all $a, b \in V$.
- **($\mathbf{b}_3$)** We have $a + (b+c) = (a+b) + c$ for all $a, b, c \in V$.
- **($\mathbf{c}_3$)** We have $a + 0_V = 0_V + a = a$ for all $a \in V$.
- **($\mathbf{d}_3$)** Each $a \in V$ has an additive inverse (i.e., there is an $a' \in V$ such that $a + a' = a' + a = 0_V$).
- **($\mathbf{e}_3$)** We have $\lambda(a+b) = \lambda a + \lambda b$ for all $\lambda \in \mathbb{K}$ and $a, b \in V$.
- **($\mathbf{f}_3$)** We have $(\lambda + \mu)a = \lambda a + \mu a$ for all $\lambda, \mu \in \mathbb{K}$ and $a \in V$.
- **($\mathbf{g}_3$)** We have $0_{\mathbb{K}}a = 0_V$ for all $a \in V$.
- **($\mathbf{h}_3$)** We have $(\lambda\mu)a = \lambda(\mu a)$ for all $\lambda, \mu \in \mathbb{K}$ and $a \in V$.
- **($\mathbf{i}_3$)** We have $1_{\mathbb{K}}a = a$ for all $a \in V$.
- **($\mathbf{j}_3$)** We have $\lambda \cdot 0_V = 0_V$ for all $\lambda \in \mathbb{K}$.

So it remains to prove these ten statements **($\mathbf{a}_3$)**, **($\mathbf{b}_3$)**, ..., **($\mathbf{j}_3$)**. Let us do so now.

The four statements **($\mathbf{a}_3$)**, **($\mathbf{b}_3$)**, **($\mathbf{c}_3$)** and **($\mathbf{d}_3$)** are literally identical with the four statements **($\mathbf{a}_1$)**, **($\mathbf{b}_1$)**, **($\mathbf{c}_1$)** and **($\mathbf{d}_1$)**, and therefore hold (since we know that the latter four statements hold). Hence, it remains to prove the other six statements.

[*Proof of statement (e_3):* Let $\lambda \in \mathbb{K}$ and $a, b \in V$. We must prove that $\lambda(a+b) = \lambda a + \lambda b$.

Applying (3) to $v = a$, we obtain $\lambda \cdot a = (\lambda \cdot 1_{\mathbb{L}}) \cdot a$. Applying (3) to $v = b$, we obtain $\lambda \cdot b = (\lambda \cdot 1_{\mathbb{L}}) \cdot b$. Applying (3) to $v = a + b$, we obtain

$$\lambda \cdot (a+b) = (\lambda \cdot 1_{\mathbb{L}}) \cdot (a+b) = (\lambda \cdot 1_{\mathbb{L}}) \cdot a + (\lambda \cdot 1_{\mathbb{L}}) \cdot b$$

(by statement **($\mathbf{e}_1$)**, applied to $\lambda \cdot 1_{\mathbb{L}}$ instead of λ). Comparing this with

$$\underbrace{\lambda a}_{\substack{=\lambda \cdot a \\ =(\lambda \cdot 1_{\mathbb{L}}) \cdot a}} + \underbrace{\lambda b}_{\substack{=\lambda \cdot b \\ =(\lambda \cdot 1_{\mathbb{L}}) \cdot b}} = (\lambda \cdot 1_{\mathbb{L}}) \cdot a + (\lambda \cdot 1_{\mathbb{L}}) \cdot b,$$

we obtain $\lambda \cdot (a+b) = \lambda a + \lambda b$. Thus, $\lambda (a+b) = \lambda \cdot (a+b) = \lambda a + \lambda b$. This proves statement **(e$_3$)**.]

[*Proof of statement (f$_3$):* Let $\lambda, \mu \in \mathbb{K}$ and $a \in V$. We must prove that $(\lambda + \mu) a = \lambda a + \mu a$.

Applying (3) to $v = a$, we obtain $\lambda \cdot a = (\lambda \cdot 1_{\mathbb{L}}) \cdot a$. Applying (3) to μ and a instead of λ and v, we obtain $\mu \cdot a = (\mu \cdot 1_{\mathbb{L}}) \cdot a$. Applying (3) to $\lambda + \mu$ and a instead of λ and v, we obtain $(\lambda + \mu) \cdot a = ((\lambda + \mu) \cdot 1_{\mathbb{L}}) \cdot a$. But statement **(f$_2$)** (applied to $1_{\mathbb{L}}$ instead of a) yields $(\lambda + \mu) \cdot 1_{\mathbb{L}} = \lambda \cdot 1_{\mathbb{L}} + \mu \cdot 1_{\mathbb{L}}$. Hence,

$$\begin{aligned}(\lambda + \mu) a &= (\lambda + \mu) \cdot a = \underbrace{((\lambda + \mu) \cdot 1_{\mathbb{L}})}_{=\lambda \cdot 1_{\mathbb{L}} + \mu \cdot 1_{\mathbb{L}}} \cdot a = (\lambda \cdot 1_{\mathbb{L}} + \mu \cdot 1_{\mathbb{L}}) \cdot a \\ &= (\lambda \cdot 1_{\mathbb{L}}) \cdot a + (\mu \cdot 1_{\mathbb{L}}) \cdot a\end{aligned}$$

(by statement **(f$_1$)**, applied to $\lambda \cdot 1_{\mathbb{L}}$ and $\mu \cdot 1_{\mathbb{L}}$ instead of λ and μ). Comparing this with

$$\underbrace{\lambda a}_{\substack{=\lambda \cdot a \\ =(\lambda \cdot 1_{\mathbb{L}}) \cdot a}} + \underbrace{\mu a}_{\substack{=\mu \cdot a \\ =(\mu \cdot 1_{\mathbb{L}}) \cdot a}} = (\lambda \cdot 1_{\mathbb{L}}) \cdot a + (\mu \cdot 1_{\mathbb{L}}) \cdot a,$$

we obtain $(\lambda + \mu) a = \lambda a + \mu a$. This proves statement **(f$_3$)**.]

[*Proof of statement (g$_3$):* Let $a \in V$. We must prove that $0_{\mathbb{K}} a = 0_V$.

Statement **(g$_2$)** (applied to $1_{\mathbb{L}}$ instead of a) yields $0_{\mathbb{K}} \cdot 1_{\mathbb{L}} = 0_{\mathbb{L}}$. But (3) (applied to $\lambda = 0_{\mathbb{K}}$ and $v = a$) yields $0_{\mathbb{K}} \cdot a = \underbrace{(0_{\mathbb{K}} \cdot 1_{\mathbb{L}})}_{=0_{\mathbb{L}}} \cdot a = 0_{\mathbb{L}} \cdot a = 0_V$ (by statement **(g$_1$)**). This proves statement **(g$_3$)**.]

[*Proof of statement (h$_3$):* Let $\lambda, \mu \in \mathbb{K}$ and $a \in V$. We must prove that $(\lambda \mu) a = \lambda (\mu a)$.

First, we shall show that

$$(\lambda \mu) \cdot 1_{\mathbb{L}} = (\lambda \cdot 1_{\mathbb{L}}) \cdot (\mu \cdot 1_{\mathbb{L}}). \qquad (15)$$

Indeed, statement **(o$_2$)** (applied to μ, $\lambda \cdot 1_{\mathbb{L}}$ and $1_{\mathbb{L}}$ instead of λ, a and b) yields $\mu ((\lambda \cdot 1_{\mathbb{L}}) 1_{\mathbb{L}}) = (\mu (\lambda \cdot 1_{\mathbb{L}})) \cdot 1_{\mathbb{L}} = (\lambda \cdot 1_{\mathbb{L}}) \cdot (\mu \cdot 1_{\mathbb{L}})$. But statement **(l$_2$)** (applied to $\lambda \cdot 1_{\mathbb{L}}$ instead of a) yields $(\lambda \cdot 1_{\mathbb{L}}) 1_{\mathbb{L}} = 1_{\mathbb{L}} (\lambda \cdot 1_{\mathbb{L}}) = \lambda \cdot 1_{\mathbb{L}}$. Hence, $\mu \underbrace{((\lambda \cdot 1_{\mathbb{L}}) 1_{\mathbb{L}})}_{=\lambda \cdot 1_{\mathbb{L}}} = \mu (\lambda \cdot 1_{\mathbb{L}})$. Thus,

$$\mu (\lambda \cdot 1_{\mathbb{L}}) = \mu ((\lambda \cdot 1_{\mathbb{L}}) 1_{\mathbb{L}}) = (\lambda \cdot 1_{\mathbb{L}}) \cdot (\mu \cdot 1_{\mathbb{L}}).$$

But statement **(h$_2$)** (applied to μ, λ and $1_{\mathbb{L}}$ instead of λ, μ and a) yields $(\mu \lambda) \cdot 1_{\mathbb{L}} = \mu (\lambda \cdot 1_{\mathbb{L}}) = (\lambda \cdot 1_{\mathbb{L}}) \cdot (\mu \cdot 1_{\mathbb{L}})$. However, $\lambda \mu = \mu \lambda$ (since $\mathbb{L}$ is commutative). Thus,

$$\underbrace{(\lambda \mu)}_{=\mu \lambda} \cdot 1_{\mathbb{L}} = (\mu \lambda) \cdot 1_{\mathbb{L}} = (\lambda \cdot 1_{\mathbb{L}}) \cdot (\mu \cdot 1_{\mathbb{L}}).$$

Thus, (15) is proven.

Now, (3) (applied to $\lambda \mu$ and a instead of λ and v) yields

$$\begin{aligned}(\lambda \mu) \cdot a &= \underbrace{((\lambda \mu) \cdot 1_{\mathbb{L}})}_{\substack{=(\lambda \cdot 1_{\mathbb{L}}) \cdot (\mu \cdot 1_{\mathbb{L}}) \\ \text{(by (15))}}} \cdot a = ((\lambda \cdot 1_{\mathbb{L}}) \cdot (\mu \cdot 1_{\mathbb{L}})) \cdot a \\ &= (\lambda \cdot 1_{\mathbb{L}}) \cdot ((\mu \cdot 1_{\mathbb{L}}) \cdot a) \qquad (16)\end{aligned}$$

(by statement **(h$_1$)**, applied to $\lambda \cdot 1_{\mathbb{L}}$ and $\mu \cdot 1_{\mathbb{L}}$ instead of λ and μ).

But (3) (applied to $v = \mu a$) yields

$$\lambda \cdot (\mu a) = (\lambda \cdot 1_{\mathbb{L}}) \cdot \underbrace{(\mu a)}_{\substack{=\mu \cdot a \\ =(\mu \cdot 1_{\mathbb{L}}) \cdot a \\ \text{(by (3), applied to } \mu \\ \text{instead of } \lambda)}} = (\lambda \cdot 1_{\mathbb{L}}) \cdot ((\mu \cdot 1_{\mathbb{L}}) \cdot a) .$$

Comparing this with (16), we obtain $(\lambda\mu) \cdot a = \lambda \cdot (\mu a) = \lambda (\mu a)$. Thus, $(\lambda\mu) a = (\lambda\mu) \cdot a = \lambda (\mu a)$. This proves statement **(h$_3$)**.]

[*Proof of statement (i$_3$):* Let $a \in V$. We must prove that $1_{\mathbb{K}} a = a$.

Statement **(i$_2$)** (applied to $1_{\mathbb{L}}$ instead of a) yields $1_{\mathbb{K}} \cdot 1_{\mathbb{L}} = 1_{\mathbb{L}}$. But (3) (applied to $\lambda = 1_{\mathbb{K}}$) yields $1_{\mathbb{K}} \cdot a = \underbrace{(1_{\mathbb{K}} \cdot 1_{\mathbb{L}})}_{=1_{\mathbb{L}}} \cdot a = 1_{\mathbb{L}} \cdot a = a$ (by statement **(i$_1$)**). This proves statement **(i$_3$)**.]

[*Proof of statement (j$_3$):* Let $\lambda \in \mathbb{K}$. We must prove that $\lambda \cdot 0_V = 0_V$.

But (3) (applied to $v = 0_V$) yields $\lambda \cdot 0_V = (\lambda \cdot 1_{\mathbb{L}}) \cdot 0_V = 0_V$ (by statement **(j$_1$)**, applied to $\lambda \cdot 1_{\mathbb{L}}$ instead of λ). This proves statement **(j$_3$)**.]

We thus have proven the ten statements **(a$_3$)**, **(b$_3$)**, ..., **(j$_3$)**. These ten statements show that V satisfies the module axioms that are required to ensure that V is a $\mathbb{K}$-module. Hence, V is a $\mathbb{K}$-module. This proves Proposition 2.4.1. □

Proof of Proposition 2.4.2. Proposition 2.4.1 shows that the set V (equipped with its addition $+$, its zero vector 0_V and the scaling $\cdot : \mathbb{K} \times V \to V$ defined by (3)) is a $\mathbb{K}$-module. Furthermore, the set V (equipped with its addition $+$, its multiplication $\cdot$, its zero 0_V and its unity 1_V) is a ring.

Now, our set V is endowed with an addition $+$, a multiplication $\cdot$, a scaling map $\cdot : \mathbb{K} \times V \to V$ (defined by (3)), a zero 0_V and a unity 1_V. Our goal is to show that V is a $\mathbb{K}$-algebra (when equipped with this addition, this multiplication, this scaling map, this zero and this unity). In other words, our goal is to show that it satisfies the ring axioms, the module axioms and the "Scale-invariance of multiplication" axiom (because this is precisely what is needed to ensure that V is a $\mathbb{K}$-algebra, according to Definition 4.1.2). But it clearly satisfies the ring axioms (since V is a ring) and the module axioms (since V is a $\mathbb{K}$-module). Hence, it suffices to prove that it satisfies the "Scale-invariance of multiplication" axiom. In other words, we must prove the following statement:

- **(k$_3$)** We have $\lambda (ab) = (\lambda a) \cdot b = a \cdot (\lambda b)$ for all $\lambda \in \mathbb{K}$ and $a, b \in V$.

Before we prove this statement, let us recall something: We know that V is an $\mathbb{L}$-algebra, and therefore satisfies the "Scale-invariance of multiplication" axiom. In other words, the following statement holds:

- **(k$_1$)** We have $\lambda (ab) = (\lambda a) \cdot b = a \cdot (\lambda b)$ for all $\lambda \in \mathbb{L}$ and $a, b \in V$.

Now, we can prove the statement **(k$_3$)**:

[*Proof of statement (k$_3$):* Let $\lambda \in \mathbb{K}$ and $a, b \in V$. We must prove that $\lambda (ab) = (\lambda a) \cdot b = a \cdot (\lambda b)$.

We have $\lambda \cdot 1_{\mathbb{L}} \in \mathbb{L}$. Thus, statement **(k$_1$)** (applied to $\lambda \cdot 1_{\mathbb{L}}$ instead of λ) yields $(\lambda \cdot 1_{\mathbb{L}}) (ab) = ((\lambda \cdot 1_{\mathbb{L}}) a) \cdot b = a \cdot ((\lambda \cdot 1_{\mathbb{L}}) b)$.

Applying (3) to $v = a$, we obtain $\lambda \cdot a = (\lambda \cdot 1_{\mathbb{L}}) \cdot a = (\lambda \cdot 1_{\mathbb{L}})\, a$. Applying (3) to $v = b$, we obtain $\lambda \cdot b = (\lambda \cdot 1_{\mathbb{L}}) \cdot b = (\lambda \cdot 1_{\mathbb{L}})\, b$. Applying (3) to $v = ab$, we obtain

$$\lambda \cdot (ab) = (\lambda \cdot 1_{\mathbb{L}}) \cdot (ab) = \underbrace{((\lambda \cdot 1_{\mathbb{L}})\, a)}_{\substack{=\lambda a \\ (\text{since } \lambda a = \lambda \cdot a = (\lambda \cdot 1_{\mathbb{L}}) a)}} \cdot b = (\lambda a) \cdot b.$$

Also,

$$\lambda \cdot (ab) = (\lambda \cdot 1_{\mathbb{L}}) \cdot (ab) = a \cdot \underbrace{((\lambda \cdot 1_{\mathbb{L}})\, b)}_{\substack{=\lambda b \\ (\text{since } \lambda b = \lambda \cdot b = (\lambda \cdot 1_{\mathbb{L}}) b)}} = a \cdot (\lambda b).$$

Combining these two equalities, we find $\lambda \cdot (ab) = (\lambda a) \cdot b = a \cdot (\lambda b)$. In other words, $\lambda\,(ab) = (\lambda a) \cdot b = a \cdot (\lambda b)$. This proves statement **(k$_3$)**.]

So we have proven that statement **(k$_3$)** holds. In other words, V satisfies the "Scale-invariance of multiplication" axiom. Thus, altogether, we have shown that V satisfies all the ring axioms as well as all the module axioms and also the "Scale-invariance of multiplication" axiom. Thus, V is a $\mathbb{K}$-algebra (by Definition 4.1.2). This proves Proposition 2.4.2. □

4.2. Appendix 2: Factoring $x^{p^g} - x$, part II

If r, m and $\mathbb{K}$ are as in Lemma 2.9.2, then every irreducible divisor $\mathbf{a}$ of the polynomial in $x^{p^{mr}} - x$ in $\mathbb{K}[x]$ satisfies $\deg \mathbf{a} \mid r$ in $\mathbb{Z}$; this is what Lemma 2.9.2 stated. But a converse also holds:

> **Lemma 4.2.1.** Let r and m be positive integers. Let $\mathbb{K}$ be a finite $\mathbb{F}_p$-field of size p^m. Let $\mathbf{a} \in \mathbb{K}[x]$ be an irreducible polynomial such that $\deg \mathbf{a} \mid r$ in $\mathbb{Z}$. Then, $\mathbf{a} \mid x^{p^{mr}} - x$ in $\mathbb{K}[x]$.

Proof of Lemma 4.2.1. Let $n = \deg \mathbf{a}$. Thus, $\mathbf{a}$ is a polynomial of degree n. Theorem 2.1.2 **(c)** (applied to $\mathbb{F} = \mathbb{K}$) yields that $\mathbb{K}[x] / \mathbf{a}$ is a field. Let $\mathbb{F}$ denote this field.

We have $n = \deg \mathbf{a} \mid r$ in $\mathbb{Z}$. Hence, there exists an integer u such that $r = nu$. Consider this u. Thus, $nu = r$. Also, it is easy to see that $u \in \mathbb{N}$ [25].

The following observations can be proven exactly as they were proven in our proof of Lemma 2.9.2 above:

- The number mn is a positive integer.
- The ring $\mathbb{K}$ is a field and is commutative.
- We have
$$([f]_{\mathbf{a}})^k = \left[f^k\right]_{\mathbf{a}} \qquad \text{for each } f \in \mathbb{K}[x] \text{ and each } k \in \mathbb{N}. \tag{17}$$
(Recall Convention 2.1.1 in order to make sense of this.)

[25] *Proof.* We have $n = \deg \mathbf{a} > 0$ (since $\mathbf{a}$ is irreducible). But we have $nu = r > 0$ (since r is positive). We can divide this inequality by n (since $n > 0$), and thus find $u > 0$. Hence, $u \in \mathbb{N}$ (since u is an integer).

- The ring $\mathbb{F}$ is an $\mathbb{F}_p$-field and has size p^{mn}.

Thus, $\mathbb{F}$ is finite. Now, $[x]_{\mathbf{a}} \in \mathbb{K}[x] / \mathbf{a} = \mathbb{F}$. Hence, Corollary 2.6.6 (applied to mn, $[x]_{\mathbf{a}}$ and u instead of n, a and r) yields $\left([x]_{\mathbf{a}}\right)^{p^{mnu}} = [x]_{\mathbf{a}}$. In view of $m \underbrace{nu}_{=r} = mr$, this rewrites as $\left([x]_{\mathbf{a}}\right)^{p^{mr}} = [x]_{\mathbf{a}}$. Comparing this with

$$\left([x]_{\mathbf{a}}\right)^{p^{mr}} = \left[x^{p^{mr}}\right]_{\mathbf{a}} \qquad \text{(by (17), applied to } f = x \text{ and } k = p^{mr}\text{)},$$

we obtain $\left[x^{p^{mr}}\right]_{\mathbf{a}} = [x]_{\mathbf{a}}$. In other words, $x^{p^{mr}} \equiv x \operatorname{mod} \mathbf{a}$ in $\mathbb{K}[x]$. In other words, $\mathbf{a} \mid x^{p^{mr}} - x$ in $\mathbb{K}[x]$. This proves Lemma 4.2.1. □

Lemma 2.9.2 and Lemma 4.2.1 can be merged into a single theorem, which gives an "explicit" factorization of $x^{p^{mr}} - x$ into irreducible polynomials[26]:

Theorem 4.2.2. Let r and m be positive integers. Let $\mathbb{K}$ be a finite $\mathbb{F}_p$-field of size p^m. Then,

$$x^{p^{mr}} - x = \prod_{\substack{\mathbf{a} \in \mathbb{K}[x] \text{ is} \\ \text{irreducible} \\ \text{and monic;} \\ \deg \mathbf{a} \mid r}} \mathbf{a}.$$

Our proof of Theorem 4.2.2 relies on the following fact about irreducible polynomials:

Proposition 4.2.3. Let $\mathbb{K}$ be a field. Let $\mathbf{p} \in \mathbb{K}[x]$ be an irreducible polynomial. Let $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_k \in \mathbb{K}[x]$ be polynomials such that $\mathbf{p} \mid \mathbf{a}_1 \mathbf{a}_2 \cdots \mathbf{a}_k$. Then, $\mathbf{p} \mid \mathbf{a}_i$ for some $i \in \{1, 2, \ldots, k\}$.

Proof of Proposition 4.2.3. Proposition 4.2.3 is the analogue of [Grinbe19a, Proposition 2.13.7] for polynomials (in $\mathbb{K}[x]$) instead of integers. It can be proven in the same way as the latter result was proven (but with the usual changes that are required to turn an argument about integers into the analogous argument about polynomials).

Alternatively, we can prove Proposition 4.2.3 using Theorem 2.1.2 as follows: Assume the contrary. Thus, we don't have ($\mathbf{p} \mid \mathbf{a}_i$ for some $i \in \{1, 2, \ldots, k\}$). In other words, we have

$$\mathbf{p} \nmid \mathbf{a}_i \qquad \text{for each } i \in \{1, 2, \ldots, k\}. \tag{18}$$

The polynomial $\mathbf{p}$ is irreducible and thus non-constant. Hence, $\deg \mathbf{p} > 0$.

Let $n = \deg \mathbf{p}$. Thus, $\mathbf{p}$ is a polynomial of degree n. Theorem 2.1.2 **(c)** (applied to $\mathbb{F} = \mathbb{K}$ and $\mathbf{a} = \mathbf{p}$) shows that $\mathbb{K}[x] / \mathbf{p}$ is a field. Recall Convention 2.1.1. The definition of the

[26] "Explicit" only in the sense that the irreducible polynomials of any given degree over $\mathbb{K}$ can be found.

multiplication on $\mathbb{K}[x]/\mathbf{p}$ shows that $[\mathbf{u}]_{\mathbf{p}}[\mathbf{v}]_{\mathbf{p}} = [\mathbf{uv}]_{\mathbf{p}}$ for any $\mathbf{u}, \mathbf{v} \in \mathbb{K}[x]$. Hence, a straightforward induction on j shows that

$$[\mathbf{u}_1]_{\mathbf{p}}[\mathbf{u}_2]_{\mathbf{p}} \cdots [\mathbf{u}_j]_{\mathbf{p}} = [\mathbf{u}_1\mathbf{u}_2 \cdots \mathbf{u}_j]_{\mathbf{p}}$$

for every $j \in \mathbb{N}$ and every $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_j \in \mathbb{K}[x]$. Applying this to $j = k$ and $\mathbf{u}_i = \mathbf{a}_i$, we conclude that

$$[\mathbf{a}_1]_{\mathbf{p}}[\mathbf{a}_2]_{\mathbf{p}} \cdots [\mathbf{a}_k]_{\mathbf{p}} = [\mathbf{a}_1\mathbf{a}_2 \cdots \mathbf{a}_k]_{\mathbf{p}} = [0]_{\mathbf{p}}$$

(since $\mathbf{a}_1\mathbf{a}_2 \cdots \mathbf{a}_k \equiv 0 \bmod \mathbf{p}$ (because $\mathbf{p} \mid \mathbf{a}_1\mathbf{a}_2 \cdots \mathbf{a}_k$)).

But $\mathbb{K}[x]/\mathbf{p}$ is a field, and thus is a commutative skew field. Hence, every nonzero element of $\mathbb{K}[x]/\mathbf{p}$ is invertible (since $\mathbb{K}[x]/\mathbf{p}$ is a skew field).

Now, let $i \in \{1, 2, \ldots, k\}$. Then, $\mathbf{p} \nmid \mathbf{a}_i$ (by (18)). In other words, $\mathbf{a}_i \not\equiv 0 \bmod \mathbf{p}$. In other words, $[\mathbf{a}_i]_{\mathbf{p}} \neq [0]_{\mathbf{p}}$. The element $[\mathbf{a}_i]_{\mathbf{p}}$ of $\mathbb{K}[x]/\mathbf{p}$ is nonzero (since $[\mathbf{a}_i]_{\mathbf{p}} \neq [0]_{\mathbf{p}} = 0_{\mathbb{K}[x]/\mathbf{p}}$) and thus invertible (since every nonzero element of $\mathbb{K}[x]/\mathbf{p}$ is invertible). In other words, there exists a multiplicative inverse of $[\mathbf{a}_i]_{\mathbf{p}}$ in $\mathbb{K}[x]/\mathbf{p}$. In other words, there exists some $\beta_i \in \mathbb{K}[x]/\mathbf{p}$ such that $[\mathbf{a}_i]_{\mathbf{p}}\beta_i = \beta_i[\mathbf{a}_i]_{\mathbf{p}} = 1_{\mathbb{K}[x]/\mathbf{p}}$. Consider this β_i.

Forget that we fixed i. Thus, for each $i \in \{1, 2, \ldots, k\}$, we have constructed some $\beta_i \in \mathbb{K}[x]/\mathbf{p}$ such that

$$[\mathbf{a}_i]_{\mathbf{p}}\beta_i = \beta_i[\mathbf{a}_i]_{\mathbf{p}} = 1_{\mathbb{K}[x]/\mathbf{p}}. \tag{19}$$

But the ring $\mathbb{K}[x]/\mathbf{p}$ is commutative (since $\mathbb{K}[x]$ is commutative). Thus,

$$\prod_{i=1}^{k}\left([\mathbf{a}_i]_{\mathbf{p}}\beta_i\right) = \underbrace{\left(\prod_{i=1}^{k}[\mathbf{a}_i]_{\mathbf{p}}\right)}_{\substack{=[\mathbf{a}_1]_{\mathbf{p}}[\mathbf{a}_2]_{\mathbf{p}}\cdots[\mathbf{a}_k]_{\mathbf{p}} \\ =[0]_{\mathbf{p}}=0_{\mathbb{K}[x]/\mathbf{p}}}}\left(\prod_{i=1}^{k}\beta_i\right) = 0_{\mathbb{K}[x]/\mathbf{p}}\left(\prod_{i=1}^{k}\beta_i\right) = 0_{\mathbb{K}[x]/\mathbf{p}} = [0]_{\mathbf{p}}.$$

Hence,

$$[0]_{\mathbf{p}} = \prod_{i=1}^{k}\underbrace{\left([\mathbf{a}_i]_{\mathbf{p}}\beta_i\right)}_{\substack{=1_{\mathbb{K}[x]/\mathbf{p}} \\ \text{(by (19))}}} = \prod_{i=1}^{k}1_{\mathbb{K}[x]/\mathbf{p}} = 1_{\mathbb{K}[x]/\mathbf{p}} = [1]_{\mathbf{p}}.$$

Thus, $[1]_{\mathbf{p}} = [0]_{\mathbf{p}}$. In other words, $1 \equiv 0 \bmod \mathbf{p}$. In other words, $\mathbf{p} \mid 1$ in $\mathbb{K}[x]$. Hence, there exists some $\mathbf{c} \in \mathbb{K}[x]$ such that $1 = \mathbf{pc}$. Consider this $\mathbf{c}$. We have $\mathbf{c} \neq 0$ (since $\mathbf{pc} = 1 \neq 0$) and thus $\deg \mathbf{c} \geq 0$. But $\deg 1 = 0$, so that $0 = \deg \underbrace{1}_{=\mathbf{pc}} = \deg(\mathbf{pc}) = \underbrace{\deg \mathbf{p}}_{>0} + \underbrace{\deg \mathbf{c}}_{\geq 0} > 0$. This is absurd. This contradiction shows that our assumption was false. Hence, Proposition 4.2.3 is proven. □

Corollary 4.2.4. Let $\mathbb{K}$ be a field. Let $\mathbf{p} \in \mathbb{K}[x]$ be a monic irreducible polynomial. Let $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_k \in \mathbb{K}[x]$ be monic irreducible polynomials such that $\mathbf{p} \mid \mathbf{a}_1\mathbf{a}_2 \cdots \mathbf{a}_k$. Then, $\mathbf{p} = \mathbf{a}_i$ for some $i \in \{1, 2, \ldots, k\}$.

Proof of Corollary 4.2.4. Proposition 4.2.3 shows that $\mathbf{p} \mid \mathbf{a}_i$ for some $i \in \{1, 2, \ldots, k\}$. Consider this i, and denote it by j. Thus, j is an element of $\{1, 2, \ldots, k\}$ and satisfies

$\mathbf{p} \mid \mathbf{a}_j$. From $\mathbf{p} \mid \mathbf{a}_j$, we conclude that there exists a polynomial $\mathbf{u} \in \mathbb{K}[x]$ such that $\mathbf{a}_j = \mathbf{pu}$. Consider this $\mathbf{u}$.

The polynomial $\mathbf{p}$ is irreducible and thus non-constant. In other words, $\deg \mathbf{p} > 0$.

The polynomial $\mathbf{a}_j$ is monic (since all k polynomials $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_k$ are monic).

The polynomial $\mathbf{a}_j$ is irreducible (since all k polynomials $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_k$ are irreducible). In other words, $\deg(\mathbf{a}_j) > 0$ and there exist no two polynomials $\mathbf{b}, \mathbf{c} \in \mathbb{K}[x]$ with $\mathbf{a}_j = \mathbf{bc}$ and $\deg \mathbf{b} > 0$ and $\deg \mathbf{c} > 0$ (because this is how "irreducible" is defined).

Assume (for the sake of contradiction) that $\deg \mathbf{u} > 0$. Then, the polynomials $\mathbf{p}, \mathbf{u} \in \mathbb{K}[x]$ satisfy $\mathbf{a}_j = \mathbf{pu}$ and $\deg \mathbf{p} > 0$ and $\deg \mathbf{u} > 0$. Hence, there exist two polynomials $\mathbf{b}, \mathbf{c} \in \mathbb{K}[x]$ with $\mathbf{a}_j = \mathbf{bc}$ and $\deg \mathbf{b} > 0$ and $\deg \mathbf{c} > 0$ (namely, $\mathbf{b} = \mathbf{p}$ and $\mathbf{c} = \mathbf{u}$). This contradicts the fact that there exist no two polynomials $\mathbf{b}, \mathbf{c} \in \mathbb{K}[x]$ with $\mathbf{a}_j = \mathbf{bc}$ and $\deg \mathbf{b} > 0$ and $\deg \mathbf{c} > 0$.

This contradiction shows that our assumption (that $\deg \mathbf{u} > 0$) was false. Hence, $\deg \mathbf{u} \leq 0$. Thus, the polynomial $\mathbf{u}$ is constant. In other words, $\mathbf{u} = \lambda$ for some $\lambda \in \mathbb{K}$. Consider this λ. Now, $\mathbf{a}_j = \mathbf{p} \underbrace{\mathbf{u}}_{=\lambda} = \mathbf{p}\lambda = \lambda\mathbf{p}$, so that $\lambda\mathbf{p} = \mathbf{a}_j \neq 0$ (because $\mathbf{a}_j$ is irreducible) and thus $\lambda \neq 0$.

The leading coefficient of the polynomial $\mathbf{p}$ is 1 (since $\mathbf{p}$ is monic). Hence, the leading coefficient of the polynomial $\lambda\mathbf{p}$ is $\lambda \cdot 1 = \lambda$. In other words, the leading coefficient of the polynomial $\mathbf{a}_j$ is λ (since $\mathbf{a}_j = \lambda\mathbf{p}$). Thus,

$$\lambda = \left(\text{the leading term of the polynomial } \mathbf{a}_j\right) = 1$$

(since the polynomial $\mathbf{a}_j$ is monic). Hence, $\mathbf{a}_j = \underbrace{\lambda}_{=1} \mathbf{p} = \mathbf{p}$, so that $\mathbf{p} = \mathbf{a}_j$. Thus, $\mathbf{p} = \mathbf{a}_i$ for some $i \in \{1, 2, \ldots, k\}$ (namely, for $i = j$). This proves Corollary 4.2.4. □

Proof of Theorem 4.2.2. Recall that m and r are positive integers. Hence, their product mr is a positive integer. Thus, Lemma 2.9.1 (applied to $g = mr$) shows that the polynomial $x^{p^{mr}} - x \in \mathbb{K}[x]$ can be written in the form $x^{p^{mr}} - x = \mathbf{u}_1\mathbf{u}_2 \cdots \mathbf{u}_k$, where $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k \in \mathbb{K}[x]$ are **distinct** monic irreducible polynomials. Consider these $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k$.

Let D be the set of all monic irreducible polynomials $\mathbf{a} \in \mathbb{K}[x]$ that satisfy $\deg \mathbf{a} \mid r$. For each $i \in \{1, 2, \ldots, k\}$, we have

$$\mathbf{u}_i \in D. \tag{20}$$

[*Proof of (20):* Let $i \in \{1, 2, \ldots, k\}$. Then, $\mathbf{u}_i$ is a monic irreducible polynomial (since $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k$ are monic irreducible polynomials). Moreover, $\mathbf{u}_i \mid \mathbf{u}_1\mathbf{u}_2 \cdots \mathbf{u}_k$ (since $\mathbf{u}_i$ is a factor in the product $\mathbf{u}_1\mathbf{u}_2 \cdots \mathbf{u}_k$). This rewrites as $\mathbf{u}_i \mid x^{p^{mr}} - x$ (since $x^{p^{mr}} - x = \mathbf{u}_1\mathbf{u}_2 \cdots \mathbf{u}_k$). Hence, Lemma 2.9.2 (applied to $\mathbf{a} = \mathbf{u}_i$) shows that $\deg(\mathbf{u}_i) \mid r$ in $\mathbb{Z}$. Thus, $\mathbf{u}_i$ is a monic irreducible polynomial in $\mathbb{K}[x]$ that satisfies $\deg(\mathbf{u}_i) \mid r$ in $\mathbb{Z}$. In other words, $\mathbf{u}_i$ is a monic irreducible polynomial $\mathbf{a} \in \mathbb{K}[x]$

that satisfies $\deg \mathbf{a} \mid r$. In other words, $\mathbf{u}_i \in D$ (since D is the set of all monic irreducible polynomials $\mathbf{a} \in \mathbb{K}[x]$ that satisfy $\deg \mathbf{a} \mid r$). This proves (20).]

Thus, we have shown that we have $\mathbf{u}_i \in D$ for each $i \in \{1, 2, \ldots, k\}$. Hence, the map

$$\{1, 2, \ldots, k\} \to D, \qquad i \mapsto \mathbf{u}_i$$

is well-defined. Denote this map by α. This map α is injective[27] and surjective[28]. Hence, this map α is bijective. Thus, α is a bijection from $\{1, 2, \ldots, k\}$ to D.

Now,

$$\begin{aligned} x^{p^{mr}} - x &= \mathbf{u}_1 \mathbf{u}_2 \cdots \mathbf{u}_k = \prod_{i \in \{1,2,\ldots,k\}} \underbrace{\mathbf{u}_i}_{\substack{=\alpha(i) \\ \text{(since } \alpha(i) = \mathbf{u}_i \\ \text{(by the definition of } \alpha\text{))}}} = \prod_{i \in \{1,2,\ldots,k\}} \alpha(i) = \prod_{\mathbf{a} \in D} \mathbf{a} \\ &\qquad \left(\begin{array}{c} \text{here, we have substituted } \mathbf{a} \text{ for } \alpha(i) \text{ in the product,} \\ \text{since the map } \alpha : \{1, 2, \ldots, k\} \to D \text{ is a bijection} \end{array} \right) \\ &= \prod_{\substack{\mathbf{a} \text{ is a monic} \\ \text{irreducible polynomial in } \mathbb{K}[x] \\ \text{that satisfies } \deg \mathbf{a} \mid r}} \mathbf{a} \\ &\qquad \left(\begin{array}{c} \text{since } D \text{ is the set of all monic irreducible} \\ \text{polynomials } \mathbf{a} \in \mathbb{K}[x] \text{ that satisfy } \deg \mathbf{a} \mid r \end{array} \right) \\ &= \prod_{\substack{\mathbf{a} \in \mathbb{K}[x] \text{ is} \\ \text{irreducible} \\ \text{and monic;} \\ \deg \mathbf{a} \mid r}} \mathbf{a}. \end{aligned}$$

This proves Theorem 4.2.2. □

[27] *Proof.* Let i and j be two elements of $\{1, 2, \ldots, k\}$ such that $\alpha(i) = \alpha(j)$. We shall prove that $i = j$.

We have $\alpha(j) = \mathbf{u}_j$ (by the definition of α) and $\alpha(i) = \mathbf{u}_i$ (similarly). Thus, $\mathbf{u}_i = \alpha(i) = \alpha(j) = \mathbf{u}_j$. Hence, $i = j$ (since the polynomials $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_k$ are distinct).

Now, forget that we fixed i and j. We thus have shown that if i and j are two elements of $\{1, 2, \ldots, k\}$ such that $\alpha(i) = \alpha(j)$, then $i = j$. In other words, the map α is injective.

[28] *Proof.* Let $\mathbf{d} \in D$. Thus, $\mathbf{d}$ is a monic irreducible polynomial $\mathbf{a} \in \mathbb{K}[x]$ that satisfies $\deg \mathbf{a} \mid r$ (since D is the set of all monic irreducible polynomials $\mathbf{a} \in \mathbb{K}[x]$ that satisfy $\deg \mathbf{a} \mid r$). In other words, $\mathbf{d}$ is a monic irreducible polynomial in $\mathbb{K}[x]$ and satisfies $\deg \mathbf{d} \mid r$. Hence, Lemma 4.2.1 (applied to $\mathbf{a} = \mathbf{d}$) shows that $\mathbf{d} \mid x^{p^{mr}} - x$ in $\mathbb{K}[x]$. Thus, $\mathbf{d} \mid x^{p^{mr}} - x = \mathbf{u}_1 \mathbf{u}_2 \cdots \mathbf{u}_k$. Hence, Corollary 4.2.4 (applied to $\mathbf{p} = \mathbf{d}$ and $\mathbf{a}_i = \mathbf{u}_i$) shows that $\mathbf{d} = \mathbf{u}_i$ for some $i \in \{1, 2, \ldots, k\}$. Consider this i. The definition of α yields $\alpha(i) = \mathbf{u}_i$. Comparing this with $\mathbf{d} = \mathbf{u}_i$, we find $\mathbf{d} = \alpha\left(\underbrace{i}_{\in \{1,2,\ldots,k\}}\right) \in \alpha(\{1, 2, \ldots, k\})$.

Now, forget that we fixed $\mathbf{d}$. We thus have shown that $\mathbf{d} \in \alpha(\{1, 2, \ldots, k\})$ for each $\mathbf{d} \in D$. In other words, $D \subseteq \alpha(\{1, 2, \ldots, k\})$. In other words, the map α is surjective.

References

[Bourba72] Nicolas Bourbaki, *Elements of Mathematics: Commutative Algebra*, Hermann 1972.

[Bourba74] Nicolas Bourbaki, *Algebra I, Chapters 1-3*, Hermann 1974.
`https://archive.org/details/ElementsOfMathematics-AlgebraPart1/page/n0`

[ChaLoi21] Antoine Chambert-Loir, *(Mostly) Commutative Algebra*, 27 January 2021.
`https://webusers.imj-prg.fr/~antoine.chambert-loir/publications/teach/sv-commalg.pdf`

[ConradF] Keith Conrad, *Finite fields*, 4 February 2018.
`https://kconrad.math.uconn.edu/blurbs/galoistheory/finitefields.pdf`

[DumFoo04] David S. Dummit, Richard M. Foote, *Abstract Algebra*, 3rd edition, Wiley 2004.

[Escofi01] Jean-Pierre Escofier, *Galois Theory*, translated by Leila Schneps, Springer 2001.

[Goodma16] Frederick M. Goodman, *Algebra: Abstract and Concrete*, edition 2.6, 12 October 2016.
`https://homepage.divms.uiowa.edu/~goodman/algebrabook.dir/algebrabook.html`

[Grinbe18] Darij Grinberg, *Why the log and exp series are mutually inverse*, May 11, 2018.
`https://www.cip.ifi.lmu.de/~grinberg/t/17f/logexp.pdf`

[Grinbe19a] Darij Grinberg, *Introduction to Modern Algebra (UMN Spring 2019 Math 4281 notes)*, 31 May 2019.
`https://www.cip.ifi.lmu.de/~grinberg/t/19s/notes.pdf`
This document is still unfinished; numbering may change in the future. For a frozen version whose numbering matches the references used above, see
`https://github.com/darijgr/algebra19s/releases/tag/2019-05-31`

[Grinbe19b] Darij Grinberg, *UMN Spring 2019 Math 4281 midterm #3 solutions.*
`https://www.cip.ifi.lmu.de/~grinberg/t/19s/mt3s.pdf`

[HucNeu13] Sophie Huczynska, Max Neunhoffer, *Finite Fields*, 25 January 2013.
`http://www.math.rwth-aachen.de/~Max.Neunhoeffer/Teaching/ff2013/ff2013.pdf`

[Hunger03] Thomas W. Hungerford, *Algebra*, 12th printing, Springer 2003.

[Hunger14] Thomas W. Hungerford, *Abstract Algebra: An Introduction*, 3rd edition, Brooks/Cole 2014.

[Knapp16a] Anthony W. Knapp, *Basic Algebra*, digital 2nd edition 2016.
`https://www.math.stonybrook.edu/~aknapp/download.html`

[Lange18] Tanja Lange, *Finite Fields*, draft of a book chapter.
`https://www.hyperelliptic.org/tanja/teaching/CCI11/online-ff.pdf`

[LidNie97] Rudolf Lidl, Harald Niederreiter, *Finite fields*, 2nd edition, Cambridge University Press 1997.
`https://doi.org/10.1017/CBO9780511525926`

[Loehr11] Nicholas A. Loehr, *Bijective Combinatorics*, Chapman & Hall/CRC 2011.

[Milne18] James S. Milne, *Fields and Galois Theory*, version 4.60, September 2018.
`https://www.jmilne.org/math/CourseNotes/`

[MonAno14] Maria Monks, Anon1, *A proof of the existence of finite fields of every possible order*, Mathematical Gemstones blog, 2014.
`https://www.mathematicalgemstones.com/gemstones/sapphire/a-proof-of-the-existence-of-finite-fields-of-every-possible-order/`

[Murphy12] Timothy Murphy, *Finite Fields (Course MA346D, Part I)*, 31 January 2012.
`https://www.maths.tcd.ie/pub/Maths/Courseware/FiniteFields/GF.pdf`

[Stewar15] Ian Stewart, *Galois theory*, 4th edition, CRC Press 2015.
`http://matematicaeducativa.com/foro/download/file.php?id=1647`

[Walker87] Elbert A. Walker, *Introduction to Abstract Algebra*, Random House/Birkhauser, New York, 1987.