

2.6 The Binomial Theorem, the Frobenius Map, and Fermat's Little Theorem

In $\mathbb{F}_5$, compute $(1+2)^5$ and $1^5 + 2^5$. The first is $3^5 = 243$, and $243 = 48 \cdot 5 + 3$, so it is 3. The second is $1 + 32 = 33 = 6 \cdot 5 + 3$, so it is 3 as well. The rule “ $(x+y)^n = x^n + y^n$ ”, the classic error of school algebra, is a theorem when n is the characteristic p of the field. This section proves it, and deduces Fermat's little theorem from it with the rigidity of Section 2.5: a homomorphism of $\mathbb{F}_p$ to itself is the identity.

The tool is the binomial theorem. School proves it for numbers; we need it in an arbitrary commutative ring, with the binomial coefficients acting as integer multiples, and so we first set up finite sums in a ring.

2.6.1 Sums and powers in a commutative ring

Sets, Relations, and Cardinality, Chapter 2 defines finite sums, products and powers of real numbers by recursion (*Sets, Relations, and Cardinality*, Definition 2.3.1, *Sets, Relations, and Cardinality*, Definition 2.3.2, both from *Sets, Relations, and Cardinality*, Theorem 2.3.1). The definitions use nothing about $\mathbb{R}$ except an addition with a 0 and a multiplication with a 1. So, read on $\mathbb{N} = \omega$ through *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Corollary 1.7.3 (b), with $X = R$, they define in every commutative ring R :

- sums $\sum_{k=m}^n a_k$ of elements $a_k \in R$, with the empty sum 0, and the three remarks after *Sets, Relations, and Cardinality*, Definition 2.3.1: a sum depends only on the terms it adds (finite lists), **shifting the index**, and **splitting off the last term**, $\sum_{k=m}^{n+1} a_k = \sum_{k=m}^n a_k + a_{n+1}$ for $m \leq n+1$;
- powers $x^0 := 1$, $x^{n+1} := x^n x$ for $x \in R$ and $n \in \mathbb{N}$, with the laws of *Sets, Relations, and Cardinality*, Proposition 2.3.4 (a)–(c):

$$x^{m+n} = x^m x^n, \quad (x^m)^n = x^{mn}, \quad (xy)^n = x^n y^n.$$

The proofs of those laws in *Sets, Relations, and Cardinality* use only (F1)–(F7), (F9) and induction, so they run unchanged in R . We use this paragraph as a template and do not repeat it. (Chapter 1 proves the same power laws for every commutative ring as Proposition 1.1.3; we compare, and cite the template.) In particular $1^n = 1$ for every n , by induction: $1^0 = 1$ and $1^{n+1} = 1^n \cdot 1 = 1$.

The binomial theorem rearranges sums term by term, and the rules it needs are collected in the next lemma. The sums start at $k = 0$; by the definition, $\sum_{k=0}^0 a_k = 0 + a_0 = a_0$.

Lemma 2.6.1. Finite Sums in a Commutative Ring

Let R be a commutative ring, $n \in \mathbb{N}$, $c \in R$, and let $(a_k)_{k \in \mathbb{N}}$ and $(b_k)_{k \in \mathbb{N}}$ be sequences in R .

- $\sum_{k=0}^n (a_k + b_k) = \sum_{k=0}^n a_k + \sum_{k=0}^n b_k$.
- $c \sum_{k=0}^n a_k = \sum_{k=0}^n c a_k$.
- $\sum_{k=0}^n m \cdot a_k = m \cdot \sum_{k=0}^n a_k$ for every $m \in \mathbb{Z}$.
- Let $j \in \mathbb{N}$, and suppose $a_k = 0$ for every $k \neq j$. Then $\sum_{k=0}^n a_k = a_j$ if $j \leq n$, and $\sum_{k=0}^n a_k = 0$ if $j > n$.

- (e) $-\sum_{k=0}^n a_k = \sum_{k=0}^n (-a_k)$.
 (f) (*Splitting off the first term.*) $\sum_{k=0}^{n+1} a_k = a_0 + \sum_{k=0}^n a_{k+1}$.

In words: a finite sum may be split termwise, multiplied termwise, and negated termwise; a sum with one non-zero term is that term; and the first term may be split off, the rest being re-indexed from 0. By the finite-lists remark, the lemma applies to finitely many terms $a_0, \dots, a_n$ as well.

Idea. A sum up to $n + 1$ is the sum up to n plus one term, so every rule that holds for one term and survives adding one more term holds for all sums: an induction on n whose step is a single axiom, (F1)–(F2) for (a), (F9) for (b), and associativity for (f). Parts (c) and (e) need no induction, because a multiple is a product, $m \cdot a = (m \cdot 1)a$, so they are (b) in disguise.

Proof. Each part is an induction on n (Logic and Proof, Axiom 4.2.1), splitting off the last term at the step, except (c) and (e), which follow from (b).

- (a) For $n = 0$ both sides are $a_0 + b_0$. If (a) holds for n , then splitting off the last term,

$$\sum_{k=0}^{n+1} (a_k + b_k) = \left(\sum_{k=0}^n a_k + \sum_{k=0}^n b_k \right) + (a_{n+1} + b_{n+1}),$$

which is $(\sum_{k=0}^n a_k + a_{n+1}) + (\sum_{k=0}^n b_k + b_{n+1})$ by (F1) and (F2), and that is the right side for $n + 1$.

- (b) For $n = 0$ both sides are ca_0 . At the step, $c(\sum_{k=0}^n a_k + a_{n+1}) = c \sum_{k=0}^n a_k + ca_{n+1}$ by (F9), and the induction hypothesis rewrites the first term.
 (c) By Lemma 2.5.1 (c), which holds for $m \in \mathbb{Z}$ by part (d) there, $m \cdot a_k = (m \cdot 1)a_k$ and $m \cdot \sum a_k = (m \cdot 1) \sum a_k$. So (c) is (b) with $c = m \cdot 1$.
 (d) For $n = 0$: if $j = 0$ the sum is $a_0 = a_j$; if $j > 0$, then $0 \neq j$, so the sum is $a_0 = 0$. Suppose (d) holds for n , and split off a_{n+1} . If $j \leq n$, the sum up to n is a_j and $a_{n+1} = 0$ (as $n + 1 \neq j$), so the total is a_j . If $j = n + 1$, the sum up to n is 0 (as $j > n$) and the total is $0 + a_{n+1} = a_j$. If $j > n + 1$, both parts are 0.
 (e) By (c) with $m = -1$, since $(-1) \cdot x = -(1 \cdot x) = -x$ (Lemma 2.5.1 (d)).
 (f) For $n = 0$ both sides are $a_0 + a_1$. If (f) holds for n , then

$$\sum_{k=0}^{n+2} a_k = \left(a_0 + \sum_{k=0}^n a_{k+1} \right) + a_{n+2} = a_0 + \sum_{k=0}^{n+1} a_{k+1},$$

by splitting off the last term, the induction hypothesis, (F2), and splitting off the last term of the sequence $(a_{k+1})_k$, whose term at $k = n + 1$ is a_{n+2} . This proves the lemma. ■

2.6.2 Binomial coefficients

In $(x + y)^n$, each product $x^k y^{n-k}$ appears a certain number of times, and that number is the binomial coefficient. We define it by Pascal's rule, which is how the coefficients arise when $(x + y)^n$ is multiplied by $x + y$, and we never divide.

Definition 2.6.1. Binomial Coefficients

The **binomial coefficients** $\binom{n}{k} \in \mathbb{N}$, for $n, k \in \mathbb{N}$, are defined by recursion on n (Sets, Relations, and Cardinality, Theorem 2.3.1, with X the set of functions $\mathbb{N} \rightarrow \mathbb{N}$):

$$\begin{aligned} \binom{0}{0} &:= 1, & \binom{0}{k} &:= 0 \quad (k \geq 1), \\ \binom{n+1}{0} &:= 1, & \binom{n+1}{k+1} &:= \binom{n}{k} + \binom{n}{k+1} \quad (k \in \mathbb{N}). \end{aligned}$$

In words: row $n + 1$ starts with 1, and each later entry is the sum of the two entries of row n above it (**Pascal's rule**). Each row is a whole function $\mathbb{N} \rightarrow \mathbb{N}$, so the recursion has values for every k , and a coefficient is a natural number, never a quotient.

Three facts follow by one induction on n each.

- $\binom{n}{k} = 0$ for $k > n$. For $n = 0$ this is the definition. If it holds for n and $k > n + 1$, write $k = j + 1$ with $j > n$; then $\binom{n+1}{j+1} = \binom{n}{j} + \binom{n}{j+1} = 0 + 0$.
- $\binom{n}{n} = 1$. Indeed $\binom{0}{0} = 1$, and $\binom{n+1}{n+1} = \binom{n}{n} + \binom{n}{n+1} = 1 + 0$ by the first fact.
- $\binom{n}{1} = n$. Indeed $\binom{0}{1} = 0$, and $\binom{n+1}{1} = \binom{n}{0} + \binom{n}{1} = 1 + n$.

The rows $n = 0, \dots, 6$, with the zeros for $k > n$ shown:

n	$k = 0$	1	2	3	4	5	6
0	1	0	0	0	0	0	0
1	1	1	0	0	0	0	0
2	1	2	1	0	0	0	0
3	1	3	3	1	0	0	0
4	1	4	6	4	1	0	0
5	1	5	10	10	5	1	0
6	1	6	15	20	15	6	1

Remark. The formula $\binom{n}{k} \cdot k! \cdot (n - k)! = n!$ for $k \leq n$ is true, but we neither prove nor use it. The route below needs one identity between neighboring coefficients and avoids division altogether, which matters because in $\mathbb{F}_p$ the factorial $p!$ is 0.

The identity we need relates row $n + 1$ to row n by a factor. It is what makes a prime divide the middle coefficients of row p .

Proposition 2.6.2. Absorption Identity

For all $n, k \in \mathbb{N}$,

$$(k + 1) \binom{n + 1}{k + 1} = (n + 1) \binom{n}{k}.$$

Idea. The definition is a recursion on n , so we induct on n , proving the statement for **all** k at once; the step then needs the hypothesis at two values of k . In the step, expand the left side by Pascal's rule, split the factor $k + 2$ as $(k + 1) + 1$ in front of one of the two terms, apply the hypothesis twice, and recombine with Pascal's rule. For $n = 2$, $k = 0$ it reads $1 \cdot 3 = 3 \cdot 1$; for $n = 3$, $k = 1$, $2 \cdot 6 = 4 \cdot 3$.

Proof. We prove by induction on n (Logic and Proof, Axiom 4.2.1) the statement “for every $k \in \mathbb{N}$, $(k + 1)\binom{n+1}{k+1} = (n + 1)\binom{n}{k}$ ”.

Base $n = 0$. For $k = 0$: $1 \cdot \binom{1}{1} = 1 = 1 \cdot \binom{0}{0}$. For $k \geq 1$: $\binom{1}{k+1} = 0$ since $k + 1 > 1$, and $\binom{0}{k} = 0$; both sides are 0.

Step. Suppose the statement holds for n . For $k = 0$, the claim for $n + 1$ reads $\binom{n+2}{1} = (n + 2)\binom{n+1}{0}$, and both sides are $n + 2$ by the facts above. For $k = j + 1$ with $j \in \mathbb{N}$, Pascal's rule gives

$$\begin{aligned} (j + 2)\binom{n+2}{j+2} &= (j + 2)\binom{n+1}{j+1} + (j + 2)\binom{n+1}{j+2} \\ &= (j + 1)\binom{n+1}{j+1} + \binom{n+1}{j+1} + (j + 2)\binom{n+1}{j+2} \\ &= (n + 1)\binom{n}{j} + \binom{n+1}{j+1} + (n + 1)\binom{n}{j+1} \\ &= (n + 1)\binom{n+1}{j+1} + \binom{n+1}{j+1} = (n + 2)\binom{n+1}{j+1}, \end{aligned}$$

where the third line uses the hypothesis at $k = j$ and at $k = j + 1$, and the fourth line Pascal's rule again. This is the claim for $n + 1$ at $k = j + 1$. This proves the proposition. ■

2.6.3 The binomial theorem

Expanding $(x + y)^n$ multiplies out n factors $x + y$ and collects the products $x^k y^{n-k}$. In a commutative ring this collecting is legitimate, and the counts are the binomial coefficients, acting as integer multiples.

Theorem 2.6.3. The Binomial Theorem in a Commutative Ring

Let R be a commutative ring, $x, y \in R$ and $n \in \mathbb{N}$. Then

$$(x + y)^n = \sum_{k=0}^n \binom{n}{k} \cdot (x^k y^{n-k}).$$

Here $\binom{n}{k} \cdot z$ is the integer multiple of Section 2.5, and $n - k \in \mathbb{N}$ since $k \leq n$.

Idea. Induct on n , with $(x + y)^{n+1} = (x + y)^n x + (x + y)^n y$. Multiplying the sum for $(x + y)^n$ by x raises every power of x by one, which shifts the coefficients one place to the right; multiplying by y leaves them in place. Adding the two rows entry by entry is exactly Pascal's rule. The work is in lining the two sums up over the same range $k = 0, \dots, n + 1$: the shifted sum gets a zero first term, and the other one a zero last term.

Proof. Induction on n (Logic and Proof, Axiom 4.2.1). For $n = 0$, $(x + y)^0 = 1$ and the right side is $\binom{0}{0} \cdot (x^0 y^0) = 1 \cdot (1 \cdot 1) = 1$.

Suppose the formula holds for n , and put $t_k := \binom{n}{k} \cdot (x^k y^{n-k})$ for $0 \leq k \leq n$. By the power recursion, (F9) and Lemma 2.6.1 (b) with (F6),

$$(x + y)^{n+1} = (x + y)^n x + (x + y)^n y = \sum_{k=0}^n t_k x + \sum_{k=0}^n t_k y.$$

By the rule $(m \cdot a)b = m \cdot (ab)$ of Lemma 2.5.1 (d), with (F5), (F6) and the power recursion,

$$t_k x = \binom{n}{k} \cdot (x^{k+1} y^{n-k}), \quad t_k y = \binom{n}{k} \cdot (x^k y^{n+1-k}).$$

For $0 \leq k \leq n + 1$ let $z_k := x^k y^{n+1-k}$, and define

$$u_0 := 0, \quad u_k := \binom{n}{k-1} \cdot z_k \quad (1 \leq k \leq n+1), \quad w_k := \binom{n}{k} \cdot z_k \quad (0 \leq k \leq n+1).$$

Then $t_k x = u_{k+1}$ and $t_k y = w_k$ for $0 \leq k \leq n$, and $w_{n+1} = 0 \cdot z_{n+1} = 0$, since $\binom{n}{n+1} = 0$. By Lemma 2.6.1 (f) and $u_0 = 0$, and by splitting off the last term $w_{n+1} = 0$,

$$\sum_{k=0}^n t_k x = \sum_{k=0}^{n+1} u_k, \quad \sum_{k=0}^n t_k y = \sum_{k=0}^{n+1} w_k.$$

So $(x + y)^{n+1} = \sum_{k=0}^{n+1} (u_k + w_k)$ by Lemma 2.6.1 (a). Finally, $u_0 + w_0 = 0 + 1 \cdot z_0 = \binom{n+1}{0} \cdot z_0$, and for $k = j + 1$ with $0 \leq j \leq n$, the sum rule of Lemma 2.5.1 (d) and Pascal's rule give

$$u_k + w_k = \binom{n}{j} \cdot z_k + \binom{n}{j+1} \cdot z_k = \binom{n+1}{j+1} \cdot z_k = \binom{n+1}{k} \cdot z_k.$$

Hence $(x + y)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} \cdot (x^k y^{n+1-k})$, which is the formula for $n + 1$. This proves the theorem. ■

The proof used (F6) at every regrouping of $x^k y^{n-k} x$, and the theorem needs it: the linear-algebra volumes meet matrices, whose multiplication is not commutative, and there the expansion holds only for pairs that commute. For $R = \mathbb{Z}$ the theorem is the familiar expansion, since there $m \cdot z = mz$ (Section 2.5).

In row 5 of the table, the four middle entries 5, 10, 10, 5 are all multiples of 5; in row 6 the middle entries 15 and 20 are not multiples of 6. Primes are special.

Lemma 2.6.4. A Prime Divides the Middle Binomial Coefficients

Let p be a prime and $k \in \mathbb{N}$ with $0 < k < p$. Then $p \mid \binom{p}{k}$.

Proof. We read the coefficients in $\mathbb{N} \subseteq \mathbb{Z}$. By [Proposition 2.6.2](#) with $n = p - 1$ and $k - 1$ in place of k ,

$$k \binom{p}{k} = p \binom{p-1}{k-1},$$

so $p \mid k \binom{p}{k}$. Since $0 < k < p$, $p \nmid k$: a positive multiple of p is at least p (Number Systems: From $\backslash(\backslash n \mathbb{N} \backslash)$ to $\backslash(\backslash n \mathbb{R} \backslash)$, Proposition 3.1.1 (e)). Hence $\gcd(p, k) = 1$ by Number Systems: From $\backslash(\backslash n \mathbb{N} \backslash)$ to $\backslash(\backslash n \mathbb{R} \backslash)$, Corollary 3.3.2 (a), and Number Systems: From $\backslash(\backslash n \mathbb{N} \backslash)$ to $\backslash(\backslash n \mathbb{R} \backslash)$, Theorem 3.3.1 gives $p \mid \binom{p}{k}$. This proves the lemma. ■

The hypothesis “prime” is needed: $\binom{4}{2} = 6$, and $4 \nmid 6$. In the proof, $4 \mid 2\binom{4}{2}$, but $\gcd(4, 2) = 2$, so Euclid’s lemma does not apply.

Quick check. Use [Proposition 2.6.2](#) to compute $\binom{7}{3}$ from $\binom{6}{2} = 15$, and check that 7 divides it.

Solution. With $n = 6$, $k = 2$: $3\binom{7}{3} = 7\binom{6}{2} = 7 \cdot 15 = 105$, so $\binom{7}{3} = 35$, and $35 = 5 \cdot 7$. (By Pascal’s rule, $\binom{7}{3} = \binom{6}{2} + \binom{6}{3} = 15 + 20 = 35$, the same.)

2.6.4 The Frobenius map

We can now expand $(x + y)^p$ in a field of characteristic p .

Theorem 2.6.5. The Frobenius Homomorphism

Let F be a field of characteristic $p > 0$.

(a) For all $x, y \in F$,

$$(x + y)^p = x^p + y^p, \quad (xy)^p = x^p y^p,$$

and $1^p = 1$. So the **Frobenius map** $\text{Fr}: F \rightarrow F$, $\text{Fr}(x) := x^p$, is a homomorphism, and it is injective.

(b) $(x - y)^p = x^p - y^p$ for all $x, y \in F$.

(c) If F is finite, then Fr is an automorphism of F .

By Theorem 2.5.3, the hypothesis $\text{char } F = p > 0$ already makes p prime.

Try it first (ten minutes): expand $(x + y)^5$ and $(x + y)^6$ in $\mathbb{F}_5$, using the rows $n = 5$ and $n = 6$ of the table above, and see which coefficients survive.

Idea. For $(x + y)^5$ the coefficients 1, 5, 10, 10, 5, 1 become 1, 0, 0, 0, 0, 1 in $\mathbb{F}_5$, and $(x + y)^5 = x^5 + y^5$. For $(x + y)^6$ the coefficients 1, 6, 15, 20, 15, 6, 1 become 1, 1, 0, 0, 0, 1, 1, and $(x + y)^6 = x^6 + x^5y + xy^5 + y^6$: the extra terms survive because 6 is not the characteristic. So the plan is: expand by the binomial theorem; every middle coefficient $\binom{p}{k}$ is a multiple of p ; and a multiple of p acts on F as 0, because $p \cdot 1 = 0$. The product rule and $1^p = 1$ are power laws, and injectivity is free for a homomorphism of fields.

Before reading on: where is it used that p is prime?

Proof.

- (a) By [Theorem 2.6.3](#), $(x + y)^p = \sum_{k=0}^p t_k$ with $t_k := \binom{p}{k} \cdot (x^k y^{p-k})$. Let $0 < k < p$. By [Lemma 2.6.4](#), $p \mid \binom{p}{k}$, so $\binom{p}{k} \cdot 1 = 0$ by [Proposition 2.5.2 \(a\)](#), and then, by [Lemma 2.5.1 \(c\)](#) and [Theorem 2.1.1 \(d\)](#),

$$t_k = \left(\binom{p}{k} \cdot 1 \right) (x^k y^{p-k}) = 0 \cdot (x^k y^{p-k}) = 0.$$

The end terms are $t_0 = 1 \cdot (x^0 y^p) = y^p$ and $t_p = 1 \cdot (x^p y^0) = x^p$. Let $b_k := t_k$ for $k = 0$ and $b_k := 0$ otherwise, and $c_k := t_k$ for $k = p$ and $c_k := 0$ otherwise. Since $p \neq 0$, $t_k = b_k + c_k$ for every $0 \leq k \leq p$, so by [Lemma 2.6.1 \(a\)](#) and (d),

$$(x + y)^p = \sum_{k=0}^p b_k + \sum_{k=0}^p c_k = t_0 + t_p = y^p + x^p,$$

which is $x^p + y^p$ by (F1). Next, $(xy)^p = x^p y^p$ is the third power law of this section's opening paragraph (Sets, Relations, and Cardinality, [Proposition 2.3.4 \(c\)](#), read in F), and $1^p = 1$. So Fr is a homomorphism ([Definition 2.4.1](#)), and it is injective by [Proposition 2.4.1 \(c\)](#).

- (b) By [Proposition 2.4.1 \(a\)](#), $\text{Fr}(x - y) = \text{Fr}(x) - \text{Fr}(y)$.
- (c) The image $\text{Fr}(F)$ is a subset of F , and Fr , with codomain $\text{Fr}(F)$, is a bijection $F \rightarrow \text{Fr}(F)$ by (a). If $\text{Fr}(F) \neq F$, this would be a bijection from the finite set F onto a proper subset, which Sets, Relations, and Cardinality, [Theorem 3.1.9](#) forbids. So $\text{Fr}(F) = F$, Fr is bijective, and a bijective homomorphism $F \rightarrow F$ is an automorphism ([Definition 2.4.1](#)). This proves the theorem. ■

Answer to the prompt. Primality is used in one place: [Lemma 2.6.4](#), whose proof needs Euclid's lemma, and so needs p prime. It costs nothing here, since a positive characteristic is always prime ([Theorem 2.5.3](#)).

In words: in characteristic p , raising to the p -th power respects sums. The map is not the identity in general; [Exercise C3](#) of [Section 2.5](#) found that on the four-element field it exchanges two elements. On $\mathbb{F}_p$ itself it is the identity, and that is Fermat's little theorem.

Warning. “ $(x + y)^n = x^n + y^n$ ” is not a general rule. In a field of characteristic $p > 0$ it holds for $n = p$ ([Theorem 2.6.5 \(a\)](#)), and so for $n = p^2$ by [Exercise B2](#) (and in the same way for every power of p). With other exponents it can fail: in $\mathbb{F}_3$, $(1 + 1)^2 = 4 = 1$, while $1^2 + 1^2 = 2$.

In a ring of composite characteristic it can fail even with n equal to the characteristic: in $\mathbb{Z}/4\mathbb{Z}$, which has characteristic 4, $([1] + [1])^4 = [16] = [0]$, while $[1]^4 + [1]^4 = [2]$; the middle coefficient $\binom{4}{2} = 6$ is not a multiple of 4. In $\mathbb{Z}$ the identity fails for every $n \geq 2$: $(1 + 1)^n = 2^n \neq 2$.

2.6.5 Fermat's little theorem

On $\mathbb{F}_p$, the Frobenius map is a homomorphism $\mathbb{F}_p \rightarrow \mathbb{F}_p$, and by Corollary 2.5.6 (b) there is only one such map, the identity. That is the whole proof of the first part below.

Theorem 2.6.6. Fermat's Little Theorem

Let p be a prime.

- (a) $a^p = a$ for every $a \in \mathbb{F}_p$.
- (b) $a^{p-1} = 1$ for every non-zero $a \in \mathbb{F}_p$; so $a^{-1} = a^{p-2}$.
- (c) For every $a \in \mathbb{Z}$, $p \mid a^p - a$; and if $p \nmid a$, then $p \mid a^{p-1} - 1$.

Proof.

- (a) $\text{char } \mathbb{F}_p = p$ (Example (The characteristics of the standard fields)), so $\text{Fr}: \mathbb{F}_p \rightarrow \mathbb{F}_p$ is a homomorphism by Theorem 2.6.5 (a). By Corollary 2.5.6 (b), the only homomorphism $\mathbb{F}_p \rightarrow \mathbb{F}_p$ is the identity. Hence $a^p = \text{Fr}(a) = a$ for every $a \in \mathbb{F}_p$.
- (b) Let $a \neq 0$. Since $p \geq 2$, $p - 1 \in \mathbb{N}$ and $a \cdot a^{p-1} = a^{p-1}a = a^p = a = a \cdot 1$, by (F6), the power recursion and (a). Canceling $a \neq 0$ (Theorem 2.1.1 (b)) gives $a^{p-1} = 1$. Likewise $p - 2 \in \mathbb{N}$ and $a \cdot a^{p-2} = a^{p-1} = 1$, so $a^{-1} = a^{p-2}$ by uniqueness of inverses (Theorem 2.1.1 (c)).
- (c) Write $[a]$ for the class of $a \in \mathbb{Z}$ in $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Since $[a][b] = [ab]$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.4.1 (b)), induction on n gives $[a]^n = [a^n]$ for every $n \in \mathbb{N}$: $[a]^0 = [1] = [a^0]$, and $[a]^{n+1} = [a]^n[a] = [a^n][a] = [a^{n+1}]$. By (a), $[a]^p = [a]^p = [a]$, so $p \mid a^p - a$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.4.1 (a), for the ideal $p\mathbb{Z}$). If $p \nmid a$, then $[a] \neq [0]$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.4.1 (d)), so $[a]^{p-1} = [a]^{p-1} = [1]$ by (b), and $p \mid a^{p-1} - 1$. This proves the theorem. ■

Primality is needed in (c). For the modulus 4 and $a = 2$, $2^4 - 2 = 14$ is not a multiple of 4 (in $\mathbb{Z}/4\mathbb{Z}$ this is $([1] + [1])^4 = [0] \neq [2]$, from the warning above), and although $4 \nmid 2$, $2^3 - 1 = 7$ is not a multiple of 4 either.

Part (b) gives a second way to invert in $\mathbb{F}_p$, besides the Euclidean algorithm of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 3: $a^{-1} = a^{p-2}$. It also reduces large exponents: for non-zero a , only the remainder of the exponent on division by $p - 1$ matters, since $a^{q(p-1)+r} = (a^{p-1})^q a^r = a^r$. Exercise C2 below gives a second proof of (a), by induction, and Chapter 4 gives another proof of (b), from a product of all the non-zero elements.

Example. Powers and inverses in prime fields

- (i) Compute 3^{100} in $\mathbb{F}_7$.
- (ii) Compute 2^{100} in $\mathbb{F}_{101}$.
- (iii) Find the inverse of 7 in $\mathbb{F}_{31}$ twice: by [Theorem 2.6.6](#) (b), and by the Euclidean algorithm.
- (iv) What is the Frobenius map of $\mathbb{F}_p$?

Solution.

- (i) 7 is prime (the small-primes remark of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Section 3.1) and $3 \neq 0$ in $\mathbb{F}_7$, so $3^6 = 1$ by [Theorem 2.6.6](#) (b). Since $100 = 16 \cdot 6 + 4$, the power laws give $3^{100} = (3^6)^{16} 3^4 = 1 \cdot 81$, and $81 = 11 \cdot 7 + 4$. So $3^{100} = 4$ in $\mathbb{F}_7$.
- (ii) 101 is prime: by the remark after *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Lemma 3.3.4 it suffices that no d with $2 \leq d$ and $d \cdot d \leq 101$, that is $2 \leq d \leq 10$, divides 101, and the remainders of 101 on division by $2, 3, \dots, 10$ are $1, 2, 1, 1, 5, 3, 5, 2, 1$. Since $2 \neq 0$ in $\mathbb{F}_{101}$, [Theorem 2.6.6](#) (b) gives $2^{100} = 2^{101-1} = 1$. No multiplication was needed.
- (iii) 31 is prime by the same test ($d = 2, 3, 4, 5$ leave remainders $1, 1, 3, 1$). *By Fermat:* since $7 \neq 0$ in $\mathbb{F}_{31}$, [Theorem 2.6.6](#) (b) gives $7^{-1} = 7^{29}$. Square repeatedly in $\mathbb{F}_{31}$: $7^2 = 49 = 18$, $7^4 = 18^2 = 324 = 14$, $7^8 = 14^2 = 196 = 10$, $7^{16} = 10^2 = 100 = 7$. With $29 = 16 + 8 + 4 + 1$,

$$7^{29} = 7^{16} 7^8 7^4 7 = 7 \cdot 10 \cdot 14 \cdot 7 = 70 \cdot 98 = 8 \cdot 5 = 40 = 9.$$

By Euclid: $31 = 4 \cdot 7 + 3$ and $7 = 2 \cdot 3 + 1$, so

$$1 = 7 - 2 \cdot 3 = 7 - 2(31 - 4 \cdot 7) = 9 \cdot 7 - 2 \cdot 31,$$

and $7^{-1} = 9$ by *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Theorem 3.5.1. Both routes give 9. Check: $7 \cdot 9 = 63 = 2 \cdot 31 + 1$. For small p the Euclidean algorithm is shorter; Fermat's route needs no back-substitution, only squaring.

- (iv) The identity, by [Theorem 2.6.6](#) (a): $\text{Fr}(a) = a^p = a$ for every $a \in \mathbb{F}_p$.

Quick check. Compute 2^6 in $\mathbb{F}_7$ and 3^{10} in $\mathbb{F}_{11}$, with and without [Theorem 2.6.6](#).

Solution. Both are 1. Without it: $2^6 = 64 = 9 \cdot 7 + 1$; and $3^5 = 243 = 22 \cdot 11 + 1$, so $3^{10} = (3^5)^2 = 1$. With it: 7 and 11 are prime, $2 \neq 0$ in $\mathbb{F}_7$ and $3 \neq 0$ in $\mathbb{F}_{11}$, and the exponents are $7 - 1$ and $11 - 1$.

2.6.6 Exercises

2.6.6.1 A. Check your understanding

Exercise. A1

These parts are about [Theorem 2.6.5](#) and its proof.

- (a) Where in the proof of (a) is it used that p is prime, and why does the theorem not need “ p prime” as a separate hypothesis?
- (b) List $\binom{5}{k}$ for $0 \leq k \leq 5$ and $\binom{6}{k}$ for $0 \leq k \leq 6$. Which are divisible by 5, and which by 6?
- (c) Why is Fr injective? Does the proof use that F is finite?
- (d) State the idea of the proof of (a) in two sentences.

Solution.

- (a) In [Lemma 2.6.4](#), through Euclid's lemma: $p \mid k \binom{p}{k}$ gives $p \mid \binom{p}{k}$ only because $\gcd(p, k) = 1$, which needs p prime. A positive characteristic is always prime (Theorem 2.5.3), so “ $\text{char } F = p > 0$ ” already includes it.
- (b) Row 5: 1, 5, 10, 10, 5, 1; the four middle ones are divisible by 5, the end ones are not. Row 6: 1, 6, 15, 20, 15, 6, 1; only the two 6's are divisible by 6, and 15, 20 are not. This is why $(x + y)^6 \neq x^6 + y^6$ in a ring of characteristic 6 such as $\mathbb{Z}/6\mathbb{Z}$.
- (c) Every homomorphism of fields is injective (Proposition 2.4.1 (c)): $\text{Fr}(a) = 0$ only for $a = 0$. The proof of injectivity does not use finiteness; finiteness is used only for surjectivity in (c).
- (d) Expand $(x + y)^p$ by the binomial theorem; every middle coefficient $\binom{p}{k}$ is a multiple of p . In characteristic p , $p \cdot 1 = 0$, so every middle term vanishes and only $x^p + y^p$ remains.

2.6.6.2 B. Practice

Exercise. B1

Compute 5^{38} in $\mathbb{F}_{13}$, and find the inverse of 5 in $\mathbb{F}_{13}$ by [Theorem 2.6.6](#).

Solution. 13 is prime (no d with $2 \leq d \leq 3$ divides it, and $4 \cdot 4 > 13$; the remark after Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Lemma 3.3.4), and $5 \neq 0$ in $\mathbb{F}_{13}$. By [Theorem 2.6.6](#) (b), $5^{12} = 1$. Since $38 = 3 \cdot 12 + 2$, $5^{38} = (5^{12})^3 5^2 = 25 = 12$ in $\mathbb{F}_{13}$. For the inverse, $5^{-1} = 5^{11}$. Now $5^2 = 12 = -1$, so $5^{10} = (5^2)^5 = (-1)^5 = -1$ and $5^{11} = -5 = 8$. Check: $5 \cdot 8 = 40 = 3 \cdot 13 + 1$. Hence $5^{38} = 12$ and $5^{-1} = 8$.

Exercise. B2

Let F be a field of characteristic $p > 0$.

- (a) Show that $(x + y)^{p^2} = x^{p^2} + y^{p^2}$ for all $x, y \in F$.
- (b) Show that $(\sum_{i=1}^m x_i)^p = \sum_{i=1}^m x_i^p$ for all $m \in \mathbb{N}$ and $x_1, \dots, x_m \in F$.

Solution.

- (a) $\text{Fr} \circ \text{Fr}$ is a homomorphism, as a composite of homomorphisms (Proposition 2.4.1 (e)),

and $(\text{Fr} \circ \text{Fr})(x) = (x^p)^p = x^{p^2}$ by the power law $(x^m)^n = x^{mn}$. Applying its additivity to $x + y$ gives the claim.

- (b) Induction on m . For $m = 0$ both sides are 0: the empty sum is 0, and $0^p = 0^{p-1} \cdot 0 = 0$ as $p \geq 1$. If the claim holds for m , split off the last term and use [Theorem 2.6.5](#) (a):

$$\left(\sum_{i=1}^{m+1} x_i\right)^p = \left(\sum_{i=1}^m x_i + x_{m+1}\right)^p = \left(\sum_{i=1}^m x_i\right)^p + x_{m+1}^p = \sum_{i=1}^{m+1} x_i^p.$$

Exercise. B3

Let p be a prime. Show that the solutions $x \in \mathbb{F}_p$ of $x^{p-1} = 1$ are exactly the non-zero elements, and that every $a \in \mathbb{F}_p$ satisfies $a^p - a = 0$.

Solution. Every non-zero a satisfies $a^{p-1} = 1$ by [Theorem 2.6.6](#) (b). The element 0 does not: since $p - 1 \geq 1$, $0^{p-1} = 0^{p-2} \cdot 0 = 0 \neq 1$. So the solutions are exactly the non-zero elements. And $a^p - a = a - a = 0$ for every a by [Theorem 2.6.6](#) (a).

2.6.6.3 C. Going deeper

Exercise. C1: Exit check: the Frobenius identity

Let F be a field of characteristic $p > 0$. Using [Theorem 2.6.3](#) and [Lemma 2.6.4](#), prove that $\text{Fr}: F \rightarrow F$, $x \mapsto x^p$, is an injective homomorphism.

Solution. Sums. By [Theorem 2.6.3](#), $(x + y)^p = \sum_{k=0}^p \binom{p}{k} \cdot (x^k y^{p-k})$. For $0 < k < p$, $\binom{p}{k} \cdot (x^k y^{p-k}) = (\binom{p}{k} \cdot 1)(x^k y^{p-k})$ by [Lemma 2.5.1](#) (c). By [Lemma 2.6.4](#), $p \mid \binom{p}{k}$, and since $\text{char } F = p$, $\binom{p}{k} \cdot 1 = 0$ ([Proposition 2.5.2](#) (a)); so the term is 0 ([Theorem 2.1.1](#) (d)). The terms $k = 0$ and $k = p$ are $1 \cdot y^p = y^p$ and $1 \cdot x^p = x^p$, since $\binom{p}{0} = \binom{p}{p} = 1$ and $x^0 = y^0 = 1$. A sum whose terms vanish except at two places is the sum of those two terms ([Lemma 2.6.1](#) (a), (d)), so $(x + y)^p = x^p + y^p$.

Products and one. $(xy)^p = x^p y^p$ by the power law $(xy)^n = x^n y^n$, and $1^p = 1$. So Fr is a homomorphism ([Definition 2.4.1](#)).

Injective. Every homomorphism of fields is injective ([Proposition 2.4.1](#) (c)).

Marking scheme. (10 points)

- 2: the binomial expansion written with integer multiples $\binom{p}{k} \cdot (x^k y^{p-k})$.
- 2: each middle term reduced to a multiple that vanishes, with the rule named (for example $(\binom{p}{k} \cdot 1)(x^k y^{p-k})$ by $(m \cdot 1)a = m \cdot a$, or $\binom{p}{k} \cdot z = q \cdot (p \cdot z)$ where $\binom{p}{k} = qp$).
- 2: that multiple is 0 from $p \mid \binom{p}{k}$ and $\text{char } F = p$, with both reasons named.
- 1: the end terms y^p and x^p .
- 1: $(xy)^p = x^p y^p$ and $1^p = 1$.
- 2: injectivity, by [Proposition 2.4.1](#) (c) or by any correct direct argument.

Second route for injectivity: $x^p = y^p \Rightarrow (x - y)^p = 0 \Rightarrow x = y$ earns the 2 points, 1 for $(x - y)^p = x^p - y^p$ with its reason ([Proposition 2.4.1](#) (a)), or $(-y)^p = -y^p$ for every prime p ,

the even one included), and 1 for $x - y = 0$ because a field has no zero divisors.

Fatal errors (0 for the step): “ $\binom{p}{k} = 0$ ” as an integer; using $(x + y)^p = x^p + y^p$ in its own proof.

Exercise. C2: Fermat by induction

Let p be a prime. Give another proof of [Theorem 2.6.6](#) (a) and of the first claim of [Theorem 2.6.6](#) (c), without [Corollary 2.5.6](#). In (a) use only [Theorem 2.6.5](#) (a) (with $\text{char } \mathbb{F}_p = p$, [Example \(The characteristics of the standard fields\)](#)) and [Number Systems: From \$\mathbb{N}\$ to \$\mathbb{R}\$](#) , [Theorem 3.4.3](#) (b), (d); in (b) you may also use [Number Systems: From \$\mathbb{N}\$ to \$\mathbb{R}\$](#) , [Theorem 3.4.1](#).

- (a) prove by induction on $r \in \mathbb{N}$ that $(r \cdot 1)^p = r \cdot 1$ in $\mathbb{F}_p$, and deduce $a^p = a$ for every $a \in \mathbb{F}_p$;
- (b) deduce that $p \mid a^p - a$ for every integer a .

Solution.

- (a) For $r = 0$: $(0 \cdot 1)^p = 0^p = 0^{p-1} \cdot 0 = 0 = 0 \cdot 1$, as $p \geq 1$. If $(r \cdot 1)^p = r \cdot 1$, then by [Theorem 2.6.5](#) (a) ($\text{char } \mathbb{F}_p = p$, [Example \(The characteristics of the standard fields\)](#)),

$$((r + 1) \cdot 1)^p = (r \cdot 1 + 1)^p = (r \cdot 1)^p + 1^p = r \cdot 1 + 1 = (r + 1) \cdot 1.$$

Every element of $\mathbb{F}_p$ is $[r]$ for some $r \in \{0, \dots, p-1\}$ ([Number Systems: From \$\mathbb{N}\$ to \$\mathbb{R}\$](#) , [Theorem 3.4.3](#) (b)), and $[r] = r \cdot [1]$ (part (d) there). So $a^p = a$ for every $a \in \mathbb{F}_p$.

- (b) Let $a \in \mathbb{Z}$. Then $[a] \in \mathbb{F}_p$, so $[a]^p = [a]$ by (a). By induction on n , $[a]^n = [a^n]$, using $[a][b] = [ab]$ ([Number Systems: From \$\mathbb{N}\$ to \$\mathbb{R}\$](#) , [Theorem 3.4.1](#) (b)), as in the proof of [Theorem 2.6.6](#) (c). So $[a^p] = [a]$, and $p \mid a^p - a$ ([Number Systems: From \$\mathbb{N}\$ to \$\mathbb{R}\$](#) , [Theorem 3.4.1](#) (a), for the ideal $p\mathbb{Z}$). (This proves only what [Theorem 2.6.6](#) already gives; it is practice with the Frobenius identity, and nothing cites it.)

Exercise. C3: Roots of order p

Let F be a finite field of characteristic p . Show that for every $a \in F$ the equation $x^p = a$ has **exactly one** solution $x \in F$. Deduce that in $\mathbb{F}_p$, the only solution of $x^p = a$ is $x = a$.

Solution. By [Corollary 2.5.7](#) (a), p is a prime, so $p > 0$, and by [Theorem 2.6.5](#) (c), Fr is a bijection $F \rightarrow F$. Surjectivity gives a solution of $\text{Fr}(x) = a$, and injectivity says there is at most one. In $\mathbb{F}_p$, $x = a$ is a solution by [Theorem 2.6.6](#) (a), $a^p = a$, so it is the only one. The uniqueness half needs only that Fr is injective, so it holds in every field of characteristic $p > 0$ ([Theorem 2.6.5](#) (a)); existence used the finiteness of F .

2.6.6.4 R. Review

Exercise. R1

Find all $z \in \mathbb{C}$ with $z^2 = -3 + 4i$, and explain why there are exactly two.

Solution. By the square-root formula of Proposition 1.4.1, with $a = -3$, $b = 4$: $r = |-3 + 4i| = 5$ (since $9 + 16 = 25$), $(r + a)/2 = 1$, $(r - a)/2 = 4$, and $b > 0$, so $w = 1 + 2i$. Check: $(1 + 2i)^2 = 1 + 4i + 4i^2 = -3 + 4i$. By Corollary 2.1.2 in the field $\mathbb{C}$ (Example (The Fields $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$)), $z^2 = w^2$ if and only if $z = w$ or $z = -w$. So the solutions are $1 + 2i$ and $-1 - 2i$. They are two, not one: $w = -w$ would give $2w = 0$, hence $w = 0$, since $2 \neq 0$ in $\mathbb{C}$ ($\text{char } \mathbb{C} = 0$, Example (The characteristics of the standard fields), with Proposition 2.5.2 (b)).

Exercise. R2

Show that 7 has no square root in $\mathbb{Q}(\sqrt{2})$.

Solution. Suppose $(a + b\sqrt{2})^2 = 7$ with $a, b \in \mathbb{Q}$. Expanding, $(a^2 + 2b^2) + 2ab\sqrt{2} = 7 + 0\sqrt{2}$, so by unique representation (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 6.4.5 (a)), $2ab = 0$ and $a^2 + 2b^2 = 7$. Since $2 \neq 0$ in $\mathbb{Q}$ ($\text{char } \mathbb{Q} = 0$, Example (The characteristics of the standard fields), with Proposition 2.5.2 (b)), Theorem 2.1.1 (f) applied twice (to $2 \cdot (ab) = 0$, then to $ab = 0$) gives $a = 0$ or $b = 0$. If $b = 0$, then $a^2 = 7$. If $a = 0$, then $2b^2 = 7$, so $(2b)^2 = 14$. Both are excluded by the claim stated with Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 6.4.6: no natural number n with $k^2 < n < (k + 1)^2$ for some $k \in \mathbb{N}$ is the square of a rational; take $(n, k) = (7, 2)$, as $4 < 7 < 9$, and $(n, k) = (14, 3)$, as $9 < 14 < 16$. So 7 has no square root in $\mathbb{Q}(\sqrt{2})$. This is the method of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 6, which showed the same for 3.

Exercise. R3

Show that no relation $<$ makes $\mathbb{Q}(i)$ (Example (Rational and Integer Complex Numbers)) an ordered field, and none makes the four-element field F of Exercise C1 of Section 2.2 an ordered field.

Solution. F . In F , $1 + 1 = (1 + 1) + (0 + 0)\alpha = 0$, by the definition of the sum, with coefficients in $\mathbb{F}_2$. So $2 \cdot 1 = 0$ and $\text{char } F \neq 0$, while every ordered field has characteristic 0 (Example (The characteristics of the standard fields)). This is the method of Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.4.3 (e) and Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Example (A field with two elements that cannot be ordered): in an ordered field $n \cdot 1 > 0$ for $n \geq 1$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (h)), while here $2 \cdot 1 = 0$.

$\mathbb{Q}(i)$. This is the method of Proposition 1.4.3; the proposition itself does not apply, since an order on the subfield $\mathbb{Q}(i)$ need not extend to $\mathbb{C}$. Suppose $<$ made $\mathbb{Q}(i)$ an ordered field. Then $i \neq 0$ gives $i^2 > 0$, and $1 \neq 0$ gives $1 > 0$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (e)). But $i^2 = -1$ (Proposition 1.1.1; the operations of $\mathbb{Q}(i)$ are those of $\mathbb{C}$), and $1 > 0$ gives $-1 < 0$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (a)).

So $0 < -1 < 0$, and $0 < 0$ by transitivity, which is impossible for the strict part of an order. The characteristic does not help here, since $\text{char } \mathbb{Q}(i) = 0$ (Example (The characteristics of the standard fields)): the obstruction for $\mathbb{Q}(i)$ is a square, not a multiple of 1.

Exercise. R4

Find all homomorphisms $\mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{R}$.

Solution. There are exactly two: the inclusion $a + b\sqrt{2} \mapsto a + b\sqrt{2}$, and $a + b\sqrt{2} \mapsto a - b\sqrt{2}$.

Every homomorphism is one of them. Let $\sigma: \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{R}$ be a homomorphism. The inclusions $\mathbb{Q} \rightarrow \mathbb{Q}(\sqrt{2})$ and $\mathbb{Q} \rightarrow \mathbb{R}$ are homomorphisms (Example (Conjugation and Other Automorphisms) (ii); $\mathbb{Q}$ is a subfield of both), so they are $\iota_{\mathbb{Q}(\sqrt{2})}$ and $\iota_{\mathbb{R}}$ by the uniqueness clause of Theorem 2.5.5 (b) (both fields have characteristic 0, Example (The characteristics of the standard fields)). By Corollary 2.5.6 (a), $\sigma \circ \iota_{\mathbb{Q}(\sqrt{2})} = \iota_{\mathbb{R}}$: $\sigma(q) = q$ for every $q \in \mathbb{Q}$. Then

$$\sigma(\sqrt{2})^2 = \sigma((\sqrt{2})^2) = \sigma(2) = 2 = (\sqrt{2})^2,$$

so $\sigma(\sqrt{2}) = \sqrt{2}$ or $\sigma(\sqrt{2}) = -\sqrt{2}$ by Corollary 2.1.2 in $\mathbb{R}$. Hence $\sigma(a + b\sqrt{2}) = \sigma(a) + \sigma(b)\sigma(\sqrt{2}) = a \pm b\sqrt{2}$.

Both occur. The inclusion is a homomorphism (Example (Conjugation and Other Automorphisms) (ii)), and so is conjugation $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ of $\mathbb{Q}(\sqrt{2})$ followed by the inclusion (Example (Conjugation and Other Automorphisms) (iii) and Proposition 2.4.1 (e)). They differ at $\sqrt{2}$, since $\sqrt{2} > 0 > -\sqrt{2}$.

The tool, and the look-alikes. The tool is rigidity on the prime subfield (Corollary 2.5.6) followed by “push the equation $x^2 = 2$ through σ ”. The uniqueness theorem for complete ordered fields of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 6 (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Theorem 6.3.4) does not apply: it concerns maps of a complete ordered field to itself, and $\mathbb{Q}(\sqrt{2})$ is not complete. Nor does “a homomorphism into an ordered field preserves order”: the second homomorphism sends $\sqrt{2} > 0$ to $-\sqrt{2} < 0$.