

2.5 Integer Multiples, the Characteristic, and the Prime Subfield

Add 1 to itself in $\mathbb{Q}$ and the sums $1, 1+1, 1+1+1, \dots$ never return to 0. In $\mathbb{F}_2$ two copies of 1 already give 0, and in $\mathbb{F}_p$ it takes p copies. This one number decides whether “ $2x = 0$, so $x = 0$ ” is a valid step, and Section 2.4 showed that homomorphisms respect it: there is none from $\mathbb{F}_2$ to $\mathbb{Q}$ (Example (Pairs of Fields with No Homomorphism) (ii)). This section names the number, the **characteristic**, proves that it is 0 or a prime, and uses it to find the smallest subfield of every field: a copy of $\mathbb{Q}$ or of exactly one $\mathbb{F}_p$.

Throughout, F and L are fields (Definition 2.1.1), 0 and 1 are the zero and one of the field in play, and we write 1_F when two fields are in play at once.

2.5.1 Integer multiples

The question “can $1+1+\dots+1$ be 0?” is about the elements $n \cdot 1$. For $n \in \mathbb{N}$ these are already defined in every commutative ring. *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Section 2.3 (“Multiples”) defines, for a commutative ring R and $a \in R$, by recursion on $\mathbb{N} = \omega$,

$$0 \cdot a := 0, \quad (n+1) \cdot a := n \cdot a + a \quad (n \in \mathbb{N}).$$

So $1 \cdot a = a$, $2 \cdot a = a + a$, and $n \cdot a$ is the sum of n copies of a . We need negative multiples too, because the divisibility arguments below write $n = qc + r$ with q possibly negative.

Negative multiples. Every integer is m or $-m$ for some $m \in \mathbb{N}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Section 2.3 (there for natural numbers), Proposition 2.2.3 (c)). For $n \in \mathbb{Z}$ with $n < 0$ we have $-n > 0$, so $-n \in \mathbb{N}$ by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.3.4 (b), and we define

$$n \cdot a := -((-n) \cdot a).$$

So $(-3) \cdot a = -(a + a + a)$. Extending the convention of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Section 2.3 (there for natural numbers), a dot with an integer on its left always means this multiple, and the product of two ring elements is written by juxtaposition, ab . When $R = \mathbb{Z}$ the two readings agree: for $n \in \mathbb{N}$ this is the remark after the definition of multiples in that section, and for $n < 0$, $n \cdot a = -((-n)a) = -(-(na)) = na$ by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.2 (c) and (a).

The lemma below collects the rules for multiples. Parts (a)–(c) are the three identities that the linear-algebra volumes cite; part (d) extends everything to integer multiples.

Lemma 2.5.1. Integer Multiples

Let R be a commutative ring, $a, b \in R$, and $m, k \in \mathbb{N}$.

- (a) $(m \cdot 1) + (k \cdot 1) = (m + k) \cdot 1$.
- (b) $(m \cdot 1)(k \cdot 1) = (mk) \cdot 1$.
- (c) $(m \cdot 1)a = m \cdot a$.

(d) The identities (a)–(c) hold for **all** $m, k \in \mathbb{Z}$, and so do

$$\begin{aligned}(m+k) \cdot a &= m \cdot a + k \cdot a, & (-m) \cdot a &= -(m \cdot a), \\ m \cdot (a+b) &= m \cdot a + m \cdot b, & (m \cdot a)b &= m \cdot (ab), \\ (mk) \cdot a &= m \cdot (k \cdot a).\end{aligned}$$

In words: integer multiples obey the rules one expects of “ m copies of a ”, with signs behaving as in $\mathbb{Z}$. Since every field is a commutative ring (the remark after Definition 2.1.1), the lemma holds in every field.

Idea. For natural numbers everything is one induction each, on the recursion that defines $m \cdot a$: four rules for natural multiples (a sum law, a distributive law, a product law and a composition law) and then (a)–(c) as special cases with $a = 1$. Negative multiples are reduced to natural ones by writing an integer as a difference $m_1 - m_2$ of natural numbers; that bookkeeping is (d), and its proof is in the fold below.

Proof. All inductions are Logic and Proof, Axiom 4.2.1, read on $\mathbb{N} = \omega$ through Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\backslash)$, Corollary 1.7.3 (b). We first prove four rules for $m, k \in \mathbb{N}$.

(i) $(m+k) \cdot a = m \cdot a + k \cdot a$. Induction on k . For $k = 0$, $(m+0) \cdot a = m \cdot a = m \cdot a + 0 = m \cdot a + 0 \cdot a$ by (F3). If it holds for k , then

$$\begin{aligned}(m+(k+1)) \cdot a &= ((m+k)+1) \cdot a = (m+k) \cdot a + a \\ &= (m \cdot a + k \cdot a) + a = m \cdot a + (k+1) \cdot a,\end{aligned}$$

by the recursion, the induction hypothesis, (F2) and the recursion again. (This is the sum law of Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\backslash)$, Proposition 2.3.5 (h), whose proof uses no order.)

(ii) $m \cdot (a+b) = m \cdot a + m \cdot b$. Induction on m . For $m = 0$ both sides are 0 (with $0+0=0$ by (F3)). If it holds for m , then $(m+1) \cdot (a+b) = (m \cdot a + m \cdot b) + (a+b) = (m \cdot a + a) + (m \cdot b + b)$ by (F1) and (F2), which is $(m+1) \cdot a + (m+1) \cdot b$.

(iii) $(m \cdot a)b = m \cdot (ab)$. Induction on m . For $m = 0$, $(0 \cdot a)b = 0b = 0 = 0 \cdot (ab)$ by Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\backslash)$, Proposition 2.3.2 (b) and (F6). If it holds for m , then $((m+1) \cdot a)b = (m \cdot a + a)b = (m \cdot a)b + ab = m \cdot (ab) + ab = (m+1) \cdot (ab)$, by (F9) with (F6), and the induction hypothesis.

(iv) $(mk) \cdot a = m \cdot (k \cdot a)$. Induction on m . For $m = 0$ both sides are 0. If it holds for m , then, since $(m+1)k = mk + k$ in $\mathbb{N}$,

$$((m+1)k) \cdot a = (mk+k) \cdot a = (mk) \cdot a + k \cdot a = m \cdot (k \cdot a) + k \cdot a = (m+1) \cdot (k \cdot a),$$

by (i), the induction hypothesis and the recursion.

Now (a) is (i) with $a = 1$. For (c), $(m \cdot 1)a = m \cdot (1a) = m \cdot a$ by (iii), then (F6) and (F7). For (b), $(m \cdot 1)(k \cdot 1) = m \cdot (1(k \cdot 1)) = m \cdot (k \cdot 1) = (mk) \cdot 1$ by (iii), (F6) with (F7), and (iv). Part (d) is proved in the fold below. This proves the lemma.

■

○ **Second reading** · *Proof of (d): from natural to integer multiples*

Idea. Every integer is a difference $m_1 - m_2$ of natural numbers, and a negative multiple is the negative of a natural one. So each identity of (d) splits into identities for natural multiples, which are rules (i)–(iv), combined with the ring rules for negatives. Only the composition law needs the four sign cases separately, and a table keeps them apart.

Proof. Step 1: $(-m) \cdot a = -(m \cdot a)$ for every $m \in \mathbb{Z}$. If $m > 0$, then $-m < 0$ and the definition gives $(-m) \cdot a = -((-(-m)) \cdot a) = -(m \cdot a)$. If $m = 0$, both sides are 0, since $-0 = 0$ ($0 + 0 = 0$ and uniqueness of negatives, Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\mathbb{R}\backslash)$, Proposition 2.3.2 (a)). If $m < 0$, the definition gives $m \cdot a = -((-m) \cdot a)$, so $-(m \cdot a) = (-m) \cdot a$ because $-(-x) = x$ (Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\mathbb{R}\backslash)$, Proposition 2.3.2 (a)).

Step 2: $(m - k) \cdot a = m \cdot a - k \cdot a$ for $m, k \in \mathbb{N}$. If $m \geq k$, then $m - k \in \mathbb{N}$ and $(m - k) + k = m$, so $m \cdot a = (m - k) \cdot a + k \cdot a$ by rule (i) of the proof above; adding $-(k \cdot a)$ to both sides gives the claim. If $m < k$, then by Step 1 and the first case

$$(m - k) \cdot a = -((k - m) \cdot a) = -(k \cdot a - m \cdot a) = m \cdot a - k \cdot a,$$

the last step because $(k \cdot a - m \cdot a) + (m \cdot a - k \cdot a) = 0$ by (F1)–(F4), and negatives are unique.

Step 3: the sum, distributive and product rules. By Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\mathbb{R}\backslash)$, Proposition 2.2.3 (c), every integer is a difference $m_1 - m_2$ of natural numbers ($m = m - 0$, $-m = 0 - m$). Let $x = m_1 - m_2$ and $y = k_1 - k_2$ with $m_1, m_2, k_1, k_2 \in \mathbb{N}$. Then $x + y = (m_1 + k_1) - (m_2 + k_2)$, and by Step 2 and rule (i),

$$\begin{aligned} (x + y) \cdot a &= (m_1 \cdot a + k_1 \cdot a) - (m_2 \cdot a + k_2 \cdot a) \\ &= (m_1 \cdot a - m_2 \cdot a) + (k_1 \cdot a - k_2 \cdot a) = x \cdot a + y \cdot a, \end{aligned}$$

using $-(u + v) = (-u) + (-v)$ (both are negatives of $u + v$) and (F1), (F2). In the same way, Step 2 with rules (ii) and (iii) gives $x \cdot (a + b) = x \cdot a + x \cdot b$ and $(x \cdot a)b = (m_1 \cdot a)b - (m_2 \cdot a)b = x \cdot (ab)$, the middle step by (F9) and $(-u)b = -(ub)$ (Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\mathbb{R}\backslash)$, Proposition 2.3.2 (c)). From the distributive rule, $x \cdot c + x \cdot (-c) = x \cdot 0$, and $x \cdot 0 = (x \cdot 1)0 = 0$ by the product rule just proved (with $a = 1$, $b = 0$) and Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\mathbb{R}\backslash)$, Proposition 2.3.2 (b); so $x \cdot (-c) = -(x \cdot c)$.

Step 4: $(xy) \cdot a = x \cdot (y \cdot a)$. Write $x = \pm m'$ and $y = \pm k'$ with $m', k' \in \mathbb{N}$. In $\mathbb{Z}$, $(-m')k' = m'(-k') = -(m'k')$ and $(-m')(-k') = m'k'$ (Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\mathbb{R}\backslash)$, Proposition 2.3.2 (c)). Each row of the table reduces both sides to rule (iv), using Step 1 and the last line of Step 3.

x, y	$(xy) \cdot a$	$x \cdot (y \cdot a)$
m', k'	$(m'k') \cdot a$	$m' \cdot (k' \cdot a)$
$-m', k'$	$-((m'k') \cdot a)$	$-(m' \cdot (k' \cdot a))$
$m', -k'$	$-((m'k') \cdot a)$	$m' \cdot (-(k' \cdot a)) = -(m' \cdot (k' \cdot a))$
$-m', -k'$	$(m'k') \cdot a$	$-(m' \cdot (-(k' \cdot a))) = m' \cdot (k' \cdot a)$

Step 5: (a)–(c) for integers. (a) is the sum rule with $a = 1$. (c): $(x \cdot 1)a = x \cdot (1a) = x \cdot a$. (b): $(x \cdot 1)(y \cdot 1) = x \cdot (1(y \cdot 1)) = x \cdot (y \cdot 1) = (xy) \cdot 1$, by the product rule and Step 4. This proves (d). ■

Two readings of the lemma are used constantly. First, by (a) and (b) with (d), the map $\mathbb{Z} \rightarrow R$, $n \mapsto n \cdot 1$, turns sums of integers into sums in R and products into products, and sends 1 to $1 \cdot 1 = 1$. Second, by (c) with (d), every multiple $n \cdot a$ is a product in R , namely $(n \cdot 1)a$: to know how multiples behave, it is enough to know the elements $n \cdot 1$.

In $\mathbb{Z}/n\mathbb{Z}$ these elements are the classes themselves: $k \cdot [1] = [k]$ for $k \in \mathbb{N}$ (Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash nR\backslash)$, Theorem 3.4.3 (d)), and for $k < 0$, $k \cdot [1] = -((-k) \cdot [1]) = -[-k] = [k]$, since $-[u] = [-u]$ in a quotient ring (Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash nR\backslash)$, Theorem 3.4.1 (b)).

Quick check. In $\mathbb{Z}/5\mathbb{Z}$, compute $(-3) \cdot [2]$ in two ways: by the definition of a negative multiple, and by (c) of Lemma 2.5.1, extended to integers by (d).

Solution. By the definition, $(-3) \cdot [2] = -(3 \cdot [2]) = -([2] + [2] + [2]) = -[6] = [-6] = [4]$, since $-6 - 4 = -10$ is divisible by 5. By (c) and (d), $(-3) \cdot [2] = ((-3) \cdot [1])[2] = [-3][2] = [-6] = [4]$, using $k \cdot [1] = [k]$ for $k = -3$.

2.5.2 The characteristic

The elements $1, 2 \cdot 1, 3 \cdot 1, \dots$ of a field either never reach 0, or reach it for some positive n . In the second case the first time they reach it is the number that matters.

The characteristic counts how many copies of 1 add up to 0, and is 0 if no number of copies does.

Definition 2.5.1. Characteristic

Let F be a field. If **there exists** a positive integer n with $n \cdot 1 = 0$, the **characteristic** of F , written $\text{char } F$, is the **least** such n . If there is none, $\text{char } F := 0$.

In words: test $n = 1, 2, 3, \dots$ in turn; $\text{char } F$ is the first n with $n \cdot 1 = 0$, and 0 if the test never stops. The same words define the characteristic of a commutative ring.

Well-definedness. If the set $S := \{n \in \mathbb{Z}_{>0} : n \cdot 1 = 0\}$ is non-empty, it is a non-empty set of integers bounded below by 1, so it has a least element by Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash nR\backslash)$, Proposition 2.3.6. So “the least such n ” names exactly one integer.

First examples.

- $\mathbb{F}_2$: $1 \cdot 1 = 1 \neq 0$ and $2 \cdot 1 = 1 + 1 = 0$ by the table of Example (Arithmetic on $\mathbb{Z}/n\mathbb{Z}$ and the Field $\mathbb{F}_2$), so $\text{char } \mathbb{F}_2 = 2$.
- $\mathbb{F}_3$: $1 \cdot 1 = 1$, $2 \cdot 1 = 2$, $3 \cdot 1 = 3 = 0$, and $1, 2 \neq 0$ in $\mathbb{F}_3$, so $\text{char } \mathbb{F}_3 = 3$.

- $\mathbb{Q}$: $n \cdot 1 = n \neq 0$ for every $n \geq 1$, so $\text{char } \mathbb{Q} = 0$. The reason is the order of $\mathbb{Q}$; the example at the end of the next subsection gives it.
- The ring $\mathbb{Z}/6\mathbb{Z}$, which is not a field: $k \cdot [1] = [k] \neq [0]$ for $k = 1, \dots, 5$ and $6 \cdot [1] = [0]$, so it has characteristic 6.

The degenerate case. In the zero ring $\{0\}$ of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Section 2.3, $1 = 0$, so $1 \cdot 1 = 1 = 0$ and the characteristic is 1. It is the only ring of characteristic 1: characteristic 1 means $1 = 1 \cdot 1 = 0$, and then every $a = a \cdot 1 = a \cdot 0 = 0$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.2 (b)). It is not a field. For fields, the clause $1 \neq 0$ of (F7) rules out characteristic 1, and that is the first step of the theorem below on which characteristics occur.

Why 0 and not “infinity”. The convention $\text{char } F = 0$ makes the next proposition read the same in every case: $n \cdot 1 = 0$ exactly when $\text{char } F$ divides n . For $\text{char } F = 0$ this says $n \cdot 1 = 0$ only for $n = 0$, because $0 \mid n$ only for $n = 0$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 3.1.1 (a)).

The proposition is the form in which the characteristic is used. Its proof is the move of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 3: take the least positive element, then divide by it.

Proposition 2.5.2. The Characteristic Divides Every Vanishing Multiple

Let F be a field, $c := \text{char } F$, and $n \in \mathbb{Z}$.

- (a) $n \cdot 1 = 0$ if and only if $c \mid n$.
- (b) $n \cdot 1$ is invertible in F if and only if $c \nmid n$. In particular $2 := 1 + 1$ is invertible in F if and only if $\text{char } F \neq 2$.

Idea. For $c > 0$, divide n by c with remainder, $n = qc + r$. The multiple $c \cdot 1$ is 0, so the rules of Lemma 2.5.1 kill the part qc and leave $n \cdot 1 = r \cdot 1$. The remainder is smaller than c , and c was the **least** positive integer with a vanishing multiple, so $r \cdot 1 = 0$ forces $r = 0$. For $c = 0$ there is nothing to divide: no positive multiple vanishes, and negatives follow by a sign.

Proof.

- (a) *Case $c = 0$.* We show $n \cdot 1 = 0$ iff $n = 0$, which is the claim since $0 \mid n$ iff $n = 0$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 3.1.1 (a)). If $n = 0$, $n \cdot 1 = 0$. If $n > 0$, then $n \cdot 1 \neq 0$ by Definition 2.5.1, since $c = 0$ means no positive multiple vanishes. If $n < 0$, then $n \cdot 1 = -((-n) \cdot 1)$ with $(-n) \cdot 1 \neq 0$; and $-x = 0$ would give $x = -(-x) = -0 = 0$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.2 (a)), so $n \cdot 1 \neq 0$.

Case $c > 0$. ($\Leftarrow$) If $c \mid n$, say $n = qc$ with $q \in \mathbb{Z}$, then by Lemma 2.5.1 (b), which holds for integers by part (d),

$$n \cdot 1 = (qc) \cdot 1 = (q \cdot 1)(c \cdot 1) = (q \cdot 1)0 = 0,$$

the last step by Theorem 2.1.1 (d) and (F6).

($\Rightarrow$) Suppose $n \cdot 1 = 0$. By Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.1.2 there are $q, r \in \mathbb{Z}$ with $n = qc + r$ and $0 \leq r < c$. By the sum rule of Lemma 2.5.1 (d) and the computation just made,

$$0 = n \cdot 1 = (qc) \cdot 1 + r \cdot 1 = 0 + r \cdot 1 = r \cdot 1,$$

using (F1) and (F3) at the end. If $r > 0$, then r is a positive integer with $r \cdot 1 = 0$ and $r < c$, against the minimality of c in [Definition 2.5.1](#). So $r = 0$, and $n = qc$, that is, $c \mid n$.

- (b) In a field an element is invertible if and only if it is non-zero: a non-zero element has an inverse by (F8), and 0 has none, since $0 \cdot y = 0 \neq 1$ (Theorem 2.1.1 (d), and $1 \neq 0$ by (F7)). So (b) is (a) negated. For $n = 2$: $2 \cdot 1 = (0 \cdot 1 + 1) + 1 = 1 + 1$. The positive divisors of 2 are 1 and 2 (2 is prime), and $0 \nmid 2$; and $c \neq 1$, since $1 \cdot 1 = 1 \neq 0$. So $c \mid 2$ iff $c = 2$, and $1 + 1$ is invertible iff $c \neq 2$. This proves the proposition. ■

This is the form the linear-algebra volumes use, in sentences such as “ $\text{char } F \neq 2$, so 2 is invertible” and “ $m \cdot 1$ is invertible when $\text{char } F \nmid m$ ”. It also says that the integers n with $n \cdot 1 = 0$ are exactly the multiples of one integer, c , with nothing else vanishing by accident.

Warning. In characteristic 2, $1 + 1 = 0$, so $-1 = 1$ and $x = -x$ for every x . The familiar step “ $x = -x$, so $2x = 0$, so $x = 0$ ” divides by $2 = 1 + 1$, which is 0 there. In $\mathbb{F}_2$, the element 1 satisfies $1 = -1$ and $1 \neq 0$. This is why many later results, for instance about symmetric and alternating bilinear forms in the linear-algebra volumes, assume $\text{char } F \neq 2$: by [Proposition 2.5.2](#) (b), that is exactly the hypothesis that makes the step valid.

Example. Completing the square in $\mathbb{F}_3$

Solve $x^2 + x + 1 = 0$ in $\mathbb{F}_3$ by completing the square.

Solution. Since $\text{char } \mathbb{F}_3 = 3 \neq 2$ (the first examples above), $2 = 1 + 1$ is invertible by [Proposition 2.5.2](#) (b); indeed $2 \cdot 2 = 4 = 1$, so $2^{-1} = 2$. Also $4 = 1 \neq 0$, so $x^2 + x + 1 = 0$ holds if and only if $4(x^2 + x + 1) = 0$ (one direction by Theorem 2.1.1 (d) and (F6), the other by (f)). By Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.2 (d), with the multiples regrouped by [Lemma 2.5.1](#) (b), (F5) and (F6), $(2x + 1)^2 = 4x^2 + 4x + 1$, so

$$4(x^2 + x + 1) = (2x + 1)^2 + 3 = (2x + 1)^2,$$

as $3 = 0$ in $\mathbb{F}_3$. So the equation says $(2x + 1)^2 = 0$, that is, $2x + 1 = 0$ by Theorem 2.1.1 (f), and $x = 2^{-1}(-1) = 2 \cdot 2 = 1$ by Proposition 2.1.3 (a), using $-1 = 2$. Testing all three elements agrees: $x = 0, 1, 2$ give 1, 3 = 0 and 7 = 1. In $\mathbb{F}_2$ the method stops at the first step: there $2 = 0$ and $4 = 0$, so multiplying by 4 cannot be undone and 2 has no inverse.

The characteristics found so far are 0, 2 and 3, and the ring $\mathbb{Z}/6\mathbb{Z}$ has characteristic 6. A field cannot.

Theorem 2.5.3. The Characteristic Is Zero or a Prime

Let F be a field. Then $\text{char } F$ is 0 or a prime.

Idea. This is the argument that showed $\mathbb{Z}/n\mathbb{Z}$ is not a field for composite n (Theorem 2.2.2), run inside F . If $c = rs$ with smaller factors, then $(r \cdot 1)(s \cdot 1) = c \cdot 1 = 0$. A field has no zero divisors, so one of the two factors is already 0, at a multiple smaller than c .

Proof. Let $c := \text{char } F$ and suppose $c > 0$. Since $1 \cdot 1 = 1 \neq 0$ by (F7), $c \neq 1$, so $c \geq 2$. Suppose c is not prime. By Sets, Relations, and Cardinality, Definition 2.2.2 it has a positive divisor $r \notin \{1, c\}$; write $c = rs$ with $s \in \mathbb{Z}$. Then $s > 0$, as $r, c > 0$, and $s \mid c$; $r \leq c$ and $s \leq c$ by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 3.1.1 (e); and $s \neq 1$, $s \neq c$, since $s = 1$ would give $r = c$ and $s = c$ would give $r = 1$ (cancel $c \neq 0$ in $\mathbb{Z}$). So $1 < r < c$ and $1 < s < c$. By Lemma 2.5.1 (b),

$$(r \cdot 1)(s \cdot 1) = (rs) \cdot 1 = c \cdot 1 = 0,$$

so $r \cdot 1 = 0$ or $s \cdot 1 = 0$ by Theorem 2.1.1 (f). Either way a positive integer smaller than c has a vanishing multiple, against the minimality of c . Hence c is prime. This proves the theorem. ■

So the possible characteristics of fields are $0, 2, 3, 5, 7, 11, \dots$, and the example at the end of the next subsection shows that each of them occurs. The hypothesis “field” is used twice, at $1 \neq 0$ and at “no zero divisors”, and the ring $\mathbb{Z}/6\mathbb{Z}$ shows the second cannot be dropped: there $[2][3] = [0]$.

2.5.3 The characteristic under subfields and homomorphisms

The characteristic is computed from 0, 1 and $+$ alone. A subfield has the same three, and a homomorphism carries them over, so both must preserve it.

Proposition 2.5.4. Subfields and Homomorphisms Preserve the Characteristic

- (a) If K is a subfield of L , then $\text{char } K = \text{char } L$.
- (b) If $\varphi: F \rightarrow L$ is a homomorphism, then $\text{char } F = \text{char } L$.
- (c) There is no homomorphism between two fields of different characteristic.

Proof.

- (a) By Proposition 2.3.1 (a), K has the zero 0_L , the one 1_L , and the restricted addition of L . Hence $n \cdot 1_K = n \cdot 1_L$ for every $n \in \mathbb{N}$, by induction (Logic and Proof, Axiom 4.2.1): both are 0_L at $n = 0$, and both add 1_L at each step. So the sets of positive n with $n \cdot 1 = 0$ are the same in K and in L , and so are their least elements, or both sets are empty.
- (b) For $n \in \mathbb{N}$, $\varphi(n \cdot 1_F) = n \cdot \varphi(1_F) = n \cdot 1_L$ by Proposition 2.4.1 (f) and Definition 2.4.1. Since $\varphi(0) = 0$ (Proposition 2.4.1 (a)) and φ is injective (part (c) there), $n \cdot 1_F = 0$ if and only if $\varphi(n \cdot 1_F) = 0$, that is, if and only if $n \cdot 1_L = 0$. As in (a), the two characteristics coincide.

(c) is (b) read contrapositively. This proves the proposition. ■

Part (c) explains two of the obstructions of Section 2.4 at once: there is no homomorphism $\mathbb{F}_2 \rightarrow \mathbb{Q}$ and none $\mathbb{Q} \rightarrow \mathbb{F}_p$ (Example (Pairs of Fields with No Homomorphism) (ii), (iii)), because the characteristics are 2 and 0, and 0 and p .

Example. The characteristics of the standard fields

Find the characteristic of every ordered field, of $\mathbb{Q}$ and $\mathbb{R}$, of $\mathbb{C}$, of $\mathbb{F}_p$ for a prime p , and of $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(i)$.

Solution. Ordered fields. Let F be an ordered field (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 2.3.2). Since $1 \neq 0$, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (h) gives $n \cdot 1 > 0$ for every $n \in \mathbb{N}$ with $n \geq 1$; in particular $n \cdot 1 \neq 0$. So no positive multiple of 1 vanishes, and $\text{char } F = 0$.

$\mathbb{Q}$ and $\mathbb{R}$. Both are ordered fields (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.5.1, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 5.3.3), so both have characteristic 0. For $\mathbb{R}$ one can also use Proposition 2.5.4 (a), as $\mathbb{Q}$ is a subfield of $\mathbb{R}$ (Example (Rational and Integer Complex Numbers) (iii)).

$\mathbb{C}$. The field $\mathbb{R}$ is a subfield of $\mathbb{C}$ (Example (Rational and Integer Complex Numbers) (iii)), so $\text{char } \mathbb{C} = \text{char } \mathbb{R} = 0$ by Proposition 2.5.4 (a). This argument uses no order on $\mathbb{C}$.

$\mathbb{F}_p$. (In this section we keep the brackets on classes of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ wherever integers and their classes appear side by side, as in $n \cdot [1] = [n]$; elsewhere elements of $\mathbb{F}_p$ are written without brackets, as in Section 2.2.) For $n \in \mathbb{N}$, $n \cdot [1] = [n]$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.4.3 (d)), and $[n] = [0]$ if and only if $n \in p\mathbb{Z}$, that is, $p \mid n$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.4.1 (d)). A positive n with $p \mid n$ has $p \leq n$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 3.1.1 (e)), and $p \mid p$. So the least positive n with $n \cdot [1] = [0]$ is p , and $\text{char } \mathbb{F}_p = p$.

$\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(i)$. They are subfields of $\mathbb{R}$ and of $\mathbb{C}$ (Example (The Field Generated by the Square Root of Two), Example (Rational and Integer Complex Numbers) (i)), so both have characteristic 0 by Proposition 2.5.4 (a).

So every prime occurs as a characteristic, and so does 0. The four-element field of Section 2.2's Exercise C1 has characteristic 2; Exercise C3 below checks it, and nothing here depends on it.

Quick check. What are $\text{char } \mathbb{F}_7$ and $\text{char } \mathbb{Q}(\sqrt{2})$? Is $7 \cdot [3] = [1]$ in $\mathbb{F}_5$?

Solution. $\text{char } \mathbb{F}_7 = 7$ and $\text{char } \mathbb{Q}(\sqrt{2}) = 0$ (Example (The characteristics of the standard fields)). Yes: $7 \cdot [3] = (7 \cdot [1])[3] = [7][3] = [21]$ by Lemma 2.5.1 (c), and $[21] = [1]$ since $21 - 1 = 20 = 4 \cdot 5$. Equivalently, $7 \cdot [3] = 2 \cdot [3]$ because $5 \cdot [3] = [0]$, and $2 \cdot [3] = [6] = [1]$.

2.5.4 The prime subfield

Section 2.3 defined the prime subfield of a field F as the smallest subfield, the intersection of all subfields of F (Definition 2.3.2), and promised to identify it. Every subfield contains 1, hence every $n \cdot 1$, hence every quotient $(m \cdot 1)(n \cdot 1)^{-1}$ with $n \cdot 1 \neq 0$. The characteristic decides which of these quotients exist, and so which number system the prime subfield copies.

The identification goes through a homomorphism into F , and the main point is that there is exactly one. For ordered fields this is *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 4's embedding $\iota_F: \mathbb{Q} \rightarrow F$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 4.2.2). We keep the name ι_F , and, as before, the brackets on the classes of $\mathbb{F}_p$.

Theorem 2.5.5. The Prime Subfield

Let F be a field and P its prime subfield (Definition 2.3.2).

- (a) If $\text{char } F = p > 0$, then $\iota_F([n]) := n \cdot 1$ ($n \in \mathbb{Z}$) is a well-defined homomorphism $\iota_F: \mathbb{F}_p \rightarrow F$. It is the **only** homomorphism $\mathbb{F}_p \rightarrow F$, and its image is P . Hence $P \cong \mathbb{F}_p$.
- (b) If $\text{char } F = 0$, then $\iota_F(m/n) := (m \cdot 1)(n \cdot 1)^{-1}$ ($m \in \mathbb{Z}$, $n \in \mathbb{Z}_{>0}$) is a well-defined homomorphism $\iota_F: \mathbb{Q} \rightarrow F$. It is the **only** homomorphism $\mathbb{Q} \rightarrow F$, and its image is P . Hence $P \cong \mathbb{Q}$.

In (a), p is prime by Theorem 2.5.3, so $\mathbb{F}_p$ is a field (Definition 2.2.1) and “homomorphism $\mathbb{F}_p \rightarrow F$ ” has a meaning.

Try it first (ten minutes): a homomorphism $\psi: \mathbb{Q} \rightarrow F$ must send 1 to 1. Where must it send 3, -3 and $1/3$? What could go wrong with $1/3$?

Idea. An attempt runs as follows. $\psi(3) = \psi(1+1+1) = 1+1+1 = 3 \cdot 1$, then $\psi(-3) = -\psi(3) = (-3) \cdot 1$, and $\psi(1/3)$ must be the inverse of $\psi(3)$, so $\psi(1/3) = (3 \cdot 1)^{-1}$. The homomorphism has no freedom at all: it is determined by $\psi(1) = 1$, through sums, negatives and inverses. That gives **uniqueness**, and it also dictates the only possible formula, $m/n \mapsto (m \cdot 1)(n \cdot 1)^{-1}$.

What can go wrong is $1/3$: if $3 \cdot 1 = 0$ in F , it has no inverse, and no homomorphism exists. The characteristic says exactly when this happens. In characteristic 0 the formula makes sense, and what remains is to check that it does not depend on how a rational is written, which follows from Lemma 2.5.1 (b) and a regrouping by (F5)–(F8), and that it respects $+$ and $\cdot$, which the fraction rules of Theorem 2.1.1 (g) give. In characteristic p , the classes $[n]$ play the role of the rationals, and $p \cdot 1 = 0$ is exactly what makes $[n] \mapsto n \cdot 1$ well defined. The image is then a subfield (Section 2.4) built from 1 alone, so it lies inside every subfield: it is the prime subfield.

Before reading on: where is $\text{char } F = 0$ used in (b), and why does the same formula fail for $F = \mathbb{F}_5$?

Proof. Part (a). Let $\text{char } F = p > 0$.

Well defined. Every element of $\mathbb{F}_p$ is a class $[n]$ with $n \in \mathbb{Z}$ (Sets, Relations, and Cardinality, Definition 2.5.4). If $[n] = [n']$, then $p \mid n - n'$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.4.1 (a), for the ideal $p\mathbb{Z}$), so $(n - n') \cdot 1 = 0$ by Proposition 2.5.2 (a), and

$n \cdot 1 - n' \cdot 1 = (n - n') \cdot 1 = 0$ by [Lemma 2.5.1](#) (d). So $n \cdot 1 = n' \cdot 1$: the value does not depend on the representative. (This is Number Systems: From $\backslash(\backslash nN \backslash)$ to $\backslash(\backslash nR \backslash)$, Theorem 2.2.1 (a) with equality as the relation on F , whose classes are the singletons $\{y\}$, followed by $\{y\} \mapsto y$.)

Homomorphism. For $m, n \in \mathbb{Z}$, by the operations of $\mathbb{Z}/p\mathbb{Z}$ (Number Systems: From $\backslash(\backslash nN \backslash)$ to $\backslash(\backslash nR \backslash)$, Theorem 3.4.1 (b)) and [Lemma 2.5.1](#) (d), parts (a) and (b) there,

$$\begin{aligned}\iota_F([m] + [n]) &= \iota_F([m + n]) = (m + n) \cdot 1 = m \cdot 1 + n \cdot 1, \\ \iota_F([m][n]) &= \iota_F([mn]) = (mn) \cdot 1 = (m \cdot 1)(n \cdot 1),\end{aligned}$$

and $\iota_F([1]) = 1 \cdot 1 = 1$. So ι_F is a homomorphism (Definition 2.4.1).

Image = P. The image $\iota_F(\mathbb{F}_p)$ is a subfield of F (Proposition 2.4.1 (d)), and P is contained in every subfield (Definition 2.3.2), so $P \subseteq \iota_F(\mathbb{F}_p)$. Conversely, let K be any subfield of F . It contains 0 and 1 and is closed under $+$ (Definition 2.3.1), so $n \cdot 1 \in K$ for every $n \in \mathbb{N}$, by induction on n (Logic and Proof, Axiom 4.2.1): $0 \cdot 1 = 0 \in K$, and $(n+1) \cdot 1 = n \cdot 1 + 1 \in K$. It is closed under negatives, so $n \cdot 1 = -((-n) \cdot 1) \in K$ for $n < 0$ as well. So $\iota_F(\mathbb{F}_p) \subseteq K$ for every subfield K , that is, $\iota_F(\mathbb{F}_p) \subseteq P$.

Uniqueness. Let $\psi: \mathbb{F}_p \rightarrow F$ be a homomorphism and $n \in \mathbb{Z}$. Then $[n] = n \cdot [1]$ (Number Systems: From $\backslash(\backslash nN \backslash)$ to $\backslash(\backslash nR \backslash)$, Theorem 3.4.3 (d), extended to $n < 0$ after [Lemma 2.5.1](#)). For $n \in \mathbb{N}$, $\psi(n \cdot [1]) = n \cdot \psi([1]) = n \cdot 1$ by Proposition 2.4.1 (f); for $n < 0$,

$$\psi(n \cdot [1]) = \psi(-((-n) \cdot [1])) = -((-n) \cdot 1) = n \cdot 1,$$

by the definition of negative multiples at both ends, and in the middle by Proposition 2.4.1 (a) followed by the case $-n \in \mathbb{N}$ just done. So $\psi([n]) = n \cdot 1 = \iota_F([n])$ for every n , and $\psi = \iota_F$.

Finally, ι_F is an isomorphism from $\mathbb{F}_p$ onto its image P by Proposition 2.4.1 (d), so $P \cong \mathbb{F}_p$.

Part (b). Let $\text{char } F = 0$. Recall that $\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}_{>0})/\sim$ (Number Systems: From $\backslash(\backslash nN \backslash)$ to $\backslash(\backslash nR \backslash)$, Definition 2.4.1), that the class $[(m, n)]$ is the quotient m/n of the integers m and n in $\mathbb{Q}$ (Number Systems: From $\backslash(\backslash nN \backslash)$ to $\backslash(\backslash nR \backslash)$, Proposition 2.4.4 (a)), and that for $n, n' \in \mathbb{Z}_{>0}$, $m/n = m'/n'$ if and only if $mn' = m'n$ (part (b) there).

The formula makes sense. For $n > 0$, $n \cdot 1 \neq 0$ by [Proposition 2.5.2](#) (a), since $0 \nmid n$. So $(n \cdot 1)^{-1}$ exists by (F8). This is the only place where $\text{char } F = 0$ is used.

Well defined. Let $m/n = m'/n'$ with $n, n' > 0$, so $mn' = m'n$. By [Lemma 2.5.1](#) (d), part (b) there,

$$(m \cdot 1)(n' \cdot 1) = (mn') \cdot 1 = (m'n) \cdot 1 = (m' \cdot 1)(n \cdot 1).$$

Multiply both sides by $(n \cdot 1)^{-1}(n' \cdot 1)^{-1}$ and regroup by (F5), (F6), (F8) and (F7): the left side becomes $(m \cdot 1)(n \cdot 1)^{-1}$ and the right side $(m' \cdot 1)(n' \cdot 1)^{-1}$. So the value does not depend on the representative.

Homomorphism. Let $m/n, r/s \in \mathbb{Q}$ with $n, s > 0$, and put $\bar{m} := m \cdot 1$, and likewise $\bar{n}, \bar{r}, \bar{s}$. By Number Systems: From $\backslash(\backslash nN \backslash)$ to $\backslash(\backslash nR \backslash)$, Definition 2.4.2, $m/n + r/s = (ms + rn)/(ns)$ and $(m/n)(r/s) = (mr)/(ns)$, with $ns > 0$. By [Lemma 2.5.1](#) (d), $(ms + rn) \cdot 1 = \bar{m}\bar{s} + \bar{r}\bar{n}$, $(mr) \cdot 1 = \bar{m}\bar{r}$ and $(ns) \cdot 1 = \bar{n}\bar{s}$. So, by the fraction rules Theorem 2.1.1 (g) in F (with

$\bar{n}, \bar{s} \neq 0$),

$$\begin{aligned}\iota_F\left(\frac{m}{n} + \frac{r}{s}\right) &= \frac{\bar{m}\bar{s} + \bar{n}\bar{r}}{\bar{n}\bar{s}} = \frac{\bar{m}}{\bar{n}} + \frac{\bar{r}}{\bar{s}}, \\ \iota_F\left(\frac{m}{n} \cdot \frac{r}{s}\right) &= \frac{\bar{m}\bar{r}}{\bar{n}\bar{s}} = \frac{\bar{m}}{\bar{n}} \cdot \frac{\bar{r}}{\bar{s}},\end{aligned}$$

where $x/y := xy^{-1}$ in F and $\bar{r}\bar{n} = \bar{n}\bar{r}$ by (F6). Also $\iota_F(1) = \iota_F(1/1) = (1 \cdot 1)(1 \cdot 1)^{-1} = 1 \cdot 1^{-1} = 1$. So ι_F is a homomorphism.

Image = P. As in (a), $P \subseteq \iota_F(\mathbb{Q})$ because the image is a subfield. Conversely, every subfield K contains $m \cdot 1$ and $n \cdot 1$ (as in (a)), hence $(n \cdot 1)^{-1}$, as $n \cdot 1 \neq 0$, and the product $(m \cdot 1)(n \cdot 1)^{-1}$ (Definition 2.3.1). So $\iota_F(\mathbb{Q}) \subseteq P$.

Uniqueness. Let $\psi: \mathbb{Q} \rightarrow F$ be a homomorphism. In $\mathbb{Q}$, the integer $m \in \mathbb{Z} \subseteq \mathbb{Q}$ is the multiple $m \cdot 1_{\mathbb{Q}}$: the embedding j of Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\backslash)$, Proposition 2.4.4 has $j(0) = 0$ and $j(k+1) = j(k) + 1$, so $j(k) = k \cdot 1_{\mathbb{Q}}$ for $k \in \mathbb{N}$ by induction, and $j(-k) = -j(k) = (-k) \cdot 1_{\mathbb{Q}}$. As in (a), $\psi(m \cdot 1_{\mathbb{Q}}) = m \cdot 1$ for every $m \in \mathbb{Z}$, by Proposition 2.4.1 (f) and (a). For $n > 0$, $m/n = mn^{-1}$ in $\mathbb{Q}$ with $n \neq 0$ (Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\backslash)$, Proposition 2.4.4 (a)), so by Proposition 2.4.1 (b),

$$\psi\left(\frac{m}{n}\right) = \psi(m) \psi(n^{-1}) = \psi(m) \psi(n)^{-1} = (m \cdot 1)(n \cdot 1)^{-1} = \iota_F\left(\frac{m}{n}\right).$$

So $\psi = \iota_F$. As in (a), ι_F is an isomorphism onto P , and $P \cong \mathbb{Q}$. This proves the theorem. ■

Answer to the prompt. In (b), $\text{char } F = 0$ is used only to know that $n \cdot 1 \neq 0$ for $n > 0$, so that $(n \cdot 1)^{-1}$ exists; every other step works in any field. In $F = \mathbb{F}_5$, $5 \cdot 1 = 0$, so “ $1/5 \mapsto (1 \cdot 1)(5 \cdot 1)^{-1}$ ” names no element: the formula has no meaning there, which matches Example (Pairs of Fields with No Homomorphism) (iii), where no homomorphism $\mathbb{Q} \rightarrow \mathbb{F}_p$ exists at all.

🔄 Second reading · Two remarks on the formulas

Two consequences of the formulas are worth recording, though nothing below rests on them. For $F = \mathbb{Q}$, $\iota_{\mathbb{Q}}(m/n) = j(m)j(n)^{-1} = m/n$, so $\iota_{\mathbb{Q}} = \text{id}_{\mathbb{Q}}$; for $F = \mathbb{F}_p$, $\iota_{\mathbb{F}_p}([n]) = n \cdot [1] = [n]$, so $\iota_{\mathbb{F}_p} = \text{id}_{\mathbb{F}_p}$. And in (b) the formula also holds for negative denominators: if $n < 0$, then $m/n = (-m)/(-n)$ with $-n > 0$, and $((-m) \cdot 1)((-n) \cdot 1)^{-1} = (-\bar{m})(-\bar{n})^{-1} = \bar{m}\bar{n}^{-1}$, because $(-\bar{n})^{-1} = -\bar{n}^{-1}$ (their product with $-\bar{n}$ is $\bar{n}\bar{n}^{-1} = 1$ by Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\backslash)$, Proposition 2.3.2 (c)).

Remark. For an ordered field F , part (b) is Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\backslash)$, Theorem 4.2.2, where order supplied $n \cdot 1 > 0$ (Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\backslash)$, Proposition 4.2.1); by uniqueness the two maps called ι_F are the same map. Here the characteristic supplies the weaker fact $n \cdot 1 \neq 0$, which is all the construction needs. The same “no freedom on 1” argument gave *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 6’s Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\backslash)$, Proposition 6.1.1.

The uniqueness half of the theorem is a rigidity statement. It says that a homomorphism has

no choice on the prime subfield, and the next corollary spells this out.

Corollary 2.5.6. Homomorphisms Respect the Prime Subfield

- (a) Let $\varphi: F \rightarrow L$ be a homomorphism. Then $\varphi \circ \iota_F = \iota_L$, and φ maps the prime subfield of F onto the prime subfield of L .
- (b) The identity is the only homomorphism $\mathbb{Q} \rightarrow \mathbb{Q}$, and the only homomorphism $\mathbb{F}_p \rightarrow \mathbb{F}_p$ for each prime p . In particular the only automorphism of $\mathbb{Q}$, and of $\mathbb{F}_p$, is the identity.
- (c) Every automorphism of a field F fixes each element of the prime subfield of F .

Proof.

- (a) By [Proposition 2.5.4](#) (b), $\text{char } F = \text{char } L$, so ι_F and ι_L have the same domain D , which is $\mathbb{Q}$ or $\mathbb{F}_p$ by [Theorem 2.5.5](#). The composite $\varphi \circ \iota_F: D \rightarrow L$ is a homomorphism ([Proposition 2.4.1](#) (e)), so it equals ι_L by the uniqueness clause of [Theorem 2.5.5](#). Hence $\varphi(\iota_F(D)) = \iota_L(D)$, and by [Theorem 2.5.5](#) these images are the prime subfields of F and of L .
- (b) The identity $\text{id}_{\mathbb{Q}}$ is a homomorphism ([Proposition 2.4.1](#) (e)), and $\text{char } \mathbb{Q} = 0$ ([Example \(The characteristics of the standard fields\)](#)), so by the uniqueness clause of [Theorem 2.5.5](#) (b) with $F = \mathbb{Q}$, every homomorphism $\mathbb{Q} \rightarrow \mathbb{Q}$ equals $\text{id}_{\mathbb{Q}}$. Likewise for $\mathbb{F}_p$, using $\text{char } \mathbb{F}_p = p$ and part (a) of the theorem. An automorphism is a homomorphism, so it is the identity.
- (c) Let σ be an automorphism of F . By (a) with $L = F$, $\sigma \circ \iota_F = \iota_F$, so $\sigma(x) = x$ for every $x = \iota_F(d)$ in the image of ι_F , which is the prime subfield. This proves the corollary. ■

For instance, complex conjugation fixes every rational number, and the automorphisms of $\mathbb{Q}(\sqrt{2})$ and of $\mathbb{Q}(i)$ in Section 2.4 had no choice on $\mathbb{Q}$; only the images of $\sqrt{2}$ and of i were free.

Finite fields are the case that matters most for computation, and for them the characteristic cannot be 0.

Corollary 2.5.7. A Finite Field Has Prime Characteristic

Let F be a finite field.

- (a) $\text{char } F$ is a prime p .
- (b) F contains a subfield isomorphic to $\mathbb{F}_p$, namely its prime subfield.
- (c) $p \cdot a = 0$ for every $a \in F$.

Proof.

- (a) Say F has N elements ([Sets, Relations, and Cardinality](#), [Definition 3.1.2](#)). Suppose $\text{char } F = 0$, and consider $f: \{1, \dots, N+1\} \rightarrow F$, $f(k) := k \cdot 1$. If $k \cdot 1 = k' \cdot 1$, then $(k - k') \cdot 1 = 0$ ([Lemma 2.5.1](#) (d)), so $0 \mid k - k'$ by [Proposition 2.5.2](#) (a), hence $k - k' = 0$ ([Number Systems: From \$\mathbb{N}\$ to \$\mathbb{R}\$](#) , [Proposition 3.1.1](#) (a)) and $k = k'$. So f is an injection from a set with $N+1$ elements into a set with N elements, which [Sets, Relations, and Cardinality](#), [Corollary 3.1.3](#) (a) forbids. Hence $\text{char } F \neq 0$, and $\text{char } F$

is a prime by [Theorem 2.5.3](#).

(b) is [Theorem 2.5.5](#) (a).

(c) By [Lemma 2.5.1](#) (c), $p \cdot a = (p \cdot 1)a = 0 \cdot a = 0$, using [Theorem 2.1.1](#) (d). This proves the corollary. ■

A finite field therefore contains one of the fields $\mathbb{F}_p$ of Section 2.2. One can show that it has p^n elements for some $n \geq 1$; that needs the vector spaces of the linear-algebra volumes, and nothing in this volume uses it.

Quick check. Can a field with 6 elements contain a copy of $\mathbb{F}_2$ and also a copy of $\mathbb{F}_3$?

Solution. No. A copy of $\mathbb{F}_2$ is a subfield K with $\text{char } K = 2$, and a copy of $\mathbb{F}_3$ a subfield with characteristic 3 ([Example \(The characteristics of the standard fields\)](#), [Proposition 2.5.4](#) (b) for the isomorphisms). By [Proposition 2.5.4](#) (a) both characteristics equal $\text{char } F$, and $2 \neq 3$. (In fact no field has 6 elements, but that is the p^n fact just mentioned, which we do not prove.)

2.5.5 Exercises

2.5.5.1 A. Check your understanding

Exercise. A1

These parts are about the proof of [Theorem 2.5.5](#).

- (a) In the proof of part (b), where is the hypothesis $\text{char } F = 0$ used, and where is it not needed?
- (b) Try to define $\mathbb{Q} \rightarrow \mathbb{F}_5$ by $m/n \mapsto [m][n]^{-1}$ ($n > 0$). Name a rational number that has no image, and explain why the rule also fails to be well defined.
- (c) What are $\iota_{\mathbb{R}}$ and $\iota_{\mathbb{C}}$? Justify your answer from the uniqueness clause.
- (d) State the idea of the proof in two sentences.

Solution.

- (a) Only in the step “the formula makes sense”: $n \cdot 1 \neq 0$ for $n > 0$ ([Proposition 2.5.2](#) (a)), so $(n \cdot 1)^{-1}$ exists. Well-definedness, the homomorphism property, the image and uniqueness are computations in an arbitrary field once these inverses exist.
- (b) $1/5$: its image would be $[1][5]^{-1}$, and $[5] = [0]$ has no inverse. The rule is not even well defined on the rationals where it seems to make sense: $1 = 1/1 = 5/5$, and the representative $(5, 5)$ gives $[5][5]^{-1}$, which does not exist, while $(1, 1)$ gives $[1]$.
- (c) Both are inclusions. $\mathbb{Q}$ is a subfield of $\mathbb{R}$ and $\mathbb{R}$ of $\mathbb{C}$ ([Example \(Rational and Integer Complex Numbers\)](#) (iii)), so $\mathbb{Q}$ is a subfield of $\mathbb{C}$, and the inclusion of a subfield is a homomorphism ([Example \(Conjugation and Other Automorphisms\)](#) (ii)). By the uniqueness clause of [Theorem 2.5.5](#) (b) (both fields have characteristic 0, [Example](#)

(The characteristics of the standard fields)), $\iota_{\mathbb{R}}$ and $\iota_{\mathbb{C}}$ are these inclusions, $q \mapsto q$.

- (d) A homomorphism out of $\mathbb{Q}$ or $\mathbb{F}_p$ is forced by $1 \mapsto 1$ to send m/n to $(m \cdot 1)(n \cdot 1)^{-1}$ (or $[n]$ to $n \cdot 1$), so there is at most one, and its image lies in every subfield. The characteristic decides whether this forced formula makes sense, and when it does, the fraction rules show it is a homomorphism, whose image is then the prime subfield.

2.5.5.2 B. Practice

Exercise. B1: Reducing multiples

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

- Show that $(p - 1) \cdot a = -a$.
- Show that $(kp + r) \cdot a = r \cdot a$ for all $k, r \in \mathbb{Z}$.
- In $\mathbb{F}_7$, compute $100 \cdot [3]$ directly, and again using (b).

Solution.

- By Lemma 2.5.1 (d) and (c), $(p - 1) \cdot a + a = (p - 1) \cdot a + 1 \cdot a = p \cdot a = (p \cdot 1)a = 0 \cdot a = 0$, using Theorem 2.1.1 (d). By uniqueness of negatives (Theorem 2.1.1 (c)), $(p - 1) \cdot a = -a$.
- By Lemma 2.5.1 (d), $(kp + r) \cdot a = (kp) \cdot a + r \cdot a = k \cdot (p \cdot a) + r \cdot a$. Now $p \cdot a = 0$ as in (a), and $k \cdot 0 = (k \cdot 1)0 = 0$ by Lemma 2.5.1 (c) with (d) and Theorem 2.1.1 (d). So $(kp + r) \cdot a = 0 + r \cdot a = r \cdot a$.
- Directly: $100 \cdot [3] = (100 \cdot [1])[3] = [100][3] = [300]$ (Lemma 2.5.1 (c), Number Systems: From $\setminus(\setminus nN \setminus)$ to $\setminus(\setminus nR \setminus)$, Theorem 3.4.3 (d)), and $300 = 42 \cdot 7 + 6$, so $100 \cdot [3] = [6]$. By (b): $100 = 14 \cdot 7 + 2$, so $100 \cdot [3] = 2 \cdot [3] = [6]$. The two agree.

Exercise. B2: Completing the square

Let F be a field with $\text{char } F \neq 2$, and write $2 := 2 \cdot 1$, $4 := 4 \cdot 1$.

- Show that $x = -x$ implies $x = 0$, for $x \in F$.
- Let $b, c \in F$. Show that the equation $x^2 + bx + c = 0$ has a solution $x \in F$ if and only if $b^2 - 4c = s^2$ for some $s \in F$, and that then its solutions are exactly $x = (-b + s)/2$ and $x = (-b - s)/2$.
- Use (b) to solve $x^2 + x + 1 = 0$ in $\mathbb{F}_7$.
- Explain why (b) says nothing in $\mathbb{F}_2$, and show that its conclusion is in fact false there.

Solution. By Proposition 2.5.2 (b), $2 \neq 0$, so 2 is invertible; and $4 = (2 \cdot 2) \cdot 1 = 2 \cdot 2 \neq 0$ by Lemma 2.5.1 (b) and Theorem 2.1.1 (f). For $u \in F$, $2u = (2 \cdot 1)u = u + u$ by Lemma 2.5.1 (c).

- If $x = -x$, then $2x = x + x = x + (-x) = 0$. Since $2 \neq 0$, $x = 0$ by Theorem 2.1.1 (f).
- Since $4 \neq 0$, $x^2 + bx + c = 0$ if and only if $4(x^2 + bx + c) = 0$ (one direction by Theorem 2.1.1 (d) and (F6), the other by (f)). By Number Systems: From $\setminus(\setminus nN \setminus)$ to $\setminus(\setminus nR \setminus)$, Proposition 2.3.2 (d), $(2x + b)^2 = (2x)^2 + 2(2x)b + b^2 = 4x^2 + 4bx + b^2$, the

products of the multiples regrouped by [Lemma 2.5.1](#) (b), (F5) and (F6). Hence, with $D := b^2 - 4c$,

$$4(x^2 + bx + c) = (2x + b)^2 - D,$$

and the equation is equivalent to $(2x + b)^2 = D$. (Multiplying this identity by 4^{-1} gives the familiar $x^2 + bx + c = (x + b/2)^2 - D/4$.) If x is a solution, $s := 2x + b$ has $s^2 = D$. Conversely, if $s^2 = D$, then by [Corollary 2.1.2](#), $(2x + b)^2 = s^2$ if and only if $2x + b = s$ or $2x + b = -s$, and by [Proposition 2.1.3](#) (a) (with $2 \neq 0$) these say $x = (-b + s)/2$ or $x = (-b - s)/2$.

- (c) Here $b = c = 1$ and $D = 1 - 4 = -3 = 4 = 2^2$ in $\mathbb{F}_7$, so $s = 2$; and $2^{-1} = 4$, since $2 \cdot 4 = 8 = 1$. The solutions are $x = 4(-1 + 2) = 4$ and $x = 4(-1 - 2) = -12 = 2$. Check: $4^2 + 4 + 1 = 21 = 0$ and $2^2 + 2 + 1 = 7 = 0$ in $\mathbb{F}_7$. This agrees with [Exercise \(C3\)](#), found there by trying all seven elements.
- (d) In $\mathbb{F}_2$, $2 = 0$ and $4 = 0$, so the first step, “ $x^2 + bx + c = 0$ iff $4(\dots) = 0$ ”, fails, and $/2$ has no meaning. The conclusion of (b) is false there: for $x^2 + x + 1 = 0$, $D = 1 - 0 = 1 = 1^2$ is a square, yet the equation has no solution, since $x = 0$ and $x = 1$ both give 1.

Exercise. B3: When the integers embed

Let F be a field.

- (a) Show that for $n, n' \in \mathbb{Z}$, $n \cdot 1 = n' \cdot 1$ if and only if $\text{char } F \mid n - n'$.
- (b) Deduce that the map $\mathbb{Z} \rightarrow F$, $n \mapsto n \cdot 1$, is injective if $\text{char } F = 0$, and is not injective if $\text{char } F = p > 0$.

Solution.

- (a) By [Lemma 2.5.1](#) (d), $n \cdot 1 - n' \cdot 1 = (n - n') \cdot 1$. So $n \cdot 1 = n' \cdot 1$ iff $(n - n') \cdot 1 = 0$, iff $\text{char } F \mid n - n'$ by [Proposition 2.5.2](#) (a).
- (b) If $\text{char } F = 0$ and $n \cdot 1 = n' \cdot 1$, then $0 \mid n - n'$ by (a), so $n - n' = 0$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 3.1.1 (a)) and $n = n'$. If $\text{char } F = p > 0$, then $p \cdot 1 = 0 = 0 \cdot 1$ with $p \neq 0$, so the map is not injective.

2.5.5.3 C. Going deeper

Exercise. C1: Exit check: the characteristic

Using only [Definition 2.5.1](#), [Lemma 2.5.1](#), division with remainder in $\mathbb{Z}$, Sets, Relations, and Cardinality, [Definition 2.2.2](#) and the rules for divisibility in $\mathbb{Z}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 3.1.1), and the field axioms with [Theorem 2.1.1](#), prove:

- (a) for a field F and $n \in \mathbb{Z}$, $n \cdot 1 = 0$ if and only if $\text{char } F \mid n$;
- (b) $\text{char } F$ is 0 or a prime.

Solution.

- (a) Let $c := \text{char } F$.
Case $c = 0$. No positive n has $n \cdot 1 = 0$, by [Definition 2.5.1](#). For $n < 0$, $n \cdot 1 = -((-n) \cdot 1)$,

and $(-n) \cdot 1 \neq 0$; since $-x = 0$ implies $x = -(-x) = 0$, also $n \cdot 1 \neq 0$. And $0 \cdot 1 = 0$. So $n \cdot 1 = 0$ iff $n = 0$, iff $0 \mid n$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Proposition 3.1.1 (a)).

Case $c > 0$. Divide: $n = qc + r$ with $q, r \in \mathbb{Z}$, $0 \leq r < c$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.1.2). By Lemma 2.5.1 (d), $(qc) \cdot 1 = (q \cdot 1)(c \cdot 1) = (q \cdot 1)0 = 0$ and $n \cdot 1 = (qc) \cdot 1 + r \cdot 1 = r \cdot 1$. If $c \mid n$, then $r = 0$ by uniqueness of the remainder, so $n \cdot 1 = 0 \cdot 1 = 0$. If $n \cdot 1 = 0$, then $r \cdot 1 = 0$ with $0 \leq r < c$; $r > 0$ would contradict the minimality of c , so $r = 0$ and $c \mid n$.

- (b) Let $c > 0$. As $1 \cdot 1 = 1 \neq 0$, $c \geq 2$. If c were not prime, by Sets, Relations, and Cardinality, Definition 2.2.2 it would have a positive divisor $r \notin \{1, c\}$; write $c = rs$. Then $s > 0$, $r, s \leq c$ by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 3.1.1 (e), and $s \notin \{1, c\}$, since $s = 1$ gives $r = c$ and $s = c$ gives $r = 1$ (cancel $c \neq 0$). So $1 < r, s < c$, and $(r \cdot 1)(s \cdot 1) = (rs) \cdot 1 = 0$ by Lemma 2.5.1 (b), so $r \cdot 1 = 0$ or $s \cdot 1 = 0$ (Theorem 2.1.1 (f)), contradicting the minimality of c . So c is prime.

Marking scheme. (10 points)

- 2: the case $c = 0$, including negative n (a negative multiple is the negative of a non-zero element, hence non-zero).
- 3: division of n by c with remainder, and $n \cdot 1 = r \cdot 1$ justified by the rules for multiples and $c \cdot 1 = 0$.
- 2: minimality of c forces $r = 0$; the converse $c \mid n \Rightarrow n \cdot 1 = 0$.
- 1: $c \neq 1$ from $1 \neq 0$.
- 2: a factorization $c = rs$ with $1 < r, s < c$, bounds justified, gives $(r \cdot 1)(s \cdot 1) = 0$, and the absence of zero divisors contradicts minimality.

Fatal errors (0 for the step): “ $c \cdot 1 = 0$, so $c \mid n$ ” for every n with $n \cdot 1 = 0$, without the division step; treating $n \cdot 1$ as the integer n (for instance “ $n \cdot 1 = 0$, so $n = 0$ ” in $\mathbb{F}_p$).

Exercise. C2: Find the error

Here is an argument.

Claim. A finite field F has prime characteristic.

Proof. (1) The elements $1 \cdot 1, 2 \cdot 1, 3 \cdot 1, \dots$ of F cannot all be different, since F is finite. (2) So $m \cdot 1 = k \cdot 1$ for some positive integers $k < m$. (3) Hence $(m - k) \cdot 1 = m \cdot 1 - k \cdot 1 = 0$. (4) So $m - k$ is the characteristic of F , and it is prime by Theorem 2.5.3.

Is the conclusion true? Does the argument prove it? Name the failing step, say what is wrong with it, and give a counterexample to the step.

Solution. The conclusion is true: it is Corollary 2.5.7 (a). Steps (1) and (2) are correct (they are the pigeonhole argument of that proof, Sets, Relations, and Cardinality, Corollary 3.1.3), and so is step (3), by Lemma 2.5.1 (d). Step (4) fails.

Step (4). The argument only produces **some** positive integer with a vanishing multiple. The characteristic is the **least** one (Definition 2.5.1), and $m - k$ need not be least: in $\mathbb{F}_3$, $7 \cdot 1 = 1 = 1 \cdot 1$ gives $m - k = 6$, while $\text{char } \mathbb{F}_3 = 3$. The step cites a property, “is the characteristic”, that no line supplies, which is (N9) of Logic and Proof, Example (What is

not allowed).

Repair. By (2) and [Lemma 2.5.1](#) (d), $(m - k) \cdot 1 = 0$ with $m - k > 0$, so the set of positive integers with a vanishing multiple is non-empty and $\text{char } F > 0$ ([Definition 2.5.1](#)); then [Theorem 2.5.3](#) makes it prime.

Marking scheme. (10 points)

- 2: the conclusion is true, with the reference.
- 2: steps (1)–(3) are correct (including $(m - k) \cdot 1 = 0$ via [Lemma 2.5.1](#) (d)).
- 6: step (4) named: only some positive multiple vanishes, the characteristic is the least one ([Definition 2.5.1](#)), with a counterexample to the step.

Exercise. C3: The four-element field

Let $F = \{0, 1, \alpha, \beta\}$ be the four-element field of Exercise (C1: A Field with Four Elements), with $\beta = 1 + \alpha$, $\alpha^2 = \beta$ and $\alpha\beta = 1$.

- Show that $\text{char } F = 2$.
- Show that the prime subfield of F is $\{0, 1\}$, and that it is isomorphic to $\mathbb{F}_2$.
- Show that the map $F \rightarrow F$, $x \mapsto x^2$, is an automorphism of F that exchanges α and β .

Solution.

- $1 \cdot 1 = 1 \neq 0$, and $2 \cdot 1 = 1 + 1 = (1 + 1) + (0 + 0)\alpha = 0$ by the addition rule of Exercise (C1: A Field with Four Elements), coefficient by coefficient in $\mathbb{F}_2$. So $\text{char } F = 2$.
- By [Theorem 2.5.5](#) (a), the prime subfield is the image of $\iota_F: \mathbb{F}_2 \rightarrow F$, which is $\{0 \cdot 1, 1 \cdot 1\} = \{0, 1\}$, and ι_F is an isomorphism from $\mathbb{F}_2$ onto it.
- Let $s(x) := x^2$. For $x, y \in F$, $(x + y)^2 = x^2 + 2xy + y^2$ by Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\mathbb{R}\backslash)$, Proposition 2.3.2 (d), where $2xy = (1 + 1)(xy) = 0(xy) = 0$, since $1 + 1 = 2 \cdot 1 = 0$ by part (a) and $0(xy) = 0$ by Theorem 2.1.1 (d); so $s(x + y) = s(x) + s(y)$. Next $(xy)^2 = (xy)(xy) = (xx)(yy) = x^2y^2$ by (F5) and (F6), and $1^2 = 1$. So s is a homomorphism ([Definition 2.4.1](#)). Its values are

$$s(0) = 0, \quad s(1) = 1, \quad s(\alpha) = \alpha^2 = \beta, \quad s(\beta) = (1 + \alpha)^2 = 1 + \alpha^2 = 1 + \beta = \alpha,$$

using the additivity just proved and $1 + \beta = 1 + 1 + \alpha = \alpha$. So s permutes the four elements, is bijective, and is an automorphism exchanging α and β . (The next section shows that $x \mapsto x^p$ is a homomorphism in every field of characteristic p , and an automorphism when the field is finite.)