

2.4 Field Homomorphisms

Section 2.3 looked at fields inside fields. This section looks at maps between fields. Two such maps have appeared already. Complex conjugation $z \mapsto \bar{z}$ turns sums into sums and products into products (Theorem 1.2.2 (a), (b)), and so does $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ on $\mathbb{Q}(\sqrt{2})$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Example (Conjugation in $\mathbb{Q}(\sqrt{2})$). A map that respects both operations carries every equation that holds in one field to an equation in the other. That single observation decides where such a map can send an element, shows that it never collapses two elements, and rules out most maps between most pairs of fields.

Throughout, F and L are fields, and $n \cdot a$ for $n \in \mathbb{N}$ is the multiple of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Section 2.3 (“Multiples”): $0 \cdot a := 0$, $(n+1) \cdot a := n \cdot a + a$. Powers in a field are defined by the same recursion with products: $a^0 := 1$ and $a^{n+1} := a^n a$ for $n \in \mathbb{N}$, as *Sets, Relations, and Cardinality*, Definition 2.3.2 does for real numbers; the power laws $a^{m+n} = a^m a^n$, $(a^m)^n = a^{mn}$ and $(ab)^n = a^n b^n$ of *Sets, Relations, and Cardinality*, Proposition 2.3.4 have proofs that use only (F1)–(F7), (F9) and induction, and hold in every field with the same proofs.

2.4.1 Maps that respect both operations

A *homomorphism* is a map that respects addition, multiplication and the number one.

Definition 2.4.1. Field Homomorphism

Let F and L be fields. A **homomorphism** (of fields) $\varphi: F \rightarrow L$ is a function such that, **for all** $a, b \in F$,

$$\varphi(a + b) = \varphi(a) + \varphi(b), \quad \varphi(ab) = \varphi(a)\varphi(b), \quad \varphi(1) = 1.$$

A **bijective** (*Sets, Relations, and Cardinality*, Definition 1.4.5) homomorphism is an **isomorphism**; F and L are **isomorphic**, written $F \cong L$, if there is an isomorphism $F \rightarrow L$. An isomorphism $F \rightarrow F$ is an **automorphism** of F .

In words: the first clause says that adding and then mapping gives the same as mapping and then adding; the second says the same for multiplying; the third pins down the image of 1, where 1 on the left is 1_F and on the right 1_L . An isomorphism is a homomorphism that is also a one-to-one correspondence of elements, so F and L are then “the same field with the elements renamed”.

Examples.

- The **identity** $\text{id}_F: F \rightarrow F$ is an automorphism.
- **Conjugation** $z \mapsto \bar{z}$ on $\mathbb{C}$ is a homomorphism by Theorem 1.2.2 (a), (b), since $\bar{1} = 1$; [Example \(Conjugation and Other Automorphisms\)](#) below shows that it is an automorphism.
- **The conjugation of $\mathbb{Q}(\sqrt{2})$** , $\sigma(a + b\sqrt{2}) := a - b\sqrt{2}$, is an automorphism (*Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Example (Conjugation in $\mathbb{Q}(\sqrt{2})$)).

Why the clause $\varphi(1) = 1$. The **zero map** $a \mapsto 0$ satisfies the first two clauses, since $0 = 0 + 0$ and $0 = 0 \cdot 0$, and it carries no information about F at all. The third clause excludes it, and the next proposition shows that the third clause is exactly what forces a homomorphism to remember every element.

Remark. The order-preserving field maps of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Section 6.1 (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Definition 6.1.1), are the homomorphisms between ordered fields that also preserve $<$. From here on, $F \cong L$ means isomorphic as fields, in the sense above; the relation of that chapter, an isomorphism that also preserves the order, is said in words, “isomorphic as ordered fields”. The two differ: the conjugation σ of $\mathbb{Q}(\sqrt{2})$ is an automorphism of the field, and it is not order-preserving, since $0 < \sqrt{2}$ while $\sigma(\sqrt{2}) = -\sqrt{2} < 0 = \sigma(0)$.

2.4.2 What a homomorphism must do

To find where a homomorphism sends an element, we take an equation that the element satisfies and apply φ to both sides. The equation in L that comes out often has only one solution.

Proposition 2.4.1. Properties of Field Homomorphisms

Let $\varphi: F \rightarrow L$ be a homomorphism of fields, and let $a, b \in F$.

- (a) $\varphi(0) = 0$, $\varphi(-a) = -\varphi(a)$ and $\varphi(a - b) = \varphi(a) - \varphi(b)$.
- (b) If $a \neq 0$, then $\varphi(a) \neq 0$ and $\varphi(a^{-1}) = \varphi(a)^{-1}$.
- (c) φ is **injective**.
- (d) The image $\varphi(F)$ is a subfield of L , and φ , with codomain $\varphi(F)$, is an isomorphism $F \rightarrow \varphi(F)$.
- (e) If $\psi: L \rightarrow M$ is a homomorphism of fields, then $\psi \circ \varphi: F \rightarrow M$ is a homomorphism. If φ is an isomorphism, its inverse function $\varphi^{-1}: L \rightarrow F$ is an isomorphism. The identity id_F is an automorphism.
- (f) $\varphi(n \cdot a) = n \cdot \varphi(a)$ and $\varphi(a^n) = \varphi(a)^n$ for every $n \in \mathbb{N}$.

Idea. For (a) and (b) the equations to push through φ are $0+0=0$, $a+(-a)=0$ and $aa^{-1}=1$; in L the results are equations with a unique solution, by cancellation and the uniqueness of negatives and inverses. For (c): a homomorphism cannot send a non-zero element to 0, because a non-zero element has an inverse, and then $\varphi(a)\varphi(a^{-1}) = \varphi(1) = 1 \neq 0$. Injectivity is that fact applied to $a - b$. The rest is bookkeeping with (a)–(c), and induction for (f).

Before reading on: in the proof of (c), where is $\varphi(1) = 1$ used, and which map satisfies the other two clauses of [Definition 2.4.1](#) but is not injective?

Proof.

- (a) Since $0 + 0 = 0$ in F ,

$$\varphi(0) + \varphi(0) = \varphi(0 + 0) = \varphi(0) = \varphi(0) + 0,$$

and additive cancellation in L (Theorem 2.1.1 (b)) gives $\varphi(0) = 0$. Next, $a + (-a) = 0$ gives $\varphi(a) + \varphi(-a) = \varphi(a + (-a)) = \varphi(0) = 0$, so $\varphi(-a)$ is a negative of $\varphi(a)$, and $\varphi(-a) = -\varphi(a)$ by the uniqueness of negatives (Theorem 2.1.1 (c)). Finally, $\varphi(a - b) = \varphi(a + (-b)) = \varphi(a) + \varphi(-b) = \varphi(a) - \varphi(b)$.

- (b) Let $a \neq 0$. Since $aa^{-1} = 1$,

$$\varphi(a)\varphi(a^{-1}) = \varphi(aa^{-1}) = \varphi(1) = 1.$$

If $\varphi(a) = 0$, the left side would be $0 \cdot \varphi(a^{-1}) = 0$ (Theorem 2.1.1 (d)), and the display would read $0 = 1$, against (F7) in L . So $\varphi(a) \neq 0$, and the display says that $\varphi(a^{-1})$ is an inverse of $\varphi(a)$; by the uniqueness of inverses (Theorem 2.1.1 (c)), $\varphi(a^{-1}) = \varphi(a)^{-1}$.

- (c) Let $\varphi(a) = \varphi(b)$. By (a), $\varphi(a - b) = \varphi(a) - \varphi(b) = 0$. By (b), read contrapositively, an element whose image is 0 is 0; so $a - b = 0$, and $a = b$ (add b to both sides, with (F2), (F1), (F4) and (F3)). So φ is injective.
- (d) We use Proposition 2.3.1 (c) for $\varphi(F) \subseteq L$. First, $1 = \varphi(1) \in \varphi(F)$. Next, two elements of $\varphi(F)$ are $\varphi(a), \varphi(b)$ with $a, b \in F$ (Sets, Relations, and Cardinality, Definition 1.6.1), and $\varphi(a) - \varphi(b) = \varphi(a - b) \in \varphi(F)$ by (a). If moreover $\varphi(b) \neq 0$, then $b \neq 0$, since $\varphi(0) = 0$; so by (b), $\varphi(a)\varphi(b)^{-1} = \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1}) \in \varphi(F)$. Hence $\varphi(F)$ is a subfield of L , a field with the operations of L (Proposition 2.3.1 (a)). The map $\varphi: F \rightarrow \varphi(F)$ still satisfies the three clauses, since the operations of $\varphi(F)$ are those of L and its one is 1_L ; it is surjective by the definition of the image, and injective by (c). So it is an isomorphism.
- (e) For the composite, $(\psi \circ \varphi)(a + b) = \psi(\varphi(a) + \varphi(b)) = \psi(\varphi(a)) + \psi(\varphi(b))$, likewise for products, and $\psi(\varphi(1)) = \psi(1) = 1$ (Sets, Relations, and Cardinality, Definition 1.4.2). Now let φ be an isomorphism, with inverse function $\varphi^{-1}: L \rightarrow F$ (Sets, Relations, and Cardinality, Definition 1.5.2, which exists by Sets, Relations, and Cardinality, Theorem 1.5.4). For $x, y \in L$,

$$\varphi(\varphi^{-1}(x) + \varphi^{-1}(y)) = \varphi(\varphi^{-1}(x)) + \varphi(\varphi^{-1}(y)) = x + y = \varphi(\varphi^{-1}(x + y)),$$

so $\varphi^{-1}(x) + \varphi^{-1}(y) = \varphi^{-1}(x + y)$, because φ is injective. The same computation with products gives $\varphi^{-1}(x)\varphi^{-1}(y) = \varphi^{-1}(xy)$. And $\varphi(1) = 1$ gives $\varphi^{-1}(1) = 1$. The function φ^{-1} is bijective, with inverse φ (Sets, Relations, and Cardinality, Theorem 1.5.4); so it is an isomorphism. The identity satisfies the three clauses trivially and is bijective.

- (f) By induction on n (Logic and Proof, Axiom 4.2.1, read on $\mathbb{N} = \omega$ through Number Systems: From $\setminus(\setminus n\mathbb{N}\setminus)$ to $\setminus(\setminus n\mathbb{R}\setminus)$, Corollary 1.7.3). For $n = 0$: $\varphi(0 \cdot a) = \varphi(0) = 0 = 0 \cdot \varphi(a)$ by (a), and $\varphi(a^0) = \varphi(1) = 1 = \varphi(a)^0$. If the two formulas hold for n , then

$$\begin{aligned}\varphi((n + 1) \cdot a) &= \varphi(n \cdot a + a) = n \cdot \varphi(a) + \varphi(a) = (n + 1) \cdot \varphi(a), \\ \varphi(a^{n+1}) &= \varphi(a^n a) = \varphi(a)^n \varphi(a) = \varphi(a)^{n+1}.\end{aligned}$$

This proves the proposition. ■

The answer to the prompt. In (c), $\varphi(1) = 1$ enters through (b): the display $\varphi(a)\varphi(a^{-1}) = 1$ is what makes $\varphi(a) = 0$ impossible. The zero map $F \rightarrow L$ satisfies the two other clauses, sends every element to 0, and is not injective. A map that respected sums and products but sent 1 to 0 would be the zero map: $\varphi(a) = \varphi(a \cdot 1) = \varphi(a)\varphi(1) = \varphi(a) \cdot 0 = 0$, by (F7), the product clause, $\varphi(1) = 0$, and Theorem 2.1.1 (d) with (F6) in L .

We call the move of this proof **push the equation through** φ : to learn $\varphi(x)$, apply φ to an equation that x satisfies, and solve the resulting equation in L . By (c) and (d), a homomorphism $F \rightarrow L$ is the same thing as a copy of F inside L : $F \cong \varphi(F)$, a subfield of L . By (e) and Sets, Relations, and Cardinality, Theorem 1.4.4 (c), composing isomorphisms gives isomorphisms, so

$\cong$ is reflexive, symmetric and transitive on any set of fields.

Warning. A bijection that respects addition alone is not an isomorphism. The map $f: \mathbb{Q} \rightarrow \mathbb{Q}$, $f(x) := 2x$, is bijective (its inverse is $x \mapsto x/2$) and satisfies $f(a + b) = f(a) + f(b)$, by (F9). But $f(1 \cdot 1) = 2$, while $f(1)f(1) = 4$; and $f(1) = 2 \neq 1$. All three clauses of Definition 2.4.1 must be checked.

Quick check. Is $a \mapsto -a$ a homomorphism $\mathbb{Q} \rightarrow \mathbb{Q}$?

Solution. No. It sends 1 to -1 , and $-1 \neq 1$ in $\mathbb{Q}$: if $-1 = 1$, then $1 + 1 = 1 + (-1) = 0$, while $1 + 1 = 2 \cdot 1 > 0$ in the ordered field $\mathbb{Q}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (h), Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.5.1). (In $\mathbb{F}_2$, where $-1 = 1$, the same map is the identity.) It also fails the product clause: $1 \cdot 1 = 1$ is sent to -1 , while the product of the images is $(-1)(-1) = 1$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.2 (c)). It does respect sums, by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.2 (c) and (F9): $-(a + b) = (-1)(a + b) = -a + (-b)$.

2.4.3 Examples, and pairs of fields with no map between them

Example. Conjugation and Other Automorphisms

- (i) Show that conjugation $z \mapsto \bar{z}$ is an automorphism of $\mathbb{C}$, that it is not the identity, and that $\bar{z} = z$ if and only if $z \in \mathbb{R}$.
- (ii) Let K be a subfield of L . Show that the inclusion $K \rightarrow L$, $x \mapsto x$, is a homomorphism, and that it is not surjective when $K \neq L$.
- (iii) Recall why $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ is an automorphism of $\mathbb{Q}(\sqrt{2})$.
- (iv) Which automorphisms does $\mathbb{R}$ have?

Solution.

- (i) By Theorem 1.2.2 (a), (b), $\overline{z + w} = \bar{z} + \bar{w}$ and $\overline{zw} = \bar{z}\bar{w}$; and $\bar{1} = \overline{1 + 0i} = 1 - 0i = 1$ (Definition 1.2.1). So conjugation is a homomorphism. By Theorem 1.2.2 (a), $\bar{\bar{z}} = z$, so conjugation is its own inverse, hence bijective (Sets, Relations, and Cardinality, Theorem 1.5.4): an automorphism. It is not the identity: $\bar{i} = -i$, and $-i \neq i$, since $i - (-i) = 2i = (0, 2) \neq (0, 0)$.

For the fixed elements, let $z = a + bi$ with $a, b \in \mathbb{R}$. Then $\bar{z} = a - bi$ (Definition 1.2.1), and comparing parts (Definition 1.1.1), $\bar{z} = z$ if and only if $-b = b$, that is $2b = 0$, that is $b = 0$ (as $2 = 2 \cdot 1 > 0$ in the ordered field $\mathbb{R}$, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 5.3.3, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (h), so $2 \neq 0$, and by Theorem 2.1.1 (f)). And $b = 0$ says $z = a + 0i = a \in \mathbb{R}$ (Proposition 1.1.1). This fact is not among the parts of Theorem 1.2.2; the two lines above prove it.

- (ii) The operations of K are those of L , and $1_K = 1_L$ (Proposition 2.3.1 (a)). So $x \mapsto x$ satisfies the three clauses. If $K \neq L$, some element of L is not in K , and it is not a value of the inclusion.
- (iii) This is Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Example (Conjugation in $\mathbb{Q}(\sqrt{2})$), recalled and not proved again: unique representation makes the formula a function, the product formula of Example (The Field Generated by the Square Root of Two) with $-b, -d$ in place of b, d shows that products go to products, and the map is its own inverse.
- (iv) Only the identity. *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 6, proved that a map $\sigma: \mathbb{R} \rightarrow \mathbb{R}$ with $\sigma(a+b) = \sigma(a) + \sigma(b)$, $\sigma(ab) = \sigma(a)\sigma(b)$ and $\sigma(1) = 1$, that is, a homomorphism $\mathbb{R} \rightarrow \mathbb{R}$, is the identity, with no order condition assumed (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 6.3.4, with $\mathbb{R}$ complete by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 5.6.3). So $\mathbb{C}$ has a symmetry and $\mathbb{R}$ has none. Section 2.5 shows that $\mathbb{Q}$ and every $\mathbb{F}_p$ have no automorphism other than the identity either.

Pushing an equation through φ also proves that no homomorphism exists: an equation that holds in F and has no counterpart in L leaves φ nowhere to go.

Example. Pairs of Fields with No Homomorphism

Show that there is no homomorphism (i) $\mathbb{C} \rightarrow \mathbb{R}$; (ii) $\mathbb{F}_2 \rightarrow \mathbb{Q}$; (iii) $\mathbb{Q} \rightarrow \mathbb{F}_p$, for any prime p . (iv) Which clause of Definition 2.4.1 does the zero map $\mathbb{Q} \rightarrow \mathbb{Q}$ fail?

Solution.

- (i) Suppose $\varphi: \mathbb{C} \rightarrow \mathbb{R}$ is a homomorphism. In $\mathbb{C}$, $i^2 = -1$. Pushing this through φ ,

$$\varphi(i)^2 = \varphi(i^2) = \varphi(-1) = -\varphi(1) = -1,$$

by (f) and (a) of Proposition 2.4.1. But $\mathbb{R}$ is an ordered field (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 5.3.3), in which every square is ≥ 0 and $1 > 0$, so $-1 < 0$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (e), (a)). So $\varphi(i)^2 = -1$ is impossible.

- (ii) Suppose $\varphi: \mathbb{F}_2 \rightarrow \mathbb{Q}$ is a homomorphism. In $\mathbb{F}_2$, $1 + 1 = 0$ (Example (Arithmetic on $\mathbb{Z}/n\mathbb{Z}$ and the Field $\mathbb{F}_2$)). Pushing it through φ , $1 + 1 = \varphi(1) + \varphi(1) = \varphi(1 + 1) = \varphi(0) = 0$ in $\mathbb{Q}$, by (a). But $1 + 1 = 2 \cdot 1 > 0$ in the ordered field $\mathbb{Q}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (h), Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.5.1). So no such φ exists.
- (iii) Suppose $\varphi: \mathbb{Q} \rightarrow \mathbb{F}_p$ is a homomorphism. In $\mathbb{F}_p$, $p \cdot 1 = 0$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.4.3 (d)). By Proposition 2.4.1 (f), $\varphi(p \cdot 1) = p \cdot \varphi(1) = p \cdot 1 = 0 = \varphi(0)$, and φ is injective by (c), so $p \cdot 1 = 0$ in $\mathbb{Q}$. But $p \cdot 1 > 0$ in $\mathbb{Q}$, as in (ii), since $p \geq 1$. So no such φ exists.
- (iv) The zero map $a \mapsto 0$ respects sums and products, since $0 + 0 = 0$ and $0 \cdot 0 = 0$, and it sends 1 to $0 \neq 1$. So it fails only $\varphi(1) = 1$, and is not a homomorphism.

Section 2.5 explains (ii) and (iii) at once: both pairs of fields differ in the number of copies of 1 that add up to 0.

2.4.4 Exercises

2.4.4.1 A. Check your understanding

Exercise. A1

These parts are about [Proposition 2.4.1](#), mainly its part (c).

- (a) Where in the proof of (c) is the clause $\varphi(1) = 1$ used?
- (b) Let $\zeta: \mathbb{Q} \rightarrow \mathbb{Q}$ be the zero map. Which clause of [Definition 2.4.1](#) fails? Which of the conclusions (a)–(f) fail for ζ ?
- (c) Run the proof of (c) with conjugation on $\mathbb{C}$ and the elements $a = 1 + i$, $b = 1 - i$: compute $a - b$, its image, and conclude.
- (d) State the idea of the proof of (c) in two sentences.

Solution.

- (a) In (b), which (c) cites: $\varphi(a)\varphi(a^{-1}) = \varphi(aa^{-1}) = \varphi(1) = 1$, and $1 \neq 0$, so $\varphi(a) \neq 0$ for $a \neq 0$.
- (b) The clause $\zeta(1) = 1$ fails: $\zeta(1) = 0$. Conclusion (a) holds ($\zeta(0) = 0 = -0$). Conclusion (b) fails: $1 \neq 0$ and $\zeta(1) = 0$. Conclusion (c) fails: $\zeta(1) = \zeta(2)$. Conclusion (d) fails: the image $\{0\}$ does not contain 1, so it is not a subfield. Conclusion (f) holds for multiples (both sides are 0) and fails for powers at $n = 0$: $\zeta(a^0) = \zeta(1) = 0$, while $\zeta(a)^0 = 1$. Conclusion (e) fails in its first clause: for a homomorphism $\psi: \mathbb{Q} \rightarrow M$ (for example $\psi = \text{id}_{\mathbb{Q}}$), $\psi \circ \zeta$ is the zero map, since $\psi(0) = 0$ by (a) for ψ , and the zero map sends 1 to 0, so it is not a homomorphism. The clause about inverses holds vacuously, since ζ is not bijective, and the clause about id_F does not involve ζ .
- (c) $a - b = 2i \neq 0$. Its image is $\overline{2i} = -2i \neq 0$, as (b) predicts; so $\overline{a - b} = \overline{a} - \overline{b} \neq 0$, and $\overline{a} \neq \overline{b}$. Indeed $\overline{a} = 1 - i$ and $\overline{b} = 1 + i$.
- (d) A non-zero element has an inverse, so its image times another image is $\varphi(1) = 1 \neq 0$; hence a homomorphism sends no non-zero element to 0. Applied to a difference $a - b$, this says that different elements have different images.

2.4.4.2 B. Practice

Exercise. B1: Images of quotients

Let $\varphi: F \rightarrow L$ be a homomorphism, and let $a, b \in F$ with $b \neq 0$. Prove that $\varphi(a/b) = \varphi(a)/\varphi(b)$. Here is the start of a proof. *Name the move, then complete it.*

“Since $a = (a/b) \cdot b$, applying φ gives $\varphi(a) = \varphi(a/b) \varphi(b)$”

Solution. The move is **push the equation through φ** : the equation $a = (a/b)b$, which holds since $(ab^{-1})b = a(b^{-1}b) = a$ by (F5), (F6), (F8) and (F7), is carried to L and solved there.

Completion. Since $b \neq 0$, $\varphi(b) \neq 0$ by [Proposition 2.4.1](#) (b), so $\varphi(b)^{-1}$ exists. Multiplying

$\varphi(a) = \varphi(a/b)\varphi(b)$ by $\varphi(b)^{-1}$, with (F5), (F8) and (F7),

$$\varphi(a)\varphi(b)^{-1} = \varphi(a/b)\varphi(b)\varphi(b)^{-1} = \varphi(a/b).$$

That is, $\varphi(a/b) = \varphi(a)/\varphi(b)$.

Exercise. B2: The automorphisms of the rational complex numbers

Show that $\mathbb{Q}(i)$ (Example (Rational and Integer Complex Numbers)) has exactly two automorphisms: the identity and conjugation $a + bi \mapsto a - bi$. Here is the first half of a proof. *Name the move, then complete it.*

“Let σ be an automorphism of $\mathbb{Q}(i)$. It fixes every rational: $\sigma(n) = \sigma(n \cdot 1) = n \cdot \sigma(1) = n$ for $n \in \mathbb{N}$ by Proposition 2.4.1 (f), $\sigma(-n) = -\sigma(n) = -n$ by (a), and $\sigma(m/n) = \sigma(m)/\sigma(n) = m/n$ for $m \in \mathbb{Z}$, $n \in \mathbb{Z}_{>0}$, by Exercise (B1: Images of quotients). Moreover $i^2 = -1$. . .”

Solution. The move is **push the equation through σ** , applied to $i^2 = -1$.

Completion. Every rational is m/n with $m \in \mathbb{Z}$, $n \in \mathbb{Z}_{>0}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Proposition 2.4.4 (b)), so $\sigma(q) = q$ for every $q \in \mathbb{Q}$. Applying σ to $i^2 = -1$,

$$\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1 = i^2.$$

By Corollary 2.1.2 in the field $\mathbb{Q}(i)$, $\sigma(i) = i$ or $\sigma(i) = -i$. For $a, b \in \mathbb{Q}$, $\sigma(a + bi) = \sigma(a) + \sigma(b)\sigma(i) = a + b\sigma(i)$. So either $\sigma(a + bi) = a + bi$ for all a, b , and σ is the identity, or $\sigma(a + bi) = a - bi$ for all a, b , and σ is conjugation. There are at most these two.

Both occur. The identity is an automorphism (Proposition 2.4.1 (e)). Conjugation sends $a + bi$ to $a + (-b)i \in \mathbb{Q}(i)$, so it maps $\mathbb{Q}(i)$ into itself; it respects sums and products and sends 1 to 1 because conjugation on $\mathbb{C}$ does (Example (Conjugation and Other Automorphisms) (i)) and the operations of $\mathbb{Q}(i)$ are those of $\mathbb{C}$; and it is its own inverse on $\mathbb{Q}(i)$, hence bijective. The two are different maps, since conjugation sends $i \in \mathbb{Q}(i)$ to $-i \neq i$ (Example (Conjugation and Other Automorphisms) (i)). So $\mathbb{Q}(i)$ has exactly two automorphisms.

Exercise. B3

Let F be the field of Exercise (B3: Which Are Fields?) (a): the set $\mathbb{Q}$ with the usual sum and the product $a \odot b := 2ab$. Show that $f: F \rightarrow \mathbb{Q}$, $f(x) := 2x$, is an isomorphism of fields, so $F \cong \mathbb{Q}$. Compare with the warning of this section.

Solution. The one of F is $1/2$: $a \odot \frac{1}{2} = 2a \cdot \frac{1}{2} = a$. We check the three clauses, with $\mathbb{Q}$'s usual product on the right. Sums: $f(a + b) = 2a + 2b = f(a) + f(b)$, by (F9). Products: $f(a \odot b) = 2(2ab) = (2a)(2b) = f(a)f(b)$, by (F5) and (F6). One: $f(1/2) = 1$. The map is bijective, with inverse $x \mapsto x/2$: $2(x/2) = x$ and $(2x)/2 = x$ (Sets, Relations, and Cardinality, Theorem 1.5.4). So f is an isomorphism.

The warning used the same formula $x \mapsto 2x$ as a map $\mathbb{Q} \rightarrow \mathbb{Q}$, with the usual product on **both** sides, and it is not a homomorphism there. Whether a map is a homomorphism

depends on the operations of the source as well as on the formula: on F , the product $\odot$ contains the factor 2 that the formula needs.

Exercise. B4: The fixed field

Let σ be an automorphism of a field F . Show that its **fixed set** $\{a \in F : \sigma(a) = a\}$ is a subfield of F . Find the fixed set of conjugation on $\mathbb{C}$ and of conjugation on $\mathbb{Q}(\sqrt{2})$.

Solution. Write K for the fixed set, and use Proposition 2.3.1 (c). $\sigma(1) = 1$, so $1 \in K$. For $a, b \in K$, $\sigma(a - b) = \sigma(a) - \sigma(b) = a - b$ by Proposition 2.4.1 (a), so $a - b \in K$. If moreover $b \neq 0$, then $\sigma(ab^{-1}) = \sigma(a)\sigma(b)^{-1} = ab^{-1}$ by (b), so $ab^{-1} \in K$. Hence K is a subfield. (Only the homomorphism property was used.)

For conjugation on $\mathbb{C}$, $K = \mathbb{R}$, by Example (Conjugation and Other Automorphisms) (i).

For conjugation on $\mathbb{Q}(\sqrt{2})$, $a - b\sqrt{2} = a + b\sqrt{2}$ holds if and only if $2b\sqrt{2} = 0$, that is, $b = 0$: in the ordered field $\mathbb{R}$, $2 = 2 \cdot 1 > 0$ (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 2.3.5 (h), Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Theorem 5.3.3), so $2 \neq 0$, and $\sqrt{2} \neq 0$ (since $0^2 = 0 \neq 2$), and a product of non-zero elements is non-zero (Theorem 2.1.1 (f)). So $K = \{a + 0\sqrt{2} : a \in \mathbb{Q}\} = \mathbb{Q}$.

2.4.4.3 C. Going deeper

Exercise. C1: Isomorphic fields have the same square roots of minus one

- (a) Let $F \cong L$. Prove that F has an element x with $x^2 = -1$ if and only if L has one.
- (b) Deduce that $\mathbb{Q}(i) \not\cong \mathbb{Q}(\sqrt{2})$ and that $\mathbb{C} \not\cong \mathbb{R}$.

Solution.

- (a) Let $\varphi: F \rightarrow L$ be an isomorphism. If $x \in F$ has $x^2 = -1$, then by Proposition 2.4.1 (f) and (a),

$$\varphi(x)^2 = \varphi(x^2) = \varphi(-1) = -\varphi(1) = -1,$$

so $\varphi(x) \in L$ is such an element. Conversely, $\varphi^{-1}: L \rightarrow F$ is an isomorphism (Proposition 2.4.1 (e)), and the same computation carries an element $y \in L$ with $y^2 = -1$ to $\varphi^{-1}(y) \in F$ with $\varphi^{-1}(y)^2 = -1$.

- (b) In $\mathbb{Q}(i)$, $i^2 = -1$. In $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$, every y has $y^2 \geq 0 > -1$, since $\mathbb{R}$ is an ordered field (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Theorem 5.3.3, Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 2.3.5 (e), (a)); so $\mathbb{Q}(\sqrt{2})$ has no such element, and by (a), $\mathbb{Q}(i) \not\cong \mathbb{Q}(\sqrt{2})$. Likewise $i \in \mathbb{C}$ and no element of $\mathbb{R}$ squares to -1 , so $\mathbb{C} \not\cong \mathbb{R}$.

The same argument works for any statement written with $+$, $\cdot$, 0 , 1 and elements: an isomorphism carries it in both directions. (For $\mathbb{C}$ and $\mathbb{R}$, Example (Pairs of Fields with No Homomorphism) (i) shows more: there is no homomorphism $\mathbb{C} \rightarrow \mathbb{R}$ at all.)

Marking scheme. (10 points) - 3: pushes $x^2 = -1$ through φ , with $\varphi(-1) = -1$ justified (by (a) and $\varphi(1) = 1$). - 3: the converse, by either route: through φ^{-1} , with the fact that it is an isomorphism (or a homomorphism) justified (Proposition 2.4.1 (e)); or directly, writing

$y = \varphi(x)$ by surjectivity, getting $\varphi(x^2) = \varphi(-1)$, and concluding $x^2 = -1$ by injectivity. - 2: no element of $\mathbb{Q}(\sqrt{2})$ (or of $\mathbb{R}$) squares to -1 , from the order of $\mathbb{R}$. - 2: both conclusions of (b) drawn from (a). Fatal errors (0 for the step): treating $\mathbb{Q}(\sqrt{2}) \not\cong \mathbb{Q}(i)$ as evident because the sets “look different”; using $\varphi(-1) = -1$ without (a).

Exercise. C2: Find the error

Here is an argument. Is its conclusion true? Does the argument prove it? If not, name the line that fails and why.

“Every homomorphism $\varphi: \mathbb{Q} \rightarrow \mathbb{Q}$ is the identity. (1) By definition, $\varphi(1) = 1$, and φ respects sums. (2) For $x \in \mathbb{Q}$, $\varphi(x) = \varphi(x \cdot 1) = x \varphi(1)$. (3) Hence $\varphi(x) = x \cdot 1 = x$.”

Solution. The conclusion is **true**: the repair below proves it, and Section 2.5 proves it again by another route. The argument does not prove it.

Line (2) fails, at the second equality. “ $\varphi(x \cdot 1) = x \varphi(1)$ ” pulls the factor x out of φ , as if φ were compatible with multiplication by a scalar x ; that is not a clause of [Definition 2.4.1](#), and nothing proved so far supplies it. So the line cites a general “fact” that is not available, entry (N9) of Logic and Proof, Example (What is not allowed). The clause that is available, multiplicativity, gives only $\varphi(x \cdot 1) = \varphi(x)\varphi(1) = \varphi(x)$, which proves nothing.

Counterexample to the step (in its general form, “a homomorphism satisfies $\varphi(x \cdot 1) = x \varphi(1)$ ”): conjugation on $\mathbb{C}$ has $\overline{i \cdot 1} = -i$, while $i \cdot \overline{1} = i$.

Repair. For $n \in \mathbb{N}$, $\varphi(n \cdot 1) = n \cdot \varphi(1) = n \cdot 1$ by [Proposition 2.4.1](#) (f), and $n \cdot 1 = n$ in $\mathbb{Q}$; so $\varphi(n) = n$. For $n \in \mathbb{N}$, $\varphi(-n) = -\varphi(n) = -n$ by (a), so $\varphi(m) = m$ for every $m \in \mathbb{Z}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{Z}$, Proposition 2.2.3 (c)). Every rational is m/n with $m \in \mathbb{Z}$, $n \in \mathbb{Z}_{>0}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.4.4 (b)), and $\varphi(m/n) = \varphi(m)/\varphi(n) = m/n$ by [Exercise \(B1: Images of quotients\)](#). So $\varphi = \text{id}_{\mathbb{Q}}$.