

FIELD AUTOMORPHISMS OF \mathbf{R} AND \mathbf{Q}_p

KEITH CONRAD

1. INTRODUCTION

An *automorphism* of a field K is an isomorphism of K with itself: a function $f: K \rightarrow K$ that is a bijective field homomorphism (additive and multiplicative). For example, the identity function $f(x) = x$ is an automorphism of K . Here are two examples of non-identity automorphisms of fields.

Example 1.1. Complex conjugation is a field automorphism of \mathbf{C} . If $f: \mathbf{C} \rightarrow \mathbf{C}$ by $f(a + bi) = a - bi$ for $a, b \in \mathbf{R}$ then f is a bijection since it is its own inverse ($f(f(z)) = z$). It is additive and multiplicative since

$$\begin{aligned} f((a + bi) + (c + di)) &= f((a + c) + (b + d)i) \\ &= (a + c) - (b + d)i \\ &= (a - bi) + (c - di) \\ &= f(a + bi) + f(c + di) \end{aligned}$$

and

$$\begin{aligned} f((a + bi)(c + di)) &= f((ac - bd) + (ad + bc)i) \\ &= (ac - bd) - (ad + bc)i \\ &= (a - bi)(c - di) \\ &= f(a + bi)f(c + di). \end{aligned}$$

Example 1.2. The set $\mathbf{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbf{Q}\}$ is a subfield of \mathbf{R} : it's clearly closed under addition and negation, it's closed under multiplication because

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$$

and it's closed under inversion because

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}.$$

The denominator $a^2 - 2b^2$ is not 0, since otherwise $2 = (a/b)^2$, which contradicts $\sqrt{2}$ being irrational.

On $\mathbf{Q}(\sqrt{2})$ we have a conjugation operation: $f(a + b\sqrt{2}) = a - b\sqrt{2}$.¹ That f is an automorphism of $\mathbf{Q}(\sqrt{2})$ is similar to complex conjugation being an automorphism of \mathbf{C} :

¹This is well-defined because the rational coefficients of a number in $\mathbf{Q}(\sqrt{2})$ are unique: if $a + b\sqrt{2} = c + d\sqrt{2}$ then $a = c$ and $b = d$. Indeed, the equation implies $a - c = (d - b)\sqrt{2}$, and if $b \neq d$ then $\sqrt{2} = (a - c)/(d - b)$ would be rational, which is false, so $b = d$ and thus $a = c$.

f is bijective since it is its own inverse ($f(f(a + b\sqrt{2})) = a + b\sqrt{2}$), and it is additive and multiplicative since

$$\begin{aligned} f((a + b\sqrt{2}) + (c + d\sqrt{2})) &= f((a + c) + (b + d)\sqrt{2}) \\ &= (a + c) - (b + d)\sqrt{2} \\ &= (a - b\sqrt{2}) + (c - d\sqrt{2}) \\ &= f(a + b\sqrt{2}) + f(c + d\sqrt{2}) \end{aligned}$$

and

$$\begin{aligned} f((a + b\sqrt{2})(c + d\sqrt{2})) &= f((ac + 2bd) + (ad + bc)\sqrt{2}) \\ &= (ac + 2bd) - (ad + bc)\sqrt{2} \\ &= (a - b\sqrt{2})(c - d\sqrt{2}) \\ &= f(a + b\sqrt{2})f(c + d\sqrt{2}). \end{aligned}$$

As an illustration of the similarities between \mathbf{R} and \mathbf{Q}_p , we will show the only automorphism of each field is the identity. In both cases this will be derived from the dense subset \mathbf{Q} having that same property: its only automorphism is the identity. However, bear in mind that even when field operations are continuous, continuity is not a necessary property of a field automorphism. For example, since $\mathbf{Q}(\sqrt{2})$ is inside of \mathbf{R} we can talk about continuous functions on $\mathbf{Q}(\sqrt{2})$ and the automorphism f in Example 1.2 is not continuous: there are rational numbers r_n that tend to $\sqrt{2}$, and $f(r_n) = r_n$ does not tend to $f(\sqrt{2}) = -\sqrt{2}$. On the other hand, complex conjugation on \mathbf{C} is continuous.

2. FIELD AUTOMORPHISMS OF \mathbf{Q}

Theorem 2.1. *The only field homomorphism $\mathbf{Q} \rightarrow \mathbf{Q}$ is the identity. In particular, the only field automorphism of \mathbf{Q} is the identity.*

Proof. Let $f: \mathbf{Q} \rightarrow \mathbf{Q}$ be a field homomorphism. Since $1^2 = 1$ we get $f(1)^2 = f(1)$, so $f(1)$ is 0 or 1. If $f(1) = 0$ then for all $x \in \mathbf{Q}$ we have $f(x) = f(x \cdot 1) = f(x)f(1) = f(x) \cdot 0 = 0$, so f is identically 0. The zero function is not considered to be a homomorphism of fields, so $f(1) = 1$. Then by induction we get $f(n) = n$ for $n \in \mathbf{Z}^+$, so $f(-n) = -f(n)$ by additivity, and thus $f(n) = n$ for all $n \in \mathbf{Z}$. Finally, for any $r \in \mathbf{Q}$, writing $r = a/b$ with $a, b \in \mathbf{Z}$ implies from $br = a$ that $f(b)f(r) = f(a)$, so $f(r) = f(a)/f(b) = a/b = r$. \square

3. FIELD AUTOMORPHISMS OF \mathbf{R}

Theorem 3.1. *The only field automorphism $\mathbf{R} \rightarrow \mathbf{R}$ is the identity.*

Proof. Let $f: \mathbf{R} \rightarrow \mathbf{R}$ be a field automorphism.

Step 1: $f(r) = r$ for all $r \in \mathbf{Q}$.

The same reasoning as in the proof of Theorem 2.1 shows $f(1) = 1$ and then from this $f(r) = r$ for all $r \in \mathbf{Q}$.

Step 2: f preserves inequalities.

The key point is that being positive can be described algebraically: $x > 0$ if and only if x is a nonzero square in \mathbf{R} . Therefore if $x > 0$, writing $x = y^2$ implies $f(x) = f(y^2) = f(y)^2$, so $f(x) > 0$ since $f(y) \neq 0$. (A field automorphism has $f(0) = 0$ and f is injective, so

$y \neq 0 \implies f(y) \neq 0$.) If $x > x'$, then $x - x' > 0$ so $f(x - x') > 0$. Since $f(x - x') = f(x) - f(x')$ we get $f(x) - f(x') > 0$, so $f(x) > f(x')$.

Step 3: $f(x) = x$ for all $x \in \mathbf{R}$.

For each $x \in \mathbf{R}$ there are rational numbers r_n and s_n such that $r_n < x < s_n$ for all n and $r_n \rightarrow x^-$ and $s_n \rightarrow x^+$. Since f preserves inequalities, $f(r_n) < f(x) < f(s_n)$, so $r_n < f(x) < s_n$ since r_n and s_n are rational. Letting $n \rightarrow \infty$, $r_n < f(x) \implies x \leq f(x)$ and $f(x) < s_n \implies f(x) \leq x$, so $f(x) = x$. \square

In this proof we did not use surjectivity of f , only that it is a field homomorphism $\mathbf{R} \rightarrow \mathbf{R}$. (We did need $y \neq 0 \implies f(y) \neq 0$, but this is true for all field homomorphisms: from $f(1) = 1$ we get for $y \neq 0$ that $1 = y(1/y)$, so $1 = f(1) = f(y)f(1/y)$ and thus $f(y) \neq 0$.) Therefore we have proved a slightly stronger result.

Corollary 3.2. *The only field homomorphism $\mathbf{R} \rightarrow \mathbf{R}$ is the identity.*

4. FIELD AUTOMORPHISMS OF \mathbf{Q}_p

Theorem 4.1. *The only field automorphism of \mathbf{Q}_p is the identity.*

Proof. Let $f: \mathbf{Q}_p \rightarrow \mathbf{Q}_p$ be a field automorphism.

Step 1: $f(r) = r$ for all $r \in \mathbf{Q}$.

The argument is the same one used in the proof of Theorem 3.1.

Step 2: If $|x|_p = 1$ then $|f(x)|_p = 1$.

We use the multiplicative decomposition²

$$\mathbf{Z}_p^\times = \mu_{p-1} \times (1 + p\mathbf{Z}_p).$$

For $x \in \mathbf{Z}_p^\times$ write $x = \omega v$ where $\omega^{p-1} = 1$ and $v \in 1 + p\mathbf{Z}_p$. Then $f(x) = f(\omega)f(v)$. Since $\omega^{p-1} = 1$ we get $f(\omega)^{p-1} = f(1) = 1$, so $|f(\omega)|_p = 1$. For every $n \in \mathbf{Z}^+$ that is not divisible by p , v is an n th power in \mathbf{Z}_p by Hensel's lemma for the polynomial $X^n - v$ with approximate root 1. When v is an n th power, $f(v)$ is also an n th power ($v = a^n \implies f(v) = f(a)^n$), so $f(v)$ is an n th power for infinitely many positive integers n . Since f is injective, $f(v) \neq 0$. Then $n \mid \text{ord}_p f(v)$ for infinitely many n , so $\text{ord}_p(f(v)) = 0$ and therefore $|f(v)|_p = 1$. Finally, $|f(x)|_p = |f(\omega)|_p |f(v)|_p = 1$.

Step 3: For x and y in \mathbf{Q}_p , $|f(x) - f(y)|_p = |x - y|_p$.

This is clear if $x = y$, so assume $x \neq y$. Write $x - y = p^n u$ where $u \in \mathbf{Z}_p^\times$. Then $f(x) - f(y) = f(x - y) = f(p^n u) = f(p)^n f(u)$. By Step 1 we have $f(p) = p$, so $f(x) - f(y) = p^n f(u)$. By Step 2 we have $|f(u)|_p = 1$, so $|f(x) - f(y)|_p = |p^n|_p = 1/p^n = |x - y|_p$.

Step 4: $f(x) = x$ for all $x \in \mathbf{Q}_p$.

For each $x \in \mathbf{Q}_p$ let r_n be a sequence of rational numbers tending p -adically to x , so $|x - r_n|_p \rightarrow 0$ as $n \rightarrow \infty$. By Step 3 $|x - r_n|_p = |f(x) - f(r_n)|_p$, which equals $|f(x) - r_n|_p$ since $f(r_n) = r_n$ (Step 1). Thus $|f(x) - r_n|_p \rightarrow 0$ as $n \rightarrow \infty$, so $f(x) = \lim_{n \rightarrow \infty} r_n = x$. \square

Our proof did not use surjectivity of f , so just as in the real case we really proved a stronger result.

Corollary 4.2. *The only field homomorphism $\mathbf{Q}_p \rightarrow \mathbf{Q}_p$ is the identity.*

²See Theorem 3.2 in <https://kconrad.math.uconn.edu/blurbs/gradnumthy/hensel.pdf>.

5. AUTOMORPHISMS OF A RATIONAL FUNCTION FIELD

For a field K , we write $K(t)$ for the field of rational functions in one indeterminate with coefficients in K . A field automorphism of $K(t)$ can be created using an invertible linear fractional transformation on t :

$$(5.1) \quad f(t) \mapsto f\left(\frac{at+b}{ct+d}\right)$$

for all $f \in K(t)$, where a, b, c, d are fixed elements of K such that $ad - bc \neq 0$. Such an automorphism of $K(t)$ fixes all the constants (*i.e.*, the elements of K) and it can be shown that every field automorphism of $K(t)$ that fixes each element of K arises in this way.³

It is not true in general that a field automorphism of $K(t)$ has to fix all of K , or even map K to K . For example, if $K = F(u)$ for a field F and an indeterminate u , then $K(t) = F(u)(t) = F(t)(u)$ and we get a field automorphism of $K(t)$ by swapping the elements t and u and fixing the elements of F . However, if K is \mathbf{R} or \mathbf{Q}_p , then we'll use our earlier work to show the field automorphisms of $K(t)$ must fix all of K , so the field automorphisms of $\mathbf{R}(t)$ and $\mathbf{Q}_p(t)$ are described using linear fractional transformations on t as indicated in (5.1).

Theorem 5.1. *Each field automorphism of $\mathbf{R}(t)$ fixes every element of \mathbf{R} .*

Proof. Each real number is an n th power of some real number for infinitely many positive integers n . For example, this is true for odd n . We will use this property to show for each field automorphism $\varphi: \mathbf{R}(t) \rightarrow \mathbf{R}(t)$ that $\varphi(\mathbf{R}) \subset \mathbf{R}$. Then φ is a field homomorphism $\mathbf{R} \rightarrow \mathbf{R}$, so φ fixes all of \mathbf{R} by Corollary 3.2.

Since φ is multiplicative, if $c \in \mathbf{R}$ then $\varphi(c)$ is an n th power for infinitely many $n \geq 1$ (*e.g.*, for odd n). To show $\varphi(c) \in \mathbf{R}$, it suffices to show nonconstant elements of $\mathbf{R}(t)$ are *not* n th powers for infinitely many n .

Let $f(t) \in \mathbf{R}(t)$ with $f(t) \notin \mathbf{R}$. Write f in reduced form as g/h , where g and h are in $\mathbf{R}[t] - \{0\}$ and are relatively prime. They are not both constant, since f is not constant. We'll show that if f is an n th power then $n \leq \max(\deg g, \deg h)$.

Suppose $f(t)$ is an n th power of a rational function written in reduced form as $a(t)/b(t)$, so $a(t)$ and $b(t)$ are relatively prime polynomials and they are not both constant (otherwise $f = (a/b)^n$ would be constant, but f is nonconstant). Since $g/h = (a/b)^n$, clearing denominators gives us $b^n g = a^n h$ in $\mathbf{R}[t]$. From $a^n \mid b^n g$ and a and b being relatively prime, $a^n \mid g$. In a similar way, $b^n \mid h$. If a is nonconstant then g is nonconstant (it's a multiple of a^n), and $a^n \mid g \Rightarrow \deg(a^n) \leq \deg g$, so $n \deg a \leq \deg g$. Thus $n \leq \deg g$ (since $\deg a > 0$). If b is nonconstant, then we get $n \leq \deg h$ in a similar way. At least one of these bounds on n holds, so $n \leq \max(\deg g, \deg h)$. \square

The argument in the last paragraph of the previous proof did not depend on the coefficients being in \mathbf{R} . For all fields K , no element of $K(t) - K$ can be an n th power for infinitely many n . That will let us carry over part of the previous proof from $\mathbf{R}(t)$ to $\mathbf{Q}_p(t)$.

Theorem 5.2. *Each field automorphism of $\mathbf{Q}_p(t)$ fixes every element of \mathbf{Q}_p .*

Proof. As in the previous theorem, it suffices (now by Corollary 4.2) to show a field automorphism φ of $\mathbf{Q}_p(t)$ maps \mathbf{Q}_p to \mathbf{Q}_p .

³See <https://math.stackexchange.com/questions/13129>.

Unlike \mathbf{R} , elements of \mathbf{Q}_p might not be n th powers in \mathbf{Q}_p infinitely often: p is not an n th power in \mathbf{Q}_p for $n > 1$. But elements of $1 + p\mathbf{Z}_p$ are n th powers infinitely often, and that will turn out to be enough.

Step 1: $\varphi(1 + p\mathbf{Z}_p) \subset \mathbf{Q}_p$. Each $v \in 1 + p\mathbf{Z}_p$ is an n th power in $1 + p\mathbf{Z}_p$ for infinitely many n , so $\varphi(v)$ is an n th power in $\mathbf{Q}_p(t)$ for infinitely many n . Just as in the previous proof, we conclude that $\varphi(v) \in \mathbf{Q}_p$ (in fact, $\varphi(v) \in \mathbf{Z}_p^\times$, but that's not strictly needed here).

Step 2: $\varphi(\mathbf{Q}_p) \subset \mathbf{Q}_p$. This is obvious at 0. For $x \in \mathbf{Q}_p^\times$, write $x = p^n u$ for $u \in \mathbf{Z}_p^\times$ and $u = \omega v$, where $\omega^{p-1} = 1$ and $v \in 1 + p\mathbf{Z}_p$. Then $\varphi(x) = \varphi(p^n \omega v) = \varphi(p)^n \varphi(\omega) \varphi(v)$. By Step 1, $\varphi(v) \in \mathbf{Q}_p$. Why are $\varphi(p)$ and $\varphi(\omega)$ in \mathbf{Q}_p ?

Since φ fixes every rational number (from fixing 1 and being a field homomorphism), $\varphi(p) = p$. Since $\varphi(\omega)^{p-1} = \varphi(\omega^{p-1}) = \varphi(1) = 1$, $\varphi(\omega)$ is a $(p-1)$ -th root of unity. The polynomial $T^{p-1} - 1$ has $p-1$ roots in \mathbf{Q}_p , which matches the degree of the polynomial, so all of the roots of $T^{p-1} - 1$ in a larger field like $\mathbf{Q}_p(t)$ must be its roots in \mathbf{Q}_p , and thus $\varphi(\omega) \in \mathbf{Q}_p$. \square

The reasoning used here never needed surjectivity of the automorphisms of $\mathbf{R}(t)$ or $\mathbf{Q}_p(t)$, so we proved a stronger result.

Theorem 5.3. *Each field homomorphism $\mathbf{R}(t) \rightarrow \mathbf{R}(t)$ or $\mathbf{Q}_p(t) \rightarrow \mathbf{Q}_p(t)$ fixes all elements of \mathbf{R} or \mathbf{Q}_p .*

6. AUTOMATIC CONTINUITY OF HOMOMORPHISMS BETWEEN LOCAL FIELDS

If you know about finite extensions of \mathbf{Q}_p , the local fields of characteristic 0, then the following result will be of interest. It says the only way there can be field homomorphisms among such fields (allowing p to vary) is when the fields are finite extensions of the same \mathbf{Q}_p , in which case the homomorphism must be continuous.

Theorem 6.1. *Let K be a finite extension of \mathbf{Q}_p and L be a finite extension of \mathbf{Q}_q for some primes p and q . If there is a field homomorphism $f : K \rightarrow L$, then $p = q$ and f is a \mathbf{Q}_p -linear isometry.*

Proof. Write the ring of integers of K and its maximal ideal as \mathcal{O}_K and \mathfrak{m}_K , and likewise define \mathcal{O}_L and \mathfrak{m}_L .

Step 1: $f(1 + \mathfrak{m}_K) \subset \mathcal{O}_L^\times$.

Let $x \in 1 + \mathfrak{m}_K$. By Hensel's lemma, x is an n th power in $1 + \mathfrak{m}_K$ for infinitely many $n \geq 1$, which makes $f(x)$ an n th power in L for infinitely many $n \geq 1$, and $f(x) \neq 0$. Thus $f(x) \in \mathcal{O}_L^\times$ for the same reason a nonzero element of \mathbf{Q}_p that's an n th power infinitely often is in \mathbf{Z}_p^\times (see Step 2 in the proof of Theorem 4.1).

Step 2: $f(\mathcal{O}_K^\times) \subset \mathcal{O}_L^\times$.

Let $x \in \mathcal{O}_K^\times$. Using Teichmüller representatives, $x = \zeta y$ where ζ is a root of unity and $y \in 1 + \mathfrak{m}_K$. Since $f(\zeta)$ is a root of unity and $f(y) \in \mathcal{O}_L^\times$ by Step 1, $f(x) = f(\zeta)f(y) \in \mathcal{O}_L^\times$.

Step 3: $f(\mathcal{O}_K) \subset \mathcal{O}_L$.

By Step 2, it suffices to show $f(\mathfrak{m}_K) \subset \mathcal{O}_L$. Let $x \in \mathfrak{m}_K$. Then $1 + x \in \mathcal{O}_K^\times$, so $f(1 + x) = 1 + f(x)$ is in \mathcal{O}_L^\times by Step 1, so $f(x) \in \mathcal{O}_L$.

Step 4: $p = q$.

By Step 3, the field homomorphism $f : K \rightarrow L$ restricts a ring homomorphism $\mathcal{O}_K \rightarrow \mathcal{O}_L$. Compose this with the standard reduction map $\mathcal{O}_L \rightarrow \mathcal{O}_L/\mathfrak{m}_L$ to get a ring homomorphism $\mathcal{O}_K \rightarrow \mathcal{O}_L/\mathfrak{m}_L$. Its kernel must be a nonzero ideal in \mathcal{O}_K since \mathcal{O}_K is infinite while $\mathcal{O}_L/\mathfrak{m}_L$

is finite. Every nonzero ideal in \mathcal{O}_K has the form \mathfrak{m}_K^i for some $i \geq 0$, so there is an injective ring homomorphism $\mathcal{O}_K/\mathfrak{m}_K^i \rightarrow \mathcal{O}_L/\mathfrak{m}_L$. Since $\mathcal{O}_L/\mathfrak{m}_L$ is a finite field, its subrings are fields, which makes $\mathcal{O}_K/\mathfrak{m}_K^i$ a field. Thus $i = 1$, so the residue field $\mathcal{O}_K/\mathfrak{m}_K$ embeds into the residue field $\mathcal{O}_L/\mathfrak{m}_L$. That implies the residue fields have the same characteristic. Since their characteristics are p and q , $p = q$.

Step 5: $|f(x)|_p = |x|_p$ for all $x \in K$, so f is an isometry.

This is obvious when $x = 0$, so take $x \neq 0$.

By Step 4, K and L are finite extensions of the same \mathbf{Q}_p . Let π be a prime element of K , so $p = \pi^e u$ for some $e \geq 1$ and $u \in \mathcal{O}_K^\times$. Since $x \neq 0$, $x = \pi^m v$ for some $m \in \mathbf{Z}$ and $v \in \mathcal{O}_K^\times$. Then $|x|_p = |\pi^m|_p = |\pi|_p^m$, so $|x^e|_p = |\pi^e|_p^m = |p|_p^m = |p^m|_p$, so $|x^e/p^m|_p = 1$. Then Step 2 implies $|f(x^e/p^m)|_p = 1$, so $|f(x)^e/p^m|_p = 1$. Thus $|f(x)|_p^e = |p|_p^m = |x^e|_p = |x|_p^e$, so $|f(x)|_p = |x|_p$.

Since f is an isometry by Step 5, f is continuous. It necessarily fixes \mathbf{Q} , so by continuity it has to fix \mathbf{Q}_p : when $c \in \mathbf{Q}_p$ there's a sequence $\{r_n\}$ in \mathbf{Q} such that $|c - r_n|_p \rightarrow 0$ as $n \rightarrow \infty$, so

$$\begin{aligned} |f(c) - c|_p &= |f(c) - r_n + r_n - c|_p \\ &\leq \max(|f(c) - r_n|_p, |r_n - c|_p) \\ &\leq \max(|f(c - r_n)|_p, |c - r_n|_p) \end{aligned}$$

since $f(r_n) = r_n$ due to $r_n \in \mathbf{Q}$. Since $|f(c - r_n)|_p = |c - r_n|_p$ by Step 5, $|f(c) - c|_p \leq |c - r_n|_p \rightarrow 0$ as $n \rightarrow \infty$, so $|f(c) - c|_p = 0$. Thus $f(c) = c$. For all $x \in K$ and $c \in \mathbf{Q}_p$, $f(cx) = f(c)f(x) = cf(x)$, so f is \mathbf{Q}_p -linear. \square

Corollary 6.2. *For different primes p and q , a finite extension of \mathbf{Q}_p and a finite extension of \mathbf{Q}_q can't be isomorphic.*

Proof. Call the fields K and L . If there is a field isomorphism $K \rightarrow L$ then $p = q$ by Theorem 6.1. \square

A special case of Corollary 6.2 is that $\mathbf{Q}_p \not\cong \mathbf{Q}_q$ as fields when p and q are different primes. This has a simple direct proof based on counting roots of unity. There are $p - 1$ roots of unity in \mathbf{Q}_p when $p > 2$ and 2 roots of unity in \mathbf{Q}_2 , so $\mathbf{Q}_p \not\cong \mathbf{Q}_q$ as fields if $p > 3$ or $q > 3$. This only leaves out the case of \mathbf{Q}_2 and \mathbf{Q}_3 , which are not isomorphic fields since 7 is a square in \mathbf{Q}_3 and 7 is not a square in \mathbf{Q}_2 . For finite extensions of \mathbf{Q}_p and \mathbf{Q}_q , the scope of examples with the same number of roots of unity becomes more varied than just \mathbf{Q}_2 and \mathbf{Q}_3 : $\mathbf{Q}_2(i)$ and $\mathbf{Q}_5(\sqrt{5})$ both have 4 roots of unity, while $\mathbf{Q}_{11}(\sqrt{2})$ and $\mathbf{Q}_5(\sqrt{2}, \zeta_5)$ both have 120 roots of unity (why?).

Corollary 6.3. *Let K be a finite extension of \mathbf{Q}_p . Every field homomorphism $K \rightarrow K$ must be continuous and is a \mathbf{Q}_p -automorphism of K .*

Proof. Let $f : K \rightarrow K$ be a field homomorphism, so it is injective. By Theorem 6.1, f is continuous and \mathbf{Q}_p -linear. Since K is a finite-dimensional vector space over \mathbf{Q}_p , f is an injective \mathbf{Q}_p -linear map of a finite-dimensional \mathbf{Q}_p -vector space to itself, so for dimension reasons the injectivity of f implies it is surjective. Thus f is a field automorphism of K . \square

Example 6.4. Let K be a finite extension of $\mathbf{Q}_5(\sqrt{2})$. A field homomorphism $f : K \rightarrow K$ has to be a \mathbf{Q}_5 -linear field automorphism of K by Corollary 6.3. It must map $\sqrt{2}$ in K to $\pm\sqrt{2}$ (why?), so f on $\mathbf{Q}_5(\sqrt{2})$ is either the identity map or the conjugation map $x + y\sqrt{2} \rightarrow x - y\sqrt{2}$ for all $x, y \in \mathbf{Q}_5$.

The real numbers lie in the larger field \mathbf{C} , which is 2-dimensional over \mathbf{R} , but it turns out we can't dig inside \mathbf{R} in a finite-dimensional way: if a field K is contained in \mathbf{R} and $[\mathbf{R} : K]$ is finite, then $K = \mathbf{R}$. The proof uses the complex numbers and a piece of algebra called the Artin–Schreier theorem.⁴ Here is a p -adic analogue based on Corollary 6.3, which I learned from Lubin's answer to <https://math.stackexchange.com/questions/2893911>.

Theorem 6.5. *If a field K is contained in \mathbf{Q}_p and $[\mathbf{Q}_p : K]$ is finite, then $K = \mathbf{Q}_p$.*

Proof. Enlarge the finite extension \mathbf{Q}_p/K to a finite Galois extension L/K and let $G = \text{Gal}(L/K)$. Each $\sigma \in G$ is a field automorphism of L , which is a finite extension of \mathbf{Q}_p , so σ is the identity on \mathbf{Q}_p by Corollary 6.3. Thus $\mathbf{Q}_p \subset L^G = K$, so $K = \mathbf{Q}_p$ by Galois theory. \square

What can be about field homomorphisms between a finite extension of \mathbf{Q}_p and \mathbf{R} or \mathbf{C} ?

Theorem 6.6. *When K is a finite extension of \mathbf{Q}_p , there are no field homomorphisms $K \rightarrow \mathbf{R}$ or $\mathbf{R} \rightarrow K$. There is no field homomorphism $\mathbf{C} \rightarrow K$ and there is no continuous field homomorphism $K \rightarrow \mathbf{C}$, but there are field homomorphisms $K \rightarrow \mathbf{C}$.*

Proof. In \mathbf{Q}_p there are negative integers that are squares (use -7 when $p = 2$ and $1-p$ when $p \geq 3$), so if there were a field homomorphism $f : K \rightarrow \mathbf{R}$ then, since f has to be injective and fix \mathbf{Z} , there would be negative integers that are squares in \mathbf{R} , which is impossible.

In \mathbf{R} , p is an n th power for all $n \geq 1$, so if there were a field homomorphism $f : \mathbf{R} \rightarrow K$ then, since f has to be injective and fix \mathbf{Z} , p would be an n th power in K for all $n \geq 1$. That would imply $p \in \mathcal{O}_K^\times$, which is false.

If there were a continuous field homomorphism $f : K \rightarrow \mathbf{C}$ then from $p^n \rightarrow 0$ in K we'd get $p^n \rightarrow 0$ in \mathbf{C} , which is false. So f doesn't exist.

The reason there are field homomorphisms $K \rightarrow \mathbf{C}$ (just not continuous ones) depends on Zorn's lemma, so it is completely non-constructive. Let \overline{K} be an algebraic closure of K . Since \mathbf{Q}_p has the same uncountable cardinality as \mathbf{R} , and thus as \mathbf{C} , the finite extension K of \mathbf{Q}_p also has the same uncountable cardinality as \mathbf{C} . Every infinite field has the same cardinality as its algebraic closure, so \overline{K} and \mathbf{C} have the same cardinality. Using Zorn's lemma (and a transcendence basis argument), it can be shown that two uncountable algebraically closed fields of the same characteristic and cardinality are isomorphic as abstract fields. (**Warning:** countable algebraically closed fields of the same characteristic need not be isomorphic, like the algebraic closures of \mathbf{Q} and $\mathbf{Q}(t)$.) Since \overline{K} and \mathbf{C} are algebraically closed of characteristic 0 with the same uncountable cardinality, they are thus (very non-constructively) isomorphic as abstract fields, so the embedding of K into its algebraic closure \overline{K} can be composed with an isomorphism $\overline{K} \rightarrow \mathbf{C}$ to produce a field homomorphism $K \rightarrow \mathbf{C}$. \square

⁴See Corollary 3.2 in <https://kconrad.math.uconn.edu/blurbs/galoistheory/artinschreier.pdf>.