

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} : f

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 $a = c$.

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 decomposition

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

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 . Thus $n \mid \text{ord}_p f(v)$ 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.*