Wild Automorphisms

Elizabeth Wolfe

2020

Introduction

In 2016, in fulfillment of the Colorado College Mathematics Thesis requirement, Beini Yu wrote a paper that found all wild automorphisms of the complex field of order 2. This paper extends the work Beini did to find wild automorphisms of order n for all $n \in \mathbb{N}$ and one of infinite order.

Section 1

A field automorphism is a bijective homomorphism from the field onto itself which also preserves the addition and multiplication operators of the field. Since field automorphisms preserve addition and multiplication, they will also preserve subtraction and division. We are studying $\mathbb{C}$, which is a field of characteristic 0, and we in this paper we will only deal with other fields of characteristic 0, such as $\mathbb{Q}$ or $\mathbb{R}$. A field with characteristic 0 will contain up to isomorphism a copy of $\mathbb{Z}$ and thus of $\mathbb{Q}$, where $\mathbb{Q}$ is called the prime subfield. Any field automorphism of a characteristic 0 field will always take the prime subfield onto itself, and thus each of the field automorphisms we will deal with in this paper will take $\mathbb{Q}$ onto itself (i.e., it will leave $\mathbb{Q}$ fixed).

For any field F, the set of $\mathrm{Aut}(F)$ is a group under composition. Note that the group $\mathrm{Aut}(\mathbb{Q})$ is trivially $\{i\}$. Like $\mathbb{Q}$, the group $\mathrm{Aut}(\mathbb{R})$ is $\{i\}$, since the field $\mathbb{Q}$ is dense in $\mathbb{R}$. Thus, since $\mathbb{R}$ is an ordered field and an automorphism of $\mathbb{R}$ will leave $\mathbb{Q}$ fixed, it will also leave $\mathbb{R}$ fixed.

For example, the group of $\mathrm{Aut}(\mathbb{C}|\mathbb{R})$ (the group of automorphisms of $\mathbb{C}$ which also fix $\mathbb{R}$), however, is equal to $\{i, \kappa_{\mathbb{R}}\}$, where i is the identity automorphism and $\kappa_{\mathbb{R}}$ is complex conjugation. So $|\mathrm{Aut}(\mathbb{C}|\mathbb{R})| = 2$. This is because if we consider the construction of the complex numbers, then $\mathbb{C} = \mathbb{R}(i) \cong \mathbb{R}[x]/\langle x^2 + 1\rangle$. Under any automorphism $x^2 + 1$ must be the same polynomial, and this can only happen if the automorphism sends the roots of the polynomial to other roots. The polynomial $x^2 + 1$ has 2 roots, i and $-i$. Therefore the group of $\mathrm{Aut}(\mathbb{C}|\mathbb{R})$ will have two elements, which have already been found.

However, if we widen our search to automorphisms of $\mathbb{C}$ which do not fix $\mathbb{R}$, called *wild automorphisms*, we have much more room to explore.

Section 2

In this paper we will be especially concerned with the cardinality of fields. The cardinality of a field is a measure of the field's size. The smallest infinite cardinality, $\aleph_0$, is countable and is the cardinality of the natural numbers. The cardinality of the real numbers, as well of the complex numbers, is the cardinal number $2^{\aleph_0}$, which is also $\mathfrak{c}$. If we consider a set S of cardinality s, the cardinality of the power set, $\mathcal{P}(S)$, the set of all subsets of S, is 2^s. This brings us to Zorn's Lemma:

Zorn's Lemma If X is a non-empty partially ordered set such that every chain in X has an upper bound, then X contains a maximal element [3].

Zorn's Lemma is equivalent to the axiom of choice. In our description of wild automorphisms, we can only construct these automorphisms using Zorn's Lemma. We will look at these automorphisms as partially ordered sets, and then apply Zorn's Lemma.

Section 3

In Theorem 1.1, we are going to apply Zorn's Lemma to a set of functions. If we consider an automorphism, θ, and the set of automorphisms which are extensions of θ, we may call this set a family, $\mathcal{F}$.

To establish that these automorphisms can be thought of as a partially ordered set, consider that each of the automorphisms in this set can be thought of as a set of ordered pairs. Since $\mathcal{F}$ is a family of automorphisms, the domain of any function in $\mathcal{F}$ is equal to its range. If $f \in \mathcal{F}$, then the set $f \subseteq X \times X$ is a function such that if $(a, b), (a, c) \in f$, then $b = c$. It follows that if $f, g, \in \mathcal{F}$, and f is a subset of g, then $\text{dom}(f) \subseteq \text{dom}(g)$. This is because if $a \in$dom(f), then $f(a) = g(a)$. Thus, $\mathcal{F}$ may be partially ordered by inclusion.

Theorem 1.1 will also rely on Lemma 3.2B and 3.2A from [2]. These Lemmas appear neatly stated in [2], but they are simply extensions of results which could be found in most Algebra textbooks (for instance, [1]). These two lemmas allow us to extend automorphisms:

Lemma 3.2A Let ϕ be an isomorphism with domain F and range F'. If α is algebraic over F then there is an isomorphism extending ϕ to $F(\alpha)$ and sending α to β iff β is a root of the polynomial obtained by applying ϕ to the coefficients of the minimal polynomial of α over F.

Lemma 3.2B Let ϕ be an isomorphism with domain F and range F'. If α is transcendental over F, then there is an isomorphism extending ϕ to $F(\alpha)$ and sending α to a number that is transcendental over F'.

Theorem 1.1 Any order n automorphism of a subfield of $\mathbb{C}$ can be extended to an order n automorphism of $\mathbb{C}$, where $n \in \mathbb{N}$.

Proof. Let θ be an order n automorphism of $K \subseteq \mathbb{C}$. Let ϕ be any automorphism of L that extends θ, where $K \subseteq L \subseteq \mathbb{C}$. Let $\mathcal{F}$ be the set of all such ϕ's of order n. We may notice $\mathcal{F} \neq \emptyset$. The domain of each ϕ is contained in $\mathbb{C}$, and $\mathcal{F}$ is a partially ordered set.

Pick a chain $\mathcal{C} = \{\phi_\alpha : \alpha \in A\} \subseteq \mathcal{F}$, where A is an index set. If we take $\cup\{\phi_\alpha\}$, we will show this union is also an automorphism. If we take $a, b \in$dom$(\cup\{\phi_\alpha\})$, then the action of

$\cup\{\phi_\alpha\}$ on a, b is the same as the action of ϕ_w for any $w \in A$ for which $a, b \in$dom(ϕ_w). Without loss of generality, we may pick ϕ_w to be any $\phi_w \subseteq \cup\{\phi_\alpha\}$. Thus, $\cup\{\phi_\alpha\}(a+b) = \phi_w(a+b) = \phi_w(a) + \phi_w(b) = \cup\{\phi_\alpha\}(a) + \cup\{\phi_\alpha\}(b)$. Similarly $\cup\{\phi_\alpha\}$ preserves multiplication. Thus, $\cup\{\phi_\alpha\}$ is a homomorphism. We can see that $(0, 0)$ and $(1, 1) \in \cup\{\phi_\alpha\}$. Therefore, $\cup\{\phi_\alpha\}$ is a function, with domain $\cup$dom(ϕ_α) and range $\cup$range(ϕ_α). Similarly, we may argue $\cup\{\phi_\alpha\}$ is injective, and surjective. Thus, $\cup\{\phi_\alpha\}$ is an automorphism. If we pick any $(a, b) \in \cup\{\phi_\alpha\}$, then for some $\alpha \in A$, $\phi_\alpha^n(a) = a$ because $\phi_\alpha \in \mathcal{F}$. Thus, since the ϕ_α's are all order n and created by extensions of ϕ, we claim $\cup\{\phi_\alpha\}$ is also an order n automorphism. The function $(\phi_\alpha)^n(a) = a$ for all ϕ_α. Therefore, if we have $a \in$dom(ϕ_α), we see that $\cup\{\phi_\alpha\}^n(a) = a$ for $\alpha \in A$. Thus, $\cup\{\phi_\alpha\}$ is an upper bound for $\mathcal{C}$ in $\mathcal{F}$. Thus $\mathcal{F}$ satisfies the conditions for Zorn's Lemma, and $\mathcal{F}$ contains a maximal element.

We may call this maximal element guaranteed by Zorn's Lemma $\phi_m \in \mathcal{F}$, where $\phi_m : K_m \to K_m$ and $K_m \subseteq \mathbb{C}$. We want to show that $K_m = \mathbb{C}$.

So, by way of contradiction, pick $q \in \mathbb{C} \backslash K_m$. If q is algebraic or transcendental over K_m, by Lemmas 3.2A and B, [2], ϕ_m may be extended to $\hat{\phi_m}$, where $\hat{\phi_m} : K_m(q) \to K_m(q)$. Since $\hat{\phi_m}$ is an extension of ϕ_m, the action of ϕ_m on dom(ϕ_m) is the same as the action of $\hat{\phi_m}$ on dom(ϕ_m). Therefore, for any $k \in$ dom(ϕ_m), $\hat{\phi_m}^n(k) = k$. Since q is the only other generator for $K_m(q)$, the action of $\hat{\phi_m}$ on $K_m(q)$ is determined solely by the action of $\hat{\phi_m}$ on q. But we may assume, without loss of generality, that $\hat{\phi_m}(q) = q$. Thus, $\hat{\phi_m}^n(q) = q$, and $\hat{\phi_m}$ is an order n automorphism of $K_q \subseteq \mathbb{C}$. But this is a contradiction of the maximality of $\phi_m \in \mathcal{F}$. Therefore, K_m contains all elements $q \in \mathbb{C}$.

Therefore, $K_m = \mathbb{C}$, and ϕ_m is an order n automorphism of $\mathbb{C}$. □

Theorem 1.1 asserts that any order n automorphism of a subfield of $\mathbb{C}$ can be extended to an order n automorphism of $\mathbb{C}$, but in order to extend such an automorphism to $\mathbb{C}$, we must have that there exists at least one automorphism of order n $\forall n \in \mathbb{N}$, so that $\mathcal{F}$ is non-empty and we may apply Zorn's Lemma. It is certainly true that such elements exist; the first proof that we have such elements was by Hilbert himself. Hilbert found that there exists a Galois group over $\mathbb{Q}$ which can be represented as S_n, and S_n has an element of order n $\forall n \in \mathbb{N}$. And if we have such elements, then it follows there exists automorphisms of the subfields of $\mathbb{C}$ that are of order n $\forall n \in N$, and Corollary 1.1 immediately follows from Theorem 1.1:

Corollary 1.1 There exists an automorphism of $\mathbb{C}$ of order n for all $n \in \mathbb{N}$.

Notice that when $n > 2$, there exists wild automorphisms of $\mathbb{C}$ for each n. This is because there certainly exist automorphisms of $\mathbb{R}$ which do not leave $\mathbb{R}$ fixed of order n for all $n \in \mathbb{N}$, and thus by Theorem 1.1, these automorphisms may be extended to $\mathbb{C}$. If there exists automorphisms of $\mathbb{C}$ of order n for all of $\mathbb{N}$, then it is natural to ask if there exist automorphisms of $\mathbb{C}$ which have infinite order. Theorem 1.2 uses the fact that if we pick two numbers that are transcendental over $\mathbb{Q}$, α, β, then $\mathbb{Q}(\alpha) \cong \mathbb{Q}(\beta)$ by an isomorphism ϕ where $\phi(\alpha) = \beta$.

Theorem 1.2 There exists an automorphism of $\mathbb{C}$ that is of infinite order.

Proof. Consider $\phi : \mathbb{Q}(\pi) \to \mathbb{Q}(\pi + 1)$, where ϕ leaves $\mathbb{Q}$ fixed, and $\phi(\pi) = \pi + 1$. Thus,

ϕ is a function, and ϕ is at least an isomorphism. The function ϕ is of infinite order, since $\phi^n(\pi) = \pi + n \neq \pi$, $\forall n \in \mathbb{N}$, $n \neq 0$. Notice that $\mathbb{Q}(\pi) = \mathbb{Q}(\pi + 1)$. Thus, ϕ is an automorphism. □

For Theorem 1.3, we will use the definition of algebraic independence from [2]:

Definition 4.8A *Algebraically Independent* If L is a field extension of K then $B \subset L$ is algebraically independent over K iff every $b \in B$ is transcendental over the field extension $K(B \backslash \{b\})$.

[2] offers the example that although π and 2π are both transcendental over $\mathbb{Q}$, they are not algebraically independent.

Now that by Theorem 1.1 we have shown that there is at least one order n automorphism of $\mathbb{C}$ for all n, Theorem 1.3 will show that there are more.

Theorem 1.3 (a) There are at least $\mathfrak{c}$ many distinct automorphisms of $\mathbb{C}$ of infinite order. (b) There are at least $\mathfrak{c}$ many distinct automorphisms of $\mathbb{C}$ of order n for all $n \in \mathbb{N}$.

Proof. (a) There exists uncountably many transcendental numbers over $\mathbb{Q}$. Consider α and β transcendental over $\mathbb{Q}$, where α and β are algebraically independent. Then let $\phi : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha + 1)$, where $\phi(\alpha) = \alpha + 1$, and $\theta : \mathbb{Q}(\beta) \to \mathbb{Q}(\beta + 1)$, where $\theta(\beta) = \beta + 1$. If we extend ϕ and θ by letting $\phi(\beta) = \beta$ and $\theta(\alpha) = \alpha$ and then apply the Zorn's Lemma argument used in Theorem 1.1, then ϕ and θ will be distinct automorphisms of $\mathbb{C}$. By Theorem 1.1, both ϕ and θ can be extended to $\mathbb{C}$. Therefore, there are at least uncountably many distinct automorphisms of $\mathbb{C}$ of infinite order.

(b) Pick α, β, $\gamma \in \mathbb{C} \backslash \mathbb{Q}$ where α, β, γ are transcendental over $\mathbb{Q}$ and algebraically independent of each other. Therefore,

$$\begin{aligned} &\alpha \text{ is transcendental over } \mathbb{Q}(\beta, \gamma) \\ &\beta \text{ is transcendental over } \mathbb{Q}(\alpha, \gamma) \\ &\gamma \text{ is transcendental over } \mathbb{Q}(\alpha, \beta) \end{aligned}$$

Additionally, $\mathbb{Q}(\alpha) \cong \mathbb{Q}(\beta)$, and since γ is transcendental over $\mathbb{Q}(\alpha, \beta)$, $\mathbb{Q}(\alpha, \gamma) \cong \mathbb{Q}(\beta, \gamma)$. Therefore, we have an isomorphism $\theta : \mathbb{Q}(\alpha, \gamma, \beta) \to \mathbb{Q}(\beta, \gamma, \alpha)$ where $\theta(\alpha) = \beta$, $\theta(\beta) = \gamma$, and $\theta(\gamma) = \alpha$. This is a 3-cycle, and θ has order 3. By Theorem 1.1, θ can be extended to an automorphism of $\mathbb{C}$.

Since there are uncountably many transcendental numbers, we can continue picking new α, β, γ until we get uncountably many distinct automorphisms of $\mathbb{C}$ that have order 3. Similarly, we can then find n algebraically independent transcendental numbers over $\mathbb{Q}$ for any finite n and extend this automorphism to an automorphism of $\mathbb{C}$. Thus, there are uncountably many distinct automorphisms of $\mathbb{C}$ of order n for all $n \in \mathbb{N}$. □

We are going to extend the reasoning in the proof for Theorem 1.3 to find $2^{\mathfrak{c}}$ many distinct automorphisms of $\mathbb{C}$ of order n $\forall n \in \mathbb{N}$. To do this, we will use the definition of a transcendence base from [4]:

Definition 4.8B *Transcendence Base*: A set $\mathcal{B} \subset L$ is a *transcendence base* of L over K iff $\mathcal{B}$ is algebraically independent over K and L is an algebraic extension of $K(\mathcal{B})$.

Returning to the example for algebraic independence above, π and 2π could thus not be a transcendence base [2].

Notice that there are $\mathfrak{c}$ transcendental numbers. There are also $\mathfrak{c}$ algebraically independent real numbers. This can be seen by considering that if I have a transcendence base for $\mathbb{C}$ over $\mathbb{Q}$, it will be an uncountable set, since any transcendence base for $\mathbb{C}$ over $\mathbb{Q}$ has to have uncountably many elements (and thus has cardinality $\mathfrak{c}$). If this transcendence base had instead countably many elements, then the base would only generate countably many elements. But $\mathbb{C}$ has uncountably many elements, and $\mathbb{C}$ must have a transcendence base with countably many elements.

First, using the fact that $\mathfrak{c} = 2^{\aleph_0}$ and cardinal arithmetic, we may notice that $\mathfrak{c}^{\mathfrak{c}} = (2^{\aleph_0})^{\mathfrak{c}} = 2^{\mathfrak{c} \times \aleph_0} = 2^{\mathfrak{c}}$. We can see that $\mathfrak{c}^{\mathfrak{c}}$ is the number of functions there are from a set of cardinality $\mathfrak{c}$ to itself, and is thus the maximum number of automorphisms of $\mathbb{C}$. Thus, the maximum number of automorphisms of $\mathbb{C}$ is $\mathfrak{c}^{\mathfrak{c}} = 2^{\mathfrak{c}}$.

Then, consider A, the set of all algebraically independent sets for $\mathbb{C}$ over $\mathbb{Q}$. By Zorn's Lemma, there exists a maximal algebraically independent set, and this set will solely consist of transcendental numbers. This is a transcendence base $\mathcal{B}$ for $\mathbb{C}$ over $\mathbb{Q}$. We know that $|\mathcal{B}| = \mathfrak{c}$, since $|\mathcal{B}|$ can't be more than $\mathfrak{c}$ because $B \subseteq \mathbb{C}$, and if $|\mathcal{B}| < \mathfrak{c}$, then $\mathcal{B}$ would be countable. There exists $2^{\mathfrak{c}}$ distinct subsets of $\mathbb{C}$, and if we look at the set of the subsets of $\mathcal{B}$, $|\mathcal{P}(\mathcal{B})| = 2^{\mathfrak{c}}$. Picking each $\mathcal{H}$ in $\mathcal{P}(\mathcal{B})$, we may form a field $\mathbb{Q}(\mathcal{H})$, which is a subfield of $\mathbb{C}$. Additionally, if we take two distinct subsets of $\mathcal{B}$, $\mathcal{H}_\infty$ and $\mathcal{H}_\in$, $\mathcal{H}_\infty \neq \mathcal{H}_\in$, then the fields we form, $\mathbb{Q}(\mathcal{H}_\infty)$ and $\mathbb{Q}(\mathcal{H}_\in)$ are distinct subfields of $\mathbb{C}$. This is because if $\mathcal{H}_\infty \neq \mathcal{H}_\in$, then we may assume without loss of generality that there exists a $\alpha \in \mathcal{H}_\infty \backslash \mathcal{H}_\in$, and α is clearly in $\mathbb{Q}(\mathcal{H}_\infty)$, and not in $\mathbb{Q}(\mathcal{H}_\in)$, because α is transcendental over $\mathbb{Q}(\mathcal{H}_\in)$. Thus, $\mathbb{Q}(\mathcal{H}_\infty)$ and $\mathbb{Q}(\mathcal{H}_\in)$ are not equal. From this process, we may find $2^{\mathfrak{c}}$ subfields $\{\mathbb{Q}(\mathcal{H}) : \mathcal{H} \subseteq \mathcal{B}\}$. As the proof of Theorem 1.4 will show, we may then build automorphisms of order n of each of these $2^{\mathfrak{c}}$ subfields of $\mathbb{C}$, and we may extend each of these automorphisms of order n to a corresponding automorphism of order n of $\mathbb{C}$. Thus, we will have $2^{\mathfrak{c}}$ automorphisms of $\mathbb{C}$ of order n for each $n \in \mathbb{N}$.

Theorem 1.4 There exist $2^{\mathfrak{c}}$ many automorphisms of $\mathbb{C}$ of order n for all $n \in \mathbb{N}$.

Proof. Pick $\alpha, \beta \in \mathcal{B}$, a transcendence base of $\mathbb{C}$ over $\mathbb{Q}$. Let $\mathcal{B}^* = \mathcal{B} \backslash \{\alpha, \beta\}$. Note that since $\{\alpha, \beta\}$ is finite, $|\mathcal{B}^*| = |\mathcal{B}| = \mathfrak{c}$, so $|\mathcal{P}(\mathcal{B}^*)| = 2^{\mathfrak{c}}$. In fact, if we pick $\eta \in \mathcal{B}^*$ and consider the set $\mathcal{C} = \{(\mathcal{H}, \eta) : \mathcal{H} \subseteq \mathcal{B}^*\}$, the cardinality of $\mathcal{C} = 2^{\mathfrak{c}} * \mathfrak{c} = 2^{\mathfrak{c}}$. For each $(\mathcal{H}, \eta) \in \mathbb{C}$, we can get a degree 3 automorphism of $\mathbb{C}$. If $(\mathcal{H}_\infty, \eta_\alpha) \neq (\mathcal{H}_\in, \eta_\epsilon)$, then we will get two distinct automorphisms from these ordered pairs. We may injectively map a pair $(\mathcal{H}, \eta)$ to a corresponding order 3 automorphism, $\mathbb{Q}(\mathcal{H})(\alpha, \beta, \eta) \to \mathbb{Q}(\mathcal{H})(\alpha, \beta, \eta)$, where $\mathbb{Q}(\mathcal{H})(\alpha, \beta, \eta) \subseteq \mathbb{C}$. Now, given any $\mathcal{H}_\infty$, $\mathcal{H}_\in \subseteq \mathcal{B}^*$, $\mathcal{H}_\infty \neq \mathcal{H}_\in$, there exists $\eta \in \mathcal{H}_\infty \backslash \mathcal{H}_\in$, and we may pick the $\mathcal{H}_\infty$, $\mathcal{H}_\in$ with just one such η without loss of generality. Thus, $(\mathcal{H}_\infty, \eta) \in \mathcal{C}$, and we may obtain an order 3 automorphism of $\mathbb{Q}(\mathcal{H}_\infty)(\alpha, \beta, \eta) \to \mathbb{Q}(\mathcal{H}_\infty)(\alpha, \beta, \eta)$ by permuting α, β, η and extending this automorphism to $\mathbb{C}$ by Theorem 1.1, where each such automorphism is distinct according to each $\mathcal{H}$ we choose. Thus if we use each element of $\mathcal{C}$, we will get $|\mathcal{C}|$ automorphisms.

Since there are $2^{\mathfrak{c}}$ subsets $\mathcal{H}$ of $\mathcal{B}$, this gives us $2^{\mathfrak{c}}$ distinct automorphisms of $\mathbb{C}$ of order 3. Since $|\mathcal{F}(\mathbb{C})| \leq |\mathcal{P}(\mathbb{C})| = 2^{\mathfrak{c}}$ [2], the most automorphisms of $\mathbb{C}$ of order 3 we may have is $2^{\mathfrak{c}}$. Thus, there are $2^{\mathfrak{c}}$ automorphisms of $\mathbb{C}$ of order 3.

We can extend the above to all $n \in \mathbb{N}$ by picking n numbers in $\mathcal{B} \backslash \mathcal{H}$ for all $n \in \mathbb{N}$, and we will be able to create distinct automorphisms of order n for all $\mathcal{H} \subseteq \mathcal{B}$ by fixing $\mathcal{H}$ and permuting the n numbers in $\mathcal{B} \backslash \mathcal{H}$. This works for all for all $\mathcal{H} \subseteq \mathcal{B}$ where $|\mathcal{B} \backslash \mathcal{H}| \geq 3$. We can thus find $2^{\mathfrak{c}}$ automorphisms of $\mathbb{C}$ of order n for all $n \in \mathbb{N}$, and using the argument above, this means there exits $2^{\mathfrak{c}}$ many automorphisms of $\mathbb{C}$ of order n for all $n \in \mathbb{N}$. □

References

[1] Anderson and Feil, A First Course in Abstract Algebra: Rings, Groups, and Fields. 3rd ed, 2015.

[2] Beini, Yu, Wild Automorphisms of the Complex Field, 2016.

[3] Halmos, Paul R., Naive Set Theory, 2011.

[4] Yale, Paul B. Automorphisms of the complex numbers. *Mathematics Magazine*, 39:135-141, 1966.