WILD AUTOMORPHISMS OF THE COMPLEX FIELD

Sidi Mohammed BOUGHALEM

https://sithlord-dev.github.io
University François Rabelais - Tours

Let $\mathbb{C}$ be the field of complex numbers. It is well known that there are many automorphisms of the said field. Very few of them are completely characterized, while the rest show a very "wild" behaviour. We shall see in this paper an existence proof and illustrate the wildness of such mathematical objects. We will see that the construction of such automorphisms requires the use of the axiom of choice, or some equivalent assumption. Here we will be using an application of Zorn's Lemma.

Any field considered in this paper will be a subfield of $\mathbb{C}$. Any isomorphism between fields is seen as an injective ring homomorphism. Finally, let F' be a subfield of F, φ and ϕ be two isomorphisms, with domain respectively F and F'. We say that φ *extend* ϕ (to F) if $\varphi_{/F'} = \phi$ (i.e. $\varphi(x) = \phi(x) \quad \forall x \in F'$).

1 Describing automorphisms of $\mathbb{C}$

Theorem 1.1. *1. Any isomorphism between subfields of $\mathbb{C}$ extends $\mathbb{I}_{\mathbb{Q}}$.*

2. The only automorphisms of $\mathbb{C}$ which are continuous are $\mathbb{I}_{\mathbb{C}}$ and complex conjugacy.

Proof. 1. Let F and F' two subfields of $\mathbb{C}$, ϕ an isomorphism from F to F'.

- $\forall n \in \mathbb{N}$:
$$\phi_{/\mathbb{Q}}(n) = \phi_{/\mathbb{Q}}(1 + ... + 1) = \phi_{/\mathbb{Q}}(1) + ... + \phi_{/\mathbb{Q}}(1) = n$$
- $\phi_{/\mathbb{Q}}$ preserves the order : $\forall x \in \mathbb{R}$
$$x > 0 \quad \Rightarrow \quad \exists y \in \mathbb{R} \;/\; x = y^2 \;\Rightarrow\; \phi(x) = \phi(y^2) = \phi(y)^2 > 0$$
Hence, ϕ is increasing on $\mathbb{R}$. Let a,b in $\mathbb{Q}$ such that $a < b$
$$a < b \Rightarrow b - a > 0 \Rightarrow \phi(b - a) > 0 \Rightarrow \phi(b) < \phi(a)$$
- Now for all $q \in \mathbb{Q}$
$$\exists a, b, p \in \mathbb{N}, p \neq 0 \quad q = \frac{b-a}{p} \Rightarrow \phi(q) = \phi(\frac{b-a}{p}) = \frac{\phi(b) - \phi(a)}{\phi(p)} = \frac{b-a}{p} = q$$
Hence $\phi_{/\mathbb{Q}} = \mathbb{I}_{\mathbb{Q}}$

2. Let $\phi \in Aut(\mathbb{C})$, ϕ continuous. Since $\mathbb{Q}$ is dense in $\mathbb{R}$

$$\forall x \in \mathbb{R} \quad \exists (x_n)_{n\in\mathbb{N}} \subset \mathbb{Q} \quad x_n \longrightarrow x \quad \Rightarrow \quad \phi(x_n) = x_n \longrightarrow \phi(x)$$

and hence, $\phi(x) = x$ for all x in $\mathbb{R}$. We have

$$\phi(i)^2 = \phi(i^2) = \phi(-1) = -1 \quad \Rightarrow \quad \phi(i) = \pm i$$

Finally, for $z = x + iy$ in $\mathbb{C}$

$$\phi(z) = \phi(x + iy) = \phi(x) + \phi(i)\phi(y)$$

- If $\phi(i) = i$: $\phi(z) = z$ and $\phi = \mathbb{I}_{\mathbb{C}}$
- If $\phi(i) = -i$: $\phi(z) = \overline{z}$ and ϕ is complex conjugacy.

□

We shall see now that any automorphism besides those two, have a very "wild" behavior. In fact, consider ϕ such an automorphism, and choose $r \in \mathbb{R}$ such that $\phi(r) \in \mathbb{C} \setminus \mathbb{R}$. Since ϕ is the identity on $\mathbb{Q}$, ϕ fix all the rationals. Every neighbourhood of r contains rationals, hence will be left fixed by ϕ while r will be moved, thus ϕ is clearly discontinuous.
Now consider a, b in $\mathbb{Q}$, $ar + b \in \mathbb{R}$ and $\phi(\{(ar + b) \ / \ a, b \in \mathbb{Q}\}) = \{a + \phi(r)b \ / \ a, b \in \mathbb{Q}\}$.
Let $\phi(r) = x + iy$ with $x, y \in \mathbb{R}, y \neq 0$

$$\phi(\{(ar + b) \ / \ a, b \in \mathbb{Q}\}) = \{(a + yb) + i(xb) \ / \ a, b \in \mathbb{Q}\} \subset \phi(\mathbb{R})$$

With $\{(a+yb)+i(xb) \ / \ a, b \in \mathbb{Q}\}$ clearly a dense subset of $\mathbb{C}$, contained in $\phi(\mathbb{R})$. Hence $\phi(\mathbb{R})$ is a dense subset of $\mathbb{C}$.

We just saw that such automorphisms are discontinuous, fix a dense subset of $\mathbb{R}$ while mapping the whole reals to a dense subset of $\mathbb{C}$, moreover they are not even measurable.

2 Isomorphism extension

We discuss in this section, how to extend an automorphism of a subfield of $\mathbb{C}$ to one of its finitely generated extensions.

Theorem 2.1. *Let F, F' be subfields of $\mathbb{C}$, ϕ an isomorphism from F to F', α transcendental over F. Then the two assertions are equivalent :*

(a) $\exists \beta$ transcendental over F'

(b) $\exists \overline{\phi}$ extending ϕ to $F(\alpha)$ such that $\overline{\phi}(\alpha) = \beta$

Proof.
- (a) $\Rightarrow$ (b)

Consider $\phi' : F[X] \longrightarrow F'[X]$ defined as

$$\phi'(P(X) = \sum_{i=0}^{n} a_i X^i) = \sum_{i=0}^{n} \phi(a_i) X^i$$

ϕ' is well defined, and clearly a ring homomorphism, from the the properties of ϕ and operations on polynomials; with $\phi'(X) = \phi(1)X = X$ and $\phi'(\lambda) = \phi(\lambda) \quad \forall\lambda \in F$.
ϕ' is injective, in fact for

$$\phi'(\sum_{i=0}^{n} a_i X^i) = 0 \Rightarrow \sum_{i=0}^{n} \phi(a_i) X^i = 0 \Rightarrow \phi(a_i) = 0 \Rightarrow a_i = 0 \quad \forall i \in \{1, ..., n\}$$

Hence, ϕ' extend ϕ to $F[X]$.
Same way, we can define $\widetilde{\phi} : F(X) \longrightarrow F'(X)$ such that $\widetilde{\phi}(X) = X$ and $\widetilde{\phi}(\lambda) = \phi'(\lambda) = \phi(\lambda) \quad \forall\lambda \in F$.
Finally, consider the (unique) isomorphisms

$$\begin{cases} u : F(\alpha) \longrightarrow F(X) \\ u(\alpha) = X \end{cases} \qquad \text{and} \qquad \begin{cases} v : F'(\beta) \longrightarrow F'(X) \\ v(\beta) = X \end{cases}$$

We get the following diagram

$$\begin{tikzcd}
 & F(X) \arrow[r, "\widetilde{\phi}"] \arrow[d, dash] & F'(X) \arrow[d, dash] \arrow[dr, "v^{-1}"] & \\
F(\alpha) \arrow[ur, "u"] & & & F'(\beta) \\
 & F[X] \arrow[r, "\phi'"] \arrow[d, dash] & F'[X] \arrow[d, dash] & \\
 & F \arrow[r, "\phi"] & F' &
\end{tikzcd}$$

Pose $\overline{\phi} = v^{-1} \circ \widetilde{\phi} \circ u$. $\overline{\phi}$ is well defined, and clearly an isomorphism, as product of isomorphisms, with

$$\overline{\phi}(\alpha) = v^{-1} \circ \widetilde{\phi}(u(\alpha)) = v^{-1}(\widetilde{\phi}(X)) = v^{-1}(X) = \beta$$

And

$$\overline{\phi}(\lambda) = v^{-1} \circ \widetilde{\phi}(u(\lambda)) = v^{-1}(\widetilde{\phi}(\lambda)) = v^{-1}(\phi(\lambda)) = \phi(\lambda)$$

- $(b) \Rightarrow (a)$

  Now consider an isomorphism $\widetilde{\phi}$ as stated. If β is not transcendental then thre exist a polynomial P' such that $P'(\beta) = \sum_{i=0}^{n} a'_i \beta^i = 0$ and $P' \neq 0$
  But, we have

$$\overline{\phi}(\sum_{i=0}^{n} a_i \alpha^i) = \sum_{i=0}^{n} \phi(a_i)\beta^i = \sum_{i=0}^{n} a'_i \beta^i = 0 \Rightarrow \sum_{i=0}^{n} a_i \alpha^i = 0 \Rightarrow \alpha \text{ is algebraic over } F$$

  which contradict the fact that α is transcendental.

$\square$

Theorem 2.2. *Let F, F' be subfields of $\mathbb{C}$, ϕ an isomorphism from F to F', α algebraic over F. Then the two assertions are equivalent :*

(a) $\exists \beta$ *such that* $P'_\alpha(\beta) = \sum_{i=0}^{n} \phi(a_i)\beta^i = 0$*,* $(a_i)_{0 \leq i \leq n}$ *coefficient of the minimal polynomial of* α *in* F*.*

(b) $\exists \overline{\phi}$ *extending* ϕ *to* $F(\alpha)$ *such that* $\overline{\phi}(\alpha) = \beta$

Proof. The proof of this version is almost similar to the previous one as we will see

- $(a) \Rightarrow (b)$

  Consider again $\phi' : F[X] \longrightarrow F'[X]$ defined as precedant, we shall extend ϕ to ϕ' the same way we did.
  Here, since $< P_\alpha >$ is an ideal of F[X], and since P'_α is irreducible in $F[X]$, $< P'_\alpha >$ is as well an ideal of $F'[X]$. We have $\phi'(< P_\alpha >) \subseteq < P'_\alpha >$.
  We shall define $\widetilde{\phi} : F[X] \big/ < P_\alpha > \longrightarrow F'[X] \Big/ < P'_\alpha >$ such that $\widetilde{\phi}(\overline{X}) = \overline{X}$ and $\widetilde{\phi}(\lambda) = \phi'(\lambda) = \phi(\lambda) \quad \forall \lambda \in F$.
  Finally, consider (again) the (unique) isomorphisms

  $$\begin{cases} u : F(\alpha) \longrightarrow F[X] \big/ < P_\alpha > \\ u(\alpha) = \overline{X} \end{cases} \quad \text{and} \quad \begin{cases} v : F'(\beta) \longrightarrow F'[X] \Big/ < P'_\alpha > \\ v(\beta) = \overline{X} \end{cases}$$

  We get the following diagram

  $$\begin{tikzcd}
  & F[X] \big/ < P_\alpha > \arrow[r, "\widetilde{\phi}"] \arrow[d, dash] & F'[X] \Big/ < P'_\alpha > \arrow[d, dash] \arrow[dr, "v^{-1}"] & \\
  F(\alpha) \arrow[ur, "u"] & F[X] \arrow[r, "\phi'"] \arrow[d, dash] & F'[X] \arrow[d, dash] & F'(\beta) \\
  & F \arrow[r, "\phi"] & F' &
  \end{tikzcd}$$

  Pose $\overline{\phi} = v^{-1} \circ \widetilde{\phi} \circ u$. $\overline{\phi}$ is well defined, and clearly an isomorphism, as product of isomorphisms, with

  $$\overline{\phi}(\alpha) = v^{-1} \circ \widetilde{\phi}(u(\alpha)) = v^{-1}(\widetilde{\phi}(\overline{X})) = v^{-1}(\overline{X}) = \beta$$

  And

  $$\overline{\phi}(\lambda) = v^{-1} \circ \widetilde{\phi}(u(\lambda)) = v^{-1}(\widetilde{\phi}(\lambda)) = v^{-1}(\phi(\lambda)) = \phi(\lambda)$$

- $(b) \Rightarrow (a)$

  The same way, consider an isomorphism $\overline{\phi}$ as stated. Let P_α be the minimal polynomilal of α in F. we have

  $$P_\alpha(\alpha) = \sum_{i=0}^{n} a_i \alpha^i = 0 \Rightarrow \overline{\phi}(\sum_{i=0}^{n} a_i \alpha^i) = \sum_{i=0}^{n} \overline{\phi}(a_i)\beta^i = 0$$

  Hence $P'_\alpha(\beta) = 0$

$\square$

We will propose an example of extending isomorphisms over extensions of the field $\mathbb{Q}$, using this two theorems. Consider

$$\psi : \mathbb{Q}(\sqrt{5}) \longrightarrow \mathbb{Q}(\sqrt{5})$$

$\sqrt{5}$ is algebraic over $\mathbb{Q}$ with minimal polynomial

$$P'_{\sqrt{5}}(X) = X^2 - \mathbb{I}_{\mathbb{Q}}(5) = X^2 - 5.$$

$P'_{\sqrt{5}}$ has only two roots in $\mathbb{C}$, which are $\pm\sqrt{5}$. For $\beta = -\sqrt{5}$, applying Theorem 2.2 we get that ψ is an (non trivial) automorphism that fix the rationals and send $\sqrt{5}$ to $-\sqrt{5}$.

Consider now a slightly bigger extension of $\mathbb{Q}(\sqrt{5})$, let's say $\mathbb{Q}(\sqrt[4]{5})$. Here again, $\sqrt[4]{5}$ is algebraic over $\mathbb{Q}(\sqrt{5})$ with minimal polynomial $P_{\sqrt[4]{5}}(X) = X^2 - \sqrt{5}$. Considering

$$P'_{\sqrt[4]{5}}(X) = X^2 - \psi(\sqrt{5}) = X^2 + \sqrt{5}$$

$P'_{\sqrt[4]{5}}$ has the only two following roots $\pm i\sqrt[4]{5}$ in $\mathbb{C}$. Applying Theorem 2.2 again, we extend ψ to a new isomorphism

$$\widetilde{\psi} : \mathbb{Q}(\sqrt[4]{5}) \longrightarrow \mathbb{Q}(i\sqrt[4]{5})$$

that fix the rationals, send $\sqrt{5}$ to $-\sqrt{5}$ and $\sqrt[4]{5}$ to $i\sqrt[4]{5}$.

Now let's get a transcendental element over $\mathbb{Q}(\sqrt[4]{5})$, let's say e. From Theorem 2.1, we can construct a new isomorphism $\overline{\psi}$ extending $\widetilde{\psi}$ to $\mathbb{Q}(\sqrt[4]{5}, e)$ sending simply e to another transcendental element over $\mathbb{Q}(i\sqrt[4]{5})$, say $\frac{1}{1+\pi}$.

3 Zorn's Lemma and $\mathbb{C}$-Automorphism extension

We can clearly see that, by using ordinary induction and Theorem 2.1 and 2.2, we can extend any isomorphism of a subfield of $\mathbb{C}$ into an isomorphism of a finitely generated extension of that same field. Since $\mathbb{C}$ is not even a countably generated extension of $\mathbb{Q}$, we will be using Zorn's lemma to deal with the transfinite aspect of our induction.

We see in the example above, that sometimes, the only possible way to extend an automorphism to a finite extension of its domain may change its range, which does not make it an automorphism anymore. To avoid this difficulty, we will first prove the following result :

Lemma 3.1. *Let E, F be two fields, ϕ an isomorphism from E to F, then ϕ can be extended to an isomorphism from $\overline{E}$ to $\overline{F}$, the algebraic closures , respectively, of E and F.*

Proof. Let L be an intermediate field of E and $\overline{E}$, and φ an isomorphism from L to a subfield of $\overline{F}$, extending ϕ.
We consider the set $\mathcal{S}$ of all pairs (L, φ). It is non-empty since it contains (E, ϕ).
We define a partial ordering "$\leq$" on $\mathcal{S}$ such that

$$(L_1, \varphi_1) \leq (L_2, \varphi_2) \quad \Rightarrow \quad L_1 \leq L_2 \text{ and } \varphi_1(x) = \varphi_2(x) \quad \forall x \in L_1$$

It is immediate to check that this relation does give a partial ordering of $\mathcal{S}$.
Let I be an index set, $C = \{(H_i, \varphi_i), i \in I\}$ be a chain of $\mathcal{S}$ we will show that C has an upper

bound (H,φ) in $\mathcal{S}$.

Consider $H = \bigcup_{i\in I} H_i$. Since $H_i \subseteq \overline{E} \quad \forall i \in I$, $H \subseteq \overline{E}$. Let $a,b \in H$, there exist $i,i' \in I$ such that $a \in H_i$ and $b \in H_{i'}$. Since C is a chain, $H_i \leq H_{i'}$ or $H_{i'} \leq H_i$.

$$\text{If, say,}\quad H_i \leq H_{i'} \quad \Rightarrow a,b \in H_i \quad \Rightarrow a \pm b, ab, \frac{a}{b} \in H_i \subset H \quad (\text{for } b \neq 0)$$

Hence, $E \leq H \leq \overline{E}$.

Define $\varphi : H \longrightarrow \varphi(H) \leq \overline{F}$ such that for $a \in H$, $\varphi(a) = \varphi_i(a)$, $(a \in H_i)$.
φ is well defined since if $a \in H_i \cap H_{i'}$, since C is a chain, $(H_i,\varphi_i) \leq (H_{i'},\varphi_{i'})$ or $(H_{i'},\varphi_{i'}) \leq (H_i,\varphi_i)$. Either way, $\varphi_i(a) = \varphi_{i'}(a)$.

We show that φ as defined above, is an isomorphism. Let $a,b \in H$, $\exists i \in I \;/\; a,b \in H_i$ and hence $a+b, ab \in H_i$.

$$\begin{cases} \varphi(a+b) = \varphi_i(a+b) = \varphi_i(a) + \varphi_i(b) = \varphi(a) + \varphi(b) \\ \varphi(ab) = \varphi_i(ab) = \varphi_i(a)\varphi_i(b) = \varphi(a)\varphi(b) \end{cases}$$

and φ is injective, since for $a \in H$ such that $\varphi(a) = 0$; $\varphi_i(a) = 0$ and from the injectivity of the ϕ_i, $a = 0$. Therefore, φ is an isomorphism.

Thus, we can see that for every chain $C = \{(H_i,\varphi_i), i \in I\}$ of $\mathcal{S}$,

$$(H_i,\varphi_i) \leq (H,\varphi) \quad \forall i \in I$$

Every chain has an upper bound, applying Zorn's Lemma, there exists a maximal element (L_M,φ_M) of $\mathcal{S}$, which means a maximal isomorphism φ_M extending ϕ to L_M, a maximal subfield of $\overline{F}$.

Now, suppose that $L_M \subset \overline{E}$, there exists then a non zero element $\alpha \in \overline{E} \setminus L_M$. in particular, α is algebraic over E.
$\overline{F}$ is algebraically closed, every polynomial in $\overline{F}[X]$ has a root in $\overline{F}$, in particular

$$P'_\alpha(X) = \sum_{i=0}^{n} \varphi(a_i)X^i$$

call such a root β, from Theorem 2.2 there is an isomorphism $\overline{\varphi}$ extending φ_M to $L_M(\alpha)$ which contradicts the maximality of φ_M. Thus, $L_M = \overline{E}$.

Since φ_M is an isomorphism, $\varphi(\overline{E})$ is an algebraically closed subset of $\overline{F}$ containing F, which happens to be $\overline{F}$. $\square$

Now we can announce our main result :

Theorem 3.2. *Any automorphism of a subfield of $\mathbb{C}$ can be extended to an automorphism of $\mathbb{C}$.*

Proof. Let E be a subfield of $\mathbb{C}$ and ϕ an automorphism of E. We consider the same way an intermediate field L, an automorphism φ extending ϕ to L and define $\mathcal{S} = \{(L,\varphi)\}$.
Leading the same construction as in Lemma 1., it is easy to see that $\mathcal{S}$ satisfies the hypothesis of Zorn's Lemma, we just have to verify that $\varphi(H) = H$

$$b \in \varphi(H) \Rightarrow \exists i \in I, a \in H_i \quad \text{and} \quad b = \varphi(a) = \varphi_i(a) \in H_i \subseteq H \quad \Rightarrow \varphi(H) = H$$

Applying Zorn's lemma, we get φ_M the maximal automorphism extending ϕ to L_M.

Now again, suppose that $L_M \subset \mathbb{C}$, there exists a non zero complex number $z \in \mathbb{C} \setminus L_M$.
If z is algebraic over L_M, then from Lemma 3.1, we can extend φ_M into an automorphism of $\overline{L_M}$ which contradicts the maximality of φ_M. If not, then z is transcendental over L_M and Theorem 2.2 gives an extending automorphism of φ_M to $L_M(z)$ (sending z to z for example) which contradicts again the maximality of φ_M. Therefore, $L_M = \mathbb{C}$ which completes the proof. $\square$

Since there's uncountably many complex numbers which are transcendental over subfields of $\mathbb{C}$, there is uncountably many way to extend an automorphism of a subfield into one of its finitely generated extension, using Theorem 2.2; thus to automorphisms of $\mathbb{C}$ according to our last result. Back to our previous example

$$\mathbb{Q} \xrightarrow{\psi} \mathbb{Q}(\sqrt{5}) \xrightarrow{\widetilde{\psi}} \mathbb{Q}(\sqrt[4]{5}) \xrightarrow{\overline{\psi}} \mathbb{Q}(\sqrt[4]{5}, e)$$

If, instead of this construction, we extended $\mathbb{I}_{\mathbb{Q}}$ as follow

$$\mathbb{Q} \xrightarrow{\mathbb{I}_{\mathbb{Q}(\sqrt{5})}} \mathbb{Q}(\sqrt{5}) \xrightarrow{\widetilde{\psi'}} \mathbb{Q}(\sqrt[4]{5}) \xrightarrow{\overline{\psi'}} \mathbb{Q}(\sqrt[4]{5}, e)$$

with

$$\begin{cases} \widetilde{\psi'} : \mathbb{Q}(\sqrt[4]{5}) \longrightarrow \mathbb{Q}(\sqrt[4]{5}) \\ \widetilde{\psi'}(\sqrt[4]{5}) = i\sqrt[4]{5} \end{cases} \quad \text{and} \quad \begin{cases} \overline{\psi'} : \mathbb{Q}(\sqrt[4]{5}, e) \longrightarrow \mathbb{Q}(\sqrt[4]{5}, e) \\ \overline{\psi'}(e) = \frac{1}{1+e} \end{cases}$$

Applying Theorem 3.2 on $\overline{\psi'}$ we get a $\mathbb{C}$-automorphism, sending e to $\frac{1}{1+e}$, $\sqrt[4]{5}$ to $i\sqrt[4]{5}$ and fixing $\sqrt{5}$, which clearly differs from $\mathbb{I}_{\mathbb{C}}$ or complex conjugacy.

References

[1] Paul B. Yale. Automorphisms of the complex numbers, Math. Mag. 39 (1966), 135-141. (Lester R. Ford Award, 1967.)

[2] G. Birkhoff and S. Mac Lane, A Survey of Modern Algebra, 4th Edition, MacMillan, NY, 1977.

[3] Fraleigh, John B. A First Course in Abstract Algebra. Reading, Mass: Addison-Wesley Pub. Co, 1982. Print.