South American Journal of Logic
Vol. 2, n. 2, pp. 361–377, 2016
ISSN: 2446-6719

A Really Simple Proof of the Artin-Schreier Characterization of Real Closed Fields

Odilon Otávio Luciano

In honor of Chico Miraglia on his 70th birthday

Abstract

The objective of this exposition is to prove a certain kind of reciprocal assertion to the Fundamental Theorem of Algebra, which is the Artin-Schreier characterization of real closed fields, without assuming previous theorems in Galois theory. Another important feature is that the proof presented here treats in a unified way both the prime and the null characteristic case.

Keywords: Artin-Schreier, Real Closed Fields, Algebraically Closed Fields, Fundamental Theorem of Algebra.

The objective of this exposition is to prove a certain kind of reciprocal assertion to the Fundamental Theorem of Algebra, which is the Artin-Schreier characterization of real closed fields, without assuming previous theorems in Galois theory. Another important feature is that the proof presented here treats in a unified way both the prime and the null characteristic case.

More precisely, the above mentioned "reciprocal" of the following theorem is proved (here, $\sqrt{-1}$ denotes a choice of a square root of -1).

Theorem 1 (Fundamental Theorem of Algebra)**.** *If $\mathcal{F}$ is a real closed field, then $\mathcal{F}(\sqrt{-1})$ is algebraically closed.*

The "reciprocal" of Theorem 1, and Theorem 1 itself determine exhaustively the occurrence of all algebraically closed fields and real closed fields: they arise in pairs, *i.e*, for all real closed field $\mathcal{F}$, by adding $\sqrt{-1}$, one gets an algebraically closed field $\mathcal{E}$ (Theorem 1) and, reciprocally, for every proper subfield $\mathcal{F}$ of an algebraically closed

field $\mathcal{E}$ such that the extension is finite, $\mathcal{F}$ is real closed (and, therefore, $\sqrt{-1} \notin \mathcal{F}$) and one obtains $\mathcal{E}$ by adding $\sqrt{-1}$.

The proof will be divided into 7 lemmas. This article is intended to be self-contained, then no previous knowledge of field theory except the definition of a field and basic linear algebra is needed.

Definition 1. Let $\mathcal{F}$ be a field. $\mathcal{F}$ is **formally real** if for all $x_1, \ldots, x_m \in \mathcal{F}$, $\sum_i x_i^2 = 0$ implies that $x_i = 0$ for all i.

Definition 2. Let $\mathcal{F}$ be a field. $\mathcal{F}$ is **real closed** if: (i) $\mathcal{F}$ is formally real; (ii) for every $f \in \mathcal{F}[x]$ having odd degree, there exists $\zeta \in \mathcal{F}$ such that $f(\zeta) = 0$; (iii) $\mathcal{F} = \mathcal{F}^2 \cup (-\mathcal{F}^2)$, *i.e.*, for every $x \in \mathcal{F}$, there exists $y \in \mathcal{F}$ such that $x = y^2$ or $x = -y^2$.

Remark 1. In 2, it's possible to impose that $\mathcal{F}^2 + \mathcal{F}^2 = \mathcal{F}^2$ and $\mathcal{F}^2 \cap (-\mathcal{F}^2) = \{0\}$ instead of requiring that $\mathcal{F}$ is formally real.

The reciprocal of the Fundamental Theorem of Algebra, originally due to E. Artin and O. Schreier, that will be proved here is the following assertion.

Theorem 2 (Artin-Schreier Theorem)**.** *Let $\mathcal{E}$ be an algebraically closed field and $\mathcal{F} \subset \mathcal{E}$ a subfield. If $\mathcal{F} \neq \mathcal{E}$ and $\dim_{\mathcal{F}} \mathcal{E} < \aleph_0$, then $\mathcal{E} = \mathcal{F}(\sqrt{-1})$.*

Furthermore, $\mathcal{F}$ is real closed. In particular, $\mathcal{F}$ have characteristic zero.

Remark 2. The above theorem says explicitly that a proper subfield of $\mathcal{E}$ of finite dimension have exactly dimension equals 2.

Remark 3. Notice that in the above theorem, it's not asserted that given an algebraically closed field $\mathcal{E}$, there exists $\mathcal{F}$ such that $\mathcal{F}(\sqrt{-1}) = \mathcal{E}$. However, indeed, this assertion is true when the characteristic of $\mathcal{E}$ is zero. This fact is related to the order 2 automorphisms of $\mathcal{E}$ (see Theorem 3 and Theorem 4).

Furthermore, no mention to the characteristic is made in the theorem hypothesis and, also, no assumptions that the extension $\mathcal{E}/\mathcal{F}$ is Galois is required.

The proof will be divided into 7 lemmas as already mentioned above.

In what follows, it will be proved for an algebraically closed $\mathcal{E}$ that there doesn't exist proper subfields $\mathcal{G}' \subset \mathcal{E}$ for which $\sqrt{-1} \in \mathcal{G}'$ and $[\mathcal{E} : \mathcal{G}']$ is finite. Now, suppose that the previous assertion doesn't hold.

Let, therefore, $\mathcal{E}$ be an algebraically closed field, $\mathcal{G} \subset \mathcal{E}$ a proper subfield such that $\sqrt{-1} \in \mathcal{G}$ and $[\mathcal{E} : \mathcal{G}] = p$ is minimal among all $[\mathcal{E} : \mathcal{G}']$ for every proper subfield $\mathcal{G}' \subset \mathcal{E}$ containing $\sqrt{-1}$ for which $[\mathcal{E} : \mathcal{G}']$ is finite.

Lemma 1. *If $t \in \mathcal{E}$ and $t \notin \mathcal{G}$, then $\mathcal{E} = \mathcal{G}(t)$.*

Proof. Since $\mathcal{G} \subset \mathcal{G}(t) \subset \mathcal{E}$,

$$[\mathcal{E} : \mathcal{G}(t)][\mathcal{G}(t) : \mathcal{G}] = [\mathcal{E} : \mathcal{G}].$$

By the assumption $t \notin \mathcal{G}$,

$$[\mathcal{G}(t) : \mathcal{G}] > 1.$$

Hence

$$[\mathcal{E} : \mathcal{G}(t)] < [\mathcal{E} : \mathcal{G}].$$

By the minimality of p, $\mathcal{G}(t)$ cannot be proper. Therefore $\mathcal{E} = \mathcal{G}(t)$. ■

Lemma 2. *If $\theta \in \mathrm{Aut}(\mathcal{E}/\mathcal{G})$,[1] $t \in \mathcal{E}$ and $\theta(t) = t$, then $t \in \mathcal{G}$ or $\theta = 1_{\mathcal{E}}$.*[2]

Proof. By 1, if $t \notin \mathcal{G}$, then $\mathcal{E} = \mathcal{G}(t)$.

Suppose $\theta(t) = t$. Let $\alpha = f(t)$ for $f \in \mathcal{G}[X]$. Since $\theta|_{\mathcal{G}} = 1_{\mathcal{G}}$,

$$\theta(\alpha) = f(\theta(t)) = f(t) = \alpha$$

for all $\alpha \in \mathcal{E}$. Therefore $\theta = 1_{\mathcal{E}}$. ■

For every $t \in \mathcal{E}$, let $f_t \in \mathcal{G}[X]$ denotes the minimal polynomial of $t \in \mathcal{E}$. Furthermore, for every $f \in \mathcal{G}[X]$, let R_f denotes the set of f roots.

Lemma 3. *If $\theta \in \mathrm{Aut}(\mathcal{E}/\mathcal{G})$ and $\theta \neq 1_{\mathcal{E}}$, then $\theta^p = 1_{\mathcal{E}}$ e $\theta^l \neq \theta^k$ for $0 \leq l < k < p$.*

Proof. Let $t \in \mathcal{E}$ such that $t \notin \mathcal{G}$, $f_t \in \mathcal{G}[X]$ the minimal polynomial of t. Then f_t have degree p. Since $\theta(R_{f_t}) \subset R_{f_t}$,

$$\{\theta^k(t) \mid 0 \leq k \leq p\} \subset R_{f_t}.$$

Since $p + 1 > p \geq \#R_{f_t}$,[3] there exists i, j such that $0 \leq i < j \leq p$ and

$$\theta^{j-i}(t) = t.$$

Let $m = j - i \leq p$ and

$$g = \prod_{r=0}^{m-1} (X - \theta^r(t)) \in \mathcal{E}[X].$$

By $\theta^m(t) = t$,

$$g^{\theta} = \prod_{r=0}^{m-1} (X - \theta^{r+1}(t)) = g.$$

[1] $\mathrm{Aut}(\mathcal{E}/\mathcal{G}) = \{\sigma \in \mathrm{Hom}(\mathcal{E}, \mathcal{E}) \mid \sigma \text{ automorphism of } \mathcal{E} \text{ such that } \sigma|_{\mathcal{G}} = 1_{\mathcal{G}}\}$.

[2] $1_{\mathcal{E}}$ denotes the identity function on $\mathcal{E}$.

[3] $\#X$ denotes the cardinality of a set X.

Hence, by Lemma2, $g \in \mathcal{G}[X]$.

Since $g(t) = 0$ and $g \in \mathcal{G}[X]$,

$$f_t | g.$$

Hence $p \leq m$. Then $p = m$ and, therefore, by Lemma 2, $\theta^p = 1_{\mathcal{E}}$.

By assuming $\theta^k = \theta^l$ for $0 \leq l < k \leq p$, an identical argument for $i = l$ and $j = k$ implies that $k - l = p$. However, if $0 \leq l < k < p$, then $k - l < p$. Therefore $\theta^l \neq \theta^k$ whenever $0 \leq l < k < p$. ■

Lemma 4. *If* $\mathrm{Aut}(\mathcal{E}/\mathcal{G}) \neq 1$,[4] *then* p *is prime.*

Proof. Let $\theta \in \mathrm{Aut}(\mathcal{E}/\mathcal{G})$ such that $\theta \neq 1_{\mathcal{E}}$, $p = rs$ and $r > 1$. By Lemma 3,

$$1_{\mathcal{E}} = \theta^p = (\theta^r)^s.$$

Since $1 \leq s < p$, again by Lemma 3, $\theta^r = 1_{\mathcal{E}}$. Once more, by Lemma 3, $r = p$. ■

Lemma 5. *If* $t \in \mathcal{E}$ *and* $t \notin \mathcal{G}$, *then* $\#R_{f_t} = p = \#\mathrm{Aut}(\mathcal{E}/\mathcal{G})$[5].

Proof. Suppose $\#R_{f_t} = 1$. Since $\mathcal{E}$ is algebraically closed, f_t factors into linear terms in $\mathcal{E}[X]$, so

$$f_t = (X - t)^p.$$

Since $f_t(0) = (-t)^p = (-1)^p t^p \in \mathcal{G}$,

$$g = X^p - t^p \in \mathcal{G}[X].$$

By $g(t) = 0$ and $g \in \mathcal{G}[X]$, $f_t | g$ and, then, since f_t and g have the same degree and both are monic,

$$(X - t)^p = f_t = g = X^p - t^p.$$

Since $f_t = X^p - ptX^{p-1} + \cdots - t^p = X^p - t^p$, $p.t = 0$ and, hence,

$$p.1 = 0.$$

Let $p = rs$, for r and s natural numbers such that $s > 1$. Since t^s is a root of $X^r - t^p$,

$$[\mathcal{G}(t^s) : \mathcal{G}] \leq r.$$

Then, by

$$[\mathcal{E} : \mathcal{G}(t^s)][\mathcal{G}(t^s) : \mathcal{G}] = [\mathcal{E} : \mathcal{G}] = p$$

[4] 1 denotes $\{1_{\mathcal{E}}\}$.

[5] See footnote 3.

and $[\mathcal{G}(t^s) : \mathcal{G}] \leq r$,

$$[\mathcal{E} : \mathcal{G}(t^s)] \geq s > 1$$

and, hence, by Lemma 1, $t^s \in \mathcal{G}$. Hence $X^s - t^s \in \mathcal{G}[X]$ and it has t as a root. Then, $f_t | X^s - t^s$. Hence

$$s \leq rs = p \leq s$$

and, then, $s = p$. Therefore p is prime.

Let $u \in \mathcal{E}$ such that $u^p = t$. By Lemma 1 and the assumption that $t \notin \mathcal{G}$, $\mathcal{G}(t) = \mathcal{E}$. Then

$$u = u_0 + u_1 t + \cdots + u_{p-1} t^{p-1},$$

where $u_i \in \mathcal{G}$ for $0 \leq i < p$. Since $p.1 = 0$ and p is prime,

$$t = u^p = u_0^p + u_1^p t^p + \cdots + u_{p-1}^p (t^p)^{p-1} \in \mathcal{G}.$$

However $t \notin \mathcal{G}$ by assumption, an absurd. Therefore $\# R_{f_t} > 1$.

Since $\# R_{f_t} > 1$, there exists $v \in R_{f_t}$ such that $v \neq t$. Let

$$\mathcal{G}[X] \underset{ev_t}{\overset{ev_v}{\rightrightarrows}} \mathcal{E}$$

denote the homomorphisms that evaluate the polynomials on v and t respectively, i.e., $ev_v(h) = h(v)$ and $ev_t(h) = h(t)$ for each $h \in \mathcal{G}[X]$. Since $f_t(t) = f_t(v) = 0$ and f_t is irreducible, $h(t) = 0$ or $h(v) = 0$ are equivalent to $f_t | h$. Then, ev_t and ev_v induce isomorphisms

$$\mathcal{G}[X]/(f_t) \underset{\epsilon_t}{\overset{\epsilon_v}{\rightrightarrows}} \mathcal{E} \ .$$

Let $\theta = \epsilon_v (\epsilon_t)^{-1}$. Since $\theta(t) = v$, $\theta \neq 1_{\mathcal{E}}$. Then, by Lemma 3,

$$\theta^k \neq \theta^l$$

for $0 \leq l < k < p$ and, by using that $\mathcal{E} = \mathcal{G}(t)$,

$$\theta^k(t) \neq \theta^l(t)$$

for $0 \leq l < k < p$. Since $\theta(R_{f_t}) \subset R_{f_t}$,

$$\{t, \theta(t), \ldots, \theta^{p-1}(t)\} \subset R_{f_t}$$

and, then, $p \leq \# R_{f_t}$. Since f_t have degree p, $\# R_{f_t} \leq p$ and, therefore, $\# R_{f_t} = p$ and

$$R_{f_t} = \{t, \theta(t), \ldots, \theta^{p-1}(t)\}.$$

Let $\sigma \in \mathrm{Aut}(\mathcal{E}/\mathcal{G})$. Since $\sigma(R_{f_t}) \subset R_{f_t} = \{t, \theta(t), \ldots, \theta^{p-1}(t)\}$, there exists l such that $0 \leq l < p$ and $\sigma(t) = \theta^l(t)$. Then $\sigma^{-1}\theta^l(t) = t$ and, by Lemma 2, $\sigma^{-1}\theta^l = 1_{\mathcal{E}}$, *i.e.*,

$$\sigma = \theta^l.$$

Hence

$$\mathrm{Aut}(\mathcal{E}/\mathcal{G}) = \{1_{\mathcal{E}}, \theta, \ldots, \theta^{p-1}\}.$$

Therefore, since $\theta^k \neq \theta^l$ for $0 \leq l < k < p$, $\#\mathrm{Aut}(\mathcal{E}/\mathcal{G}) = p$.

■

Lemma 6.

1. *$\#R_{X^p-1} = p$ is equivalent to the existence of $\lambda \in \mathcal{E}$ such that $\lambda \neq 1$ and $\lambda^p = 1$;*
2. *For any $\lambda \in \mathcal{E}$ such that $\lambda \neq 1$ and $\lambda^p = 1$,*

$$R_{X^p-1} = \{\lambda^i |\ 0 \leq i \leq p\}.$$

Proof.

[Proof of 1] Suppose that $\lambda \in \mathcal{E}$ such that $\lambda \neq 1$ and $\lambda^p = 1$. If $\lambda^i = \lambda^j$ for $0 \leq i < j < p$, then $\lambda^q = 1$ for $q = j - i$ and $p > q \geq 1$. Since, by Lemmas 4 and 5, p is prime and, then, $aq + bp = 1$ for some integers a and b. Hence

$$\lambda = \lambda^{aq+bp} = (\lambda^q)^a(\lambda^p)^b = 1.1 = 1,$$

an absurd. Then

$$\#\{\lambda^i \mid 0 \leq i < p\} = p.$$

Since $(\lambda^i)^p = (\lambda^p)^i = 1$ for $0 \leq i < p$,

$$\{\lambda^i \mid 0 \leq i < p\} \subset R_{X^p-1}$$

and, then, $\#R_{X^p-1} \geq p$. Also, since the degree of $X^p - 1$ is equal p, $\#R_{X^p-1} \leq p$ and, therefore, $\#R_{X^p-1} = p$. As a consequence

$$R_{X^p-1} = \{\lambda^i \mid 0 \leq i < p\}.$$

Conversely, suppose $\#R_{X^p-1} = p$. Since $1 \in R_{X^p-1}$, $p > 1$, there exists $\lambda \neq 1$ such that $\lambda^p = 1$.

[Proof of 2] An identical argument to the first part of Proof of 1 also proves 2. ■

Lemma 7. $\#R_{X^p-1} = p$.

Proof. If $R_{X^p-1} < p$, by Lemma 6, $R_{X^p-1} = \{1\}$. Then, since $\mathcal{E}$ is algebraically closed,

$$X^p - 1 = (X-1)^p = X^p - pX^{p-1} + \cdots + (-1)^p$$

and, therefore, $p.1 = 0$. Let $\sigma \in \mathrm{Aut}(\mathcal{E}/\mathcal{G})$ such that $\sigma \neq 1_{\mathcal{E}}$, which exists by Lemma 5. By Lemma 3, $\sigma^p - 1_{\mathcal{E}} = 0$. Since $p.1 = 0$ and, by Lemmas 4 and 5, p is prime, then

$$0 = \sigma^p - 1_{\mathcal{E}} = (\sigma - 1_{\mathcal{E}})^p.$$

Let $\tau = \sigma - 1_{\mathcal{E}}$. Then, by the Newton binomial formula,

$$\tau^{p-1} = \sigma^{p-1} - (p-1)\sigma^{p-2} + \cdots + (p-1)\sigma(-1)^{p-2} + (-1_{\mathcal{E}})^{p-1}.$$

By Lemma 3, $\sigma^i \neq \sigma^j$ for $0 \leq i < j < p$. Then, by Dedekind Theorem (Appendix A) with

$$\Gamma = \{\sigma^l \mid 0 \leq l < p\},$$

$\{\sigma^l \mid 0 \leq l < p\}$ is linearly independent over $\mathcal{E}$ and, therefore, $\tau^{p-1} \neq 0$.

Since $\tau^{p-1} \neq 0$, there exists $t \in \mathcal{E}$ such that $\tau^{p-1}(t) \neq 0$. In view of

$$0 = \tau^p(t) = \tau\tau^{p-1}(t) = (\sigma - 1_{\mathcal{E}})\tau^{p-1}(t),$$

$\sigma(c) = c$ for $c = \tau^{p-1}(t)$. By Lemma 1 and $\sigma \neq 1_{\mathcal{E}}$, $c \in \mathcal{G}$ and, then, $\tau^{p-1}(z) = 1$ for $z = \frac{t}{c}$.

One wishes to prove that $\{z, \tau(z), \ldots, \tau^{p-1}(z)\}$ is linearly independent in $\mathcal{E}$ as a vector space over $\mathcal{G}$. Suppose there exists $c_0, \ldots, c_{p-1} \in \mathcal{G}$ such that

$$c_0 z + c_1\tau(z) + \cdots + c_{p-1}\tau^{p-1}(z) = 0$$

and $c_j \neq 0$ for some $0 \leq j < p$. Let l be the least j such that $c_j \neq 0$. Then

$$c_l t^l(z) + c_{l+1}\tau^{l+1}(z) + \cdots + c_{p-1}\tau^{p-1}(z) = 0.$$

Hence

$$c_l = c_l\tau^{p-1}(z) = \tau^{p-l-1}(c_l\tau^l(z) + c_{l+1}\tau^{l+1}(z) + \cdots + c_{p-1}\tau^{p-1}(z)) = 0,$$

a contradiction. Therefore $\{z, \tau(z), \ldots, \tau^{p-1}(z)\}$ is linearly independent over $\mathcal{G}$.

Since $\dim_{\mathcal{G}} \mathcal{E} = p$ and $\{z, \tau(z), \ldots, \tau^{p-1}(z)\}$ is linearly independent over $\mathcal{G}$, its cardinality is equals to p and, hence, $\{z, \tau(z), \ldots, \tau^{p-1}(z)\}$ is a basis for $\mathcal{E}$ over $\mathcal{G}$. Let $c_0, \ldots, c_{p-1} \in \mathcal{G}$ such that

$$z^p = c_0 z + c_1\tau(z) + \cdots + c_{p-1}\tau^{p-1}(z).$$

Since

$$\tau(x^p) = \sigma(x^p) - x^p = (\sigma(x))^p - x^p = (\sigma(x) - x)^p = (\tau(x))^p$$

for every $x \in \mathcal{E}$, $\tau^j(x^p) = (\tau^j(x))^p$ for every natural j and $x \in \mathcal{E}$. Particularly,

$$\tau^{p-1}(z^p) = (\tau^{p-1}(z))^p = 1.$$

Since $\tau^{p-1}(z^p) = c_0$,

$$z^p - z = c_1\tau(z) + \cdots + c_{p-1}\tau^{p-1} = \tau(w)$$

with $w = c_1 z + \cdots + c_{p-1}\tau^{p-2}(z)$.[6] Let $\zeta \in \mathcal{E}$ be a root of $X^p - X - w$. Since

$$(\sigma(\zeta))^p - \zeta^p = (\sigma(\zeta) - \zeta)^p,$$

$\sigma(\zeta)$ is a root of

$$X^p - X - \sigma(w)$$

and $\tau(\zeta) = \sigma(\zeta) - \zeta$ is a root of

$$X^p - X - \tau(w).$$

Similarly, $\tau(\zeta) - z$ is a root of

$$X^p - X.$$

Since the set of roots of $X^p - X$ is exactly $\mathbb{F}_p$, there exists $c \in \mathbb{F}_p$ such that $\tau(\zeta) - z = c$, equivalently,

$$\tau(\zeta) = c + z.$$

However, since $\tau(c) = 0$ and $\tau^{p-1}(z) = 1$,

$$0 = \tau^{p-1}(\tau(\zeta)) = \tau^{p-1}(c + z) = 1,$$

an absurd.

Therefore, $\#R_{X^p-1} = p$.

■

Remark 4. Notice that Lemma 7 is trivial in characteristic 0 since every extension is separable and $\mathcal{E}$ is algebraically closed. The result, of course, is not trivial in positive characteristic as the above proof shows.

Now we are ready to provide a proof of the main Theorem

Proof. (Artin-Schreier Theorem) Let $\sigma \in \mathrm{Aut}(\mathcal{E}/\mathcal{F})$ such that $\sigma \neq 1_{\mathcal{E}}$ and $\sigma^p = 1_{\mathcal{E}}$, which exists by Lemmas 4 and 5. Let $\lambda \in \mathcal{E}$ such that $\lambda \neq 1$ and $\lambda^p = 1$, which exists by Lemmas 6 and 7. Since $\lambda \neq 1$, $\lambda^p = 1$ and $(\lambda - 1)(\lambda^{p-1} + \cdots + \lambda + 1) = \lambda^p - 1 = 0$,

$$\lambda^{p-1} + \cdots + \lambda + 1 = 0,$$

[6] If $p = 2$, $w = 0$

equivalently, λ is root of the polynomial

$$X^{p-1} + \cdots + X + 1 \in \mathcal{G}[X]$$

and, hence, $[\mathcal{G}(\lambda) : \mathcal{G}] < p$. By

$$[\mathcal{E} : \mathcal{G}(\lambda)][\mathcal{G}(\lambda) : \mathcal{G}] = p$$

and $[\mathcal{G}(\lambda) : \mathcal{G}] < p$, $[\mathcal{E} : \mathcal{G}(\lambda)] > 1$ and, then, by Lemma 1, $\lambda \in \mathcal{G}$. Let $\varphi = \sigma^{p-1} + \cdots + \lambda^i\sigma^{p-i-1} + \cdots + \lambda^p 1_{\mathcal{E}}$. Hence, by Theorem 5, $\varphi \neq 0$ since the coefficients $1, \lambda, \ldots, \lambda^i, \ldots, \lambda^{p-1}$ are nonzero. Let $t \in \mathcal{E}$ such that $\varphi(t) = u \neq 0$. Since $\lambda \in \mathcal{G}$, $\sigma(\lambda) = \lambda$. Then $\sigma(\lambda 1_{\mathcal{E}}) = (\lambda 1_{\mathcal{E}})\sigma$ and, hence,

$$0 = \sigma^p - (\lambda 1_{\mathcal{E}})^p = (\sigma - \lambda 1_{\mathcal{E}})(\sigma^{p-1} + \cdots + \lambda^j\sigma^{p-j-1} + \cdots + \lambda^p 1_{\mathcal{E}}) = (\sigma - \lambda 1_{\mathcal{E}})\varphi.$$

Then $(\sigma - \lambda 1_{\mathcal{E}})u = 0$, *i.e.*, $\sigma(u) = \lambda u$.

Let $v \in \mathcal{E}$ be a root of $X^p - u$ and $\xi = \frac{\sigma(v)}{v}$. Then

$$\xi^p = \frac{\sigma(v^p)}{v^p} = \frac{\sigma(u)}{u} = \lambda$$

and, since $\lambda \in \mathcal{G}$

$$\left(\frac{\sigma(\xi)}{\xi}\right)^p = \frac{\sigma(\xi^p)}{\xi^p} = \frac{\sigma(\lambda)}{\lambda} = 1.$$

Hence there exists i such that $0 \leq i < p$ and

$$\frac{\sigma(\xi)}{\xi} = \lambda^i.$$

Suppose that p is odd, *i.e.*, $p = 2q + 1$ for some natural q. Then

$$v = \sigma^p(v) = \sigma^{p-1}(\sigma(v)) = \sigma^{p-1}(\xi v) = \sigma^{p-2}(\sigma(\xi)\sigma(v)) = \sigma^{p-2}(\lambda^i\xi\xi v) =$$

$$= \lambda^i\sigma^{p-2}(\xi^2 v) = \ldots = \lambda^{i+\cdots+ki}\sigma^{p-(k+1)}(\xi^{k+1}v) = \ldots = \lambda^{i+\cdots+(p-1)i}\xi^p v = \lambda v$$

since

$$i + \cdots + (p-1)i = i(1 + \cdots + (p-1)) = ipq,$$

$\lambda^{ipq} = (\lambda^p)^{iq} = 1$ and $\xi^p = \lambda$. Hence $v = \lambda v$ and $v \neq 0$ implies that $\lambda = 1$. Then p cannot be odd and, therefore $p = 2$. In this case, $\xi^2 = \lambda = -1$ since $\lambda \neq 1$, $\lambda^2 = 1$ and $\lambda^2 - 1 = (\lambda + 1)(\lambda - 1)$. Then, by the assumption that $\sqrt{-1} \in \mathcal{G}$, $\xi \in \mathcal{G}$. Hence

$$v = \sigma^2(v) = \sigma(\sigma(v)) = \sigma(\xi v) = \sigma(\xi)\sigma(v) = \xi\xi v = \lambda v,$$

where the last equality follows from $\sigma(\xi) = \xi$. Then $\lambda = 1$ or $v = 0$. However, by assumption, $\lambda \neq 1$ and $v \neq 0$, an absurd. Therefore there are no proper subfields $\mathcal{G}'$ of $\mathcal{E}$ such that $[\mathcal{E} : \mathcal{G}'] < \aleph_0$ and $\sqrt{-1} \in \mathcal{G}'$.

Let $\mathcal{F}$ be a proper subfield of $\mathcal{E}$ such that $[\mathcal{E} : \mathcal{F}] < \aleph_0$. Since

$$[\mathcal{E} : \mathcal{F}(\sqrt{-1})][\mathcal{F}(\sqrt{-1}) : \mathcal{F}] = [\mathcal{E} : \mathcal{F}]$$

and $\sqrt{-1} \notin \mathcal{F}$,

$$[\mathcal{E} : \mathcal{F}(\sqrt{-1})] < [\mathcal{E} : \mathcal{F}] < \aleph_0$$

and, therefore, $\mathcal{E} = \mathcal{F}(\sqrt{-1})$.

Now, to conclude the proof of Theorem 2, we will regard its latter statement, concerning real closedness.

For every $t \in \mathcal{E}$, there exists uniques $x, y \in \mathcal{F}$ such that $t = x + \sqrt{-1}y$. Let $a, b \in \mathcal{F}$. Since $\mathcal{E}$ is algebraically closed, there exists $c, d \in \mathcal{F}$ such that

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

Then $a = c^2 - d^2$ and $b = 2cd$ and, hence

$$a^2 + b^2 = (c^2 - d^2)^2 + (2cd)^2 = (c^2 + d^2)^2 = e^2$$

for $e = c^2 + d^2$. More generally by induction, for every $x_1, \ldots, x_n \in \mathcal{F}$, there exists $y \in \mathcal{F}$ such that $x_1^2 + \cdots + x_n^2 = y^2$. Let $a^2 + x_1^2 + \cdots + x_n^2 = 0$. Since, $x_1^2 + \cdots + x_n^2 = y^2$ for some $y \in \mathcal{F}$,

$$0 = a^2 + y^2 = (a + y\sqrt{-1})(a - y\sqrt{-1})$$

and, then, $a + y\sqrt{-1} = 0$ or $a - y\sqrt{-1} = 0$. Hence $a = y = 0$ and, consequently, $x_1^2 + \cdots + x_n^2 = 0$. Proceeding by induction, $a = x_1 = \ldots = x_n = 0$. Therefore $\mathcal{F}$ is formally real.

Let $a \in \mathcal{F}$ and $b = 0$, by the equality

$$a + b\sqrt{-1} = c^2 - d^2 + 2cd\sqrt{-1}$$

for c and d as before, $2cd = 0$. Then, if $c = 0$, $a = -d^2$ and , if $d = 0$, $a = c^2$. Hence

$$\mathcal{F} = \mathcal{F}^2 \cup (-\mathcal{F}^2).$$

If $f \in \mathcal{F}[X]$ have odd degree, then there exists $g \in \mathcal{F}[X]$ irreducible, of odd degree, such that $g|f$, since the degree of f is the sum of the degrees of the polynomials appearing in a factorization of f in irreducible factors. Let $t \in \mathcal{E}$ such that $g(t) = 0$. Since

$$[\mathcal{E} : \mathcal{F}(t)][\mathcal{F}(t) : \mathcal{F}] = [\mathcal{E} : \mathcal{F}] = 2$$

and $\deg(g) = [\mathcal{F}(t) : \mathcal{F}]$ is odd, $[\mathcal{F}(t) : \mathcal{F}] = 1$ and, then, $t \in \mathcal{F}$, which is a root of f. Therefore $\mathcal{F}$ is real closed.

Therefore $\mathcal{F}$ is real closed and $\mathcal{E} = \mathcal{F}(\sqrt{-1})$

■

By the absence of any mention to the characteristic of $\mathcal{E}$ in the hypotheses of Artin-Schreier Theorem, it follows the corollary.

Corollary 1. *Let $\mathcal{E}$ be algebraically closed of characteristic $p > 0$. For any proper subfield $\mathcal{F} \subset \mathcal{E}$, the extension $\mathcal{E}/\mathcal{F}$ is infinite.*

Corollary 2. *Let $\mathcal{E}$ be algebraically closed. If $G < \mathrm{Aut}(\mathcal{E})$ has finite order and $G \neq 1$, then G have order 2.*

Proof. By Proposition B.1 (Appendix B), $[\mathcal{E} : \mathcal{E}^G] = |G| < \aleph_0$. By Artin-Schreier Theorem (Theorem 2) and the fact that $\mathcal{E}^G \neq \mathcal{E}$, $|G| = [\mathcal{E} : \mathcal{E}^G] = 2$. ■

In particular, this stablishes a surprising fact about the absolute Galois group $G_{\mathbb{Q}}$, which is the main source of problems in arithmetic geometry.

Corollary 3. *Let $\sigma \in G_{\mathbb{Q}}$ be such that $\sigma \neq 1$ and σ has finite order, then σ has order 2 and satisfies $\sigma(\sqrt{-1}) = -\sqrt{-1}$.*

Proof. Consider the subgroup $\langle\sigma\rangle < \mathrm{Aut}(\mathcal{E})$ generated by σ and use Corollary 2 and Theorem 2 applied to the subfield $\mathcal{E}^\sigma < \mathcal{E}$, consisting of the fixed elements of σ. ■

The article now ends with the proof of the existence of $\mathcal{F}$ (as stated in Remark 3) and the existence of a bijective correspondence between real closed fields and involutions.

Theorem 3. *For every algebraically closed field $\mathcal{E}$ of characteristic zero, there exists a subfield $\mathcal{F}$ such that $\mathcal{F}(\sqrt{-1}) = \mathcal{E}$. Furthermore any such $\mathcal{F}$ is real closed.*

Proof. [Sketch] Let $\mathscr{R}$ the set of all formally real subfields of $\mathcal{E}$ partially ordered by inclusion. For any chain $\mathscr{S} \subset \mathscr{R}$, $\bigcup \mathscr{S}$ is the maximum of $\mathscr{S}$ and, then, by Zorn's Lemma, there exists a maximal element in $\mathscr{R}$, say $\mathcal{F}$.

For any $a \in \mathcal{F}$, $\alpha \in \mathcal{E}$ and $\beta \in \mathcal{E}$ such that $\alpha^2 = a$, and $\beta^2 = -a$, $\mathcal{F}(\alpha)$ or $\mathcal{F}(\beta)$ is formally real. Hence, by the maximality of $\mathcal{F}$, $\alpha \in \mathcal{F}$ or $\beta \in F$. It follows, then, that $\mathcal{F} = \mathcal{F}^2 \cup (-\mathcal{F}^2)$.

Let $p \in \mathcal{F}[X]$ be of odd degree. Since the degree of p is the sum of the degrees of of the irreducible factors of a decomposition of p in $\mathcal{F}[X]$, there is $q|p$ irreducible over $\mathcal{F}[X]$ of odd degree such that $q \in \mathcal{F}[X]$. If $\zeta \in \mathcal{E}$ be a root of q, then $\mathcal{F}(\zeta)$ is again formally real. Hence $\zeta \in \mathcal{F}$. Therefore $\mathcal{F}$ is real closed.

By the Fundamental Theorem of Algebra, $\mathcal{F}(\sqrt{-1})$ is algebraically closed.

Notice that no element $\tau \in \mathcal{E}$ can be transcendent over $\mathcal{F}$, otherwise $\mathcal{F}(\tau)$ would be a proper formally real extension of $\mathcal{F}$. The extension $\mathcal{E}/\mathcal{F}$, then, is algebraic and, as a consequence, also the extension $\mathcal{E}/\mathcal{F}(\sqrt{-1})$. Hence any $\zeta \in \mathcal{E}$ is a root of a non-constant polynomial $p \in \mathcal{F}(\sqrt{-1})[X]$. Since $\mathcal{F}(\sqrt{-1})$ is algebraically closed, p decomposes in $\mathcal{F}(\sqrt{-1})$ into linear factors. Then $\zeta \in \mathcal{F}(\sqrt{-1})$. Therefore $\mathcal{E} = \mathcal{F}(\sqrt{-1})$.

The argument developed above in the proof of the Artin-Schreier Theorem presented after Remark 4 can be applied in the same way to conclude that for any proper subfield $\mathcal{F} < \mathcal{E}$ such that $\mathcal{E} = \mathcal{F}(\sqrt{-1})$, $\mathcal{F}$ is real closed. ■

Remark 5. The claims in the above proof sketch concerning extensions of formally real fields by adjoining to $\mathcal{F}$ square roots of elements of $\mathcal{F}$, roots of odd degree irreducible polynomials in $\mathcal{F}[X]$ or transcendent elements over $\mathcal{F}$ are of an elementary character, and are accessible to any beginner student in the subject.

Remark 6. The last reasoning in the above proof sketch (which refers to the argument used in the proof of the Artin-Schreier Theorem presented after Remark 4) indicates that to find a proper subfield $\mathcal{F} < \mathcal{E}$ such that $\mathcal{E} = \mathcal{F}(\sqrt{-1})$, one must consider at least the formally real subfields of $\mathcal{E}$.

For this reason, $\mathscr{R}$ and Zorn's lemma are used. Using only elementary properties of formally real subfields, the maximal in $\mathscr{R}$ turns out to the real closed. The real closedness, then, guarentees the conditions to apply the Fundamental Theorem of Algebra to get the desired result, which is the claim of existence.

Symmetrically, when one already has, hypothetically, a proper subfield $\mathcal{F}$ such that $\mathcal{E} = \mathcal{F}(\sqrt{-1})$, $\mathcal{F}$ is real closed as mentioned in the end of the above proof sketch.

Remark 7. The last reasoning in the above proof sketch also applies to the statement of Theorem 4. In this context, it implies that all elements of $\mathscr{R}_{\mathcal{E}}$ are real closed.

Theorem 4. *Let $\mathcal{E}$ be an algebraically closed field of characteristic zero. Let $\mathscr{R}_{\mathcal{E}}$, $\mathscr{L}_{\mathcal{E}}$ be, respectively, the set of all proper subfields $\mathcal{F}$, such that $\mathcal{E} = \mathcal{F}(\sqrt{-1})$, and the set of involutions*[7] *of E. The set*

$$\Theta = \{(\mathcal{F}, \sigma) \mid ((\mathcal{F}, \sigma) \in \mathscr{R}_{\mathcal{E}} \times \mathscr{L}_{\mathcal{E}}) \wedge (\mathcal{E}^{\sigma} = \mathcal{F})\}$$

is a bijection

$$\Theta : \mathscr{R}_{\mathcal{E}} \xrightarrow{\sim} \mathscr{L}_{\mathcal{E}}.$$

Proof. Let $\mathcal{F} \in \mathscr{R}_{\mathcal{E}}$. If $\zeta \in \mathcal{E}$, then there exists only one pair $(x, y) \in \mathcal{F} \times \mathcal{F}$ such that $\zeta = x + y\sqrt{-1}$. Let $\mathcal{E} \xrightarrow{\sigma} \mathcal{E}$ be the morphism determined by $\sigma(\zeta) = x - y\sqrt{-1}$. Notice that $\sigma \in \mathscr{L}_{\mathcal{E}}$ and $\mathcal{E}^{\sigma} = \mathcal{F}$. Therefore $\mathrm{dom}(\Theta) = \mathscr{R}_{\mathcal{E}}$.

[7] Let $\mathcal{F}$ be a field. $\sigma \in \mathrm{Aut}(\mathcal{F})$ is an involution of $\mathcal{F}$ iff $\sigma^2 = 1_{\mathcal{F}}$.

Suppose $(\mathcal{F},\sigma),(\mathcal{F}',\sigma')\in\Theta$. Since $\sigma,\sigma'\neq 1_{\mathcal{E}}$, $\sigma(\sqrt{1})=-\sqrt{-1}=\sigma'(\sqrt{1})$. Then, for every $\zeta=x+y\sqrt{-1}$ such that $(x,y)\in\mathcal{F}\times\mathcal{F}$,

$$\sigma(\zeta)=\sigma(x)+\sigma(y)\sigma(\sqrt{-1})=x-y\sqrt{-1}=\sigma'(x)+\sigma'(y)\sigma'(\sqrt{-1})=\sigma'(\zeta)$$

by the fact that $\mathcal{E}^{\sigma}=\mathcal{F}=\mathcal{E}^{\sigma'}$ Therefore Θ is a function.

If $(\mathcal{F},\sigma),(\mathcal{F}',\sigma')\in\Theta$, then $\mathcal{F}=\mathcal{E}^{\sigma}=\mathcal{F}'$. Therefore Θ is injective.

Let $\sigma\in\mathscr{L}_{\mathcal{E}}$ such that $\mathcal{F}=\mathcal{E}^{\sigma}<\mathcal{E}$ is a proper subfield. Let $\zeta\in\mathcal{E}$ such that $\sigma(\zeta)\neq\zeta$, and $\xi\in\mathcal{E}$ such that $\xi^2=\zeta-\sigma(\zeta)$. Then

$$\Big(\frac{\sigma(\xi)}{\xi}\Big)^2=\frac{\sigma(\xi^2)}{\xi^2}=\frac{\sigma(\zeta-\sigma(\zeta))}{\zeta-\sigma(\zeta)}=\frac{\sigma(\zeta)-\zeta}{\zeta-\sigma(\zeta)}=-1$$

and

$$\sigma\Big(\frac{\sigma(\xi)}{\xi}\Big)=\frac{\xi}{\sigma(\xi)}=-\frac{\sigma(\xi)}{\xi}.$$

Hence $\sigma(\sqrt{-1})=-\sqrt{-1}$. Let $\lambda\in\mathcal{E}$, $\lambda=x+y\sqrt{-1}$,

$$x=\frac{\lambda+\sigma(\lambda)}{2}$$

and

$$y=\frac{\lambda-\sigma(\lambda)}{2\sqrt{-1}}.$$

Then $x,y\in\mathcal{F}$ and, finally, $\mathcal{E}=\mathcal{F}(\sqrt{-1})$. Then Θ is surjective and, therefore, it's a bijection. ■

Appendices

A Dedekind Theorem

Theorem 5 (Dedekind Theorem)**.** *Let $\mathcal{E}$ and $\mathcal{F}$ be fields, and $\Gamma\subset\mathrm{Aut}(\mathcal{E}/\mathcal{F})$. Γ is linearly independent over $\mathcal{E}$.*

Proof. Suppose that

$$c_1\gamma_1+\cdots+c_n\gamma_n=0$$

for $\gamma_i\neq\gamma_j$, $1\leq i<j<n$, $\gamma_i\in\Gamma$, $c_j\in\mathcal{E}$, $c_j\neq 0$ for some j and n minimal under these conditions. Then $n>1$ and $c_i\neq 0$ for every $0\leq i\leq n$. Let $x\in\mathcal{E}$ such that $\gamma_1(x)\neq\gamma_n(x)$. Then

$$0=c_1\gamma_1(x)\gamma(y)+\cdots+c_n\gamma_n(x)\gamma_n(y)$$

for every $y \in \mathcal{E}$. Hence

$$0 = c_1(\gamma_1(x) - \gamma_n(x))\gamma_1(y) + \cdots + c_{n-1}(\gamma_{n-1}(x) - \gamma_n(x))\gamma_{n-1}(y)$$

for all $y \in \mathcal{E}$, *i.e.*,

$$0 = c_1(\gamma_1(x) - \gamma_n(x))\gamma_1 + \cdots + c_{n-1}(\gamma_{n-1}(x) - \gamma_n(x))\gamma_{n-1}$$

which contradicts the minimality of n since $c_1(\gamma_1(x) - \gamma_n(x)) \neq 0$. ■

B $\quad [\mathcal{E} : \mathcal{E}^G] = |G|$

Lemma 8. *Let $\mathcal{E}$ be a field, $S \subset \mathrm{Aut}(\mathcal{E})$ finite subset and Γ a generator of $\mathcal{E}$ as a vector space over $\mathcal{E}^S$.*[8] *Then $\#\Gamma \geq \#S$.*

Proof. Suppose that $\#\Gamma < \#S$. Let

$$\Gamma \to \mathscr{F}(S, \mathcal{E})^* \quad [9]$$

be given by $\gamma \mapsto f_\gamma$ where $f_\gamma(\alpha) = \sum_{g \in S} g(\gamma)\alpha(g)$. Since

$$\#\{f_\gamma |\ \gamma \in \Gamma\} \leq \#\Gamma < \#S = \dim_{\mathcal{E}}(\mathscr{F}(S, \mathcal{E})),$$

$\bigcap_{\gamma \in \Gamma} \mathrm{Ker}(f_\gamma) \neq 0$. In other words, a linear system with more variables than equations has a nonzero solution. Then there exists $\alpha : S \to \mathcal{E}$ such that $\alpha \neq 0$ and

$$\sum_{g \in S} g(\gamma)\alpha(g) = 0$$

for every $\gamma \in \Gamma$. By the fact that Γ generates $\mathcal{E}$ over $\mathcal{E}^S$, for every $\xi \in \mathcal{E}$, there exists $\lambda : \Gamma \to \mathcal{E}^S$ such that

$$\xi = \sum_{\gamma \in \Gamma} \lambda(\gamma)\gamma.$$

Then

$$0 = \sum_{\gamma \in \Gamma}(\lambda(\gamma) \sum_{g \in S} g(\gamma)\alpha(g)) = \sum_{g \in S}(\alpha(g) \sum_{\gamma \in \Gamma} \lambda(\gamma)g(\gamma)) = \sum_{g \in S}(\alpha(g) \sum_{\gamma \in \Gamma} g(\lambda(\gamma)\gamma)) =$$

[8] Let $\mathcal{F}$ be a field and S be a subset of $\mathrm{Aut}(\mathcal{F})$. $\mathcal{F}^S$ denotes the subset of $\mathcal{F}$ fixed by all elements of S.

[9] (i) Let S be a set and $\mathcal{F}$ a field. $\mathscr{F}(S, \mathcal{F})$ denotes the $\mathcal{F}$-vector space of functions from S to $\mathcal{F}$;
(ii) Let $\mathcal{F}$ be a field and V a $\mathcal{F}$-vector space. $V^* = \mathrm{Hom}_{\mathcal{F}}(V, \mathcal{F})$ denotes the dual vector space, *i.e.*, the vector space of $\mathcal{F}$ linear homomorphisms.

$$= \sum_{g\in S}(\alpha(g)g(\sum_{\gamma\in\Gamma}\lambda(\gamma)\gamma)) = \sum_{g\in S}\alpha(g)g(\xi) = (\sum_{g\in S}\alpha(g)g)(\xi)$$

for every $\xi \in \mathcal{E}$. Hence $\sum_{g\in S}\alpha(g)g = 0$. By Dedekind Theorem (Appendix A) for $\Gamma = S$, $\alpha(g) = 0$ for all $g \in S$, an absurd since $\alpha \neq 0$. Therefore $\#\Gamma \geq \#S$. ■

Lemma 9. *Let $\mathcal{E}$ be a field, $G < \mathrm{Aut}(\mathcal{E})$ a finite subgroup and $\mathcal{L}$ a linearly independent subset of $\mathcal{E}$ as a vector space over $\mathcal{E}^G$. Then $\#\mathcal{L} \leq \#G$.*

Proof. Suppose that $\#G < \#\mathcal{L}$. One can choose a finite subset of $\mathcal{L}$ with cardinality greater than G. For this reason, $\mathcal{L}$ will denote such subset from now on. Let

$$G \to \mathscr{F}(\mathcal{L}, \mathcal{E})^* \quad [10]$$

be given by $g \mapsto \varphi_g$ where $\varphi_g(\beta) = \sum_{\xi\in\mathcal{L}} g(\xi)\beta(\xi)$. Since

$$\#\{\varphi_g |\ g \in G\} \leq \#G < \#\mathcal{L} = \dim_{\mathcal{E}}(\mathscr{F}(\mathcal{L}, \mathcal{E})),$$

$\bigcap_{g\in G}\mathrm{Ker}(\varphi_g) \neq 0$. Then there exists $\beta : \mathcal{L} \to \mathcal{E}$ such that $\beta \neq 0$ and

$$\sum_{\xi\in\mathcal{L}} g(\xi)\beta(\xi) = 0$$

for every $g \in G$.

Consider $\beta \neq 0$ as above such that $T = \{\xi \in \mathcal{L} \mid \beta(\xi) \neq 0\}$ has minimal cardinality. Then

$$0 = h(\sum_{\xi\in T} g(\xi)\beta(\xi)) = \sum_{\xi\in T} h(g(\xi)\beta(\xi)) = \sum_{\xi\in T} hg(\xi)h(\beta(\xi))$$

for every $g, h \in G$. Hence, since $hG = G$ for every $h \in G$,

$$\sum_{\xi\in T} g(\xi)h(\beta(\xi)) = 0$$

for every $g, h \in G$.

Since $\beta \neq 0$, $\#T \geq 1$. If $\#T = 1$, then $g(T) = \{0\}$ for every $g \in G$. Hence $T = \{0\}$, an absurd since $T \subset \mathcal{L}$ is linearly independent over $\mathcal{E}^G$.

Suppose $\#T \geq 2$. Let $\zeta \in T$. Since

$$\sum_{\xi\in\mathcal{L}} g(\xi)h(\beta(\xi))\beta(\zeta) = 0$$

[10] See footnote 9.

and

$$\sum_{\xi\in\mathcal{L}} g(\xi)\beta(\xi)h(\beta(\zeta)) = 0$$

for every $g, h \in G$,

$$\sum_{\xi\in T\setminus\{\zeta\}} g(\xi)(h(\beta(\xi))\beta(\zeta) - h(\beta(\zeta))\beta(\xi)) = 0$$

for every $g, h \in G$. By the minimality of T as mentioned above,

$$h(\beta(\xi))\beta(\zeta) - h(\beta(\zeta))\beta(\xi) = 0$$

for every $h \in G$ and $\xi \in T$. Since $\beta(\zeta) \neq 0$,

$$h\Big(\frac{\beta(\xi)}{\beta(\zeta)}\Big) = \frac{\beta(\xi)}{\beta(\zeta)}$$

and, therefore, $\lambda_\xi = \frac{\beta(\xi)}{\beta(\zeta)} \in \mathcal{E}^G$, for every $h \in G$ and $\xi \in T$. Since $\beta(\xi) = \lambda_\xi\beta(\zeta)$,

$$\beta(\zeta)g(\zeta) + \sum_{\xi\in T\setminus\{\zeta\}} \lambda_\xi\beta(\zeta)g(\xi) = 0$$

for every $g \in G$. Setting $g = 1_\mathcal{E}$,

$$\zeta = -\sum_{\xi\in T\setminus\{\zeta\}} \lambda_\xi\xi$$

and, then, $T \subset \mathcal{L}$ is not linearly independent over $\mathcal{E}^G$, an absurd. Therefore $\#\mathcal{L} \leq \#G$. ■

Proposition B.1. *Let $\mathcal{E}$ be a field and $G < \mathrm{Aut}(\mathcal{E}/\mathcal{E}^G)$ a finite subgroup. Then $[\mathcal{E} : \mathcal{E}^G] = |G|$.*

Proof. By Lemma 9, every subset of $S \subset \mathcal{E}$ linearly independent over $\mathcal{E}^G$ has at most $\#G$ elements. Let T be a maximal subset of $\mathcal{E}$ among all subsets of $\mathcal{E}$ that are linearly independent over $\mathcal{E}^G$. By a standard argument, T generates $\mathcal{E}$ over $\mathcal{E}^G$, then it is a basis of $\mathcal{E}$ over $\mathcal{E}^G$. By Lemma 8, $\#T \geq \#G$. Therefore T has exactly $\#G$ elements. ■

References

[1] E. Artin and O. Schreier. Eine kennzeichnngen des körpers der reellen algebraischen zahlen. *Abh. Math. Sem. Hamb. Univ.*, 3:319–323, 1924.

[2] E. Artin and O. Schreier. Algebraische konstruktion reeller körper. *Abh. Math. Sem. Hamb. Univ.*, 5:85–99, 1927.

[3] E. Artin and O. Schreier. Eine kennzeichnung der reell abgeschlossenen körper. *Abh. Math. Sem. Hamb. Univ.*, 5:225–231, 1927.

[4] R. Baer. Die automorphismengruppen eines algebraisch abgeschlossenen körpers der characteristik 0. *Math.Zeitschrift*, 117(7-17), 1970.

[5] M. A. Dickmann. Applications of model theory to real algebraic geometry. In Carlos Augusto Di Prisco, editor, *Methods in Mathematical Logic. Proceedings of the 6th Latin American Symposium on Mathematical Logic held in Caracas, Venezuela August 1–6, 1983*, volume 1130 of *Lect.Notes in Math. 1130*, chapter 5. Springer, Caracas, 1985.

[6] J. Dieudonné. Sur les automorphismes des corps algébriquement clos. *Boletim da Sociedade Brasileira de Matemática*, 5(2):123–126, 1974.

[7] B. Jacob. The model theory of generalized real closed fields. *J. für Reine und Angewandt Mathematik*, 323:213–220, 1981.

[8] N. Jacobson. *Lectures on Abstract Algebra – vol.III – Theory of Fields and Galois Theory.* Van Nostrand, N.J., 1964.

[9] N. Jacobson. *Basic Algebra II.* Dover, 2 edition, 1989.

[10] S. Lang. *Algebra.* Springer-Verlag, New York, 3 edition, 2002.

[11] D. Marker, M. Messmer, and A. Pillay. *Model theory of fields*, volume 5 of *Lect. Notes on Logic.* Springer-Verlag, La Jolla, CA, USA, 1996.

Odilon Otávio Luciano
Department of Mathematics
Instituto de Matemática e Estatística (IME-USP)
University of São Paulo (USP)
Rua do Matão, 1010, Butantã, CEP 05508-090, São Paulo, SP, Brazil
E-mail: odilon.luciano@gmail.com