THE ARTIN-SCHREIER THEOREM

JAMES TAYLOR

1. The Theorem

We aim to prove the following theorem. We follow the notes by Keith Conrad.

Theorem 1.1 (Artin-Schreier). *Suppose that F is a field with $0 < [\overline{F} \colon F] < \infty$. Then:*

(1) $\overline{F} = F(i)$, *for* $i \in \overline{F}$ *with* $i^2 = -1$,
(2) *For any* $a \in F^\times$, *exactly one of* a *and* $-a$ *is a square in* F, *and every finite non-empty sum of non-zero squares is again a non-zero square in* F.

In particular, F *has a unique structure as an ordered field with set of positive elements*

$$\mathbb{P} \coloneqq \{a^2 \mid a \in F^\times\},$$

and therefore, F *has characteristic* 0.

Let's recall some of the notions involved the statement.

Definition 1.2. An order on a field is a subset $\mathbb{P} \subset F$ is a set of *positive elements*:

(1) $F = -\mathbb{P} \sqcup \{0\} \sqcup \mathbb{P}$,
(2) $\mathbb{P}$ is closed under addition and multiplication.

Remark 1.3. This is equivalent to giving a strict total order $<$ on F such that

- $a < b \Rightarrow a + c < b + c$,
- $a < b \Rightarrow ad < bd$,

for any $a, b, c, d \in F$ with $d > 0$.

Lemma 1.4. *Suppose that* $\mathbb{P}$ *is a set of positive elements in some field* F. *Then:*

$$\{a^2 \mid a \in F^\times\} \subset \mathbb{P},$$

and F *has characteristic* 0.

Proof. Suppose that $a \in F^\times$. Then either a or $-a$ is in $\mathbb{P}$. So $a^2 = (-a)^2 \in \mathbb{P}$. Now $1^2 = 1$ is positive, and $\mathbb{P}$ is closed under addition and doesn't contain 0, so F has characteristic 0. ☐

Note that $1 = 1^2$ is always positive, and therefore -1 is never positive. In particular, for $F(i)/F$ as in the main theorem, $F(i)/F$ will not admit a set of positive elements: fields which admit such a set of positive elements are often called *formally real*, and if they admit no totally real algebraic extension, *real closed*. In fact, one can show that being formally real is equivalent to -1 being a sum of squares. Note that a set of positive elements for a field need not be unique in general.

What we will actually prove is the following theorem.

Theorem 1.5 (Strong Artin-Schreier). *Suppose that F is a field with $0 < [F^{\text{sep}} \colon F] < \infty$. Then:*

(1) $\overline{F} = F(i)$, *for* $i \in \overline{F}$ *with* $i^2 = -1$,
(2) *For any* $a \in F^\times$, *exactly one of* a *and* $-a$ *is a square in* F, *and every finite non-empty sum of non-zero squares is again a non-zero square in* F.

In particular, F *has a unique structure as an ordered field with set of positive elements*

$$\mathbb{P} \coloneqq \{a^2 \mid a \in F^\times\},$$

and therefore, F *has characteristic* 0.

Date: January 26, 2024.

In order to see that this implies Theorem 1.1, we use the following lemma.

Lemma 1.6. *Suppose that F has characteristic p. Then if $a \in F \setminus F^p$, the polynomial*
$$X^{p^n} - a$$
is irreducible in $F[X]$ for any $n \geq 1$.

Proof. Suppose that $f(X) = X^{p^n} - 1 = g(X)h(X)$ is a product of $g(X), h(X) \in F[X]$, both monic and non-constant. Let $b \in \overline{F}$ be a root of $f(X)$. Then
$$f(X) = X^{p^n} - a = (X - b)^{p^n}.$$
Because $F[X]$ is a UFD, $g(X) = (X - b)^m$ for some $0 < m < p^n$. If $m = p^r k$ for k coprime to p, then
$$g(X) = (X - b)^{p^r k} = (X^{p^r} - b^{p^r})^k.$$
The coefficient of $X^{(k-1)p^r}$ is $-kb^{p^r}$. Because k is coprime to p, b^{p^r} is therefore in F. Therefore,
$$a = (b^{p^r})^{p^{n-r}} \in F^{p^{n-r}} \subset F^p,$$
a contradiction. □

Corollary 1.7. *If $F = F^{\mathrm{sep}}$ and $\overline{F} \neq F$, then $\overline{F}/F$ is an infinite extension. In particular, Theorem 1.5 implies Theorem 1.1.*

Proof. As $\overline{F} \neq F^{\mathrm{sep}}$, F has characteristic p and $F \neq F^p$. Then the family from Lemma 1.6 shows that $\overline{F}/F$ is infinite. □

Now we focus on proving Theorem 1.5. For notational simplicity we write $L := F^{\mathrm{sep}}$. The key special case is the following.

Proposition 1.8. *Suppose that F is as in the hypotheses of Theorem 1.5, and $[L\colon F] = p$ is prime. Then $p = 2$, $\mathrm{char}(F) \neq 2$, and $L = F(i)$ where $i^2 = -1$.*

We will leave proving this for later, and show how we can use it to prove Theorem 1.5.

Proof of Theorem 1.5. The extension L/F is Galois by definition. Let G be the Galois group of L/K. If $p \mid |G|$ is a prime, then we can find an element of G of order p. Let K/F be the intermediate field fixed by this element. Then L/K is an extension of degree p, and we may apply Proposition 1.8 to L/K to deduce that $p = 2$. So $|G| = 2^m$ for some $m \geq 1$. To show that $m = 1$, suppose for a contradiction that $4 \mid |G|$. Because p-groups of order p^m contain subgroups of order p^k for all $0 \leq k \leq m$, we can look at the field fixed by a subgroup of order $4 = p^2$ and assume that $|G| = 4$. Then taking an element of order 2 in $|G|$ and looking at the fixed field, we obtain by Proposition 1.8, an intermediate field $F \subset K \subset L$, such that $L = K(i)$, where $i^2 = -1$ and $i \notin K$. But in this case, we can consider the distinct intermediate field $F(i)$. If we also plug in $F(i)$ to Proposition 1.8, as $F(i)/F$ must have degree two because $|G| = 4$, and this tells us that $L = F(i)(j)$ for some $j^2 = -1$ and $j \notin F(i)$. This is a contradiction, as we must have $j = i$ or $j = -i$, both of which are in $F(i)$.

Using the following lemma (which we can apply because $\mathrm{char}(F) \neq 2$ so the extensions defined by square root of elements are separable), it remains to show that for any $a \in F^\times$, exactly one of a and $-a$ is a square in F. If they are both squares, then -1 is a square, so assume that both a and $-a$ are both non-squares. Then $L = F(\sqrt{a}) = F(\sqrt{-a})$. Writing
$$\sqrt{-a} = x + y\sqrt{a},$$
and squaring,
$$-a = x^2 + y^2 a + 2xy\sqrt{a}.$$
Therefore, $x = 0$ or $y = 0$, because $\mathrm{char}(F) \neq 2$, and $\sqrt{-a} \notin F$, hence $x = 0$. So $y = \sqrt{-a}/\sqrt{a}$ is an element of F which squares to -1, a contradiction. □

Lemma 1.9. *Suppose that -1 is not a square in F, and every element of $F(i)$ is a square in $F(i)$, where $i^2 = -1$. Then any non-empty finite sum of non-zero squares of F is a non-zero square of F.*

Proof. It is sufficient to show that if $x, y \in F^{\times}$, then $x^2 + y^2$ is a non-zero square of F. We can define the element $z = x + iy \in F(i)$, and by the assumption have that

$$x + iy = (c + di)^2 = (c^2 - d^2) + 2cdi$$

for some $c, d \in F$. Therefore,

$$x^2 + y^2 = (c^2 - d^2)^2 + 4c^2d^2 = c^4 + d^4 + 2c^2d^2 = (c^2 + d^2)^2$$

is again a square. This is non-zero, as if $x^2 + y^2 = 0$, $(x/y)^2 = -1$ contrary to the assumption on F. □

Now we are left with proving the key Proposition 1.8.

Proof of Proposition 1.8. Suppose first that F has characteristic p. Then by Artin-Schreier theory, $L = F(\alpha)$ for some α a root of $X^p - X - a$, where $a \in F$. For any $b \in L$, there are unique $a_0, \cdots, a_{p-1} \in F$ with

$$b = a_0 + a_1\alpha + \cdots + a_{p-1}\alpha^{p-1}.$$

Consider

$$\begin{aligned} b^p - b &= \left(\sum_{j=0}^{p-1} a_i\alpha^j\right)^p - \sum_{j=0}^{p-1} a_i\alpha^j, \\ &= \sum_{j=0}^{p-1} a_i^p\alpha^{jp} - \sum_{j=0}^{p-1} a_i\alpha^j, \\ &= \sum_{j=0}^{p-1} a_i^p(a + \alpha)^j - \sum_{j=0}^{p-1} a_i\alpha^j. \end{aligned}$$

Choose $b \in L$ such that $b^p - b = a\alpha^{p-1}$, and compare the terms of α^{p-1}. On the right hand side this is $a_{p-1}^p - a_{p-1}$, and on the right hand side this is a. So we have found a root in F of the irreducible polynomial $X^p - X - a \in F[X]$, a contradiction.

Therefore, F does not have characteristic p. Because L is separably closed, L contains a primitive pth root of unity ζ. Furthermore, $[F(\zeta) \colon F] \leq p - 1 < p$, hence $F(\zeta) = F$, and $\zeta \in F$. Therefore, by Kummer theory, $L = F(\gamma)$, where $\gamma^p \in F$.

Because L is separably closed, we can find $\beta \in L$ with $\beta^p = \gamma$. Let $\sigma \in \mathrm{Gal}(L/F)$ be non-trivial. Then $\sigma(\beta^{p^2}) = \beta^{p^2}$, so $\sigma(\beta) = \omega\beta$, where $\omega^{p^2} = 1$. Furthermore, if $\omega^p = 1$, then $\sigma(\beta^p) = \sigma(\beta)^p = \beta^p$, so $\beta^p = \gamma \in F$, a contradiction. Therefore ω is a primitive p^2 root of 1. Because σ is an automorphism and $\omega^p \in F$, $\sigma(\omega)/\omega$ is a pth root of 1, so

$$\sigma(\omega) = \omega\omega^{pk} = \omega^{1+pk}$$

for some $k \in \mathbb{Z}$. We have that

$$\beta = \sigma^p(\beta) = \sigma^{p-1}(\sigma(\omega)\sigma(\beta)) = \cdots = \omega\sigma(\omega)\cdots\sigma^{p-1}(\omega)\beta,$$

and therefore,

$$1 + (1 + pk) + \cdots + (1 + pk)^{p-1} = 0 \mod p^2.$$

Equivalently,

$$\sum_{j=0}^{p-1}(1 + jpk) = 0 \mod p^2,$$

or

$$p + \frac{p(p-1)}{2}pk = \mod p^2.$$

Therefore,

$$\frac{p(p-1)}{2}k = -1 \mod p.$$

Thus p is even, and k is odd. Consequently, ω has order $4 = p^2$, and $\omega^2 \neq 1$, thus $\omega^2 = -1$, as ω has order 4. Because $\omega \notin F$, then $L = F(\omega)$. □

2. Application: $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

As a consequence of the above, we know that all torsion elements of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ have order 1 or 2. We can use this to describe all torsion elements of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

We will use the following fact:

Theorem 2.1 (Neukirch-Uchida)**.** *Every automorphism of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *is inner.*

Therefore, in order to understand the automorphisms of $\overline{\mathbb{Q}}/\mathbb{Q}$, we just need to understand the conjugation action.

Lemma 2.2. *The stabiliser of complex conjugation σ is $\langle\sigma\rangle$.*

Proof. If commutes with σ, then preserves $\mathbb{R}$. By the uniqueness of the order, we have that any automorphism ϕ of $\mathbb{R}$ preserves the order. But this forces ϕ to be the identity: if $\phi(a) \neq a$ for some $a \in \mathbb{R}$, then choose some rational q strictly between a and $\phi(a)$. If

$$a < q < \phi(a),$$

then $\phi(a) < \phi(q) = q$, a contradiction. Similarly if $\phi(a) < q < a$. □

Corollary 2.3. *The centre $Z(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) = 1$, and the natural map*

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$$

is an isomorphism.

The previous lemma also shows us that the conjugation action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the set of order two elements is faithful. The next proposition shows that this action is also transitive.

Proposition 2.4. *Any two order two elements are conjugate in* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$*.*

Proof. Take σ_1, σ_2 order two automorphisms of $\overline{\mathbb{Q}}$. Let K_1, K_2 be the fixed fields inside $\overline{\mathbb{Q}}$. By the Artin-Schreier Theorem, these are both real-closed field extensions of $\mathbb{Q}$, which extend the unique (by Lemma 1.4) order on $\mathbb{Q}$. The real closure of $\mathbb{Q}$ is unique up to isomorphism, and this extends to an automorphism of $\overline{\mathbb{Q}}$ because $\overline{\mathbb{Q}}$ is algebraically closed. This automorphism maps σ_1 to σ_2, and by the previous corollary is given by conjugation. □

In fact it is a possible to characterise $\overline{\mathbb{Q}}$ up to field isomorphism as the unique algebraically closed field for which $\mathrm{Aut}(\mathbb{Q})$ has non-trivial torsion elements and all torsion elements are conjugate.