The Two Artin-Schreier Theorems

Jose Capco (jcapco@risc.jku.at)

We first provide the necessary results to prove the Artin-Schreier[1] Theorem in characteristic $p \neq 0$

Definition. Let G be a group and K be a field then a group homomorphism $\sigma : G \to K^*$ (where the codomain is the multiplicative group of the field) is also known as a *character*.

Example of a Character. Consider $K < L$ as proper field extensions such $L = K(\alpha)$ for some $\alpha \in L \backslash K$. Then any $\sigma \in \mathrm{Aut}(L/K)$ that permutes the zeros of the minimal polynomial of α (while fixing any element in K). If this σ is restricted to L^* it becomes a character $L^* \to L^*$.

Theorem (Dedekind Independence of Character Theorem). For a fixed group G and a field K and any finite number of distinct characters $\sigma_i : G \to K^*$, with say $i = 1, \ldots, n$, we have the following

$$\sum_{i=1}^{n} a_i \sigma_i \equiv 0 \Leftrightarrow a_i = 0 \qquad \forall i = 1, \ldots, n$$

where $a_i \in K$ and the equality in the left means that the function is a zero function (i.e. taking all $g \in G$ to $0 \in K$).

Proof. We prove by the following steps:

1. Start with induction on n, for $n = 1$ the result is trivial.
2. Let g be such that $\sigma_1(g) \neq \sigma_2(g)$ and consider $\sum a_i \sigma_i(gx) = 0$ and $\sum a_i \sigma_1(g) \sigma_i(x) = 0$
3. Cancel one summand by showing $a_2 = 0$ and eventually show all $a_i = 0$

One can prove by induction. Let $a_1 \sigma_1 \equiv 0$ then since σ_1 does not map to $0 \in K$ one must have $a_1 = 0$. Suppose now that for any linear combination of $n - 1$ characters ($n \in \mathbb{N}$) one has linear independence as described in the Theorem. Suppose now that $\sum_{i=1}^{n} a_i \sigma_i \equiv 0$ for some $a_i \in K$ and characters $\sigma_i : G \to K^*$ with $i = 1, \ldots, n$. Since the characters are mutually different there is a $g \in G$ such that $\sigma_1(g) \neq \sigma_2(g)$. For all $x \in G$, one has $\sigma_1(g) \sum_{i=1}^{n} a_i \sigma_i(x) = 0$ and $\sum_{i=1}^{n} a_i \sigma_i(g) \sigma_i(x) = 0$. Subtracting the two gives

$$\sum_{i=2}^{n} a_i (\sigma_i(g) - \sigma_1(g)) \sigma_i(x) = 0 \qquad \forall x \in G$$

By induction hypothesis this would mean that in particular $a_2(\sigma_2(g) - \sigma_1(g)) = 0$ in K. Since the right factor is not 0, we get $a_2 = 0$. Looking at the original sum we have

$$\sum_{i=1}^{n} a_i \sigma_i = a_1 \sigma_1 + \sum_{i=3}^{n} a_i \sigma_i \equiv 0$$

but this is a sum of a linear combination of $n - 1$ characters and, by induction hypothesis, this implies that each of the other a_i $(i = 1, 3, 4, \ldots, n)$ is 0. □

Now we are ready to state and prove the first Artin-Schreier Theorem:

Theorem (Artin-Schreier Theorem for Characteristic p ≠ 0). Let $K \leq L$ be a Galois extension of fields and suppose that $\mathrm{char}\, L = p$ and that $|\mathrm{Aut}(L/K)| = p$ then there is an $\alpha \in L$ such that $K(\alpha) = L$ and α is the zero of an irreducible polynomial in $K[T]$ of the form $T^n - T - a$ for some $a \in K$.

[1] Emil Artin (1898-1962): Austrian algebraist and number theorist. Artinian rings are named after him. Otto Schreier (1901-1929): Austrian algebraist and group theorist. He migrated and worked in Hamburg Germany and later died of sepsis. Both these mathematician were educated from the University of Vienna.

Proof. Clearly the field extension is proper (because the automorphism group has an order greater than 1). Consider now a generator σ of $G := \mathrm{Aut}(L/K)$ (G is cyclic!). We note that throughout when we write σ^n for some $n \in \mathbb{N}$ we mean n-times composition of σ. We prove using the following steps:

1. Show that for $x \in L \backslash K$ one has $z := \sum_{i=0}^{p-1} \sigma^i(x)$ is invariant under σ and is in K^*.
2. Set $y := \sum_{i=0}^{p-1}(p-1-i)\sigma^i(x) \in K$ and see that $\sigma(y) = y + z$
3. Set $\alpha := y/z$ then $\alpha \notin K$ because σ does not fix it ($\sigma(\alpha) = \alpha + 1$)
4. By Fermat's little we can set $f(T) := T^p - T = \prod_{i=0}^{p-1}(T-i)$ and observe that it is additive, i.e. $f(a+b) = f(a) + f(b)$
5. Show
$$\prod_{i=0}^{p-1}(T - \sigma^i(\alpha)) = T^p - T + (-1)^p \prod_{i=0}^{p-1}(\alpha + i)$$
is in $K[T]$ (the constant part is σ-invariant) and has p distinct zeros, including α, and is the minimum polynomial and so $K(\alpha) = L$

1 is because σ is a generator of G and the extension is Galois, so every invariant of σ belongs to K. In particular z cannot be 0 because of the Dedekind's independence of character Theorem. For *2* we see the following (the last line is because the field has characteristic p and because the factor $p - 1 - (p-1) = 0$)

$$\sigma(y) = \sum_{i=0}^{p-1}(p-1-i)\sigma^{i+1}(x) = \sum_{i=0}^{p-1}(p-1-i)\sigma^{i+1}(x)$$
$$\sum_{i=0}^{p-1}(p-1-(i+1))\sigma^{i+1}(x) + z = \sum_{i=1}^{p-2}(p-1-i)\sigma^i(x) + (-1)\sigma^p(x) + z$$
$$\sum_{i=1}^{p-2}(p-1-i)\sigma^i(x) + (-1)x + z = \sum_{i=1}^{p-2}(p-1-i)\sigma^i(x) + (p-1)x + z =$$
$$\sum_{i=0}^{p-2}(p-1-i)\sigma^i(x) + z = \sum_{i=0}^{p-1}(p-1-i)\sigma^i(x) + z = y + z$$

Now, *3* is self-explanatory. For *4*, by using Fermat's little theorem, it is clear that $T - i$ divides $f(T)$ for all $i = 0, 1, \ldots, p-1$. Thus $f(T)$ is the product of all these linear factors. Since we have p linear factors forming a monic polynomial, this will be the only factors of $f(T)$. The additivity of $f(T)$ comes from the fact that in a field of characteristic $p > 0$, after taking binomial expansion, the following identity holds

$$(a+b)^p = a^p + b^p \quad \forall a, b$$

For *5*, by applying *3* i-times for any $i = 1, \ldots, p-1$ we get $\sigma^i(\alpha) = \alpha + i$ so we have

$$g(T) := \prod_{i=0}^{p-1}(T - \sigma^i(\alpha)) = \prod_{i=0}^{p-1}(T - \alpha - i) = f(T - \alpha) =$$
$$f(T) + f(-\alpha) = T^p - T + \prod_{i=0}^{p-1}(-\alpha - i) = T^p - T + (-1)^p \prod_{i=0}^{p-1}(\alpha + i)$$

We set $a := (-1)^p \prod_{i=0}^{p-1}(\alpha + i)$ and observe, by *3* and because the extension is Galois, that

$$\sigma(a) = (-1)^p \prod_{i=0}^{p-1}(\alpha + i + 1) = (-1)^p \prod_{i=0}^{p-1}(\alpha + i) = a \in K$$

We can now write $g(T)$ in the following way

$$g(T) = f(T) + (-1)^p \prod_{i=0}^{p-1}(\alpha + i) = f(T) + (-1)^p \prod_{i=0}^{p-1}(\alpha - i) = \prod_{i=0}^{p-1}(\alpha - i) + (-1)^p \prod_{i=0}^{p-1}(\alpha - i)$$

so if p is an odd prime we have

$$g(\alpha) = g(\alpha + 1) = \cdots = g(\alpha + p - 1) = 0$$

If p is even (=2) then

$$g(\alpha) = g(\alpha + 1) = \cdots = g(\alpha + p - 1) = 2f(\alpha) = 0$$

So $\alpha, \alpha + 1, \ldots, \alpha + p - 1$ are p distinct zeros of the polynomial $g(T)$. These are the only zeros of $g(T)$ and they are all not in K (because their image under σ is a translation by 1, so not an invariant element). Apply now $\sigma, \sigma^2, \ldots, \sigma^{p-1}$ (and the identity map) restricted to $K(\alpha)$ to the Dedekind's character independence theorem, we see that the roots are also linearly independent over K and so

$$p \leq [K(\alpha) : K] \leq [L : K]$$

In general, $[L : K] \leq |G| = p$ (even if L is not a Galois field extension of K as long as K is the G-invariant subfield of L. This is also known as Artin's Theorem, see [Milne] Theorem 3.4). Thus $[L : K] = p$ and so $g(T)$ is the minimal polynomial of α and $L = K(\alpha)$. □

To continue we need a definition and some properties in algebraic number theory, namely the norm of finite field extensions

Definition. Let $K \leq L$ be a finite field extension, then any $\alpha \in L$ defines a linear transformation

$$L \to L \qquad x \mapsto \alpha x$$

between K-vector spaces (the extended field L). This linear transformation has a square representative matrix (with entries all in K) which we we denote M_α. Using the notation for representative matrix, we define a function

$$N_{L/K} : L^* \to K^* \qquad \alpha \mapsto \det(M_\alpha)$$

If the field extension is known we sometimes write $N(\alpha)$ instead of $N_{L/K}(\alpha)$

We note the following facts which we state without proof (the proof can be found in a nice expository paper by Keith Conrad [Con])

Remark 1. Let $K \leq L$ be a finite field extension and let $N := N_{L/K}$ be the norm associated to it.

- N is multiplicative, i.e. $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in L$
- If $a \in K$ then $N(a) = a^{[L:K]}$
- Let $\alpha \in L$ and $\chi(T) \in K[T]$ be the characteristic polynomial of M_α then

$$N(\alpha) = (-1)^{\deg(\chi(T))}\chi(0)$$

- If $L = K(\alpha)$ for some $\alpha \in K$, then the minimal polynomial of α in $K[T]$ is the same as the characteristic polynomial of M_α.

Norms are powerful tools to determine whether certain elements have roots in the field. For instance ...

Lemma 2. Let K be a field and suppose $a \in K$ has no p-th root for some prime number p. Then $x^p - a \in K[x]$ is irreducible. Thus, by Abel's Irreducibility Lemma, $x^p - a$ is necessarily the minimal polynomial of all p-th roots of a.

Proof. We prove using the following steps

1. By contradiction, let the minimal polynomial μ of some $\alpha = a^{1/p}$ properly divide $x^p - a$
2. Then show in K that $a^{\deg(\mu)} = N(\alpha)^p$
3. Use $\deg(\mu)$ and p are coprime to find some $a^{1/p}$ in K (some $a^c N(\alpha)^d$).

Suppose, by contradiction, that $f(x) := x^p - a$ is reducible. Let α be a p-th root of a in an extension field of K, then by hypothesis the minimal polynomial divides $f(x)$ and their quotient is non-constant. Thus, the minimal polynomial has a degree $n = [K(\alpha) : K]$ which is strictly less than p. Consider the norm function $N := N_{K(\alpha)/K}$ then we have

$$a^n = N(a) = N(\alpha^p) = (N(\alpha))^p$$

Since $N(\alpha) \in K$ and the numbers n and p are coprime, there are $c, d \in \mathbb{Z}$ such that $pc + dn = 1$. Consider $a^c N(\alpha)^d \in K$ (we are in a field, so taking negative powers are allowed) and take its p-th power. We have

$$(a^c N(\alpha)^d)^p = a^{pc} + N(\alpha)^{dp} = a^{pc} + a^{nd} = a^{pc+nd} = a$$

Thus a has a p-th root in K which is a contradiction. □

Lemma (Kummer Extension Lemma). Let $K \leq L$ be Galois field extensions and $[L : K] = p$ for some prime number p. Suppose furthermore that K contains all the p-th root of unity. Then $L = K[\alpha]$ for some $\alpha \in L$ such that $\alpha^p \in K$.

Proof. See §4.7 Lemma 3 p.253 of [Jac]. □

Finally we show a theorem published in 1927 also known as Artin-Schreier theorem that is more known in real algebra:

Theorem (Artin-Schreier Theorem for Characteristic 0). Let $K < \bar{K}$ be a proper field extension such that $\bar{K}$ is the algebraic closure of K and $[L : K] < \infty$ then

- The characteristic of L is 0
- $\bar{K} = K[\sqrt{-1}]$
- K is a real closed field

Proof. We prove using the following steps

1. Prove K is perfect by contradiction. Show that you can algebraically infinitely extend K by several $p, p^2, \ldots$ roots of a certain element $a \in K$ (without a p-th root) for some prime p and arrive to a contradiction
2. Having shown K is perfect conclude that the extension $K < \bar{K}$ is a finite Galois extension.
3. Pick the largest proper subfield $L < \bar{K}$ such that $K \leq L$. Show by contradiction that $p \neq [\bar{K} : L]$, where $p := \operatorname{char} K$.
   (a) Use Artin-Schreier to show that there is a $\alpha \in \bar{K}$ such that $\bar{K} = L(\alpha)$ and α has minimal polynomial $T^p - T + a \in L[T]$ for some $a \in L$
   (b) Show that for a solution $b \in \bar{K}$ of $T^p - T + a\alpha^{p-1}$ in $\bar{K}$, we can expand b^p from a linear combination of the canonical basis induced by α and show that an element of K satisfies $T^p - T + a$.

4. Show that $[\bar{K} : L] = 2$
   (a) Look at the $[\bar{K} : L]$-th cyclotomic polynomial and show that K must contain all the $[\bar{K} : L]$-th root of unity.
   (b) Use Kummer Extension Lemma to show the final result. Show that $\bar{K} = L[\beta]$ for some $\beta \in \bar{K}$ and β is an element without square root in L.
5. Prove that $L = K$ and K is real closed.
   (a) Show that $\sqrt{-1} \notin L$ and so $\bar{K} = L[\sqrt{-1}]$
   (b) Show that $L = K$
   (c) Show that sum of squares in K are squares and conclude real closedness of K.

For *1*, assume otherwise (i.e. K is not perfect). A characterization (or definition) of a non-perfect field is that it has a prime characteristic p and that some elements of the field do not have a p-th root. So let $a \in K$ be such that no p-th root is in K, where $\operatorname{char} K = p$. Denote one p-th root of a as α in an extension field $K(\alpha)$ of K. We have p-degree field extension $K < K(\alpha)$ because, by Lemma 2, $X^p - a$ is the minimal polynomial of α over K. If α has a p-th root in $K(\alpha)$, say β, and if we consider the norm function $N = N_{K(\alpha)/K}$ we get[2] (see Remark 1)

$$N(\alpha) = N(\beta^p) = N(\beta)^p = N(\alpha) = (-1)^p(-a) = (-1)^{p+1}a$$

So a has a p-th root in K and this is a contradiction to our assumption. Thus, $K(\beta)$ is a p^2 degree field extension $K < K(\beta)$. Iterating this procedure would give us $p, p^2, p^3, \ldots$ degree field extensions of K. This is a contradiction to $[\bar{K} : K] < \infty$. Because $\bar{K}$ is an extension of the perfect field K, $\bar{K}$ is a separable extension (see p.27 of [Milne]). Clearly $\bar{K}$ is also a normal extension of K, because it is algebraic closed. Thus $\bar{K}$ is a Galois extension of K.

We start with *3* and choose a largest intermediate field L such that $K \leq L < \bar{K}$. Now $\operatorname{Aut}(\bar{K}/K)$ is the automorphism group of a finite Galois extension, so by the Fundamental Theorem of Galois Theory (see [Milne] Theorem 3.16 p.29 or [Jac] p.239-240) and Cauchy's Theorem (see [Jac] p.80) $[\bar{K} : L]$ must necessarily be a prime number. Now, for *3*a, assume that $[\bar{K} : L] = \operatorname{char} K = p$. By Artin-Schreier for prime characteristic, there is an $\alpha \in \bar{K}$ such that $L(\alpha) = \bar{K}$ and α is the zero of an irreducible polynomial in $L[T]$ of the form $T^n - T + a$ for some $a \in L$.

Now for *3*b. Because $\bar{K}$ is algebraically closed, the polynomial $T^p - T + a\alpha^{p-1}$ has a root $b \in \bar{K}$. Also, $\bar{K}$ is a vector space over L with basis $1, \alpha, \alpha^2, \ldots, \alpha^{p-1}$. So we may write

$$b = c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{p-1}\alpha^{p-1} \qquad c_i \in L$$

We know that $b^p - b + a\alpha^{p-1} = 0$ and substituting the equation for b gives

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

But this is a linear combination of the basis of L with coefficients in K that equates to 0, thus $c_{p-1} \in K$ is a zero of the polynomial $T^p - T + a$. This is a contradiction to irreducibility of $T^p - T + a$ (see the 'Factor Theorem' in [Jac] §2.11 Corollary 2 p.130).

For *4*, we set $q := [\bar{K} : L]$ (recall, by construction, that this is a prime number). K must contains all the q-th roots of unity because the q-cyclotomic polynomial (this divides $x^q - 1$) is of degree $q - 1$ and has, as roots, all non-trivial q-th roots of unity and if this were not in L one has a field extension by adjoining a non-trivial q-th root and this must be equal to $\bar{K}$ (by the maximality of L) but this extension has degree at most $q - 1$ and this is a contradiction. By the Kummer Extension Lemma, there is an $\alpha \in \bar{K} \backslash L$ such that $\alpha^q \in L$ and that $\bar{K} = L[\alpha]$. Since

[2] Notice that $(-1)^{p+1} \equiv 1$ even for $p = 2$ because every element is the additive inverse of itself in a characteristic 2 field.

char $K \neq q$, by Lemma 2, the polynomial $T^q - a \in L[T]$, where $a := \alpha^q$, is irreducible and is the minimal polynomial of α (over L). Setting $N = N_{\bar{K}/L}$ gives us (see Remark 1)

$$N(a) = N(\alpha^q) = N(\alpha)^q = N(a) = (-1)^{q+1}a$$

If q were odd then $T^q - a$ has a zero $N(\alpha) \in L$ and is not irreducible, thus $q = 2$.

To prove 5a, we show first that $\bar{K} = L[i]$ (where $i \in \bar{K}$ is a root of $T^2 + 1$, i.e. $i = \sqrt{-1}$). If $i \in L$ then we have (for N, α and a as in the proof above for 4)

$$N(-a) = N((i\alpha)^2) = N(i\alpha)^2 = -N(\alpha)^2 = N(-a) = (-1)^{2+1}(-a) = a$$

which implies that a has a square root in L (recall we proved $q = 2$), and this is contradiction. Thus $i \notin L$ and so $\bar{K} = L[i]$.

To prove 5b one may show by contradiction that if $L \backslash K$ is non-empty thus $K[i]$ is a proper field of $\bar{K}$ (i and K alone cannot span elements in $L \backslash K$). The extension $\bar{K}/K[i]$ is finite and one may replace K by $K[i]$ and prove everything from 1 to 5a to arrive to a contradiction (L in this case already contains i and this is a contradiction). Finally for 5c we first show that K is a real field. First we show that the sum of squares in K is also a square. It suffices to show that the sum of two square is a square. So let $a, b \in K$ then we have $a + ib = (c + id)^2$ for some $c, d \in K$ (because $K[i] = \bar{K}$ is algebraically closed) and by taking the conjugate of i we have $a - ib = (c - id)^2$ Thus we have shown

$$a^2 + b^2 = (c^2 + d^2)^2$$

i.e. the sum of two squares (thus all finite sum of squares) is a square in K. Now suppose that K is not real, because the sum of squares is a square in K, there exists $a, b \in K^*$ such that $a^2 + b^2 = 0$. This implies that $(a/b)^2 = -1$ in K. So -1 is a square in K (i.e. $i \in K$) and so this is a contradiction. Thus K is a real field and so of characteristic 0. The next proper algebraic extension of K is $K[i] = \bar{K}$ which is algebraically closed (and thus, not real). Thus, K must be real closed. □

References

[Jac] **N. Jacobson**, *Basic Algebra I*, 2nd Edition. W.H. Freeman and Company 1985

[Milne] **J.S. Milne**, *Fields and Galois Theory*, Version 4.21 Sept. 28, 2008. Online: www.jmilne.org/math/. Accessed: 04.2009.

[Con] **K. Conrad**, *Trace and Norm*, Online: http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/tracenorm.pdf. Accessed: 06.2014.