

**SEPARABLE EXTENSIONS OF DEGREE p IN
CHARACTERISTIC p ; FAILURE OF HERMITE'S THEOREM IN
CHARACTERISTIC p**

JIM STANKEWICZ

1. SEPARABLE FIELD EXTENSIONS OF DEGREE p

Exercise: Let K be a field of characteristic p and $\wp_p : \bar{K} \rightarrow \bar{K}$ by $x \mapsto x^p - x$ be the Artin-Schreier isogeny. It is a group homomorphism with kernel $(\mathbb{F}_p, +)$. The separable degree p extensions of K are in some way in bijection with $K/\wp_p(K)$.

1.1. Solution 1 (Cohomology): Note first that $\wp_p : \bar{K} \rightarrow \bar{K}$ is onto, because if $a \in \bar{K}$, we can find $x \in \bar{K}$ such that $x^p - x = a$ because $t^p - t - a$ is an algebraic equation. Moreover the same is true replacing \bar{K} with K^{sep} since $t^p - t - a$ is a separable polynomial because its derivative over K is $-1 \neq 0$. In either case, the kernel is $\mathbb{F}_p \subset K$ so we have the short exact sequence

$$0 \rightarrow \mathbb{F}_p \rightarrow K^{\text{sep}} \xrightarrow{\wp_p} K^{\text{sep}} \rightarrow 0.$$

Clearly each of these is a $G_K = \text{Gal}(K^{\text{sep}}/K)$ -module, with \mathbb{F}_p possessing the trivial action since it is contained in K . (Thus, as a Galois module, $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$.)

Hence $H^1(G_K, \mathbb{Z}/p\mathbb{Z}) = \text{Hom}(G_K, \mathbb{Z}/p\mathbb{Z})$. The natural thing to do then is to take the long exact sequence of cohomology:

$$0 \rightarrow \mathbb{Z}/p\mathbb{Z} \rightarrow K \xrightarrow{\wp_p} K \rightarrow H^1(G_K, \mathbb{Z}/p\mathbb{Z}) \rightarrow H^1(G_K, K^{\text{sep}}) \rightarrow \dots$$

By the additive version of Hilbert's Theorem 90, that $H^1(G_K, K^{\text{sep}}) = 0$, we have that $K/\wp_p(K) \cong H^1(G_K, \mathbb{Z}/p\mathbb{Z}) = \text{hom}(G_K, \mathbb{Z}/p\mathbb{Z})$. Now recall that if we restrict our attention to separable degree p extensions which are actually *Galois*, these are in bijection with the open normal subgroups H of G_K with quotient $\mathbb{Z}/p\mathbb{Z}$. Each of these gives a nonzero homomorphism $r : G_K \rightarrow \mathbb{Z}/p\mathbb{Z}$ just by modding out by H .

Now given homomorphisms $\phi, \psi : G_K \rightarrow \mathbb{Z}/p\mathbb{Z}$ with the same kernel H , we let g_1, \dots, g_p be a complete set of coset representatives for G_K/H . We can define an automorphism α of G_K/H by $\alpha(\phi(g_i)) = \psi(g_i)$ since ϕ, ψ are both onto. Likewise if β is an automorphism of $\mathbb{Z}/p\mathbb{Z}$ and $\phi : G_K \rightarrow \mathbb{Z}/p\mathbb{Z}$ is an onto homomorphism then $\psi = \beta \circ \phi$ is a homomorphism with $\ker \phi = \ker \psi$. Therefore the open normal subgroups of G_K with quotient $\mathbb{Z}/p\mathbb{Z}$ are in bijection with the nonconstant (equivalently onto) homomorphisms $G_K \rightarrow \mathbb{Z}/p\mathbb{Z}$ modulo the automorphisms of $\mathbb{Z}/p\mathbb{Z}$, which are of course $(\mathbb{Z}/p\mathbb{Z})^\times$.

Important Note It's crucial to mod out by this action as we can see in the case that $K = \mathbb{Z}/p\mathbb{Z}$. In this case \wp_p is identically zero, so $K/\wp_p(K) = K = \mathbb{Z}/p\mathbb{Z}$, but it is well-known that $\mathbb{Z}/p\mathbb{Z}$ has exactly one degree p field extension.

Therefore

$$\begin{aligned} \{\mathbb{Z}/p\mathbb{Z} - \text{cyclic extensions of } K\} &\leftrightarrow (\mathbb{Z}/p\mathbb{Z})^\times \setminus \text{hom}(G_K, \mathbb{Z}/p\mathbb{Z}) - \{0\} \\ &\cong (\mathbb{Z}/p\mathbb{Z})^\times \setminus (K/\wp_p(K) - \{0\}) \end{aligned}$$

Note that we use “double coset” notation even though K is abelian because $\wp_p(K)$ is a normal subgroup of K while $\mathbb{Z}/p\mathbb{Z}^\times$ acts on K by left multiplication (as we will see when we do this in a more concrete setting).

Finally we provide a proof of the additive version of Hilbert’s Theorem 90. This proof (once we restrict to a finite extension) is adapted from Patrick Morandi’s *Field and Galois Theory*. Note first that by Proposition II.4.2 in Milne’s *Class Field Theory*, $H^1(G_K, K^{\text{sep}}) = \varinjlim_{[L:K] < \infty} H^1(\text{Gal}(L/K), L)$. Now note that one definition we can take of a finite separable field extension L/K is that the trace map Tr provides an isomorphism $L \rightarrow \text{hom}(L, K)$ by $\alpha \mapsto Tr(\alpha)$. Thus there exists $\alpha \in L$ such that $Tr(\alpha) = a \neq 0$ so without loss of generality, we may replace α with αa^{-1} which has trace 1. Now suppose $g : \text{Gal}(L/K) \rightarrow L$ is a cocycle and for simplicity just call $\text{Gal}(L/K)$ G . Define b to be

$$\sum_{\sigma \in G} g(\sigma)\sigma(\alpha)$$

Thus if $\tau \in G$,

$$\begin{aligned} \tau(b) &= \sum_{\sigma \in G} \tau g(\sigma)\tau\sigma(\alpha) = \sum_{\sigma \in G} (g(\tau\sigma) - g(\tau))\tau\sigma(\alpha) \\ &= b - g(\tau)\tau \left(\sum_{\sigma \in G} \sigma(\alpha) \right) = b - g(\tau)\tau(1) = b - g(\tau) \end{aligned}$$

Thus for all τ , $g(\tau) = b - \tau(b)$.

We also note a well-known corollary, which states that if L is a cyclic extension (say of degree n) then if $\beta \in L$ has trace zero then $\beta = b - \sigma b$ for some $b \in L$. Note that the converse is trivially true since $Tr(b - \sigma b) = Tr(b) - Tr(\sigma b) = Tr(b) - Tr(b) = 0$.

The way to do this is to fix an isomorphism $\langle \sigma \rangle = \text{Gal}(L/K) \cong \mathbb{Z}/n\mathbb{Z}$ define a map $\tilde{\beta} : \mathbb{Z}/n\mathbb{Z} \rightarrow L$ by $i \mapsto \sum_{k=0}^{i-1} \sigma^k(\beta)$. We note that

$$\tilde{\beta}(i+j) = \sum_{k=0}^{j-1} \sigma^k(\beta) + \sigma^j \left(\sum_{k=0}^{i-1} \sigma^k(\beta) \right) = \tilde{\beta}(j) + j \cdot \tilde{\beta}(i).$$

Thus we have a cocycle, and by Hilbert’s Theorem 90 above, there exists a b such that for all j , $\tilde{\beta}(j) = (1 - \sigma^j)(b)$ and so if $j = 1$, $\beta = b - \sigma(b)$.

1.2. Solution 2: Separable algebras. Let us provide a second solution, more constructive this time.

Consider the assignment $a \mapsto K[t]/(t^p - t - a) = B_a$. This construction need not produce a field extension, but rather a *separable algebra* of degree p over K . Recall:

Lemma 1. (*Separable algebras*)

Let K be an arbitrary field and let A/K be a finite-dimensional commutative K -algebra. TFAE:

(i) $A \cong \prod_{i=1}^n L_i$, where each L_i/K is a finite-dimensional separable field extension.

- (ii) $A \otimes_K \overline{K}$ is reduced (i.e., has no nonzero nilpotent elements).
- (iii) $A \otimes_K \overline{K} \cong \overline{K}^{\dim A}$.
- (iv) The bilinear form $(x, y) \mapsto \text{Tr}(xy)$ is nondegenerate.

C.f. Theorem 2.7 in Lenstra's *Galois Theory for schemes* and a proof can be found there.

Note that this really yields a separable algebra as $t^p - t - a$ has distinct roots over \overline{K} since the derivative is $-1 \neq 0$. In fact, we might even call this a *Galois Algebra* with $\text{Gal}(B_a/K) \cong \mathbb{Z}/p\mathbb{Z} \cong \langle \sigma \rangle$ because if $\alpha \in \overline{K}$ is a root of $t^p - t - a$ then $\alpha + 1, \alpha + 2, \dots, \alpha - 1 = \alpha + (p - 1)$ are also roots. Therefore this is a complete set of roots in \overline{K} and $\mathbb{Z}/p\mathbb{Z}$ permutes the roots by $\sigma \mapsto \sigma + 1$. Note that this does not generally determine the action on all of B_a unless we make a choice of $\alpha \in B_a \setminus K$, so $\{1, \alpha, \dots, \alpha^{p-1}\}$ forms a basis for B_a as a vector space over K .

In the case that $t^p - t - a$ is irreducible, $\alpha \notin K$ so $\{1, \alpha, \dots, \alpha^{p-1}\}$ already provides a convenient basis and the Galois definition of trace is the same as the multiplicative definition. In the case there is a root $\alpha \in K$, we know by the Chinese Remainder Theorem that as a K -algebra

$$B_a = K[t]/(t^p - t - a) \cong K[t]/(t - \alpha) \oplus K[t]/(t - \alpha - 1) \oplus \dots \oplus K[t]/(t - \alpha + 1) \cong K^p$$

Therefore, we have to find a vector $\vec{\alpha} \in B_a \setminus K$ such that $\vec{\alpha}^p - \vec{\alpha} = a$. Recall that in K^p , the multiplicative identity is $(1, \dots, 1)$ so as a ring K embeds via the diagonal map. Since $\alpha \in K$ is a root of $t^p - t - a$, (α, \dots, α) is a root of $t^p - t - a$ in our copy of K . For a copy which is not in K , we draw inspiration from the Chinese Remainder Theorem decomposition and suggest

$$\vec{\alpha} = (\alpha, \alpha + 1, \dots, \alpha - 1).$$

As we've already discussed, each of these is a root of $t^p - t - a$ and so when we add and multiply coordinate-wise, we see that $\vec{\alpha}^p - \vec{\alpha} = (a, \dots, a) \in B_a$. We could show that the set $\{1, \vec{\alpha}, \dots, \vec{\alpha}^{p-1}\}$ forms a basis, but we've already got the convenient standard basis to work with where the matrix for multiplying by (r_0, \dots, r_{p-1}) is the diagonal matrix with the same entries. Thus the trace of (r_0, \dots, r_{p-1}) is $\sum r_i$. Note further that this is exactly the "Galois Trace" if we extend the action on the roots $\vec{\alpha}, \vec{\alpha} + 1, \dots, \vec{\alpha} - 1$ to $\sigma(r_0, \dots, r_{p-1}) = (r_1, \dots, r_{p-1}, r_0)$, a ring automorphism of B_a fixing K and only K .

Note that the key in each case was finding an element $\alpha \in B_a$ such that $\sigma(\alpha) = \alpha + 1$. We could also pick $\sigma(\alpha) = \alpha + i$ for $i \in \mathbb{Z}/p\mathbb{Z}^\times$, because if there is such an α then

$$\begin{aligned} \sigma(\alpha^p - \alpha) &= \sigma(\alpha)^p - \sigma(\alpha) \\ &= (\alpha + i)^p - (\alpha + i) \\ &= \alpha^p - i - \alpha + i \\ &= \alpha^p - \alpha \end{aligned}$$

so $\alpha^p - \alpha \in K$. Moreover note that this is exactly the ambiguity we deal with by modding out by $\mathbb{Z}/p\mathbb{Z}^\times$, which is concretely expressed that if $\sigma(\alpha) = \alpha + i$ then $\sigma(\alpha/i) = \alpha/i + 1$. It is also plain to see that this action preserves $\wp_p(K)$ because $i(r^p - r) = (ir)^p - (ir)$, so we can focus on the case $\sigma(\alpha) = \alpha + 1$ without fear that anything will change if we have to mod out by $\wp_p(K)$ at any point.

Claim The assignment $a \mapsto B_a$ is onto. That is, every $\mathbb{Z}/p\mathbb{Z}$ -Galois Algebra is isomorphic to B_a for some $a \in K$.

To prove this, recall that for the proof of the corollary to the additive version of Hilbert's Theorem 90, we used only the fact that the Galois trace was the same as the multiplicative trace to create a cocycle. That is to say, it's the same to consider $H^1(\mathbb{Z}/p\mathbb{Z}, L)$ as it is $H^1(\mathbb{Z}/p\mathbb{Z}, B)$. Therefore, for any $\mathbb{Z}/p\mathbb{Z}$ -Galois K -Algebra B , $b \in B$ has trace zero if and only if there exists some $\alpha \in B$ such that $b = \alpha - \sigma(\alpha)$. In particular, $Tr(-1) = [B : K](-1) = -p = 0$. Thus there is some $\alpha \in B$ such that $-1 = \alpha - \sigma(\alpha)$ or rather that $\sigma(\alpha) = \alpha + 1$. As we saw above, this implies that $\alpha^p - \alpha =: a \in K$. Thus $B \supset B_a$ but then dimension considerations demand that they be equal.

Now suppose that in addition to $\alpha \in B_a$ such that $\alpha^p - \alpha = a$ and $\sigma(\alpha) = \alpha + 1$, there were some $\beta \in B_a$ such that $\sigma(\beta) = \beta + 1$. As before, $\beta^p - \beta =: b \in K$, so $B_b = B_a$. What can we say about $b - a$, that is, what is the kernel of $a \mapsto B_a$?

Recall that since $\beta - \sigma(\beta) = -1 = \alpha - \sigma(\alpha)$, we have that $\sigma(\beta - \alpha) = \beta - \alpha =: r \in K$. Therefore we consider

$$b = \beta^p - \beta = (\alpha + r)^p - (\alpha + r) = (\alpha^p - \alpha) + (r^p - r) = a + (r^p - r)$$

It follows then that if $B_b \cong B_a$ then $b \in a + \wp_p(K)$ or rather that $b - a \in \wp_p(K)$. Therefore, the set of $\mathbb{Z}/p\mathbb{Z}$ -Galois K -algebras is in bijection with $(\mathbb{Z}/p\mathbb{Z})^\times \setminus K/\wp_p(K)$.

Now let's use this to solve another exercise.

2. THERE ARE FIELDS FOR WHICH A HERMITE FINITENESS THEOREM DOES NOT HOLD

It is a well known theorem of Hermite that there are finitely many number fields of bounded degree and discriminant. Given the usual view of $K(t)$ as the field of rational functions of $\mathbb{P}^1 = \mathbb{A}^1 \cup \infty$ (the choice of infinity corresponding to the choice of t), this can be thought of as the number field analogue of the topological fact that there are only finitely many covers of \mathbb{P}^1 of bounded degree and ramification. Show however, that this fails for some fields.

Pick any field such that $K/\wp_p(K)$ is infinite

The key here is that the *Artin-Schreier algebra* B_a/K is an unramified cover of K for all $a \in K$. Put differently, the discriminant

$$\Delta(B_a/K) = \det(Tr(\alpha^i \alpha^j)) = (-1)^{p+(p-1)(p-2)/2}$$

for all a and for all K , so whatever rings R lie inside of K , there are no primes of R which divide the discriminant, which is to say that there are no ramification points. Given this, B_a is for all intents and purposes a covering space of K , except that the arrow $K \rightarrow B_a$ is going the wrong way. This is easily fixed by looking in the opposite category, so $\text{Spec}(B_a) \rightarrow \text{Spec}(K)$.

Note also that although we didn't check that $\{1, \bar{\alpha}, \dots, \bar{\alpha}^{p-1}\}$ is a basis for $B_0 = K^p/K$, K^p is the p -fold disconnected cover of K .

Let's prove, assuming that $\{1, \alpha, \dots, \alpha^{p-1}\}$ is a basis for B_a/K , that the discriminant is 1. Using this basis, the matrix for multiplication by α^i is

$$\left(\begin{array}{c|ccc} 0 & J_i(a) & & \\ \hline & 0 & \dots & 0 & 1 \\ I_{p-i} & 0 & \dots & 0 & 0 \end{array} \right),$$

where I_{p-i} is the $(p-i) \times (p-i)$ identity matrix and $J_i(a)$ is the $i \times i$ lower-triangular Jordan Block with eigenvalue a . It follows that the trace of this matrix is 0 for $0 \leq i \leq p-2$ and if $i = p-1$, then it is $p-1$ or more simply, -1 . Therefore the trace pairing matrix $\text{Tr}(\alpha^{i+j})$ is zero above the anti-diagonal and is -1 on the anti-diagonal. Therefore the determinant is, after reversing the order of the basis, $(-1)^p$.

So we've shown that if $K/\wp_p(K)$ is infinite, there are infinitely many extensions that are unramified, or at least, only ramified at ∞ . Now we just need to exhibit a field where $K/\wp_p(K)$ is actually infinite. In fact we can exhibit a *local* field with this property. Take $K = \mathbb{Z}/p\mathbb{Z}((t))$, as Brian Conrad does in <http://math.stanford.edu/~conrad/248APage/handouts/weirdfield.pdf>. Then, as he shows, each t^n where $n < 0$ and $p \nmid n$ lies in a distinct $\wp_p(K)$ -coset of K .