Abstract

Let $K$ be a local field of characteristic $p$ with perfect residue field $k$. In this paper we find a set of representatives for the $k$-isomorphism classes of totally ramified separable extensions $L/K$ of degree $p$. This extends work of Klopsch, who found representatives for the $k$-isomorphism classes of totally ramified Galois extensions $L/K$ of degree $p$.

1. Introduction and results

Let $K$ be a local field with perfect residue field $k$ and let $K_s$ be a separable closure of $K$. The problem of enumerating finite subextensions $L/K$ of $K_s/K$ has a long history (see for instance [5]). Alternatively, one might wish to enumerate isomorphism classes of extensions. Say that the finite extensions $L_1/K$ and $L_2/K$ are $K$-isomorphic if there is a field isomorphism $\sigma : L_1 \to L_2$ which induces the identity map on $K$. In this case the extensions $L_1/K$ and $L_2/K$ share the same field-theoretic and arithmetic data; for instance their degrees, automorphism groups, and ramification data must be the same. In the case where $K$ is a finite extension of the $p$-adic field $\mathbb{Q}_p$, Monge [6] computed the number of $K$-isomorphism classes of extensions $L/K$ of degree $n$, for arbitrary $n \geq 1$.

One says that the finite extensions $L_1/K$ and $L_2/K$ are $k$-isomorphic if there is a field isomorphism $\sigma : L_1 \to L_2$ such that $\sigma(K) = K$ and $\sigma$ induces the identity map on $k$. Such an isomorphism is automatically continuous (see Lemma 3.1). If the extensions $L_1/K$ and $L_2/K$ are $k$-isomorphic then they have the same field-theoretic and arithmetic properties. Let Aut$_k(K)$ denote the group of field automorphisms of $K$ which induce the identity map on $k$. Then Aut$_k(K)$ is finite if char$(K) = 0$, infinite if char$(K) = p$. Since every $k$-isomorphism $\sigma$ from $L_1/K$ to $L_2/K$ induces an element of Aut$_k(K)$, this suggests that $k$-isomorphisms should be more plentiful when char$(K) = p$. In
this paper we consider the problem of classifying $k$-isomorphism classes of finite totally ramified extensions of a local field $K$ of characteristic $p$.

As one might expect, the tame case is straightforward: It is easily seen that if $n \in \mathbb{N}$ is relatively prime to $p$ then there is a unique $k$-isomorphism class of totally ramified extensions $L/K$ of degree $n$. We will focus on ramified extensions of degree $p$, which are the simplest non-tame extensions. Since any two $k$-isomorphic extensions have the same ramification data, it makes sense to classify $k$-isomorphism classes of degree-$p$ extensions with fixed ramification break $b > 0$.

Let $\mathcal{E}_b$ denote the set of all totally ramified subextensions of $K_s/K$ of degree $p$ with ramification break $b$, and let $\mathcal{S}_b$ denote the set of $k$-isomorphism classes of elements of $\mathcal{E}_b$. Let $\mathcal{S}_b^0$ denote the set of $k$-isomorphism classes of Galois extensions in $\mathcal{E}_b$, and let $\mathcal{S}_b^a$ denote the set of $k$-isomorphism classes of non-Galois extensions in $\mathcal{E}_b$. As we will see in Section 2, if $b$ is the ramification break of an extension of degree $p$ then $(p-1)b \in \mathbb{N} \smallsetminus p\mathbb{N}$. Hence $\mathcal{S}_b$ is empty if $b \not\in \frac{1}{p-1} \cdot (\mathbb{N} \smallsetminus p\mathbb{N})$.

**Theorem 1.1.** Let $b \in \frac{1}{p-1} \cdot (\mathbb{N} \smallsetminus p\mathbb{N})$ and write $b = \frac{(m-1)p+1}{p-1}$ with $1 \leq \lambda \leq p-1$. Let $R = \{\omega_i : i \in I\}$ be a set of coset representatives for $k^x/(k^x)^{(p-1)b}$. For each $\omega_i \in R$ let $\pi_i \in K_s$ be a root of the polynomial $X^p - \omega_i \pi_K^m X^\lambda - \pi_K$. Then the map which carries $\omega_i$ onto the $k$-isomorphism class of $K(\pi_i)/K$ gives a bijection from $R$ to $\mathcal{S}_b$. Furthermore, $K(\pi_i)/K$ is Galois if and only if $b \in \mathbb{N} \smallsetminus p\mathbb{N}$ and $\lambda \omega_i \in (k^x)^{p-1}$.

**Corollary 1.2.** Let $b \in \frac{1}{p-1} \cdot (\mathbb{N} \smallsetminus p\mathbb{N})$ and assume that $|k| = q < \infty$. Then

$$|\mathcal{S}_b| = \gcd(q-1, (p-1)b).$$

Furthermore, if $b \in \mathbb{N} \smallsetminus p\mathbb{N}$ then

$$|\mathcal{S}_b^0| = \gcd\left(\frac{q-1}{p-1}, b\right),$$

$$|\mathcal{S}_b^a| = (p-2) \cdot \gcd\left(\frac{q-1}{p-1}, b\right).$$

**Proof.** This follows from Theorem 1.1 and the formulas

$$|k^x/(k^x)^{(p-1)b}| = \gcd(q-1, (p-1)b),$$

$$|(k^x)^{p-1}/(k^x)^{(p-1)b}| = \gcd\left(\frac{q-1}{p-1}, b\right) \quad \text{for} \ b \in \mathbb{N} \smallsetminus p\mathbb{N}.$$ 

The proof of Theorem 1.1 relies heavily on the work of Amano, who showed in [1] that every degree-$p$ extension of a local field of characteristic 0 is generated by a root of an Eisenstein polynomial with a special form, which we call an *Amano polynomial* (see Definition 2.3). In Section 2 we show how Amano’s results can be adapted to the characteristic-$p$ setting. In Section 3 we prove Theorem 1.1 by computing the orbits of the action of $\text{Aut}_k(K)$ on the set of Amano polynomials over $K$. 

2
2. Amano polynomials in characteristic $p$

Let $F$ be a finite extension of the $p$-adic field $\mathbb{Q}_p$ and let $E/F$ be a totally ramified extension of degree $p$. In [1], Amano constructs an Eisenstein polynomial $g(X)$ over $F$ with at most 3 terms such that $E$ is generated over $F$ by a root of $g(X)$. In this section we reproduce a part of Amano’s construction in characteristic $p$. We associate a family of 3-term Eisenstein polynomials to each ramified separable extension of $L/K$ of degree $p$, but we don’t choose representatives for these families. Many of the proofs from [1] remain valid in this new setting.

Let $K$ be a local field of characteristic $p$ with perfect residue field $k$. Let $K_s$ be a separable closure of $K$ and let $\nu_K$ be the valuation of $K_s$ normalized so that $\nu_K(K_s) = \mathbb{Z}$. Fix a prime element $\pi_K$ for $K$; since $k$ is perfect we may identify $K$ with $k((\pi_K))$. Let $U_K$ denote the group of units of $K$, and let $U_{1,K}$ denote the subgroup of 1-units. If $u \in U_{1,K}$ and $\alpha \in \mathbb{Z}_p$ is a $p$-adic integer then $u^\alpha$ is defined as a limit of positive integer powers of $u$. This applies in particular when $\alpha$ is a rational number whose denominator is not divisible by $p$.

Let $L/K$ be a finite totally ramified subextension of $K_s/K$ and let $\nu_L$ be the valuation of $K_s$ normalized so that $\nu_L(L^\times) = \mathbb{Z}$. Let $\pi_L$ be a prime element for $L$ and let $\sigma : L \to K_s$ be a $K$-embedding of $L$ into $K_s$, such that $\sigma \neq \mathrm{id}_L$. We define the ramification number of $\sigma$ to be $\nu_L(\sigma(\pi_L) - \pi_L) - 1$. It is easily seen that this definition does not depend on the choice of $\pi_L$. We say that $b$ is a (lower) ramification break of the extension $L/K$ if $b$ is the ramification number of some nonidentity $K$-embedding of $L$ into $K_s$.

Suppose $L/K$ is a separable totally ramified extension of degree $p$. Then Lemma 1 of [1] shows that $L/K$ has a unique ramification break. Every prime element $\pi_L$ of $L$ is a root of an Eisenstein polynomial

$$f(X) = X^p - \sum_{i=0}^{p-1} c_i X^i$$

over $K$, with $\nu_K(c_0) = 1$ and $\nu_K(c_i) \geq 1$ for $1 \leq i \leq p - 1$. Let $\pi'_L \neq \pi_L$ be a conjugate of $\pi_L$ in $K_s$. Then the ramification break of $L/K$ is given by

$$b = \nu_L \left( \frac{\pi'_L}{\pi_L} - 1 \right).$$

Since $L/K$ is separable, we have $c_i \neq 0$ for some $i$ with $1 \leq i \leq p - 1$. Therefore

$$m = \min\{\nu_K(c_1), \ldots, \nu_K(c_{p-1})\}$$

is finite. Let $\lambda$ be minimum such that $\nu_K(c_\lambda) = m$ and let $\omega \in k^\times$ satisfy $c_\lambda \equiv \omega \pi_K^m \pmod{\pi_K^{m+1}}$. We say that the Eisenstein polynomial $f(X)$ is of type $\langle \lambda, m, \omega \rangle$. Note that while $\omega$ depends on the choice of $\pi_K$, the positive integers $m$ and $\lambda$ do not. If $f(X)$ is of type $\langle \lambda, m, \omega \rangle$ then by Lemma 1 of [1] the ramification break $b$ of $L/K$ is given by

$$b = \frac{(m - 1)p + \lambda}{p - 1}. \quad (2.1)$$
Conversely, given \( b \in \frac{1}{p} \cdot (\mathbb{N} \searrow p\mathbb{N}) \), equation (2.1) uniquely determines \( m \) and \( \lambda \), and we can easily construct Eisenstein polynomials of type \( \langle \lambda, m, \omega \rangle \) for every \( \omega \in k^\times \).

For Eisenstein polynomials \( f(X), g(X) \in K[X] \), write \( f(X) \sim g(X) \) if there is a \( K \)-isomorphism

\[
K[X]/(f(X)) \cong K[X]/(g(X)).
\]

Then \( \sim \) is an equivalence relation on Eisenstein polynomials over \( K \).

**Theorem 2.1.** Suppose \( f(X), g(X) \in K[X] \) are Eisenstein polynomials of degree \( p \) such that \( f(X) \sim g(X) \). Then \( f(X) \) and \( g(X) \) are of the same type.

**Proof.** The proof of Theorem 1 of [1] applies here, except that in characteristic \( p \) we don’t have to consider polynomials of type \( \langle 0 \rangle \).

Henceforth we say that an extension \( L/K \) has type \( \langle \lambda, m, \omega \rangle \) if \( L/K \) is \( K \)-isomorphic to \( K[X]/(f(X)) \) for some Eisenstein polynomial \( f(X) \) of type \( \langle \lambda, m, \omega \rangle \).

**Theorem 2.2.** Let \( L/K \) be an extension of type \( \langle \lambda, m, \omega \rangle \). Then \( L/K \) is Galois if and only if \( b = \frac{(m-1)p+\lambda}{p-1} \) is an integer and \( \lambda \omega \in (k^\times)^{p-1} \).

**Proof.** The proof of Theorem 3(ii) of [1] applies without change.

**Theorem 2.3.** Suppose \( L/K \) is an extension of type \( \langle \lambda, m, \omega \rangle \). Then there exists a prime element \( \pi_L \in L \) which is a root of a polynomial

\[
A_{\omega,u}^b(X) = X^p - \omega \pi_K^m X^\lambda - u \pi_K
\]
for some \( u \in U_{1,K} \).

**Proof.** The proof of Theorem 4 of [1] applies here, except that we don’t have to consider extensions of type \( \langle 0 \rangle \). Briefly, one defines a function \( \phi : L \to K \) by

\[
\phi(\alpha) = \alpha^p - \omega \pi_K^m \alpha^n - N_{L/K}(\alpha),
\]
where \( N_{L/K} \) is the norm from \( L \) to \( K \). Using an iterative procedure one gets a prime element \( \pi \) in \( L \) such that \( \nu_L(\phi(\pi)) > p(\lambda + 1) \) and \( N_{L/K}(\pi) = u \pi_K \) for some \( u \in U_{1,K} \). Let \( \pi^{(1)}, \ldots, \pi^{(p)} \in K_s \) be the roots of \( A_{\omega,u}^b(X) \). Then

\[
\phi(\pi) = A_{\omega,u}^b(\pi) = \prod_{i=1}^p (\pi - \pi^{(i)}), \quad (2.2)
\]
so we have

\[
\sum_{i=1}^p \nu_L(\pi - \pi^{(i)}) = \nu_L(\phi(\pi)) > p(\lambda + 1). \quad (2.3)
\]

Hence \( \nu_L(\pi - \pi^{(j)}) > \lambda + 1 \) for some \( j \), so we get \( L \subset K(\pi^{(j)}) \) by Krasner’s Lemma. Since \( [K(\pi^{(j)}) : K] = [L : K] = p \), it follows that \( L = K(\pi^{(j)}) \). Therefore \( \pi_L = \pi^{(j)} \) satisfies the conditions of the theorem. \( \square \)
**Definition 2.4.** We say that \( A^b_{u,\nu}(X) \) is an *Amano polynomial* over \( K \) with ramification break \( b \).

Let \( b = \frac{(m-1)p+\lambda}{p-1} \) with \( 1 \leq \lambda \leq p-1 \). We denote the set of Amano polynomials over \( K \) with ramification break \( b \) by

\[
\mathcal{P}_b = \{ X^p - \omega \pi_k^m X^\lambda - u \pi_K : \omega \in k^\times, u \in U_{1,K} \}.
\]

Let \( \mathcal{P}_b/\sim \) denote the set of equivalence classes of \( \mathcal{P}_b \) with respect to \( \sim \). For \( f(X) \in \mathcal{P}_b \), we denote the equivalence class of \( f(X) \) by \( [f(X)] \). It follows from Theorem \( 2.3 \) that these equivalence classes are in one-to-one correspondence with the elements of \( \mathcal{E}_b \).

3. The action of \( \text{Aut}_k(K) \) on extensions

In this section we show how \( \text{Aut}_k(K) \) acts on the set of equivalence classes of Amano polynomials with ramification break \( b \). We determine the orbits of this action, and give a representative for each orbit. This allows us to construct representatives for the elements of \( \mathcal{S}_b \), and leads to the proof of Theorem \( 1.1 \).

The following lemma is certainly well-known (see, for instance, the answers to \([10]\)) but we could find no reference for it.

**Lemma 3.1.** Let \( L_1 \) and \( L_2 \) be local fields. Assume that \( L_1 \) and \( L_2 \) have the same residue field \( k \), and that \( k \) is a perfect field of characteristic \( p \). Let \( \sigma : L_1 \to L_2 \) be a field isomorphism. Then \( \nu_{L_2} \circ \sigma = \nu_{L_1} \).

**Proof.** The group \( U_{1,L_1} \) is \( n \)-divisible for all \( n \) prime to \( p \), so we have \( \sigma(U_{1,L_1}) \subset U_{1,L_2} \). For \( i = 1, 2 \) the group \( T_i \) of nonzero Teichmüller representatives of \( L_i \) is equal to \( \bigcap_{n=1}^\infty (L_i^\times)^p \), so we have \( \sigma(T_1) = T_2 \). Since \( U_{L_1} = T_1 \cdot U_{L_1,1} \) this implies \( \sigma(U_{L_1}) \subset U_{L_2} \). The same reasoning shows that \( \sigma^{-1}(U_{L_2}) \subset U_{L_1} \), so we get \( \sigma(U_{L_1}) = U_{L_2} \). It follows that \( \nu_{L_2} \circ \sigma \), like \( \nu_{L_1} \), induces an isomorphism of \( L_1^\times/U_{L_1} \) onto \( \mathbb{Z} \). Let \( \pi_{L_1} \) be a prime element of \( L_1 \). Then \( 1 + \pi_{L_1} \in U_{L_1,1} \), so \( \nu_{L_2}(\sigma(1 + \pi_{L_1})) = 0 \). Hence \( \nu_{L_2}(\sigma(\pi_{L_1})) \geq 0 \). Since \( \nu_{L_2}(\sigma(\pi_{L_1})) \) generates \( \mathbb{Z} \), it follows that \( \nu_{L_2}(\sigma(\pi_{L_1})) = 1 \). We conclude that \( \nu_{L_2} \circ \sigma = \nu_{L_1} \).

For \( f(X) \in K[X] \) and \( \varphi \in \text{Aut}_k(K) \) we let \( f^\varphi(X) \) denote the polynomial obtained by applying \( \varphi \) to the coefficients of \( f(X) \). The following lemma is a straightforward “transport of structure” result:

**Lemma 3.2.** Let \( f(X) \) and \( g(X) \) be Eisenstein polynomials with coefficients in \( K \) such that \( f(X) \sim g(X) \), and let \( \varphi \in \text{Aut}_k(K) \). Then \( f^\varphi(X) \sim g^\varphi(X) \).

Let \( \mathcal{A} = \text{Aut}_k(K) \) denote the group of \( k \)-automorphisms of \( K \). Since all \( k \)-automorphisms of \( K = k((\pi_K)) \) are continuous by Lemma \( 3.1 \) every \( \varphi \in \mathcal{A} \) is determined by the value of \( \varphi(\pi_K) \). Furthermore, \( \mathcal{A} \) acts transitively on the set of prime elements of \( K \). It follows that the group consisting of the power series

\[
\left\{ \sum_{i=1}^{\infty} a_i t^i : a_i \in k, \ a_1 \neq 0 \right\}
\]
with the operation of substitution is isomorphic to the opposite group $\mathcal{A}^{op}$ of $\mathcal{A}$. For every $\varphi \in \mathcal{A}$ there are $l_\varphi \in k^\times$ and $v_\varphi \in U_{1,K}$ such that $\varphi(\pi_K) = l_\varphi \cdot v_\varphi \cdot \pi_K$.

Let

$$\mathcal{N} = \{ \sigma \in \mathcal{A} : \sigma(\pi_K) \in U_{1,K} \cdot \pi_K \}$$

be the group of wild automorphisms of $K$. Then $\mathcal{N}^{op}$ is isomorphic to the Nottingham Group over $k$ (see [4]). Furthermore, $\mathcal{N}$ is normal in $\mathcal{A}$, and $\mathcal{A} / \mathcal{N} \cong k^\times$.

Let $\varphi \in \mathcal{A}$ and let $A^b_{\omega,u}(X) \in \mathcal{B}_b$. Then by Theorem 2.3 there exist $\omega' \in k^\times$ and $u' \in U_{1,K}$ such that

$$K[X]/((A^b_{\omega,u})^\varphi(X)) = K[X]/(X^p - \varphi(\omega \pi_K^m)X^\lambda - \varphi(\pi_K u))$$

$$\cong K[X]/(A^b_{\omega',u'}(X)).$$

It follows from Lemma 3.2 that

$$\varphi \cdot [A^b_{\omega,u}(X)] = [A^b_{\omega',u'}(X)] \quad (3.1)$$

gives a well-defined action of $\mathcal{A}$ on $\mathcal{B}_b / \sim$. The following theorem computes explicit values for $\omega'$ and $u'$ in (3.1). Note that since $k$ is perfect, $l_\varphi$ has a unique $p$th root $l_\varphi^{1/p}$ in $k$.

**Theorem 3.3.** Let $\varphi \in \mathcal{A}$ and $A^b_{\omega,u}(X) \in \mathcal{B}_b$. Then $\varphi[A^b_{\omega,u}(X)] = [A^b_{\omega',u'}(X)]$, with $\omega' = \omega \cdot l_\varphi^{(p-1)/p}$, $u' = \varphi(u) \cdot v_\varphi^p$, and $h = \frac{p - \lambda - pm}{p - \lambda}$.

**Proof.** By applying $\varphi$ to the coefficients of $A^b_{\omega,u}(X)$ we get

$$(A^b_{\omega,u})^\varphi(X) = X^p - \omega l_\varphi^m v_\varphi^m \pi_K^m X^\lambda - \varphi(u) l_\varphi v_\varphi \pi_K.$$

Set $X = l_\varphi^b v_\varphi^{-m} Z$. Then

$$l_\varphi^{-1} v_\varphi^{-m} (A^b_{\omega,u})^\varphi(X) = Z^p - \omega l_\varphi^{(p-1)/p} \pi_K^m Z^\lambda - \varphi(u) l_\varphi^h \pi_K$$

$$= Z^p - \omega \pi_K^m Z^\lambda - u' \pi_K.$$

Since $l_\varphi^b v_\varphi^{-m} \in K$, it follows that

$$K[X]/(A^b_{\omega,u}(X)) \cong K[X]/(A^b_{\omega',u'}(X)).$$

□

To determine the orbit of $[A^b_{\omega,u}(X)]$ under the action of $\mathcal{A}$ we need the following lemmas. Let $\mathbb{Z}_p^\times$ denote the unit group of the ring of $p$-adic integers.

**Lemma 3.4.** Let $u \in U_{1,K}$, and $h \in \mathbb{Z}_p^\times$. Then

$$U_{1,K} = \left\{ \sigma(u) \cdot \left(\frac{\sigma(\pi_K)}{\pi_K}\right)^h : \sigma \in \mathcal{N} \right\}.$$
Proof. Let \( v = u^\frac{1}{h} \in U_{1,K} \). Then \( \pi'_K = v\pi_K \) is a prime element of \( K \). We have

\[
U_{1,K} = \left\{ \frac{v\sigma(\pi'_K)}{\pi_K} : \sigma \in \mathcal{N} \right\}
\]

\[
= \left\{ \frac{\sigma(v\pi_K)}{\pi_K} : \sigma \in \mathcal{N} \right\}
\]

\[
= \left\{ \sigma(u)^\frac{1}{h} \cdot \frac{\sigma(\pi_K)}{\pi_K} : \sigma \in \mathcal{N} \right\}.
\]

Since \( h \in \mathbb{Z}_p^\times \), we have \( U_{h,1,K} = U_{1,K} \). Hence by raising to the power \( h \) we obtain

\[
U_{1,K} = \left\{ \sigma(u) \cdot \left( \frac{\sigma(\pi_K)}{\pi_K} \right)^h : \sigma \in \mathcal{N} \right\}.
\]

Lemma 3.5. Let \( c \in k^\times \) and define \( \tau_c \in \mathfrak{A} \) by \( \tau_c(\pi_K) = c\pi_K \). Let \( \mathcal{N}_c = \mathcal{N}\tau_c \) be the right coset of \( \mathcal{N} \) in \( \mathfrak{A} \) represented by \( \tau_c \). Then for \( u \in U_{1,K} \) and \( h \in \mathbb{Z}_p^\times \) we have

\[
U_{1,K} = \left\{ \varphi(u) \cdot v^h : \varphi \in \mathcal{N}_c \right\}.
\]

Proof. Let \( u' = \tau_c(u) \in U_{1,K} \). Then

\[
\left\{ \varphi(u) \cdot v^h : \varphi \in \mathcal{N}_c \right\} = \left\{ \sigma\tau_c(u) \cdot v^h : \sigma \in \mathcal{N} \right\}
\]

\[
= \left\{ \sigma(u') \cdot v^h : \sigma \in \mathcal{N} \right\}
\]

\[
= U_{1,K},
\]

where the last equality follows from Lemma 3.3.

Theorem 3.6. The orbit of \( [A_{\omega,1,u}(X)] \) under \( \mathfrak{A} \) is

\[
\mathfrak{A} \cdot [A_{\omega,1,u}(X)] = \{ [A_{\omega,\theta,u}(X)] : \theta \in (k^\times)^{(p-1)b}, \ v \in U_{1,K} \}.
\]

Proof. Let \( c \in k^\times \) and \( \varphi \in \mathcal{N}_c \). Then \( l_{\varphi} = c \), so by Theorem 3.3 we have

\[
\varphi \cdot [A_{\omega,1,u}(X)] = [A_{\omega',u'}],
\]

with \( \omega' = \omega c^{\frac{(p-1)b}{p-1}}, u' = \varphi(u)v^h \), and \( h = \frac{p-\lambda-m}{p-1} \). Hence by Lemma 3.5 we have

\[
\mathcal{N}_c \cdot [A_{\omega,1,u}(X)] = \{ [A_{\omega',v'}] : \omega' = \omega c^{\frac{(p-1)b}{p-1}}, v \in U_{1,K} \}.
\]

Since \( \mathfrak{A} \) is the union of \( \mathcal{N}_c \) over all \( c \in k^\times \), and \( k \) is perfect, the theorem follows.

We now give the proof of Theorem 1.1. Let \( R = \{ \omega_i : i \in I \} \) be a set of coset representatives for \( k^\times / (k^\times)^{(p-1)b} \). For each \( \omega_i \in R \) let \( \pi_i \in K^\times \) be a root of the Amano polynomial

\[
A_{\omega_i,1}(X) = X^p - \omega_i \pi_K^m X^\lambda - \pi_K.
\]
It follows from Theorem 3.6 that for every equivalence class $C \in S_k$ there is $i \in I$ such that $K(\pi_i)/K \in C$. On the other hand, if $K(\pi_i)/K$ is $k$-isomorphic to $K(\pi_j)/K$ then by Theorem 3.3 for some $\varphi \in \mathcal{A}$ we have
\[ [A^b_{\omega_j,1}(X)] = \varphi \cdot [A^b_{\omega_i,1}(X)] = [A^b_{\omega_i,1}(X)]. \]
with $\omega'_j = \omega_j l_{\varphi} \cdot p^b$. It follows from Theorem 2.1 that $A^b_{\omega_j,1}(X)$ and $A^b_{\omega_i,1}(X)$ have the same type, so we have $\omega_j = \omega_i l_{\varphi} \cdot p^b$. Since $\omega_i$ and $\omega_j$ are coset representatives for $k^\times/(k^\times)^{(p-1)b}$, we get $\omega_i = \omega_j$. This proves the first part of Theorem 1.1. The second part follows from Theorem 2.2.

**Remark 3.7.** In [4], Klopsch uses a different method to compute the cardinality of $S_k$. Let $L = k((\pi^\infty))$ be a local function field with residue field $k$, and set $\mathcal{F} = \text{Aut}_k(L)$. Then there is a one-to-one correspondence between cyclic subgroups $G \leq \mathcal{F}$ of order $p$ and subfields $M = L^G$ of $L$ such that $L/M$ is a cyclic totally ramified extension of degree $p$. For $i = 1, 2$ let $G_i$ be a cyclic subgroup of $\mathcal{F}$ of order $p$ and set $K_i = L^{G_i}$. Say the extensions $L/K_1$ and $L/K_2$ are $k^\times$-isomorphic if there exists $\eta \in \mathcal{F} = \text{Aut}_k(L)$ such that $\eta(K_1) = K_2$; this is equivalent to $\eta^{-1}G_1 \eta = G_2$.

For $i = 1, 2$ let $\psi_i : K \to L$ be a $k$-linear field embedding such that $\psi_i(K) = K_i$. We can use $\psi_i$ to identify $K$ with $K_i$, which makes $L$ an extension of $K$. We easily see that the extensions $\psi_1 : K \hookrightarrow L$ and $\psi_2 : K \hookrightarrow L$ are $k$-isomorphic if and only if $L/K_1$ and $L/K_2$ are $k^\times$-isomorphic. Therefore classifying $k$-isomorphism classes of degree-$p$ Galois extensions of $K$ is equivalent to classifying conjugacy classes of subgroups of order $p$ in $\mathcal{F}$.

For $i = 1, 2$ let $G_1 = \langle \gamma_i \rangle$. If $G_1$ and $G_2$ have ramification break $b$ then
\[
\begin{align*}
\gamma_1(\pi_L) &\equiv \pi_L + r_{b+1}\pi_L^{b+1} \pmod{\pi_L^{b+2}} \\
\gamma_2(\pi_L) &\equiv \pi_L + s_{b+1}\pi_L^{b+1} \pmod{\pi_L^{b+2}}
\end{align*}
\]
for some $r_{b+1}, s_{b+1} \in k^\times$. Hence for $1 \leq j \leq p - 1$, we have
\[
\gamma_j^i(\pi_L) \equiv \pi_L + jr_{b+1}\pi_L^{b+1} \pmod{\pi_L^{b+2}}.
\]
By Proposition 3.3 of [4], $\gamma_1^i$ and $\gamma_2$ are conjugate in $\mathcal{F}$ if and only if $s_{b+1} = jtr_{b+1}^{-1}1^b$, for some $t \in k^\times$. Therefore the subgroups $G_1$ and $G_2$ are conjugate in $\mathcal{F}$ if and only if $s_{b+1} \equiv r_{b+1}^{-1}\pi_L^{-b} \cdot (k^\times)^{b}$. It follows that the number of conjugacy classes of subgroups of order $p$ with ramification break $b$ is
\[
|k^\times/(\pi_L^{-b} \cdot (k^\times)^b)| = |(k^\times)^{p-1}/(k^\times)^{(p-1)b}|.
\]
In particular, if $|k| = q < \infty$ then there are $\gcd\left(\frac{q-1}{p-1}, b\right)$ such conjugacy classes, in agreement with Corollary 1.2.
References

[1] Shigeru Amano, Eisenstein equations of degree p in a p-adic field, J. Fac. Sci. Univ. Tokyo Sect. IA Math. 18 (1971), 1–21.

[2] Ivan Fesenko and Sergei Vostokov, Local Fields and Their Extensions, Translation of Mathematical Monographs V. 121, (AMS, 2002).

[3] Kevin Keating, Automorphisms of k((X)),
http://mathoverflow.net/questions/193757 (2015).

[4] Benjamin Klopsch, Automorphisms of the Nottingham Group, Journal of Algebra 223 (2000) 37–56.

[5] Marc Krasner, Nombre des extensions d’un degré donné d’un corps p-adique. (French) 1966 Les Tendances Géom. en Algèbre et Théorie des Nombres pp. 143–169 Editions du Centre National de la Recherche Scientifique, Paris.

[6] Maurizio Monge, Determination of the number of isomorphism classes of extensions of a p-adic field. J. Number Theory 131 (2011), no. 8, 1429–1434.