Department of Mathematics
University of Florida

Enumerating k-isomorphism classes of totally ramified degree-p extensions of the local field $k((\pi))$

Duc Van Huynh

May 19, 2014

Sources

- Shigeru Amano, Eisenstein equations of degree p in a p-adic field, J. Fac. Sci. Univ. Tokyo Sect. IA Math. 18 (1971), 1-21
- Ivan Fesenko and Sergei Vostokov, Local Fields and Their Extensions, Translation of Mathematical Monographs V. 121, (AMS, 2002)
- Benjamin Klopsch, Automorphisms of the Nottingham Group, Journal of Algebra 223 (2000) 37-56

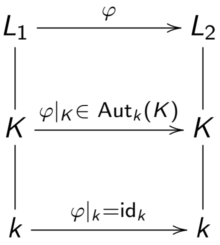
Enumeration of Isomorphism Classes

Statement of the problem

1. Let K be a local field of characteristic p with residue field k of order q, where q is p-power.
2. Let E_λ be the set of all totally ramified extensions L/K of degree p in K_s with ramification break λ.
3. Say $L_1/K, L_2/K$ are k-isomorphic if there exists an isomorphism $\varphi : L_1 \to L_2$ such that $\varphi(K) = K$ and φ is the identity on k.
4. We would like to enumerate the k-isomorphism classes of E_λ.

Enumeration of Isomorphism Classes

$$L_1/K \cong_k L_2/K$$



Enumeration of Isomorphism Classes

Theorem

Let $\lambda \in \frac{1}{p-1}\mathbb{N}$, and let d be the denominator of λ when it is in reduced form. Define $\mathcal{S}_\lambda$ to be the set of k-isomorphism classes of E_λ. Then we have

$$|\mathcal{S}_\lambda| = (p-1)\gcd\left(\frac{q-1}{p-1}, d\lambda\right).$$

Enumeration of Isomorphism Classes

Theorem

Define $\mathcal{S}_\lambda^g$ (resp. $\mathcal{S}_\lambda^{ng}$) to be the set of k-isomorphism classes of degree p totally ramified Galois (resp. non-Galois) extensions with ramification break λ. Then, if λ is an integer, we have

(i) $\left|\mathcal{S}_\lambda^g\right| = \gcd\left(\frac{q-1}{p-1}, \lambda\right)$ and

(ii) $|\mathcal{S}_\lambda^{ng}| = (p-2)\gcd\left(\frac{q-1}{p-1}, \lambda\right)$, while

(iii) $|\mathcal{S}_\lambda^{ng}| = (p-1)\gcd\left(\frac{q-1}{p-1}, d\lambda\right)$ if λ is not an integer.

Outline of Attack on the Problem

Group of automorphisms

1. Let $A = \text{Aut}_k(K)$.
2. Let $U_{1,K} = 1 + \pi_K O_K$, where π_K is a prime element of K.
3. $\varphi \in A$ is defined by its action on π_K.
4. $\varphi(\pi_K) = av_\varphi \pi_K$, where $a \in k^\times$ and $v_\varphi \in U_{1,K}$.

Outline of Attack on the Problem

Strategy of attack

1. Find an Eisenstein polynomial in a *standard form* corresponding to each $L/K \in E_\lambda$. Let P_λ be the set of all such Eisenstein polynomials.
2. For $f(X), g(X) \in P_\lambda$, we denote $f(X) \sim g(X)$ if $K[X]/(f(X)) \cong K[X]/(g(X))$.
3. Let $\varphi \in A$ and $f(X) = X^p + a_{p-1}X^{p-1} + \cdots + a_1X + a_0$. Define

$$\varphi(f(X)) = X^p + \varphi(a_{p-1})X^{p-1} + \ldots + \varphi(a_1)X + \varphi(a_0).$$

4. Enumerating the k-isomorphism classes of E_λ is equivalent to enumerating the orbits of the action of A on $P_\lambda/\sim$.

The Work of Amano

Invariants of L/K

1. A prime element $\pi_L \in L$ satisfies an Eisenstein polynomial
$$f(X) = X^p - \sum_{i=1}^{p-1} a_i X^i - \pi_K a_0, \text{ with } a_0 \in U_{1,K}.$$
2. Set $m = \min\{\nu_K(a_1), \ldots, \nu_K(a_{p-1})\}$, where ν_K is the valuation of K_s such that $\nu_K(\pi_K) = 1$. Denote by n the least positive integer such that $\nu_K(a_n) = m$. Let $\omega \in k^\times$ be such that $\nu_K(a_n - \omega\pi_K^m) > \nu_K(a_n)$.
3. n, m, ω are invariants of L/K. We say that L/K has type (n, m, ω).
4. We can write $\lambda = \dfrac{(m-1)p + n}{p-1}$, where $1 \leq n \leq p - 1$.

The Work of Amano

$L \cong K[X]/(A_{\omega,u}(X))$, where $A_{\omega,u}(X) = X^p - \omega\pi_K^m X^n - u\pi_K$, where $u \in U_{1,K}$ and $\omega \in k^\times$.

5. For each prime element π of L, define $\psi(\pi) = \pi^p - \omega\pi_K^m \pi^n - N_{L/K}(\pi)$.
6. Let ν_L be the valuation of K_s normalized on L. If $\psi(\pi_1) \neq 0$, then there exists a prime element π_2 of L such that $\nu_L(\psi(\pi_2)) > \nu_L(\psi(\pi_1))$.
7. Let $\pi \in L$ be such that $\nu_L(\pi) > p(\lambda + 1)$. Let $\pi_K a = N_{L/K}(\pi)$ for some $a \in U_{1,K}$.
8. For $1 \leq i \leq p$, let $\pi^{(i)}$ be the roots of $A_{\omega,a}(X) = X^p - \omega\pi_K^m X^n - \pi_K a$. Then we find that $\nu_L(\pi - \pi^{(j)}) > \lambda + 1$ for some j. It follows that $L = K(\pi^{(j)})$ by Krasner's Lemma.

The Work of Amano

L/K is Galois if and only λ is an integer and $n\omega \in (k^\times)^{p-1}$.

1. We show that if λ is an integer, then L/K is Galois exactly when $n\omega \in (k^\times)^{p-1}$.
2. Write $L = K(\pi_1)$, where π_1 is a root of the Amano polynomial $A_{\omega,u}(X)$. Let $\pi_2 \neq \pi_1$ be a conjugate of π_1. We can write $\pi_2 = \pi_1(1 + \pi_1^\lambda Y)$ for some unit $Y \in K_s$.
3. $\pi_2 \in L$ exactly when $Y \in L$.
4. Using the fact that π_1, π_2 are roots of $A_{\omega,u}(X)$, we find that $Y^p - \sum_{i=1}^p \binom{n}{i} \omega \pi_K^m \pi_1^{\lambda(i-1)-pm} Y^i = 0$.
5. We find that $Y^p - n\omega Y \equiv 0 \pmod{\pi_1}$.

Action on Amano Polynomials

Outline of proof

1. Let $P_\lambda = \{X^p - \omega\pi_K^m X^n - u\pi_K : \omega \in k^\times, u \in U_{1,K}\}$.
2. Let $\varphi \in A$ and let $A_{\omega,u}(X) = X^p - \omega\pi_K^m X^n - u\pi_K \in P_\lambda$.
3. There exist ω', u' such that
$$K[X]/(\varphi(A_{\omega,u}(X)) \cong K[X]/(A_{\omega',u'}(X)).$$
4. Define action of A on $P_\lambda/\sim$ by
$$\varphi \cdot [A_{\omega,u}(X)] = [A_{\omega',u'}(X)].$$

Action on Amano Polynomials

Outline of proof

5 We find that

$$A_{\omega,u}(X) \sim A_{\omega a^{(p-1)\lambda},v}(X),$$

for all $a \in k^\times$ and $v \in U_{1,K}$.

6 Let

$$\{r_1, r_2, \ldots, r_{p-2}, r_{p-1}\}$$

be a set of representatives of $k^\times/(k^\times)^{p-1}$. Assume without loss of generality that $r_1 = 1$.

7 Write $n\omega = r_i t^{p-1}$, for some r_i and $t \in k^\times$.

8 Recall that L/K is Galois if and only λ is an integer and $n\omega \in (k^\times)^{p-1}$.

Action on Amano Polynomials

Outline of proof

9. Cardinality of $\mathcal{S}_\lambda^g$ for $\lambda \in \mathbb{Z}$.
   (a) If $r_i \neq 1$, then $n\omega \notin (k^\times)^{p-1}$, which implies L/K not Galois.
   (b) Hence, $r_i = 1$.
   (c) $|\mathcal{S}_\lambda^g| = |(k^\times)^{p-1}/(k^\times)^{\lambda(p-1)}|$.
10. Cardinality of $\mathcal{S}_\lambda^{ng}$ for $\lambda \in \mathbb{Z}$.
    (a) We want $r_i \neq 1$, else $n\omega \in (k^\times)^{p-1}$, which implies L/K is Galois.
    (b) There are $p-2$ choices for r_i.
    (c) $|\mathcal{S}_\lambda^{ng}| = (p-2)|(k^\times)^{p-1}/(k^\times)^{\lambda(p-1)}|$.
11. Cardinality of $\mathcal{S}_\lambda^{ng}$ for $\lambda \notin \mathbb{Z}$.
    (a) There are $p-1$ choices for r_i.
    (b) $|\mathcal{S}_\lambda^{ng}| = (p-1)|(k^\times)^{p-1}/(k^\times)^{\lambda(p-1)}|$.