Wild ramification in number field extensions of prime degree

By

Darrin Doud

Abstract. We show that if L/K is a degree p extension of number fields which is wildly ramified at a prime $\mathfrak{p}$ of K of residue characteristic p, then the ramification groups of $\mathfrak{p}$ (in the splitting field of L over K) are uniquely determined by the $\mathfrak{p}$-adic valuation of the discriminant of L/K.

1. Introduction. Although the relative discriminant of an extension of number fields depends on the ramification in the extension and can be determined by studying the ramification in the Galois closure of the extension, in general, the ramification is not uniquely determined by the discriminant. In this note we show that in certain cases it is possible to determine wild ramification (including the filtration of higher ramification subgroups) in terms of the relative discriminant. The relationship between the discriminant and the ramification subgroups is in fact given (for the fields which we consider) by a simple formula.

Let $\Delta_{L/K}$ denote the relative discriminant of a extension L/K of number fields. We prove the following theorem (using the notation defined in Section 2):

Theorem 1. *Let L/K be a degree p extension of number fields, and let $\mathfrak{p}$ be a prime of K lying over $p \in \mathbb{Q}$. Suppose that $\mathfrak{p}$ is wildly ramified in L/K. Let $n = v_{\mathfrak{p}}(\Delta_{L/K})$. Then there are integers d and t such that*

$$|G_{i,\mathfrak{p}}| = \begin{cases} pt & \text{if } i = 0 \\ p & \text{if } 0 < i \leq d \\ 1 & \text{if } i > d \end{cases},$$

with $n = (p-1)(1 + d/t)$, and $(d,t) = 1$.

We note that due to the condition that $(d,t) = 1$, the integers d and t are in fact uniquely defined in terms of n as

$$d = \frac{n-(p-1)}{(n,p-1)}, \quad \text{and} \quad t = \frac{p-1}{(n,p-1)}.$$

We prove the theorem in two parts–in Section 3 we prove the formula for n in terms of d and t, and in Section 4 we prove that d and t are relatively prime.

2. Ramification groups. Let M denote the Galois closure of L/K. Then we know that $\mathrm{Gal}(M/K)$ is a subgroup of S_p. Choose a prime $\mathfrak{P}|\mathfrak{p}$, and define the ramification groups

$$G_{i,\mathfrak{p}} = \{\sigma \in \mathrm{Gal}(M/K) : v_{\mathfrak{P}}(\sigma(\alpha) - \alpha) \geq i + 1 \text{ for all } \alpha \in M\}.$$

1991 *Mathematics Subject Classification.* 11R29,11S15.

This research was partially supported by an NSF postodoctoral research fellowship.

Note that although the groups $G_{i,\mathfrak{p}}$ depend on the choice of $\mathfrak{P}$, their order does not. In fact, changing the choice of $\mathfrak{P}$ has the effect of conjugating the $G_{i,\mathfrak{p}}$. Denote by e the order of $G_{0,\mathfrak{p}}$ (the ramification index), by f the inertial degree of any prime of M lying over $\mathfrak{p}$, and by g the number of primes of M lying over $\mathfrak{p}$.

It is well known that $G_{i,\mathfrak{p}}$ is normal in $G_{0,\mathfrak{p}}$ for all i, and that $G_{1,\mathfrak{p}}$ is the p-Sylow subgroup of $G_{0,\mathfrak{p}}$. Since p exactly divides the order of S_p, the only possible orders for $G_{i,\mathfrak{p}}$ with $i > 0$ are 1 and p. Hence, if we determine the last nontrivial $G_{i,\mathfrak{p}}$, and the order of $G_{0,p}$, then we have fully determined the filtration of ramification subgroups. This shows that determining d and t as described in the theorem does determine the ramification filtration.

We further note that the inertia group $G_{0,\mathfrak{p}}$ must be not only a subgroup of S_p, but also a subgroup of the normalizer $N_{S_p}(G_{1,\mathfrak{p}})$. Since $\mathfrak{p}$ is assumed to be wildly ramified in L, the order of $G_{1,\mathfrak{p}}$ must be p, and as a subgroup of S_p it is generated by a p-cycle τ. The normalizer of $\langle\tau\rangle$ in S_p is metacyclic, and is generated by τ and a $(p-1)$-cycle ψ. For each k dividing $p-1$, there is a unique subgroup of this normalizer of order pk, and this subgroup is generated by τ and $\psi^{(p-1)/k}$. Finally, note that the action of $\langle\psi\rangle$ on $\langle\tau\rangle$ is faithful, so that the only power of ψ which fixes τ is the identity.

3. Different calculations. Let L/K be an extension of number fields satisfying the conditions of the theorem, and let M be the Galois closure of L over K. Note that there is a unique prime $\mathfrak{P}$ of L lying over $\mathfrak{p}$. Since the degree of M/L is prime to p, $\mathfrak{P}$ is tamely ramified in M/L. By [2, Chapter IV, Prop. 4], we have that the relative different $\mathcal{D}_{M/L}$ satisfies

$$v_P(\mathcal{D}_{M/L}) = t-1,$$

where P is any prime of M lying over $\mathfrak{P}$. Then

$$v_{\mathfrak{P}}(\Delta_{M/L}) = v_{\mathfrak{P}}(N_{M/L}(\mathcal{D}_{M/L})) = fg(t-1).$$

Similarly, we have that

$$v_P(\mathcal{D}_{M/K}) = (e-1)+d(p-1),$$

so that

$$v_{\mathfrak{p}}(\Delta_{M/K}) = fg((e-1)+d(p-1)).$$

Using the relationship [1, Theorem 2.5.1]

$$\Delta_{M/K} = \Delta_{L/K}^{[M:L]} N_{L/K}(\Delta_{M/L})$$

and the fact that the norm (from L to K) of $\mathfrak{P}$ is $\mathfrak{p}$, we find, by taking p-adic valuations, that

$$fg((e-1)+d(p-1)) = \frac{efg}{p}n + fg(t-1).$$

Solving for n gives

$$n = (p-1)(1+d/t),$$

as desired.

4. Action of tame ramification on wild ramification. It remains to show that $(d,t)=1$. In order to show this, we require several additional results concerning ramification groups [2, Chapter IV, Section 2].

First, there is an injective homomorphism

$$\theta_0 : G_{0,\mathfrak{p}}/G_{1,\mathfrak{p}} \to \bar{\mathbb{F}}_p^\times,$$

so that in particular, $G_{0,\mathfrak{p}}/G_{1,\mathfrak{p}}$ is cyclic. Let ψ be a generator. In addition, for each $i>0$, there is a homomorphism

$$\theta_i : G_{i,\mathfrak{p}}/G_{i+1,\mathfrak{p}} \to \bar{\mathbb{F}}_p^\times.$$

Finally, there is a compatibility between θ_0 and θ_i, such that for $s \in G_{0,\mathfrak{p}}$ and $t \in G_{i,\mathfrak{p}}/G_{i+1,p}$, we have

$$\theta_i(sts^{-1}) = \theta_0(s)^i \theta_i(t).$$

Note that if we take $i=d$ to be the depth of the filtration, $G_{i+1,\mathfrak{p}}$ is trivial, so that we may identify $G_{d,\mathfrak{p}}$ (a multiplicative group) with its image under θ_d (an additive group). Hence, the compatibility condition above shows that for $t \in G_{d,\mathfrak{p}}$,

$$sts^{-1} = t^{\theta_0(s)^d}.$$

We now let σ and τ be generators of $G_{0,\mathfrak{p}}$, as described previously, so that τ is a p-cycle, σ is a power of a $(p-1)$-cycle, and the only power of σ which fixes τ is the identity. Then τ is an element of $G_{i,p}$ for any $1 \le i \le d$, and σ is a generator of $G_{0,\mathfrak{p}}/G_{1,\mathfrak{p}}$. Note that we may in fact identify $G_{d,\mathfrak{p}}$ with the image of θ_d, since $G_{d+1,\mathfrak{p}}$ is trivial.

We then have that

$$\theta_d(\sigma\tau\sigma^{-1}) = \theta_d(\tau)^{\theta_0(\sigma)^d},$$

which reduces to

$$\sigma\tau\sigma^{-1} = \tau^{\theta_0(\sigma)^d}$$

Now since the action of σ on $\langle\tau\rangle$ is faithful, we must have $\sigma\tau\sigma^{-1} = \tau^k$ with k of order t in $(\mathbb{Z}/p\mathbb{Z})^\times$. This implies that $\theta_0(\sigma)^d$ has order t, and since $\theta_0(\sigma)$ has order t, it also implies that $(d,t)=1$ (because $\theta_0(\sigma)^d$ has order $t/(d,t)$).

5. Remarks. For a fixed ground field, one may use a simple bound on wild ramification subgroups [2, pg. 72] and the fact that t is at most $p-1$ to compile a list of all the possible ramification structures for the types of extensions dealt with in this theorem. We also note that the theorem also holds (with the same proof) for extensions of local fields.

References

[1] Henri Cohen, *Advanced topics in computational number theory*, Graduate Texts in Mathematics, vol. 193, Springer-Verlag, New York-Berlin, 1999.

[2] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York-Berlin, 1979.

Anschrift des Autors:

Darrin Doud
Brigham Young University
Department of Mathematics
292 TMCB
Provo, UT 84602
E-mail address: doud@math.byu.edu