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 $p$ of $K$ of residue characteristic $p$, then the ramification groups of $p$ (in the splitting field of $L$ over $K$) are uniquely determined by the $p$-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 an 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 $n = v_p(\Delta_{L/K})$. Then there are integers $d$ and $t$ such that

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

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


This research was partially supported by an NSF postdoctoral research fellowship.
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 $\text{Gal}(M/K)$ is a subgroup of $S_p$. Choose a prime $\mathfrak{P} | p$, and define the ramification groups

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

Note that although the groups $G_{i,p}$ 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 $G_{i,p}$. Denote by $e$ the order of $G_{0,p}$ (the ramification index), by $f$ the inertial degree of any prime of $M$ lying over $p$, and by $g$ the number of primes of $M$ lying over $p$.

It is well known that $G_{i,p}$ is normal in $G_{0,p}$ for all $i$, and that $G_{1,p}$ is the $p$-Sylow subgroup of $G_{0,p}$. Since $p$ exactly divides the order of $S_p$, the only possible orders for $G_{i,p}$ with $i > 0$ are 1 and $p$. Hence, if we determine the last nontrivial $G_{i,p}$, and the order of $G_{0,p}$, then we have fully determined the filtration of ramification subgroups. Defining $d$ as the smallest integer such that $|G_{i,p}| = 1$ for $i > d$, and $t$ as the prime to $p$ part of the order of $G_{0,p}$, we then see that $d$ and $t$ uniquely determine the ramification filtration. To prove the theorem, it remains to show that $(d, t) = 1$, and that $v_p(\Delta_{L/K}) = n = (p - 1)(1 + d/t)$.

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

\[v_p(D_{M/L}) = t - 1,
\]

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

\[v_p(\Delta_{M/L}) = v_p(\Delta_{M/L}(D_{M/L})) = fg(t - 1).
\]

Similarly, we have that

\[v_p(D_{M/K}) = (e - 1) + d(p - 1),
\]