DISCRIMINANTS AND RAMIFIED PRIMES

KEITH CONRAD

1. Introduction

A prime number $p$ is said to be ramified in a number field $K$ if the prime ideal factorization

\[(p) = p\mathcal{O}_K = p_{1}^{e_1} \cdots p_{g}^{e_g}\]

has some $e_i$ greater than 1. If every $e_i$ equals 1, we say $p$ is unramified in $K$.

Example 1.1. In $\mathbb{Z}[i]$, the only prime which ramifies is 2: $(2) = (1 + i)^2$.

Example 1.2. Let $K = \mathbb{Q}(\alpha)$ where $\alpha$ is a root of $f(X) = T^3 - 9T - 6$. Then $6 = \alpha^3 - 9\alpha = \alpha(\alpha - 3)(\alpha + 3)$. For $m \in \mathbb{Z}$, $\alpha + m$ has minimal polynomial $f(T - m)$ in $\mathbb{Q}[T]$, so $N_{K/\mathbb{Q}}(\alpha + m) = -f(-m) = m^3 - 9m + 6$ and the principal ideal $(\alpha - m)$ has norm $N(\alpha - m) = |m^3 - 9m + 6|$.

Therefore $N(\alpha) = 6$, $N(\alpha - 3) = 6$, and $N(\alpha + 3) = 6$. It follows that $(\alpha) = p_2 p_3$, $(\alpha - 3) = p_2^2 p_3$, and $(\alpha + 3) = p_2 p_3^2$ (so, in particular, $\alpha + 3$ and $\alpha - 3$ are unit multiples of each other). Thus

\[(2)(3) = (6) = (\alpha)(\alpha - 3)(\alpha + 3) = p_2 p_2^2 p_3^2,
\]

so $(2) = p_2^3 p_3^2$ and $(3) = p_3^3$. This shows 2 and 3 are ramified in $K$. Note that one of the exponents in the factorization of $(2)$ exceeds 1, while the other equals 1.

One way to think about ramified primes is in terms of the ring structure of $\mathcal{O}_K/(p)$. By (1.1) and the Chinese Remainder Theorem,

\[(1.2) \quad \mathcal{O}_K/(p) \cong \mathcal{O}_K/p_{1}^{e_1} \times \cdots \times \mathcal{O}_K/p_{g}^{e_g}.\]

If some $e_i$ is greater than 1, then the quotient ring $\mathcal{O}_K/p_i^{e_i}$ has a nonzero nilpotent element (use the reduction modulo $p_i^{e_i}$ of any element of $p_i - p_i^{e_i}$), so the product ring (1.2) has a nonzero nilpotent element. If each $e_i$ equals 1, then $\mathcal{O}_K/(p)$ is a product of (finite) fields, and a product of fields has no nonzero nilpotent elements. Thus, $p$ ramifies in $K$ if and only if $\mathcal{O}_K/(p)$ has a nonzero nilpotent element.

Our goal in this handout is to prove the following result, which characterizes the prime numbers ramifying in a number field in terms of the discriminant.

Theorem 1.3. For a number field $K$, the primes which ramify are those dividing the integer $\text{disc}_\mathbb{Z}(\mathcal{O}_K)$.

Since $\text{disc}_\mathbb{Z}(\mathcal{O}_K) \neq 0$, only finitely many primes ramify in $K$. 

2. The power-basis case

We will first consider Theorem 1.3 when \( \mathcal{O}_K \) has a power basis over \( \mathbb{Z} \). The treatment of the general case in Section 3 will not rely on the power-basis case at all, but the power-basis case is technically simpler. We will just sketch the basic ideas behind this special case.

**Proof.** Assume \( \mathcal{O}_K = \mathbb{Z}[\alpha] \) for some \( \alpha \in \mathcal{O}_K \). Let \( f(T) \) be the minimal polynomial of \( \alpha \) over \( \mathbb{Q} \), so \( f(T) \) is monic in \( \mathbb{Z}[T] \). With \( p\mathcal{O}_K \) factoring into primes as in (1.1), by definition \( p \) ramifies in \( \mathcal{O}_K \) if and only if some \( e_i > 1 \). The factorization of the mod \( p \) reduction \( \bar{f}(T) \) in \( (\mathbb{Z}/p\mathbb{Z})[T] \) is

\[
\bar{f}(T) = \pi_1^{e_1} \cdots \pi_g^{e_g}
\]

for some distinct monic irreducibles \( \pi_i \in (\mathbb{Z}/p\mathbb{Z})[T] \).

The \( \pi_i(T) \)'s are separable (all irreducibles over a finite field are separable), so some \( e_i > 1 \) if and only if \( \bar{f}(T) \) has a repeated root in a splitting field over \( \mathbb{Z}/p\mathbb{Z} \). This is equivalent to \( \bar{f}(T) \) having discriminant 0: \( p \) ramifies in \( \mathcal{O}_K \) if and only if \( \text{disc}(\bar{f}) = 0 \) in \( \mathbb{Z}/p\mathbb{Z} \). Since the discriminant of a monic polynomial is a universal polynomial in its coefficients (consider the quadratic case, where \( T^2 + bT + c \) has discriminant \( b^2 - 4c \)), discriminants of monic polynomials behave well under reduction: \( \text{disc}(f(T) \mod p) = \text{disc}(\bar{f}(T)) \mod p \). Therefore \( \text{disc}(\bar{f}(T)) = 0 \) in \( \mathbb{Z}/p\mathbb{Z} \) if and only if \( \text{disc}(f) \equiv 0 \mod p \). Thus \( p \) ramifies in \( \mathcal{O}_K \) if and only if \( p|\text{disc}(f) \). Since \( \mathcal{O}_K = \mathbb{Z}[\alpha] \cong \mathbb{Z}[T]/(f(T)) \), \( \text{disc}(f) = \text{disc}_{\mathbb{Z}}(\mathbb{Z}[T]/(f)) = \text{disc}_{\mathbb{Z}}(\mathcal{O}_K) \). \( \square \)

3. The general case

To prove Theorem 1.3 for every \( \mathcal{O}_K \), we will examine discriminants of ring extensions to show computing the discriminant commutes with reduction mod \( p \): \( \text{disc}_{\mathbb{Z}}(\mathcal{O}_K) \mod p = \text{disc}_{\mathbb{Z}/p\mathbb{Z}}(\mathcal{O}_K/\mathcal{O}_K^{(p)}) \). Then we will use (1.2) to write \( \text{disc}_{\mathbb{Z}/p\mathbb{Z}}(\mathcal{O}_K/\mathcal{O}_K^{(p)}) \) as a product of discriminants of rings of type \( \mathcal{O}_K/p^e \) and compute the discriminants of these particular rings.

**Definition 3.1.** Let \( A \) be a commutative ring and \( B \) be a ring extension of \( A \) which is a finite free \( A \)-module:

\[
B = Ae_1 \oplus \cdots \oplus Ae_n.
\]

Then we set

\[
\text{disc}_A(e_1, \ldots, e_n) = \det(\text{Tr}_{B/A}(e_ie_j)) \in A.
\]

**Remark 3.2.** The discriminant of a basis is an algebraic concept of “volume”. To explain this viewpoint, we should think about \( \text{Tr}_{B/A}(xy) \) as an analogue of the dot product \( v \cdot w \) in \( \mathbb{R}^n \). For a basis \( v_1, \ldots, v_n \) in \( \mathbb{R}^n \), the ordinary Euclidean volume of the parallelopotope

\[
\left\{ \sum_{i=1}^n a_i v_i : 0 \leq a_i \leq 1 \right\}
\]

having edges \( v_i \) is \( \sqrt{|\det(v_i \cdot v_j)|} \). The discriminant of an \( A \)-basis of \( B \) uses the \( A \)-valued pairing \( \langle x, y \rangle = \text{Tr}_{B/A}(xy) \) on \( B \) in place of the \( \mathbb{R} \)-valued dot product on \( \mathbb{R}^n \) and we just drop the absolute value and the square root when we make the algebraic analogue.

How are the discriminants of two \( A \)-module bases for \( B \) related? Pick a second basis \( e'_1, \ldots, e'_n \) of \( B \) as an \( A \)-module. Then

\[
e'_i = \sum_{j=1}^n a_{ij}e_j,
\]
where \(a_{ij} \in A\) and the change of basis matrix \((a_{ij})\) has determinant in \(A^\times\). Then

\[
\text{Tr}_{B/A}(e'_i e'_j) = \text{Tr}_{B/A} \left( \sum_{k=1}^{n} a_{ik} e_k \sum_{\ell=1}^{n} a_{j\ell} e_\ell \right) = \sum_{k=1}^{n} \sum_{\ell=1}^{n} a_{ik} \text{Tr}_{B/A}(e_k e_\ell) a_{j\ell},
\]

so

\[
(\text{Tr}_{B/A}(e'_i e'_j)) = (a_{ij})(\text{Tr}_{B/A}(e_i e_j))(a_{ij})^T.
\]

Therefore

\[
\text{disc}_A(e'_1, \ldots, e'_n) = (\det(a_{ij}))^2 \text{disc}_A(e_1, \ldots, e_n).
\]

We set

\[
\text{disc}_A(B) = \text{disc}_A(e_1, \ldots, e_n) \in A
\]

for any \(A\)-module basis \(\{e_1, \ldots, e_n\}\) of \(B\). It is well-defined up to a unit square. In particular, the condition \(\text{disc}_A(B) = 0\) is independent of the choice of basis.

Given a number field \(K\), ramification of the prime \(p\) in \(K\) has been linked to the structure of the ring \(\mathcal{O}_K/(p)\) in Section 1. Let’s look at the discriminant of this ring over \(\mathbb{Z}/p\mathbb{Z}\). Letting \(K\) have degree \(n\) over \(\mathbb{Q}\), the ring \(\mathcal{O}_K\) is a free rank-\(n\) \(\mathbb{Z}\)-module, say \(\mathcal{O}_K = \bigoplus_{i=1}^{n} \mathbb{Z}\omega_i\).

Reducing both sides modulo \(p\),

\[
\mathcal{O}_K/(p) = \bigoplus_{i=1}^{n} (\mathbb{Z}/p\mathbb{Z})\overline{\omega}_i,
\]

so \(\mathcal{O}_K/(p)\) is a vector space over \(\mathbb{Z}/p\mathbb{Z}\) of dimension \(n\). The discriminant of \(\mathcal{O}_K\) is \(\text{disc}_{\mathbb{Z}}(\mathcal{O}_K)\).

The next lemma says reduction modulo \(p\) commutes (in a suitable sense) with the formation of discriminants.

**Lemma 3.3.** Choosing bases appropriately for \(\mathcal{O}_K\) and \(\mathcal{O}_K/(p)\),

\[
\text{disc}_{\mathbb{Z}}(\mathcal{O}_K) \mod p = \text{disc}_{\mathbb{Z}/p\mathbb{Z}}(\mathcal{O}_K/(p)).
\]

**Proof.** Pick a \(\mathbb{Z}\)-basis \(\omega_1, \ldots, \omega_n\) of \(\mathcal{O}_K\). The reductions \(\overline{\omega}_1, \ldots, \overline{\omega}_n\) in \(\mathcal{O}_K/(p)\) are a \(\mathbb{Z}/p\mathbb{Z}\)-basis, so the multiplication matrix \([m_x]\) for any \(x \in \mathcal{O}_K\), with respect to the basis \(\{\omega_i\}\), reduces modulo \(p\) to the multiplication matrix \([m_\overline{x}]\) for \(\overline{x}\) on \(\mathcal{O}_K/(p)\) with respect to the basis \(\{\overline{\omega}_i\}\). Therefore

\[
\text{Tr}_{(\mathcal{O}_K/(p))/(\mathbb{Z}/p\mathbb{Z})}(\overline{x}) = \text{Tr}(m_\overline{x}) = \text{Tr}(m_x) \mod p = \text{Tr}_{\mathcal{O}_K/\mathbb{Z}}(x) \mod p.
\]

Thus, the mod \(p\) reduction of the matrix \((\text{Tr}_{\mathcal{O}_K/\mathbb{Z}}(\omega_i \omega_j))\) is \((\text{Tr}_{(\mathcal{O}_K/(p))/(\mathbb{Z}/p\mathbb{Z})}(\overline{\omega}_i \overline{\omega}_j))\). Now take determinants.

**Lemma 3.4.** Let \(A\) be a commutative ring and \(B_1\) and \(B_2\) be commutative ring extensions of \(A\) which are each finite free \(A\)-modules. Then, choosing \(A\)-module bases appropriately,

\[
\text{disc}_A(B_1 \times B_2) = \text{disc}_A(B_1) \text{disc}_A(B_2).
\]
Proof. Pick $A$-module bases for $B_1$ and $B_2$:  
\[ B_1 = \bigoplus_{i=1}^m Ae_i, \quad B_2 = \bigoplus_{j=1}^n Af_j. \]
As an $A$-module basis for $B_1 \times B_2$ we will use the $m + n$ elements $e_1, \ldots, e_m, f_1, \ldots, f_n$. Since $e_if_j = 0$ in $B_1 \times B_2$, the matrix whose determinant is $\text{disc}_A(B_1 \times B_2)$ is a block diagonal matrix  
\[ \begin{pmatrix} (\text{Tr}_{(B_1 \times B_2)/A}(e_1e_k)) & O \\ O & (\text{Tr}_{(B_1 \times B_2)/A}(f_1f_l)) \end{pmatrix}. \]
For any $x \in B_1$, multiplication by $x$ on $B_1 \times B_2$ kills the $B_2$ component and acts on the $B_1$-component in the way $x$ multiplies on $B_1$, so a matrix for multiplication by $x$ on $B_1 \times B_2$ is a matrix whose upper left block is a matrix for multiplication by $x$ on $B_1$ and other blocks are 0. Thus  
\[ \text{Tr}_{(B_1 \times B_2)/A}(x) = \text{Tr}_{B_1/A}(x) \quad \text{for } x \in B_1. \]
Similarly,  
\[ \text{Tr}_{(B_1 \times B_2)/A}(x) = \text{Tr}_{B_2/A}(x) \quad \text{for } x \in B_2. \]
and taking determinants gives  
\[ \text{disc}_A(B_1 \times B_2) = \text{disc}_A(B_1) \text{ disc}_A(B_2). \]

Now we prove Theorem 1.3.

Proof. We have $p|\text{disc}_Z(\mathcal{O}_K)$ if and only if $\text{disc}_Z(\mathcal{O}_K) \equiv 0 \mod p$. By Lemma 3.3
\[ \text{disc}_Z(\mathcal{O}_K) \mod p = \text{disc}_{Z/pZ}(\mathcal{O}_K/(p)), \]
so $p|\text{disc}_Z(\mathcal{O}_K)$ if and only if $\text{disc}_{Z/pZ}(\mathcal{O}_K/(p)) = \overline{0}$ in $\mathbb{Z}/p\mathbb{Z}$.

In (1.2), each factor $\mathcal{O}_K/p_i^{e_i}$ is a $\mathbb{Z}/p\mathbb{Z}$-vector space since $p \in p_i^{e_i}$. Using (1.2) and Lemma 3.4,
\[ \text{disc}_{Z/pZ}(\mathcal{O}_K/(p)) = \prod_{i=1}^g \text{disc}_{Z/pZ}(\mathcal{O}_K/p_i^{e_i}). \]
Therefore we need to show for any prime number $p$ and prime-power ideal $p^e$ such that $p^e|\mathcal{O}_K$ that $\text{disc}_{Z/pZ}(\mathcal{O}_K/p^e)$ is $\overline{0}$ in $\mathbb{Z}/p\mathbb{Z}$ if and only if $e > 1$. (Recall that the vanishing of a discriminant is independent of the choice of basis.)

Suppose $e > 1$. Then any $x \in p - p^e$ is a nonzero nilpotent element in $\mathcal{O}_K/p^e$. By linear algebra over fields, such an $\mathfrak{a}$ can be used as part of a $\mathbb{Z}/p\mathbb{Z}$-basis of $\mathcal{O}_K/p^e$, say $\{\mathfrak{a}_1, \ldots, \mathfrak{a}_n\}$ with $\mathfrak{a} = \mathfrak{a}_1$. Writing the trace map $\text{Tr}_{(\mathcal{O}_K/p^e)/(\mathbb{Z}/p\mathbb{Z})}$ as $\text{Tr}_\mathfrak{a}$ for short, the first column of the matrix $(\text{Tr}(\mathfrak{a}_i, \mathfrak{a}_j))$ contains the numbers $\text{Tr}(\mathfrak{a}_i, \mathfrak{a}_j)$. These traces are all $\overline{0}$: $\mathfrak{a}_i\mathfrak{a}$ is nilpotent, so the linear transformation $m_{\mathfrak{a}_i, \mathfrak{a}}$ on $\mathcal{O}_K/p^e$ is nilpotent and thus its eigenvalues all equal zero. Since one column of the trace-pairing matrix $(\text{Tr}(\mathfrak{a}_i, \mathfrak{a}_j))$ is all $\overline{0}$, $\text{disc}_{Z/pZ}(\mathcal{O}_K/p^e) = \overline{0}$.

Now suppose $e = 1$. Then $\mathcal{O}_K/p^e = \mathcal{O}_K/p$ is a finite field of characteristic $p$. We want to prove $\text{disc}_{Z/pZ}(\mathcal{O}_K/p) \neq \overline{0}$. If this discriminant is $\overline{0}$, then (because $\mathcal{O}_K/p$ is a field) the trace function $\text{Tr}: \mathcal{O}_K/p \to \mathbb{Z}/p\mathbb{Z}$ is identically zero. However, from the theory of finite fields, this trace function can be written as a polynomial function:
\[ \text{Tr}(t) = t + t^p + t^{p^2} + \cdots + t^{p^{e-1}}, \]
where \( \#(\mathcal{O}_K/p) = p^r \). Since the degree of this polynomial is less than the size of \( \mathcal{O}_K/p \), this function is not identically zero on \( \mathcal{O}_K/p \). Therefore the discriminant of a finite extension of \( \mathbb{Z}/p\mathbb{Z} \) does not equal zero. \(\square\)