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

$$(p) = p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g} \tag{1.1}$$

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

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

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

$$\mathrm{N}(\alpha - m) = |m^3 - 9m + 6|.$$

Therefore $\mathrm{N}(\alpha) = 6$, $\mathrm{N}(\alpha-3) = 6$, and $\mathrm{N}(\alpha+3) = 6$. It follows that $(\alpha) = \mathfrak{p}_2\mathfrak{p}_3$, $(\alpha - 3) = \mathfrak{p}_2'\mathfrak{p}_3$, and $(\alpha+3) = \mathfrak{p}_2'\mathfrak{p}_3$ (so, in particular, $\alpha+3$ and $\alpha-3$ are unit multiples of each other). Thus

$$(2)(3) = (6) = (\alpha)(\alpha-3)(\alpha+3) = \mathfrak{p}_2\mathfrak{p}_2'^2\mathfrak{p}_3^3,$$

so $(2) = \mathfrak{p}_2^2\mathfrak{p}_2'$ and $(3) = \mathfrak{p}_3^3$. 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,

$$\mathcal{O}_K/(p) \cong \mathcal{O}_K/\mathfrak{p}_1^{e_1} \times \cdots \times \mathcal{O}_K/\mathfrak{p}_g^{e_g}. \tag{1.2}$$

If some e_i is greater than 1, then the quotient ring $\mathcal{O}_K/\mathfrak{p}_i^{e_i}$ has a nonzero nilpotent element (use the reduction modulo $\mathfrak{p}_i^{e_i}$ of any element of $\mathfrak{p}_i - \mathfrak{p}_i^{e_i}$), 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* $\mathrm{disc}_{\mathbf{Z}}(\mathcal{O}_K)$.

Since $\mathrm{disc}_{\mathbf{Z}}(\mathcal{O}_K) \neq 0$, 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 $\mathbf{Z}$. 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 $\mathcal{O}_K = \mathbf{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$. Let $f(T)$ be the minimal polynomial of α over $\mathbf{Q}$, so $f(T)$ is monic in $\mathbf{Z}[T]$. 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 $\overline{f}(T)$ in $(\mathbf{Z}/p\mathbf{Z})[T]$ is

$$\overline{f}(T) = \pi_1^{e_1} \cdot \dots \cdot \pi_g^{e_g}$$

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

The $\pi_i(T)$'s are separable (all irreducibles over a finite field are separable), so some $e_i > 1$ if and only if $\overline{f}(T)$ has a repeated root in a splitting field over $\mathbf{Z}/p\mathbf{Z}$. This is equivalent to $\overline{f}(T)$ having discriminant 0: p ramifies in $\mathcal{O}_K$ if and only if $\operatorname{disc}(\overline{f}) = 0$ in $\mathbf{Z}/p\mathbf{Z}$. 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: $\operatorname{disc}(f(T) \bmod p) = \operatorname{disc}(f(T)) \bmod p$. Therefore $\operatorname{disc}(\overline{f}(T)) = 0$ in $\mathbf{Z}/p\mathbf{Z}$ if and only if $\operatorname{disc}(f) \equiv 0 \bmod p$. Thus p ramifies in $\mathcal{O}_K$ if and only if $p \mid \operatorname{disc}(f)$. Since $\mathcal{O}_K = \mathbf{Z}[\alpha] \cong \mathbf{Z}[T]/(f(T))$, $\operatorname{disc}(f) = \operatorname{disc}_{\mathbf{Z}}(\mathbf{Z}[T]/(f)) = \operatorname{disc}_{\mathbf{Z}}(\mathcal{O}_K)$. □

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: $\operatorname{disc}_{\mathbf{Z}}(\mathcal{O}_K) \bmod p = \operatorname{disc}_{\mathbf{Z}/p\mathbf{Z}}(\mathcal{O}_K/(p))$. Then we will use (1.2) to write $\operatorname{disc}_{\mathbf{Z}/p\mathbf{Z}}(\mathcal{O}_K/(p))$ as a product of discriminants of rings of type $\mathcal{O}_K/\mathfrak{p}^e$ 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

$$\operatorname{disc}_A(e_1, \dots, e_n) = \det(\operatorname{Tr}_{B/A}(e_i e_j)) \in A.$$

Remark 3.2. The discriminant of a basis is an algebraic concept of "volume". To explain this viewpoint, we should think about $\operatorname{Tr}_{B/A}(xy)$ as an analogue of the dot product $v \cdot w$ in $\mathbf{R}^n$. For a basis $v_1, \dots, v_n$ in $\mathbf{R}^n$, the ordinary Euclidean volume of the parallelotope

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

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 $\langle x, y \rangle = \operatorname{Tr}_{B/A}(xy)$ on B in place of the $\mathbf{R}$-valued dot product on $\mathbf{R}^n$ 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 $e_1', \dots, e_n'$ 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

$$\begin{aligned}\operatorname{Tr}_{B/A}(e_i'e_j') &= \operatorname{Tr}_{B/A}\left(\sum_{k=1}^n a_{ik}e_k \sum_{\ell=1}^n a_{j\ell}e_\ell\right) \\ &= \sum_{k=1}^n\sum_{\ell=1}^n a_{ik}\operatorname{Tr}_{B/A}(e_ke_\ell)a_{j\ell},\end{aligned}$$

so

$$(\operatorname{Tr}_{B/A}(e_i'e_j')) = (a_{ij})(\operatorname{Tr}_{B/A}(e_ie_j))(a_{ij})^\top.$$

Therefore

$$\operatorname{disc}_A(e_1',\ldots,e_n') = (\det(a_{ij}))^2 \operatorname{disc}_A(e_1,\ldots,e_n).$$

We set

$$\operatorname{disc}_A(B) = \operatorname{disc}_A(e_1,\ldots,e_n) \in A$$

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 $\operatorname{disc}_A(B) = 0$ 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 $\mathbf{Z}/p\mathbf{Z}$. Letting K have degree n over $\mathbf{Q}$, the ring $\mathcal{O}_K$ is a free rank-n $\mathbf{Z}$-module, say

$$\mathcal{O}_K = \bigoplus_{i=1}^n \mathbf{Z}\omega_i.$$

Reducing both sides modulo p,

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

so $\mathcal{O}_K/(p)$ is a vector space over $\mathbf{Z}/p\mathbf{Z}$ of dimension n. The discriminant of $\mathcal{O}_K$ is $\operatorname{disc}_{\mathbf{Z}}(\mathcal{O}_K)$. 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 $\mathcal{O}_K/(p)$,*

$$\operatorname{disc}_{\mathbf{Z}}(\mathcal{O}_K) \bmod p = \operatorname{disc}_{\mathbf{Z}/p\mathbf{Z}}(\mathcal{O}_K/(p)).$$

Proof. Pick a $\mathbf{Z}$-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 $\mathbf{Z}/p\mathbf{Z}$-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

$$\operatorname{Tr}_{(\mathcal{O}_K/(p))/(\mathbf{Z}/p\mathbf{Z})}(\overline{x}) = \operatorname{Tr}(m_{\overline{x}}) = \operatorname{Tr}(m_x) \bmod p = \operatorname{Tr}_{\mathcal{O}_K/\mathbf{Z}}(x) \bmod p.$$

Thus, the mod p reduction of the matrix $(\operatorname{Tr}_{\mathcal{O}_K/\mathbf{Z}}(\omega_i\omega_j))$ is $(\operatorname{Tr}_{(\mathcal{O}_K/(p))/(\mathbf{Z}/p\mathbf{Z})}(\overline{\omega}_i\overline{\omega}_j))$. 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,*

$$\operatorname{disc}_A(B_1 \times B_2) = \operatorname{disc}_A(B_1)\operatorname{disc}_A(B_2).$$

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 $e_1, \dots, e_m, f_1, \dots, f_n$. Since $e_i f_j = 0$ in $B_1 \times B_2$, the matrix whose determinant is $\mathrm{disc}_A(B_1 \times B_2)$ is a block diagonal matrix

$$\begin{pmatrix} (\mathrm{Tr}_{(B_1\times B_2)/A}(e_ie_k)) & O \\ O & (\mathrm{Tr}_{(B_1\times B_2)/A}(f_jf_\ell)) \end{pmatrix}.$$

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

$$\mathrm{Tr}_{(B_1\times B_2)/A}(x) = \mathrm{Tr}_{B_1/A}(x) \quad \text{for } x \in B_1.$$

Similarly, $\mathrm{Tr}_{(B_1\times B_2)/A}(x) = \mathrm{Tr}_{B_2/A}(x)$ for $x \in B_2$. Thus

$$\begin{pmatrix} (\mathrm{Tr}_{(B_1\times B_2)/A}(e_ie_k)) & O \\ O & (\mathrm{Tr}_{(B_1\times B_2)/A}(f_jf_\ell)) \end{pmatrix} = \begin{pmatrix} (\mathrm{Tr}_{B_1/A}(e_ie_k)) & O \\ O & (\mathrm{Tr}_{B_2/A}(f_jf_\ell)) \end{pmatrix},$$

and taking determinants gives

$$\mathrm{disc}_A(B_1 \times B_2) = \mathrm{disc}_A(B_1)\,\mathrm{disc}_A(B_2).$$

□

Now we prove Theorem 1.3.

Proof. We have $p \mid \mathrm{disc}_{\mathbf{Z}}(\mathcal{O}_K)$ if and only if $\mathrm{disc}_{\mathbf{Z}}(\mathcal{O}_K) \equiv 0 \bmod p$. By Lemma 3.3

$$\mathrm{disc}_{\mathbf{Z}}(\mathcal{O}_K) \bmod p = \mathrm{disc}_{\mathbf{Z}/p\mathbf{Z}}(\mathcal{O}_K/(p)),$$

so $p \mid \mathrm{disc}_{\mathbf{Z}}(\mathcal{O}_K)$ if and only if $\mathrm{disc}_{\mathbf{Z}/p\mathbf{Z}}(\mathcal{O}_K/(p)) = \overline{0}$ in $\mathbf{Z}/p\mathbf{Z}$.

In (1.2), each factor $\mathcal{O}_K/\mathfrak{p}_i^{e_i}$ is a $\mathbf{Z}/p\mathbf{Z}$-vector space since $p \in \mathfrak{p}_i^{e_i}$. Using (1.2) and Lemma 3.4,

$$\mathrm{disc}_{\mathbf{Z}/p\mathbf{Z}}(\mathcal{O}_K/(p)) = \prod_{i=1}^{g} \mathrm{disc}_{\mathbf{Z}/p\mathbf{Z}}(\mathcal{O}_K/\mathfrak{p}_i^{e_i}).$$

Therefore we need to show for any prime number p and prime-power ideal $\mathfrak{p}^e$ such that $\mathfrak{p}^e \mid (p)$ that $\mathrm{disc}_{\mathbf{Z}/p\mathbf{Z}}(\mathcal{O}_K/\mathfrak{p}^e)$ is $\overline{0}$ in $\mathbf{Z}/p\mathbf{Z}$ 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 $x \in \mathfrak{p} - \mathfrak{p}^e$ is a nonzero nilpotent element in $\mathcal{O}_K/\mathfrak{p}^e$. By linear algebra over fields, such an $\overline{x}$ can be used as part of a $\mathbf{Z}/p\mathbf{Z}$-basis of $\mathcal{O}_K/\mathfrak{p}^e$, say $\{\overline{x}_1, \dots, \overline{x}_n\}$ with $\overline{x} = \overline{x}_1$. Writing the trace map $\mathrm{Tr}_{(\mathcal{O}_K/\mathfrak{p}^e)/(\mathbf{Z}/p\mathbf{Z})}$ as Tr for short, the first column of the matrix $(\mathrm{Tr}(\overline{x}_i\overline{x}_j))$ contains the numbers $\mathrm{Tr}(\overline{x}_i\overline{x})$. These traces are all $\overline{0}$: $\overline{x}_i\overline{x}$ is nilpotent, so the linear transformation $m_{\overline{x}_i\overline{x}}$ on $\mathcal{O}_K/\mathfrak{p}^e$ is nilpotent and thus its eigenvalues all equal zero. Since one column of the trace-pairing matrix $(\mathrm{Tr}(\overline{x}_i\overline{x}_j))$ is all $\overline{0}$, $\mathrm{disc}_{\mathbf{Z}/p\mathbf{Z}}(\mathcal{O}_K/\mathfrak{p}^e) = \overline{0}$.

Now suppose $e = 1$. Then $\mathcal{O}_K/\mathfrak{p}^e = \mathcal{O}_K/\mathfrak{p}$ is a finite field of characteristic p. We want to prove $\mathrm{disc}_{\mathbf{Z}/p\mathbf{Z}}(\mathcal{O}_K/\mathfrak{p}) \neq \overline{0}$. If this discriminant is $\overline{0}$, then (because $\mathcal{O}_K/\mathfrak{p}$ is a field) the trace function $\mathrm{Tr}\colon \mathcal{O}_K/\mathfrak{p} \to \mathbf{Z}/p\mathbf{Z}$ is identically zero. However, from the theory of finite fields, this trace function can be written as a polynomial function:

$$\mathrm{Tr}(t) = t + t^p + t^{p^2} + \cdots + t^{p^{r-1}},$$

where $\#(\mathcal{O}_K/\mathfrak{p}) = p^r$. Since the degree of this polynomial is less than the size of $\mathcal{O}_K/\mathfrak{p}$, this function is not identically zero on $\mathcal{O}_K/\mathfrak{p}$. Therefore the discriminant of a finite extension of $\mathbf{Z}/p\mathbf{Z}$ does not equal zero. $\square$