Discriminants and ramified primes

Presented by: Boris Fouotsa

Under the supervision of: Pr Francesco Pappalardi

University of Roma Tre

June 2019

Let $\mathbb{F} = \mathbb{Q}[T]/(f(T))$ be a number field, then the ring of integers $\mathcal{O}_{\mathbb{F}}$ of $\mathbb{F}$ is a Dedekind ring. This implies that every nonzero fractional ideal of $\mathcal{O}_{\mathbb{F}}$ has a unique factorization. Let p be a prime number, then

$$(p) = p\mathcal{O}_{\mathbb{F}} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g} \tag{1}$$

where the $\mathfrak{p}_i$ are distinct prime ideals of $\mathcal{O}_{\mathbb{F}}$. If the previous prime ideals factorization is square free, we say that p is **unramified** $\mathcal{O}_{\mathbb{F}}$, else we say that p is **ramified in** $\mathcal{O}_{\mathbb{F}}$.

Example 1

Set $\mathbb{F} = \mathbb{Q}[T]/(T^2+1) = \mathbb{Q}(i)$, $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}[i]$. *Then by the Kummer's lemma,*

$$(2) = (1+i)^2, \quad (3) = (3), \quad (5) = (5, 2+i)(5, 3+i);$$

hence 2 *is ramified in* $\mathbb{Z}[i]$, 3 *and* 5 *are unramified in* $\mathbb{Z}[i]$.

Can we distinguish ramified primes?

Theorem 1

Let $\mathbb{F}$ be a number field of discriminant $\Delta_{\mathbb{F}}$. Then a prime p is ramified in $\mathbb{F}$ if and only if $p|\Delta_{\mathbb{F}}$.

Our aim is to present a proof of this theorem available in [Con]. We start by discussing the power basis case, then we present the tools we will use in the proof, and we end by the concrete proof of the theorem.

The power basis case

We start by looking at the structure of the ring $\mathcal{O}_{\mathbb{F}}/(p)$. Since the prime ideals in equation 1 are all distinct, then by the Chinese Remainder Theorem:

$$\mathcal{O}_{\mathbb{F}}/(p) = \mathcal{O}_{\mathbb{F}}/(\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}) \simeq \mathcal{O}_{\mathbb{F}}/\mathfrak{p}_1^{e_1} \times \cdots \times \mathcal{O}_{\mathbb{F}}/\mathfrak{p}_g^{e_g} \qquad (2)$$

If p is ramified, then for some $i \in \{1, \cdots, g\}$, $e_i > 1$. Hence $\mathcal{O}_{\mathbb{F}}/\mathfrak{p}_i^{e_i}$ has a nonzero nilpotent element, so the ring $\mathcal{O}_{\mathbb{F}}/(p)$ has a nonzero nilpotent element.

If p is not ramified, then all the e_i are equal to 1 and the rings $\mathcal{O}_{\mathbb{F}}/\mathfrak{p}_i^{e_i}$ are fields. So $\mathcal{O}_{\mathbb{F}}/(p)$ is isomorphic to a product of fields, hence has no nonzero nilpotent element.

This proves that p is ramified if and only if $\mathcal{O}_{\mathbb{F}}/(p)$ has a nonzero nilpotent element.

The proof of the theorem is very short if we suppose that $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}[\alpha]$ for some α root of $f(T)$. In this case:

$$\mathcal{O}_{\mathbb{F}}/(p) = \mathbb{Z}[\alpha]/(p) = \mathbb{Z}[T]/(f(T), p) \simeq \mathbb{F}_p[T]/(f(T)) \quad (3)$$

Let

$$\bar{f}(T) = f_1(T)^{e_1} \cdots f_k(T)^{e_k} \quad (4)$$

be the factorization of $f(T)$ in $\mathbb{F}_p$. Since finite extensions of finite fields are separable, then $f_i(T)$ are separable. Hence $f(T)$ has a multiple root if and only if some $e_i > 1$, if and only p ramifies.

Since $\bar{f}(T)$ has a multiple root if and only if $disc(f) = 0 \ mod \ p$, then the theorem follows because $disc(f) = disc(\mathcal{O}_{\mathbb{F}}) = \Delta_{\mathbb{F}}$. □

This works because we used the fact that $disc(f) = disc(\mathcal{O}_{\mathbb{F}}) = \Delta_{\mathbb{F}}$ since $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}[\alpha]$. When $\mathcal{O}_{\mathbb{F}}$ has no power basis, we can't use this equality. We need to compute $disc(\mathcal{O}_{\mathbb{F}})$ another way.

We will prove that

$$disc_{\mathbb{F}_p}(\mathcal{O}_{\mathbb{F}}/(p)) = disc(\mathcal{O}_{\mathbb{F}}) \; mod \; p, \tag{5}$$

express this discriminant in terms of the discriminants of the $\mathcal{O}_{\mathbb{F}}/\mathfrak{p}_i^{e_i}$. Finally, we compute the discriminant of a ring of the form $\mathcal{O}_{\mathbb{F}}/\mathfrak{p}^e$ and prove the theorem.

Some neccessary tools

Definition 2.1

Let A be a commutative ring and B be a ring extension of A which is a free $A-$module of finite rank:

$$B = e_1A \oplus \cdots \oplus e_nA.$$

Then set

$$disc_A(e_1, \cdots, e_n) = det(Tr_{B/A}(e_ie_j)) \in A$$

Remark 2.1

This definition is just an extension of the concept of volume. $disc_A(e_1, \cdots, e_n)$ can be understood as the volume of the "algebraic" parallelotope of edges $e_1, \cdots, e_n$.

Given another basis $(e'_1, \cdots, e'_n)$ of B, there exist a matrix $M = (a_{ij})$ such that

$$e'_i = \sum_{k=1}^{n} a_{ik} e_k$$

Since $(e'_1, \cdots, e'_n)$ and $(e_1, \cdots, e_n)$ are both basis, then $det(M) \in A^{\times}$. Then

$$\begin{aligned} Tr_{B/A}(e'_i e'_j) &= Tr_{B/A}(\sum_{k=1}^{n} a_{ik} e_k \sum_{l=1}^{n} a_{jl} e_l) \\ &= \sum_{k=1}^{n} \sum_{l=1}^{n} a_{ik} Tr_{B/A}(e_k e_l) a_{jl} \\ &= (a_{i1}, \cdots, a_{in}) \cdot (Tr_{B/A}(e_k e_l)) \cdot \begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix} \end{aligned}$$

So

$$(Tr_{B/A}(e'_i e'_j)) = (a_{ij})(Tr_{B/A}(e_i e_j))(a_{ij})^T$$

Therefore

$$disc_A(e'_1, \cdots, e'_n) = det(M)^2 disc_A(e_1, \cdots, e_n)$$

Since $det(M) \in A^\times$, then for every basis $(e_1, \cdots, e_n)$, $(e'_1, \cdots, e'_n)$ of B:

$$disc_A(e'_1, \cdots, e'_n) = 0 \quad \Leftrightarrow disc_A(e_1, \cdots, e_n) = 0$$

We define:

$$disc_A(B) = disc_A(e_1, \cdots, e_n) \in A \quad \text{for any basis } (e_1, \cdots, e_n)$$

Notice that this discriminant is not unique but the condition $disc_A(B) = 0$ does not depend on the basis chosen.

Let $(w_1, \cdots, w_n)$ be a basis of $\mathcal{O}_{\mathbb{F}}$, then :

$$\mathcal{O}_{\mathbb{F}} = \bigoplus_{i=1}^{n} \mathbb{Z}w_1 \quad \text{and} \quad \mathcal{O}_{\mathbb{F}}/(p) = \bigoplus_{i=1}^{n} \mathbb{F}_p \overline{w_i}$$

So $\mathcal{O}_{\mathbb{F}}/(p)$ is a vector space over $\mathbb{F}_p$ of dimension n.

Lemma 2.1

If the bases of $\mathcal{O}_{\mathbb{F}}$ and $\mathcal{O}_{\mathbb{F}}/(p)$ are chosen appropriately, then:

$$disc_{\mathbb{F}_p}(\mathcal{O}_{\mathbb{F}}/(p)) = disc(\mathcal{O}_{\mathbb{F}}) \ mod \ p.$$

Proof.

Let $(w_1, \cdots, w_n)$ be a basis of $\mathcal{O}_{\mathbb{F}}$, then $(\overline{w_1}, \cdots, \overline{w_n})$ be a basis of $\mathcal{O}_{\mathbb{F}}/(p)$ over $\mathbb{F}_p$. For any $x \in \mathcal{O}_{\mathbb{F}}$, the multiplication by x matrix $[m_x]$, with respect to the basis $(w_1, \cdots, w_n)$, reduces modulo p to the multiplication by $\bar{x}$ matrix $[m_{\bar{x}}]$, with respect to the basis $(w_1, \cdots, w_n)$. Hence

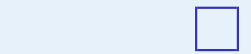
$$Tr_{(\mathcal{O}_{\mathbb{F}}/(p))/\mathbb{F}_p}(\bar{x}) = Tr([m_{\bar{x}}]) = Tr([m_x]) \ mod \ p = Tr(x) \ mod \ p.$$

So

$$Tr_{(\mathcal{O}_{\mathbb{F}}/(p))/\mathbb{F}_p}(\overline{w_i w_j}) = Tr(w_i w_j) \ mod \ p.$$

By taking the determinants of the respective matrices, we obtain:

$$disc_{\mathbb{F}_p}(\mathcal{O}_{\mathbb{F}}/(p)) = disc(\mathcal{O}_{\mathbb{F}}) \ mod \ p.$$



Lemma 2.2

If B_1 and B_2 are two ring extensions of the ring A which are each free $A-$modules of finite rank, then

$$disc_A(B_1 \times B_2) = disc_A(B_1) \times disc_A(B_2)$$

Proof.

Set

$$B_1 = e_1A \oplus \cdots \oplus e_nA \quad \text{and} \quad B_2 = f_1A \oplus \cdots \oplus f_nA,$$

then

$$B_1 \times B_2 = e_1A \oplus \cdots \oplus e_nA \oplus f_1A \oplus \cdots \oplus f_mA = \bigoplus_{i=1}^{n+m} b_iA$$

and $e_if_j = 0$ for all i, j. □

Proof.

Hence

$$\left(Tr_{((B_1\times B_2)/A)}(b_ib_j)\right) = \begin{pmatrix} \left(Tr_{((B_1\times B_2)/A)}(e_ie_j)\right) & 0 \\ 0 & \left(Tr_{((B_1\times B_2)/A)}(f_if_j)\right) \end{pmatrix}$$

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 same way as the multiplication by x on B_1. So

$$Tr_{((B_1\times B_2)/A)}(x) = Tr_{B_1/A}(x)$$

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

$$\left(Tr_{((B_1\times B_2)/A)}(b_ib_j)\right) = \begin{pmatrix} \left(Tr_{B_1/A}(e_ie_j)\right) & 0 \\ 0 & \left(Tr_{B_2/A}(f_if_j)\right) \end{pmatrix}$$

By taking the determinants, obtain the result. □

The concrete proof

Proof of the theorem:

From the above lemmas, if $(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$, then

$$\begin{aligned} \Delta_{\mathbb{F}} \ mod \ p &= disc(\mathcal{O}_{\mathbb{F}}) \ mod \ p \\ &= disc_{\mathbb{F}_p}(\mathcal{O}_{\mathbb{F}}/(p)) \\ &= disc_{\mathbb{F}_p}\left(\mathcal{O}_{\mathbb{F}}/\mathfrak{p}_1^{e_1} \times \cdots \times \mathcal{O}_{\mathbb{F}}/\mathfrak{p}_g^{e_g}\right) \\ &= disc_{\mathbb{F}_p}\left(\mathcal{O}_{\mathbb{F}}/\mathfrak{p}_1^{e_1}\right) \times \cdots \times disc_{\mathbb{F}_p}\left(\mathcal{O}_{\mathbb{F}}/\mathfrak{p}_g^{e_g}\right) \end{aligned}$$

$$\text{So} \quad p|\Delta_{\mathbb{F}} \Leftrightarrow \exists i \in \{1, \cdots, g\} : disc_{\mathbb{F}_p}\left(\mathcal{O}_{\mathbb{F}}/\mathfrak{p}_i^{e_i}\right) = \overline{0} \text{ in } \mathbb{F}_p$$

Since p is ramified if and only if some e_j is greater than 1, then we need to prove the following: for any prime ideal power $\mathfrak{p}^e$ above (p),

$$disc_{\mathbb{F}_p}\left(\mathcal{O}_{\mathbb{F}}/\mathfrak{p}^e\right) = \overline{0} \text{ in } \mathbb{F}_p \quad \Leftrightarrow \quad e > 1$$

Proof of the theorem:

Suppose $e > 1$, then choose $x \in \mathfrak{p} \setminus \mathfrak{p}^e$, x is a nonzero nilpotent element. Since $\overline{x}$ is nonzero, then $\overline{x}$ can be used in a basis $\mathbb{F}_p$ basis of $\mathcal{O}_{\mathbb{F}}/\mathfrak{p}^e$, say $\{\overline{x_1} = \overline{x}, \overline{x_2}, \cdots, \overline{x_k}\}$. Since $\overline{x_1}$ is nilpotent, then $\overline{x_i x_1}$ is nilpotent for every i and all the eigenvalues of the multiplication by $\overline{x_i x_1}$ a zero. So

$$Tr_{(\mathcal{O}_{\mathbb{F}}/\mathfrak{p}^e)/\mathbb{F}_p}(\overline{x_i x_1}) = \overline{0} \quad \forall i.$$

Therefore the first column of the matrix $\left(Tr_{(\mathcal{O}_{\mathbb{F}}/\mathfrak{p}^e)/\mathbb{F}_p}(\overline{x_i x_j})\right)$ is zero and

$$disc_{\mathbb{F}_p}(\mathcal{O}_{\mathbb{F}}/\mathfrak{p}^e) = det\left(Tr_{(\mathcal{O}_{\mathbb{F}}/\mathfrak{p}^e)/\mathbb{F}_p}(\overline{x_i x_j})\right) = \overline{0}.$$

Proof of the theorem:

Suppose $e = 1$, then $\mathcal{O}_{\mathbb{F}}/\mathfrak{p}^e$ is a field of characteristic p. We proceed by contradiction.
If for a certain basis $\{\overline{x_1}, \cdots, \overline{x_k}\}$ of $\mathcal{O}_{\mathbb{F}}/\mathfrak{p}$ we have

$$disc_{\mathbb{F}_p}\left(\mathcal{O}_{\mathbb{F}}/\mathfrak{p}\right) = det\left(Tr_{(\mathcal{O}_{\mathbb{F}}/\mathfrak{p})/\mathbb{F}_p}(\overline{x_i x_j})\right) = \overline{0},$$

then the matrix $\left(Tr_{(\mathcal{O}_{\mathbb{F}}/\mathfrak{p})/\mathbb{F}_p}(\overline{x_i x_j})\right)$ can be transformed (by replacing a suitable chosen column j_0 by a zero linear combination of this column and other columns) into a matrix where the j_0 column is zero. This linear combination transforms the $\{\overline{x_1}, \cdots, \overline{x_k}\}$ to another basis $\{\overline{y_1}, \cdots, \overline{y_k}\}$. Hence

$$\forall i,\ Tr_{(\mathcal{O}_{\mathbb{F}}/\mathfrak{p})/\mathbb{F}_p}(\overline{y_i y_{j_0}}) = \overline{0}, \quad \text{so } Tr_{(\mathcal{O}_{\mathbb{F}}/\mathfrak{p})/\mathbb{F}_p}(\overline{y y_{j_0}}) = \overline{0}\ \forall y \in \mathcal{O}_{\mathbb{F}}/\mathfrak{p}$$

□

Proof of the theorem:

Since $\mathcal{O}_{\mathbb{F}}/\mathfrak{p}$ is a field and $\overline{y_{j_0}} \neq \overline{0}$, then the multiplication by $\overline{y_{j_0}}$ is bijective. So

$$Tr_{(\mathcal{O}_{\mathbb{F}}/\mathfrak{p})/\mathbb{F}_p}(\overline{y}) = \overline{0} \quad \forall \overline{y} \in \mathcal{O}_{\mathbb{F}}/\mathfrak{p}.$$

Set $\sharp\mathcal{O}_{\mathbb{F}}/\mathfrak{p} = p^r$, then

$$Tr_{(\mathcal{O}_{\mathbb{F}}/\mathfrak{p})/\mathbb{F}_p}(t) = t + t^p + \cdots + t^{p^{r-1}} \quad \forall t \in \mathcal{O}_{\mathbb{F}}/\mathfrak{p}$$

Then we have shown that a polynomial of degre p^{r-1} has at least p^r roots, contradiction.
So

$$disc_{\mathbb{F}_p}(\mathcal{O}_{\mathbb{F}}/\mathfrak{p}) \neq \overline{0},$$

 Keith Conrad.
Discriminants and ramified primes.
https://kconrad.math.uconn.edu/blurbs/gradnumthy/disc.pdf.

THANK YOU FOR YOUR KIND ATTENTION !
THANK YOU FOR YOUR KIND ATTENTION !
THANK YOU FOR YOUR KIND ATTENTION !
THANK YOU FOR YOUR KIND ATTENTION !
THANK YOU FOR YOUR KIND ATTENTION !

THANK YOU FOR YOUR KIND ATTENTION !
THANK YOU FOR YOUR KIND ATTENTION !
THANK YOU FOR YOUR KIND ATTENTION !
THANK YOU FOR YOUR KIND ATTENTION !
THANK YOU FOR YOUR KIND ATTENTION !