

RAMIFICATION OF PRIMES: A PRESENTATION FOR MATH 8600: COMMUTATIVE ALGEBRA

GEORGE H. SEELINGER

1. INTRODUCTION

Let $K|\mathbb{Q}$ be a finite field extension with $[K : \mathbb{Q}] = n$. Then, we may consider the integral closure of \mathbb{Z} in K , say \mathcal{O}_K . Thus, we have the following setup.

$$\begin{array}{ccc} K & \longleftrightarrow & \mathcal{O}_K \\ | & & | \\ \mathbb{Q} & \longleftrightarrow & \mathbb{Z} \end{array}$$

where $\mathcal{O}_K|\mathbb{Z}$ is an integral ring extension. Now, recall the following facts.

1.1. Proposition. *Given the setup above*

- (a) \mathcal{O}_K is a Dedekind domain.
- (b) Given a prime $p \in \mathbb{Z}$, the ideal $(p) = p\mathcal{O}_K \trianglelefteq \mathcal{O}_K$ has a unique decomposition

$$(p) = \prod_{i=1}^g P_i^{e_i}$$

for prime ideals $P_i \trianglelefteq \mathcal{O}_K$ and $e_i \in \mathbb{N}$.

- (c) \mathcal{O}_K is a finitely-generated, free \mathbb{Z} -module, say

$$\mathcal{O}_K \cong \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n \text{ as a } \mathbb{Z}\text{-module.}$$

Thus, $\mathcal{O}_K/p\mathcal{O}_K$ is a finitely-generated $\mathbb{Z}/p\mathbb{Z}$ -module, that is

$$\mathcal{O}_K/p\mathcal{O}_K \cong (\mathbb{Z}/p\mathbb{Z})\overline{\alpha_1} \oplus \cdots \oplus (\mathbb{Z}/p\mathbb{Z})\overline{\alpha_n}$$

Furthermore, by the Chinese Remainder Theorem,

$$\mathcal{O}_K/p\mathcal{O}_K \cong \mathcal{O}_K/P_1^{e_1} \times \cdots \times \mathcal{O}_K/P_g^{e_g}$$

so each $\mathcal{O}_K/P_i^{e_i}$ is an \mathbb{F}_p -vector space, and in fact, an \mathbb{F}_p -algebra since $p \in P_i^{e_i}$.

This leads us to the following definition:

Date: May 2018.

1.2. Definition. We say a prime $p \in \mathbb{Z}$ is *ramified* in \mathcal{O}_K if

$$p\mathcal{O}_K = \prod_{i=1}^g P_i^{e_i}$$

has some $e_i > 1$ for prime ideals $P_i \subseteq \mathcal{O}_K$. If every $e_i = 1$, then p is *unramified* in \mathcal{O}_K .

1.3. Example. Consider $2 \in \mathbb{Z}[i]$. Then, since

$$-i(1+i)(1+i) = -i(1+2i-1) = -i2i = 2,$$

we have that $(2) \subseteq (1+i)^2$. Furthermore, since $(1+i)$ is prime in $\mathbb{Z}[i]$ using norm arguments, and (2) has norm 4, it must be that $(2) = (1+i)^2$. Therefore, 2 ramifies in $\mathbb{Z}[i]$.

We wish to come up with some method to determine when a prime will ramify in \mathcal{O}_K . One such characterization uses the notion of the “discriminant.”

1.4. Definition. Let V be an m -dimensional vector space over K . Then, given a symmetric bilinear form $b: V \times V \rightarrow K$ and $\{\omega_1, \dots, \omega_m\}$ a basis of V , we define

$$\text{disc}(b; \omega_1, \dots, \omega_m) := \det(b(\omega_i, \omega_j))_{1 \leq i, j \leq m}$$

1.5. Proposition. Given another K -basis of V as above, say $\{\omega'_1, \dots, \omega'_m\}$ such that

$$M \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_m \end{pmatrix} = \begin{pmatrix} \omega'_1 \\ \vdots \\ \omega'_m \end{pmatrix}$$

we get that

$$\text{disc}(b; \omega'_1, \dots, \omega'_m) = (\det M)^2 \text{disc}(b; \omega_1, \dots, \omega_m)$$

Proof. Consider that if

$$B = (b(\omega_i, \omega_j))_{1 \leq i, j \leq m}, \quad B' = (b(\omega'_i, \omega'_j))_{1 \leq i, j \leq m}$$

then,

$$B'_{i,j} = b(\omega'_i, \omega'_j) = b\left(\sum_{k=1}^n m_{k,i} \omega_k, \sum_{\ell=1}^n m_{\ell,j} \omega_\ell\right) = \sum_{k=1}^n \sum_{\ell=1}^n m_{i,k} b(\omega_k, \omega_\ell) m_{j,\ell} = (MBM^t)_{i,j}$$

and so $B' = MBM^t$. Then the result is obtained by taking the determinant of both sides. \square

1.6. Definition. Let K be a field and let A be a finite-dimensional K -algebra with basis $\{x_1, \dots, x_n\}$. Then,

- (a) The *trace* $\text{Tr}_{A|K}(z) := \text{tr } m_z$ where, if

$$zx_i = \sum_{j=1}^n a_{i,j} x_j, \quad a_{i,j} \in K$$

then $m_z = (a_{i,j})_{1 \leq i,j \leq n}$. Note that this is independent of choice of basis since a different choice will give a matrix m'_z that is conjugate to m_z , which will not change the trace.

- (b) The *trace form* $T: A \times A \rightarrow K$ is given by

$$T(x, y) = \text{Tr}_{A|K}(xy)$$

Since we are in a commutative ring, the form is symmetric. Since matrix trace is bilinear, then so is the trace form.

- (c) The *discriminant* of A is

$$\text{disc}(A) := \text{disc}(T; x_1, \dots, x_n)$$

1.7. Remark. Consider the case that $K|\mathbb{Q}$ is a finite separable field extension with $\mathcal{O}_K \subseteq K$ the integral closure of \mathbb{Z} in K .

- (a) Then, the discriminant is independent of choice of integral basis since, given another integral basis $\{x'_1, \dots, x'_n\}$, we have

$$\text{disc}(T; x'_1, \dots, x'_n) = (\det M)^2 \text{disc}(T; x_1, \dots, x_n)$$

However, M is an invertible matrix with entries in \mathbb{Z} , so it must be that $\det M = \pm 1 \implies (\det M)^2 = 1$.

- (b) Note $\text{disc}(K)$ is always an integer because $\text{Tr}_{K|\mathbb{Q}}(\mathcal{O}_K) \subseteq \mathbb{Z}$.

1.8. Example. Consider the field extension $\mathbb{Q}(i)|\mathbb{Q}$. Then, if we take integral basis $\{1, i\}$, we get

$$m_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, m_i = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \text{ and } m_{-1} = -m_1$$

Thus,

$$\text{Tr}(1) = 2, \text{Tr}(i) = 0, \text{Tr}(-1) = -2$$

and so

$$\text{disc}(\{1, i\}) = \det \begin{pmatrix} \text{Tr}(1) & \text{Tr}(i) \\ \text{Tr}(i) & \text{Tr}(-1) \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix} = -4$$

This paper seeks to prove the following useful characterization for when a prime p ramifies in \mathcal{O}_K .

1.9. Theorem. *A prime $p \in \mathbb{Z}$ ramifies in \mathcal{O}_K if and only if $p \mid \text{disc}(K)$.*

From this result, we also have the useful corollary

1.10. Corollary. *Only a finite number of primes $p \in \mathbb{Z}$ ramify in \mathcal{O}_K .*

Thus, from our running example, 2 is the only prime that ramifies in $\mathbb{Z}[i]$. In the next section, we will follow a synthesis of the programs by [Ash03, 4.2] and [Con] to prove this theorem.

2. STRUCTURE AND TRACE OF THE QUOTIENT $\mathcal{O}_K/p\mathcal{O}_K$

Using our same setup, let $(p) = p\mathcal{O}_K = \prod_i P_i^{e_i}$ for prime ideals $P_i \subseteq \mathcal{O}_K$ and $e_i \in \mathbb{N}$.

2.1. Lemma. *p ramifies if and only if the ring $\mathcal{O}_K/(p)$ has nonzero nilpotent elements.*

Proof. • (\implies) . Let p ramify in \mathcal{O}_K . Then, $\mathcal{O}_K/p\mathcal{O}_K \cong \mathcal{O}_K/P_1^{e_1} \times \cdots \times \mathcal{O}_K/P_n^{e_n}$ by the Chinese Remainder Theorem, where at least one $e_i > 1$, let us say e_1 . Then, the quotient ring $\mathcal{O}_K/P_1^{e_1}$ has a nonzero nilpotent element since, for $x \in P_1 \setminus P_1^{e_1}$, we get $(x + P_1^{e_1})^{e_1} = x^{e_1} + P_1^{e_1} = P_1^{e_1}$.
 • (\impliedby) . If p does not ramify in \mathcal{O}_K , then $\mathcal{O}_K/p\mathcal{O}_K \cong \mathcal{O}_K/P_1 \times \cdots \times \mathcal{O}_K/P_n$, each of which is a field since each P_i is maximal in \mathcal{O}_K . Furthermore, each of these fields is finite by Proposition 1.1(c). Thus, $\mathcal{O}_K/p\mathcal{O}_K$ cannot have any nonzero nilpotent elements. \square

We also have, as a corollary to the proof, that

2.2. Corollary. *If p is unramified in \mathcal{O}_K , then $\mathcal{O}_K/p\mathcal{O}_K$ is a product of finite fields.*

This is a useful fact since

2.3. Lemma. *A nilpotent element has zero trace.*

Proof. Let $x^n = 0$ for some $n \in \mathbb{N}$. Then, since $m_{x^k} = (m_x)^k$, it must be that $(m_x)^n = 0$, so m_x is a nilpotent matrix, which has trace 0 since its minimal polynomial $\mu_{m_x}(t) \mid t^n$. Therefore,

$$\mathrm{Tr}_{K|\mathbb{Q}}(x) = \mathrm{tr} m_x = 0$$

\square

And so, we get

2.4. Lemma. *For prime $p \in \mathbb{Z}$, let $p\mathcal{O}_K = \prod_{i=1}^g P_i^{e_i}$. For any $e_i > 1$, $\mathrm{disc}_{\mathbb{F}_p}(\mathcal{O}_K/P_i^{e_i}) = \bar{0}$.*

Proof. From 1.1(c), we have that $\mathcal{O}_K/P_i^{e_i}$ is an \mathbb{F}_p -algebra. By the above, since at least one $e_i > 1$, p ramifies and so we know $\mathcal{O}_K/P_i^{e_i}$ has a nonzero nilpotent element, say x . Then, extend $\{x\}$ to a basis of $\mathcal{O}_K/P_i^{e_i}$ over \mathbb{F}_p , say $\{x, x_2, \dots, x_k\}$. Each xx_i is nilpotent, so, for all i ,

$$\mathrm{Tr}_{\mathcal{O}_K/P_i^{e_i}|\mathbb{F}_p}(xx_i) = \bar{0}$$

and so, since the trace form matrix will have a row of all zeros, it must have determinant equal to $\bar{0}$ and so the discriminant is 0. \square

2.5. Lemma. *Let p is in \mathcal{O}_K be unramified, that is, $p\mathcal{O}_K = \prod_{i=1}^g P_i$. Then, the trace form of \mathcal{O}_K/P_i over \mathbb{F}_p is nondegenerate. Thus, given the field extension $\mathcal{O}_K/P_i|\mathbb{F}_p$, the discriminant*

$$\text{disc}(\mathcal{O}_K/P_i) \neq \bar{0} \in \mathbb{F}_p$$

Proof. By the arguments above, we already know that \mathcal{O}_K/P_i is a finite field, and since \mathbb{F}_p is perfect, we have that $\mathcal{O}_K/P_i|\mathbb{F}_p$ is a separable field extension. Therefore, by Lemma 2.2.3 in class, it must be that the trace form is nondegenerate. Therefore, fixing an \mathbb{F}_p -basis of \mathcal{O}_K/P_i , $\{\omega_1, \dots, \omega_k\}$ the matrix

$$(T(\omega_i, \omega_j))_{1 \leq i, j \leq n} \text{ is invertible } \iff \det(T(\omega_i, \omega_j))_{1 \leq i, j \leq n} \neq \bar{0}$$

Therefore, $\text{disc}(\mathcal{O}_K/P) \neq \bar{0}$. \square

3. DISCRIMINANT BEHAVES WELL WITH REDUCTION mod p AND PRODUCTS

3.1. Lemma. *For an appropriate choice of bases,*

$$\text{disc}(K) \bmod p = \text{disc}(\mathcal{O}_K/p\mathcal{O}_K)$$

Proof. Let $\{\alpha_1, \dots, \alpha_n\}$ be an integral basis for $\mathcal{O}_K|\mathbb{Z}$. Then, for $x \in \mathcal{O}_K$, we have $a_{i,j} \in \mathbb{Z}$ such that

$$x\alpha_i = \sum_j a_{i,j}\alpha_j \implies x\alpha_i + p\mathcal{O}_K = \sum_j \overline{a_{i,j}}\alpha_j + p\mathcal{O}_K$$

where $\overline{a_{i,j}} = a_{i,j} \bmod p$. Thus, m_x with the entries reduced mod p is equal to $m_{x+p\mathcal{O}_K}$. Thus,

$$\text{Tr}_{\mathcal{O}_K/p\mathcal{O}_K|\mathbb{F}_p}(x+p\mathcal{O}_K) = \text{tr}(m_{x+p\mathcal{O}_K}) = \text{tr}(m_x) \bmod p = \text{Tr}_{K|\mathbb{Q}}(x) \bmod p$$

giving us that

$$(\text{Tr}_{K|\mathbb{Q}}(\alpha_i\alpha_j))_{1 \leq i, j \leq n} \bmod p = \text{Tr}_{\mathcal{O}_K/(p)|\mathbb{Z}/p\mathbb{Z}}(\overline{\alpha_i}\overline{\alpha_j})$$

and so, taking determinants of both sides gives the desired result. \square

3.2. Lemma. *Let F be a field with B_1, B_2 finitely-generated F -algebras. Then, up to appropriate choice of basis,*

$$\text{disc}(B_1 \times B_2) = \text{disc}(B_1) \text{disc}(B_2)$$

Proof. Let

$$B_1 = \bigoplus_{i=1}^m F e_i, \quad B_2 = \bigoplus_{j=1}^n F f_j$$

Then, take the standard choice of F -basis of $B_1 \times B_2$, $\{e_1, \dots, e_m, f_1, \dots, f_n\}$. Since $e_i f_j = 0$ in $B_1 \times B_2$, we get that

$$\text{disc}(B_1 \times B_2) = \det \begin{pmatrix} \text{Tr}_{B_1 \times B_2|F}(e_i e_k) & 0 \\ 0 & \text{Tr}_{B_1 \times B_2|F}(f_j f_\ell) \end{pmatrix}$$

Also, for $x \in B_1$, since $xy = 0$ for all $y \in B_2$, we have

$$\mathrm{Tr}_{B_1 \times B_2|F}(x) = \mathrm{Tr}_{B_1|F}(x)$$

and similarly for $y \in B_2$

$$\mathrm{Tr}_{B_1 \times B_2|F}(y) = \mathrm{Tr}_{B_2|F}(y)$$

Thus,

$$\begin{pmatrix} \mathrm{Tr}_{B_1 \times B_2|F}(e_i e_k) & 0 \\ 0 & \mathrm{Tr}_{B_1 \times B_2|F}(f_j f_\ell) \end{pmatrix} = \begin{pmatrix} \mathrm{Tr}_{B_1|F}(e_i e_k) & 0 \\ 0 & \mathrm{Tr}_{B_2|F}(f_j f_\ell) \end{pmatrix}$$

and so, taking the determinant of both sides, we get the desired result. \square

4. PROOF OF THE RAMIFICATION THEOREM

We now prove our theorem.

Proof of 1.9. We first observe that

$$\begin{aligned} p \mid \mathrm{disc}(K) &\iff \mathrm{disc}(K) \equiv 0 \pmod{p} \\ &\iff \mathrm{disc}(\mathcal{O}_K/(p)) = \bar{0} && \text{by Lemma 3.1} \\ &\iff \prod \mathrm{disc}(\mathcal{O}_K/P_i^{e_i}) = \bar{0} && \text{by Lemma 3.2} \end{aligned}$$

Thus, if any $e_i > 1$, we get that $\mathcal{O}_K/P_i^{e_i}$ has a nonzero nilpotent element by 2.1, and so $\mathrm{disc}(\mathcal{O}_K/P_i^{e_i}) = \bar{0}$ by 2.4, thus giving $p \mid \mathrm{disc}_{\mathbb{Z}}(\mathcal{O}_K)$ by the equivalences above.

If all $e = 1$, then each \mathcal{O}_K/P_i is a finite field, so $\mathrm{disc}(\mathcal{O}_K/P_i) \neq \bar{0}$ by 2.5. Therefore, it must be that $p \nmid \mathrm{disc}(K)$. \square

5. FACTORIZATION IN QUADRATIC NUMBER FIELDS

In this section, we follow [Ash03] to determine some results about factorization of primes in quadratic number fields. First, recall the theorem

5.1. Theorem (Ram-Rel Identity). *Let A be an integral domain with field of fractions K , $L|K$ a finite separable field extension of degree n , and B the integral closure of A in L . Given a prime ideal $P \subseteq A$, if*

$$PB = \prod_{i=1}^g P_i^{e_i} \quad f_i = [B/P_i : A/P]$$

then

$$\sum_{i=1}^g e_i f_i = [B/PB : A/P] = n$$

Thus, for $m \in \mathbb{Z} \setminus \{0, 1\}$, a squarefree integer, $\mathbb{Q}(\sqrt{m})|\mathbb{Q}$ has degree 2. Thus, for a prime $p \in \mathbb{Z}$, there are only three possible situations.

(a) $g = 2, e_1 = e_2 = f_1 = f_2 = 1$, that is,

$$(p) = P_1 P_2$$

In this situation, we say that p *splits* in \mathcal{O}_K .

(b) $g = 1, e_1 = 1, f_1 = 2$, that is, (p) is a prime ideal of \mathcal{O}_K . In this situations, we say that (p) is *inert*.

(c) $g = 1, e_1 = 2, f_1 = 1$, that is,

$$(p) = P_1^2$$

so p ramifies.

Furthermore, we will use the following result about the discriminant of $\mathbb{Q}(\sqrt{m})$.

5.2. Proposition. *The discriminant of $\mathbb{Q}(\sqrt{m})$ is m if $m \equiv 1 \pmod{4}$ and it is $4m$ if $m \equiv 2, 3 \pmod{4}$. In particular, the discriminant is always 0 or 1 mod 4.*

Proof. If $m \not\equiv 1 \pmod{4}$, $\{1, \sqrt{m}\}$ is an integral basis of $\mathbb{Q}(\sqrt{m})$. Then,

$$\text{Tr}(a+b\sqrt{m}) = \text{tr} \begin{pmatrix} a & b \\ bm & a \end{pmatrix} = 2a \implies \text{disc}(\mathbb{Q}(\sqrt{m})) = \det \begin{pmatrix} 2 & 0 \\ 0 & 2m \end{pmatrix} = 4m$$

If $m \equiv 1 \pmod{4}$, then $\{1, \frac{1+\sqrt{m}}{2}\}$ forms an integral basis and

$$\left(\frac{1+\sqrt{m}}{2}\right)^2 = \frac{m-1}{4} + \frac{1+\sqrt{m}}{2}$$

So, $\text{Tr}(1) = 2$ and

$$\begin{aligned} \text{Tr}\left(\frac{1+\sqrt{m}}{2}\right) &= \text{tr} \begin{pmatrix} 0 & 1 \\ \frac{m-1}{4} & 1 \end{pmatrix} = 1, \\ \text{Tr}\left(\frac{m-1}{4} + \frac{1+\sqrt{m}}{2}\right) &= \text{tr} \begin{pmatrix} \frac{m-1}{4} & 1 \\ \frac{m-1}{4} & \frac{m+3}{4} \end{pmatrix} = \frac{m+1}{2} \end{aligned}$$

Thus

$$\text{disc}(\mathbb{Q}(\sqrt{m})) = \det \begin{pmatrix} 2 & 1 \\ 1 & \frac{1+m}{2} \end{pmatrix} = m$$

□

We then have the following result.

5.3. Theorem. *Let prime $p \neq 2$. Then,*

- (a) (p) ramifies as $(p, \sqrt{m})^2$ in $\mathbb{Q}(\sqrt{m})$ if and only if $m \equiv 0 \pmod{p}$.
- (b) (p) splits as $(p) = (p, a + \sqrt{m})(p, a - \sqrt{m})$ in $\mathbb{Q}(\sqrt{m})$ if and only if $m \equiv a^2 \pmod{p}$ for some $a \not\equiv 0 \pmod{p}$.
- (c) (p) is inert in $\mathbb{Q}(\sqrt{m})$ if and only if $m \not\equiv a^2 \pmod{p}$ for all a .

If $p = 2$ and m is odd, then

- (a) (2) ramifies in $\mathbb{Q}(\sqrt{m})$ if and only if $m \equiv 3 \pmod{4}$.

- (b) (2) splits as $\left(2, \frac{1+\sqrt{m}}{2}\right) \left(2, \frac{1-\sqrt{m}}{2}\right)$ in $\mathbb{Q}(\sqrt{m})$ if and only if $m \equiv 1 \pmod{8}$.
- (c) (2) is inert in $\mathbb{Q}(\sqrt{m})$ if and only if $m \equiv 5 \pmod{8}$.

Proof. We break down the various situations. Throughout, let $D = \text{disc}(\mathbb{Q}(\sqrt{m}))$.

- Assume p is an odd prime with p not dividing m . p does not divide the discriminant, so (p) cannot ramify.

– If $m \equiv a^2 \pmod{p}$, $a \not\equiv 0 \pmod{p}$, then $(p) = (p, a + \sqrt{m})(p, a - \sqrt{m})$ because

$$(p, a + \sqrt{m})(p, a - \sqrt{m}) = (p^2, pa + p\sqrt{m}, pa - p\sqrt{m}, \underbrace{a^2 - m}_{\equiv 0 \pmod{p}}) \subseteq (p)$$

and since

$$p(a + \sqrt{m} + a - \sqrt{m}) = 2ap \in (p, a + \sqrt{m})(p, a - \sqrt{m})$$

but $a \not\equiv 0 \pmod{p}$, so $\gcd(2ap, p^2) = p$, and thus $p \in (p, a + \sqrt{m})(p, a - \sqrt{m})$.

– If $m \not\equiv a^2 \pmod{p}$, then $x^2 - m$ is irreducible \pmod{p} . Assume $(p) = Q_1 Q_2$. Each Q_i must have norm p , thus giving $\mathcal{O}_K/Q_i \cong \mathbb{F}_p$. However, $\sqrt{m} \in \mathcal{O}_K \implies m$ has a square root in \mathbb{F}_p , a contradiction. Thus, (p) is inert.

- Let p divide m . Then, p divides the discriminant and so (p) ramifies. In fact,

$$(p, \sqrt{m})^2 = (p^2, p\sqrt{m}, m) \subseteq (p)$$

However, since m is squarefree, $p^2 \nmid m$, so $\gcd(p^2, m) = p$, so $p \in (p, \sqrt{m})^2$.

- Let $p = 2$ and m be odd.
 - If $m \equiv 3 \pmod{4} \implies D = 4m$, then 2 divides the discriminant, so (2) ramifies. We claim $(2) = (2, 1 + \sqrt{m})^2$. First, we check

$$(2, 1 + \sqrt{m})^2 = (4, 2(1 + \sqrt{m}), \underbrace{1 + 2\sqrt{m} + m}_{\equiv 0 \pmod{2}}) \subseteq (2)$$

Furthermore,

$$1 + 2\sqrt{m} + m - 2(1 + \sqrt{m}) = m - 1 \equiv 2 \pmod{4}$$

so there is some $x \in \mathbb{Z}$ such that

$$m - 1 + 4x = 2$$

thus giving us equality of ideals.

- If $m \equiv 1 \pmod{8}$, then $m \equiv 1 \pmod{4}$, so we get an integral basis $\{1, \frac{1+\sqrt{m}}{2}\}$ and the discriminant is $D = m$. Therefore, $2 \nmid D$, so (2) does not ramify. We then compute,

$$(2, \frac{1 + \sqrt{m}}{2})(2, \frac{1 - \sqrt{m}}{2}) = (4, 1 - \sqrt{m}, 1 + \sqrt{m}, \underbrace{\frac{1 - m}{4}}_{\text{Even}}) \subseteq (2)$$

However, we also have

$$1 - \sqrt{m} + 1 + \sqrt{m} = 2 \in (2, \frac{1 + \sqrt{m}}{2})(2, \frac{1 - \sqrt{m}}{2})$$

giving us the desired ideal equality.

- If $m \equiv 5 \pmod{8}$, then $m \equiv 1 \pmod{4}$, so $D = m$, meaning 2 does not ramify. Consider

$$f(x) = x^2 - x + \frac{1 - m}{4} \in (\mathcal{O}_K/P)[x]$$

where $(2) \subseteq P$ a prime ideal in \mathcal{O}_K . The roots of f are $\frac{1 \pm \sqrt{m}}{2}$, so f has a root in \mathcal{O}_K and hence in \mathcal{O}_K/P . However, since $\frac{1-m}{4} \equiv 1 \pmod{2}$, f has no root in \mathbb{F}_2 . Therefore, \mathcal{O}_K/P and \mathbb{F}_2 cannot be isomorphic. If $(2) = P_1 P_2$ in \mathcal{O}_K , then the norm of (2) is 4 and so P_1, P_2 each have norm 2. Therefore, $\mathcal{O}_K/P_i \cong \mathbb{F}_2$, which is a contradiction. Thus, (2) must remain prime.

□

REFERENCES

- [Ash03] R. B. Ash, *A Course In Algebraic Number Theory*, 2003. <https://faculty.math.illinois.edu/~r-ash/ANT.html>.
- [Con] K. Conrad, *Discriminants and Ramified Primes*. <http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/disc.pdf>.
- [MC16] S. Mack-Crane, *Prime Splitting in Quadratic Extensions I: One Prime, Many Fields* (2016). <https://algebrateahousejmath.wordpress.com/2016/11/23/prime-splitting-in-quadratic-extensions-i-one-prime-many-fields/>.