TOTALLY RAMIFIED PRIMES AND EISENSTEIN POLYNOMIALS

KEITH CONRAD

1. Introduction

A (monic) polynomial in $\mathbf{Z}[T]$,

$$f(T) = T^n + c_{n-1}T^{n-1} + \cdots + c_1T + c_0,$$

is *Eisenstein* at a prime p when each coefficient c_i is divisible by p and the constant term c_0 is not divisible by p^2. Such polynomials are irreducible in $\mathbf{Q}[T]$, and this Eisenstein criterion for irreducibility is the way nearly everyone first meets Eisenstein polynomials. Here, we will show Eisenstein polynomials are closely related to total ramification of primes in number fields.

Let K be a number field, with degree n over $\mathbf{Q}$. A prime number p is said to be *totally ramified* in K when $p\mathcal{O}_K = \mathfrak{p}^n$. For example, in $\mathbf{Z}[i]$ we have $(2) = (1+i)^2$, so 2 is totally ramified in $\mathbf{Q}(i)$.

The link between Eisenstein polynomials and totally ramified primes is described in the following two theorems, which are converses of each other.

Theorem 1.1. *Let $K = \mathbf{Q}(\alpha)$, where α is the root of a polynomial which is Eisenstein at p. Then p is totally ramified in K.*

Theorem 1.2. *Let K be a number field, and suppose there is a prime p which is totally ramified in K. Then $K = \mathbf{Q}(\alpha)$ for some α which is the root of an Eisenstein polynomial at p.*

Let's illustrate Theorem 1.1.

Example 1.3. Let $K = \mathbf{Q}(\sqrt[3]{2})$. Since $\sqrt[3]{2}$ is a root of $T^3 - 2$, which is Eisenstein at 2, the prime number 2 is totally ramified in K. Indeed, $(2) = (\sqrt[3]{2})^3$. Similarly, since $K = \mathbf{Q}(\sqrt[3]{2}+1)$ and $\sqrt[3]{2}+1$ is a root of

$$(T-1)^3 - 2 = T^3 - 3T^2 + 3T - 3,$$

which is Eisenstein at 3, we must have $(3) = \mathfrak{p}^3$ as well. In fact,

$$(\sqrt[3]{2}+1)^3 = 3(1 + \sqrt[3]{2} + \sqrt[3]{4}),$$

and the second factor is a unit in $\mathbf{Z}[\sqrt[3]{2}]$, so $(3) = (\sqrt[3]{2}+1)^3$.

Example 1.4. Let $K = \mathbf{Q}(\sqrt{-5})$. Since $1 + \sqrt{-5}$ is a field generator and is a root of $T^2 - 2T + 6$, which is Eisenstein at 2, we have $(2) = \mathfrak{p}^2$ for some prime ideal $\mathfrak{p}$. The ideal $\mathfrak{p}$ is $(2, 1+\sqrt{-5})$, which is not principal.

2. Proofs

Now we prove Theorem 1.1.

Proof. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ which divides $(p) = p\mathcal{O}_K$ and $n = [K : \mathbf{Q}]$. We want to show that $(p) = \mathfrak{p}^n$.

Let $e \geq 1$ be the multiplicity of $\mathfrak{p}$ in (p), so

$$(p) = \mathfrak{p}^e\mathfrak{a},$$

where $\mathfrak{p}$ does not divide $\mathfrak{a}$. Then $e \leq n$. We will show $e = n$, which implies by taking norms that $\mathfrak{a} = (1)$ (and $\mathrm{N}\mathfrak{p} = p$).

Let $f(T)$ be the Eisenstein polynomial at p with α as a root, say

$$f(T) = T^n + c_{n-1}T^{n-1} + \cdots + c_1T + c_0.$$

Since $c_i \equiv 0 \bmod p$, the equation $f(\alpha) = 0$ implies $\alpha^n \equiv 0 \bmod \mathfrak{p}$, so

$$\alpha \equiv 0 \bmod \mathfrak{p}, \tag{2.1}$$

since $\mathfrak{p}$ is prime.

Since $c_1, \ldots, c_{n-1}$ are divisible by p, and thus by $\mathfrak{p}^e$, we get from (2.1) that

$$c_i\alpha^i \equiv 0 \bmod \mathfrak{p}^{e+1}$$

for $i = 1, \ldots, n-1$. Therefore all intermediate terms in $f(\alpha)$ are divisible by $\mathfrak{p}^{e+1}$, so

$$\alpha^n + c_0 \equiv 0 \bmod \mathfrak{p}^{e+1}. \tag{2.2}$$

Since c_0 is divisible by p exactly once, $c_0\mathcal{O}_K = \mathfrak{p}^e\mathfrak{b}$ where $\mathfrak{p}$ does not divide $\mathfrak{b}$. Therefore $c_0 \not\equiv 0 \bmod \mathfrak{p}^{e+1}$, so (2.2) implies $\alpha^n \not\equiv 0 \bmod \mathfrak{p}^{e+1}$. As α is divisible by $\mathfrak{p}$ at least once, so α^n is divisible by $\mathfrak{p}^n$, we must have $e + 1 > n$. Therefore $e > n - 1$. Since $e \leq n$, the only choice is $e = n$. □

The proof of Theorem 1.2 will tell us quite explicitly how to find the element α which is the root of an Eisenstein polynomial.

Proof. Let $n = [K : \mathbf{Q}]$ and $p\mathcal{O}_K = \mathfrak{p}^n$. Then, taking ideal norms, $p^n = \mathrm{N}\mathfrak{p}^n$, so $\mathrm{N}\mathfrak{p} = p$.

We will use as α any number in $\mathfrak{p}$ which is not in $\mathfrak{p}^2$. (In other words, (α) is divisible by $\mathfrak{p}$ exactly once.) It will turn out that the characteristic polynomial of α over $\mathbf{Q}$, which we know is monic of degree n in $\mathbf{Z}[T]$, is an Eisenstein polynomial at p. That implies this characteristic polynomial is irreducible, so $K = \mathbf{Q}(\alpha)$ and we're done.

Consider the characteristic polynomial of α over $\mathbf{Q}$:

$$T^n + a_{n-1}T^{n-1} + \cdots + a_1T + a_0,$$

where $a_i \in \mathbf{Z}$. The constant term is $a_0 = \pm\,\mathrm{N}_{K/\mathbf{Q}}(\alpha)$. Let's show this is divisible by p exactly once.

Since $\alpha \in \mathfrak{p} - \mathfrak{p}^2$,

$$(\alpha) = \mathfrak{p}\mathfrak{a}, \tag{2.3}$$

where $\mathfrak{p}$ does not divide $\mathfrak{a}$. Taking ideal norms in (2.3),

$$|\,\mathrm{N}_{K/\mathbf{Q}}(\alpha)| = p\,\mathrm{N}\mathfrak{a}.$$

Thus $a_0 = \pm\,\mathrm{N}_{K/\mathbf{Q}}(\alpha)$ is divisible by p. To show p^2 does not divide a_0, we show p is not a factor of $\mathrm{N}\mathfrak{a}$. The prime numbers dividing $\mathrm{N}\mathfrak{a}$ are the prime numbers lying under the prime

ideals dividing $\mathfrak{a}$. Since $\mathfrak{p}$ does not divide $\mathfrak{a}$, and $\mathfrak{p}$ is the only prime ideal dividing p, $\mathrm{N}\mathfrak{a}$ is not divisible by p.

Now we show every a_i is divisible by p. We may assume $n \geq 2$. (Otherwise, if $n = 1$, $K = \mathbf{Q}$ and the characteristic polynomial is $T + a_0$, which is Eisenstein at p.) Assume for some i from 1 to $n-1$ that we know $a_0, \ldots, a_{i-1} \equiv 0 \bmod p$. To show $a_i \equiv 0 \bmod p$, reduce the equation

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$$

modulo $p\mathcal{O}_K$:

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_i\alpha^i \equiv 0 \bmod p\mathcal{O}_K. \tag{2.4}$$

Raising both sides of (2.3) to the n-th power,

$$(\alpha^n) = (p)\mathfrak{a}^n,$$

so

$$\alpha^n \in p\mathcal{O}_K. \tag{2.5}$$

Multiply through (2.4) by α^{n-1-i}, and take into account (2.5):

$$a_i\alpha^{n-1} \equiv 0 \bmod p\mathcal{O}_K.$$

Now take norms:

$$a_i^n \,\mathrm{N}_{K/\mathbf{Q}}(\alpha)^{n-1} \equiv 0 \bmod p^n\mathbf{Z}.$$

Since $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$ is divisible by p just once, the left side is a multiple of p^n only if $p|a_i$. Thus, by induction, every a_i is a multiple of p. □

So far we have been discussing Eisenstein polynomials in $\mathbf{Z}[T]$. Let's generalize the concept to polynomials over other rings of integers.

Definition 2.1. Let K be a number field. A monic polynomial

$$f(T) = T^n + c_{n-1}T^{n-1} + \cdots + c_1T + c_0 \in \mathcal{O}_K[T]$$

is called Eisenstein at the nonzero prime ideal $\mathfrak{p}$ when $c_i \equiv 0 \bmod \mathfrak{p}$ for all i and $c_0 \not\equiv 0 \bmod \mathfrak{p}^2$.

Theorem 2.2. *Any Eisenstein polynomial in $\mathcal{O}_K[T]$ is irreducible in $K[T]$.*

Proof. Let $f(T) \in \mathcal{O}_K[T]$ be Eisenstein at some prime ideal. If $f(T)$ is reducible in $K[T]$ then $f(T) = g(T)h(T)$ for some nonconstant $g(T)$ and $h(T)$ in $K[T]$.

We first show that g and h can be chosen in $\mathcal{O}_K[T]$. As f is monic, we can assume g and h are monic by rescaling if necessary. Every root of g or h is an algebraic integer (since their roots are roots of $f(T)$, so they're integral over $\mathcal{O}_K$ and thus also over $\mathbf{Z}$). Because both are monic, their coefficients are polynomials in their roots, hence their coefficients are algebraic integers. Thus g and h both lie in $\mathcal{O}_K[T]$.

Let $n = \deg f$, $r = \deg g$, and $s = \deg h$. All of these degrees are positive. Let $\mathfrak{p}$ be a prime at which f is Eisenstein. Reduce the equation $f = gh$ in $\mathcal{O}_K[T]$ modulo $\mathfrak{p}$ to get $\overline{f} = \overline{g}\overline{h}$ in $(\mathcal{O}_K/\mathfrak{p})[T]$. As f, g, and h are all monic, their reductions modulo $\mathfrak{p}$ have the same degree as the original polynomials (n, r, and s respectively). Since f is Eisenstein at $\mathfrak{p}$, $\overline{f} = T^n$. Therefore, by unique factorization in $(\mathcal{O}_K/\mathfrak{p})[T]$, $\overline{g}$ and $\overline{h}$ are powers of T too, so $\overline{g} = T^r$ and $\overline{h} = T^s$. But, because r and s are positive, we conclude that g and h have constant term in $\mathfrak{p}$. Then the constant term of f is $f(0) = g(0)h(0) \in \mathfrak{p}^2$. This contradicts the definition of an Eisenstein polynomial. □

Theorems 1.1 and 1.2 generalize as follows.

Theorem 2.3. *Let F be a number field and $E = F(\alpha)$, where α is the root of a polynomial in $\mathcal{O}_F[T]$ which is Eisenstein at a prime $\mathfrak{p}$. Then $\mathfrak{p}$ is totally ramified in E: $\mathfrak{p}\mathcal{O}_E = \mathfrak{P}^n$ for some prime ideal $\mathfrak{P}$ of $\mathcal{O}_E$, where $n = [E : F]$.*

Theorem 2.4. *Let E/F be a finite extension, and suppose there is a prime $\mathfrak{p}$ of F which is totally ramified in E. Then $E = F(\alpha)$ for some α which is the root of an Eisenstein polynomial at $\mathfrak{p}$.*

It is left to the reader to work out the proofs, which are quite similar to the case of base field $\mathbf{Q}$.

3. p-Divisibility of coefficients

As an application of Eisenstein polynomials, we extract information about coefficients for algebraic integers in the power basis generated by the root of an Eisenstein polynomial. Theorems 1.1 and 1.2 will not be used.

Lemma 3.1. *Let $K/\mathbf{Q}$ be a number field with degree n. Assume $K = \mathbf{Q}(\alpha)$, where $\alpha \in \mathcal{O}_K$ and its minimal polynomial over $\mathbf{Q}$ is Eisenstein at p. For $a_0, a_1, \ldots, a_{n-1} \in \mathbf{Z}$, if*

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \equiv 0 \bmod p\mathcal{O}_K, \tag{3.1}$$

then $a_i \equiv 0 \bmod p\mathbf{Z}$ for all i.

Proof. We will argue by induction from a_0 up to a_{n-1}.

Multiply through the congruence (3.1) by α^{n-1}, making all but the first term $a_0\alpha^{n-1}$ a multiple of α^n. Since α is the root of an Eisenstein polynomial at p, $\alpha^n \equiv 0 \bmod p\mathcal{O}_K$, so

$$a_0\alpha^{n-1} \equiv 0 \bmod p\mathcal{O}_K.$$

Now take norms down to $\mathbf{Z}$:

$$a_0^n \,\mathrm{N}_{K/\mathbf{Q}}(\alpha)^{n-1} \equiv 0 \bmod p^n\mathbf{Z}.$$

The norm of α is, up to sign, the constant term of its characteristic polynomial for $K/\mathbf{Q}$. Since α generates $K/\mathbf{Q}$, its characteristic polynomial is its minimal polynomial, which is Eisenstein. Therefore $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$ is divisible by p exactly once, so the above congruence modulo p^n implies $p|a_0^n$, so $p|a_0$. Now the congruence (3.1) becomes

$$a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \equiv 0 \bmod p\mathcal{O}_K$$

Multiply this by α^{n-2} to get $a_1\alpha^{n-1} \equiv 0 \bmod p\mathcal{O}_K$ and take norms again. The conclusion now will be $p|a_1$. We can now take out the a_1-term from the original congruence and iterate this idea all the way to the last term, so each a_i is divisible by p. □

Theorem 3.2. *Let $K/\mathbf{Q}$ be a number field with degree n. Assume $K = \mathbf{Q}(\alpha)$, where α is an algebraic integer whose minimal polynomial over $\mathbf{Q}$ is Eisenstein at p. If*

$$r_0 + r_1\alpha + \cdots + r_{n-1}\alpha^{n-1} \in \mathcal{O}_K$$

with $r_i \in \mathbf{Q}$, then each r_i has no p in its denominator.

Proof. Assume some r_i has a p in its denominator. Let d be the least common denominator, so $p|d$, $dr_i \in \mathbf{Z}$ for all i, and some dr_i is not a multiple of p. Then

$$dr_0 + dr_1\alpha + \cdots + dr_{n-1}\alpha^{n-1} \in p\mathcal{O}_K,$$

so Lemma 3.1 tells us $dr_i \in p\mathbf{Z}$ for every i. This is a contradiction. □

Theorem 3.3. *Let $K = \mathbf{Q}(\alpha)$ where α is the root of an Eisenstein polynomial at p, with degree n. Then*

(a) $p \nmid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$.
(b) $p^{n-1} || \operatorname{disc}(K)$ if $p \nmid n$ and $p^n \mid \operatorname{disc}(K)$ if $p \mid n$.

Proof. (a) We argue by contradiction. Suppose $p \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$. Then $\mathcal{O}_K/\mathbf{Z}[\alpha]$, viewed as a finite abelian group, has an element of order p: there is some $\gamma \in \mathcal{O}_K$ such that $\gamma \notin \mathbf{Z}[\alpha]$ but $p\gamma \in \mathbf{Z}[\alpha]$. Using the basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$ for $K/\mathbf{Q}$, write

$$\gamma = r_0 + r_1\alpha + \cdots + r_{n-1}\alpha^{n-1}$$

with $r_i \in \mathbf{Q}$. Since $\gamma \notin \mathbf{Z}[\alpha]$, some r_i is not in $\mathbf{Z}$. Since $p\gamma \in \mathbf{Z}[\alpha]$ we have $pr_i \in \mathbf{Z}$. Hence r_i has a p in its denominator, which contradicts Theorem 3.2.

(b) Since $\operatorname{disc}(\mathbf{Z}[\alpha]) = [\mathcal{O}_K : \mathbf{Z}[\alpha]]^2 \operatorname{disc}(K)$, by part a the highest power of p in $\operatorname{disc}(K)$ and $\operatorname{disc}(\mathbf{Z}[\alpha])$ is the same. We now use the formula

$$\operatorname{disc}(\mathbf{Z}[\alpha]) = \operatorname{disc}(f(T)) = \pm \operatorname{N}_{K/\mathbf{Q}}(f'(\alpha))$$

to find the highest power of p that is a factor.

Write $(p) = \mathfrak{p}^n$ and $(\alpha) = \mathfrak{p}\mathfrak{a}$ with $\mathfrak{p} \nmid \mathfrak{a}$. Let the minimal polynomial of α over $\mathbf{Q}$ be $f(T) = \sum_{i=0}^{n} c_i T^i$, so

$$f'(\alpha) = n\alpha^{n-1} + (n-1)c_{n-1}\alpha^{n-2} + \cdots + 2c_2\alpha + c_1.$$

Since each c_i is divisible by p and thus by $\mathfrak{p}^n$, all terms in $f'(\alpha)$ except the leading term are divisible by $\mathfrak{p}^n$. Thus

$$f'(\alpha) \equiv n\alpha^{n-1} \bmod \mathfrak{p}^n. \tag{3.2}$$

We know α^{n-1} is divisible by $\mathfrak{p}^{n-1}$ and not by $\mathfrak{p}^n$. Therefore if $n \not\equiv 0 \bmod \mathfrak{p}$, which is the same as $n \not\equiv 0 \bmod p$, (3.2) says $(f'(\alpha))$ is divisibile by $\mathfrak{p}$ exactly $n-1$ times, while if $n \equiv 0 \bmod p$ then $(f'(\alpha))$ is divisible by $\mathfrak{p}$ at least n times. In the first case, $(f'(\alpha)) = \mathfrak{p}^{n-1}\mathfrak{b}$ where $\mathfrak{p} \nmid \mathfrak{b}$, so taking norms gives us $\operatorname{N}_{K/\mathbf{Q}}(f'(\alpha)) = p^{n-1}b$ where $p \nmid b$. In the second case, $\mathfrak{p}^n \mid (f'(\alpha))$, so $p^n \mid \operatorname{N}_{K/\mathbf{Q}}((f'(\alpha))$. □

Example 3.4. We show the ring of algebraic integers of $\mathbf{Q}(\sqrt[3]{2})$ is $\mathbf{Z}[\sqrt[3]{2}]$. Let $\mathcal{O}$ be the full ring of algebraic integers of $\mathbf{Q}(\sqrt[3]{2})$, so $\mathbf{Z}[\sqrt[3]{2}] \subset \mathcal{O}$ and

$$\operatorname{disc}(\mathbf{Z}[\sqrt[3]{2}]) = [\mathcal{O} : \mathbf{Z}[\sqrt[3]{2}]]^2 \operatorname{disc}(\mathcal{O}).$$

By an explicit calculation, $\operatorname{disc}_{\mathbf{Z}}(\mathbf{Z}[\sqrt[3]{2}]) = -108 = -2^2 3^3$, so 2 and 3 are the only primes which could divide $[\mathcal{O} : \mathbf{Z}[\sqrt[3]{2}]]$. Since $\sqrt[3]{2}$ is the root of $T^3 - 2$, which is Eisenstein at 2, 2 does not divide $[\mathcal{O} : \mathbf{Z}[\sqrt[3]{2}]]$ by Corollary 3.3. The number $\sqrt[3]{2}+1$ is a root of $(T-1)^3 - 2 = T^3 - 3T^2 + 3T - 3$, which is Eisenstein at 3, so 3 does not divide $[\mathcal{O} : \mathbf{Z}[\sqrt[3]{2}+1]] = [\mathcal{O} : \mathbf{Z}[\sqrt[3]{2}]]$. Hence $[\mathcal{O} : \mathbf{Z}[\sqrt[3]{2}]]$ must be 1, so $\mathcal{O} = \mathbf{Z}[\sqrt[3]{2}]$.

Example 3.5. We show the ring $\mathcal{O}$ of algebraic integers of $\mathbf{Q}(\sqrt[4]{2})$ is $\mathbf{Z}[\sqrt[4]{2}]$. Since

$$\operatorname{disc}(\mathbf{Z}[\sqrt[4]{2}]) = [\mathcal{O} : \mathbf{Z}[\sqrt[4]{2}]]^2 \operatorname{disc}(\mathcal{O})$$

and the discriminant of $\mathbf{Z}[\sqrt[4]{2}]$ is -2^{11}, $[\mathcal{O} : \mathbf{Z}[\sqrt[4]{2}]]$ is a power of 2. Because $\sqrt[4]{2}$ is a root of $T^4 - 2$ which is Eisenstein at 2, 2 does not divide $[\mathcal{O} : \mathbf{Z}[\sqrt[4]{2}]]$ by Corollary 3.3. Therefore the index is 1.

Example 3.6. We show the ring $\mathcal{O}$ of algebraic integers of $\mathbf{Q}(\sqrt[5]{2})$ is $\mathbf{Z}[\sqrt[5]{2}]$. The discriminant of $\mathbf{Z}[\sqrt[5]{2}]$ is $2^4 5^5$, so the only prime factors of $[\mathcal{O} : \mathbf{Z}[\sqrt[5]{2}]]$ could be 2 and 5. Since $\sqrt[5]{2}$ is a root of $T^5 - 2$, which is Eisenstein at 2, and $\sqrt[5]{2} - 2$ is a root of

$$(T+2)^5 - 2 = T^5 + 10T^4 + 40T^3 + 80T^2 + 80T + 30,$$

which is Eisenstein at 5, neither 2 nor 5 divides the index since $\mathbf{Z}[\sqrt[5]{2} - 2] = \mathbf{Z}[\sqrt[5]{2}]$, by Corollary 3.3.

Example 3.7. As a final use of Corollary 3.3, we compute the ring of integers of 3 cubic fields. For $i = 1, 2, 3$, define three number fields $K_i = \mathbf{Q}(\alpha_i)$ where α_i is the root of the cubic polynomial $f_i(T)$:

$$f_1(T) = T^3 - 18T - 6, \quad f_2(T) = T^3 - 36T - 78, \quad f_3(T) = T^3 - 54T - 150. \tag{3.3}$$

These polynomials are all Eisenstein at 2 and 3, so they are irreducible over $\mathbf{Q}$. Each polynomial has 3 real roots and the same discriminant: $22356 = 2^2 \cdot 3^5 \cdot 23$. (Recall $\mathrm{disc}(T^3 + aT + b) = -4a^3 - 27b^2$.) Let's show $\mathbf{Z}[\alpha_i]$ is the ring of integers of K_i in each case. Since $22356 = \mathrm{disc}(\mathbf{Z}[\alpha_i]) = [\mathcal{O}_{K_i} : \mathbf{Z}[\alpha_i]]^2 \,\mathrm{disc}(\mathcal{O}_{K_i})$, $[\mathcal{O}_{K_i} : \mathbf{Z}[\alpha_i]]$ divides $2 \cdot 3^2$. Since all the polynomials are Eisenstein at 2 and 3, neither 2 nor 3 divides the index of $\mathbf{Z}[\alpha_i]$ in $\mathcal{O}_{K_i}$ by Corollary 3.3. That proves the index is 1 in all three cases. Therefore

$$\mathrm{disc}(\mathcal{O}_{K_i}) = \mathrm{disc}(\mathbf{Z}[\alpha_i]) = \mathrm{disc}(\mathbf{Z}[T]/(f_i(T))) = \mathrm{disc}(f_i(T)) = 22356$$

for $i = 1, 2, 3$.

The fields K_1, K_2, and K_3 are all cubic extensions of $\mathbf{Q}$ with the same discriminant and the ring of integers of K_i has a power basis. The primes 2 and 3 are both totally ramified in each K_i. So far the K_i's seem to be quite similar. Are they isomorphic fields? No. To prove this, we show some primes besides 2 and 3 factor differently in the fields. Since $\mathcal{O}_{K_i} = \mathbf{Z}[\alpha_i]$, Dedekind's factorization criterion tells us that the way p factors in $\mathcal{O}_{K_i}$ is the same as the way $f_i(T)$ factors in $\mathbf{F}_p[T]$ for the polynomials $f_i(T)$ in (3.3).

In $\mathbf{F}_5[T]$, $f_1(T)$ and $f_2(T)$ are irreducible but $f_3(T) = T(T-2)(T-3)$. Therefore 5 stays prime in K_1 and K_2 but it splits completely in K_3, so K_3 is not isomorphic to K_1 or K_2. In $\mathbf{F}_7[T]$, all three polynomials factor as a linear times a quadratic, so 7 factors in the same way in each K_i. But 11 behaves differently and will distinguish K_1 and K_2: in $\mathbf{F}_{11}[T]$, $f_1(T) = (T-3)(T-9)(T-10)$ while $f_2(T)$ and $f_3(T)$ are irreducible, so 11 splits completely in K_1 and remains prime in K_2 and K_3.