TOTALLY RAMIFIED PRIMES AND EISENSTEIN POLYNOMIALS

KEITH CONRAD

1. Introduction

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

$$f(T) = T^n + c_{n-1}T^{n-1} + \cdots + c_1 T + c_0,$$

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 essentially everyone first meets Eisenstein polynomials. Here we will show Eisenstein polynomials at a prime p give us useful information about p-divisibility of coefficients of a power basis and ramification of p in a number field.

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 $\mathbf{Z}[i]$ and $\mathbf{Z}[\sqrt{-5}]$ we have $(2) = (1+i)^2$ and $(2) = (2, 1+\sqrt{-5})^2$, so 2 is totally ramified in $\mathbf{Q}(i)$ and $\mathbf{Q}(\sqrt{-5})$.

2. Eisenstein polynomials and p-divisibility of coefficients

Our first use of Eisenstein polynomials will be to extract information about coefficients for algebraic integers in the power basis generated by the root of an Eisenstein polynomial.

Lemma 2.1. *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*

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \equiv 0 \bmod p\mathcal{O}_K, \tag{2.1}$$

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

Proof. Assume for some $j \in \{0, 1, \ldots, n-1\}$ that $a_i \equiv 0 \bmod p\mathbf{Z}$ for $i < j$ (this is an empty condition for $j = 0$). We will prove $a_j \equiv 0 \bmod p\mathbf{Z}$.

Since $a_i \equiv 0 \bmod p\mathbf{Z}$ for $i < j$, (2.1) implies

$$a_j\alpha^j + a_{j+1}\alpha^{j+1} + \cdots + a_{n-1}\alpha^{n-1} \equiv 0 \bmod p\mathcal{O}_K. \tag{2.2}$$

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

$$a_j\alpha^{n-1} \equiv 0 \bmod p\mathcal{O}_K. \tag{2.3}$$

Write this congruence as an equation, say $a_j\alpha^{n-1} = p\gamma$ with $\gamma \in \mathcal{O}_K$. Now take norms of both sides down to $\mathbf{Q}$:

$$a_j^n \operatorname{N}_{K/\mathbf{Q}}(\alpha)^{n-1} = p^n \operatorname{N}_{K/\mathbf{Q}}(\gamma).$$

The right side is an integral multiple of p^n. On the left side the norm of α is, up to sign, the constant term of its minimal polynomial for $K/\mathbf{Q}$ since α generates $K/\mathbf{Q}$. The integer $\operatorname{N}_{K/\mathbf{Q}}(\alpha)$ is divisible by p exactly once (Eisenstein condition!), so divisibility of $a_j^n \operatorname{N}_{K/\mathbf{Q}}(\alpha)^{n-1}$ by p^n implies $p \mid a_j^n$, so $p \mid a_j$. Thus $a_i \equiv 0 \bmod p\mathbf{Z}$ for $i < j+1$. Repeat this for $j = 0, 1, \ldots, n-1$ to get $p \mid a_i$ for all i. □

Theorem 2.2. *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 of the r_i's, so $p \mid d$. Write $r_i = a_i/d$ where $a_i \in \mathbf{Z}$, so some a_i is not divisible by p (otherwise d, being divisible by p, would not be the least common denominator). Then

$$r_0 + r_1\alpha + \cdots + r_{n-1}\alpha^{n-1} \in \mathcal{O}_K \Longrightarrow \frac{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}}{d} \in \mathcal{O}_K.$$

Multiply through by the integer d to get

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \in d\mathcal{O}_K \subset p\mathcal{O}_K.$$

Lemma 2.1 tells us $a_i \in p\mathbf{Z}$ for every i. This is a contradiction. □

Theorem 2.3. *Let $K = \mathbf{Q}(\alpha)$ where $\alpha \in \mathcal{O}_K$ is the root of an Eisenstein polynomial at p, with degree n. Then $p \nmid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$.*

Proof. 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 2.2. □

Example 2.4. 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 that 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 Theorem 2.3. The number $1 + \sqrt[3]{2}$ is a root of $(T-1)^3 - 2 = T^3 - 3T^2 + 3T - 3$, which is Eisenstein at 3, so 3 does not divide $[\mathcal{O} : \mathbf{Z}[1 + \sqrt[3]{2}]]$. The ring $\mathbf{Z}[1 + \sqrt[3]{2}]$ equals $\mathbf{Z}[\sqrt[3]{2}]$, so $[\mathcal{O} : \mathbf{Z}[\sqrt[3]{2}]]$ is not divisible by 3. Therefore this index is 1, so $\mathcal{O} = \mathbf{Z}[\sqrt[3]{2}]$.

Example 2.5. 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 $T^4 - 2$ that is Eisenstein at 2, 2 does not divide $[\mathcal{O} : \mathbf{Z}[\sqrt[4]{2}]]$ by Theorem 2.3. Therefore the index is 1.

Example 2.6. 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 $\mathbf{Z}[\sqrt[5]{2} - 2] = \mathbf{Z}[\sqrt[5]{2}]$.

Remark 2.7. It is natural to ask if the ring of integers of $\mathbf{Q}(\sqrt[n]{2})$ is $\mathbf{Z}[\sqrt[n]{2}]$ for all n. It is true for all $n \leq 1000$, it is not always true! See `https://kconrad.math.uconn.edu/blurbs/gradnumthy/integersradical.pdf`,

Example 2.8. We show the ring $\mathcal{O}$ of algebraic integers of $\mathbf{Q}(\sqrt[3]{3})$ is $\mathbf{Z}[\sqrt[3]{3}]$. Since

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

and the discriminant of $\mathbf{Z}[\sqrt[3]{3}]$ is -3^5, $[\mathcal{O} : \mathbf{Z}[\sqrt[3]{3}]]$ divides 3^2. Since $T^3 - 3$ is Eisenstein at 3, $[\mathcal{O} : \mathbf{Z}[\sqrt[3]{3}]]$ is not divisible by 3 by Theorem 2.3, so the index is 1: $\mathcal{O} = \mathbf{Z}[\sqrt[3]{3}]$.

Example 2.9. We show the ring $\mathcal{O}$ of algebraic integers of $\mathbf{Q}(\sqrt[3]{5})$ is $\mathbf{Z}[\sqrt[3]{5}]$. Since

$$\operatorname{disc}(\mathbf{Z}[\sqrt[3]{5}]) = [\mathcal{O} : \mathbf{Z}[\sqrt[3]{5}]]^2 \operatorname{disc}(\mathcal{O})$$

and the discriminant of $\mathbf{Z}[\sqrt[3]{5}]$ is $-3^3 \cdot 5^2$, $[\mathcal{O} : \mathbf{Z}[\sqrt[3]{5}]]$ is a factor of 15. Since $T^3 - 5$ is Eisenstein at 5, 5 does not divide $[\mathcal{O} : \mathbf{Z}[\sqrt[3]{5}]]$ by Theorem 2.3. The number $1 + \sqrt[3]{5}$ is a root of $(T-1)^3 - 5 = T^3 - 3T^2 - 3T - 6$, which is Eisenstein at 3, so 3 does not divide $[\mathcal{O} : \mathbf{Z}[1 + \sqrt[3]{5}]]$, and $\mathbf{Z}[1 + \sqrt[3]{5}] = \mathbf{Z}[\sqrt[3]{5}]$, so $[\mathcal{O} : \mathbf{Z}[\sqrt[3]{5}]]$ is not divisible by 3. Therefore this index is 1, so $\mathcal{O} = \mathbf{Z}[\sqrt[3]{5}]$.

Example 2.10. We show the ring $\mathcal{O}$ of algebraic integers of $\mathbf{Q}(\sqrt[3]{6})$ is $\mathbf{Z}[\sqrt[3]{6}]$. Since

$$\operatorname{disc}(\mathbf{Z}[\sqrt[3]{6}]) = [\mathcal{O} : \mathbf{Z}[\sqrt[3]{6}]]^2 \operatorname{disc}(\mathcal{O})$$

and the discriminant of $\mathbf{Z}[\sqrt[3]{6}]$ is $-2^2 \cdot 3^5$, $[\mathcal{O} : \mathbf{Z}[\sqrt[3]{6}]]$ divides $2 \cdot 3^2$. Since $T^3 - 6$ is Eisenstein at 2 and 3, $[\mathcal{O} : \mathbf{Z}[\sqrt[3]{5}]]$ is not divisible by 2 or 3 by Theorem 2.3. Therefore this index is 1, so $\mathcal{O} = \mathbf{Z}[\sqrt[3]{6}]$.

Example 2.11. We show the ring $\mathcal{O}$ of algebraic integers of $\mathbf{Q}(\sqrt[3]{7})$ is $\mathbf{Z}[\sqrt[3]{7}]$. Since

$$\operatorname{disc}(\mathbf{Z}[\sqrt[3]{7}]) = [\mathcal{O} : \mathbf{Z}[\sqrt[3]{7}]]^2 \operatorname{disc}(\mathcal{O})$$

and the discriminant of $\mathbf{Z}[\sqrt[3]{7}]$ is $-3^3 \cdot 7^2$, $[\mathcal{O} : \mathbf{Z}[\sqrt[3]{7}]]$ is a factor of 21. Since $T^3 - 7$ is Eisenstein at 7, 7 does not divide $[\mathcal{O} : \mathbf{Z}[\sqrt[3]{7}]]$ by Theorem 2.3. The number $-1 + \sqrt[3]{7}$ is a root of $(T+1)^3 - 7 = T^3 + 3T^2 + 3T - 6$, which is Eisenstein at 3, so 3 does not divide $[\mathcal{O} : \mathbf{Z}[-1 + \sqrt[3]{7}]] = [\mathcal{O} : \mathbf{Z}[\sqrt[3]{7}]]$. Therefore $[\mathcal{O} : \mathbf{Z}[\sqrt[3]{7}]]$ is 1, so $\mathcal{O} = \mathbf{Z}[\sqrt[3]{7}]$.

Example 2.12. As a final use of Theorem 2.3, 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 $f_i(T)$:

$$f_1(T) = T^3 - 18T - 6, \quad f_2(T) = T^3 - 36T - 78, \quad f_3(T) = T^3 - 54T - 150. \tag{2.4}$$

These polynomials are each Eisenstein at both 2 and 3, so they are irreducible over $\mathbf{Q}$. Each polynomial has the same discriminant: $22356 = 2^2 \cdot 3^5 \cdot 23$. (Recall $\operatorname{disc}(T^3 + aT + b) = -4a^3 - 27b^2$.) Let's show $\mathbf{Z}[\alpha_i]$ is the ring of integers of K_i in each case. Since $22356 = \operatorname{disc}(\mathbf{Z}[\alpha_i]) = [\mathcal{O}_{K_i} : \mathbf{Z}[\alpha_i]]^2 \operatorname{disc}(\mathcal{O}_{K_i})$, $[\mathcal{O}_{K_i} : \mathbf{Z}[\alpha_i]]$ 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 Theorem 2.3. That proves the index is 1 in all three cases. Therefore

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

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 cubic polynomials f_i each have 3 real roots.

So far the K_i's seem to be quite similar. Are they isomorphic fields? No. To prove this, we show some prime numbers 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 (2.4). We factor $f_i(T)$ mod p for the first few primes p in the table below.

p	$f_1(T)$ mod p	$f_2(T)$ mod p	$f_3(T)$ mod p
2	T^3	T^3	T^3
3	T^3	T^3	T^3
5	irred.	irred.	$T(T-2)(T-3)$
7	$(T-4)(T^2+4T+5)$	$(T-5)(T^2+5T+3)$	$(T-1)(T^2+T+3)$
11	$(T-3)(T-9)(T-10)$	irred.	irred.

The key rows are $p = 5$ and $p = 11$: 5 stays prime in K_1 and K_2 but not in K_3, and 11 stays prime in K_2 and K_3 but not in K_1. This is enough to distinguish each field from the other two.

3. The Eisenstein condition and total ramification

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

Theorem 3.1. *Let $K = \mathbf{Q}(\alpha)$, where α is the root of a polynomial that is Eisenstein at p. Then p is totally ramified in K.*

Theorem 3.2. *Let K be a number field, and suppose a prime p is totally ramified in K. Then $K = \mathbf{Q}(\alpha)$ for some α that is the root of an Eisenstein polynomial at p.*

Let's illustrate Theorem 3.1.

Example 3.3. Since $\sqrt[3]{10}$ is a root of $T^3 - 10$, which is Eisenstein at 2 and 5, 2 and 5 are totally ramified in $K = \mathbf{Q}(\sqrt[3]{10})$: $(2) = \mathfrak{p}^3$ and $(5) = \mathfrak{q}^3$ in $\mathcal{O}_K$. (The ring of integers is *not* $\mathbf{Z}[\sqrt[3]{10}]$: $\alpha = \frac{1}{3}(1 + \sqrt[3]{10} + \sqrt[3]{100})$ is a root of $T^3 - T^2 - 3T - 3$, and in fact $\mathcal{O}_K = \mathbf{Z}[\alpha]$.)

Example 3.4. Let $K = \mathbf{Q}(\sqrt{-5})$. Since $K = \mathbf{Q}(1 + \sqrt{-5})$ and $1 + \sqrt{-5}$ 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 $(2, 1 + \sqrt{-5})$.

Now we prove Theorem 3.1.

Proof. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ that 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

$$(p) = \mathfrak{p}^e \mathfrak{a}, \tag{3.1}$$

where $\mathfrak{p}$ does not divide $\mathfrak{a}$. Then $e \leq n$. We will show $e = n$, which implies by taking ideal norms in (3.1) that $p^n = \mathrm{N}(\mathfrak{p})^n \, \mathrm{N}(\mathfrak{a})$. Since $\mathrm{N}(\mathfrak{p})$ is a power of p, this equation implies $\mathrm{N}(\mathfrak{p}) = p$, so $\mathrm{N}(\mathfrak{a}) = 1$ and thus $\mathfrak{a} = (1)$.

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

$$f(T) = T^n + c_{n-1}T^{n-1} + \cdots + c_1 T + c_0.$$

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

$$\alpha \equiv 0 \bmod \mathfrak{p}, \tag{3.2}$$

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 (3.2) that

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

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

$$\alpha^n + c_0 \equiv 0 \bmod \mathfrak{p}^{e+1}. \tag{3.3}$$

Since c_0 is divisible by p exactly once, and $p\mathcal{O}_K$ divisible by $\mathfrak{p}^e$ but not $\mathfrak{p}^{e+1}$, unique factorization of ideals implies that $c_0\mathcal{O}_K$ is divisible by $\mathfrak{p}^e$ but not $\mathfrak{p}^{e+1}$. (Here are details on that. Write $c_0 = pb$, where b is an integer that is relatively prime to p, so $c_0\mathcal{O}_K = p\mathcal{O}_K b\mathcal{O}_K = \mathfrak{p}^e\mathfrak{a}(b\mathcal{O}_K)$, using (3.1). Thus $\mathfrak{p}^e$ divides $c_0\mathcal{O}_K$. If $\mathfrak{p}^{e+1}$ divided $c_0\mathcal{O}_K$ then $\mathfrak{p} \mid b\mathcal{O}_K$, so $b \in b\mathcal{O}_K \subset \mathfrak{p}$, so $b \in \mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$, which is false.) In terms of congruences, $c_0 \equiv 0 \bmod \mathfrak{p}^e$ and $c_0 \not\equiv 0 \bmod \mathfrak{p}^{e+1}$. Combining this with (3.3) 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 $\mathfrak{p}^n$, the condition $\alpha^n \not\equiv 0 \bmod \mathfrak{p}^{e+1}$ implies $n < e+1$. Therefore $n \leq e$. Since $e \leq n$, the only choice is $e = n$. □

Corollary 3.5. *If $K = \mathbf{Q}(\alpha)$ where α is the root of an Eisenstein polynomial at p and $\mathfrak{p}$ is the unique prime lying over p in $\mathcal{O}_K$, then (α) is divisible by $\mathfrak{p}$ exactly once.*

Proof. Using notation of the proof of Theorem 3.1, (3.3) tells us $\alpha^n + c_0 \equiv 0 \bmod \mathfrak{p}^{n+1}$ since $e = n$. Also $\alpha^n \equiv 0 \bmod \mathfrak{p}^n$ and $\alpha^{n+1} \not\equiv 0 \bmod \mathfrak{p}^{n+1}$, so $\mathfrak{p}^n$ is the highest power of $\mathfrak{p}$ dividing $(\alpha^n) = (\alpha)^n$. By unique factorization of ideals, $\mathfrak{p}$ is the highest power of $\mathfrak{p}$ dividing (α). □

The proof of Theorem 3.2 will tell us quite explicitly how to find the element α that 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 a number in $\mathfrak{p}$ that 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 $\alpha \in \mathfrak{p} - \mathfrak{p}^2$,

$$(\alpha) = \mathfrak{p}\mathfrak{a}, \tag{3.4}$$

where $\mathfrak{p}$ does not divide $\mathfrak{a}$. Taking ideal norms in (3.4),

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

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 $a_0, \dots, a_{i-1} \equiv 0 \bmod p$. 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 $p\mathcal{O}_K$:

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_i\alpha^i \equiv 0 \bmod p\mathcal{O}_K. \tag{3.5}$$

Raising both sides of (3.4) to the n-th power,

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

so

$$\alpha^n \in p\mathcal{O}_K. \tag{3.6}$$

Multiply through (3.5) by α^{n-1-i}, and take into account (3.6):

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

Write this congruence as an equation, say $a_i\alpha^{n-1} = p\gamma$, and take norms down to $\mathbf{Q}$:

$$a_i^n \operatorname{N}_{K/\mathbf{Q}}(\alpha)^{n-1} = p^n \operatorname{N}_{K/\mathbf{Q}}(\gamma).$$

The right side is an integral multiple of p^n. The left side is $a_i^n \operatorname{N}_{K/\mathbf{Q}}(\alpha)^{n-1} = \pm a_i^n a_0^{n-1}$, and a_0 is divisible by p just once, so $a_i^n a_0^{n-1}$ being divisible by p^n forces p to divide a_i. Thus, by induction, every a_i is a multiple of p. □

Theorem 3.6. *Let $K = \mathbf{Q}(\alpha)$ where $\alpha \in \mathcal{O}_K$ is the root of an Eisenstein polynomial at p, with degree n. Then $p^{n-1} || \operatorname{disc}(K)$ if $p \nmid n$ and $p^n \mid \operatorname{disc}(K)$ if $p \mid n$.*

Proof. We will first show $p^{n-1} \mid \operatorname{disc}(K)$ and then refine this to show $p^{n-1} || \operatorname{disc}(K)$ if $p \nmid n$ and $p^n \mid \operatorname{disc}(K)$ if $p \mid n$.

Let the minimal polynomial of α over $\mathbf{Q}$ be $f(T) = \sum_{i=0}^n c_iT^i$, so by hypothesis this is monic and Eisenstein at p: $c_n = 1$, $p \mid c_i$ for $i < n$, and $p^2 \nmid c_0$. 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'll use the formula

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

to examine the highest power of p dividing $\operatorname{disc}(\mathbf{Z}[\alpha])$.

We have

$$f'(\alpha) = n\alpha^{n-1} + (n-1)c_{n-1}\alpha^{n-2} + \cdots + 2c_2\alpha + c_1. \tag{3.7}$$

By Theorem 3.1 and Corollary 3.5, $(p) = \mathfrak{p}^n$ and $(\alpha) = \mathfrak{p}\mathfrak{a}$ with $\mathfrak{p} \nmid \mathfrak{a}$. Since each c_i for $i < n$ is divisible by p and thus by $\mathfrak{p}^n$, all terms on the right side of (3.7) except the first term are divisible by $\mathfrak{p}^n$. Collecting together all terms on the right in (3.7) except the first term,

$$f'(\alpha) = n\alpha^{n-1} + \beta, \text{ where } \beta \in \mathfrak{p}^n. \tag{3.8}$$

Since (α) is divisible by $\mathfrak{p}$, (α^{n-1}) is divisible by $\mathfrak{p}^{n-1}$, so (3.8) implies $(f'(\alpha))$ is divisible by $\mathfrak{p}^{n-1}$. Therefore $\operatorname{N}_{K/\mathbf{Q}}(f'(\alpha))$ is divisible by $\operatorname{N}(\mathfrak{p})^{n-1} = p^{n-1}$.

If $p \nmid n$, we want to show $p^{n-1} || \operatorname{N}_{K/\mathbf{Q}}(f'(\alpha))$. We will prove the contrapositive: if $p^n \mid \operatorname{N}_{K/\mathbf{Q}}(f'(\alpha))$ then $p \mid n$. The only prime over p in $\mathcal{O}_K$ is $\mathfrak{p}$, which has ideal norm p, and the ideal $(f'(\alpha))$ has norm $|\operatorname{N}_{K/\mathbf{Q}}(f'(\alpha))|$, so $\mathfrak{p}^n \mid (f'(\alpha))$. Then (3.8) implies $n\alpha^{n-1} \equiv 0 \bmod \mathfrak{p}^n$. The highest power of $\mathfrak{p}$ dividing (α) is $\mathfrak{p}$, so the highest power of $\mathfrak{p}$ dividing $(\alpha)^{n-1}$ is $\mathfrak{p}^{n-1}$. Therefore $\mathfrak{p} \mid (n)$, so $p \mid n$.

If $p \mid n$, we want to show $p^n \mid \mathrm{N}_{K/\mathbf{Q}}(f'(\alpha))$. Since $\mathfrak{p}$ is the only prime over p, $n \equiv 0 \bmod \mathfrak{p}$, so both terms on the right side of (3.8) are divisible by $\mathfrak{p}^n$. Thus $\mathrm{N}(\mathfrak{p}^n)$ divides $\mathrm{N}((f'(\alpha))) = |\,\mathrm{N}_{K/\mathbf{Q}}(f'(\alpha))|$. □

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 3.7. Let K be a number field. A monic polynomial

$$f(T) = T^n + c_{n-1}T^{n-1} + \cdots + c_1 T + c_0 \in \mathcal{O}_K[T]$$

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 3.8. *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 g and h are monic, their coefficients are polynomials in their roots with $\mathbf{Z}$-coefficients, 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 each 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 3.1 and 3.2 generalize as follows.

Theorem 3.9. *Let F be a number field and $E = F(\alpha)$, where α is the root of a polynomial in $\mathcal{O}_F[T]$ that is Eisenstein at a prime $\mathfrak{p}$ in $\mathcal{O}_F$. 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 3.10. *Let E/F be a finite extension of number fields, and suppose there is a prime $\mathfrak{p}$ of $\mathcal{O}_F$ that is totally ramified in E. Then $E = F(\alpha)$ for some α that 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 $\mathbf{Q}$.

Remark 3.11. I first learned about results like Theorems 3.1 and 3.2, connecting Eisenstein polynomials to total ramification, from exercise 9 in [1, Chap. 3, Sect. 5] about totally ramified primes in a finite extension of the fraction field of a Krull domain (which includes the integers of a number field as a special case) and from the first proposition in [2, Chap. III, Sect. 3] about totally ramified extensions of the p-adic numbers.

4. A ring of integers without a power basis

Using Eisenstein polynomials, we'll describe many pure cubic fields $\mathbf{Q}(\sqrt[3]{m})$ whose ring of integers does not have the form $\mathbf{Z}[\alpha]$.

Theorem 4.1. *Let p and q be distinct primes not equal to 3 such that $pq^2 \not\equiv \pm 1 \bmod 9$. The cubic field $K = \mathbf{Q}(\sqrt[3]{pq^2})$ has ring of integers $\mathbf{Z} + \mathbf{Z}\sqrt[3]{pq^2} + \mathbf{Z}\sqrt[3]{p^2q}$ and discriminant $-27p^2q^2$. The ramified primes in K are 3, p, and q, and they are all totally ramified. If $p \bmod q$ or $q \bmod p$ is not a cube then $\mathcal{O}_K \neq \mathbf{Z}[\gamma]$ for every $\gamma \in \mathcal{O}_K - \mathbf{Z}$.*

Proof. Set $\alpha = \sqrt[3]{pq^2}$ and $\beta = \sqrt[3]{p^2q} = \alpha^2/q$. Then α is a root of $T^3 - pq^2$ and β is a root of $T^3 - p^2q$, which are Eisenstein at p and q, respectively. Since pq^2 is not divisible by 3 and is not $\pm 1 \bmod 9$, we have $pq^2 \equiv 2, 4, 5,$ or $7 \bmod 9$. Therefore pq^2 is 1 away from 3 or 6 mod 9, which makes one of $pq^2 \pm 1$ divisible by 3 precisely once. That means one of the polynomials

$$(T+1)^3 - pq^2 = T^3 + 3T^2 + 3T + (1 - pq^2) \quad \text{with root } \alpha - 1 \tag{4.1}$$

or

$$(T-1)^3 - pq^2 = T^3 + 3T^2 + 3T - (1 + pq^2) \quad \text{with root } \alpha + 1 \tag{4.2}$$

is Eisenstein at 3. Therefore by Theorem 2.3,

$$p \nmid [\mathcal{O}_K : \mathbf{Z}[\alpha]], \quad q \nmid [\mathcal{O}_K : \mathbf{Z}[\beta]], \quad 3 \nmid [\mathcal{O}_K : \mathbf{Z}[\alpha \pm 1]] \tag{4.3}$$

for some choice of sign in the last relation, and $\mathbf{Z}[\alpha \pm 1] = \mathbf{Z}[\alpha]$ for either sign.

We will show the abelian group $R = \mathbf{Z} + \mathbf{Z}\alpha + \mathbf{Z}\beta$ equals $\mathcal{O}_K$. First of all, R is a ring since $\alpha^2 = q\beta$, $\beta^2 = p\alpha$, and $\alpha\beta = pq$, and R contains both $\mathbf{Z}[\alpha] = \mathbf{Z} + \mathbf{Z}\alpha + \mathbf{Z}q\beta$ with index q and $\mathbf{Z}[\beta] = \mathbf{Z} + \mathbf{Z}\beta + \mathbf{Z}p\alpha$ with index p. We have

$$\operatorname{disc}(\mathbf{Z}[\alpha]) = -27(pq^2)^2 = -3^3p^2q^4 = [\mathcal{O}_K : \mathbf{Z}[\alpha]]^2 \operatorname{disc}(K) \tag{4.4}$$

and

$$\operatorname{disc}(\mathbf{Z}[\beta]) = -27(p^2q)^2 = -3^3p^4q^2 = [\mathcal{O}_K : \mathbf{Z}[\beta]]^2 \operatorname{disc}(K). \tag{4.5}$$

By (4.3) and (4.4), $3^3p^2 \mid \operatorname{disc}(K)$, By (4.3) and (4.5), $q^2 \mid \operatorname{disc}(K)$. Thus $3^3p^2q^2 \mid \operatorname{disc}(K)$. Feeding this divisibility relation back into (4.4) and (4.5), $[\mathcal{O}_K : \mathbf{Z}[\alpha]] \mid q$ and $[\mathcal{O}_K : \mathbf{Z}[\beta]] \mid p$. We get reverse divisibility relations from

$$[\mathcal{O}_K : \mathbf{Z}[\alpha]] = [\mathcal{O}_K : R][R : \mathbf{Z}[\alpha]] = [\mathcal{O}_K : R]q \Longrightarrow q \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]] \tag{4.6}$$

and

$$[\mathcal{O}_K : \mathbf{Z}[\beta]] = [\mathcal{O}_K : R][R : \mathbf{Z}[\beta]] = [\mathcal{O}_K : R]p \Longrightarrow p \mid [\mathcal{O}_K : \mathbf{Z}[\beta]]. \tag{4.7}$$

Therefore $[\mathcal{O}_K : \mathbf{Z}[\alpha]] = q$ and $[\mathcal{O}_K : \mathbf{Z}[\beta]] = p$, so either (4.4) or (4.5) implies $\operatorname{disc}(K) = -3^3p^2q^2$. By the index equations in (4.6) or (4.7), $[\mathcal{O}_K : R] = 1$ and thus $\mathcal{O}_K = R$.

The prime factors of $\operatorname{disc}(K)$ are 3, p, and q, so these are the primes that ramify in K. They are totally ramified by Theorem 3.1 since K is generated by the root of an Eisenstein polynomial at p ($T^3 - pq^2$ with root α), at q ($T^3 - pq^2$ with root $\beta = \alpha^2/q$), and at 3 (one of the polynomials in (4.1) or (4.2), with root $\alpha \pm 1$).

To show there is no γ in $\mathcal{O}_K - \mathbf{Z}$ such that $\mathcal{O}_K = \mathbf{Z}[\gamma]$, we will show the index $[\mathcal{O}_K : \mathbf{Z}[\gamma]]$ is always greater than 1. Write $\gamma = a + b\alpha + c\beta$ for integers a, b, c with b and c not both 0.

Then $\mathbf{Z}[\gamma] = \mathbf{Z}[b\alpha + c\beta]$, so we may take $a = 0$. Writing $\{1, b\alpha + c\beta, (b\alpha + c\beta)^2\}$ as $\mathbf{Z}$-linear combinations of $\{1, \alpha, \beta\}$, we have

$$\begin{pmatrix} 1 \\ b\alpha + c\beta \\ (b\alpha + c\beta)^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & b & c \\ 2pqbc & pc^2 & qb^2 \end{pmatrix} \begin{pmatrix} 1 \\ \alpha \\ \beta \end{pmatrix}.$$

since $\alpha^2 = q\beta$, $\beta^2 = p\alpha$, and $\alpha\beta = pq$. The determinant of the 3×3 matrix is $qb^3 - pc^3$, and this can't be 1 or -1 since if $qb^3 - pc^3 = \pm 1$ then $qb^3 \equiv \pm 1 \bmod p$ and $pc^3 \equiv \pm 1 \bmod q$, which imply $q \bmod p$ is a cube and $p \bmod q$ is cube. As long as either of those properties is not true, $[\mathcal{O}_K : \mathbf{Z}[\gamma]] > 1$ no matter which γ is used from $\mathcal{O}_K - \mathbf{Z}$. □

Remark 4.2. Since $[\mathcal{O}_K : \mathbf{Z}[\alpha]] = q$ and $[\mathcal{O}_K : \mathbf{Z}[\beta]] = p$, the set of all indices $[\mathcal{O}_K : \mathbf{Z}[\gamma]]$ does not have a common prime factor. That makes this example of a ring of integers not of the form $\mathbf{Z}[\gamma]$ more subtle than "Dedekind's field" $L = \mathbf{Q}(\theta)$ where $\theta^3 - \theta^2 - 2\theta - 8 = 0$, since $\mathcal{O}_L$ isn't of the form $\mathbf{Z}[\gamma]$ because all the indices $[\mathcal{O}_L : \mathbf{Z}[\gamma]]$ are even.[1]

Example 4.3. The primes $p = 13$ and $q = 2$ fit all the conditions of Theorem 4.1, with $pq^2 = 52 \equiv 7 \bmod 9$ and $2 \bmod 13$ not being a cube, so the ring of integers of $\mathbf{Q}(\sqrt[3]{52})$ is not of the form $\mathbf{Z}[\gamma]$.

Example 4.4. The primes $p = 7$ and $q = 5$ fit all the conditions of Theorem 4.1, with $pq^2 = 175 \equiv 4 \bmod 9$ and $5 \bmod 7$ not being a cube, so the ring of integers of $\mathbf{Q}(\sqrt[3]{175})$ is not of the form $\mathbf{Z}[\gamma]$.

Example 4.5. The primes $p = 7$ and $q = 2$ do *not* fit all the conditions of Theorem 4.1: $pq^2 = 28 \equiv 1 \bmod 9$. In $\mathbf{Q}(\sqrt[3]{28})$, it turns out that the ring $\mathbf{Z} + \mathbf{Z}\sqrt[3]{pq^2} + \mathbf{Z}\sqrt[3]{p^2q}$ is not all of $\mathcal{O}_K$ (it has index 3 in $\mathcal{O}_K$) and $\mathcal{O}_K$ has a power basis $\{1, \gamma, \gamma^2\}$ where $\gamma = (\sqrt[3]{28}^2 - 2\sqrt[3]{28} - 2)/6$ and γ has minimal polynomial $T^3 + T^2 + 5T - 1$. This polynomial modulo 3 is $(T-1)(T-2)^2$, so in $\mathcal{O}_K$ the prime 3 is ramified but not totally ramified: $3\mathcal{O}_K = \mathfrak{p}\mathfrak{q}^2$ for some prime ideals $\mathfrak{p}$ and $\mathfrak{q}$ of norm 3.

References

[1] V. I. Borevich and I. R. Shafarevich, "Number Theory," Academic Press, 1966.

[2] N. Koblitz, "p-adic Numbers, p-adic Analysis, and Zeta-functions," 2nd ed., Springer-Verlag, 1984.

[1] See Section 1 in https://kconrad.math.uconn.edu/blurbs/gradnumthy/nopowerbasis.pdf.