

DEDEKIND'S INDEX THEOREM

KEITH CONRAD

1. INTRODUCTION

Let $K = \mathbf{Q}(\alpha)$ where α is an algebraic integer with minimal polynomial $f(T) \in \mathbf{Z}[T]$. For a prime p , Dedekind [3, Sect. 2] showed the prime ideal decomposition of p in \mathcal{O}_K can be read off from the irreducible factorization of $f(T) \bmod p$ in $\mathbf{F}_p[T]$ provided $p \nmid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$:

$$(1.1) \quad f(T) \equiv \bar{\pi}_1(T)^{e_1} \cdots \bar{\pi}_g(T)^{e_g} \bmod p \implies p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g},$$

where $\bar{\pi}_1(T), \dots, \bar{\pi}_g(T)$ are distinct monic irreducibles in $\mathbf{F}_p[T]$, $N(\mathfrak{p}_i) = p^{\deg \bar{\pi}_i}$, and $\mathfrak{p}_i = (p, \pi_i(\alpha))$ where $\pi_i(T)$ is an arbitrary monic lift of $\bar{\pi}_i(T)$ to $\mathbf{Z}[T]$.

If $p \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$ then the factorization of $p\mathcal{O}_K$ may or may not match that of $f(T) \bmod p$.

Example 1.1. If $K = \mathbf{Q}(\sqrt[3]{12})$ and $f(T) = T^3 - 12$ then $f(T) \equiv T^3 \bmod 2$ and $2\mathcal{O}_K = \mathfrak{p}^3$, but the factorization of $2\mathcal{O}_K$ is not based on (1.1) with $\alpha = \sqrt[3]{12}$ since $[\mathcal{O}_K : \mathbf{Z}[\sqrt[3]{12}]] = 2$: $\mathcal{O}_K = \mathbf{Z} + \mathbf{Z}\sqrt[3]{12} + \mathbf{Z}\sqrt[3]{18} = \mathbf{Z} + \mathbf{Z}\sqrt[3]{12} + \mathbf{Z}\sqrt[3]{12}^2/2$.

We can instead rewrite K as $\mathbf{Q}(\sqrt[3]{18})$, set $f(T) = T^3 - 18$, and now $[\mathcal{O}_K : \mathbf{Z}[\sqrt[3]{18}]] = 3$, an index not divisible by 2, so the factorization $T^3 - 18 \equiv T^3 \bmod 2$ implies $2\mathcal{O}_K = \mathfrak{p}^3$.

Example 1.2. If $K = \mathbf{Q}(\sqrt[3]{10})$ and $f(T) = T^3 - 10$ then $f(T) \equiv (T-1)^3 \bmod 3$ but $3\mathcal{O}_K = \mathfrak{p}\mathfrak{q}^2$. Here $[\mathcal{O}_K : \mathbf{Z}[\sqrt[3]{10}]] = 3$. It turns out that $\mathcal{O}_K = \mathbf{Z}[\alpha]$ for $\alpha = (\sqrt[3]{10}^2 + \sqrt[3]{10} + 1)/3$, whose minimal polynomial over \mathbf{Q} is $T^3 - T^2 - 3T - 3$ and $T^3 - T^2 - 3T - 3 \equiv (T-1)T^2 \bmod 3$.

Example 1.3. The number $\alpha = \sqrt{10 + 3\sqrt{10}}$ is a root of $f(T) = T^4 - 20T^2 + 10$, which is irreducible over \mathbf{Q} (why?). Set $K = \mathbf{Q}(\alpha)$. We have $f(T) \equiv (T-1)^2(T-2)^2 \bmod 3$ but it turns out that 3 splits completely in K . Here $[\mathcal{O}_K : \mathbf{Z}[\alpha]] = 9$ and the factorization of $3\mathcal{O}_K$ can't be found by (1.1) since $3 \mid [\mathcal{O}_K : \mathbf{Z}[\beta]]$ for all β in \mathcal{O}_K such that $K = \mathbf{Q}(\beta)$.

We can apply (1.1) to primes not dividing $\text{disc}(f)$ since $[\mathcal{O}_K : \mathbf{Z}[\alpha]]^2 \mid \text{disc}(f)$. To know whether (1.1) applies to a prime dividing $\text{disc}(f)$, we want to know which prime factors of $\text{disc}(f)$ in fact divide $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$. For an arbitrary prime p , here is a necessary and sufficient condition for $p \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$ that does *not* require knowing \mathcal{O}_K .

Theorem 1.4. *Let $K = \mathbf{Q}(\alpha)$ where α is an algebraic integer with minimal polynomial $f(T) \in \mathbf{Z}[T]$. For a prime p , let the monic irreducible factorization of $f(T) \bmod p$ be*

$$(1.2) \quad f(T) \equiv \bar{\pi}_1(T)^{e_1} \cdots \bar{\pi}_g(T)^{e_g} \bmod p.$$

Let $\pi_j(T)$ be a monic lift of $\bar{\pi}_j(T)$ to $\mathbf{Z}[T]$ and define $F(T) \in \mathbf{Z}[T]$ by

$$(1.3) \quad f(T) = \pi_1(T)^{e_1} \cdots \pi_g(T)^{e_g} + pF(T).$$

Then $p \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]] \iff \bar{\pi}_j(T) \mid \bar{F}(T)$ in $\mathbf{F}_p[T]$ for some j such that $e_j \geq 2$.

This is due to Dedekind [3, Sect. 3], so we call it *Dedekind's index theorem*. (It is called Dedekind's criterion by Cohen [2, Theorem 6.1.4(2)] and Pohst and Zassenhaus [6, p. 295].)

2. EXAMPLES

Before proving Dedekind's index theorem, let's look at some examples of it at work. Since $[\mathcal{O}_K : \mathbf{Z}[\alpha]]^2 \mid \text{disc}(f)$, the only primes that might divide $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$ are primes dividing $\text{disc}(f)$ with multiplicity at least 2.

Example 2.1. Let $K = \mathbf{Q}(\sqrt[3]{12})$ and $f(T) = T^3 - 12$. Since $\text{disc}(f(T)) = -3888 = -2^4 \cdot 3^5$, the only possible prime factors of $[\mathcal{O}_K : \mathbf{Z}[\sqrt[3]{12}]]$ are 2 or 3.

Case 1: $p = 2$.

Since $f(T) \equiv T^3 \pmod{2}$, take $\pi_1(T) = T$. Write

$$f(T) = T^3 + 2F(T) \text{ for } F(T) = -6,$$

so $F(T) \equiv 0 \pmod{2}$. Therefore $\bar{\pi}_1(T) \mid \bar{F}(T)$ in $\mathbf{F}_2[T]$, so $\boxed{2 \mid [\mathcal{O}_K : \mathbf{Z}[\sqrt[3]{12}]]}$.

Case 2: $p = 3$.

Since $f(T) \equiv T^3 \pmod{3}$, take $\pi_1(T) = T$. Then

$$f(T) = T^3 + 3F(T) \text{ for } F(T) = -4,$$

so $\bar{\pi}_1(T) \nmid \bar{F}(T)$ in $\mathbf{F}_3[T]$. Thus $3 \nmid [\mathcal{O}_K : \mathbf{Z}[\sqrt[3]{12}]]$.

Example 2.2. Let $K = \mathbf{Q}(\sqrt[3]{10})$ and $f(T) = T^3 - 10$. Since $\text{disc}(f(T)) = -2700 = -2^2 \cdot 3^3 \cdot 5^2$, the only possible prime factors of $[\mathcal{O}_K : \mathbf{Z}[\sqrt[3]{10}]]$ are 2, 3, and 5.

Case 1: $p = 2$.

Since $f(T) \equiv T^3 \pmod{2}$, take $\pi_1(T) = T$. Then

$$f(T) = T^3 + 2F(T) \text{ for } F(T) = -5,$$

so $\bar{\pi}_1(T) \nmid \bar{F}(T)$ in $\mathbf{F}_2[T]$. Thus $2 \nmid [\mathcal{O}_K : \mathbf{Z}[\sqrt[3]{10}]]$.

Case 2: $p = 3$.

Since $f(T) \equiv (T - 1)^3 \pmod{3}$, take $\pi_1(T) = T - 1$. Then

$$f(T) = (T - 1)^3 + 3F(T) \text{ for } F(T) = T^2 - T - 3,$$

so $F(T) \equiv T(T - 1) \pmod{3}$. Thus $\bar{\pi}_1(T) \mid \bar{F}(T)$ in $\mathbf{F}_3[T]$, so $\boxed{3 \mid [\mathcal{O}_K : \mathbf{Z}[\sqrt[3]{10}]]}$.

Case 3: $p = 5$.

Since $f(T) \equiv T^3 \pmod{5}$, take $\pi_1(T) = T$. Then

$$f(T) = T^3 + 5F(T) \text{ for } F(T) = -2,$$

so $\bar{\pi}_1(T) \nmid \bar{F}(T)$ in $\mathbf{F}_5[T]$. Thus $5 \nmid [\mathcal{O}_K : \mathbf{Z}[\sqrt[3]{10}]]$.

Example 2.3. Let $K = \mathbf{Q}(\sqrt[3]{2})$ and $f(T) = T^3 - 2$, so $\text{disc}(f(T)) = -108 = -2^2 \cdot 3^3$. The only primes that might divide $[\mathcal{O}_K : \mathbf{Z}[\sqrt[3]{2}]]$ are 2 and 3.

Case 1: $p = 2$.

Since $f(T) \equiv T^3 \pmod{2}$, take $\pi_1(T) = T$. Then

$$f(T) = T^3 + 2F(T) \text{ for } F(T) = -1,$$

so $\bar{\pi}_1(T) \nmid \bar{F}(T)$ in $\mathbf{F}_2[T]$. Thus $2 \nmid [\mathcal{O}_K : \mathbf{Z}[\sqrt[3]{2}]]$.

Case 2: $p = 3$.

Since $f(T) \equiv (T + 1)^3 \pmod{3}$, take $\pi_1(T) = T + 1$. Then

$$f(T) = (T + 1)^3 + 3F(T) \text{ for } F(T) = -T^2 - T - 1,$$

so $F(T) \equiv -(T + 2)^2 \pmod{3}$. Thus $\bar{\pi}_1(T) \nmid \bar{F}(T)$ in $\mathbf{F}_3[T]$, so $3 \nmid [\mathcal{O}_K : \mathbf{Z}[\sqrt[3]{2}]]$.

By Cases 1 and 2, $[\mathcal{O}_K : \mathbf{Z}[\sqrt[3]{2}]] = 1$, so $\mathcal{O}_K = \mathbf{Z}[\sqrt[3]{2}]$.

Example 2.4. Let $K = \mathbf{Q}(\sqrt[3]{44})$ and $f(T) = T^3 - 44$. Since $\text{disc}(f(T)) = -52272 = -2^4 \cdot 3^3 \cdot 11^2$, the only possible prime factors of $[\mathcal{O}_K : \mathbf{Z}[\sqrt[3]{44}]]$ are 2, 3, and 11.

Case 1: $p = 2$.

From $f(T) \equiv T^3 \pmod{2}$, take $\pi_1(T) = T$. Then

$$f(T) = T^3 + 2F(T) \text{ for } F(T) = -22,$$

so $F(T) \equiv 0 \pmod{2}$. Therefore $\bar{\pi}_1(T) \mid \bar{F}(T)$ in $\mathbf{F}_2[T]$, so $2 \mid [\mathcal{O}_K : \mathbf{Z}[\sqrt[3]{44}]]$.

Case 2: $p = 3$.

From $f(T) \equiv (T+1)^3 \pmod{3}$, take $\pi_1(T) = T+1$. Then

$$f(T) = (T+1)^3 + 3F(T) \text{ for } F(T) = -T^2 - T - 15,$$

so $F(T) \equiv -T(T+1) \pmod{3}$, which shows $\bar{\pi}_1(T) \nmid \bar{F}(T)$ in $\mathbf{F}_3[T]$. Thus $3 \nmid [\mathcal{O}_K : \mathbf{Z}[\sqrt[3]{44}]]$.

Case 3: $p = 11$.

From $f(T) \equiv T^3 \pmod{11}$, take $\pi_1(T) = T$. Then

$$f(T) = T^3 + 11F(T) \text{ for } F(T) = -4,$$

so $\bar{\pi}_1(T) \nmid \bar{F}(T)$ in $\mathbf{F}_{11}[T]$. Thus $11 \nmid [\mathcal{O}_K : \mathbf{Z}[\sqrt[3]{44}]]$.

Example 2.5. Let $K = \mathbf{Q}(\alpha)$ where α is a root of $f(T) = T^3 - T^2 - 2T - 8$. Since $\text{disc}(f(T)) = -2012 = -2^2 \cdot 503$, the only prime that might divide $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$ is 2.

From $f(T) \equiv T^2(T+1) \pmod{2}$, take $\pi_1(T) = T$, and $\pi_2(T) = T+1$. Then

$$f(T) = T^2(T+1) + 2F(T) \text{ for } F(T) = -T^2 - T - 4,$$

so $F(T) \equiv T(T+1) \pmod{2}$. Since $\bar{\pi}_1(T) \mid \bar{F}(T)$ in $\mathbf{F}_2[T]$, $2 \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$.

Example 2.6. Let $K = \mathbf{Q}(\alpha)$ where α is a root of $f(T) = T^3 + 2T + 4$, which is irreducible over \mathbf{Q} since it is irreducible mod 3. Since $\text{disc}(f(T)) = -464 = -2^4 \cdot 29$, the only possible prime factor of $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$ is 2.

From $f(T) \equiv T^3 \pmod{2}$, take $\pi_1(T) = T$. Then

$$f(T) = T^3 + 2F(T) \text{ for } F(T) = T + 2,$$

so $F(T) \equiv T \pmod{2}$. Therefore $\bar{\pi}_1(T) \mid \bar{F}(T)$ in $\mathbf{F}_2[T]$, so $2 \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$.

Example 2.7. Let $K = \mathbf{Q}(\alpha)$ where α is a root of $f(T) = T^3 + 2T + 22$. Since $\text{disc}(f(T)) = -13100 = -2^2 \cdot 5^2 \cdot 131$, the only primes that might divide $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$ are 2 and 5.

Case 1: $p = 2$.

From $f(T) \equiv T^3 \pmod{2}$, take $\pi_1(T) = T$. Then

$$f(T) = T^3 + 2F(T) \text{ for } F(T) = T + 11,$$

so $F(T) \equiv T + 1 \pmod{2}$. Therefore $\bar{\pi}_1(T) \nmid \bar{F}(T)$ in $\mathbf{F}_2[T]$, so $2 \nmid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$.

Case 2: $p = 5$.

From $f(T) \equiv (T+2)(T-1)^2 \pmod{5}$, take $\pi_1(T) = T+2$ and $\pi_2(T) = T-1$. Then

$$f(T) = (T+2)(T-1)^2 + 5F(T) \text{ for } F(T) = T + 4,$$

so $F(T) \equiv T - 1 \pmod{5}$. Therefore $\bar{\pi}_2(T) \mid \bar{F}(T)$ in $\mathbf{F}_5[T]$, so $5 \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$.

Example 2.8. Let $K = \mathbf{Q}(\alpha)$ where $\alpha = \sqrt{10 + 3\sqrt{10}}$ is a root of $f(T) = T^4 - 20T^2 + 10$. Since $\text{disc}(f(T)) = 20736000 = 2^{11} \cdot 3^4 \cdot 5^3$, primes dividing $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$ can only be 2, 3, or 5.

Case 1: $p = 2$.

From $f(T) \equiv T^4 \pmod{2}$, take $\pi_1(T) = T$. Then

$$f(T) = T^4 + 2F(T) \text{ for } F(T) = -10T^2 + 5,$$

so $F(T) \equiv 1 \pmod{2}$. Therefore $\bar{\pi}_1(T) \nmid \bar{F}(T)$ in $\mathbf{F}_2[T]$, so $2 \nmid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$.

Case 2: $p = 3$.

From $f(T) \equiv (T-1)^2(T-2)^2 \pmod{3}$, take $\pi_1(T) = T-1$ and $\pi_2(T) = T-2$. Then

$$f(T) = (T-1)^2(T-2)^2 + 3F(T) \text{ for } F(T) = 2T^3 - 11T^2 + 4T + 2,$$

so $F(T) \equiv 2(T-1)^2(T-2) \pmod{3}$. Since $\bar{F}(T)$ in $\mathbf{F}_3[T]$ is divisible by $\bar{\pi}_1(T)$ (or $\bar{\pi}_2(T)$),

$$\boxed{3 \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]}.$$

Case 3: $p = 5$.

From $f(T) \equiv T^4 \pmod{5}$, take $\pi_1(T) = T$. Then

$$f(T) = T^4 + 5F(T) \text{ for } F(T) = -4T^2 + 2,$$

so $F(T) \equiv T^2 + 2 \pmod{5}$. Therefore $\bar{\pi}_1(T) \nmid \bar{F}(T)$ in $\mathbf{F}_5[T]$, so $5 \nmid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$.

Example 2.9. Let $K = \mathbf{Q}(\alpha)$ where α is a root of $f(T) = T^4 + 2T^2 + 3T + 1$. Since $\text{disc}(f(T)) = 117 = 3^2 \cdot 13$, the only prime that might divide $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$ is 3.

Since $f(T) \equiv (T^2 + 1)^2 \pmod{3}$, take $\pi_1(T) = T^2 + 1$. Then

$$f(T) = (T^2 + 1)^2 + 3F(T) \text{ for } F(T) = T,$$

so $\bar{\pi}_1(T) \nmid \bar{F}(T)$ in $\mathbf{F}_3[T]$. Therefore $3 \nmid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$, so $\mathcal{O}_K = \mathbf{Z}[\alpha]$.

Example 2.10. Let $K = \mathbf{Q}(\alpha)$ and $f(T) = T^4 + T^2 + 4$. Since $\text{disc}(f(T)) = 14400 = 2^6 \cdot 3^2 \cdot 5^2$, the only possible prime factors of $[\mathcal{O}_K : \mathbf{Z}[\sqrt[4]{5}]]$ are 2, 3, and 5.

Case 1: $p = 2$.

From $f(T) \equiv T^2(T+1)^2 \pmod{2}$, take $\pi_1(T) = T$ and $\pi_2(T) = T+1$. Then

$$f(T) = T^2(T+1)^2 + 2F(T) \text{ for } F(T) = -T^3 + 2,$$

so $F(T) \equiv T^3 \pmod{2}$. Therefore $\bar{\pi}_1(T) \mid \bar{F}(T)$ in $\mathbf{F}_2[T]$, so $\boxed{2 \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]}$.

Case 2: $p = 3$.

From $f(T) \equiv (T+1)^2(T+2)^2 \pmod{3}$, take $\pi_1(T) = T+1$ and $\pi_2(T) = T+2$. Then

$$f(T) = (T+1)^2(T+2)^2 + 3F(T) \text{ for } F(T) = -2T^3 - 4T^2 - 4T,$$

so $F(T) \equiv T(T^2 + 2T + 2) \pmod{3}$. In $\mathbf{F}_3[T]$, $\bar{F}(T)$ is not divisible by $\bar{\pi}_1(T)$ or $\bar{\pi}_2(T)$, so $3 \nmid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$.

Case 3: $p = 5$.

From $f(T) \equiv (T^2 - 2)^2 \pmod{5}$, take $\pi_1(T) = T^2 - 2$. Then

$$f(T) = (T^2 - 2)^2 + 5F(T) \text{ for } F(T) = T^2,$$

so $\bar{F}(T)$ in $\mathbf{F}_5[T]$ is not divisible by $\bar{\pi}_1(T)$ or $\bar{\pi}_2(T)$. Therefore $5 \nmid [\mathcal{O}_K : \mathbf{Z}[\sqrt[4]{5}]]$.

Example 2.11. Let's generalize Example 2.6. Say $f(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_1T + a_0$ in $\mathbf{Z}[T]$ for $n \geq 2$ and $p \mid a_j$ for all j . Then $f(T) \equiv T^n \pmod{p}$, so

$$f(T) = T^n + pF(T) \text{ for } F(T) = \frac{a_{n-1}}{p}T^{n-1} + \cdots + \frac{a_1}{p}T + \frac{a_0}{p}.$$

By Dedekind's index theorem with $\pi_1(T) = T$, $p \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$ if and only if $\overline{F}(T)$ is divisible by T in $\mathbf{F}_p[T]$, which is equivalent to $p^2 \mid a_0$ in \mathbf{Z} . Thus $p \nmid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$ if and only if $p^2 \nmid a_0$, which is equivalent to $f(T)$ being Eisenstein at p . (This is false for $n = 1$, e.g., $f(T) = T$.)

Example 2.12. Suppose $f(T) \bmod p$ is separable. Then every e_j is 1 in Theorem 1.4, so $p \nmid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$. That also follows from the fact that $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$ divides $\text{disc}(f)$ and $\text{disc}(f) \not\equiv 0 \bmod p$ by separability of $f(T) \bmod p$.

Example 2.13. Let $f_n(T) = T^n - T - 1$. For each $n \geq 2$, $f_n(T)$ is irreducible over \mathbf{Q} .¹ There is a general discriminant formula

$$\text{disc}(T^n + aT + b) = (-1)^{n(n-1)/2}((-1)^{n-1}(n-1)^{n-1}a^n + n^n b^{n-1}),$$

and for $a = -1$ and $b = -1$ this becomes

$$\text{disc}(f_n(T)) = (-1)^{n(n-1)/2+1}((n-1)^{n-1} + (-n)^n).$$

Let $K_n = \mathbf{Q}(\alpha_n)$, where α_n is a root of $f_n(T)$, so $[K_n : \mathbf{Q}] = n$. Numerical data suggest $\text{disc}(f_n(T))$ is nearly always squarefree. When it is squarefree, $\mathcal{O}_{K_n} = \mathbf{Z}[\alpha_n]$. The first n where $\text{disc}(f_n(T))$ is not squarefree is $n = 130$, with $\text{disc}(f_{130}(T))$ divisible by 83^2 (and not by the square of another prime). It turns out that

$$(2.1) \quad T^{130} - T - 1 \equiv (T-8)^2(T-20)\overline{\pi}_{22}(T)\overline{\pi}_{42}(T)\overline{\pi}_{63}(T) \bmod 83$$

where $\overline{\pi}_d(T)$ is monic irreducible of degree d in $\mathbf{F}_{83}[T]$. We'll use Dedekind's index theorem to show $83 \mid [\mathcal{O}_{K_{130}} : \mathbf{Z}[\alpha_{130}]]$.

Let $\pi_d(T)$ be a monic lift of $\overline{\pi}_d(T)$ to $\mathbf{Z}[T]$, so

$$T^{130} - T - 1 = (T-8)^2(T-20)\pi_{22}(T)\pi_{42}(T)\pi_{63}(T) + 83F(T)$$

for some $F(T) \in \mathbf{Z}[T]$. The only repeated factor of $T^{130} - T - 1 \bmod 83$ is $(T-8)^2$, and it turns out that $F(8) \equiv 0 \bmod 83$, so $(T-8) \mid \overline{F}(T)$ in $\mathbf{F}_{83}[T]$. Therefore $[\mathcal{O}_{K_{130}} : \mathbf{Z}[\alpha_{130}]]$ is divisible by 83.

3. PROOF OF DEDEKIND'S INDEX THEOREM

Now we'll prove Dedekind's index theorem using Dedekind's argument in [3, Sect. 3].

Proof. (\Leftarrow) We prove the contrapositive: if $p \nmid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$ then $\overline{\pi}_j(T) \nmid \overline{F}(T)$ in $\mathbf{F}_p[T]$ whenever $e_j \geq 2$, where e_j is taken from (1.2).

If $\overline{\pi}_j(T) \mid \overline{F}(T)$ in $\mathbf{F}_p[T]$ for some j then $F(T) = \pi_j(T)A(T) + pB(T)$ for some $A(T)$ and $B(T)$ in $\mathbf{Z}[T]$, which upon setting $T = \alpha$ shows $F(\alpha) \in (p, \pi_j(\alpha))$. Thanks to (1.1), which can be used since $p \nmid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$, we have $\mathfrak{p}_j = (p, \pi_j(\alpha))$, so $\mathfrak{p}_j \mid (F(\alpha))$. We will show for $e_j \geq 2$ that $\mathfrak{p}_j \nmid (F(\alpha))$, so $\overline{\pi}_j(T) \nmid \overline{F}(T)$ in $\mathbf{F}_p[T]$.

In (1.3), set $T = \alpha$ to get

$$\pi_1(\alpha)^{e_1} \cdots \pi_g(\alpha)^{e_g} = -pF(\alpha),$$

so we have an equation of principal ideals

$$(3.1) \quad (\pi_1(\alpha))^{e_1} \cdots (\pi_g(\alpha))^{e_g} = (p)(F(\alpha)).$$

To get $\mathfrak{p}_j \nmid (F(\alpha))$ from this, we'll compute the highest power of \mathfrak{p}_j on both sides.

Since $\mathfrak{p}_j = (p, \pi_j(\alpha)) = \gcd((p), (\pi_j(\alpha)))$ and $e_j \geq 2$, $\mathfrak{p}_j^2 \mid (p)$ by the factorization of (p) in (1.1). Thus $\mathfrak{p}_j^2 \nmid (\pi_j(\alpha))$, so \mathfrak{p}_j divides $(\pi_j(\alpha))$ just once. For $i \neq j$, \mathfrak{p}_i and \mathfrak{p}_j are distinct

¹See <https://kconrad.math.uconn.edu/blurbs/ringtheory/irredselpoly.pdf>.

prime ideals, so $\mathfrak{p}_j \nmid (\pi_i(\alpha))$, (otherwise \mathfrak{p}_j divides $\gcd((p), (\pi_i(\alpha))) = \mathfrak{p}_i$, which it doesn't). On the left side of (3.1), the highest power of \mathfrak{p}_j in its factorization is therefore e_j . Since $\mathfrak{p}_j^{e_j} \mid (p)$, (3.1) tells us $\mathfrak{p}_j \nmid (F(\alpha))$.

(\implies) Assuming $p \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$, we will show $\overline{F}(T)$ is divisible by some $\overline{\pi}_j(T)$ in $\mathbf{F}_p[T]$ such that $\overline{\pi}_j(T)^2 \mid \overline{f}(T)$ (i.e., $e_j \geq 2$ in (1.2)).

That $\mathcal{O}_K/\mathbf{Z}[\alpha]$ has order divisible by p implies some $\beta \in \mathcal{O}_K$ is in $(1/p)\mathbf{Z}[\alpha] - \mathbf{Z}[\alpha]$. Therefore

$$p\beta = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}$$

where $n = [K : \mathbf{Q}] = \deg f$ and the coefficients c_j are integers where at least one of them is not divisible by p . In $\mathbf{F}_p[T]$, set

$$\overline{A}(T) = \gcd(\overline{c}_0 + \overline{c}_1T + \cdots + \overline{c}_{n-1}T^{n-1}, \overline{f}(T)).$$

This is a proper factor of $\overline{f}(T)$ since the first term in the gcd is nonzero of degree less than n , and for simplicity take $\overline{A}(T)$ to be a monic gcd. Write

$$(3.2) \quad \overline{f}(T) = \overline{A}(T)\overline{B}(T) \text{ in } \mathbf{F}_p[T],$$

so $\overline{B}(T)$ is monic and nonconstant.

By unique factorization in $\mathbf{F}_p[T]$, $\overline{A}(T)$ and $\overline{B}(T)$ are complementary factors in the irreducible factorization $\prod_{j=1}^g \overline{\pi}_j(T)^{e_j}$ of $\overline{f}(T)$. Let $A(T)$ and $B(T)$ be the monic lifts of $\overline{A}(T)$ and $\overline{B}(T)$ to $\mathbf{Z}[T]$ that are built from the monic lifts $\pi_j(T)$ of $\overline{\pi}_j(T)$, so

$$A(T)B(T) = \prod_{j=1}^g \pi_j(T)^{e_j} = f(T) - pF(T).$$

Setting $T = \alpha$,

$$(3.3) \quad A(\alpha)B(\alpha) = -pF(\alpha).$$

In $\mathbf{F}_p[T]$, we can write $\overline{A}(T)$ as an $\mathbf{F}_p[T]$ -linear combination using its definition as a gcd:

$$\overline{A}(T) = (\overline{c}_0 + \overline{c}_1T + \cdots + \overline{c}_{n-1}T^{n-1})u(T) + \overline{f}(T)v(T).$$

We can set $T = \alpha$ on both sides as long as we view the values on both sides in $\mathcal{O}_K/p\mathcal{O}_K$:

$$A(\alpha) \equiv (c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1})u(\alpha) \equiv (p\beta)u(\alpha) \equiv 0 \pmod{p\mathcal{O}_K}$$

since $\beta \in \mathcal{O}_K$. Thus $\boxed{p \mid A(\alpha)}$ in \mathcal{O}_K .

Since $A(\alpha)/p$ is an algebraic integer in K , it satisfies a monic relation of integral dependence over \mathbf{Z} , say

$$\left(\frac{A(\alpha)}{p}\right)^d + a_{d-1}\left(\frac{A(\alpha)}{p}\right)^{d-1} + \cdots + a_1\left(\frac{A(\alpha)}{p}\right) + a_0 = 0$$

for some $d \geq 1$ and integers a_0, \dots, a_{d-1} . Multiply through by p^d :

$$(3.4) \quad A(\alpha)^d + pa_{d-1}A(\alpha)^{d-1} + \cdots + p^{d-1}a_1A(\alpha) + p^da_0 = 0.$$

Every polynomial in $\mathbf{Z}[T]$ vanishing at α is divisible by $f(T)$ in $\mathbf{Z}[T]$, so

$$A(T)^d + pa_{d-1}A(T)^{d-1} + \cdots + p^{d-1}a_1A(T) + p^da_0 = f(T)h(T)$$

for some $h(T) \in \mathbf{Z}[T]$. Reducing both sides modulo p ,

$$\overline{A}(T)^d = \overline{f}(T)\overline{h}(T) = \overline{A}(T)\overline{B}(T)\overline{h}(T)$$

in $\mathbf{F}_p[T]$. Therefore each irreducible factor of $\overline{B}(T)$ in $\mathbf{F}_p[T]$ divides $\overline{A}(T)$.

We explained earlier why $\overline{B}(T)$ is nonconstant, so $\overline{B}(T)$ has a monic irreducible factor, say $\overline{\pi}(T)$. Then $\overline{\pi}(T) \mid \overline{A}(T)$ too, so $\overline{\pi}(T)^2 \mid \overline{f}(T)$ by (3.2). That shows $\overline{\pi}(T)$ is some $\overline{\pi}_j(T)$ where $e_j \geq 2$. Next we will show $\overline{\pi}(T) \mid \overline{F}(T)$.

Multiply both sides of (3.4) by $B(\alpha)^d$ and use (3.3):

$$p^d(-F(\alpha))^d + p^d a_{d-1} B(\alpha)(-F(\alpha))^{d-1} + \cdots + p^d a_1 B(\alpha)^{d-1}(-F(\alpha)) + p^d a_0 B(\alpha)^d = 0.$$

Each term on the left has a factor p^d , so divide through by p^d :

$$(-F(\alpha))^d + a_{d-1} B(\alpha)(-F(\alpha))^{d-1} + \cdots + a_1 B(\alpha)^{d-1}(-F(\alpha)) + a_0 B(\alpha)^d = 0.$$

Therefore

$$(-F(T))^d + a_{d-1} B(T)(-F(T))^{d-1} + \cdots + a_1 B(T)^{d-1}(-F(T)) + a_0 B(T)^d = f(T)k(T)$$

for some $k(T) \in \mathbf{Z}[T]$. Reduce both sides modulo p . Since $\overline{f}(T)$ and $\overline{B}(T)$ are divisible by $\overline{\pi}(T)$ in $\mathbf{F}_p[T]$, we get $\overline{\pi}(T) \mid \overline{F}(T)$ in $\mathbf{F}_p[T]$. \square

4. AN ALGEBRAIC INTEGER NOT IN $\mathbf{Z}[\alpha]$ WHEN $p \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$

If $p \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$ then $\mathcal{O}_K/\mathbf{Z}[\alpha]$ has order divisible by p : there's some $h(\alpha) \in \mathbf{Z}[\alpha]$ such that $h(\alpha)/p \in \mathcal{O}_K - \mathbf{Z}[\alpha]$. In principle, we can find $h(\alpha)$ by searching for an algebraic integer among representatives of the $p^n - 1$ nonzero cosets of $(1/p)\mathbf{Z}[\alpha]/\mathbf{Z}[\alpha]$; there is at least one. Such a brute force search is not necessary: Dedekind gave a method of constructing $h(\alpha)$ from a choice of $\overline{\pi}_j(T)$ dividing $\overline{F}(T)$ with $e_j \geq 2$ in (1.2). Such $\overline{\pi}_j(T)$ exists by Dedekind's index theorem because $p \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$.

Theorem 4.1. *With the notation of Theorem 1.4, suppose $\overline{\pi}(T) \mid \overline{F}(T)$ in $\mathbf{F}_p[T]$ where $\overline{\pi}(T)^2 \mid \overline{f}(T)$. Here are two ways to build $h(T) \in \mathbf{Z}[T]$ such that $h(\alpha)/p \in \mathcal{O}_K - \mathbf{Z}[\alpha]$.*

- *If $h(T) \in \mathbf{Z}[T]$ is a monic lift of $\overline{f}(T)/\overline{\pi}(T)$ to $\mathbf{Z}[T]$, then $h(\alpha)/p \in \mathcal{O}_K - \mathbf{Z}[\alpha]$.*
- *If $f(T) = \pi(T)q(T) + r(T)$ in $\mathbf{Z}[T]$ where $\deg r < \deg \pi$, then $q(\alpha)/p \in \mathcal{O}_K - \mathbf{Z}[\alpha]$, so use $h(T) = q(T)$.²*

In the second method, $\overline{r}(T) = 0$ in $\mathbf{F}_p[T]$ since $\overline{\pi}(T) \mid \overline{f}(T)$ and $\pi(T)$ is monic, but $r(T) \neq 0$ in $\mathbf{Z}[T]$: otherwise $\pi(T) \mid f(T)$, which would contradict the irreducibility of $f(T)$ in $\mathbf{Z}[T]$, since $\deg \pi \leq (\deg f)/2$ from $\overline{\pi}(T)^2 \mid \overline{f}(T)$.

The table below shows how Theorem 4.1 works in previous examples, leading to algebraic integers in $\mathcal{O}_K - \mathbf{Z}[\alpha]$ in the last column.

Example	$f(T)$	p	$\pi(T)$	$h(T)$	$h(\alpha)/p \in \mathcal{O}_K - \mathbf{Z}[\alpha]$
2.1	$T^3 - 12$	2	T	T^2	$\sqrt[3]{12^2}/2$
2.2	$T^3 - 10$	3	$T - 1$	$T^2 + T + 1$	$(\sqrt[3]{10^2} + \sqrt[3]{10} + 1)/3$
2.4	$T^3 - 44$	2	T	T^2	$\sqrt[3]{44^2}/2$
2.4	$T^3 - 44$	3	$T + 1$	$T^2 - T + 1$	$(\sqrt[3]{44^2} - \sqrt[3]{44} + 1)/3$
2.5	$T^3 - T^2 - 2T - 8$	2	T	$T^2 + T$	$(\alpha^2 + \alpha)/2$
2.6	$T^3 + 2T + 4$	2	T	T^2	$\alpha^2/2$
2.7	$T^3 + 2T + 22$	5	$T - 1$	$T^2 + T + 3$	$(\alpha^2 + \alpha + 3)/5$
2.8	$T^4 - 20T^2 + 10$	3	$T - 1$	$(T - 1)(T + 1)^2$	$(\alpha - 1)(\alpha + 1)^2/3$
2.8	$T^4 - 20T^2 + 10$	3	$T + 1$	$(T + 1)(T - 1)^2$	$(\alpha + 1)(\alpha - 1)^2/3$
2.10	$T^4 + T^2 + 4$	2	T	$T^3 + T$	$(\alpha^3 + \alpha)/2$

²This is from Theorem 8.2 of <https://www.math.leidenuniv.nl/~psh/ANTproc/08psh.pdf>.

Remark 4.2. In the first and third rows, $\sqrt[3]{12^2}/2 = \sqrt[3]{18}$ and $\sqrt[3]{44^2}/2 = \sqrt[3]{242}$.

Here are two general examples using $h(T) = T^{n-1}$, which includes $T^3 - 12$, $T^3 - 44$, and $T^3 + 2T + 4$ for $p = 2$.

- If $f(T) = T^n - p^2m$ for $n \geq 2$ and $m \in \mathbf{Z}$, then $\alpha^{n-1}/p \notin \mathbf{Z}[\alpha]$ and $\alpha^{n-1}/p \in \mathcal{O}_K$ since α^{n-1}/p is integral over $\mathbf{Z}[\alpha]$:

$$\left(\frac{\alpha^{n-1}}{p}\right)^2 = \frac{\alpha^{2(n-1)}}{p^2} = \alpha^{n-2} \frac{\alpha^n}{p^2} = \alpha^{n-2}m \in \mathbf{Z}[\alpha].$$

This fits Theorem 4.1 with $\pi(T) = T$, $F(T) = -pm$, and $h(T) = T^{n-1}$.

- If $f(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0$ for $n \geq 2$, $p \mid a_j$ for all $j < n$, and $p^2 \mid a_0$, then $\alpha^{n-1}/p \notin \mathbf{Z}[\alpha]$ and $\alpha^{n-1}/p \in \mathcal{O}_K$ since α^{n-1}/p is integral over $\mathbf{Z}[\alpha]$: from $\alpha^n = -\sum_{j=0}^{n-1} a_j \alpha^j$,

$$\left(\frac{\alpha^{n-1}}{p}\right)^2 = \frac{\alpha^n}{p^2} \alpha^{n-2} = -\sum_{j=0}^{n-1} \frac{a_j}{p^2} \alpha^{n-2+j} = -\left(\sum_{j=1}^{n-1} \frac{a_j}{p} \alpha^{j-1}\right) \frac{\alpha^{n-1}}{p} - \frac{a_0}{p^2} \alpha^{n-2}.$$

This fits Theorem 4.1 with $\pi(T) = T$, $F(T) = -\sum_{j=0}^{n-1} (a_j/p)T^j$, and $h(T) = T^{n-1}$.

The general $f(T)$ is more complicated than these ($h(T)$ need not be a power of T), but these special cases give some intuition for “why” the theorem might be true.

Now let’s prove Theorem 4.1, following Dedekind [3, Sect. 3].

Proof. Of the two ways to build $h(T)$, the second way is a consequence of the first way since $q(T)$ must be monic and $\bar{f}(T) = \bar{q}(T)\bar{\pi}(T)$, so we can use $q(T)$ as $h(T)$.

If $h_1(T)$ and $h_2(T)$ are both monic lifts of $\bar{f}(T)/\bar{\pi}(T)$ to $\mathbf{Z}[T]$, then $h_1(T) = h_2(T) + pm(T)$ for some $m(T) \in \mathbf{Z}[T]$, so $h_1(\alpha)/p = h_2(\alpha)/p + m(\alpha)$ and $m(\alpha) \in \mathbf{Z}[\alpha]$. Therefore it suffices to prove the first method works for just one monic lift of $\bar{f}(T)/\bar{\pi}(T)$ to $\mathbf{Z}[T]$: then it automatically works for all other monic lifts.

Let $\bar{\pi}(T) = \bar{\pi}_j(T)$. We will show $h(\alpha)/p \in \mathcal{O}_K - \mathbf{Z}[\alpha]$ for the specific monic lift $h(T) := \prod_{i \neq j} \pi_i(T)^{e_i} \pi_j(T)^{e_j-1}$. The degree of $h(T)$ is less than n (the rank of $\mathbf{Z}[\alpha]$ as a \mathbf{Z} -module), so $h(\alpha)/p \notin \mathbf{Z}[\alpha]$ since the coefficient of its highest power of α is $1/p$. It remains to show that $h(\alpha)/p \in \mathcal{O}_K$. We will prove this ratio is an algebraic integer by showing for each prime ideal \mathfrak{p} dividing (p) that the multiplicity of \mathfrak{p} in $(h(\alpha))$ is at least as large as the multiplicity of \mathfrak{p} in (p) . Since $p \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$, we can *not* assume (p) factors in the same way as $\bar{f}(T)$ factors: (1.1) is unavailable to us.

Setting $T = \alpha$ in (1.3), $\pi_1(\alpha)^{e_1} \cdots \pi_g(\alpha)^{e_g} = -pF(\alpha)$, so $\pi(\alpha)h(\alpha) = -pF(\alpha)$ by the way we defined $h(T)$. Therefore we have the equation of principal ideals

$$(4.1) \quad (\pi_1(\alpha))^{e_1} \cdots (\pi_g(\alpha))^{e_g} = (\pi_j(\alpha))(h(\alpha)) = (p)(F(\alpha)).$$

Let \mathfrak{p} be a prime ideal dividing (p) , so \mathfrak{p} divides some $(\pi_i(\alpha))$ by (4.1).

Case 1: $\pi_i(T) \neq \pi_j(T)$. In $\mathbf{F}_p[T]$, $\bar{\pi}_i(T)$ and $\bar{\pi}_j(T)$ are distinct monic irreducibles, so they are relatively prime: $\bar{\pi}_i(T)u(T) + \bar{\pi}_j(T)v(T) = 1$, so $\pi_i(T)U(T) + \pi_j(T)V(T) = 1 + pM(T)$ where $U(T), V(T), M(T) \in \mathbf{Z}[T]$. Setting $T = \alpha$, $\pi_i(\alpha)U(\alpha) + \pi_j(\alpha)V(\alpha) = 1 + pM(\alpha)$. Since \mathfrak{p} divides (p) and $(\pi_i(\alpha))$, $\pi_j(\alpha)V(\alpha) \equiv 1 \pmod{\mathfrak{p}}$, so $\mathfrak{p} \nmid (\pi_j(\alpha))$.

Therefore the second equation in (4.1) implies the multiplicity of \mathfrak{p} in $(h(\alpha))$ is at least as large as the multiplicity of \mathfrak{p} in (p) .

Case 2: $\pi_i(T) = \pi_j(T)$.

Now \mathfrak{p} divides (p) and $(\pi_j(\alpha))$. Let \mathfrak{p} divide (p) with multiplicity a , divide $(\pi_j(\alpha))$ with multiplicity b , and divide $(F(\alpha))$ with multiplicity c :

$$(p) = \mathfrak{p}^a \mathfrak{a}, \quad (\pi_j(\alpha)) = \mathfrak{p}^b \mathfrak{b}, \quad (F(\alpha)) = \mathfrak{p}^c \mathfrak{c},$$

where \mathfrak{p} does not divide \mathfrak{a} , \mathfrak{b} , or \mathfrak{c} . We have $a \geq 1$, $b \geq 1$, and $c \geq 0$.

The argument in Case 1 shows a prime ideal dividing (p) divides only one of the ideals $(\pi_1(\alpha)), \dots, (\pi_g(\alpha))$, so the multiplicity of \mathfrak{p} in the first product of (4.1) is $e_j b$, while its multiplicity in the third product of (4.1) is $a + c$. Therefore

$$e_j b = a + c.$$

Since $(h(\alpha)) = \prod_{k \neq j} (\pi_k(\alpha))^{e_k} (\pi_j(\alpha))^{e_j-1}$, the multiplicity of \mathfrak{p} in $(h(\alpha))$ is $(e_j - 1)b$. We want to show this is at least as large as the multiplicity of \mathfrak{p} in (p) : $e_j b - b \geq a$. That is the same as $a + c - b \geq a$, or in other words $c \geq b$. Why is $c \geq b$? We'll break this up into two cases depending on which of a or b is larger.

Case (i) $b \geq a$. Since $e_j \geq 2$, $a + c = e_j b \geq 2b$, so $c - b \geq b - a \geq 0$, and thus $c \geq b$.

Case (ii): $b \leq a$. Since $\pi_j(T) \mid \overline{F}(T)$ in $\mathbf{F}_p[T]$, $F(T) = \pi_j(T)H(T) + pJ(T)$ for some $H(T)$ and $J(T)$ in $\mathbf{Z}[T]$. Therefore $F(\alpha) = \pi_j(\alpha)H(\alpha) + pJ(\alpha)$ in $\mathbf{Z}[\alpha] \subset \mathcal{O}_K$. The multiplicity of \mathfrak{p} in $(\pi_j(\alpha))$ is b and the multiplicity of \mathfrak{p} in (p) is a . Since $b \leq a$, \mathfrak{p}^b divides $(\pi_j(\alpha))$ and (p) , so $\pi_j(\alpha)H(\alpha) + pJ(\alpha) \equiv 0 \pmod{\mathfrak{p}^b}$. Thus $\mathfrak{p}^b \mid (F(\alpha))$, which implies $b \leq c$.

This completes the proof. \square

Remark 4.3. In the proof of Theorem 4.1, we did not need Dedekind's index theorem. The proof starts with some $\pi_j(T)$ dividing $\overline{F}(T)$ with $e_j \geq 2$ in (1.2) and constructs an algebraic integer not in $\mathbf{Z}[\alpha]$ of the form $h(\alpha)/p$ where $h(T) \in \mathbf{Z}[T]$. In $\mathcal{O}_K/\mathbf{Z}[\alpha]$, $h(\alpha)/p$ has order p , so $p \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$. Hence the proof of Theorem 4.1 is actually a second proof of (\Leftarrow) in Dedekind's index theorem. Dedekind gave both of the proofs of the direction (\Leftarrow) in his index theorem that are shown here.

If $p \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$ and we use Theorem 4.1 to find a number $\beta \in \mathcal{O}_K - \mathbf{Z}[\alpha]$, it is not necessarily the case that $\mathbf{Z}[\alpha] \subset \mathbf{Z}[\beta]$. Here is an example of this.

Example 4.4. Let $\alpha = \sqrt[3]{12}$, $\beta = \sqrt[3]{18}$, and $K = \mathbf{Q}(\sqrt[3]{12}) = \mathbf{Q}(\sqrt[3]{18})$. Since $\alpha = \beta^2/3$ and $\beta = \alpha^2/2$, α and β are in \mathcal{O}_K but $\beta \notin \mathbf{Z}[\alpha]$ and $\alpha \notin \mathbf{Z}[\beta]$.

It can be shown that $[\mathcal{O}_K : \mathbf{Z}[\alpha]] = 2$ and $[\mathcal{O}_K : \mathbf{Z}[\beta]] = 3$, so $A := \mathbf{Z}[\alpha] + \mathbf{Z}[\beta]$ is an additive group such that $\mathbf{Z}[\alpha] \subset A \subset \mathcal{O}_K$ and $\mathbf{Z}[\beta] \subset A \subset \mathcal{O}_K$, so $[\mathcal{O}_K : A]$ divides 2 and 3. Therefore $[\mathcal{O}_K : A] = 1$, which tells us

$$\mathcal{O}_K = A = \mathbf{Z} + \mathbf{Z}\alpha + \mathbf{Z}\alpha^2 + \mathbf{Z} + \mathbf{Z}\beta + \mathbf{Z}\beta^2 = \mathbf{Z} + \mathbf{Z}\alpha + \mathbf{Z}\beta$$

since $\alpha^2 = 2\beta$ and $\beta^2 = 3\alpha$.

In a number field K , \mathcal{O}_K might have the form $\mathbf{Z}[\gamma]$ for some γ or it might not.

Example 4.5. If $K = \mathbf{Q}(\sqrt[3]{12})$ then $\mathcal{O}_K = \mathbf{Z}[\gamma]$ where $\gamma = \sqrt[3]{12} + \sqrt[3]{18}$, but if $K = \mathbf{Q}(\sqrt[3]{52})$ then $\mathcal{O}_K \neq \mathbf{Z}[\gamma]$ for all γ in \mathcal{O}_K .

This illustrates why Theorems 1.4 and 4.1 can't always be iterated to enlarge a subring $\mathbf{Z}[\alpha]$ in stages to reach all of \mathcal{O}_K , but Theorem 1.4 is a preliminary step in the following algorithm that computes \mathcal{O}_K and is called the "round 2" algorithm.

Step 1: Write a number field K as $\mathbf{Q}(\alpha)$ for $\alpha \in \mathcal{O}_K$ with minimal polynomial $f(T)$.

Step 2: Since $[\mathcal{O}_K : \mathbf{Z}[\alpha]]^2 \mid \text{disc}(f)$, factor $\text{disc}(f)$ to assemble a list of primes p such that $p^2 \mid \text{disc}(f)$. These are the possible prime factors of $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$.

Step 3: Use Dedekind's index theorem on the primes at the end of Step 2 to determine the finite set of primes that divide $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$. If there are no such primes then $[\mathcal{O}_K : \mathbf{Z}[\alpha]] = 1$, so $\mathcal{O}_K = \mathbf{Z}[\alpha]$ and we are done. If $[\mathcal{O}_K : \mathbf{Z}[\alpha]] > 1$, then let S be the set of prime factors of $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$.

Step 4: For $p \in S$, and an order \mathcal{O} in K , such as $\mathbf{Z}[\alpha]$, we want to build an order \mathcal{O}_p containing \mathcal{O} with $p \nmid [\mathcal{O}_K : \mathcal{O}_p]$.

Set $I_p = \{x \in \mathcal{O} : x^m \equiv 0 \pmod{p\mathcal{O}} \text{ for some } m \geq 1\}$. This is a nonzero ideal in \mathcal{O} (the radical of the ideal $p\mathcal{O}$), *e.g.*, $p \in I_p$. Let \mathcal{O}' be the multiplier ring of I_p in K :

$$\mathcal{O}' = \{x \in K : xI_p \subset I_p\},$$

so $\mathcal{O} \subset \mathcal{O}' \subset \mathcal{O}_K$. Methods of computing I_p and \mathcal{O}' starting from a \mathbf{Z} -basis of \mathcal{O} , are in [2, Sect. 6.1.1].

Step 5: For \mathcal{O}' as in Step 4, $[\mathcal{O}' : \mathcal{O}]$ is a power of p : since $p \in I_p$, $p\mathcal{O}' \subset I_p \subset \mathcal{O}$, so $\mathcal{O} \subset \mathcal{O}' \subset (1/p)\mathcal{O}$. Thus $[\mathcal{O}' : \mathcal{O}] \mid p^n$, where $n = [K : \mathbf{Q}]$.

- If \mathcal{O}' is bigger than \mathcal{O} then the highest power of p dividing $[\mathcal{O}_K : \mathcal{O}']$ is less than the highest power of p dividing $[\mathcal{O}_K : \mathcal{O}]$. Rename \mathcal{O}' as \mathcal{O} and repeat Step 4.
- If $\mathcal{O}' = \mathcal{O}$ then $p \nmid [\mathcal{O}_K : \mathcal{O}]$. This result, due to Pohst and Zassenhaus, is not obvious! A proof is in [2, Sect. 6.1.3]. (The converse is true too: if $p \nmid [\mathcal{O}_K : \mathcal{O}]$ then $[\mathcal{O}' : \mathcal{O}]$ is a p -power dividing $[\mathcal{O}_K : \mathcal{O}]$, so $[\mathcal{O}' : \mathcal{O}] = 1$ and thus $\mathcal{O}' = \mathcal{O}$.) Set $\mathcal{O}_p = \mathcal{O}$.

Step 6: Run through Steps 4 and 5 for each $p \in S$, starting with the initial order \mathcal{O} being $\mathbf{Z}[\alpha]$, to get an order \mathcal{O}_p containing $\mathbf{Z}[\alpha]$ such that $p \nmid [\mathcal{O}_K : \mathcal{O}_p]$.

Set $A := \sum_{p \in S} \mathcal{O}_p$. This additive subgroup of \mathcal{O}_K contains \mathcal{O}_p for each p in S , so $p \nmid [\mathcal{O}_K : A]$ for $p \in S$. Since $\mathbf{Z}[\alpha] \subset A \subset \mathcal{O}_K$, $[\mathcal{O}_K : A]$ is 1 (as in Example 4.4), so $\mathcal{O}_K = A = \sum_{p \in S} \mathcal{O}_p$. That “computes” \mathcal{O}_K in terms of the rings \mathcal{O}_p for $p \in S$.

5. EXISTENCE OF ELEMENT WITH INDEX NOT DIVISIBLE BY p

Here are the key items we have discussed about primes p and indices $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$.

- (1) If there is an $\alpha \in \mathcal{O}_K$ such that $K = \mathbf{Q}(\alpha)$ and $p \nmid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$, then we can read off how $p\mathcal{O}_K$ decomposes into prime ideals from the way $f(T) \pmod{p}$ decomposes into irreducibles in $\mathbf{F}_p[T]$, where $f(T)$ is the minimal polynomial of α over \mathbf{Q} .
- (2) If there is an $\alpha \in \mathcal{O}_K$ such that $K = \mathbf{Q}(\alpha)$, then a necessary and sufficient condition for $p \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$ is a divisibility criterion in $\mathbf{F}_p[T]$ (Dedekind's index theorem).
- (3) When $p \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$, there is a systematic way to find an element of order p in $\mathcal{O}_K/\mathbf{Z}[\alpha]$ (Theorem 4.1).

A natural issue to address that would round out this list of properties is how to determine if there is an α in \mathcal{O}_K such that $K = \mathbf{Q}(\alpha)$ and $p \nmid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$. Here we don't pick α and look for p such that $p \nmid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$, but pick p and look for α such that $p \nmid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$. The *index* of K is

$$i(K) := \gcd([\mathcal{O}_K : \mathbf{Z}[\alpha]]),$$

where the gcd runs over all α in \mathcal{O}_K such that $K = \mathbf{Q}(\alpha)$. We have $p \nmid i(K)$ if and only there is an α such that $p \nmid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$. If $i(K) > 1$ then $\mathcal{O}_K \neq \mathbf{Z}[\alpha]$ for all α in \mathcal{O}_K .

From (1.1), which is a consequence of $p \nmid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$ for some α but makes no direct reference to α , we get a necessary condition for $p \nmid i(K)$ in terms of the prime ideal factorization $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$: writing $N(\mathfrak{p}_i) = p^{f_i}$, *there must be distinct monic irreducibles $\bar{\pi}_1(T), \dots, \bar{\pi}_g(T)$ in $\mathbf{F}_p[T]$ such that $\deg(\bar{\pi}_i(T)) = f_i$ for $i = 1, \dots, g$.*

Example 5.1. Since $\mathbf{F}_2[T]$ has two irreducibles of degree 1 and one irreducible of degree 2, if $2\mathcal{O}_K$ has at least three prime ideal factors with residue field degree 1 (making $[K : \mathbf{Q}] \geq 3$) or at least two prime ideal factors with residue field degree 2 (making $[K : \mathbf{Q}] \geq 4$) then it's impossible to have $2 \nmid i(K)$: for all α in \mathcal{O}_K that generate K/\mathbf{Q} , $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$ is even. An example of the first case is $K = \mathbf{Q}(\beta)$ where β is a root of $T^3 - T^2 - 2T - 8$ (a cubic field in which 2 splits completely) and an example of the second case is $K = \mathbf{Q}(\gamma)$ where γ is a root of $T^4 - 3T^2 - 4T + 5$ (a quartic field in which $(2) = \mathfrak{p}\mathfrak{p}'$ with $f(\mathfrak{p}|2) = f(\mathfrak{p}'|2) = 2$).

Dedekind [3, Sect. 4] showed the necessary condition above for $p \nmid i(K)$ is sufficient too, so we have the following equivalence.

Theorem 5.2. *Let $[K : \mathbf{Q}] = n$ and p be a prime. When $p\mathcal{O}_K$ has prime ideal factorization $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$ and $N(\mathfrak{p}_i) = p^{f_i}$, we have $p \nmid i(K)$ if and only if there are distinct monic irreducibles $\bar{\pi}_1(T), \dots, \bar{\pi}_g(T)$ in $\mathbf{F}_p[T]$ such that $\deg(\bar{\pi}_i(T)) = f_i$ for $i = 1, \dots, g$.*

Proof. We already indicated from (1.1) that if $p \nmid i(K)$, meaning $p \nmid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$ for a primitive integral α in K , then there are distinct monic irreducible $\bar{\pi}_i(T)$ in $\mathbf{F}_p[T]$ with degree f_i for $i = 1, \dots, g$.

Now assume there are distinct monic irreducible $\bar{\pi}_i(T) \in \mathbf{F}_p[T]$ such that $\deg \bar{\pi}_i(T) = f_i$ for $i = 1, \dots, g$. Let $\pi_i(T) \in \mathbf{Z}[T]$ be a monic lifting of $\bar{\pi}_i(T)$, so $\deg(\pi_i(T)) = \deg(\bar{\pi}_i(T)) = f_i$. We will use these polynomials and the Chinese remainder theorem (among other tools) to show K/\mathbf{Q} has a primitive integral element α such that $p \nmid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$, so $p \nmid i(K)$.

We break up the rest of the proof into four steps. If you find it too long, you can skip it.

Step 1: There is an $\alpha \in \mathcal{O}_K$ such that $\mathfrak{p}_i = (p, \pi_i(\alpha))$ for $i = 1, \dots, g$.

The field $\mathcal{O}_K/\mathfrak{p}_i$ has order p^{f_i} . A standard property of finite fields is that each irreducible of degree f_i in $\mathbf{F}_p[T]$ has a root (in fact a full set of roots) in each field of size p^{f_i} . Therefore $\pi_i(r_i) \equiv 0 \pmod{\mathfrak{p}_i}$ for some $r_i \in \mathcal{O}_K$, so $\mathfrak{p}_i \mid (\pi_i(r_i))$. Also $\mathfrak{p}_i \mid (p)$, so $\mathfrak{p}_i \mid (p, \pi_i(r_i))$. It can happen that $\mathfrak{p}_i \neq (p, \pi_i(r_i))$, and one reason would be that $\mathfrak{p}_i^2 \mid (p)$ and $\mathfrak{p}_i^2 \mid (\pi_i(r_i))$. To fix that, if $\mathfrak{p}_i^2 \mid (\pi_i(r_i))$ then we can adjust r_i modulo \mathfrak{p}_i so that $\mathfrak{p}_i^2 \nmid (\pi_i(r_i))$, as follows.

Pick $\beta_i \in \mathfrak{p}_i - \mathfrak{p}_i^2$, so \mathfrak{p}_i divides (β_i) just once. Then $\pi_i(r_i + \beta_i) \equiv \pi_i(r_i) \equiv 0 \pmod{\mathfrak{p}_i}$ while

$$\pi_i(r_i + \beta_i) = \pi_i(r_i) + \pi_i'(r_i)\beta_i \equiv \pi_i'(r_i)\beta_i \pmod{\mathfrak{p}_i^2}$$

from the assumption that $\pi_i(r_i) \equiv 0 \pmod{\mathfrak{p}_i^2}$. Since $\bar{\pi}_i(T)$ is separable in $\mathbf{F}_p[T]$, $\pi_i(r_i) \equiv 0 \pmod{\mathfrak{p}_i}$ implies $\pi_i'(r_i) \not\equiv 0 \pmod{\mathfrak{p}_i^2}$, so the ideal $(\pi_i'(r_i)\beta_i) = (\pi_i'(r_i))(\beta_i)$ is divisible by \mathfrak{p}_i just once: $\mathfrak{p}_i \nmid (\pi_i'(r_i))$, $\mathfrak{p}_i \mid (\beta_i)$, and $\mathfrak{p}_i^2 \nmid (\beta_i)$. Replacing r_i by $r_i + \beta_i$ puts us in the situation that $\pi_i(r_i) \equiv 0 \pmod{\mathfrak{p}_i}$ as before and now $\pi_i(r_i) \not\equiv 0 \pmod{\mathfrak{p}_i^2}$, so \mathfrak{p}_i divides $(p, \pi_i(r_i))$ just once.

Now let's use the Chinese remainder theorem: there is an $\alpha \in \mathcal{O}_K$ such that $\alpha \equiv r_i \pmod{\mathfrak{p}_i^2}$ for $i = 1, \dots, g$, so $\pi_i(\alpha) \equiv \pi_i(r_i) \equiv 0 \pmod{\mathfrak{p}_i}$ and $\pi_i(\alpha) \equiv \pi_i(r_i) \not\equiv 0 \pmod{\mathfrak{p}_i^2}$. We are going to show $\mathfrak{p}_i = (p, \pi_i(\alpha))$. Since \mathfrak{p}_i divides (p) and divides $(\pi_i(\alpha))$ just once, \mathfrak{p}_i divides $(p, \pi_i(\alpha))$ just once. What other prime ideal divides $(p, \pi_i(\alpha))$? If \mathfrak{q} is a prime ideal dividing $(p, \pi_i(\alpha))$ then $\mathfrak{q} \mid (p)$, so \mathfrak{q} is some \mathfrak{p}_j . Then $\pi_i(\alpha) \equiv 0 \pmod{\mathfrak{p}_j}$. Also $\pi_j(\alpha) \equiv 0 \pmod{\mathfrak{p}_j}$, so $\alpha \pmod{\mathfrak{p}_j}$ is a common root in $\mathcal{O}_K/\mathfrak{p}_j$ of $\bar{\pi}_i(T)$ and $\bar{\pi}_j(T)$. Distinct monic irreducibles in $\mathbf{F}_p[T]$ don't have common roots in an extension field of \mathbf{F}_p , so $\bar{\pi}_j(T) = \bar{\pi}_i(T)$. That means $j = i$, so $\mathfrak{q} = \mathfrak{p}_i$: the only prime ideal dividing $(p, \pi_i(\alpha))$ is \mathfrak{p}_i . Since \mathfrak{p}_i divides $(p, \pi_i(\alpha))$ just once, $(p, \pi_i(\alpha)) = \mathfrak{p}_i$ for $i = 1, \dots, g$.

Step 2: For α as in Step 1, $\mathfrak{p}_i^{e_i} = (p, \pi_i(\alpha)^{e_i})$ for $i = 1, \dots, g$, where $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$.

The ideal $(p, \pi_i(\alpha)^{e_i})$ is the greatest common divisor of (p) and $(\pi_i(\alpha))^{e_i}$. Let \mathfrak{q} be a prime ideal dividing $(p, \pi_i(\alpha)^{e_i})$. Then $\mathfrak{q} \mid (p)$ and $\mathfrak{q} \mid (\pi_i(\alpha))^{e_i}$, so \mathfrak{q} divides (p) and $(\pi_i(\alpha))$. Since $(p, \pi_i(\alpha)) = \mathfrak{p}_i$, \mathfrak{q} must be \mathfrak{p}_i , so $(p, \pi_i(\alpha)^{e_i})$ is a power of \mathfrak{p}_i . The highest power of \mathfrak{p}_i dividing (p) is $\mathfrak{p}_i^{e_i}$, and $\mathfrak{p}_i^{e_i} \mid (\pi_i(\alpha)^{e_i})$ since $\mathfrak{p}_i \mid (\pi_i(\alpha))$, so $(p, \pi_i(\alpha)^{e_i}) = \mathfrak{p}_i^{e_i}$.

Step 3: Evaluation at $\alpha \bmod \mathfrak{p}_i^{e_i}$ is a ring isomorphism $\mathbf{F}_p[T]/(\bar{\pi}_i(T)^{e_i}) \rightarrow \mathcal{O}_K/\mathfrak{p}_i^{e_i}$ for $i = 1, \dots, g$.

The ring $\mathcal{O}_K/\mathfrak{p}_i^{e_i}$ has characteristic p since $p \equiv 0 \bmod \mathfrak{p}_i^{e_i}$. Thus evaluation at $\alpha \bmod \mathfrak{p}_i^{e_i}$ is a ring homomorphism $\mathbf{F}_p[T] \rightarrow \mathcal{O}_K/\mathfrak{p}_i^{e_i}$. We have $\pi_i(\alpha)^{e_i} \equiv 0 \bmod \mathfrak{p}_i^{e_i}$ since $\mathfrak{p}_i \mid (\pi_i(\alpha))$, so $\bar{\pi}_i(T)^{e_i}$ is in the kernel: we get a ring homomorphism $\mathbf{F}_p[T]/(\bar{\pi}_i(T)^{e_i}) \rightarrow \mathcal{O}_K/\mathfrak{p}_i^{e_i}$ by $\bar{g}(T) \mapsto g(\alpha) \bmod \mathfrak{p}_i^{e_i}$. We will show this is injective, and therefore it is an isomorphism since $|\mathbf{F}_p[T]/(\bar{\pi}_i(T)^{e_i})| = p^{e_i f_i} = |\mathcal{O}_K/\mathfrak{p}_i^{e_i}|$.

Each element of $\mathbf{F}_p[T]/(\bar{\pi}_i(T)^{e_i})$ can be written uniquely in base $\bar{\pi}_i(T)$ as

$$(5.1) \quad \bar{c}_0(T) + \bar{c}_1(T)\bar{\pi}_i(T) + \dots + \bar{c}_{e_i-1}(T)\bar{\pi}_i(T)^{e_i-1} \bmod \bar{\pi}_i(T)^{e_i}$$

where the coefficients $\bar{c}_k(T)$ in $\mathbf{F}_p[T]$ are 0 or have degree less than $\deg(\bar{\pi}_i(T)) = f_i$. Suppose (5.1) is mapped to 0 in $\mathcal{O}_K/\mathfrak{p}_i^{e_i}$ after we substitute $\alpha \bmod \mathfrak{p}_i^{e_i}$ for T :

$$c_0(\alpha) + c_1(\alpha)\pi_i(\alpha) + \dots + c_{e_i-1}(\alpha)\pi_i(\alpha)^{e_i-1} \bmod \mathfrak{p}_i^{e_i}.$$

We want the kernel of $\mathbf{F}_p[T]/(\bar{\pi}_i(T)^{e_i}) \rightarrow \mathcal{O}_K/\mathfrak{p}_i^{e_i}$ to be 0, so all $\bar{c}_k(T)$ should be 0 in $\mathbf{F}_p[T]$. If any are not, let $k \leq e_i - 1$ be minimal with $\bar{c}_k(T) \neq 0$ in $\mathbf{F}_p[T]$. Then

$$c_k(\alpha)\pi_i(\alpha)^k + \dots + c_{e_i-1}(\alpha)\pi_i(\alpha)^{e_i-1} \equiv 0 \bmod \mathfrak{p}_i^{e_i}.$$

Since $k \leq e_i - 1$, we can reduce the congruence to modulus \mathfrak{p}_i^{k+1} :

$$c_k(\alpha)\pi_i(\alpha)^k \equiv 0 \bmod \mathfrak{p}_i^{k+1},$$

so $\mathfrak{p}_i^{k+1} \mid (c_k(\alpha))(\pi_i(\alpha))^k$. The ideal $(\pi_i(\alpha))$ is divisible by \mathfrak{p}_i just once by the *method* used to construct α in Step 1 (that is, $\alpha \equiv r_i \bmod \mathfrak{p}_i^2$ and $\pi_i(r_i) \not\equiv 0 \bmod \mathfrak{p}_i^2$), so $\mathfrak{p}_i \mid (c_k(\alpha))$. Write that as $\bar{c}_k(\alpha) = 0$ in the field $\mathcal{O}_K/\mathfrak{p}_i$. Since $\deg(\bar{c}_k(T)) < f_i$ and $\alpha \bmod \mathfrak{p}_i$ is the root of an irreducible $\bar{\pi}_i(T)$ of degree f_i in $\mathbf{F}_p[T]$, $\alpha \bmod \mathfrak{p}_i$ is not the root of a polynomial in $\mathbf{F}_p[T]$ of degree less than f_i . Therefore $\bar{c}_k(T) = 0$ in $\mathbf{F}_p[T]$, which is a contradiction.

Step 4: For α as in Step 1, $K = \mathbf{Q}(\alpha)$ and $p \nmid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$.

By the Chinese remainder theorem, we can combine the isomorphisms $\mathbf{F}_p[T]/(\bar{\pi}_i(T)^{e_i}) \rightarrow \mathcal{O}_K/\mathfrak{p}_i^{e_i}$ for $i = 1, \dots, g$ from Step 3 that use evaluation at $\alpha \bmod \mathfrak{p}_i^{e_i}$ to get an isomorphism

$$(5.2) \quad \mathbf{F}_p[T]/(\bar{\pi}_1(T)^{e_1} \dots \bar{\pi}_g(T)^{e_g}) \rightarrow \mathcal{O}_K/p\mathcal{O}_K$$

using evaluation at $\alpha \bmod p\mathcal{O}_K$.

Let $f(T)$ be the minimal polynomial of α over \mathbf{Q} , so $f(T)$ is monic in $\mathbf{Z}[T]$ and $\deg f \leq [K : \mathbf{Q}]$. Also

$$f(\alpha) = 0 \implies f(\alpha) \equiv 0 \bmod p\mathcal{O}_K \implies \bar{\pi}_1(T)^{e_1} \dots \bar{\pi}_g(T)^{e_g} \mid \bar{f}(T) \text{ in } \mathbf{F}_p[T] \text{ by (5.2).}$$

Since f is monic,

$$\deg f = \deg \bar{f} \geq \sum_{i=1}^g e_i \deg(\bar{\pi}_i) = \sum_{i=1}^g e_i f_i = [K : \mathbf{Q}].$$

Therefore $\deg f = [K : \mathbf{Q}]$, so $K = \mathbf{Q}(\alpha)$ and

$$\bar{f}(T) = \bar{\pi}_1(T)^{e_1} \dots \bar{\pi}_g(T)^{e_g}$$

in $\mathbf{F}_p[T]$ since both sides are monic and the right side is a factor of the left side. We can rewrite (5.2) as an isomorphism

$$(5.3) \quad \mathbf{F}_p[T]/(\bar{f}(T)) \rightarrow \mathcal{O}_K/p\mathcal{O}_K$$

using evaluation at $\alpha \bmod p\mathcal{O}_K$.

To prove $p \nmid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$, we argue by contradiction. Suppose $p \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$, so $\mathcal{O}_K/\mathbf{Z}[\alpha]$ has order divisible by p and thus it has an element β of order p : $\beta \in \mathcal{O}_K - \mathbf{Z}[\alpha]$ and $p\beta \in \mathbf{Z}[\alpha]$. Write $p\beta = h(\alpha)$, where $h(T) \in \mathbf{Z}[T]$. Then $h(\alpha) \equiv 0 \bmod p\mathcal{O}_K$, so the isomorphism (5.3) vanishes on $\bar{h}(T)$, which means $\bar{f}(T) \mid \bar{h}(T)$ in $\mathbf{F}_p[T]$, so $h(T) \in (p, f(T))$ in $\mathbf{Z}[T]$. Evaluating that at α , $h(\alpha) \in p\mathbf{Z}[\alpha]$ since $f(\alpha) = 0$, so $\beta = h(\alpha)/p \in \mathbf{Z}[\alpha]$, which is a contradiction. Thus $p \nmid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$. \square

The condition in Theorem 5.2 that is equivalent to $p \nmid i(K)$ can be described using inequalities. For $d \geq 1$, let $g_{p,K}(d)$ be the number of prime ideal factors of $p\mathcal{O}_K$ with residue field degree d and $N_p(d)$ be the number of monic irreducible polynomials of degree d in $\mathbf{F}_p[T]$. Then Theorem 5.2 says

$$(5.4) \quad p \nmid i(K) \iff g_{p,K}(d) \leq N_p(d) \text{ for all } d \leq [K : \mathbf{Q}].$$

The right side of (5.4) is formulated in terms of the number of prime ideal factors of $p\mathcal{O}_K$ with each residue field degree, and it might seem hard to count how often each residue field degree occurs in the factorization of $p\mathcal{O}_K$ if we don't know that (1.1) can be applied to p . Nevertheless, by negating both sides of (5.4) we get

$$(5.5) \quad p \mid i(K) \iff N_p(d) < g_{p,K}(d) \text{ for some } d \leq [K : \mathbf{Q}].$$

Theorem 5.3. *A prime that is less than $[K : \mathbf{Q}]$ and splits completely in K divides $i(K)$.*

Proof. We use $d = 1$ in (5.5). Since $N_p(1) = p$ and $g_{p,K}(1) = [K : \mathbf{Q}]$ if p splits completely in K , if $p < [K : \mathbf{Q}]$ and p splits completely in K then (5.5) tells us $p \mid i(K)$. \square

The next result, due to von Zylinski [8], shows all p dividing $i(K)$ are bounded by $[K : \mathbf{Q}]$.

Theorem 5.4. *If $p \mid i(K)$ then $p < [K : \mathbf{Q}]$.*

Proof. If $p \mid i(K)$ then $g_{p,K}(d) > N_p(d)$ for some $d \leq [K : \mathbf{Q}]$. By the formula $\sum_{i=1}^g e_i f_i = [K : \mathbf{Q}]$ for the prime p , $dg_{p,K}(d) \leq [K : \mathbf{Q}]$ by summing on the left side only over i where $f_i(p) = d$. Therefore $dN_p(d) < mg_{p,K}(d) \leq [K : \mathbf{Q}]$. The number $N_p(d)$ is divisible by p since if $\pi(T)$ is irreducible in $\mathbf{F}_p[T]$ then so is $\pi(T + c)$ for all $c \in \mathbf{F}_p$. Positivity of $N_p(d)$ therefore implies $dN_p(d) \geq p$, so $p \leq dN_p(d) < [K : \mathbf{Q}]$. \square

Conversely, Bauer [1] showed that if $p < n$ for an integer n then there are number fields K of degree n over \mathbf{Q} such that $p \mid i(K)$ by showing for each prime p and $n \in \mathbf{Z}^+$ that there are number fields K of degree n such that p splits completely in K . Such p divide $i(K)$ if $p < n$, by Theorem 5.3.

Example 5.5. If $[K : \mathbf{Q}] = 2$ then there is no prime less than $[K : \mathbf{Q}]$, so $i(K) = 1$. This is well-known since the ring of integers of a quadratic field has the form $\mathbf{Z}[\alpha]$ for some α .³

³The condition $i(K) = 1$ does not require $\mathcal{O}_K = \mathbf{Z}[\alpha]$. If two indices $[\mathcal{O}_K : \mathbf{Z}[\beta]]$ and $[\mathcal{O}_K : \mathbf{Z}[\gamma]]$ are greater than 1 and are relatively prime, then $i(K) = 1$. For example, if $K = \mathbf{Q}(\sqrt[3]{175})$ then $\mathcal{O}_K \neq \mathbf{Z}[\alpha]$ for all α in K , but $[\mathcal{O}_K : \mathbf{Z}[\sqrt[3]{175}]] = 5$ and $[\mathcal{O}_K : \mathbf{Z}[\sqrt[3]{245}]] = 7$, so $i(K) = 1$. Those calculations are explained in Example 4.16 in <https://kconrad.math.uconn.edu/blurbs/gradnumthy/different.pdf>.

Example 5.6. If $[K : \mathbf{Q}] = 3$ then the only possible prime factor of $i(K)$ is 2, and $2 \mid i(K)$ if and only if $g_{2,K}(1) > N_2(1) = 2$, $g_{2,K}(2) > N_2(2) = 1$, or $g_{2,K}(3) > N_2(3) = 2$. The first inequality says 2 splits completely in K (since 2 has at most 3 prime ideal factors in a cubic field), and the second and third inequalities are impossible in a cubic field, *e.g.*, if there were at least two prime ideal factors with residue field degree 2 then $[K : \mathbf{Q}] \geq 4$. Engstrom [4, p. 234] showed $i(K)$ is 1 or 2 for all cubic fields.

Example 5.7. If $[K : \mathbf{Q}] = 4$ then the only possible prime factors of $i(K)$ are 2 and 3. We have $2 \mid i(K)$ if and only if either 2 splits completely, $(2) = \mathfrak{p}_2^2 \mathfrak{p}'_2 \mathfrak{p}''_2$, or $(2) = \mathfrak{p}_4 \mathfrak{p}'_4$, and $3 \mid i(K)$ if and only if 3 splits completely in K . For example, 3 splits completely in $\mathbf{Q}(\sqrt{-5}, \sqrt{7})$ (first check it splits completely in $\mathbf{Q}(\sqrt{-5})$ and $\mathbf{Q}(\sqrt{7})$), so $3 \mid i(K)$. Engstrom [4, p. 234] showed $i(K)$ is 1, 2, 3, 4, 6, or 12 for quartic fields.

Example 5.8. Number fields of arbitrary 2-power degree in which 2 splits completely can be built as composites of quadratic fields. For squarefree $m \neq 1$, 2 splits completely in $\mathbf{Q}(\sqrt{m})$ if and only if $m \equiv 1 \pmod{8}$. So when m_1, \dots, m_r are pairwise relatively prime integers that are each 1 mod 8 and don't equal 1, such as r different primes that are each 1 mod 8, the field $K = \mathbf{Q}(\sqrt{m_1}, \dots, \sqrt{m_r})$ has degree 2^r over \mathbf{Q} and 2 splits completely in K . In a similar way, for each $r \geq 1$ there is a composite of quadratic fields of degree 2^r in which any chosen prime number splits completely.

The next two examples are a family of cubic fields in which 2 splits completely and a family of quartic fields in which 2 and 3 both split completely.

Example 5.9. Let $f_n(T) = T(T-1)(T+1) + 2^n = T^3 - T + 2^n$ for $n \geq 1$. This is irreducible for all n : it is cubic with the only possible roots in \mathbf{Q} being $\pm 2^j$ for $0 \leq j \leq n$, and $f(\pm 2^j) \neq 0$ by looking at 2-divisibility of the three terms (treat $j = 0$ and $j = n$ separately from $0 < j < n$). Set $K_n = \mathbf{Q}(r_n)$ where r_n is a root of $f_n(T)$, so $[K_n : \mathbf{Q}] = 3$. For $n \geq 3$, 2 splits completely in K_n because $f_n(T)$ splits completely over the 2-adic numbers \mathbf{Q}_2 by Hensel's lemma with approximate roots 0, 1, and -1 . Thus $i(K_n)$ is divisible by 2 for $n \geq 3$.⁴

Example 5.10. Let $f_n(T) = T(T-1)(T-2)(T-3) + 6^n = T^4 - 6T^3 + 11T^2 - 6T + 6^n$ for $n \geq 1$. This is irreducible for $1 \leq n \leq 10$ and probably is irreducible for all n , but I haven't bothered to check this⁵. Assume $f_n(T)$ is irreducible over \mathbf{Q} and set $L_n = \mathbf{Q}(r_n)$ where r_n is a root of $f_n(T)$, so $[L_n : \mathbf{Q}] = 4$. By Hensel's lemma over the 2-adic and 3-adic numbers with approximate roots 0, 1, 2, and 3, $f_n(T)$ splits completely over \mathbf{Q}_2 and \mathbf{Q}_3 for $n \geq 3$, so 2 and 3 split completely in L_n . Therefore $i(L_n)$ is divisible by 2 and 3 for $n \geq 3$.

Prime factors of $i(K)$ divide all indices $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$, so they have been called *common index divisors* of K , as in the title of [4], as well as inessential discriminant divisors [7], which is a translation of the original German term *ausserwesentliche Discriminantenteiler* (see the title of [1]), where *ausserwesentliche* literally means “outside of the essence” (*ausser* = outer and *Wesen* = being) and is no longer in common use. These primes have also been called essential discriminant divisors [2, p. 197], which is surprising: why label them as both inessential and essential?

⁴The intuition that led to the construction of the fields K_n is 2-adic: $f_n(T)$ is 2-adically close to the split polynomial $T(T-1)(T+1)$, so it should split completely over \mathbf{Q}_2 for large enough n by p -adic continuity of roots when $p = 2$, and Hensel's lemma confirms this for $n \geq 3$.

⁵Note $f_n(T-1) = T^4 - 10T^3 + 35T^2 - 50T + 24 + 6^n$ is Eisenstein at 5 when $5 \nmid n$, so $f_n(T)$ is irreducible over \mathbf{Q} when $5 \nmid n$.

The story goes back to Kronecker's work [5] on algebraic functions. For $F(x, y) \in \mathbf{C}[x, y]$ that is irreducible and monic in y (like $y^3 + (x^2 - x)y + x - 1$), let $F(x, r) = 0$. The field $\mathbf{C}(x, r)$ is a finite extension of $\mathbf{C}(x)$ and r is integral over $\mathbf{C}[x]$. Let A be the integral closure of $\mathbf{C}[x]$ in $\mathbf{C}(x, r)$. Both A and its subring $\mathbf{C}[x, r]$ are finite free $\mathbf{C}[x]$ -modules of equal rank, and are analogous to \mathcal{O}_K and $\mathbf{Z}[\alpha]$ in the number field $K = \mathbf{Q}(\alpha)$. The analogue for A and $\mathbf{C}[x, r]$ of the number-theoretic formula $\text{disc}(\mathbf{Z}[\alpha]) = [\mathcal{O}_K : \mathbf{Z}[\alpha]]^2 \text{disc}(K)$ is

$$D(x) = R(x)^2 \Delta(x),$$

where $D(x)$ is $\text{disc}_{\mathbf{C}[x]}(A)$, $R(x)$ is the $\mathbf{C}[x]$ -index of $\mathbf{C}[x, r]$ in A , and $\Delta(x)$ is $\text{disc}_{\mathbf{C}[x]}(A)$. (The polynomials $D(x)$, $R(x)$ and $\Delta(x)$ are defined only up to multiplication by a nonzero complex number in order to account for different choices of $\mathbf{C}[x]$ -bases to compute them.) Because A is more fundamental than $\mathbf{C}[x, r]$, Kronecker [5, p. 313] called $\Delta(x) = \text{disc}_{\mathbf{C}[x]}(A)$ the essential divisor (wesentlichen Theiler) of $D(x)$ and $R(x)^2$ the inessential divisor (ausserwesentlichen Theiler) of $D(x)$. Thus “essential” and “inessential” for Kronecker described the relative importance of two complementary divisors of $D(x)$.⁶

In number fields, the analogue of the inessential divisor $R(x)^2$ is $[\mathcal{O}_K : \mathbf{Z}[\alpha]]^2$. We could (but don't) call this number the inessential divisor of the discriminant of α , so a prime dividing all indices $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$ could be called “a common prime factor of the inessential divisors of all discriminants.” When that is shortened to “inessential discriminant divisor” as a label for certain primes, the original intent behind “inessential” (that $[\mathcal{O}_K : \mathbf{Z}[\alpha]]^2$ is less important than $\text{disc}(K)$) becomes lost and common prime factors of all indices $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$ seem essential, not inessential. The name “common index divisor” for such primes is better.

REFERENCES

- [1] M. Bauer, “Über die ausserwesentlichen Diskriminantenteiler einer Gattung,” *Math. Ann.* **64** (1907), 573–576. URL <https://eudml.org/doc/158337>.
- [2] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, NY, 1993.
- [3] R. Dedekind, “Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Congruenzen,” *Abhandlungen der Königlichen Gesellschaft der Wissenschaften in Göttingen* **23** (1878), 3–38. URL <https://eudml.org/doc/135827>. English translation: <https://arxiv.org/abs/2107.08905>.
- [4] H. T. Engstrom, “On the common index divisors of an algebraic field,” *Trans. Amer. Math. Soc.* **32** (1930), 223–237. URL <https://www.ams.org/journals/tran/1930-032-02/S0002-9947-1930-1501535-0/home.html>.
- [5] L. Kronecker, “Ueber die Discriminante algebraischer Functionen einer Variabeln,” *J. Reine Angew. Mathematik* **91** (1881), 301–334. URL <https://eudml.org/doc/148482>.
- [6] M. Pohst and H. Zassenhaus, *Algorithmic Algebraic Number Theory*, Cambridge Univ. Press, Cambridge, 1989.
- [7] L. Tornheim, “Minimal basis and inessential discriminant divisors for a cubic field,” *Pac. J. Math.* **5** (1955), 623–631.
- [8] E. von Zylinski, “Zur Theorie der ausserwesentlichen Diskriminantenteiler algebraischer Körper,” *Math. Ann.* **73** (1913), 273–274. URL <https://eudml.org/doc/158603>.

⁶I thank Darij Grinberg for linguistic assistance with Kronecker's paper.