DEDEKIND’S INDEX THEOREM

KEITH CONRAD

1. Introduction

Let \( K = \mathbb{Q}(\alpha) \) where \( \alpha \) is an algebraic integer with minimal polynomial \( f(T) \in \mathbb{Z}[T] \). 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 \( f(T) \mod p \) in \( \mathbb{F}_p[T] \) provided \( p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]] \):

\[
f(T) \equiv \pi_1(T)^{e_1} \cdots \pi_g(T)^{e_g} \mod p \implies p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g},
\]

where \( \pi_1(T), \ldots, \pi_g(T) \) are distinct monic irreducibles in \( \mathbb{F}_p[T] \), \( N(p_i) = p^{\deg \pi_i} \), and \( p_i = (p, \pi_i(\alpha)) \) where \( \pi_i(T) \) is an arbitrary monic lift of \( \pi_i(T) \) to \( \mathbb{Z}[T] \).

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

Example 1.1. If \( K = \mathbb{Q}(\sqrt[3]{12}) \) and \( f(T) = T^3 - 12 \) then \( f(T) \equiv T^3 \mod 2 \) and \( 2\mathcal{O}_K = \mathfrak{p}_1^3 \), but the factorization of \( 2\mathcal{O}_K \) is not based on (1.1) with \( \alpha = \sqrt[3]{12} \) since \( [\mathcal{O}_K : \mathbb{Z}[\sqrt[3]{12}]] = 2: \mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt[3]{12} + \mathbb{Z}\sqrt[3]{18} = \mathbb{Z} + \mathbb{Z}\sqrt[3]{12} + \mathbb{Z}\sqrt[3]{2^2} \).

We can instead rewrite \( K \) as \( \mathbb{Q}(\sqrt[18]{9}) \), set \( f(T) = T^9 - 18 \), and now \( [\mathcal{O}_K : \mathbb{Z}[\sqrt[3]{18}]] = 3 \), an index not divisible by 2, so the factorization \( T^9 - 18 \equiv T^3 \mod 2 \) implies \( 2\mathcal{O}_K = \mathfrak{p}_1^3 \).

Example 1.2. If \( K = \mathbb{Q}(\sqrt[10]{10}) \) and \( f(T) = T^3 - 10 \) then \( f(T) \equiv (T - 1)^3 \mod 3 \) but \( 3\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2 \). Here \( [\mathcal{O}_K : \mathbb{Z}[\sqrt[10]{10}]] = 3 \). It turns out that \( \mathcal{O}_K = \mathbb{Z}[\alpha] \) for \( \alpha = (\sqrt[10]{10}^2 + \sqrt[10]{10} + 1)/3 \), whose minimal polynomial over \( \mathbb{Q} \) is \( T^3 - T^2 - 3T - 3 \equiv (T - 1)^2 T^2 \mod 3 \).

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

We can apply (1.1) to primes not dividing \( \text{disc}(f) \) since \( [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 \mid \text{disc}(f) \). 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 \( [\mathcal{O}_K : \mathbb{Z}[\alpha]] \). For an arbitrary prime \( p \), here is a necessary and sufficient condition for \( p \mid [\mathcal{O}_K : \mathbb{Z}[\alpha]] \) that does not require knowing \( \mathcal{O}_K \).

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

\[
f(T) \equiv \pi_1(T)^{e_1} \cdots \pi_g(T)^{e_g} \mod p.
\]

Let \( \pi_j(T) \) be a monic lift of \( \pi_j(T) \) to \( \mathbb{Z}[T] \) and define \( F(T) \in \mathbb{Z}[T] \) by

\[
f(T) = \pi_1(T)^{e_1} \cdots \pi_g(T)^{e_g} + pF(T).
\]

Then \( p \mid [\mathcal{O}_K : \mathbb{Z}[\alpha]] \iff \pi_j(T) \mid F(T) \) in \( \mathbb{F}_p[T] \) 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 $[\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 \mid \text{disc}(f)$, the only primes that might divide $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ are primes dividing $\text{disc}(f)$ with multiplicity at least 2.

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

Case 1: $p = 2$.
Since $f(T) \equiv T^3 \mod 2$, take $\pi_1(T) = T$. Write
$$f(T) = T^3 + 2F(T) \text{ for } F(T) = -6,$$
so $F(T) \equiv 0 \mod 2$. Therefore $\pi_1(T) \mid \overline{F}(T)$ in $\mathbb{F}_2[T]$, so $2 \nmid [\mathcal{O}_K : \mathbb{Z}[\sqrt[3]{12}]]$.

Case 2: $p = 3$.
Since $f(T) \equiv T^3 \mod 3$, take $\pi_1(T) = T$. Then
$$f(T) = T^3 + 3F(T) \text{ for } F(T) = -4,$$
so $\pi_1(T) \mid \overline{F}(T)$ in $\mathbb{F}_3[T]$. Thus $3 \nmid [\mathcal{O}_K : \mathbb{Z}[\sqrt[3]{12}]]$.

**Example 2.2.** Let $K = \mathbb{Q}(\sqrt[3]{10})$ 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 $[\mathcal{O}_K : \mathbb{Z}[\sqrt[3]{10}]]$ are 2, 3, and 5.

Case 1: $p = 2$.
Since $f(T) \equiv T^3 \mod 2$, take $\pi_1(T) = T$. Then
$$f(T) = T^3 + 2F(T) \text{ for } F(T) = -5,$$
so $\pi_1(T) \mid \overline{F}(T)$ in $\mathbb{F}_2[T]$. Thus $2 \nmid [\mathcal{O}_K : \mathbb{Z}[\sqrt[3]{10}]]$.

Case 2: $p = 3$.
Since $f(T) \equiv (T - 1)^3 \mod 3$, take $\pi_1(T) = T - 1$. Then
$$f(T) = (T - 1)^3 + 3F(T) \text{ for } F(T) = T^2 - T - 3,$$
so $F(T) \equiv T(T - 1) \mod 3$. Thus $\pi_1(T) \mid \overline{F}(T)$ in $\mathbb{F}_3[T]$, so $3 \mid [\mathcal{O}_K : \mathbb{Z}[\sqrt[3]{10}]]$.

Case 3: $p = 5$.
Since $f(T) \equiv T^3 \mod 5$, take $\pi_1(T) = T$. Then
$$f(T) = T^3 + 5F(T) \text{ for } F(T) = -2,$$
so $\pi_1(T) \mid \overline{F}(T)$ in $\mathbb{F}_5[T]$. Thus $5 \nmid [\mathcal{O}_K : \mathbb{Z}[\sqrt[3]{10}]]$.

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

Case 1: $p = 2$.
Since $f(T) \equiv T^3 \mod 2$, take $\pi_1(T) = T$. Then
$$f(T) = T^3 + 2F(T) \text{ for } F(T) = -1,$$
so $\pi_1(T) \mid \overline{F}(T)$ in $\mathbb{F}_2[T]$. Thus $2 \mid [\mathcal{O}_K : \mathbb{Z}[\sqrt[3]{2}]]$.

Case 2: $p = 3$.
Since $f(T) \equiv (T + 1)^3 \mod 3$, take $\pi_1(T) = T + 1$. Then
$$f(T) = (T + 1)^3 + 3F(T) \text{ for } F(T) = -T^2 - T - 1,$$
so $F(T) \equiv -(T + 2)^2 \mod 3$. Thus $\pi_1(T) \mid \overline{F}(T)$ in $\mathbb{F}_3[T]$, so $3 \mid [\mathcal{O}_K : \mathbb{Z}[\sqrt[3]{2}]]$.

By Cases 1 and 2, $[\mathcal{O}_K : \mathbb{Z}[\sqrt[3]{2}]] = 1$, so $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$. 
Example 2.4. Let $K = \mathbb{Q}(\sqrt[4]{44})$ 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 $[\mathcal{O}_K : \mathbb{Z}[\sqrt[4]{44}]]$ are 2, 3, and 11.

Case 1: $p = 2$.
From $f(T) \equiv T^3$ mod 2, take $\pi_1(T) = T$. Then

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

so $F(T) \equiv 0 \text{ mod } 2$. Therefore $\pi_1(T) | \overline{F}(T)$ in $\mathbb{F}_2[T]$, so $2 \mid [\mathcal{O}_K : \mathbb{Z}[\sqrt[4]{44}]].$

Case 2: $p = 3$.
From $f(T) \equiv (T + 1)^3$ mod 3, take $\pi_1(T) = T + 1$. Then

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

so $F(T) \equiv -T(T + 1)$ mod 3, which shows $\pi_1(T) | \overline{F}(T)$ in $\mathbb{F}_3[T]$. Thus $3 \mid [\mathcal{O}_K : \mathbb{Z}[\sqrt[4]{44}]].$

Case 3: $p = 11$.
From $f(T) \equiv T^3$ mod 11, take $\pi_1(T) = T$. Then

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

so $\pi_1(T) \not| \overline{F}(T)$ in $\mathbb{F}_{11}[T]$. Thus $11 | [\mathcal{O}_K : \mathbb{Z}[\sqrt[4]{44}]].$

Example 2.5. Let $K = \mathbb{Q}(\alpha)$ where $\alpha$ 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 $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ is 2.

From $f(T) \equiv T^2(T + 1) \text{ mod } 2$, 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 $F(T) \equiv T(T + 1)$ mod 2. Since $\pi_1(T) | \overline{F}(T)$ in $\mathbb{F}_2[T]$, $2 \mid [\mathcal{O}_K : \mathbb{Z}[\alpha]].$

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

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

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

so $F(T) \equiv T \text{ mod } 2$. Therefore $\pi_1(T) | \overline{F}(T)$ in $\mathbb{F}_2[T]$, so $2 \mid [\mathcal{O}_K : \mathbb{Z}[\alpha]].$

Example 2.7. Let $K = \mathbb{Q}(\alpha)$ where $\alpha$ 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 $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ are 2 and 5.

Case 1: $p = 2$.
From $f(T) \equiv T^3 \text{ mod } 2$, take $\pi_1(T) = T$. Then

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

so $F(T) \equiv T + 1 \text{ mod } 2$. Therefore $\pi_1(T) \not| \overline{F}(T)$ in $\mathbb{F}_2[T]$, so $2 \mid [\mathcal{O}_K : \mathbb{Z}[\alpha]].$

Case 2: $p = 5$.
From $f(T) \equiv (T + 2)(T - 1)^2 \text{ mod } 5$, 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 $F(T) \equiv T - 1 \text{ mod } 5$. Therefore $\pi_2(T) | \overline{F}(T)$ in $\mathbb{F}_5[T]$, so $5 \mid [\mathcal{O}_K : \mathbb{Z}[\alpha]].$
Example 2.8. Let $K = \mathbb{Q}(\alpha)$ 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 $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ 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 $\overline{\pi}_1(T) \nmid \overline{F}(T)$ in $\mathbb{F}_2[T]$, so $2 \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$.

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 $\overline{F}(T)$ in $\mathbb{F}_3[T]$ is divisible by $\overline{\pi}_1(T)$ (or $\overline{\pi}_2(T)$),

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

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 $\overline{\pi}_1(T) \nmid \overline{F}(T)$ in $\mathbb{F}_5[T]$, so $5 \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$.

Example 2.9. Let $K = \mathbb{Q}(\alpha)$ where $\alpha$ 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 $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ is 3.

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

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

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

Example 2.10. Let $K = \mathbb{Q}(\alpha)$ 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 $[\mathcal{O}_K : \mathbb{Z}[\sqrt{5}]]$ 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 $\overline{\pi}_1(T) \mid \overline{F}(T)$ in $\mathbb{F}_2[T]$, so $2 \mid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$.

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

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

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 $\mathbb{Z}[T]$ 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 \( \pi_1(T) = T, p \mid [\mathcal{O}_K : \mathbb{Z}[\alpha]] \) if and only if \( \mathcal{F}(T) \) is divisible by \( T \) in \( \mathbb{F}_p[T] \), which is equivalent to \( p^2 \mid a_0 \) in \( \mathbb{Z} \). Thus \( p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]] \) 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 \( f(T) \mod p \) is separable. Then every \( e_j \) is 1 in Theorem 1.4, so \( p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]] \). That also follows from the fact that \([\mathcal{O}_K : \mathbb{Z}[\alpha]] \) divides \( \text{disc}(f) \) and \( \text{disc}(f) \neq 0 \) mod \( p \) by separability of \( f(T) \mod p \).

**Example 2.13.** Let \( f_n(T) = T^n - T - 1 \). For each \( n \geq 2 \), \( f_n(T) \) is irreducible over \( \mathbb{Q} \).

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

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

Let \( K_n = \mathbb{Q}(\alpha_n) \), where \( \alpha_n \) is a root of \( f_n(T) \), so \( [K_n : \mathbb{Q}] = n \). Numerical data suggest \( \text{disc}(f_n(T)) \) is nearly always squarefree. When it is squarefree, \( \mathcal{O}_{K_n} = \mathbb{Z}[\alpha_n] \). 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

\[
(2.1) \quad T^{130} - T - 1 \equiv (T - 8)^2(T - 20)\bar{\pi}_{22}(T)\pi_{42}(T)\pi_{63}(T) \mod 83
\]

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

Let \( \pi_d(T) \) be a monic lift of \( \pi_d(T) \) to \( \mathbb{Z}[T] \), so

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

for some \( F(T) \in \mathbb{Z}[T] \). The only repeated factor of \( T^{130} - T - 1 \mod 83 \) is \( (T - 8)^2 \), and it turns out that \( F(8) \equiv 0 \mod 83 \), so \( (T - 8) \mid \mathcal{F}(T) \) in \( \mathbb{F}_{83}[T] \). Therefore \([\mathcal{O}_{K_{130}} : \mathbb{Z}[\alpha_{130}]] \) 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.** (\( \Leftarrow \Rightarrow \)) We prove the contrapositive: if \( p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]] \) then \( \pi_j(T) \nmid \mathcal{F}(T) \) in \( \mathbb{F}_p[T] \) whenever \( e_j \geq 2 \), where \( e_j \) is taken from (1.2).

If \( \pi_j(T) \mid \mathcal{F}(T) \) in \( \mathbb{F}_p[T] \) for some \( j \) then \( F(T) = \pi_j(T)A(T) + pB(T) \) for some \( A(T) \) and \( B(T) \in \mathbb{Z}[T] \), which upon setting \( T = \alpha \) shows \( F(\alpha) \in (p, \pi_j(\alpha)) \). Thanks to (1.1), which can be used since \( p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]] \), 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 \( \mathfrak{p}_j \mid (F(\alpha)) \), so \( \pi_j(T) \nmid \mathcal{F}(T) \) in \( \mathbb{F}_p[T] \).

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

\[
(\pi_1(\alpha))^{e_1} \cdots (\pi_g(\alpha))^{e_g} = (p)(F(\alpha)).
\]

To get \( \mathfrak{p}_j \mid (F(\alpha)) \) 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 \( \mathfrak{p}_j^2 \mid (\pi_j(\alpha)) \), 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/irredselmerpoly.pdf.
prime ideals, so $p_j \nmid (\pi_j(\alpha))$, (otherwise $p_j$ divides $\gcd((p), (\pi_j(\alpha))) = p_i$, which it doesn’t). On the left side of (3.1), the highest power of $p_j$ in its factorization is therefore $e_j$. Since $p_j^{e_j} \mid (p)$, (3.1) tells us $p_j \nmid (F(\alpha))$.

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

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

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

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

$$\overline{A}(T) = \gcd(\overline{\alpha}_0 + \overline{\alpha}_1 T + \cdots + \overline{\alpha}_{n-1} T^{n-1}, \overline{f}(T)).$$

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

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

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

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

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

Setting $T = \alpha$,

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

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

$$\overline{A}(T) = (\overline{\alpha}_0 + \overline{\alpha}_1 T + \cdots + \overline{\alpha}_{n-1} T^{n-1})u(T) + \overline{f}(T)v(T).$$

We can set $T = \alpha$ on both sides as long as we view the values on both sides in $O_K/pO_K$:

$$A(\alpha) \equiv (c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1})u(\alpha) \equiv (p\beta)u(\alpha) \equiv 0 \mod pO_K$$

since $\beta \in O_K$. Thus $\left[\frac{p}{A(\alpha)}\right]$ in $O_K$.

Since $A(\alpha)/p$ is an algebraic integer in $K$, it satisfies a monic relation of integral dependence over $\mathbb{Z}$, 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 $a_0, \ldots, a_{d-1}$. Multiply through by $p^d$:

$$(3.4) \quad A(\alpha)^d + pa_{d-1}A(\alpha)^{d-1} + \cdots + p^{d-1}a_1A(\alpha) + p^da_0 = 0.$$
Such a brute force search is not necessary: Dedekind gave a method of constructing from a choice of integers in \(\mathbb{Z}[\alpha]\) in \(p\) index theorem because each term on the left has a factor \(p^d\), so divide through by \(p^d\):
\[
(F(\alpha))^d + a_d B(\alpha) (F(\alpha))^{d-1} + \cdots + a_1 B(\alpha) (F(\alpha)) + a_0 B(\alpha)^d = 0.
\]
Therefore
\[
(-F(T))^d + a_d B(T) (-F(T))^{d-1} + \cdots + a_1 B(T) (-F(T)) + a_0 B(T)^d = f(T) k(T)
\]
for some \(k(T) \in \mathbb{Z}[T]\). Reduce both sides modulo \(p\). Since \(\text{gcd}(f(T), \overline{B}(T))\) are divisible by \(\pi(T)\) in \(\mathbb{F}_p[T]\), we get \(\pi(T) | \overline{f}(T)\) in \(\mathbb{F}_p[T]\). \(\square\)

4. An algebraic integer not in \(\mathbb{Z}[\alpha]\) when \(p | [\mathcal{O}_K : \mathbb{Z}[\alpha]]\)

If \(p | [\mathcal{O}_K : \mathbb{Z}[\alpha]]\) then \(\mathcal{O}_K / \mathbb{Z}[\alpha]\) has order divisible by \(p\); there’s some \(h(\alpha) \in \mathbb{Z}[\alpha]\) such that \(h(\alpha)/p \in \mathcal{O}_K - \mathbb{Z}[\alpha]\). In principle, we can find \(h(\alpha)\) by searching for an algebraic integer among representatives of the \(p^n - 1\) nonzero cosets of \((1/p)\mathbb{Z}[\alpha]/\mathbb{Z}[\alpha]\); 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 \(\pi_j(T)\) dividing \(\overline{f}(T)\) with \(e_j \geq 2\) in (1.2). Such \(\pi_j(T)\) exists by Dedekind’s index theorem because \(p | [\mathcal{O}_K : \mathbb{Z}[\alpha]]\).

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

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

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

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

<table>
<thead>
<tr>
<th>Example</th>
<th>(f(T))</th>
<th>(p)</th>
<th>(\pi(T))</th>
<th>(h(T))</th>
<th>(h(\alpha)/p \in \mathcal{O}_K - \mathbb{Z}[\alpha])</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>(T^3 - 12)</td>
<td>2</td>
<td>(T)</td>
<td>(T^2)</td>
<td>(\sqrt[3]{12}^2/2)</td>
</tr>
<tr>
<td>2.2</td>
<td>(T^3 - 10)</td>
<td>3</td>
<td>(T - 1)</td>
<td>(T^2 + T + 1)</td>
<td>((\sqrt[3]{10}^2 + \sqrt[3]{10} + 1)/3)</td>
</tr>
<tr>
<td>2.4</td>
<td>(T^3 - 44)</td>
<td>2</td>
<td>(T)</td>
<td>(T^2)</td>
<td>(\sqrt[3]{44}^2/2)</td>
</tr>
<tr>
<td>2.4</td>
<td>(T^3 - 44)</td>
<td>3</td>
<td>(T + 1)</td>
<td>(T^2 - T + 1)</td>
<td>((\sqrt[3]{44}^2 - \sqrt[3]{44} + 1)/3)</td>
</tr>
<tr>
<td>2.5</td>
<td>(T^3 - T^2 - 2T - 8)</td>
<td>2</td>
<td>(T)</td>
<td>(T^2 + T)</td>
<td>((\alpha^2 + \alpha)/2)</td>
</tr>
<tr>
<td>2.6</td>
<td>(T^3 + 2T + 4)</td>
<td>2</td>
<td>(T)</td>
<td>(T^2)</td>
<td>(\alpha^2/2)</td>
</tr>
<tr>
<td>2.7</td>
<td>(T^3 + 2T + 22)</td>
<td>5</td>
<td>(T - 1)</td>
<td>(T^2 + T + 3)</td>
<td>((\alpha^2 + \alpha + 3)/5)</td>
</tr>
<tr>
<td>2.8</td>
<td>(T^4 - 20T^2 + 10)</td>
<td>3</td>
<td>(T - 1)</td>
<td>((T - 1)(T + 1)^2)</td>
<td>((\alpha - 1)(\alpha + 1)^2/3)</td>
</tr>
<tr>
<td>2.8</td>
<td>(T^4 - 20T^2 + 10)</td>
<td>3</td>
<td>(T + 1)</td>
<td>((T + 1)(T - 1)^2)</td>
<td>((\alpha + 1)(\alpha - 1)^2/3)</td>
</tr>
<tr>
<td>2.10</td>
<td>(T^4 + T^2 + 4)</td>
<td>2</td>
<td>(T)</td>
<td>(T^3 + T)</td>
<td>((\alpha^3 + \alpha)/2)</td>
</tr>
</tbody>
</table>

\(^2\)This is from Theorem 8.2 of https://www.math.leidenuniv.nl/~psh/ANTproc/08psh.pdf.
Remark 4.2. In the first and third rows, $\sqrt{12^2/2} = \sqrt{18}$ and $\sqrt{44^2/2} = \sqrt{242}$.

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 $\alpha^{n-1}/p$ is integral over $\mathbf{Z} [\alpha]$:
  \[
  \left( \frac{\alpha^{n-1}}{p} \right)^2 = \frac{\alpha^{2(n-1)}}{p^2} = \frac{\alpha^{n-2}\alpha^n}{p^2} = \alpha^{n-2}m \in \mathbf{Z} [\alpha].
  \]
  This fits Theorem 4.1 with $\pi(T) = T$, $F(T) = -pm$, and $h(T) = T^{n-1}$.

- If $f(T) = T^n + an + T^{n-1} + \cdots + a_0$ 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 $\alpha^{n-1}/p$ is integral over $\mathbf{Z} [\alpha]$:
  \[
  \alpha^n = -\sum_{j=0}^{n-1} a_j \alpha^j,
  \]
  \[
  \left( \frac{\alpha^{n-1}}{p} \right)^2 = \frac{\alpha^n}{p^2} \alpha^{n-2} = -\sum_{j=0}^{n-1} \frac{a_j}{p^2} \alpha^{n-2+j} = -\left( \sum_{j=1}^{n-1} \frac{a_j}{p} \alpha^{j-1} \right) \frac{\alpha^{n-1}}{p} - \frac{a_0}{p^2} \alpha^{n-2}.
  \]
  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 $\overline{f}(T) = \overline{q(T)}\overline{\pi(T)}$, so we can use $q(T)$ as $h(T)$.

If $h_1(T)$ and $h_2(T)$ are both monic lifts of $\overline{f}(T)/\overline{\pi(T)}$ 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 of $\overline{f}(T)/\overline{\pi(T)}$ to $\mathbf{Z}[T]$: then it automatically works for all other monic lifts.

Let $\overline{\pi}(T) = \overline{\pi}_j(T)$. We will show $h(\alpha)/p \in \mathcal{O}_K - \mathbf{Z} [\alpha]$ for the specific monic lift $h(T) := \prod_{i \neq j} \pi_i(T)\pi_j(T)^{\alpha_i - 1}$. 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 $\alpha$ 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 $p$ dividing $(p)$ that the multiplicity of $p$ in $(h(\alpha))$ is at least as large as the multiplicity of $p$ in $(p)$. Since $p \mid [\mathcal{O}_K : \mathbf{Z} [\alpha]]$, we can not assume $(p)$ factors in the same way as $\overline{f}(T)$ factors: (1.1) is unavailable to us.

Setting $T = \alpha$ in (1.3), $\pi_1(\alpha)\pi_2(\alpha)\cdots\pi_g(\alpha) = -pF(\alpha)$, so $\pi(\alpha)h(\alpha) = -pF(\alpha)$ by the way we defined $h(T)$. Therefore we have the equation of principal ideals

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

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

Case 1: $\pi_i(T) \neq \pi_j(T)$. In $\mathbf{F}_p[T]$, $\pi_i(T)$ and $\pi_j(T)$ are distinct monic irreducibles, so they are relatively prime: $\pi_i(T)u(T) + \pi_j(T)v(T) = 1$, 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 $T = \alpha$, $\pi_i(\alpha)U(\alpha) + \pi_j(\alpha)V(\alpha) = 1 + pM(\alpha)$. Therefore the second equation in (4.1) implies the multiplicity of $p$ in $(h(\alpha))$ is at least as large as the multiplicity of $p$ in $(p)$.

Case 2: $\pi_i(T) = \pi_j(T)$.
Now \( p \) divides \((p)\) and \((\pi_j(\alpha))\). Let \( p \) divide \((p)\) with multiplicity \( a \), divide \((\pi_j(\alpha))\) with multiplicity \( b \), and divide \((F(\alpha))\) with multiplicity \( c \):
\[
(p) = p^a a, \quad (\pi_j(\alpha)) = p^b b, \quad (F(\alpha)) = p^c c,
\]
where \( p \) does not divide \( a \), \( b \), or \( c \). 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 \((\pi_1(\alpha)), \ldots, (\pi_\mu(\alpha))\), so the multiplicity of \( p \) 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 \( p \) in \((h(\alpha))\) is \((e_j - 1)b\). We want to show this is at least as large as the multiplicity of \( p \) 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 \( e_j \geq 2 \), \( a + c = e_j b \geq 2 b \), so \( c - b \geq b - a \geq 0 \), and thus \( c \geq b \).

Case (ii): \( b \leq a \). Since \( \pi_j(T) \mid F(T) \mid F_p[T], F(T) = \pi_j(T)H(T) + pJ(T) \) for some \( H(T) \) and \( J(T) \) in \( \mathbb{Z}[T] \). Therefore \( F(\alpha) = \pi_j(\alpha)H(\alpha) + pJ(\alpha) \) in \( \mathbb{Z}[^{\alpha}] \subset \mathcal{O}_K \). The multiplicity of \( p \) in \((\pi_j(\alpha))\) is \( b \) and the multiplicity of \( p \) in \((p)\) is \( a \). Since \( b \leq a \), \( p^b \) divides \((\pi_j(\alpha))\) and \((p)\), so \( \pi_j(\alpha)H(\alpha) + pJ(\alpha) \equiv 0 \mod p^b \). Thus \( p^b \mid (F(\alpha)) \), 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 \( F(T) \) with \( e_j \geq 2 \) in \((1.2)\) and constructs an algebraic integer not in \( \mathbb{Z}[^\alpha] \) of the form \( h(\alpha)/p \) where \( h(\alpha) \in \mathbb{Z}[T] \). In \( \mathcal{O}_K/\mathbb{Z}[\alpha] \), \( h(\alpha)/p \) has order \( p \), so \( p \mid [\mathcal{O}_K : \mathbb{Z}[^\alpha]] \). 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 \( p \mid [\mathcal{O}_K : \mathbb{Z}[^\alpha]] \) and we use Theorem 4.1 to find a number \( \beta \in \mathcal{O}_K - \mathbb{Z}[^\alpha] \), it is not necessarily the case that \( \mathbb{Z}[^\alpha] \subset \mathbb{Z}[^\beta] \). Here is an example of this.

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

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

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

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

This illustrates why Theorems 1.4 and 4.1 can’t always be iterated to enlarge a subring \( \mathbb{Z}[\alpha] \) 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 \( \mathbb{Q}(\alpha) \) for \( \alpha \in \mathcal{O}_K \) with minimal polynomial \( f(T) \).

Step 2: Since \([\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 \mid \text{disc}(f) \text{, factor disc}(f) to assemble a list of primes } p \text{ such that } p^2 \mid \text{disc}(f) \). These are the possible prime factors of \([\mathcal{O}_K : \mathbb{Z}[\alpha]]\).
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 \([O_K : \mathbb{Z}[\alpha]]\). If there are no such primes then \([O_K : \mathbb{Z}[\alpha]] = 1\), so \(O_K = \mathbb{Z}[\alpha]\) and we are done. If \([O_K : \mathbb{Z}[\alpha]] > 1\), then let \(S\) be the set of prime factors of \([O_K : \mathbb{Z}[\alpha]]\).

Step 4: For \(p \in S\), and an order \(O\) in \(K\), such as \(\mathbb{Z}[\alpha]\), we want to build an order \(O_p\) containing \(O\) with \(p \nmid [O_K : O_p]\).

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

\[O' = \{x \in K : xI_p \subset I_p\},\]

so \(O \subset O' \subset O_K\). Methods of computing \(I_p\) and \(O'\) starting from a \(\mathbb{Z}\)-basis of \(O\), are in [2, Sect. 6.1.1].

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

- If \(O' > O\) then the highest power of \(p\) dividing \([O_K : O']\) is less than the highest power of \(p\) dividing \([O_K : O]\). Rename \(O'\) as \(O\) and repeat Step 4.
- If \(O' = O\) then \(p \nmid [O_K : O]\). 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 \(p \nmid [O_K : O]\) then \([O' : O]\) is a \(p\)-power dividing \([O_K : O]\), so \([O' : O] = 1\) and thus \(O' = O\).) Set \(O_p = O\).

Step 6: Run through Steps 4 and 5 for each \(p \in S\), starting with the initial order \(O\) being \(\mathbb{Z}[\alpha]\), to get an order \(O_p\) containing \(\mathbb{Z}[\alpha]\) such that \(p \nmid [O_K : O_p]\).

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

1. If there is an \(\alpha \in O_K\) such that \(K = \mathbb{Q}(\alpha)\) and \(p \mid [O_K : \mathbb{Z}[\alpha]]\), then we can read off how \(pO_K\) decomposes into prime ideals from the way \(f(T) \mod p\) decomposes into irreducibles in \(\mathbb{F}_p[T]\), where \(f(T)\) is the minimal polynomial of \(\alpha\) over \(\mathbb{Q}\).

2. If there is an \(\alpha \in O_K\) such that \(K = \mathbb{Q}(\alpha)\), then a necessary and sufficient condition for \(p \mid [O_K : \mathbb{Z}[\alpha]]\) is a divisibility criterion in \(\mathbb{F}_p[T]\) (Dedekind’s index theorem).

3. When \(p \mid [O_K : \mathbb{Z}[\alpha]]\), there is a systematic way to find an element of order \(p\) in \(O_K/\mathbb{Z}[\alpha]\) (Theorem 4.1).

A natural issue to address would round out this list of properties is how to determine if there is an \(\alpha \in O_K\) such that \(K = \mathbb{Q}(\alpha)\) and \(p \mid [O_K : \mathbb{Z}[\alpha]]\). Here we don’t pick \(\alpha\) and look for \(p\) such that \(p \mid [O_K : \mathbb{Z}[\alpha]]\), but pick \(p\) and look for \(\alpha\) such that \(p \mid [O_K : \mathbb{Z}[\alpha]]\). The index of \(K\) is

\[i(K) = \gcd([O_K : \mathbb{Z}[\alpha]]),\]

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

From (1.1), which is a consequence of \(p \nmid [O_K : \mathbb{Z}[\alpha]]\) for some \(\alpha\) but makes no direct reference to \(\alpha\), we get a necessary condition for \(p \nmid i(K)\) in terms of the prime ideal factorization \(pO_K = p_1^{e_1} \cdots p_g^{e_g}\): writing \(N(p) = p_i^{f_i}\), there must be distinct monic irreducibles \(\pi_1(T), \ldots, \pi_g(T)\) in \(\mathbb{F}_p[T]\) such that \(\deg(\pi_i(T)) = f_i\) for \(i = 1, \ldots, g\).
Example 5.1. Since $F_2[T]$ has two irreducibles of degree 1 and one irreducible of degree 2, if $2O_K$ has at least three prime ideal factors with residue field degree 1 (making $[K : Q] \geq 3$) or at least two prime ideal factors with residue field degree 2 (making $[K : Q] \geq 4$) then it’s impossible to have $2 \nmid i(K)$: for all $\alpha$ in $O_K$ that generate $K/Q$, $[O_K : Z[\alpha]]$ is even. An example of the first case is $K = Q(\beta)$ where $\beta$ 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 $K = Q(\gamma)$ where $\gamma$ is a root of $T^4 - 3T^2 - 4T + 5$ (a quartic field in which $2 = pp'$ with $f(p|2) = f(p'|2) = 2$).

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 $[K : Q] = n$ and $p$ be a prime. When $pO_K$ has prime ideal factorization $p_1^{e_1} \cdots p_g^{e_g}$ and $N(p_i) = p^{f_i}$, we have $p \nmid i(K)$ if and only if there are distinct monic irreducibles $\pi_i(T), \ldots, \pi_g(T)$ in $F_p[T]$ such that $\deg(\pi_i(T)) = f_i$ for $i = 1, \ldots, g$.

Proof. We already indicated from (1.1) that if $p \nmid i(K)$, meaning $p \mid [O_K : Z[\alpha]]$ for a primitive integral $\alpha$ in $K$, then there are distinct monic irreducible $\pi_i(T)$ in $F_p[T]$ with degree $f_i$ for $i = 1, \ldots, g$.

Now assume there are distinct monic irreducible $\pi_i(T) \in F_p[T]$ such that $\deg \pi_i(T) = f_i$ for $i = 1, \ldots, g$. Let $\pi_i(T) \in Z[T]$ be a monic lifting of $\pi_i(T)$, so $\deg(\pi_i(T)) = \deg(\pi_i(T)) = f_i$. We will use these polynomials and the Chinese remainder theorem (among other tools) to show $K/Q$ has a primitive integral element $\alpha$ such that $p \nmid [O_K : Z[\alpha]]$, 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 $\alpha \in O_K$ such that $p_i = (p, \pi_i(\alpha))$ for $i = 1, \ldots, g$.

The field $O_K/p_i$ has order $p^{f_i}$. A standard property of finite fields is that each irreducible of degree $f_i$ in $F_p[T]$ has a root (in fact a full set of roots) in each field of size $p^{f_i}$. Therefore $\pi_i(r_i) \equiv 0 \mod p_i$ for some $r_i \in O_K$, so $p_i \mid (\pi_i(r_i))$. Also $p_i \mid (p)$, so $p_i \mid (p, \pi_i(r_i))$. It can happen that $p_i \not\equiv (p, \pi_i(r_i))$, and one reason would be that $p_i^2 \not\equiv \deg(p_i) \equiv \deg(\pi_i) \equiv f_i$. To fix that, if $p_i^2 \not\equiv (\pi_i(r_i))$ then we can adjust $r_i$ modulo $p_i$ so that $p_i^2 \equiv (\pi_i(r_i))$, as follows.

Pick $\beta_i \in p_i - p_i^2$, so $p_i$ divides $p_i$ just once. Then $\pi_i(r_i + \beta_i) \equiv \pi_i(r_i) \equiv 0 \mod p_i$, while $\pi_i(r_i + \beta_i) = \pi_i(r_i) + \pi_i'(r_i) \beta_i \equiv \pi_i(r_i) \beta_i \equiv p_i^2 \equiv 0 \mod p_i^2$ from the assumption that $\pi_i(r_i) \equiv 0 \mod p_i^2$. Since $\pi_i(T)$ is separable in $F_p[T]$, $\pi_i(r_i) \equiv 0 \mod p_i$ implies $\pi_i'(r_i) \not\equiv 0 \mod p_i^2$, so the ideal $(\pi_i'(r_i) \beta_i) = (\pi_i(r_i) \beta_i)$ is divisible by $p_i$ just once: $p_i \dagger (\pi_i'(r_i))$, $p_i \nmid (\beta_i)$, and $p_i^2 \nmid (\beta_i)$. Replacing $r_i$ by $r_i + \beta_i$ puts us in the situation that $\pi_i(r_i) \equiv 0 \mod p_i$ as before and now $\pi_i(r_i) \equiv 0 \mod p_i^2$, so $p_i$ divides $(p, \pi_i(r_i))$ just once.

Now let’s use the Chinese remainder theorem: there is an $\alpha \in O_K$ such that $\alpha \equiv r_i \mod p_i^2$ for $i = 1, \ldots, g$, so $\pi_i(\alpha) \equiv \pi_i(r_i) \equiv 0 \mod p_i$ and $\pi_i(\alpha) \equiv \pi_i(r_i) \not\equiv 0 \mod p_i^2$. We are going to show $p_i = (p, \pi_i(\alpha))$. Since $p_i$ divides $(p)$ and divides $(\pi_i(\alpha))$ just once, $p_i$ divides $(p, \pi_i(\alpha))$ just once. What other prime ideal divides $(p, \pi_i(\alpha))$? If $q$ is a prime ideal dividing $(p, \pi_i(\alpha))$ then $q \mid (p)$, so $q$ is some $p_j$. Then $\pi_i(\alpha) \equiv 0 \mod p_j$. Also $\pi_i(\alpha) \equiv 0 \mod p_j$, so $\alpha \mod p_j$ is a common root in $O_K/p_j$ of $\pi_i(T)$ and $\pi_j(T)$. Distinct monic irreducibles in $F_p[T]$ don’t have common roots in an extension field of $F_p$, so $\pi_i(T) \equiv \pi_j(T)$. That means $j = i$, so $q = p_i$: the only prime ideal dividing $(p, \pi_i(\alpha))$ is $p_i$. Since $p_i$ divides $(p, \pi_i(\alpha))$ just once, $(p, \pi_i(\alpha)) = p_i$ for $i = 1, \ldots, g$.

Step 2: For $\alpha$ as in Step 1, $p_i^{e_i} = (p, \pi_i(\alpha)^{e_i})$ for $i = 1, \ldots, g$, where $pO_K = p_1^{e_1} \cdots p_g^{e_g}$.
The ideal \((p, \pi_i(\alpha)^{e_i})\) is the greatest common divisor of \((p)\) and \((\pi_i(\alpha)^{e_i})\). Let \(q\) be a prime ideal dividing \((p, \pi_i(\alpha)^{e_i})\). Then \([p] = [q] \mid (\pi_i(\alpha)^{e_i})\), so \(q\) divides \((p)\) and \((\pi_i(\alpha))\).

Since \((p, \pi_i(\alpha)) = (p_i, q)\), \(q\) must be \(p_i\), so \((p, \pi_i(\alpha)^{e_i})\) is a power of \(p_i\). The highest power of \(p_i\) dividing \((p)\) is \(p_i^{e_i}\), and \(p_i^{e_i} \mid (\pi_i(\alpha)^{e_i})\) since \(p_i \mid (\pi_i(\alpha))\), so \((p, \pi_i(\alpha)^{e_i}) = p_i^{e_i}\).

Step 3: Evaluation at \(\alpha \mod p_i^{e_i}\) is a ring isomorphism \(F_p[T]/(\pi_i(T)^{e_i}) \to \mathcal{O}_K/p_i^{e_i}\) for \(i = 1, \ldots, g\).

The ring \(\mathcal{O}_K/p_i^{e_i}\) has characteristic \(p\) since \(p \equiv 0 \mod p_i^{e_i}\). Thus evaluation at \(\alpha \mod p_i^{e_i}\) is a ring homomorphism \(F_p[T] \to \mathcal{O}_K/p_i^{e_i}\). We have \(\pi_i(\alpha)^{e_i} \equiv 0 \mod p_i^{e_i}\) since \(p_i \mid (\pi_i(\alpha))\), so \(\pi_i(T)^{e_i}\) is in the kernel: we get a ring homomorphism \(F_p[T]/(\pi_i(T)^{e_i}) \to \mathcal{O}_K/p_i^{e_i}\) by \(\overline{g}(T) \mapsto g(\alpha) \mod p_i^{e_i}\). We will show this is injective, and therefore it is an isomorphism since \(\frac{F_p[T]}{(\pi_i(T)^{e_i})} = \mathbb{F}^{e_i}_{p_i} = \mathcal{O}_K/p_i^{e_i}\).

Each element of \(F_p[T]/(\pi_i(T)^{e_i})\) can be written uniquely in base \(\pi_i(T)\) as

\[
\tau_0(T) + \tau_1(T)\pi_i(T) + \cdots + \tau_{e_i-1}(T)\pi_i(T)^{e_i-1} \mod \pi_i(T)^{e_i}
\]

where the coefficients \(\tau_k(T)\) in \(F_p[T]\) are 0 or have degree less than \(\deg(\pi_i(T)) = f_i\). Suppose (5.1) is mapped to 0 in \(\mathcal{O}_K/p_i^{e_i}\) after we substitute \(\alpha \mod p_i^{e_i}\) for \(T\):

\[
c_0(\alpha) + c_1(\alpha)\pi_i(T) + \cdots + c_{e_i-1}(\alpha)\pi_i(T)^{e_i-1} \mod p_i^{e_i}.
\]

We want the kernel of \(F_p[T]/(\pi_i(T)^{e_i}) \to \mathcal{O}_K/p_i^{e_i}\) to be 0, so all \(\tau_k(T)\) should be 0 in \(F_p[T]\).

If any are not, let \(k \leq e_i - 1\) be minimal with \(\tau_k(T) \neq 0 \in F_p[T]\). Then

\[
c_k(\alpha)\pi_i(\alpha)^k + \cdots + c_{e_i-1}(\alpha)\pi_i(\alpha)^{e_i-1} \equiv 0 \mod p_i^{e_i}.
\]

Since \(k \leq e_i - 1\), we can reduce the congruence to modulus \(p_i^{k+1}\):

\[
c_k(\alpha)\pi_i(\alpha)^k \equiv 0 \mod p_i^{k+1},
\]

so \(p_i^{k+1} \mid (c_k(\alpha))(\pi_i(\alpha))^k\). The ideal \((\pi_i(\alpha))\) is divisible by \(p_i\) just once by the \emph{method} used to construct \(\alpha\) in Step 1 (that is, \(\alpha \equiv r_i \mod p_i^2\) and \(\pi_i(r_i) \not\equiv 0 \mod p_i^2\)), so \(p_i \mid (c_k(\alpha))\).

Write that as \(\tau_k(\alpha) = 0\) in the field \(\mathcal{O}_K/p_i\). Since \(\deg(\tau_k(T)) < f_i\) and \(\alpha \mod p_i\) is the root of an irreducible \(\pi_i(T)\) of degree \(f_i\) in \(F_p[T]\), \(\alpha \mod p_i\) is not the root of a polynomial in \(F_p[T]\) of degree less than \(f_i\). Therefore \(\tau_k(T) = 0\) in \(F_p[T]\), which is a contradiction.

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

By the Chinese remainder theorem, we can combine the isomorphisms \(F_p[T]/(\pi_i(T)^{e_i}) \to \mathcal{O}_K/p_i^{e_i}\) for \(i = 1, \ldots, g\) from Step 3 that use evaluation at \(\alpha \mod p_i^{e_i}\) to get an isomorphism

\[
F_p[T]/(\pi_1(T)^{e_1} \cdots \pi_g(T)^{e_g}) \to \mathcal{O}_K/p\mathcal{O}_K
\]

using evaluation at \(\alpha \mod p\mathcal{O}_K\).

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

\[
f(\alpha) = 0 \implies f(\alpha) \equiv 0 \mod p\mathcal{O}_K \implies \pi_1(T)^{e_1} \cdots \pi_g(T)^{e_g} \mid \overline{f}(T)\text{ in } F_p[T]\text{ by (5.2).}
\]

Since \(f\) is monic,

\[
\deg f = \deg \overline{f} = \sum_{i=1}^g e_i \deg(\pi_i) = \sum_{i=1}^g e_i f_i = [K : \mathbb{Q}].
\]

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

\[
\overline{f}(T) = \pi_1(T)^{e_1} \cdots \pi_g(T)^{e_g}
\]
in $F_p[T]$ since both sides are monic and the right side is a factor of the left side. We can rewrite (5.2) as an isomorphism

$$F_p[T]/(f(T)) \to O_K/pO_K$$

using evaluation at $\alpha \text{ mod } pO_K$.

To prove $p \nmid [O_K : Z[\alpha]]$, we argue by contradiction. Suppose $p \mid [O_K : Z[\alpha]]$, so $O_K/Z[\alpha]$ has order divisible by $p$ and thus it has an element $\beta$ of order $p$: $\beta \in O_K - Z[\alpha]$ and $p\beta \in Z[\alpha]$. Write $p\beta = h(\alpha)$, where $h(T) \in Z[T]$. Then $h(\alpha) \equiv 0 \text{ mod } pO_K$, so the isomorphism (5.3) vanishes on $h(T)$, which means $\bar{f}(T) \mid \bar{h}(T)$ in $F_p[T]$, so $h(T) \in (p, f(T))$ in $Z[T]$. Evaluating that at $\alpha$, $h(\alpha) \in pZ[\alpha]$ since $f(\alpha) = 0$, so $\beta = h(\alpha)/p \in Z[\alpha]$, which is a contradiction. Thus $p \nmid [O_K : Z[\alpha]]$. \hfill \Box

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 $pO_K$ with residue field degree $d$ and $N_p(d)$ be the number of monic irreducible polynomials of degree $d$ in $F_p[T]$. Then Theorem 5.2 says

$$p \nmid i(K) \iff g_{p, K}(d) \leq N_p(d) \text{ for all } d \leq \lceil K : Q \rceil.$$

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

$$p \mid i(K) \iff N_p(d) < g_{p, K}(d) \text{ for some } d \leq \lceil K : Q \rceil.$$

**Theorem 5.3.** A prime that is less than $\lceil K : Q \rceil$ and splits completely in $K$ divides $i(K)$.

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

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

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

*Proof. If $p \mid i(K)$ then $g_{p, K}(d) > N_p(d)$ for some $d \leq \lceil K : Q \rceil$. By the formula $\sum_{i=1}^g c_i f_i = \lceil K : Q \rceil$ for the prime $p$, $d g_{p, K}(d) \leq \lceil K : Q \rceil$ by summing on the left side only over $i$ where $f(p_i|p) = d$. Therefore $d N_p(d) < m g_{p, K}(d) \leq \lceil K : Q \rceil$. The number $N_p(d)$ is divisible by $p$ since if $\pi(T)$ is irreducible in $F_p[T]$ then so is $\pi(T + c)$ for all $c \in F_p$. Positivity of $N_p(d)$ therefore implies $d N_p(d) \geq p$, so $p \leq d N_p(d) < \lceil K : Q \rceil$. \hfill \Box

Conversely, Bauer [1] showed that if $p < n$ for an integer $n$ then there are number fields $K$ of degree $n$ over $Q$ such that $p \mid i(K)$ by showing for each prime $p$ and $n \in Z^+$ 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 $[K : Q] = 2$ then there is no prime less than $[K : Q]$, so $i(K) = 1$. This is well-known since the ring of integers of a quadratic field has the form $Z[\alpha]$ for some $\alpha$.\footnote{The condition $i(K) = 1$ does not require $O_K = Z[\alpha]$. If two indices $[O_K : Z[\beta]]$ and $[O_K : Z[\gamma]]$ are greater than 1 and are relatively prime, then $i(K) = 1$. For example, if $K = Q(\sqrt{175})$ then $O_K \neq Z[\alpha]$ for all $\alpha$ in $K$, but $[O_K : Z[\sqrt{175}]] = 5$ and $[O_K : Z[\sqrt{245}]] = 7$, 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 \([K : \mathbb{Q}] = 3\) 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 \([K : \mathbb{Q}] \geq 4\). Engstrom [4, p. 234] showed \(i(K)\) is 1 or 2 for all cubic fields.

Example 5.7. If \([K : \mathbb{Q}] = 4\) 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, \(2 = p^3p_2p_3^2\), or \(2 = p_4p_4'\), and \(3 \mid i(K)\) if and only if 3 splits completely in \(K\). For example, 3 splits completely in \(\mathbb{Q}(\sqrt{-5}, \sqrt{7})\) (first check it splits completely in \(\mathbb{Q}(\sqrt{-5})\) and \(\mathbb{Q}(\sqrt{7})\)), 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 \(\mathbb{Q}(\sqrt{m})\) if and only if \(m \equiv 1 \mod 8\). So when \(m_1, \ldots, m_r\) 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 \(K = \mathbb{Q}(\sqrt{m_1}, \ldots, \sqrt{m_r})\) has degree \(2^r\) over \(\mathbb{Q}\) 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 \(\mathbb{Q}\) being \(\pm 2j\) for \(0 \leq j \leq n\), and \(f(\pm 2j) \neq 0\) by looking at 2-divisibility of the three terms (treat \(j = 0\) and \(j = n\) separately from \(0 < j < n\)). Set \(K_n = \mathbb{Q}(r_n)\) where \(r_n\) is a root of \(f_n(T)\), so \([K_n : \mathbb{Q}] = 3\). For \(n \geq 3\), 2 splits completely in \(K_n\) because \(f_n(T)\) splits completely over the 2-adic numbers \(\mathbb{Q}_2\) by Hensel’s lemma with approximate roots 0, 1, and \(-1\). Thus \(i(K_n)\) is divisible by 2 for \(n \geq 3\).

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 this.\(^5\) Assume \(f_n(T)\) is irreducible over \(\mathbb{Q}\) and set \(L_n = \mathbb{Q}(r_n)\) where \(r_n\) is a root of \(f_n(T)\), so \([L_n : \mathbb{Q}] = 4\). 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 \(\mathbb{Q}_2\) and \(\mathbb{Q}_3\) 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 \([\mathcal{O}_K : \mathbb{Z}[\alpha]]\), 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?

\(^4\)The 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 \(\mathbb{Q}_2\) for large enough \(n\) by \(p\)-adic continuity of roots when \(p = 2\), and Hensel’s lemma confirms this for \(n \geq 3\).

\(^5\)Note \(f_n(T - 1) = T^4 - 10T^4 + 35T^2 - 50T + 24 + 6^n\) is Eisenstein at 5 when \(5 \nmid n\), so \(f_n(T)\) is irreducible over \(\mathbb{Q}\) when \(5 \nmid n\).
The story goes back to Kronecker’s work \([5]\) on algebraic functions. For \(F(x, y) \in \mathbb{C}[x, y]\) that is irreducible and monic in \(y\) (like \(y^3 + (x^2 - x)y + x - 1\), let \(F(x, r) = 0\). The field \(\mathbb{C}(x, r)\) is a finite extension of \(\mathbb{C}(x)\) and \(r\) is integral over \(\mathbb{C}(x)\). Let \(A\) be the integral closure of \(\mathbb{C}[x]\) in \(\mathbb{C}(x, r)\). Both \(A\) and its subring \(\mathbb{C}[x, r]\) are finite free \(\mathbb{C}[x]\)-modules of equal rank, and are analogous to \(\mathcal{O}_K\) and \(\mathbb{Z}[\alpha]\) in the number field \(K = \mathbb{Q}(\alpha)\). The analogue for \(A\) and \(\mathbb{C}[x, r]\) of the number-theoretic formula \(\text{disc}(\mathbb{Z}[\alpha]) = |\mathcal{O}_K : \mathbb{Z}[\alpha]|^2 \text{disc}(K)\) is

\[
D(x) = R(x)^2 \Delta(x),
\]

where \(D(x)\) is \(\text{disc}_{\mathbb{C}[x]}(A)\), \(R(x)\) is the \(\mathbb{C}[x]\)-index of \(\mathbb{C}[x, r]\) in \(A\), and \(\Delta(x)\) is \(\text{disc}_{\mathbb{C}[x]}(A)\). (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 \(\mathbb{C}[x]\)-bases to compute them.) Because \(A\) is more fundamental than \(\mathbb{C}[x, r]\), Kronecker \([5, \text{p. 313}]\) called \(\Delta(x) = \text{disc}_{\mathbb{C}[x]}(A)\) the essential divisor (wesentlichen Theiler) of \(D(x)\) and \(R(x)^2\) the inessential divisor (aussерwesentlichen 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 \(|\mathcal{O}_K : \mathbb{Z}[\alpha]|^2\). We could (but don’t) call this number the inessential divisor of the discriminant of \(\alpha\), so a prime dividing all indices \(|\mathcal{O}_K : \mathbb{Z}[\alpha]|\) 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 \(|\mathcal{O}_K : \mathbb{Z}[\alpha]|^2\) is less important than \(\text{disc}(K)\)) becomes lost and common prime factors of all indices \(|\mathcal{O}_K : \mathbb{Z}[\alpha]|\) seem essential, not inessential. The name “common index divisor” for such primes is better.

References


---

\(^6\) I thank Darij Grinberg for linguistic assistance with Kronecker’s paper.