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 number p, its prime ideal decomposition in the ring of integers $\mathcal{O}_K$ can be read off from the irreducible factorization of $f(T)$ mod p in $\mathbf{F}_p[T]$ provided $p \nmid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$:

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

where $\overline{\pi}_1(T), \ldots, \overline{\pi}_g(T)$ are distinct monic irreducibles in $\mathbf{F}_p[T]$, $\mathrm{N}(\mathfrak{p}_i) = p^{\deg \overline{\pi}_i}$, and $\mathfrak{p}_i = (p, \pi_i(\alpha))$ where $\pi_i(T)$ is an arbitrary monic lift of $\overline{\pi}_i(T)$ to $\mathbf{Z}[T]$. This important result is due to Dedekind [2, Sect. 2].

If $p \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$ then the factorization of $p\mathcal{O}_K$ may or may not match that of $f(T)$ mod 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 from (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 $f(T) \equiv (T-1)^3 \bmod 3$ while $3\mathcal{O}_K = \mathfrak{p}\mathfrak{q}^2$. Here $[\mathcal{O}_K : \mathbf{Z}[\sqrt[3]{10}]] = 3$, and in fact $\mathcal{O}_K = \mathbf{Z}[\alpha]$ where $\alpha = (\sqrt[3]{10}^2 + \sqrt[3]{10} + 1)/3$ has minimal polynomial $T^3 - T^2 - 3T - 3$ over $\mathbf{Q}$ and $T^3 - T^2 - 3T - 3 \equiv (T-1)T^2 \bmod 3$.

Without knowing $\mathcal{O}_K$, we can apply (1.1) to the primes p not dividing the discriminant of $f(T)$ since $[\mathcal{O}_K : \mathbf{Z}[\alpha]]^2 \mid \mathrm{disc}(f)$. To know whether (1.1) is applicable to a prime dividing $\mathrm{disc}(f)$, we would like to know which prime factors of $\mathrm{disc}(f)$ actually divide $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$.

It turns out that there is a nice necessary and sufficient condition for $p \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$ that is valid for all primes and does not require knowing $\mathcal{O}_K$.

Theorem 1.3. *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 $f(T)$ mod p be*

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

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

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

Then

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

This is due to Dedekind [2, Sect. 3], so we call it Dedekind's index theorem.

2. Examples

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

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

Case 1: $p = 2$.

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

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

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

Case 2: $p = 3$.

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

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

so $\overline{\pi}_1(T) \nmid \overline{F}(T)$ 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 $\mathrm{disc}(f(T)) = -2700 = -2^2 \cdot 3^3 \cdot 5^2$, the only possible prime factors of $[\mathcal{O}_K : \mathbf{Z}[\sqrt[3]{10}]]$ are 2, 3, and 5.

Case 1: $p = 2$.

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

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

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

Case 2: $p = 3$.

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

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

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

Case 3: $p = 5$.

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

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

so $\overline{\pi}_1(T) \nmid \overline{F}(T)$ 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 $\mathrm{disc}(f(T)) = -108 = -2^2 \cdot 3^3$. The only primes that might divide $[\mathcal{O}_K : \mathbf{Z}[\sqrt[3]{2}]]$ are 2 and 3.

Case 1: $p = 2$.

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

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

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

Case 2: $p = 3$.

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

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

so $F(T) \equiv -(T+2)^2 \bmod 3$. Thus $\overline{\pi}_1(T) \nmid \overline{F}(T)$ 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 $\mathrm{disc}(f(T)) = -52272 = -2^4 \cdot 3^3 \cdot 11^2$, the only possible prime factors of $[\mathcal{O}_K : \mathbf{Z}[\sqrt[3]{44}]]$ are 2, 3, and 11.

Case 1: $p = 2$.

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

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

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

Case 2: $p = 3$.

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

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

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

Case 3: $p = 11$.

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

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

so $\overline{\pi}_1(T) \nmid \overline{F}(T)$ 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 $\mathrm{disc}(f(T)) = -2012 = -2^2 \cdot 503$, the only prime that might divide $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$ is 2.

From $f(T) \equiv T^2(T+1) \bmod 2$, 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 $F(T) \equiv T(T+1) \bmod 2$. Since $\overline{\pi}_1(T) \mid \overline{F}(T)$ in $\mathbf{F}_2[T]$, $\boxed{2 \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]}$.

Example 2.6. Let $K = \mathbf{Q}(\alpha)$ where α is a root of $f(T) = T^3 + 2T + 22$. Since $\mathrm{disc}(f(T)) = -13100 = -2^2 \cdot 5^2 \cdot 131$, the only primes that might divide $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$ are 2 and 5.

Case 1: $p = 2$.

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

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

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

Case 2: $p = 5$.

From $f(T) \equiv (T+2)(T-1)^2 \bmod 5$, 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 $F(T) \equiv T - 1 \bmod 5$. Therefore $\overline{\pi}_2(T) \mid \overline{F}(T)$ in $\mathbf{F}_5[T]$, so $\boxed{5 \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]}$.

Example 2.7. Let $K = \mathbf{Q}(\alpha)$ where α is a root of $f(T) = T^4 + 2T^2 + 3T + 1$. Since $\mathrm{disc}(f(T)) = 117 = 3^2 \cdot 13$, the only prime that might divide $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$ is 3.

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

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

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

Example 2.8. Let $K = \mathbf{Q}(\alpha)$ and $f(T) = T^4 + T^2 + 4$. Since $\mathrm{disc}(f(T)) = 14400 = 2^6 \cdot 3^2 \cdot 5^2$, the only possible prime factors of $[\mathcal{O}_K : \mathbf{Z}[\sqrt[4]{5}]]$ are 2, 3, and 5.

Case 1: $p = 2$.

From $f(T) \equiv T^2(T+1)^2 \bmod 2$, 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 $F(T) \equiv T^3 \bmod 2$. Therefore $\overline{\pi}_1(T) \mid \overline{F}(T)$ in $\mathbf{F}_2[T]$, so $\boxed{2 \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]}$.

Case 1: $p = 3$.

From $f(T) \equiv (T+1)^2(T+2)^2 \bmod 3$, 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 $F(T) \equiv T(T^2 + 2T + 2) \bmod 3$. In $\mathbf{F}_3[T]$, $\overline{F}(T)$ is not divisible by $\overline{\pi}_1(T)$ or $\overline{\pi}_2(T)$, so $3 \nmid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$.

Case 3: $p = 5$.

From $f(T) \equiv (T^2 - 2)^2 \bmod 5$, 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 $\mathbf{F}_5[T]$ is not divisible by $\overline{\pi}_1(T)$ or $\overline{\pi}_2(T)$. Therefore $5 \nmid [\mathcal{O}_K : \mathbf{Z}[\sqrt[4]{5}]]$.

Example 2.9. Suppose $f(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_1T + a_0$ in $\mathbf{Z}[T]$ where $p \mid a_j$ for all j. Then $f(T) \equiv T^n \bmod p$. Then

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

so $p \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$ 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 $\mathbf{Z}$. Therefore $p \nmid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$ if and only if $p^2 \nmid a_0$, which is equivalent to $f(T)$ being Eisenstein at p.

For instance, if $f(T) = T^3 + 2T + 4$ (it is irreducible over $\mathbf{Q}$ since it is irreducible mod 3), then $\boxed{2 \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]}$ where $f(\alpha) = 0$.

Example 2.10. Suppose $f(T) \bmod p$ is separable. Then every e_j is 1 in Theorem 1.3, so $p \nmid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$. That also follows from the fact that $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$ divides $\operatorname{disc}(f)$ and $\operatorname{disc}(f) \not\equiv 0 \bmod p$ by separability mod p.

3. Proof of Dedekind's index theorem

Now we'll prove Dedekind's index theorem, following Dedekind's own argument.

Proof. ($\Longleftarrow$) 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 $p \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$, $\mathfrak{p}_j \mid (F(\alpha))$. 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

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

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

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 $\mathfrak{p}_j \nmid (F(\alpha))$.

($\Longrightarrow$) 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

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

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

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

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 from 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 $T = \alpha$,

$$A(\alpha)B(\alpha) = -pF(\alpha). \tag{3.3}$$

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:

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

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

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

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 $a_0, \ldots, a_{d-1}$. Multiply through by p^d:

$$A(\alpha)^d + pa_{d-1}A(\alpha)^{d-1} + \cdots + p^{d-1}a_1A(\alpha) + p^d a_0 = 0. \tag{3.4}$$

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

$$A(T)^d + pa_{d-1}A(T)^{d-1} + \cdots + p^{d-1}a_1A(T) + p^d a_0 = f(T)h(T)$$

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 $\overline{\pi}(T)$, we get $\overline{\pi}(T) \mid \overline{F}(T)$. □

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 through the $p^n - 1$ nonzero cosets of $(1/p)\mathbf{Z}[\alpha]/\mathbf{Z}[\alpha]$ until we find an algebraic integer. But 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 1.3, 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 $h(\alpha) \in \mathbf{Z}[\alpha]$ 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 $q(\alpha)/p \in .\mathcal{O}_K - \mathbf{Z}[\alpha]$.*[1]

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 $\deg \pi \leq (\deg f)/2$ since $\overline{\pi}(T)^2 \mid \overline{f}(T)$.

Let's put Theorem 4.1 to work before proving it, to appreciate what it does.

Example 4.2. In Example 2.1, where $K = \mathbf{Q}(\sqrt[3]{12})$ and $f(T) = T^3 - 12$, $2 \mid [\mathcal{O}_K : \mathbf{Z}[\sqrt[3]{12}]]$ with $\pi(T) = T$, $f(T) \equiv \pi(T)T^2 \bmod 2$, so we can use $h(T) = T^2$. Therefore $\sqrt[3]{12}^2/2 \in \mathcal{O}_K - \mathbf{Z}[\sqrt[3]{12}]$. Note $\sqrt[3]{12}^2/2 = \sqrt[3]{18}$.

Example 4.3. In Example 2.2, where $K = \mathbf{Q}(\sqrt[3]{10})$ and $f(T) = T^3 - 10$, $3 \mid [\mathcal{O}_K : \mathbf{Z}[\sqrt[3]{10}]]$ with $\pi(T) = T - 1$, $f(T) \equiv \pi(T)(T-1)^2 \bmod 3$, so $h(T)$ be be a monic lift of $(T-1)^2 \equiv T^2 + T + 1 \bmod 3$. Use $h(T) = T^2 + T + 1$, so $(\sqrt[3]{10}^2 + \sqrt[3]{10} + 1)/3 \in \mathcal{O}_K - \mathbf{Z}[\sqrt[3]{10}]$.

Example 4.4. In Example 2.4, where $K = \mathbf{Q}(\sqrt[3]{44})$ and $f(T) = T^3 - 44$, 2 and 3 both divide $[\mathcal{O}_K : \mathbf{Z}[\sqrt[3]{44}]]$.

For $p = 2$, $\pi(T) = T$ and $f(T) \equiv \pi(T)T^2 \bmod 2$, so we can use $h(T) = T^2$: $\sqrt[3]{44}^2/2 \in \mathcal{O}_K - \mathbf{Z}[\sqrt[3]{44}]$.

[1] This comes from Theorem 8.2 of https://www.math.leidenuniv.nl/~psh/ANTproc/08psh.pdf.

For $p = 3$, $\pi(T) = T + 1$ and $f(T) \equiv \pi(T)(T+1)^2 \bmod 3$, so $h(T)$ can be a monic lift of $(T+1)^2 \equiv T^2+2T+1 \bmod 3$. Using $h(T) = T^2-T+1$, $(\sqrt[3]{44}^2 - \sqrt[3]{44}+1)/3 \in \mathcal{O}_K - \mathbf{Z}[\sqrt[3]{44}]$.

Example 4.5. In Example 2.5, $K = \mathbf{Q}(\alpha)$ where α is a root of $f(T) = T^3 - T^2 - 2T - 8$ and $2 \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$. Here $\pi(T) = T$ and $f(T) \equiv \pi(T)(T^2+T) \bmod 2$, so use $h(T) = T^2+T$: $(\alpha^2 + \alpha)/2 \in \mathcal{O}_K - \mathbf{Z}[\alpha]$.

Example 4.6. in Example 2.6, $K = \mathbf{Q}(\alpha)$ where α is a root of $f(T) = T^3 + 2T + 22$ and $5 \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$. Here $\pi(T) = T - 1$ and $f(T) \equiv \pi(T)(T^2 + T + 3) \bmod 5$, so use $h(T) = T^2 + T + 3$: $(\alpha^2 + \alpha + 3)/5 \in \mathcal{O}_K - \mathbf{Z}[\alpha]$.

Example 4.7. In Example 2.8, $K = \mathbf{Q}(\alpha)$ where α is a root of $f(T) = T^4 + T^2 + 4$ and $2 \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$. Here $\pi(T)$ is T and $f(T) \equiv \pi(T)(T^3 + T) \bmod 2$, so use $h(T) = T^3 + T$: $(\alpha^3 + \alpha)/2 \in \mathcal{O}_K - \mathbf{Z}[\alpha]$. (In fact, $(\alpha^3 + \alpha)/2$ is another root of $f(T)$.)

Example 4.8. In Example 2.9, , $K = \mathbf{Q}(\alpha)$ where α is a root of $f(T) = T^3 + 2T + 4$ and $2 \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$. We have $f(T) \equiv T^3 \bmod 2$ and

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

so $F(T) \equiv T \bmod 2$. Take $\pi(T) = T$, so $\overline{\pi}(T)^2 \mid \overline{f}(T)$ and $\overline{\pi}(T) \mid \overline{F}(T)$ in $\mathbf{F}_2[T]$. Since $f(T) \equiv \pi(T)T^2 \bmod 2$, use $h(T) = T^2$: $\alpha^2/2 \in \mathcal{O}_K - \mathbf{Z}[\alpha]$.

Here are two cases covering Examples 4.2, 4.4 (for $p = 2$), and 4.8, with $h(T) = T^{n-1}$.

- If $f(T) = T^n - p^2 m$ 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.

Proof. The second method is a consequence of the first method 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 $h(T) := \prod_{i\neq j}\pi_i(T)^{e_i}\pi_j(T)^{e_j-1}$. 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 $\overline{f}(T)$ 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

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

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 $\mathbf{F}_p[T]$, $\overline{\pi}_i(T)$ and $\overline{\pi}_j(T)$ are distinct monic irreducibles, so they are relatively prime: $\overline{\pi}_i(T)u(T) + \overline{\pi}_j(T)v(T) = 1$, 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 $(\pi_i(\alpha))$, $\pi_j(\alpha)V(\alpha) \equiv 1 \bmod \mathfrak{p}$, 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 $(\pi_1(\alpha)), \ldots, (\pi_g(\alpha)))$, so the multiplicity of $\mathfrak{p}$ in the first product of (4.1) is e_jb, while its multiplicity in the third product of (4.1) is $a + c$. Therefore

$$e_jb = a + c.$$

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): $e_jb - b \geq a$. 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 $e_j \geq 2$, $a + c = e_jb \geq 2b$, so $c - b \geq b - a \geq 0$, and thus $c \geq b$.

Case (ii): $b \leq a$. Since $\overline{\pi}_j(T) \mid \overline{F}(T)$ in $\mathbf{F}_p[T]$, $F(T) = \pi_j(T)H(T) + pK(T)$ for some $H(T)$ and $K(T)$ in $\mathbf{Z}[T]$. Therefore $F(\alpha) = \pi_j(\alpha)H(\alpha) + pK(\alpha)$ 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 $\pi_j(\alpha)H(\alpha) + pK(\alpha) \equiv 0 \bmod \mathfrak{p}^b$. Thus $\mathfrak{p}^b \mid (F(\alpha))$, which implies $b \leq c$.

This completes the proof. □

Remark 4.9. In the proof of Theorem 4.1, we did not need Dedekind's index theorem. The proof starts with some $\overline{\pi}_j(T)$ 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 ($\Longleftarrow$) in Dedekind's index theorem. Dedekind gave both proofs of ($\Longleftarrow$) that are worked out 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 4.10. 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 4.11. 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 1.3 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 1.3 is a preliminary step in the following algorithm that computes $\mathcal{O}_K$. It 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 $[\mathcal{O}_K : \mathbf{Z}[\alpha]]^2 \mid \mathrm{disc}(f)$, factor $\mathrm{disc}(f)$ to assemble a list of primes p such that $p^2 \mid \mathrm{disc}(f)$. 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 $I_p = \{x \in \mathcal{O} : x^m \equiv 0 \bmod p\mathcal{O} \text{ for some } m \geq 1\}$. 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 [1, 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 ower 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 [1, 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 4.10), 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 $p \in S$.

References

[1] H. Cohen, A Course in Computational Algebraic Number Theory, Springer-Verlag, 1993.

[2] R. Dedekind, "Ueber 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. Online at https://eudml.org/doc/135827.