FACTORING AFTER DEDEKIND

KEITH CONRAD

Let K be a number field and p be a prime number. When we factor $(p) = p\mathcal{O}_K$ into prime ideals, say

$$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g},$$

we refer to the data of the e_i's, the exponents f_i in the norms $\mathrm{N}\mathfrak{p}_i = p^{f_i}$, and g (the number of $\mathfrak{p}_i$'s), as the "shape" of the factorization of (p). (What we are leaving out of this is explicit information about generators for the ideals $\mathfrak{p}_i$.) Similarly, if a monic polynomial in $\mathbf{F}_p[T]$ factors into monic irreducibles as

$$\pi_1(T)^{e_1} \cdots \pi_g(T)^{e_g},$$

we refer to the exponents e_i, the degrees $\deg \pi_i$, and g as the "shape" of the factorization of the polynomial in $\mathbf{F}_p[T]$. (This leaves out knowledge of the π_i's themselves as polynomials.) There is a lovely theorem of Dedekind, building on earlier work of Kummer, which describes a polynomial in $\mathbf{Z}[T]$ whose factorization in $\mathbf{F}_p[T]$ for all but finitely many primes p determines the shape of the factorization of $p\mathcal{O}_K$. In other words, factoring (p) into prime ideals for all but finitely many p can be done by factoring a polynomial over a finite field instead.

Theorem 1 (Dedekind)**.** *Let K be a number field and $\alpha \in \mathcal{O}_K$ such that $K = \mathbf{Q}(\alpha)$. Let $f(T)$ be the minimal polynomial of α in $\mathbf{Z}[T]$. For any prime p not dividing $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$, write*

$$f(T) \equiv \pi_1(T)^{e_1} \cdots \pi_g(T)^{e_g} \bmod p$$

where the $\pi_i(T)$'s are distinct monic irreducibles in $\mathbf{F}_p[T]$. Then $(p) = p\mathcal{O}_K$ factors into prime ideals as

$$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$$

where there is a bijection between the $\mathfrak{p}_i$'s and $\pi_i(T)$'s such that $\mathrm{N}\mathfrak{p}_i = p^{\deg \pi_i}$. In particular, this applies for all p if $\mathcal{O}_K = \mathbf{Z}[\alpha]$.

Before proving Theorem 1, let's look at two examples.

Example 2. Let $K = \mathbf{Q}(\sqrt{d})$ with d a squarefree integer. Then $\mathcal{O}_K = \mathbf{Z}[\omega]$ where $\omega = \sqrt{d}$ if $d \equiv 2, 3 \bmod 4$ and $\omega = (1+\sqrt{d})/2$ if $d \equiv 1 \bmod 4$. In the first case, ω is a root of $T^2 - d$, so the way a prime p factors in $\mathcal{O}_K$ is reflected by how $T^2 - d$ factors in $\mathbf{F}_p[T]$. In the second case, ω is a root of $T^2 - T + (1-d)/4$, so the way this polynomial factors modulo p tells us how p factors in $\mathcal{O}_K$.

For instance, Table 1 shows how $T^2 - 10$ factors modulo the first few primes and then how the first few primes factor into prime ideals in $\mathbf{Z}[\sqrt{10}]$. Table 2 shows corresponding information for the ring of integers $\mathbf{Z}[(1+\sqrt{5})/2]$ of $\mathbf{Q}(\sqrt{5})$ using the polynomial $T^2 - T - 1$, which has $(1+\sqrt{5})/2$ as a root. (**Warning**: since the ring of integers is not $\mathbf{Z}[\sqrt{5}]$, we can't tell how all prime numbers factor in $\mathbf{Q}(\sqrt{5})$ by seeing how $T^2 - 5$ factors. For example, (2) is prime in $\mathbf{Z}[(1+\sqrt{5})/2]$ because $T^2 - T - 1 \bmod 2$ is irreducible; if you look instead at how $T^2 - 5 \bmod 2$ factors, you might be misled into thinking $(2) = \mathfrak{p}^2$, but that is false.)

p	$T^2 - 10 \bmod p$	(p)
2	T^2	$\mathfrak{p}_2^2$
3	$(T-1)(T+1)$	$\mathfrak{p}_3\mathfrak{p}_3'$
5	T^2	$\mathfrak{p}_5^2$
7	$T^2 - 10$	(7)
11	$T^2 - 10$	(11)
13	$(T-6)(T-7)$	$\mathfrak{p}_{13}\mathfrak{p}_{13}'$

TABLE 1. Factoring in $\mathbf{Q}(\sqrt{10})$

p	$T^2 - T - 1 \bmod p$	(p)
2	$T^2 + T + 1$	(2)
3	$T^2 - T - 1$	(3)
5	$(T+2)^2$	$\mathfrak{p}_5^2$
7	$T^2 - T - 1$	(7)
11	$(T-4)(T-8)$	$\mathfrak{p}_{11}\mathfrak{p}_{11}'$
13	$T^2 - T - 1$	(13)

TABLE 2. Factoring in $\mathbf{Q}(\sqrt{5})$

Regardless of the value of $d \bmod 4$, $\mathbf{Z}[\sqrt{d}]$ is a subring of $\mathcal{O}_K$ with index 1 or 2. What this means, by Theorem 1, is that in all cases we can determine how any *odd* prime p factors in $\mathcal{O}_K$ by factoring $T^2 - d \bmod p$, even if $\mathcal{O}_K \neq \mathbf{Z}[\sqrt{d}]$. We look at $\mathbf{Q}(\sqrt{5})$ again in this light in Table 3. The prime 2 can't be factored this way ($T^2 - 5$ is reducible mod 2, but 2 stays prime in the integers of $\mathbf{Q}(\sqrt{5})$), and Theorem 1 doesn't apply to the prime 2 and polynomial $T^2 - 5$ anyway since $2 \mid [\mathcal{O}_K : \mathbf{Z}[\sqrt{5}]]$. For the remaining primes in Table 3, the shapes of the factorizations in Tables 2 and 3 match up prime by prime.

p	$T^2 - 5 \bmod p$	(p)
2	$(T-1)^2$	(2)
3	$T^2 - 5$	(3)
5	T^2	$\mathfrak{p}_5^2$
7	$T^2 - 5$	(7)
11	$(T-4)(T-7)$	$\mathfrak{p}_{11}\mathfrak{p}_{11}'$
13	$T^2 - 5$	(13)

TABLE 3. Factoring in $\mathbf{Q}(\sqrt{5})$

Example 3. Let $K = \mathbf{Q}(\sqrt[4]{2})$. Without knowing $\mathcal{O}_K$ explicitly, certainly $\mathbf{Z}[\sqrt[4]{2}] \subset \mathcal{O}_K$. Also, $\operatorname{disc}(\mathbf{Z}[\sqrt[4]{2}]) = -2048 = -2^{11}$ and $\operatorname{disc}(\mathbf{Z}[\sqrt[4]{2}]) = [\mathcal{O}_K : \mathbf{Z}[\sqrt[4]{2}]]^2 \operatorname{disc}(\mathcal{O}_K)$, so any prime $p \neq 2$ does not divide the index $[\mathcal{O}_K : \mathbf{Z}[\sqrt[4]{2}]]$. Hence the way $T^4 - 2$ factors modulo p is also the way $(p) = p\mathcal{O}_K$ factors in $\mathcal{O}_K$ for all $p \neq 2$. Some sample calculations are in Table 4.

Now that the reader has sufficient motivation to care about Theorem 1, let's prove it.

p	$T^4 - 2 \bmod p$	(p)
3	$(T^2+T+2)(T^2+2T+2)$	$\mathfrak{p}_9\mathfrak{p}_9'$
5	T^4-2	(5)
7	$(T-2)(T-5)(T^2+4)$	$\mathfrak{p}_7\mathfrak{p}_7'\mathfrak{p}_{49}$
11	$(T^2+4T+8)(T^2+7T+8)$	$\mathfrak{p}_{121}\mathfrak{p}_{121}'$
73	$(T-18)(T-25)(T-48)(T-55)$	$\mathfrak{p}_{73}\mathfrak{p}_{73}'\mathfrak{p}_{73}''\mathfrak{p}_{73}'''$

TABLE 4. Factoring in $\mathbf{Q}(\sqrt[4]{2})$

Proof. The main idea is that when $p \nmid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$ we will show the rings $\mathcal{O}_K/(p)$ and $\mathbf{F}_p[T]/(\overline{f}(T))$ are isomorphic. Then we will determine the shapes of the factorizations of (p) and $f(T) \bmod p$ in the same way from the structure of these isomorphic rings.

Let $m = [\mathcal{O}_K : \mathbf{Z}[\alpha]]$, so

$$m\mathcal{O}_K \subset \mathbf{Z}[\alpha] \subset \mathcal{O}_K. \tag{1}$$

For any prime p, there is a natural ring homomorphism $\mathbf{Z}[\alpha]/(p) \to \mathcal{O}_K/(p)$. When p does not divide m, (1) implies the map $\mathbf{Z}[\alpha]/(p) \to \mathcal{O}_K/(p)$ is onto: let $mm' \equiv 1 \bmod p\mathbf{Z}$, so for any $x \in \mathcal{O}_K$ we have $x \equiv m' \cdot mx \bmod p\mathcal{O}_K$ and $mx \in \mathbf{Z}[\alpha]$, so $m' \cdot mx \in \mathbf{Z}[\alpha]$ too. Both $\mathbf{Z}[\alpha]$ and $\mathcal{O}_K$ are free rank n $\mathbf{Z}$-modules, so $\mathbf{Z}[\alpha]/(p)$ and $\mathcal{O}_K/(p)$ both have size p^n, hence the surjective ring homomorphism between them is an isomorphism:

$$\mathbf{Z}[\alpha]/(p) \cong \mathcal{O}_K/(p).$$

Now we turn $\mathbf{Z}[\alpha]/(p)$ into a quotient ring of $\mathbf{F}_p[T]$. We have $\mathbf{Z}[T]/(f(T)) \cong \mathbf{Z}[\alpha]$ as rings by $h(T) \bmod f(T) \mapsto h(\alpha)$, reducing both sides of the isomorphism modulo p implies

$$\mathbf{Z}[\alpha]/(p) \cong \mathbf{Z}[T]/(f(T), p)^{1} \cong (\mathbf{Z}/p\mathbf{Z})[T]/(\overline{f}(T)) = \mathbf{F}_p[T]/(\overline{f}(T)).$$

Thus $\mathbf{F}_p[T]/(\overline{f}(T))$ and $\mathcal{O}_K/(p)$ are isomorphic rings, since both are isomorphic to $\mathbf{Z}[\alpha]/(p)$.

Let $\overline{f}(T) = \pi_1(T)^{e_1} \cdots \pi_g(T)^{e_g}$ in $\mathbf{F}_p[T]$ where the $\pi_i(T)$'s are distinct monic irreducibles and $a_i \geq 1$. How can we determine g, e_i, and $\deg \pi_i$ for all i from the structure of the ring $\mathbf{F}_p[T]/(\overline{f}(T))$? The number g is the number of maximal ideals in $\mathbf{F}_p[T]/(\overline{f}(T))$. Indeed,the maximal ideals of $\mathbf{F}_p[T]/(\overline{f}(T))$ are the ideals of the form $M/(\overline{f}(T))$ where M is a maximal ideal of $\mathbf{F}_p[T]$ containing $(\overline{f}(T))$. Any maximal ideal in $\mathbf{F}_p[T]/(\overline{f}(T))$ has the form (π) for one monic irreducible π in $\mathbf{F}_p[T]$, and (π) contains $(\overline{f}(T))$ precisely when $\pi \mid \overline{f}(T)$ in $\mathbf{F}_p[T]$.

For each maximal ideal M of $\mathbf{F}_p[T]/(\overline{f}(T))$, writing it as $(\pi_i)/(\overline{f}(T))$, we have

$$(\mathbf{F}_p[T]/(\overline{f}(T)))/M \cong \mathbf{F}_p[T]/(\pi_i(T)),$$

whose size is $p^{\deg \pi_i}$. So counting the size of the residue ring modulo M tells us the degree of the irreducible polynomial associated to M. Finally, we show the multiplicity e_i of $\pi_i(T)$ in the factorization of $\overline{f}(T)$ is the number of different positive integral powers of M. Under the reduction map $\mathbf{F}_p[T] \to \mathbf{F}_p[T]/(\overline{f}(T))$, the ideal (π_i) maps onto the ideal $M = (\pi_i)/(\overline{f}(T))$, so we can compute powers of M by computing powers of (π_i) in $\mathbf{F}_p[T]$ first and then reducing. For $k \geq 1$, the kth power of (π_i) in $\mathbf{F}_p[T]$ is $(\pi_i)^k = (\pi_i^k)$, whose

[1]The ideal $(f(T), p)$ need not be prime in $\mathbf{Z}[T]$, *e.g.*, $(T^2+1, 5)$ is not prime in $\mathbf{Z}[T]$ since $T^2+1 \bmod 5$ is reducible: $T^2+1 \equiv (T-2)(T-3) \bmod 5$ and $(T-2)(T-3) \in (T^2+1, 5)$ with $T-2, T-3 \notin (T^2+1, 5)$.

image in $\mathbf{F}_p[T]/(\overline{f}(T))$ is $((\pi_i^k) + (\overline{f}(T)))/(\overline{f}(T))$. This image is also M^k. Since

$$(\pi_i^k) + (\overline{f}(T)) = (\gcd(\pi_i^k, \overline{f}(T))) = \begin{cases} (\pi_i^k), & \text{if } 1 \leq k < e_i, \\ (\pi_i^{e_i}), & \text{if } k \geq e_i, \end{cases}$$

we have

$$M^k = \begin{cases} (\pi_i^k)/(\overline{f}(T)), & \text{if } 1 \leq k < e_i, \\ (\pi_i^{e_i})/(\overline{f}(T)), & \text{if } k \geq e_i. \end{cases}$$

Thus the positive integral powers of M in $\mathbf{F}_p[T]/(\overline{f}(T))$ are the ideals $(\pi_i^k)/(\overline{f}(T))$ for $1 \leq k \leq e_i$. The ring modulo such an ideal is isomorphic to $\mathbf{F}_p[T]/(\pi_i^k)$, which has different size for different k, so these powers of M are different from each other.

To summarize, the monic irreducible factors of $\overline{f}(T)$ in $\mathbf{F}_p[T]$ are in bijection with the maximal ideals of the ring $\mathbf{F}_p[T]/(\overline{f}(T))$. For each monic irreducible factor, its degree as a polynomial and its multiplicity in the factorization of $\overline{f}(T)$ can be read off from counting the size of the residue ring modulo the corresponding maximal ideal in $\mathbf{F}_p[T]$ and the number of different positive powers of this maximal ideal.

Now we turn to $\mathcal{O}_K/(p)$. Factor $(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$ with distinct primes $\mathfrak{p}_i$ and $e_i \geq 1$. (We use the same notation g, e_i as in the polynomial factorization because we'll see these are the same parameters, but we will not be using the polynomial information in our discussion, so this duplication of notation should not lead to any confusion.) Let $\mathrm{N}\mathfrak{p}_i = p^{f_i}$. Every maximal ideal of $\mathcal{O}_K/(p)$ has the form $\mathfrak{p}/(p)$ where $\mathfrak{p}$ is a maximal ideal of $\mathcal{O}_K$ containing (p), and containing (p) is the same as dividing (p), so $\mathfrak{p}$ is one of $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$. This shows the maximal ideals of $\mathcal{O}_K/(p)$ are in bijection with the prime factors of (p): they all look like $\mathfrak{p}_i/(p)$ for some $i = 1, 2, \ldots, g$. For each maximal ideal $\mathfrak{p}_i/(p)$ in $\mathcal{O}_K/(p)$, its residue ring $(\mathcal{O}_K/(p))/(\mathfrak{p}_i/(p)) \cong \mathcal{O}_K/\mathfrak{p}_i$ has size $\mathrm{N}\mathfrak{p}_i = p^{f_i}$. What are the powers of $\mathfrak{p}_i/(p)$ in $\mathcal{O}_K/(p)$? They are images of powers of $\mathfrak{p}_i$ in $\mathcal{O}_K$ under the reduction map $\mathcal{O}_K \to \mathcal{O}_K/(p)$. The image of $\mathfrak{p}_i^k$ under this reduction is $(\mathfrak{p}_i^k + (p))/(p)$ and

$$\mathfrak{p}_i^k + (p) = \gcd(\mathfrak{p}_i^k, (p)) = \begin{cases} \mathfrak{p}_i^k, & \text{if } 1 \leq k < e_i, \\ \mathfrak{p}_i^{e_i}, & \text{if } k \geq e_i, \end{cases}$$

so the positive integral powers of $\mathfrak{p}_i/(p)$ are the ideals $\mathfrak{p}_i^k/(p)$ for $1 \leq k \leq e_i$. Such ideals are different for different k (for instance, the quotients of $\mathcal{O}_K/(p)$ by these ideals are rings of different size), so e_i is the number of different positive integral powers of $\mathfrak{p}_i/(p)$ in $\mathcal{O}_K/(p)$. We have read off the shape of the factorization of (p) from the ring structure of $\mathcal{O}_K/(p)$ in the same way that we did for the shape of the factorization of $\overline{f}(T)$ from the structure of $\mathbf{F}_p[T]/(\overline{f}(T))$: for each maximal ideal in $\mathcal{O}_K/(p)$, count the size of its residue ring as a power of p and also count the number of different positive powers of the maximal ideal. Such counting over all maximal ideals returns the same answers for isomorphic finite rings, so the isomorphism between $\mathbf{F}_p[T]/(\overline{f}(T))$ and $\mathcal{O}_K/(p)$ shows the factorizations of $\overline{f}(T)$ and (p) have the same shape. □

Corollary 4. *Let $K = \mathbf{Q}(\alpha)$ and $\alpha \in \mathcal{O}_K$ have minimal polynomial $f(T)$ in $\mathbf{Z}[T]$. For any prime p not dividing $\mathrm{disc}(\mathbf{Z}[\alpha])$, the shapes of the factorizations of (p) in $\mathcal{O}_K$ and $\overline{f}(T)$ in $\mathbf{F}_p[T]$ agree. In particular, if $f(T) \bmod p$ is separable then the shapes of the factorizations of (p) and $\overline{f}(T)$ agree.*

Proof. Since $\mathrm{disc}(\mathbf{Z}[\alpha]) = [\mathcal{O}_K : \mathbf{Z}[\alpha]]^2 \mathrm{disc}(\mathcal{O}_K)$, if $p \nmid \mathrm{disc}(\mathbf{Z}[\alpha])$ then $p \nmid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$, so Theorem 1 applies to p. The ring discriminant $\mathrm{disc}(\mathbf{Z}[\alpha])$ and polynomial discriminant

$\mathrm{disc}(f)$ are equal, and if $f(T)$ mod p is separable then $\mathrm{disc}(f) \not\equiv 0 \bmod p$ (and conversely!), so we can apply Theorem 1 to all primes p such that $f(T)$ mod p is separable. □

In practice, Corollary 4 is the way one applies Theorem 1 to factor most primes, because the hypotheses in Corollary 4 are computable in terms of α alone; no knowledge of the full ring $\mathcal{O}_K$ is required and all but finitely many primes don't divide $\mathrm{disc}(\mathbf{Z}[\alpha])$. If $p \mid \mathrm{disc}(\mathbf{Z}[\alpha])$, how can we determine the factorization of $p\mathcal{O}_K$? Well, try to change α: look for a $\beta \in \mathcal{O}_K$ such that $K = \mathbf{Q}(\beta)$ and p does not divide $\mathrm{disc}(\mathbf{Z}[\beta])$ instead. If we can do this, then we can factor (p) using the minimal polynomial of β in place of that of α.

Example 5. Let $K = \mathbf{Q}(\alpha)$ where α is a root of $T^3+2T+22$ (Eisenstein at 2, so irreducible). Since $\mathrm{disc}(\mathbf{Z}[\alpha]) = -2^2 \cdot 5^2 \cdot 131$, any prime $p \neq 2, 5$, or 131 can be factored in $\mathcal{O}_K$ by factoring $T^3+2T+22$ in $\mathbf{F}_p[T]$. The number $\beta = \frac{1}{5}(\alpha^2+\alpha-2)$ generates K (since $\beta \in K$, $[K : \mathbf{Q}] = 3$ is prime, and $\beta \notin \mathbf{Q}$),[2] β is a root of $T^3 + 2T^2 + 4T - 2$, and $\mathrm{disc}(\mathbf{Z}[\beta]) = -2^2 \cdot 131$. This discriminant is not divisible by 5, so the way 5 factors in $\mathcal{O}_K$ is the way $T^3 + 2T^2 + 4T - 2$ factors in $\mathbf{F}_5[T]$. The factorization is $(T-1)(T-3)(T-4)$, so $5\mathcal{O}_K = \mathfrak{p}_5\mathfrak{p}_5'\mathfrak{p}_5''$ where each prime ideal has norm 5.

Observe that, using the polynomial for α, we have $T^3+2T+22 \equiv (T-1)^2(T-3) \bmod 5$, which would predict the wrong factorization of 5 in $\mathcal{O}_K$.

Example 6. Let $K = \mathbf{Q}(\sqrt[3]{10})$, so $\mathbf{Z}[\sqrt[3]{10}] \subset \mathcal{O}_K$. Since $\mathrm{disc}(\mathbf{Z}[\sqrt[3]{10}]) = -2700 = -2^2 \cdot 3^3 \cdot 5^2$, any prime p other than 2, 3, or 5 can be factored in $\mathcal{O}_K$ by seeing how $T^3 - 10$ factors in $\mathbf{F}_p[T]$.

Let $\beta = \frac{1}{3} + \frac{1}{3}\sqrt[3]{10} + \frac{1}{3}\sqrt[3]{100}$. This is integral, being a root of $T^3 - T^2 - 3T - 3$. The discriminant of $\mathbf{Z}[\beta]$ is $-300 = -2^2 \cdot 3 \cdot 5^2$, which is still divisible by 2, 3, and 5. However, notice the exponent of 3 is just 1. Since $\mathrm{disc}(\mathbf{Z}[\beta]) = [\mathcal{O}_K : \mathbf{Z}[\beta]]^2 \,\mathrm{disc}(\mathcal{O}_K)$, $[\mathcal{O}_K : \mathbf{Z}[\beta]]$ is *not* divisible by 3. Therefore Theorem 1, *rather than* Corollary 4, tells us that the way 3 factors in $\mathcal{O}_K$ is the way $T^3 - T^2 - 3T - 3$ factors modulo 3: the polynomial modulo 3 is $T^2(T-1)$, so $3\mathcal{O}_K = \mathfrak{p}_3^2\mathfrak{p}_3'$.

We knew we weren't justified in factoring 3 in $\mathcal{O}_K$ by factoring $T^3 - 10$ mod 3, and now we see for sure that the two factorizations don't match: $T^3 - 10 \equiv (T-1)^3 \bmod 3$.

Because $\mathrm{disc}(\mathcal{O}_K)$ is a factor of $\mathrm{disc}(\mathbf{Z}[\alpha])$ for any $\alpha \in \mathcal{O}_K$ which generates K over $\mathbf{Q}$, no prime factor of $\mathrm{disc}(\mathcal{O}_K)$ will ever be factored using Corollary 4. Since Theorem 1 is about $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$ rather than its multiple $\mathrm{disc}(\mathbf{Z}[\alpha])$, if we know $\mathcal{O}_K$ well enough to compute the indices $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$ for varying α, we may hope that, for any prime number p, there is an α such that $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$ is not divisible by p. Then Theorem 1 will tell us the shape of the factorization of (p) from the shape of the factorization of $f(T)$ mod p, where $f(T)$ is the minimal polynomial of α over $\mathbf{Q}$. Alas, there are some number fields K such that a certain prime number divides the index $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$ for all α in $\mathcal{O}_K$. Then it is not possible to determine the factorization of that prime number by the method of Theorem 1.

Example 7. Let $K = \mathbf{Q}(\gamma)$ where $\gamma^3 - \gamma^2 - 2\gamma - 8 = 0$. We will call this Dedekind's field. Since $\mathrm{disc}(\mathbf{Z}[\gamma]) = -2^2 \cdot 503$, Corollary 4 tells us that any prime p other than 2 and 503 can be factored in $\mathcal{O}_K$ by factoring $T^3 - T^2 - 2T - 8$ mod p. Table 5 shows how this works.

It can be shown that $[\mathcal{O}_K : \mathbf{Z}[\gamma]] = 2$, so by Theorem 1 we can also get the factorization of 503 by factoring the same cubic:

$$T^3 - T^2 - 2T - 8 \equiv (T - 299)(T - 354)^2 \bmod 503,$$

[2]Since $K = \mathbf{Q}(\beta)$, there must be a formula for α in terms of β. Explicitly, $\alpha = -\beta^2 - \beta - 2$.

p	$T^3 - T^2 - 2T - 8 \bmod p$	(p)
3	$T^3 - T^2 - 2T - 8$	(3)
5	$(T-1)(T^2+3)$	$\mathfrak{p}_5\mathfrak{p}_{25}$
59	$(T-11)(T-20)(T-29)$	$\mathfrak{p}_{59}\mathfrak{p}'_{59}\mathfrak{p}''_{59}$

TABLE 5. Factoring in Dedekind's field

so $(503) = \mathfrak{p}\mathfrak{p}'$ where $\mathrm{N}\mathfrak{p} = 503$ and $\mathrm{N}\mathfrak{p}' = 503^2$. If we naively try to apply Theorem 1 to $p = 2$ in Dedekind's field using the same cubic we get an incorrect result: $T^3 - T^2 - 2T - 8 \equiv T^2(T+1) \bmod 2$, but (2) is not of the form $\mathfrak{p}_2^2\mathfrak{p}_2'$: it decomposes as $\mathfrak{p}_2\mathfrak{p}_2'\mathfrak{p}_2''$.

In fact, we can't use Theorem 1 to factor 2 in Dedekind's field because it can be shown that $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$ is even for every $\alpha \in \mathcal{O}_K$. Historically, K was the first known number field for which $\mathcal{O}_K$ does not have the form $\mathbf{Z}[\alpha]$ for some α. It was found by Dedekind [1, pp. 30–36], and even though he described K using a root of $f(X) = X^3 - X^2 - 2X - 8$, it often appears in the literature using a root of $-f(-X) = X^3 + X^2 - 2X + 8$, which makes it harder to remember the signs of the coefficients.

So far we have used the shape of a factorization of a polynomial over $\mathbf{F}_p$ to tell us the shape of the factorization of p in $\mathcal{O}_K$, but we have said nothing about how to find generators of the prime ideals dividing $p\mathcal{O}_K$. Generators can be written down using the irreducible factors of the polynomial modulo p.

Theorem 8. *In the notation of Theorem 1, when $\mathfrak{p}_i$ is the prime ideal corresponding to $\pi_i(T)$ we have the formula $\mathfrak{p}_i = (p, \Pi_i(\alpha))$ where $\Pi_i(T)$ is any polynomial in $\mathbf{Z}[T]$ that reduces mod p to $\pi_i(T) \bmod p$.*

Let's look at examples to understand how the formula for $\mathfrak{p}_i$ works before proving it.

Example 9. In $\mathbf{Z}[\sqrt{10}]$, $T^2 - 10 \equiv (T+1)(T-1) \bmod 3$, so the factorization of (3) in $\mathbf{Z}[\sqrt{10}]$ is $\mathfrak{p}_3\mathfrak{p}_3'$ where $\mathfrak{p}_3 = (3, \sqrt{10}+1)$ and $\mathfrak{p}_3' = (3, \sqrt{10}-1)$. Another factorization mod 3 is $T^2 - 10 \equiv (T+4)(T-7) \bmod 3$, so these prime ideals are also $(3, \sqrt{10}+4)$ and $(3, \sqrt{10}-7)$. It is easy to check the first of these ideals is $\mathfrak{p}_3$ and the second is $\mathfrak{p}_3'$.

By the way, these ideals are non-principal since they have norm 3 while no element of $\mathbf{Z}[\sqrt{10}]$ has absolute norm 3: if $x^2 - 10y^2 = \pm 3$ then $x^2 \equiv \pm 3 \bmod 5$, but neither 3 nor -3 is a square modulo 5.

To factor 5 in $\mathbf{Z}[\sqrt{10}]$, since $T^2 - 10 \equiv T^2 \bmod 5$ we have $(5) = (5, \sqrt{10})^2$. The prime $(5, \sqrt{10})$ is also non-principal since it has norm 5 and (exercise) no element of $\mathbf{Z}[\sqrt{10}]$ has norm ± 5.

Example 10. In $\mathbf{Z}[\sqrt[3]{2}]$, which is the ring of integers of $\mathbf{Q}(\sqrt[3]{2})$, let's factor 5. Since $T^3 - 2 \equiv (T-3)(T^2+3T+4) \bmod 5$ we have $(5) = \mathfrak{p}_5\mathfrak{p}_{25}$. Explicitly,

$$\mathfrak{p}_5 = (5, \sqrt[3]{2} - 2), \quad \mathfrak{p}_{25} = (5, \sqrt[3]{4} + 3\sqrt[3]{2} + 4).$$

These ideals are actually principal, because we can find elements with norm 5 and 25. The general formula for norms of elements is

$$\mathrm{N}_{\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}}(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = a^3 + 2b^3 + 4c^3 - 6abc,$$

so $\mathrm{N}_{\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}}(1+\sqrt[3]{4}) = 5$ and $\mathrm{N}_{\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}}(3+\sqrt[3]{2}+2\sqrt[3]{4}) = 25$. This means the ideal $(1+\sqrt[3]{4})$ is prime, and $\mathfrak{p}_5$ is the only ideal with norm 5, so $(1+\sqrt[3]{4}) = \mathfrak{p}_5$. Does $\mathfrak{p}_5$ divide $(3+\sqrt[3]{2}+2\sqrt[3]{4})$?

Since $\mathfrak{p}_5 = (5, \sqrt[3]{2}-2)$, we have $\sqrt[3]{2} \equiv 2 \bmod \mathfrak{p}_5$, so $3+\sqrt[3]{2}+2\sqrt[3]{4} \equiv 3+2+4 \equiv 9 \not\equiv 0 \bmod \mathfrak{p}_5$, so $\mathfrak{p}_5$ does not divide $(3+\sqrt[3]{2}+2\sqrt[3]{4})$. Therefore we must have $(3+\sqrt[3]{2}+2\sqrt[3]{4}) = \mathfrak{p}_{25}$.

Now let's prove Theorem 8.

Proof. Let's look closely at the isomorphism between $\mathbf{F}_p[T]/(\overline{f}(T))$ and $\mathcal{O}_K/(p)$ from the proof of Theorem 1 to see how maximal ideals in these two rings are identified with each other. When p does not divide $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$, we constructed the isomorphism using other rings as intermediaries:

$$\mathbf{F}_p[T]/(\overline{f}(T)) \cong \mathbf{Z}[T]/(p, f(T)) \cong \mathbf{Z}[\alpha]/(p) \cong \mathcal{O}_K/(p). \tag{2}$$

Working through these isomorphisms, a recipe for the composite isomorphism is this: pick a congruence class $\overline{h}(T) \bmod \overline{f}(T)$, lift it to $h(T) \in \mathbf{Z}[T]$, reduce modulo $(p, f(T))$ and then substitute in α for X. What we get at the end is $h(\alpha) \bmod (p) \in \mathcal{O}_K/(p)$.

To figure out what the ideals $\mathfrak{p}_i$ are, we can just trace through the isomorphisms to find the image in $\mathcal{O}_K/(p)$ of the maximal ideals of $\mathbf{F}_p[T]/(\overline{f}(T))$. The maximal ideals in $\mathbf{F}_p[T]/(\overline{f}(T))$ are those of the form $(\pi(T))/(\overline{f}(T))$ where $\pi(T)$ is a monic irreducible factor of $\overline{f}(T)$. Let $\Pi(T) \in \mathbf{Z}[T]$ be a lifting of $\pi(T)$ into $\mathbf{Z}[T]$. (We could choose the lifting so that $\deg \Pi = \deg \pi$, but this is not required.) Looking at equation (2), the ideal $(\pi(T))/(\overline{f}(T))$ in $\mathbf{F}_p[T]/(\overline{f}(T))$ is identified with the ideal $(p, \Pi(T))/(p, f(T))$ in $\mathbf{Z}[T]/(p, f(T))$, and this is identified with the ideal $(p, \Pi(\alpha))/(p)$ in $\mathcal{O}_K/(p)$. This is the reduction from $\mathcal{O}_K$ of the ideal $(p, \Pi(\alpha))$, which is necessarily maximal in $\mathcal{O}_K$ since $(p, \Pi(\alpha))/(p)$ is maximal in $\mathcal{O}_K$.

Therefore the prime ideals dividing (p) in $\mathcal{O}_K$ are $\mathfrak{p}_i = (p, \Pi_i(\alpha))$ as $\Pi_i(T)$ runs over lifts of the different monic irreducible factors $\pi_i(T)$ of $f(T) \bmod p$. If we choose our liftings $\Pi_i(T)$ to have the same degree as $\pi_i(T)$ for all i, which is possible, then $\mathrm{N}\mathfrak{p}_i = p^{\deg \Pi_i}$ for all i. □

References

[1] R. Dedekind, *Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Congruenzen*, Abh. Kgl. Ges. Wiss. Gottingen **23** (1878), 3–38. URL https://eudml.org/doc/135827.