Explicit Methods in Algebraic Number Theory

Amalia Pizarro Madariaga
Instituto de Matemáticas
Universidad de Valparaíso, Chile
amalia.pizarro@uv.cl

1 Lecture 2

1.1 Factorization in Ring of Integers

If K is a number field, we know that $\mathcal{O}_K$ is a Dedekind domain. Then, each ideal in $\mathcal{O}_K$ may be written as a product of prime ideals.
Problem: Find $\mathfrak{p}_i$ and e_i:

$$\begin{array}{ccc} K & \mathcal{O}_K & p\mathcal{O}_K = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\dots\mathfrak{p}_r^{e_r} \\ \Big| & \Big| & \Big| \\ \mathbb{Q} & \mathbb{Z} & p \end{array}$$

1.2 Factorization in Quadratic Fields

Let $K = \mathbb{Q}(\sqrt{d})$, with d squarefree and $\mathcal{O}_K = \mathbb{Z}[\alpha]$ with

$$\alpha = \begin{cases} \sqrt{d}, & \text{if } d \equiv 2,3 \pmod 4 \\ \frac{1+\sqrt{d}}{2}, & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

If f is the minimal polynomial of α over $\mathbb{Q}$, then

$$f(x) = \begin{cases} x^2 - d, & \text{if } d \equiv 2,3 \pmod 4 \\ x^2 - x + \frac{1+\sqrt{d}}{2}, & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

Remark 1. *The following isomorphism holds canonically:*

$$\mathcal{O}_K/p\mathcal{O}_K \cong (\mathbb{Z}[x]/(f(x)))/(p\mathcal{O}_K) \cong \mathbb{Z}[x]/(p, f(x)) \cong \mathbb{Z}_p[x]/(\overline{f}(x))$$

Let us see the possible factors of $\overline{f}(x)$ in $\mathbb{Z}_p[x]$:

- $\overline{f}(x)$ is irreducible.
  This implies $\mathbb{Z}_p[x]/(\overline{f}(x))$ is a field, then $\mathcal{O}_K/p\mathcal{O}_K$ is also a field and so $p\mathcal{O}_K$ is a prime ideal.

For the remaining cases, observe that:

$$\begin{tikzcd}
\mathcal{O}_K \arrow[r] \arrow[d] & \mathcal{O}_K/p\mathcal{O}_K \arrow[d] & \\
\mathcal{O}_K/(f(x)) \arrow[r] & \mathbb{Z}[x]7(p, f(x)) \arrow[r] & \mathbb{Z}_p[x]/(\overline{f}(x))
\end{tikzcd}$$

- $\overline{f}(x) = \overline{g}(x)\overline{h(x)}$, with $\overline{g}(x)$ and $\overline{h(x)}$ distinct, monic and linear.
  From Chinese remainder theorem

$$\mathbb{Z}_p[x]/(\overline{f}(x)) \cong \mathbb{Z}_p[x]/(\overline{g}(x)) \times \mathbb{Z}_p[x]/(\overline{h}(x)).$$

Restricting to each factor we see that the kernel of the map

$$\mathcal{O}_K \to \mathbb{Z}_p[x]/(\overline{g}(x)) \times \mathbb{Z}_p[x]/(\overline{h}(x)),$$

is in the first factor the ideal $(p, g(\alpha))$ and in the second factor $(p, h(\alpha))$. Then, the kernel is $(p, g(\alpha)) \cap (p, h(\alpha))$.

Remark 2. *The ideals $(p, g(\alpha))$ and $(p, h(\alpha))$ are prime and relatively primes (i.e their sum is the whole ring) and it holds that*

$$(p, g(\alpha) \cap (p, h(\alpha)) = (p, g(\alpha)) \cdot (p, h(\alpha)).$$

(Exercise)

But from the diagram, the kernel of the map is in fact $p\mathcal{O}_K$, so the factorization of this ideal is

$$p\mathcal{O}_K = (p, g(\alpha)) \cdot (p, h(\alpha)).$$

- $\overline{f}(x) = \overline{g}(x)^2$, with $\overline{g}(x)$ monic and irreducible.
  First, we assume that $p \neq 2$.

Remark 3. *If $d \equiv 2, 3$ (mod 4), then $\overline{f}(x) = x^2 - d$ is a square in $\mathbb{Z}_p[x]$ if and only if $p|d$.*

In fact,

$$x^2 - d \equiv (x+a)^2 \text{ (mod) } p \Leftrightarrow (d(2x + a + d) \equiv 0 \text{ (mod) } \Leftrightarrow p|d.$$

We take $\overline{g}(x) = x$. Then the kernel of the map

$$\mathcal{O}_K \to \mathbb{Z}_p[x]/(x^2)$$

is for one hand $(p, g(\alpha)) = (p, \alpha^2)$ and for the other hand is $p\mathcal{O}_K$. Then,

$$p\mathcal{O}_K = (p, \alpha^2) = (p, \alpha)^2.$$

It remains to see what happens when $p = 2$, but it will be left as an exercise.

We resume the previous results in the next proposition,

Proposition 1. *Let $K = \mathbb{Q}(\sqrt{d})$, with d squarefree and let $f(x)$ be the minimal polynomial of $\sqrt{d}$ over $\mathbb{Q}$. If p is a prime number, then the factorization in irreducible factors in $\mathbb{Z}_p[x]$*

$$\overline{f}(x) = \overline{g}_1(x)^{e_1}\overline{g}_2(x)^{e_2}, \ \ \textit{with } e_i = 1 \textit{ or } 2$$

implies

$$p\mathcal{O}_K = (p, g_1(\alpha))^{e_1}(p, g_2(\alpha))^{e_2}.$$

A more general result is the following:

Theorem 1.1. *Let $K = \mathbb{Q}(\theta)$ with θ an algebraic integer. Let us suppose that $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$ and let $g(x)$ be the minimal polynomial of θ. If*

$$f(x) \equiv g_1(x)^{e_1}g_2(x)^{e_2}\dots g_r(x)^{e_r} \ (mod \ \ p),$$

then

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\dots\mathfrak{p}_r^{e_r},$$

where $\mathfrak{p}_i = (p, g_i(\theta))$ are prime ideals, $N(\mathfrak{p}_i) = p^{f_i}$ and $f_i = deg(g_i)$.

Remark 4. *If $\mathcal{O}_K = \mathbb{Z}[\theta]]$, then the theorem holds for every prime. Also if $g(x)$ in Einsenstein in p.*

Definition 1. *Let p be a prime number and K a number field with $[K : \mathbb{Q}] = n$.*

- *p is totally ramified if $p\mathcal{O}_K = \mathfrak{p}^n$, for some prime $\mathfrak{p}$.*
- *p is inert if $p\mathcal{O}_K$ is prime.*
- *p splits completely if $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\dots\mathfrak{p}_n$.*

Corollary 1. *Let θ be an algebraic integer such that its minimal polynomial is Einsenstein in the prime p. If $K = \mathbb{Q}(\theta)$, then p is totally ramified in $\mathcal{O}_K$.*

Corollary 2. *If $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$, then p ramifies in $\mathcal{O}_K$ if and only of $p \nmid D_K$.*

Proof. If $g(x) = \prod_{i=n}^{n}(x - \theta_i)$ is the minimal polynomial of θ over $\mathbb{Q}$, then

$$D_K(1, \theta, \theta^2, \dots, \theta^{n-1}) = \prod_{i<j}(\theta_i - \theta_j)^2$$

and therefore, $\overline{g}(x)$ has multiple roots mod p if and only if $p|D_K(\theta) = [\mathcal{O}_K : \mathbb{Z}[\theta]]D_K$. □

1.3 Action of the Galois Group over primes

Theorem 1.2. *Let K be a Galois extension over $\mathbb{Q}$ and p a prime number. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the primes in K over p. Then Gal($K/\mathbb{Q}$) acts transitively in this set, i.e., for all i, j, there exists $\sigma \in$ Gal($K/\mathbb{Q}$) such that $\sigma(\mathfrak{p}_i) = \mathfrak{p}_j$.*

Proof. Note that $\sigma(\mathcal{O}_K) = \mathcal{O}_K$ and if $\mathfrak{p}$ is a prime over p, then $\sigma(\mathfrak{p})$ is also a prime ideal over p. Let $\mathfrak{p}_i$ and $\mathfrak{p}_j$ different primes over p. Suppose that $\sigma(\mathfrak{p}_i) \neq \mathfrak{p}_j$, for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Both ideals are maximal, so $\mathfrak{p}_j \subsetneq \mathfrak{p}_j$. Let $x \in \mathfrak{p}_j$ but $x \notin \sigma(\mathfrak{p}_i)$. Taking the norm

$$N_K(x) = \prod_{\sigma} \sigma(x) = x \cdot \prod_{\sigma \neq \ id} \sigma(x) \in \mathfrak{p}_j.$$

For the other hand, $N_K(x) \in \mathbb{Z}$, then $N_K(x) \in p\mathbb{Z} = \mathbb{Z} \cap \mathfrak{p}_j = \mathbb{Z} \cap \mathfrak{p}_i \subset \mathfrak{p}_i$. But $N_K(x) \notin \sigma^{-1}$, so we have a contradiction. □

Corollary 3. *Let K be a Galois extension over $\mathbb{Q}$ of degree n and let $\mathfrak{p}$ be a prime over p. Then, if $p\mathcal{O}_K = \mathfrak{b}_1^{e_1} \mathfrak{b}_2^{e_2} \ldots \mathfrak{b}_r^{e_r}$, then $e_1 = e_2 \ldots = e_r$, $f_1 = f_2 \ldots = f_r$ and $erf = n$.*

2 Factorization in Cyclotomic Fields

Let $m \geq 1$ and $K = \mathbb{Q}(\zeta_m)$. Then $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$ and p a prime in $\mathbb{Z}$. Then

$$\Phi_m(x) \equiv (g_1(x) g_2(x) \ldots g_r(x))^e \pmod{\text{p}},$$

deg ($g_i(x)$)=f for all i and $erf = \phi(m)$. Suppose that $p \nmid m$. So, $x^m - 1 = \prod_{d|m} \phi_d(x)$ has no factors with multiplicity greater than one, in particular $\phi_m(x)$. Then $e = 1$.

- Suppose $f = 1$, then $\phi_m(x)$ has only linear factors in $\mathbb{Z}_p[x]$.

  Lemma 1. *Let m be a positive integer and L be a field with char(L) $\nmid m$. If $\alpha \in L$, then $\phi_m(\alpha) = 0$ if and only if α is a primitive m-th root of unity.*

  Follow the previous lemma, $\mathbb{Z}_p$ has a primitive m-th root of unity. $\mathbb{Z}_p^*$ is a cyclic group of order $p-1$, then its elements of order m are exactly those $m|p-1$. So, $\mathbb{Z}_p^*$ has elements of order m if and only if $p \equiv 1 \pmod{m}$.

  Proposition 2. *p splits completely in $\mathcal{O}_K$ if and only $p \nmid m$ and $p \equiv 1$ (mod m).*

- $f > 1$. Let $g(x)$ be an irreducible factor of $\Phi_m(x)$ in $\mathbb{Z}_p[x]$, with deg($g(x)$)=f. Let α be a root of $g(x)$ and $F = \mathbb{Z}_p[\alpha] \cong \mathbb{Z}_p[x]/(g(x))$. Then $[F : \mathbb{Z}_p] = f$ and F has a primitive m-th root of unity, so $|F| = p^f$ and F^* is cyclic with order $p^f - 1$.

  Proposition 3. *f is the order of p in $\mathbb{Z}_p^*$ and there are $\phi(m)/f$ primes over p.*

If $p|m$, then p ramifies.

Example 1. *p in $\mathbb{Q}(\zeta_p)$. From $x^p - 1 \equiv (x-1)^p$ (mod p) and $\Phi_p(x) = \frac{x^p-1}{x-1}$, we have $\Phi_p(x) \equiv (x-1)^{p-1}$ (mod p), then*

$$p\mathcal{O}_K = (p, \zeta_p - 1)^{p-1},$$

that is, p is totally ramified.

2.1 Exercises

1. Let $\mathcal{O}_K = \mathbb{Z}[\alpha]$, where $K = \mathbb{Q}(\sqrt{d})$, d square free.If f is the minimal polynomial of α over $\mathbb{Q}$, show that

$$f(x) = \begin{cases} x^2 - d, & \text{if } d \equiv 2, 3 \pmod 4 \\ x^2 - x + \frac{1+\sqrt{d}}{2}, & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

2. Determine the factorization of 7,29 and 31 in $\mathbb{Q}(\sqrt[3]{2})$.

3. Determine the factorization of 5 in $\mathbb{Q}(\zeta_5)$.