Algebraic Number Theory

Dr. Anuj Jakhar

Lectures 13-16

Indian Institute of Technology Bhilai

anujjakhar@iitbhilai.ac.in

June 28, 2021

- Let K be an algebraic number field. For a given rational prime p, our main aim will be to factorize $p\mathcal{O}_K$ as a product of prime ideals of $\mathcal{O}_K$.
- We shall first introduce the notions of ramification index and residual degree.
- For a non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, $\mathcal{O}_K/\mathfrak{p}$ is a finite field in view of finite norm property. So $\mathfrak{p}$ contains a unique rational prime p which is the characteristic of the finite field $\mathcal{O}_K/\mathfrak{p}$; in this situation $\mathfrak{p}$ contains $p\mathcal{O}_K$ and hence $\mathfrak{p}$ divides $p\mathcal{O}_K$.

Definition. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ containing a prime p. If $\mathfrak{p}^e | p\mathcal{O}_K$ and $\mathfrak{p}^{e+1} \nmid p\mathcal{O}_K$, then e is called the index of ramification of $\mathfrak{p}$ over p or the absolute index of ramification of $\mathfrak{p}$.

Definition. Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_K$, then $\mathcal{O}_K/\mathfrak{p}$ being a finite field has order a power p^f of a prime p. The number f is called the residual degree of $\mathfrak{p}/p$ or the absolute residual degree of $\mathfrak{p}$.

Definition. Let S be a ring having a subring R. Let A, B be ideals of R and S respectively such that $A \subseteq B$. We say that B lies above A or A lies below B if $B \cap R = A$.

When a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ lies above $p\mathbb{Z}$, then by abuse of language we say that $\mathfrak{p}$ lies over p or that $\mathfrak{p}$ lies above p.

The following theorem gives us information about the prime ideals of $\mathcal{O}_K$ lying over a rational prime p when $K/\mathbb{Q}$ is a Galois extension.

Theorem 1. Let $K/\mathbb{Q}$ be a finite Galois extension and p be a rational prime. Let $\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_r^{e_r}$ be the factorization of $p\mathcal{O}_K$ with $\mathfrak{p}_1,\ldots,\mathfrak{p}_r$ distinct prime ideals of $\mathcal{O}_K$ and $e_1,\ldots,e_r$ positive. Then for any given pair $\mathfrak{p}_i,\mathfrak{p}_j$, there exists $\sigma\in\mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma(\mathfrak{p}_i)=\mathfrak{p}_j$.

We shall prove the following more general theorem.

Theorem 2. Let R be an integrally closed domain with quotient field L and L' be a finite Galois extension of L. Let R' be the integral closure of R in L'. Let $\mathfrak{p}',\mathfrak{q}'$ be maximal ideals of R' lying over a maximal ideal $\mathfrak{p}$ of R. Then there exists $\sigma\in\mathrm{Gal}(L'/L)$ such that $\sigma(\mathfrak{p}')=\mathfrak{q}'$.

Using the above theorem, we now prove

Theorem 3. Let $K/\mathbb{Q}$, $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ be as in Theorem **??**. Let f_i denote the residual degree of $\mathfrak{p}_i/p$. Then $e_i = e_1$ and $f_i = f_1$ for $2 \leq i \leq r$.

We establish an equality which relates the indices of ramification and the residual degrees of various prime ideals of $\mathcal{O}_K$ lying over p with the degree of $K/\mathbb{Q}$.

Fundamental Equality. Let $K/\mathbb{Q}$ be an extension of degree n and p be a rational prime. Let $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ be the factorisation of $p\mathcal{O}_K$ as a product of powers of distinct prime ideals of $\mathcal{O}_K$ and f_i denote the residual degree of $\mathfrak{p}_i/p$. Then

$$\sum_{i=1}^{r} e_i f_i = n = [K : \mathbb{Q}].$$

The following simple result is sometimes useful for computung index of ramification and residual degree.

Theorem 4. Let $K = \mathbb{Q}(\theta)$ be an algebraic number field of degree n, where θ is an algebraic integer. If the minimal polynomial of θ over $\mathbb{Q}$ is an Eisenstein polynomial with respect to a rational prime p, then there exists exactly one prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ which lies over p and $p\mathcal{O}_K = \mathfrak{p}^n$.

Notation. Let p be a prime. For $f(X) \in \mathbb{Z}[X], \overline{f}(X)$ will denote the polynomial obtained by replacing each coefficient of $f(X)$ by its image under the canonical homomorphism from $\mathbb{Z}$ onto $\mathbb{Z}/p\mathbb{Z}$. $\overline{f}(X)$ will be called the reduction of $f(X)$ modulo p.

Dedekind's Theorem on splitting of primes. Let $K = \mathbb{Q}(\theta)$ be an algebraic number field of degree n with θ an algebraic integer. Let $F(X)$ be the minimal polynomial of θ over $\mathbb{Q}$ and p be a rational prime not dividing the index of $\mathbb{Z}[\theta]$ in $\mathcal{O}_K$. Let $\overline{F}(X) = \overline{F}_1(X)^{e_1} \cdots \overline{F}_r(X)^{e_r}$ be the factorization of $\overline{F}(X)$ into powers of distinct irreducible polynomials over $\mathbb{Z}/p\mathbb{Z}$, where each $F_i(X) \in \mathbb{Z}[X]$ is monic. Then $\mathfrak{p}_i = \langle F_i(\theta), p \rangle$ for $1 \leq i \leq r$ are distinct prime ideals of $\mathcal{O}_K$ and $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$; moreover the residual degree of $\mathfrak{p}_i/p$ is $\deg F_i(X)$ for $1 \leq i \leq r$.

The following two lemmas are helpful in the proof of above theorem.

Lemma 5. Let $K = \mathbb{Q}(\theta)$ be an algebraic number field of degree n with θ an algebraic integer. If a rational prime p does not divide $[\mathcal{O}_K : \mathbb{Z}[\theta]]$, then the classes of $1, \theta, \ldots, \theta^{n-1}$ form a basis of $\mathcal{O}_K/p\mathcal{O}_K$ as a vector space over $\mathbb{Z}/p\mathbb{Z}$.

It may be pointed out that the converse of the above lemma is also true which can be proved by retracing the steps of the proof.

Lemma 6. Let $K = \mathbb{Q}(\theta)$ be an algebraic number field of degree n with θ an algebraic integer. Let p be a rational prime not dividing $[\mathcal{O}_K : \mathbb{Z}[\theta]]$. Let $G(X) \in \mathbb{Z}[X]$ be a polynomial whose reduction modulo p is irreducible over $\mathbb{Z}/p\mathbb{Z}$. Then the ideal generated by $G(\theta)$ and p in $\mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$ or it equals $\mathcal{O}_K$.

Remark.

We wish to point out that the converse of Theorem **??** is also true. This was proved in 2008. It can be stated as follows:

Converse.. Let $K = \mathbb{Q}(\theta)$ be an algebraic number field of degree n with θ an algebraic integer having minimal polynomial $F(X)$ over $\mathbb{Q}$. For a given prime p, let $\overline{F}(X) = \overline{F}_1(X)^{e_1} \cdots \overline{F}_r(X)^{e_r}$ be the factorization of the reduction of $F(X)$ modulo p into a product of powers of distinct irreducible polynomials over $\mathbb{Z}/p\mathbb{Z}$ with each $F_i(X) \in \mathbb{Z}[X]$ is monic. If $p\mathcal{O}_K$ has the analogous factorization into a product of powers of distinct prime ideals as $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, where $\mathfrak{p}_i = \langle F_i(\theta), p \rangle$ is prime ideal of $\mathcal{O}_K$ having $N(\mathfrak{p}_i) = p^{\deg F_i}$ for $1 \leq i \leq r$, then p does not divide the index of θ.

The examples given below illustrate Dedekind's theorem on splitting of primes.

Example.

- Let $K = \mathbb{Q}(\theta)$ with θ a root of the polynomial $f(X) = X^4 + 8X + 8$.
- Note that the polynomial $f(X)$ is irreducible over $\mathbb{Q}$ in view of Eisenstein-Dumas Irreducibility Criterion.
- One can easily check that $D_{K/\mathbb{Q}}(1, \theta, \theta^2, \theta^3) = 2^{12} \cdot 5$, so 5 does not divide the index of θ.
- Here $f(X)$ factors as a product $(X-2)^2(X^2+4X+2)$ of powers of irreducible polynomials modulo 5. So by Dedekind's theorem, $5\mathcal{O}_K = \mathfrak{p}_5^2\mathfrak{p}_5'$ where $\mathfrak{p}_5 = \langle 5, \theta - 2\rangle$, $\mathfrak{p}_5' = \langle 5, \theta^2 + 4\theta + 2\rangle$ are prime ideals of $\mathcal{O}_K$ with $N(\mathfrak{p}_5) = 5$ and $N(\mathfrak{p}_5') = 5^2$.

we shall apply Dedekind's theorem on splitting of primes to describe splitting of primes in quadratic and cyclotomic fields. For this, we define the following notion.

Notation. Let p be an odd prime. For any integer a, the Legendre symbol $\left(\frac{a}{p}\right)$ is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p|a, \\ 1 & \text{if } x^2 \equiv a \pmod{p} \text{ is solvable and } p \nmid a, \\ -1 & \text{if } x^2 \equiv a \pmod{p} \text{ is not solvable.} \end{cases}$$

For $a \equiv 0$ or $1 \pmod 4$, the Kronecker symbol is given by

$$\left(\frac{a}{2}\right) = \begin{cases} 0 & \text{if } 4|a, \\ 1 & \text{if } a \equiv 1 \pmod 8, \\ -1 & \text{if } a \equiv 5 \pmod 8. \end{cases}$$

With the above notations, using Dedekind's theorem, we prove

Theorem 7. Let K be a quadratic field having discriminant D. Let p be any prime odd or even. Then the following hold:

(i) If $p|D$, then $p\mathcal{O}_K = \mathfrak{p}^2, \mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ and $N(\mathfrak{p}) = p$.

(ii) If $\left(\frac{D}{p}\right) = 1$, then $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}_1, \mathfrak{p} \neq \mathfrak{p}_1$ are prime ideals of $\mathcal{O}_K$ and $N(\mathfrak{p}) = N(\mathfrak{p}_1) = p$.

(iii) If $\left(\frac{D}{p}\right) = -1$, then $p\mathcal{O}_K = \mathfrak{p}, \mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ and $N(\mathfrak{p}) = p^2$.

Definition. Let K be an algebraic number field. If there is a non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ such that $\mathfrak{p}^2$ divides $p\mathcal{O}_K$, then p is said to be ramified in K otherwise, it is called unramified in K. So p is unramified in K if $p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_m$, where $\mathfrak{p}_i$'s are distinct prime ideals of $\mathcal{O}_K$.

Definition. Let K be an algebraic number field of degree n. A prime p is said to be totally ramified in K if $p\mathcal{O}_K = \mathfrak{p}^n$ for some prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. A prime p is said to split completely in K if $p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_n$, where $\mathfrak{p}_i$'s are distinct prime ideals of $\mathcal{O}_K$.

Remark. By the last theorem, wesee that a rational prime p is totally ramified in a quadratic field K with discriminant D if and only if p divides D. Similarly p splits completely in K if and only if $\left(\frac{D}{p}\right) = 1$ and p is unramified in K if and only if p does not divide D.

We shall now discuss the splitting of a rational prime in a cyclotomic field for which the following lemma is needed.

Lemma 8. Let $m \geq 2$ be an integer, ζ a primitive mth root of unity and $K = \mathbb{Q}(\zeta)$. Let p be a rational prime not dividing m. Then p does not divide $D_{K/\mathbb{Q}}(1, \zeta, \ldots, \zeta^{\phi(m)-1})$.

Definition. Let p be a prime and $m \geq 1$ be a number not divisible by p. If h is the smallest positive integer such that $p^h \equiv 1 \pmod{m}$, then h is called the order of p modulo m. In fact h is the order of $m\mathbb{Z} + p$ in the multiplicative group $(\mathbb{Z}/m\mathbb{Z})^\times$ of reduced residue classes modulo m.

We first discuss the splitting of a prime p in the mth cyclotomic field when $p \nmid m$.

Theorem 8. Let $m \geq 2$ be an integer, ζ a primitive mth root of unity and $K = \mathbb{Q}(\zeta)$. Let p be a rational prime not dividing m and having order h modulo m. Then $p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_g$, where $g = \dfrac{\phi(m)}{h}$ and each prime ideal $\mathfrak{p}_i$ has residual degree h.

For obtaining the splitting of rational primes p dividing m in the mth cyclotomic field, we shall use the following lemma.

Lemma 9. Let $\mathbb{Q} \subseteq K_1 \subseteq K$ be algebraic number fields. Let p be a prime number. Suppose that $p\mathcal{O}_{K_1} = \mathfrak{p}'_1 \cdots \mathfrak{p}'_g$, where $\mathfrak{p}'_1, \ldots, \mathfrak{p}'_g$ are distinct prime ideals of $\mathcal{O}_{K_1}$ with $N(\mathfrak{p}'_i) = p^{f'_i}$. If $\mathfrak{p}'_i\mathcal{O}_K = \mathfrak{p}_i^{e_i}$ for $1 \leq i \leq g$ with $\mathfrak{p}_i$ an ideal of $\mathcal{O}_K$ and if $\sum_{i=1}^{g} e_i f'_i = [K : \mathbb{Q}]$, then each $\mathfrak{p}_i$ is a prime ideal of $\mathcal{O}_K$ and the residual degree of $\mathfrak{p}_i/p$ is f'_i for $1 \leq i \leq g$.

Recall for the proof of next theorem. Two elements α, β of $\mathcal{O}_K$ are said to be associates if there exists a unit ϵ of $\mathcal{O}_K$ such that $\beta = \alpha\epsilon$. If ζ_0 is a primitive (p^r)th root of unity, p prime, then for any positive integer k not divisible by p, $1 - \zeta_0^k$ and $1 - \zeta_0$ are associates because each divides the other in the ring $\mathbb{Z}[\zeta_0]$ as $1 - \zeta_0$ can also be written as $1 - \zeta_0^{kl}$, where $kl \equiv 1 \pmod{p^r}$.

Theorem 10. Let $m = p^r m'$ be an integer, where p is a prime number, $p \nmid m'$. Let ζ be a primitive mth root of unity. Then in the field $K = \mathbb{Q}(\zeta)$, $p\mathcal{O}_K = (\mathfrak{p}_1 \cdots \mathfrak{p}_g)^{\phi(p^r)}$, where $g = \dfrac{\phi(m')}{h}$ and h is the order of p modulo m'.

Finiteness of Ramified Primes

We shall prove the following theorem whose converse is also true.

Theorem 11 (Dedekind's theorem). If a rational prime p is ramified in an algebraic number field K, then p divides d_K.

Exercises

- Find how the primes $5, 7$ and 11 split in $\mathbb{Q}(\theta)$ where θ is a root of $x^3 - 18x - 6$.
- Find how the primes $2, 3$ and 5 split in $\mathbb{Q}(\theta)$ where θ is a root of $x^3 - x - 1$.
- Find how the primes $2, 3$ and 5 splits in $\mathbb{Q}(\sqrt{5})$.
- Find all rational primes p that ramify in K together with their prime ideal factorizations in $\mathcal{O}_K$, when K is one of the following fields:
  (a) $\mathbb{Q}(\sqrt[3]{6})$;
  (b) $\mathbb{Q}(\sqrt[3]{20})$.
- Find how the primes $2, 3$ and 5 split in $\mathbb{Q}(\zeta)$ where ζ is a primitive 28th root of unity.
- Find how the prime 5 splits in $\mathbb{Q}(\zeta)$ where ζ is a primitive 27th root of unity.