Introduction to Algebraic Number Theory
Lecture 9

Andrei Jorza

2014-02-02

Today: Ramification and inertia indices, norms of ideals. Textbook here is `http://wstein.org/books/ant/ant.pdf`

5 Ideals under extensions (continued)

(5.1) (Continued)

Example 1. Suppose m is square-free, different from 1 and $\equiv 2, 3 \pmod 4$. Let $K = \mathbb{Q}(\sqrt{m})$ in which case $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}]$.

1. If $X^2 - m = 0$ has no solutions in $\mathbb{F}_p$ then

$$\mathcal{O}_K \cong \mathbb{Z}[X]/(X^2 - m) \to \mathbb{F}_p[X]/(X^2 - m)$$

   is surjective onto the field $\mathbb{F}_p[X]/(X^2 - m)$ and has kernel $(p)\mathcal{O}_K$. Thus $(p)\mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$.

2. If $X^2 - m = 0$ has two solutions in $\mathbb{F}_p$, with representatives a and $-a$ in $\mathbb{Z}$ then

$$\mathcal{O}_K \cong \mathbb{Z}[X]/(X^2 - m) \to \mathbb{F}_p[X]/(X^2 - m) \cong \mathbb{F}_p[X]/(X - a) \oplus \mathbb{F}_p[X]/(X + a) \cong \mathbb{F}_p \oplus \mathbb{F}_p$$

   is again surjective. The preimage of $\mathbb{F}_p \oplus 0$ is the ideal $(p, \sqrt{m} - a)$ which is then prime since the image is a field. Similarly the preimage of $0 \oplus \mathbb{F}_p$ is the prime ideal $(p, \sqrt{m} + a)$ and

$$(p)\mathcal{O}_K = (p, \sqrt{m} - a)(p, \sqrt{m} + a)$$

   is the decomposition into primes.

(5.2) Ramification and inertia index.

Definition 2. If R is a Dedekind domain and $\mathfrak{p}$ is a prime (and therefore maximal) ideal then the **residue field** at $\mathfrak{p}$ is $k_{\mathfrak{p}} = R/\mathfrak{p}$.

Suppose now that L/K are number fields, $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ and $\mathfrak{q}$ is a prime ideal of $\mathcal{O}_L$ such that $\mathfrak{q} \mid \mathfrak{p}$. Then $k_{\mathfrak{q}} = \mathcal{O}_L/\mathfrak{q} \supset (\mathfrak{q} + \mathcal{O}_K)/\mathfrak{q} \cong \mathcal{O}_K/\mathfrak{p} = k_{\mathfrak{p}}$ and so $k_{\mathfrak{q}}$ is a finite extension of $k_{\mathfrak{p}}$.

Definition 3. The **inertia index** $f_{\mathfrak{q}/\mathfrak{p}} = [k_{\mathfrak{q}} : k_{\mathfrak{p}}]$. The **ramification index** is the exponent $v_{\mathfrak{q}}(\mathfrak{p}\mathcal{O}_L)$ of the prime ideal $\mathfrak{q}$ in the prime ideal decomposition of $\mathfrak{p}\mathcal{O}_L$.

Example 4. Let $K = \mathbb{Q}(i)$. We already know that $(2)\mathcal{O}_K = (1 + i)^2$, $(p)\mathcal{O}_K$ is prime when $p \equiv 3 \pmod 4$ and if $p \equiv 1 \pmod 4$ then $(p)\mathcal{O}_K = (a + bi)(a - bi)$ where $p = a^2 + b^2$. Let's compute the ramification and inertia indices.

1. $p = 2$ and $\mathfrak{q} = (2 + i)$. Then $e_{\mathfrak{q}/p} = 2$ and $k_{\mathfrak{q}} = \mathbb{Z}[i]/(1 + i) \cong \mathbb{Z}[X]/(X^2 + 1, X + 1) \cong \mathbb{Z}/2 \cong \mathbb{F}_2$ and so $f_{\mathfrak{q}/p} = 1$.

2. $p \equiv 1 \pmod 4$ with $a^2 + 1 \equiv 0 \pmod p$. Let $\mathfrak{q}_1 = (p, a+i)$ and $\mathfrak{q}_2 = (p, a-i)$ (If $p = u^2 + v^2$ then $(p, a+i) = (u+vi)$ and $(p, a-i) = (u-vi)$). Since the setup is symmetric we only compute for $\mathfrak{q} = \mathfrak{q}_1$. Clearly $e_{\mathfrak{q}/p} = 1$ from the prime decomposition. Next, $\mathbb{Z}[i]/(p, a+i) \cong \mathbb{Z}[X]/(X^2+1, p, a+X) \cong \mathbb{F}_p/(a^2+1) = \mathbb{F}_p$ and so $f_{\mathfrak{q}/p} = 1$.

3. If $p \equiv 3 \pmod 4$ then $\mathfrak{q} = (p)\mathbb{Z}[i]$ is a prime ideal and so $e_{\mathfrak{q}/p} = 1$. Now $\mathbb{Z}[i]/p\mathbb{Z}[i] \cong \mathbb{F}_p[X]/(X^2+1) \cong \mathbb{F}_{p^2}$ since X^2+1 doesn't have a root mod p. Thus $f_{\mathfrak{q}/p} = 2$.

We want the following theorem, for which we need to talk about norms of ideals first.

Theorem 5. *If L/K are number fields, $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ are the distinct prime ideals of $\mathcal{O}_L$ appearing in the prime factorization of $\mathfrak{p}\mathcal{O}_L$. Then*

$$\sum_{i=1}^{r} e_{\mathfrak{q}_i/\mathfrak{p}} f_{\mathfrak{q}_i/\mathfrak{p}} = [L : K]$$

In order to prove this we need to study norms of ideals.

(5.3) Norms of ideals.

Definition 6. Suppose V is a vector space over $\mathbb{Q}$ and $L, M \subset V$ are $\mathbb{Z}$-submodules of full rank. Define $[L : M] = |\det(A)|$ for any invertible matrix $A \in \mathrm{GL}(V)$ such that $A(L) = M$.

Definition 7. If K is a number field and I is a fractional ideal define $||I|| = [\mathcal{O}_K : I]$.

Example 8. Say $K = \mathbb{Q}(\sqrt{-23})$ and $I = (2, (-1+\sqrt{-23})/2)$. Then $\mathcal{O}_K$ is generated as a module over $\mathbb{Z}$ by 1 and $(1+\sqrt{-23})/2$ and so I as a $\mathbb{Z}$-module is generated by $2, 1+\sqrt{-23}, (-1+\sqrt{-23})/2$ and $(\sqrt{-23}+23)/2$. Playing with generator you see that I is generated over $\mathbb{Z}$ by 2 and $(-1+\sqrt{-23})/2$ and so the diagonal matrix $(2,1)$ takes $\mathcal{O}_K$ to I (with respect to the basis $1, (-1+\sqrt{-23})/2$ of K over $\mathbb{Q}$) and so $||I|| = 2$.

Proposition 9. *Suppose K is a number field.*

1. *If $a \in K$ and I is a fractional ideal of K then $||(a)I|| = |N_{K/\mathbb{Q}}(a)|||I||$.*

2. *If I and J are fractional ideals of K then $||IJ|| = ||I||||J||$.*

Proof. Part 1 done in class, see textbook Lemma 6.3.3

Part 2 will do next time, see textbook Proposition 6.3.4. The crucial ingredient is the following Lemma + Corollary. □

Lemma 10. *Suppose R is a Dedekind domain and $\mathfrak{p}$ is a prime ideal. Then $\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong R/\mathfrak{p}$.*

Proof. Will do in class, see textbook Proposition 5.2.4. □

Corollary 11. *If R is a Dedekind domain and $\mathfrak{p}$ is a prime ideal then $|R/\mathfrak{p}^n| = |k_\mathfrak{p}|^n$.*

Proof. In the filtration $R/\mathfrak{p}^n \supset \mathfrak{p}/\mathfrak{p}^n \supset \ldots \supset \mathfrak{p}^{n-1}/\mathfrak{p}^n$ each successive quotient is $\mathfrak{p}^i/\mathfrak{p}^{i+1} \cong k_\mathfrak{p}$. Thus $|R/\mathfrak{p}^n| = \prod_{i=0}^{n-1} |\mathfrak{p}^i/\mathfrak{p}^{i+1}| = |k_\mathfrak{p}|^n$. □