Algebraic Number Theory – Lecture 9

Andrew Potter

> "The difficulty lies, not in the new ideas, but in escaping from the old ones, which ramify, for those brought up as most of us have been, into every corner of our minds."
>
> – John Maynard Keynes

Recall that every ring of integers $\mathcal{O}_K$ is a Dedekind domain, i.e. we get unique factorisation of ideals into prime ideals. We are interested in how a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ factorises in the ring of integers $\mathcal{O}_L$ of a finite extension field L of K. In particular, if $K = \mathbb{Q}$, we will see how (p) factorises in a larger number field.

1. Separable extensions

Let $L : K$ be a separable extension of degree n, i.e. $L = K(\alpha)$ where α is a root of a separable polynomial (a polynomial with no repeated roots in an algebraic closure of K). Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal. We will write $\mathfrak{p}\mathcal{O}_L$ to mean $\mathfrak{p}$ considered as an ideal of $\mathcal{O}_L$, and just $\mathfrak{p}$ when we are thinking of it as an ideal of $\mathcal{O}_K$.

Now, $\mathfrak{p}\mathcal{O}_L$ factorises uniquely as a product of prime ideals in $\mathcal{O}_L$. Write

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

for prime ideals $\mathfrak{P}_i \subset \mathcal{O}_L$. We say the ideals $\mathfrak{P}_i$ *lie over* $\mathfrak{p}$, because, for each i, $\mathfrak{p} = \mathfrak{P}_i \cap \mathcal{O}_K$. For each i, e_i is called the *ramification index* of $\mathfrak{P}_i$. We define $f_i = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$. This is called the *inertia degree.*

Theorem. *We have the fundamental identity*

$$\sum_{i=1}^{r} e_i f_i = n.$$

Proof. See Neukirch's *Algebraic Number Theory*, pages 46–47. □

We say:

- $\mathfrak{p}$ *splits completely* if $r = n$. In that case $e_i = f_i = 1$, $(1 \leqslant i \leqslant r)$.
- $\mathfrak{p}$ is *nonsplit* if $r = 1$.
- $\mathfrak{P}_i$ is *unramified* if $e_i = 1$, $(1 \leqslant i \leqslant r)$, and $(\mathcal{O}_L/\mathfrak{P}_i) : (\mathcal{O}_K/\mathfrak{p})$ is a separable extension.[1]
- $\mathfrak{P}_i$ is *ramified* if it's not unramified, and *totally ramified* if $f_i = 1$, $(1 \leqslant i \leqslant r)$.
- $\mathfrak{p}$ is *unramified* if all the $\mathfrak{P}_i$ are unramified.
- $\mathfrak{p}$ is *ramified* if it's not unramified.

Theorem. *Only finitely many prime ideals in $\mathcal{O}_K$ ramify in $\mathcal{O}_L$.*

Those prime ideals that do ramify are given by the discriminant $\mathfrak{d}$ of $\mathcal{O}_L : \mathcal{O}_K$, defined to the ideal of $\mathcal{O}_K$ generated by the discriminants $d(\omega_1, \ldots, \omega_n)$ of all bases $\omega_1, \ldots, \omega_n$ of $L : K$ contained in $\mathcal{O}_L$. The prime (ideal) divisors of $\mathfrak{d}$ are exactly the primes in $\mathcal{O}_K$ that ramify.

[1] The separability condition gets around some 'pathological' cases.

2. Galois extensions

Assume now that $L:K$ is a Galois extension – i.e. separable and normal. Recall that $L:K$ is normal if every polynomial in $K[X]$ that has a root in L has all its roots in L. We can then define a Galois group $G=\mathrm{Gal}(L:K)=\mathrm{Aut}(L:K)$.

The Galois group acts on the prime ideals $\mathfrak{P}_1,\dots,\mathfrak{P}_r$ above a prime ideal $\mathfrak{p}$, i.e. if $\mathfrak{P}$ lies over $\mathfrak{p}$ then $\sigma\mathfrak{P}$ lies over $\mathfrak{p}$ for any $\sigma\in G$. This is because

$$\begin{aligned}(\sigma\mathfrak{P})\cap\mathcal{O}_K &= \sigma(\mathfrak{P}\cap\mathcal{O}_K)\\ &= \sigma\mathfrak{p}\\ &= \mathfrak{p}.\end{aligned}$$

Theorem. *G acts transitively on the primes over $\mathfrak{p}$. That is, for every pair of prime ideals $\mathfrak{P}_1,\mathfrak{P}_2$ over $\mathfrak{p}$, there is $\sigma\in G$ such that $\sigma\mathfrak{P}_1=\mathfrak{P}_2$.*

Definition. Let $\mathfrak{P}$ be a prime ideal over $\mathfrak{p}$. Then

$$G_{\mathfrak{P}}=\{\sigma\in G\,:\,\sigma\mathfrak{P}=\mathfrak{P}\}$$

is a subgroup of G called the *decomposition group* of $\mathfrak{P}$ over K. And

$$Z_{\mathfrak{P}}=\{x\in L\,:\,\sigma x=x \text{ for all } \sigma\in G_{\mathfrak{P}}\}$$

is called the *decomposition field* of $\mathfrak{P}$ over K.

The decomposition group encodes the number of prime ideals that $\mathfrak{p}$ splits into. For example,

$$G_{\mathfrak{P}}=\{\mathrm{id}\}\quad\Leftrightarrow\quad Z_{\mathfrak{P}}=L\quad\Leftrightarrow\quad \mathfrak{p}\text{ splits completely},$$

$$G_{\mathfrak{P}}=G\quad\Leftrightarrow\quad Z_{\mathfrak{P}}=K\quad\Leftrightarrow\quad \mathfrak{p}\text{ is nonsplit}.$$

Theorem. *The inertia degrees f_i and the ramification indices e_i are independent of i. That is, $e_1=\ldots=e_r=e$, and $f_1=\ldots=f_r=f$.*

Proof. Let $\mathfrak{P}=\mathfrak{P}_1$, then for every i, $\mathfrak{P}_i=\sigma_i\mathfrak{P}$ for some $\sigma_i\in G$. The isomorphism $\sigma_i:\mathcal{O}_L\to\mathcal{O}_L$ induces an isomorphism $\mathcal{O}_L/\mathfrak{P}\xrightarrow{\sim}\mathcal{O}_L/\sigma_i\mathfrak{P}$ given by $a \pmod{\mathfrak{P}}\mapsto\sigma_i a \pmod{\sigma_i\mathfrak{P}}$. So

$$\begin{aligned}f_i &= [\mathcal{O}_L/\sigma_i\mathfrak{P}:\mathcal{O}_K/\mathfrak{p}]\\ &= [\mathcal{O}_L/\mathfrak{P}:\mathcal{O}_K/\mathfrak{p}]\end{aligned}$$

for each i.

Furthermore, since $\sigma_i(\mathfrak{p}\mathcal{O}_L)=\mathfrak{p}\mathcal{O}_L$,

$$\begin{aligned}\mathfrak{P}^e\mid\mathfrak{p}\mathcal{O}_L\quad&\Leftrightarrow\quad\sigma_i\mathfrak{P}^e\mid\sigma_i(\mathfrak{p}\mathcal{O}_L)\\ &\Leftrightarrow\quad\sigma_i\mathfrak{P}^e\mid\mathfrak{p}\mathcal{O}_L.\end{aligned}$$

□

3. Example: Gaussian integers

We want to see how $(p)\subset\mathbb{Z}\subset\mathbb{Q}$ factorises in $\mathbb{Q}(i)$. $\mathbb{Q}(i):\mathbb{Q}$ is a Galois extension with $G=\{\mathrm{id},\sigma\}$ where σ is complex conjugation. There are three cases.

$p = 2$**:**

The ideal (2) ramifies in $\mathbb{Z}[i]$, indeed, $(2) = (1+i)^2$. So $e = 2$ and hence $f = 1$ by the fundamental identity. Thus

$$[\mathbb{Z}[i]/(1+i) : \mathbb{Z}[i]/(2)] = 1.$$

And $G_{(1+i)} = G$ since there is only one prime ideal over (2). This is the only prime that ramifies, since the discriminant of $\mathbb{Z}[i]$ is -4.

$p \equiv 1 \pmod 4$**:**

Fermat proved that any such (p) splits into two distinct primes over $\mathbb{Z}[i]$. For example, $13 = (2+3i)(2-3i)$. Then

$$G_{(2+3i)} = G_{(2-3i)} = \{\mathrm{id}\}.$$

$p \equiv 3 \pmod 4$**:**

Any prime of this form is inert in $\mathbb{Z}[i]$, i.e. the prime ideal (p) is still a prime ideal in $\mathbb{Z}[i]$.