Introduction to Algebraic Number Theory
Lecture 11

Andrei Jorza

2014-02-07

5 Ideals under extension (continued)

(5.5) Splitting.

Proposition 1. *Suppose $M/L/K$ is a tower of number fields and $\mathfrak{p}$, $\mathfrak{q}$ and $\mathfrak{r}$ ideals of $\mathcal{O}_K$, $\mathcal{O}_L$ and $\mathcal{O}_M$ respectively such that $\mathfrak{p} \mid \mathfrak{q} \mid \mathfrak{r}$. Then*

$$e_{\mathfrak{r}/\mathfrak{p}} = e_{\mathfrak{r}/\mathfrak{q}} e_{\mathfrak{q}/\mathfrak{p}}$$
$$f_{\mathfrak{r}/\mathfrak{p}} = f_{\mathfrak{r}/\mathfrak{q}} f_{\mathfrak{q}/\mathfrak{p}}$$

Proof. □

Definition 2. Let L/K be number fields. A prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ **splits completely** in $\mathcal{O}_L$ if $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1 \dots \mathfrak{q}_n$ where $n = [L : K]$. Say $\mathfrak{p}$ is **inert** in $\mathcal{O}_L$ if $\mathfrak{p}\mathcal{O}_L$ is prime in $\mathcal{O}_L$.

Corollary 3. *Let $M/L/K$ be number fields and $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$. If $\mathfrak{p}$ splits completely in M then it splits completely in L.*

Proof. $\mathfrak{p}$ splits completely in M iff for every $\mathfrak{r} \mid \mathfrak{p}$ have $e_{\mathfrak{r}/\mathfrak{p}} = f_{\mathfrak{r}/\mathfrak{p}} = 1$. The statement follows from the previous proposition. □

In fact the following also holds, but the general proof is beyond us (it uses analysis). (Most cases treated on the problem set.)

Proposition 4. *Suppose $L, L'/K$ are number fields and $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$. Then $\mathfrak{p}$ splits completely in LL' if and only if it splits completely in each of L and L'.*

The following homework problem provides an algorithm for factoring prime ideals is almost all cases.

Theorem 5. *Let L/K be number fields and $\mathfrak{p}$ a prime ideal of K lying above the prime p of $\mathbb{Z}$. Suppose $\alpha \in \mathcal{O}_L$ such that $L = K(\alpha)$ and $p \nmid |\mathcal{O}_L/\mathcal{O}_K[\alpha]|$. Let $f \in \mathcal{O}_K[X]$ be the minimal polynomial of α over K with $\mod \mathfrak{p}$ decomposition $f(X) \equiv \prod g_i(X)^{e_i} \pmod{\mathfrak{p}}$ where $g_i \mod \mathfrak{p}$ are distinct irreducibles. Then $\mathfrak{p}\mathcal{O}_L = \prod \mathfrak{q}_i^{e_i}$ where $\mathfrak{q}_i = \mathfrak{p}\mathcal{O}_L + g_i(\alpha)\mathcal{O}_L$ are distinct prime ideals with $f_{\mathfrak{q}_i/\mathfrak{p}} = \deg g_i$.*

(5.6) Ramification.

Definition 6. Let L/K be number fields and $\mathfrak{q} \mid \mathfrak{p}$ prime ideals of $\mathcal{O}_L$ and $\mathcal{O}_K$. Say that $\mathfrak{q}/\mathfrak{p}$ is **unramified** if $e_{\mathfrak{q}/\mathfrak{p}} = 1$ and **ramified** otherwise. Say that it is **totally ramified** if $f_{\mathfrak{q}/\mathfrak{p}} = 1$.

Say that $\mathfrak{p}$ ramified in L if $\mathfrak{q}/\mathfrak{p}$ is ramified for some $\mathfrak{q} \mid \mathfrak{p}$.

Example 7. From problem set 2: If $K = \mathbb{Q}(\zeta_p)$ then $(p)\mathcal{O}_K = (p, 1+\zeta_p)^{p-1}$ and so $(p, 1+\zeta_p)/(p)$ is totally ramified. If $q \neq p$ is a prime of exact order r in the cyclic group $\mathbb{F}_p^\times$ then $(q)\mathcal{O}_K = \mathfrak{q}_1 \dots \mathfrak{q}_{(p-1)/r}$ and $\mathfrak{q}_i/(q)$ is unramified.

Theorem 8. *Let $K/\mathbb{Q}$ be a number field. Then the prime p ramifies in K if and only if $p \mid \operatorname{disc}(K)$.*

Proof. For now the "only if" direction, the other part begin deferred until after Galois theory.

Suppose $\mathfrak{q}^2 \mid (p)\mathcal{O}_K$. Then $(p)\mathcal{O}_K = \mathfrak{q}I$ where I is divisible by all the prime ideals dividing (p). Let $\alpha \in I - (p)$. Then $\alpha \in \mathfrak{q}$ for every $\mathfrak{q} \mid (p)$.

Let $\sigma_1, \dots, \sigma_n : K \hookrightarrow \mathbb{C}$ be the embeddings fixing $\mathbb{Q}$ and let $L = \prod \sigma_i(K)$ be the composite. For every prime ideal $\mathfrak{q} \mid (p)$ of $\mathcal{O}_K$ write $\mathfrak{q}\mathcal{O}_L = \prod \mathfrak{r}_i$ as a product of (not necessarily distinct) prime ideals of $\mathcal{O}_L$. Since $\alpha \in \mathfrak{q}$ it follows that $\alpha \in \mathfrak{r}_i$ and as $\mathfrak{q}$ varies across the prime ideals dividing $(p)\mathcal{O}_K$, $\mathfrak{r}_i$ varies across the prime ideals dividing $(p)\mathcal{O}_L$. Thus $\alpha \in \mathfrak{r}$ for every prime ideal $\mathfrak{r} \mid (p)$ of $\mathcal{O}_L$.

For every $\sigma = \sigma_i$, $\sigma(\mathfrak{r})$ is also a prime ideal of $\sigma(\mathcal{O}_L) = \mathcal{O}_L$. Thus $\alpha \in \sigma(\mathfrak{r})$ and so $\sigma(\alpha) \in \mathfrak{r}$ for every σ.

Suppose $\alpha_1, \dots \alpha_n$ is an integral basis of $\mathcal{O}_K$ and $\alpha = \sum m_i \alpha_i$. Since $\alpha \notin (p)$ it follows that at least one m_i, say m_1 is not divisible by p. Now the determinant $\det(\sigma_i(\alpha), \sigma_i(\alpha_2), \dots \sigma_i(\alpha_n))_{i=1,\dots,n}$ is a linear combination of products of elements of $\mathcal{O}_L$ with at least one fact in $\mathfrak{r}$ which implies that $D = \operatorname{disc}_{K/\mathbb{Q}}(\alpha, \alpha_2, \dots, \alpha_n)$, which is the square of this determinant, must be in $\mathfrak{r}$ for all $\mathfrak{r} \mid (p)$ of $\mathcal{O}_L$. Thus $D \in \mathfrak{r} \cap \mathbb{Q} = (p)$.

But we've seen before that $\operatorname{disc}(\alpha, \alpha_2, \dots, \alpha_n) = \det(B)^2 \operatorname{disc}(\alpha_1, \dots, \alpha_n) = \det(B)^2 \operatorname{disc}(K)$ where B is the matrix taking $\alpha_1, \dots, \alpha_n$ to $\alpha, \alpha_2, \dots, \alpha_n$. Since $\det(B) = m_1$ is coprime to p is follows that $p \mid \operatorname{disc}(K)$ as desired.

□

Remark 1.

1. If $M/L/K$ are number fields and $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ which ramifies in L then $\mathfrak{p}$ ramifies in M.
2. If L/K are number fields, $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$ above p then $\mathfrak{p}$ ramifies in L implies $p \mid \operatorname{disc}(L)$.
3. As a corollary only finitely many prime ideals of $\mathcal{O}_K$ can ramify in L because the previous remark implies that if $\mathfrak{p}$ ramifies in L then $\mathfrak{p} \mid \operatorname{disc}(L)\mathcal{O}_K$.

6 Galois Theory

(6.1) In the proof of the first part of the previous theorem we used the composite $\prod \sigma(K)$, an awkward procedure which accounted for the fact that the embeddings of K into $\mathbb{C}$ fixing $\mathbb{Q}$ need not invary K.

Definition 9. An algebraic extension L/K of fields is said to be **Galois** if it is **separable** (i.e., every element of L has a minimal polynomial over K with no double root) and **normal** (i.e., if an irreducible polynomial in $K[X]$ has one root in L then it has all roots in L).

Remark 2. It turns out that finite Galois extension can all be obtained by adjoining to K all the roots of a polynomial with no double root.

Example 10.

Definition 11. The Galois group of a Galois extension L/K is $\operatorname{Gal}(L/K)$. It's size is $[L : K]$.

Fact 12. Suppose L/K is Galois. Then

1. $|\operatorname{Gal}(L/K)| = [L : K]$.
2. $\operatorname{Gal}(L/K)$ takes the root of an irreducible polynomial to another such root.

If L/K is any extension then the composite $\prod \sigma(L)$ over all embeddings $\sigma : L \hookrightarrow \overline{K}$ is called the **normal closure** of L over K and is the smallest normal extension of K containing L. If L/K is separable then its normal closure is called the **Galois closure**.

Example 13. $\mathbb{Q}(\sqrt{m})$, $\mathbb{Q}(\sqrt{2+\sqrt{2}})$, cyclotomic fields, finite fields.