Introduction to Algebraic Number Theory
Lecture 15

Andrei Jorza

6 Galois theory (continued)

(6.9) Back to ramification.

Theorem 1. *Let $K/\mathbb{Q}$ be a number field and p a prime. Then p ramifies in K iff $p \mid \operatorname{disc}(K)$.*

Proof. We already proved one direction.

Now the other direction: suppose $p \mid \operatorname{disc}(K)$. Let α_i be an integral basis of $\mathcal{O}_K$. It follows that the rows of $((\alpha_i, \alpha_j))$ must have a nontrivial dependence $\pmod p$ since p divides the determinant. There exist integers m_i, not all divisible by p, such that $\sum m_i(\alpha_i, \alpha_j) \equiv 0 \pmod p$ for all j. Say $p \nmid m_1$ and let $\alpha = \sum m_i \alpha_i$. Thus $(\alpha, x) \equiv 0 \pmod p$ for all $x \in \mathcal{O}_K$ with $\alpha \notin (p)\mathcal{O}_K$.

If p were unramified in K then $(p) = \prod \mathfrak{q}_i$ where $\mathfrak{q}_i$ are distinct prime ideals of $\mathcal{O}_K$. If $\alpha \in \mathfrak{q}_i$ for all i then $\alpha \in \cap \mathfrak{q}_i = \prod \mathfrak{q}_i$ which cannot be. Say $\alpha \notin \mathfrak{q} = \mathfrak{q}_1$.

Let $L/\mathbb{Q}$ be the normal closure of $K/\mathbb{Q}$. Since p is unramified in K it is also unramified in L. As before this implies that $\alpha \notin \mathfrak{q}$ for some $\mathfrak{q} \mid p$ an ideal of $\mathcal{O}_L$. Then

$$\begin{aligned}
\operatorname{Tr}_{L/\mathbb{Q}}(\alpha\Omega_L) &= \operatorname{Tr}_{K/\mathbb{Q}} \circ \operatorname{Tr}_{L/K}(\alpha\mathcal{O}_L) \\
&= \operatorname{Tr}_{K/\mathbb{Q}}(\alpha \operatorname{Tr}_{L/K}(\mathcal{O}_L)) \\
&\subset \operatorname{Tr}_{K/\mathbb{Q}}(\alpha\mathcal{O}_K) \\
&\subset p\mathbb{Z} \\
&\subset \mathfrak{q}
\end{aligned}$$

Choose $\beta \in (p)\mathfrak{q}^{-1} - \mathfrak{q}$. Then $\alpha\beta\mathcal{O}_L \subset (p)\mathfrak{q}^{-1} - \mathfrak{q}$. If $\sigma \in G_{L/\mathbb{Q}} - D_{\mathfrak{q}/p}$ then $\sigma(\mathfrak{q}) \neq \mathfrak{q}$ and so $\sigma(\alpha\beta\mathcal{O}_L) \subset \mathfrak{q}$ because $(p)\sigma(\mathfrak{q})^{-1}$ contains $\mathfrak{q}$ as a factor. Therefore

$$\sum_{\sigma \in D_{\mathfrak{q}/p}} \sigma(\alpha\beta\mathcal{O}_L) = \operatorname{Tr}_{L/\mathbb{Q}}(\alpha\beta\mathcal{O}_L) - \sum_{\sigma \notin D_{\mathfrak{q}/p}} \sigma(\alpha\beta\mathcal{O}_L) \in \mathfrak{q}$$

Therefore $\sum_{\sigma \in D} \sigma(\alpha\beta\mathcal{O}_L) \equiv 0$ in $k_\mathfrak{q}$ where we use the identification $D_{\mathfrak{q}/p} \cong \operatorname{Gal}(k_\mathfrak{q}/k_{(p)})$ from the fact that p is unramified in L. By choice $\alpha\beta \notin \mathfrak{q}$ and so is a unit in $k_\mathfrak{q}$ which implies that $\sum_{\sigma \in D} \sigma(x) = 0$ for all $x \in k_\mathfrak{q}$ which cannot be by linear independence of characters. ☐

7 The Class Group

(7.1) Finiteness of the class group.

Definition 2. Let K be a number field. We already know that the fractional ideals of K from a group. The **class group** $\operatorname{Cl}(K)$ of K is the quotient of the group of fractional ideals by the (normal) subgroup of principal fractional ideals. If K is a number field then the class number is $h_K = |\operatorname{Cl}(K)|$.

From the definition $\mathcal{O}_K$ is a PID if and only if $\operatorname{Cl}(K) = 1$ iff $h_K = 1$.

Theorem 3. *Let K be a number field.*

1. *Suppose there exists $\lambda > 0$ such that for every fractional ideal I there exists $\alpha \in I$ with $|N_{K/\mathbb{Q}}(\alpha)| \leq \lambda||I||$. Then $\mathrm{Cl}(K)$ is finite and is generated by prime ideals dividing $(n)\mathcal{O}_K$ for $n \leq \lambda$.*

2. *Such a λ exists and it has an effective albeit inefficient value.*

Proof. Part one: First note that if the assumption is satisfied by ideals then it is also satisfied by fractional ideals because we proved before that $||(a)I|| = |N_{K/\mathbb{Q}}(a)|||I||$ and some multiple of a fractional ideal is an ideal.

Let I be any fractional ideal and let $\alpha \in I^{-1}$ be such that $|N_{K/\mathbb{Q}}(\alpha)| \leq \lambda||I^{-1}||$. Then $J = (\alpha)I \subset I^{-1}I = \mathcal{O}_K$ has the property that $||J|| = |N_{K/\mathbb{Q}}(\alpha)|||I|| \leq \lambda||I^{-1}||||I|| = \lambda$. Denoting $[I]$ the image of the fractional ideal I in $\mathrm{Cl}(K)$ it follows that some ideal $J \in [I]$ has the property that $||J|| \leq \lambda$.

The finiteness of $\mathrm{Cl}(K)$ is immediate: indeed, if $||J|| = n \leq \lambda$ then $\mathcal{O}_K/J$ has n elements. But $\mathcal{O}_K$ is a finite free $\mathbb{Z}$-module and only finitely many quotients of $\mathbb{Z}^{[K:\mathbb{Q}]}$ have cardinality n.

If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ lying above the prime p of $\mathbb{Z}$ then $||\mathfrak{p}|| = p^{f_{\mathfrak{p}/p}}$. Thus if $J = \prod \mathfrak{p}_i^{e_i}$ then $||J|| = \prod p_i^{e_i f_{\mathfrak{p}_i/p_i}}$ and every prime factor of J must lie above n.

Part two: Let $\alpha_1, \ldots, \alpha_n$ be an integral basis of $\mathcal{O}_K$ and $\sigma_1, \ldots, \sigma_n : K \hookrightarrow \overline{\mathbb{Q}}$ be the embeddings fixing $\mathbb{Q}$. Then $\lambda = \prod_i \sum_j |\sigma_i(\alpha_j)|$ will work. Indeed, let $m = \lfloor \sqrt[n]{||I||} \rfloor$. The set $\{\sum_{j=1}^n m_j\alpha_j | 0 \leq m_i \leq m\} \subset \mathcal{O}_K$ has $(m+1)^n > ||I||$ elements and so at least two elements must be congruent $\mod I$. Let α be the difference of these two elements in which case $\alpha = \sum k_j\alpha_j$ with $-m \leq k_i \leq m$ and $\alpha \in I$. But then

$$\begin{aligned}
|N_{K/\mathbb{Q}}(\alpha)| &= \prod_i |\sigma_i(\sum k_j\alpha_j)| \\
&\leq \prod_i \sum_j |k_j||\sigma_i(\alpha_j)| \\
&\leq m^n\lambda \\
&\leq \lambda||I||
\end{aligned}$$

□

Remark 1. The explicit value of λ obtained above is effective in that for every K it can be computed but it is inefficient in that it's value can be large.