Introduction to Algebraic Number Theory
Lecture 13

Andrei Jorza

2014-02-12

6 Galois Theory (continued)

(6.4) Suppose L/K is a Galois extension of number fields. Let $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$ and $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^r \mathfrak{q}_i^e$ with $f = f_{\mathfrak{q}/\mathfrak{p}}$. Let $L^D = L^{D_{\mathfrak{q}/\mathfrak{p}}}$ and $L^I = L^{I_{\mathfrak{q}/\mathfrak{p}}}$ in which case we get extensions $L/L^I/L^D/K$. Let $\mathfrak{q}_I = \mathfrak{q} \cap L^I$ and $\mathfrak{q}_D = \mathfrak{q} \cap L^D$ in which case $\mathfrak{q} \mid \mathfrak{q}_I \mid \mathfrak{q}_D \mid \mathfrak{p}$.

Theorem 1. *We have $e_{\mathfrak{q}/\mathfrak{q}_I} = e$ and $f_{\mathfrak{q}_I/\mathfrak{q}_D} = f$. This implies that $|I_{\mathfrak{q}/\mathfrak{p}}| = e$ and we get surjection in the exact sequence $0 \to I_{\mathfrak{q}/\mathfrak{p}} \to D_{\mathfrak{q}/\mathfrak{p}} \to \mathrm{Gal}(k_{\mathfrak{q}}/k_{\mathfrak{p}}) \to 0$.*

Proof. First, $[L : L^D] = ef$ from the previous proposition and so $[L^D : K] = r$. Since $\mathrm{Gal}(L/L^D) = D_{\mathfrak{q}/\mathfrak{p}}$ acts transitively on the primes above $\mathfrak{q}_D$ but acts trivially on $\mathfrak{q}$ it follows that $f_{\mathfrak{q}/\mathfrak{q}_D} e_{\mathfrak{q}/\mathfrak{q}_D} = [L : L^D] = ef$. But $e = e_{\mathfrak{q}/\mathfrak{q}_D} e_{\mathfrak{q}_D/\mathfrak{p}}$ and $f = f_{\mathfrak{q}/\mathfrak{q}_D} f_{\mathfrak{q}_D/\mathfrak{p}}$ and so $e_{\mathfrak{q}_D/\mathfrak{p}} = f_{\mathfrak{q}_D/\mathfrak{p}} = 1$.

Next, if $\alpha \in \mathcal{O}_L$ then $g(X) = \prod_{\sigma \in I_{\mathfrak{q}/\mathfrak{p}}} (X - \sigma(\alpha)) \in \mathcal{O}_{L^I}[X]$. Since $\sigma(\alpha) \equiv \alpha \pmod{\mathfrak{q}}$ for $\sigma \in I_{\mathfrak{q}/\mathfrak{p}}$ it follows that $g(X) \equiv (X-\alpha)^{|I_{\mathfrak{q}/\mathfrak{p}}|} \pmod{\mathfrak{q}}$ and so $g(X) - (X-\alpha)^{|I_{\mathfrak{q}/\mathfrak{p}}|} \in k_{\mathfrak{q}_I}[X]$. The minimal polynomial of $\alpha \pmod{\mathfrak{q}}$ over $\mathfrak{q}_I$ divides $g(X) \pmod{\mathfrak{q}}$ and is irreducible and so it must be $X - \alpha \pmod{\mathfrak{q}}$ which implies that $\alpha \pmod{\mathfrak{q}} \in k_{\mathfrak{q}_I}$. Therefore $k_{\mathfrak{q}} = k_{\mathfrak{q}_I}$. This implies that $f_{\mathfrak{q}/\mathfrak{q}_I} = 1$.

Since the inertial index is multiplicative we deduce that $f_{\mathfrak{q}_I/\mathfrak{q}_D} = f_{\mathfrak{q}/\mathfrak{p}}$. If k is the number of primes of L^I above $\mathfrak{q}_D$ then $k e_{\mathfrak{q}_I/\mathfrak{q}_D} f_{\mathfrak{q}_I/\mathfrak{q}_D} = [L^I : L^D] = [D_{\mathfrak{q}/\mathfrak{p}} : I_{\mathfrak{q}/\mathfrak{p}}] \le [k_{\mathfrak{q}} : k_{\mathfrak{p}}] = f_{\mathfrak{q}/\mathfrak{p}}$. We conclude that $k = e_{\mathfrak{q}_I/\mathfrak{q}_D} = 1$ and so $e_{\mathfrak{q}/\mathfrak{q}_I} = e_{\mathfrak{q}/\mathfrak{p}}$. ☐

Corollary 2.

1. *$\mathfrak{p}$ splits completely in L^D*
2. *$\mathfrak{q}_D$ is inert in L^I*
3. *$\mathfrak{q}/\mathfrak{q}_I$ is totally ramified.*

Proof. First part: $\mathfrak{p}$ splits completely in L^D because $e_{\mathfrak{q}_D/\mathfrak{p}} = f_{\mathfrak{q}_D/\mathfrak{p}} = 1$.

Second part: since $f_{\mathfrak{q}_I/\mathfrak{q}_D} = [L^I : L^D]$ it follows that the number of primes of L^I above $\mathfrak{q}_D$ is 1 and appears with exponent 1.

Third part: $f_{\mathfrak{q}/\mathfrak{q}_I} = 1$. ☐

Proposition 3. *Suppose L/K, $\mathfrak{q} \mid \mathfrak{p}$, L^I and L^D as before.*

1. *L^D is the largest subextension in which $\mathfrak{p}$ splits completely (equivalently L^D is the largest extension with e and f equal to 1).*
2. *L^I is the smallest subextension such that L/L^I is totally ramified (equivalently L^I is the largest extension in which $\mathfrak{p}$ is unramified).*

Proof. First part: Suppose $L/K'/K$ such that $\mathfrak{p}$ splits completely in K' and let $H = G_{L/K'}$. Let $\mathfrak{p}' = \mathfrak{q} \cap K'$ in which case immediately from the definition it follows that $D' = D_{\mathfrak{q}/\mathfrak{p}'} = D_{\mathfrak{q}/\mathfrak{p}} \cap H$ and similarly $I' = I_{\mathfrak{q}/\mathfrak{p}'} = I_{\mathfrak{q}/\mathfrak{p}} \cap H$. Thus the tower $L/L^I/L^D/K$ in the case of L/K' and $\mathfrak{q} \mid \mathfrak{p}'$ becomes $L/L^{I'}/L^{D'}/K'$ with $L^{I'}/L^I$ and $L^{D'}/L^D$.

Since $\mathfrak{p}$ splits completely in K' it follows that $e_{\mathfrak{p}'/\mathfrak{p}} = f_{\mathfrak{p}'/\mathfrak{p}} = 1$ and so $e_{\mathfrak{q}/\mathfrak{p}'} = e_{\mathfrak{q}/\mathfrak{p}}$ and $f_{\mathfrak{q}/\mathfrak{p}'} = f_{\mathfrak{q}/\mathfrak{p}}$. This implies that $[L : L^{I'}] = [L : L^I]$ and $[L^{I'} : L^{D'}] = [L^I : L^D]$. But since $L^D \subset L^{D'}$ it follows that $L^D = L^{D'}$ and so $D_{\mathfrak{q}/\mathfrak{p}} \subset H$. This gives $K' \subset L^D$ as desired.

Second part: suppose K'/K is the largest subextension in which $\mathfrak{p}$ is unramified. Then $e_{\mathfrak{q}/\mathfrak{p}'} = e_{\mathfrak{q}/\mathfrak{p}}$ and the same argument as in the first part shows that $L^I \subset L^{I'} \subset L$ are such that $[L : L^{I'}] = [L : L^I]$ which implies that $L^I = L^{I'}$. But then $K' \subset L^{I'} = L^I$ as desired.

$\square$

Corollary 4. *Suppose L/K are number fields and $\mathfrak{p}$ is a prime of $\mathcal{O}_K$. If $\mathfrak{p}$ is unramified in L then it is unramified in the Galois closure of L/K.*

Proof. Let M/K be the normal closure of L/K. Since $\mathfrak{p}$ is unramified in L it is also unramified in $\sigma(L)$ for every $\sigma \in \mathrm{Gal}(M/K)$. Therefore, if $\mathfrak{q} \mid \mathfrak{p}$ is a prime of $\mathcal{O}_M$ and $M^I = M^{I_{\mathfrak{q}/\mathfrak{p}}}$ it follows that $\sigma(L) \subset M^I$ as M^I is the maximal extension in which p is unramified. This implies that $M = \prod \sigma(L) \subset M^I$ which means that $\mathfrak{p}$ is unramified in M. $\square$