Introduction to Algebraic Number Theory
Lecture 14

Andrei Jorza

2014-02-14

6 Galois Theory (continued)

(6.5) Frobenius. If L/K with ideals $\mathfrak{q} \mid \mathfrak{p}$ such that $\mathfrak{q}/\mathfrak{p}$ is unramified then $D_{\mathfrak{q}/\mathfrak{p}} \cong G_{k_\mathfrak{q}/k_\mathfrak{p}}$.

Since $G_{k_\mathfrak{q}/k_\mathfrak{p}}$ is cyclic generated by a lift of $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$ it follows that we may lift $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$ to $D_{\mathfrak{q}/\mathfrak{p}}$.

Lemma 1. *If $\sigma \in G_{L/K}$ then $\mathrm{Frob}_{\sigma(\mathfrak{q})/\mathfrak{p}} = \sigma \,\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}\, \sigma^{-1}$ and thus the conjugacy class of $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$ is independent of the choice of $\mathfrak{q}$. In particular if $G_{L/K}$ is abelian then $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$ as a Galois element does not depend on $\mathfrak{q}$.*

Proof. Follows from the fact that $D_{\sigma(\mathfrak{q})/\mathfrak{p}} = \sigma D_{\mathfrak{q}/\mathfrak{p}} \sigma^{-1}$. □

Example 2. If $p \neq q$ are odd primes then $\mathbb{Q}(\zeta_p)$ is unramified at q. Say $\mathfrak{r} \mid q$. What is $\mathrm{Frob}_{\mathfrak{r}/q} \in \mathrm{Gal}(K/\mathbb{Q})$? We know $G_{K/\mathbb{Q}} \cong \mathbb{F}_p^\times$ and if q has exact order r in $\mathbb{F}_p^\times$ then $f_{\mathfrak{r}/q} = r$ and so $\mathrm{Frob}_{\mathfrak{r}/q}(x) = x^q$ in $\mathbb{F}_{q^r}^\times$. Since $\zeta_p \in \mathbb{F}_{q^r}^\times$ it follows that $\mathrm{Frob}_{\mathfrak{r}/q}(\zeta_p) = \zeta_p^q$ and so $\mathrm{Frob}_{\mathfrak{r}/q}$ has image $q \in \mathbb{F}_p^\times$.

(6.6) Quadratic reciprocity. Let p be an odd prime and $p \nmid a$. If $x^2 \equiv a \pmod p$ has a solution with $x \in \mathbb{Z}$ write $\left(\dfrac{a}{p}\right) = 1$; otherwise write $\left(\dfrac{a}{p}\right) = -1$. This is called the Legendre symbol and has numerous applications including in cryptography.

Theorem 3 (Quadratic reciprocity)**.** *If $p \neq q$ are odd primes then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

We begin with a lemma.

Lemma 4. *Let $p \neq q$ be two odd primes and write $p^* = (-1)^{(p-1)/2}p$. Then q splits completely in $\mathbb{Q}(\sqrt{p^*})$ if and only if it splits into an even number of primes in $\mathbb{Q}(\zeta_p)$.*

Proof. Let $K = \mathbb{Q}(\sqrt{p^*}) \subset L = \mathbb{Q}(\zeta_p)$. If $q\mathcal{O}_K = \mathfrak{q}_1\mathfrak{q}_2$ then there exists $\sigma \in G_{K/\mathbb{Q}}$ such that $\sigma(\mathfrak{q}_1) = \mathfrak{q}_2$. Since $G_{K/\mathbb{Q}} \cong G_{L/\mathbb{Q}}/G_{L/K}$ (as $G_{L/\mathbb{Q}}$ is abelian) we can lift σ to $\sigma \in G_{L/\mathbb{Q}}$. Then σ takes the prime factorization $\mathfrak{q}_1\mathcal{O}_L = \prod \mathfrak{r}_j$ (recall that q is unramified in L) and yield $\mathfrak{q}_2\mathcal{O}_L = \prod \sigma(\mathfrak{r}_i)$ which implies that $q\mathcal{O}_L$ splits into an even number of primes of L.

Reciprocally, suppose $q\mathcal{O}_L = \prod_{i=1}^r \mathfrak{r}_i$ where r is even. Then $D_{\mathfrak{r}_i/q}$ has index r in $G_{L/\mathbb{Q}}$. Since $G_{L/\mathbb{Q}} \cong \mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$ it follows that $G_{L/\mathbb{Q}}/D_{\mathfrak{r}_i/q}$ is a cyclic abelian group of even order and so has a quotient isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Since $\mathbb{Z}/(p-1)\mathbb{Z}$ has a unique quotient isomorphic to $\mathbb{Z}/2\mathbb{Z}$ it follows that this quotient is $G_{K/\mathbb{Q}}$ and thus $G_K \supset G_{L/L^D}$ where $L^D = L^{D_{\mathfrak{r}_i/q}}$.

We already know that q splits completely in L^D and so, since K is a subfield, it must split completely in K as well, as desired. □

Proof of Theorem: We already showed that $x^2 \equiv -1 \pmod p$ has a root iff $p \equiv 1 \pmod 4$. Thus $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. Since $q \neq 2$ we can study its splitting in $\mathbb{Q}(\sqrt{p^*})$ using the polynomial $X^2 - p^* \pmod q$ and q splits completely iff $\left(\frac{p^*}{q}\right) = 1$. By the lemma this occurs iff q splits into an even number of primes in L. But we know how to split in $\mathbb{Q}(\zeta_p)$: if u is the order of q in $\mathbb{F}_p^\times$ then q splits into $(p-1)/u$ primes. This number of primes is even iff $2 \mid (p-1)/u$ iff $u \mid (p-1)/2$ in which case we'd have $q^{(p-1)/2} \equiv 1 \pmod p$. Let g be a generator of $\mathbb{F}_p^\times$ and $q \equiv g^m \pmod p$. Then $q^{(p-1)/2} \equiv g^{m(p-1)/2} \equiv 1$ iff m is even as g has order $p-1$, i.e., $\left(\frac{q}{p}\right) = 1$. Thus $\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$.

Now we're done since $\left(\frac{a}{p}\right)$ is multiplicative:

$$\begin{aligned}\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) &= \left(\frac{p^*}{q}\right)\left(\frac{(-1)^{(p-1)/2}}{q}\right)\left(\frac{q}{p}\right) \\ &= \left(\frac{-1}{q}\right)^{\frac{p-1}{2}} \\ &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\end{aligned}$$

□

(6.7) Higher ramification.

Definition 5. Suppose L/K is a Galois extension of number fields and $\mathfrak{q} \mid \mathfrak{p}$ are prime ideals of $\mathcal{O}_L$ and $\mathcal{O}_K$. Let $V_m = \{\sigma \in D_{\mathfrak{q}/\mathfrak{p}} | \sigma(x) \equiv x \pmod{\mathfrak{q}^{m+1}}\}$. Under this notation $I_{\mathfrak{q}/\mathfrak{p}} = V_0$. These are called higher ramification groups. The group V_1 is called the "wild inertia" group and is denoted $P_{\mathfrak{q}/\mathfrak{p}}$.

Theorem 6. *Suppose L/K, $\mathfrak{q} \mid \mathfrak{p}$ and V_m as above.*

1. *For $m \geq 0$ the group V_m is normal in $D_{\mathfrak{q}/\mathfrak{p}}$.*
2. *The filtration $V_0 \supset V_1 \supset \ldots$ is separated, i.e., $\cap V_m = \{1\}$.*
3. *Have injections $I_{\mathfrak{q}/\mathfrak{p}}/P_{\mathfrak{q}/\mathfrak{p}} \hookrightarrow k_{\mathfrak{q}}^\times$ and for $m \geq 1$, $V_m/V_{m+1} \hookrightarrow k_{\mathfrak{q}}$.*
4. *$P_{\mathfrak{q}/\mathfrak{p}}$ is the p-Sylow subgroup of $I_{\mathfrak{q}/\mathfrak{p}}$.*

Proof. ... □

Definition 7. We say that $\mathfrak{q}/\mathfrak{p}$ is tamely ramified if $p \nmid e_{\mathfrak{q}/\mathfrak{p}}$ or equivalently is $P_{\mathfrak{q}/\mathfrak{p}} = \{1\}$. We say that $\mathfrak{q}/\mathfrak{p}$ is wildly ramified otherwise, and totally wildly ramified if $I = P$.

Corollary 8. *The group $D_{\mathfrak{q}/\mathfrak{p}}$ is solvable.*

(6.8) Different.

Definition 9. Suppose L/K are number fields and I is a fractional ideal of L. The dual $I^\vee$ under the trace pairing is defined as

$$I^\vee = \{x \in L | (x, I)_{L/K} \subset \mathcal{O}_K\}$$

Proposition 10.

1. *The dual $\mathcal{O}_L^\vee$ is a fractional ideal of L.*
2. *For any fractional ideal I, the dual $I^\vee$ is a fractional ideal and $I^\vee = I^{-1}\mathcal{O}_L^\vee$.*
3. *Have $I^{\vee\vee} = I$.*

Definition 11. Let L/K be number fields. The **different** is the (fractional) ideal $\mathcal{D}_{L/K} = (\mathcal{O}_L^\vee)^{-1}$.

Remark 1. Since $\mathrm{Tr}_{L/K}(\mathcal{O}_L) \subset \mathcal{O}_K$ it follows that $\mathcal{O}_L \subset \mathcal{O}_L^\vee$ and so $\mathcal{D}_{L/K} \subset \mathcal{O}_L$ is an ideal.

Theorem 12. *Suppose L/K are number fields and $\mathfrak{q} \mid \mathfrak{p}$ prime ideals of $\mathcal{O}_L$ and $\mathcal{O}_K$. Then:*

1. *$\mathfrak{q}/\mathfrak{p}$ is ramified if and only if $\mathfrak{q} \mid \mathcal{D}_{L/K}$.*
2. *If $\mathfrak{q}/\mathfrak{p}$ is tamely ramified then $v_\mathfrak{q}(\mathcal{D}_{L/K}) = e_{\mathfrak{q}/\mathfrak{p}} - 1$.*
3. *If $\mathfrak{q}/\mathfrak{p}$ is totally ramified then*
$$v_\mathfrak{q}(\mathcal{D}_{L/K}) = \sum_{m \geq 0} (|V_m| - 1)$$
4. *If $\mathfrak{q}/\mathfrak{p}$ is wildly but not necessarily totally ramified then at least $v_\mathfrak{q}(\mathcal{D}_{L/K}) \geq e_{\mathfrak{q}/\mathfrak{p}}$.*

Proof. . . . □

(6.9) A geometric perspective.

Consider the multiplication map $\mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_L \to \mathcal{O}_L$ with kernel I. The differentials $\Omega^1_{\mathcal{O}_L/\mathcal{O}_K} = I/I^2$. and one can show that $\mathcal{D}_{L/K} = \mathrm{Ann}_{\mathcal{O}_L}(\Omega^1_{\mathcal{O}_L/\mathcal{O}_K})$.

On the geometric side suppose you have a finite cover $X \to Y$ of Riemann surfaces. Prime ideals of $\mathcal{O}_K$ or $\mathcal{O}_L$ correspond to points or curves in Y or X and prime decomposition is simply computing the preimage. Having prime ideal divide the different is equivalent to having that prime ideal contain the annihilator of $\Omega^1_{\mathcal{O}_L/\mathcal{O}_K}$ which is equivalent to saying that the prime ideal is in the support of $\Omega^1_{\mathcal{O}_L/\mathcal{O}_K}$. On the geometric side would be equivalent to saying that the curve is contained in the support of $\Omega^1_{X/Y}$ which is the ramification locus.