Introduction to Algebraic Number Theory
Lecture 12

Andrei Jorza

2014-02-10

6 Galois theory (continued)

(6.1) Basics (continued)

Example 1. Examples of Galois extensions and Galois groups.

1. $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$ has Galois group $\mathbb{Z}/2\mathbb{Z}$ sending $\sqrt{m} \mapsto \pm\sqrt{m}$.
2. $\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q}$ has Galois group $\mathbb{Z}/4\mathbb{Z}$ with generator sending $\sqrt{2+\sqrt{2}} \mapsto \sqrt{2-\sqrt{2}}$ and $\sqrt{2-\sqrt{2}} \mapsto -\sqrt{2+\sqrt{2}}$.
3. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois but has Galois closure $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ whose Galois group over $\mathbb{Q}$ is S_3 generated by $\sqrt[3]{2} \mapsto \zeta_3\sqrt[3]{2}$, $\zeta_3 \mapsto \zeta_3$ and $\sqrt[3]{2} \mapsto \sqrt[3]{2}$, $\zeta_3 \mapsto \zeta_3^2$.
4. The cyclotomic field $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ has Galois group $(\mathbb{Z}/n\mathbb{Z})^\times$. The Galois automorphism corresponding to $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ sends $\zeta_n \mapsto \zeta_n^a$.
5. The finite field extension $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$ (here $m \mid n$) is Galois with Galois group $\mathbb{Z}/\frac{n}{m}\mathbb{Z}$ generated by ϕ^m where $\phi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is the "Frobenius" map $\phi(x) = x^p$.

(6.2) Prime ideals and the Galois group.

Proposition 2. *Let L/K be a Galois extension of number fields.*

1. *$\sigma \in \mathrm{Gal}(L/K)$ acts on $\mathcal{O}_L$.*
2. *if $\mathfrak{q}$ is a prime ideal of $\mathcal{O}_L$ above a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ then $\sigma(\mathfrak{q})$ is also a prime ideal of $\mathcal{O}_L$ above $\mathfrak{p}$.*
3. *$\mathrm{Gal}(L/K)$ acts transitively on the set of prime factors of $\mathfrak{p}\mathcal{O}_L$.*
4. *if $\mathfrak{q}, \mathfrak{q}' \mid \mathfrak{p}$ then*
$$e_{\mathfrak{q}/\mathfrak{p}} = e_{\mathfrak{q}'/\mathfrak{p}}$$
$$f_{\mathfrak{q}/\mathfrak{p}} = f_{\mathfrak{q}'/\mathfrak{p}}$$
5. *If $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^r \mathfrak{q}_i^e$ with e the common ramification index and f the common inertia index then $ref = [L : K]$.*

Proof. First part: same polynomial.

Second part: if $xy \in \sigma(\mathfrak{q})$ then $\sigma^{-1}(x)\sigma^{-1}(y) \in \mathfrak{q}$ and so $x \in \sigma(\mathfrak{q})$ or $y \in \sigma(\mathfrak{q})$. Thus $\sigma(\mathfrak{q})$ is a prime ideal. Also $\sigma(\mathfrak{q}) \cap K = \sigma(\mathfrak{q} \cap K) = \sigma(\mathfrak{p}) = \mathfrak{p}$.

Third part: Suppose $\mathfrak{q}$ and $\mathfrak{q}'$ are distinct prime factors of $\mathfrak{p}\mathcal{O}_L$ and $\mathfrak{q}' \neq \sigma(\mathfrak{q})$ for all $\sigma \in \mathrm{Gal}(L/K)$. By the Chinese Remainder Theorem we can find $\alpha \in \mathcal{O}_L$ such that

$$\begin{aligned} \alpha &\equiv 0 \pmod{\mathfrak{q}'} \\ \alpha &\equiv 1 \pmod{\alpha(\mathfrak{q})} \end{aligned}$$

for all $\alpha \in \mathrm{Gal}(L/K)$. Then $N_{L/K}(\alpha) = \prod \sigma_i(\alpha) \in \mathfrak{q}' \cap K = \mathfrak{p}$. But $\sigma_i(\alpha) \notin \mathfrak{p} \subset \mathfrak{q}$ for all σ giving a contradiction.

Fourth part: If $\mathfrak{p}\mathcal{O}_L = \prod \mathfrak{q}_i^{e_i}$ then $\mathfrak{p}\mathcal{O}_L = \prod \sigma(\mathfrak{q}_i)^{e_i}$. Since $\mathrm{Gal}(L/K)$ acts transitively it follows that $e_i = e_j$ for all i, j. Moreover, $k_{\mathfrak{q}_i} = k_{\mathfrak{q}_j}$ by the same argument and so the equality of inertial indices follows.

Fifth part: immediate from $\sum e_i f_i = [L : K]$. □

(6.3) Main results of Galois theory.

Theorem 3. *Suppose L/K is a Galois extension.*

1. *If $L/M/K$ then L/M is Galois.*
2. *If $H \subset \mathrm{Gal}(L/K)$ is a subgroup then $L^H = \{x \in L | \sigma(x) = x, \forall \sigma \in H\}$ is a subfield $L/L^H/K$.*
3. *We have $\mathrm{Gal}(L/L^H) = H$ and $L^{\mathrm{Gal}(L/M)} = M$.*
4. *The maps $M \mapsto \mathrm{Gal}(L/M)$ and $H \mapsto L^H$ are inverse bijections between the set of subextensions $L/M/K$ and the subgroups $H \subset \mathrm{Gal}(L/K)$.*
5. *M/K (or L^H/K) is Galois if and only if $\mathrm{Gal}(L/M)$ (or H) is a normal subgroup of $\mathrm{Gal}(L/K)$, in which case $\mathrm{Gal}(M/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M)$ ($\mathrm{Gal}(L^H/K) \cong \mathrm{Gal}(L/K)/H$).*

Example 4. In class I did the subfields of $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ and the corresponding subgroups of S_3. This is found in any book on Galois theory.

(6.4) Decomposition groups.

Definition 5. Suppose L/K are number fields and $\mathfrak{q} \mid \mathfrak{p}$ ideals of $\mathcal{O}_L$ and $\mathcal{O}_K$. The **decomposition group** $D_{\mathfrak{q}/\mathfrak{p}} = \{\sigma \in \mathrm{Gal}(L/K) | \sigma(\mathfrak{q}) = \mathfrak{q}\}$. Then $D_{\mathfrak{q}/\mathfrak{p}} = \mathrm{Stab}_{\mathrm{Gal}(L/K)}(\mathfrak{q})$.

Lemma 6.
1. *If $\sigma \in \mathrm{Gal}(L/K)$ then $\sigma D_{\mathfrak{q}/\mathfrak{p}} \sigma^{-1} = D_{\sigma(\mathfrak{q})/\mathfrak{p}}$.*
2. *If $\mathfrak{p} = \prod_{i=1}^r \mathfrak{q}_i^e$ then $|D_{\mathfrak{q}/\mathfrak{p}}| = ef$.*
3. *If $\sigma \in D_{\mathfrak{q}/\mathfrak{p}}$ then σ induces an automorphism σ on $k_{\mathfrak{q}}$ which fixes $k_{\mathfrak{p}}$. This yields a homomorphism $D_{\mathfrak{q}/\mathfrak{p}} \to \mathrm{Gal}(k_{\mathfrak{q}}/k_{\mathfrak{p}})$.*

Proof. Part 1: This is true of all group actions. This implies that all decomposition groups have the same cardinality.

Part 2: Since $\mathrm{Gal}(L/K)$ acts transitively on the set of primes $\mathfrak{q}_i$ in $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^r \mathfrak{q}_i^e$ it follows that $[L : K] = |\mathrm{Gal}(L/K)| = r|D_{\mathfrak{q}/\mathfrak{p}}|$ and so $|D_{\mathfrak{q}/\mathfrak{p}}| = ef$. Here I use that if G acts on a finite set X and $x \in X$ has stabilizer H then $Gx = (G/H)x$ has as many elements as the set G/H; if the action is transitive then $|X| = |G/H|$ and so $|H| = |G|/|X|$.

Part 3: Follows from definitions. □

Definition 7. For $\mathfrak{q} \mid \mathfrak{p}$ the **inertia subgroup** $I_{\mathfrak{q}/\mathfrak{p}}$ is the kernel $0 \to I_{\mathfrak{q}/\mathfrak{p}} \to D_{\mathfrak{q}/\mathfrak{p}} \to \mathrm{Gal}(k_{\mathfrak{q}}/k_{\mathfrak{p}})$. It consists of $\sigma \in D_{\mathfrak{q}/\mathfrak{p}}$ such that $\sigma(x) \equiv x \pmod{\mathfrak{q}}$ for all $x \in \mathcal{O}_L$.