More tame Galois module structure and an introduction to wild Galois module structure

Alessandro Cobbe

1 Tame and wild extensions

Let L/K be a finite extension of number field or local fields.

Recall: p char of $\mathcal{O}_K/P$. If $\forall Q|P\mathcal{O}_L$, $\gcd(p, e_{Q/P}) = 1$ then L/K is tame at P. Otherwise wilde.

Let us assume L/K is local and Galois with $\mathrm{Gal}(L/K) = G$. Then

$$G_i = \{\sigma \in G \ : \ \sigma(x) \equiv x \pmod{Q^{i+1}} \ \forall x \in \mathcal{O}_L\}.$$

Note that $G_{-1} = G$ and G_0 is the usual inertia group, which is of order e.

Clearly enough to check for an x which generates $\mathcal{O}_L$ as an $\mathcal{O}_K$-algebra.

Equivalently: G acts on $\mathcal{O}_L/Q^{i+1}$ and G_i is the kernel of the action. So G_i are a decreasing filtration of normal groups and $G_i = \{1\}$ for i big enough.

Proposition 1.1. *Let $i \in \mathbb{N}$, $\sigma \in G_0$, let π be a uniformizer in L. Then*

$$\sigma \in G_i \Leftrightarrow \sigma(\pi)/\pi \equiv 1 \pmod{Q^i}$$

Proof. Since $\sigma \in G_0$ it is enough to check $\sigma(x) \equiv x \pmod{Q^{i+1}}$ for a generator x of $\mathcal{O}_L$ over $\mathcal{O}_{K_0}$, where $K_0 = L^{G_0}$.

Since L/K_0 is totally ramified we can take $x = \pi$.

Then divide $\sigma(\pi) \equiv \pi \pmod{Q^{i+1}}$ by π. □

We also have a filtration of the group of units U_L, by $U_L^i = 1 + Q^i$.

Proposition 1.2. *There is an injective map*

$$\theta_i : G_i/G_{i+1} \to U_L^i/U_L^{i+1}$$

induced by

$$s \mapsto s(\pi)/\pi.$$

It is independent of the choice of π.

Proof. Let $\pi' = \pi u$ with $u \in U_L$, then

$$s(\pi')/\pi' = s(\pi)/\pi s(u)/u$$

and $s(u)/u \in U_L^{i+1}$.

Homomorphism:

$$st(\pi)/\pi = s(t(\pi))/t(\pi) \cdot t(\pi)/\pi.$$

Injectivity is clear. □

Corollary 1.3. *G_0/G_1 is cyclic of order co-prime to p and G_1 is a p-group.*

Proof. G_0/G_1 is isomorphic to a subgroup of $\kappa_L^\times$; for $i > 1$, G_i/G_{i+1} is isomorphic to $U_L^i/U_L^{i+1} \cong \kappa_L$. □

Corollary 1.4. *L/K is tame iff $G_1 = 0$.*

Proof. L/K is tame iff the order of G_0 is co-prime to p iff $G_1 = 0$. □

Definition 1.5. *An extension is weakly ramified if $G_2 = 0$.*

[See Serre]

2 Orders

Let R be a noetherian domain with field of fractions K.

Definition 2.1. *An R-lattice M in a K-vector space V is a finitely generated R-submodule in V such that $V = KM$.*

Definition 2.2. *An R-order in a K-algebra A is a subring Λ of A (with the same 1) and such that Λ is an R-lattice.*

Examples:

- $\mathcal{O}_L$ is an $\mathcal{O}_K$-order in L;
- $\mathrm{Mat}_{n\times n}(R)$ is an R-order in $\mathrm{Mat}_{n\times n}(K)$;
- Let G be a finite group. $R[G]$ is an R-order in $K[G]$.
- Let L/K be a finite G-Galois extension of number fields or p-adic fields. The associated order is

  $$\mathcal{A}_{L/K} = \{x \in K[G] | x\mathcal{O}_L \subseteq \mathcal{O}_L\}.$$

  To prove that it is an order note that it is a subring of $K[G]$ and an $\mathcal{O}_K$-module.

Let $y \in K[G]$, then there exists $r \in \mathcal{O}_K$ such that $ry \in \mathcal{O}_K[G] \subseteq \mathcal{A}_{L/K}$. Hence $K\mathcal{A}_{L/K} = K[G]$.

Let $\alpha \in \mathcal{O}_L$ be such that $K[G] \cdot \alpha = L$; let $M \subseteq K[G]$ be such that $M \cdot \alpha = \mathcal{O}_L$. Then M is an $\mathcal{O}_K$-lattice in $K[G]$ and $\mathcal{A}_{L/K} \subseteq M$. Since $\mathcal{O}_K$ is noetherian and M is finitely generated, so is $\mathcal{A}_{L/K}$.

Proposition 2.3. *Let L/K and G be as above, let Γ be an $\mathcal{O}_K$-order in $K[G]$. If $\mathcal{O}_L$ is free over Γ, then $\Gamma = \mathcal{A}_{L/K}$.*

Proof. If $\mathcal{O}_L = \Gamma \cdot \alpha$ then $L = K[G] \cdot \alpha$ is also free. Let $x \in \mathcal{A}_{L/K}$, then $x\alpha \in \mathcal{O}_L = \Gamma \cdot \alpha$, hence $\exists y \in \Gamma$ with $x\alpha = y\alpha$ and $x = y$. Hence $\mathcal{A}_{L/K} \subseteq \Gamma$.

Let $\gamma \in \Gamma$, then $\gamma \cdot \mathcal{O}_L = \gamma \cdot (\Gamma \cdot \alpha) = (\gamma\Gamma) \cdot \alpha \subseteq \Gamma \cdot \alpha = \mathcal{O}_L$ and so $\gamma \in \mathcal{A}_{L/K}$. Hence $\Gamma \subseteq \mathcal{A}_{L/K}$. □

Example: $\alpha = 1 + i \in \mathbb{Z}[i]$, $e_1 = \frac{1+\sigma}{2}$, $e_{-1} = \frac{1-\sigma}{2}$, $\Gamma = \mathbb{Z}[e_1, e_2]$. Then $\Gamma \cdot \alpha = \mathbb{Z}[i]$. Hence $\mathcal{A}_{K[i]/K} = \Gamma$.

Corollary 2.4. *Let L/K be p-adic fields. Then $\mathcal{A}_{L/K} = \mathcal{O}_K[G]$ iff L/K is tame.*

Proof. Ilaria: If tame then NIB, then use the above proposition.

Conversely. Ilaria: If L/K is wild then $\mathrm{Tr}_{L/K}(\mathcal{O}_L) \subsetneq \mathcal{O}_K$, i.e. $\mathrm{Tr}_{L/K}(\mathcal{O}_L) \subseteq \pi_K\mathcal{O}_K$. Then $\frac{1}{\pi_K}\mathrm{Tr}_{L/K} \in \mathcal{A}_{L/K}$. □

[See Johnston, Section 3]

3 Locally free class groups

Let $\mathcal{O}_K$ be a Dedekind domain with field of fractions K, let Λ be an $\mathcal{O}$-order in a finite dimensional separable K-algebra (example: $K[G]$).

Definition 3.1. *A Λ-lattice is a Λ-module which is an $\mathcal{O}_K$-lattice.*

Definition 3.2. *Two Λ-lattices M and N are locally isomorphic if $M_p \cong N_p$ for each p. Notation: $M \vee N$. M is locally free if $M \vee \Lambda^{(n)}$.*

Theorem 3.3. *Let L/K be a finite tame extension of number fields with Galois group G. Then $\mathcal{O}_L$ is a locally free $\mathcal{O}_K[G]$-module of rank 1.*

Proof. Main ideas: $\mathcal{O}_{L_P}$ is a free $\mathcal{O}_{K_p}[G_P]$-module and $\mathcal{O}_{L,p} = \bigoplus_{P|p} \mathcal{O}_{L_P}$. □

We introduce an equivalence relation on the set of locally free Λ-lattices, writing $M \sim N$ if $\exists r, s \in \mathbb{N}$ such that $M \oplus \Lambda^{(r)} \cong N \oplus \Lambda^{(s)}$. Lattices in $[\Lambda]$ are called stably free.

Given M, M' locally free, there exists a locally free ideal M'' and $t \in \mathbb{N}$ such that $M \oplus M' = \Lambda^{(r)} \oplus M''$ [see Reiner, Maximal Orders, Theorem

(27.4)]; then we define $[M]+[M']=[M'']$. Also this shows that every class is represented by a locally free ideal.

The locally free class group $\mathrm{Cl}(\Lambda)$ is the group of the equivalence classes with the addition.

Example: $\mathrm{Cl}(\mathcal{O}_K)$ is the usual class group.

Theorem 3.4 (Jordan-Zassenhaus)**.** *If K is a global field, then $\mathrm{Cl}(\Lambda)$ is finite. (More precisely: $\forall t \in \mathbb{N}$ there are only finitely many isomorphism classes of Λ-lattices of $\mathcal{O}_K$-rank at most t.)*

Proof. See [Reiner, Maximal orders, Theorem (26.4)] □

Example: $[\mathcal{O}_L] \in \mathrm{Cl}(\mathcal{O}_K[G])$.

Warning: $[\mathcal{O}_L]$ trivial means $\exists r \in \mathbb{N}$ such that $\mathcal{O}_L \oplus \mathcal{O}_K[G]^{(r)} \cong \mathcal{O}_K[G]^{(r+1)}$ as $\mathcal{O}_K[G]$-modules. Actually one can take $r=1$. Cougnard gives an example of $K/\mathbb{Q}$ with Galois group Q_{32} (the generalized quaternion group of order 32) such that $\mathcal{O}_K$ is stably free but not free over $\mathbb{Z}[Q_{32}]$.

We say that Λ has locally free cancellation if $X \oplus \Lambda^{(k)} \cong Y \oplus \Lambda^{(k)}$ implies $X \cong Y$. In this case stably free is equivalent to free. This is tha case when the so-called Eichler condition holds. Concretely if K is totally complex or G is abelian, dihedral, symmetric or of odd order.

Martin Taylor proved the following:

Theorem 3.5 (Fröhlich's Conjecture - special case)**.** *Let L/K be a tame Galois extension of number fields with Galois group G. Then $[\mathcal{O}_L]^2$ is trivial in $\mathrm{Cl}(\mathbb{Z}[G])$. If G has no irreducible symplectiv characters then $\mathcal{O}_L$ is free of rank $[K:\mathbb{Q}]$ over $\mathbb{Z}[G]$.*

The condition on G holds for example when G is abelian, dihedral, symmetric or of odd order.

[See Johnston, Sections 10 and 15]

4 Leopoldt's Theorem

Lemma 4.1.

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_{p^{n+m}})/\mathbb{Q}(\zeta_{p^n})}(\zeta_{p^k}) = \begin{cases} \zeta_{p^k} p^m & \text{if } 0 \le k \le n, \\ 0 & \text{if } n < k \le n+m. \end{cases}$$

Proposition 4.2. *Let p be a rational prime, $n \in \mathbb{N}$, $G = \mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})$ and let $\alpha = \sum_{k=1}^{n} \zeta_{p^k}$. For $1 \le k \le n$, let $e_k = \frac{1}{p^{n-k}} \mathrm{Tr}_{\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}(\zeta_{p^k})}$. Then*

$$\mathbb{Z}[\zeta_{p^n}] = \mathcal{A}_{\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}} \cdot \alpha, \qquad \mathcal{A}_{\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}} = \mathbb{Z}[G][\{e_k\}_{k=1}^{n-1}].$$

Proof.

$$e_k(\zeta_{p^l}) = \begin{cases} \zeta_{p^l} & \text{if } 0 \le l \le k, \\ 0 & \text{if } k < l \le n \end{cases}$$

and $e_k(g\zeta_{p^l}) = ge_k(\zeta_{p^l})$. Therefore $e_k \in \mathcal{A}_{\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}}$ and $\mathcal{B} := \mathbb{Z}[G][\{e_k\}_{k=1}^{n-1}] \subseteq \mathcal{A}_{\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}}$.

Then $\mathcal{B} \cdot \alpha \subseteq \mathbb{Z}[\zeta_{p^n}]$.

Also $ge_1(\alpha) = g\zeta_p$ and $g(e_k - e_{k-1})(\alpha) = g\zeta_{p^k}$ for $2 \le k \le n$. Hence $\mathcal{B} \cdot \alpha \supseteq \mathbb{Z}[\zeta_{p^n}]$.

By Proposition 2.3, $\mathcal{B} = \mathcal{A}_{\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}}$. □

Lemma 4.3. *Let L_1 and L_2 be arithmetically disjoint, finite Galois extensions of K, let $L = L_1L_2$. Then*

(i) $\mathcal{A}_{L/L_2} = \mathcal{A}_{L_1/K} \otimes_{\mathcal{O}_K} \mathcal{O}_{L_2}$ *and* $\mathcal{A}_{L/K} = \mathcal{A}_{L_1/K} \otimes_{\mathcal{O}_k} \mathcal{A}_{L_2/K}$.

(ii) If $\exists \alpha_1 \in \mathcal{O}_{L_1}$ with $\mathcal{O}_{L_1} = \mathcal{A}_{L_1/K} \cdot \alpha_1$, then $\mathcal{O}_L = \mathcal{A}_{L/L_2} \cdot \alpha_1$.
If also $\exists \alpha_2 \in \mathcal{O}_{L_2}$ with $\mathcal{O}_{L_2} = \mathcal{A}_{L_2/K} \cdot \alpha_2$, then $\mathcal{O}_L = \mathcal{A}_{L/K} \cdot \alpha_1\alpha_2$.

It follows that $\mathbb{Z}(\zeta_n)$ is free over $\mathcal{A}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}$ for all n.

Lemma 4.4. *Let $K \subseteq L \subseteq L'$ be a tower of Galois extensions of number fields, assume L'/L is tame. If $\mathcal{O}_{L'} = \mathcal{A}_{L'/K} \cdot \alpha$ for some $\alpha \in \mathcal{O}_{L'}$. Then $\mathcal{A}_{L/K} = \pi(\mathcal{A}_{L'/K})$ and $\mathcal{O}_L = \mathcal{A}_{L/K} \cdot \mathrm{Tr}_{L'/L}(\alpha)$.*

Proof. Since L'/L is tame, $\mathrm{Tr}_{L'/L}(\mathcal{O}_{L'}) = \mathcal{O}_L$.

The trace is central in $K[\mathrm{Gal}(L'/K)]$:

$$\mathcal{O}_L = \mathrm{Tr}_{L'/L}(\mathcal{O}_{L'}) = \mathrm{Tr}_{L'/L}(\mathcal{A}_{L'/K} \cdot \alpha) = \mathcal{A}_{L'/K} \cdot \mathrm{Tr}_{L'/L}(\alpha) = \pi(\mathcal{A}_{L'/K}) \cdot \mathrm{Tr}_{L'/L}(\alpha).$$

That $\mathcal{A}_{L/K} = \pi(\mathcal{A}_{L'/K})$ follows from Proposition 2.3. □

Lemma 4.5. *Let K be an abelian extension of $\mathbb{Q}$ of conductor n. Then $\mathbb{Q}(\zeta_n)/K$ is tamely ramified at all primes lying above rational odd primes. If $i \in K$ the same is true for primes above 2.*

Proof. Let $p|n$ odd, so $n = p^r m$. Note that $N = K\mathbb{Q}(\zeta_{pm})$ is intermediate between $\mathbb{Q}(\zeta_{p^r m})$ and $\mathbb{Q}(\zeta_{pm})$; hence $N = \mathbb{Q}(\zeta_{p^s m})$ for some s (because $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^r m})/\mathbb{Q}(\zeta_{pm}))$ is cyclic of order a power of p), but s cannot be smaller than r. So $N = \mathbb{Q}(\zeta_{p^r m})$. Now N/K is tamely ramified at primes above p since $\mathbb{Q}(\zeta_{pm})/\mathbb{Q}$ is.

For primes above 2 the proof is analogous since $\mathrm{Gal}(\mathbb{Q}(\zeta_{2^r m})/\mathbb{Q}(\zeta_{4m}))$ is cyclic of order 2^{r-2}. □

Theorem 4.6 (Leopoldt)**.** *Let K be a finite abelian extension of $\mathbb{Q}$ of conductor n. Suppose that n is odd or $i \in K$. Let $\alpha = \mathrm{Tr}_{\mathbb{Q}(\zeta_n)/K}(\sum_{r(n)|d|n} \zeta_d)$. Then $\mathcal{O}_K = \mathcal{A}_{K/\mathbb{Q}} \cdot \alpha$.*

One can prove Leopoldt's Theorem for all finite abelian extensions of $\mathbb{Q}$ using an adjusted trace map.

One can recover Hilbert-Speiser Theorem as a special case.

There are several relative versions for absolutely abelian extensions of $\mathbb{Q}$, i.e. L/K with $L/\mathbb{Q}$ abelian.

[See Jonnston, Sections 11 and 12]