Student seminar notes week 2

Eva Terzolo after the talk of Dimitri Wyss

Recall: Let K/F be a finite extension of number fields. A prime ideal $\mathfrak{p} \subset \mathcal{O}_F$ is decomposed in a unique way: $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$, where the e_i's are called the *ramification indices* and the $\mathfrak{P}_i$'s are prime ideals which live "over" the prime ideal $\mathfrak{p}$ in the ring $\mathcal{O}_K$.

Definition 0.1. Let K/F be a finite extension of number fields and $\mathfrak{p} \subset \mathcal{O}_F$ be a prime ideal, the *residue field* of $\mathfrak{p}$ is defined as $\mathbb{F}_\mathfrak{p} := \mathcal{O}_F/\mathfrak{p}$. Moreover, $f_i = f(\mathfrak{P}_i/\mathfrak{p}) = [\mathbb{F}_{\mathfrak{P}_i} : \mathbb{F}_\mathfrak{p}]$ is the *residue field degree*.

To be a little less abstract, we can now consider the following diagram describing inclusions of fields:

$$\mathbb{Z}/\mathfrak{p} \cap \mathbb{Z} \qquad \subset \qquad \mathcal{O}_F/\mathfrak{p} \qquad \subset \qquad \mathcal{O}_K/\mathfrak{P}_i$$

In other words, we are looking at every prime ideal of the ring $\mathcal{O}_F$ and count how many prime ideals from the ring $\mathcal{O}_K$ are part of the decomposition of $\mathfrak{p}\mathcal{O}_K$.

Lemma 0.2. $\sum_{i=1}^{g} e_i \cdot f_i = [K : F]$

Remark 0.3. If the extension K/F is Galois, then $\mathrm{Gal}(K/F)$ acts transitively on the prime ideals $\mathfrak{P}_i$ (exercise 1(b) from exercise sheet 1). Hence, $e_1 = e_2 = \cdots = e_g = e$ and $f_1 = f_2 = \cdots = f_g = f$.

In general, we have that the degree of K/F is

$$\sum_{i=1}^{g} e_i \cdot f_i = [K : F]$$

and since K/F is Galois, we conclude that

$$[K : F] = \sum_{i=1}^{g} e \cdot f = e \cdot f \cdot g$$

Definition 0.4. Let K/F an extension of number fields, then a prime ideal $\mathfrak{p} \subset \mathcal{O}_F$ is

- *unramified* if $e_i = 1$, for all i.
- *ramified* if $e_i > 1$ for some i.

- *totally ramified* if $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}^e$ and $e = [K : F]$, i.e f = 1. This means that nothing happens on the residue field.
- *inert* if $\mathfrak{p}\mathcal{O}_K$ is prime, i.e doesn't split.
- *completely split* if $g = [K : F]$.

1 Discriminant

Let K/F be an extension of degree n, let $v_1, ..., v_n$ a F-basis of K.

Definition 1.1. The *discriminant* of the basis $v_1, ..., v_n$ is

$$d(v_1, ..., v_n) = \det(\mathrm{Tr}_{K/F}(v_i \cdot v_j)) = \det(\sigma_i(v_j))^2 \in F,$$

where Tr is the trace map of the extension K/F and $\sigma_1, ..., \sigma_n$ are the n different embeddings of K $\to F$.

If $K = F(\alpha)$ is a degree n extension, then $1, \alpha, ..., \alpha^{n-1}$ form a basis. Then the "classical" definition of the discriminant is

$$d(1, \alpha, \alpha^2, ..., \alpha^{n-1}) = \prod_{1 \leq i < j \leq n} (\sigma_i(\alpha) - \sigma_j(\alpha))^2$$

Note that, here, the discriminant depends on the choice of the basis, but can we generalize by not having to define a basis each time ? The answer is the following generalization over modules:

Definition 1.2. Let K/F be an extension, let $\mathcal{O}_F$ be the integral closure of $\mathbb{Z}$ inside F, let M be a $\mathcal{O}_F$-submodule of K containing an F-basis of K. We define the *discriminant* $d(M)$ to be the $\mathcal{O}_F$-module generated by the set of all possible discriminants

$$\{d(v_1, ..., v_n) : v_1, ..., v_n \in M \text{ is an } F\text{-basis of } K\}$$

Remark 1.3. If M is a fractional ideal, i.e a non zero, finitely generated $\mathcal{O}_F$-submodule of F, so is $d(M)$.

Example 1.4.

If M is *free*, i.e if $M = \oplus_{i=1}^n \mathcal{O}_F \cdot v_i$, $v_i \in K$. Then, $d(M) = d(v_1, ..., v_n) \cdot \mathcal{O}_F$.

If $M = \mathcal{O}_K$, we write $d_{K/F} = d(\mathcal{O}_K)$. It is called the *relative discriminant of* K/F.

The *(absolute) discriminant* of a number field F is $d_F = d_{F/\mathbb{Q}}$.

Then, we have the following important theorem.

Theorem 1.5. *A prime ideal* $\mathfrak{p} \subset \mathcal{O}_F$ *is ramified in* $K/F \iff \mathfrak{p} \mid d_{K/F}$

In particular, this implies that the set of ramified primes in $K|F$ is finite.

2 Norm

Recall: for any finite extension K/F, there is a *norm map* $N_{K/F} : K \to F$ such that $x \mapsto \det(f)$, where $f : K \to K$ is defined as $f(y) = x \cdot y$. But can we generalize this definition to ideals ?

Definition 2.1. Let K/F be an extension of number fields, $\mathfrak{P} \subset \mathcal{O}_K$ a prime ideal and $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_F$, then the *norm of* $\mathfrak{P}$ is $N_{K/F}(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})}$. More generally, if $U \subset K$ is a fractional ideal, i.e $U = \mathfrak{P}_1^{a_1} \cdots \mathfrak{P}_l^{a_l}$, $a_i \in \mathbb{Z}$, then $N_{K/F}(U) = \prod_{i=1}^{l} N_{K/F}(\mathfrak{P}_i)^{a_i} \subset F$.

Proposition 2.2. *Here are some properties of the norm of* $\mathfrak{P}$*:*

- *If* K/F *is Galois, then* $N_{K/F}(U) = \prod_{\sigma \in Gal(K/F)} \sigma(U) \cap F$
- *If* $\alpha \in K$, $N_{K/F}(\alpha\mathcal{O}_K) = N_{K/F}(\alpha)\mathcal{O}_F$. *More generally,* $N_{K/F}(U) =$ *fractional ideal generated by* $\{N_{K/F}(\alpha) : \alpha \in U\}$.
- *If* $F \subset E \subset K$, *then* $N_{K/F} = N_{E/F} \circ N_{K/E}$.
- *If* $F = \mathbb{Q}$, *then* $N_{K/\mathbb{Q}}(U) = a\mathbb{Z}$, *for some* $a \in \mathbb{Q}$.

One will, for now on, use the following notations: $NU = N_{K/\mathbb{Q}}(U)$ and $NU = |a|$, with a as above. In this case, if $\mathfrak{P} \subset \mathcal{O}_K$ is a prime ideal, then $N\mathfrak{P} = (\mathfrak{P} \cap \mathbb{Z})^{f(\mathfrak{P}/\mathfrak{P}\cap\mathbb{Z})} = (|\mathcal{O}_K/\mathfrak{P}|) = |\mathbb{F}_\mathfrak{P}| \subset \mathbb{Z}$.

3 Decomposition groups

Let K/F be a Galois extension with $G = \mathrm{Gal}(K/F)$, let $\mathfrak{p} \subset \mathcal{O}_F$ be a prime ideal and $\mathfrak{P} \subset \mathcal{O}_K$ with $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_K$.

Definition 3.1. The *decomposition group of* $(\mathfrak{p}, \mathfrak{P})$ is $Z(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in G : \sigma(\mathfrak{P}) = \mathfrak{P}\} \subset G$

In other words, the decomposition group of a prime ideal $\mathfrak{P}$ is the subgroup of G that consists of all automorphisms that "fix" the prime $\mathfrak{P}$. But beware of the fact that it's the prime ideal that is invariant and not the elements in it.
By definition, $Z(\mathfrak{P}/\mathfrak{p})$ acts on the finite field $\mathbb{F}_\mathfrak{P} = \mathcal{O}_K/\mathfrak{P}$ and fixes $\mathbb{F}_\mathfrak{p}$. Moreover, with the decomposition $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$, the stabilizer of a prime ideal $\mathfrak{P}_i$ under the action of the Galois group $\mathrm{Gal}(K/F)$ on the set $\{\mathfrak{P}_1, ..., \mathfrak{P}_g\}$ is given by $\mathrm{Stab}(\mathfrak{P}_i) = \{\sigma \in \mathrm{Gal}(K/F) | \sigma(\mathfrak{P}_i) = \mathfrak{P}_i\} =: \mathrm{Z}(\mathfrak{P}_i/\mathfrak{p})$, the decomposition group.
Thus, we have the following homomorphism:

$$Z(\mathfrak{P}/\mathfrak{p}) \to \mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}). \tag{1}$$

Theorem 3.2.

- *The degree* $[G : Z(\mathfrak{P}/\mathfrak{p})] = |\{\mathfrak{P} \subset \mathcal{O}_K \text{ prime } : \mathfrak{P} \mid \mathfrak{p}\mathcal{O}_K\}|$*, since* G *acts transitively on* $\mathfrak{P}$*. Moreover, if* $\mathfrak{P}, \mathfrak{P}' \mid \mathfrak{p}\mathcal{O}_K$*, then the two decomposition groups* $Z(\mathfrak{P}/\mathfrak{p})$ *and* $Z(\mathfrak{P}'/\mathfrak{p})$ *are* G*-conjugate.*
- *The homomorphism* (1) *is surjective, its kernel* $T(\mathfrak{P}/\mathfrak{p})$ *is called the* ***inertia subgroup****. In particular,* $[Z(\mathfrak{P}/\mathfrak{p}) : T(Z(\mathfrak{P}/\mathfrak{p})] = f$ *and* $|T(\mathfrak{P}/\mathfrak{p})| = e$*, i.e is exactly the ramification.*

Remark 3.3. If K/F is an abelian extension (G is abelian), then by the first part of the previous theorem, $Z(\mathfrak{P}/\mathfrak{p}) = Z(\mathfrak{p})$ depends only on $\mathfrak{p}$!

Now consider the following fields extensions:

$$\begin{array}{lll} K & & \\ | & & \\ K^{T(\mathfrak{P}/\mathfrak{p})} & = K_T & \text{(inertia field)} \\ | & & \\ K^{Z(\mathfrak{P}/\mathfrak{p})} & = K_Z & \text{(decomposition field)} \\ | & & \\ F & = K^G & \end{array}$$

Note that $F = K^G$ because the group G is Galois.

Theorem 3.4. *(Layer Theorem) Let* K/F *be an abelian extension, let* $\mathfrak{p} \subset \mathcal{O}_F$ *a prime ideal, then*

- $\mathfrak{p}$ *splits completely in* K_Z/F *(the "first layer" in our diagram above).*
- *The primes above* $\mathfrak{p}$ *remain inert in* K_T/K_Z *and ramify totally in* K/K_T*.*

4 Artin automorphism

This new section is motivated by the quadratic reciprocity.

Definition 4.1. Let K/F be Galois and an unramified prime ideal $\mathfrak{p} \subset \mathcal{O}_F$, by the previous theorem, there exists an isomorphism

$$Z(\mathfrak{P}/\mathfrak{p}) \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}).$$

Thus, if we take a look at the codomain, we see that the Galois group $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ is generated by one element: $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}) =< \varphi_{\mathfrak{p}} >$, where $\varphi_{\mathfrak{p}}(x) = x^{|\mathbb{F}_{\mathfrak{p}}|}, \forall x \in \mathbb{F}_{\mathfrak{P}}$ is the *Frobenius*.
We call the correspondent element of the Frobenius in $Z(\mathfrak{P}/\mathfrak{p})$ the *Frobenius element at* $\mathfrak{P}$ and denote it by $\left(\frac{\mathfrak{P}}{K/F}\right) = (\mathfrak{P}, K/F) \in Z(\mathfrak{P}/\mathfrak{p}) \subset G$.

Furthermore, if the extension K/F is abelian, then the Frobenius element $\left(\frac{\mathfrak{P}}{K/F}\right)$ only depends on $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_F$. In this case, it is the *Artin automorphism at* $\mathfrak{p}$, denoted $\left(\frac{\mathfrak{p}}{K/F}\right)$. It defines a map

$$\{ \text{ primes of } \mathcal{O}_F \text{ unramified in } K/F\} \to \mathrm{Gal}(K/F)$$

$$\mathfrak{p} \mapsto \left(\frac{\mathfrak{p}}{K/F}\right)$$

Let's look at some examples:

Example 4.2.

Let $F = \mathbb{Q}$, $K = \mathbb{Q}(\zeta_m)$ a cyclotonic extension, without loss of generality m is either odd or $4 \mid m$, because if $m = 2k$, with k odd then $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_k)$.

Then, in the Exercise sheet week 2, exercise 2(a), we prove that $p\mathbb{Z}$ ramifies in $K \iff p \mid m$

If $p \nmid m$, we have $\sigma \in \left(\frac{p\mathbb{Z}}{K/F}\right) \in \mathrm{Gal}(K/F) = (\mathbb{Z}/m\mathbb{Z})^\times$ is exactly $[p] \in (\mathbb{Z}/m\mathbb{Z})^\times$.

Example 4.3.

Let $K = \mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z}$, square-free, then $\mathrm{Gal}(K/F) = \{\pm 1\}$ and

$$d_K = \begin{cases} d & \text{if } d \equiv 1 \mod 4 \\ 4d & \text{if } d \not\equiv 1 \mod 4 \end{cases}$$

If $p \nmid d_K$ unramified and odd, then $\left(\frac{p\mathbb{Z}}{K/\mathbb{Q}}\right) = \left(\frac{d_K}{p}\right) \in \{\pm 1\}$, the Legendre symbol of the discriminant d_K (Exercise sheet 2, exercise 4(b)).

Note that writing $\mathrm{Gal}(K/F) = \{\pm 1\}$ means that the elements -1 and 1 are the non-trivial and trivial automorphisms respectively and not integers.