Galois modules torsion in Number fields

Eliharintsoa RAJAONARIMIRANA (mirana@aims.ac.za)
Université de Bordeaux
France

Supervised by: Prof Boas Erez
Université de Bordeaux, France

July 2014

Université de Bordeaux

Algebra, Geometry and Number Theory

2:3

ALGANT Erasmus Mundus

Abstract

Let E be a number fields with ring of integers R and N be a tame galois extension of E with group G. The ring of integers S of N is an $RG-$module, so an $\mathbb{Z}G-$module. In this thesis, we study some other $RG-$modules which appear in the study of the module structure of S as $RG-$ module. We will compute their Hom-representatives in Frohlich Hom-description using Stickelberger's factorisation and show their triviliaty in the class group $Cl(\mathbb{Z}G)$.

Acknowledgements

My appreciation goes first to my supervisor Prof Boas Erez for his guidance and support through out the thesis. His encouragements and criticisms of my work were of immense help. I will not forget to thank the entire ALGANT staffs in Bordeaux and Stellenbosch and all students for their help. Last but not the least, my profond gratitude goes to my family for their prayers and support through out my stay here.

Contents

Chapter 1

Introduction

1.1 Statement of the problem

The theory of Galois modules is a usefull topic in Mathematics, especially in Number Theory. For example, let N/E be a finite Galois extensions of number fields with group G, and let R and S be the ring of integers of E and N, respectively.

From Galois theory, a well known result says that the $EG-$module N has a normal basis, that is $N \simeq EG$ as E-vector space. For a long time, people wondered whether the same result holds for the $RG-$module S, namely, is $RG \simeq S$ as $RG-$module. This is the normal integral basis problem.

In general, the answer is no. Since R is not always a principal domain, there are examples of extensions N/E with S is not free over R. In tame case, Noether's theorem states that S is locally free. This allows to define a class of the ring of integers S in the class group $Cl(RG)$, which is the quotient of the set of locally free RG module by stable isomorphism. The class group $Cl(RG)$ measures how far a module is being free over RG.

So the question becomes, let N/E be tamely ramified Galois extension. Is $S \simeq \mathbb{Z}G^{[E:\mathbb{Q}]}$ as $\mathbb{Z}G$-module? Here $\mathbb{Z}$ is principal integral domain. Again, this is about the $\mathbb{Z}G$-structure of S in tamely ramified extensions.

The module structure of S in such extension has been studied. For example,if $E = \mathbb{Q}$, the normal integral basis problem was tackled by A. Fröhlich and solved by MJ Taylor.

Question: What about the other RG-modules in N?

Some of them have also been studied, among of which the inverse different, $\mathcal{C}_{N/E}$. In tame case, this module is locally free $\mathbb{Z}G-$module.

In this thesis, we will study some modules which appear in the study of the RG-structure of S which contains of course the inverse different of N/E.

The simplest of these modules is defined by the equality

$$T_{N/E} = \mathcal{C}_{N/E}/S.$$

From basic result in number theory, $\mathcal{C}_{N/E}$ is isomorphic to the dual of the module S, which is $\mathrm{Hom}_R(S, R)$, so S and $\mathcal{C}_{N/E}$ are dual of each other. This duality relation accounts for comparing their $\mathbb{Z}G$-module structures.

When N/E is tamely ramified, it amounts to comparing their classes $(\mathcal{C}_{N/E})$ and (S) in $Cl(\mathbb{Z}G)$. A. Fröhlich conjectured that $(\mathcal{C}_{N/E}) = (S)$. M J Taylor proved this equality under some stronger hypthesis and S. Chase proved it in general case. Chase's proof examine the torsion module $T_{N/E} = \mathcal{C}_{N/E}/S$.

B. Erez has considered the square root of the inverse different, $\mathcal{A}_{N/E}$. He proved for example that when N/E is tame and of odd degree, then the class of $\mathcal{A}_{N/E}$ in $Cl(\mathbb{Z}G)$ is trivial. In this thesis, we work with a tame Galois extension N/E where its $\mathcal{A}_{N/E}$ exists. In order to study it, we introduce the module

$$S_{N/E} = \mathcal{A}_{N/E}/S.$$

The last module that we are interested in is the torsion module $\mathcal{R}_{N/E}$ whose definition will be given later in Chapter 2. This was introduced by S. Chase.

Their triviliaty in the class group $Cl(\mathbb{Z}G)$ can be shown directly, for example as the proof of Chase, but we will give here an other proof by finding their precise Hom-representatives in Hom-description of Frohlich and showing that they lie in the denominator of $Cl(\mathbb{Z}G)$.

We mention that all the results of this thesis are due to Luca Caputo and Stéphane Vinatier in the article [CV].

1.2 Strategy of the work

The strategy of this thesis is as follows: In the definition of $T_{N/E}$ and $S_{N/E}$, we see that they are of the form S/I and I^{-1}/S for some G-stable ideal I, so we will study the general case of modules of such form. The study of $S_{N/E}$ will always be under the assumption that N/E is locally abelian. Working in this more general situation requires no additional effort and allows us to easily recover the cases of $T_{N/E}$ and $S_{N/E}$. But the study of the torsion module $\mathcal{R}_{N/E}$ is slightly different.

The most canonical way to study these modules is via localization, that is, by transition to local completions. Thus, after citing basic results from number theory, modules and algebras, we prove that the torsion modules we are interested in can be studied locally. That is, we consider the torsion modules $T_{N/E}, \mathcal{R}_{N/E}$ and $S_{N/E}$, then we reduce to the study for, every prime $\mathfrak{q}$ of S, of their $\mathbb{Z}I_{\mathfrak{q}}$-module structures, where $I_{\mathfrak{q}}$ is the inertia group at $\mathfrak{q}$. That is way we named the second chapter to be the Reduction to inertia group.

Suppose now that K/k is a finite Galois extensions of local fields with group Γ and inertia subgroup Δ. If we set F to be the fixed field of Δ, we show that it is sufficient to prove the triviality of $T_{K/F}$, $S_{K/F}$ and $\mathcal{R}_{K/F}$ in $Cl(\mathbb{Z}\Delta)$. That is, we can reduce the group G to the inertia group $I_{\mathfrak{q}}$. That is nice since the inertia group is a cyclic group hence abelian and the situation becomes much easier.
Let's state the main theorem in the chapter 2. For the statement we introduce some terminology.

N/E is a finite tame Galois extensions of number fields with group G and ring of integers R and S, respectively. For any prime ideal $\mathfrak{p}$ of R we fix a prime ideal $\mathfrak{q}$ of S dividing $\mathfrak{p}$. We denote by $D_{\mathfrak{q}}$ (resp. $I_{\mathfrak{q}}$) the decomposition group (resp. the inertia group) of $\mathfrak{q}$ in the group G. Then, the cardinality of $I_{\mathfrak{q}}$ only depends on $\mathfrak{p}$ and we denote it by $e_{\mathfrak{p}}$.

We fix an injective character $\chi_{\mathfrak{q}} : I_{\mathfrak{q}} \to \overline{\mathbb{Q}}^{\times}$ and an embedding $\iota_{\mathfrak{q}} : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_p$ where p is the rational number below $\mathfrak{p}$ such that $\iota_{\mathfrak{q}} \circ \chi_{\mathfrak{q}} = \chi_{N_{\mathfrak{q}}/F_{\mathfrak{q}}}$ where $N_{\mathfrak{q}}$ is the completion of N with respect to $\mathfrak{q}$ and $F_{\mathfrak{q}}$ is the fixed field of the inertia group $I_{\mathfrak{q}}$, i.e $F_{\mathfrak{q}} = N_{\mathfrak{q}}^{I_{\mathfrak{q}}}$. These choice determine a prime ideal $\mathfrak{p}$ in the ring of integers $\mathcal{O}_{e_{\mathfrak{p}}}$ of $\mathbb{Q}(\mu_{e_{\mathfrak{p}}}) \subset \overline{\mathbb{Q}}$ satisfying $\iota_{\mathfrak{q}}(\mathfrak{p}) \subset \mathfrak{q}S_{\mathfrak{q}}$, where $S_{\mathfrak{q}}$ is the valuation ring of $N_{\mathfrak{q}}$. The injection $\iota_{\mathfrak{q}}$ makes $\mathcal{O}_{F_{\mathfrak{q}}}$ into $\mathcal{O}_{e_{\mathfrak{p}}}-$module where $Ram(N/E)$ is the set of primes of E that ramify in N/E.

The followinig theorem is the main result of the chapter 2 which says that

1.2.1 Theorem. *For every $\mathfrak{p} \in Ram(N/E)$, choose a prime $\mathfrak{q}$ of N above $\mathfrak{p}$. Then, with the notation introduced above, there is an ismorphism of $\mathbb{Z}G-$modules:*

$$T_{N/E} \simeq \bigoplus_{\mathfrak{p} \in Ram(N/E)} \left(\mathbb{Z}G \otimes_{\mathbb{Z}D_{\mathfrak{q}}} T(p, \mathbb{Z}I_{\mathfrak{q}})\right)^{\oplus[R/\mathfrak{p}:\mathbb{F}_p]}.$$

Furthermore, for every choice of injective characters $\chi_{\mathfrak{q}} : I_{\mathfrak{q}} \to \overline{\mathbb{Q}}^{\times}$ for every prime $\mathfrak{q}$ as above, one can find primes $\mathcal{P}$ of $\mathcal{O}_{e_{\mathfrak{p}}}$ and injections $\mathcal{O}_{e_{\mathfrak{p}}}/\mathcal{P} \to S/\mathfrak{q}$ such that there is isomorphisms of $\mathbb{Z}G-$modules:

$$\mathcal{R}_{N/E} \simeq \bigoplus_{\mathfrak{p} \in Ram(N/E)} \left(\mathbb{Z}G \otimes_{\mathbb{Z}I_{\mathfrak{q}}} R_{\chi_{\mathfrak{q}}}(\mathcal{P}, \mathcal{O}_{e_{\mathfrak{p}}} I_{\mathfrak{q}})\right)^{\oplus[G:D_{\mathfrak{q}}][S/\mathfrak{q}:\mathcal{O}_{e_{\mathfrak{p}}}/\mathcal{P}]}.$$

Moreover, if N/E is locally abelian, then the injections $\mathcal{O}_{e_{\mathfrak{p}}}/\mathcal{P} \to S/\mathfrak{q}$ factor through $R/\mathfrak{p} :\to S/\mathfrak{q}$ and there is an isomorphism of $\mathbb{Z}G-$modules:

$$S_{N/E} \simeq \bigoplus_{\mathfrak{p} \in Ram(N/E)} \left(\mathbb{Z}G \otimes_{\mathbb{Z}I_{\mathfrak{q}}} S_{\chi_{\mathfrak{q}}}(\mathcal{P}, \mathcal{O}_{e_{\mathfrak{p}}} I_{\mathfrak{q}})\right)^{\oplus[R/\mathfrak{p}:\mathcal{O}_{e_{\mathfrak{p}}}/\mathcal{P}]},$$

where $T(p, \mathbb{Z}I_{\mathfrak{q}}), R_{\chi_{\mathfrak{q}}}(\mathcal{P}, \mathcal{O}_{e_{\mathfrak{p}}} I_{\mathfrak{q}})$ and $S_{\chi_{\mathfrak{q}}}(\mathcal{P}, \mathcal{O}_{e_{\mathfrak{p}}} I_{\mathfrak{q}})$ are $\mathcal{O}_{e_{\mathfrak{p}}}/\mathcal{P}I_{\mathfrak{q}}$-modules.

Thanks to this Theorem and the functoriality :

$$Cl(\mathbb{Z}I_{\mathfrak{q}}) \to Cl(\mathbb{Z}G)$$

it is sufficient to study the new modules introduced above, which are $\mathcal{T} := T(p, \mathbb{Z}I_{\mathfrak{q}}), \mathcal{R} := R_{\chi_{\mathfrak{q}}}(\mathcal{P}, \mathcal{O}_{e_{\mathfrak{p}}} I_{\mathfrak{q}})$ and $\mathcal{S} := S_{\chi_{\mathfrak{q}}}(\mathcal{P}, \mathcal{O}_{e_{\mathfrak{p}}} I_{\mathfrak{q}})$, so in the next chapter we focus only on the study of these new modules. These modules are much easier to study since they are Galois module of a cyclotomic fields in which many known results can be used to treat the problem.

In Chapter 3, we are thus in the cyclotomic setting introduced as follows: we fix an integer e, a cyclic group Δ of order e and an injective character $\chi : \Delta \to \mu_e$, the group of e^{th} roots of unity in the algebraic closure of $\mathbb{Q}$. We denote by $\mathcal{O}$ the ring of integers of $\mathbb{Q}(\mu_e)$ and p the rational prime such that $p \nmid e$. Let $\mathcal{P}$ be a prime ideal of $\mathcal{O}$ above p. We set $\kappa = \mathcal{O}/\mathcal{P}$. We are now ready to state the main result of the third chapter which is also the core of this work.

1.2.2 Theorem. *The classes $(\mathcal{T}), (\mathcal{R})$ and $(\mathcal{S})$ are trivial in $Cl(\mathbb{Z}\Delta)$. More precisely, they are represented in $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_\Delta, J(\mathbb{Q}(\mu_e)))$ by the morphisms with $\mathfrak{q}^{th}-$components equal to 1 if the prime $\mathfrak{q} \nmid e$ and to*

$$\mathrm{Det}(p^{-1}u_t), \mathrm{Det}(u_r^{-1}), \mathrm{Det}(u_s^{-1})$$

respectively, at prime ideals $\mathfrak{q}$ of $\mathcal{O}$ if $\mathfrak{q}|e$, where $u_t, u_r, u_s \in \mathbb{Z}\Delta$ are defined by

$$u_t = \sum_{i=0}^{p-1} \delta^i, u_r = \sum_{i=0}^{e-1} m_i \delta^i, u_s = \sum_{i=0}^{e-1} n_i \delta^i$$

and satisfy $u_t, u_r, u_s \in \mathbb{Z}_q\Delta^{\times}$ for any rational prime $q|e$.

Using the reduction results of Chapter 2, and Theorem 1.2.2 we deduce the following consequence:

1.2.3 Theorem. *Let N/E be a Galois tamely ramified extension of number fields. Then the classes of $T_{N/E}, \mathcal{R}_{N/E}$ and $\mathcal{S}_{N/E}$ are trivial in $Cl(\mathbb{Z}G)$. In particular, we have*

$$(S) = (\mathcal{C}_{N/E}) \text{ and } (S \otimes_R S) = (S)^{[N:E]} = 1.$$

If further N/E is locally abelian, then the class of $\mathcal{S}_{N/E}$ is trivial in $Cl(\mathbb{Z}G)$. In particular we have

$$(S) = (\mathcal{A}_{N/E}),$$

thus $S, \mathcal{C}_{N/E}$ and $\mathcal{A}_{N/E}$ define the same class in $Cl(\mathbb{Z}G)$.

1.3 Commutative Algebras

In this section, we recall some definitions and general results in commutative algebras. The good reference of this is [DF04].

Modules and tensor products

Let R be a ring and let $I \subset R$. I is said to be two-sided ideal of R if it is both right ideal and left ideal. If R is commutative ring, where left and right are equivalent, a two- sided ideal is called simply an ideal.

If M is an $R-$module and for some two-sided ideal I of R, we say that M is annihilated by I if $am = 0$ for all $a \in I, m \in M$. In this situation we can make M into $R/I-$module by defining an action of the quotient ring R/I on M as follows: for each $m \in M$ and $r + I \in R/I$,

$$(r + I).m = r.m$$

This is well defined since $am = 0, \forall a \in I, m \in M$.

As a consequence of this, if M, N are $R-$modules annihilated by I, then any $R-$homomorphism from M to N is $R/I-$homomorphism.

1.3.1 Definition. Tensor product Let R, S be any rings. An abelian group M is called $(S, R)-$bimodule if M is a left $S-$module and right $R-$module and $s(mr) = (sm)r$ for all $s \in R, s \in S, m \in M$.

For example, if I is an ideal of a ring R, then the quotient R/I is an $(R/I, R)-$bimodule.

Now, suppose that N is a left $R-$module and M is an $(S, R)-$bimodule, then the tensor product $M \otimes_R N$ is the set of finite sum of $m \otimes n, m \in M, n \in N$. It is a left $S-$module by the action

$$s.(\sum m_i \otimes n_i) = \sum (sm_i) \otimes n_i, m_i \in M, n_i \in N.$$

Extension fo scalars on change of base. Let $f : R \to S$ be a homomorphism of rings. Then $s.r = sf(r)$ gives S the strucutre of right $R-$module and with respect to it, S is an $(S, R)-$bimodule. Then for any left $R-$module N, the tensor product $S \otimes_R N$ is a left $S-$module obtained by changing the base from R to S.

In paricular, if we have a ring homomorphism $f : R \to S$, then we have $S \otimes_R R \simeq S$ as left $S-$ module via the map $s \otimes r \mapsto sf(r)$.

Let R be a ring, I a two-sided ideal of R. Let N be a left $R-$module, then R/I is $(R/I, R)$,bimodule, so the tensor product $R/I \otimes_R N$ is a left $R/I-$module and we have an isomorphism $R/I \otimes_R N \simeq N/IN$ via the map $(r + I) \otimes n \mapsto rn + IN$.

Let M, M' be $(S, R)-$bimodule and let N, N' be left $R-$module and $\phi : M \to M', \psi : N \to N'$ are $R-$module homomorphisms. Then there is a unique $S-$module homomorphism denoted by $\phi \otimes \psi$ mapping $M \otimes_R N \to M' \otimes_R N'$ defined by $\phi \otimes \psi(m \otimes n) = \phi(m) \otimes \psi(n)$.

In particular, if R is commutative ring, then $\phi \otimes \psi$ is an $R-$ module homomorphism.

(Associativity of tensor product) Suppose that M is a right $(S, R)-$bimodule, N an $(R, T)-$bimodule and L is a left $T-$module. Then, there is a unqiue isomorphism of $S-$modules:

$$(M \otimes_R) \otimes_T L \simeq M \otimes_R (N \otimes_T L)$$

given by $(m \otimes n) \otimes l \mapsto m \otimes (n \otimes l)$
If R is commutative and M, N, L are left $R-$modules then $(M \otimes_R N) \otimes_R L \simeq M \otimes_R (N \otimes_R L)$ as $R-$modules.

(Tensor product of direct sum) Let M, M' be (S, R)-bimodules, N, N' be left $R-$modules. Then we have isomorphisms of left $S-$modules

$$(M \oplus M') \otimes_R N \simeq (M \otimes_R N) \oplus (M \otimes_R N')$$
$$M \otimes_R (N \oplus N') \simeq (M \otimes_R N) \oplus (M \otimes_R N')$$

In particular, if R is a commutative ring these are also isomorphisms of R-modules as well.

As a consequence, the module obtained from the free $R-$module $N \simeq R^n$ by extension of scalars from R to S is the free $S-$module S^n, i.e $S \otimes_R R^n \simeq S^n$ as S-modules.

(The group $\operatorname{Hom}_R(D, -)$) and projective module Let R be a ring and let M, N be left R-modules. Denote by $\operatorname{Hom}_R(M, N)$ the set of all R-homomosprhism from M to N.

Let D, L, M be $R-$modules and let $\psi L :\to M$ be an $R-$module homomorphism, then we have a homorphism of group $\psi' : \operatorname{Hom}_R(D, L) \to \operatorname{Hom}_R(D, M)$ given by $f \mapsto \psi o f$.

If ψ is injective then ψ' is injective.
Let D, L, M, N be $R-$modules then

- $\operatorname{Hom}_R(D, L \oplus N) \simeq \operatorname{Hom}_R(D, L) \oplus \operatorname{Hom}_R(D, N)$
- $\operatorname{Hom}_R(L \oplus N, D) \simeq \operatorname{Hom}_R(L, D) \oplus \operatorname{Hom}_R(N, D)$

We say that M is projective if for any surjective homomorphism $\psi : M \to N$ of $R-$modules, the homomorpshim of groups ψ' is surjective.

(Flat module) Suppose that D is a $(S, R)-$bimodule. For any homomorphism $f : X \to Y$ of left $R-$modules, we obtain a homomorphism of left $S-$module $1 \otimes f : D \otimes_R X \to D \otimes_R Y$. If f is surjective, then $1 \otimes f$ is surjective.

We say that D is flat $R-$module if for any injective homomorphism $f : X \to Y$ of left $R-$module, the homomorphism $1 \otimes f$ is injective.

(Relation between $\operatorname{Hom}_R(D, -)$ and $D \otimes_R -$) Let R and S be rings, let A be a right $R-$module, let B be an $(R, S)-$bimodule and let C be a right $S-$module. Then there is an isomorphism of abelian groups

$$\operatorname{Hom}_S(A \otimes_R B, C) \simeq \operatorname{Hom}_S(B, C)$$

If $R = S$ is commutitaive ring then this is an isomorphism of $R-$modules as well.

1.3.2 Lemma. (Snake lemma)
Let R be a commutative rings. Given the following diagram of $R-$modules with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r] \arrow[d, "\alpha"'] & N \arrow[r] \arrow[d, "\beta"'] & L \arrow[r] \arrow[d, "\gamma"'] & 0 \\
0 \arrow[r] & A \arrow[r] & B \arrow[r] & C \arrow[r] & 0
\end{tikzcd}$$

then, there is an exact sequence:

$$\ker \alpha \to \ker \beta \to \ker \gamma \to \operatorname{Coker} \alpha \to \operatorname{Coker} \beta \to \operatorname{Coker} \gamma$$

1.3.3 Definition. (Group ring) Let R be a commutative ring and G be a finite group. The group ring RG consists of the free $R-$module on the set G, that is

$$RG = \{\sum_{g\in G} a_g g, a_g \in R\}$$

Addition is defined by componentwise and multipication is defined by extending $(rg)(sh) = (rs)(gh)$ for all $r, s \in R, g, h \in G$ by distributive law. It makes RG into a ring. Note that $R = R.1$ is a subring of RG.

1.3.4 Definition. An $G-$ module is an abelian group M where G acts on it and the action commutes with the group law of M. Moreover if M is an $R-$module for any ring R, and the action of G commutes with the R-module structure of M then we say that M is an $RG-$module.

If G is a Galois group of some extension of fields, we say that M is a Galois module.

1.3.5 Remark. An abelian group is the same as a module over $\mathbb{Z}$, so an $G-$module M is the same as a module over the group ring $\mathbb{Z}G$.

1.3.6 Definition. Let R be a commutative ring and G be a finite group.
Let H be a subgroup of a finite group G and M is an $H-$module. Define the induced $G-$module to be $\mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G, M)$. More precisely, it is the set $\{f : G \to M/f(hg) = hf(g), h \in H, g \in G\}$. The action of G on $\mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G, M)$ is given by: $(g.f)(x) = f(xg)$.

1.3.7 Lemma. Let H be a subgroup of finite index of a group G and M an $H-$module. Then the module $\mathbb{Z}G \otimes_{\mathbb{Z}H} M$ obtained by extension of scalars from $\mathbb{Z}H$ to $\mathbb{Z}G$ is a $G-$module and we have an isomorphism of G-modules

$$\mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G, M) \simeq \mathbb{Z}G \otimes_{\mathbb{Z}H} M.$$

Proof. Let $g_1, \dots, g_n$ be a set of left coset of representatives for H in G and write $G = g_1H \bigcup \cdots \bigcup g_nH$. So as an abelian group, we have $\mathbb{Z}G = \oplus_{i=1}^n g_i\mathbb{Z}H$.

Also, $\mathbb{Z}G \otimes_{\mathbb{Z}H} M = (\oplus_{i=1}^n g_i\mathbb{Z}H) \otimes_{\mathbb{Z}H} M = \oplus_{i=1}^n (g_i \otimes_{\mathbb{Z}H} M)$ by the property of tensor product and direct sum.

Consider the map $\varphi : \mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G, M) \to \mathbb{Z}G \otimes_{\mathbb{Z}H} M$ defined by $\varphi(f) = \sum_{i=1}^n g_i \otimes f(g_i^{-1})$. We want to show that φ is an $G-$isomorphism. Clearly, it is linear. Let $g \in G$, then $\varphi(g.f) = \sum_{i=1}^n g_i \otimes (g.f)(g_i^{-1}) = \sum_{i=1}^n g_i \otimes f(g_i^{-1}g)$. Write $g_i^{-1}g = h_i g_{i'}^{-1}, i = 1, \dots, n$. Then we have

$$\begin{aligned}
\sum_{i=1}^n g_i \otimes f(g_i^{-1}g) = &\ sum_{i=1}^n g_i \otimes f(h_i g_{i'}^{-1}) \\
&= \sum_{i=1}^n g_i \otimes h_i f(g_{i'}^{-1}) \\
&= \sum_{i=1}^n g_i h_i \otimes f(g_{i'}^{-1}) \\
&= \sum_{i=1}^n g h_i \otimes f(g_{i'}^{-1}) \\
&= g \sum_{i=1}^n h_i \otimes f(g_{i'}^{-1}) \\
&= g\varphi(g).
\end{aligned}$$

Hence φ is $G-$homomorphism. The injectivity of φ comes from the fact that $f = 0 \in \mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G, M)$ if and only if $f(g_i) = 0$ for all $i = 1, \dots n$.

To prove surjectivity, let $g_i \otimes m \in \mathbb{Z}G \otimes_{\mathbb{Z}H} M$. Define the function from $\mathbb{Z}G$ to M defined by $f_{i,m}(g) = hm$ if $g = hg_i^{-1}, h \in H$, and 0 otherwise. $f_{i,m} \in \mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G, M)$ since if $g = hg_i^{-1} \in G$, and $h' \in H$, then $h'g = h'hg_i^{-1}$ and we have $f_{i,m}(h'g) = h'hm$ if $x = hg_i^{-1}$ and 0 otherwise. Now, it easy to see that, for any $g_i \otimes m \in \mathbb{Z}G \otimes_{\mathbb{Z}H} M$, we have $\varphi(1 \otimes f_{i,m}) = g_i \otimes m$. □

Galois algebras

We recall some usefull results on Galois algebras. The details can be seen in [DI71]

1.3.8 Definition. Let R be a commutative ring. An $R-$algebra is a ring S (not necessary commutative) with a ring homomorphism ϕ from R to the center of S.

This induces an $R-$module structure on S by the operation

$$r.s = \phi(r)s \text{for all } r \in R, s \in S.$$

Then any $R-$ algebra can be viewed as an $R-$ module.

In most of the cases, we are interested in the following examples of algebras.

1.3.9 Example. Let R be a Dedekind domain and G a finite group. The group ring RG is an R-algebra.

Denote by $\mathrm{Map}(G, R)$ the set of all functions from G to S. It is a ring via the operations:

$$(f + g)(\sigma) = f(\sigma) + g(\sigma), (fg)(\sigma) = f(\sigma)g(\sigma) \text{ for all } f, g \ \mathrm{Map}(G, R), \sigma \in G$$

Consider the map $\phi : R \to \mathrm{Map}(G, R)$ defined by $\phi(r)(\sigma) = r.1$, the constant map, for $r \in R, \sigma \in G$. It makes $\mathrm{Map}(G, R)$ into $R-$algebra.

If we let G act on it by $(\sigma.f)(g) = f(g\sigma)$ for $\sigma, g \in G$ and $f \in \mathrm{Map}(G, R)$, it becomes an $RG-$module. So, we have an isomorphism of $RG-$modules:

$$\mathrm{Map}(G, R) \simeq RG$$

via the map $f \mapsto \sum_{g \in G} f(g)g^{-1}$. In other words, $\mathrm{Map}(G, R)$ is the dual of the $R-$algebra RG.

1.3.10 Definition. Let R be a commutative ring and S an $R-$algebra. We say that S is an extension of the ring R if S is commutative $R-$algebra and faithful as $R-$module.

Recall that an $R-$module M is faithful if 0 is the only annihilator of M.

Let H be a group and S a ring on which H acts. Set

$$S^H := \{x \in S / \sigma(x) = x, \ \forall \sigma \in H\}.$$

1.3.11 Definition. Let R be a commutative ring and S a commutative $R-$algebra. Let G be a finite group acting on S.

The extension S of R is said to be Galois with group G if $R = S^G$ and the map

$$r_{S,G} : S \otimes_R S \to \mathrm{Map}(G, S)$$

given by $a \otimes b \mapsto (a \otimes b)(\sigma) = a\sigma(b)$ is an isomorphism of left $S-$modules, where $\mathrm{Map}(G, S)$ is defined in the Example 1.3.9.

1.3.12 Example. We show that if S and R are fields, then this definition is the same as the usual definition of Galois extension of fields.
Take $S = N, R = E$ where N/E is finite Galois extension of fields with group G. Before proving the equivalence of the definitions, we need the Dedekind's lemma on the linearly independence of homomorphisms of algebras.

1.3.13 Lemma. Let N/E and L/E be field extensions. The set of distinct $E-$ algebra homomorphisms from N to L is linearly independent over L.

Proof. Suppose that the sequence $(\varphi_i)_{i\in I}$ of $E-$algebra homomorphisms is linearly dependent. Then, there exists a minimal integer $n \geq 2$ such that

$$\sum_{i=1}^{n} a_i\varphi_{j_i} = 0 \text{ where } a_i \neq 0 \in L. \tag{1.1}$$

Since $\varphi_{j_1} \neq \varphi_{j_n}$, then there exists $\alpha \in L$ such that $\varphi_{j_1}(\alpha) \neq \varphi_{j_n}(\alpha)$. For all $\beta \in L$, we have

$$\sum_{i=1}^{n} a_i\varphi_{j_i}(\alpha\beta) = \sum_{i=1}^{n} a_i\varphi_{j_i}(\alpha)\varphi_{j_i}(\beta) = 0 \tag{1.2}$$

Multiplying through 1.2 by $\varphi_{i_n}(\alpha)$, we get

$$\varphi_{i_n}(\alpha)\sum_{i=1}^{n} a_i\varphi_{j_i}(\beta) = 0 \tag{1.3}$$

((1.2)) - (1.3) gives us

$$\sum_{i=1}^{n-1} (a_i\varphi_{j_1}(\alpha) - \varphi_{i_n}(\alpha))\varphi_{j_i}(\beta) = 0.$$

Since $\varphi_{j_1}(\alpha) - \varphi_{i_n}(\alpha)) \neq 0$, this contradicts the minimality of n. Thus $(\varphi_i)_{i\in I}$ is linearly independent over L. □

Claim. *Let N/E be a field extension and let G be a finite group of $K-$automorphisms of N. Suppose that $N^G = E$, then the extension N/E is Galois(in the sens of the Definition 1.3.11)with group G if and only if G acts faithfully on N.*

In fact, if N/E is galois, the composition $r_{N,G} \circ (1 \otimes id_N)$ allows us to embed N in $\mathrm{Map}(G, N)$, and this implies that G acts faithfully on N.

Conversely, since $dim_N(N \otimes_E N) = dim_N(\mathrm{Map}(G, N)) = |G|$, it is sufficient to prove that $r_{N,G}$ is injective. Let $\sum_{\text{finite}} a_i \otimes b_i \in \ker(r_{N,G})$. Then for every $\sigma \in G$, we have

$$\sum_{\text{finite}} a_i\sigma(b_i) = 0$$

If G acts faithfully on N, then by the Lemma1.3.13, the matrix $(\sigma(b_i))_{\sigma,i}$ is invertible, then the above system of equations in a_i's has only the trivial solution. Thus, our claim follows.

Now, suppose that R is a Dedekind domain with fractional field E and S is its integral closure in Galois extension N of E. We have seen that N/E is Galois in the sens of Definition 1.3.11. A natural question is, do we have Galois extension for the ring of integers S/R. In general, the answer is no. The following proposition will tell us when the extension of ring of integers is Galois if their fractional fields is Galois extension. In order to do this, we have to introduce some definitions in extension of rings.

For a prime $\mathfrak{p}$ of R, we denote by $R_{(\mathfrak{p})}$ the localisation of R at $\mathfrak{p}$ and by $k(\mathfrak{p})$ the residue field of $\mathfrak{p}$, that is $R_{(\mathfrak{p})}/\mathfrak{p}R_{(\mathfrak{p})}$.

1.3.14 Definition. Let S be an $R-$algebra such that S is finitely generated as $R-$module. The extension, S/R is unramified if for every prime ideal $\mathfrak{p}$ of R and all prime ideals $\mathfrak{q}$ of S such that $\mathfrak{q} \cap R = \mathfrak{p}$ we have:

1 $\mathfrak{p}S = \mathfrak{q}S$

2 the residue field extension $k(\mathfrak{q})/k(\mathfrak{p})$ is separable.

We see that if R and S are ring of integers of extensions of fields N/E, respectively, then the extension S/R unramified is the same as the field extension N/E is unramified in the usual sens of unramified extension.

Now, consider the map $\mu : S \otimes_R S \to S$ given by $x \otimes y \mapsto xy$. Define by $J(S) := \ker(\mu)$.
So we have an exact sequence of $S \otimes_R S$-modules

$$0 \to J(S) \to S \otimes_R S \to S \to 0$$

where the $S \otimes_R S-$module structure on S is given by $(x \otimes y)s = xsy = xys$ for all $x, y, s \in S$.

1.3.15 Definition. The extension S/R is separable if there exists $e \in S \otimes_R S$ such that $\mu(e) = 0$ and $J(S)e = 0$. Such an element is called the separability idempontent.

Again, we recover the usual notion of separability for commutative finite dimensional algebras over a field.

1.3.16 Example. Let R be a commutative ring and G a finite group whose order is unit in R. The R-algebra RG is separable by taking $e = \frac{1}{n} \sum_{g \in G} g \otimes g^{-1}$.

1.3.17 Definition. The details of this can be seen in [I.R03]. Let K be a field and A a finite dimensional semisimple $K-$algebra. We are especially interested in the case $A = KG$, the group ring algebra of a finite group G over K.

Let R be a Dedekind ring with fractional field K. An $R-$ order in A is a subring Λ of A such that R is contained in the center of Λ, Λ is finitely generated as $R-$module and $K\Lambda = A$, that is, Λ contains an $K-$basis of A.

For example, the integral group RG is an $R-$order in the $K-$algebra KG. Indeed, R can be identified with $R.1$ in RG and it is contained in the center of RG. It is finitely generated $R-$module since G is finite. Of course, $KRG = KG$.

1.3.18 Definition. An order in the semisimple algebra A is said to be maximal order if it is not properly contained in any other order of A.

1.3.19 Proposition. Let R be a Dedekind ring and let E be its field of fractions. Let N/E be a Galois extension with group G and let S be the integral closure of R in N. The following are equivalent:

a. S/R is Galois with group G.

b. S/R is unramified.

Proof. We prove the equivalence using the determinant. We know that S/R is unramified is the same as N/E is unramified. From the basic result in number theory, for example ([FT91] p.121), we know that N/E is unramified if and only if the dicriminant $d(S/R)$ is R.

The integral closure of R in $\mathrm{Map}(G, N)$ is $\mathrm{Map}(G, S)$. Since $\mathrm{Map}(G, N) \simeq NG$ is separable (Example1.3.16), and $\mathrm{Map}(G, S)$ is finitely generated over R so it is the maximal order in $\mathrm{Map}(G, N)$.

Since N/E is Galois, then

$$r_{N,G} : N \otimes_E N \to \mathrm{Map}(G, N)$$

is an isomorphism. In particular, its restriction to $S \otimes_R S$ is injective and we have an injection

$$r_{S,G} : S \otimes_R S \hookrightarrow \mathrm{Map}(G, S).$$

If S/R is Galois, then $r_{S,G}$ is an isomorphism. The discriminant of $\mathrm{Map}(G, N)$ over R is R so, by the formula for discrimininants applied to the inclusions

$$R \subseteq S \subseteq S \otimes_R S$$

we deduce that the discriminant of S over R is R as well. Hence S/R is unramified. The converse will follow immediately from the next lemma.

1.3.20 Lemma. Let $S_1/R, S_2/R,$ be extensions of Dedekind rings. Let N_i be the field of fractions of $S_i, i = 1, 2$. If S_1/R is unramified, then $S_1 \otimes S_2$ is the maximal order in $N_1 \otimes_E N_2$, where E is the fractional field of R.

Proof. Let $\mathcal{O}$ be the maximal order in $N_1 \otimes_E N_2$. We have the following inclusions

$$S_2 \subseteq S_1 \otimes_R S_2 \subseteq \mathcal{O}$$

and the property of discriminant see ([FT91] pages.121) gives that:

$$d(S_1 \otimes_R S_2/S_2) = [\mathcal{O} : S_1 \otimes_R S2]^2 d(\mathcal{O}/S_2).$$

Hence, $d(S_1 \otimes_R S_2/S_2) \subseteq d(\mathcal{O}/S_2) \subseteq S_2$. On the other hand, $d(S_1 \otimes_R S_2/S_2) = d(S_1/R)S_2$. By assumption, $d(S_1/R) = R$, so $d(S_1 \otimes_R S_2/S_2) = S_2$. It follows that $\mathcal{O} = S_1 \otimes_R S_2$.
We will use later this lemma several times. □

For the proof of the theorem, we apply the lemma with $S_1 = S_2 = S$. So the maximal order of $N \otimes_E N$ is $S \otimes_R S$ and the equivalence follows. □

Representation of finite group

Notes here can be seen in [Ser71].

Let V be a vector space over a field K. The general linear group $\mathrm{GL}(V)$ is the set of all automorphisms of V viewed as group under composition. If V has finite dimensional n, then $\mathrm{GL}(V) = GL_n(K)$, which is the group of invertible $n \times n$ matrix with entries in K.

1.3.21 Definition. A representation of group G is a homomorphism $\rho : G \to GL(V)$. We say that V is faithful if ρ is injective, and we say V is trivial if $\rho = 1$.

Recall that an KG-module is a vector space over K together with group action, that is, $\forall g \in G, \alpha \in K, u, v \in V$, the operation $g.v$ is defined and satisfies:

- $g.(u + v) = g.u + g.v$
- $g.(\alpha u) = \alpha(g.u)$.

  We now let $g.v = \rho(g)v$. Sometimes, we call V the representation of G instead of ρ. So ρ gives V the structure of $FG-$module.

A subrepresentation of V is a subspace W which is invariant under the action of G, that is

$$\forall g \in G, w \in W, g.w = \rho(g)w \in W.$$

A representation V is said to be irreducible or simple if the only subrepresentation of V are V and $\{0\}$.

1.3.22 Definition. Let V and W representations of G. A function $\phi : V \to W$ is called $G-$linear map or $G-$invariant if it is a linear transformation and satisfies:

$$\phi(g.v) = g.\phi(v), \forall v \in V, g \in G$$

We say that two representations V and W are isomorphic if there axists a $G-$linear map $\phi : V \to W$ that is invertible.

1.3.23 Lemma. Let W, V be representations of G and $\phi : V \to W$ a $G-$linear map. Then, $\ker(\phi)$ is a subrepresentaion of V and $\phi(V)$ is a subrepresentaion of W.

Proof. Let $g \in V$ and $v \in \ker \phi$. Then $\phi(g.v) = g\phi(v) = 0$, hence $g.v \in \ker \phi$. Take $g \in G, w \in \phi(V) \subset W$. There exists $u \in V$ such that $\phi(u) = w$. Thus, $g.w = g.\phi(u) = \phi(g.u) \in \phi(V)$. □

1.3.24 Lemma. (Maschke's theorem) Let V be a representation of finite group G and the order of G is a unit in K. If there exists a subrepresentation W of V, then there must also be U subrepresentation of V such that $V = U \oplus W$.

Proof. Suppose that there is a subrepresentation W of V. Choose any complementary subspace S of V such that $V = W \oplus S$. Then an element $v \in V$ can be written as $v = w + s$ where $w \in W, s \in S$. Consider the projection $p : V \to W$ of V on W sending $v \mapsto w$. Let $\pi(v) = \frac{1}{|G|}\sum_{g\in G} g^{-1}p(g.v)$. We need to show that π is a $G-$linear map. For $u, v \in V$ write $u = w_0 + s_0, v = w_1 + s_1$.

$$\begin{aligned}\pi(u+v) &= \frac{1}{|G|}\sum_{g\in G} g^{-1}p(g.(v+w)) \\ &= \frac{1}{|G;|}\sum_{g\in G} g^{-1}p(g.w_0 + g.s_0 + g.w_1 + g.s_1)) \\ &= \frac{1}{|G|}\sum_{g\in G} g^{-1}(g.w_0 + g.w_1) \\ &= \pi(u) + \pi(v).\end{aligned}$$

Let $\lambda \in K, u \in V, \pi(\lambda u) = \frac{1}{|G|}\sum_{g\in G} g^{-1}p(g.(\lambda u)) = \frac{1}{|G|}\lambda\sum_{g\in G} g^{-1}p(g.u) = \lambda\pi(u)$.
Let $h \in G, u \in V$.

$$\begin{aligned}\pi(h.u) &= \frac{1}{|G|}\sum_{g\in G} g^{-1}(g.(h.u)) \\ &= \frac{1}{|G|}\sum_{g\in G} g^{-1}(gh).u)) \\ &= \frac{1}{|G|}\sum_{d\in G} hd^{-1}(d.u)) \\ &= h\pi(u).\end{aligned}$$

Hence, π is a $G-$linear map. It is easy to see that $\pi(W) = W$. By the previous lemma, $\ker \pi$ is also a subrepresentation of V. It follows the conclusion by taking $U = \ker \pi$. □

1.3.25 Definition. A representation V of G is called completely reducible or semisimple if V can be written as direct sum of irreducible subrepresentations.

1.3.26 Corollary. If the $\text{char}(K)$ does not divide the order of the group G, then every representation of G is completely reducible.

Proof. Just argue by induction on dimension of V. □

Character theory

1.3.27 Definition. Let V be a representation of a group G. The character associated to V is a map $\chi : G \to K$ defined by $g \mapsto \mathrm{Tr}(g.v)$, where Tr means the trace of the action of g on v.
Note that χ does not depend on the choice of the basis of V. We say that a character is irreducible if the associated representation is irreducible. The trivial character of G is the character $\chi(g) = 1$ for all $g \in G$.

If G is finite of order n, a character χ of G takes values in the n^{th} roots of unity μ_n.

1.3.28 Theorem. *Let U, V be two irreducible representations with characters χ_1, χ_2, respectively. Set $W = U \oplus W$. Then the character χ associated to W is $\chi_1 + \chi_2$ and the character associated to $U \otimes V$ is $\chi_1\chi_2$.*

Proof. Let $u_1, \dots, u_n$ be a basis of U and $v_1, \dots, v_m$ a basis of V, then $u_1, \dots u_n, v_1, \dots, v_m$ form a basis of W. Hence, the matrix of $g.v$ for $g \in G, w = u + v \in W$ with respect to this basis has the form:

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$$

where the matrix A is the matrix of $g.u$ with respect to the basis u_i, and B the matrix of $g.v$ in the basis v_i. The second assertion follows from Theorem 1.3.30 below. □

Using Proposition 1.3.28, the set of charcters of a finite group G form a ring.

Induced character

Let H be a subgroup of a finite group G, K a field. Then KH is a subring of KG and the latter is an $(KG - KH-)$bimodule. So, for any left $KH-$module M, we have a left $KG-$module $KG \otimes_{KH} M$ which is the extension of scalar from KH to KG.

1.3.29 Definition. Let H be a subgroup of the finite group G, and let M be an $KH-$module affording the representation ρ of H. The $KG-$module $KG \otimes_{KH} M$ is called the induced module of M and the representaion of G it affords is the induced representation of ρ. If χ is the character of ρ, then the character of the induced representation is called the induced character, and we denote by $Ind_H^G(\chi)$.

1.3.30 Theorem. *Let H be a subgroup of the finite group G and let $g_1, \dots, g_n$ be representatives of the distinct left cosets of H in G. Let V be an $KH-$module with matrix representation ρ of H of dimension n. Denote by $W = KG \otimes_{KH} V$. There is a basis of W such that the matrix of $\varphi(g), g \in G$ with repesct to that basis has of the form:*

$$\begin{pmatrix} \triangle_{11} & \cdot & \cdot & \cdot & \triangle_{1n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \triangle_{m1} & \cdot & \cdot & \cdot & \triangle_{mn} \end{pmatrix}$$

where $\triangle ij = \rho(g_i^{-1}gg_j)$ is an $n \times n$ block appearing in the i, j block position of $\varphi(g)$ and $\rho(g_i^{-1}gg_j)$ is the zero matrix if $g_i^{-1}gg_j \notin H$.

Proof. We know that KG is free right $KH-$module of rank n and we have

$$KG = KHg_1 \oplus \cdots \oplus KHg_n.$$

Since tensor product commutes with direct sum, we have

$$W = KG \otimes_{KH} V \simeq (g_1 \otimes_{KH} V) \oplus \cdots \oplus (g_n \otimes_{KH})V$$

Since K is the center of KG, then KG is a vector space over K and the above isomorphism is a $K-$ ismorphism as well. Then if $v_1, \dots v_m$ is basis of V then $B = \{v_i \oplus g_j\}_{i,j}$ is a basis of W.

Let us now compute the matrix of $\rho(g), g \in G$ with respect to the basis B. Fix j and write $gg_j = g_i h$, for some index i and some $h \in H$. For every k,

$$\begin{aligned} g(g_j \otimes v_k) &= (gg_j) \otimes v_k = g_i \otimes hv_k \\ &= \sum_{r=1}^{m} a_{rk}(h)(g_i \otimes v_r), \end{aligned}$$

where a_{rk} is the r, k coefficients of the matrix h acting V with respect to the basis $v_1, \ldots, v_m$, that is, the action of g on W maps the j^{th} block of n basis vectors of W to the i^{th} block of basis vector, and then the matrix of $\rho(h)$ on that block. Since $h = g_i^{-1} g g_j$ thus, we get the desired matrix of W. □

1.3.31 Corollary. If χ is the charcter of V, then the induced character of W is given by

$$Ind_H^G(\chi) = \sum_{x \in G} \chi(x^{-1} g x)$$

1.4 Completions, unramified and totally ramified extensions

If E is a field of fractions of a Dedekind domain R, then every non-zero prime ideal $\mathfrak{p}$ is associated the $\mathfrak{p}-$adic valuation $v_\mathfrak{p}$ of E defined by $v_\mathfrak{p}(a) = v_\mathfrak{p}$ where $(a) = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}}$. The valuation ring of $v_\mathfrak{p}$ is the localization of R at $\mathfrak{p}$. If S is the integral closure of R in any extension field N of E, and if $\mathfrak{p}S = \mathfrak{q}_1^{e_1} \ldots \mathfrak{q}_r^{e_r}$ is the prime decomposition of $\mathfrak{p}$ in N, then the valuation $w_i = \frac{1}{e_i} v_{\mathfrak{q}_i}, i = 1, \ldots, r$ are precisely the extensions of $v = v_\mathfrak{p}$ to N, e_i are the corresponding ramification indices and $f_i = [S/\mathfrak{q}_i : R/\mathfrak{p}]$ are the inertia degree.

Suppose now that N/E is Galois number fields extensions with group G. For each prime $\mathfrak{q}$ of S and a prime $\mathfrak{p}$ of R, we denote by $N_\mathfrak{q}$ the completion of N with respect to $v_\mathfrak{q}$ and $E_\mathfrak{p}$ the completion of E at $v_\mathfrak{p}$. We denote by $D_\mathfrak{q}$ (resp. $I_\mathfrak{q}$) the decomposition group (resp. inertia group) of $\mathfrak{q}$ in G.

If V is a finite dimension E-vector space, we denote by $V_\mathfrak{p} := E_\mathfrak{p} \otimes_E V$ its completion with respect to $v_\mathfrak{p}$. In the same way, for any finitely generated R module M, we denote its completion with respect to $v_\mathfrak{p}$ by $M_\mathfrak{p} := R_p \otimes_R M$.

In case $V = N$, if $\mathfrak{p}S = \mathfrak{q}_1^{e_1} \ldots \mathfrak{q}_s^{e_s}$ is the factorisation of prime ideals of p in S, we still denote it by $N_\mathfrak{p}$ but it is different from $N_\mathfrak{q}$, which is the completion of N with respect to $v_\mathfrak{q}$ where $\mathfrak{q}$ is a prime ideal of S. The difference will be clear because we will always use $\mathfrak{p}$ for a prime of R and $\mathfrak{q}$ for that of S. So, $N_\mathfrak{p}$ may not be a field but it is only an $E-$algebra. The next lemma gives information on $N_\mathfrak{p}$.

1.4.1 Lemma ([Ser79] Theorem 1, Proposition 4, Pages 31-32)**.** We have isomorphism of $E-$ algebras

$$E_\mathfrak{p} \otimes_E N \simeq \prod_{i=1}^{s} N_{\mathfrak{q}_i}$$

and isomoprhism of R-modules

$$R_\mathfrak{p} \otimes S \simeq \prod_{i=1}^{s} S_{\mathfrak{q}_i}$$

where $N_{\mathfrak{q}_i}, S_{\mathfrak{q}_i}$ are the completions of N and S at $\mathfrak{q}_i$, respectively.

Since G acts transitively on the set of primes of S above $\mathfrak{p}$ [[Ser79],Prposition 19,p.20], we can define an action of G on the $E-$ algebra $E_\mathfrak{p} \otimes_E N \simeq \prod_{i=1}^{s} N_{\mathfrak{q}_i} = \prod_{\mathfrak{q}|\mathfrak{p}} N_\mathfrak{q}$ as follows: for $(x_\mathfrak{q})_{\mathfrak{q}|\mathfrak{p}}$ and $g \in G$, the $\mathfrak{q}_0^{th}$ component of $g.(x_\mathfrak{q})_{\mathfrak{q}|\mathfrak{p}}$ is given by $g(x_{g^{-1}(\mathfrak{q}_0)})$, for any $\mathfrak{q}_0$ prime of S above $\mathfrak{p}$. Precisely,

$$\big(g.(x_\mathfrak{q})_{\mathfrak{q}|\mathfrak{p}}\big)_{\mathfrak{q}_0} = g(x_{g^{-1}(\mathfrak{q}_0)}).$$

Using the same notation as in the example 1.3.9, consider $\mathrm{Map}(G, N_{\mathfrak{q}})$ the set of all functions from G to N and define the action of G to be $(g.f)(\sigma) = f(\sigma g), f \in \mathrm{Map}(G, N_{\mathfrak{q}}), \sigma, g \in G$. Define $\mathrm{Map}(G, N_{\mathfrak{q}})^{D_{\mathfrak{q}}}$, the set of all elements in $\mathrm{Map}(G, N_{\mathfrak{q}})$ fixed by the action of H, that is:

$$\mathrm{Map}(G, N_{\mathfrak{q}})^{D_{\mathfrak{q}}} := \{f : G \to N_{\mathfrak{q}}, f(hg) = h(f(g)), h \in D_{\mathfrak{q}}, g \in G\}$$

1.4.2 Lemma. For any prime $\mathfrak{q}_0$ of S above $\mathfrak{p}$, the above $S-$ isomorphisms induce isomorphisms of $EG-$ modules and $RG-$modules:

$$\prod_{\mathfrak{q}|\mathfrak{p}} N_{\mathfrak{q}} \simeq \mathrm{Map}(G, N_{\mathfrak{q}_0})^{D_{\mathfrak{q}_0}} \text{ and } R_{\mathfrak{p}} \otimes S \simeq \prod_{\mathfrak{q}|\mathfrak{p}} S_{\mathfrak{q}_i} \simeq \mathrm{Map}(G, S_{\mathfrak{q}_0})^{D_{\mathfrak{q}_0}}$$

given by $(x_{\mathfrak{q}})_{\mathfrak{q}|\mathfrak{p}} \mapsto (x_{\mathfrak{q}})_{\mathfrak{q}|\mathfrak{p}}(g) = g\left(x_{g^{-1}(\mathfrak{q}_0)}\right)$.

Proof. We only need to show that this is well defined, that is, we have to prove that $(x_{\mathfrak{q}})_{\mathfrak{q}|\mathfrak{p}}(hg) = h((x_{\mathfrak{q}})_{\mathfrak{q}|\mathfrak{p}}(g))$ for any $h \in D_{\mathfrak{q}}, g \in G$.

Let $h \in D_{\mathfrak{q}}, g \in G$, then $(x_{\mathfrak{q}})_{\mathfrak{q}|\mathfrak{p}}(hg) = hg(x_{g^{-1}h^{-1}(\mathfrak{q}_0)}) = hg(x_{g^{-1}(\mathfrak{q}_0)}) = h(g(x_{g^{-1}(\mathfrak{q}_0)})) = h((x_{\mathfrak{q}})_{\mathfrak{q}|\mathfrak{p}}(g))$. The second equality follows from the fact that $h^{-1}(\mathfrak{q}_0) = \mathfrak{q}_0$ since $h \in D_{\mathfrak{q}_0}$. □

Note that these are still true for any finite dimensional vector space V over N on which G acts and any finitely generated S-module M on which G acts, that means, we have also $RG-$isomoprhisms for M and $EG-$isomorphism for V for any prime $\mathfrak{q}_0$ of S above $\mathfrak{p}$.

$$M \otimes_R R_{\mathfrak{p}} \simeq \prod_{\mathfrak{q}|\mathfrak{p}} M_{\mathfrak{q}} \simeq \mathrm{Map}(G, M_{\mathfrak{q}_0})^{D_{\mathfrak{q}_0}} \text{ and } M \otimes_R E_{\mathfrak{p}} \simeq \prod_{\mathfrak{q}|\mathfrak{p}} V_{\mathfrak{q}} \simeq \mathrm{Map}(G, V_{\mathfrak{q}_0})^{D_{\mathfrak{q}_0}}$$

1.4.3 Lemma. [[Ser79], Corollary 4, p.31] The extension $N_{\mathfrak{q}}/E_{\mathfrak{p}}$ is Galois with group $\mathrm{Gal}(N_{\mathfrak{q}}/E_{\mathfrak{p}}) \simeq D_{\mathfrak{q}}$. Moreover, if $F = N_{\mathfrak{q}}^{I_{\mathfrak{q}}}$ is the fixed field of the inertia group of $\mathfrak{q}$, then $N_{\mathfrak{q}}/F$ is totally ramified and $F/E_{\mathfrak{p}}$ is unramified.

1.4.4 Definition. Let $\mathfrak{p}$ be a prime ideal of R and $\mathfrak{q}$ a prime ideal of S above $\mathfrak{p}$. We say that the extension N/E is tame (or tamely ramified) at $\mathfrak{q}$ if the ramification index $e(\mathfrak{q}/\mathfrak{p})$ does not divide the characteristic of the residue field $R/\mathfrak{p}$ and the extension $S/\mathfrak{q}$ of $R/\mathfrak{p}$ is separable. We say that the extension N/E is tame if it is tame at all primes $\mathfrak{q}$.

1.4.5 Lemma. [[FT91], Theorem 26,p.140] Let K/k be a finite Galois extension of local fields with valuation ring $\mathcal{O}_K$ and $\mathcal{O}_k$, respectively. Then the following are equivalent:

- K/k is tamely ramified.
- $\mathrm{Tr}_{K/k}(\mathcal{O}_K) = \mathcal{O}_k$, where Tr is the trace map of K over k.
- $\mathcal{C}_{K/k} = \mathfrak{p}_K^{-e+1}$, where $\mathfrak{p}_K$ is the prime ideal of $\mathcal{O}_K$ and $\mathcal{C}_{K/k}$ is the inverse different of K over k.

1.4.6 Proposition. [[FT91, **?**, **?**]]Let K/k be a totally ramified tame extension of a discrete complete local field. Then there exists a primitive element π_k of k such that $\pi_K^e = \pi_k$ where $e = e_{K/k} = [K : k]$. (That is, $\pi_K^e = \pi_k$ for these elements, not only $(\pi_K)^e = (\pi_k)$ for the ideals.)

Proof. For π_k and π_K we have $\pi_K^e = \pi_k\eta$ for some $\eta \in \mathcal{O}_K^\times$. Since the extension is totally ramified, $\bar{K} : \mathcal{O}_K/\mathfrak{p}_K = \bar{k} := \mathcal{O}_k/\mathfrak{p}_k$. So there exists $\theta \in \mathcal{O}_k^\times$ such that $\eta \equiv \theta \pmod{\pi_K}$. Replacing π_k with $\pi_k\theta$ and η with η, θ^{-1}, we may assume $\eta \equiv 1 \pmod{\pi_K}$.

Claim. *If* $\mathrm{char}\,\bar{K} \nmid m$, *then every* $\alpha \in \mathcal{O}_K$ *satisfying* $\alpha \equiv 1 \pmod{\pi_K}$ *is an* m*-th power.*

(Indeed, we can apply Hensel to the polynomial $f(X) = X^m - \alpha$ and $\alpha_0 = 1$; by the assumption $f'(\alpha_0) = m \not\equiv 0 \pmod{\mathrm{char}(\bar{K})}$.)

The claim can be applied since K/k is tame. So η is an e-th root, $\eta = \epsilon^e$ for some $\epsilon \in \mathcal{O}_K^\times$. Replacing π_K with $\pi_K\,\epsilon^{-1}$, we obtain $\pi_K^e = \pi_k$. □

1.4.7 Theorem. *If K/k is Galois totally ramified tame extension of a discrete complete local field with group Γ, then K/k is cyclic and k contains the e^{th} roots of unity.*

Proof. Since K/k is totally ramified, the Galois group Γ coincides with the inertia group Γ_0. Consider the map

$$\begin{aligned} \theta\colon \Gamma &\to \overline{K}^\times := \mathcal{O}_K/(\pi_K)^\times, \\ \sigma &\mapsto \frac{\pi_K}{\sigma(\pi_K)} (\bmod\ \pi_K), \end{aligned}$$

where (π_K) is the prime ideal of $\mathcal{O}_K$. Note that θ does not depend on the choice of the uniformizer π_K. In fact, if π is an other uniformizer of $\mathcal{O}_K$, then there exists $\eta \in \mathcal{O}_K^\times$ such that $\pi_K = \pi\eta$. By assumption, $\overline{K} = \overline{k}$, so there exists $\mu \in \mathcal{O}_k$ such that $\eta \equiv \mu \bmod \pi_K$. Hence, we have

$$\theta(\sigma) = \sigma(\pi_K^{-1})\pi_K \bmod \pi_K = \sigma(\pi^{-1}\eta^{-1})\pi\eta \equiv \sigma(\pi^{-1}\mu^{-1})\pi\mu \equiv \sigma(\pi^{-1})\pi \bmod \pi_K.$$

It is easy to see that θ is a homomorphism. Since the extension is tame, one can show that $\ker\theta = \Gamma_1 = \{1\}$, where Γ_1 is the ramification group. Hence θ is injective, so it can be identified with a subgroup of the multiplicative group $\overline{K}^\times$, so Γ is cyclic. Since the extension is totally ramified, we have in particular that $\overline{k}$ contains the e^{th} roots of unity. Since $X^e - 1$ is separable over $\overline{k}^\times$, these roots of unity can be lifted to k by Hensel's lemma, and it completes the proof. □

1.4.8 Theorem. *(Chinese Remainder theorem) Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be ideals in a commutaive ring R such that $\mathfrak{a}_i + \mathfrak{a}_j = R$, for $i \neq j$. Let M be an $R-$module. Then there is an isomorphism of R-modules*

$$\frac{M}{\bigcap_{i=1}^n \mathfrak{a}_i M} \simeq \oplus_{i=1}^n \frac{M}{\mathfrak{a}_i M}$$

Proof. For each K, $\bigcap_{i=1}^n \mathfrak{a}_i M \subset \mathfrak{a}_k M$, so there is a map

$$\frac{M}{\bigcap_{i=1}^n \mathfrak{a}_i M} \to \frac{M}{\mathfrak{a}_k M}$$

Therefore, there is a map

$$\frac{M}{\bigcap_{i=1}^n \mathfrak{a}_i M} \to \oplus_{i=1}^n \frac{M}{\mathfrak{a}_i M}$$

Since $\mathfrak{a}_i + \mathfrak{a}_j = R$ for all $i \neq j$, then a prime ideal $\mathfrak{p}$ of R can contain at most one ideal $\mathfrak{a}_i$ and $(\mathfrak{a}_i M)_\mathfrak{p} = M_\mathfrak{p}$ if $\mathfrak{a}_i \not\subseteq \mathfrak{p}$. Thus, if $\mathfrak{a}_k \subset \mathfrak{p}$, then $(\bigcap_{i=1}^n \mathfrak{a}_i M)_\mathfrak{p} = (\mathfrak{a}_k M)_\mathfrak{p}$ and $M_\mathfrak{p}/\mathfrak{a}_i M_\mathfrak{p} = 0$ if $i \neq k$. Therefore, for all prime $\mathfrak{p}$, we have an isomorphism

$$M_\mathfrak{p}/\mathfrak{a}_k M_\mathfrak{p} = \left(\frac{M}{\bigcap_{i=1}^n \mathfrak{a}_i M}\right)_\mathfrak{p} \to \left(\oplus_{i=1}^n \frac{M}{\mathfrak{a}_i M}\right)_\mathfrak{p} = (M/\mathfrak{a}_k M)_\mathfrak{p}$$

This is for all prime $\mathfrak{p}$, so the result follows from the fact that f is an isomorphism of $R-$modules if and only if the localised function $f_\mathfrak{p}$ is an isomorphism for all prime $\mathfrak{p}$ of R. □

1.4.9 Theorem. *(Analogue of the Chinese Remainder theorem) Let $\mathfrak{a}_1, \mathfrak{a}_2$ be ideals of a Dedekind ring R such that $\mathfrak{a}_1 + \mathfrak{a}_2 = R$. Then there is an isomorphism of $R-$modules:*

$$\frac{(\mathfrak{a}_1\mathfrak{a}_2)^{-1}}{R} \simeq \frac{\mathfrak{a}_1^{-1}}{R} \times \frac{\mathfrak{a}_2^{-1}}{R}.$$

Proof. We claim that the inclusions $\mathfrak{a}_1^{-1} \to (\mathfrak{a}_1\mathfrak{a}_2)^{-1}$ and $\mathfrak{a}_1^{-2} \to (\mathfrak{a}_1\mathfrak{a}_2)^{-1}$ induce $R-$modules isomorphisms

$$f_1 : \frac{\mathfrak{a}_1^{-1}}{R} \to \frac{(\mathfrak{a}_1\mathfrak{a}_2)^{-1}}{\mathfrak{a}_2^{-1}} \text{ and } f_2 : \frac{\mathfrak{a}_1^{-1}}{R} \to \frac{(\mathfrak{a}_1\mathfrak{a}_2)^{-1}}{\mathfrak{a}_1^{-1}}$$

and the natural projections $\frac{(\mathfrak{a}_1\mathfrak{a}_2)^{-1}}{R} \to \frac{(\mathfrak{a}_1\mathfrak{a}_2)^{-1}}{\mathfrak{a}_2^{-1}}$ and $\frac{(\mathfrak{a}_1\mathfrak{a}_2)^{-1}}{R} \to \frac{(\mathfrak{a}_1\mathfrak{a}_2)^{-1}}{\mathfrak{a}_1^{-1}}$ induce an $R-$isomorphism.

$$f : \frac{(\mathfrak{a}_1\mathfrak{a}_2)^{-1}}{R} \to \frac{(\mathfrak{a}_1\mathfrak{a}_2)^{-1}}{\mathfrak{a}_2^{-1}} \times \frac{(\mathfrak{a}_1\mathfrak{a}_1)^{-1}}{\mathfrak{a}_2^{-1}}$$

- Injectivity of f_1, f_2, f.

  Note that $\ker f_1 = \ker f_2 = \ker f = \dfrac{\mathfrak{a}_1^{-1} \bigcap \mathfrak{a}_2^{-1}}{R}$.

  To prove their injectivity, we have to prove that $\mathfrak{a}_1^{-1} \bigcap \mathfrak{a}_2^{-1} = R$. The inclusion $R \subset \mathfrak{a}_1^{-1} \bigcap \mathfrak{a}_2^{-1}$ is clear since $\mathfrak{a}_i, i = 1, 2$ are ideals of R. To prove the converse inclusion, take $x \in \mathfrak{a}_1^{-1} \cap \mathfrak{a}_2^{-1}$. Since $\mathfrak{a}_1 + \mathfrak{a}_2 = R$, and $1 \in R$, we can write $1 = a + b$ for $a \in \mathfrak{a}_1, b \in \mathfrak{a}_2$. Thus $x.1 = xa + xb$. Since $x \in \mathfrak{a}_1^{-1} \bigcap \mathfrak{a}_2^{-1} \subset \mathfrak{a}_1^{-1}$ and $a \in \mathfrak{a}_1$, then $xa \in \mathfrak{a}_1^{-1}a \in \mathfrak{a}_1 = R$. Similarly, $xb \in R$. Hence $x = xa + xb \in R$. Thus f_1, f_2, f are injective.

- Surjectivity of f_1, f_2.

  We only prove the surjectivity of f_1 since the proof of that of f_2 is similar. Let $y \in (\mathfrak{a}_1\mathfrak{a}_2)^{-1}$, then $y.1 = ya + yb$. Since $y \in (\mathfrak{a}_1\mathfrak{a}_2)^{-1}$ and $a \in \mathfrak{a}_1$, then $ya \in \mathfrak{a}_2^{-1}$, therefore $y - ya$ and y have the same image in $\dfrac{(\mathfrak{a}_1\mathfrak{a}_2)^{-1}}{\mathfrak{a}_2^{-1}}$. On the other hand $y - ya = yb \in \mathfrak{a}_2^{-1}$, hence $y = f_1(yb)$ and this shows that f_1 is surjective.

- Surjectivity of f. Let $y, z \in (\mathfrak{a}_1\mathfrak{a}_2)^{-1}$. Set $x = ya + zb$ where $a + b = 1$ as in the previous argument. Since $(\mathfrak{a}_1\mathfrak{a}_2)^{-1}$ is an R-module then $ya, za \in (\mathfrak{a}_1\mathfrak{a}_2)^{-1}$ and $x \in (\mathfrak{a}_1\mathfrak{a}_2)^{-1}$. As in the above proof, we have $y - yb \equiv ya \equiv y \bmod \mathfrak{a}_1^{-1}$. But $x - ya \equiv zb \equiv 0 \bmod \mathfrak{a}_1^{-1}$ then $x \equiv ya \equiv y \equiv y - yb \bmod \mathfrak{a}_1^{-1}$. Similarly, we have $x \equiv zb \equiv z \equiv z - za \bmod \mathfrak{a}_2^{-1}$. Then, $f(x + R) = (y + \mathfrak{a}_1^{-1}, z + \mathfrak{a}_2^{-1})$. It proves that f is surjective and our claim is proved.

  Let us prove the lemma: consider the following isomorphism obtained from the above isomorphisms: $(f_1 \times f_2)^{-1} : \dfrac{(\mathfrak{a}_1\mathfrak{a}_2)^{-1}}{\mathfrak{a}_2^{-1}} \times \dfrac{(\mathfrak{a}_1\mathfrak{a}_2)^{-1}}{\mathfrak{a}_1^{-1}} \to \frac{\mathfrak{a}_1^{-1}}{R} \times \frac{\mathfrak{a}_2^{-1}}{R}$ and compose it with f, we get the isomorphism of the lemma:

$$(f_1 \times f_2)^{-1} \circ f : \frac{(\mathfrak{a}_1\mathfrak{a}_2)^{-1}}{R} \to \frac{\mathfrak{a}_1^{-1}}{R} \times \frac{\mathfrak{a}_2^{-1}}{R}$$

□

If $\mathfrak{a}_i, i = 1, 2$ are $G-$ invariant, then this isomorphism is an RG-isomoprhism as well.

Chapter 2

Reduction to inertia subgroup

2.1 The torsion module $\mathcal{R}_{N/E}$

The aim of this section is to introduce the definition of the torsion module $\mathcal{R}_{N/E}$ using the notes from Chapter 1, and prove that this module can be studied locally.

2.1.1 Definition. Let K/k be a Galois extension with group G, global or local. In Definition 1.3.11 of Galois extension of algebras, we recall the $kG-$isomorphism

$$r_{K,G} : K \otimes_k K \to \mathrm{Map}(G, K).$$

In the proof the Proposition 1.3.19, we had an injection

$$r_{\mathcal{O}_K,G} : \mathcal{O}_K \otimes_{\mathcal{O}_k} \mathcal{O}_K \to \mathrm{Map}(G, \mathcal{O}_K).$$

We define $\mathcal{R}_{K/k}$ to be the Coker of $r_{\mathcal{O}_K,G}$. Precisely, $\mathcal{R}_{K/k} := \mathrm{Map}(G, \mathcal{O}_K)/r_{\mathcal{O}_K,G}(\mathcal{O}_K \otimes_{\mathcal{O}_k} \mathcal{O}_K)$.

Since $\mathrm{Map}(G, \mathcal{O}_K)$ is finitely generated and $\mathcal{O}_K$-modules and $\mathcal{O}_K \otimes_{\mathcal{O}_k} \mathcal{O}_K$ contains a $K-$basis of $K \otimes_k K$, then $\mathcal{R}_{K/k}$ is a finitely generated torsion $\mathcal{O}_K$-module.

Let us go back to our notations. Let N/E be finite Galois tame extensions of number fields with group G. For each prime $\mathfrak{q}$ of S and a prime $\mathfrak{p}$ of R, we denote by $N_\mathfrak{q}$ the completion of N with respect to $v_\mathfrak{q}$ and $E_\mathfrak{p}$ the completion of E at $v_\mathfrak{p}$. We denote by $D_\mathfrak{q}$ (resp. $I_\mathfrak{q}$) the decomposition group (resp. inertia group) of $\mathfrak{q}$ in G.

Denote by $Ram(N/E)$ the set of primes of R which ramify in S. Recall that for each prime $\mathfrak{p}$ in $Ram(N/E)$, we fix a prime $\mathfrak{q}$ of S above $\mathfrak{p}$.

2.1.2 Lemma. See [[Cha84] Corollary 3.11] There is an isomorphism of $RG-$mdoules:

$$\mathcal{R}_{N/E} \simeq \bigoplus_{\mathfrak{p} \in Ram(N/E)} (\mathbb{Z}G \otimes_{\mathbb{Z}D_\mathfrak{q}} \mathcal{R}_{N_\mathfrak{q}/E_\mathfrak{p}})^{\oplus [G:D_\mathfrak{q}]}.$$

Thanks to the above lemma, we can focus on the local setting. In this section, we will concentrate in the following situation. Fix a prime p and a tamely ramified Galois extension K/k of $\mathbb{Q}_p$ with group Γ. Let Δ be the inertia group of K/k. By Proposition 1.4.6, Δ is cyclic of order e and its fixed field $F = K^\Delta$ is totally ramified extension. As usual, we denote by $\mathcal{O}_K, \mathcal{O}_F, \mathcal{O}_k$ the ring of integers of K, F and k, repectively, and we shall denote by $\mathfrak{p}_K, \mathfrak{p}_F$ and $\mathfrak{p}_k$ the corresponding maximal ideals. We denote by $\bar{K}, \bar{F}$ and $\bar{k}$, the residue fields of K, F and k, respectively.

The following proposition makes things easy because it restricts our situation into the case of totally ramified tame local extension.

2.1.3 Proposition. There is an isomorphism of $\mathcal{O}_k\Gamma-$modules

$$\mathcal{R}_{K/k} \simeq \mathbb{Z}\Gamma \otimes_{\mathbb{Z}\Delta} \mathcal{R}_{K/F}.$$

Proof. The proof of this uses the fact that F/k is unramified and by Proposition 1.3.19 $\mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{O}_F \simeq \mathrm{Map}(\Gamma, \mathcal{O}_K)$, hence $\mathcal{R}_{F/k} = 1$. The complete proof can be seen in [[Cha84],Corollary 3.8]. □

Recall that by Theorem 1.4.7, F contains the group of units $\mu_{e,p} \subseteq \overline{\mathbb{Q}_p}$ and Proposition 1.4.6 says that there exists a uniformizer π_K of K such that $\pi_F := \pi_K^e \in F$. In the proof of that Proposition, we have a group of homomorphism $\chi_{K/F} : \Delta \to \mu_{e,p}$ (this is the inverse of θ in the proof of the Theorem 1.4.7) and it does not depend on the choice of the uniformizer. We have seen that it is injective, hence isomorphism by comparing cardinals: $\sharp\Delta = \sharp\mu_{e,p}$.

2.1.4 Lemma. The isomorphism $\chi_{K/F}$ is also an $\Gamma-$isomorphism if we let Γ act on Δ by conjugation and act by Galois action on $\mu_{e,p}$.

Proof. It is sufficient to show that for all $\sigma \in \Gamma, \delta \in \Delta$, we have $\chi_{K/F}(\sigma\delta\sigma^{-1}) = \sigma(\chi_{K/F}(\delta))$.

If π_K is a uniformizer of K such that $\pi_K^e \in F$, then

$$\chi_{K/F}(\sigma\delta\sigma^{-1}) = \frac{\sigma\delta\sigma^{-1}(\pi_K)}{\pi_K} = \sigma(\frac{\delta\sigma^{-1}(\pi_K)}{\sigma^{-1}(\pi_K)} = \sigma(\chi_{K/F}(\delta)).$$

The last equality follows from the fact that $\sigma^{-1}(\pi_K)$ is a uniformizer of K whose e^{th} power is in F and $\chi_{K/F}$ does not depend on the choice of the uniformizer. It follows that $\chi_{K/F}$ is $\Gamma-$isomorphism. □

2.1.5 Remark. We see that if Γ is abelian, then Γ acts trivially on Δ and $\mu_{e,p} \subset k$.

If M is an $\mathcal{O}_K-$module, and if we let Δ act on M by the operation $\delta.m = \chi_{K/F}^i(\delta)m$, M becomes an $\mathcal{O}_K\Delta-$module and we denote it by $M(\chi_{K/F}^i)$.
The next proposition shows that the $\mathcal{O}_F\Delta-$module $\mathcal{R}_{K/F}$ can be still decomposed in smaller pieces.

2.1.6 Proposition. The action of $\mathcal{O}_F$ on $\mathcal{R}_{K/F}$ factors through $\overline{F}$ and there is an isomorphism of $\overline{F}\Delta-$modules:

$$\mathcal{R}_{K/F} \simeq \bigoplus_{i=1}^{e-1} (\mathfrak{p}_K^i/\mathfrak{p}_K^{i+1})^{\oplus i}$$

Claim.

$$\mathcal{R}_{K/F} \simeq \bigoplus_{i=1}^{e-1} (\mathcal{O}_K/\mathfrak{p}_K^i)(\chi_{K/F}^i)$$

[Cha84], Theorem 2.8. Sketch of the proof of the claim: In fact, from Theorem 1.4.6, $\{1, \pi_K, \dots, \pi_K^{e-1}\}$ is a $\mathcal{O}_F-$basis of $\mathcal{O}_K$, thus $\{1\otimes 1, \dots, 1\otimes\pi_K^{e-1}\}$ is a basis of the free $\mathcal{O}_K-$module $\mathcal{O}_K \otimes_{\mathcal{O}_F} \mathcal{O}_K$. Consider the well known bijection $r_{K,\Delta} : K \otimes_F K \to \mathrm{Map}(\Delta, K)$. Define $u_i(\sigma) = \chi_{K/F}^i(\sigma), u_i \in \mathrm{Map}(\Delta, \mathcal{O}_K)$, then one can show that $r_{K,\Delta}(1 \otimes \pi_K^i) = \pi_K^i u_i$ and $\{u_0, \dots, u_{e-1}\}$ form an $\mathcal{O}_K-$basis of $\mathrm{Map}(\Delta, \mathcal{O}_K)$. Since $(\pi_K)^i = \mathfrak{p}_K^i$, then the claim follows. □

Proof. Let us now prove the theorem. Since $\mathfrak{p}_F\mathcal{O}_K = \mathfrak{p}_K^e \subset \mathfrak{p}_K^i$, for all $i = 0, \dots, e$, then $\mathcal{O}_K/\mathfrak{p}_K^i$ is annihilated by $\mathfrak{p}_F$ so it has a structure of $\overline{F}-$module (see notes above Definition 1.3.1). By definition, $\mathcal{R}_{K/F}$ is an $\mathcal{O}_F$-module, hence by the claim, it becomes an $\overline{F}-$module and the isomorphism in claim becomes an $\overline{F}\Delta-$isomorphism.

Note that $\mathcal{O}_K/\mathfrak{p}_K^i(\chi_{K/F}^i)$ is an $\overline{F}\Delta-$module with finite filtration of sub $\overline{F}\Delta-$modules:

$$\mathcal{O}_K/\mathfrak{p}_K^i(\chi_{K/F}^i) \supset \mathfrak{p}_K/\mathfrak{p}_K^i(\chi_{K/F}^i) \supset \dots \supset \mathfrak{p}_K^{i-1}/\mathfrak{p}_K^i(\chi_{K/F}^i) \supset \{0\}$$

and its associated graded $\overline{F}\Delta-$module is given by $\oplus_{j=0}^{i-1}\mathfrak{p}_K^j/\mathfrak{p}_K^{j+1}(\chi_{K/F}^i)$. Since e is prime to the characteristic of $\overline{F}$, then $\overline{F}\Delta$ is semisimple, hence we get

$$\mathcal{O}_K/\mathfrak{p}_K^i(\chi_{K/F}^i) \simeq \bigoplus_{j=0}^{i-1}\mathfrak{p}_K^j/\mathfrak{p}_K^{j+1}(\chi_{K/F}^i). \tag{2.1}$$

On the other hand, for each j, we have an $\overline{F}-$isomorphism $\mathcal{O}_K/\mathfrak{p}_K \simeq \mathfrak{p}_K^j/\mathfrak{p}_K^{j+1}$ by sending $[x] \mapsto [\pi_K^j x]$, where $[x]$ denote the class of x, hence an isomorphism of $\overline{F}\Delta$-modules $\mathcal{O}_K/\mathfrak{p}_K(\chi_{K/F}^i) \simeq \mathfrak{p}_K^j/\mathfrak{p}_K^{j+1}(\chi_{K/F}^i)$. Combine this with the equation 2.1, we have:

$$\mathcal{O}_K/\mathfrak{p}_K^i(\chi_{K/F}^i) \simeq \oplus_{j=0}^{i-1}\mathcal{O}_K/\mathfrak{p}_K(\chi_{K/F}^i) = \mathcal{O}_K/\mathfrak{p}_K(\chi_{K/F}^i)^{\oplus i}.$$

Observe that the Galois action of Δ on $\mathfrak{p}_K^i/\mathfrak{p}_K^{i+1}$ is the same as the action given by multiplication by $\chi_{K/F}^i$ since for all $x \in \mathfrak{p}_K^i, \delta \in \Delta$, we have

$$\delta[\pi_K^i x] = [\delta(\pi_K^i x)] = [\chi_{K/F}^i(\delta)\pi_K^i\delta(x)] = [\chi_{K/F}^i(\delta)\pi_K^i x].$$

The last equality follows from the fact that Δ acts trivially on $\mathcal{O}_K/\mathfrak{p}_K = \mathcal{O}_F/\mathfrak{p}_F$. Thus $\mathfrak{p}_K^i/\mathfrak{p}_K^{i+1}$ and $\mathcal{O}_K/\mathfrak{p}_K(\chi_{K/F}^i)$ are $\overline{F}-$vector spaces of 1 dimension on which Δ acts by multiplication by $\chi_{K/F}^i$. Then, $\mathcal{O}_K/\mathfrak{p}_K^i(\chi_{K/F}^i) \simeq (\mathfrak{p}_K^i/\mathfrak{p}_K^{i+1})^{\oplus i}$ as $\overline{F}\Delta-$modules and the proposition follows. □

2.2 Torsion modules arising from ideals

In this section, we recall the definition of the torsion modules $\mathcal{T}_{N/E}$ and $\mathcal{S}_{N/E}$ and prove that they can be studied locally as the case of $\mathcal{R}_{N/E}$.

Let R be a Dedekind ring and E its fractional field. Let N be a finite Galois extension of E with group G and ring of integers S. Let I be an $G-$stable or G-invariant ideal of S, that is $g.a \in I$ for all $g \in G, a \in I$. Recall that for a fractional ideal I of S, the dual of I with respect to the trace $\mathrm{Tr}_{N/E}$ from N to E is the fractional ideal

$$I^* := \{x \in N |\, \mathrm{Tr}_{N/E}(xI) \subseteq R\}.$$

This is G-isomorphic to $\mathrm{Hom}_R(I, R)$ since the $\mathrm{Tr}_{N/E}$ is non-degenerate map.

By definition, $\mathcal{C}_{N/E} := S^*$ and it is called the inverse different of N/E. It is a fractional ideal of S containing S so its inverse, $\mathcal{D}_{N/E}$ which is called the different of N/E is an ideal of S. Of course, $\mathcal{D}_{N/E}$ is a $G-$stable ideal of S.

For any fractional ideal I of S, we have

$$I^* = \mathcal{C}_{N/E}I^{-1}.$$

We denote by $\mathcal{A}_{N/E}$ be the square root of $\mathcal{C}_{N/E}$. By the above formula, we have $\mathcal{A}_{N/E}^* = \mathcal{A}_{N/E}$.

As announced in the introduction, to study these two modules we define $\mathcal{T}_{N/E} := \mathcal{C}_{N/E}/S$ and $\mathcal{S}_{N/E} := \mathcal{A}_{N/E}/S$.

Denote by $Div(I)$ the set of primes of R below the primes of S dividing I such that for each prime $\mathfrak{p} \in Div(I)$ we fix a prime $\mathfrak{q}$ of S above $\mathfrak{p}$.

2.2.1 Proposition. Let I be a $G-$stable ideal of S. For every prime $\mathfrak{p} \in R$, let $n_{\mathfrak{p}}$ be the valuation of I at any prime of S above $\mathfrak{p}$. Then there are isomorphisms of $RG-$ modules

$$S/I \simeq \bigoplus_{\mathfrak{p}\in Div(I)} \mathbb{Z}G \otimes_{\mathbb{Z}D_{\mathfrak{p}}} (S_{\mathfrak{q}}/\mathfrak{q}^{n_{\mathfrak{q}}}S_{\mathfrak{q}})$$

$$I^{-1}/S \simeq \bigoplus_{\mathfrak{p}\in Div(I)} \mathbb{Z}G \otimes_{\mathbb{Z}D_{\mathfrak{p}}} (\mathfrak{q}^{-n_{\mathfrak{p}}}S_{\mathfrak{q}}/S_{\mathfrak{q}})$$

Proof. Write $I = \prod_{\mathfrak{p}\in Div(I)} \prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{n_\mathfrak{p}}$. For any $\mathfrak{p}, \mathfrak{p}' \in Div(I), \mathfrak{p} \neq \mathfrak{p}'$, we have $\prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{n_\mathfrak{p}} + \prod_{\mathfrak{q}|\mathfrak{p}'} \mathfrak{q}^{n_{\mathfrak{p}'}} = S$. Applying the Chinese Remainder Theorem 1.4.8 with $M = S$, we have an isomorphism of $S-$modules

$$S/I \simeq \oplus_{\mathfrak{p}\in Div(I)} S/(\prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{n_\mathfrak{p}}).$$

Since I is $G-$stable, this is also an isomorphism of $RG-$modules. For any $\mathfrak{q}, \mathfrak{q}'$ dividing $\mathfrak{p}$ such that $\mathfrak{q} \neq \mathfrak{q}'$, we have $\mathfrak{q}^{n_\mathfrak{p}} + \mathfrak{q}'^{n_\mathfrak{p}} = S$, so applying again the Chinese Remainder theorem with $M = S$, we have an isomorphism of S-modules

$$S/(\prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{n_\mathfrak{p}}) \simeq \prod_{\mathfrak{q}|\mathfrak{p}} S/\mathfrak{q}^{n_\mathfrak{p}}$$

Set $M = S/\mathfrak{q}^{n_\mathfrak{p}}$. It is a finitely generated $S-$module and its completion with respect to $v_\mathfrak{q}$ is given by

$$M_\mathfrak{q} = S_\mathfrak{q} \otimes_S M = S_\mathfrak{q} \otimes_S S/\mathfrak{q}^{n_\mathfrak{p}} \simeq S_\mathfrak{q}/\mathfrak{q}^{n_\mathfrak{p}} S_\mathfrak{q}.$$

The last isomorphism follows from the fact that $R/I \otimes_R M \simeq M/IM$ for any $R-$module M and commutative ring R and ideal I of R.

On the other hand, for every $\mathfrak{q}|\mathfrak{p}$, the inclusion $S \to S_\mathfrak{q}$ induces an isomorphism $S/\mathfrak{q}^{n_\mathfrak{p}} \simeq S_\mathfrak{q}/\mathfrak{q}^{n_\mathfrak{p}} S_\mathfrak{q}$ of $RD_\mathfrak{q}-$modules. By Lemma 1.4.2, for any prime $\mathfrak{q}_0$ of S,

$$\prod_{\mathfrak{q}|\mathfrak{p}} S/\mathfrak{q}^{n_\mathfrak{p}} \simeq \prod_{\mathfrak{q}|\mathfrak{p}} M_\mathfrak{q} \simeq \mathrm{Map}(G, M)^{D_{\mathfrak{q}_0}} \simeq \mathbb{Z}G \otimes_{\mathbb{Z}D_\mathfrak{q}} M,$$

where $M = S/\mathfrak{q}_0^{n_\mathfrak{p}}$.
This shows the first isomorphism of the lemma. The proof of the second isomorphism is similar using the analogue of the Chinese Remainder theorem instead of the Chinese Remainder Theorem 1.4.9.

□

We will apply this Proposition with $I = \mathcal{D}_{N/E}$, the different of N/E.

Local setting

The previous proposition and lemma allow us to work in local case to treat the modules $T_{N/E}, S_{N/E}$ and $\mathcal{R}_{N/E}$ so let us introduce the local setting of our situation.
Let us start from the local analogue of the isomorphism, $r_{K,\Gamma}$ introduced above. Recall the isomorphism

$$\begin{array}{rcl} r_{K,\Gamma} \colon K \otimes_k K & \to & \mathrm{Map}(\Gamma, K), \\ x \otimes y & \mapsto & \delta \mapsto x\delta(y), \end{array}$$

Let $(\Gamma \times \Gamma)$ act on $K \otimes_k K$ by $(\delta, \delta')(x \otimes y) = \delta(x) \otimes \delta'(y)$ and define an action of $(\Gamma \times \Gamma)$ on $\mathrm{Map}(\Gamma, K)$ by $((\delta, \delta').f)(g) = \delta(f(\delta^{-1} g \delta'))$ for all $\delta, \delta', g \in \Gamma, f \in \mathrm{Map}(\Gamma, K)$. These operations make $r_{K,\Delta}$ into $(\Gamma \times \Gamma)-$isomorphism.

The action of the subgroup $(1 \times \Gamma)$ on $\mathrm{Map}(\Gamma, K)$ is the same as the action of Γ introduced in the beginning of the section of Galois algebras when we identify $(1 \times \Gamma)$ with Γ.

Recall the definition of $\mathrm{Map}(\Gamma, K)^\Delta$ which is the set of invariant maps under the action of the subgroup $(\Gamma \times 1)$ of $\Gamma \times \Gamma$. More precisely,

$$\mathrm{Map}(\Gamma, K)^\Delta = \{f : \Gamma \to K, \delta(f(g)) = f(g\delta) \text{ for all } \delta, g \in \Gamma, f \in \mathrm{Map}(\Gamma, K)\}.$$

As we have seen, $\mathrm{Map}(\Gamma, K)^{\Delta}$ is an $F-$algebra with the pointwise operations and an Γ-module where Γ acts as $1 \times \Gamma$.

Then from Lemma 1.3.7, there is an isomorphism of both $F-$algebra and $F\Gamma-$modules:

$$\begin{aligned} \mathrm{Map}(\Gamma, K)^{\Delta} &\rightarrow \mathbb{Q}\Gamma \otimes_{\mathbb{Q}\Delta} K, && (2.2) \\ f &\mapsto \sum_{\gamma \in \Gamma} \gamma^{-1} \otimes f(\gamma), && (2.3) \end{aligned}$$

Note that, $\mathbb{Q}\Gamma \otimes_{\mathbb{Q}\Delta} K$ has the structure of $\Gamma-$module via its left-hand factor and the structure of an $F-$algebra via its right-hand factor.

Since $F \otimes_k K$ is an $F-$algebra via its left factor and as $\Gamma-$module via its right factor, then the isomorphism $r_{K,\Gamma}$ induces both an $F-$algebra isomorphism and $F\Gamma-$module:

$$F \otimes_k K \simeq \mathrm{Map}(\Gamma, K)^{\Delta}.$$

Composing this with the isomorphism in (2.2), then we get :

$$\widetilde{r}_{K,\Gamma} : F \otimes_k K \rightarrow \mathbb{Q}\Gamma \otimes_{\mathbb{Q}\Delta} K.$$

Since F/k is unramified then from Lemma 1.3.20, $\mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{O}_K$ is the maximal order of $F \otimes_k K$ and $\mathbb{Z}\Gamma \otimes_{\mathbb{Z}\Delta} \mathcal{O}_K$ is the maximal order of $\mathbb{Q}\Gamma \otimes_{\mathbb{Q}\Delta} K$. Hence from Proposition 2.2, $\widetilde{r}_{K,\Gamma}$ induces an isomorphism of rings and of $\mathcal{O}_F\Gamma-$modules:

$$\mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{O}_K \simeq \mathbb{Z}\Gamma \otimes_{\mathbb{Z}\Delta} \mathcal{O}_K.$$

2.2.2 Proposition. For every $n \in \mathbb{N}$, the homomorphism $\widetilde{r}_{K,\Gamma}$ induces isomorphisms of $\mathcal{O}_F\Gamma-$modules

$$\mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{O}_K/\mathfrak{p}_K^n \simeq \mathbb{Z}\Gamma \otimes_{\mathbb{Z}\Delta} \mathcal{O}_K/\mathfrak{p}_K^n,$$
$$\mathcal{O}_F \otimes_{\mathcal{O}_k} \mathfrak{p}_K^{-n}/\mathcal{O}_K \simeq \mathbb{Z}\Gamma \otimes_{\mathbb{Z}\Delta} \mathfrak{p}_K^{-n}/\mathcal{O}_K.$$

Proof. Consider the following short exact sequence:

$$0 \rightarrow \mathfrak{p}_K^n \rightarrow \mathcal{O}_K \rightarrow \mathcal{O}_K/\mathfrak{p}_K^n \rightarrow 0.$$

Since F/k is unramified, then $\mathcal{O}_F$ is free $\mathcal{O}_k-$module hence flat $\mathcal{O}_k-$module. We know also that $\mathbb{Z}\Gamma$ is free $\mathbb{Z}\Delta-$module, hence flat $\mathbb{Z}\Delta-$module. Then we have the following commutative diagram of $\mathcal{O}_F\Gamma-$modules:

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{O}_F \otimes_{\mathcal{O}_k} \mathfrak{p}_K^n \arrow[r] \arrow[d, "\widetilde{r}_{K,\Gamma}"'] & \mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{O}_K \arrow[r] \arrow[d, "\widetilde{r}_{K,\Gamma}"'] & \mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{O}_K/\mathfrak{p}_K^n \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathbb{Z}\Gamma \otimes_{\mathbb{Z}\Delta} \mathfrak{p}_K^n \arrow[r] & \mathbb{Z}\Gamma \otimes_{\mathbb{Z}\Delta} \mathcal{O}_K \arrow[r] & \mathbb{Z}\Gamma \otimes_{\mathbb{Z}\Delta} \mathcal{O}_K/\mathfrak{p}_K^n \arrow[r] & 0
\end{tikzcd}$$

The central vertical arrow is an isomorphism as we have just discussed above. So, the right hand vertical arrow is surjective. Comparing the cardinals, we have

$$\sharp(\mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{O}_K/\mathfrak{p}_K^n) = \sharp(\mathcal{O}_K/\mathfrak{p}_K^n)^{[F:k]} = \sharp(\mathcal{O}_K/\mathfrak{p}_K^n)^{[\Gamma:\Delta]}) = \sharp(\mathbb{Z}\Gamma \otimes_{\mathbb{Z}\Delta} \mathcal{O}_K/\mathfrak{p}_K^n).$$

Hence the right-hand vertical arrow is an isomorphism. By the Snake's lemma in Lemma 1.3.2, the left-hand arrow is an isomorphism and the first isomorphism follows.

The proof of the second isomorphism is similar by considering the short sequence

$$0 \rightarrow \mathcal{O}_K \rightarrow \mathfrak{p}_K^{-n} \rightarrow \mathfrak{p}_K^{-n}/\mathcal{O}_K \rightarrow 0$$

and the following commutative diagram of $\mathcal{O}_F\Gamma-$modules with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{O}_K \arrow[r] \arrow[d, "\widetilde{r}_{K,\Gamma}"'] & \mathcal{O}_F \otimes_{\mathcal{O}_k} \mathfrak{p}_K^{-n} \arrow[r] \arrow[d, "\widetilde{r}_{K,\Gamma}"'] & \mathcal{O}_F \otimes_{\mathcal{O}_k} \mathfrak{p}_K^{-n}/\mathcal{O}_K \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathbb{Z}\Gamma \otimes_{\mathbb{Z}\Delta} \mathcal{O}_K \arrow[r] & \mathbb{Z}\Gamma \otimes_{\mathbb{Z}\Delta} \mathfrak{p}_K^{-n} \arrow[r] & \mathbb{Z}\Gamma \otimes_{\mathbb{Z}\Delta} \mathfrak{p}_K^{-n}/\mathcal{O}_K \arrow[r] & 0
\end{tikzcd}$$

We have seen that the left-hand arrow is an isomorphism. Comparing the cardinals as before it is enough to prove that the central arrow is injective. To prove this, consider the following commutative diagram of $\mathcal{O}_F\Gamma-$modules:

$$\begin{tikzcd}
\mathcal{O}_F \otimes_{\mathcal{O}_k} \mathfrak{p}_K^{-n} \arrow[r] \arrow[d, "\widetilde{r}_{K,\Gamma}"'] & F \otimes_k K \arrow[d] \\
\mathbb{Z}\Gamma \otimes_{\mathbb{Z}\Delta} \mathfrak{p}_K^{-n} \arrow[r] & \mathbb{Z}\Gamma \otimes_{\mathbb{Z}\Delta} K
\end{tikzcd}$$

The right arrow is an isomorphism from the above discussions. Note that $F \otimes_k K$ is the localisation of $\mathcal{O}_F \otimes_{\mathcal{O}_k} \mathfrak{p}_K^{-n}$ at the multiplicative set $k^{\times}$. Since $\mathcal{O}_F \otimes_{\mathcal{O}_k} \mathfrak{p}_K^{-n}$ is torsion free $\mathcal{O}_k$-module, then the top row is injective. In particular, the left-hand row is injective. This proves the second isomorphism of the proposition. □

The following proposition shows that the Δ-modules $\mathfrak{p}_K^{-n}/\mathcal{O}_K$ and $\mathcal{O}_K/\mathfrak{p}_K^n$ can be decomposed as in Proposition 2.1.6.

2.2.3 Proposition. For each $n = 0, \ldots, e$, the action of $\mathcal{O}_F$ on $\mathcal{O}_K/\mathfrak{p}_K^n$ and $\mathfrak{p}_K^{-n}/\mathcal{O}_K$ factors through an action of $\mathcal{O}_F/\mathfrak{p}_F$ and we have isomorphisms of $\overline{F}\Delta-$modules:

$$\mathcal{O}_K/\mathfrak{p}_K^n \simeq \oplus_{i=1}^{n-1}\mathfrak{p}_K^i/\mathfrak{p}_K^{i+1} \text{ and } \mathfrak{p}_K^{-n}/\mathcal{O}_K \simeq \oplus_{i=0}^{n}\mathfrak{p}_K^{e-i}/\mathfrak{p}_K^{e-(i-1)}$$

Proof. We have seen in Proposition 2.1.6 that $\mathcal{O}_K/\mathfrak{p}_K^n$ and $\mathfrak{p}_K^{-n}/\mathcal{O}_K$ are both $\overline{F}\Delta-$modules, and they have the filtrations $\{\mathfrak{p}_K^i/\mathfrak{p}_k^n\}_{i=0}^n$ and $\{\mathfrak{p}_K^{-i}/\mathcal{O}_K\}_{i=0}^n$, respectively. Using the semisimplicity of $\overline{F}\Delta$, we have $\overline{F}\Delta-$isomoprhisms:

$$\mathcal{O}_K/\mathfrak{p}_K^n \simeq \oplus_{i=0}^{n-1}\mathfrak{p}_K^i/\mathfrak{p}_K^{i+1} \text{ and } \mathfrak{p}_K^{-n}/\mathcal{O}_K \simeq \oplus_{i=1}^{n-1}\mathfrak{p}_K^{-i}/\mathfrak{p}_K^{-i+1}.$$

On the other hand, the multiplication by the e^{th} power of any uniformizer gives a $\overline{F}\Delta-$isomoprhism between $\mathfrak{p}_K^{-i}/\mathfrak{p}_K^{-i+1}$ and $\mathfrak{p}_K^{e-i}/\mathfrak{p}_K^{e-(i-1)}$, and this proves the second isomoprhism. □

2.3 Switch to a global cyclotomic field

In this subsection, we will perfom a further reduction relating the modules $\mathcal{O}_K/\mathfrak{p}_K^n$, $\mathfrak{p}_K^{-n}/\mathcal{O}_K$ and $\mathcal{R}_{K/F}$ to new torsion Galois modules, associated to the ring of integers of a certain cyclotomic fields.

Let μ_e denote the group of e^{th} roots of unity in a fixed field algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ and let denote by $\mathcal{O}$ the ring of integers of $\mathbb{Q}(\mu_e)$.

Let $\chi : \Delta \to \mu_e$ be a character of Δ. For any $\mathcal{O}-$module M, we let Δ act on M by $\delta.m = \chi(\delta)m$. It makes M into an $\mathcal{O}\Delta$-module and we denote it by $M(\chi)$. We will concentrate with the case M is the residue field of a prime $\mathcal{P}$ of $\mathcal{O}$ not dividing e, that is, $M = \mathcal{O}/\mathcal{P}$.

Let's now explain the relation between the module M introduced above and the modules $\mathcal{O}_K/\mathfrak{p}_K^n$, $\mathfrak{p}_K^{-n}/\mathcal{O}_K$ and $\mathcal{R}_{K/F}$. Thanks to the following lemma, we can switch the local case to a global case.

2.3.1 Lemma. If the character $\chi : \Delta \to \mu_e$ is injective, then there exists an embedding $\iota : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_p$ such that $\iota \circ \chi = \chi_{K/F}$.

Proof. Define $\iota : \mathbb{Q}(\mu_e) \to \overline{\mathbb{Q}}_p$ by $\iota(\chi(\delta)) = \chi_{K/F}(\delta)$ for every $\delta \in \Delta$. Since Δ and μ_e have the same cardinality, thus χ is an isomorphism. Thus, i is injective since $\chi_{K/F}$ also is an isomorphism.

Then we can extend ι to an embedding $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_p$ in infinitely many ways and each of these extensions satisfies the conditions $\iota \circ \chi = \chi_{K/F}$. □

Let's fix now an injective character $\chi : \Delta \to \mu_e$ and an embedding $\iota : \mathbb{Q}(\mu_e) \to \overline{\mathbb{Q}}_p$ such that $\iota \circ \chi = \chi_{K/F}$ as in the Lemma. Since $\mu_{e,p} \subset F$, then $\iota(\mathcal{O}) \subseteq \mathcal{O}_F$. Hence via the homomorphism ι, any $\mathcal{O}_F-$module can be viewed as $\mathcal{O}$-module.

2.3.2 Proposition. Let $\mathcal{P}$ be the prime ideal above p such that $\iota(\mathcal{P}) \subset \mathfrak{p}_F$. Then for every, natural integer i and every uniformizer π_K of K, we have an isomorphism of $\mathcal{O}_F\Delta-$modules :

$$\mathfrak{p}_K^i/\mathfrak{p}_K^{i+1} \simeq \mathcal{O}/\mathcal{P}(\chi^i) \otimes_{\mathcal{O}/\mathcal{P}} \overline{F},$$

where $\mathcal{O}/\mathcal{P}(\chi^i) \otimes_{\mathcal{O}/\mathcal{P}} \overline{F}$ is an $\overline{F}-$module via its right factor and $\Delta-$module via its left factor.

Proof. Since K/F is totally ramified, we have $\overline{F} = \overline{K}$. Then we have an $\mathcal{O}_F$-isomorphism:

$$\begin{aligned} \varphi \colon \mathfrak{p}_K^i/\mathfrak{p}_K^{i+1} &\to \mathcal{O}/\mathcal{P}(\chi^i) \otimes_{\mathcal{O}/\mathcal{P}} \overline{F}, \\ \pi_K^i x &\mapsto 1 \otimes x. \end{aligned}$$

Recall that the Galois action of Δ on $\mathfrak{p}_K^i/\mathfrak{p}_K^{i+1}$ is the same as the action given by multiplication by $\chi_{K/F}^i$ since for all $x \in \mathfrak{p}_K^i, \delta \in \Delta$, we have

$$\delta[\pi_K^i x] = [\delta(\pi_K^i x)] = [\chi_{K/F}^i(\delta)\pi_K^i \delta(x)] = [\chi_{K/F}^i(\delta)\pi_K^i x]$$

as we have seen in Proposition 2.1.6, hence we have $\varphi(\delta.[\pi_K^i x]) = [1] \otimes [(\chi_{K/F}^i)(\delta)x] = [1] \otimes \iota\chi^i(\delta)[x] = \chi^i(\delta)[1] \otimes [x] = ([\delta.1]) = \delta.([1] \otimes [x])$. This proves that φ is Δ-isomorphism. □

2.3.3 Proposition. Let $\mathcal{P}$ be the prime ideal of $\mathcal{O}$ above a prime number p such that $\iota(\mathcal{P}) \subset \mathfrak{p}_F$. Assume that K/k is abelian, and let $0 < n \leq e$ be an integer. Then ι induces an inclusion $\mathcal{O}/\mathcal{P} \to \mathcal{O}_k/\mathfrak{p}_k$ and there are isomorphisms of $\mathcal{O}_k/\mathfrak{p}_k\Gamma-$modules:

$$\mathcal{O}_K/\mathfrak{p}_K^n \simeq \mathcal{O}_k/\mathfrak{p}_k \otimes_{\mathcal{O}/\mathcal{P}} (\mathbb{Z}\Gamma \otimes_{\mathbb{Z}\Delta} (\oplus_{i=0}^{n-1}\mathcal{O}/\mathcal{P}(\chi^i))),$$

$$\mathfrak{p}_K^{-n}/\mathcal{O}_K \simeq \mathcal{O}_k/\mathfrak{p}_k \otimes_{\mathcal{O}/\mathcal{P}} (\mathbb{Z}\Gamma \otimes_{\mathbb{Z}\Delta} (\oplus_{i=}^{n}\mathcal{O}/\mathcal{P}(\chi^{e-i})))$$

where the right-hand sides of the above isomorphisms are $\mathcal{O}_k/\mathfrak{p}_k-$modules via their left factors and $\Gamma-$modules via their right factors.

Proof. Since K/k is abelian then $\mu_{e,p} \subset k$ and hence $\iota(\mathcal{O}) \subset \mathcal{O}_k$. Thus $\iota(\mathcal{O}/\mathcal{P}) \subset \mathcal{O}_k/\mathfrak{p}_k$ and this makes $\mathcal{O}_k/\mathfrak{p}_k$ into a $\mathcal{O}/\mathcal{P}-$module. On the other hand, we have

$$\mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{O}_K/\mathfrak{p}_K^n \simeq \mathcal{O}_F/\mathfrak{p}_F \otimes_{\mathcal{O}_k/\mathfrak{p}_k} \mathcal{O}_K/\mathfrak{p}_K^n.$$

By Proposition 2.2.2, we have

$$\mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{O}_K/\mathfrak{p}_K^n \simeq \mathbb{Z}\Gamma \otimes_{\mathbb{Z}\Delta} \mathcal{O}_K/\mathfrak{p}_K^n.$$

From Proposition 2.2.3, we get

$$\mathbb{Z}\Gamma \otimes_{\mathbb{Z}\Delta} \mathcal{O}_K/\mathfrak{p}_K^n \simeq \mathbb{Z}\Gamma \otimes_{\mathbb{Z}\Delta} (\oplus_{i=0}^{n-1}\mathfrak{p}_K^i/\mathfrak{p}_K^{i+1}).$$

Using Proposition 2.3.2, we have

$$\mathbb{Z}\Gamma \otimes_{\mathbb{Z}\Delta} (\oplus_{i=0}^{n-1} \mathfrak{p}_K^i/\mathfrak{p}_K^{i+1}) \simeq \mathbb{Z}\Gamma \otimes_{\mathbb{Z}\Delta} \left((\mathcal{O}/\mathcal{P}(\chi^i) \otimes_{\mathcal{O}/\mathcal{P}} \overline{F}) \right).$$

Since $\mathcal{O}_k/\mathfrak{p}_k$ is an $\mathcal{O}/\mathcal{P}$-module, using the properties of tensor product, we can write

$$\mathcal{O}_F/\mathfrak{p}_F \otimes_{\mathcal{O}_k/\mathfrak{p}_k} \mathcal{O}_K/\mathfrak{p}_K^n \simeq \big(\mathbb{Z}\Gamma \otimes_{\mathbb{Z}\Delta} \big((\mathcal{O}/\mathcal{P}(\chi^i)\big) \otimes_{\mathcal{O}/\mathcal{P}} \mathcal{O}_k/\mathfrak{p}_k\big) \otimes_{\mathcal{O}_k/\mathfrak{p}_k} \mathcal{O}_F/\mathfrak{p}_F.$$

The isomorphism between $\mathcal{O}_K/\mathfrak{p}_K^n$ and $\big(\mathbb{Z}\Gamma \otimes_{\mathbb{Z}\Delta} \big((\mathcal{O}/\mathcal{P}(\chi^i)\big) \otimes_{\mathcal{O}/\mathcal{P}} \mathcal{O}_k/\mathfrak{p}_k\big)$ now follows from this by cancellation of $\overline{F}\Gamma-$modules, which is a consequence of the Krull-Schimidt Theorem:

let A be a finite dimensional algebra over the field K and let M be an A-module of finite type with two decompositions

$$M = M_1 \oplus \cdots \oplus M_n = N_1 \oplus \cdots \oplus N_m$$

into indecomposable submodules, then $n = m$ and there exists a permutatuion π of the indices $1, \dots, n$ such that $M_{\pi(i)=N_i}$. The proof of the second isomorphism is similar. □

2.3.4 Corollary. If K/k is unramified, then $\mathcal{O}_K/\mathfrak{p}_K$ and $\mathfrak{p}_K^{-1}/\mathcal{O}_K$ are free $\mathcal{O}_k/\mathfrak{p}_k\Gamma-$modules.

Proof. If K/k is unramified, then it is abelian and Δ is trivial. In particular $e = 1, \chi$ is trivial and $\mathcal{O}/\mathcal{P} = \mathbb{F}_p$ which is the field with p elements. Then Proposition 2.3.3 says that we have the following isomorphisms of $\mathcal{O}_k/\mathfrak{p}_k\Gamma$-modules:

$$\begin{aligned} \mathcal{O}_K/\mathfrak{p}_K &\simeq \mathcal{O}_k/\mathfrak{p}_k \otimes_{\mathbb{F}_p} \big(\mathbb{Z}\Gamma \otimes_{\mathbb{F}_p} \mathbb{F}_p\big) \simeq \mathcal{O}_k/\mathfrak{p}_k\Gamma, \\ \mathfrak{p}_K^n/\mathcal{O}_K &\simeq \mathcal{O}_k/\mathfrak{p}_k \otimes_{\mathbb{F}_p} \big(\mathbb{Z}\Gamma \otimes_{\mathbb{F}_p} \mathbb{F}_p\big) \simeq \mathcal{O}_k/\mathfrak{p}_k\Gamma. \end{aligned}$$

□

Since we are mainly interested in the modules $T_{N/E}, S_{N/E},$ and $\mathcal{P}_{N/E}$ let us introduce the following notation for any prime $\mathcal{P}$ of $\mathcal{O}$ not dividing e:

$$T_\chi(\mathcal{P}, \mathcal{O}\Delta) \quad = \bigoplus_{i=1}^{e-1} \mathcal{O}/\mathcal{P}(\chi^i), \tag{2.4}$$

$$S_\chi(\mathcal{P}, \mathcal{O}\Delta) \quad = \bigoplus_{i=\frac{e+1}{2}}^{e-1} \mathcal{O}/\mathcal{P}(\chi^i), \tag{2.5}$$

$$R_\chi(\mathcal{P}, \mathcal{O}\Delta) \quad = \bigoplus_{i=1}^{e-1} \mathcal{O}/\mathcal{P}(\chi^i)^{\oplus i}. \tag{2.6}$$

Consider the Swan module $\sum_\Delta(p) = p\mathbb{Z}\Delta + \mathrm{Tr}_\Delta$. Recall that $\Delta =< \delta >, \mathrm{Tr}_\Delta = \sum_{i=0}^{i=e-1} \in \mathbb{Z}\Delta$ and p is the residual character of $\mathcal{P}$. Using the decomposition of $\mathcal{O}/\mathcal{P}\Delta$ given by primitive idempontents, we have an isomorphism $\mathcal{O}\Delta$-modules

$$\mathcal{O}/\mathcal{P}\Delta \simeq \bigoplus_{i=0}^{e-1} \mathcal{O}/\mathcal{P}(\chi^i).$$

Let e_0 be the primitive idempotent attached to χ^0. Since $e \in \mathcal{O}/\mathcal{P}^\times$, then $\frac{1}{e}\mathrm{Tr}_\Delta$ is an idempotent and we have

$$\mathcal{O}/\mathcal{P}\Delta/\,\mathrm{Tr}_\Delta \simeq \bigoplus_{i=0}^{e-1} \mathcal{O}/\mathcal{P}(\chi^i)/\mathcal{O}/\mathcal{P}(\chi^0) \simeq \bigoplus_{i=1}^{e-1} \mathcal{O}/\mathcal{P}(\chi^i) = T_\chi(\mathcal{P}, \mathbb{Z}\Delta).$$

This shows that $T_\chi(\mathcal{P}, \mathcal{O}\Delta)$ is independent of the chosen injective character χ.

On the other hand, we have the torsion module $\mathcal{T}(p, \mathbb{Z}\Delta) := \mathbb{Z}\Delta/\sum_\Delta(p) = \mathbb{F}_p/(\mathrm{Tr}_\Delta)$. Since $\mathcal{O}/\mathcal{P}$ is an $\mathbb{F}_p$-vector space, then we have

$$T_\chi(\mathcal{P}, \mathbb{Z}\Delta) = T(p, \mathbb{Z}\Delta) \otimes_{\mathbb{F}_p} \mathcal{O}/\mathcal{P}.$$

Hence we can eliminate the hypothesis K/k abelian for the case $\mathcal{T}_{K/k} = \mathfrak{p}^{1-e/\mathcal{O}_K}$ (Lemma 1.4.5.)

Choose $\mathcal{P}$ as in the Proposition 2.3.3 and argue as in that Proposition, we have $\mathcal{T}_{K/k} \simeq \mathcal{O}_k/\mathfrak{p}_k \otimes_{\mathbb{F}_p} (\mathbb{Z}\Gamma \otimes_{\mathbb{Z}\Delta} T(p, \mathbb{Z}\Delta))$.

We are now ready to prove the main result of this chapter but we recall first our notations:
N/E is a finite tame Galois extensions of number fields with group G and ring of integers R and S, respectively. For any prime ideal $\mathfrak{p}$ of R we fix a prime ideal $\mathfrak{q}$ of S dividing $\mathfrak{p}$. We denote by $D_\mathfrak{q}$ (resp. $I_\mathfrak{q}$) the decomposition group (resp. the inertia group) of $\mathfrak{q}$ in the group G. Then, the cardinality of $I_\mathfrak{q}$ only depends on $\mathfrak{p}$ and we denote it by $e_\mathfrak{p}$. By Lemma 2.3.1, we fix an injective character $\chi_\mathfrak{q} : I_\mathfrak{q} \to \overline{\mathbb{Q}}^\times$ and an embedding $\iota_\mathfrak{q} : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_p$ where p is the rational number below $\mathfrak{p}$ such that $\iota_\mathfrak{q} \circ \chi_\mathfrak{q} = \chi_{N_\mathfrak{q}/F_\mathfrak{q}}$ where $N_\mathfrak{q}$ is the completion of N with respect to $\mathfrak{q}$ and $F_\mathfrak{q}$ is the fixed field of the inertia group $I_\mathfrak{q}$, i.e $F_\mathfrak{q} = N_\mathfrak{q}^{I_\mathfrak{q}}$. These choices determine a prime ideal $\mathfrak{p}$ in the ring of integers $\mathcal{O}_{e_\mathfrak{p}}$ of $\mathbb{Q}(\mu_{e_\mathfrak{p}}) \subset \overline{\mathbb{Q}}$ satisfying $\iota_\mathfrak{q}(\mathfrak{p}) \subset \mathfrak{q}S_\mathfrak{q}$, where $S_\mathfrak{q}$ is the valuation ring of $N_\mathfrak{q}$. The injection $\iota_\mathfrak{q}$ makes $\mathcal{O}_{F_\mathfrak{q}}$ into $\mathcal{O}_{e_\mathfrak{p}}-$module. We recall that $Ram(N/E)$ is the set of primes of E that ramify in N/E. In other words, if we consider the ideal $I = \mathcal{C}_{N/E}^{-1}$, which is the different of N/E, then $Ram(N/E)$ is precisely the set $Div(I)$. We are going to prove the main result of this chapter:

2.3.5 Theorem. *For every $\mathfrak{p} \in Ram(N/E)$, choose a prime $\mathfrak{q}$ of N above $\mathfrak{p}$. Then, with the notation introduced above, there is an iosmorphism of $\mathbb{Z}G-$modules:*

$$T_{N/E} \simeq \bigoplus_{\mathfrak{p}\in Ram(N/E)} \left(\mathbb{Z}G \otimes_{\mathbb{Z}D_\mathfrak{q}} T(p, \mathbb{Z}I_\mathfrak{q})\right)^{\oplus[R/\mathfrak{p}:\mathbb{F}_p]}.$$

Furthermore, for every choice of injective characters $\chi_\mathfrak{q} : I_\mathfrak{q} \to \overline{\mathbb{Q}}^\times$ for every prime $\mathfrak{q}$ as above, one can find primes $\mathcal{P}$ of $\mathcal{O}_{e_\mathfrak{p}}$ and injections $\mathcal{O}_{e_\mathfrak{p}}/\mathcal{P} \to S/\mathfrak{q}$ such that there is isomorphism of $\mathbb{Z}G-$modules:

$$\mathcal{R}_{N/E} \simeq \bigoplus_{\mathfrak{p}\in Ram(N/E)} \left(\mathbb{Z}G \otimes_{\mathbb{Z}I_\mathfrak{q}} R_{\chi_\mathfrak{q}}(\mathcal{P}, \mathcal{O}_{e_\mathfrak{p}} I_\mathfrak{q})\right)^{\oplus[G:D_\mathfrak{q}][S/\mathfrak{q}:\mathcal{O}_{e_\mathfrak{p}}/\mathcal{P}]}.$$

Moreover, if N/E is locally abelian, then the injections $\mathcal{O}_{e_\mathfrak{p}}/\mathcal{P} \to S/\mathfrak{q}$ factor through $R/\mathfrak{p} :\to S/\mathfrak{q}$ and there is an isomorphism of $\mathbb{Z}G-$modules:

$$S_{N/E} \simeq \bigoplus_{\mathfrak{p}\in Ram(N/E)} \left(\mathbb{Z}G \otimes_{\mathbb{Z}I_\mathfrak{q}} S_{\chi_\mathfrak{q}}(\mathcal{P}, \mathcal{O}_{e_\mathfrak{p}} I_\mathfrak{q})\right)^{\oplus[R/\mathfrak{p}:\mathcal{O}_{e_\mathfrak{p}}/\mathcal{P}]}.$$

Proof. Consider the ideal $I = \mathcal{C}_{N/E}^{-1}$ of S. By definition $T_{N/E} = \mathcal{C}_{N/E}/S = I^{-1}/S$.
By Proposition 2.2.1,

$$T_{N/E} \simeq \bigoplus_{\mathfrak{p}\in Div(I)} \mathbb{Z}G \otimes_{\mathbb{Z}D_\mathfrak{p}} (\mathfrak{q}^{-e_\mathfrak{p}+1} S_\mathfrak{q}/S_\mathfrak{q}).$$

By lemma 1.4.5, $\mathfrak{q}^{-e_\mathfrak{p}+1} S_\mathfrak{q}/S_\mathfrak{q} = T_{N_\mathfrak{q}/E_\mathfrak{p}}$.

By Proposition above,

$$T_{N_\mathfrak{q}/E_\mathfrak{p}} \simeq \left(\mathbb{Z}D_\mathfrak{q} \otimes_{\mathbb{Z}I_\mathfrak{p}} T(p, \mathbb{Z}I_\mathfrak{q})\right)^{\oplus[R/\mathfrak{p}:\mathbb{F}_p]}.$$

Thus the first isomorphism of the Theorem follows using the fact that $Div(I) = Ram(N/E)$.
We now prove the second isomorphism about $\mathcal{R}_{N/E}$ with choices of $\chi_\mathfrak{q}$ and $\iota_\mathfrak{q}$ as described above.
By Lemma 2.1.2 we have,

$$\mathcal{R}_{N/E} \simeq \bigoplus_{\mathfrak{p}\in Ram(N/E)} (\mathbb{Z}G \otimes_{\mathbb{Z}D_\mathfrak{q}} \mathcal{R}_{N_\mathfrak{q}/E_\mathfrak{p}})^{\oplus[G:D_\mathfrak{q}]}.$$

By Proposition 2.1.3 we have,

$$\mathcal{R}_{N_\mathfrak{q}/E_\mathfrak{p}} \simeq \mathbb{Z}D_\mathfrak{q} \otimes_{\mathbb{Z}I_\mathfrak{q}} \mathcal{R}_{N_\mathfrak{q}/F_\mathfrak{q}}.$$

By Proposition 2.1.6 we have,

$$\mathcal{R}_{N_{\mathfrak{q}}/F_{\mathfrak{q}}} \simeq \bigoplus_{i=1}^{e_{\mathfrak{p}}-1} \left(\mathfrak{q}^i S_{\mathfrak{q}}/\mathfrak{q}^{i+1} S_{\mathfrak{q}}\right).$$

By Proposition 2.3.2 we have,

$$\mathfrak{q}^i S_{\mathfrak{q}}/\mathfrak{q}^{i+1} S_{\mathfrak{q}} \simeq \mathcal{O}_{e_{\mathfrak{p}}}/\mathcal{P}(\chi_{\mathfrak{q}}^i) \otimes_{\mathcal{O}/\mathcal{P}} \mathcal{O}_{F_{\mathfrak{q}}}/\mathfrak{q}^{f_{\mathfrak{p}}\mathcal{O}_{F_{\mathfrak{q}}}}.$$

By definition

$$R_{\chi_{\mathfrak{q}}}(\mathcal{P}, \mathcal{O}_{e_{\mathfrak{p}}} I_{\mathfrak{q}}) = \bigoplus_{i=1}^{e_{\mathfrak{p}}-1} \mathcal{O}_{e_{\mathfrak{p}}}/\mathcal{P}(\chi_{\mathfrak{q}}^i).$$

Hence using the fact that $S_{\mathfrak{q}}/\mathfrak{q}S_{\mathfrak{q}} = \mathcal{O}_{F_{\mathfrak{q}}}/\mathfrak{q}^{f_{\mathfrak{p}}\mathcal{O}_{F_{\mathfrak{q}}}}$,, we have:

$$\mathcal{R}_{N_{\mathfrak{q}}/F_{\mathfrak{q}}} \simeq R_{\chi_{\mathfrak{q}}}(\mathcal{P}, \mathcal{O}_{e_{\mathfrak{p}}} I_{\mathfrak{q}}) \otimes_{\mathcal{O}_{e_{\mathfrak{p}}}/\mathcal{P}} S_{\mathfrak{q}}/\mathfrak{q}S_{\mathfrak{q}}.$$

Finally, using the property of tensor product, we have isomorphism of $\mathbb{Z}G$-modules:

$$R_{\chi_{\mathfrak{q}}}(\mathcal{P}, \mathcal{O}_{e_{\mathfrak{p}}} I_{\mathfrak{q}}) \otimes_{\mathcal{O}_{e_{\mathfrak{p}}}/\mathcal{P}} S_{\mathfrak{q}}/\mathfrak{q}S_{\mathfrak{q}} \simeq R_{\chi_{\mathfrak{q}}}(\mathcal{P}, \mathcal{O}_{e_{\mathfrak{p}}} I_{\mathfrak{q}})^{[S/\mathfrak{q}:\mathcal{O}_{e_{\mathfrak{p}}}/\mathcal{P}]},$$

and we have the second isomorphism of the theorem.
Suppose now that N/E is locally abelian. Then $E_{\mathfrak{p}}$ contains the $e_{\mathfrak{p}}^{th}$ roots of unity in $\overline{\mathbb{Q}}_p^{\times}$ and therefore $\iota_{\mathfrak{q}}$ induces an inclusion $\mathcal{O}_{e_{\mathfrak{p}}}/\mathcal{P} \to \mathcal{O}_{E_{\mathfrak{p}}}/\mathfrak{p}\mathcal{O}_{E_{\mathfrak{p}}} \simeq R/\mathfrak{p}$. Moreover, using Proposition 2.2.1 and 2.3.3, we have, isomorphisms of $\mathbb{Z}G$-modules:

$$\begin{aligned} S_{N/E} &\simeq \bigoplus_{\mathfrak{p}\in Ram(N/E)} \mathbb{Z}G \otimes_{\mathbb{Z}I_{\mathfrak{q}}} S_{N_{\mathfrak{q}}}/E_{\mathfrak{p}}, \\ &\simeq \bigoplus_{\mathfrak{p}\in Ram(N/E)} \left(\mathbb{Z}G \otimes_{\mathbb{Z}I_{\mathfrak{q}}} S_{\chi_{\mathfrak{q}}}(\mathcal{P}, \mathcal{O}_{e_{\mathfrak{p}}} I_{\mathfrak{q}})\right)^{\oplus[R/\mathfrak{p}:\mathcal{O}_{e_{\mathfrak{p}}}/\mathcal{P}]} \end{aligned}$$

□

2.4 Classes of cohomologically trivial modules

2.4.1 Definition. Let A be a $G-$module and let $i \geq 0$. We denote by $H^i(G, A)$ to be the i^{th} cohomology group of G with coefficients in A and $H_i(G, A)$ to be the i^{th} homology group of G with coefficients in A
If G is a finite group and A is a G-module, then there is a natural norm map $\overline{N}\colon H_0(G, A) \to H^0(G, A)$ taking a representative a to $\sum_{g\in G} g(a)$. **The Tate cohomology groups** $\hat{H}^i(G, A)$ are given by

- $\hat{H}^i(G, A) := H^i(G, A)$ for $i \geq 1$.
- $\hat{H}^0(G, A) := \ker \overline{N}$.
- $\hat{H}^{-1}(G, A) := \operatorname{Coker} \overline{N}$.
- $\hat{H}^i(G, A) := H_{-(i+1)}(G, A)$ for $i \leq -2$.

2.4.2 Definition. Let G be a finite group. A G-module M is said to be G-cohomologically free if, for every $i \in \mathbb{Z}$ and every subgroup H of G, the Tate cohomology group $\hat{H}^i(H, M)$ is trivial.

2.4.3 Definition. Let A be the ring of integers of a number field and M an AG-module. For any prime $\mathfrak{p}$ of A, we denote by $M_{\mathfrak{p}} := A_{\mathfrak{p}} \otimes_A M$ the completion of M with respect to $\mathfrak{p}$ where $A_{\mathfrak{p}}$ is the completion of A at $\mathfrak{p}$. We know that $M_{\mathfrak{p}}$ is an $A_{\mathfrak{p}}$-module.

- We say that M is **AG-locally free module** if $M_{\mathfrak{p}}$ is free $A_{\mathfrak{p}}$-module for all prime $\mathfrak{p}$.
- The class group of $\Lambda := AG$, denoted by $Cl(\Lambda)$ is the group

  $$Cl(\Lambda) := \frac{\{\text{ locally free modules over } \Lambda\}}{\sim},$$

  where $\sim$ is defined as follows: for all M, N locally free modules over Λ,

  $$M \sim N \text{ if and only if } M \oplus \Lambda^n \simeq N \oplus \Lambda^n \text{ for some positive integer } n.$$

The following lemma will be usefull in this section. We will omit the proof but it can be seen in [CV].

2.4.4 Lemma. Let A be the ring of integers of a number field. Let M be a finitely generated AG-module.

i M is AG-projective if and only if it is AG-locally free.

ii M is G-cohomologically trivial if and only if there exists an AG-resolution

$$0 \to P_1 \to P_0 \to M \to 0$$

of M with P_i locally free, $i = 0, 1$. In this case the class $(P_0)^{-1}(P_1)$ in $Cl(AG)$ is independent of the chosen locally free resolution of M and will be denoted by $(M)_{AG}$.

iii If H is a subgroup of a finite group G and M is $H-$cohomologically trivial, then the induced module $M \otimes_{AH} AG$ is $G-$cohomologically trivial and we have

$$(M \otimes_{AH} AG)_{AG} = Ind_H^G((M)_{AH})$$

where $Ind_H^G : Cl(AH) \to Cl(AG)$ is the map which sends the class $(P)_{AH} \in Cl(AH)$ of locally free AH-module P to the class $(P \otimes_{AH} AG)_{AG}$ in $Cl(AG)$.

In this section, we will use this lemma with $A = \mathbb{Z}$ but later we will take A to be the ring of integers of a cyclotomic field. To simplify the notation, we write (M) for the class of M in $Cl(\mathbb{Z}G)$ instead of $(M)_{\mathbb{Z}G}$.

Local case

Let us start first for the local case. Let K/k be tame Galois extension of $\mathbb{Q}_p$ with group Γ and inertia group Δ. Set $F = K^{\Delta}$.

By [[Ull69], Theorem 2], we have that for any $a, b \in \mathbb{Z}$, with $b \geq a$ the ideals $\mathfrak{p}_K^a$ and $\mathfrak{p}_K^b$ are $\Gamma-$cohomologically trivial. Hence the $\mathbb{Z}\Gamma-$module $\mathfrak{p}_K^a/\mathfrak{p}_K^b$ is $\Gamma-$cohomologically trivial.

2.4.5 Proposition. For every natural integer m and n such that $m \equiv n \bmod e$, we have

$$(\mathcal{O}_K/\mathfrak{p}_K^n) = (\mathcal{O}_K/\mathfrak{p}_K^m) \in Cl(\mathbb{Z}G).$$

Proof. Assume that $n \geq m$ and write $n = m + ae$, for some $a \in \mathbb{N}$. We have equality in $Cl(\mathbb{Z}\Gamma)$

$$(\mathcal{O}_K/\mathfrak{p}_K^n) = (\mathcal{O}_K/\mathfrak{p}_K^m)(\mathfrak{p}_K^m/\mathfrak{p}_K^n) = (\mathcal{O}_K/\mathfrak{p}_K^m)\prod_{j=1}^{a}(\mathfrak{p}_K^{m+(j-1)e}/\mathfrak{p}_K^{m+je}).$$

Thus it is enough to prove that for every $b \in \mathbb{N}, (\mathfrak{p}_K^b/\mathfrak{p}_K^{b+e}) = 0$ in $Cl(\mathbb{Z}\Gamma)$. Arguing as in the proof of Proposition 2.1.6, $\mathfrak{p}_K^b/\mathfrak{p}_K^{b+e}$ is an $\mathcal{O}_F/\mathfrak{p}_F\Delta$-module and since $\mathcal{O}_F/\mathfrak{p}_F\Delta$ is semisimple, we have an isomorphism of $\mathcal{O}_k\Gamma$-modules , (in particular $\mathbb{Z}\Gamma$-modules)

$$\mathfrak{p}_K^b/\mathfrak{p}_K^{b+e} \simeq \mathcal{O}_k/\mathfrak{p}_k \otimes_{\mathbb{F}_p} \mathbb{F}_p\Gamma$$

On ther hand, $\mathbb{F}_p\Gamma$ is a cohomologically trivial Γ-module with trivial class in $Cl(\mathbb{Z}\Gamma)$ thanks to the $\mathbb{Z}\Gamma$-free resolution

$$0 \to p\mathbb{Z}\Gamma \to \mathbb{Z}G \to \mathbb{F}_p\Gamma \to 0.$$

Hence we have $(\mathfrak{p}_K^b/\mathfrak{p}_K^{b+e}) = 0$ and the result follows. □

Global case

We now back to the global case. We recall that N/E is tame Galois extension of number fields with finite group G. From Proposition 1.3 of [Ull69], every G-stable is fractional ideal of N is $\mathbb{Z}G$-projective, hence locally free by Lemma 2.4.4. In particular, if I is a G-stable ideal of S, then S/I and I^{-1}/S are $G-$cohomologically trivial by Lemma 2.4.4 again. Therefore, we can consider the classes (S/I) and (I^{-1}/S) in $Cl(\mathbb{Z}G)$. Note that

$$(S/I) = (I)(S)^{-1} \text{ and } (I^{-1}/S) = (I)^{-1}(S).$$

Similarly, $\mathcal{R}_{N/E}$ defines a class in $Cl(\mathbb{Z}G)$. In fact, we know that $\mathrm{Map}(G,S)$ is free RG-module of rank 1 hence $\mathbb{Z}G$-free of rank $[N:\mathbb{Q}]$. Noether's theorem states that S is RG-locally free module, hence $S \otimes_R S$ is SG-locally free. Thus,

$$(\mathcal{R}_{N/E}) = (S \otimes_R S) \in Cl(\mathbb{Z}G).$$

On the other hand, for every prime $\mathfrak{p}$ of R we fix a prime $\mathfrak{q}$ of S. For any integer i, the $I_\mathfrak{q}$-module $\mathcal{O}_{e_\mathfrak{p}}(\chi_\mathfrak{q}^i)$ is cohomologically trivial. In fact, for every $i \in \mathbb{Z}$ and every subgroup I of $I_\mathfrak{q}$, the Tate cohomology $\hat{H}^i(I, \mathcal{O}_{e_\mathfrak{p}}(\chi_\mathfrak{q}^i))$ is annhilated by $e_\mathfrak{p}$ and p since p annihilates $\mathcal{O}_{e_\mathfrak{p}}(\chi_\mathfrak{q}^i)$.

Since N/E is tame, we have $\gcd(e,p) = 1$ and hence $\hat{H}^i(I, \mathcal{O}_{e_\mathfrak{p}}(\chi_\mathfrak{q}^i)) = 0$. Thus, $\mathcal{O}_{e_\mathfrak{p}}(\chi_\mathfrak{q}^i)$ defines a class in $Cl(\mathbb{Z}I_\mathfrak{q})$ by Lemma 2.4.4.

2.4.6 Proposition. Let I be a $G-$invariant ideal of S and assume that N/E is locally abelian at $\mathfrak{p} \in Div(I)$. For every prime $\mathfrak{p} \in Div(I)$, we fix a prime $\mathfrak{q}$ of S dividng $\mathfrak{p}$ and let $n_\mathfrak{p}$ be the valuation of I at $\mathfrak{q}$. ($n_\mathfrak{p}$ depends only on $\mathfrak{p}$.) For every choice of character $\chi_\mathfrak{q} : I_\mathfrak{q} \to \overline{\mathbb{Q}}^\times$ for every $\mathfrak{q}$ as above, one can find primes $\mathcal{P} \subset \mathcal{O}_{e_\mathfrak{p}}$ and injections $\mathcal{O}_{e_\mathfrak{p}}/\mathcal{P} \to S/\mathfrak{q}$ such that we have equalities in $Cl(\mathbb{Z}G)$

$$(S/I) = \bigoplus_{\mathfrak{p}\in Div(I)} \bigoplus_{i=0}^{m_\mathfrak{p}-1} Ind_{I_\mathfrak{q}}^G \left((\mathcal{O}_{e_\mathfrak{p}}/\mathcal{P}(\chi_\mathfrak{q}^i))\right)^{[R/\mathfrak{p}:\mathcal{O}_{e_\mathfrak{p}}/\mathcal{P}]},$$

$$(I^{-1}/S) = \bigoplus_{\mathfrak{p}\in Div(I)} \bigoplus_{i=0}^{m_\mathfrak{p}} Ind_{I_\mathfrak{q}}^G \left((\mathcal{O}_{e_\mathfrak{p}}/\mathcal{P}(\chi_\mathfrak{q}^{e_\mathfrak{p}-i}))\right)^{[R/\mathfrak{p}:\mathcal{O}_{e_\mathfrak{p}}/\mathcal{P}]}$$

where $m_\mathfrak{p}$ is the smallest nonegative integer congruent to $n_\mathfrak{p}$ modulo $e_\mathfrak{p}$. In particular, if I is coprime to the different of N/E, then $(S/I) = (I^{-1}/S) = 1$.

Proof. We prove only the first isomorphism since the proof of the second is similar.

By Proposition 2.2.1, we get an isomorphism of RG-modules:

$$S/I \simeq \bigoplus_{\mathfrak{p}\in Div(I)} \mathbb{Z}G \otimes_{\mathbb{Z}I_\mathfrak{q}} S_{N_\mathfrak{q}}/\mathfrak{q}^{n_\mathfrak{p}} S_\mathfrak{q}.$$

By Proposition 2.4.5 and 2.3.3, we have the following equality in $Cl(\mathbb{Z}D_\mathfrak{q})$:

$$\begin{aligned}(\mathcal{O}_{N_\mathfrak{q}}/\mathfrak{q}^{n_\mathfrak{p}}\mathcal{O}_{N_\mathfrak{q}}) &= (\mathcal{O}_{N_\mathfrak{q}}/\mathfrak{q}^{m_\mathfrak{p}}\mathcal{O}_{N_\mathfrak{q}}) \\ &= \left(\mathbb{Z}D_\mathfrak{q} \otimes_{\mathbb{Z}I_\mathfrak{q}} (\oplus_{i=0}^{m_\mathfrak{p}-1}(\mathcal{O}_{e_\mathfrak{p}}/\mathcal{P}(\chi_\mathfrak{q}^i)))\right)^{R/\mathfrak{p}:\mathcal{O}_{e_\mathfrak{p}}/\mathcal{P}}.\end{aligned}$$

The results now follows from the Lemma 2.4.4. For the last assertion, we know that if I is coprime with the different of N/E, then for every prime $\mathfrak{q}$ dividing I we have $I_\mathfrak{q}$ is trivial. In particular the character $\chi_\mathfrak{q}$ is trivial, $e_\mathfrak{p} = 1$ and $\mathcal{O}_{e_\mathfrak{p}}/\mathcal{P} = \mathbb{F}_p$, by Corollary 2.3.4. Thus for every $i \in \mathbb{Z}$, we have

$$\begin{aligned}Ind_{I_\mathfrak{q}}^G((\mathcal{O}_{e_\mathfrak{p}}/\mathcal{P})(\chi_\mathfrak{q}^i)) &= ((\mathcal{O}_{e_\mathfrak{p}}/\mathcal{P})(\chi_\mathfrak{q}^i)) \otimes_{\mathbb{Z}I_\mathfrak{q}} \mathbb{Z}G) \\ &= (\mathbb{F}_p \otimes_\mathbb{Z} \mathbb{Z}G) \\ &= (\mathbb{F}_p) \\ &= 1.\end{aligned}$$

□

This Proposition can be used to prove the following interesting Theorem. Recall that $S \otimes_R S$ is an $\mathbb{Z}G-$module by the action for all $a, b \in S$ and $g \in G$,

$$g.(a \otimes b) = a \otimes g(b).$$

Before stating the theorem, we recall the Chebotarev's density theorem

2.4.7 Lemma. Let L be a finite Galois extension of a number field K with Galois group G. Let X be a subset of G that is stable under conjugation. The set of primes $\mathfrak{p}$ of K that are unramified in L and whose associated Frobenius conjugacy class $\sigma_{\mathfrak{p}}$ is contained in X has density $\frac{\#X}{\#G}$. In paritcular, this ratio is strictly positive so there always exist such primes.

2.4.8 Theorem.

$$(S \otimes_R S) = (S)^{[N:E]} \text{ } in \text{ } Cl(\mathbb{Z}G).$$

Proof. Write $n = [N : E]$. By the structure theorem for modules over Dedekind Domain, we know that S is R-isomorphic to $R^{\oplus(n-1)} \oplus J$, where J is an ideal of R. By Chebotarev's density theorem (Lemma 2.4.7), there exists an ideal I of R belonging to the ideal class of J and such that I is coprime with the discriminant of N/E. Thus S is isomorphic to $R^{\oplus(n-1)} \otimes I$ as $R-$module. By the property of the tensor product, we have RG-isomorphisms since G acts only on the right factor of $S \otimes_R S$:

$$S \otimes_R S \simeq (R \otimes_R S)^{\oplus(n-1)} \oplus (I \otimes_R S) \simeq S^{\oplus(n-1)} \oplus IS.$$

In partiular,

$$(S \otimes_R S) = (S)^{\oplus(n-1)}(IS).$$

IS is of course a $G-$stable ideal of S since I is an ideal of R, then it is locally free because N/E is tame. Hence S/IS is $G-$cohomologically trivial by Lemma 2.4.4 and we have

$$(IS) = (S)(S/IS) \text{ in } Cl(\mathbb{Z}G).$$

Since IS is coprime with the different of N/E, then by Proposition 2.4.6 $(IS) = (S)$, and the results follows. □

Chapter 3

Hom-representatives

In this chapter, we are going to prove the Theorem 1.2.2 in the introduction which is the core of this work as we said. We apply Frohlich's machinery to get a description of Hom-representatives of the classes involved in its statements.

We now focus on the cyclotomic fields to study the modules $\mathcal{T}, \mathcal{R}$ and $\mathcal{S}$. Let's recall the notation in the introduction.

We fix an integer e, a cyclic group $\Delta =< \delta >$ of order e and an injective character $\chi : \Delta \to \mu_e$, where μ_e is the group of e^{th} roots of unity in $\mathbb{Q}$. We denote by $\mathcal{O}$ the ring of integers of the cyclotomic field $\mathbb{Q}(\mu_e)$. Let p be a rational prime such that $p \nmid e$ and let $\mathfrak{p}$ be a prime of $\mathcal{O}$ above p. Set $\kappa = \mathcal{O}/\mathfrak{p}$. To simplify the notation, we set

$$\mathcal{T}_{\mathbb{Z}} = T(p, \mathbb{Z}\Delta), \mathcal{R} = \mathcal{R}_\chi(\mathfrak{p}, \mathcal{O}\Delta), \mathcal{S} = \mathcal{S}_\chi(\mathfrak{p}, \mathcal{O}\Delta).$$

We fix a primitive e^{th} root of unity $\zeta \in \mu_e$ and for $\delta \in \Delta$ we define by $\chi(\delta) = \zeta$.

3.1 Hom description of the class group

3.1.1 Definition. (The group of idele)

Let L be a number field and $\mathcal{O}_L$ its ring of integers. Set $\Omega_L = \mathrm{Gal}(\overline{\mathbb{Q}}/L)$. The ring A_L of finite adeles is defined as the set of elements $x = (x_\mathfrak{p})_\mathfrak{p}$ in the direct product of the completions $L_\mathfrak{p}$ of L at the finite primes $\mathfrak{p}$ of L, such that, except for finitely many prime $\mathfrak{p}$, the components $x_\mathfrak{p}$ lie in the valuation ring $\mathcal{O}_{L,\mathfrak{p}}$ of $L_\mathfrak{p}$. More precisely,

$$A_L = \{x = (x_\mathfrak{p})_\mathfrak{p} \in \prod_\mathfrak{p} L_\mathfrak{p}, x_\mathfrak{p} \in \mathcal{O}_{L,\mathfrak{p}} \text{ for almost all primes } \mathfrak{p}\}.$$

The group of finite ideles $J(L)$ is the group of units of A_L. An adele $(x_\mathfrak{p})_\mathfrak{p}$ is an idele if and only if its components are all non-zero and except for finitely many $\mathfrak{p}$, they lie in the units of $\mathcal{O}_{L,\mathfrak{p}}$, that is

$$J(L) = \{x = (x_\mathfrak{p})_\mathfrak{p} \in \prod_\mathfrak{p} L_\mathfrak{p}, x_\mathfrak{p} \in \mathcal{O}_{L,\mathfrak{p}}^\times \text{ for almost all primes } \mathfrak{p}\}.$$

For any extension F of L we have

$$A_F = F \otimes_L A_L.$$

If F/L is Galois, we thus get an action on A_F by the Galois group $G = (\mathrm{Gal}(F/L))$, via its action on F and this action induces an action $J(L)$. The action on ideles is defined as follows. Let $x = (x_\mathfrak{q})_\mathfrak{q}$ be an idele of

F. We know that the group G acts transitively on the primes $\mathfrak{q}$ above a given prime $\mathfrak{p}$ of L. For any prime $\mathfrak{q}$ of F, an element $\sigma \in G$ induces an isomorphism $\sigma_{\mathfrak{q}} : F_{\mathfrak{q}} \to F_{\sigma(\mathfrak{q})}$. So the idele σx is the idele given by

$$(\sigma x)_{\sigma(\mathfrak{q})} = \sigma_{\mathfrak{q}}(x_{\mathfrak{q}}).$$

It follows from the above that $J(F)^{G_L} = J(L)$.

3.1.2 Definition. (The group of virtual character)
Let G be a finite group. The group of virtual character R_G is the $\mathbb{Z}$-linear combinations of the irreducible characters of G. R_G can also be equipped with a ring structure coming from the tensor product of representations (Theorem 1.3.28).

If G is Galois group of extension of number fields F/L, then G acts on R_G by acting on the values of the characters: that is, for any $\sigma \in G$ and $\chi \in R_G$

$$(\sigma.\chi)(g) = \sigma(\chi(g)), g \in G.$$

If F is a big enough extension of L contained in $\overline{\mathbb{Q}}$, contains L and the values of the characters of G then we can consider the group of all homomorphisms between the commutative groups R_G and $J(F)$ and which commute with the action of G i.e: the group of Galois equivariant homomorphisms

$$\mathrm{Hom}_G(R_G, J(F)).$$

We know that $F^\times$ can be embedded diagonally in $J(F)$, hence we get a subgroup $\mathrm{Hom}_G(R_G, F^\times)$ of $\mathrm{Hom}_G(R_G, J(F))$.

Let $\mathcal{U}(\mathcal{O}_L)$ denote the ring of finite integral adeles of L, that is the product over all prime ideals $\mathfrak{p}$ in $\mathcal{O}_L$ of the completed localisations $\mathcal{O}_{L,\mathfrak{p}}$ of $\mathcal{O}_L$.

We define

$$\mathcal{U}(\mathcal{O}_L G) = \prod_{\mathfrak{p}} \mathcal{O}_{L,\mathfrak{p}} G^\times \subseteq \prod_{\mathfrak{p}} L_{\mathfrak{p}} G^\times.$$

Recall that by Lemma 1.4.2, we have

$$F \otimes_L L_{\mathfrak{p}} \simeq \prod_{\mathfrak{q}|\mathfrak{p}} F_{\mathfrak{q}},$$

then, $(F \otimes_L L_{\mathfrak{p}})^\times$ can be embedded in $J_{\mathfrak{p}}(F) := \prod_{\mathfrak{q}|\mathfrak{p}} F_{\mathfrak{q}}^\times$.
Let us now define the determinant homomorphism Det:

Let $x = (x_{\mathfrak{p}})_{\mathfrak{p}} \in \prod_{\mathfrak{p}} L_{\mathfrak{p}} G^\times$. The the determinant homomorphism $\mathrm{Det}(x) = (\mathrm{Det}(x_{\mathfrak{p}}))_{\mathfrak{p}}$ is defined componentwise. For each prime $\mathfrak{p}$ of L, the component $\mathrm{Det}(x_{\mathfrak{p}})$ takes values in $(F \otimes_L L_{\mathfrak{p}})^\times \subset J_{\mathfrak{p}}(F)$. So we only need to define $\mathrm{Det}(x_{\mathfrak{p}})$ for each prime $\mathfrak{p}$. By linearity, it is sufficient to define $\mathrm{Det}(x_{\mathfrak{p}})$ only on the irreducible characters χ of G. Write $x_{\mathfrak{p}} = \sum_{g \in G} x_{\mathfrak{p},g} g$, and let χ be an irreducible character of G with matrix representation $X = (a_{ij})_{i,j}$. Then we define $\mathrm{Det}(x_{\mathfrak{p}}(\chi)$ to be the determinant of the matrix

$$\left(\sum_{g \in G} a_{ij}(g) \otimes x_{\mathfrak{p},g} \right)_{i,j},$$

where $\sum_{g \in G} a_{ij}(g) \otimes x_{\mathfrak{p},g} \in F \otimes_L L_{\mathfrak{p}}$.

We are now ready to give the Hom-description of $Cl(\mathcal{O}_L G)$ which is the group

$$\frac{\mathrm{Hom}_G(R_G, J(F))}{\mathrm{Hom}_G(R_G, F^\times)\,\mathrm{Det}(\mathcal{U}(\mathcal{O}_L G))}$$

In case where G is abelian group, we know that each character is of dimension 1 so there is no determinant. Thus using the notation as above, we have

$$\mathrm{Det}(x_{\mathfrak{p}})(\chi) = \sum_{g\in G} x_{\mathfrak{p},g}\chi(g).$$

In our cyclotomic setting introduced above, we shall only be concerned with the cases where $L = \mathbb{Q}$,$F = \mathbb{Q}(\mu_e)$ and $G = \Delta$. We are now in the case that Δ is abelian even cyclic, so we have the simple formula of the determinant map. This is why we do the reduction to the inertia group in Chapter 2.

3.2 Hom-representative of $(T_{\mathbb{Z}})$

Let us consider the Swan module $\sum_{\Delta}(p) := p\mathbb{Z}\Delta + \mathrm{Tr}\,\mathbb{Z}\Delta$ and its associated torsion module $\mathcal{T}_{\mathbb{Z}} = \mathbb{Z}\Delta/\sum_{\Delta}(p)$. We have the following exact sequence of $\mathbb{Z}\Delta$-modules:

$$0 \to \sum_{\Delta}(p) \to \mathbb{Z}\Delta \to \mathcal{T}_{\mathbb{Z}} \to 0.$$

By Swan, $\sum_{\Delta}(p)$ is $\mathbb{Z}\Delta$-projective so locally free by Lemma 2.4.4. Therefore, $\mathcal{T}_{\mathbb{Z}}$ is Δ-cohomologically trivial and $\mathcal{T}_{\mathbb{Z}}$ and $\sum_{\Delta}(p)$ define the same classes in $Cl(\mathbb{Z}\Delta)$, that is

$$(\mathcal{T}_{\mathbb{Z}}) = (\sum_{\Delta}(p)) \text{ in } Cl(\mathbb{Z}\Delta).$$

So we are going to find a representative of $\sum_{\Delta}(p)$.

3.2.1 Lemma. The class of the Swan module $\sum_{\Delta}(p)$ in $Cl(\mathbb{Z}\Delta)$ is represented by $v \in \mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_{\Delta}, J(\mathbb{Q}))$ which is defined by for any $h = 1, \ldots, e$ and any rational prime q, the q^{th}component of $v(\chi^h)$ is given by 1 if $q \neq p$ or $h = e$, and given by p otherwise.

Proof. Since $\sum_{\Delta}(p)$ is locally free $\mathbb{Z}\Delta$-module, then for any rational prime q, the $\mathbb{Z}_q\Delta$- module $\mathbb{Z}_q \otimes_{\mathbb{Z}} \sum_{\Delta}(p)$ is free of rank 1. We are now going to find its generator α_q.

If $q \neq p$, then $p\mathbb{Z}_q = \mathbb{Z}_q$ and $\mathbb{Z}_q \otimes_{\mathbb{Z}} \sum_{\Delta}(p) = \mathbb{Z}_q\Delta$. Thus, we can take $\alpha_q = 1$.

If $q = p$, we consider the idempotent elements $\epsilon_0 := \frac{1}{e}\mathrm{Tr}_{\Delta}$ and $\epsilon_1 := 1 - \epsilon_0$. Since e is coprime to p, then e is invertible in $\mathbb{Z}_q$ and $\epsilon_0, \epsilon_1 \in \mathbb{Z}_q\Delta$. By definition of $\sum_{\Delta}(p)$, we have $\mathbb{Z}_q \otimes_{\mathbb{Z}} \sum_{\Delta}(p) = p\mathbb{Z}_p\Delta + \frac{1}{e}\mathbb{Z}_q\Delta$. Take $\alpha_p = \epsilon_0 + p\epsilon_1$. We have to show that $(\epsilon_0 + p\epsilon_1)\mathbb{Z}_q\Delta = \mathbb{Z}_q \otimes_{\mathbb{Z}} \sum_{\Delta}(p)$. Clearly, $\epsilon_0 + p\epsilon_1 \in p\mathbb{Z}_p\Delta + \frac{1}{e}\mathbb{Z}_q\Delta$. The other inclusion follows by writting $p = (\epsilon_0 + p\epsilon_1)(p\epsilon_0 + \epsilon_1)$ and $\epsilon_0 = (\epsilon_0 + p\epsilon_1)\epsilon_0$ since $\epsilon_0\epsilon = 0$.

On the other hand, by Frohlich's theory, the homomorphism $\chi^h \mapsto (\mathrm{Det}(\alpha_q)(\chi^h))_q$ represents the modules $\sum_{\Delta}(p)$ in $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_{\Delta}, J(\mathbb{Q}))$. By computation $\mathrm{Det}(\alpha_p)(\chi^h) = p + (1-p)\delta_{h,e}$, where $\delta_{h,e}$ is the Kronecker Delta. Thus the lemma follows. □

3.3 Hom-representatives of $(\mathcal{R})$ and $(\mathcal{S})$

In this section, we will find the Hom-representatives of $(\mathcal{R})$ and $(\mathcal{S})$. Recall that in the previous section we saw that (with the assumption that e is odd for the case of $\mathcal{S}$.)

$$\mathcal{R} = \prod_{i=1}^{e-1} \kappa(\chi^i)^i \text{ and } \mathcal{S} = \prod_{i=e+1/2}^{e-1} \kappa(\chi^i).$$

Thus we have the equalities of classes

$$(\mathcal{R}) = \prod_{i=1}^{e-1} (\kappa(\chi^i)) \text{ and } (\mathcal{S}) = \prod_{i=e+1/2}^{e-1} (\kappa(\chi^i)).$$

Since the Hom-description is a group isomorphism, then we are done once we have the representatives of $\kappa(\chi^i)$ for all $i = 1, \ldots, e-1$.

Let's now compute the Hom-representative of $\kappa(\chi^i)$ for a fixed i. Recall first that $\Delta =< \delta >$ is cyclic of order e and $\kappa(\chi^i)$ is an $\mathcal{O}\Delta-$module with underling set $\kappa = \mathcal{O}/\mathfrak{p}$ and with Δ-action defined by

$$\delta.x = \chi^i(\delta)x = \zeta^i x, \text{ for all } x \in \kappa.$$

Before computing this, we have to introduce a new $\mathcal{O}\Delta$-module M_i defined by

$$M_i := \mathfrak{p}\mathcal{O}\Delta + (\delta - \zeta^i)\mathcal{O}\Delta.$$

The next lemma shows that M_i is locally free and gives us a precise local generator. The proof can be seen in [Proposition 3.4 of [**?**]].

3.3.1 Lemma. For avery prime $\mathfrak{q}$ of $\mathcal{O}$, $\mathcal{O}_\mathfrak{q} \otimes_\mathcal{O} M_i = x_{i,\mathfrak{q}}\mathcal{O}_\mathfrak{q}\Delta$ where

$$x_{i,\mathfrak{q}} = \begin{cases} 1 & \text{if } \mathfrak{q} \neq \mathfrak{p}. \\ 1 + (p-1)\epsilon_i & \text{if } \mathfrak{q} = \mathfrak{p}. \end{cases}$$

and $\epsilon_i = \frac{1}{e}\sum_{j=0}^{e-1} \zeta^{ij}\delta^{-j} \in \mathcal{O}_\mathfrak{q}\Delta$. In particular, the $\mathcal{O}\Delta$-module M_i is locally free.

3.3.2 Proposition. The $\mathcal{O}\Delta$-modules $\kappa(\chi^i)$ and M_i define the same classes in $Cl(\mathcal{O}\Delta)$. Furthermore, the homomorphism v_i with values in the ideles group $J(\mathbb{Q}(\zeta))$, defined at any prime $\mathfrak{q}$ of $\mathcal{O}$ by

$$v_i(\chi^h)_\mathfrak{q} = \begin{cases} p & \text{if } \mathfrak{q} = \mathfrak{p}, i \equiv h(\bmod e). \\ 1 & \text{otherwise.} \end{cases}$$

represents the class of $(\kappa(\chi^i))_{\mathcal{O}\Delta}$ in $\mathrm{Hom}_{\Omega_\mathbb{Q}}(R_\Delta, J(\mathbb{Q}(\zeta)))$.

Proof. We show the first assertion. Consider the homomorphism of $\mathcal{O}\Delta$-modules

$$\phi_i : \mathcal{O}\Delta \to \kappa(\chi^i)$$

sending 1 to 1. In particular, we have $\phi_i(\delta) = \zeta^i$. Clearly, ϕ_i is surjective since $\mathcal{O} \to \kappa$ is surjective. By definition of M_i we have $M_i \subset \ker(\phi_i)$. On the other hand, we have $\sharp\mathcal{O}\Delta/M_i = \sharp\mathcal{O}/\mathfrak{p}$. Thus we have the following exact sequence

$$0 \to M_i \to \mathcal{O}\Delta \to \kappa(\chi^i) \to 0.$$

We know that $\mathcal{O}\Delta$ is free $\mathbb{Z}\Delta$-module, so it is $\Delta-$cohomologically trivial. We have seen also that $\kappa(\chi^i)$ is cohomologically trivial. By Lemma 3.3.1, M_i is locally free. So by Lemma 2.4.4, we have

$$(\kappa(\chi^i))_{\mathcal{O}\Delta} = (\mathcal{O}\Delta)^{-1}_{\mathcal{O}\Delta}(M_i)_{\mathcal{O}\Delta} = (M_i)_{\mathcal{O}\Delta} \text{ in } Cl(\mathcal{O}\Delta).$$

This proves the first assertion.

To prove the last assertion, by Lemma 3.2.1 $\chi^h \mapsto (\mathrm{Det}(x_{i,\mathfrak{q}})(\chi^h))_\mathfrak{q}$ is a representative of $(\kappa(\chi^i))_{\mathcal{O}\Delta}$ in $Cl(\mathcal{O}\Delta)$. Consider the idempotent $\epsilon_i = \frac{1}{e}\sum_{j=0}^{e-1} \zeta^{ij} \det^{-j}$ as in Lemma 3.3.1.

If $\mathfrak{q} \neq \mathfrak{p}$, we have $x_{i,\mathfrak{q}} = 1$ and $(\mathrm{Det}(x_{i,\mathfrak{q}})(\chi^h))_{\mathfrak{q}} = 1$.

If $\mathfrak{q} = \mathfrak{p}$, we have $x_{i,\mathfrak{p}} = 1 + (p-1)\epsilon_i$ and

$$\begin{aligned}(\mathrm{Det}(x_{i,\mathfrak{p}})(\chi^h))_{\mathfrak{p}} &= (\mathrm{Det}(1 + (p-1)\epsilon_i)(\chi^h))_{\mathfrak{p}} \\ &= (1 + \frac{p-1}{e})\chi^h(1) + \frac{1}{e}\sum_{j=1}^{e-1} \zeta^{ij}\chi^h(\delta^{-j}) \\ &= 1 + \frac{p-1}{e}\sum_{j=1}^{e-1}\zeta^{(i-h)j})\end{aligned}$$

If $i - h \neq 0 \bmod e$, then $\sum_{j=1}^{e-1}\zeta^{(i-h)j} = 0$ by the well known fact saying that the sum of all n^{th} roots of unity is 0.

If $i - h \equiv 0 \bmod e$, thus $\sum_{j=1}^{e-1}\zeta^{(i-h)j} = e$ and the result follows.

□

By the above Proposition, we get a representative of the class $(\kappa(\chi^i))_{\mathcal{O}\Delta}$. Now, we want to find a representative of the class $((\kappa(\chi^i))_{\mathbb{Z}\Delta})$. In order to find it, as usual we take the norm of v_i but here we have to define the norm of a homomorphism, denoted $\mathcal{N}(v_i) = \mathcal{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(v_i)$.

3.3.3 Definition. For each $h = 0, \dots, e-1$, the $\mathfrak{q}^{th}$ component of $\mathcal{N}(v_i)(\chi^h)$ is defined by

$$\mathcal{N}(v_i)(\chi^h)_{\mathfrak{q}} = (\prod_{\sigma\in\Delta}\sigma^{-1}.(v_i(\sigma.\chi^h)))_{\mathfrak{q}}.$$

where $\sigma.\chi^h$ is the action of σ on χ^h and $\sigma^{-1}.v_i(\sigma.\chi^h)$ is the action of σ^{-1} on the idele $(v_i(\sigma.\chi^h)_{\mathfrak{q}})$.

Since Δ is cyclic, using the following notation, we can re-write $\mathcal{N}(v_i)$ precisely.
Let us recall some basic results from number theory.

3.3.4 Remark. Denote $\bar{n}$ to be the $n \bmod e$. We have a group isomorphism,

$$\begin{array}{rcl}\sigma\colon (\mathbb{Z}/e\mathbb{Z})^\times & \to & \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}), \\ \bar{n} & \mapsto & \sigma_n(\zeta) = \zeta^n.\end{array}$$

This sends the subgroup generated by $\bar{p}$ to the decomposition group of $\mathfrak{p}$ dividing p. We have only one decomposition group D since the extension is abelian.

In particular, $\sigma_p(\mathfrak{p}) = \mathfrak{p}$. Thus for any $\Lambda \in \mathbb{Z}/e\mathbb{Z})^\times / < \bar{p} >$, $\sigma_\Gamma(\mathfrak{p}) = \sigma_\lambda(\mathfrak{p}).D$ for any lift $\lambda \in \mathbb{Z}/e\mathbb{Z})^\times$ of Γ. Then we can denote by $\sigma_\Gamma(\mathfrak{p})$ the ideal $\sigma_\lambda(\mathfrak{p})$ for any lift λ of Λ. Note also that $\sigma_\Lambda(\mathfrak{p}), \Lambda \in \mathbb{Z}/e\mathbb{Z})^\times / < \bar{p} >$ are the prime ideals of $\mathcal{O}$ above p and for $\alpha \in \mathbb{Z}/e\mathbb{Z})^\times$, we have

$$\sigma_\alpha(\mathfrak{p}) = \sigma_\Lambda(\mathfrak{p}) \Leftrightarrow \alpha \in \Lambda. \tag{3.1}$$

Using this notation, we can write

$$\mathcal{N}(v_i)(\chi^h)_{\mathfrak{q}} = \prod_k \sigma_k^{-1}\left((v_i(\chi^{hk})_{\sigma_k(\mathfrak{p})})\right).$$

where the product runs over the integers $k = 0, \dots, e-1$ and coprime to e.

The following Proposition gives us an easy formula of $\mathcal{N}(v_i)(\chi^h)_{\mathfrak{q}}$. Set $n(\Lambda, i, h) = \sharp\{\alpha \in \Lambda, \alpha\bar{i} = \bar{h}\}$ for any $i, h \in \{0, e-1\}$.

3.3.5 Proposition. For any prime $\mathfrak{q}$ of $\mathcal{O}$ and for any $h = 0, \ldots, e-1$, we have

$$\mathcal{N}(v_i)(\chi^h)_{\mathfrak{q}} = \begin{cases} 1 & \text{if } \mathfrak{q} \nmid p \\ p^{n(\Lambda,i,h)} & \text{if } \mathfrak{q} = \sigma_\Lambda(\mathfrak{p}) \text{ for some } \Lambda \in \mathbb{Z}/e\mathbb{Z})^\times / < \bar{p} > . \end{cases}$$

Proof. If $\mathfrak{q} \nmid p$, it is clear that $\mathcal{N}(v_i)(\chi^h)_{\mathfrak{q}} = 1$.

If $\mathfrak{q}|p$, then it is of the form $\mathfrak{q} = \sigma_\Lambda(\mathfrak{p})$ for some $\Lambda \in \mathbb{Z}/e\mathbb{Z})^\times / < \bar{p} >$.

For any integer $k = 0, \ldots, e-1$ and coprime to e, we have

$$\begin{aligned} \sigma_k(\mathfrak{q}) = \mathfrak{p} \quad &\Leftrightarrow \quad \sigma_\Lambda(\mathfrak{p}) = \sigma_{k^{-1}}(\mathfrak{p}) \\ &\Leftrightarrow \quad \bar{k}^{-1} \in \Lambda. \end{aligned}$$

By Proposition 3.3.2, we have

$$v_i(\chi^{hk})_{\sigma_k(\mathfrak{q})} = \begin{cases} p & \text{if } \bar{k}^{-1} \in \Lambda, i \equiv hk \bmod e, \\ 1 & \text{otherwise.} \end{cases}$$

□

3.3.6 Remark. For any divisor d of e, denote by f_d the multiplicative order of $p \bmod e$, hence $f_e = f$ the residue degree of $\mathfrak{p}$ over p. It is not hard to prove that $n(\Lambda, i, h)$ satisfies the following property
If $\gcd(i, e) \neq \gcd(h, e)$ then $n(\Lambda, i, h) = 0$.

If $\gcd(i, e) = \gcd(h, e)$, we can write $e = de', h = dh'$ and $i = di'$. One has

$$n(\Lambda, i, h) = \begin{cases} f/f_{e'} & \text{if } (h' \bmod e) \in (i' \bmod e')\Lambda' \\ 0 & \text{otherwise .} \end{cases}$$

where $\Lambda' = (\Lambda \bmod e) \in (\mathbb{Z}/e'\mathbb{Z})^\times / \langle (p \bmod e') \rangle$.

3.3.7 Corollary. Denote by r and s the representatives of $(\mathcal{R})$ and $(\mathcal{S})$ in $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_\Delta, J(\mathbb{Q}(\zeta)))$, respectively. For any $h = 0, \ldots, e-1$, we have

- if $\mathfrak{q} \nmid p$ then $r(\chi^h)_{\mathfrak{q}} = s(\chi^h)_{\mathfrak{q}} = 1$,
- if $\mathfrak{q} = \sigma_\Lambda(\mathfrak{p})$ for some $\Lambda \in n\mathbb{Z}/e\mathbb{Z})^\times / < \bar{p} >$ then

$$r(\chi^h)_{\mathfrak{q}} = p^{\sum_{i=1}^{e-1} in(\Lambda,i,h)},$$

$$s(\chi^h)_{\mathfrak{q}} = p^{\sum_{i=\frac{e+1}{2}}^{e-1} n(\Lambda,i,h)}.$$

Proof. In fact, we know that

$$\mathcal{R} = \prod_{i=1}^{e-1} \kappa(\chi^i)^i \text{ and } \mathcal{S} = \prod_{i=e+1/2}^{e-1} \kappa(\chi^i).$$

Since $(\kappa(\chi^i))_{\mathbb{Z}\Delta}$ is represented by $\mathcal{N}(v_i)$ Hence

$$r = \prod_{i=1}^{e-1} \mathcal{N}(v_i)^i \text{ and } s = \prod_{i=\frac{e+1}{2}}^{e-1} \mathcal{N}(v_i)^i.$$

Applying the previous Proposition, the results follows. □

3.4 Contents of r and s

3.4.1 Definition. The content of an idele $x = (x_\mathfrak{q})_\mathfrak{q}$ is the fractional ideal $cont(x) = \prod_\mathfrak{q} \mathfrak{q}^{\mathrm{val}_\mathfrak{q}}(x_\mathfrak{q})$ of $\mathcal{O}$ where $\mathrm{val}_\mathfrak{q}$ is the $\mathfrak{q}$-valuation and the product runs over finite prime ideals $\mathfrak{q}$ of $\mathcal{O}$.

3.4.2 Proposition. For $i, h \in \{0, \dots, e-1\}$, we have

$$\begin{aligned} cont(\mathcal{N}(v_i)(\chi^h)) &= \mathfrak{p}^{\sum_\Lambda n(\Lambda,i,h)\sigma_\Lambda}, & (3.2)\\ cont(r(\chi^h)) &= \mathfrak{p}^{\sum_\Lambda \sum_{i=1}^{e-1} n(\Lambda,i,h)\sigma_\Lambda}, & (3.3)\\ cont(s(\chi^h)) &= \mathfrak{p}^{\sum_\Lambda \sum_{i=\frac{e+1}{2}}^{e-1} n(\Lambda,i,h)\sigma_\Lambda}, & (3.4)\end{aligned}$$

where Λ runs over $(\mathbb{Z}/e\mathbb{Z})^\times / < \bar{p} >$.

Proof. By Proposition 3.3.5,

if $\mathfrak{q} \nmid p, \mathcal{N}(v_i)(\chi^h)_\mathfrak{q} = 1$ and $\mathrm{val}_\mathfrak{q}(1) = 0$,

if $\mathfrak{q} = \sigma_\Lambda(\mathfrak{p})$ for some $\Lambda \in \mathbb{Z}/e\mathbb{Z})^\times / < \bar{p} >$, $\mathcal{N}(v_i)(\chi^h)_\mathfrak{q} = p^{n(\Lambda,i,h)}$ and $\mathrm{val}_\mathfrak{q}(p^{n(\Lambda,i,h)}) = n(\Lambda, i, h)\,\mathrm{val}_\mathfrak{q}(p) = n(\Lambda, i, h)$.

Thus we have the results. □

3.4.3 Remark. The homomorphisms $\mathcal{N}(v_i), r$ and s are determined by the values at χ^d for any d dividing e. In fact, for any $h = 0, \dots, e-1$, if d =gcd(e, h), we can write $h = dh'$ where h' and e are coprime. Therefore, $\chi^h = \sigma_{h'}.\chi^d$. By construction, $\mathcal{N}(v_i), r$ and s are $\Omega_\mathbb{Q}$-equivariant, hence we have

$$\mathcal{N}(v_i)(\chi^h) = \mathcal{N}(v_i)(\sigma_{h'}.\chi^d) = \sigma_{h'}.\mathcal{N}(v_i).$$

Similarly for r and s.
In the remaining of this chapter, we are going to find the explicit values of $\mathcal{N}(v_i), r$ and s on χ^d for any $d|e$. That is, to give an expresion of the value $\mathfrak{p}^{\sum_\Lambda n(\Lambda,i,h)\sigma_\Lambda}$.

Recall that if $e = de'$, $\zeta_{e'} := \zeta^d$ (Thus we have $\zeta_e = \zeta$) is e'^{th} root of unity with $\mathbb{Q}(\zeta_{e'}) \subseteq \mathbb{Q}(\zeta_e)$ and $[\mathbb{Q}(\zeta_{e'} : \mathbb{Q}] = \varphi(e')$ (The Euler function of e').

For any $\alpha' \in (\mathbb{Z}/e'\mathbb{Z})^\times$, denote by $\sigma_{e',\alpha'}$ the automoprhism in $\mathrm{Gal}(\mathbb{Q}(\zeta_{e'})/\mathbb{Q})$ sending $\zeta_{e'}$ to $\zeta_{e'}^{\alpha'}$(thus $\sigma_{e,\alpha'} = \sigma_{\alpha'}$).

Hence, $\sigma_{e',\alpha'}$ can be lifted in Δ in $\varphi(e)/\varphi(e')$ many ways.

To simplify notation, we shall write $\sigma_{e',j}$ instead of $\sigma_{e',j \bmod e'}$ if j is an integer coprime to e'.

Set $\mathcal{O}_{e'} := \mathbb{Z}[\zeta_{e'}]$ the ring of integers of $\mathbb{Q}(\zeta_{e'})$ and $\mathfrak{p}_{e'} = \mathfrak{p} \bigcap \mathcal{O}_{e'}$. In particular we have $\mathfrak{p}_e = \mathfrak{p}, \mathcal{O}_e = \mathcal{O}$.

As in Remark 3.3.4, if $\Lambda' \in (\mathbb{Z}/e'\mathbb{Z})^\times / \langle (p \bmod e') \rangle$, we denote by $\sigma_{\Lambda'}(\mathfrak{p}_{e'})$ the ideal $\sigma_{e',\alpha'}(\mathfrak{p}_{e'})$ for any lift α' of Λ' in $(\mathbb{Z}/e'\mathbb{Z})^\times$.

Using these notations, we have the lemma about the content of $\mathcal{N}(v_i)(\chi^h)$.

3.4.4 Lemma. Let $d|e$ and write $e = de'$. If $\Lambda' \in (\mathbb{Z}/e'\mathbb{Z})^\times / \langle (p \bmod e') \rangle$, then

$$\sum_{\Lambda \in \Lambda'} \sigma_\Lambda(\mathfrak{p}) = \sigma_{\Lambda'}(\mathfrak{p}_{e'})\mathcal{O},$$

where the sum is on the elements Λ of the coset Λ' in $(\mathbb{Z}/e'\mathbb{Z})^\times / \langle (p \bmod e) \rangle$.

Proof. Let $\Lambda \in \mathbb{Z}/e\mathbb{Z})^{\times}/ < \bar{p} >$ and $\Lambda' \in (\mathbb{Z}/e'\mathbb{Z})^{\times}/\langle (p \bmod e')\rangle$. Since $\mathfrak{p}|\mathfrak{p}_{e'}\mathcal{O}$, we have

$$\sigma_{\Lambda}(\mathfrak{p})|\sigma_{\Lambda'}(\mathfrak{p}_{e'}\mathcal{O}) \Longrightarrow \sigma_{\Lambda_{|\mathbb{Q}(\zeta_{e'})}} = \sigma_{\Lambda'}.$$

This implies that $\Lambda \in \Lambda'$ and $\sigma_{\Lambda'}(\mathfrak{p}_{e'}\mathcal{O})|\sum_{\Lambda\in\Lambda'}\sigma_{\Lambda}(\mathfrak{p})$.

On the other hand, $\mathfrak{p}|\mathfrak{p}_{e'}$ is unramified since $p \nmid e$, then the number of primes of $\mathcal{O}$ above $\mathfrak{p}_{e'}$ is given by

$$\frac{\frac{\varphi(e)}{\varphi(e')}}{\frac{f}{f_{e'}}} = \sharp\Lambda'.$$

Thus, the equality follows. □

3.4.5 Theorem. *Let $d|e$ and write $e = de'$. Then we have*

$$cont(\mathcal{N}(v_i)(\chi^d)) = \begin{cases} \mathcal{O} & \textit{if } gcd(i,e) \neq d \\ (\sigma_{\Lambda_i'}(\mathfrak{p}_{e'}\mathcal{O}))^{\frac{f}{f_{e'}}} & \textit{if } gcd(i,e) = d, \end{cases}$$

where $i = di'$ and $\Lambda_i' \in (\mathbb{Z}/e'\mathbb{Z})^{\times}/\langle (p \bmod e')\rangle$ such that $(i \bmod e')^{-1} \in \Lambda_i'$.

Proof. Since $\gcd(d,e) = d$, then in the case $\gcd(i,e) \neq d$, the result follows from Remark 3.3.6 and Proposition 3.3.5.

If $\gcd(i,e) = d$, we can write $e = de', i = di'$ such that i' and e' are coprime. Take $\Lambda_i' \in \Lambda_i' \in (\mathbb{Z}/e'\mathbb{Z})^{\times}/\langle (p \bmod e')\rangle$ such that $(i \bmod e')^{-1} \in \Lambda_i'$. From Remark 3.3.6,

$$n(\Lambda, i, d) = \begin{cases} f/f_{e'} & \text{if } \Lambda \in \Lambda_i' \\ 0 & \text{otherwise }, \end{cases}$$

hence by Proposition 3.3.5, we have $(\sigma_{\Lambda_i'}(\mathfrak{p}_{e'}\mathcal{O}))^{\frac{f}{f_{e'}}}$. Applying the Lemma 3.4.4, then we get the wanted result. □

For the contents of r and s, we need to introduce further notation. For any e' divisor of e, we set Δ' to be the Galois group of $\mathbb{Q}(\zeta_e)$ over $\mathbb{Q}(\zeta_{e'})$ and $Z_{e'} := \sigma^{-1}(\Delta')$ where σ is defined in Remark 3.3.4.
Denote by $N_{e,e'}$ the relative norm

$$N_{e,e'} := \sum_{\alpha\in Z_{e'}} \sigma_{\alpha} \in \mathbb{Z}\Delta',$$

and by $\Theta_{e'}$ the Stickelberger's element,

$$\Theta_{e'} := \frac{1}{e'}\sum_{j} j\sigma_{e',j}^{-1} \in \mathbb{Q}(\zeta_{e'})$$

where the sum on j runs over $j = 1, \ldots, e'-1$ and $\gcd(e', j) = 1$.
Note that $N_{e,1}$ is the absolute norm.

Thus we have the following theorem:

3.4.6 Theorem. *Let d be a divisor of e and write $e = de'$. We have*

$$cont(r(\chi^d)) = (e\Theta_{e'}N_{e,e'}(\mathfrak{p}),$$
$$cont(s(\chi^d)) = (2 - \sigma_{e',2})\Theta_{e'}N_{e,e'}(\mathfrak{p}).$$

Proof. We prove this by computing the two sides of the equality.

Since $N_{e,e'}$ is the relative norm, then we have $N_{e,e'}(\mathfrak{p}) = \mathfrak{p}_{e'}^{f/f_{e'}}\mathcal{O}$. Replacing $\Theta_{e'}$ with its value, we have

$$e\Theta_{e'}N_{e,e'}(\mathfrak{p}) = \mathfrak{p}^x$$

where

$$x := d\frac{f}{f_{e'}}\sum_{\Lambda'}\left(\sum_{\substack{0\le j\le e'-1\\ j \bmod e'\in\Lambda'}} j\right)\sigma_{\Lambda'}^{-1}$$

and the first sum runs over $\Lambda' \in (\mathbb{Z}/e'\mathbb{Z})^\times/\langle(p \bmod e')\rangle$.

For the left-hand-side. Using Proposition 3.4.2 and Remark 3.3.6, since gcd(e',d) =gcd$(d,e) = d$, we have *cont*$(r(\chi^d))$ equals $\mathfrak{p}^y$ where the value of y is given by

$$y := \sum_{\Lambda}\left(\sum_{i'\in H_{e'}} di'\frac{f}{f_{e'}}\right)\sigma_\Lambda = d\frac{f}{f_{e'}}\sum_{\Lambda'}\left(\sum_{i'\in H'_{e'}} i'\right)\sum_{\Lambda\in\Lambda'}\sigma_\Lambda,$$

where $H_{e'} := \{i', 0 \le i' \le e'-1, 1 \bmod e' \in (i' \bmod e')\Lambda\}, H'_{e'} := \{i', 0 \le i' \le e'-1, 1 \bmod e' \in (i' \bmod e')\Lambda'\}, \Lambda$ runs over $(\mathbb{Z}/e\mathbb{Z})^\times < \bar{p} >$ in the first sum to the left, Λ' runs over $(\mathbb{Z}/e'\mathbb{Z})^\times/\langle(p \bmod e')\rangle$ in the first sum to the right, and seen as a coset of $(\mathbb{Z}/e\mathbb{Z})^\times < \bar{p} >$ in the last sum to the right for the reduction modulo e'.

By Lemma 3.4.4, we have *cont*$(r(\chi^d))$ equals $(\mathfrak{p}_{e'}\mathcal{O})^z$ where the value of z is

$$z := d\frac{f}{f_{e'}}\sum_{\Lambda'}\left(\sum_{\substack{0\le i'\le e'-1\\ 1\in(i' \bmod e')\Lambda'^{-1}}} i'\right)\sum_{\Lambda\in\Lambda'}\sigma_\Lambda,$$

and the two sides are equal. □

We do similar calculation for the content of s.

Chapter 4

Explicit unit elements

In this chapter, we are going to find explicit unit elements associated to the classes, $\mathcal{T}_{\mathbb{Z}}, \mathcal{R}$,and $\mathcal{S}$ in $Cl(\mathbb{Z}\Delta)$. We will see that, they lie in the denominator of $Cl(\mathbb{Z}\Delta)$ so we get easily their triviality.

4.1 Cyclotomic unit to describe $(T_{\mathbb{Z}})$

The triviliaty of $\mathcal{T}_{\mathbb{Z}}$ is a well know result of Swan. Since we have computed a representative v of $\mathcal{T}_{\mathbb{Z}}$ in the previous chapter, what we will do next is to modify v by an equivariant function on character of Δ with values in $\mathbb{Q}^{\times}$. This is the simplest case since we will use a well known result in cyclotomic units but for the case of $\mathcal{R}$ and $\mathcal{S}$, it will be slightly complicated since we will use Jacobi and Gauss sums instead of cyclotomic units. We have the proposition

4.1.1 Proposition. The class of $\sum_{\Delta}(p)$ is represented in $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_{\Delta}, J(Q(\zeta))$ by the homomorphism with $\mathfrak{q}^{th}$-component at a prime $\mathfrak{q}$ of $\mathcal{O}$ given by

$$\begin{cases} 1 & \text{if } \mathfrak{q} \nmid e, \\ \mathrm{Det}(p^{-1}u_t) & \text{if } \mathfrak{q}|e, \end{cases}$$

where $u_t = \sum_{i=0}^{p-1} \delta^i \in \mathbb{Z}\Delta$.

Further, if $\mathfrak{q} \bigcap \mathbb{Z} = q\mathbb{Z}$ with $q \neq p$, then $u_t \in \mathbb{Z}_q\Delta^{\times}$.
Consequently,

$$(\mathcal{T}_{\mathbb{Z}}) = (\sum_{\Delta}(p)) = 1 \in Cl(\mathbb{Z}\Delta).$$

Proof. Consider the embedding

$$\begin{array}{ccc} J(\mathbb{Q}) & \to & J(\mathbb{Q}(\zeta)), \\ (x_q)_q & \mapsto & (x_{\mathfrak{q}})_{\mathfrak{q}} \end{array}$$

given by $x_{\mathfrak{q}} = x_q$ if $\mathfrak{q}$ is a prime ideal of $\mathcal{O}$ above the rational prime q. Thanks to this embedding, we can look v (defined in Lemma 3.2.1) as a morphism with values in the idele group $J(\mathbb{Q}(\zeta))$. By Lemma 3.2.1, we have that

$$cont(v(\chi^h)) = (p^{1-\delta_{h,e}}) \text{ a principal ideal of } \mathcal{O}.$$

Consider the morphism $c_v \in \mathrm{Hom}(R_{\Delta}, \mathbb{Q}^{\times}(\zeta)$ defined by

$$c_v(\chi^h) = \begin{cases} 1 & \text{if } h = e, \\ \dfrac{1-\zeta^h}{1-\zeta^{ph}}p & \text{if } h \in \{1, \dots, e-1\}. \end{cases}$$

It is easy to see that this is $\Omega_{\mathbb{Q}}$ equivariant, then vc_v^{-1} is an other representative of $\sum_\Delta(p)$. A well known result on cyclotomic units says that $\dfrac{1-\zeta^{ph}}{1-\zeta^h}$ is a unit, thus belongs to $\mathcal{O}^\times$. It follows that $vc_v^{-1} \in \mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_\Delta, \mathcal{U}(\mathbb{Q}(\zeta)))$. By [[Fro83], P.23 I. (2.19)], $vc_v^{-1} \in \mathrm{Det}(\mathcal{U}(\mathfrak{M}))$ where $\mathfrak{M}$ is the maximal order of $\mathbb{Q}\Delta$.

If $q \nmid e$, since $\mathfrak{M}_q := \mathfrak{M} \otimes_{\mathbb{Z}} \mathbb{Z}_q = \mathbb{Z}_q\Delta, \mathfrak{M}_\infty = \mathbb{R}\Delta$, then we get $(vc_v^{-1})_{\mathfrak{q}} \in \mathrm{Det}((\mathbb{Z}_q\Delta)^\times)$ if $\mathfrak{q} \nmid e$ and $\mathfrak{q}|q$. The case $\mathfrak{q}|e$, will follows from the following lemma.

4.1.2 Lemma. Let $\mathfrak{q}$ be a prime ideal of $\mathcal{O}$ dividing a rational prime $q \neq p$. Then

$$(vc_v^{-1})_{\mathfrak{q}} = \mathrm{Det}(p^{-1}u_t),$$

and $u_t \in (\mathbb{Z}_q\Delta)^\times$. Thus $(vc_v^{-1})_{\mathfrak{q}} \in \mathrm{Det}((\mathbb{Z}_q\Delta)^\times)$.

Proof. Let $h \in \{1, \ldots, e\}$.
If $h = e$, then $\chi^e = 1$ and $\mathrm{Det}(u_t)(\chi^e) = p$.

If $h \in \{1, \ldots, e-1\}$, then $\mathrm{Det}(u_t)(\chi^h) = \sum_{i=0}^{p-1} \chi^h(\delta^i) = \sum_{i=0}^{p-1} \zeta^{ih} = \dfrac{1-\zeta^{ph}}{1-\zeta^h}$.

Since $p \neq q$, then $\mathfrak{q} \nmid p$. Thus $v(\chi^h)_{\mathfrak{q}} = 1$ and $p^{-1}\,\mathrm{Det}(u_t)(\chi^h) = (vc_v^{-1})_{\mathfrak{q}} = \mathrm{Det}(p^{-1}u_t)$.
As in the above proof, $(vc_v^{-1})_{\mathfrak{q}} = \mathrm{Det}(w_{\mathfrak{q}})$ for some $w_{\mathfrak{q}} \in \mathfrak{M}_{\mathfrak{q}}^\times$.

Hence $\mathrm{Det}(w_{\mathfrak{q}}) = \mathrm{Det}(p^{-1}u_t)$. Since Δ is abelian by Frohlich [[Fro83],II(5.2)], we have $w_{\mathfrak{q}} = p^{-1}u_t$.

Since $\mathfrak{q} \nmid p$, then

$$p^{-1}u_t \in \mathfrak{M}_{\mathfrak{q}}^\times \cap \mathbb{Z}_q\Delta = (\mathfrak{M}_{\mathfrak{q}}^\times \cap \mathcal{O}_{\mathfrak{q}}\Delta) \cap \mathbb{Z}_q\Delta = (\mathcal{O}\Delta)^\times \cap \mathbb{Z}_q\Delta = (\mathbb{Z}_q\Delta)^\times$$

thus for u_t □

To finish the proof of the Proposition, change vc_v^{-1} by multiplying its $\mathfrak{q}^{th}$-component whenever $\mathfrak{q} \nmid e$, by its inverse, we get the representative stated in the proposition. We have seen now that $vc_v^{-1} \in \mathrm{Det}(\mathcal{U}(\mathbb{Q}(\zeta)))$ which means that $\sum_\Delta(p)$ has trivial class in $Cl(\mathbb{Z}\Delta)$. So the assertion about $\mathcal{T}_{\mathbb{Z}}$ in Theorem 1.2.2 is now achieved. □

4.2 Gauss and Jacobi sums to describe (R) and (S)

The aim of this section is to compute the Gauss and Jacobi sums of $\mathcal{R}$ and $\mathcal{S}$ so let's start from the definitions of Gauss and Jacobi sums.
Denote by μ_∞ the group of unity in $\overline{\mathbb{Q}}^\times$. Let $\xi \in \mu_\infty$ an element of order p.

For e' divisor of e, we denote by $\mathcal{O}_{e'} := \mathbb{Z}[\zeta_{e'}]$ the ring of integers of $\mathbb{Q}(\zeta_{e'})$ and $\mathfrak{p}_{e'} = \mathfrak{p} \cap \mathcal{O}_{e'}$ the prime ideal of $\mathcal{O}_{e'}$ below $\mathfrak{p}$. Let θ denote a multiplicative character of $\mathcal{O}_{e'}/\mathfrak{p}_{e'}$, that is

$$(\mathcal{O}_{e'}/\mathfrak{p}_{e'})^\times \to \mu_\infty.$$

By the convention $\theta(0) = 0$, this is extended to $\mathcal{O}_{e'}/\mathfrak{p}_{e'}$.

4.2.1 Definition. The Gauss sum relative to θ is

$$G(\theta) := \sum_{x \in \mathcal{O}_{e'}/\mathfrak{p}_{e'}} \theta(x)\xi^{\mathrm{Tr}_{e'}(x)},$$

where $\mathrm{Tr}_{e'} : \mathcal{O}_{e'}/\mathfrak{p}_{e'} \to \mathbb{Z}/p\mathbb{Z}$ is the residue field trace homomorphism.

4.2.2 Definition. For any $x \in (\mathcal{O}_{e'}/\mathfrak{p}_{e'})^{\times}$, $\left(\frac{x}{\mathfrak{p}_{e'}}\right)$ is the e'^{th} root of unity defined by the congruence

$$\left(\frac{x}{\mathfrak{p}_{e'}}\right) \equiv x^{\frac{p^{f_{e'}}-1}{e'}} \bmod \mathfrak{p}_{e'}.$$

We are interested in case $\theta = \left(\frac{}{\mathfrak{p}_{e'}}\right)^{-1}$, the inverse of the e'^{th} power residue symbol, that is the inverse of the above symbol.

4.2.3 Lemma. Suppose that θ is a multiplicative character of $\mathcal{O}_{e'}/\mathfrak{p}_{e'}$ with values in $0 \cup \mu_{e'}$, then $G(\theta) \in \mathcal{O}_{e'}[\xi]$ and we have

$$G(\theta)^{e'} \in \mathcal{O}_{e'}.$$

Proof. There is nothing to prove for the first asseertion.

For the second assertion, let $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_{e'}, \xi)/\mathbb{Q}(\zeta_{e'})$ and $\beta \in \mathbb{F}_p^{\times}$ b such that $\tau(\xi) = \xi^{\beta}$. Since β is a unit, then the map

$$\begin{aligned} \mathcal{O}_{e'}/\mathfrak{p}_{e'} &\rightarrow \mathcal{O}_{e'}/\mathfrak{p}_{e'} && (4.1)\\ x &\mapsto \beta x && (4.2)\end{aligned}$$

is a bijection. Hence we get

$$\begin{aligned}\tau(G(\theta)) &= \sum_{x \in \mathcal{O}_{e'}/\mathfrak{p}_{e'}} \theta(x)\tau(\xi)^{\mathrm{Tr}_{e'}(x)},\\ &= \sum_{y \in \mathcal{O}_{e'}/\mathfrak{p}_{e'}} \theta(\beta^{-1}y)\tau(\xi)^{\mathrm{Tr}_{e'}(y)},\\ &= \theta(\beta)^{-1}G(\theta).\end{aligned}$$

The second equality follows from the above bijection. Since $\theta(\beta) \in \mu_{e'}$, then we have $G(\theta)^{e'} \in \mathcal{O}_{\mathfrak{p}_{e'}}$. □

If we set $G_{e'} = G(\left(\frac{}{\mathfrak{p}_{e'}}\right)^{-1})$, by the above lemma we have $G_{e'}^{e'} \in \mathcal{O}_{e'}$.

4.2.4 Definition. Let θ, θ' be multiplicative character of $\mathcal{O}_{e'}/\mathfrak{p}_{e'}$. The Jacobi sum relative to θ and θ' is

$$J(\theta, \theta') := \sum_{x \in \mathcal{O}_{e'}/\mathfrak{p}_{e'}} \theta(x)\theta'(1-x).$$

The Gauss and Jacobi sums are related by the following theorem:

4.2.5 Theorem (Theorem 2.1.3,[BCW98])**.** *If $\theta\theta'$ is non trivial character, then*

$$J(\theta, \theta') = \frac{G(\theta)G(\theta')}{G(\theta\theta')}.$$

Since we are interested in $\theta = \left(\frac{}{\mathfrak{p}_{e'}}\right)^{-1}$, we set

$$J_{e'} := J(\left(\frac{}{\mathfrak{p}_{e'}}\right)^{-1}, \left(\frac{}{\mathfrak{p}_{e'}}\right)^{-1}).$$

Recall that $\sigma_{e',2}$ is an element of $\mathrm{Gal}(\mathbb{Q}(\zeta_{e'})/\mathbb{Q})$ sending $\zeta_{e'}$ to $\zeta_{e'}^2$. We lift it in $\mathrm{Gal}(\mathbb{Q}(\zeta_{e'}, \xi)/\mathbb{Q})$ in such a way that $\sigma_{e',2}(\xi) = \xi$, and we still denote it by $\sigma_{e',2}$.

Thus we have

$$J_{e'} = (2-\sigma_{e',2})G_{e'} \in \mathcal{O}_{e'}.$$

We have the following result about the ideals of $\mathcal{O}_{e'}$ generated by $G_{e'}$ and $J_{e'}$ using the Stickelberger element defined by $\Theta_{e'} := \frac{1}{e'}\sum_j j\sigma_{e',j}^{-1} \in \mathbb{Q}(\zeta_{e'})$(defined below the Theorem 3.4.5). Recall the notation $\Delta_{e'} = \mathrm{Gal}(\mathbb{Q}(\zeta_{e'})/\mathbb{Q})$.

4.2.6 Theorem. *We have* $(2-\sigma_{e',2})\Theta_{e'}\mathbb{Z}\Delta_{e'}$, *and*

$$(G_{e'}) = e'\Theta_{e'}(\mathfrak{p}_{e'}) \text{ and } (J_{e'}) = (e'-\sigma_{e',2})\Theta_{e'}(\mathfrak{p}_{e'})$$

As a consequence of this Theorem, we get that the fractional ideals $cont(r(\chi^d))$ and $cont(s(\chi^d))$, where $d|e, e = de'$, are principal ideal of $\mathcal{O}$ generated respectively by

$$(G_{e'}^{ef/f_{e'}}) \text{ and } (J_{e'}^{f/f_{e'}})$$

As we did in the case of $\mathcal{T}_{\mathbb{Z}}$, we define two elements c_r and c_s in $\mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_\Delta, \mathbb{Q}(\zeta)^\times)$.
For any $d|e, e = de'$, we define

$$c_r(\chi^d) := (-1)^e(-G_{e'}^{ef/f_{e'}}) \text{ and } c_s(\chi^d) := -(-J_{e'})^{f/f_{e'}}.$$

We get the following result as a corollary

4.2.7 Corollary. The homomorphisms rc_r^{-1} and sc_s^{-1} belong to $\mathrm{Det}(\mathcal{U}(\mathfrak{M}))$, where $\mathfrak{M}$ is the maximal order of $\mathbb{Q}\Delta$.

Proof. For any $d|e$, we have $(c_r(\chi^d)) = (cont(r(\chi^d)))$ and $(c_s(\chi^d)) = (cont(s(\chi^d)))$, thus, $rc_r^{-1}, sc_s^{-1} \in \mathrm{Hom}_{\Omega_{\mathbb{Q}}}(R_\Delta, \mathcal{U}(\mathbb{Q}(\zeta)))$. By Frohlich again, we have the desired result. Note that rc_r^{-1} and sc_s^{-1} are still representatives of $\mathcal{R}$ and $\mathcal{S}$, repesctively. □

The result does not depend of the the signs in the definition of c_r and c_s but the choice of these signs will be clear later in the proof of next result. We are now going to prove the Theorem 1.2.2 concerning r and s.

4.2.8 Theorem. *The homomorphisms* rc_r^{-1} *and* sc_s^{-1} *belong to* $\mathrm{Det}(\mathcal{U}(\mathbb{Z}\Delta))$. *In particular* $(\mathcal{R})$ *and* $(\mathcal{S})$ *are trivial in* $Cl(\mathbb{Z}\Delta$.)

Proof. Using Corollary 4.2.7 and arguing as in Proposition 4.1.1, we have that if $\mathfrak{q} \nmid e$ but $\mathfrak{q}|q$, the $\mathfrak{q}^{th}$-component of rc_r^{-1} and sc_s^{-1} are in $\mathrm{Det}(\mathbb{Z}_q\Delta^\times)$.

It remains then to prove the theorem for the case $\mathfrak{q}|e$.

If $\mathfrak{q}|e$, then $\mathfrak{q} \nmid p$, and the Corollary 3.3.7 gives

$$(rc_r^{-1})_{\mathfrak{q}} = c_r{}^{-}1 \text{ and } (sc_s^{-1})_{\mathfrak{q}} = c_s^{-1},$$

where c_r^{-1}, c_s^{-1} are seen as moprhisms with values in $\mathbb{Q}(\zeta)$, diagonally embedded in $J_q(\mathbb{Q}(\zeta)) = \prod_{\mathfrak{q}|q}\mathbb{Q}(\zeta)_{\mathfrak{q}}$. □

4.3 Unit of $\mathcal{S}$

Let $i \in \{0, \ldots, e-1\}$. Set

$$A_i := \{x \in \mathcal{O}/\mathfrak{p} : \left(\frac{x}{\mathfrak{p}}\right)^{-1}\left(\frac{1-x}{\mathfrak{p}}\right)^{-1} = \zeta^i\},$$

and $n_i = \sharp A_i$.
By definition of J_e, we have

$$J_e = \sum_{i=0}^{e-1} n_i\zeta^i.$$

4.3.1 Lemma. Let $u_s := \sum_{i=0}^{e-1} n_i \delta^i \in \mathbb{Z}\Delta$. For any prime ideal $\mathfrak{q}$ above a rational prime q such that $q|e$, we have $u_s \in (\mathbb{Z}\Delta)^\times$ and the $\mathfrak{q}^{th}$ component of sc_s^{-1} is given by

$$(sc_s^{-1})_{\mathfrak{q}} = \mathrm{Det}(u_s^{-1}) \in \mathrm{Det}((\mathbb{Z}_q\Delta)^\times)$$

Claim. *For any $d|e$, $(e = de')$, $\mathrm{Det}(u_s)(\chi^d) = -(-J_{e'})^{f/f_{e'}}$.*

In fact, The Davenport-Hasse theorem in [[BCW98], Theorem 11 3.5] gives us that

$$(-1)^{f/f_{e'}-1} J_{e'}^{f/f_{e'}} = \sum_{x \in \mathcal{O}/\mathfrak{p}} \left(\frac{N'_{e,e'}(x)}{\mathfrak{p}} \right)^{-1} \left(\frac{N'_{e,e'}(1-x)}{\mathfrak{p}} \right)^{-1},$$

where $N'_{e,e} : \mathcal{O}/\mathfrak{p} :\to \mathcal{O}_{e'}/\mathfrak{p}_{e'}$ is the residual relative norm.

By definition, for any $x \in \mathcal{O}/\mathfrak{p}$, we have $\left(\frac{x}{\mathfrak{p}}\right)^d \equiv \left(x^{\frac{p^f-1}{e}}\right)^d \bmod \mathfrak{p}$.

On the other hand, we have

$$\begin{aligned}
\sum_{t=0}^{f/f_{e'}-1} p^{f_{e'}t} . \frac{p^{f_{e'}}-1}{e'} &= \frac{1}{e'} (\sum_{t=0}^{f/f_{e'}-1} p^{f_{e'}(t+1)} - \sum_{t=0}^{f/f_{e'}-1} p^{f_{e'}t}), \\
&= \frac{1}{e'}(p^f - 1), \\
&= \frac{p^f-1}{e} d.
\end{aligned}$$

hence ,

$$\begin{aligned}
\left(x^{\sum_{t=0}^{f/f_{e'}-1} p^{f_{e'}t} . \frac{p^{f_{e'}}-1}{e'}} \right) &= \left(x^{\sum_{t=0}^{f/f_{e'}-1} p^{f_{e'}t}} \right)^{\frac{p^{f_{e'}}-1}{e'}}, \\
&\equiv N'_{e,e'}(x)^{\frac{p^{f_{e'}}-1}{e'}} \bmod \mathfrak{p}.
\end{aligned}$$

Thus,

$$\left(\frac{x}{\mathfrak{p}}\right)^d = \left(\frac{N'_{e,e'}(x)}{\mathfrak{p}_{e'}} \right),$$

and

$$\begin{aligned}
-(-J_{e'})^{f/f_{e'}} &= \sum_{x \in \mathcal{O}/\mathfrak{p}} \left(\frac{x}{\mathfrak{p}}\right)^{-d} \left(\frac{1-x}{\mathfrak{p}}\right)^{-d}, \\
&= \sum_{i=0}^{e-1} n_i \zeta^{id}, \\
&= \mathrm{Det}(u_s)(\chi^d).
\end{aligned}$$

The case $\mathfrak{q} \nmid e$ is already done. For $\mathfrak{q}|e$, we have seen that for any $d|ee = de'$,

$(sc_s^{-1})_{\mathfrak{q}} = c_s^{-1}$ hence $(sc_s^{-1})_{\mathfrak{q}}(\chi^d) = -(-J_{e'})^{-f/f_{e'}} = \mathrm{Det}(u_s^{-1})(\chi^d)$.Corollary 4.2.7 implies the existence of $w_{\mathfrak{q}} \in \mathfrak{M}_{\mathfrak{q}}^\times$ such that

$$(sc_s^{-1})_{\mathfrak{q}} = \mathrm{Det}(w_{\mathfrak{q}}))$$

Thus

$$\mathrm{Det}(w_{\mathfrak{q}}) = \mathrm{Det}(u_s).$$

As in the proof of Lemma 4.1.2, we have

$$w_{\mathfrak{q}} = u_s \in \mathfrak{M}_{\mathfrak{q}}^{\times} \cap \mathbb{Z}_q\Delta = (\mathbb{Z}_q\Delta)^{\times}.$$

And it completes the proof of the claim. To complete the proof of the theorem, we just argue as in the proof of Proposition 4.1.1 to get the desired representative of $\mathcal{S}$.

4.4 Unit of $\mathcal{R}$

For the proof of $\mathcal{R}$, we have to introduce further notation in order to get a similar proof of $\mathcal{S}$. Let θ be a multiplicative character of $\mathcal{O}/\mathfrak{p}$.
Define,

$$\mathcal{C}_e := \{(k_1, \ldots, k_{p^f}) \in \mathbb{N}, \sum_{h=1}^{p^f} = e\},$$

the partition of e into sum of p^f integers.
Since $\sharp(\mathcal{O}/\mathfrak{p}) = p^f$ their elements can be written as $x_h, h = 1, \ldots, p^f$.
Denote Tr to be the trace map from $\mathcal{O}/\mathfrak{p}$ to $\mathbb{Z}/p\mathbb{Z}$. Since Tr is linear and θ is multiplicative, using the Binomial formula, we have

$$G(\theta)^e = \sum_{\mathcal{C}_e} \frac{e!}{\prod_{h=1}^{p^f} k_h!} \theta\left(\prod_{h=1}^{p^f} x_h^{k_h}\right) \xi^{\mathrm{Tr}(\sum_{h=1}^{p^f} k_h x_h)}$$

For $j \in \mathbb{F}_p$, define

$$\mathcal{C}_{e,j} := \{(k_1, \ldots, k_{p^f} \in \mathcal{C}_e, \mathrm{Tr}(\sum_{h=1}^{p^f} k_h x_h) = j\},$$

and

$$g_j(\theta) := \sum_{\mathcal{C}_{e,j}} \frac{e!}{\prod_{h=1}^{p^f} k_h!} \theta\left(\prod_{h=1}^{p^f} x_h^{k_h}\right).$$

We have a nice formula of $G(\theta)$ similar to J_e:

$$G(\theta)^e = \sum_{j\in\mathbb{F}_p} g_j(\theta)\xi^j = \sum_{j\in\mathbb{F}_p-\{1\}} (g_j(\theta) - g_1(\theta))\xi^j.$$

Assume now that θ takes values in $\{0\} \cup \mu_e$, then $G(\theta)^e \in \mathcal{O}$ and we have

$$G(\theta)^e = g_0(\theta) - g_1(\theta).$$

For $j \in \mathbb{F}_p$ and $i \in \{0, \ldots, e-1\}$, we let

$$\mathcal{C}_{e,j,i(\theta)} := \{(k_1, \ldots, k_{p^f} \in \mathcal{C}_{e,j}, \theta\left(\prod_{h=1}^{p^f} x_h^{k_h}\right) = \zeta^i\},$$

and

$$m_i(\theta) := \sum_{\mathcal{C}_{e,0,i(\theta)}} \frac{e!}{\prod_{h=1}^{p^f} k_h!} - \sum_{\mathcal{C}_{e,1,i(\theta)}} \frac{e!}{\prod_{h=1}^{p^f} k_h!}$$

such that $m_i(\theta) \in \mathbb{Z}, , i = 0, \dots, e-1$ and

$$G(\theta)^e = \sum_{i=0}^{e-1} m_i(\theta)\zeta^i.$$

If θ is a multiplicative character of $\mathcal{O}/\mathfrak{p}$ taking values in $\{0\} \cup \mu_e$ and d is any divisor of e, it is not hard to check that

$$G(\theta^d)^e = \sum_{i=0}^{e-1} m_i(\theta)\zeta^{id}.$$

If $\theta = \left(\frac{-}{\mathfrak{p}}\right)^{-1}$, we set $G_e := G(\theta)$ and $m_i := m_i(\theta)$ for all $i = 0, \dots, e-1$.

Set also $u_r := \sum_{i=0}^{e-1} m_i \delta^i \in \mathbb{Z}\Delta$.
Using these notations we have for any prime $\mathfrak{q}$ above a rational prime $q|e$, $u_r \in (\mathbb{Z}_q\Delta)^\times$ and

$$(rc_r^{-1})_{\mathfrak{q}} = \mathrm{Det}(u_r^{-1}) \in \mathrm{Det}((\mathbb{Z}_q\Delta)^\times).$$

and arguing as in the proof concerning $\mathcal{T}_{\mathbb{Z}}$ and $\mathcal{S}$ we get the desired result.

Chapter 5

Conclusions and counter example

To summarize what we have done, in tamely ramified Galois extension of number fields N/E with group G and ring of integers S and R, respectively, the Galois module inverse different $\mathcal{C}_{N/E}$ defines the same class as S in $Cl(\mathbb{Z}G)$, it means that asking the freeness of $\mathcal{C}_{N/E}$ on $\mathbb{Z}G$ is exactly the same as asking the freeness of S on $\mathbb{Z}G$ which is nothing that the normal integral basis problem.

We proved that the torsion module $\mathcal{R}_{N/E}$ is trivial in $Cl(\mathbb{Z}G)$. This triviality of $\mathcal{R}_{N/E}$ gives a nice result saying that $S \otimes_R S$ and $S^{[N:E]}$ define the same classes in $Cl(\mathbb{Z}G)$.

If N/E is locally abelian, then the square root $\mathcal{A}_{N/E}$ and S define the same classes in $Cl(\mathbb{Z}G)$.
Thus it is the same case as that of $\mathcal{C}_{N/E}$.

These can be putted in one Theorem which is the Theorem 1.2.3, in the Introduction stating that

5.0.1 Theorem. *Let N/E be a Galois tamely ramified extension of number fields. Then the classes of $T_{N/E}, \mathcal{R}_{N/E}$ and $\mathcal{S}_{N/E}$ are trivial in $Cl(\mathbb{Z}G)$. In particular, we have*

$$(S) = (\mathcal{C}_{N/E}) \text{ and } (S \otimes_R S) = (S)^{[N:E]} = 1.$$

If further N/E is locally abelian, then the class of $\mathcal{S}_{N/E}$ is trivial in $Cl(\mathbb{Z}G)$. In particular we have

$$(S) = (\mathcal{A}_{N/E}),$$

thus $S, \mathcal{C}_{N/E}$ and $\mathcal{A}_{N/E}$ define the same class in $Cl(\mathbb{Z}G)$.

This theorem is obtained easily from Lemma 2.4.4 and Theorem 1.2.2.

However the class of the square root of the inverse different, $\mathcal{S}_{N/E}$, is not trivial in general. Recall that we always worked under the assumption that N/E is locally abelian or N/E is of odd degree in dealing with the torsion module $\mathcal{S}_{N/E}$ associated to $\mathcal{A}_{N/E}$.

Luca Caputo and Stéphan Vinatier say in [CV] that there exists a tame Galois extension $N/\mathbb{Q}$ of even degree such that $\mathcal{A}_{N/E}$ exists and has nontrivial class in $Cl(\text{Gal}(N/\mathbb{Q}))$. Proving this needs more further notion which can be considered as a future work.

They give a precise example by taking N to be the splitting field of the polynomial

$$\begin{aligned} f(X) = {} & X^{24} - 3X^{23} - 2X^{22} + 16X^{21} - 12X^{20} + 52X^{19} - 324X^{18} - \\ & 436X^{17} + 3810X^{10} - 1638X^{15} - 8012X^{14} - 12988X^{13} + \\ & 67224X^{12} - 76152X^{11} + 41175X^{10} - 3958X^{9} + 70068X^{8} - \\ & 66440X^{7} + 38488X^{6} - 23248X^{5} + 16672X^{4} - 6976X^{3} + 2816X^{2} - 1280X + 512. \end{aligned}$$

In this extension, they proved that the classes of $\mathcal{A}_{N/E}$ and $\mathcal{O}_N$ are both nontrivial in $Cl(\mathbb{Z}G)$ where G is the Galois group of $N/\mathbb{Q}$.

References

[BCW98] Ronald J. Evans Bruce C.Berndt and Kenneth S. Williams, *Gauss and jacobi sums*, John Wiley and sons, Inc, 1998.

[Cha84] Stephen U. Chase, *Ramification invariants and torsion galois module structure in number fields*, Journal Of Algebra **91** (1984), 207–257.

[CV] Luca Caputo and Stephan Vinatier, *Cyclotomic units, gauss and jacobi sums related to torsion galois modules*, To be published.

[DF04] David S. Dummit and Richard M. Foote, *Abstract algebra*, Springer, 2004.

[DI71] Frank DeMeyer and Edward Ingraham, *Separable algebras over commutative rings*, Springer-Verlag, 1971.

[Ere13] Boas Erez, *Galois modules in arithmetic*, Preprint, 2013.

[Fro83] Albert Frohlich, *Galois module structure of algebraic integers*, Springer, 1983.

[FT91] A. Frohlich and M.J Taylor, *Algebraic number theory*, Cambridge University Press, 1991.

[I.R03] I.Reiner, *Maximal orders*, Clarendon Press-Oxford, 2003.

[Lan65] Serge Lang, *Algebra*, Addison Wesley, 1965.

[Lan78] ______, *Cyclotomic fields*, Springer-Verlag, 1978.

[Rei87] Charles W.Curtis Irving Reiner, *Methods of representation theory with applications to finite groups and orders*, vol. 2, A Wiley-Interscience Series Of Texts, Monographs and Tracts, 1987.

[RS72] I. Reiner and S.Ullom, *Class group of integral group rings*, Transactions of The American Mathematical Society **170** (1972).

[Ser71] Jean-Pierre Serre, *Linear representation of finite groups*, Springer-Verlag, 1971.

[Ser79] ______, *Local fields*, Springer, 1979.

[Tay84] Martin Taylor, *Classgroups of group rings*, London Mathematics Society Lecture Notes **91** (1984), 428–442.

[Ull69] S. Ullom, *Galois cohomology of ambiguous ideals*, Journal Of Number Theory **1** (1969), 11–15.