Università degli Studi di Padova

UNIVERSITÄT DUISBURG ESSEN

Offen im Denken

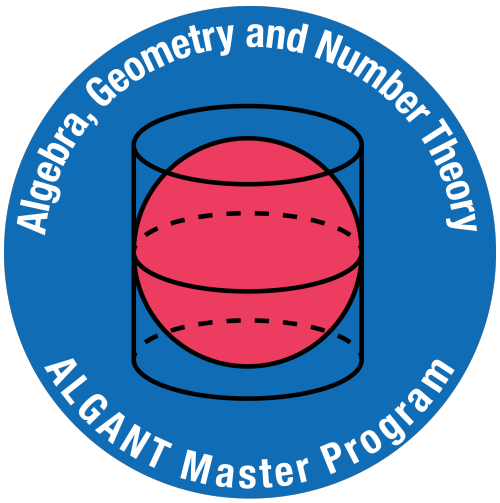
Master Thesis in Mathematics

Duality theorems and Kolyvagin systems for elliptic curves

Marco Morosin

advised by

Prof. Dr. Massimo Bertolini



ALGANT Program 2019-2021

Contents

Introduction

After developing the theory of arithmetic duality for Galois cohomology with a particular focus on the cohomology of an elliptic curve over a local field or a number field, we use these results to define Kolyvagin systems and show how they provide bounds for the Selmer groups of the elliptic curve.

The first chapter is dedicated to the study of arithmetic duality, which consists in relating, for a given Galois module M, the groups

$$H^r(G, M)^* = \mathrm{Hom}(H^r(G, M), \mathbb{Q}/\mathbb{Z})$$

to the cohomology groups of the Cartier dual $M^D = \mathrm{Hom}(M, K^{s\times})$. These results are mainly due to Tate [Tat62] and later collected and generalized by Milne [Mil20].

We begin in Section 1.2 from the abstract setting of *class formations*, pairs (G, C) of a profinite group and a G-module, satisfying properties which allow us to formulate results of local class field theory in a purely algebraic language. In particular, they provide us with so-called invariant maps, isomorphisms $H^2(G, C) \cong \mathbb{Q}/\mathbb{Z}$; these are crucial for the definition of pairings into $\mathbb{Q}/\mathbb{Z}$ which will be the building blocks for the duality isomorphisms.

In Section 1.3 G is the Galois group of a local field K. The natural map $M^D \times M \to K^{s\times}$ induces cup products $H^r(G, M^D) \times H^{2-r}(G, M) \to H^2(G, K^{s\times})$. The pair $(G, K^{s\times})$ is (the prototypical example of) a class formation, so we may compose cup products with the invariant isomorphism to induce maps $H^r(G, M^D) \to H^{2-r}(G, M)^*$. Local Tate duality essentially states that these maps are isomorphisms.

In Section 1.4 we work with abelian varieties A over a local field K. We define their cohomology groups as the cohomology groups of $M = A(K^s)$. The main theorem of this section is an isomorphism of the kind $H^r(K, A^t) \cong H^{1-r}(K, A)^*$, where A^t is the dual abelian variety.

In Section 1.5 we specialize the previous results to the torsion group $M = E_n(K^s)$ of an elliptic curve. In this case self-duality of the curve, together with the Weil pairing, gives a relation $M^D = M$. When K is a number field, we define a global pairing as the sum of the local pairings for the completions K_v.

In Section 1.6 we define the Tate-Shafarevich and Selmer groups of an elliptic curve over a number field. These are fundamental objects in the study of its arithmetic, because their knowledge provides information on the rank of the curve. The rest of the thesis aims to show how Selmer groups can be controlled. The last prerequisite for this is global Poitou-Tate duality, an exact sequence which determines in particular a pairing between the Tate-Shafarevich groups; this is the topic of Section 1.7.

In Chapter 2 we apply these duality theorems. Given an R-module T with a Galois action, we first define Selmer modules in full generality, i.e. modules of cohomology classes satisfying given local conditions (Section 2.2). The Selmer groups of an elliptic curve are then

a particular example. Using our duality theory, a Selmer structure induces a structure on the dual module. It is actually these dual Selmer modules that we are going to study.

We construct *Stark systems* (Section 2.3) and, finally, *Kolyvagin systems* (Section 2.4), collections of elements obtained from these Selmer modules, more precisely by some exterior power thereof, with certain compatibility properties.

The exterior power appearing in the definition of a Kolyvagin system is the *core rank* of the Selmer structure. As of today, this theory is only well-established in the case of core rank 1, where the systems consist of simple cohomology classes; this is, for instance, the case of elliptic curves over $\mathbb{Q}$. To provide an upper bound for the Selmer group of T^D, Kolyvagin originally introduced *Euler systems*, collections of cohomology classes over different extensions of the base field, compatible when projecting via norms from an extension to a smaller one. From an Euler system he then constructed a 'derived system', a new collection of cohomology classes, now over the base field K alone. Mazur and Rubin showed in [MR04] that these classes satisfied stronger interrelations than previously known, and called *Kolyvagin system* any system satisfying these relations. This defines a 'Kolyvagin derivative' map from the module of Euler systems to that of Kolyvagin systems and this link allows for a much more concrete treatment of the core rank 1 case: by choosing a specific Euler system, for example related to L-values, one gets similar relations for the corresponding Kolyvagin system and the order of the Selmer group.

In the case of general core rank as we allow, the link between Euler and Kolyvagin systems is still mysterious and we cannot treat any explicit examples. The theory of Kolyvagin systems themselves, however, can still be developed and used to control Selmer groups, assuming the knowledge of a Kolyvagin system. We do so, following [MR16].

By means of these systems and some associated invariants, we are able to bound the length (in the module sense) of the dual Selmer modules. If E is an elliptic curve and we consider the $\mathbb{Z}/p^k\mathbb{Z}$-module E_{p^k} of torsion points (resp. the Tate module $T_p(E)$ over $\mathbb{Z}_p$), then the dual Selmer module will be the classical Selmer group $S_{p^k}(K,E)$ (resp. $S_{p^\infty}(K,E)$) as desired, so we will work in this setting, although the results hold for more general R and T.

Stark systems also control Selmer groups but we especially use them as a tool in the final section, thanks to an equivalence between the module of Stark systems and a particular type of Kolyvagin systems. In both cases, the theory is first explained for $\mathbb{Z}/p^k\mathbb{Z}$ and then extended to $\mathbb{Z}_p$ passing to inverse limits.

Chapter 1

Duality theorems

1.1 Preliminaries

1.1.1 Group cohomology

Let G be a group; we say that A is a G-module if it is a $\mathbb{Z}[G]$-module, and we write $A \in G\text{-Mod}$. We use notations

$$\mathrm{Hom}_G(A,B) \coloneqq \mathrm{Hom}_{\mathbb{Z}[G]}(A,B)$$

$$\mathrm{Hom}(A,B) \coloneqq \mathrm{Hom}_{\mathbb{Z}}(A,B).$$

Definition 1.1.1. For $A \in G\text{-Mod}$, we define its r-th cohomology group as

$$H^r(G,A) \coloneqq \mathrm{Ext}^r_G(\mathbb{Z},A) \coloneqq R^r \,\mathrm{Hom}_G(\mathbb{Z},-)(A),$$

where R^r denotes the r-th right derived functor.

More explicitly, we may compute this as follows: choose a projective G-resolution $P_\bullet \to \mathbb{Z} \to 0$ of $\mathbb{Z}$ (seen as a G-module via the trivial action), consider the complex

$$0 \to \mathrm{Hom}_G(P_0,A) \to \mathrm{Hom}_G(P_1,A) \to \cdots$$

and define $H^r(G,A)$ as the r-th cohomology group of this complex. Even more explicitly, we can choose the above resolution in a standard way by setting $P_i \coloneqq \mathbb{Z}[G^{i+1}]$ with differentials

$$d\colon P_i \to P_{i-1}, \quad (g_0,\dots,g_i) \mapsto \sum_{j=0}^{i} (-1)^j (g_0,\dots,g_{j-1},g_{j+1},\dots,g_i)$$

for $i \geqslant 1$, and

$$\varepsilon\colon P_0 = \mathbb{Z}[G] \to \mathbb{Z}, \quad \sum_g n_g g \mapsto \sum_g n_g$$

The elements of $\mathrm{Hom}_G(P_i,A)$ are functions $f\colon G^{i+1} \to A$ satisfying the property $f(sg_0,\dots,sg_i) = sf(g_0,\dots,g_i)$; so, by multiplying the arguments by suitable elements,

f is determined by its values on elements of the form $(1, g_1, g_1g_2, \dots, g_1 \cdots g_i)$, and thus we can identify it with a function

$$\varphi\colon G^i \to A, \quad \varphi(g_1, \dots, g_i) \coloneqq f(1, g_1, g_1g_2, \dots, g_1 \cdots g_i).$$

For these φ we get the following boundary formula

$$\begin{aligned}(d\varphi)(g_1, \dots, g_{i+1}) = {} & g_1\varphi(g_2, \dots, g_{i+1}) + \\ & + \sum_{j=1}^{i} (-1)^j \varphi(g_1, \dots, g_jg_{j+1}, \dots, g_{i+1}) + (-1)^{i+1}\varphi(g_1, \dots, g_i)\end{aligned}$$

and we can describe the homology classes accordingly. For example, for $r = 1$, the cocycles are maps $G \to A$ such that $\varphi(gg') = g\varphi(g') + \varphi(g)$ and the coboundaries are maps $\varphi(g) = ga - a$ for $a \in A$.

Remark 1.1.2. We will usually deal with profinite groups G. In this case we will always assume that all G-modules are *discrete*, meaning equivalently that

- the action $G \times A \to A$ is continuous for the discrete topology on A;
- $A = \bigcup_U A^U$, union over all open $U \trianglelefteqslant G$;

and we will compute cohomology using continuous cochains, i.e. in the above description we will restrict ourselves to those functions φ which are continuous.

For $A, B \in G\text{-Mod}$, the abelian group $\mathrm{Hom}(A, B)$ has a G-module structure given by $g\varphi(a) = g\varphi(g^{-1}a)$. Then we have $\mathrm{Hom}_G(A, B) = (\mathrm{Hom}(A, B))^G$ and, in particular,

$$H^0(G, A) \coloneqq \mathrm{Hom}_G(\mathbb{Z}, A) = (\mathrm{Hom}(\mathbb{Z}, A))^G \cong A^G.$$

Moreover, if $0 \to A \to B \to C \to 0$ is an exact sequence of G-modules, we have the usual cohomology long exact sequence

$$\cdots \to H^q(G, A) \to H^q(G, B) \to H^q(G, C) \xrightarrow{\delta} H^{q+1}(G, A) \to \cdots.$$

If $H \leqslant G$, we define the restriction morphism as the morphism

$$\mathrm{Res}\colon H^r(G, A) \to H^r(H, A)$$

induced by the inclusion $H \hookrightarrow G$. When H is normal, we define the inflation morphism as the composition

$$\mathrm{Inf}\colon H^r(G/H, A^H) \to H^r(G, A^H) \to H^r(G, A)$$

of the morphisms induced by $G \to G/H$ and $A^H \hookrightarrow A$ respectively. A fundamental result is the exactness of the restriction-inflation sequence,

$$0 \to H^1(G/H, A^H) \xrightarrow{\mathrm{Inf}} H^1(G, A) \xrightarrow{\mathrm{Res}} H^1(H, A).$$

Given a finite group G and a bilinear G-equivariant pairing of G-modules $A \times B \to C$, there are cup-product pairings

$$(x, y) \mapsto x \cup y\colon \widehat{H}^r(G, A) \times \widehat{H}^r(G, B) \to \widehat{H}^{r+s}(G, C)$$

($\widehat{H}^r$ denotes the Tate cohomology groups, see proof of Theorem 1.2.3) satisfying properties

- $dx \cup y = d(x \cup y)$ and $x \cup dy = (-1)^r d(x \cup y)$
- $x \cup (y \cup z) = (x \cup y) \cup z$
- $x \cup y = (-1)^{rs} y \cup x$
- $\mathrm{Res}(x \cup y) = \mathrm{Res}(x) \cup \mathrm{Res}(y)$ and $\mathrm{Inf}(x \cup y) = \mathrm{Inf}(x) \cup \mathrm{Inf}(y)$

Theorem 1.1.3 (Tate-Nakayama)**.** Let G be a finite group, A a G-module, $u \in H^2(G, A)$. Suppose that, for all $H \leqslant G$,

- $H^1(H, A) = 0$,
- $H^2(H, A) = \langle \mathrm{Res}(u) \rangle$ and $|H^2(H, A)| = |H|$.

Then, for any G-module B with $\mathrm{Tor}_1^{\mathbb{Z}}(B, A) = 0$, cup product with u induces an isomorphism

$$x \mapsto x \cup u \colon \widehat{H}^r(G, B) \to \widehat{H}^{r+2}(G, B \otimes A)$$

for all $r \in \mathbb{Z}$.

1.1.2 Spectral sequences

Definition 1.1.4. A *first-quadrant E_2-spectral sequence* in a category $\mathcal{C}$, denoted by $E_2^{p,q} \implies E^{p+q}$, consists of the following data:

- objects $E_r^{p,q} \in \mathcal{C}$ for $p, q \geqslant 0$, $r \geqslant 2$
- morphisms $d_r^{p,q} \colon E_r^{p,q} \to E_r^{p+r,q-r+1}$ such that:
  - $d \circ d = 0$
  - for every (p, q), d_r^{pq} and $d_r^{p-r,q+r-1}$ vanish for large enough r
  - $\ker d_r^{p,q} / \operatorname{im} d_r^{p-r,q+r-1} \cong E_{r+1}^{p,q}$

  (this implies that, for r large enough, $E_r^{p,q}$ is independent of r and we can denote it by $E_\infty^{p,q}$)
- objects E^n with a finite filtration $E^n \supset \cdots \supset \mathcal{F}_k E^n \supset \mathcal{F}_{k+1} E^n \supset \cdots \supset 0$ such that $E_\infty^{p,q} \cong \mathcal{F}_p E^{p+q} / \mathcal{F}_{p+1} E^{p+q}$

This setting provides us with useful exact sequences:

Lemma 1.1.5.

1. If $E_2^{p,q} = 0$ for all $p \geqslant 0$ and $q > 1$, then there is a long exact sequence
$$0 \to E_2^{1,0} \to E^1 \to E_2^{0,1} \xrightarrow{d} E_2^{2,0} \to E^2 \to E_2^{1,1} \xrightarrow{d} E_2^{3,0} \to \cdots$$
2. If $E_2^{p,q} = 0$ for all $q \geqslant 0$ and $p > 1$, then there is a short exact sequence
$$0 \to E_2^{1,n-1} \to E^n \to E_2^{0,n} \to 0.$$

Proof. See, for example, [Neu93]. □

We introduce a spectral sequence of great importance. For M, $N \in G$-Mod and $H \leqslant G$, we define $\mathcal{H}om_H(M,N) \coloneqq \bigcup_{H \leqslant U \leqslant G} \mathrm{Hom}(M,N)^U$, U open. This is a discrete G/H-module and defines a left-exact functor $\mathcal{H}om_H(M,-)$ from (discrete) G-Mod to (discrete) G/H-Mod. We denote its right derived functors in the natural way, $\mathcal{E}xt^r_H(M,N) \coloneqq R^r\,\mathcal{H}om_H(M,-)(N)$.

Theorem 1.1.6. Let $H \leqslant G$ be a normal closed subgroup, N, $P \in G$-Mod, $M \in G/H$-Mod with $\mathrm{Tor}^{\mathbb{Z}}_1(M,N) = 0$. Then there is a spectral sequence

$$\mathrm{Ext}^r_{G/H}(M, \mathcal{E}xt^s_H(N,P)) \implies \mathrm{Ext}^{r+s}_G(M \otimes_{\mathbb{Z}} N, P).$$

Proof. This is a particular case of Grothendieck's spectral sequence, which relates the derived functor of a composition $G \circ F$ to the derived functors of F and G. The result, proven in Grothendieck's Tôhoku paper [Gro57], states

$$(R^pG \circ R^qF)(A) \implies R^{p+q}(G \circ F)(A)$$

if F maps injective objects to G-acyclic objects. Hence, it is enough to show that $\mathrm{Hom}_G(M \otimes_{\mathbb{Z}} N, -) = G \circ F$ for $F = \mathcal{H}om_H(N,-)$ and $G = \mathrm{Hom}_{G/H}(M,-)$, and that F has the required property. □

From this we can easily deduce the famous

Corollary 1.1.7 (Hochschild-Serre spectral sequence)**.** If we choose $(M,N,P) \coloneqq (\mathbb{Z},\mathbb{Z},M)$, we get

$$H^r(G/H, H^s(H,M)) \implies H^{r+s}(G,M).$$

Corollary 1.1.8. If we choose $(M,N,P) \coloneqq (\mathbb{Z},M,N)$ and $H = 1$, we get

$$H^r(G, \mathcal{E}xt^s(M,N)) \implies \mathrm{Ext}^{r+s}_G(M,N).$$

and, if M is finitely generated, Lemma 1.1.5 then yields a long exact sequence

$$\begin{aligned} 0 \to &H^1(G, \mathrm{Hom}(M,N)) \to \mathrm{Ext}^1_G(M,N) \to H^0(G, \mathrm{Ext}^1(M,N)) \to \\ \to &H^2(G, \mathrm{Hom}(M,N)) \to \cdots \end{aligned}$$

and we can also deduce that:

- $\mathrm{Ext}^r_G(M,N)$ is torsion for $r \geqslant 1$;
- if N is divisible by all primes occurring as the order of an element in M, then $\mathrm{Ext}^1(M,N) = 0$ and consequently

$$H^r(G, \mathrm{Hom}(M,N)) = \mathrm{Ext}^r_G(M,N).$$

1.1.3 Ext pairings

Given a pairing of G-modules $M \times N \to P$, there is a canonical product $\mathrm{Ext}^r_G(N,P) \times \mathrm{Ext}^s_G(M,N) \to \mathrm{Ext}^{r+s}_G(M,P)$ which becomes, in the case $M = \mathbb{Z}$,

$$\mathrm{Ext}^r_G(N,P) \times H^s(G,N) \to H^{r+s}(G,P).$$

This pairing will be the starting point for our duality theorems. It is compatible with the cup-pairing, in the sense that the following diagram commutes:

$$\begin{array}{ccc} H^r(G,M) & \times & H^s(G,N) \longrightarrow H^{r+s}(G,P) \\ \downarrow & & \| \qquad\qquad \| \\ H^r(G,\mathcal{H}om(N,P)) & & \| \qquad\qquad \| \\ \downarrow & & \| \qquad\qquad \| \\ \mathrm{Ext}^r_G(N,P) & \times & H^s(G,N) \longrightarrow H^{r+s}(G,P) \end{array}$$

where the map $H^r(G,\mathcal{H}om(N,P)) \to \mathrm{Ext}^r_G(N,P)$ exists because of the spectral sequence in Theorem 1.1.6.

If K is a field, the category of algebraic group schemes over K is abelian, hence we can define $\mathrm{Ext}^r_K(A,B)$ for A,B algebraic group schemes over K. In this setting we will write

$$G = \mathrm{Gal}(K^{\mathrm{s}}/K),$$

$$H^r(K,A) \coloneqq H^r(G,A(K^{\mathrm{s}})).$$

If K is perfect, $A \mapsto A(K^{\mathrm{s}})$ is an exact functor (since K^{s} is algebraically closed) and there is a canonical pairing

$$\mathrm{Ext}^r_K(A,B) \times H^s(K,A) \to H^{r+s}(K,B)$$

defined so that the following compatibility holds:

$$\begin{array}{ccc} \mathrm{Ext}^r_K(A,B) & \times & H^s(K,A) \longrightarrow H^{r+s}(K,B) \\ \downarrow & & \| \qquad\qquad \| \\ \mathrm{Ext}^r_G(A(K^{\mathrm{s}}),B(K^{\mathrm{s}})) & \times & H^s(G,A(K^{\mathrm{s}})) \longrightarrow H^{r+s}(G,B(K^{\mathrm{s}})) \end{array}$$

where the bottom row is the previously defined Ext pairing for G-modules.

Proposition 1.1.9. For perfect K there is also a spectral sequence resembling 1.1.8 for algebraic group schemes over K,

$$H^r(G,\mathrm{Ext}^s_{K^{\mathrm{s}}}(A,B)) \implies \mathrm{Ext}^{r+s}_K(A,B)$$

which can be used to show the following [Oor66]: if A is a finite group scheme over K of order not divisible by $\mathrm{char}(K)$, then

$$\mathrm{Ext}^r_K(A,\mathbb{G}_m) \cong \mathrm{Ext}^r_G(A(K^{\mathrm{s}}),K^{\mathrm{s}\times}).$$

1.2 Class formations

Definition 1.2.1. If G is a profinite group and C is a G-module, we say (G,C) is a *class formation* if there is a system of isomorphisms $\{\mathrm{inv}_U \colon H^2(U,C) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z} \mid U \leqslant G \text{ open}\}$, $H^1(U,C) = 0$ and, whenever $V \trianglelefteq U \leqslant G$,

$$\begin{array}{ccc} H^2(U,C) & \xrightarrow{\mathrm{Res}} & H^2(V,C) \\ \downarrow{\scriptstyle \mathrm{inv}_U} & & \downarrow{\scriptstyle \mathrm{inv}_V} \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{[U:V]} & \mathbb{Q}/\mathbb{Z} \end{array}$$

commutes.

Equivalently, the requirement that inv_U are isomorphisms may be replaced with the requirement that they be injections inducing isomorphisms

$$H^2(U/V, C^V) \xrightarrow{\sim} \tfrac{1}{[U:V]}\mathbb{Z}/\mathbb{Z},$$

if we add the condition that $|G|$ is divisible by all integers, where $|G|$ denotes the profinite order of $G = \varprojlim G_i$, defined formally as $\prod_p p^{\max_i\{|G_i|_p\}}$ (product over all primes, $|G_i|_p$ denoting the p-factor in $|G_i|$).

This notion is an abstraction of the following fundamental situation from local class field theory:

Theorem 1.2.2. Let K be a local field, $G = \mathrm{Gal}(K^{\mathrm{s}}/K)$. Then $(G, K^{\mathrm{s}\times})$ is a class formation.

To construct the invariant maps we need to recall some facts. Let I be the inertia subgroup $\mathrm{Gal}(K^{\mathrm{s}}/K^{\mathrm{un}})$, hence $G/I = \mathrm{Gal}(K^{\mathrm{un}}/K)$. Then:

1. $H^2(G, K^{\mathrm{s}\times}) \cong H^2(G/I, K^{\mathrm{un}})$.
2. the map $H^2(G/I, K^{\mathrm{un}}) \to H^2(G/I, \mathbb{Z})$, induced by the additive valuation $v\colon K^\times \to \mathbb{Z}$, is an isomorphism.
3. $H^2(G/I, \mathbb{Z}) \cong H^1(G/I, \mathbb{Q}/\mathbb{Z})$: indeed, consider the long cohomology sequence arising from $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ considered as trivial G/I-modules. Since $\mathbb{Q}$ is uniquely divisible, it has trivial cohomology, hence the connecting morphisms are isomorphisms.
4. $H^1(G/I, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G/I, \mathbb{Q}/\mathbb{Z})$ because the action on $\mathbb{Q}/\mathbb{Z}$ is trivial (Hom denotes continuous homomorphisms). $\mathrm{Hom}(G/I, \mathbb{Q}/\mathbb{Z})$ is isomorphic to $\mathbb{Q}/\mathbb{Z}$ via $\varphi \mapsto \varphi(1)$.

Composing these isomorphisms together, we define

$$\mathrm{inv}_K = \mathrm{inv}_G\colon H^2(G, K^{\mathrm{s}\times}) \to \mathbb{Q}/\mathbb{Z}.$$

If L/K is a finite Galois extension of K corresponding to a subgroup $H \leqslant G$, we construct in the same way the map $\mathrm{inv}_L = \mathrm{inv}_H\colon H^2(H, L^{\mathrm{s}\times}) = H^2(H, K^{\mathrm{s}\times}) \to \mathbb{Q}/\mathbb{Z}$ and we can finally check that

$$\begin{array}{ccc} H^2(G, K^{\mathrm{s}\times}) & \xrightarrow{\mathrm{Res}} & H^2(H, K^{\mathrm{s}\times}) \\ \downarrow{\scriptstyle \mathrm{inv}_K} & & \downarrow{\scriptstyle \mathrm{inv}_L} \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{[G:H]} & \mathbb{Q}/\mathbb{Z} \end{array}$$

commutes, hence $(G, K^{\mathrm{s}\times})$ is a class formation. For the proof of this, as well as of facts (1) and (2) (and of the following statements about local class field theory), one can refer to [Ser67].

Theorem 1.2.3. If (G, C) is a class formation, there is a canonical map, called the *reciprocity map*,

$$\mathrm{rec}_G\colon C^G \to G^{\mathrm{ab}}$$

with dense image and $\ker \mathrm{rec}_G = \bigcap N_{G/U} C^U$ (intersection over $U \trianglelefteqslant G$ open of finite index; recall $N_{G/U} = \sum_{\sigma \in G/U} \sigma$).

Proof. This follows from the Tate-Nakayama theorem 1.1.3: first apply the theorem to the particular case

$$(G/U)^{\mathrm{ab}} = \widehat{H}^{-2}(G/U, \mathbb{Z}) \xrightarrow{\sim} \widehat{H}^0(G/U, \mathbb{Z} \otimes C^U) = C^G/N_{G/U}C^U$$
$$a \mapsto a \cup u_{G/U},$$

then pass to the inverse maps; by examining the morphisms in the inverse systems we see that these bijections induce a morphism of inverse systems which, passing to the limit, provides an injection

$$C^G/\bigcap_U N_{G/U}C^U \to G^{\mathrm{ab}}.$$

Composing on the left with the projection from C^G gives the required map rec_G; then, composing on the right with $G^{\mathrm{ab}} \to (G/U)^{\mathrm{ab}}$ for any open $U \leqslant G$ gives a surjection, showing that the image is dense. □

Example 1.2.4. This is again a construction which arises naturally in local class field theory. For a finite Galois extension L/K, the isomorphism between $K^\times/N_{L/K}L^\times$ and $\mathrm{Gal}(L/K)^{\mathrm{ab}}$ is called the *local reciprocity map*. Passing to projective limits we get the reciprocity map $K^\times \to G^{\mathrm{ab}}$: it is injective but not surjective, and it factors as

$$K^\times \hookrightarrow (K^\times)^\wedge \coloneqq \varprojlim_L K^\times/N_{L/K}L^\times \xrightarrow{\sim} G^{\mathrm{ab}}$$

through the completion of $K^\times$ for the topology defined by the so-called norm subgroups.

1.2.1 Duality for class formations

When $M \in G\text{-Mod}$ and (G, C) is a class formation, we can compose the Ext pairings with the invariant map to obtain pairings

$$\mathrm{Ext}^r_G(M, C) \times H^{2-r}(G, M) \to H^2(G, C) \xrightarrow{\mathrm{inv}} \mathbb{Q}/\mathbb{Z}.$$

Writing $A^* = \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$ for A an abelian group, this induces maps

$$\alpha^r(G, M)\colon \mathrm{Ext}^r_G(M, C) \to H^{2-r}(G, M)^*.$$

The following theorem holds:

Theorem 1.2.5 (Duality for class formations)**.**

- $\alpha^r(G, M)$ $(r \geqslant 2)$ is bijective for all finitely generated M.
- $\alpha^1(G, M)$ is bijective for all torsion-free finitely generated M;
  it is bijective for all finitely generated M if $\alpha^1(U, \mathbb{Z}/m\mathbb{Z})$ is bijective for all open $U \leqslant G$ and all m.
- $\alpha^0(G, M)$ is bijective for all finite M if $\alpha^1(G, M)$ is and in addition $\alpha^0(U, \mathbb{Z}/m\mathbb{Z})$ is bijective for all open $U \leqslant G$ and all m.

We start by examining the particular cases $M = \mathbb{Z}$ and $M = \mathbb{Z}/m\mathbb{Z}$; that is, when the G-action is trivial. In the case $M = \mathbb{Z}$:

$\alpha^0(G,\mathbb{Z})\colon C^G = H^0(G,C) \to H^2(G,\mathbb{Z})^* = \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z})^* = G^{\mathrm{ab}}$ is the reciprocity map rec_G

(recall the identification of $H^2(G,\mathbb{Z})$ with $\mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z})$ as in Theorem 1.2.2. Moreover, the equality involving G^{ab} follows from Pontryagin duality for profinite abelian groups);

$\alpha^1(G,\mathbb{Z})\colon 0 = H^1(G,C) \to H^1(G,\mathbb{Z})^* = 0$ is the zero map;

$\alpha^2(G,\mathbb{Z})\colon H^2(G,C) \to H^0(G,\mathbb{Z})^* = \mathbb{Q}/\mathbb{Z}$ is the map inv_G.

They follow easily from the definitions except for α^0. For this, first note that in this case the Ext pairing coincides with the cup-product pairing $H^0(G,C) \times H^2(G,\mathbb{Z}) \to H^2(G,C)$, which we can identify with a pairing $\langle -,-\rangle\colon C^G \times \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z}) \to \mathbb{Q}/\mathbb{Z}$. We want to check that the induced morphism $c \mapsto \langle c,-\rangle$ coincides with the composition

$$C^G \xrightarrow{\mathrm{rec}_G} G^{\mathrm{ab}} \xrightarrow{\sim} \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z})^*, \quad c \mapsto \Big(\chi \mapsto \chi(\mathrm{rec}_G(c))\Big),$$

that is, $\langle c,\chi\rangle = \chi(\mathrm{rec}_G(c))$ for all $c \in C^G$ and $\chi \in \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z})$: this is a well known result in local class field theory, see [Ser80, XI.3, Proposition 2].

The case $M = \mathbb{Z}/m\mathbb{Z}$ then follows:

$\alpha^0(G,\mathbb{Z}/m\mathbb{Z})$ is such that the composition

$$C^G[m] \xrightarrow{\alpha^0} H^2(G,\mathbb{Z}/m\mathbb{Z})^* \twoheadrightarrow G^{\mathrm{ab}}[m]$$

is induced by rec_G on the kernels of the multiplication by m;

$\alpha^1(G,\mathbb{Z}/m\mathbb{Z})\colon C^G/mC^G \to G^{\mathrm{ab}}/mG^{\mathrm{ab}}$ is induced by rec_G;

$\alpha^2(G,\mathbb{Z}/m\mathbb{Z})\colon H^2(G,C)[m] \to \frac{1}{m}\mathbb{Z}/\mathbb{Z}$ is induced by inv_G.

Proof of Theorem 1.2.5. Let us first show that domain and codomain of the maps both vanish for large r. Precisely: for M finitely generated, $\mathrm{Ext}^r_G(M,C) = 0$ $(r \geqslant 4)$; if M is torsion-free, also $\mathrm{Ext}^3_G(M,C) = 0$. To show this, it is enough to show $\mathrm{Ext}^r_G(M,C) = 0$ $(r \geqslant 3)$ in the torsion-free case, because then, for general M, a resolution $0 \to M_1 \to M_0 \to M \to 0$ with M_i finitely generated torsion-free will yield a sequence $\mathrm{Ext}^3_G(M_1,C) = 0 \to \mathrm{Ext}^4_G(M,C) \to 0 = \mathrm{Ext}^4_G(M_0,C)$.

Set $N = \mathrm{Hom}(M,\mathbb{Z})$, hence $N \otimes_{\mathbb{Z}} C \cong \mathrm{Hom}(M,C)$ as G-modules; by Corollary 1.1.8 we have

$$\mathrm{Ext}^r_G(M,C) \cong H^r(G, N \otimes C) = \varinjlim H^r(G/U, N \otimes C^U)$$

where the limit over $N \trianglelefteq G$ open with $N^U = N$ is relative to the Inf maps. This limit is zero when $r \geqslant 3$: indeed, we have a diagram

$$\begin{array}{ccc} H^{r-2}(G/U,N) & \xrightarrow{\sim} & H^r(G/U, N \otimes C^U) \\ \downarrow{\scriptstyle [U:V]\mathrm{Inf}} & & \downarrow{\scriptstyle \mathrm{Inf}} \\ H^{r-2}(G/V,N) & \xrightarrow{\sim} & H^r(G/V, N \otimes C^V) \end{array}$$

where the rows are the isomorphisms $a \mapsto a \cup u$ from the Tate-Nakayama Theorem 1.1.3, for $r-2 \geqslant 1$; the diagram commutes because $\mathrm{Inf}(u_{G/U}) = [U:V]u_{G/V}$ (by definition) and $\mathrm{Inf}(a \cup b) = \mathrm{Inf}(a) \cup \mathrm{Inf}(b)$. As $H^{r-2}(G/U,N)$ is torsion (Corollary 1.1.8) and the

profinite order $|U|$ is divisible by all integers (see definition of class formation), the limit $\varinjlim H^{r-2}(G/U, N)$ relative to the maps $[U : V]\mathrm{Inf}$ is zero, as we claimed.

This proves the cases $r \geqslant 4$. It also implies that $\mathrm{Ext}^3_G(\mathbb{Z}, C) = 0$, and we easily deduce $\mathrm{Ext}^3(\mathbb{Z}/m\mathbb{Z}, C) = 0$: indeed, from the exact sequence $0 \to \mathbb{Z} \xrightarrow{m} \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \to 0$ we get

$$\mathrm{Ext}^2(\mathbb{Z}, C) \to \mathrm{Ext}^2(\mathbb{Z}, C) \to \mathrm{Ext}^3(\mathbb{Z}/m\mathbb{Z}, C) \to 0 = \mathrm{Ext}^3(\mathbb{Z}, C)$$

and $\mathrm{Ext}^2(\mathbb{Z}, C) = H^2(G, C) \cong \mathbb{Q}/\mathbb{Z}$ is divisible, hence $\mathrm{Ext}^3(\mathbb{Z}/m\mathbb{Z}, C) = 0$. Together with the previous analysis of the cases $M = \mathbb{Z}$ or $\mathbb{Z}/m\mathbb{Z}$, this proves the theorem in case of trivial G-action.

In the general case, embed M in a sequence $0 \to M \to M_* \to M_1 \to 0$ where $M_* := \mathrm{Hom}(\mathbb{Z}[G/U], M) = \mathbb{Z}[G/U] \otimes M$ for $U \leqslant G$ open satisfying $M^U = M$. Then $H^r(G, M_*) = H^r(U, M)$ and $\mathrm{Ext}^r_G(M_*, C) = \mathrm{Ext}^r_U(M, C)$ by applying Theorem 1.1.6 with $\mathbb{Z}[G/U]$, M, C. We get a commutative diagram with exact rows

$$\begin{array}{ccccccccc}
\mathrm{Ext}^r_G(M_1, C) & \longrightarrow & \mathrm{Ext}^r_U(M, C) & \longrightarrow & \mathrm{Ext}^r_G(M, C) & \longrightarrow & \mathrm{Ext}^{r+1}_G(M_1, C) & \longrightarrow \\
\downarrow{\scriptstyle \alpha^r(G,M_1)} & & \downarrow{\scriptstyle \alpha^r(U,M)} & & \downarrow{\scriptstyle \alpha^r(G,M)} & & \downarrow{\scriptstyle \alpha^{r+1}(G,M_1)} & \\
H^{2-r}(G, M_1)^* & \longrightarrow & H^{2-r}(U, M)^* & \longrightarrow & H^{2-r}(G, M)^* & \longrightarrow & H^{1-r}(G, M_1)^* & \longrightarrow
\end{array}$$

$\alpha^3(U, M)$, $\alpha^4(G, M_1)$ and $\alpha^4(U, M)$ are isomorphisms because of the above discussion, so by the five-lemma $\alpha^3(G, M)$ is surjective. Since this holds for all M, $\alpha^3(G, M_1)$ is also an isomorphism, and again by the five lemma $\alpha^3(G, M)$ is an isomorphism. Now we can repeat the argument to show $\alpha^2(G, M)$ is an isomorphism.

If M is torsion-free or if $\alpha^1(U, \mathbb{Z}/m\mathbb{Z})$ is bijective, then also $\alpha^1(U, M)$ is an isomorphism (because the theorem is true in case of trivial action), and we use the five lemma twice as before. The proof for $\alpha^0(G, M)$ proceeds in the same way. □

1.3 Local duality for G-modules

Throughout this section:

> K is a non-archimedean local field and $G = \mathrm{Gal}(K^s/K)$;
>
> if M is a G-module, we set $M^D = \mathrm{Hom}(M, K^{s\times})$;
>
> if N is a group, $N^\wedge$ denotes its completion with respect to the subgroups of finite index or, if N has a natural topology induced from K, the completion relative to the subgroups of finite index which are open for that topology.

Recalling that $(G, K^{s\times})$ is a class formation (Theorem 1.2.2), we apply the result of the previous section to this particular case.

Theorem 1.3.1 (Local Tate duality)**.** Let M be a finitely generated G-module with $\mathrm{char}(K)$ not dividing $|\mathrm{Tors}(M)|$. Then, the cup product induces isomorphisms

$$\begin{aligned}
&H^r(G, M^D) \to H^{2-r}(G, M)^* \qquad (r \geqslant 1)\\
&H^0(G, M^D)^\wedge \to H^2(G, M)^*
\end{aligned}$$

Moreover, $H^1(G, M)$ and $H^1(G, M^D)$ are finite.

Proof. $K^{s\times}$ is divisible by all primes except for $\mathrm{char}(K)$, so $\mathrm{Ext}^r(M, K^{s\times}) = 0$ for all $r \geqslant 1$, and therefore using Corollary 1.1.8 we may write $H^r(G, M^D) = \mathrm{Ext}^r_G(M, K^{s\times})$. The result then follows as a particular case from the next theorem. □

Theorem 1.3.2. Let M be a finitely generated G-module; then, there are isomorphisms

$$\begin{aligned}
&\mathrm{Ext}^r_G(M, K^{s\times}) \to H^{2-r}(G, M)^* \qquad (r \geqslant 1)\\
&\mathrm{Hom}_G(M, K^{s\times})^\wedge \to H^2(G, M)^*\\
&(\mathrm{Hom}_G(M, K^{s\times}) \to H^2(G, M)^* \text{ if } M \text{ is finite}).
\end{aligned}$$

Moreover, $\mathrm{Ext}^r_G(M, K^{s\times})$ and $H^r(G, M)$ are

- finite for all r if M is finite with $\mathrm{char}(K) \nmid |M|$
- finite for $r = 1$ if M is finitely generated with $\mathrm{char}(K) \nmid |\mathrm{Tors}(M)|$.

Proof. Duality for class formations (Theorem 1.2.5) immediately implies the isomorphisms for $r \geqslant 2$; for $r = 1$ it will follow once we check that every $\alpha^1(U, \mathbb{Z}/m\mathbb{Z})$ is an isomorphism; and, if M is finite, it will also follow for $r = 0$ if we show that every $\alpha^0(U, \mathbb{Z}/m\mathbb{Z})$ is an isomorphism. Recall that these two maps are induced by rec_G resp. on cokernels and kernels of m; recall the following diagram from local class field theory

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathcal{O}_K^\times & \longrightarrow & K^\times & \xrightarrow{v} & \mathbb{Z} & \longrightarrow & 0\\
 & & \downarrow\sim & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & I^{\mathrm{ab}} & \longrightarrow & G^{\mathrm{ab}} & \longrightarrow & \widehat{\mathbb{Z}} & \longrightarrow & 0
\end{array}$$

[Ser67, p. 144]; then consider the induced diagrams respectively on cokernels and kernels by m to conclude that α^1 (and α^0 for finite M) are isomorphisms.

When M is not finite, the statement still holds if the G-action is trivial, because $\alpha^0(G, \mathbb{Z})$ defines a morphism on the completion

$$\alpha^0(G, \mathbb{Z})^\wedge \colon (K^\times)^\wedge \xrightarrow{\sim} G^{\mathrm{ab}}$$

which is an isomorphism, being the reciprocity map of local class field theory (Example 1.2.4): one should just note that norm subgroups of $K^\times$ coincide with the open finite index subgroups, see [Ser67, Theorem 3]. In general, consider a finite Galois L/K such that $U := \mathrm{Gal}(K^s/L)$ acts trivially, then $\mathrm{Hom}_G(M, K^{s\times}) = \mathrm{Hom}_G(M, L^\times)$, and this contains the open compact subgroup $\mathrm{Hom}_G(M, \mathcal{O}_L^\times)$. Therefore, using notation as in Theorem 1.2.5 for $0 \to M \to M_* \to M_1 \to 0$, the exact sequence

$$0 \to \mathrm{Hom}_G(M_1, K^{s\times}) \to \mathrm{Hom}_U(M_*, K^{s\times}) \to \mathrm{Hom}_G(M, K^{s\times}) \to$$

remains exact after completion, and we complete the proof as in Theorem 1.2.5.

We can now move to the proof of the finiteness statements. If $\mathrm{char}(K) \nmid n$, from the Kummer sequence

$$0 \to \mu_n(K^s) \to K^{s\times} \xrightarrow{n} K^{s\times} \to 0$$

we find, passing to the long cohomology sequence,

$$H^r(G, \mu_n(K^s)) = \begin{cases} \mu_n(K) & r = 0\\ K^\times/K^{\times n} & r = 1\\ \frac{1}{n}\mathbb{Z}/\mathbb{Z} & r = 2\\ 0 & r \geqslant 3 \end{cases}$$

If M is finite with $\mathrm{char}(K) \nmid |M|$, choose a finite Galois extension L/K containing all m-th roots of 1 for $m \mid |M|$ and such that $\mathrm{Gal}(K^{\mathrm{s}}/L)$ acts trivially on M; then

$$M \cong \bigoplus_{m||M|} \mu_m$$

hence we know $H^r(\mathrm{Gal}(K^{\mathrm{s}}/L), M)$ is always finite, and zero for $r \geqslant 3$. The Hochschild-Serre spectral sequence with $H = \mathrm{Gal}(K^{\mathrm{s}}/L)$ becomes

$$H^r(\mathrm{Gal}(L/K), H^s(\mathrm{Gal}(K^{\mathrm{s}}/L), M)) \implies H^{r+s}(G, M)$$

and implies that $H^r(G, M)$ is finite for all r, because the cohomology groups of finite groups $\mathrm{Gal}(L/K)$ with values in finite modules $H^s(\mathrm{Gal}(K^{\mathrm{s}}/L), M)$ are finite. Then by Theorem 1.2.5 all $\alpha^r(G, M)$ are isomorphisms, so $\mathrm{Ext}^r_G(M, K^{\mathrm{s}\times})$ are also finite.

If M is finitely generated with $\mathrm{char}(K) \nmid |\mathrm{Tors}(M)|$, we want to show that $H^1(G, M)$ is finite. We may assume $\mathrm{Tors}(M) = 0$, by the previous case. Choose a finite Galois extension L/K such that $\mathrm{Gal}(K^{\mathrm{s}}/L)$ acts trivially on M. From the exact sequence

$$0 \to H^1(\mathrm{Gal}(L/K), M) \to H^1(G, M) \to H^1(\mathrm{Gal}(K^{\mathrm{s}}/L), M) = 0$$

we have $H^1(G, M) \cong H^1(\mathrm{Gal}(L/K), M)$, which is finite. Theorem 1.2.5 makes it is isomorphic to $\mathrm{Ext}^1_G(M, K^{\mathrm{s}\times})$, which therefore is also finite. □

1.4 Local duality for abelian varieties

1.4.1 Local Euler-Poincaré characteristic

We need a technical result first. For a G-module M of finite order m with $\mathrm{char}(K) \nmid m$, the groups $H^r(G, M)$ are finite for all r and zero for $r \geqslant 3$ (Theorem 1.3.2), so we can define its *Euler-Poincaré characteristic*

$$\chi(G, M) = \frac{|H^0(G, M)||H^2(G, M)|}{|H^1(G, M)|}$$

(note that this recalls the usual Euler characteristic of algebraic topology, but written multiplicatively). We now prove that, for such a module,

Theorem 1.4.1. $\chi(G, M) = (\mathcal{O}_K : m\mathcal{O}_K)^{-1}$.

Set $p = \mathrm{char}(k)$, where k is the residue field of K. Let us first consider the following special case.

Lemma 1.4.2. If the order of M is prime to $\mathrm{char}(K)$, then $\chi(G, M) = 1$.

Proof. Let $I = \mathrm{Gal}(K^{\mathrm{s}}/K^{\mathrm{un}}) \leqslant G$ be the inertia group of G, and $I_p \trianglelefteq I$ be its p-Sylow subgroup. We have

$$I/I_p \cong \widehat{\mathbb{Z}}/\mathbb{Z}_p$$

(see [Ser80, IV]). Consider the Hochschild-Serre spectral sequence

$$H^r(I/I_p, H^s(I_p, M)) \implies H^{r+s}(I, M);$$

since $H^r(I_p, M) = 0$ for $r \geqslant 1$, its long exact sequence from Lemma 1.1.5 reads

$$0 \to H^1(I/I_p, M^{I_p}) \to H^1(I, M) \to 0 \to H^2(I/I_p, M^{I_p}) \to H^2(I, M) \to 0 \to$$

so $H^r(I, M) = H^r(I/I_p, M^{I_p})$; moreover this is finite for all r and zero for $r \geqslant 2$ (see [Ser80, XIII]). Then the Hochschild-Serre spectral sequence

$$H^r(G/I, H^s(I, M)) \implies H^{r+s}(G, M)$$

shows $H^0(G, M) = H^0(G/I, M^I)$ and an exact sequence

$$\begin{aligned} 0 \to H^1(G/I, M^I) \to H^1(G, M) \to H^0(G/I, H^1(I, M)) \to 0 \to \\ \to H^2(G, M) \xrightarrow{\sim} H^1(G/I, H^1(I, M)) \to 0 \end{aligned}$$

Since $G/I \cong \widehat{\mathbb{Z}}$, for any finite $\mathbb{Z}$-module N the exact sequence

$$0 \to H^0(\mathbb{Z}, N) \to N \xrightarrow{\sigma^{-1}} N \to H^1(\widehat{\mathbb{Z}}, N) \to 0$$

(with σ a topological generator of $\widehat{\mathbb{Z}}$) shows $[H^0(\widehat{\mathbb{Z}}, N)] = [H^1(\widehat{\mathbb{Z}}, N)]$, hence

$$\chi(G, M) = \frac{[H^0(G/I, M^I)][H^0(G/I, H^1(I, M))]}{[H^1(G/I, M^I)][H^1(G/I, H^1(I, M))]} = 1.$$

□

By the lemma and the fact that both sides in Theorem 1.4.1 are additive, we may assume $pM = 0$ and $\mathrm{char}(K) = 0$. Suppose L/K is a finite Galois extension such that $L \subseteq K^{\mathrm{s}}$ and $M = M^{\mathrm{Gal}(L^{\mathrm{s}}/L)}$. Then M is an $\mathbb{F}_p[\mathrm{Gal}(L/K)]$-module. For any such module N, denote by $[N]$ its class modulo the equivalence relation

$$[N] = [N_1] + [N_2] \iff 0 \to N_1 \to N \to N_2 \to 0 \text{ is exact}$$

and denote the group of these symbols by $R(\mathrm{Gal}(L/K))$. The left and right sides of Theorem 1.4.1 define morphisms of groups

$$\chi_l, \chi_r \colon R(\mathrm{Gal}(L/K)) \to \mathbb{Q}_{>0}$$

Since $\mathbb{Q}_{>0}$ is torsion-free, it suffices to show $\chi_l = \chi_r$ on a set of generators for $R(\mathrm{Gal}(L/K)) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Lemma 1.4.3. If G is a finite group, then $R(G) \otimes \mathbb{Q}$ is generated by the images of the morphism

$$\mathrm{Ind}_H^G \colon R(H) \otimes \mathbb{Q} \to R(G) \otimes \mathbb{Q}, \quad [N] \mapsto [\oplus gN]$$

where $H \leqslant G$ is cyclic of order prime to p, N is an H-module, the direct sum is over a system of representatives mod H.

Proof. From [Ser70]. □

Hence it is enough to prove the theorem for M of the form $\mathrm{Ind}_N^{\mathrm{Gal}(L/K)}$. Let $K' = L^H$ and $n = |N|$; then we have

$$\begin{aligned} \chi(G, M) &= \chi(\mathrm{Gal}(K^{\mathrm{s}}/K'), N) \\ (\mathcal{O}_K : m\mathcal{O}_K) &= (\mathcal{O}_K : n\mathcal{O}_K)^{[K':K]} = (\mathcal{O}_{K'} : n\mathcal{O}_{K'}) \end{aligned}$$

which shows it is enough to prove the theorem for N, and therefore we can assume $\mathrm{Gal}(L/K)$ to be cyclic of order prime to p. In this case, when $r \geqslant 1$, $H^r(\mathrm{Gal}(L/K), M) = 0$ and so $H^r(G, M) = H^r(\mathrm{Gal}(K^{\mathrm{s}}/L), M)^{\mathrm{Gal}(L/K)}$.

Consider the group morphisms

$$\begin{aligned} \chi' \colon R(\mathrm{Gal}(L/K)) &\to R(\mathrm{Gal}(L/K)) \\ [N] &\mapsto \sum (-1)^i [H^i(\mathrm{Gal}(K^{\mathrm{s}}/L), N)] \end{aligned}$$

$$\begin{aligned} \theta \colon R(\mathrm{Gal}(L/K)) &\to \mathbb{Q}_{>0} \\ [N] &\mapsto |N^{\mathrm{Gal}(L/K)}| \end{aligned}$$

Lemma 1.4.4. $\chi'(M) = -\dim(M)[K : \mathbb{Q}_p]\#\mathbb{F}_p[\mathrm{Gal}(L/K)]$

Note that, since $\theta \circ \chi' = \chi$ and $\theta[\mathbb{F}_p[\mathrm{Gal}(L/K)]] = p$, this lemma would show

$$\chi(M) = \theta \circ \chi'(M) = p^{-[K:\mathbb{Q}_p]\dim(M)} = (\mathcal{O}_K : m\mathcal{O}_K)^{-1}$$

proving the theorem. So we proceed with the proof of this lemma.

Proof. Tensoring M with an injective $\frac{\mathbb{Z}}{p\mathbb{Z}}[\mathrm{Gal}(L/K)]$-resolution of $\mathbb{Z}/p\mathbb{Z}$, we see that the cup product defines isomorphisms of $\mathrm{Gal}(L/K)$-modules

$$H^r(\mathrm{Gal}(K^{\mathrm{s}}/L), \mathbb{Z}/p\mathbb{Z}) \otimes M \to H^r(\mathrm{Gal}(K^{\mathrm{s}}/L), M)$$

hence $\chi'(M) = \dim(M)\chi'(\mathbb{Z}/p\mathbb{Z})$. Let M_0 be the G-module with underlying set M and trivial G-action. The isomorphism

$$\begin{aligned} \mathbb{F}_p[\mathrm{Gal}(L/K)] \otimes M_0 &\xrightarrow{\sim} \mathbb{F}_p[\mathrm{Gal}(L/K)] \otimes M \\ \sigma \otimes m &\mapsto \sigma \otimes \sigma m \end{aligned}$$

shows $\dim(M)\#\mathbb{F}_p[\mathrm{Gal}(L/K)] = \#\mathbb{F}_p[\mathrm{Gal}(L/K)]|M|$, so the general equality in the lemma follows from the special case $M = \mathbb{Z}/p\mathbb{Z}$.

$$\begin{aligned} H^0(\mathrm{Gal}(K^{\mathrm{s}}/L), \mathbb{Z}/p\mathbb{Z}) &= \mathbb{Z}/p\mathbb{Z} \\ H^1(\mathrm{Gal}(K^{\mathrm{s}}/L), \mathbb{Z}/p\mathbb{Z}) &= H^1(\mathrm{Gal}(K^{\mathrm{s}}/L), \mu_p(K^{\mathrm{s}}))^* = (L^\times/L^{\times p})^* \\ H^2(\mathrm{Gal}(K^{\mathrm{s}}/L), \mathbb{Z}/p\mathbb{Z}) &= \mu_p(L)^* \end{aligned}$$

where $(-)^*$ denotes $\mathrm{Hom}(-, \mathbb{F}_p)$ seen as a $\mathrm{Gal}(L/K)$-module. Since the functor $\mathrm{Hom}(-, \mathbb{F}_p)$ is exact (because $\mathbb{F}_p$ is divisible), it is defined on $R(\mathrm{Gal}(L/K))$. Hence

$$\begin{aligned} \chi'(\mathbb{Z}/p\mathbb{Z})^* &= [\mu_p(L)] + [\mathbb{Z}/p\mathbb{Z}] - [L^\times/L^{\times p}] \\ &= [\mu_p(L)] - [\mathcal{O}_L^\times/\mathcal{O}_L^{\times p}] \\ &= [\mu_p(\mathcal{O}_L^\times)] - [\mathcal{O}_L^\times/\mathcal{O}_L^{\times p}], \end{aligned}$$

second line following from the exact sequence $0 \to \mathcal{O}_L^\times/\mathcal{O}_L^{\times p} \to L^\times/L^{\times p} \to \mathbb{Z}/p\mathbb{Z} \to 0$.

Note now the following fact: for W and W' finitely generated $\mathbb{Z}_p[H]$-modules with H finite group, if $W \otimes \mathbb{Q}_p \cong W' \otimes \mathbb{Q}_p$, then

$$[W/pW] - [W_p] = [W'/pW'] - [W'_p] \text{ in } \mathbb{F}_p[H].$$

This is shown by reducing to the case $pW \subset W' \subset W$, in which case we have the exact sequence (given by the snake lemma)

$$0 \to W'_p \to W_p \to W/W' \to W'/pW' \to W/pW \to W/W' \to 0.$$

We apply this result as follows. The exponential series maps an open subgroup of $\mathcal{O}_L^\times$ onto an open subgroup of $(\mathcal{O}_L, +)$, hence

$$[\mathcal{O}_L^\times/\mathcal{O}_L^{\times p}] - [\mu_p(\mathcal{O}_L^\times)] = [\mathcal{O}_L/p\mathcal{O}_L] - [(\mathcal{O}_L)_p] = [\mathcal{O}_L/p\mathcal{O}_L].$$

The normal basis theorem says $L \cong \mathbb{Q}_p[\mathrm{Gal}(L/K)]^{[K:\mathbb{Q}_p]}$ as $\mathrm{Gal}(L/K)$-modules, hence

$$[\mathcal{O}_L/p\mathcal{O}_L] = [K:\mathbb{Q}_p][\mathbb{F}_p[\mathrm{Gal}(L/K)]]$$

and we conclude by $[\mathbb{F}_p[\mathrm{Gal}(L/K)]]^* = [\mathbb{F}_p[\mathrm{Gal}(L/K)]]$. Putting things together,

$$\begin{aligned}\chi'(M) &= \dim(M)\chi'(\mathbb{Z}/p\mathbb{Z}) \\ &= -\dim(M)[K:\mathbb{Q}_p][\mathbb{F}_p[\mathrm{Gal}(L/K)]]^* \\ &= -\dim(M)[K:\mathbb{Q}_p][\mathbb{F}_p[\mathrm{Gal}(L/K)]].\end{aligned}$$

□

1.4.2 Local duality for abelian varieties

In this paragraph, the notion of *dual abelian variety* comes into play. Since we are interested with the self-dual case of elliptic curves, we do not develop a rigorous theory for this notion. However, since the arguments would be the same, we will state the results for general abelian varieties, and we will content ourselves with the following definition of dual abelian variety:

$$A^t = \mathrm{Ext}^1(A, \mathbb{G}_m)$$

so $A^t(K^s) = \mathrm{Ext}^1_{K^s}(A, \mathbb{G}_m)$. As for elliptic curves, also for general abelian varieties there is a *Weil pairing*, a perfect pairing

$$A_n(K^s) \times A^t_n(K^s) \to \mu_n(K^s)$$

inducing an isomorphism

$$A^t_n(K^s) \cong \mathrm{Hom}(A_n(K^s), K^{s\times}).$$

If we set $M = A_n(K^s)$, this means that $M^D = A^t_n(K^s)$, relating these two types of duals.

We set the following notation:

$H^r(K, A) = H^r(\mathrm{Gal}(K^s/K), A(K^s))$

the subscript n, whether on groups or on the group scheme A, denotes the kernel of multiplication by n.

When K is perfect, there is a pairing

$$\mathrm{Ext}^r_K(A, \mathbb{G}_m) \times H^{2-r}(K, A) \to H^2(K, \mathbb{G}_m) = H^2(G, K^{s\times}) \cong \mathbb{Q}/\mathbb{Z}$$

obtained composing the Ext pairing in Section 1.1.3 and the inv_G isomorphism. This induces a canonical map

$$\alpha^r(K, A)\colon \mathrm{Ext}^r_K(A, \mathbb{G}_m) \to H^{2-r}(K, A)^*.$$

Tate proved the following result:

Theorem 1.4.5. When K is perfect, there is a canonical pairing

$$H^r(K, A^t) \times H^{1-r}(K, A) \to \mathbb{Q}/\mathbb{Z}.$$

When $\operatorname{char} K = 0$, it induces isomorphisms $H^r(K, A^t) \cong H^{1-r}(K, A)^*$, that is

- $A^t(K) \xrightarrow{\sim} H^1(K, A)^*$ for $r = 0$,
- $H^1(K, A^t) \xrightarrow{\sim} A(K)^*$ for $r = 1$,
- $0 \to 0$ for $r \neq 0, 1$.

Proof. When K is perfect, there is a canonical isomorphism

$$H^r(K, A^t) \cong \operatorname{Ext}^{r+1}_K(A, \mathbb{G}_m)$$

following from the spectral sequence in Proposition 1.1.9 using that $\operatorname{Ext}^r_{K^s}(A, \mathbb{G}_m)$ is 0 for $r \geqslant 2$ [Oor66] and $\operatorname{Hom}_{K^s}(A, \mathbb{G}_m) = 0$ because A is an abelian variety, so it is projective, whereas $\mathbb{G}_m$ is affine (as it corresponds to the K-algebra $K[X, Y]/(XY - 1)$). This shows the existence of the stated pairing.

Suppose now $\operatorname{char}(K) = 0$. Consider the sequence $0 \to A_n \to A \xrightarrow{n} A \to 0$; applying $\operatorname{Ext}^r_K(-, \mathbb{G}_m)$ and using the canonical maps as vertical arrows, we get the following diagram (superscript (n) denotes cokernel of the map induced by multiplication by n)

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \operatorname{Ext}^r_K(A, \mathbb{G}_m)^{(n)} & \longrightarrow & \operatorname{Ext}^r_K(A_n, \mathbb{G}_m) & \longrightarrow & \operatorname{Ext}^{r+1}_K(A, \mathbb{G}_m)_n & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \alpha^r(K,A)^{(n)}} & & \downarrow{\scriptstyle \alpha^r(K,A_n)} & & \downarrow{\scriptstyle \alpha^{r+1}(K,A)_n} & & \\
0 & \longrightarrow & \left(H^{2-r}(K, A)_n\right)^* & \longrightarrow & H^{2-r}(K, A_n)^* & \longrightarrow & H^{1-r}(K, A)^{(n)*} & \longrightarrow & 0
\end{array}$$

Using $\operatorname{Ext}^r_K(A_n, \mathbb{G}_m) \cong \operatorname{Ext}^r_G(A_n(K^s), K^{s\times})$ we identify $\alpha^r(K, A_n)$ with $\alpha^r(G, A_n(K^s))$, so we see that the diagram commutes; by Theorem 1.3.2, this map is an isomorphism of finite groups for all r (recall for example that, for elliptic curves, $A_n(K^s)$ is $(\mathbb{Z}/n\mathbb{Z})^2$ when $\operatorname{char}(K)$ does not divide n). Hence, $\alpha^r(K, A)^{(n)}$ is injective; taking inverse limits we still get an injective map

$$\varprojlim_n \alpha^r(K, A)^{(n)} \colon \varprojlim_n \operatorname{Ext}^r_K(A, \mathbb{G}_m)^{(n)} \to \operatorname{Tors}(H^{2-r}(K, A))^*.$$

Let $r = 1$, and recall $\operatorname{Ext}^1_K(A, \mathbb{G}_m) = A^t(K)$. [Mat55] assures that, if B is an abelian variety of dimension d over a local field K of characteristic 0, then $B(K)$ contains an open subgroup of finite index isomorphic to $\mathcal{O}_K^d$. It implies that $B(K) = B(K)^\wedge$, the completion for the profinite topology. Applying this to the variety A^t and using the previous equality in terms of Ext, we get

$$\operatorname{Ext}^1_K(A, \mathbb{G}_m) = A^t(K) = \varprojlim A^t(K)^{(n)} = \varprojlim \operatorname{Ext}^1_K(A, \mathbb{G}_m)^{(n)}.$$

Furthermore

$$\operatorname{Tors}(H^1(K, A)) = H^1(K, A)$$

since it is finite (Theorem 1.3.2); we conclude $\alpha^1(K, A) = \varprojlim_n \alpha^r(K, A)^{(n)}$, hence $\alpha^1(K, A)$ is injective.

We now show $H^r(K,A)=0$ for $r\geqslant 2$. For $r\geqslant 3$ this follows from 1.3.2, i.e. G has cohomological dimension 2. To show $H^2(K,A)=0$, take $r=0$ in the diagram above: we get an exact commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & 0 & \longrightarrow & \mathrm{Hom}_K(A_n,\mathbb{G}_m) & \longrightarrow & \mathrm{Ext}^1_K(A,\mathbb{G}_m) \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \left(H^2(K,A)_n\right)^* & \longrightarrow & H^2(K,A_n)^* & \longrightarrow & H^1(K,A)^* \end{array}$$

Since the middle vertical arrow is an isomorphism and the left arrow is injective, we deduce $H^2(K,A)_n=0$ and hence $H^2(K,A)=0$. We also conclude that $\mathrm{Ext}^r_K(A,\mathbb{G}_m)$ (which equals $H^{r-1}(G,A^t)$) is 0 for $r\neq 1,2$.

To show that $\alpha^1(K,A)$ is an isomorphism, we show that the injections $A^t(K)\to H^1(K,A)^*$ give surjections $A^t(K)^{(n)}\to\left(H^1(K,A)_n\right)^*$ for all n. It is enough to show the groups have the same orders. Set $M=A_n(K^{\mathrm{s}})$, $M^D=A^t_n(K^{\mathrm{s}})$, $d=\dim A$. We have, from Theorem 1.4.1:

$$\chi(G,M)=(\mathcal{O}_K:n\mathcal{O}_K)^{-2d}=\chi(G,M^D),$$
$$\frac{|A(K)^{(n)}|}{|A(K)_n|}=[R:nR]^d=\frac{|A^t(K)^{(n)}|}{|A^t(K)_n|}.$$

From $H^0(G,M^D)=A^t_n(K)$ we get

$$|H^1(G,A)_n|=(\mathcal{O}_K:n\mathcal{O}_K)^d|A^t_n(K)|=|A^t(K)^{(n)}|$$

and we conclude.

To show that $\alpha^2(K,A)$ is an isomorphism, consider the first diagram: we have surjectivity of

$$\alpha^2(K,A)\colon\ \mathrm{Ext}^2_K(A,\mathbb{G}_m)\cong H^1(K,A^t)\to A(K)^*=H^0(K,A)^*.$$

Repeating the calculations of the orders with A and A^t interchanged gives $|H^1(G,A^t)_n|=|A(K)^{(n)}|$ implying that the map is an isomorphism. □

1.5 Specialization to elliptic curves

1.5.1 Local duality

We use notations:

E is an elliptic curve over K

$H^r(K,E)=H^r(\mathrm{Gal}(K^{\mathrm{s}}/K),E(K^{\mathrm{s}}))$

$H^r(L/K,E)=H^r(\mathrm{Gal}(L/K),E(L))$

the subscript n, whether on groups or on the group scheme E, denotes the kernel of multiplication by n.

Consider the composition, denoted by $\langle -,-\rangle$:

$$H^1(K,E_n)\times H^1(K,E_n)\xrightarrow{\cup}H^2(K,E_n\otimes E_n)\to H^2(K,\mu_n)\cong\mathbb{Z}/n\mathbb{Z}$$

of the cup product and the map induced by the Weil pairing

$$E_n(K^{\mathrm{s}})\otimes E_n(K^{\mathrm{s}})\to\mu_n(K^{\mathrm{s}}).$$

Theorem 1.5.1. The pairing $\langle -,-\rangle\colon H^1(K,E_n)\times H^1(K,E_n)\to \mathbb{Z}/n\mathbb{Z}$ is a perfect, symmetric, Galois-equivariant pairing.

Proof. This is a particular case of the duality theorem 1.3.1. The Weil pairing is perfect, hence gives an isomorphism of abelian groups

$$E_n(K^{\mathrm{s}})\cong \mathrm{Hom}(E_n(K^{\mathrm{s}}),\mu_n(K^{\mathrm{s}})).$$

Setting $M=E_n(K^{\mathrm{s}})$, we have

$$M^D\coloneqq \mathrm{Hom}(M,K^{\mathrm{s}\times})=\mathrm{Hom}(M,\mu_n(K^{\mathrm{s}}))\cong M.$$

Therefore, the cup-product pairing

$$H^1(G,M^D)\times H^1(G,M)\to H^2(G,K^{\mathrm{s}\times})$$

is actually a pairing into $H^2(G,\mu_n(K^{\mathrm{s}}))$, and using $M^D\cong M$ we can now write it as

$$H^1(K,E_n)\times H^1(K,E_n)\to H^2(K,\mu_n).$$

□

Theorem 1.5.2. Assume $\mathrm{char}(k)\nmid n$, where k is the residue field of K. Then:

1. the subgroup $E(K)/nE(K)$ of $H^1(K,E_n)$ is isotropic for $\langle -,-\rangle$;
2. if E has good reduction, $\langle -,-\rangle$ induces a non-degenerate pairing of abelian groups
$$[-,-]\colon E(K)/nE(K)\times H^1(K,E)_n\to \mathbb{Z}/n\mathbb{Z}.$$

Proof. (1) From the commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E(K^{\mathrm{un}})_n & \longrightarrow & E(K^{\mathrm{un}}) & \xrightarrow{n} & E(K^{\mathrm{un}}) & \longrightarrow & 0\\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E(K^{\mathrm{s}})_n & \longrightarrow & E(K^{\mathrm{s}}) & \xrightarrow{n} & E(K^{\mathrm{s}}) & \longrightarrow & 0
\end{array}$$

we pass to cohomology and extract Kummer sequences

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \dfrac{E(K)}{nE(K)} & \longrightarrow & H^1(K^{\mathrm{un}}/K,E_n) & \longrightarrow & H^1(K^{\mathrm{un}}/K,E)_n & \longrightarrow & 0\\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \dfrac{E(K)}{nE(K)} & \longrightarrow & H^1(K,E_n) & \longrightarrow & H^1(K,E)_n & \longrightarrow & 0
\end{array}$$

Commutativity of the left square implies the existence of a commutative diagram

$$\begin{array}{ccc}
E(K)/nE(K)\times E(K)/nE(K) & & \\
\downarrow & & \\
H^1(K^{\mathrm{un}}/K,E_n)\times H^1(K^{\mathrm{un}}/K,E_n) & \longrightarrow & H^2(K^{\mathrm{un}}/K,\mu_n)\\
\downarrow{\scriptstyle \mathrm{Inf}\times\mathrm{Inf}} & & \downarrow{\scriptstyle \mathrm{Inf}}\\
H^1(K,E_n)\times H^1(K,E_n) & \longrightarrow & H^2(K,\mu_n)
\end{array}$$

where the horizontal maps are given by the pairing $\langle -, - \rangle$. However

$$H^2(K^{\mathrm{un}}/K, \mu_n) = 0,$$

so the restriction of $\langle -, - \rangle$ to $E(K)/nE(K)$ factors through the trivial group.

(2) It is enough to check that $E(K)/nE(K)$ is maximal isotropic.

Since E has good reduction at v, $H^1(K^{\mathrm{un}}/K, E) = 0$ hence $E(K)/nE(K)$ is isomorphic to $H^1(K^{\mathrm{un}}/K, E_n)$. We conclude by the following more general theorem, applied to $M = E_n(K^{\mathrm{un}})$. □

Theorem 1.5.3. Let $I = \mathrm{Gal}(K^{\mathrm{s}}/K^{\mathrm{un}})$, $M^d = \mathrm{Hom}(M, \mathcal{O}_{K^{\mathrm{un}}}^{\times})$.

If M is a finitely generated G-module with $\mathrm{char}(k) \nmid |\mathrm{Tors}(M)|$ such that $M^I = M$, then $H^1(G/I, M)$ and $H^1(G/I, M^d)$ are the exact annihilators of each other in the pairing

$$H^1(G, M) \times H^1(G, M^D) \to \mathbb{Q}/\mathbb{Z}.$$

Proof. Since $\mathrm{Ext}_I^1(\mathbb{Z}, K^{\mathrm{s}\times}) = H^1(I, K^{\mathrm{s}\times}) = 0$ by local class field theory, the spectral sequence 1.1.6

$$\mathrm{Ext}_{G/I}^r(M, \mathrm{Ext}_I^s(\mathbb{Z}, K^{\mathrm{s}\times})) \implies \mathrm{Ext}_G^{r+s}(M, K^{\mathrm{s}\times})$$

gives an isomorphism $\mathrm{Ext}_{G/I}^1(M, K^{\mathrm{un}\times}) \cong \mathrm{Ext}_G^1(M, K^{\mathrm{s}\times})$. The split sequence

$$0 \to \mathcal{O}_{K^{\mathrm{un}}}^{\times} \to K^{\mathrm{un}\times} \to \mathbb{Z} \to 0$$

shows, after applying $\mathrm{Ext}_{G/I}^1(M, -)$,

$$\mathrm{Ext}_{G/I}^1(M, \mathcal{O}_{K^{\mathrm{un}}}^{\times}) = \ker\left(\mathrm{Ext}_G^1(M, K^{\mathrm{s}\times}) \to \mathrm{Ext}_{G/I}^1(M, \mathbb{Z})\right).$$

The following diagram commutes

$$\begin{array}{ccc} \mathrm{Ext}_G^1(M, K^{\mathrm{s}\times}) & \xrightarrow{\sim} & H^1(G, M)^* \\ \downarrow & & \downarrow{\scriptstyle \mathrm{Inf}^*} \\ \mathrm{Ext}_{G/I}^1(M, \mathbb{Z}) & \xrightarrow{\sim} & H^1(G/I, M)^* \end{array}$$

showing that also

$$\mathrm{Ext}_{G/I}^1(M, \mathcal{O}_{K^{\mathrm{un}}}^{\times}) = \ker\left(\mathrm{Ext}_G^1(M, K^{\mathrm{s}\times}) \to \mathrm{Ext}_{G/I}^1(M, \mathbb{Z})\right).$$

Since $\mathrm{Ext}_G^1(M, K^{\mathrm{s}\times}) \cong H^1(G, M^D)$ and $\mathrm{Ext}_{G/I}^1(M, \mathcal{O}_{K^{\mathrm{un}}}^{\times}) \cong H^1(G/I, M^d)$ by Corollary 1.1.8, we can write

$$H^1(G/I, M^d) = \ker\left(H^1(G, M^D) \to H^1(G/I, M)^*\right).$$

□

1.5.2 Global duality

Let K be a number field. For every prime v of K, K_v is a local field and there are pairings

$$\langle -,-\rangle_v \colon H^1(K_v,E_n)\times H^1(K_v,E_n)\to \mathbb{Z}/n\mathbb{Z}$$
$$[-,-]_v \colon E(K_v)/nE(K_v)\times H^1(K_v,E)_n\to \mathbb{Z}/n\mathbb{Z}$$

as in the previous paragraph.

Let $\Pi^1(K,E_n)$ denote the restricted direct product of the groups $H^1(K_v,E_n)$ with respect to their subgroups $E(K_v)/nE(K_v)$. The sum of all local pairings yields a global pairing

$$\langle -,-\rangle \colon \Pi^1(K,E_n)\times \Pi^1(K,E_n)\to \mathbb{Z}/n\mathbb{Z}$$
$$(a,b)\mapsto \sum_v \langle a_v,b_v\rangle_v$$

This is a good definition because $\langle a_v,b_v\rangle_v$ can be non-zero only for the finitely many v such that one of a_v, b_v is not in $E(K_v)/nE(K_v)$.

Proposition 1.5.4. The image of $H^1(K,E_n)$ in $\Pi^1(K,E_n)$ is isotropic with respect to $\langle -,-\rangle$.

Proof. Let $a,b\in H^1(K,E_n)$;

$$\langle a,b\rangle = \sum_v \langle a_v,b_v\rangle_v = \sum_v \mathrm{inv}_v(w(a_v\cup b_v))$$

and $(w(a_v\cup b_v))_v = (w(a\cup b)_v)_v \in \mathrm{Br}(K)$. Then, by global class field theory, the sum of its invariants is 0; in other words, there is an exact sequence

$$0\to \mathrm{Br}(K)\to \bigoplus_v \mathrm{Br}(K_v)\xrightarrow{\sum\circ\,\mathrm{inv}} \mathbb{Q}/\mathbb{Z}\to 0$$

(see [Tat67, VII.10, Theorem B]). □

1.6 The Tate-Shafarevich and Selmer groups

Let now K be a number field, E/K an elliptic curve.

The Selmer and Tate-Shafarevich groups arise when trying to compute generators for the weak Mordell-Weil groups $E(K)/nE(K)$ or the rank of E, i.e. the rank of the free part of $E(K)$. We introduce them directly using Galois cohomology, rather than by homogeneous spaces. Given the diagram with exact rows

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \dfrac{E(K)}{nE(K)} & \xrightarrow{\kappa} & H^1(K,E_n) & \longrightarrow & H^1(K,E)_n & \longrightarrow & 0\\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \displaystyle\prod_v \frac{E(K_v)}{nE(K_v)} & \longrightarrow & \displaystyle\prod_v H^1(K_v,E_n) & \longrightarrow & \displaystyle\prod_v H^1(K_v,E)_n & \longrightarrow & 0
\end{array}$$

the ultimate goal is the image of the Kummer map κ, or equivalently the kernel of the top-row surjection. This is locally easy, suggesting the definition of the following objects:

Definition 1.6.1.

The *n-Selmer group* is defined as

$$\begin{aligned} S_n(K,E) &= \ker\left(H^1(K,E_n) \to \prod_v H^1(K_v,E)\right) \\ &= \ker\left(H^1(K,E_n) \to \prod_v \frac{H^1(K_v,E_n)}{\operatorname{im}\kappa_v}\right) \end{aligned}$$

The *Tate-Shafarevich group* is defined as

$$Ш(K,E) = \ker\left(H^1(K,E) \to \prod_v H^1(K_v,E)\right)$$

Remark 1.6.2. If $a \in H^1(K,A)$, its image in $H^1(K_v,A)$ is zero for almost all primes v. Therefore, we can substitute the direct product with a direct sum in the above definition.

By the above diagram, we immediately get a relation between these two groups by the short exact sequence

$$0 \to E(K)/nE(K) \to S_n(K,E) \to Ш(K,E)_n \to 0.$$

Moreover, Selmer groups are proven to be finite and, in theory, computable. Hence, the order $|S_n(K,E)| = |E(K)/nE(K)||Ш(K,E)_n|$ can be used to bound the rank of E, and the Tate-Shafarevich group measures the difference between the bound and the actual rank. When we are able to compute $Ш(K,E)_n$, then generators for $E(K)/mE(K)$ can be found, hence for $E(K)$.

In the interpretation via homogeneous spaces, elements of $S_n(K,E)$ can be seen as (classes of) homogeneous spaces which locally have rational points at every v; in particular, those which fail to have a global rational point in K correspond to the non-trivial elements of $Ш(K,E)_n$. This occurence is a failure of the so-called *Hasse principle*.

A useful tool in studying these groups is the following

Proposition 1.6.3 (The Cassels-Tate pairing)**.** There exists a canonical alternating pairing

$$\langle -,- \rangle_{CT} \colon Ш(K,E) \times Ш(K,E) \to \mathbb{Q}/\mathbb{Z}$$

whose left and right kernel is the divisible subgroup of $Ш(K,E)$.

This was defined by Cassels in [Cas62] using homogeneous spaces and generalized to abelian varieties by Tate in [Tat62]. We will now describe a cohomological construction of the induced pairing on the torsion

$$\langle -,- \rangle_{CT} \colon Ш(K,E)_n \times Ш(K,E)_n \to \mathbb{Q}/\mathbb{Z};$$

note that this also lifts to a pairing on the Selmer groups

$$\langle -,- \rangle_{CT} \colon S_n(K,E) \times S_n(K,E) \to \mathbb{Q}/\mathbb{Z}.$$

Let $a, a' \in Ш(K,E)_n$; we can lift them to $b, b' \in H^1(K, E_n)$. By definition of $Ш(K,E)$, $a_v = 0$ in $H^1(K_v, E)$ for every v; hence, looking at

$$\begin{array}{ccccc} E(K_v) & \longrightarrow & H^1(K_v, E_n) & \longrightarrow & H^1(K_v, E) \\ \| & & \uparrow & & \\ E(K_v) & \longrightarrow & H^1(K_v, E_{n^2}) & & \end{array}$$

we can lift b_v to $b_{v,1} \in H^1(K_v, E_{n^2})$.

Suppose that a is divisible by n in $H^1(K,E)$, write $a = na_1$; lift a_1 to $b_1 \in H^1(K_v, E_{n^2})$. Then $b_{v,1} - b_{1,v}$ maps to zero in $H^1(K_v, E_n)$, so it is the image in $H^1(K_v, E_{n^2})$ of some $c_v \in H^1(K_v, A_m)$. Set

$$\langle a, a' \rangle = \sum_v \mathrm{inv}_v(c_v \cup b'_v) \in \mathbb{Q}/\mathbb{Z}$$

where the cup product is induced by the Weil pairing.

In general, let β be a cocycle representing b and lift it to a cochain $\beta_1 \in C^1(K, E_n)$. Choose $\beta_{v,1} \in Z^1(K_v, E_{n^2})$ representing $b_{v,1}$ and $\beta' \in Z^1(K_v, E_n)$ representing b'. The coboundary $d\beta_1$ takes values in E_n and $d\beta_1 \cup \beta'$ represents an element in $H^3(K, \mathbb{G}_m)$. This group is zero by, hence $d\beta_1 \cup \beta' = d\varepsilon$ for some $\varepsilon \in C^2(K, \mathbb{G}_m)$. We define

$$\langle a, a' \rangle = \sum_v \mathrm{inv}_v \left((\beta_{v,1} - \beta_{1,v}) \cup \beta'_v - \varepsilon_v \right) \in \mathbb{Q}/\mathbb{Z}.$$

It can then be checked that this construction does not depend on the choices made.

Remark 1.6.4. We may also define a general Selmer group

$$S(K,E) \coloneqq \ker \left(H^1(K, \mathrm{Tors}(E)) \to \bigoplus_v \frac{H^1(K_v, \mathrm{Tors}(E))}{\mathrm{im}\, \kappa_v} \right)$$

where $\kappa_v \colon E(K_v) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z}) \to H^1(K_v, \mathrm{Tors}(E))$, and we denote its p-primary component by

$$S_{p^\infty}(K,E) \coloneqq \ker \left(H^1(K, E_{p^\infty}) \to \bigoplus_v \frac{H^1(K_v, E_{p^\infty})}{\mathrm{im}\, \kappa_v} \right)$$

where $\kappa_v \colon E(K_v) \otimes_{\mathbb{Z}} (\mathbb{Q}_p/\mathbb{Z}_p) \to H^1(K_v, E_{p^\infty})$ and the subscript p^∞ denotes the p-primary part.

1.7 Global duality

Let K be a global field, $G = \mathrm{Gal}(K^{\mathrm{s}}/K)$. Denote:

S a non-empty set of primes containing the archimedean primes

K_S the maximal subfield of K^{s} unramified outside S

$G_S = \mathrm{Gal}(K_S/K)$

$\mathcal{O}_{K,S} = \bigcap_{v \notin S} \mathcal{O}_v = \{a \in K \mid \mathrm{ord}_v(a) \geqslant 0 \text{ for all } v \notin S\}$

$G_v = \mathrm{Gal}(K_v^{\mathrm{s}}/K_v)$, which is isomorphic to $\{\sigma \in G \mid \sigma w = w\}$, the decomposition group of w after choosing some $w \mid v$

P the set of rational primes $\ell \in \mathbb{Z}$ such that ℓ^∞ divides $[K_S : K] \coloneqq |G_S|$

We also let F/K be a finite extension contained in K_S, and let S_F be the set of primes of F lying over primes in S; denote:

$J_F = \prod' F_w^\times$ the idéle group of F ($\prod'$ will denote restricted product with respect to the specified subgroups)

$C_F = J_F/F^\times$ the idéle class group of F

$J_{F,S} = \{(a_w) \in J_F \mid a_w = 1 \text{ for } w \notin S\} \cong \prod'_{w \in S} F_w^\times$

$\mathcal{O}_{F,S} = \bigcap_{w \notin S_F} \mathcal{O}_w$ the ring of S_F-integers

$C_{F,S} = J_{F,S}/\mathcal{O}_{F,S}^\times$ the group of S_F-idéle classes

$U_{F,S} = \{(a_w)_w \in J_F \mid a_w \in \widehat{\mathcal{O}}_w^\times \text{ if } w \notin S, a_w = 1 \text{ if } w \in S\} \cong \prod_{w \notin S} \widehat{\mathcal{O}}_w^\times$

Taking limits over all finite extensions F/K contained in K_S, define

$$E_S = \varinjlim \mathcal{O}_{F,S}^\times \qquad J_S = \varinjlim J_{F,S} \qquad C_S = \varinjlim C_{F,S}$$
$$\mathcal{O}_S = \varinjlim \mathcal{O}_{F,S} \qquad U_S = \varinjlim U_{F,S}$$

Let M be a finitely generated G_S-module. For v non-archimedean, write $k(v)$ for the residue field, $g_v = \mathrm{Gal}(k(v)^{\mathrm{s}}/k(v)) \cong G_v/I_v$; the embedding $K^{\mathrm{s}} \hookrightarrow K_v^{\mathrm{s}}$ determines maps $G_v \to G \twoheadrightarrow G_S$, which induce localization maps

$$H^r(G_S, M) \to H^r(G_v, M).$$

We write

$H^r(K_v, M) = H^r(G_v, M)$ if v is non-archimedean,

$H^r(K_v, M) = \widehat{H}^r(G_v, M)$ if v is archimedean.

Consider the map

$$H^r(G_S, M) \to \prod_{v \in S} H^r(K_v, M)$$

We may restrict its codomain as follows. Every $\gamma \in H^r(G_S, M)$ comes from some $\gamma' \in H^r(\mathrm{Gal}(L/K), M)$ for some $K_S/L/K$; almost all v are unramified in L, and for these the image of γ in $H^r(K_v, M)$ lies in

$$\begin{aligned} H^r_{\mathrm{un}}(K_v, M) &\coloneqq \mathrm{im}\left(H^r(g_v, M) \to H^r(G_v, M)\right) \\ &= \ker\left(H^r(G_v, M) \to H^r(I_v, M)\right). \end{aligned}$$

Therefore, if we define $\Pi_S^r(K, M)$ as the restricted product $\prod'_{v \in S} H^r(K_v, M)$ relative to $H^r_{\mathrm{un}}(K_v, M)$, we have maps

$$\beta^r \colon H^r(G_S, M) \to \Pi_S^r(K, M)$$

whose kernels we denote by

$$Ш^r_S(K, M) = \ker \beta^r.$$

By our previous duality results, $H^r(-, M) \cong H^{2-r}(-, M^D)^*$, so the dual maps γ^r to $\beta^{2-r}(K, M^D)$ can be written as

$$\gamma^r \colon \Pi^r_S(K, M^D) \to H^{2-r}(G_S, M)^*$$

We can now state the main theorem of this section.

Theorem 1.7.1 (Poitou-Tate duality)**.** Let M be a finite G_S-module such that $|M| \in \mathcal{O}^\times_{K,S}$. Then:

1. there is a canonical non-degenerate pairing
$$Ш^1_S(K, M) \times Ш^2_S(K, M^D) \to \mathbb{Q}/\mathbb{Z}$$
2. β^0 is injective, γ^2 is surjective and $\operatorname{im} \beta^r = \ker \gamma^r$ for $r = 0, 1, 2$
3. for $r \geqslant 3$, β^r is a bijection $H^r(G_S, M) \to \prod_{v \text{ real}} H^r(K_v, M)$.

These statements can be represented by an exact sequence

$$\begin{aligned} 0 \longrightarrow H^0(G_S, M) &\xrightarrow{\beta^0} \Pi^0_S(K, M) \xrightarrow{\gamma^0} H^2(G_S, M^D)^* \longrightarrow \\ \longrightarrow H^1(G_S, M) &\xrightarrow{\beta^1} \Pi^1_S(K, M) \xrightarrow{\gamma^1} H^1(G_S, M^D)^* \longrightarrow \\ \longrightarrow H^2(G_S, M) &\xrightarrow{\beta^2} \Pi^2_S(K, M) \xrightarrow{\gamma^2} H^0(G_S, M^D)^* \longrightarrow 0 \end{aligned}$$

The proof consists in identifying the above sequence with the $\operatorname{Ext}_{G_S}(M^D, -)$-sequence coming from $0 \to E_S \to J_S \to C_S \to 0$, up to a few adjustments.

Denote by M^d the following object:

$\operatorname{Hom}(M, E_S)$ when viewing M as a G_S-module,

$\operatorname{Hom}(M, \widehat{\mathcal{O}}_v^{\mathrm{un}\times})$ when viewing M as a g_v-module for $v \notin S$,

$\operatorname{Hom}(M, K_v^{\mathrm{s}\times})$ when viewing M as a G_v-module for $v \in S$.

Lemma 1.7.2. In the hypothesis of the theorem, $\operatorname{Ext}^r_{G_S}(M, E_S) = H^r(G_S, M^d)$ for all r.

Proof. By Corollary 1.1.8 we have $\operatorname{Ext}^r_{G_S}(M, E_S) = H^r(G_S, \operatorname{Hom}(M, E_S))$ since E_S is divisible by all integers which are units in $\mathcal{O}_{K,S}$, hence by all primes which are orders of elements of M, as its order is a unit in $\mathcal{O}_{K,S}$. □

Lemma 1.7.3. For $r \geqslant 1$, $\operatorname{Ext}^r_{G_S}(M, J_S) = \Pi^r_S(K, M^d)$. For $r = 0$, it is $\Pi^0_S(K, M^d)$ if K is a function field and $\prod_{v \in S} H^0(G_v, M^d)$ if K is a number field.

Proof. Choose a finite subset $T \subset S$ still containing all the archimedean primes and the primes at which M ramifies, and such that $|M|$ is a unit in $\mathcal{O}_{K,T}$. Define

$$J_{F,S,T} \coloneqq \prod_{w \in T} F_w^\times \times \prod_{w \in S \setminus T} \widehat{\mathcal{O}}_w^\times.$$

Then $J_S = \varinjlim J_{F,S,T}$ (limit over T and $F \subset K_T$), hence

$$\mathrm{Ext}^r_{G_S}(M, J_S) = \varinjlim_{F,T} \mathrm{Ext}^r_{\mathrm{Gal}(F/K)}(M, J_{F,S,T}).$$

Since the Ext functor commutes with products in the second entry, the terms inside the limit can be written as

$$\mathrm{Ext}^r_{\mathrm{Gal}(F/K)}(M, J_{F,S,T}) = \left(\prod_{v\in T} \mathrm{Ext}^r_{\mathrm{Gal}(F_w/K_v)}(M, F_w^\times)\right) \times \left(\prod_{v\in S\setminus T} \mathrm{Ext}^r_{\mathrm{Gal}(F_w/K_v)}(M, \widehat{\mathcal{O}}_{F_w}^\times)\right)$$

We can now write the factors in the second line as

$$\mathrm{Ext}^r_{\mathrm{Gal}(F_w/K_v)}(M, \widehat{\mathcal{O}}_{F_w}^\times) = \mathrm{Ext}^r_{g_v}(M, \widehat{\mathcal{O}}_v^{\mathrm{un}\times}) = H^r(g_v, M^d).$$

The first equality follows by the usual spectral sequence 1.1.8 using the fact that $\widehat{\mathcal{O}}_v^{\mathrm{un}\times}$ has trivial cohomology [Ser67, Proposition 1]. The second is by 1.1.8 as in the previous lemma ($\widehat{\mathcal{O}}_v^{\mathrm{un}\times}$ is divisible by all integers dividing $|M|$). Hence

$$\mathrm{Ext}^r_{G_S}(M, J_S) = \varinjlim_{F,T} \left(\prod_{v\in T} \mathrm{Ext}^r_{\mathrm{Gal}(F_w/K_v)}(M, F_w^\times) \times \prod_{v\in S\setminus T} H^r(g_v, M^D)\right)$$

By 1.1.8, when $r = 0, 1$, the (finitely many) factors for $v \in T$ can be written as

$$\mathrm{Ext}^r_{\mathrm{Gal}(F_w/K_v)}(M, F_w^\times) = \mathrm{Ext}^r_{G_v}(M, K_v^\times) = H^r(G_v, M^d);$$

when $r \geqslant 2$, $\mathrm{Ext}^r_{g_v}(M, \widehat{\mathcal{O}}_v^{\mathrm{un}\times}) = 0$ because by cohomological triviality of $\widehat{\mathcal{O}}^{\mathrm{un}\times}$ one can find an injective resolution by g_v-modules $0 \to \widehat{\mathcal{O}}^{\mathrm{un}\times} \to I^0 \to I^1 \to 0$ [Ser80]. We conclude

$$\mathrm{Ext}^r_{G_S}(M, J_S) = \begin{cases} \prod_{v\in S} H^0(G_v, M^d) & r = 0 \\ \Pi^1_S(K, M) & r = 1 \\ \bigoplus_{v\in S} \varinjlim_F \mathrm{Ext}^r_{\mathrm{Gal}(F_w/K_v)}(M, F_w^\times) & r \geqslant 2 \end{cases}$$

We know that S contains all primes lying over ℓ if ℓ divides $|M|$, therefore

$$\varinjlim_F H^2(\mathrm{Gal}(K_v^s/F_w), K_v^{s\times})(\ell) = 0,$$

hence the spectral sequence 1.1.8

$$\mathrm{Ext}^r_{\mathrm{Gal}(F_w/K_v)}(M, H^s(\mathrm{Gal}(K_v^s/F_w))) \implies \mathrm{Ext}^r_{G_v}(M, K_v^{s\times})$$

shows that

$$\varinjlim_F \mathrm{Ext}^r_{\mathrm{Gal}(F_w/K_v)}(M, F_w^\times) = \mathrm{Ext}^r_{G_v}(M, K_v^{s\times}) = \\ = H^r(G_v, M^d) =: H^r(K_v, M^d)$$

which concludes the proof. □

The last essential step in the identification of the Poitou-Tate sequence with the Ext sequence in our claim is the isomorphism $\mathrm{Ext}^r_{G_S}(M, C_S)(\ell) \cong H^{2-r}(G_S, M)^*(\ell)$. To prove it, we need the following notions.

1.7.1 P-class formations

Let P be a set of rational prime numbers.

Definition 1.7.4. If G is a profinite group and C is a G-module, a P-class formation (G, C) is defined as a class formation, except that instead of requiring the maps inv_U to be isomorphisms, we require that they are injections inducing isomorphisms:

- $\mathrm{inv}_{U/V} H^2(U/V, C^V) \xrightarrow{\sim} [U : V]^{-1}\mathbb{Z}/\mathbb{Z}$ for all $V \trianglelefteq \mathrm{U}$,
- $H^2(U, C)(\ell) \xrightarrow{\sim} (\mathbb{Q}/\mathbb{Z})(\ell)$ for all $\ell \in P$.

Let P be the set of prime numbers ℓ such that ℓ^∞ divides the degree of K_S over K, defined as the profinite order $|\mathrm{Gal}(K_S/K)|$. When P contains all primes, a P-class formation is just a class formation. We can immediately generalize duality for class formations (Theorem 1.2.5) to:

Theorem 1.7.5 (Duality for P-class formations)**.**

- $\alpha^r(G, M)(\ell)\colon \mathrm{Ext}^r_G(M, C)(\ell) \to H^{2-r}(G, M)^*(\ell)$ $(r \geqslant 2)$ is bijective for all finitely generated M,
- $\alpha^1(G, M)(\ell)$ is bijective for all torsion-free M;
  it is bijective for all finitely generated M if $\alpha^1(U, \mathbb{Z}/\ell^m\mathbb{Z})$ is bijective for all open $U \leqslant G$ and all m,
- $\alpha^0(G, M)$ is bijective for all finite ℓ-primary M if $\alpha^0(U, \mathbb{Z}/\ell^m\mathbb{Z})$ is bijective for all open $U \leqslant G$ and all m.

We claim that:

Proposition 1.7.6. (G_S, C_S) is a P-class formation.

Proof. In general, whenever (G, C) is a class formation and $H \trianglelefteq G$ is closed, then $(G/H, C^H)$ is a P-class formation for P the set of primes ℓ such that ℓ^∞ divides $[G : H]$.

Set $C = \varinjlim_F C_F$ indexed over the separable finite extensions of K and let G be the absolute Galois group of K as before; then (G, C) is a class formation. Hence, (G_S, C^{H_S}) is a P-class formation. Now there is a canonical isomorphism $H^r(G_S, C^{H_S}) \to H^r(G_S, C_S)$ for all $r \geqslant 1$ and the same holds for any open subgroup of G_S. Indeed, there is an exact sequence

$$0 \to U_S \to C^{H_S} \to C_S \to 0$$

(when S is finite pass to direct limits over the isomorphisms $C_{F,S} \xrightarrow{\sim} C_F/U_{F,S}$ to obtain an isomorphism $C_S \xrightarrow{\sim} C_S^{H_S}/U_S$; for a general S one should show that the limit of the ideal class groups $\varinjlim \mathrm{Id}(\mathcal{O}_{F,S})$ is zero, and this is done by global class field theory). Now we have $H^r(G_S, U_S) = 0$ for $r \geqslant 1$, because by definition

$$H^r(G_S, U_S) = \varinjlim_F H^r(\mathrm{Gal}(F/K), \prod_{w \notin S_F} \widehat{\mathcal{O}}_w^\times),$$

the terms inside the limit can be written as

$$\prod_{v \notin S_K} \prod_{w|v} H^r(\mathrm{Gal}(F_w/K_v), \widehat{\mathcal{O}}_w^\times)$$

and each of the single factors is zero because v is unramified in F and $\widehat{\mathcal{O}}_w^\times$ is cohomologically trivial, as before [Ser67, Proposition 1].

Now taking the long cohomology sequence from the above exact sequence allows to conclude. □

Lemma 1.7.7. Let M be a finitely generated G_S-module, $\ell \in P$. Then there are isomorphisms

$$\alpha^r(G_S, M)(\ell)\colon \operatorname{Ext}^r_{G_S}(M, C_S)(\ell) \xrightarrow{\sim} H^{2-r}(G_S, M)^*(\ell)$$

for all $r \geqslant 1$.

Proof. Follows from Theorem 1.7.5 since (G_S, C_S) is a P-class formation. Just note that, for all $\ell \in P$ and m, $\alpha^1(G_S, \mathbb{Z}/\ell^m\mathbb{Z})$ is bijective. □

1.7.2 End of the proof

By lemmas 1.7.2, 1.7.3 and 1.7.7, the sequence

$$\to \operatorname{Ext}^r_{G_S}(M^D, E_S) \to \operatorname{Ext}^r_{G_S}(M^D, J_S) \to \operatorname{Ext}^r_{G_S}(M^D, C_S) \to$$

can be rewritten as

$$\begin{array}{ccccccccc}
0 & \to & H^0(G_S, M) & \to & \prod_{v\in S} H^0(K_v, M) & \to & \operatorname{Hom}_{G_S}(M^D, C_S) & \to \\
 & \to & H^1(G_S, M) & \to & \Pi^1_S(K, M) & \to & H^1(G_S, M^D)^* & \to \\
 & \to & H^2(G_S, M) & \to & \Pi^2_S(K, M) & \to & H^0(G_S, M^D)^* & \to \\
 & \to & H^3(G_S, M) & \to & \bigoplus_{v \text{ real}} H^3(G_v, M) & \to & 0 & \to \\
 & \to & H^r(G_S, M) & \xrightarrow{\sim} & \bigoplus_{v \text{ real}} H^r(G_v, M) & \to & 0 &
\end{array}$$

($r \geqslant 4$). This is almost the Poitou-Tate sequence, except that we must change the first three terms to

$$0 \longrightarrow H^0(G_S, M) \xrightarrow{\beta^0} \Pi^0_S(K, M) \xrightarrow{\gamma^0} H^2(G_S, M^D)^* \longrightarrow$$

and check surjectivity of $\Pi^2_S(K, M^D) \to H^0(G_S, M)^*$. Surjectivity holds because this map is dual to $H^0(G_S, M) \to \Pi^0_S(K, M)$, which is injective. So, now we have a sequence

$$\begin{array}{ccccccccc}
0 & \to H^0(G_S, M) & \to & \prod_{v\in S} H^0(K_v, M) & \to & \operatorname{Hom}_{G_S}(M^D, C_S) & \to & \\
 & \to H^1(G_S, M) & \to & \Pi^1_S(K, M) & \to & H^1(G_S, M^D)^* & \to & \\
 & \to H^2(G_S, M) & \to & \Pi^2_S(K, M) & \to & H^0(G_S, M^D)^* & \to & 0
\end{array}$$

and it is enough to substitute the first half (up to $\Pi^1_S(K, M)$) with the dual of the second half, which is exactly the beginning of the Poitou-Tate sequence, concluding the proof.

Chapter 2

Kolyvagin systems

The main results of this chapter are the following: for Selmer groups $S_{p^k}(K,E)$ (resp. $S_{p^\infty}(K,E)$), Theorem 2.3.8 (resp. Theorem 2.3.13) using Stark systems; Theorem 2.4.13 (resp. Theorem 2.4.17) using Kolyvagin systems.

2.1 Preliminaries

2.1.1 Ray class fields

Given a number field K, we construct extensions which generalize the cyclotomic extensions of $\mathbb{Q}$. Recall the idele class group $C_K = J_K/K^\times$, where J_K is the idele group.

Definition 2.1.1. For an ideal $\mathfrak{m} = \prod_\mathfrak{p} \mathfrak{p}^{n_\mathfrak{p}}$, the *ray class group* mod $\mathfrak{m}$ is

$$J_K/J_K^\mathfrak{m} K^\times \quad (\cong C_K/C_K^\mathfrak{m})$$

where, setting $n_\mathfrak{p} = 0$ for $\mathfrak{p} \mid \infty$, we defined $J_K^\mathfrak{m} = \prod_\mathfrak{p} U_\mathfrak{p}^{(n_\mathfrak{p})}$ ($C_K^\mathfrak{m} = J_K^\mathfrak{m} K^\times/K^\times$),

$$U_\mathfrak{p}^{(0)} = U_\mathfrak{p}, \quad U_\mathfrak{p}^{(n_\mathfrak{p})} = \begin{cases} 1+\mathfrak{p}^{n_\mathfrak{p}} & \mathfrak{p} \nmid \infty \\ \mathbb{R}_+^\times \subset K_\mathfrak{p}^\times & \mathfrak{p} \text{ real} \\ \mathbb{C}^\times = K_\mathfrak{p}^\times & \mathfrak{p} \text{ complex} \end{cases} \quad \text{if } n_\mathfrak{p} > 0.$$

Proposition 2.1.2. The closed subgroups of finite index of C_K are exactly the subgroups that contain some $C_K^\mathfrak{m}$.

From global class field theory we have

Theorem 2.1.3 (Existence theorem)**.** The map $L \mapsto N_{L/K} C_L$ is a 1-1 correspondence between the finite abelian extensions of K and the closed subgroups of finite index of C_K. The field corresponding to such a subgroup N is called the *class field* of N.

Proof. By studying the global reciprocity map $C_K/N_{L/K}C_L \xrightarrow{\sim} \mathrm{Gal}(L/K)^{\mathrm{ab}}$. □

Hence, combining this with the proposition we can immediately make the following

Definition 2.1.4. For an ideal $\mathfrak{m}$, the extension $K^\mathfrak{m}/K$ corresponding to the subgroup $C_K^\mathfrak{m}$ is called the *ray class field* mod $\mathfrak{m}$.

This extension is such that $\mathrm{Gal}(K^{\mathfrak{m}}/K) \cong C_K/C_K^{\mathfrak{m}}$ and every finite abelian extension L/K is contained in some $K^{\mathfrak{m}}$. We see now why these extensions $K^{\mathfrak{m}}$ generalize cyclotomic extensions: the Kronecker-Weber theorem states that every finite abelian extension of $\mathbb{Q}$ is contained in some cyclotomic field; moreover, one also has

Proposition 2.1.5. If $K = \mathbb{Q}$ and $\mathfrak{m} = (m)$, then $C_{\mathbb{Q}}/C_{\mathbb{Q}}^{\mathfrak{m}} \cong (\mathbb{Z}/m\mathbb{Z})^{\times}$ ($\cong \mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q})$).

2.1.2 Exterior algebras

We quote a technical result which will be used later. Assume R is a local principal ideal ring (in our examples we will be working with $R = \mathbb{Z}/p^k\mathbb{Z}$ or $\mathbb{Z}_p$).

Proposition 2.1.6. Suppose $0 \to N \to M \xrightarrow{\psi} C$ is an exact sequence of finitely generated R-modules with C free of rank 1. Then, if $r \geqslant 1$, there is a unique map

$$\widehat{\psi}\colon \bigwedge^r M \to C \otimes \bigwedge^{r-1} N$$

such that

1. the composition
$$\bigwedge^r M \xrightarrow{\widehat{\psi}} C \otimes \bigwedge^{r-1} N \to C \otimes \bigwedge^{r-1} M$$
is given by
$$m_1 \wedge \cdots \wedge m_r \mapsto \sum_{i=1}^{r} (-1)^{i+1} \psi(m_i) \otimes (m_1 \wedge \cdots \wedge m_{i-1} \wedge m_{i+1} \wedge \cdots \wedge m_r)$$

2. the image of $\widehat{\psi}$ is the image of
$$\operatorname{im}\psi \otimes \bigwedge^{r-1} N \to C \otimes \bigwedge^{r-1} N.$$

Proof. [MR16, Proposition A.1]. □

2.2 Generalities

Throughout this chapter, we will use the following notation:

$p \in \mathbb{Z}$ is a rational prime.

R will be usually $\mathbb{Z}/p^k\mathbb{Z}$; when otherwise stated, $R = \mathbb{Z}_p$. We always denote the maximal ideal of R by $\mathfrak{m}$, i.e. $\mathbb{Z}/p\mathbb{Z}$ or $p\mathbb{Z}_p$ respectively. (The results, however, hold more generally for R principal artinian local ring or discrete valuation ring, respectively).

T is a free finitely generated R-module with a continuous G_K-action, where K will be a local or number field; we are mainly thinking of $T = E_{p^k}$, the torsion group of an elliptic curve E in the case of finite R, or $T = T_p(E)$, the Tate module, in the case of $R = \mathbb{Z}_p$.

$T^D = \mathrm{Hom}(T, \mu_{p^\infty})$ as an $R[[G_K]]$-module.

len denotes the length of a module.

2.2.1 Local conditions

In addition to the previously fixed notation, K here is a local field; if non-archimedean, we denote

$\mathcal{O}$ its ring of integers;

$\mathbb{F}$ its residue field;

$I = \mathrm{Gal}(\overline{K}/K^{\mathrm{un}})$ its inertia group, hence $G_{\mathbb{F}} = G_K/I$.

We also suppose that T is unramified, i.e. $T^I = T$.

Definition 2.2.1. A *local condition* $\mathcal{F}$ on T over K is an R-submodule $H^1_{\mathcal{F}}(K,T) \subset H^1(K,T)$.

The following cases are important:

- if L/K is a Galois extension, the *L-transverse* local condition is

$$H^1_{L\text{-tr}}(K,T) = \ker(H^1(K,T) \to H^1(L,T)) = H^1(L/K, T^{G_L})$$

  (where the last equality follows from the inflation-restriction sequence). The following are special cases of this:

- $L = \overline{K}$ gives the *unrestricted* or *relaxed* condition $H^1(K,T)$;
- $L = K$ gives the *strict* condition 0;
- $L = K^{\mathrm{un}}$, when K is non-archimedean and T is unramified, gives the *finite* (or *unramified*) condition

$$H^1_{\mathrm{f}}(K,T) = \ker(H^1(K,T) \to H^1(K^{\mathrm{un}},T)) = H^1(K^{\mathrm{un}}/K,T);$$

- if L/K is a totally tamely ramified cyclic extension such that $[L:K]T = 0$, we write $H^1_{\mathrm{tr}}(K,T)$ for $H^1_{L\text{-tr}}(K,T)$.

Lemma 2.2.2.

1. There is a canonical functorial isomorphism $H^1_{\mathrm{f}}(K,T) \cong T/(\mathrm{Fr}-1)T$.
2. There are canonical functorial isomorphisms

$$H^1_{\mathrm{tr}}(K,T) \cong \mathrm{Hom}(I, T^{\mathrm{Fr}=1}) \qquad H^1_{\mathrm{tr}}(K,T) \otimes \mathrm{Gal}(L/K) \cong T^{\mathrm{Fr}=1}$$

3. The composition $H^1_{\mathrm{tr}}(K,T) \hookrightarrow H^1(K,T) \twoheadrightarrow H^1(K,T)/H^1_{\mathrm{f}}(K,T)$ is an isomorphism, hence there is a canonical splitting

$$H^1(K,T) = H^1_{\mathrm{f}}(K,T) \oplus H^1_{\mathrm{tr}}(K,T).$$

Proof. (1) Evaluating cocycles at the Frobenius gives a well-defined injection

$$H^1(K^{\mathrm{un}}/K,T) \to T/(\mathrm{Fr}-1)T, \quad c \mapsto c(\mathrm{Fr})$$

which can be shown to be surjective [Ser80, XIII.1].

(2) We have an exact sequence

$$0 \to H^1(K^{\mathrm{un}}/K, T^I) \to H^1(K,T) \to H^1(I,T)^{G_k} \to H^2(K^{\mathrm{un}}/K, T^I)$$

and the last term is 0, so there is an isomorphism $H^1_{\mathrm{f}}(K,T) \cong \mathrm{Hom}(I,T)^{\mathrm{Fr}=1}$. From $|\mathbb{F}^\times|T = 0$ and $I/|\mathbb{F}^\times|I \cong \mathbb{F}^\times$, we get

$$\mathrm{Hom}(I,T)^{\mathrm{Fr}=1} = \mathrm{Hom}(I/|\mathbb{F}^\times|I, T)^{\mathrm{Fr}=1} = \mathrm{Hom}(\mathbb{F}^\times, T)^{\mathrm{Fr}=1} = \mathrm{Hom}(\mathbb{F}^\times, T^{\mathrm{Fr}=1})$$

and we conclude.

(3) Since L/K is totally ramified and T is unramified, we have

$$T^{G_L} = T^{G_K} = T^{G_k} = T^{\mathrm{Fr}=1}$$

and therefore there is a commutative diagram

$$\begin{array}{ccccc}
H^1_{\mathrm{tr}}(K,T) & \hookrightarrow & H^1(K,T) & \twoheadrightarrow & H^1_{\mathrm{f}}(K,T) \\
\downarrow \sim & & & & \downarrow \sim \\
 & & & & \mathrm{Hom}(I, T^{\mathrm{Fr}=1}) \\
 & & & & \uparrow \sim \\
H^1(L/K, T^{G_L}) & \xrightarrow{\sim} & \mathrm{Hom}(\mathrm{Gal}(L/K), T^{\mathrm{Fr}=1}) & \xrightarrow{\sim} & \mathrm{Hom}(I/|\mathbb{F}^\times|I, T^{\mathrm{Fr}=1})
\end{array}$$

□

By the hypothesis $T^I = T$, $G_{\mathbb{F}}$ acts on T, so the Frobenius action induces an endomorphism

$$\mathrm{Fr}_T \colon T \to T, \quad t \mapsto \mathrm{Fr} \cdot t.$$

Suppose $\det(\mathrm{id} - \mathrm{Fr}_T) = 0$, and define

$$P(x) \coloneqq \det(1 - \mathrm{Fr}_T \circ x) \in R[x]$$

where $\mathrm{Fr}_T \circ x \colon t \mapsto \mathrm{Fr} \cdot xt$ when $x \in R$. Since $P(1) = 0$, we can factor $P(x) = (x-1)Q(x)$ in $R[x]$; moreover, by the Cayley-Hamilton theorem, $P(\mathrm{Fr}_T^{-1})$ is the zero endomorphism of T, that is,

$$P(\mathrm{Fr}^{-1})T = (\mathrm{Fr}^{-1} - 1)Q(\mathrm{Fr}^{-1})T = 0.$$

Therefore $Q(\mathrm{Fr}^{-1})T \subset T^{\mathrm{Fr}=1}$, and the following definition makes sense:

Definition 2.2.3. The *finite-singular comparison map* φ^{fs} on T is the composition

$$H^1_{\mathrm{f}}(K,T) \xrightarrow{\sim} T/(\mathrm{Fr}-1)T \xrightarrow{Q(\mathrm{Fr}^{-1})} T^{\mathrm{Fr}=1} \xrightarrow{\sim} H^1_{\mathrm{tr}}(K,T) \otimes \mathrm{Gal}(L/K).$$

Lemma 2.2.4. If $T/(\mathrm{Fr}-1)T$ is a free R-module of rank 1, then $\det(1-\mathrm{Fr}_T) = 0$ and φ^{fs} is an isomorphism. In particular, $H^1_{\mathrm{f}}(K,T)$ and $H^1_{\mathrm{tr}}(K,T)$ are both free R-modules of rank 1.

Recalling the local pairing

$$\langle -, - \rangle \colon H^1(K,T) \times H^1(K,T^D) \to H^2(K, \mu_{p^\infty}) \cong \mathbb{Q}_p/\mathbb{Z}_p,$$

a local condition $\mathcal{F}$ on T induces a local condition $\mathcal{F}^D$ on T^D by taking

$$\begin{aligned} H^1_{\mathcal{F}^D}(K,T^D) &:= H^1_{\mathcal{F}}(K,T)^\perp \\ &:= \{a \in H^1(K,T^D) \mid \langle a,b\rangle = 0 \ \ \forall b \in H^1_{\mathcal{F}}(K,T)\} \end{aligned}$$

the orthogonal complement. This operation behaves well since the pairing is perfect (hence non-degenerate), e.g. $H^1_{\mathcal{F}}(K,T)^{\perp\perp} = H^1_{\mathcal{F}}(K,T)$. So, the dual structure $\mathcal{F}^D$ also gives a structure on T by taking $H^1_{\mathcal{F}^D}(K,T) = H^1_{\mathcal{F}}(K,T^D)^\perp$, which in this case denotes the left orthogonal. Note that $\mathrm{f}^D = \mathrm{f}$ and $\mathrm{tr}^D = \mathrm{tr}$ as structures on T: this follows from the next proposition.

Proposition 2.2.5.

1. $H^1_{\mathrm{f}}(K,T)^\perp = H^1_{\mathrm{f}}(K,T^D)$
2. $H^1_{\mathrm{tr}}(K,T)^\perp = H^1_{\mathrm{tr}}(K,T^D)$

Proof. (1) see Theorem 1.5.3.

(2) It suffices to show that $\langle \alpha, \alpha'\rangle = 0$ for every $\alpha \in H^1_{\mathrm{tr}}(K,T)$ and $\alpha' \in H^1_{\mathrm{tr}}(K,T^D)$; then maximality will follow from (1) using the decompositions

$$H^1(K,T) = H^1_{\mathrm{f}}(K,T) \oplus H^1_{\mathrm{tr}}(K,T)$$

of Lemma 2.2.2 for T and T^D.

Suppose first $p^k \mid |\mathbb{F}^\times|$, $R = \mathbb{Z}_p$, $T = \mathbb{Z}/p^k\mathbb{Z}$ with trivial G_K-action. Then $\mu_{p^k} \subset K^\times$ and

$$\begin{aligned} H^1_{\mathrm{tr}}(K,T) &= \mathrm{Hom}(\mathrm{Gal}(L/K), \mathbb{Z}/p^k\mathbb{Z}) \cong \mathrm{Hom}(K^\times/N_{L/K}L^\times, \mathbb{Z}/p^k\mathbb{Z}) \\ H^1_{\mathrm{tr}}(K,T^D) &= \mathrm{Hom}(\mathrm{Gal}(L/K), \mu_{p^k}) \cong \ker\left(K^\times/(K^\times)^{p^k} \to L^\times/(L^\times)^{p^k}\right), \end{aligned}$$

recalling results from class field theory and Kummer theory, and the pairing can be identified with the natural pairing

$$\mathrm{Hom}(K^\times, \mathbb{Z}/p^k\mathbb{Z}) \times K^\times \to \mathbb{Z}/p^k\mathbb{Z}.$$

Let α be a representative of some element in $H^1_{\mathrm{tr}}(K,T^D)$ according to the above identification, so $\alpha = \beta^{p^k}$ with $\beta \in L^\times$. Then we can compute

$$N_{L/K}\beta = \alpha^{|\mathbb{F}^\times|/p^k}.$$

$K^\times/N_{L/K}L^\times$ is cyclic of order $|\mathbb{F}^\times|$ and α is divisible by p^k, so it is sent to zero by every element of $\mathrm{Hom}(K^\times/N_{L/K}L^\times, \mathbb{Z}/p^k\mathbb{Z})$. This proves the special case.

In the general case, since T is unramified and L/K is totally ramified we have

$$T^{G_K} = T^{G_K/I_K} = T^{G_k} = T^{G_l} = T^{G_L/I_L} = T^{G_L}$$

and analogously for T^D. Therefore

$$H^1_{\mathrm{tr}}(K,T) = H^1(L/K, T^{G_L}) = H^1(L/K, T^{G_K}) = H^1_{\mathrm{tr}}(K, T^{G_K})$$

and analogously for T^D. Writing now $T^{G_K} \cong \bigoplus_n \mathbb{Z}/p^{k_n}\mathbb{Z}$, the thesis follows from previous case. □

2.2.2 Selmer structures

Here K is a number field with algebraic closure $\overline{K} \subset \mathbb{C}$; for a prime $\mathfrak{q}$ of K, $\overline{K_\mathfrak{q}}$ is a fixed algebraic closure containing $\overline{K}$, i.e. we fix an extension of $\mathfrak{q}$ to $\overline{K}$. Moreover:

$D_\mathfrak{q} \coloneqq \mathrm{Gal}(\overline{K_\mathfrak{q}}/K_\mathfrak{q}) \subset G_K$ is a fixed decomposition group;

$\mathcal{I}_\mathfrak{q} \subset D_\mathfrak{q}$ is the inertia group;

$\mathrm{Fr}_\mathfrak{q} \in D_\mathfrak{q}/\mathcal{I}_\mathfrak{q}$ is the Frobenius element;

$K(\mathfrak{q})$ is maximal p-power extension of the ray class field of K modulo $\mathfrak{q}$ and $K(\mathfrak{q})_\mathfrak{q}$ is its completion at the fixed prime above $\mathfrak{q}$.

If $\mathfrak{q}$ is principal, then $K(\mathfrak{q})_\mathfrak{q}$ is cyclic and totally tamely ramified. In this case, if T is unramified at $\mathfrak{q}$ and $[K(\mathfrak{q})_\mathfrak{q} : K_\mathfrak{q}]T = 0$, then we define as before the transverse submodule

$$H^1_{\mathrm{tr}}(K_\mathfrak{q}, T) = \ker\left(H^1(K_\mathfrak{q}, T) \to H^1(K(\mathfrak{q})_\mathfrak{q}, T)\right).$$

Definition 2.2.6. A *Selmer structure* $\mathcal{F}$ on T is the following data:

- $\Sigma(\mathcal{F})$, a finite set of places of K including all infinite places, all primes above p and all primes where T is ramified;
- for every $\mathfrak{q} \in \Sigma(\mathcal{F})$, a local condition $H^1_\mathcal{F}(K_\mathfrak{q}, T) \subset H^1(K_\mathfrak{q}, T)$.

Definition 2.2.7. If $\mathcal{F}$ is a Selmer structure, we define the *Selmer module* $H^1_\mathcal{F}(K, T)$ as the kernel of the sum of restriction maps:

$$H^1_\mathcal{F}(K, T) \coloneqq \ker\left(H^1(K_{\Sigma(\mathcal{F})}/K, T) \to \bigoplus_{\mathfrak{q}\in\Sigma(\mathcal{F})} \frac{H^1(K_\mathfrak{q}, T)}{H^1_\mathcal{F}(K_\mathfrak{q}, T)}\right) \subset H^1(K, T)$$

where $K_{\Sigma(\mathcal{F})}$ denotes the maximal extension of K unramified outside $\Sigma(\mathcal{F})$. That is, the Selmer module consists of the classes which are unramified outside $\Sigma(\mathcal{F})$ and satisfy the local condition given by $\mathcal{F}$ for every $\mathfrak{q} \in \Sigma(\mathcal{F})$.

Using the local Tate pairings $\langle -, - \rangle_\mathfrak{q}$, a Selmer structure $\mathcal{F}$ on T induces a dual structure $\mathcal{F}^D$ by taking dual local conditions

$$H^1_{\mathcal{F}^D}(K_\mathfrak{q}, T^D) \coloneqq H^1_\mathcal{F}(K_\mathfrak{q}, T)^\perp$$

as in the previous section.

These constructions generalize the Selmer groups we have seen in Section 1.6. Let E/K be an elliptic curve, $R = \mathbb{Z}/p^k\mathbb{Z}$, $T = E_{p^k}$ and $\mathcal{F}$ given as follows:

- $\Sigma(\mathcal{F}) \coloneqq \{v : E \text{ has bad reduction at } v\} \cup \{v : v \mid p\} \cup \{v : v \mid \infty\}$
- $H^1_\mathcal{F}(K_v, T) \coloneqq \mathrm{im}\left(\kappa_v \colon E(K_v)/p^k E(K_v) \hookrightarrow H^1(K_v, E_{p^k})\right)$.

Then $H^1_\mathcal{F}(K, T)$ is the usual Selmer group from Definition 1.6.1. As we already know, the Weil pairing identifies $E^D_{p^k} = E_{p^k}$, and we can also show $\mathcal{F}^D = \mathcal{F}$.

As another example, let $R = \mathbb{Z}_p$, $T = T_p(E) \coloneqq \varprojlim_k E_{p^k}$ the p-adic Tate module, $\mathcal{F}$ defined analogously. In this case $T^D = E^t_{p^\infty} = E_{p^\infty}$ and $H^1_\mathcal{F}(K, T^D) = S_{p^\infty}(K, E)$ is the Selmer group defined in Remark 1.6.4.

Definition 2.2.8. $\mathcal{F}$ is called *cartesian* (on the category of quotients of T) if the local condition is cartesian for every $\mathfrak{q} \in \Sigma(\mathcal{F})$, i.e. for any injection $\alpha\colon T/IT \hookrightarrow T/JT$ between quotients of T, $H^1_{\mathcal{F}}(K_\mathfrak{q}, T/IT)$ is the inverse image of $H^1_{\mathcal{F}}(K_\mathfrak{q}, T/JT)$ under the map induced by α on cohomology.

Equivalently, for all $\mathfrak{q} \in \Sigma(\mathcal{F})$, there is a cartesian square

$$\begin{array}{ccc} & H^1(K_\mathfrak{q}, T/IT) & \\ \nearrow & & \searrow^{\alpha} \\ H^1_{\mathcal{F}}(K_\mathfrak{q}, T/IT) & & H^1(K_\mathfrak{q}, T/JT) \\ \searrow^{\alpha} & & \nearrow \\ & H^1_{\mathcal{F}}(K_\mathfrak{q}, T/JT) & \end{array}$$

Definition 2.2.9. By *Selmer data* we mean a triple $(T, \mathcal{F}, \mathcal{P})$ where T is as before and unramified outside finitely many primes, $\mathcal{F}$ is a Selmer structure on T and $\mathcal{P}$ is a set of primes of K disjoint from $\Sigma(\mathcal{F})$.

Definition 2.2.10. If $\mathfrak{q} \nmid p\infty$ is principal, let $I_\mathfrak{q}$ be the maximal power of $\mathfrak{m}$ which contains $[K(\mathfrak{q})_\mathfrak{q} : K_\mathfrak{q}]R$ and such that

$$\frac{T}{(\mathrm{Fr}_\mathfrak{q} - 1)T + I_\mathfrak{q} T}$$

is free of rank 1 over $R/I_\mathfrak{q}$, if one such power exists; if it does not exist or if $\mathfrak{q}$ is not principal, set $I_\mathfrak{q} = R$.

Let us make a remark on the above definition; in case $I_\mathfrak{q} = 0$, it follows that $T/(\mathrm{Fr}_\mathfrak{q} - 1)T$ is a free R-module of rank 1, which is the assumption required to apply Lemma 2.2.4 and conclude that $H^1_{\mathrm{f}}(K_\mathfrak{q}, T)$ and $H^1_{\mathrm{tr}}(K_\mathfrak{q}, T)$ are also free R-modules of rank 1. Therefore, in the most interesting cases we will often make assumptions of the kind $I_\mathfrak{q} = 0$ for all $\mathfrak{q} \in \mathcal{P}$.

Set moreover

$\mathcal{P}_k \coloneqq \{\mathfrak{q} \in \mathcal{P} \mid I_\mathfrak{q} \subset \mathfrak{m}^k\}$ for $k \geqslant 1$;

$\mathcal{N} \coloneqq \mathcal{N}(\mathcal{P}) \coloneqq \{$squarefree products of primes in $\mathcal{P}\} \cup \{1\}$ where 1 denotes the ideal $(1) = \mathcal{O}$;

$I_\mathfrak{n} \coloneqq \sum_{\mathfrak{q}|\mathfrak{n}} I_\mathfrak{q}$ for $1 \neq \mathfrak{n} \in \mathcal{N}$, $I_1 \coloneqq 0$.

We have the inclusions

$$\mathcal{P}_{k+1} \subset \mathcal{P}_k \subset \mathcal{P} \subset \mathcal{N}.$$

If $\mathcal{F}$ is a Selmer structure and $\mathfrak{a}$, $\mathfrak{b}$ and $\mathfrak{n}$ are pairwise coprime ideals of K with $\mathfrak{n} \in \mathcal{N}$ and $I_\mathfrak{n} T = 0$, we define a new Selmer structure $\mathcal{F}^\mathfrak{b}_\mathfrak{a}(\mathfrak{n})$ by:

- $\Sigma(\mathcal{F}^\mathfrak{b}_\mathfrak{a}(\mathfrak{n})) \coloneqq \Sigma(\mathcal{F}) \cup \{\mathfrak{q} : \mathfrak{q} \mid \mathfrak{a}\mathfrak{b}\mathfrak{n}\}$,
- $H^1_{\mathcal{F}^\mathfrak{b}_\mathfrak{a}(\mathfrak{n})}(K_\mathfrak{q}, T) \coloneqq \begin{cases} H^1_{\mathcal{F}}(K_\mathfrak{q}, T) & \mathfrak{q} \in \Sigma(\mathcal{F}) \\ 0 & \mathfrak{q} \mid \mathfrak{a} \\ H^1(K_\mathfrak{q}, T) & \mathfrak{q} \mid \mathfrak{b} \\ H^1_{\mathrm{tr}}(K_\mathfrak{q}, T) & \mathfrak{q} \mid \mathfrak{n}. \end{cases}$

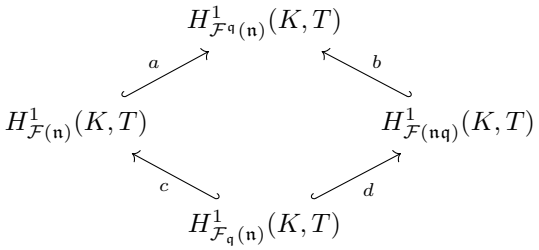
If any of $\mathfrak{a}$, $\mathfrak{b}$ or $\mathfrak{n}$ are equal to 1, we omit them from the notation.

We have $\mathcal{F}^{\mathfrak{b}}_{\mathfrak{a}}(\mathfrak{n})^D = (\mathcal{F}^D)^{\mathfrak{a}}_{\mathfrak{b}}(\mathfrak{n})$, since

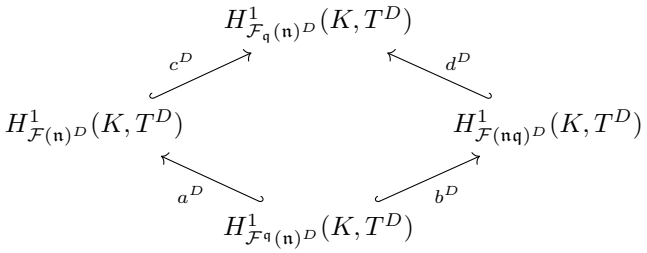
$$\begin{aligned} H^1_{\mathcal{F}^{\mathfrak{b}}_{\mathfrak{a}}(\mathfrak{n})^D}(K_{\mathfrak{q}}, T) &= H^1_{\mathcal{F}^{\mathfrak{b}}_{\mathfrak{a}}(\mathfrak{n})}(K_{\mathfrak{q}}, T^D)^\perp \\ &= \begin{cases} H^1_{\mathcal{F}}(K_{\mathfrak{q}}, T^D)^\perp = H^1_{\mathcal{F}^D}(K_{\mathfrak{q}}, T) & \mathfrak{q} \in \Sigma(\mathcal{F}) \\ 0^\perp = H^1(K_{\mathfrak{q}}, T) & \mathfrak{q} \mid \mathfrak{a} \\ H^1(K_{\mathfrak{q}}, T^D)^\perp = 0 & \mathfrak{q} \mid \mathfrak{b} \\ H^1_{\mathrm{tr}}(K_{\mathfrak{q}}, T^D)^\perp = H^1_{\mathrm{tr}^D}(K_{\mathfrak{q}}, T) = H^1_{\mathrm{tr}}(K_{\mathfrak{q}}, T) & \mathfrak{q} \mid \mathfrak{n} \end{cases} \\ &= H^1_{(\mathcal{F}^D)^{\mathfrak{a}}_{\mathfrak{b}}(\mathfrak{n})}(K_{\mathfrak{q}}, T). \end{aligned}$$

where in the last line we used properties of the transverse conditions under dualization (Proposition 2.2.5).

These structures satisfy the following diagram, where $\mathfrak{q}$ is prime and $\mathfrak{nq} \in \mathcal{N}$:



and the same diagram for T^D becomes



Lemma 2.2.11. Let $R = \mathbb{Z}/p^k\mathbb{Z}$, $\mathfrak{q}$ prime, $\mathfrak{nq} \in \mathcal{N}$ with $I_{\mathfrak{nq}} = 0$ and let the letters on the arrows above denote the lengths of the corresponding cokernels. Then the following equalities hold:

1. $0 \leqslant a, b, c, d, a^D, b^D, c^D, d^D \leqslant k$
2. $a + c = b + d$, $a^D + c^D = b^D + d^D$
3. $k = a + a^D = b + b^D = c + c^D = d + d^D$
4. $a \geqslant d$, $b \geqslant c$, $c^D \geqslant b^D$, $d^D \geqslant a^D$.

Proof. (1) We have by definition

$$H^1_{\mathcal{F}(\mathfrak{n})}(K,T) = \ker\left(H^1_{\mathcal{F}^{\mathfrak{q}}(\mathfrak{n})}(K,T) \to H^1_{\mathrm{tr}}(K_{\mathfrak{q}}, T)\right)$$
$$H^1_{\mathcal{F}_{\mathfrak{q}}(\mathfrak{n})}(K,T) = \ker\left(H^1_{\mathcal{F}(\mathfrak{n})}(K,T) \to H^1_{\mathrm{f}}(K_{\mathfrak{q}}, T)\right)$$

so we can write the cokernels in question as quotients modulo the kernels above; using the canonical isomorphism they are submodules of free R-modules of rank 1 (by Lemma 2.2.4) and (1) follows.

(2) is immediate from the diagrams.

(3) Consider the exact sequences

$$\begin{aligned} 0 \longrightarrow H^1_{\mathcal{G}_1}(K,T) \longrightarrow H^1_{\mathcal{G}_2}(K,T) \xrightarrow{\mathrm{loc}} \bigoplus_{\mathfrak{q}} \frac{H^1_{\mathcal{G}_2}(K_\mathfrak{q},T)}{H^1_{\mathcal{G}_1}(K_\mathfrak{q},T)} \\ 0 \longrightarrow H^1_{\mathcal{G}_2^D}(K,T^D) \longrightarrow H^1_{\mathcal{G}_1^D}(K,T^D) \xrightarrow{\mathrm{loc}^D} \bigoplus_{\mathfrak{q}} \frac{H^1_{\mathcal{G}_1^D}(K_\mathfrak{q},T^D)}{H^1_{\mathcal{G}_2^D}(K_\mathfrak{q},T^D)} \end{aligned} \tag{2.1}$$

with $\mathcal{G}_2 = \mathcal{F}^\mathfrak{q}(\mathfrak{n})$, $\mathcal{G}_1 = \mathcal{F}(\mathfrak{n})$. By the Poitou-Tate sequence Theorem 1.7.1, $\operatorname{im}\mathrm{loc}$ and $\operatorname{im}(\mathrm{loc}^D)$ are orthogonal complements with respect to the pairing $\sum_\mathfrak{q}\langle -,-\rangle_\mathfrak{q}$, and (3) follows.

(4) By definition $H^1_{\mathcal{F}(\mathfrak{n})}(K,T) \cap H^1_{\mathcal{F}(\mathfrak{nq})}(K,T) = H^1_{\mathcal{F}_\mathfrak{q}(\mathfrak{n})}(K,T)$, whence the first two inequalities of (4); for the other two, replace $(T,\mathcal{F})$ with $(T^D,\mathcal{F}^D)$. □

Lemma 2.2.12. With hypothesis as in the above lemma, denote $\overline{T} \coloneqq T/\mathfrak{m}T$,

$$\lambda(\mathfrak{n},T) \coloneqq \operatorname{len} H^1_{\mathcal{F}(\mathfrak{n})}(K,T) \qquad \lambda(\mathfrak{n},T^D) \coloneqq \operatorname{len} H^1_{\mathcal{F}(\mathfrak{n})^D}(K,T^D)$$

Then:

1. there are inequalities

$$|\lambda(\mathfrak{nq},T) - \lambda(\mathfrak{n},T)| \leqslant k \qquad |\lambda(\mathfrak{nq},T^D) - \lambda(\mathfrak{n},T^D)| \leqslant k$$

2. if the localization $H^1_{\mathcal{F}(\mathfrak{n})}(K,T) \to H^1_{\mathrm{f}}(K_\mathfrak{q},T)$ is surjective, then

$$H^1_{\mathcal{F}(\mathfrak{nq})^D}(K,T^D) = H^1_{\mathcal{F}^\mathfrak{q}(\mathfrak{n})^D}(K,T^D) \subset H^1_{\mathcal{F}(\mathfrak{n})^D}(K,T^D)$$

3. the image of

$$\mathfrak{m}^{\lambda(\mathfrak{n},T^D)} H^1_{\mathcal{F}(\mathfrak{n})}(K,T) \xrightarrow{\mathrm{loc}_\mathfrak{q}} H^1_{\mathrm{f}}(K_\mathfrak{q},T) \xrightarrow{\varphi^{\mathrm{fs}}_\mathfrak{q}} H^1_{\mathrm{tr}}(K_\mathfrak{q},T) \otimes G_\mathfrak{q}$$

is equal to the image of

$$\mathfrak{m}^{\lambda(\mathfrak{n},T^D)} H^1_{\mathcal{F}(\mathfrak{nq})}(K,T) \xrightarrow{\mathrm{loc}_\mathfrak{q}} H^1_{\mathrm{tr}}(K_\mathfrak{q},T) \otimes G_\mathfrak{q}$$

4. If both localization maps

$$H^1_{\mathcal{F}(\mathfrak{n})}(K,T)[\mathfrak{m}] \to H^1_{\mathrm{f}}(K_\mathfrak{q},T) \qquad H^1_{\mathcal{F}(\mathfrak{n})^D}(K,T^D)[\mathfrak{m}] \to H^1_{\mathrm{f}}(K_\mathfrak{q},T^D)$$

are non-zero, then

$$\lambda(\mathfrak{nq},\overline{T}) = \lambda(\mathfrak{n},\overline{T}) - 1 \qquad \lambda(\mathfrak{nq},\overline{T}^D) = \lambda(\mathfrak{n},\overline{T}^D) - 1$$

Proof. (1) follows from the diagrams studied in the above lemma.

(2) If the localization map is surjective, then $c = k$ (because the image of the map, a free rank-1 R-module, is isomorphic to the cokernel whose length is c) and so $b^D = 0$ by (3) and (4) above.

(3) Denote the images by $C_{\mathfrak{n}}$, $C_{\mathfrak{nq}}$ respectively. It is enough to show they have the same length. The previous diagrams show

$$\operatorname{len} C_{\mathfrak{n}} = \max\{0, c - \lambda(\mathfrak{n}, T^D)\} \qquad \operatorname{len} C_{\mathfrak{nq}} = \max\{0, d - \lambda(\mathfrak{nq}, T^D)\}$$

$$\lambda(\mathfrak{n}, T^D) - \lambda(\mathfrak{nq}, T^D) = d^D - c^D = c - d$$

and we conclude $\operatorname{len} C_{\mathfrak{n}} - \operatorname{len} C_{\mathfrak{nq}} = 0$.

(4) If the localization maps in the statement are non-zero, then the localization maps

$$H^1_{\mathcal{F}(\mathfrak{n})}(K, \overline{T}) \to H^1_{\mathrm{f}}(K_{\mathfrak{q}}, \overline{T}) \qquad H^1_{\mathcal{F}(\mathfrak{n})^D}(K, \overline{T}^D) \to H^1_{\mathrm{f}}(K_{\mathfrak{q}}, \overline{T}^D)$$

are surjective (see the next proposition). By (2) we have $\lambda(\mathfrak{nq}, \overline{T}^D) = \lambda(\mathfrak{n}, \overline{T}^D) - 1$ and we conclude $\lambda(\mathfrak{nq}, \overline{T}) = \lambda(\mathfrak{n}, \overline{T}) - 1$ as required (since the differences $\lambda(\mathfrak{n}, T) - \lambda(\mathfrak{n}, T^D)$ are independent of $\mathfrak{n} \in \mathcal{N}$: see (3) of the next proof). □

Proposition 2.2.13. Let $R = \mathbb{Z}/p^k\mathbb{Z}$. Let $\mathcal{F}$ be a cartesian Selmer structure on T and suppose $T^{G_K} = (T^D)^{G_K} = 0$. If $\mathfrak{n} \in \mathcal{N}$ satisfies $I_{\mathfrak{n}} = 0$, then:

1. the exact sequence $0 \to T/\mathfrak{m}^i T \to T \to T/\mathfrak{m}^{k-i}T \to 0$ induces an isomorphism

$$H^1_{\mathcal{F}(\mathfrak{n})}(K, T/\mathfrak{m}^i T) \xrightarrow{\sim} H^1_{\mathcal{F}(\mathfrak{n})}(K, T)[\mathfrak{m}^i]$$

   and an exact sequence

$$0 \to H^1_{\mathcal{F}(\mathfrak{n})}(K, T)[\mathfrak{m}^i] \to H^1_{\mathcal{F}(\mathfrak{n})}(K, T) \to H^1_{\mathcal{F}(\mathfrak{n})}(K, T/\mathfrak{m}^{k-i}T) \to 0$$

2. the inclusion $T^D[\mathfrak{m}^i] \hookrightarrow T^D$ induces an isomorphism

$$H^1_{\mathcal{F}(\mathfrak{n})^D}(K, T^D[\mathfrak{m}^i]) \xrightarrow{\sim} H^1_{\mathcal{F}(\mathfrak{n})^D}(K, T^D)[\mathfrak{m}^i]$$

3. there is a unique $r \in \mathbb{Z}$, independent of $\mathfrak{n}$, such that there are non-canonical isomorphisms

$$H^1_{\mathcal{F}(\mathfrak{n})}(K, T) \cong H^1_{\mathcal{F}(\mathfrak{n})^D}(K, T^D) \oplus R^r \qquad \text{if } r \geqslant 0$$
$$H^1_{\mathcal{F}(\mathfrak{n})}(K, T) \oplus R^{-r} \cong H^1_{\mathcal{F}(\mathfrak{n})^D}(K, T^D) \qquad \text{if } r \leqslant 0$$

Proof. (1) Cohomology of the exact sequences

$$0 \longrightarrow T/\mathfrak{m}^i T \xrightarrow{\iota_{k-i}} T \longrightarrow T/\mathfrak{m}^{k-i}T \longrightarrow 0$$

$$0 \longrightarrow T/\mathfrak{m}^{k-i}T \longrightarrow T$$

shows that $\iota_{k-i} \colon H^1(K, T/\mathfrak{m}^i T) \xrightarrow{\sim} H^1(K, T)[\mathfrak{m}^i]$ is an isomorphism, and one can easily see that it induces a map $\iota_{k-i} \colon H^1_{\mathcal{F}}(K, T/\mathfrak{m}^i T) \xrightarrow{\sim} H^1_{\mathcal{F}}(K, T)[\mathfrak{m}^i]$. To show that this map is an isomorphism amounts to showing that $\iota_{k-i}^{-1}(H^1_{\mathcal{F}}(K, T))$ satisfies the local conditions to lie in

$H^1_{\mathcal{F}}(K, T/\mathfrak{m}^i T)$. For $v \in \Sigma(\mathcal{F})$ this holds by the hypothesis of the structure being cartesian; for $v \notin \Sigma(\mathcal{F})$, let us show $\iota_{k-i}^{-1}(H^1_{\mathcal{F}}(K_v, T)) \subset H^1_{\mathcal{F}}(K_v, T/\mathfrak{m}^i T)$. Writing I_v for the inertia group of G_v, we have a diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^1_{\mathrm{f}}(K_v, T/\mathfrak{m}^i T) & \longrightarrow & H^1(K_v, T/\mathfrak{m}^i T) & \longrightarrow & \mathrm{Hom}(I_v, T/\mathfrak{m}^i T) \\ & & \downarrow{\scriptstyle \iota_{k-i}} & & \downarrow{\scriptstyle \iota_{k-i}} & & \downarrow{\scriptstyle \iota_{k-i}} \\ 0 & \longrightarrow & H^1_{\mathrm{f}}(K_v, T) & \longrightarrow & H^1(K_v, T) & \longrightarrow & \mathrm{Hom}(I_v, T) \end{array}$$

with exact rows; the right vertical map is injective, so, if $c \in H^1(K_v, T/\mathfrak{m}^i T)$ and $\iota_{k-i}(c)$ is unramified, then c is also unramified.

(2) Let β be the generator of $\mathfrak{m}^i$; cohomology of the exact sequences

$$0 \longrightarrow T^D[\mathfrak{m}^i] \longrightarrow T^D \xrightarrow{\beta} \mathfrak{m}^i T^D \longrightarrow 0$$

$$0 \longrightarrow \mathfrak{m}^i T^D \longrightarrow T^D \longrightarrow T^D/\mathfrak{m}^i T^D \longrightarrow 0$$

yields, writing $G = \mathrm{Gal}(K_{\Sigma(\mathcal{F})}/K)$,

$$0 \longrightarrow H^1(G, T^D[\mathfrak{m}^i]) \longrightarrow H^1(G, T^D) \xrightarrow{\beta} H^1(G, \mathfrak{m}^i T^D)$$

$$0 \longrightarrow H^1(G, \mathfrak{m}^i T^D) \longrightarrow H^1(G, T^D)$$

whence $H^1(K_{\Sigma(\mathcal{F})}/K, T^D[\mathfrak{m}^i]) \xrightarrow{\sim} H^1(K_{\Sigma(\mathcal{F})}/K, T^D)[\mathfrak{m}^i]$. The Selmer structure $\mathcal{F}^D$ on $T^D[\mathfrak{m}^i]$ is induced by the same Selmer structure on T^D; consider then

$$\begin{array}{ccccccc} 0 & \to & H^1_{\mathcal{F}^D}(K, T^D[\mathfrak{m}^i]) & \to & H^1(K_{\Sigma(\mathcal{F})}/K, T^D[\mathfrak{m}^i]) & \to & \displaystyle\bigoplus_{v \in \Sigma(\mathcal{F})} \frac{H^1(K_v, T^D[\mathfrak{m}^i])}{H^1_{\mathcal{F}^D}(K_v, T^D[\mathfrak{m}^i])} \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \to & H^1_{\mathcal{F}^D}(K, T^D)[\mathfrak{m}^i] & \to & H^1(K_{\Sigma(\mathcal{F})}/K, T^D)[\mathfrak{m}^i] & \longrightarrow & \displaystyle\bigoplus_{v \in \Sigma(\mathcal{F})} \frac{H^1(K_v, T^D)}{H^1_{\mathcal{F}^D}(K_v, T^D)}. \end{array}$$

The rows are exact by definition, the middle vertical map is an isomorphism by the above, the right vertical map is injective by definition of induced Selmer structure; therefore, the left vertical map is an isomorphism as was to be shown.

(3) Since R is principal, we can write every finitely generated R-module B as a direct sum $B = \bigoplus_i R/\mathfrak{m}^{k_i}$, hence its isomorphism class is determined by the function $i \mapsto \mathrm{len}(B[\mathfrak{m}^i])$. We have to show that there is an integer t such that

$$\mathrm{len}\left(H^1_{\mathcal{F}(\mathfrak{n})}(K, T)[\mathfrak{m}^i]\right) - \mathrm{len}\left(H^1_{\mathcal{F}(\mathfrak{n})^D}(K, T^D)[\mathfrak{m}^i]\right) = ti.$$

Using points (1) and (2) we rewrite the left term as

$$\mathrm{len}\left(H^1_{\mathcal{F}(\mathfrak{n})}(K, T/\mathfrak{m}^i T)\right) - \mathrm{len}\left(H^1_{\mathcal{F}(\mathfrak{n})^D}(K, T^D[\mathfrak{m}^i])\right).$$

Let us first observe that this quantity does not depend on the choice of $\mathfrak{n}$ satisfying $I_{\mathfrak{n}} = 0$, so we may take $\mathfrak{n} = 1$, i.e. replace $\mathcal{F}(\mathfrak{n})$ with $\mathcal{F}$. Indeed, by Poitou-Tate duality one proves

the following equality, holding for finite T [MR04, Proposition 2.3.5]:

$$\begin{aligned}\operatorname{len} H^1_{\mathcal{F}}(K,T) - \operatorname{len} H^1_{\mathcal{F}^D}(K,T^D) = \\ = \operatorname{len} H^0(K,T) - \operatorname{len} H^0(K,T^D) - \\ \sum_{v\in\Sigma(\mathcal{F})} \left(\operatorname{len} H^0(K_v,T) - H^1_{\mathcal{F}}(K_v,T)\right);\end{aligned}$$

then, if $I_{\mathfrak{n}} = 0$, we apply Lemma 2.2.4 to get $\operatorname{len} H^1_{\mathrm{f}}(K_v,T) = \operatorname{len} H^1_{\mathrm{tr}}(K_v,T)$ for $v \mid \mathfrak{n}$, so the left side of the equality is unchanged when we replace $\mathcal{F}$ by $\mathcal{F}(\mathfrak{n})$, which was the claim. Now, applying this equality to $T/\mathfrak{m}^iT$, we get a formula for the difference we want to compute. At the right side of the equality, the first two terms will be zero (because $S^{G_K} = 0$ for every subquotient S of T), and the non-zero terms will be linear in i: indeed, if we denote by $l(i) = \operatorname{len}\left(H^0(K,T/\mathfrak{m}^iT)\right) - \operatorname{len}\left(H^1_{\mathcal{F}}(K,T/\mathfrak{m}^iT)\right)$, using the cartesian condition and propagation of $\mathcal{F}$ to quotients, cohomology induces an exact sequence

$$\begin{aligned}0 \to H^0(K,T/\mathfrak{m}^iT) \to H^0(K,T/\mathfrak{m}^{i+j}T) \to H^0(K,T/\mathfrak{m}^jT) \to \\ \to H^1_{\mathcal{F}}(K,T/\mathfrak{m}^iT) \to H^1_{\mathcal{F}}(K,T/\mathfrak{m}^{i+j}T) \to H^1_{\mathcal{F}}(K,T/\mathfrak{m}^jT)\end{aligned}$$

whence $l(i+j) = l(i) + l(j)$. This allows us to conclude. □

Definition 2.2.14. For a Selmer structure $(T,\mathcal{F})$ with $R = \mathbb{Z}/p^k\mathbb{Z}$, the number r from the above proposition is called the *core rank* of $(T,\mathcal{F})$, denoted by $\chi(T)$. If $(T,\mathcal{F})$ is a Selmer structure with $R = \mathbb{Z}_p$, we define $\chi(T) \coloneqq \chi(T/\mathfrak{m}T)$.

From now on, $r \coloneqq \chi(T)$. For $\mathfrak{n} \in \mathcal{N}$, we denote:

$\lambda(\mathfrak{n}) \coloneqq \operatorname{len} H^1_{\mathcal{F}(\mathfrak{n})^D}(K,T^D)$;

$\mu(\mathfrak{n}) \coloneqq \operatorname{len} H^1_{(\mathcal{F}^{\mathfrak{n}})^D}(K,T^D)$;

$\nu(\mathfrak{n})$ the number of primes dividing $\mathfrak{n}$.

Corollary 2.2.15. Let $R = \mathbb{Z}/p^k\mathbb{Z}$, $r = \chi(T) \geqslant 0$, $\mathfrak{n} \in \mathcal{N}$, $I_{\mathfrak{n}} = 0$. There are non-canonical isomorphisms

1. $H^1_{\mathcal{F}(\mathfrak{n})}(K,T) \cong H^1_{\mathcal{F}(\mathfrak{n})^D}(K,T^D) \oplus R^r$;
2. $H^1_{\mathcal{F}^{\mathfrak{n}}}(K,T) \cong H^1_{(\mathcal{F}^{\mathfrak{n}})^D}(K,T^D) \oplus R^{r+\nu(\mathfrak{n})}$;
3. $\mathfrak{m}^{\lambda(\mathfrak{n})} \bigwedge^r H^1_{\mathcal{F}(\mathfrak{n})}(K,T) \cong \mathfrak{m}^{\lambda(\mathfrak{n})}$;
4. $\mathfrak{m}^{\mu(\mathfrak{n})} \bigwedge^{r+\nu(\mathfrak{n})} H^1_{\mathcal{F}^{\mathfrak{n}}}(K,T) \cong \mathfrak{m}^{\mu(\mathfrak{n})}$.

Proof. (1) is Proposition 2.2.13.3.

(2) Applying Proposition 2.2.13.3. to $(T,\mathcal{F}^{\mathfrak{n}})$, we get

$$H^1_{\mathcal{F}^{\mathfrak{n}}}(K,T) \cong H^1_{(\mathcal{F}^{\mathfrak{n}})^D}(K,T^D) \oplus R^{\chi(T,\mathcal{F}^{\mathfrak{n}})}$$

and we conclude by observing $\chi(T,\mathcal{F}^{\mathfrak{n}}) = \chi(T) + \nu(\mathfrak{n})$, which is a consequence of Poitou-Tate global duality (apply the sequences 2.1 above to $\mathcal{F}^{\mathfrak{n}}$ and $\mathcal{F}$).

(3) follows directly from (1).

(4) follows directly from (2). □

2.3 Stark systems

The aim of this section is to describe the structure of the *dual Selmer group* $H^1_{\mathcal{F}^D}(K,T^D)$ in terms of so-called Stark systems.

Let $R=\mathbb{Z}/p^k\mathbb{Z}$ and let $(T,\mathcal{F},\mathcal{P})$ satisfy $I_\mathfrak{q}=0$ for every $\mathfrak{q}\in\mathcal{P}$.

Recalling definition 2.2.10 of $I_\mathfrak{q}$, the condition $I_\mathfrak{q}=0$ ensures that $T/(\mathrm{Fr}_\mathfrak{q}-1)T$ is a free R-module of rank 1 and therefore, by Lemma 2.2.4, $H^1_{\mathrm{f}}(K_\mathfrak{q},T)$ and $H^1_{\mathrm{tr}}(K_\mathfrak{q},T)$ are also free R-modules of rank 1.

Definition 2.3.1. For $\mathfrak{n}\in\mathcal{N}$, define

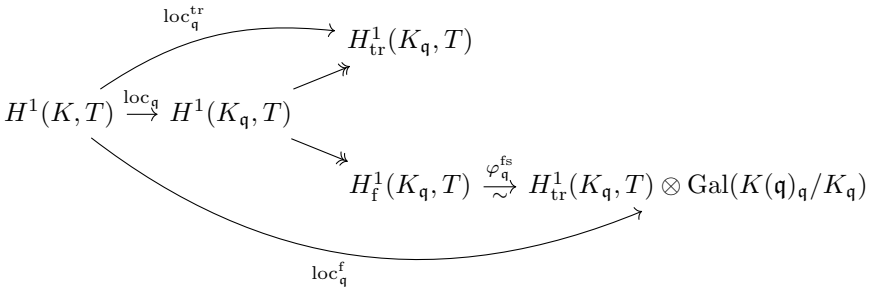
$$W_\mathfrak{n} \coloneqq \bigoplus_{\mathfrak{q}\mid\mathfrak{n}} \mathrm{Hom}(H^1_{\mathrm{tr}}(K_\mathfrak{q},T),R),$$
$$Y_\mathfrak{n} \coloneqq \bigwedge^{r+\nu(\mathfrak{n})} H^1_{\mathcal{F}^\mathfrak{n}}(K,T)\otimes\bigwedge^{\nu(\mathfrak{n})} W_\mathfrak{n}.$$

By the above observation, $W_\mathfrak{n}$ is free of rank $\nu(\mathfrak{n})$.

Writing $\mathfrak{n}=\mathfrak{q}_1\cdots\mathfrak{q}_{\nu(\mathfrak{n})}$ and fixing generators h_i of $\mathrm{Hom}(H^1_{\mathrm{tr}}(K_{\mathfrak{q}_i},T),R)$, then $\bigwedge^{\nu(\mathfrak{n})} W_\mathfrak{n}$ is a rank 1 free R-module generated by $h_1\wedge\cdots\wedge h_{\nu(\mathfrak{n})}$.

We will now construct maps making the $Y_\mathfrak{n}$ into an inverse system indexed over $\mathcal{N}$.

Definition 2.3.2. We define maps $\mathrm{loc}^{\mathrm{tr}}_\mathfrak{q}$ and $\mathrm{loc}^{\mathrm{f}}_\mathfrak{q}$ by composing the localization map with the two projections from $H^1(K,T)=H^1_{\mathrm{f}}(K,T)\oplus H^1_{\mathrm{tr}}(K,T)$ (recall Lemma 2.2.2) and, in the second case, also with $\varphi^{\mathrm{fs}}_\mathfrak{q}$ (from Definition 2.2.3), which is an isomorphism by Lemma 2.2.4:



We now construct maps that make the $Y_\mathfrak{n}$ into an inverse system. Let $\mathfrak{n}=\mathfrak{q}_1\cdots\mathfrak{q}_t\in\mathcal{N}$ and $\mathfrak{n}'=\mathfrak{q}_1\cdots\mathfrak{q}_s\mid\mathfrak{n}$; there is a map

$$\Psi_{\mathfrak{n},\mathfrak{n}'}\colon Y_\mathfrak{n}\to Y_{\mathfrak{n}'}$$

given as follows. Let $\mathfrak{n}_i\coloneqq\prod_{j\leqslant i}\mathfrak{q}_j$, denote $\psi_i\coloneqq h_i\circ\mathrm{loc}^{\mathrm{tr}}_{\mathfrak{q}_i}$ and consider the exact sequence $0\to H^1_{\mathcal{F}^{\mathfrak{n}_{i-1}}}(K,T)\to H^1_{\mathcal{F}^{\mathfrak{n}_i}}(K,T)\xrightarrow{\psi_i}R$; by Proposition 2.1.6, there are unique maps

$$\widehat{\psi}_i\colon\ \bigwedge^i H^1_{\mathcal{F}^{\mathfrak{n}_i}}(K,T)\to R\otimes\bigwedge^{i-1}H^1_{\mathcal{F}^{\mathfrak{n}_{i-1}}}(K,T)$$

whose composition with $R\otimes\bigwedge^i H^1_{\mathcal{F}^{\mathfrak{n}_i}}(K,T)$ is given by

$$m_1\wedge\cdots\wedge m_i\mapsto\sum_{j=1}^{i}(-1)^{j+1}\psi_i(m_j)\otimes(m_1\wedge\cdots\wedge m_{j-1}\wedge m_{j+1}\wedge\cdots\wedge m_i)$$

and whose image is the image of

$$\operatorname{im}\psi_i \otimes \bigwedge^{i-1} H^1_{\mathcal{F}^{\mathfrak{n}_{i-1}}}(K,T) \to R \otimes \bigwedge^{i-1} H^1_{\mathcal{F}^{\mathfrak{n}_{i-1}}}(K,T).$$

We can compose these maps as

$$\widehat{\psi_{s+1}} \circ \cdots \circ \widehat{\psi_t} \colon \bigwedge^{r+t} H^1_{\mathcal{F}^{\mathfrak{n}}}(K,T) \to \bigwedge^{r+s} H^1_{\mathcal{F}^{\mathfrak{n}'}}(K,T).$$

Taking the tensor product of the above with the isomorphism $\bigwedge^{\nu(\mathfrak{n})} W_{\mathfrak{n}} \to \bigwedge^{\nu(\mathfrak{n}')} W_{\mathfrak{n}'}$, $(h_1 \wedge \cdots \wedge h_t) \mapsto (h_1 \wedge \cdots \wedge h_s)$, finally gives a map $\Psi_{\mathfrak{n},\mathfrak{n}'}$ which is independent of the choices made. One can moreover check the following compatibility property: if $\mathfrak{n} \in \mathcal{N}$ and $\mathfrak{n}'' \mid \mathfrak{n}' \mid \mathfrak{n}$, then

$$\Psi_{\mathfrak{n}',\mathfrak{n}''} \circ \Psi_{\mathfrak{n},\mathfrak{n}'} = \Psi_{\mathfrak{n},\mathfrak{n}''}.$$

This property allows us to make the following definition:

Definition 2.3.3. Given Selmer data $(T,\mathcal{F},\mathcal{P})$, we define the R-module of *Stark systems of rank r* as the inverse limit of the inverse system $(Y_{\mathfrak{n}}, \Psi_{\mathfrak{n},\mathfrak{n}'})$:

$$\mathbf{SS}_r(T) = \mathbf{SS}_r(T,\mathcal{F},\mathcal{P}) \coloneqq \varprojlim_{\mathfrak{n}\in\mathcal{N}} Y_{\mathfrak{n}}.$$

We will denote a Stark system by $\varepsilon = (\varepsilon_{\mathfrak{n}})_{\mathfrak{n}\in\mathcal{N}}$.

Lemma 2.3.4. Let $Y'_{\mathfrak{n}} \coloneqq \mathfrak{m}^{\mu(\mathfrak{n})} Y_{\mathfrak{n}}$ recalling $\mu(\mathfrak{n}) = \operatorname{len} H^1_{(\mathcal{F}^{\mathfrak{n}})^D}(K,T^D)$. Then:

1. $Y'_{\mathfrak{n}}$ is a cyclic R-module and $\operatorname{len}(Y'_{\mathfrak{n}}) = \max\{k-\mu(\mathfrak{n}),0\}$;
2. there is $\mathfrak{n}\in\mathcal{N}$ such that $H^1_{(\mathcal{F}^{\mathfrak{n}})^D}(K,T^D) = 0$;
3. if $H^1_{(\mathcal{F}^{\mathfrak{n}})^D}(K,T^D) = 0$ then $Y_{\mathfrak{n}}$ is a free R-module of rank 1;
4. if $H^1_{(\mathcal{F}^{\mathfrak{n}})^D}(K,T^D) = 0$ and $\mathfrak{n}' \mid \mathfrak{n}$ then $\Psi_{\mathfrak{n},\mathfrak{n}'} = Y'_{\mathfrak{n}}$.

Proof. (1) follows from Corollary 2.2.15.4.

(2) Use $\mathfrak{n} \coloneqq \prod_i \mathfrak{q}_i$ with $\mathfrak{q}_i \in \mathcal{N}$ satisfying $\operatorname{loc}_{\mathfrak{q}_i}(c_i) \neq 0$ for generators $c_1,\dots,c_t$ of $H^1_{\mathcal{F}^D}(K,T^D)[\mathfrak{m}]$; their existence is proven in [MR04, Proposition 3.6.1] using the Cebotarev density theorem (see also the proof of Proposition 2.3.6 below).

(3) follows from Corollary 2.2.15.4.

(4) $\Psi_{\mathfrak{n},\mathfrak{n}'}(Y_{\mathfrak{n}}) = \mathfrak{m}^{\operatorname{len} H^1_{\mathcal{F}^{\mathfrak{n}'}}(K,T) - k(r+\nu(\mathfrak{n}'))} Y_{\mathfrak{n}'}$ and from Corollary 2.2.15.2 we conclude

$$\operatorname{len} H^1_{\mathcal{F}^{\mathfrak{n}'}}(K,T) - k(r+\nu(\mathfrak{n}')) = \operatorname{len} H^1_{(\mathcal{F}^D)_{\mathfrak{n}'}}(K,T^D).$$

□

Theorem 2.3.5. $\mathbf{SS}_r(T)$ is a free R-module of rank 1. For every $\mathfrak{n}\in\mathcal{N}$, the image of the projection $\mathbf{SS}_r(T) \to Y_{\mathfrak{n}}$ is $Y'_{\mathfrak{n}}$.

Proof. By the lemma, point (2), we can choose $\mathfrak{d}$ such that $H^1_{(\mathcal{F}^D)_{\mathfrak{d}}}(K,T^D) = 0$; so, $H^1_{(\mathcal{F}^D)_{\mathfrak{n}}}(K,T^D) = 0$ for all $\mathfrak{d} \mid \mathfrak{n} \in \mathcal{N}$, and we conclude by the lemma, point (4). □

For $\varepsilon \in \mathbf{SS}_r(T)$, define the following objects:

- $\varphi_\varepsilon(\mathfrak{n}) \coloneqq \max\{j \mid \varepsilon_\mathfrak{n} \in \mathfrak{m}^j Y_\mathfrak{n}\}$ for $\mathfrak{n} \in \mathcal{N}$;
- the operator ∂ by

$$\left(f\colon \mathcal{N} \to \mathbb{N} \cup \{\infty\}\right) \mapsto \begin{pmatrix} \partial f\colon \mathbb{N} \to \mathbb{N} \cup \{\infty\} \\ \qquad i \mapsto \min\{f(\mathfrak{n}) \mid \mathfrak{n} \in \mathcal{N},\, \nu(\mathfrak{n}) = i\} \end{pmatrix}$$

- $\operatorname{ord}(\varepsilon) \coloneqq \min\{\nu(\mathfrak{n}) \mid \mathfrak{n} \in \mathcal{N},\, \varepsilon_\mathfrak{n} \neq 0\} = \min\{i \mid \partial\varphi_\varepsilon(i) \neq \infty\}$;
- $d_\varepsilon(i) \coloneqq \partial\varphi_\varepsilon(i) - \partial\varphi_\varepsilon(i+1)$ for $i \geqslant \operatorname{ord}(\varepsilon)$.

As will be clear soon, $d_\varepsilon(i)$ and $\operatorname{ord}(\varepsilon)$ are independent of the choice of non-zero $\varepsilon \in \mathbf{SS}_r(T)$ and are attached to information about the dual Selmer module $H^1_{\mathcal{F}^D}(K, T^D)$.

Recall that we have defined

$$\lambda(\mathfrak{n}) \coloneqq \operatorname{len} H^1_{\mathcal{F}(\mathfrak{n})^D}(K, T^D) \qquad\qquad \mu(\mathfrak{n}) \coloneqq \operatorname{len} H^1_{(\mathcal{F}^\mathfrak{n})^D}(K, T^D)$$

We can compute the functions $\partial\lambda$ and $\partial\mu$:

Proposition 2.3.6. Let $R = \mathbb{Z}/p^k\mathbb{Z}$. Write $H^1_{\mathcal{F}^D}(K, T^D) \cong \bigoplus_{i \geqslant 1} R/\mathfrak{m}^{e_i}$ with $e_1 \geqslant e_2 \geqslant \cdots \geqslant 0$. Then

$$\partial\lambda(t) = \partial\mu(t) = \sum_{i>t} e_i \quad \text{for every } t \geqslant 0.$$

Proof. Let $\mathfrak{n} \in \mathcal{N}$, write $\nu(\mathfrak{n}) = t$; consider the map

$$H^1_{\mathcal{F}^D}(K, T^D) \to \bigoplus_{\mathfrak{q}\mid\mathfrak{n}} H^1_{\mathrm{f}}(K_\mathfrak{q}, T^D)$$

induced by composition of projection and localization as usual. The right side is a free R-module of rank t, so the image of this map is a quotient of $H^1_{\mathcal{F}^D}(K, T^D)$ generated by at most t elements. Therefore it has length at most $\sum_{i \leqslant t} e_i$ and the kernel has length at least $\sum_{i>t} e_i$. By definition the kernel is $H^1_{(\mathcal{F}^D)_\mathfrak{n}}(K, T^D)$, which is contained in $H^1_{\mathcal{F}(\mathfrak{n})^D}(K, T^D)$, so

$$\lambda(\mathfrak{n}) \geqslant \mu(\mathfrak{n}) \geqslant \sum_{i>t} e_i.$$

We prove by induction on t that, for any $t \geqslant 0$, we can choose some $\mathfrak{n}$ satisfying $\nu(\mathfrak{n}) = t$ and $H^1_{\mathcal{F}(\mathfrak{n})^D}(K, T^D) \cong \bigoplus_{i>t} R/\mathfrak{m}^{e_i}$, in which case we have equalities in the above formula and the lemma follows.

For $t = 0$ it suffices to take $\mathfrak{n} = 1$.

For $t \geqslant 1$, let $\mathfrak{n} \in \mathcal{N}$ satisfy $\nu(\mathfrak{n}) = t - 1$ and $H^1_{\mathcal{F}(\mathfrak{n})^D}(K, T^D) \cong \bigoplus_{i>t-1} R/\mathfrak{m}^{e_i}$. Since $\chi(T) > 0$, then $\mathfrak{m}^{k-1} H^1_{\mathcal{F}(\mathfrak{n})}(K, T) \neq 0$ by Corollary 2.2.15. Fix a non-zero element

$$c \in \mathfrak{m}^{k-1} H^1_{\mathcal{F}(\mathfrak{n})}(K, T) \subset \mathfrak{m}^{k-1} H^1_{\mathcal{F}(\mathfrak{n})}(K, T)[\mathfrak{m}].$$

If $e_t > 0$, choose a non-zero element

$$c' \in \mathfrak{m}^{e_t - 1} H^1_{\mathcal{F}(\mathfrak{n})^D}(K, T^D) \subset \mathfrak{m}^{k-1} H^1_{\mathcal{F}(\mathfrak{n})^D}(K, T^D)[\mathfrak{m}].$$

We may choose $\mathfrak{q} \in \mathcal{P}$ with $\operatorname{loc}_\mathfrak{q}(c) \neq 0$ and, if $e_t > 0$, $\operatorname{loc}_\mathfrak{q}(c') \neq 0$ as well: this is done by Cebotarev's density theorem (*if C is a conjugacy class in* $\operatorname{Gal}(L/K)$, *then the primes v*

whose Frobenius conjugacy class is C have density $|C|/|G|$) and is proven in [MR04, Proposition 3.6.1]. Since $H^1_{\mathrm{f}}(K_{\mathfrak{q}}, T)$ is free of rank 1 and, by our choice of $\mathfrak{q}$, the localization of $\mathfrak{m}^{k-1}H^1_{\mathcal{F}(\mathfrak{n})}(K,T)$ at $\mathfrak{q}$ is non-zero, it follows that the localization map $H^1_{\mathcal{F}(\mathfrak{n})}(K,T) \to H^1_{\mathrm{f}}(K_{\mathfrak{q}}, T)$ is surjective. Similarly $\mathfrak{m}^{e_t}H^1_{\mathcal{F}(\mathfrak{n})^D}(K,T^D) = 0$ and, if $e_t > 0$, then the localization of $\mathfrak{m}^{e_t-1}H^1_{\mathcal{F}(\mathfrak{n})^D}(K,T^D)$ at $\mathfrak{q}$ is non-zero, so

$$\frac{H^1_{\mathcal{F}(\mathfrak{n})^D}(K,T^D)}{H^1_{\mathcal{F}^{\mathfrak{q}}(\mathfrak{n})^D}(K,T^D)} \cong \mathrm{loc}_{\mathfrak{q}}\left(H^1_{\mathcal{F}(\mathfrak{n})^D}(K,T^D)\right) \cong R/\mathfrak{m}^{e_t}$$

and therefore $H^1_{\mathcal{F}^{\mathfrak{q}}(\mathfrak{n})^D}(K,T^D) \cong \bigoplus_{i>t} R/\mathfrak{m}^{e_i}$. Moreover $H^1_{\mathcal{F}(\mathfrak{nq})^D}(K,T^D) = H^1_{\mathcal{F}^{\mathfrak{q}}(\mathfrak{n})^D}(K,T^D)$ by Lemma 2.2.12.2. so $\mathfrak{nq} \in \mathcal{N}$ satisfies the request. □

Recall that $\mathbf{SS}_r(T)$ is free of rank 1 over $\mathbb{Z}/p^k\mathbb{Z}$ by Theorem 2.3.5, so the submodule generated by an arbitrary ε is $\mathfrak{m}^s\mathbf{SS}_r(T)$ for some power of $\mathfrak{m}$.

Proposition 2.3.7. Let R and e_i be as in the previous proposition. Let $\varepsilon \in \mathbf{SS}_r(T)$ generate $\mathfrak{m}^s\mathbf{SS}_r(T)$ for some s; then

$$\partial\varphi_\varepsilon(t) = \begin{cases} s + \sum_{i>t} e_i & \text{if } s + \sum_{i>t} e_i < k \\ \infty & \text{if } s + \sum_{i>t} e_i \geqslant k \end{cases} \quad \text{for every } t \geqslant 0.$$

Proof. It is enough to prove the case $s = 0$; so, assume ε generates $\mathbf{SS}_r(T)$. By Theorem 2.3.5, $\mathbf{SS}_r(T)$ projects onto $Y'_{\mathfrak{n}}$, which is therefore generated by $\varepsilon_{\mathfrak{n}}$:

$$R\varepsilon_{\mathfrak{n}} = Y'_{\mathfrak{n}} \coloneqq \mathfrak{m}^{\mu(\mathfrak{n})}Y_{\mathfrak{n}}$$

which is cyclic of length $\max\{k - \mu(\mathfrak{n}), 0\}$ by Lemma 2.3.4.1; hence $\varepsilon_{\mathfrak{n}} \in \mathfrak{m}^{\mu(\mathfrak{n})+1}Y_{\mathfrak{n}}$ if and only if $\mu(\mathfrak{n}) \geqslant k$, and therefore

$$\partial\varphi_\varepsilon(t) = \begin{cases} \partial\mu(t) & \text{if } \partial\mu(t) < k \\ \infty & \text{if } \partial\mu(t) \geqslant k \end{cases} \quad \text{for every } t \geqslant 0.$$

We conclude by the previous proposition which computes $\partial\mu(t) = \sum_{i>t} e_i$. □

We can now describe the dual of the Selmer group in terms of Stark systems.

Theorem 2.3.8. Let $R = \mathbb{Z}/p^k\mathbb{Z}$ and e_i as before, let $\varepsilon \in \mathbf{SS}_r(T)$ such that $\varepsilon_1 \neq 0$. Then

$$\partial\varphi_\varepsilon(0) \geqslant \partial\varphi_\varepsilon(1) \geqslant \partial\varphi_\varepsilon(2) \geqslant \cdots \geqslant 0$$
$$d_\varepsilon(0) \geqslant d_\varepsilon(1) \geqslant d_\varepsilon(2) \geqslant \cdots \geqslant 0$$

and

$$H^1_{\mathcal{F}^D}(K,T^D) \cong \bigoplus_{i\geqslant 0} R/\mathfrak{m}^{d_\varepsilon(i)}.$$

Proof. Write $R\varepsilon = \mathfrak{m}^s\mathbf{SS}_r(T)$; if $\varepsilon_1 \neq 0$, then $\partial\varphi_\varepsilon(0) < k$, so the above proposition gives $\partial\varphi_\varepsilon(t) = s + \sum_{i>t} e_i$ for every t, and the first chain of inequalities follows. Moreover,

$$d_\varepsilon(t) = \partial\varphi_\varepsilon(t) - \partial\varphi_\varepsilon(t+1) = s + \sum_{i>t} e_i - s - \sum_{i>t+1} e_i = e_{t+1}$$

and, since we are assuming the e_t are decreasing, the remaining inequalities follow, as well as the structure isomorphism. □

This shows that the quantities $d_\varepsilon(i)$ are independent of ε such that $\varepsilon_1 \neq 0$.

2.3.1 The DVR case

We study the case $R = \mathbb{Z}_p$ in order to obtain results involving the p-torsion E_{p^∞} of an elliptic curve. Recall that this is obtained as a dual module T^D where $T = T_p(E) \coloneqq \varprojlim_k E_{p^k}$ is the Tate module, and the Selmer module in this case is $H^1_{\mathcal{F}}(K, T^D) = S_{p^\infty}(K, E)$, the Selmer group defined in Remark 1.6.4.

Denote again by $\mathfrak{m}$ the maximal ideal of R, i.e. $p\mathbb{Z}_p$. In order to study $\mathbf{SS}_r(T)$, we will apply our previous results to $R/\mathfrak{m}^k = \mathbb{Z}/p^k\mathbb{Z}$, considered with the canonical Selmer structure induced by $\mathcal{F}$. Indeed, a local condition $\mathcal{F}$ on T propagates canonically to the quotients T/IT by taking $H^1_{\mathcal{F}}(K_v, T/IT)$ to be the image of $H^1_{\mathcal{F}}(K_v, T)$ under the projection $T \twoheadrightarrow T/IT$.

Recall that we have sets $\mathcal{P}_j \coloneqq \{\mathfrak{q} \in \mathcal{P} \mid I_\mathfrak{q} \in \mathfrak{m}^j\}$ and inclusions

$$\mathcal{P}_{j+1} \subset \mathcal{P}_j \subset \mathcal{P} \subset \mathcal{N}.$$

Definition 2.3.9. Let $\mathfrak{n} \in \mathcal{N}$. We define:

$$\begin{aligned} W_\mathfrak{n} &\coloneqq \bigoplus_{\mathfrak{q}\mid\mathfrak{n}} \mathrm{Hom}(H^1_{\mathrm{tr}}(K_\mathfrak{q}, T/I_\mathfrak{n}T), R/I_\mathfrak{n}) \\ Y_\mathfrak{n} &\coloneqq \textstyle\bigwedge^{r+\nu(\mathfrak{n})} H^1_{\mathcal{F}^\mathfrak{n}}(K, T/I_\mathfrak{n}T) \otimes \bigwedge^{\nu(\mathfrak{n})} W_\mathfrak{n} \\ Y'_\mathfrak{n} &\coloneqq \mathfrak{m}^{\operatorname{len} H^1_{(\mathcal{F}^\mathfrak{n})^D}(K, T^D[I_\mathfrak{n}])} Y_\mathfrak{n} \end{aligned}$$

and we define a Stark system of rank r for $(T, \mathcal{F}, \mathcal{P})$ as a collection $\{\varepsilon_\mathfrak{n} \in Y_\mathfrak{n} \mid \mathfrak{n} \in \mathcal{N}\}$ satisfying, for $\mathfrak{n}' \mid \mathfrak{n}$,

$$\Psi_{\mathfrak{n},\mathfrak{n}'}(\varepsilon_\mathfrak{n}) = \overline{\varepsilon}_{\mathfrak{n}'}$$

where $\overline{\varepsilon}_{\mathfrak{n}'}$ is the image of $\varepsilon_{\mathfrak{n}'}$ in $Y_{\mathfrak{n}'} \otimes R/I_\mathfrak{n}$ and $\Psi_{\mathfrak{n},\mathfrak{n}'} \colon Y_\mathfrak{n} \to Y_{\mathfrak{n}'} \otimes R/I_\mathfrak{n}$ is obtained from the map defined for $T/I_\mathfrak{n}T$ and $R/I_\mathfrak{n}$ as in the previous case of finite ring (recall that by definition $I_\mathfrak{n}$ is some power of $\mathfrak{m}$ and therefore $R/I_\mathfrak{n}$ is some finite ring $\mathbb{Z}/p^k\mathbb{Z}$). Again, we denote by $\mathbf{SS}_r(T, \mathcal{F}, \mathcal{P})$ the R-module of Stark systems.

Lemma 2.3.10. If $j \leqslant k$, then the projection $T/\mathfrak{m}^kT \to T/\mathfrak{m}^jT$ and the restriction to $\mathcal{P}_k$ induce a surjection and an isomorphism, respectively:

$$\mathbf{SS}_r(T/\mathfrak{m}^kT, \mathcal{P}_k) \longrightarrow\!\!\!\!\!\rightarrow \mathbf{SS}_r(T/\mathfrak{m}^jT, \mathcal{P}_k) \xleftarrow{\sim} \mathbf{SS}_r(T/\mathfrak{m}^jT, \mathcal{P}_j).$$

Proof. Let $\mathfrak{n} \in \mathcal{N}_k$ be such that $H^1_{(\mathcal{F}^D)_\mathfrak{n}}(K, T^D[\mathfrak{m}]) = 0$. Then, by Theorem 2.3.5, projecting to $Y_\mathfrak{n}$ gives a diagram

$$\begin{array}{ccccc} \mathbf{SS}_r(T/\mathfrak{m}^kT, \mathcal{P}_k) & \longrightarrow & \mathbf{SS}_r(T/\mathfrak{m}^jT, \mathcal{P}_k) & \longleftarrow & \mathbf{SS}_r(T/\mathfrak{m}^jT, \mathcal{P}_j) \\ \downarrow\sim & & \downarrow\sim & & \downarrow\sim \\ Y_\mathfrak{n} \otimes R/\mathfrak{m}^k & \longrightarrow\!\!\!\!\!\rightarrow & Y_\mathfrak{n} \otimes R/\mathfrak{m}^j & \xleftarrow{=} & Y_\mathfrak{n} \otimes R/\mathfrak{m}^j \end{array}$$

whence we conclude immediately. □

Composing the surjection with the (inverse of the) isomorphism above gives maps $\mathbf{SS}_r(T/\mathfrak{m}^kT, \mathcal{P}_k) \to \mathbf{SS}_r(T/\mathfrak{m}^jT, \mathcal{P}_j)$ for $j \leqslant k$ which make the R-modules $\mathbf{SS}_r(T/\mathfrak{m}^kT, \mathcal{P}_k)$ into an inverse system, and we can form the inverse limit. Then:

Theorem 2.3.11.

1. The maps $T \twoheadrightarrow T/\mathfrak{m}^k T$ and $\mathcal{P}_k \hookrightarrow \mathcal{P}$ induce an isomorphism
$$\mathbf{SS}_r(T,\mathcal{P}) \xrightarrow{\sim} \varprojlim \mathbf{SS}_r(T/\mathfrak{m}^k T, \mathcal{P}_k).$$
2. $\mathbf{SS}_r(T,\mathcal{P})$ is free of rank 1 over R, generated by a Stark system ε whose image in $\mathbf{SS}_r(T/\mathfrak{m}T,\mathcal{P})$ is non-zero.
3. The maps $\mathbf{SS}_r(T,\mathcal{P}) \to \mathbf{SS}_r(T/\mathfrak{m}^k T, \mathcal{P}_k)$ are surjective for all k.

Proof. (1) If $0 \neq \varepsilon \in \mathbf{SS}_r(T)$, there is $\mathfrak{n}$ such that $0 \neq \varepsilon_\mathfrak{n} \in Y_\mathfrak{n}$. If $\mathfrak{n} \neq 1$ then $I_\mathfrak{n} \neq 0$ and we let k be such that $\mathfrak{m}^k = I_\mathfrak{n}$. If $\mathfrak{n} = 1$ choose k so that $\varepsilon_1 \neq 0$ in $\bigwedge^r H^1_\mathcal{F}(K, T/\mathfrak{m}^k T)$. In either case $I_\mathfrak{n} \subset \mathfrak{m}^k$ and the image of ε in $\mathbf{SS}_r(T/\mathfrak{m}^k T, \mathcal{P}_k)$ is non-zero, proving injectivity.

To prove surjectivity, let $(\varepsilon^{(k)})_k \in \varprojlim \mathbf{SS}_r(T/\mathfrak{m}^k T, \mathcal{P}_k)$. If $\mathfrak{n} \in \mathcal{N}$ and $\mathfrak{n} \neq 1$, let j be such that $I_\mathfrak{n} = \mathfrak{m}^j$ and define $\varepsilon_\mathfrak{n} := \varepsilon_\mathfrak{n}^{(j)} \in Y_\mathfrak{n}$. If $\mathfrak{n} = 1$, define

$$\varepsilon_1 = \lim_{k\to\infty} \varepsilon_1^{(k)} \in \lim_{k\to\infty} \bigwedge^r H^1_\mathcal{F}(K, T/\mathfrak{m}^k T) = \bigwedge^r H^1_\mathcal{F}(K,T) = Y_1.$$

This defines an element $\varepsilon := (\varepsilon_\mathfrak{n})_\mathfrak{n} \in \mathbf{SS}_r(T,\mathcal{P})$ that maps to $\varepsilon^{(k)}$ for every k, proving surjectivity.

(2) and (3) By Theorem 2.3.5, $\mathbf{SS}_r(T/\mathfrak{m}^k T, \mathcal{P}_k)$ is free of rank 1 over $R/\mathfrak{m}^k$ for all k. The maps $\mathbf{SS}_r(T/\mathfrak{m}^{k+1}T, \mathcal{P}_{k+1}) \to \mathbf{SS}_r(T/\mathfrak{m}^k T, \mathcal{P}_k)$ are surjective by Lemma 2.3.10, so we conclude by the previous point. □

We say that $\varepsilon \in \mathbf{SS}_r(T)$ is *primitive* if it generates $\mathbf{SS}_r(T)$ as an R-module; such elements exist by the above theorem. We apply these results to obtain an analogue of Proposition 2.3.7 and Theorem 2.3.8 for the case of $R = \mathbb{Z}_p$ discrete valuation ring.

Proposition 2.3.12. Let

$$\begin{aligned} a &:= \operatorname{corank}_R H^1_{\mathcal{F}^D}(K, T^D) \\ &:= \operatorname{rank}_R \operatorname{Hom}_R(H^1_{\mathcal{F}^D}(K,T^D), \mathbb{Q}_p/\mathbb{Z}_p) \end{aligned}$$

and e_i be such that

$$\frac{H^1_{\mathcal{F}^D}(K,T^D)}{H^1_{\mathcal{F}^D}(K,T^D)_{\mathrm{div}}} \cong \bigoplus_{i>a} R/\mathfrak{m}^{e_i}, \quad e_{a+1} \geqslant e_{a+2} \geqslant \cdots$$

Let $\varepsilon \in \mathbf{SS}_r(T)$ generate $\mathfrak{m}^s \mathbf{SS}_r(T)$; then

$$\partial\varphi_\varepsilon(t) = \begin{cases} s + \sum_{i>t} e_i & \text{if } t \geqslant a \\ \infty & \text{if } t < a. \end{cases}$$

Proof. $H^1_{\mathcal{F}^D}(K,T^D) = \varinjlim_k H^1_{\mathcal{F}^D}(K, T^D[\mathfrak{m}^k])$ By Proposition 2.2.13, we have

$$H^1_{\mathcal{F}^D}(K, T^D[\mathfrak{m}^k]) = H^1_{\mathcal{F}^D}(K,T^D)[\mathfrak{m}^k] \cong \bigoplus_{i\geqslant 1} R/\mathfrak{m}^{\min\{k,e_i\}}$$

where we set $e_1 = \cdots = e_a = \infty$. For $k \geqslant 0$ let $\varepsilon^{(k)}$ be the image of ε in $\mathbf{SS}_r(T/\mathfrak{m}^k T, \mathcal{P}_k)$ and write $R\varepsilon = \mathfrak{m}^s \mathbf{SS}_r(T)$. Then $\varepsilon^{(k)}$ generates $\mathfrak{m}^s \mathbf{SS}_r(T/\mathfrak{m}^k T)$, by the above theorem.

Let t and $\mathfrak{n} \in \mathcal{N}$ with $\nu(\mathfrak{n}) = t$, write $I_{\mathfrak{n}} = \mathfrak{m}^k$. By the computation of $\partial\varphi_\varepsilon(t)$ in the case of finite R we have

$$\begin{aligned} \varepsilon_{\mathfrak{n}}^{(k)} &= 0 && \text{if } t < a \\ \varepsilon_{\mathfrak{n}}^{(k)} &\in \mathfrak{m}^{s+\sum_{i>t} e_i} Y_{\mathfrak{n}} && \text{if } t \geqslant a \end{aligned}$$

Since $\varepsilon_{\mathfrak{n}}^{(k)} = \varepsilon_{\mathfrak{n}} \in Y_{\mathfrak{n}}$, we conclude

$$\begin{aligned} \partial\varphi_\varepsilon(t) &= \infty && \text{if } t < a \\ \partial\varphi_\varepsilon(t) &\geqslant s + \sum_{i>t} e_i && \text{if } t \geqslant a \end{aligned}$$

If $t \geqslant a$, we must show equality: by Proposition 2.3.7, for any $k > s + \sum_{i>t} e_i$ one can find $\mathfrak{n} \in \mathcal{N}$ with $I_{\mathfrak{n}} \subset \mathfrak{m}^k$ such that $\varepsilon_{\mathfrak{n}}^{(k)} \notin \mathfrak{m}^{s+1+\sum_{i>t} e_i} Y_{\mathfrak{n}}$, hence also $\varepsilon_{\mathfrak{n}}$, and we conclude. □

We can now conclude easily. Here, φ_ε, ∂, $\operatorname{ord}(\varepsilon)$ and $d_\varepsilon(i)$ are defined as in Section 2.3.

Theorem 2.3.13. Let $R = \mathbb{Z}_p$, $\varepsilon \in \mathbf{SS}_r(T)$, $\varepsilon \neq 0$. Then:

1. There are sequences
$$\partial\varphi_\varepsilon(0) \geqslant \partial\varphi_\varepsilon(1) \geqslant \partial\varphi_\varepsilon(2) \geqslant \cdots \geqslant 0$$
$$d_\varepsilon(0) \geqslant d_\varepsilon(1) \geqslant d_\varepsilon(2) \geqslant \cdots \geqslant 0$$
whose terms are finite for $t \geqslant \operatorname{ord}(\varepsilon)$.

2. There is an isomorphism
$$\frac{H^1_{\mathcal{F}^D}(K, T^D)}{H^1_{\mathcal{F}^D}(K, T^D)_{\mathrm{div}}} \cong \bigoplus_{i \geqslant \operatorname{ord}(\varepsilon)} R/\mathfrak{m}^{d_\varepsilon(i)}$$

3. Setting $\partial\varphi_\varepsilon(\infty) := \lim_{t\to\infty} \partial\varphi_\varepsilon(t)$,
$$\operatorname{len}\left(\frac{H^1_{\mathcal{F}^D}(K, T^D)}{H^1_{\mathcal{F}^D}(K, T^D)_{\mathrm{div}}}\right) = \partial\varphi_\varepsilon(\operatorname{ord}\varepsilon) - \partial\varphi_\varepsilon(\infty)$$

4. $\operatorname{len} H^1_{\mathcal{F}^D}(K, T^D) < \infty$ if and only if $\varepsilon_1 \neq 0$.

5. $\operatorname{len} H^1_{\mathcal{F}^D}(K, T^D) \leqslant \partial\varphi_\varepsilon(0) = \max\{s \mid \varepsilon_1 \in \mathfrak{m}^s \bigwedge^r H^1_{\mathcal{F}}(K, T)\}$ and equality holds if and only if ε is primitive.

Proof. (1) and (2) follow as before using the previous proposition and writing $d_\varepsilon(i) = e_{i+1}$, $a = \operatorname{ord}(\varepsilon)$.

(3) The length is the sum of the lengths of the direct summands in (2), i.e.

$$\sum_{i \geqslant \operatorname{ord}(\varepsilon)} d_\varepsilon(i) = \sum_{i \geqslant \operatorname{ord}(\varepsilon)} \big(\partial\varphi_\varepsilon(i) - \partial\varphi_\varepsilon(i+1)\big) = \partial\varphi_\varepsilon(\operatorname{ord}\varepsilon) - \partial\varphi_\varepsilon(\infty).$$

(4) If $\varepsilon_1 = 0$ then $\operatorname{ord}(\varepsilon) \geqslant 1$, so $H^1_{\mathcal{F}^D}(K, T^D)$ has infinite length since $\operatorname{ord}(\varepsilon)$ is its corank. Conversely, if $\varepsilon_1 \neq 0$ then $\partial\varphi_\varepsilon(0)$ is finite, so the claim follows from the next point.

(5) The inequality follows by writing

$$H^1_{\mathcal{F}(\mathfrak{n})^D}(K,T^D) = \bigcup_i H^1_{\mathcal{F}(\mathfrak{n})^D}(K,T^D)[\mathfrak{m}^i]$$

where $\operatorname{len} H^1_{\mathcal{F}(\mathfrak{n})^D}(K,T^D[\mathfrak{m}^i]) = \operatorname{len} H^1_{\mathcal{F}(\mathfrak{n})^D}(K,T^D)[\mathfrak{m}^i]$ by the isomorphism in Proposition 2.2.13.2; so we are reduced to the case of finite R and we can apply Theorem 2.4.13. Finally, if $R\varepsilon = \mathfrak{m}^s\mathbf{SS}_r(T)$, for t big enough we have $\partial\varphi_\varepsilon(t) = s + \sum_{i>t} e_i$ by Proposition 2.3.12, so $\partial\varphi_\varepsilon(\infty) = 0$ if and only if ε generates $\mathbf{SS}_r(T)$ (i.e. ε is primitive) and in this case the stated equality follows from (3). □

2.4 Kolyvagin systems

2.4.1 Sheaves on a graph

A graph is as usual a couple (V,E) where V is a set of vertices and E is a set of edges $\{\{v,w\} \mid v,w \in V,\ v \neq w\}$. Let us introduce some general notions.

Definition 2.4.1.

- A *sheaf* S of R-modules associated to a graph is the data of
  - an R-module $S(v)$ for every vertex v,
  - an R-module $S(e)$ for every edge e,
  - an R-module morphism $\psi^e_v\colon S(v) \to S(e)$ for every e and $v \in e$.
- A *global section* of S is a set $\{\kappa_v \in S(v) \mid v \text{ vertex}\}$ such that

  $$\psi^e_v(\kappa_v) = \psi^e_{v'}(\kappa_{v'}) \in S(e)$$

  whenever $e = \{v,v'\}$.

  Denote by $\Gamma(S)$ the R-module of global sections.
- S is *locally cyclic* if $S(v)$ and $S(e)$ are cyclic and ψ^e_v are surjective for all v and e.
- A vertex v is a *hub* of S if, for every vertex w, there is a *surjective path* from v to w, i.e. a path $(v = v_1, v_2, \dots, w = v_k)$ such that $\psi^{e_i}_{v_{i+1}}$ is an isomorphism if $e_i = \{v_i, v_{i+1}\}$.

  Given a surjective path P as above, there is a surjective map $S(v) \to S(w)$ defined as

  $$\psi_P \coloneqq (\psi^{e_{k-1}}_{v_k})^{-1} \circ \psi^{e_{k-1}}_{v_{k-1}} \circ \cdots \circ (\psi^{e_1}_{v_2})^{-1}\psi^{e_1}_{v_1} \in \operatorname{Hom}(S(v),S(w))$$

- S has *trivial monodromy* if, given surjective paths $P = (v,\dots,w)$ and $P' = (v,\dots,w')$ and an edge $e = \{w,w'\}$, then

  $$\psi^e_w \circ \psi_P = \psi^e_{w'} \circ \psi_{P'} \in \operatorname{Hom}(S(v),S(e)).$$

  In particular, given two surjective paths P and P' from v to w, we have $\psi_P = \psi_{P'} \in \operatorname{Hom}(S(v),S(w))$.

Proposition 2.4.2. If S is locally cyclic and v is a hub, then:

1. The map $f_v\colon \Gamma(S) \to S(v)$, $\kappa = (\kappa_v)_v \mapsto \kappa_v$ is injective. It is surjective if and only if S has trivial monodromy.
2. If $\kappa \in \Gamma(S)$ and u is a vertex such that $\kappa_u \neq 0$ and $R\kappa_u = \mathfrak{m}^i S(u)$ for some i, then $R\kappa_w = \mathfrak{m}^i S(w)$ for every vertex w.

Proof. We can write $\kappa_w = \psi_{P_w}(\kappa_v)$ for any w, P_w a surjective path from v to w; whence injectivity of f_v. To show surjectivity, let $c \in S(v)$ and define $\kappa_w \coloneqq \psi_{P_w}(c)$ for every w. If S has trivial monodromy, then this is independent of P_w, so $\kappa = (\kappa_w)_w \in \Gamma(S)$ and $c = \kappa_v$; conversely, suppose f_v is surjective and write $c = \kappa_v$ for some κ. Then $\kappa_w = \psi_{P_w}(\kappa_v) = \psi_{P_w}(c)$ so, if we consider an edge $e = \{w, w'\}$, we have

$$\psi^e_w \circ \psi_{P_w}(c) = \psi^e_w(\kappa_w) = \psi^e_{w'}(\kappa_{w'}) = \psi^e_{w'} \circ \psi_{P_{w'}}(c) \in S(e)$$

hence S has trivial monodromy.

□

2.4.2 The Selmer sheaf

Definition 2.4.3. Let $\mathcal{X} = \mathcal{X}(\mathcal{P})$ be the graph whose set of vertices is $\mathcal{N}$ and whose edges join exactly the vertices $\mathfrak{n}$, $\mathfrak{nq} \in \mathcal{N}$ for $\mathfrak{q}$ prime.

We want to define a sheaf on this graph $\mathcal{X}$. For $\mathfrak{n} \in \mathcal{N}$, define

$$G_\mathfrak{n} \coloneqq \bigotimes_{\mathfrak{q}\mid\mathfrak{n}} \mathrm{Gal}(K(\mathfrak{q})_\mathfrak{q}/K_\mathfrak{q}).$$

By definition of the fields $K(\mathfrak{q})_\mathfrak{q}$, every $\mathrm{Gal}(K(\mathfrak{q})_\mathfrak{q}/K_\mathfrak{q})$ is cyclic and its order is contained in $I_\mathfrak{n}$, since $I_\mathfrak{n} \supset I_\mathfrak{q} \supset [K(\mathfrak{q})_\mathfrak{q} : K_\mathfrak{q}]R$ by definition of $I_\mathfrak{n}$. It follows that $G_\mathfrak{n} \otimes (R/I_\mathfrak{n})$ is a free $R/I_\mathfrak{n}$-module of rank 1.

For $\mathfrak{q}$ prime dividing $\mathfrak{n}$,

$$\frac{T/I_\mathfrak{n}T}{(\mathrm{Fr}_\mathfrak{q} - 1)(T/I_\mathfrak{n}T)}$$

is a free $R/I_\mathfrak{n}$-module of rank 1, hence Lemma 2.2.4 says that

$$\varphi^{\mathrm{fs}}_\mathfrak{q}\colon H^1_{\mathrm{f}}(K_\mathfrak{q}, T/I_\mathfrak{n}T) \xrightarrow{\sim} H^1_{\mathrm{tr}}(K_\mathfrak{q}, T/I_\mathfrak{n}T) \otimes G_\mathfrak{q}$$

is an isomorphism and both the finite and the transverse submodules are free of rank 1. Therefore, using again exterior algebra Proposition 2.1.6 we define maps as in the previous section and get a diagram

$$\begin{array}{c}
\mathcal{S}(\mathfrak{n}) \coloneqq \left(\bigwedge^r H^1_{\mathcal{F}(\mathfrak{n})}(K, T/I_\mathfrak{n}T)\right) \otimes G_\mathfrak{n} \\
\Big\downarrow {\scriptstyle \widehat{\mathrm{loc}^{\mathrm{f}}_\mathfrak{q}} \otimes 1 =: \psi^e_\mathfrak{n}} \\
\mathcal{S}(e) \coloneqq H^1_{\mathrm{tr}}(K_\mathfrak{q}, T/I_{\mathfrak{nq}}T) \otimes \left(\bigwedge^{r-1} H^1_{\mathcal{F}_\mathfrak{q}(\mathfrak{n})}(K, T/I_{\mathfrak{nq}}T)\right) \otimes G_{\mathfrak{nq}} \\
\Big\uparrow {\scriptstyle \widehat{\mathrm{loc}^{\mathrm{tr}}_\mathfrak{q}} \otimes 1 =: \psi^e_{\mathfrak{nq}}} \\
\mathcal{S}(\mathfrak{nq}) \coloneqq \left(\bigwedge^r H^1_{\mathcal{F}(\mathfrak{nq})}(K, T/I_{\mathfrak{nq}}T)\right) \otimes G_{\mathfrak{nq}}
\end{array}$$

Definition 2.4.4. The *Selmer sheaf* $\mathcal{S}$ associated to $(T, \mathcal{F}, \mathcal{P})$ is the sheaf on $\mathcal{X}$ defined taking $\mathcal{S}(\mathfrak{n})$, $\mathcal{S}(\mathfrak{nq})$, $\mathcal{S}(e)$, $\psi^e_{\mathfrak{n}}$ and $\psi^e_{\mathfrak{nq}}$ as in the diagram above.

We can finally give the definition of Kolyvagin system:

Definition 2.4.5. A *Kolyvagin system of rank* r for $(T, \mathcal{F}, \mathcal{P})$ is a global section of $\mathcal{S}$, i.e. a collection

$$\{\kappa_{\mathfrak{n}} \in \mathcal{S}(\mathfrak{n}) \mid \mathfrak{n} \in \mathcal{N},\ \psi^e_{\mathfrak{n}}(\kappa_{\mathfrak{n}}) = \psi^e_{\mathfrak{nq}}(\kappa_{\mathfrak{nq}}) \in \mathcal{S}(e),\ \mathfrak{q} \text{ prime}\} \in \Gamma(\mathcal{S}).$$

We also write $\mathbf{KS}_r(T) = \mathbf{KS}_r(T, \mathcal{F}, \mathcal{P}) \coloneqq \Gamma(\mathcal{S})$ for the R-module of Kolyvagin systems.

Let now $R = \mathbb{Z}/p^k\mathbb{Z}$.

Definition 2.4.6. A vertex $\mathfrak{n} \in \mathcal{N}$ is a *core vertex* for T if $\lambda(\mathfrak{n}) \coloneqq \operatorname{len} H^1_{\mathcal{F}(\mathfrak{n})^D}(K, T^D) = 0$.

Proposition 2.4.7. The following are equivalent:

1. $\mathfrak{n}$ is a core vertex for T;
2. $H^1_{\mathcal{F}(\mathfrak{n})}(K, T)$ is a free R-module of rank $\chi(T)$;
3. $\mathcal{S}(\mathfrak{n})$ is a free R-module of rank 1;
4. $\mathfrak{n}$ is a core vertex for $T/\mathfrak{m}T$.

Proof. (1) $\iff$ (2) follows from Corollary 2.2.15.
(1) $\iff$ (4) follows from Proposition 2.2.13.2.
(2) $\iff$ (3) is easy to see. □

We define a subsheaf of $\mathcal{S}$. The definition is prompted by the following observation:

Proposition 2.4.8. If $\mathfrak{n}$, $\mathfrak{nq} \in \mathcal{N}$ and e is the edge joining them, then

$$\psi^e_{\mathfrak{n}}(\mathfrak{m}^{\lambda(\mathfrak{n})}\mathcal{S}(\mathfrak{n})) = \psi^e_{\mathfrak{nq}}(\mathfrak{m}^{\lambda(\mathfrak{nq})}\mathcal{S}(\mathfrak{nq})) \subset \mathcal{S}(e).$$

Proof. By definition of the maps and using exterior algebra Proposition 2.1.6, we have

$$\begin{aligned}\psi^e_{\mathfrak{n}}(\mathcal{S}(\mathfrak{n})) &= \operatorname{im}(\widehat{\operatorname{loc}^{\mathrm{f}}_{\mathfrak{q}}} \otimes 1) = \operatorname{im}(\varphi^{\mathrm{fs}}_{\mathfrak{q}}\operatorname{loc}_{\mathfrak{q}} \otimes 1) = \\ &= \varphi^{\mathrm{fs}}_{\mathfrak{q}}(\operatorname{loc}_{\mathfrak{q}} H^1_{\mathcal{F}(\mathfrak{n})}(K, T)) \otimes \textstyle\bigwedge^{r-1} H^1_{\mathcal{F}_{\mathfrak{q}}(\mathfrak{n})}(K, T) \otimes G_{\mathfrak{n}}\end{aligned}$$

$$\begin{aligned}\psi^e_{\mathfrak{nq}}(\mathcal{S}(\mathfrak{nq})) &= \operatorname{im}(\widehat{\operatorname{loc}^{\mathrm{tr}}_{\mathfrak{q}}} \otimes 1) = \operatorname{im}(\operatorname{loc}_{\mathfrak{q}} \otimes 1) = \\ &= \operatorname{loc}_{\mathfrak{q}} H^1_{\mathcal{F}(\mathfrak{nq})}(K, T) \otimes \textstyle\bigwedge^{r-1} H^1_{\mathcal{F}_{\mathfrak{q}}(\mathfrak{n})}(K, T) \otimes G_{\mathfrak{nq}}\end{aligned}$$

and by Lemma 2.2.12.3 we have

$$\mathfrak{m}^{\lambda(\mathfrak{n})}\varphi^{\mathrm{fs}}_{\mathfrak{q}}(\operatorname{loc}_{\mathfrak{q}} H^1_{\mathcal{F}(\mathfrak{n})}(K, T)) = \mathfrak{m}^{\lambda(\mathfrak{nq})}\operatorname{loc}_{\mathfrak{q}} H^1_{\mathcal{F}(\mathfrak{nq})}(K, T) \otimes G_{\mathfrak{q}}$$

and we conclude. □

Definition 2.4.9. The sheaf of *stub Selmer modules* is the subsheaf $\mathcal{S}' \subset \mathcal{S}$ defined by

$$\begin{aligned}\mathcal{S}'(\mathfrak{n}) :=& \mathfrak{m}^{\lambda(\mathfrak{n})}\mathcal{S}(\mathfrak{n}) \\ =& \mathfrak{m}^{\lambda(\mathfrak{n})}\left(\bigwedge^r H^1_{\mathcal{F}(\mathfrak{n})}(K,T)\right) \otimes G_{\mathfrak{n}} \subset \mathcal{S}(\mathfrak{n})\end{aligned}$$

and, taking their images through the vertex-to-edge maps, we define the modules for the edges

$$\mathcal{S}'(e) := \psi^e_{\mathfrak{n}}(\mathfrak{m}^{\lambda(\mathfrak{n})}\mathcal{S}(\mathfrak{n})) = \psi^e_{\mathfrak{nq}}(\mathfrak{m}^{\lambda(\mathfrak{nq})}\mathcal{S}(\mathfrak{nq})) \subset \mathcal{S}(e)$$

which is a good definition by the above proposition. The vertex-to-edge maps for $\mathcal{S}'$ are the restrictions of the $\psi^e_{\mathfrak{n}}$.

Definition 2.4.10. A *stub Kolyvagin system* is a global section of the sheaf $\mathcal{S}'$; the R-module of stub Kolyvagin systems is $\mathbf{KS}'_r(T) = \mathbf{KS}'_r(T,\mathcal{F},\mathcal{P}) := \Gamma(\mathcal{S}') \subset \mathbf{KS}_r(T)$.

We mention that, in the case of core rank $r = 1$, stub Kolyvagin systems and Kolyvagin systems are the same, that is, $\mathbf{KS}'_1(T) = \mathbf{KS}_1(T)$: see [MR04, Theorem 4.4.1].

Theorem 2.4.11. Let $(T,\mathcal{F},\mathcal{P})$ be Selmer data and $\mathcal{S}$ its associated Selmer sheaf on the graph $\mathcal{X}$. Then the following hold:

1. There are core vertices.
2. If $\mathfrak{n}$, $\mathfrak{n}'$ are core vertices, there is a path

$$\mathfrak{n} = \mathfrak{n}_0 \overset{e_1}{\text{———}} \mathfrak{n}_1 \overset{e_2}{\text{———}} \cdots \overset{e_t}{\text{———}} \mathfrak{n}_t = \mathfrak{n}'$$

   in $\mathcal{X}$ such that every $\mathfrak{n}_i$ is a core vertex and all the maps $\psi^{e_i}_{\mathfrak{n}_i}$, $\psi^{e_{i+1}}_{\mathfrak{n}_i}$ are isomorphisms.
3. The stub subsheaf $\mathcal{S}'$ is locally cyclic and every core vertex is a hub. For every $\mathfrak{n} \in \mathcal{N}$ there is a core vertex $\mathfrak{n}' \in \mathcal{N}$ divisible by $\mathfrak{n}$.

Proof. Let $\overline{T} := T/\mathfrak{m}T$ and $\overline{\lambda}$ be the correspondent of λ for $\overline{T}$.

To show that there are core vertices, we show more precisely that

- for every $\mathfrak{n} \in \mathcal{N}$ there is a coprime $\mathfrak{n}' \in \mathcal{N}$ such that $\nu(\mathfrak{n}') = \overline{\lambda}(\mathfrak{n})$ and $\mathfrak{nn}'$ is a core vertex.

If $\mathfrak{n}' \in \mathcal{N}$ is prime to $\mathfrak{n}$, then $\overline{\lambda}(\mathfrak{nn}') \geqslant \overline{\lambda}(\mathfrak{n}) - \nu(\mathfrak{n}')$. Construct a sequence $\mathfrak{n}_i \in \mathcal{N}$ such that $\mathfrak{n}_{i+1} = \mathfrak{n}_i\mathfrak{q}_i$ for some prime $\mathfrak{q}_i \in \mathcal{N}$ and $\overline{\lambda}(\mathfrak{n}_{i+1}) < \overline{\lambda}(\mathfrak{n}_i)$ (this can be done by the next point): then we reach a $\mathfrak{n}_d$ with $\overline{\lambda}(\mathfrak{n}_d) = 0$. Then $\mathfrak{n}_d$ is equivalently a core vertex for T (recall the equivalence in Proposition 2.4.7). Then we have $\overline{\lambda}(\mathfrak{nn}') = 0$ and consequently $\nu(\mathfrak{n}') \geqslant \overline{\lambda}(\mathfrak{n})$, so we have equality as required. Let us show that such a sequence can be constructed:

- if $\mathfrak{n} \in \mathcal{N}$ with $\lambda(\mathfrak{n},\overline{T}^D) > 0$, then there is $\mathfrak{q} \in \mathcal{P}$ prime to $\mathfrak{n}$ such that $\lambda(\mathfrak{nq},\overline{T}^D) < \lambda(\mathfrak{n},\overline{T}^D)$ and $\psi^e_{\mathfrak{n}}$ is an isomorphism where $e = \{\mathfrak{n},\mathfrak{nq}\}$.

By the Cebotarev density theorem we may choose $\mathfrak{q} \in \mathcal{P}$ such that the localization maps

$$\mathfrak{m}^{k-1}H^1_{\mathcal{F}(\mathfrak{n})}(K,T) \to H^1_{\mathrm{f}}(K_{\mathfrak{q}},T) \qquad H^1_{\mathcal{F}(\mathfrak{n})^D}(K,T^D)[\mathfrak{m}] \to H^1_{\mathrm{f}}(K_{\mathfrak{q}},T^D)$$

are non-zero. Then we have $\overline{\lambda}(\mathfrak{n}\mathfrak{q}) < \overline{\lambda}(\mathfrak{n})$ by Poitou-Tate global duality (Lemma 2.2.12.4). The localization $H^1_{\mathcal{F}(\mathfrak{n})}(K,T) \to H^1_{\mathrm{f}}(K_\mathfrak{q},T)$ is surjective, so

$$\widehat{\mathrm{loc}_\mathfrak{q}}\colon \bigwedge^r H^1_{\mathcal{F}(\mathfrak{n})}(K,T) \to H^1_{\mathrm{f}}(K_\mathfrak{q},T) \otimes \left(\bigwedge^{r-1} H^1_{\mathcal{F}_\mathfrak{q}(\mathfrak{n})}(K,T)\right)$$

is also surjective. Looking at the definition of $\mathcal{S}'(e)$, we deduce then that

$$\mathcal{S}'(e) = \mathfrak{m}^{\lambda(\mathfrak{n})} H^1_{\mathrm{tr}}(K_\mathfrak{q},T) \otimes \left(\bigwedge^{r-1} H^1_{\mathcal{F}_\mathfrak{q}(\mathfrak{n})}(K,T)\right) \otimes G_{\mathfrak{n}\mathfrak{q}},$$

and therefore $\mathrm{len}_R(\mathcal{S}'(e)) \geqslant k - \lambda(\mathfrak{n}) = \mathrm{len}_R(\mathcal{S}'(\mathfrak{n}))$ where the last equality follows from Corollary 2.2.15.3 Since the map $\mathcal{S}'(\mathfrak{n}) \to \mathcal{S}'(e)$ is surjective, it must therefore be an isomorphism.

- If $\mathfrak{n}$, $\mathfrak{n}'$ are core vertices, there is a path

$$\mathfrak{n} = \mathfrak{n}_0 \overset{e_1}{\text{———}} \mathfrak{n}_1 \overset{e_2}{\text{———}} \cdots \overset{e_t}{\text{———}} \mathfrak{n}_t = \mathfrak{n}'$$

  in $\mathcal{X}$ such that every $\mathfrak{n}_i$ is a core vertex and all the maps $\psi^{e_i}_{\mathfrak{n}_i}$, $\psi^{e_{i+1}}_{\mathfrak{n}_i}$ are isomorphisms.

The case for core rank 1 is proved in [MR04, Theorem 4.3.12]; the case for general core rank can be done in the same way, or by induction as in [MR16, Theorem 14.4].

- $\mathcal{S}'$ is locally cyclic and every core vertex is a hub.

By Corollary 2.2.15.3, $\mathcal{S}'(\mathfrak{n})$ is a cyclic R-module for every $\mathfrak{n} \in \mathcal{N}$. By definition of $\mathcal{S}'$, the maps $\psi^e_\mathfrak{n}$ are surjective, so the $\mathcal{S}'(e)$ are also cyclic.

Let $\mathfrak{n}_0$ be a core vertex and $\mathfrak{n} \in \mathcal{N}$ be any other vertex. Let us show by induction on $\overline{\lambda}(\mathfrak{n})$ that the two vertices are joined by a surjective path in $\mathcal{S}'$. If $\overline{\lambda}(\mathfrak{n}) = 0$ then $\mathfrak{n}$ is also a core vertex and we know the claim is true. If $\overline{\lambda}(\mathfrak{n}) > 0$, we may find $\mathfrak{q} \in \mathcal{P}$ not dividing $\mathfrak{n}$ such that $\overline{\lambda}(\mathfrak{n}\mathfrak{q}) < \overline{\lambda}(\mathfrak{n})$ and $\psi^{\{\mathfrak{n},\mathfrak{n}\mathfrak{q}\}}_\mathfrak{n}$ is an isomorphism. By the inductive hypothesis there is a surjective path from $\mathfrak{n}_0$ to $\mathfrak{n}\mathfrak{q}$; adjoining it to the edge $\{\mathfrak{n},\mathfrak{n}\mathfrak{q}\}$ we get the desired path.

□

Theorem 2.4.12.

1. $\mathbf{KS}'_r(T)$ is free of rank 1 over R. For every core vertex $\mathfrak{n}$, the specialization map

$$\begin{aligned} \mathbf{KS}'_r(T) &\to \mathcal{S}'(\mathfrak{n}) = \left(\bigwedge^r H^1_{\mathcal{F}(\mathfrak{n})}(K,T)\right) \otimes G_\mathfrak{n} \\ \kappa = (\kappa_\mathfrak{n})_\mathfrak{n} &\mapsto \kappa_\mathfrak{n} \end{aligned}$$

   is an isomorphism.

2. There is a (stub) Kolyvagin system $\kappa \in \mathbf{KS}'_r(T)$ such that $\kappa_\mathfrak{n}$ generates $\mathcal{S}'(\mathfrak{n})$ for every $\mathfrak{n} \in \mathcal{N}$.

3. $\mathcal{S}'$ has trivial monodromy.

Proof. By the previous theorem, every core vertex is a hub and the sheaf is locally cyclic, so we may apply Proposition 2.4.2. □

We say that $\kappa \in \mathbf{KS}'_r(T)$ is *primitive* if it generates $\mathbf{KS}'_r(T)$ as an R-module, or equivalently if $\kappa_\mathfrak{n}$ generates $\mathcal{S}'(\mathfrak{n})$ for every $\mathfrak{n}$; such elements exist by the above theorem. We can now state and prove the following bounds for the length of Selmer groups.

Theorem 2.4.13. Suppose $R = \mathbb{Z}/p^k\mathbb{Z}$ and let $\kappa \in \mathbf{KS}'_r(T)$; then:

1. if $\kappa_1 \neq 0$, then
$$\operatorname{len} H^1_{\mathcal{F}^D}(K, T^D) \leqslant k - \operatorname{len} R\kappa_1 = \max\{i \mid \kappa_1 \in \mathfrak{m}^i \textstyle\bigwedge^r H^1_{\mathcal{F}}(K,T)\};$$
2. if κ is primitive and $\kappa_1 \neq 0$, equality holds in 1;
3. if κ is primitive and $\kappa_1 = 0$, then $\operatorname{len} H^1_{\mathcal{F}^D}(K, T^D) \geqslant k$.

Proof. We recall that by definition $\lambda(1) = \operatorname{len} H^1_{\mathcal{F}^D}(K, T^D)$. By definition and using Corollary 2.2.15.3,
$$\kappa_1 \in \mathcal{S}'(1) \coloneqq \mathfrak{m}^{\lambda(1)} \textstyle\bigwedge^r H^1_{\mathcal{F}}(K,T) \cong \mathfrak{m}^{\lambda(1)}$$
is cyclic of length $\max\{0, k - \lambda(1)\}$, which is $k - \lambda(1)$ if $\kappa_1 \neq 0$ (since otherwise we would have $\mathcal{S}'(1) = 0$ hence $\kappa_1 = 0$). Therefore,
$$\operatorname{len}(R\kappa_1) \leqslant \operatorname{len}(\mathcal{S}'(1)) = k - \lambda(1)$$
proving (1). If moreover κ is primitive then $\mathcal{S}'(1) = R\kappa_1$ so we have equality in the above, proving (2).

On the other hand, if κ is primitive and $\kappa_1 = 0$ then $\mathcal{S}'(1) = R\kappa_1 = 0$, hence
$$0 = \operatorname{len}(R\kappa_1) = \operatorname{len}(\mathcal{S}'(1)) = \max\{0, k - \lambda(1)\} \geqslant k - \lambda(1).$$

□

We now show how to build a correspondence between Stark systems and stub Kolyvagin systems. Let $R = \mathbb{Z}/p^k\mathbb{Z}$ and consider the following cartesian diagram:
$$\begin{array}{ccc} H^1_{\mathcal{F}(\mathfrak{n})}(K,T) & \hookrightarrow & H^1_{\mathcal{F}^{\mathfrak{n}}}(K,T) \\ \downarrow & & \downarrow{\scriptstyle \oplus \mathrm{loc}_{\mathfrak{q}}^{\mathrm{f}}} \\ 0 & \hookrightarrow & \displaystyle\bigoplus_{\mathfrak{q}\mid\mathfrak{n}} H^1_{\mathrm{tr}}(K_{\mathfrak{q}},T) \otimes G_{\mathfrak{q}} \end{array}$$

Using Proposition 2.1.6, this diagram yields a map
$$\textstyle\bigwedge^{r+\nu(\mathfrak{n})} H^1_{\mathcal{F}^{\mathfrak{n}}}(K,T) \otimes \bigwedge^{\nu(\mathfrak{n})} \operatorname{Hom}\Big(\bigoplus_{\mathfrak{q}\mid\mathfrak{n}} H^1_{\mathrm{tr}}(K_{\mathfrak{q}},T) \otimes G_{\mathfrak{q}}, R\Big)$$
$$\downarrow$$
$$\textstyle\bigwedge^r H^1_{\mathcal{F}(\mathfrak{n})}(K,T)$$

and, tensoring both sides with $G_{\mathfrak{n}}$, we get a map
$$\Pi_{\mathfrak{n}} \colon Y_{\mathfrak{n}} \to \mathcal{S}'(\mathfrak{n}) = \textstyle\bigwedge^r H^1_{\mathcal{F}(\mathfrak{n})}(K,T) \otimes G_{\mathfrak{n}}.$$

The next theorem, whose technical proof we omit, describes the desired correspondence:

Theorem 2.4.14. Let $\varepsilon \in \mathbf{SS}_r(T)$ and define

$$\Pi(\varepsilon) \coloneqq \{(-1)^{\nu(\mathfrak{n})}\Pi_{\mathfrak{n}}(\varepsilon_{\mathfrak{n}}) \mid \mathfrak{n} \in \mathcal{N}\}.$$

Then:

1. $\Pi(\varepsilon) \in \mathbf{KS}'_r(T)$.
2. The resulting R-module morphism $\Pi\colon \mathbf{SS}_r(T) \to \mathbf{KS}'_r(T)$ is an isomorphism.

Proof. [MR16, 12.2, 12.3, 12.4]. □

2.4.3 The DVR case

In this paragraph we obtain results in the case $R = \mathbb{Z}_p$ analogous to the previous section, replacing Stark systems by (stub) Kolyvagin systems. We begin with the following theorem, analogous to Theorem 2.3.11.

Theorem 2.4.15.

1. $T \twoheadrightarrow T/\mathfrak{m}^k T$ and $\mathcal{P}_k \hookrightarrow \mathcal{P}$ induce an isomorphism
$$\mathbf{KS}'_r(T, \mathcal{P}) \xrightarrow{\sim} \varprojlim \mathbf{KS}'_r(T/\mathfrak{m}^k T, \mathcal{P}_k).$$
2. $\mathbf{KS}'_r(T, \mathcal{P})$ is free of rank 1 over R, generated by a Kolyvagin system κ whose image in $\mathbf{KS}'_r(T/\mathfrak{m}T)$ is non-zero.
3. The maps $\mathbf{KS}'_r(T, \mathcal{P}) \to \mathbf{KS}'_r(T/\mathfrak{m}^k T, \mathcal{P}_k)$ are surjective.

Proof. By Theorem 2.4.12, stub Kolyvagin systems are free of rank 1 in the case of finite R, so the proof can be done directly as for Stark systems, Theorem 2.3.11. □

We can use this correspondence to prove replace Stark systems with stub Kolyvagin systems. Define the following objects, in complete analogy with the Stark system case:

- $\varphi_\kappa(\mathfrak{n}) \coloneqq \max\{j \mid \kappa_{\mathfrak{n}} \in \mathfrak{m}^j \bigwedge^r H^1_{\mathcal{F}(\mathfrak{n})}(K, T)\}$ for $\kappa \in \mathbf{KS}_r(T)$;
- the previously defined operator ∂,
$$\left(f\colon \mathcal{N} \to \mathbb{N} \cup \{\infty\}\right) \mapsto \begin{pmatrix} \partial f\colon \mathbb{N} \to \mathbb{N} \cup \{\infty\} \\ \qquad i \mapsto \min\{f(\mathfrak{n}) \mid \mathfrak{n} \in \mathcal{N},\ \nu(\mathfrak{n}) = i\} \end{pmatrix}$$
- $\operatorname{ord}(\kappa) \coloneqq \min\{\nu(\mathfrak{n}) \mid \mathfrak{n} \in \mathcal{N},\ \kappa_{\mathfrak{n}} \neq 0\} = \min\{i \mid \partial\varphi_\kappa(i) \neq \infty\}$;
- $d_\kappa(i) \coloneqq \partial\varphi_\kappa(i) - \partial\varphi_\kappa(i+1)$ for $i \geqslant \operatorname{ord}(\kappa)$.

The following proposition states that the invariants defined above for a stub Kolyvagin system are the same as the invariants for the corresponding Stark system.

Proposition 2.4.16. Let $\kappa \in \mathbf{KS}'_r(T)$, $\varepsilon \in \mathbf{SS}_r(T)$ and $\kappa = \Pi(\varepsilon)$. Then:

$$\operatorname{ord}(\kappa) = \operatorname{ord}(\varepsilon) \qquad \partial\varphi_\kappa(i) = \partial\varphi_\varepsilon(i) \qquad d_\kappa(i) = d_\varepsilon(i)$$

for all i.

Proof. Let us first consider $R = \mathbb{Z}/p^k\mathbb{Z}$; if κ generates $\mathbf{KS}'_r(T)$ and ε generates $\mathbf{SS}_r(T)$, then we know $\kappa_{\mathfrak{n}}$ generates $\mathfrak{m}^{\lambda(\mathfrak{n})}\mathcal{S}(\mathfrak{n})$ and $\varepsilon_{\mathfrak{n}}$ generates $\mathfrak{m}^{\mu(\mathfrak{n})}Y_{\mathfrak{n}}$. Therefore:

$$\partial\varphi_\kappa(i) = \begin{cases} \partial\lambda(i) & \text{if } \partial\lambda(i) < k \\ \infty & \text{if } \partial\lambda(i) \geqslant k \end{cases} \qquad \partial\varphi_\varepsilon(i) = \begin{cases} \partial\mu(i) & \text{if } \partial\mu(i) < k \\ \infty & \text{if } \partial\mu(i) \geqslant k \end{cases}$$

By the computation of $\partial\lambda$ and $\partial\mu$ (Proposition 2.3.6), we know $\partial\lambda(i) = \partial\mu(i)$ and the theorem follows. For $R = \mathbb{Z}_p$, the proof follows as for Stark systems (Proposition 2.3.12). □

By recalling Theorem 2.3.13 for Stark systems and using the isomorphism Π and the above property concerning invariants, we immediately get the analogous result for stub Kolyvagin systems:

Theorem 2.4.17. Let $R = \mathbb{Z}_p$, $\kappa \in \mathbf{KS}'_r(T)$, $\kappa \neq 0$. Then:

1. There are sequences
$$\partial\varphi_\kappa(0) \geqslant \partial\varphi_\kappa(1) \geqslant \partial\varphi_\kappa(2) \geqslant \cdots \geqslant 0$$
$$d_\kappa(0) \geqslant d_\kappa(1) \geqslant d_\kappa(2) \geqslant \cdots \geqslant 0$$
whose terms are finite for $t \geqslant \operatorname{ord}(\kappa)$.

2. There is an isomorphism
$$\frac{H^1_{\mathcal{F}^D}(K, T^D)}{H^1_{\mathcal{F}^D}(K, T^D)_{\mathrm{div}}} \cong \bigoplus_{i \geqslant \operatorname{ord}(\kappa)} R/\mathfrak{m}^{d_\kappa(i)}$$

3. Setting $\partial\varphi_\kappa(\infty) := \lim_{t\to\infty} \partial\varphi_\kappa(t)$,
$$\operatorname{len}\left(\frac{H^1_{\mathcal{F}^D}(K, T^D)}{H^1_{\mathcal{F}^D}(K, T^D)_{\mathrm{div}}}\right) = \partial\varphi_\kappa(\operatorname{ord}\kappa) - \partial\varphi_\kappa(\infty)$$

4. $\operatorname{len} H^1_{\mathcal{F}^D}(K, T^D) < \infty$ if and only if $\kappa_1 \neq 0$.

5. $\operatorname{len} H^1_{\mathcal{F}^D}(K, T^D) \leqslant \partial\varphi_\kappa(0) = \max\{s \mid \kappa_1 \in \mathfrak{m}^s \bigwedge^r H^1_{\mathcal{F}}(K, T)\}$ and equality holds if and only if κ is primitive.

Proof. By Theorem 2.3.13 we can prove the result for the corresponding $\varepsilon \in \mathbf{SS}_r(T)$. By the previous proposition, the same result holds for κ. □

Bibliography

[BD07] M. Bertolini and H. Darmon. *Derived heights and generalized Mazur-Tate regulators.* 2007.

[Bro04] M.L. Brown. *Heegner Points and Elliptic Curves.* Springer, 2004.

[Cas62] J.W.S. Cassels. Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung. *Journal für die reine und angewandte Mathematik, 211*, 1962.

[CF67] J.W.S. Cassels and A. Fröhlich. *Algebraic Number Theory.* Academic Press, 1967.

[Gre10] R. Greenberg. Selmer groups and congruences. *Proceedings of the International Congress of Mathematicians*, 2010.

[Gro57] A. Grothendieck. Sur quelques points d'algèbre homologique. *Tohoku Math. Journal, Vol. 9, No. 2*, 1957.

[Mat55] A. Mattuck. Abelian varieties over p-adic ground fields. *Annals of Mathematics, Jul. 1955, Vol. 62, No. 1. Mathematics Department, Princeton University*, 1955.

[Mil20] J.S. Milne. *Arithmetic Duality Theorems. Third Edition.* 2020.

[MR04] B. Mazur and K. Rubin. *Kolyvagin Systems.* Mem. Amer. Math. Soc. 168, 2004.

[MR16] B. Mazur and K. Rubin. *Controlling Selmer groups in the higher core rank case.* Journal de Théorie des Nombres de Bordeaux, 2016.

[Neu93] J. Neukirch. *Cohomology of Number Fields.* Springer-Verlag, 1993.

[Neu99] J. Neukirch. *Algebraic Number Theory.* Springer-Verlag, 1999.

[Oor66] F. Oort. *Commutative Group Schemes.* Springer, 1966.

[Ser67] J.-P. Serre. Local class field theory. *Algebraic Number Theory by J.W.S. Cassels and A. Fröhlich*, 1967.

[Ser70] J.-P. Serre. *Linear Representations of Finite Groups.* Springer, 1970.

[Ser80] J.-P. Serre. *Local Fields.* Springer, 1980.

[Sil09] J. H. Silverman. *The Arithmetic of Elliptic Curves.* Springer, 2009.

[Tat62] J. Tate. Duality theorems in galois cohomology over number fields. *Proc. Intern. Congress Math.*, 1962.

[Tat67] J. T. Tate. Global class field theory. *Algebraic Number Theory by J.W.S. Cassels and A. Fröhlich*, 1967.

Versicherung an Eides statt

Ich, Marco Morosin; via Ravizza 14, 35136 Padova, Italien; Matrikelnummer 3117425

versichere an Eides statt durch meine Unterschrift, dass ich die vorstehende Arbeit selbständig und ohne fremde Hilfe angefertigt und alle Stellen, die ich wörtlich oder annähernd wörtlich aus Veröffentlichungen entnommen habe, als solche kenntlich gemacht habe, mich auch keiner anderen als der angegebenen Literatur oder sonstiger Hilfsmittel bedient habe.

Ich versichere an Eides Statt, dass ich die vorgenannten Angaben nach bestem Wissen und Gewissen gemacht habe und dass die Angaben der Wahrheit entsprechen und ich nichts verschwiegen habe.

Die Strafbarkeit einer falschen eidesstattlichen Versicherung ist mir bekannt, namentlich die Strafandrohung gemäß § 156 StGB bis zu drei Jahren Freiheitsstrafe oder Geldstrafe bei vorsätzlicher Begehung der Tat bzw. gemäß § 161 Abs.1 StGB bis zu einem Jahr Freiheitsstrafe oder Geldstrafe bei fahrlässiger Begehung.

Ort, Datum

Unterschrift (Marco Morosin)