SELMER COMPLEXES

(Final version, March 2007, to appear in Astérisque)

Jan Nekovář

0. Introduction

(0.0) Big Galois representations

In this work we study cohomological invariants of "big Galois representations"

$$\rho : G \longrightarrow \mathrm{Aut}_R(T),$$

where

(i) G is a suitable Galois group.
(ii) R is a complete local noetherian ring, with a finite residue field of characteristic p.
(iii) T is an R-module of finite type.
(iv) ρ is a continuous homomorphism of pro-finite groups.

We develop a general machinery that covers duality theory, Iwasawa theory, generalized Cassels-Tate pairings and generalized height pairings.

(0.1) Examples

(0.1.0) An archetypal example of a big Galois representation arises as follows. Let K be a field of characteristic $char(K) \neq p$. For every K-scheme $X \longrightarrow \mathrm{Spec}(K)$ put $\overline{X} = X \otimes_K K^{sep}$, where K^{sep} is a fixed separable closure of K. Given a projective system $X_\infty = (X_\alpha)_{\alpha \in I}$ (indexed by some directed set I) of separated K-schemes of finite type with *finite* transition morphisms $X_\beta \longrightarrow X_\alpha$, put

$$H^i(X_\infty) := \varprojlim_\alpha H^i_{et}(\overline{X}_\alpha, \mathbf{Z}_p) = \varprojlim_\alpha \varprojlim_n H^i_{et}(\overline{X}_\alpha, \mathbf{Z}/p^n\mathbf{Z}),$$

where the transition morphisms are given by trace maps. This is a representation of $G_K = \mathrm{Gal}(K^{sep}/K)$, linear over the $\mathbf{Z}_p$-algebra generated by "endomorphisms" of the tower X_∞. In practice, $H^i(X_\infty)$ is often too big and must be first decomposed into smaller constituents. One can also use more general coefficient sheaves, not just $\mathbf{Z}/p^n\mathbf{Z}$.

(0.1.1) Iwasawa theory. Let K_∞/K be a Galois extension (contained in K^{sep}) with $\Gamma = \mathrm{Gal}(K_\infty/K)$ isomorphic to $\mathbf{Z}_p^r$ for some $r \geq 1$. Write $K_\infty = \bigcup K_\alpha$ as a union of finite extensions of K. For a fixed separated K-scheme of finite type $X \longrightarrow \mathrm{Spec}(K)$, consider the projective system $X_\alpha = X \otimes_K K_\alpha$. In this case

$$H^i(X_\infty) \xrightarrow{\sim} H^i_{et}(\overline{X}, \mathbf{Z}_p) \otimes_{\mathbf{Z}_p} \Lambda,$$

where

$$\Lambda = \mathbf{Z}_p[[\Gamma]] \xrightarrow{\sim} \mathbf{Z}_p[[X_1, \ldots, X_r]]$$

is the Iwasawa algebra of Γ and G_K acts on Λ by the tautological character

$$\chi_\Gamma : G_K \twoheadrightarrow \Gamma \hookrightarrow \Lambda^*$$

(or its inverse, depending on the sign conventions). Thus $T = H^i(X_\infty)$ is a big Galois representation of $G = G_K$ over $R = \Lambda$.

(0.1.2) Hida theory. Let $N \geq 1$ be an integer not divisible by p (and such that $Np > 4$). Let X_∞ be the projective system of modular curves [(1)]

[(1)] There are two choices of transition morphisms; see e.g. [N-P] for more details.

$$X_1(Np) \longleftarrow \cdots \longleftarrow X_1(Np^r) \longleftarrow X_1(Np^{r+1}) \longleftarrow \cdots$$

over $K = \mathbf{Q}$. The tower X_∞ has many endomorphisms, namely Hecke correspondences.

The Galois module $H^1(X_\infty)$ is too big, but its *ordinary part* $H^1(X_\infty)^{ord}$, defined as the maximal $\mathbf{Z}_p$-submodule on which the Hecke operator [(2)] $T(p)$ is invertible, is of finite type over the *ordinary Hecke algebra* $\mathfrak{h}^{ord}$, defined as the projective limit of the ordinary parts of the $\mathbf{Z}_p$-Hecke algebras acting on $S_2(\Gamma_1(Np^r))$ (for variable r).

The ring $\mathfrak{h}^{ord}$ is semilocal, in fact finite and free over $\Lambda = \mathbf{Z}_p[[\Gamma]] \xrightarrow{\sim} \mathbf{Z}_p[[X]]$, where $\Gamma = 1 + p\mathbf{Z}_p$ (resp., $\Gamma = 1 + 4\mathbf{Z}_2$, if $p = 2$) acts on X_∞ by diamond operators. If we fix a maximal ideal $\mathfrak{m} \subset \mathfrak{h}^{ord}$, then $T = H^1(X_\infty)^{ord}_{\mathfrak{m}}$ is a big Galois representation of $G = G_{\mathbf{Q}}$ over $R = \mathfrak{h}^{ord}_{\mathfrak{m}}$.

(0.1.3) One can, of course, combine the constructions in 0.1.1-2.

(0.2) Selmer groups

In the case when K is a number field and the projective system X_∞ has good reduction (i.e. each X_α has) outside a finite set S of places of K containing all places above p, then $H^i(X_\infty)$ is a representation of the Galois group with restricted ramification $G_{K,S} = \mathrm{Gal}(K_S/K)$, where K_S is the maximal extension of K which is unramified outside S.

In general, given a big Galois representation T of $G_{K,S}$, the main objects of interest are the following:

(i) (continuous) Galois cohomology groups $H^i_{\mathrm{cont}}(G_{K,S}, T)$.

(ii) Selmer groups

$$Sel(G_{K,S}, T) \subset H^1_{\mathrm{cont}}(G_{K,S}, T),$$

consisting of elements satisfying suitable local conditions in $H^1_{\mathrm{cont}}(G_v, T)$ for $v \in S$ (where $G_v = \mathrm{Gal}(\overline{K}_v/K_v)$).

Similar objects were first considered by R. Greenberg [Gre 4] as a natural generalization of Iwasawa theory. Greenberg expressed hope that there should be a variant of the Main Conjecture of Iwasawa theory in this context, i.e. a relation between the “characteristic power series” of a big Selmer group and an appropriate p-adic L-function.

A big Galois representation ρ can be viewed as a family of “usual” Galois representations $\rho_\lambda : G_{K,S} \longrightarrow GL_n(\mathbf{Z}_p)$, which depends analytically on the parameter λ. One of the main motivations of the present work was to develop a homological machinery that would control the variation of the Selmer groups attached to the individual ρ_λ's as a function of λ. A statement such as the Main Conjecture for T should then imply a relation between the Selmer group of ρ_λ and the special value at λ of the p-adic L-function in question.

(0.3) Big vs. finite Galois representations

Every big Galois representation $\rho : G \longrightarrow \mathrm{Aut}_R(T)$ is the projective limit of Galois representations $\rho_n : G \longrightarrow \mathrm{Aut}_R(T/\mathfrak{m}^n T)$ with finite targets. Using known properties of ρ_n one can sometimes pass to the limit and deduce results valid for ρ.

Consider, for example, a representation $\rho : G_K \longrightarrow \mathrm{Aut}_R(T)$ of $G_K = \mathrm{Gal}(K^{sep}/K)$ for a local field K (with finite residue field) of characteristic $char(K) \neq p$. Writing D for the Pontrjagin dual functor

$$D(-) = \mathrm{Hom}_{\mathrm{cont}}(-, \mathbf{R}/\mathbf{Z}),$$

Tate's local duality states that the (finite) cohomology groups

$$H^i(G_K, T/\mathfrak{m}^n T) \overset{D}{\longleftrightarrow} H^{2-i}(G_K, D(T/\mathfrak{m}^n T)(1))$$

are Pontrjagin duals of each other. Taking projective limit one obtains Pontrjagin duality between a compact and a discrete R-module

$$H^i(G_K, T) \overset{D}{\longleftrightarrow} H^{2-i}(G_K, D(T)(1)),$$

where

---

(2) Again, there are two choices of $T(p)$; which one is correct depends on the choice made in (1).

$$H^i(G_K, T) = H^i_{\mathrm{cont}}(G_K, T) = \varprojlim_n H^i(G_K, T/\mathfrak{m}^n T).$$

(0.4) Compact vs. discrete modules

Attentive readers will have noticed that Greenberg [Gre 2-4] considers Selmer groups for discrete Galois modules, while our T is compact. Let us investigate the relationship between discrete and compact Galois representations more closely. In fact, understanding the interplay between discrete and compact modules is at the basis of the whole theory developed in this work.

Let us first consider the "classical" case of $R = \mathbf{Z}_p$. Given a representation

$$\rho : G \longrightarrow \mathrm{Aut}_{\mathbf{Z}_p}(T),$$

where T is free of finite rank over $\mathbf{Z}_p$, there are three more representations of G attached to T, namely

$$A = T \otimes_{\mathbf{Z}_p} \mathbf{Q}_p/\mathbf{Z}_p, \qquad T^* = \mathrm{Hom}_{\mathbf{Z}_p}(T, \mathbf{Z}_p) = D(A), \qquad A^* = T^* \otimes_{\mathbf{Z}_p} \mathbf{Q}_p/\mathbf{Z}_p = D(T). \tag{0.4.1}$$

They can be arranged into the following diagram:

$$\begin{tikzcd} T \arrow[rr, leftrightarrow, "\mathscr{D}"] \arrow[d, "\Phi"] \arrow[drr] & & T^* \arrow[d, "\Phi"] \arrow[dll, "D"'] \\ A & & A^* \end{tikzcd} \tag{0.4.2}$$

Here $\mathscr{D}(-) = \mathrm{Hom}_{\mathbf{Z}_p}(-, \mathbf{Z}_p)$ and $\Phi(-) = (-) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p/\mathbf{Z}_p$.

What is the analogue of this construction for general R (or even for $R = \mathbf{Z}_p$ if T is not free over $\mathbf{Z}_p$)? Let us temporarily ignore the action of G and consider this question only for R-modules. For $R = \mathbf{Z}_p$, the tensor product

$$T \otimes_{\mathbf{Z}_p} \mathbf{Q}_p/\mathbf{Z}_p$$

loses any information about the torsion submodule $T_{\mathrm{tors}} \subset T$. On the other hand,

$$T_{\mathrm{tors}} \xrightarrow{\sim} \mathrm{Tor}_1^{\mathbf{Z}_p}(T, \mathbf{Q}_p/\mathbf{Z}_p).$$

This suggests that one should consider the derived tensor product

$$A = T \overset{\mathbf{L}}{\otimes}_{\mathbf{Z}_p} \mathbf{Q}_p/\mathbf{Z}_p$$

as a correct version of (0.4.1). In concrete terms, $\mathbf{Q}_p/\mathbf{Z}_p$ has a natural flat resolution

$$[\mathbf{Z}_p \longrightarrow \mathbf{Q}_p] \tag{0.4.3}$$

(in degrees $-1, 0$) and A is represented by the complex

$$T \otimes_{\mathbf{Z}_p} [\mathbf{Z}_p \longrightarrow \mathbf{Q}_p] = \left[T \longrightarrow T \otimes_{\mathbf{Z}_p} \mathbf{Q}_p\right],$$

again in degrees $-1, 0$.

What is the analogue of (0.4.3) for general R? Fix a system of parameters of R, i.e. elements $x_1, \ldots, x_d \in \mathfrak{m}$ (where $d = \dim(R)$) such that $\dim(R/(x_1, \ldots, x_d)) = 0$. An analogue of (0.4.3) is then given by the complex

$$C^\bullet = C^\bullet(R, (x_i)) = \left[R \longrightarrow \bigoplus_i R_{x_i} \longrightarrow \bigoplus_{i<j} R_{x_i x_j} \longrightarrow \cdots \longrightarrow R_{x_1 \cdots x_d} \right]$$

in degrees $[-d, 0]$, with standard "Čech differentials". This complex depends on the chosen system of parameters. In order to remove this ambiguity it is necessary to consider $C^\bullet$ as an object of the (bounded) derived category $D^b({}_R\mathrm{Mod})$. In more rigorous terms, if (y_j) is another system of parameters of R, then there is a canonical isomorphism

$$R \xrightarrow{\sim} \mathrm{Hom}_{D^b({}_R\mathrm{Mod})}(C^\bullet(R, (x_i)), C^\bullet(R, (y_j))).$$

Given $T \in D_{ft}({}_R\mathrm{Mod})$, we then define

$$A = \Phi(T) = T \overset{\mathbf{L}}{\otimes}_R C^\bullet = T \otimes_R C^\bullet$$

(for the last equality note that $C^\bullet$ is a complex of flat R-modules).
The Pontrjagin dual of R

$$I = D(R)$$

is an injective hull of the (finite) residue field $k = R/\mathfrak{m}$; we abandon our earlier convention about D and instead define

$$D(M) = \mathrm{Hom}_R(M, I)$$

for every R-module M. This functor coincides with Pontrjagin dual for noetherian (hence compact) or artinian (hence discrete) R-modules.
We have, so far, defined analogues of the vertical and diagonal arrows in the diagram (0.4.2). What about the horizontal arrow? A derived version of the adjunction isomorphism

$$\mathrm{adj} : \mathbf{R}\mathrm{Hom}_R(X \overset{\mathbf{L}}{\otimes}_R Y, Z) \xrightarrow{\sim} \mathbf{R}\mathrm{Hom}_R(X, \mathbf{R}\mathrm{Hom}_R(Y, Z)),$$

applied to $X = T$, $Y = C^\bullet$, $Z = I$, shows that

$$D \circ \Phi(-) \xrightarrow{\sim} \mathbf{R}\mathrm{Hom}_R(-, D(C^\bullet)).$$

The object of $D^b({}_R\mathrm{Mod})$ represented by the complex

$$D(C^\bullet)$$

is known as the *dualizing complex* $\omega \in D^b_{ft}({}_R\mathrm{Mod})$ and the functor

$$\mathscr{D}(-) = \mathbf{R}\mathrm{Hom}_R(-, \omega)$$

as Grothendieck's dual (if $R = \mathbf{Z}_p$, then $\omega = \mathbf{Z}_p$).
To sum up, a general version of (0.4.2) is given by the following "duality diagram"

$$\begin{tikzcd}
T \arrow[rr, leftrightarrow, "\mathscr{D}"] \arrow[d, "\Phi"] \arrow[drr, leftrightarrow] & & T^* \arrow[d, "\Phi"] \arrow[dll, leftrightarrow, "D"'] \\
A & & A^*
\end{tikzcd} \tag{0.4.4}$$

with $T, T^* \in D_{ft}({}_R\mathrm{Mod})$, $A, A^* \in D_{coft}({}_R\mathrm{Mod})$,

$$\begin{aligned}
D(-) &= \mathrm{Hom}_R(-, I) \\
\mathscr{D}(-) &= \mathbf{R}\mathrm{Hom}_R(-, \omega) \\
\Phi(-) &= (-) \overset{\mathbf{L}}{\otimes}_R D(\omega).
\end{aligned}$$

Commutativity of this diagram (up to canonical isomorphisms) is equivalent to three duality theorems: Matlis duality ($\mathrm{id} \xrightarrow{\sim} D \circ D$), Grothendieck duality ($\mathrm{id} \xrightarrow{\sim} \mathscr{D} \circ \mathscr{D}$) and local duality ($\mathscr{D} \xrightarrow{\sim} D \circ \Phi$ together with the isomorphism $\Phi[-d] \xrightarrow{\sim} \mathbf{R}\Gamma_{\{\mathfrak{m}\}}$).

The diagram (0.4.4) gives rise to a spectral sequence

$$E_2^{i,j} = \mathbb{E}\mathrm{xt}^i_R(D(H^j(A)), \omega) = \mathbb{E}\mathrm{xt}^i_R(H^{-j}(T^*), \omega) \Longrightarrow H^{i+j}(\mathscr{D}(T^*)) = H^{i+j}(T). \tag{0.4.5}$$

(0.5) (Ind-)admissible $R[G]$-modules

In order to incorporate the Galois action into the diagram (0.4.4), it is necessary to enlarge the category of Galois modules we consider. For example, $T \otimes_R C^\bullet$ has components of the form

$$T \otimes_R R_x = \varinjlim_n [T \xrightarrow{x} T \xrightarrow{x} T \xrightarrow{x} \cdots] = \bigcup_{n \geq 1} T \otimes_R \{\frac{r}{x^n} \mid r \in R\}.$$

This suggests that we should consider $R[G]$-modules M satisfying the following condition (which makes sense for any topological group G):

Axiom 1. *$M = \bigcup M_\alpha$, where $M_\alpha \subset M$ are $R[G]$-submodules of M, which are of finite type over R and such that the map $G \longrightarrow \mathrm{Aut}_R(M_\alpha)$ is continuous (with respect to the pro-finite topology on the target).*

As

$$D(\bigoplus_\alpha M_\alpha) = \prod_\alpha D(M_\alpha),$$

there are cases when Axiom 1 is satisfied by M, but not by $D(M)$. For this reason we impose an additional, purely algebraic, condition:

Axiom 2. $\mathrm{Im}(R[G] \longrightarrow \mathrm{End}_R(M))$ *is an R-module of finite type.*

An $R[G]$-module satisfying (Axiom 1) and (Axiom 2) (resp., only (Axiom 1)) will be called *admissible* (resp., *ind-admissible*). Admissible modules form a full subcategory $({}^{ad}_{R[G]}\mathrm{Mod})$ of $({}_{R[G]}\mathrm{Mod})$, which is stable under subquotients, finite direct sums, tensor products and internal Hom's. In particular, if T is admissible, so is $T \otimes_R R_x$, for every $x \in R$.
The duality diagram

$$\begin{tikzcd} T \arrow[rr, leftrightarrow, "\mathscr{D}"] \arrow[d, "\Phi"] \arrow[drr] & & T^* \arrow[d, "\Phi"] \arrow[dll, "D"'] \\ A & & A^* \end{tikzcd} \tag{0.5.1}$$

then makes sense for $T, T^* \in D_{R-ft}({}^{ad}_{R[G]}\mathrm{Mod})$, $A, A^* \in D_{R-coft}({}^{ad}_{R[G]}\mathrm{Mod})$.

(0.6) Continuous cohomology

For an admissible $R[G]$-module M we define the complex of continuous (non-homogeneous) cochains of G with values in M as

$$C^\bullet_{\mathrm{cont}}(G, M) = \varinjlim_\alpha C^\bullet_{\mathrm{cont}}(G, M_\alpha) = \varinjlim_\alpha \varprojlim_n C^\bullet_{\mathrm{cont}}(G, M_\alpha/\mathfrak{m}^n M_\alpha),$$

where each $M_\alpha/\mathfrak{m}^n M_\alpha$ has discrete topology. The functor $M \mapsto C^\bullet_{\mathrm{cont}}(G, M)$ gives rise to an exact functor

$$\mathbf{R}\Gamma_{\mathrm{cont}}(G, -) : D^*({}^{ad}_{R[G]}\mathrm{Mod}) \longrightarrow D^*({}_R\mathrm{Mod})$$

for $* = +$ (resp., for $* = +, b$, if G is a pro-finite group satisfying $cd_p(G) < \infty$). In fact, this construction requires only (Axiom 1), and so it makes sense for ind-admissible modules.

In the situation of (0.5.1), the functor $\mathbf{R}\Gamma_{\rm cont}(G,-)$ commutes with Φ (up to a canonical isomorphism). For $R = \mathbf{Z}_p$ this statement boils down to the fact that there exists a long cohomology sequence of continuous G-cohomology atttached to

$$0 \longrightarrow T \longrightarrow V \longrightarrow A \longrightarrow 0,$$

where $V = T \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$.

(0.7) Duality for Galois cohomology

The machinery behind the duality diagram (0.5.1) makes the passage from finite to big Galois representations very easy. As we have seen in 0.3, classical duality results for finite Galois modules imply a duality with respect to D, while compatibility of $\mathbf{R}\Gamma_{\rm cont}(G,-)$ with Φ is automatic; combining the two facts we obtain a duality with respect to $\mathscr{D}$. The final outcome (cf. Chapter 5) is the following:

(0.7.0) Duality over local fields (Tate). Let K be a local field (with finite residue field) of characteristic $char(K) \neq p$ and $G = G_K$. If $T, T^* \in D^b_{R-ft}({}^{ad}_{R[G_K]}\mathrm{Mod})$ and $A, A^* \in D^b_{R-coft}({}^{ad}_{R[G_K]}\mathrm{Mod})$ are related as in (0.5.1), then the four objects of $D^b_{(co)ft}({}_R\mathrm{Mod})$ in the diagram

$$\begin{tikzcd}
\mathbf{R}\Gamma_{\rm cont}(G_K,T) \arrow[r, leftrightarrow, "\mathscr{D}"] \arrow[d, "\Phi"] \arrow[dr, leftrightarrow] & \mathbf{R}\Gamma_{\rm cont}(G_K,T^*(1))[2] \arrow[d, "\Phi"] \arrow[dl, leftrightarrow, "D"'] \\
\mathbf{R}\Gamma_{\rm cont}(G_K,A) & \mathbf{R}\Gamma_{\rm cont}(G_K,A^*(1))[2]
\end{tikzcd}$$

are related as in (0.4.4).

(0.7.1) Duality over global fields (Poitou - Tate). Let K be a global field of characteristic $char(K) \neq p$ and S a finite set of primes of K containing all primes above p and all archimedean primes of K. If $p = 2$, assume for simplicity that K has no real prime (otherwise one would have to consider also Tate cohomology groups at real primes). Denote by S_f the set of all non-archimedean primes in S; for $v \in S_f$ put $G_v = G_{K_v}$ and fix an embedding $\overline{K} \hookrightarrow \overline{K}_v$. Set $G_{K,S} = \mathrm{Gal}(K_S/K)$, where K_S the maximal extension of K unramified outside S. For every admissible $G_{K,S}$-module M define the complex of continuous cochains with compact support by [(3)]

$$C^\bullet_{c,\rm cont}(G_{K,S},M) = \mathrm{Cone}\left(C^\bullet_{\rm cont}(G_{K,S},M) \longrightarrow \bigoplus_{v\in S_f} C^\bullet_{\rm cont}(G_v,M) \right)[-1].$$

This defines an exact functor

$$\mathbf{R}\Gamma_{c,\rm cont}(G_{K,S},-) : D^*({}^{ad}_{R[G_{K,S}]}\mathrm{Mod}) \longrightarrow D^*({}_R\mathrm{Mod})$$

($* = +, b$). If $T, T^* \in D^b_{R-ft}({}^{ad}_{R[G_{K,S}]}\mathrm{Mod})$ and $A, A^* \in D^b_{R-coft}({}^{ad}_{R[G_{K,S}]}\mathrm{Mod})$ are related as in (0.5.1) (for $G = G_{K,S}$), then the objects of $D^b_{(co)ft}({}_R\mathrm{Mod})$ in the diagram

$$\begin{tikzcd}
\mathbf{R}\Gamma_{\rm cont}(G_{K,S},T) \arrow[r, leftrightarrow, "\mathscr{D}"] \arrow[d, "\Phi"] \arrow[dr, leftrightarrow] & \mathbf{R}\Gamma_{c,\rm cont}(G_{K,S},T^*(1))[3] \arrow[d, "\Phi"] \arrow[dl, leftrightarrow, "D"'] \\
\mathbf{R}\Gamma_{\rm cont}(G_{K,S},A) & \mathbf{R}\Gamma_{c,\rm cont}(G_{K,S},A^*(1))[3]
\end{tikzcd}$$

are related as in (0.4.4).

(0.7.2) As in (0.4.5), the previous diagram gives rise to the following spectral sequences:

(3) This differs from the cochains with compact support as defined by Kato [Ka 1]. Our definition makes the duality theorem work, while Kato's definition, which incorporates cochains at all infinite places, gives rise to objects naturally related to "zeta elements".

$$E_2^{i,j} = \mathbb{E}\mathrm{xt}^i_R(H^{3-j}_{c,\mathrm{cont}}(G_{K,S}, T^*(1)), \omega) = \mathbb{E}\mathrm{xt}^i_R(D(H^j_{\mathrm{cont}}(G_{K,S}, A)), \omega) \Longrightarrow H^{i+j}_{\mathrm{cont}}(G_{K,S}, T)$$
$$'E_2^{i,j} = \mathbb{E}\mathrm{xt}^i_R(H^{3-j}_{\mathrm{cont}}(G_{K,S}, T^*(1)), \omega) = \mathbb{E}\mathrm{xt}^i_R(D(H^j_{c,\mathrm{cont}}(G_{K,S}, A)), \omega) \Longrightarrow H^{i+j}_{c,\mathrm{cont}}(G_{K,S}, T).$$

(0.8) Selmer complexes

Let us keep the notation of 0.7.1. Selmer groups have been traditionally defined as subgroups of elements of $H^1(G_{K,S}, -)$ satisfying suitable local conditions in $H^1(G_v, -)$ (for $v \in S$). In our approach we have no choice but to impose local conditions on the level of complexes, rather than cohomology.

(0.8.0) Let T, T^*, A, A^* be bounded complexes of admissible $R[G_{K,S}]$-modules, which are related in the derived category as in (0.5.1). *Local conditions* for any $X \in \{T, A, T^*(1), A^*(1)\}$ are given by a collection $\Delta(X) = (\Delta_v(X))_{v \in S_f}$, where each $\Delta_v(X)$ is a morphism of complexes of R-modules

$$i_v^+(X) : U_v^+(X) \longrightarrow C^\bullet_{\mathrm{cont}}(G_v, X),$$

with $U_v^+(X)$ satisfying appropriate finiteness conditions.

The *Selmer complex* attached to the local conditions $\Delta(X)$ is defined as the total complex

$$\mathrm{Tot}\begin{pmatrix} C^\bullet_{\mathrm{cont}}(G_{K,S}, X) & \longrightarrow & \bigoplus_{v\in S_f} C^\bullet_{\mathrm{cont}}(G_v, X) \\ & & \uparrow \\ & & \bigoplus_{v \in S_f} U_v^+(X) \end{pmatrix}.$$

The corresponding object of the derived category will be denoted by

$$\widetilde{\mathbf{R}\Gamma}_f(X) = \widetilde{\mathbf{R}\Gamma}_f(G_{K,S}, X; \Delta(X)) \in D_*({}_R\mathrm{Mod}), \qquad * = \begin{cases} ft, & X = T, T^*(1) \\ coft, & X = A, A^*(1) \end{cases}$$

and its cohomology by $\widetilde{H}^i_f(X) = \widetilde{H}^i_f(G_{K,S}, X; \Delta(X))$. If we put

$$U_v^-(X) = \mathrm{Cone}\left(U_v^+(X) \longrightarrow C^\bullet_{\mathrm{cont}}(G_v, X)\right),$$

then the exact triangle

$$\widetilde{\mathbf{R}\Gamma}_f(X) \longrightarrow \mathbf{R}\Gamma_{\mathrm{cont}}(G_{K,S}, X) \longrightarrow \bigoplus_{v \in S_f} U_v^-(X)$$

gives rise to a long exact sequence

$$\cdots \longrightarrow \bigoplus_{v\in S_f} H^{i-1}(U_v^-(X)) \longrightarrow \widetilde{H}^i_f(X) \longrightarrow H^i_{\mathrm{cont}}(G_{K,S}, X) \longrightarrow \bigoplus_{v \in S_f} H^i(U_v^-(X)) \longrightarrow \cdots \qquad (0.8.0.1)$$

In particular, the canonical map

$$\widetilde{H}^1_f(X) \longrightarrow H^1_{\mathrm{cont}}(G_{K,S}, X)$$

need not be injective.

(0.8.1) In the present work we consider only *Greenberg's local conditions*, defined as follows (these are the only local conditions that can be handled by elementary methods; the general case would require a heavy dose of crystalline machinery, which is not yet available). Fix a subset $\Sigma \subset S_f$ containing all primes above p and put $\Sigma' = S_f - \Sigma$.

(i) For $v \in \Sigma$, assume that we are given a morphism of complexes of admissible $R[G_v]$-modules $X_v^+ \longrightarrow X$; put

$$U_v^+(X) = C^\bullet_{\mathrm{cont}}(G_v, X_v^+).$$

(ii) For $v \in \Sigma'$ we take the "unramified local conditions"

$$U_v^+(X) = C^\bullet_{ur}(G_v, X).$$

Morally, these should defined as

$$\text{“}C^\bullet_{\mathrm{cont}}(G_v/I_v, \tau_{\leq 0}\, C^\bullet_{\mathrm{cont}}(I_v, X)) \longrightarrow C^\bullet_{\mathrm{cont}}(G_v/I_v, C^\bullet_{\mathrm{cont}}(I_v, X)) \xrightarrow{\sim} C^\bullet_{\mathrm{cont}}(G_v, X)\text{”},$$

where $I_v \subset G_v$ is the inertia subgroup. Unfortunately, there does not seem to be a satisfactory general formalism of the Hochschild-Serre spectral sequence for continuous cohomology. As a result, we define $C^\bullet_{ur}$ by explicit formulas. For example, if $X = X^0$ is concentrated in degree zero, then

$$C^\bullet_{ur}(G_v, X) = C^\bullet_{\mathrm{cont}}(G_v/I_v, (X^0)^{I_v})$$

is quasi-isomorphic to the complex

$$\big[(X^0)^{I_v} \xrightarrow{f_v - 1} (X^0)^{I_v}\big]$$

in degrees $0, 1$; here $f_v \in G_v/I_v$ denotes the geometric Frobenius element.

(0.9) Duality for Selmer complexes

In order to obtain a duality result similar to 0.7.1 for various $\widetilde{\mathbf{R}\Gamma}_f(X)$, it is necessary to impose suitable "orthogonality constraints" on the local conditions. For example, we require, for all $v \in S_f$, the composite morphism of complexes

$$U_v^-(X) \longrightarrow C^\bullet_{\mathrm{cont}}(G_v, X) \xrightarrow{\alpha} D(C^\bullet_{\mathrm{cont}}(G_v, D(X)(1)))[-2] \longrightarrow D(U_v^+(D(X)(1)))[-2]$$

(in which the map α underlies Tate's local duality) to be a quasi-isomorphism.

For Greenberg's local conditions 0.8.1, this follows from a suitable orthogonality of X_v^+ and $D(X)(1)_v^+$. This implies that the following pairs of Selmer complexes are related by Pontrjagin duality:

$$\begin{aligned} \widetilde{\mathbf{R}\Gamma}_f(T) &\xleftrightarrow{\;D\;} \widetilde{\mathbf{R}\Gamma}_f(A^*(1))[3] \\ \widetilde{\mathbf{R}\Gamma}_f(A) &\xleftrightarrow{\;D\;} \widetilde{\mathbf{R}\Gamma}_f(T^*(1))[3] \end{aligned} \tag{0.9.1}$$

In general, (0.9.1) cannot be completed to a full duality diagram

$$\begin{tikzcd} \widetilde{\mathbf{R}\Gamma}_f(T) \arrow[r, leftrightarrow, "\mathscr{D}"] \arrow[d, "\Phi"] \arrow[dr, leftrightarrow, "D"] & \widetilde{\mathbf{R}\Gamma}_f(T^*(1))[3] \arrow[d, "\Phi"] \arrow[dl, leftrightarrow] \\ \widetilde{\mathbf{R}\Gamma}_f(A) & \widetilde{\mathbf{R}\Gamma}_f(A^*(1))[3], \end{tikzcd} \tag{0.9.2}$$

as the local conditions need not be compatible with respect to Φ. In other words, there is an exact (= distinguished) triangle

$$\Phi(U_v^+(T)) \longrightarrow U_v^+(A) \longrightarrow \mathrm{Err}_v(\Phi, T)$$

involving an "error term" $\mathrm{Err}_v(\Phi, T)$, which leads to another exact triangle

$$\Phi(\widetilde{\mathbf{R}\Gamma}_f(T)) \longrightarrow \widetilde{\mathbf{R}\Gamma}_f(A) \longrightarrow \bigoplus_{v \in S_f} \mathrm{Err}_v(\Phi, T).$$

For Greenberg's local conditions 0.8.1 we have $\mathrm{Err}_v(\Phi, T) = 0$ for $v \in \Sigma$, but not for $v \in \Sigma'$, in general. For example, assume that $R = \mathbf{Z}_p$ and T is a free $\mathbf{Z}_p$-module of finite rank, concentrated in degree zero. As before, $A = V/T$ for $V = T \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. The unramified local conditions at $v \in \Sigma'$ are quasi-isomorphic to

$$U_v^+(X) = \left[X^{I_v} \xrightarrow{f_v - 1} X^{I_v}\right] \qquad\qquad (X = T, A),$$

hence $\Phi(U_v^+(T))$ is quasi-isomorphic to

$$\left[V^{I_v}/T^{I_v} \xrightarrow{f_v-1} V^{I_v}/T^{I_v}\right] = \left[(A^{I_v})_{\mathrm{div}} \xrightarrow{f_v-1} (A^{I_v})_{\mathrm{div}}\right].$$

It follows that $\mathrm{Err}_v(\Phi, T)$ is quasi-isomorphic to

$$\left[(A^{I_v})/(A^{I_v})_{\mathrm{div}} \xrightarrow{f_v-1} (A^{I_v})/(A^{I_v})_{\mathrm{div}}\right] = \left[H^1(I_v, T)_{\mathrm{tors}} \xrightarrow{f_v-1} H^1(I_v, T)_{\mathrm{tors}}\right].$$

The cohomology groups of $\mathrm{Err}_v(\Phi, T)$ are finite groups of common order

$$|H^0(\mathrm{Err}_v(\Phi, T))| = |H^1(\mathrm{Err}_v(\Phi, T))| = |H^1(I_v, T)_{\mathrm{tors}}^{f_v=1}|,$$

equal to the "local Tamagawa factor" of T at $v \in \Sigma'$, which appears in the formulation of the Bloch-Kato conjecture in the language of [Fo-PR] (this is a generalization of the "fudge factors" in the conjecture of Birch and Swinnerton-Dyer).

Similarly, there is an error term for the horizontal arrow $\mathscr{D}$ in (0.9.2). Under a suitable boundedness hypothesis, the arrow corresponds to a cup product

$$\widetilde{\mathbf{R}\Gamma}_f(T) \overset{\mathbf{L}}{\otimes}_R \widetilde{\mathbf{R}\Gamma}_f(T^*(1)) \longrightarrow \omega[-3]. \tag{0.9.3}$$

(0.10) Comparison with classical Selmer groups

Let E be an elliptic curve over $\mathbf{Q}$, with good reduction outside a finite set of primes $S \supset \{p, \infty\}$. The classical p-power descent on E gives rise to Selmer groups

$$Sel(G_{\mathbf{Q},S}, -) \subset H^1(G_{\mathbf{Q},S}, -)$$

(for $- = T = T_p(E)$ or $- = A = E[p^\infty]$), sitting in exact sequences

$$0 \longrightarrow E(\mathbf{Q}) \otimes \mathbf{Z}_p \longrightarrow Sel(G_{\mathbf{Q},S}, T) \longrightarrow T_p\text{Ш}(E/\mathbf{Q}) \longrightarrow 0$$
$$0 \longrightarrow E(\mathbf{Q}) \otimes \mathbf{Q}_p/\mathbf{Z}_p \longrightarrow Sel(G_{\mathbf{Q},S}, A) \longrightarrow \text{Ш}(E/\mathbf{Q})[p^\infty] \longrightarrow 0.$$

We also use the notation

$$Sel(G_{\mathbf{Q},S}, V) = Sel(G_{\mathbf{Q},S}, T) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$$

for $V = V_p(E) = T_p(E) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$.

Assume that E has *ordinary reduction* [(4)] at p and, for simplicity, that $p \neq 2$. As a representation of $G_p = G_{\mathbf{Q}_p}$, the Tate module T is reducible. There is an exact sequence of $\mathbf{Z}_p[G_p]$-modules

$$0 \longrightarrow T_p^+ \longrightarrow T \longrightarrow T_p^- \longrightarrow 0,$$

in which each $T_p^\pm$ is free of rank 1 over $\mathbf{Z}_p$ and I_p acts trivially on T_p^- (i.e. T_p^- is unramified). Consider Greenberg's local conditions for T, given by

$$U_v^+(T) = \begin{cases} C^\bullet_{\mathrm{cont}}(G_p, T_p^+), & v = p \\ C^\bullet_{\mathrm{cont}}(G_v/I_v, T^{I_v}), & v \in S_f,\ v \neq p. \end{cases}$$

One deduces from (0.8.0.1) an exact sequence (cf. 9.6.3,7)

$$0 \longrightarrow H^0(G_p, T_p^-) \longrightarrow \widetilde{H}^1_f(T) \longrightarrow Sel(G_{\mathbf{Q},S}, T) \longrightarrow C \longrightarrow 0,$$

(4) I.e. either good ordinary or multiplicative reduction.

in which C is a finite group and

$$H^0(G_p, T_p^-) = \begin{cases} \mathbf{Z}_p, & \text{if } E \text{ has split multiplicative reduction at } p \\ 0, & \text{otherwise.} \end{cases}$$

In other words, $\widetilde{H}_f^1(T)$ is an "extended Selmer group" in the sense of Mazur, Tate and Teitelbaum [M-T-T] and the term $H^0(G_p, T_p^-)$ detects the presence of a "trivial zero" of the p-adic L-function of E. This is one of the simplest instances of the following general principle: classical Selmer groups correspond to complex L-functions, while Selmer complexes to p-adic L-functions.

(0.11) Iwasawa theory

The formalism of big Galois representations greatly simplifies Iwasawa theory. Let K be a number field and S as in 0.7.1. Assume that we are given an intermediate Galois extension $K \subset K_\infty \subset K_S$ with $\Gamma = \mathrm{Gal}(K_\infty/K) \xrightarrow{\sim} \mathbf{Z}_p^r$ for some $r \geq 1$ (in fact, one can treat in the same way also "tame Iwasawa theory", when $\Gamma \xrightarrow{\sim} \mathbf{Z}_p^r \times \Delta$, for a finite abelian group Δ). Put $G = G_{K,S}$.

Writing $K_\infty = \bigcup K_\alpha$ as a union of finite extensions of K, we define the Iwasawa algebra of Γ over R as

$$\overline{R} = R[[\Gamma]] = \varprojlim_\alpha R[\mathrm{Gal}(K_\alpha/K)].$$

As in the classical case ($R = \mathbf{Z}_p$), any choice of an isomorphism $\Gamma \xrightarrow{\sim} \mathbf{Z}_p^r$ gives an isomorphism of R-algebras

$$\overline{R} \xrightarrow{\sim} R[[X_1, \ldots, X_r]].$$

We denote by

$$\chi_\Gamma : G \twoheadrightarrow \Gamma \hookrightarrow R[\Gamma]^*$$

the tautological character of G and by

$$\iota : \overline{R} \longrightarrow \overline{R}$$

the R-linear involution satisfying $\iota(\gamma) = \gamma^{-1}$ for all $\gamma \in \Gamma$.

If M is an $\overline{R}[G]$-module and $n \in \mathbf{Z}$, we define $\overline{R}[G]$-modules $M < n >$ and M^ι by requiring that

(i) $M < n >= M$ as an $\overline{R}$-module; $g \in G$ acts by

$$g_{M<n>} = \chi_\Gamma(g)^n g_M.$$

(ii) $M^\iota = M$ as an $R[G]$-module; $\gamma \in \Gamma$ acts by

$$\gamma_{M^\iota} = \iota(\gamma)_M = (\gamma^{-1})_M.$$

(0.12) Duality for Galois cohomology in Iwasawa theory

The main point is that cohomology of R-representations over K_∞ can be expressed in terms of cohomology of $\overline{R}$-representations over K (cf. [Gre 4], Prop. 3.2; [Col], Prop. 2).

Let T, T^* (resp., A, A^*) be bounded complexes of admissible $R[G]$-modules, of finite (resp., co-finite) type over R. In Iwasawa theory one is often interested in the cohomology groups

$$H^i_{\mathrm{Iw}}(K_\infty/K, T) = \varprojlim_\alpha H^i_{\mathrm{cont}}(\mathrm{Gal}(K_S/K_\alpha), T)$$
$$H^i(K_S/K_\infty, A) = \varinjlim_\alpha H^i_{\mathrm{cont}}(\mathrm{Gal}(K_S/K_\alpha), A)$$

(and their counterparts with compact support). An easy application of Shapiro's Lemma (cf. Sect. 8.3 and 8.4) shows that these are the cohomology groups of the following objects of $D({}_{\overline{R}}\mathrm{Mod})$:

$$\begin{aligned}\mathbf{R}\Gamma_{\mathrm{Iw}}(K_\infty/K,T) &= \mathbf{R}\Gamma_{\mathrm{cont}}(G_{K,S},\mathscr{F}_\Gamma(T))\\ \mathbf{R}\Gamma(K_S/K_\infty,A) &= \mathbf{R}\Gamma_{\mathrm{cont}}(G_{K,S},F_\Gamma(A)),\end{aligned}$$

where

$$\begin{aligned}\mathscr{F}_\Gamma(T) &= (T\otimes_R \overline{R}) < -1 >\\ F_\Gamma(A) &= \mathrm{Hom}_{R,\mathrm{cont}}(\overline{R},A) < -1 >\end{aligned}$$

(and similarly for cohomology with compact support).

The crucial observation (cf. 8.4.6.6) is the following: if T, T^*, A, A^* are related (over R) as in (0.5.1), then $\mathscr{F}_\Gamma(T), \mathscr{F}_\Gamma(T^*)$, $F_\Gamma(A), F_\Gamma(A^*)$ are related by the duality diagram

$$\begin{tikzcd} \mathscr{F}_\Gamma(T) \arrow[r, leftrightarrow, "\overline{\mathscr{D}}"] \arrow[d, "\overline{\Phi}"] \arrow[dr, leftrightarrow] & \mathscr{F}_\Gamma(T^*)^\iota \arrow[d, "\overline{\Phi}"] \arrow[dl, leftrightarrow, "\overline{D}"'] \\ F_\Gamma(A) & F_\Gamma(A^*)^\iota \end{tikzcd} \tag{0.12.1}$$

over $\overline{R}$ (here we use the notation $\overline{\mathscr{D}}(-) = \mathbf{R}\mathrm{Hom}_{\overline{R}}(-,\omega_{\overline{R}})$, and similarly for $\overline{\Phi}$ and $\overline{D}$).

Applying the Poitou-Tate duality 0.7.1 (over $\overline{R}$) to (0.12.1), we obtain a duality diagram in $D({}_{\overline{R}}\mathrm{Mod})$

$$\begin{tikzcd} \mathbf{R}\Gamma_{\mathrm{Iw}}(K_\infty/K,T) \arrow[r, leftrightarrow, "\overline{\mathscr{D}}"] \arrow[d, "\overline{\Phi}"] \arrow[dr, leftrightarrow] & \mathbf{R}\Gamma_{c,\mathrm{Iw}}(K_\infty/K,T^*(1))^\iota[3] \arrow[d, "\overline{\Phi}"] \arrow[dl, leftrightarrow, "\overline{D}"'] \\ \mathbf{R}\Gamma(K_S/K_\infty,A) & \mathbf{R}\Gamma_c(K_S/K_\infty,A^*(1))^\iota[3] \end{tikzcd} \tag{0.12.2}$$

and spectral sequences

$$\begin{aligned} E_2^{i,j} &= \mathbb{E}\mathrm{xt}^i_{\overline{R}}(\overline{D}(H^j(K_S/K_\infty,A)),\omega_{\overline{R}}) = \mathbb{E}\mathrm{xt}^i_{\overline{R}}(H^{3-j}_{c,\mathrm{Iw}}(K_\infty/K,T^*(1)),\omega_{\overline{R}})^\iota \Longrightarrow H^{i+j}_{\mathrm{Iw}}(K_\infty/K,T)\\ {}'E_2^{i,j} &= \mathbb{E}\mathrm{xt}^i_{\overline{R}}(\overline{D}(H^j_c(K_S/K_\infty,A)),\omega_{\overline{R}}) = \mathbb{E}\mathrm{xt}^i_{\overline{R}}(H^{3-j}_{\mathrm{Iw}}(K_\infty/K,T^*(1)),\omega_{\overline{R}})^\iota \Longrightarrow H^{i+j}_{c,\mathrm{Iw}}(K_\infty/K,T).\end{aligned} \tag{0.12.3}$$

In the classical case $R=\mathbf{Z}_p$ the ring $\overline{R}=\mathbf{Z}_p[[\Gamma]]=\Lambda$ is the usual Iwasawa algebra. The spectral sequence

$$E_2^{i,j} = \mathrm{Ext}^i_{\overline{R}}(\overline{D}(H^j(K_S/K_\infty,A)),\Lambda) \Longrightarrow H^{i+j}_{\mathrm{Iw}}(K_\infty/K,T)$$

was in this case constructed in an unpublished note of Jannsen [Ja 3] (who also considered the case of non-commutative Γ).

Back to the general case, recall that an $\overline{R}$-module M is *pseudo-null* if it is finitely generated and its support $\mathrm{supp}(M)$ has codimension ≥ 2 in $\mathrm{Spec}(\overline{R})$. As $\mathrm{codim}_{\overline{R}}(\mathrm{supp}(E_2^{i,j}))\geq i$, the spectral sequence E_r degenerates in the quotient category $({}_{\overline{R}}\mathrm{Mod})/(pseudo-null)$ into short exact sequences

$$0\longrightarrow E_2^{1,n-1}\longrightarrow H^n_{\mathrm{Iw}}(K_\infty/K,T)\longrightarrow E_2^{0,n}\longrightarrow 0,$$

in which $E_2^{0,n}$ has no $\overline{R}$-torsion and $E_2^{1,n-1}$ has support in codimension ≥ 1.

(0.13) Duality for Selmer complexes in Iwasawa theory

Given suitably compatible systems of local conditions $U_v^+(X)$ along the tower of fields $\{K_\alpha\}$, one can define Selmer complexes

$$\widetilde{\mathbf{R}\Gamma}_{f,\mathrm{Iw}}(K_\infty/K,X),\qquad \widetilde{\mathbf{R}\Gamma}_f(K_S/K_\infty,Y)\qquad\qquad (X=T,T^*(1),Y=A,A^*(1)).$$

Although over each finite layer K_α the diagram (0.9.2) may involve non-zero error terms, the limit of these error terms over K_∞ is very often pseudo-null (or co-pseudo-null).

For example, Greenberg's local conditions 0.8.1 induce similar local conditions over each K_α. If we assume that no prime $v \in \Sigma'$ splits completely in K_∞/K, then (cf. 8.9.9)

$$\begin{tikzcd} \widetilde{\mathbf{R}\Gamma}_{f,\mathrm{Iw}}(K_\infty/K,T) \arrow[rr, leftrightarrow, "\overline{\mathscr{D}}"] \arrow[d, "\overline{\Phi}"] \arrow[drr] & & \widetilde{\mathbf{R}\Gamma}_{f,\mathrm{Iw}}(K_\infty/K,T^*(1))^\iota[3] \arrow[d, "\overline{\Phi}"] \arrow[dll, "\overline{D}"'] \\ \widetilde{\mathbf{R}\Gamma}_f(K_S/K_\infty,A) \arrow[urr] & & \widetilde{\mathbf{R}\Gamma}_f(K_S/K_\infty,A^*(1))^\iota[3] \arrow[ull] \end{tikzcd} \qquad (0.13.1)$$

becomes a duality diagram without any error terms, if we consider the top (resp., bottom) two objects in $D_{ft}((_{\overline{R}}\mathrm{Mod})/(pseudo-null))$ (resp., in $D_{coft}((_{\overline{R}}\mathrm{Mod})/(co-pseudo-null))$). Equivalently, for every prime ideal $\overline{\mathfrak{p}} \in \mathrm{Spec}(\overline{R})$ of height $ht(\overline{\mathfrak{p}}) = 1$, the localization of (0.13.1) at $\overline{\mathfrak{p}}$ is a duality diagram in $D(_{\overline{R}_{\overline{\mathfrak{p}}}}\mathrm{Mod})$. As in 0.12, this leads to exact sequences of $\overline{R}_{\overline{\mathfrak{p}}}$-modules

$$0 \longrightarrow \mathrm{Ext}^1_{\overline{R}}(\widetilde{H}^{4-q}_{f,\mathrm{Iw}}(K_\infty/K,T^*(1)),\omega_{\overline{R}})^\iota_{\overline{\mathfrak{p}}} \longrightarrow \widetilde{H}^q_{f,\mathrm{Iw}}(K_\infty/K,T)_{\overline{\mathfrak{p}}} \longrightarrow \mathrm{Hom}_{\overline{R}}(\widetilde{H}^{3-q}_{f,\mathrm{Iw}}(K_\infty/K,T^*(1)),\omega_{\overline{R}})^\iota_{\overline{\mathfrak{p}}} \longrightarrow 0, \qquad (0.13.2)$$

in which $X^\iota_{\overline{\mathfrak{p}}}$ is a shorthand for $(X^\iota)_{\overline{\mathfrak{p}}}$ and

$$\widetilde{H}^q_{f,\mathrm{Iw}}(K_\infty/K,T^*(1)) \xrightarrow{\sim} \overline{D}(\widetilde{H}^{3-q}_f(K_S/K_\infty,A)^\iota)$$

(and similarly for T and $A^*(1)$). If R has no embedded primes, then we obtain isomorphisms

$$\widetilde{H}^q_{f,\mathrm{Iw}}(K_\infty/K,T)_{\overline{R}-\mathrm{tors}} \xrightarrow{\sim} \mathrm{Ext}^1_{\overline{R}}(\widetilde{H}^{4-q}_{f,\mathrm{Iw}}(K_\infty/K,T^*(1)),\omega_{\overline{R}})^\iota$$

in $(_{\overline{R}}\mathrm{Mod})/(pseudo-null)$.

If there is a prime $v \in \Sigma'$ that splits completely in K_∞/K, then the above statements hold for those prime ideals $\overline{\mathfrak{p}} \in \mathrm{Spec}(\overline{R})$ of height $ht(\overline{\mathfrak{p}}) = 1$ which are not of the form $\overline{\mathfrak{p}} = \mathfrak{p}\overline{R}$, where $\mathfrak{p} \in \mathrm{Spec}(R)$ has $ht(\mathfrak{p}) = 1$ (cf. 8.9.8).

In particular, if R is regular and no prime $v \in \Sigma'$ splits completely in K_∞/K, then the $\overline{R}$-modules

$$(\overline{D}(\widetilde{H}^1_f(K_S/K_\infty,A)))_{\mathrm{tors}} \quad \text{and} \quad (\overline{D}(\widetilde{H}^1_f(K_S/K_\infty,A^*(1))))^\iota_{\mathrm{tors}}$$

are pseudo-isomorphic. This is a generalization of Greenberg's results ([Gre 2], Thm. 2; [Gre 3], Thm. 1), according to which for $R = \mathbf{Z}_p$ and K_∞/K the cyclotomic $\mathbf{Z}_p$-extension [(5)] the two Λ-modules in question have the same characteristic power series (more precisely, Greenberg works with his "strict Selmer groups" $S^{\mathrm{str}}_A(K_\infty)$ and $S^{\mathrm{str}}_{A^*(1)}(K_\infty)$; their relation to our $\widetilde{H}^1_f$ is explained in 9.6). A similar result for Selmer groups of abelian varieties defined in terms of flat cohomology was proved by Wingberg [Win].

If the complex $T = \sigma_{\leq 0}T$ is concentrated in non-positive degrees, then one can say much more: the horizontal arrow in (0.13.1) becomes an isomorphism after tensoring with $R_\mathfrak{q}$, for any minimal prime $\mathfrak{q}$ of R (8.9.11-12).

Greenberg [Gre 2] also defined "non-strict" Selmer groups $S_A \supseteq S^{\mathrm{str}}_A$. One of their interesting features is the fact that a trivial zero over K can sometimes be detected by the Λ-module $S_A(K_\infty)$ (but *not* by the Selmer group $S_A(K)$ over K). Although the Pontrjagin duals of $S_A(K_\infty)$ and $\widetilde{H}^1_f(K_S/K_\infty,A)$ may often have the same characteristic power series, they need not be isomorphic as Λ-modules, as $S^{\mathrm{str}}_A(K_\infty)$ is a subgroup of $S_A(K_\infty)$, but a quotient of $\widetilde{H}^1_f(K_S/K_\infty,A)$ (cf. 9.6.2-6). It seems that in the presence of a trivial zero $\widetilde{H}^1_f(K_S/K_\infty,A)$ has better semi-simplicity properties than $S_A(K_\infty)$.

(0.14) Classical Iwasawa theory

(0.14.0) Traditionally, the main objects of interest in Iwasawa theory have been the following:

---

(5) And assuming, in addition, that both $\overline{D}(\widetilde{H}^1_f(K_S/K_\infty,A))$ and $\overline{D}(\widetilde{H}^1_f(K_S/K_\infty,A^*(1)))$ are torsion over $\Lambda = \mathbf{Z}_p[[\Gamma]]$.

(i) The Galois group $\mathrm{Gal}(M_\infty/K_\infty)$ of the maximal abelian pro-p-extension of K_∞, unramified outside primes above S.
(ii) The projective (resp., inductive) limit X_∞ (resp., A_∞) of the p-primary parts of the ideal class groups of $\mathcal{O}_{K_\alpha}$.
(iii) The projective (resp., inductive) limit X'_∞ (resp., A'_∞) of the p-primary parts of the ideal class groups of $\mathcal{O}_{K_\alpha,S_\alpha}$, where S_α is the set of primes of K_α above S.

These are closely related to $\mathbf{R}\Gamma_{\mathrm{Iw}}(K_\infty/K,T)$ and $\mathbf{R}\Gamma_{c,\mathrm{Iw}}(K_\infty/K,T)$ for $T=\mathbf{Z}_p,\mathbf{Z}_p(1)$ (with $R=\mathbf{Z}_p$, $\overline{R}=\Lambda=\mathbf{Z}_p[[\Gamma]]$). Can one obtain anything interesting from the general machinery (0.12-13) in this classical setup?

(0.14.1) First of all, the spectral sequence ${}'E_r$ in (0.12.3) for $T=\mathbf{Z}_p$ and $T=\mathbf{Z}_p(1)$ gives very short proofs of the following well-known results (cf. 9.3):

(i) The Pontrjagin dual of A'_∞ contains no non-zero pseudo-null Λ-submodules.
(ii) If the weak Leopoldt conjecture holds for K_∞ (i.e. $H^2(K_S/K_\infty,\mathbf{Q}_p/\mathbf{Z}_p)=0$), then $\mathrm{Gal}(M_\infty/K_\infty)$ contains no non-zero pseudo-null Λ-submodules.

(0.14.2) For $\Gamma\xrightarrow{\sim}\mathbf{Z}_p$, Iwasawa [Iw] constructed canonical isomorphisms in $({}_\Lambda\mathrm{Mod})/(\mathit{pseudo}-\mathit{null})$

$$\mathrm{Ext}^1_\Lambda(X_\infty,\Lambda)\xrightarrow{\sim}\overline{D}(A_\infty),\qquad\qquad \mathrm{Ext}^1_\Lambda(X'_\infty,\Lambda)\xrightarrow{\sim}\overline{D}(A'_\infty).$$

One expects analogous statements to hold for arbitrary $\Gamma\xrightarrow{\sim}\mathbf{Z}_p^r$ (cf. [McCa 2]).

Our machinery gives only partial results in this direction, such as the following (cf. 9.4-5):

(i) There is a canonical morphism of Λ-modules

$$\alpha':X'_\infty\longrightarrow\mathrm{Ext}^1_\Lambda(\overline{D}(A'_\infty),\Lambda).$$

(ii) $\mathrm{Coker}(\alpha')$ is almost pseudo-null in the sense that there is an explicit finite set P of height one prime ideals $\mathfrak{p}\in\mathrm{Spec}(\Lambda)$ such that $\mathrm{Coker}(\alpha')_\mathfrak{p}=0$ for all $\mathfrak{p}\in\mathrm{Spec}(\Lambda)$, $ht(\mathfrak{p})=1$, $\mathfrak{p}\notin P$.
(iii) The characteristic power series of $\overline{D}(A'_\infty)$ divides that of X'_∞.

Slightly weaker results can be proved for X_∞ and A_∞.

In 1998 the author announced a proof of the fact that $\mathrm{Coker}(\alpha')$ is pseudo-null. Unfortunately, the argument for exceptional $\mathfrak{p}\in P$ turned out to be flawed, which means that the claim has to be retracted.

(0.14.3) Greenberg's local conditions have built into them a fundamental base change property (cf. 8.10.1)

$$\widetilde{\mathbf{R}\Gamma}_{f,\mathrm{Iw}}(K_\infty/K,T)\overset{\mathbf{L}}{\otimes}_{\overline{R}}R\xrightarrow{\sim}\widetilde{\mathbf{R}\Gamma}_f(T)$$

with respect to the augmentation map $\overline{R}\longrightarrow R$. This can be interpreted as a derived version of Mazur's "control theorem" for Selmer groups, according to which the canonical map

$$Sel(G_{K,S},E[p^\infty])\longrightarrow Sel(G_{K_\infty,S},E[p^\infty])^\Gamma$$

has finite kernel and cokernel (assuming that $\Gamma\xrightarrow{\sim}\mathbf{Z}_p$ and E has good ordinary reduction at all primes dividing p).

More generally, there are canonical isomorphisms

$$\widetilde{\mathbf{R}\Gamma}_{f,\mathrm{Iw}}(K_\infty/K,T)\overset{\mathbf{L}}{\otimes}_{\overline{R}}R[[\mathrm{Gal}(L/K)]]\xrightarrow{\sim}\widetilde{\mathbf{R}\Gamma}_{f,\mathrm{Iw}}(L/K,T)\qquad(0.14.3.1)$$

for arbitrary intermediate fields $K\subset L\subset K_\infty$.

(0.14.4) A typical situation in which Mazur's control theorem fails for the clasical Selmer groups but holds for the extended Selmer groups $\widetilde{H}^1_f(-,E[p^\infty])$ is the following: E is an elliptic curve defined over $\mathbf{Q}$ with multiplicative reduction at p and K_∞/K is the anti-cyclotomic $\mathbf{Z}_p$-extension of an imaginary quadratic field K in which p is inert. Note that a trivial zero is again lurking behind this example.

(0.14.5) Our duality results also show that, in the classical case when $R=\mathbf{Z}_p$ and $T=T^0$ is concentrated in degree zero, the objects $\widetilde{\mathbf{R}\Gamma}_{f,\mathrm{Iw}}(K_\infty/K,T)$ can often be represented by relatively simple complexes (see

9.7), which then control $\widetilde{\mathbf{R}\Gamma}_{f,\mathrm{Iw}}(L/K,T)$ and the corresponding height pairings for *all* subextensions L/K of K_∞/K, thanks to (0.14.3.1). These results were used, in the context of classical Selmer groups, in the work of Mazur and Rubin [M-R 2] on "organizing complexes" in Iwasawa theory of elliptic curves.

(0.15) Generalized Cassels-Tate pairings

One of the main applications of the duality theory for Selmer complexes is a construction of higher-dimensional generalizations of Cassels-Tate pairings (cf. Chapter 10). These pairings are used in 10.7 to prove several versions of the following general principle (for Greenberg's local conditions): the parity of ranks of *extended* Selmer groups $\widetilde{H}^1_f(T_\lambda)$ attached to a one-parameter family T_λ of self-dual Galois representations (with respect to a family of skew-symmetric isomorphisms $T_\lambda \xrightarrow{\sim} T^*_\lambda(1)$ respecting the local conditions) is constant. In [N-P], [Ne 3], [Ne 5] and in Chapter 12 we deduce from this principle parity results for ranks of Selmer groups attached to modular forms, elliptic curves and Hilbert modular forms, respectively.

On should keep in mind the following topological analogue (see 10.1): if X is a compact oriented topological manifold of (real) dimension 3, then Poincaré duality with finite coefficients induces a non-degenerate symmetric pairing

$$H^2(X,\mathbf{Z})_{\mathrm{tors}} \times H^2(X,\mathbf{Z})_{\mathrm{tors}} \longrightarrow \mathbf{Q}/\mathbf{Z}.$$

(0.15.0) Let us return to the exact sequence (0.13.2), assuming in addition that $\mathrm{depth}(\overline{R}_{\overline{\mathfrak{p}}}) = \dim(\overline{R}_{\overline{\mathfrak{p}}}) = 1$. Under this assumption the first term in (0.13.2) is canonically isomorphic to

$$\mathrm{Hom}_{\overline{R}_{\overline{\mathfrak{p}}}}\Big(\Big(\widetilde{H}^{4-q}_{f,\mathrm{Iw}}(K_\infty/K,T^*(1))^{\iota}_{\overline{\mathfrak{p}}}\Big)_{(\overline{R}_{\overline{\mathfrak{p}}})-\mathrm{tors}}, I_{\overline{R}_{\overline{\mathfrak{p}}}}\Big),$$

where $I_{\overline{R}_{\overline{\mathfrak{p}}}} \xrightarrow{\sim} H^0(\omega_{\overline{R}})_{\overline{\mathfrak{p}}} \otimes_{\overline{R}_{\overline{\mathfrak{p}}}} (\mathrm{Frac}(\overline{R}_{\overline{\mathfrak{p}}})/\overline{R}_{\overline{\mathfrak{p}}})$ denotes the injective hull of the $(\overline{R}_{\overline{\mathfrak{p}}})$-module $\overline{R}_{\overline{\mathfrak{p}}}/\overline{\mathfrak{p}}\overline{R}_{\overline{\mathfrak{p}}}$ (e.g. $I_{\overline{R}_{\overline{\mathfrak{p}}}} = \mathrm{Frac}(\overline{R}_{\overline{\mathfrak{p}}})/\overline{R}_{\overline{\mathfrak{p}}}$, if $\overline{R}_{\overline{\mathfrak{p}}}$ is a discrete valuation ring). As a result, one obtains a non-degenerate bilinear form (cf. 10.3.3, 10.5.5)

$$\Big(\widetilde{H}^q_{f,\mathrm{Iw}}(K_\infty/K,T)_{\overline{\mathfrak{p}}}\Big)_{(\overline{R}_{\overline{\mathfrak{p}}})-\mathrm{tors}} \times \Big(\widetilde{H}^{4-q}_{f,\mathrm{Iw}}(K_\infty/K,T^*(1))^{\iota}_{\overline{\mathfrak{p}}}\Big)_{(\overline{R}_{\overline{\mathfrak{p}}})-\mathrm{tors}} \longrightarrow I_{\overline{R}_{\overline{\mathfrak{p}}}}.$$

This pairing is of particular interest for $q = 2$. In the **self-dual case**, i.e. when there is a skew-symmetric isomorphism $T_{\mathfrak{p}} \xrightarrow{\sim} T^*(1)_{\mathfrak{p}}$ compatible with isomorphisms $(T^+_v)_{\mathfrak{p}} \xrightarrow{\sim} (T^*(1)^+_v)_{\mathfrak{p}}$ for all $v \in \Sigma$, then the induced pairing

$$\langle\ ,\ \rangle : \Big(\widetilde{H}^2_{f,\mathrm{Iw}}(K_\infty/K,T)_{\overline{\mathfrak{p}}}\Big)_{(\overline{R}_{\overline{\mathfrak{p}}})-\mathrm{tors}} \times \Big(\widetilde{H}^2_{f,\mathrm{Iw}}(K_\infty/K,T)^{\iota}_{\overline{\mathfrak{p}}}\Big)_{(\overline{R}_{\overline{\mathfrak{p}}})-\mathrm{tors}} \longrightarrow I_{\overline{R}_{\overline{\mathfrak{p}}}} \qquad (0.15.0.1)$$

is skew-hermitian (cf. 10.3.4.2).

(0.15.1) All of the above makes sense in the absence of Γ (i.e. for $\overline{R} = R$ and $\overline{\mathfrak{p}} = \mathfrak{p}$), when we obtain bilinear forms (cf. 10.3.2, 10.5.3)

$$\Big(\widetilde{H}^q_f(T)_{\mathfrak{p}}\Big)_{R_{\mathfrak{p}}-\mathrm{tors}} \times \Big(\widetilde{H}^{4-q}_f(T^*(1))_{\mathfrak{p}}\Big)_{R_{\mathfrak{p}}-\mathrm{tors}} \longrightarrow I_{R_{\mathfrak{p}}},$$

which can be degenerate (because of the presence of error terms in (0.9.2)).

In the self-dual case, the induced pairing

$$\Big(\widetilde{H}^2_f(T)_{\mathfrak{p}}\Big)_{R_{\mathfrak{p}}-\mathrm{tors}} \times \Big(\widetilde{H}^2_f(T)_{\mathfrak{p}}\Big)_{R_{\mathfrak{p}}-\mathrm{tors}} \longrightarrow I_{R_{\mathfrak{p}}}$$

is *skew-symmetric* (cf. 10.2.5).

For $R = \mathbf{Z}_p$, $\mathfrak{p} = (p)$ and $T = T_p(E)$ (where E is an elliptic curve with ordinary reduction at all primes above p), we recover essentially the classical Cassels-Tate pairing on the quotient of $Sel(G_{K,S}, E[p^\infty])$ by its maximal divisible subgroup (combining 10.8.7 with 9.6.7.3 and 9.6.3).

Perhaps the simplest non-classical example comes from Hida theory (cf. [N-P]). For simplicity, let us begin with an elliptic curve E over $\mathbf{Q}$, with good ordinary reduction at p (if $p = 2$, then the following discussion has

to be slightly modified). It is known that E is modular [B-C-D-T], hence $L(E,s)=L(f_E,s)$ for a newform $f_E\in S_2(\Gamma_0(N),\mathbf{Z})$, where N is the conductor of E.
Our assumptions imply that $p\nmid N$ and $f_E=f_2$ is a member of a Hida family of ordinary eigenforms [(6)] $f_k\in S_k(\Gamma_0(N),\mathbf{Z}_p)$, for weights $k\in\mathbf{Z}_{\geq 2}$ sufficiently close to 2 in the p-adic space of weights $\mathbf{Z}_p\times\mathbf{Z}/(p-1)\mathbf{Z}$.
The Galois representations attached to various f_k can be interpolated by a big Galois representation

$$\rho: G_{\mathbf{Q},S}\longrightarrow \mathrm{Aut}_R(T),$$

where S consists of all primes dividing Np (and infinity) and R,T are as in (0.1.2). Replacing T by a suitable twist ([N-P], 3.2.3), one obtains a representation (also denoted by T) with the following properties:

(i) There is a prime ideal $\mathcal{P}\in\mathrm{Spec}(R)$ with $ht(\mathcal{P})=1$ such that

$$(T/\mathcal{P}T)\otimes_{\mathbf{Z}_p}\mathbf{Q}_p\xrightarrow{\sim}V_p(E).$$

Moreover, $R_{\mathcal{P}}$ is a discrete valuation ring, unramified over $\Lambda_{\mathcal{P}\cap\Lambda}$.

(ii) T is self-dual, i.e. there is a skew-symmetric isomorphism

$$T\xrightarrow{\sim}T^*(1)=\mathrm{Hom}_\Lambda(T,\Lambda)(1).$$

(iii) There is a self-dual exact sequence of $R_{\mathcal{P}}[G_{\mathbf{Q}_p}]$-modules

$$0\longrightarrow T^+_{\mathcal{P}}\longrightarrow T_{\mathcal{P}}\longrightarrow T^-_{\mathcal{P}}\longrightarrow 0,$$

in which $T^{\pm}_{\mathcal{P}}$ is free of rank one over $R_{\mathcal{P}}$ and there is an isomorphism $T^+_{\mathcal{P}}/\mathcal{P}T^+_{\mathcal{P}}\xrightarrow{\sim}V_p(E)^+$ (compatible with that in (i)).

The corresponding big Selmer complex $\widetilde{\mathbf{R}\Gamma}_f(G_{\mathbf{Q},S},T_{\mathcal{P}})$ satisfies the base change property 12.7.13.4(i)

$$\widetilde{\mathbf{R}\Gamma}_f(T_{\mathcal{P}})\overset{\mathbf{L}}{\otimes}_{R_{\mathcal{P}}}R_{\mathcal{P}}/\mathcal{P}\xrightarrow{\sim}\widetilde{\mathbf{R}\Gamma}_f(V_p(E)),\tag{0.15.1.1}$$

which gives an exact cohomology sequence

$$0\longrightarrow\widetilde{H}^1_f(T_{\mathcal{P}})/\mathcal{P}\longrightarrow\widetilde{H}^1_f(V_p(E))\longrightarrow\widetilde{H}^2_f(T_{\mathcal{P}})[P]\longrightarrow 0,$$

in which the middle term is equal to the classical Selmer group $Sel(G_{\mathbf{Q},S},V_p(E))$.
The existence of a canonical non-degenerate skew-symmetric pairing

$$\widetilde{H}^2_f(T_{\mathcal{P}})_{R_{\mathcal{P}}-\mathrm{tors}}\times\widetilde{H}^2_f(T_{\mathcal{P}})_{R_{\mathcal{P}}-\mathrm{tors}}\longrightarrow\mathrm{Frac}(R_{\mathcal{P}})/R_{\mathcal{P}}$$

then implies the following result (see 12.7.13.5).

(0.15.2) Let E be an elliptic curve over $\mathbf{Q}$ with a good ordinary reduction at p. Then:

(i) There exists a canonical decreasing filtration by $\mathbf{Q}_p$-vector spaces on $S=Sel(G_{\mathbf{Q},S},V_p(E))$:

$$S=S^1\supseteq S^2\supseteq\cdots.$$

(ii) There exist non-degenerate skew-symmetric pairings

$$S^i/S^{i+1}\times S^i/S^{i+1}\longrightarrow\mathbf{Q}_p\qquad\qquad (i\geq 1)$$

depending on the choice of an isomorphism $\Gamma=1+q\mathbf{Z}_p\xrightarrow{\sim}\mathbf{Z}_p$, and otherwise canonical (where $q=p$ (resp., $q=4$) if $p\neq 2$ (resp., $p=2$)).

(iii) The common kernel

$$S^\infty=\bigcap_{i\geq 1}S^i$$

[(6)] In this introduction we ignore the phenomenon of p-stabilization.

is equal to the "generic subspace of S"

$$S^{gen} = \mathrm{Im}\left(\widetilde{H}^1_f(T_{\mathcal{P}}) \longrightarrow \widetilde{H}^1_f(V_p(E))\right).$$

In particular,

$$\dim_{\mathbf{Q}_p}(S) \equiv \dim_{\mathbf{Q}_p}(S^{gen}) \pmod 2.$$

Above, $\dim_{\mathbf{Q}_p}(S^{gen}) = \dim_{\mathscr{L}} \widetilde{H}^1_f(\mathscr{V})$, where $\mathscr{L} = \mathrm{Frac}(R_{\mathcal{P}})$, $\mathscr{V} = T \otimes_R \mathscr{L}$ and $\widetilde{H}^1_f(\mathscr{V}) = \widetilde{H}^1_f(T_{\mathcal{P}}) \otimes_{R_{\mathcal{P}}} \mathscr{L}$ is the Selmer group attached to the whole Hida family passing through f_E.

A similar result holds for extended Selmer groups $\widetilde{H}^1_f$ of self-dual Galois representations attached to Hilbert modular forms (see 12.7.13.5).

The results of [N-P] show that certain non-vanishing conjectures for the two-variable p-adic L-function of E would imply (at least for $p > 3$) that

$$\dim_{\mathbf{Q}_p}(S^{gen}) = \begin{cases} 0, & \text{if } 2 \mid \mathrm{ord}_{s=1} L(E,s) \\ 1, & \text{if } 2 \nmid \mathrm{ord}_{s=1} L(E,s) \end{cases}$$

(in the language of 12.7.13.5, $\widetilde{h}^1_f(\mathbf{Q}, V') = 0$ (resp., $= 1$) for infinitely many $\mathcal{P}'$, hence $\dim_{\mathbf{Q}_p}(S^{gen}) = \dim F^\infty$ is also equal to 0 (resp., to 1)).

(0.15.3) Self-duality in Iwasawa theory is more complicated; because of the presence of the involution ι, we obtain skew-hermitian pairings (10.3.4.2(ii)). In an important *dihedral case* it is possible to get rid of the involution and obtain, as in 0.15.2, skew-symmetric pairings.

Consider, for example, the following situation. Let $K = \mathbf{Q}(\sqrt{D})$, $D < 0$, be an imaginary quadratic field and K_∞/K the *anti-cyclotomic* $\mathbf{Z}_p$-extension of K. This is a dihedral extension of $\mathbf{Q}$, i.e.

$$\Gamma^+ = \mathrm{Gal}(K_\infty/\mathbf{Q}) = \Gamma \rtimes \{1, \tau\},$$

where

$$\tau^2 = 1, \qquad \tau\gamma\tau^{-1} = \gamma^{-1} \qquad\qquad (\gamma \in \Gamma \overset{\sim}{\longrightarrow} \mathbf{Z}_p).$$

This implies that, for every $R[\Gamma^+]$-module M, the action of $\tau \in \Gamma^+$ induces an isomorphism of $R[\Gamma]$-modules

$$\tau : M \overset{\sim}{\longrightarrow} M^\iota.$$

Applying this remark to $M = \widetilde{H}^2_{f,\mathrm{Iw}}(K_\infty/K, T_p(E))$, where E is an elliptic curve over $\mathbf{Q}$ with good ordinary reduction at p, the non-degenerate skew-hermitian pairing

$$\langle\ ,\ \rangle : \left(\widetilde{H}^2_{f,\mathrm{Iw}}(K_\infty/K, T_p(E))_{\mathfrak{p}}\right)_{\Lambda_{\mathfrak{p}}-\mathrm{tors}} \times \left(\widetilde{H}^2_{f,\mathrm{Iw}}(K_\infty/K, T_p(E))_{\mathfrak{p}}\right)_{\Lambda_{\mathfrak{p}}-\mathrm{tors}} \longrightarrow \mathrm{Frac}(\Lambda_{\mathfrak{p}})/\Lambda_{\mathfrak{p}}$$

from (0.15.0.1) (where $R = \mathbf{Z}_p$, $\overline{R} = \Lambda = \mathbf{Z}_p[[\Gamma]]$, $T = T_p(E)$, $\mathfrak{p} \in \mathrm{Spec}(\Lambda) = \mathrm{Spec}(\mathbf{Z}_p[[\Gamma]])$, $ht(\mathfrak{p}) = 1$, $\mathfrak{p} \neq (p)$) induces a non-degenerate skew-symmetric pairing

$$(\ ,\ ) : \left(\widetilde{H}^2_{f,\mathrm{Iw}}(K_\infty/K, T_p(E))_{\mathfrak{p}}\right)_{\Lambda_{\mathfrak{p}}-\mathrm{tors}} \times \left(\widetilde{H}^2_{f,\mathrm{Iw}}(K_\infty/K, T_p(E))_{\mathfrak{p}}\right)_{\Lambda_{\mathfrak{p}}-\mathrm{tors}} \longrightarrow \mathrm{Frac}(\Lambda_{\mathfrak{p}})/\Lambda_{\mathfrak{p}},$$
$$(x, y) = \langle x, \tau y\rangle.$$

This implies that, for each prime ideal $\mathfrak{p}$ as above, we have

$$\widetilde{H}^2_{f,\mathrm{Iw}}(K_\infty/K, T_p(E))^\iota_{\mathfrak{p}} \overset{\sim}{\longrightarrow} \left(\overline{D}(Sel(G_{K_\infty,S}, E[p^\infty]))\right)_{\mathfrak{p}},$$

with

$$\left(\overline{D}(Sel(G_{K_\infty,S},E[p^\infty]))_{\mathfrak{p}}\right)_{\Lambda_{\mathfrak{p}}-\mathrm{tors}} \xrightarrow{\sim} Y \oplus Y$$

for some $\Lambda_{\mathfrak{p}}$-module Y of finite length. The control theorem 0.14.3 for Selmer groups then gives a congruence analogous to that in (0.15.2)(iii)

$$\dim_{\mathbf{Q}_p}(Sel(G_{K,S},V_p(E))) \equiv \mathrm{rk}_\Lambda \overline{D}(Sel(G_{K_\infty,S},E[p^\infty])) \pmod 2 \tag{0.15.3.1}$$

(which holds in a general "dihedral" context; see 10.7.19).

If $p \neq 2$ and K satisfies the following "Heegner condition"

$(Heeg)$ Every prime dividing N_E splits in K,

then everything works even for $\mathfrak{p} = (p)$ (see 10.7.18). A recently proved ([Cor], [Va]) conjecture of Mazur [Maz 2] implies that, assuming (Heeg), the R.H.S. in (0.15.3.1) is equal to 1. As shown in [Ne 3], the congruence (0.15.3.1) for suitably chosen K implies that

$$\dim_{\mathbf{Q}_p}(Sel(G_{\mathbf{Q},S},V_p(E))) \equiv \mathrm{ord}_{s=1}L(E,s) \pmod 2$$

(still assuming that E has good ordinary reduction at p).

A generalization of this parity result to Hilbert modular forms is proved in Chapter 12.

If

$$\dim_{\mathbf{Q}_p}(Sel(G_{K,S},V_p(E))) \equiv 1 \pmod 2,$$

the congruence (0.15.3.1) together with the control theorem 0.14.3 imply that

$$\dim_{\mathbf{Q}_p}(Sel(G_{K',S},V_p(E))) \geq [K' : K],$$

for all finite subextensions K'/K of K_∞/K (cf. 10.7.19). The phenomenon of systematic growth of Selmer groups in dihedral extensions was systematically investigated by Mazur and Rubin [M-R 3,4] (cf. 12.12).

(0.16) Generalized height pairings

(0.16.0) Our formalism also gives a new approach to p-adic (in fact, R-valued) height pairings, which greatly simplifies all previous constructions (due to many people, including Zarhin, Schneider, Perrin-Riou, Mazur and Tate, Rubin, and the author; see the references in [Ne 2] and in Sect. 11.3 below). Let

$$J = \mathrm{Ker}(\overline{R} \longrightarrow R)$$

be the augmentation ideal of $\overline{R}$; there is a canonical isomorphism

$$\begin{aligned} J/J^2 &\xrightarrow{\sim} \Gamma_R = \Gamma \otimes_{\mathbf{Z}_p} R \\ \gamma - 1 \pmod{J^2} &\mapsto \gamma \otimes 1 \qquad\qquad (\gamma \in \Gamma). \end{aligned}$$

Assume that Γ_R is flat over R. For T as in (0.12.1), denote $\mathscr{F}_\Gamma(T)$ by $\overline{T}$. The exact triangle

$$T \otimes_R J/J^2 \longrightarrow \overline{T}/J^2\overline{T} \longrightarrow \overline{T}/J\overline{T} \longrightarrow T \otimes_R J/J^2[1]$$

is canonically isomorphic to

$$T \otimes_R \Gamma_R \longrightarrow \overline{T}/J^2\overline{T} \longrightarrow T \longrightarrow T \otimes_R \Gamma_R[1]. \tag{0.16.0.1}$$

Greenberg's local conditions for T induce similar local conditions for each term in (0.16.0.1); the corresponding Selmer complexes also form an exact triangle in $D^b_{ft}({}_R\mathrm{Mod})$

$$\widetilde{\mathbf{R}\Gamma}_f(T) \otimes_R \Gamma_R \longrightarrow \widetilde{\mathbf{R}\Gamma}_f(\overline{T}/J^2\overline{T}) \longrightarrow \widetilde{\mathbf{R}\Gamma}_f(T) \longrightarrow \widetilde{\mathbf{R}\Gamma}_f(T) \otimes_R \Gamma_R[1],$$

which can also be obtained by applying $\widetilde{\mathbf{R}\Gamma}_f(\overline{T})\overset{\mathbf{L}}{\otimes}_{\overline{R}}(-)$ to the exact triangle

$$J/J^2 \longrightarrow \overline{R}/J^2 \longrightarrow R \longrightarrow J/J^2[1].$$

The cup product (0.9.3) and the "Bockstein map"

$$\beta : \widetilde{\mathbf{R}\Gamma}_f(T) \longrightarrow \widetilde{\mathbf{R}\Gamma}_f(T) \otimes_R \Gamma_R[1]$$

induce a morphism in $D^b_{ft}({}_R\mathrm{Mod})$

$$\widetilde{\mathbf{R}\Gamma}_f(T)\overset{\mathbf{L}}{\otimes}_R\widetilde{\mathbf{R}\Gamma}_f(T^*(1)) \longrightarrow \omega \otimes_R \Gamma_R[-2],$$

which is a derived version of the height pairing. In practice, the only interesting component of this pairing is given by

$$\widetilde{h} : \widetilde{H}^1_f(T) \otimes_R \widetilde{H}^1_f(T^*(1)) \longrightarrow H^0(\omega) \otimes_R \Gamma_R,$$

which can be written as

$$\widetilde{h}(x \otimes y) = \mathrm{Tr}(\beta(x) \cup y).$$

This construction makes sense also in the case when Γ is a finite abelian group of exponent p^m and R is an $\mathbf{Z}/p^m\mathbf{Z}$-algebra. It is very likely that there is a similar cohomological formalism behind real-valued heights.

There is also a more general version of this construction, which yields pairings

$$\widetilde{\mathbf{R}\Gamma}_{f,\mathrm{Iw}}(L/K,T)\overset{\mathbf{L}}{\otimes}_{R[[\mathrm{Gal}(L/K)]]}\widetilde{\mathbf{R}\Gamma}_{f,\mathrm{Iw}}(L/K,T^*(1))^\iota \longrightarrow \omega \otimes_R R[[\mathrm{Gal}(L/K)]] \otimes_R \mathrm{Gal}(K_\infty/L)_R[-2]$$

for arbitrary subextensions L/K of K_∞/K (assuming that $\mathrm{Gal}(K_\infty/L)_R$ is flat over R).

(0.16.1) This approach to height pairings has many advantages over traditional treatments even in the simplest case when $R = \mathbf{Z}_p$ and $T = T_p(E)$, where E is an elliptic curve over $\mathbf{Q}$ with ordinary reduction at p. For example,

(i) The pairing

$$\widetilde{h} : \widetilde{H}^1_f(T_p(E)) \otimes_R \widetilde{H}^1_f(T_p(E)) \longrightarrow \mathbf{Z}_p$$

has values in $\mathbf{Z}_p$; there are *no denominators* involved.

(ii) If E has split multiplicative reduction at p, then $\widetilde{h}$ is a *natural* height pairing on the *extended Selmer group* (Mazur, Tate and Teitelbaum [M-T-T] and their followers used an ad-hoc definition).

(iii) Universal norms in $\widetilde{H}^1_f(T_p(E))$ (i.e. the image of $\widetilde{H}^1_{f,\mathrm{Iw}}(K_\infty/K, T_p(E))$) lie in $\mathrm{Ker}(\beta)$, hence are *automatically* contained in the kernel of the height pairing.

(0.16.2) The definition of $\widetilde{h}$ in terms of the Bockstein map β also sheds new light on the formulas of the Birch and Swinnerton-Dyer type proved by Perrin-Riou [PR 2-5] and Schneider [Sch 2,3]. These formulas express (for $\Gamma \xrightarrow{\sim} \mathbf{Z}_p$) the leading term of the "arithmetic p-adic L-function" (i.e. of the characteristic power series of $\det_{\overline{R}}\widetilde{\mathbf{R}\Gamma}_{f,\mathrm{Iw}}(K_\infty/K,T)$) as a product of the determinant of the height pairing $\widetilde{h}$ with, essentially, the p-part of the various rational terms appearing in the conjecture of Birch and Swinnerton-Dyer.

In our approach, such formulas boil down to the additivity of Euler characteristics in a suitable exact triangle (see 11.7.11). For example, in the classical case $R = \mathbf{Z}_p$, the leading term in question is equal, up to a p-adic unit, to the product of

$$\det(\widetilde{h}) \prod_{i=1}^{3} |\widetilde{H}^i_f(T)_{\mathrm{tors}}|^{(-1)^i}$$

with a certain fudge factor. As in the classical case, all this works under the following assumptions:

(i) The $\overline{R}$-modules $\widetilde{H}^i_{f,\mathrm{Iw}}(K_\infty/K,X)$ $(X = T, T^*(1))$ satisfy suitable finiteness properties.

(ii) $\widetilde{h}$ is non-degenerate.

If (i) holds but (ii) fails, then it is necessary to consider also higher order terms E_r in the Bockstein spectral sequence and suitable higher order height pairings that generalize the "derived heights" of Bertolini and Darmon [B-D 1,2].

In [PR 3], Perrin-Riou considered the case of anti-cyclotomic $\mathbf{Z}_p$-extensions and proved a suitable Λ-valued version of the formulas alluded to above. This result is also covered by our machinery.

Burns and Venjakob [Bu-Ve] combined our approach to the formulas of the Birch and Swinnerton-Dyer type with the formalism of non-commutative Iwasawa theory.

(0.17) Parity results

The symplectic pairings constructed in Chapter 10 can be used to generalize the parity results proved in [Ne 3] to Hilbert modular forms and abelian varieties of $GL(2)$-type over totally real number fields. We refer the reader to Sections 12.1-2 for a detailed description of our results, which include, for example, the following generalization of [Ne 3, Thm. A] (see Corollary 12.2.10 below):

Theorem. *Let F be a totally real number field, F_0/F an abelian 2-extension, E an elliptic curve over F which is potentially modular in the sense of 12.11.3(1) below* [7] *and p a prime number such that E has potentially ordinary (= potentially good ordinary or potentially multiplicative) reduction at each prime of F above p. Assume that at least one of the following conditions holds:*

(1) *$j(E) \notin \mathcal{O}_F$.*

(2) *E is modular over F and $2 \nmid [F : \mathbf{Q}]$.*

(3) *$j(E) \in \mathcal{O}_F$, E has good ordinary reduction at each prime of F above p, the prime number p is unramified in $F_0/\mathbf{Q}$ and $p > 3$. If E does not have CM, assume, in addition, that $\mathrm{Im}(G_F \longrightarrow \mathrm{Aut}(E[p])) \supseteq SL_2(\mathbf{F}_p)$.*

Then: for each finite Galois extension of odd degree F_1/F_0,

$$\mathrm{rk}_{\mathbf{Z}} E(F_1) + \mathrm{cork}_{\mathbf{Z}_p} Ш(E/F_1)[p^\infty] \equiv \mathrm{ord}_{s=1} L(E/F_1, s) \pmod 2.$$

These parity results can be combined with (generalizations of) (0.15.3.1), giving rise to many situations in which Selmer groups "grow systematically" in the sense of [M-R 3]. See Sect. 12.12 for more details.

(0.18) Contents

Let us give a brief description of the contents of each chapter of this work. In Chapter 1 we collect the necessary background material from homological algebra. We pay particular attention to signs, as one of our main goals is to construct higher-dimensional generalizations of the Cassels-Tate pairing, and verify that they are skew-symmetric. The reader is strongly advised to skip this chapter and return to it only when necessary. In Chapter 2 we recall the formalism of Grothendieck's duality theory over (complete) local rings. In Chapter 3 we develop from scratch the formalism of continuous cohomology for what we call (ind)-admissible $R[G]$-modules. Chapter 4 deals with finiteness results for continuous cohomology of pro-finite groups. In Chapter 5 we deduce from the classical duality results for Galois cohomology of finite Galois modules over local and global fields (due to Tate and Poitou) the corresponding results for big Galois representations. In Chapter 6 we introduce Selmer complexes in an axiomatic setting and prove a duality theorem for them (as a consequence of the Poitou-Tate duality in our formalism). In Chapter 7 we investigate a generalization of unramified cohomology (over local fields) in our set-up. In Chapter 8 we apply Shapiro's Lemma to deduce duality results in Iwasawa theory from those over number fields. Chapter 9 is devoted to applications to classical Iwasawa theory, namely to p-parts of ideal class groups (resp., of S-ideal class groups). It also includes comparison results between the extended Selmer groups $\widetilde{H}^1_f$, Greenberg's (strict) Selmer groups and classical Selmer groups for abelian varieties. In Chapter 10 we construct and study various incarnations of generalized Cassels-Tate pairings. We pay particular attention to the self-dual case, which is important for arithmetic applications. In Chapter 11 we construct generalized p-adic height pairings and relate them to the formulas of the Birch and Swinnerton-Dyer type. In Chapter 12, we apply the results from Chapter 10 to big Galois representations arising from Hida families of Hilbert modular forms of parallel

[7] *Potential modularity of E seems to be well-known to the experts [Tay 5]; a proof is expected to appear in a forthcoming thesis of a student of R. Taylor.*

weight, and also to anticyclotomic Iwasawa theory of CM points on Shimura curves. This allows us to deduce a far-reaching generalization of the parity results from [Ne 3].

(0.19) Directions for further research

The fact that Selmer complexes 'see' trivial zeros of p-adic L-functions and satisfy the base change properties 0.14.3 and (0.15.1.1) indicates that they – and not the usual Selmer groups – are the correct algebraic counterparts of p-adic L-functions. It would be of some interest, therefore, to reformulate all aspects of Iwasawa theory from this perspective.

(0.19.1) Non-commutative Iwasawa theory. It seems very likely that the results discussed in 0.11-13 can be generalized to a fairly large class of non-commutative p-adic Lie groups Γ. One would expect the duality diagram (0.12.1) to hold over $\overline{R} = R[[\Gamma]]$ again with $\omega_{\overline{R}} = \omega_R \otimes_R \overline{R}$ (this time as a complex of $\overline{R}$-bimodules) and $\mathscr{F}_\Gamma$, F_Γ defined as in 8.3.1. Note that both $\mathscr{F}_\Gamma(M)$ and $F_\Gamma(M)$ are $\overline{R}$-bimodules equipped with an involution compatible with the bimodule structure, and the action of $G = G_{K,S}$ commutes with one of the $\overline{R}$-module structures. It seems that this extra structure can be used to generalize the cohomological theory of admissible $\overline{R}[G]$-modules to the non-commutative setting.

(0.19.2) Local Iwasawa theory. It would be highly desirable to develop a theory of local conditions at primes dividing p that would go beyond Greenberg's local conditions. One should view Perrin-Riou's theory [PR 6] interpolating the Bloch-Kato exponential in the local cyclotomic $\mathbf{Z}_p$-extension as a first step in this direction. Another challenge is posed by the families of Galois representations arising from Coleman's theory of rigid analytic families of modular forms. It is clear that in this generality one would have to work with more general coefficient rings R. In fact, there should be a common generalization of 0.19.1 and 0.19.2, perhaps in the context of "Fréchet-Stein algebras" introduced by Schneider-Teitelbaum [Sch-Te]. One can also envisage a version of the theory involving directly étale cohomology of towers of varieties, rather than Galois cohomology.

(0.19.3) Euler systems. The machinery of Euler systems is a powerful tool for obtaining upper bounds for the size of (dual) Selmer groups. It would seem natural to incorporate Selmer complexes into this theory, which would allow for the treatment of trivial zeros.

In practice, elements of an Euler system are obtained from suitable elements of motivic cohomology to which one applies the p-adic regulator or the p-adic Abel-Jacobi map. It is a natural question whether one can, in the presence of a trivial zero, canonically lift an Euler system from the Selmer group to its extended version $\widetilde{H}^1_f$. This can be done, for example, for the Euler system of Heegner points in the presence of an "anticyclotomic trivial zero" ([B-D 3], 2.6).

(0.20) Miscellaneous

(0.20.1) An embryonic version of Selmer complexes appears in [Fo 1] (following a suggestion of Deligne). The first consistent use of derived categories in Iwasawa theory is due to Kato [Ka 1]; his approach has been incorporated into the general formalism of Equivariant Tamagawa Number Conjecture [Bu-Fl 1,2]. Recent articles of Burns-Greither [Bu-Gr], Burns-Venjakob [Bu-Ve], Fukaya-Kato [Fu-Ka] and Mazur-Rubin [M-R 1-3] are also closely related to our framework.

(0.20.2) To our great embarrassment, it has proved impossible to keep the length of this work under control, even though much of what we do is just an exercise in linear algebra. This is a consequence of our early decision not to use any homotopical machinery (such as infinite hierarchies of higher-order homotopies) in our treatment of Selmer complexes, only brute force.

(0.20.3) The idea of a 'Selmer complex' occurred to the author while he was staying at Institut Henri Poincaré in Paris in spring 1997. It was further developed during stays at the Isaac Newton Institute in Cambridge in spring 1998 and (again) at Institut Henri Poincaré in spring 2000. During the visits at IHP the author was partially supported by a grant from EPSRC and by the EU research network "Arithmetic Algebraic Geometry". Main results of this theory were presented in a series of lectures at University of Tokyo in spring 2001; this visit was supported by a fellowship from JSPS. The first version of this work was completed during the author's visit at Institut de Mathématiques de Jussieu in Paris in October 2001. The author is grateful to all these institutions for their support. He would also like to thank D. Blasius, D. Burns, O. Gabber, R. Greenberg, H. Hida, U. Jannsen, B. Mazur, K. Rubin, P. Schneider, A.J. Scholl, C. Skinner,

R. Taylor and A. Wiles for helpful discussions and inspiring questions, and to C. Cornut, D. Mauger, J. Oesterlé, L. Orton, J. Pottharst and the referee for pointing out several inaccuracies in the text.

(0.20.4) To sum up, this work gives a unified treatment of much of (commutative) Iwasawa theory [8] organized around a small number of simple, but sufficiently general principles. We hope that our attempt to Grothendieckify the subject will help integrate it into a wider landscape of arithmetic geometry.

Selmer groups are dead. Long live Selmer complexes!

[8] We consider only the algebraic side of the subject. The relation of Selmer complexes to p-adic L-functions remains to be explored, but it is natural to expect that $\det_{\overline{R}} \widetilde{\mathbf{R}\Gamma}_{f,\mathrm{Iw}}(K_\infty/K, T)$, whenever defined, should be closely related to a suitable analytic p-adic L-function.