AWS 2018, Problem Session
(Algebraic aspects of Iwasawa theory)

Kâzım Büyükboduk

March 3-7, 2018

Contents

1 Commutative Algebra

1.1. For a positive integer m, we let μ_m denote the mth roots of unity. Prove that the integral closure $\mathcal{O}$ of $\mathbb{Z}$ in $\mathbb{Q}(\mu_{p^\infty}) := \bigcup_n \mathbb{Q}(\mu_{p^n})$ is not a Dedekind ring.

1.2. Suppose $\Gamma \cong \mathbb{Z}_p$ and let $\Lambda := \mathbb{Z}_p[[\Gamma]]$. If

$$0 \longrightarrow M \longrightarrow N \longrightarrow K \longrightarrow 0$$

is a short exact sequence of Λ-modules, prove that there exists an exact sequence

$$0 \longrightarrow M^\Gamma \longrightarrow N^\Gamma \longrightarrow K^\Gamma \longrightarrow M_\Gamma \longrightarrow N_\Gamma \longrightarrow K_\Gamma \longrightarrow 0.$$

1.3. Let $\Lambda := \mathbb{Z}_p[[T]]$ and $f = \sum_{i=0}^{\infty} a_i T^i \in \Lambda$ with $a_0 \neq 0$.

1.3.1. Prove that $f \in \mathbb{Q}_p[[T]]^\times$.

1.3.2. Write $f^{-1} = \sum_{i=0}^{\infty} b_i T^i$ with $b_i \in \mathbb{Q}_p$. Prove that $\mathrm{ord}_p(b_i) \geq -(i+1)\mathrm{ord}_p(a_0)$.

1.3.3. Conclude that $\mathrm{Frac}(\Lambda)$ is not contained in the Laurent series ring $\mathbb{Q}_p((T))$.

1.4. Suppose that R is a complete local Noetherian domain.

1.4.1. Prove that pseudo-isomorphism is an equivalence relation in the category of finitely generated R-modules.

1.4.2. Suppose that

$$0 \longrightarrow M \longrightarrow N \longrightarrow K \longrightarrow 0$$

is a short exact sequence of finitely generated torsion R-modules. If there no height-one primes of R contained in $\mathrm{supp}(M) \cap \mathrm{supp}(K)$, then N is pseudo-isomorphic to $M \oplus K$.

1.5. Let $\Lambda = \mathbb{Z}_p[[T]]$ and M be a finitely generated torsion Λ-module. Suppose that we are given a sequence $g_n \in \Lambda$ of distinguished polynomial such that $\lim_{n\to\infty} \deg g_n = \infty$. If the sequence $\{\dim_{\mathbb{F}_p} M/(g_n, p)M\}_n$ is bounded, prove that $\mu(M) = 0$.

1.6. Let K be any field that contains $2p$th roots of unity and let K_∞/K denote its cyclotomic $\mathbb{Z}_p$-extension. Set $\Gamma_K := \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$ and $\Lambda := \mathbb{Z}_p[[\Gamma_K]]$. Let γ denote a topological generator of Γ_K and identify Λ with $\mathbb{Z}_p[[T]]$ via $\gamma \mapsto 1 + T$. Set $u := \chi_{\mathrm{cyc}}(\gamma)$.

1.6.1. Prove that $u \in 1 + q\mathbb{Z}_p$, where $q = p$ if $p > 2$ or $q = 4$ otherwise.

1.6.2. For any $f \in \mathbb{Z}_p[[T]]$, we may consider $M := \Lambda/f\Lambda$ as a G_K-module. Let $M(i)$ denote its ith Tate-twist. Prove that we have an isomorphism

$$M(i) \xrightarrow{\sim} \Lambda/f(u^{-i}(1+T) - 1)\Lambda$$

of Λ-modules.

1.6.3. For a finitely generated Λ-module M, prove that $M(i)^{\Gamma_K}$ is finite for all but finitely many i.

2 Classical Iwasawa Theory (of Tate motives)

2.1. Find a number field K and a prime p such that the first layer K_1/K in the cyclotomic $\mathbb{Z}_p$-tower of K is unramified.

2.3. Suppose L/K is a finite extension of number fields.

2.3.1. If Leopoldt's conjecture is valid for L and p, prove that it also holds true for K and p.

2.3.2. Suppose L is a CM extension and $K := L^+$ its maximal totally real subfield. If the Leopoldt conjecture holds for K and p, prove that it is also true for L and p.

2.3.3. Prove that Leopoldt's conjecture for abelian extensions of $\mathbb{Q}$ follows from Leopoldt's conjecture for totally real abelian extensions.

2.4. Let K be a number field and K_∞/K a $\mathbb{Z}_p$-extension of K. For $n \geq 0$, let K_n/K denote the unique subsextension of K_∞/K that has degree p^n over K, set $\Gamma_n = \mathrm{Gal}(K_\infty/K_n)$ and let A_n denote the p-Sylow subgroup of the ideal class group of K_n. Let L_∞ denote the maximal abelian unramified pro-p extension of K_∞ and let $X := \mathrm{Gal}(L_\infty/K_\infty)$ denote its Galois group over K_∞.

2.4.1. Prove that $\mu(X) = 0$ if and only if $\{\dim_{\mathbb{F}_p} A_n/pA_n\}$ is bounded as n tends to infinity.

2.4.2. Calculate $\mu(X)$ and $\lambda(X)$ for $K = \mathbb{Q}$ (and for the obvious choice of K_∞).

2.4.3. Suppose there is only one prime of K that ramifies in K_∞/K and that prime is totally ramified. Prove that $X_{\Gamma_n} \xrightarrow{\sim} A_n$ and that $A_0 = 0$ if and only if $A_n = 0$ for all $n \geq 0$.

2.4.4. Find a number field K and a prime p such that the ν-invariant for the cyclotomic $\mathbb{Z}_p$-tower is non-zero.

2.5. Suppose $\Gamma \xrightarrow{\sim} \mathbb{Z}_p$ and for each non-negative integer n, set $\Gamma_n := \Gamma^{p^n}$. Let $\Lambda = \mathbb{Z}_p[[\Gamma]]$ and let M be a finitely generated torsion Λ-module with characteristic polynomial f. Prove that the following three conditions are equivalent:

(i) M^{Γ_n} is finite.

(ii) M_{Γ_n} is finite.

(iii) $f(\zeta - 1)$ is non-zero for any $\zeta \in \mu_{p^n}$.

When this is the case, prove that

$$\frac{|M^{\Gamma_n}|}{|M_{\Gamma_n}|} = p^{-\mu(M)p^n} \prod_{\zeta \in \mu_{p^n}} |f(\zeta - 1)|_p \,.$$

2.6. Let F be an imaginary quadratic field and p be an odd prime. Let $h_F^{(p)}$ denote the order of the p-Sylow subgroup of the ideal class group of F. Let F_∞/F denote the cyclotomic $\mathbb{Z}_p$-extension of K and X the Galois group of the maximal abelian unramified pro-p extension of F_∞ over F_∞. Let $f_X(T)$ denote any generator of the characteristic ideal of X. Suppose the prime p is either inert or ramified in $F/\mathbb{Q}$.

2.6.1. Prove that $f_X(0) \neq 0$.

2.6.2. Prove that $\mathrm{ord}_p h_F^{(p)} = \mathrm{ord}_p f_X(0)$.

2.7. Let F be an imaginary quadratic field and p be an odd prime. Let $h_F^{(p)}$ denote the order of the p-Sylow subgroup of the ideal class group of F. Let F_∞/F denote the cyclotomic $\mathbb{Z}_p$-extension of K and X the Galois group of the maximal abelian unramified pro-p extension of F_∞ over F_∞. Let $f_X(T)$ denote any generator of the characteristic ideal of X. Suppose the prime p is split in $F/\mathbb{Q}$.

2.7.1. Prove that $f_X(T)$ has a simple zero at $T = 0$.

2.7.2. Suppose $F = \mathbb{Q}(i)$. Calculate $f_X'(0)$.

2.7.3. More generally, calculate the ratio $f_X'(0)/h_F^{(p)}$.

2.8. With the notation of Problem 2.5, let N be a finitely generated Λ-module. Prove for sufficiently large n that

$$\mathrm{rank}_{\mathbb{Z}_p} N_{\Gamma_n} = p^n \mathrm{rank}_\Lambda N + c$$

for some constant c that doesn't depend on n.

2.9. Let K be a number field and K_∞/K its cyclotomic $\mathbb{Z}_p$-extension. Let X_K denote the Galois group of the maximal abelian unramified pro-p extension of K_∞ over K_∞. Set $\mu_K := \mu(X_K)$. Let L be a finite extension of K. If $\mu_L = 0$, prove that $\mu_K = 0$ as well.

2.10. Let K be a number field and let S denote a set of places of K, containing all primes above p and places above ∞. Let K_∞/K be a $\mathbb{Z}_p$-extension of K and let X_S denote the Galois group of the maximal abelian pro-p extension of K_∞ unramified outside S. Prove that the weak Leopoldt conjecture for K_∞/K holds true if and only if $\mathrm{rank}_\Lambda X_S = r_2(K)$.

2.11. Suppose p is odd, K is a totally real number field and $K' = K(\mu_p)$. Let S and X_S be as in the previous problem. If $\mu_{K'} = 0$ (with the notation of Problem 2.9), prove then that $\mu(X_S) = 0$ for all choices of the finite set S (containing all primes of K above p and ∞).

3 Galois cohomology and Selmer groups

3.1. Let n be a positive integer and let μ_{p^n} denote the Galois module of p^nth roots of unity.

3.1.1. Let F be any field. Prove that $H^1(F, \mu_{p^n}) \cong F^\times/(F^\times)^{p^n}$.

3.1.2. Conclude that $H^1(F, \mathbb{Z}_p(1)) \cong \widehat{F^\times} := \varprojlim F^\times/(F^\times)^{p^n}$, the p-adic completion of $F^\times$.

3.1.3. Let ℓ be a prime and suppose F is a finite extension of $\mathbb{Q}_\ell$. Calculate

$$|H^0(F, \mu_{p^n})| - |H^1(F, \mu_{p^n})| + |H^2(F, \mu_{p^n})|\,.$$

3.2. Suppose F is any field. Let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbb{Q}_p$ and let χ be an $\mathcal{O}$-valued character of G_F that has finite prime-to-p order. Let L denote the finite extension of F, which is the fixed field of $\ker(\chi)$. We write $\mathcal{O}(\chi)$ to denote the free $\mathcal{O}$-module of rank one on which G_F acts by χ. Set $T_n := \mu_{p^n} \otimes \mathcal{O}(\chi^{-1})$. Observe that $T_n^* = \mathcal{O}(\chi)/p^n\mathcal{O}(\chi)$.

3.2.1. Prove that $H^1(F, T_n) \cong \left(L^\times/(L^\times)^{p^n}\right)^\chi$, where for an $\mathcal{O}[[G_F]]$-module M, we write M^χ for the χ-isotypic component of its p-adic completion.

3.2.2. Prove that $H^1(F, T_n^*) \cong \mathrm{Hom}(G_F, \mathbb{Z}/p^n\mathbb{Z})^{\chi^{-1}}$.

3.3.3. Set $T := \varprojlim T_n = \mathbb{Z}_p(1) \otimes \mathcal{O}(\chi^{-1})$ and $T^* = \varinjlim T_n^* = \mathcal{O}(\chi) \otimes \mathbb{Q}_p/\mathbb{Z}_p$. Show that $H^1(F, T) \cong (L^\times)^\chi$ and $H^1(F, T^*) \cong \mathrm{Hom}(G_L, \mathbb{Q}_p/\mathbb{Z}_p)^{\chi^{-1}}$.

3.3.4. Let ℓ be a prime and suppose F is a finite extension of $\mathbb{Q}_\ell$. Let L be given as above and let λ denote its maximal ideal. Let $\mathcal{I}_L \subset G_L$ denote the inertia subgroup so that the Galois group $\mathrm{Gal}(L^{\mathrm{ur}}/L)$ of the maximal unramified extension of L equals $G_L/\mathcal{I}_L$. Prove that

$$H^1_{\mathrm{ur}}(F, T^*) \cong \mathrm{Hom}(G_L/\mathcal{I}_L, \mathbb{Q}_p/\mathbb{Z}_p)^{\chi^{-1}},$$

the module of unramified homomorphisms into $\mathbb{Q}_p/\mathbb{Z}_p$.

3.3.5. In the situation of previous example, use local class field theory to conclude that

$$H^1_{\mathrm{ur}}(F, T) \cong U_L^\chi,$$

where $U_L \subset F^\times$ is the subgroup of units.

3.4. Suppose F is a number field and all other notation in this problem follows that we have set in Problem 3.3. Let $\mathcal{F}_{\mathrm{can}}$ denote the canonical Selmer structure on T, as defined in Appendix A.

3.4.1. For each prime $\lambda \in \Sigma(\mathcal{F}_{\mathrm{can}})$ of F that does not lie above p, prove that

$$H^1_{\mathcal{F}_{\mathrm{can}}}(F_\lambda, T) \cong \bigoplus_{\mathfrak{q}|\lambda} U_{L_\mathfrak{q}}^\chi\,;$$

$$H^1_{\mathcal{F}^*_{\mathrm{can}}}(F_\lambda, T^*) \cong \bigoplus_{\mathfrak{q}|\lambda} \mathrm{Hom}(G_{L_\mathfrak{q}}/\mathcal{I}_{L_\mathfrak{q}}, \mathbb{Q}_p/\mathbb{Z}_p)^{\chi^{-1}}\,.$$

Hint: You may wish to figure out what "semi-local Shapiro's lemma" should look like.

3.4.2. Deduce that $H^1_{\mathcal{F}_{\mathrm{can}}}(F, T) = (\mathcal{O}_L[1/p]^\times)^\chi$ and $H^1_{\mathcal{F}^*_{\mathrm{can}}}(F, T^*)^\vee = \mathrm{Pic}(\mathcal{O}_L[1/p])^\chi$.

3.4.3. Suppose that $\chi(\mathfrak{p}) \neq 1$ for primes $\mathfrak{p}$ of F lying above p. Prove that

$$\left(\mathcal{O}_L[1/p]^\times\right)^\chi = \left(\mathcal{O}_L^\times\right)^\chi \quad \text{and} \quad \mathrm{Pic}(\mathcal{O}_L[1/p])^\chi = \mathrm{Cl}(L)^\chi.$$

3.4.4. Conclude that

$$\operatorname{rank}_{\mathcal{O}} H^1_{\mathcal{F}_{\mathrm{can}}}(F,T) - \operatorname{rank}_{\mathcal{O}} H^1_{\mathcal{F}^*_{\mathrm{can}}}(F,T^*)^\vee = r_1(F) + r_2(F) + \sum_{\mathfrak{p}|p,\chi(\mathfrak{p})=1} 1$$

if χ is non-trivial, and otherwise, that

$$\operatorname{rank}_{\mathcal{O}} H^1_{\mathcal{F}_{\mathrm{can}}}(F,T) - \operatorname{rank}_{\mathcal{O}} H^1_{\mathcal{F}^*_{\mathrm{can}}}(F,T^*)^\vee = r_1(F) + r_2(F) + g(F) - 1$$

where $g(F)$ is the number of primes of F that lie above p.

3.4.5. Prove that for $\mathbb{T} := \mathbb{Z}_p(1) \otimes \Lambda_{\mathrm{cyc}}$ we have

$$\begin{aligned}\operatorname{rank}_{\Lambda_{\mathrm{cyc}}} H^1_{\mathcal{F}_\Lambda}(F,\mathbb{T}) - \operatorname{rank}_{\Lambda_{\mathrm{cyc}}} H^1_{\mathcal{F}^*_\Lambda}(F,\mathbb{T}^*)^\vee &= r_1(F) + r_2(F) \\ &= \operatorname{rank}_{\mathbb{Z}_p}\left(\operatorname{Ind}_{F/\mathbb{Q}} \mathbb{Z}_p(1)\right)^-\end{aligned}$$

3.5. Let $\mathcal{F}_{\mathrm{str}}$ denote the Selmer structure on $\mathbb{T} := \mathbb{Z}_p(1) \otimes \Lambda_{\mathrm{cyc}}$ given as in Example A.4.

3.5.1. Given a number field F, let $\widehat{\mathcal{O}}_F^{\times,\circ}$ denote the kernel of

$$\widehat{\mathcal{O}_F^\times} \longrightarrow \prod_{\wp|p} \widehat{\mathcal{O}_{F_\wp}^\times}\,.$$

Prove that $H^1_{\mathcal{F}_{\mathrm{str}}}(K,\mathbb{T}) \cong \varprojlim_n \widehat{\mathcal{O}}_{K_n}^{\times,\circ}$. In particular, weak Leopoldt conjecture in this set up is equivalent to the requirement that $H^1_{\mathcal{F}_{\mathrm{str}}}(K,\mathbb{T}) = 0$.

3.5.2. Let S denote the set of places of K above p and ∞ and let X_S denote the module introduced in Problem 2.10 (with $K_\infty = K_{\mathrm{cyc}}$, the cyclotomic $\mathbb{Z}_p$-extension). Prove that $H^1_{\mathcal{F}^*_{\mathrm{str}}}(K,\mathbb{T}^*)^\vee \cong X_S$.

3.5.3. Prove that

$$\operatorname{rank}_{\Lambda_{\mathrm{cyc}}} H^1_{\mathcal{F}_{\mathrm{str}}}(K,\mathbb{T}) - \operatorname{rank}_{\Lambda_{\mathrm{cyc}}} H^1_{\mathcal{F}^*_{\mathrm{str}}}(K,\,\mathbb{T}^*)^\vee = -r_2(F)\,.$$

Remark. As you will learn in J. Coates' lectures, Iwasawa has proved Leopoldt's conjecture for cyclotomic $\mathbb{Z}_p$-extensions. This, together with Problem 2.10, is a refinement of the equality above.

3.6. Suppose T is a free $\mathbb{Z}_p$-module of finite rank, which is endowed with a continuous $G_{\mathbb{Q}}$-action such that the residual representation T/pT is absolutely irreducible, non-trivial and unramified outside a finite set of primes. Prove that

$$\operatorname{rank}_{\mathbb{Z}_p} H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbb{Q},T) - \operatorname{rank}_{\mathbb{Z}_p} H^1_{\mathcal{F}^*_{\mathrm{can}}}(\mathbb{Q},T^*)^\vee = \operatorname{rank}_{\mathbb{Z}_p} T^- + \operatorname{corank}_{\mathbb{Z}_p}(H^0(\mathbb{Q}_p,T^*))$$

and explain how this generalizes the conclusion of Problem 3.4.4.

3.7. Suppose T is as in Problem 3.6. Set $\mathbb{T} := T \otimes \Lambda_{\mathrm{cyc}}$ and let $\mathcal{F}_\Lambda$ denote the Selmer structure on $\mathbb{T}$ we have introduced in Appendix A.

3.7.1. Prove for $\ell \neq p$ that $H^1(\mathbb{Q}_\ell^{\mathrm{ur}}, \mathbb{T}) = 0$.

3.7.2. Prove that

$$\mathrm{rank}_{\Lambda_{\mathrm{cyc}}} H^1_{\mathcal{F}_\Lambda}(\mathbb{Q}, \mathbb{T}) - \mathrm{rank}_{\Lambda_{\mathrm{cyc}}} H^1_{\mathcal{F}^*_\Lambda}(\mathbb{Q}, \mathbb{T}^*)^\vee = \mathrm{rank}_{\mathbb{Z}_p} T^- =: d_-(T)\,.$$

3.7.3. We say that weak Leopoldt conjecture for T holds if $H^1_{\mathcal{F}^*_\Lambda}(\mathbb{Q}, \mathbb{T}^*)^\vee$ is torsion (in view of Problem 3.7.2, this is equivalent to the requirement that $\mathrm{rank}_{\Lambda_{\mathrm{cyc}}} H^1_{\mathcal{F}_\Lambda}(\mathbb{Q}, \mathbb{T}) = d_-(T)$). If $H^0(\mathbb{Q}_\infty, T) = 0$ and weak Leopoldt conjecture holds for T, prove that $H^1_{\mathcal{F}_\Lambda}(\mathbb{Q}, \mathbb{T})$ is in fact a free Λ_{cyc}-module of rank $d_-(T)$.

4 Iwasawa Invariants of Elliptic Curves

4.1. Assume that p is an odd prime and $E_{/\mathbb{Q}}$ is an elliptic curve with ordinary reduction at p. Assume also that $E[p^\infty]$ contains a $G_{\mathbb{Q}}$-invariant subgroup Φ of order p, which is either ramified at p and even; or unramified at p and odd. Let Σ denote the set of places that consists of all bad primes for E, the prime p and the infinite place.

4.1.1. Let $\Psi := E[p]/\Phi$ denote the one-dimensional $\mathbb{F}_p$-vector space. Prove that the $G_{\mathbb{Q}}$-action on Ψ is either unramified at p and odd (in case Φ is ramified at p and even) or else it is ramified at p and even (in case Φ is unramified at p and odd).

4.1.2. Suppose that M is a one-dimensional $\mathbb{F}_p$-vector space which is endowed with a $G_{\mathbb{Q}}$-action. For each prime v of $\mathbb{Q}_\infty$ above $\ell \neq p$, prove that $H^1(\mathbb{Q}_{\infty,v}, M)$ has finite cardinality.

4.1.3. Let M be as in the previous problem. Suppose $G_{\mathbb{Q}}$ acts on M via the character χ. Set $H^1_{\mathrm{ur}}(\mathbb{Q}_{\Sigma/\mathbb{Q}_\infty}, M)$ denote the collection of everywhere unramified cohomology classes. Prove that

$$H^1_{\mathrm{ur}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, M) = \mathrm{Hom}(\mathfrak{X}^\chi, M)$$

where $\mathfrak{X} = \mathrm{Gal}(L_\infty/F_\infty)$, with $F_\infty = F\mathbb{Q}_\infty$ and $F = \overline{\mathbb{Q}}^{\ker\chi}$; L_∞ the maximal abelian unramified pro-p extension of F_∞.

4.1.4. Show that Ferrero-Washington theorem implies $H^1_{\mathrm{ur}}(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, M)$ for M as in the previous two problems.

4.1.5. Prove that $H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p]) \xrightarrow{\sim} H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p^\infty])[p]$.

4.1.6. Prove that $\mu_E = 0$.

4.1.7. Use Mazur's theorem to determine all possible primes p that the conditions of this problem can apply.

4.2. Let p be an odd prime and suppose $E_{/\mathbb{Q}}$ is an elliptic curve with good ordinary reduction at p. Suppose $E(\mathbb{Q})[p] = 0$.

4.2..1. Prove that $E(K)[p] = 0$ for every pro-p extension $K/\mathbb{Q}$.

4.2.2. Prove that all three arrows

$$\varinjlim_n H^1_{\mathcal{F}^*_{\mathrm{Gr}}}(\mathbb{Q}_n, E[p]) \longrightarrow \varinjlim_n H^1_{\mathcal{F}^*_{\mathrm{Gr}}}(\mathbb{Q}_n, E[p^\infty])[p] \longrightarrow H^1_{\mathcal{F}^*_{\mathrm{Gr}}}(\mathbb{Q}, \mathbb{T}_p(E)^*)[p]$$

are isomorphisms. Conclude that the following assertions are equivalent:

* $\mu_E = 0$.
* $\varinjlim_n H^1_{\mathcal{F}^*_{\mathrm{Gr}}}(\mathbb{Q}_n, E[p])$ has finite cardinality.
* The sequence of integers $\{\#H^1_{\mathcal{F}^*_{\mathrm{Gr}}}(\mathbb{Q}_n, E[p])\}_n$ is bounded.

4.2.3. Let Σ denote the set of places that consists of all bad primes for E, the prime p and the infinite place. Choose any subset Σ_0 of Σ which contains all places of bad reduction, but does not contain p and ∞. We define $\mathrm{Sel}^{\Sigma_0}_{E[p^\infty]}(\mathbb{Q}_\infty)$ to denote the Selmer group by relaxing all local requirements at primes $\ell \in \Sigma_0$. Define similarly $\mathrm{Sel}^{\Sigma_0}_{E[p]}(\mathbb{Q}_\infty)$.

4.2.3.1. Prove that $\mathrm{Sel}^{\Sigma_0}_{E[p]}(\mathbb{Q}_\infty) \xrightarrow{\sim} \mathrm{Sel}^{\Sigma_0}_{E[p^\infty]}(\mathbb{Q}_\infty)[p]$.

4.2.3.2. Prove that $\mathrm{Sel}^{\Sigma_0}_{E[p^\infty]}(\mathbb{Q}_\infty)^\vee$ is Λ-torsion and its μ-invariant equals μ_E.

4.2.4. Suppose that E_1 and E_2 are two elliptic curves defined over $\mathbb{Q}$, both with ordinary reduction at p. Suppose moreover that $E_1[p] \cong E_2[p]$ as $G_\mathbb{Q}$-modules. Let Σ denote the set of places that consists of all bad primes for E_1 and E_2, the prime p and the infinite place. Choose any subset Σ_0 of Σ which contains all places of bad reduction both for E_1 and E_2, but does not contain p and ∞.

4.2.4.1. Prove that the module $\mathrm{Sel}^{\Sigma_0}_{E_1[p^\infty]}(\mathbb{Q}_\infty)[p]$ has finite cardinality if and only if $\mathrm{Sel}^{\Sigma_0}_{E_2[p^\infty]}(\mathbb{Q}_\infty)[p]$ does.

4.2.4.2. Deduce that $\mu_{E_1} = 0$ if and only if $\mu_{E_2} = 0$.

A Selmer groups: Definitions and Examples

Let K be a number field and let R be a complete local noetherian $\mathbb{Z}_p$-algebra. Let M be a $R[[G_K]]$-module which is free of finite rank over R.

Definition A.1. *A* Selmer structure $\mathcal{F}$ *on* M *is a collection of the following data:*

- *A finite set* $\Sigma(\mathcal{F})$ *of places of* K*, including all infinite places and primes above* p *as well as all primes where* M *is ramified.*
- *For every* $\lambda \in \Sigma(\mathcal{F})$ *a local condition on* M*, i.e., a choice of* R*-submodule*

$$H^1_{\mathcal{F}}(K_\lambda, M) \subset H^1(K_\lambda, M).$$

Definition A.2. *The semi-local cohomology group at a rational prime ℓ is defined by setting*

$$H^i(K_\ell, M) := \bigoplus_{\lambda|\ell} H^i(K_\lambda, M),$$

where the direct sum is over all primes λ of K lying above ℓ.

Let λ be a prime of K. There is the perfect local Tate pairing

$$\langle\ ,\ \rangle_\lambda : H^1(K_\lambda, M) \otimes H^1(K_\lambda, M^*) \longrightarrow H^2(K_\lambda, \mu_{p^\infty}) \xrightarrow{\sim} \mathbb{Q}_p/\mathbb{Z}_p,$$

where $M^* := \mathrm{Hom}(M, \mu_{p^\infty})$ stands for the Cartier dual of M. For a Selmer structure $\mathcal{F}$ on M, define $H^1_{\mathcal{F}^*}(K_\lambda, M^*) := H^1_{\mathcal{F}}(k_\lambda, M)^\perp$ as the orthogonal complement of $H^1_{\mathcal{F}}(K_\lambda, M)$ with respect to the local Tate pairing. The Selmer structure $\mathcal{F}^*$ on M^*, with $\Sigma(\mathcal{F}) = \Sigma(\mathcal{F}^*)$, defined in this way will be called the *dual Selmer structure*.

Definition A.3. *If $\mathcal{F}$ is a Selmer structure on M, we define the* Selmer module $H^1_{\mathcal{F}}(K, M)$ *as*

$$H^1_{\mathcal{F}}(k, M) := \ker\left(H^1\left(\mathrm{Gal}(K_{\Sigma(\mathcal{F})}/K\right), M) \longrightarrow \bigoplus_{\lambda\in\Sigma(\mathcal{F})} H^1(K_\lambda, M)/H^1_{\mathcal{F}}(K_\lambda, M) \right),$$

where $K_{\Sigma(\mathcal{F})}$ is the maximal extension of K which is unramified outside $\Sigma(\mathcal{F})$. We also define the dual Selmer structure in a similar fashion; just replace M by M^* and $\mathcal{F}$ by $\mathcal{F}^*$ above.

Example A.4. (i) *Let $R = \mathbb{Z}_p$ and let M be a free R-module endowed with a continuous action of G_K, which is unramified outside a finite set of places of K. We define a Selmer structure $\mathcal{F}_{\mathrm{can}}$ on M by setting*

$$\Sigma(\mathcal{F}_{\mathrm{can}}) = \{\lambda : M \text{ is ramified at } \lambda\} \cup \{\wp|p\} \cup \{v|\infty\},$$

and

- *if $\lambda \in \Sigma(\mathcal{F}_{\mathrm{can}})$, $\lambda \nmid p\infty$, we define the local condition at λ to be*

$$H^1_{\mathcal{F}_{\mathrm{can}}}(K_\lambda, M) = \ker(H^1(K_\lambda, M) \longrightarrow H^1(K_\lambda^{\mathrm{ur}}, M \otimes \mathbb{Q}_p)),$$

  where K_λ^{ur} is the maximal unramified extension of K_λ;
- *if $\wp|p$, we define the local condition at $\wp$ by setting*

$$H^1_{\mathcal{F}_{\mathrm{can}}}(k_\wp, M) = H^1(k_\wp, M).$$

The Selmer structure $\mathcal{F}_{\mathrm{can}}$ is called the canonical Selmer structure *on M.*

(ii) *Let now $R = \Lambda$ be the cyclotomic Iwasawa algebra and let M be as in the previous example. We define a Selmer structure $\mathcal{F}_\Lambda$ on $\mathbb{M} := M \otimes \Lambda$ (which we endow with diagonal Galois action) by setting $\Sigma(\mathcal{F}_\Lambda) = \mathcal{F}_{\mathrm{can}}$ and $H^1_{\mathcal{F}_\Lambda}(K_\lambda, \mathbb{M}) = H^1(K_\lambda, \mathbb{M})$ for every $\lambda \in \Sigma(\mathcal{F}_\Lambda)$. A trivial extension of Problem 3.7.1 tells us that for any $\lambda \nmid p\infty$,*

$$H^1_{\mathcal{F}_\Lambda}(K_\lambda, \mathbb{M}) = \ker\left(H^1(K_\lambda, \mathbb{M}) \longrightarrow H^1(K_\lambda^{\mathrm{ur}}, \mathbb{M})\right)$$

consists of unramified classes.

As above, we then have a dual Selmer structure $\mathcal{F}^*_\Lambda$ on $\mathbb{M}^* := \mathrm{Hom}(\mathbb{M}, \mu_{p^\infty})$. In explicit terms, it is given by the local conditions $H^1_{\mathcal{F}^*_\Lambda}(K_\lambda, \mathbb{M}^*) = 0$ for $\lambda \in \Sigma(\mathcal{F}_{\mathrm{can}})$.

(iii) *For a general R (of characteristic zero) and M, we let $\mathcal{F}_{\mathrm{str}}$ denote the strict Selmer structure, which we define by setting*

$$\Sigma(\mathcal{F}_{\mathrm{str}}) = \{\lambda : M \text{ is ramified at } \lambda\} \cup \{\wp | p\} \cup \{v | \infty\},$$

and

- *if $\lambda \in \Sigma(\mathcal{F}_{\mathrm{str}})$, $\lambda \nmid p\infty$, we define the local condition at λ to be*

$$H^1_{\mathcal{F}_{\mathrm{str}}}(K_\lambda, M) = \ker(H^1(K_\lambda, M) \longrightarrow H^1(K_\lambda^{\mathrm{ur}}, M[1/p])),$$

- *if $\wp | p$, we define the local condition at $\wp$ by setting*

$$H^1_{\mathcal{F}_{\mathrm{can}}}(k_\wp, M) = 0.$$

Definition A.5. *Suppose that $\mathcal{F}$ is a local condition (at a prime λ of K) on M. If M' is a submodule of M* (resp. *M'' is a quotient module*), *then $\mathcal{F}$ induces local conditions (which we still denote by $\mathcal{F}$) on M'* (resp. *on M''*), *by taking $H^1_{\mathcal{F}}(k_\lambda, M')$ (resp. $H^1_{\mathcal{F}}(k_\lambda, M'')$) to be the inverse image* (resp. *the image*) *of $H^1_{\mathbb{F}}(k_\lambda, M)$ under the natural maps induced by*

$$M' \hookrightarrow M, \qquad M \twoheadrightarrow M''.$$

Propagation *of a local condition $\mathcal{F}$ on M to a submodule M' (and a quotient M'') of M is the local condition $\mathcal{F}$ on M' (and on M'') obtained following the above procedure.*

For example, if I is an ideal of R, then a local condition on M induces local conditions on M/IM and $M[I]$, by *propagation* (which is customarily denoted by the same symbol).

A.1 Greenberg local conditions and Selmer groups

For the sake of simplicity (and since we do not offer anything original in these notes anyway and there are certainly better places to learn more about this material we shall present), we shall only concentrate in the case when $K = \mathbb{Q}$.

Definition A.6. *Let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbb{Q}_p$. Suppose T is a free $\mathcal{O}$-module of finite rank which is endowed with a continuous action of $G_{\mathbb{Q}}$, that is unramified outside a finite set of places Σ (which we assume to contain p and ∞). Set $V := T \otimes \mathbb{Q}_p$ and $A := V/T$.*

We say that V (or T) is **geometric** *if V is de Rham as a $G_{\mathbb{Q}_p}$-representation.*

A geometric Galois representation V (or T) is **critical** *if the number of positive Hodge-Tate weights of $V|_{G_{\mathbb{Q}_p}}$ (counted with multiplicities) equals the dimension of the $+1$-eigenspace acting on V.*

Suppose h_+ denotes the number of positive Hodge-Tate weights of $V|_{G_{\mathbb{Q}_p}}$ (counted with multiplicities). We say that V satisfies the **Panchishkin condition** *if T contains a $G_{\mathbb{Q}_p}$-stable direct summand F_p^+T which has rank h_+ over $\mathcal{O}$ and whose all Hodge-Tate weights are positive as well as that the Hodge-Tate weights of T/F_p^+T are all non-negative.*

A critical V that satisfies Panchishkin condition is called **Panchishkin-ordinary**.

Exercise A.7. *Suppose f is a newform of weight k and let K_f denote its Hecke field, $\wp$ a fixed prime of K_f and finally, $M_{f,\wp}$ its $\wp$-adic Galois representation (with Hodge-Tate weights 0 and $k-1$) attached to f by Deligne. If $\mathrm{ord}_\wp a_p(f) = 0$, then it is known thanks to Wiles that $M_{f,\wp}$ is Panchishkin-ordinary. Determine all integers j such that $M_f(j)$ is Panchishkin-ordinary.*

Exercise A.8. *Suppose f and g are two newforms of respective weights k and l. Let F denote a common extension of K_f and K_g, and let $\wp$ be a prime of F. Let $M_{f,\wp}$ and $M_{g,\wp}$ denote Deligne's Galois representations. Suppose $\mathrm{ord}_\wp a_p(f)a_p(g) = 0$. Determine all integers j such that $M_{f,\wp} \otimes M_{g,\wp}(j)$ is Panchishkin-ordinary.*

Definition A.9 (Compact Greenberg Selmer groups)**.** *Suppose V is a Panchishkin-ordinary $G_{\mathbb{Q}}$-representation and $T \subset V$ is a $G_{\mathbb{Q}}$-stable lattice. Set*

$$F_p^- T := T/F_p^+ T\,.$$

We define the compact Greenberg Selmer group $H^1_{\mathcal{F}_{\mathrm{Gr}}}(\mathbb{Q}, T)$ by setting

$$H^1_{\mathcal{F}_{\mathrm{Gr}}}(\mathbb{Q}, T) := \ker\left(H^1(\mathbb{Q}_\Sigma/\mathbb{Q}, T) \longrightarrow \prod_{\ell \neq p\,,\, \ell \in \Sigma} H^1(\mathbb{Q}_\ell^{\mathrm{ur}}, V) \times H^1(\mathbb{Q}_p, F_p^- T) \right).$$

Likewise, set $F_p^-\mathbb{T} := F_p^- T \otimes \Lambda$ and define the compact Iwasawa theoretic Greenberg Selmer group by setting

$$H^1_{\mathcal{F}_{\mathrm{Gr}}}(\mathbb{Q}, \mathbb{T}) := \ker\left(H^1(\mathbb{Q}, \mathbb{T}) \longrightarrow H^1(\mathbb{Q}_p, F_p^-\mathbb{T}) \right).$$

Note that

$$H^1(\mathbb{Q}_\ell^{\mathrm{ur}}, \mathbb{T}) = 0, \forall \ell \neq p$$

according to Problem 3.7.1, so the classes that in $H^1_{\mathcal{F}_{\mathrm{Gr}}}(\mathbb{Q}, \mathbb{T})$ are unramified everywhere (away from p).

Definition A.10 (Discrete Greenberg Selmer groups)**.** *We retain the notation in the previous definition. We define the discrete Greenberg Selmer group* $H^1_{\mathcal{F}^*_{\mathrm{Gr}}}(\mathbb{Q}, T^*)$ *as the dual Selmer group, in the sense of Definition A.3. In more precise form,*

$$H^1_{\mathcal{F}_{\mathrm{Gr}}}(\mathbb{Q}, T^*) := \ker\left(H^1(\mathbb{Q}_\Sigma/\mathbb{Q}, T^*) \longrightarrow \prod_{\ell\neq p\,,\,\ell\in\Sigma} \frac{H^1(\mathbb{Q}_\ell, T^*)}{H^1_f(\mathbb{Q}_\ell, T^*)} \times H^1(\mathbb{Q}_p, F_p^- T^*) \right).$$

where

$$H^1_f(\mathbb{Q}_\ell, T^*) := \mathrm{im}\left(\ker\left(H^1(\mathbb{Q}_\ell, V^*) \to H^1(\mathbb{Q}_\ell^{\mathrm{ur}}, V^*)\right) \longrightarrow H^1(\mathbb{Q}_\ell, T^*)\right)$$

and $F_p^- T^* := \left(F_p^+ T\right)^*$.

Likewise, set $F_p^-\mathbb{T}^* := \left(F_p^+\mathbb{T}\right)^*$ *and define the discrete Iwasawa theoretic Greenberg Selmer group by setting*

$$H^1_{\mathcal{F}_{\mathrm{Gr}}}(\mathbb{Q}, \mathbb{T}^*) := \ker\left(H^1(\mathbb{Q}, \mathbb{T}^*) \longrightarrow \prod_{\ell\neq p\,,\,\ell\in\Sigma} H^1(\mathbb{Q}_\ell, \mathbb{T}^*) \times H^1(\mathbb{Q}_p, F_p^-\mathbb{T}^*) \right).$$

Exercise A.11. *Prove that*

$$H^1_f(\mathbb{Q}_\ell, T^*) \subset H^1_{\mathrm{ur}}(\mathbb{Q}_\ell, T^*) := \ker\left(H^1(\mathbb{Q}_\ell, T^*) \to H^1(\mathbb{Q}_\ell^{\mathrm{ur}}, T^*)\right)$$

and the quotient $H^1_{\mathrm{ur}}(\mathbb{Q}_\ell, T^*)/H^1_f(\mathbb{Q}_\ell, T^*)$ *is isomorphic to* $\left(\dfrac{H^0(I_\ell, T^*)}{H^0(I_\ell, T^*)_{\mathrm{div}}}\right)^{\mathrm{Fr}_\ell=1}$.

The cardinality of the latter $\mathbb{Z}_p$*-module is precisely the definition of the* p*-part of the Tamagawa number (due to Fontaine and Perrin-Riou).*

Remark A.12. *Greenberg has defined his Iwasawa theoretic Selmer group* $\mathrm{Sel}_{T^*}(\mathbb{Q}_\infty)_p$ *by setting*

$$\mathrm{Sel}_{T^*}(\mathbb{Q}_\infty)_p := \ker\left(H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T^*) \longrightarrow \prod_{\substack{\eta|\ell\neq p\\ \ell\in\Sigma}} H^1(I_\eta, T^*) \times H^1(I_{\infty,p}, F_p^- T^*) \right)$$

where I_η *is the inertia subgroup in* $G_{\mathbb{Q}_{\infty,\eta}}$ *for each prime* η *of* $\mathbb{Q}_\infty$ *as above and likewise,* $I_{\infty,p}$ *is the inertia group in* $G_{\mathbb{Q}_{\infty,p}}$ *at the unique prime of* $\mathbb{Q}_\infty$ *above* p *(that we also denote by* p*, by slight abuse).*

See Exercise A.15 where this is compared to the Selmer groups $H^1_{\mathcal{F}^*_{\mathrm{Gr}}}(\mathbb{Q}, \mathbb{T}^*)$ *introduced above in the particular case when* $V = V_p(E)$ *(or more generally, when* $V = M_{f,\wp}$*).*

Exercise A.13. *For* T^* *as above, prove that the natural map*

$$\mathrm{Hom}(\Lambda, T^*) =: \mathrm{Hom}(\Lambda, \mathrm{Hom}(T, \mu_{p^\infty})) \longrightarrow \mathrm{Hom}(T \otimes \Lambda, \mu_{p^\infty}) =: \mathbb{T}^*$$

is an isomorphism of $\Lambda[[G_{\mathbb{Q}}]]$*-modules.*

Exercise A.14. *Using the fact that the restriction maps induce an isomorphism*

$$\varinjlim_n H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_n, T^*) \xrightarrow{\text{res}} H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T^*)$$

is an isomorphism, prove that $H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T^*)$ is naturally isomorphic to $H^1(\mathbb{Q}_\Sigma/\mathbb{Q}, \mathbb{T}^*)$.

Exercise A.15. *Suppose $E_{/\mathbb{Q}}$ is an elliptic curve with ordinary reduction at p and set $T = T_p(E)$, $T^* = E[p^\infty]$* (HW*: Use Weil pairing to check that this choice of notation is consistent with our previous definitions*)*. In this case, it follows from a theorem of Lutz that*

$$\mathrm{Sel}_{T^*}(\mathbb{Q}_\infty)_p := \ker\left(H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, T^*) \longrightarrow \prod_{\substack{\eta|\ell\neq p \\ \ell\in\Sigma}} H^1(\mathbb{Q}_{\infty,\eta}, T^*) \times H^1(I_{\infty,p}, F_p^- T^*) \right).$$

Prove that we have an exact sequence

$$0 \longrightarrow H^1_{\mathcal{F}_{\mathrm{Gr}}}(\mathbb{Q}, \mathbb{T}^*) \longrightarrow \mathrm{Sel}_{T^*}(\mathbb{Q}_\infty)_p \longrightarrow M_p$$

where the module M_p depends only on $F_p^- T^*$ and it has finite cardinality unless E has split multiplicative reduction at p. In this case, deduce that the Iwasawa μ and λ-invariants of $H^1_{\mathcal{F}_{\mathrm{Gr}}}(\mathbb{Q}, \mathbb{T}^*)^\vee$ equal to μ_E and λ_E, respectively.

Prove analogous assertions for a general newform f that is ordinary at p (this once, relying on the local-global compatibility of Langlands' correspondence).