Introduction to Iwasawa Theory for Elliptic Curves

Ralph Greenberg

1 Mordell-Weil Groups.

Let E be an elliptic curve defined over $\mathbb{Q}$. Suppose that K is a finite extension of $\mathbb{Q}$. The famous Mordell-Weil Theorem states that the abelian group $E(K)$ of K-rational points on E is finitely generated. That is,

$$E(K) \cong \mathbb{Z}^r \times T \tag{1}$$

where $r = \mathrm{rank}_{\mathbb{Z}}(E(K))$ is a nonnegative integer and $T = E(K)_{\mathrm{tors}}$ is finite. Of course, this may fail to be true if K is an infinite extension of $\mathbb{Q}$. For example, let $\overline{\mathbb{Q}}$ denote the algebraic closure of $\mathbb{Q}$ in the complex numbers $\mathbb{C}$. Then

$$E(\overline{\mathbb{Q}})_{\mathrm{tors}} = E(\mathbb{C})_{\mathrm{tors}} \cong (\mathbb{Q}/\mathbb{Z})^2 \tag{2}$$

which is certainly not finite. Also, the quotient group $E(\overline{\mathbb{Q}})/E(\overline{\mathbb{Q}})_{\mathrm{tors}}$ has infinite rank. More precisely, $E(\overline{\mathbb{Q}})$ is a divisible group and so one can consider $E(\overline{\mathbb{Q}})/E(\overline{\mathbb{Q}})_{\mathrm{tors}}$ as a vector space over $\mathbb{Q}$. It turns out that its dimension is infinite. This is equivalent to the statement that $\mathrm{rank}_{\mathbb{Z}}(E(L))$ is unbounded as L varies over all finite extensions of $\mathbb{Q}$. A proof is outlined in exercises 1.5–1.8.

But there are infinite algebraic extensions K of $\mathbb{Q}$ such that $E(K)$ is finitely generated. The following simple theorem (pointed out by B. Mazur in [Ma1]) gives a sufficient (and obviously necessary) condition for Galois extensions.

Theorem 1.1 *Let K be a Galois extension of $\mathbb{Q}$. Assume that $E(K)_{\mathrm{tors}}$ is finite and that $\mathrm{rank}_{\mathbb{Z}}(E(L))$ is bounded as L varies over all finite extensions of $\mathbb{Q}$ contained in K. Then $E(K)$ is finitely generated.*

Proof. Choose a finite extension L of $\mathbb{Q}$ contained in K such that $\operatorname{rank}_{\mathbb{Z}}(E(L))$ is as large as possible. Then $E(K)/E(L)$ must be a torsion group. Suppose that $P \in E(K)$. Then there exists an integer $m \geq 1$ such that $mP \in E(L)$. Let $\sigma \in \operatorname{Gal}(K/L)$. Then

$$m(\sigma(P) - P) = \sigma(mP) - mP = O_E.$$

Therefore, $\sigma(P) - P \in E(K)_{\text{tors}}$. If $t = |E(K)_{\text{tors}}|$, then $t(\sigma(P) - P) = O_E$. That is, $\sigma(tP) = tP$ for all $\sigma \in \operatorname{Gal}(K/L)$. This implies that $tP \in E(L)$ for all $P \in E(K)$. Hence we can define a homomorphism $\varphi : E(K) \to E(L)$ by $\varphi(P) = tP$. The image of φ is finitely generated since it is a subgroup of $E(L)$. The kernel of φ is just $E(K)_{\text{tors}}$. It follows that $E(K)$ is indeed finitely generated. ■

Verifying the hypotheses of the above theorem is hard, especially the hypothesis concerning the behavior of $\operatorname{rank}_{\mathbb{Z}}(E(L))$. Here is one interesting and rather deep result, which is a consequence of theorems of K. Kato and D. Rohrlich.

Theorem 1.2 *Suppose that E is a modular elliptic curve. Let Σ be a finite set of primes. Then $\operatorname{rank}_{\mathbb{Z}}(E(L))$ is bounded as L varies over all finite, abelian extensions of $\mathbb{Q}$ which are unramified outside Σ.*

Suppose that $\Sigma = \{p_1, \ldots, p_n\}$. By the Kronecker-Weber theorem, the fields L in the above theorem are just the finite extensions of $\mathbb{Q}$ contained in $K = \mathbb{Q}(\mu_{p_1^\infty}, \ldots, \mu_{p_n^\infty})$, where, for any prime p, we let μ_{p^∞} denote the group of p-power roots of unity in $\overline{\mathbb{Q}}$. This field K is just $\mathbb{Q}_\Sigma^{\text{ab}}$, the maximal abelian extension of $\mathbb{Q}$ unramified outside Σ. A theorem of K. Ribet [Ri] implies that $E(\mathbb{Q}_\Sigma^{\text{ab}})_{\text{tors}}$ is finite. (His theorem is much stronger than this. It states that $A(F\mathbb{Q}^{\text{ab}})_{\text{tors}}$ is finite, where F is any number field, A is an abelian variety defined over F, and $\mathbb{Q}^{\text{ab}}$ is the maximal abelian extension of $\mathbb{Q}$.) Thus the hypotheses in theorem 1.1 are satisfied for $K = \mathbb{Q}_\Sigma^{\text{ab}}$ and one obtains the following consequence:

Theorem 1.3 *Suppose that E is modular and that Σ is any finite set of primes. Then $E(\mathbb{Q}_\Sigma^{\text{ab}})$ is finitely generated.*

One result which we will prove completely is the following theorem of B. Mazur (from [Ma1]). We will assume that K/F is a $\mathbb{Z}_p$-extension. That is, K/F is a Galois extension and $\operatorname{Gal}(K/F) \cong \mathbb{Z}_p$, the additive group of

p-adic integers. Since $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$, one could equivalently require that $K = \bigcup_n F_n$, where F_n is a cyclic extension of F of degree p^n and $F_n \subset F_{n+1}$ for all $n \geq 0$. If E is an elliptic curve defined over a number field F, we let $\text{Ш}_E(F)$ denote the corresponding Tate-Shafarevich group (which will be defined in Chapter 2), and $\text{Ш}_E(F)_p$ denotes its p-primary subgroup. Here is Mazur's theorem.

Theorem 1.4 *Suppose that E is an elliptic curve defined over a number field F. Let p be a prime such that E has good, ordinary reduction at all primes of F lying over p. Assume that both $E(F)$ and $\text{Ш}_E(F)_p$ are finite. Let $K = \bigcup_n F_n$ be a $\mathbb{Z}_p$-extension of F. Then* $\mathrm{rank}_{\mathbb{Z}}(E(F_n))$ *is bounded for $n \geq 0$.*

The proof of this theorem is a good illustration of the ideas of Iwasawa theory, but we wait until chapter 4 to describe it. The theorem is a consequence of Mazur's "Control Theorem" (which is the main result of chapter 4) together with basic results about the structure of modules over a certain ring Λ (which will be the subject of chapter 3). But instead of studying Mordell-Weil groups directly, we study the behavior of Selmer groups which are introduced in chapter 2. The assumption that E has good, ordinary reduction at primes over p is crucial. To briefly recall the definition, suppose that v is a prime of F where E has good reduction and let $\widetilde{E}_v$ denote the reduction of E modulo v (so that $\widetilde{E}_v$ is an elliptic curve over the residue field f_v of v). Let $p = \mathrm{char}(f_v)$ and let $\overline{f}_v$ denote an algebraic closure of f_v. If $\widetilde{E}_v(\overline{f}_v)$ has points of order p, then we say that $\widetilde{E}_v$ is ordinary and that E has ordinary reduction at v. Otherwise, we say that $\widetilde{E}_v$ is supersingular and that E has supersingular reduction at v.

If F is any number field and p is any prime, then there is one $\mathbb{Z}_p$-extension of F which can be described explicitly. It is a subfield of $F(\mu_{p^\infty})$. There is a canonical homomorphism

$$\chi : \mathrm{Gal}(F(\mu_{p^\infty})/F) \to \mathbb{Z}_p^\times$$

defined in the following way: Let $\sigma \in \mathrm{Gal}(F(\mu_{p^\infty})/F)$. Suppose that ζ_{p^n} is a primitive p^n-th root of unity. Then $\sigma(\zeta_{p^n}) = \zeta_{p^n}^{u_n}$, where $u_n \in \mathbb{Z}$ and $(u_n, p) = 1$. (Each u_n is only well-defined modulo p^n.) It is easy to see that $\{u_n\}$ is a Cauchy sequence in $\mathbb{Z}_p$ converging to a well-defined element $u \in \mathbb{Z}_p^\times$. We define $\chi(\sigma) = u$. Then $\sigma(\zeta) = \zeta^{\chi(\sigma)}$ for all $\zeta \in \mu_{p^\infty}$. (See exercises 1.1

and 1.2.) The homomorphism χ is continuous, injective, and its image has finite index in $\mathbb{Z}_p^\times$. Using the p-adic log, one sees that $\mathbb{Z}_p^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}_p$ if p is odd (or $\{\pm 1\} \times \mathbb{Z}_2$ if $p = 2$). One can then show that $\mathrm{im}(\chi) \cong \Delta \times \Gamma$, where Δ is a finite group and $\Gamma \cong \mathbb{Z}_p$. Therefore, there is a unique subfield F_∞ of $F(\mu_{p^\infty})$ such that $\mathrm{Gal}(F_\infty/F) \cong \Gamma \cong \mathbb{Z}_p$. F_∞ is called the "cyclotomic $\mathbb{Z}_p$-extension" of F.

If F is totally real, then it is conjectured that the only $\mathbb{Z}_p$-extension of F is the one constructed above. This is known as Leopoldt's conjecture. But if F is not totally real, then it turns out that there are infinitely many different $\mathbb{Z}_p$-extensions of F. For example, if F is an imaginary quadratic field, then, for any prime p, there exists a Galois extension $\widetilde{F}$ of F which contains all $\mathbb{Z}_p$-extensions of F and such that $\mathrm{Gal}(\widetilde{F}/F) \cong \mathbb{Z}_p^2$. Thus $\mathrm{Gal}(\widetilde{F}/F)$ has infinitely many (in fact uncountably many) quotients isomorphic to $\mathbb{Z}_p$, and each such quotient corresponds to $\mathrm{Gal}(F_\infty/F)$ for some F_∞. All of this can be proved by class field theory. There are two such $\mathbb{Z}_p$-extensions F_∞/F which have the property that $F_\infty/\mathbb{Q}$ is Galois. One of them is the cyclotomic $\mathbb{Z}_p$-extension F_∞^{c}/F, and then $\mathrm{Gal}(F_\infty^{\mathrm{c}}/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}_p$. In fact, $F_\infty^{\mathrm{c}} = F\mathbb{Q}_\infty$, where $\mathbb{Q}_\infty \subset \mathbb{Q}(\mu_{p^\infty})$ is the unique $\mathbb{Z}_p$-extension of $\mathbb{Q}$. The other is the so-called anticyclotomic $\mathbb{Z}_p$-extension F_∞^{ac}/F which is characterized by $F_\infty^{\mathrm{ac}} = \bigcup_n F_n^{\mathrm{ac}}$, $F_n^{\mathrm{ac}} \subset F_{n+1}^{\mathrm{ac}}$, where F_n^{ac} is Galois over $\mathbb{Q}$ and $\mathrm{Gal}(F_n^{\mathrm{ac}}/\mathbb{Q})$ is isomorphic to the dihedral group of order $2p^n$.

We can now state two more theorems, both of which are rather deep and will not be proven. (Their proofs are a combination of results of K. Rubin, myself, D. Rohrlich, and Gross-Zagier.)

Theorem 1.5 *Suppose that F is an imaginary quadratic field and that E is an elliptic curve defined over $\mathbb{Q}$ such that $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q} \cong F$. Suppose that p is any prime and that $F_\infty = \bigcup_n F_n$ is a $\mathbb{Z}_p$-extension of F. Assume that $F_\infty \neq F_\infty^{\mathrm{ac}}$. Then $\mathrm{rank}_{\mathbb{Z}}(E(F_n))$ is bounded for $n \geq 0$.*

Theorem 1.6 *Suppose that F and E are as in theorem 1.5. Let p be a prime where E has good reduction. Let $F_\infty^{\mathrm{ac}} = \bigcup_n F_n^{\mathrm{ac}}$ be the anticyclotomic $\mathbb{Z}_p$-extension.*

(i) If E has supersingular reduction at p, then $\mathrm{rank}_{\mathbb{Z}}(E(F_n^{\mathrm{ac}})) \to \infty$ as $n \to \infty$.

(ii) Assume that E has ordinary reduction at p. If the Hasse-Weil L-series $L(E/\mathbb{Q}, s)$ has an odd order zero at $s = 1$, then $\mathrm{rank}_{\mathbb{Z}}(E(F_n^{\mathrm{ac}})) \to \infty$

as $n \to \infty$. But if $L(E/\mathbb{Q}, s)$ has an even order zero at $s = 1$, then $\mathrm{rank}_{\mathbb{Z}}(E(F_n^{\mathrm{ac}}))$ is bounded for $n \geq 0$.

What one can prove is actually quite a bit more precise. Assume first that E has ordinary reduction at p and that $L(E/\mathbb{Q}, s)$ has an odd order zero at $s = 1$. Then the rank of $E(F_n^{\mathrm{ac}})$ grows quite regularly and is given by the formula

$$\mathrm{rank}_{\mathbb{Z}}(E(F_n^{\mathrm{ac}})) = 2p^n + c. \tag{3}$$

for all sufficiently large n, where c is some constant. That is, the rank increases by exactly $2\varphi(p^n)$ at the n-th layer for all $n \gg 0$. (Compare this with exercise 1.9.) On the other hand, if E has supersingular reduction, one has

$$\mathrm{rank}_{\mathbb{Z}}(E(F_n^{\mathrm{ac}})) - \mathrm{rank}_{\mathbb{Z}}(E(F_{n-1}^{\mathrm{ac}})) = \varepsilon_n \varphi(p^n) \tag{4}$$

for all sufficiently large n, where ε_n is either 0 or 2, depending just on the parity of n. That is, new points of infinite order appear in every other layer of the anticyclotomic $\mathbb{Z}_p$-extension of F. More precisely, if $L(E/\mathbb{Q}, s)$ has an even order zero at $s = 1$, then $\varepsilon_n = 0$ for odd n and $\varepsilon_n = 2$ for even n (and $n \gg 0$). The reverse holds when $\mathrm{ord}_{s=1}(L(E/\mathbb{Q}, s))$ is odd. We should remark that $\mathrm{rank}_{\mathbb{Z}}(E(L))$ must be even if L is any finite extension of F. This is simply because $E(L)$ is a module over the ring $R = \mathrm{End}(E)$, this ring is an order in F and hence $\mathrm{rank}_{\mathbb{Z}}(R) = 2$, and therefore $\mathrm{rank}_{\mathbb{Z}}(E(L)) = 2\,\mathrm{rank}_R(E(L))$.

The above theorems suggest that there are some systematic patterns influencing the behavior of $\mathrm{rank}_{\mathbb{Z}}(E(L))$ as L varies over finite extensions of $\mathbb{Q}$. The anticyclotomic $\mathbb{Z}_p$-extension of an imaginary quadratic field seems to play a special role. This turns out to be related to the following group theoretic fact. If G is a dihedral group, then g and g^{-1} are conjugate elements for all $g \in G$. The same statement is true for projective limits of dihedral groups such as $\mathrm{Gal}(F_\infty^{\mathrm{ac}}/\mathbb{Q})$, where F_∞^{ac} is the anticyclotomic $\mathbb{Z}_p$-extension of any imaginary quadratic field F (and for any prime p). Another profinite group with the property that g and g^{-1} are always conjugate is $G = \mathrm{PGL}_2(\mathbb{Z}_p)$. (See exercise 1.11.) This group can also be realized as a Galois group. For example, let E be an elliptic curve defined over $\mathbb{Q}$. For any prime p, let $T_p(E)$ denote the Tate module for E and p. Thus, $T_p(E) \cong \mathbb{Z}_p^2$ and $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts continuously and $\mathbb{Z}_p$-linearly on $T_p(E)$. This gives a homomorphism

$$\rho = \rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_{\mathbb{Z}_p}(T_p(E)) \cong \mathrm{GL}_2(\mathbb{Z}_p).$$

There is also an induced homomorphism $\widetilde{\rho}: \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{Z}_p)$. If $M = \overline{\mathbb{Q}}^{\ker(\rho)}$, then $\mathrm{Gal}(M/\mathbb{Q}) \cong \mathrm{im}(\rho)$. If E does not have complex multiplication (i.e., if $\mathrm{End}(E) = \mathbb{Z}$), then a theorem of Serre states that $\mathrm{im}(\rho)$ is of finite index in $\mathrm{GL}_2(\mathbb{Z}_p)$ for all p, with equality for all but finitely many p. Thus, for $p \gg 0$, $\mathrm{Gal}(M/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}_p)$, and M contains a subfield $K = \overline{\mathbb{Q}}^{\ker(\widetilde{\rho})}$ such that $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{PGL}_2(\mathbb{Z}_p)$. In addition, the symmetric groups S_n for $n \geq 1$ have the above conjugacy property, as well as any group of exponent 2. Suppose that G is any group with the above property. Then it is easy to see that the following property holds: *If χ is the character of any finite dimensional representation $\sigma : G \to \mathrm{GL}_n(\mathbb{C})$, then χ is real-valued.* Conversely, if G is a profinite group with this property, then G also has the property that g and g^{-1} are conjugate for all $g \in G$.

If K is any finite Galois extension of $\mathbb{Q}$, then there is a well-known factorization of the Dedekind zeta function $\zeta_K(s)$:

$$\zeta_K(s) = \prod_{\chi} L(\chi, s)^{d_\chi}$$

where χ runs over the characters of all irreducible representations over $\mathbb{C}$ of $\mathrm{Gal}(K/\mathbb{Q})$ and d_χ denotes the dimensional of the corresponding representation. The factor $L(\chi, s)$ is the Artin L-function associated to χ (or to the $\mathbb{C}$-representation it determines), which is defined by a certain Euler product. The well-known functional equation for $\zeta_K(s)$ relates the values $\zeta_K(s)$ and $\zeta_K(1-s)$. The functional equation for $L(\chi, s)$ relates the values $L(\chi, s)$ and $L(\overline{\chi}, 1-s)$. Of course, $\overline{\chi}$ is the character of $\mathrm{Gal}(K/\mathbb{Q})$ obtained by complex conjugation, which is also irreducible. If E is an elliptic curve defined over $\mathbb{Q}$, then the Hasse-Weil L-function $L(E/K, s)$ is conjectured to have an analytic continuation to the entire complex plane and to satisfy a functional equation relating the values $L(E/K, s)$ to $L(E/K, 2-s)$. But one can define L-functions $L(E/\mathbb{Q}, \chi, s)$ for every irreducible character χ of $\mathrm{Gal}(K/\mathbb{Q})$, again by a certain Euler product. One then has a factorization (which is proved by a formal calculation with the Euler factors):

$$L(E/K, s) = \prod_{\chi} L(E/\mathbb{Q}, \chi, s)^{d_\chi} \tag{5}$$

where χ runs over the characters of the irreducible $\mathbb{C}$-representations of $\mathrm{Gal}(K/\mathbb{Q})$ as before. There is a conjectural functional equation which relates $L(E/\mathbb{Q}, \chi, s)$ to $L(E/\mathbb{Q}, \overline{\chi}, 2-s)$. More precisely, it takes the following form. Let $\Lambda(E/\mathbb{Q},\chi,s) = A_\chi^s \Gamma(s)^{d_\chi} L(E/\mathbb{Q},\chi,s)$, where A_χ is a certain positive constant. Then the conjectured functional equation is

$$\Lambda(E/\mathbb{Q},\chi,s) = w(E,\chi)\Lambda(E/\mathbb{Q},\overline{\chi},2-s) \tag{6}$$

and the so-called root number $w(E,\chi)$ is a complex number of absolute value 1. If χ is real-valued, then $\overline{\chi} = \chi$, and $w(E,\chi) = \pm 1$. If one considers the power series expansion of $\Lambda(E/\mathbb{Q},\chi,s)$ about $s = 1$ (assuming the conjectured analyticity), it is easy to see that

$$w(E,\chi) = (-1)^{\mathrm{ord}_{s=1}(L(E/\mathbb{Q},\chi,s))}.$$

In particular, if $w(E,\chi) = -1$, then $L(E/\mathbb{Q},\chi,1) = 0$, and this would contribute at least d_χ to the order of vanishing of $L(E/K,s)$ at $s = 1$.

If σ is the irreducible representation with character χ, then we can regard σ as a continuous, finite-dimensional, complex representation of $G_{\mathbb{Q}}$. Every such representation σ factors through $\mathrm{Gal}(K/\mathbb{Q})$ for some finite, Galois extension $K/\mathbb{Q}$. The definition of $L(E/\mathbb{Q},\chi,s)$ does not depend on the choice of $K/\mathbb{Q}$.

The conjectures about L-functions and their analytic continuation even provide conjectural values for the root numbers. We will mention one useful formula. Let w_E denote the root number for $L(E/\mathbb{Q},s)$. Thus $w_E = (-1)^{\mathrm{ord}_{s=1}(L(E/\mathbb{Q},s))}$. Let N_E denote the conductor of the elliptic curve E (which is a product of certain powers of the primes where E has bad reduction). If σ is the representation of $G_{\mathbb{Q}}$ with character χ, let $K_\chi = \overline{\mathbb{Q}}^{\ker(\sigma)}$. Thus σ can be regarded as a faithful representation of $\mathrm{Gal}(K_\chi/\mathbb{Q})$. We let N_χ denote the conductor of χ, which is a certain product of the primes ramified in $K_\chi/\mathbb{Q}$. Assume that $(N_E, N_\chi) = 1$. Let $\delta_\chi = \det(\sigma)$, which can be regarded as a Dirichlet character. Then it turns out that

$$\omega(E,\chi) = \delta_\chi(-N_E)\omega_E^{d_\chi}. \tag{7}$$

For a proof that the conjectural root number turns out to be given by (7), see proposition 10 in [Ro4]. It follows that under the hypothesis that $(N_E, N_\chi) = 1$, the value of $\omega(E,\chi)$ depends only on δ_χ, N_E, ω_E, and the parity of d_χ.

Suppose for example that $d_\chi = 1$ so that χ can be regarded as a Dirichlet character whose conductor is relatively prime to N_E. The L-function $L(E/\mathbb{Q},\chi,s)$ then has a simple description in terms of $L(E/\mathbb{Q},s)$. If we write $L(E/\mathbb{Q}, s)$ as the Dirichlet series $\sum\limits_{n=1}^{\infty} a_n n^{-s}$, then

$$L(E/\mathbb{Q}, \chi, s) = \sum_{n=1}^{\infty} a_n \chi(n) n^{-s}.$$

It is only when χ is real-valued that the functional equation can force the function $L(E/\mathbb{Q}, \chi, s)$ to vanish at $s = 1$. According to (7), the sign in the functional equation is then $w(E, \chi) = \chi(-N_E)w_E$.

Suppose that K is Galois over $\mathbb{Q}$ and $G = \mathrm{Gal}(K/\mathbb{Q})$ is dihedral of order $2n$, where n is odd. The irreducible representations of G over $\mathbb{C}$ are all 2-dimensional except for the two which factor through $G/G' \cong \mathbb{Z}/2\mathbb{Z}$. Let σ be any such 2-dimensional representation and let χ denote its character. Then χ is real-valued and δ_χ is the nontrivial character φ of $\mathrm{Gal}(F/\mathbb{Q})$, where $F = K^{G'}$ is the unique quadratic field contained in K. Assuming that the primes dividing N_E are unramified in $K/\mathbb{Q}$, the sign in the functional equation for $L(E/\mathbb{Q}, \chi, s)$ is $\varphi(-N_E)$.

As another example, suppose that E' is an elliptic curve without complex multiplication whose conductor is relatively prime to the conductor of E. Let p be a prime. By Serre's theorem, the representation $\rho_{E'} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_p)$ giving the action of $G_{\mathbb{Q}}$ on $E'[p^\infty]$ is surjective for all but finitely many primes p. Let p be any such prime. Thus $\mathrm{Gal}(\mathbb{Q}(E'[p^\infty])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}_p)$ and $\mathbb{Q}(E'[p^\infty])$ contains a subfield K such that $G = \mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{PGL}_2(\mathbb{Z}_p)$. ($K$ is the field $\overline{\mathbb{Q}}^{\ker(\tilde{\rho}_{E',p})}$.) If χ is the character of an irreducible representation of G, then χ is real-valued. This follows from exercise 1.11. Also d_χ is even for all but finitely many χ's, and δ_χ is one of the two characters of $G/G' \cong \mathbb{Z}/2\mathbb{Z}$. The field $F = K^{G'}$ is the unique quadratic subfield of $\mathbb{Q}(\mu_{p^\infty}) : F = \mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}} p}\right)$. Each of these two characters occurs as δ_χ for infinitely many χ's. If d_χ is even, then $w(E, \chi) = \delta_\chi(-N_E)$. In particular, if $(\frac{-N_E}{p}) = -1$ then both signs ± 1 occur infinitely often in the functional equations for $L(E/\mathbb{Q}, \chi, s)$, but if $(\frac{-N_E}{p}) = +1$, then the signs are $+1$ (with finitely many exceptions) and so the functional equation will not force $L(E/\mathbb{Q}, \chi, 1)$ to vanish.

All of these remarks are relevant to the behavior of the ranks of Mordell-Weil groups because of the Birch and Swinnerton-Dyer conjecture which states in part that, for any finite extension K of $\mathbb{Q}$, we should have

$$\mathrm{rank}_{\mathbb{Z}}(E(K)) = \mathrm{ord}_{s=1}(L(E/K, s)). \tag{8}$$

There is a refined version of this conjecture which is suggested by the factorization (5). Assume that $K/\mathbb{Q}$ is Galois and let $G = \mathrm{Gal}(K/\mathbb{Q})$. Then G acts on $E(K)$ and one can consider the finite-dimensional representation space $E(K) \otimes_{\mathbb{Z}} \mathbb{C}$. Its dimension is $\mathrm{rank}_{\mathbb{Z}}(E(K))$. We have a decomposition as a direct sum of irreducible representations

$$E(K) \otimes_{\mathbb{Z}} \mathbb{C} \cong \bigoplus_{\chi} V_{\chi}^{m_\chi(E)} \tag{9}$$

where χ varies over the irreducible characters of G and V_χ denotes the underlying vector space for the corresponding representation of G. The multiplicities $m_\chi(E)$ are nonnegative integers which depend only on E and χ, and not on the choice of Galois extension $K/\mathbb{Q}$. (See exercise 1.3.) If χ_0 is the character of the trivial representation of G, then $m_{\chi_0}(E) = \mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q}))$. Also, if τ is any automorphism of the field $\mathbb{Q}(\chi)$ generated by the values of χ, then the conjugate character χ^τ is the character of another irreducible representation of G and one can easily show that $m_{\chi^\tau}(E) = m_\chi(E)$ for all such τ. (This is exercise 1.4.)

If $K/\mathbb{Q}$ is a finite Galois extension, then it is clear that

$$\mathrm{rank}_{\mathbb{Z}}(E(K)) = \sum_{\chi} d_\chi m_\chi(E) \tag{10}$$

where χ runs over the irreducible character of $G = \mathrm{Gal}(K/\mathbb{Q})$. Assuming analytic continuation, it is also clear from (5) that

$$\mathrm{ord}_{s=1}(L(E/K,s)) = \sum_{\chi} d_\chi \,\mathrm{ord}_{s=1}(L(E/\mathbb{Q},\chi,s)). \tag{11}$$

The refined version of the Birch and Swinnerton-Dyer conjecture states that

$$m_\chi(E) = \mathrm{ord}_{s=1}(L(E/\mathbb{Q},\chi,s)) \tag{12}$$

for every irreducible character χ of G.

We can now say a little more about the proofs of some of the theorems stated earlier. If we use (10) for $K = L$, where L is any finite, abelian extension of $\mathbb{Q}$ unramified outside Σ, then theorem 1.2 amounts to the assertion that $m_\chi(E) = 0$ for all but finitely many one-dimensional characters χ such that $K_\chi/\mathbb{Q}$ is unramified outside Σ. Such χ's can be identified with Dirichlet characters whose conductor is divisible only by primes in Σ. Therefore, theorem 1.2 is a consequence of the following two theorems.

Theorem 1.7 (Rohrlich [Ro1, Ro3]) *Suppose that E is a modular elliptic curve and let Σ be a finite set of primes. Then $L(E/\mathbb{Q}, \chi, 1) \neq 0$ for all but finitely many Dirichlet character χ whose conductors are divisible only by primes in Σ.*

Theorem 1.8 (Kato) *Suppose that E is a modular elliptic curve and that χ is a one-dimensional character of* $\mathrm{Gal}(K/\mathbb{Q})$ *for some abelian extension $K/\mathbb{Q}$. Assume that $L(E/\mathbb{Q}, \chi, 1) \neq 0$. Then $m_\chi(E) = 0$.*

As a special case, let $\mathbb{Q}_\infty = \bigcup_n \mathbb{Q}_n$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$, where p is any prime. Then theorem 1.2 implies that $\mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q}_n))$ is bounded, which means that there is an integer $n_0 = n_0(E, p)$ such that $\mathrm{rank}(E(\mathbb{Q}_n)) = \mathrm{rank}(E(\mathbb{Q}_{n_0}))$ for all $n \geq n_0$. Can $n_0(E, p)$ be chosen independently of E and/or p? We know nothing about this question. But here are some examples.

(1) $E : y^2 + xy = x^3 - 3x + 1$ and $p = 3$. Then $N_E = 34$. It turns out that $\mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q})) = 0$, but $\mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q}_n)) = 2$ for all $n \geq 1$. For each of the two faithful characters χ of $\mathrm{Gal}(\mathbb{Q}_1/\mathbb{Q})$, we have $m_\chi(E) = 1$. A point of infinite order on $E(\mathbb{Q}_1)$ is $P = (\beta, -\beta)$ where $\beta = \zeta_9 + \zeta_9^{-1}$ and ζ_9 is a primitive 9-th root of unity. (Note: $\mathbb{Q}_1$ is the maximal real subfield of $\mathbb{Q}(\zeta_9)$ and is generated over $\mathbb{Q}$ by β.) It is easy to check that $P \in E(\mathbb{Q}_1)$. To see that it has infinite order, it is enough to verify that $E(\mathbb{Q}_1)_{\mathrm{tors}} = E(\mathbb{Q})_{\mathrm{tors}}$. Now $E(\mathbb{Q})_{\mathrm{tors}}$ also has order 2. (Cremona's tables [Cre] give all of the needed data about this and other examples.) We must show that $E(\mathbb{Q}_1)_{\mathrm{tors}}$ also has order 2. Let η denote the unique prime of $\mathbb{Q}_1$, lying above 3. The residue field of η is $\mathbb{F}_3$ and one can verify that $\widetilde{E}(\mathbb{F}_3)$ has order 6. But the reduction map $E(\mathbb{Q}_1)_{\mathrm{tors}} \to \widetilde{E}(\mathbb{F}_3)$ is injective on the prime-to-3 torsion. (See proposition 3.1 in [Si1]. This standard result will also be very helpful in several exercises.) Also by exercise 1.13, one sees that the 3-primary subgroup of $E(\mathbb{Q}_1)_{\mathrm{tors}}$ is trivial and so $E(\mathbb{Q}_1)_{\mathrm{tors}}$ does indeed have order 2.

(2) $E : y^2 + xy = x^3 - 115x + 392$ and $p = 2$. Then $N_E = 195$. It turns out that $E(\mathbb{Q})$ is finite (of order 8). Now $\mathbb{Q}_1 = \mathbb{Q}(\sqrt{2})$ and $P = (0, 14\sqrt{2}) \in E(\mathbb{Q}_1)$. But one can check that $E(\mathbb{Q}_1)_{\mathrm{tors}}$ still has order 8. (Consider the reduction of E at the primes of $\mathbb{Q}_1$ lying over 2 and over 7.) Hence P must have infinite order. It turns out that $\mathrm{rank}(E(\mathbb{Q}_1)) = 1$. Now $\mathbb{Q}_2 = \mathbb{Q}_1(\sqrt{1 + \sqrt{2}})$ and, with the assistance of a computer, one can explicitly find a point $Q \in E(\mathbb{Q}_2)$ such that $Tr_{\mathbb{Q}_2/\mathbb{Q}_1}(Q) = O_E$. One can also verify that $E(\mathbb{Q}_2)_{\mathrm{tors}} = E(\mathbb{Q})_{\mathrm{tors}}$.

(See exercise 3.10, where a proof that $E(\mathbb{Q}_\infty)_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}$ is outlined.) Using these facts, it is not hard to show that Q and P are independent and that $\text{rank}(E(\mathbb{Q}_2)) \geq 3$. For a more detailed discussion of this example, see [Gre2], page 88 where it is shown that $\text{rank}(E(\mathbb{Q}_2)) = 3$ and that there is no further increase in the rank, i.e., $\text{rank}(E(\mathbb{Q}_n)) = 3$ for all $n \geq 2$.

Remark. According to a theorem of Rohrlich [Ro5], there should be examples of elliptic curves E such that $\text{rank}(E(\mathbb{Q}_n)) > \text{rank}(E(\mathbb{Q}_{n-1}))$ if $[\mathbb{Q}_n : \mathbb{Q}] \leq 9$, i.e., if $p = 2$, $n = 1, 2$, or 3, $p = 3$, $n = 1$ or 2, and $p = 5$ or 7, $n = 1$.

Let Σ be a fixed finite set of primes, E a fixed elliptic curve defined over $\mathbb{Q}$, and d a fixed positive integer. Theorem 1.2 suggests the following question. Let χ vary over all irreducible characters of $\text{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q})$ such that $d_\chi = d$. What can one say about the behavior of $m_\chi(E)$? (Note: $\mathbb{Q}_\Sigma$ denotes the compositum of all finite extensions of $\mathbb{Q}$ unramified outside Σ. A continuous finite-dimensional representation $\sigma : \text{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}) \to \text{GL}_d(\mathbb{C})$ must factor through a quotient group $\text{Gal}(K/\mathbb{Q})$ for some finite Galois extension K of $\mathbb{Q}$. We are letting χ vary over the characters of all such irreducible representations σ.)

Theorems 1.2, 1.7, and 1.8 concern the case where $d = 1$. Only finitely many χ's will be real-valued. Thus theorem 1.7 really concerns the values $L(E/\mathbb{Q}, \chi, 1)$ where $\chi \neq \overline{\chi}$ and these values *cannot* be forced to vanish by the functional equations. If χ is real-valued, then theorem 1.8 is a result of Kolyvagin. In the special case where E has complex multiplication, then theorem 1.8 is a consequence of a theorem of Rubin (generalizing the Coates-Wiles Theorem proved in [C-W].

Let $d = 2$. There may be infinitely many χ's such that $d_\chi = 2$ and $\chi = \overline{\chi}$. Suppose for example that $\mathbb{Q}_\Sigma$ contains an imaginary quadratic field F and let F_∞^{ac} be the anticyclotomic $\mathbb{Z}_p$-extension of F for some $p \in \Sigma$. Then $F_\infty^{\text{ac}} \subset \mathbb{Q}_\Sigma$. (See exercise 1.14.) All the irreducible characters of $\text{Gal}(F_\infty^{\text{ac}}/\mathbb{Q})$ will be real-valued and all but finitely many will be 2-dimensional. In light of theorems 1.7 and 1.8, it is natural to make the following *tentative* conjecture.

(1) *Let χ vary over all irreducible 2-dimensional characters of* $\text{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q})$ *such that $\chi \neq \overline{\chi}$. Then $L(E/\mathbb{Q}, \chi, 1) \neq 0$ and $m_\chi(E) = 0$ for all but finitely many such χ's.*

As for the real-valued characters, the following conjecture seems natural (but also very tentative.)

(2) *Assume that E does not have complex multiplication. Let χ vary over all irreducible 2-dimensional characters of* $\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q})$ *such that $\chi = \overline{\chi}$. Then, for all but finitely many such χ's, (a) $L(E/\mathbb{Q}, \chi, 1) \neq 0$ and $m_\chi(E) = 0$ if $w(E, \chi) = +1$, and (b) $L'(E/\mathbb{Q}, \chi, 1) \neq 0$ and $m_\chi(E) = 1$ if $w(E, \chi) = -1$.*

Virtually nothing is known to support these conjectures. It may suffice to allow χ to vary over irreducible representations of any fixed dimension d, but as a later example will show, some restriction on d_χ is necessary at least for the second conjecture.

Theorem 1.5 is a consequence of the first conjecture (and is really the only supporting evidence we have). Suppose that E satisfies the hypotheses in that theorem. If F_∞ is the cyclotomic $\mathbb{Z}_p$-extension of the imaginary quadratic field F, then the conclusion of theorem 1.5 follows from theorem 1.2 and is valid for any modular elliptic curve. If F_∞ is any other $\mathbb{Z}_p$-extension of F (except F_∞^{ac}), then F_n will not be Galois over $\mathbb{Q}$ for $n \gg 0$. Nevertheless it is possible to factor $L(E/F_n, s)$ as a certain product of L-functions of the form $L(E/\mathbb{Q}, \chi, s)$ for suitable irreducible characters χ of $\mathrm{Gal}(K/\mathbb{Q})$, where K is a Galois extension of $\mathbb{Q}$ containing F_n. Also, $\mathrm{rank}_{\mathbb{Z}}(E(F_n))$ can be expressed as the corresponding sum of the quantities $m_\chi(E)$. The χ's which occur here will mostly be the characters of the irreducible 2-dimensional representations of $G_{\mathbb{Q}}$ induced form the 1-dimensional representations ρ of G_F which factor through $\mathrm{Gal}(F_n/F)$. With finitely many exceptions, we will have $\chi \neq \overline{\chi}$ and so the first conjecture above would imply that $L(E/\mathbb{Q}, \chi, 1) \neq 0$ and $m_\chi(E) = 0$ for all but finitely many such χ's. One can actually prove these statements (assuming E has complex multiplication by F) and deduce that $\mathrm{rank}(E(F_n))$ is indeed bounded.

Theorem 1.6 is somewhat different, but is still an illustration of the same philosophy. The difference is that if χ is an irreducible character of dimension 2 for the dihedral group $\mathrm{Gal}(F_n^{\mathrm{ac}}/\mathbb{Q})$ and if E has complex multiplication by F, then $L(E/\mathbb{Q}, \chi, s)$ can itself be factored in a natural way as a product of two L-functions and it is the signs in the functional equations for these L-functions which explain the results stated in theorem 1.6. This is the so-called "exceptional case" in the terminology of Mazur's ICM talk [Ma2] on this topic.

The next example was a real surprise to me. The possibility of such an example was suggested by L. Howe. Let E be the elliptic curve defined by the equation

$$E : y^2 + y = x^3 - x. \tag{13}$$

Then E has conductor 37. (There are four elliptic curves of conductor 37, falling into two isogeny classes. We could take E to be any of these curves for this example.) Let E' be the elliptic curve defined by the equation

$$E' : y^2 + xy + y = x^3 + x^2 - 8x + 6. \tag{14}$$

The conductor of E' is 1225. The special property that this elliptic curve has is that it admits an isogeny defined over $\mathbb{Q}$ of degree 37. That is, there is another elliptic curve E'' defined over $\mathbb{Q}$ (whose equation we won't bother to write down) and a $\mathbb{Q}$-isogeny $\varphi : E' \to E''$ such that $\Phi = \ker(\varphi)$ has order 37. E' and E'' don't have complex multiplication and so Serre's theorem implies that $\mathrm{Gal}(\mathbb{Q}(E'[p^\infty])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}_p)$ for all but finitely many primes p. Pick one such prime (except $p = 2$ or $p = 37$). As mentioned earlier, $\mathbb{Q}(E'[p^\infty])$ then contains a subfield K such that $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{PGL}_2(\mathbb{Z}_p)$ and every irreducible character χ of $\mathrm{Gal}(K/\mathbb{Q})$ is real-valued. Note that $N_E = 37$ and N_χ is a product of the primes 5, 7, and p. Hence $(N_E, N_\chi) = 1$ and so (as discussed earlier), we have $w(E, \chi) = \delta_\chi(-37)w_E^{d_\chi}$. (For the above choice of E, we have $w_E = -1$.) Assume now that $(\frac{-37}{p}) = +1$. Then $w(E, \chi) = +1$ for all irreducible characters χ of $\mathrm{Gal}(K/\mathbb{Q})$ which have even dimension (which means all but four). Thus one might guess that $L(E/\mathbb{Q}, \chi, 1) \neq 0$ and $m_\chi(E) = 0$ for all but finitely many such χ's and therefore that $\mathrm{rank}(E(L))$ is bounded as L varies over the finite extensions of $\mathbb{Q}$ contained in K. Using exercise 1.12 and theorem 1.1, one would then conclude that $E(K)$ is finitely generated. But this turns out not to be so. One can in fact construct many points on $E(K)$ by using the projection map $\pi_0 : X_0(37) \to E$.

Suppose more generally that E is any elliptic curve defined over $\mathbb{Q}$ and that there is a curve X defined over $\mathbb{Q}$ of genus at least 2 together with a nonconstant rational map $\pi : X \to E$, also defined over $\mathbb{Q}$. The following lemma is quite useful for systematically constructing points on E.

Lemma 1.9 *Let K be a Galois extension of $\mathbb{Q}$ such that only finitely many primes of $\mathbb{Q}$ are ramified in $K/\mathbb{Q}$. Assume that $E(K)_{\mathrm{tors}}$ is finite and that $X(K)$ is infinite. Then* $\mathrm{rank}(E(L))$ *is unbounded as L varies over the finite extensions of $\mathbb{Q}$ contained in K.*

Proof. Assume to the contrary that $E(L)$ has bounded rank. Then, by theorem 1.1, there is a finite extension L of $\mathbb{Q}$ contained in K such that $E(K) = E(L)$. Now by a theorem of Faltings (formerly known as the Mordell Conjecture), $X(L)$ is finite. But $X(K)$ is infinite and so we can pick a point $x \in X(K)$ such that $x \notin X(L)$. Then $\pi(x) \in E(K) = E(L)$. Also, for any $g \in \mathrm{Gal}(K/L)$, we have $\pi(g(x)) = g(\pi(x)) = \pi(x)$. That is, if we let $P = \pi(x)$, then

$$\{g(x)\}_{g\in\mathrm{Gal}(K/L)} \subset \pi^{-1}(P).$$

Let $n = \deg(\pi)$. Then $\pi^{-1}(P)$ has at most n elements. (One can think of the map $\pi : X(\mathbb{C}) \to E(\mathbb{C})$ as an n-sheeted covering of Riemann surfaces.) It follows that, for every $x \in X(K)$, $[L(x) : L] \leq n$. Thus $[L(x) : \mathbb{Q}]$ is bounded and $L(x)/\mathbb{Q}$ can be ramified only at primes in the fixed finite set of primes ramified in $K/\mathbb{Q}$. By a well-known theorem of Hermite, there can only be finitely many possibilities for the field $L(x)$ as x varies over $X(K)$. Hence there must be a finite extension L' of L contained in K such that $X(K) = X(L')$. But this contradicts the theorem of Faltings. ■

To apply this lemma to the example, we take X to be the curve defined by the modular equation $f_{37}(x, y) = 0$. For any N, the modular polynomial $f_N(x, y)$ is an element of $\mathbb{Z}[x, y]$, irreducible over $\mathbb{C}$, such that the solutions over $\mathbb{C}$ of the equation $f_N(x, y) = 0$ are the points of the form $(j(z), j(Nz))$. Recall that $j(z)$ is defined for all z in the upper half-plane $\mathcal{H}$ and is just the j-invariant of the elliptic curve $E' = \mathbb{C}/(\mathbb{Z}1 + \mathbb{Z}z)\Omega$, where Ω is any nonzero complex number. The isomorphism class of an elliptic curve over $\mathbb{C}$ is determined by its j-invariant. Now $E'' = \mathbb{C}/(\mathbb{Z}1 + \mathbb{Z}Nz)\Omega$ has j-invariant $j(Nz)$, and the pair (E', E'') could be any pair of elliptic curves connected by a cyclic isogeny of degree N. Thus if X is defined by $f_N(x, y) = 0$, then the points on $X(K)$ correspond to such pairs where E' and E'' are both defined over K. The curve X is birationally equivalent over $\mathbb{Q}$ to the curve $X_0(N)$ and hence has the same genus.

Let $N = 37$ and let E', E'' be as specified earlier. (E' is defined by the equation (14) and $E'' = E'/\Phi$ where Φ has order 37.) Both E' and E'' are defined over $\mathbb{Q}$. Now let Π be any cyclic subgroup of $E'[p^\infty]$ of order p^m where $m \geq 1$. Let E'_Π denote the elliptic curve E'/Π which is defined over the field $\mathbb{Q}(E'[p^\infty])$. Let $g \in \mathrm{Gal}(E'[p^\infty]/K)$. Then g acts on $E'[p^\infty]$ as a scalar and so $g(\Pi) = \Pi$. That means that the j-invariant of E'_Π is fixed by g and so belongs to K. Since $p \neq 37$, $\varphi(\Pi)$ is a cyclic subgroup of $E''[p^\infty]$ of order p^m. Letting $E''_\Pi = E''/\varphi(\Pi)$, we have that E''_Π is also defined over K. Obviously E'_Π and E''_Π are related by an isogeny of degree 37 and so the pair (E'_Π, E''_Π) corresponds to a point on X defined over K. These are all distinct points for different choices of Π. (Here is a sketch of the reason. Suppose that Π_1 and Π_2 are cyclic subgroups of $E'[p^\infty]$ of order p^m. If $(E'_{\Pi_1}, E''_{\Pi_1})$ and $(E'_{\Pi_2}, E''_{\Pi_2})$ correspond to the same point of X, then E'_{Π_1} and E'_{Π_2} have the same j-invariant and so there would be an isomorphism $\varepsilon : E'_{\Pi_1} \xrightarrow{\sim} E'_{\Pi_2}$ defined over $\mathbb{C}$. For $i = 1, 2$, let $\varphi_i : E' \to E'_{\Pi_i}$ be the natural isogeny with kernel Π_i and let $\widehat{\varphi}_i$ denote the dual isogeny. Then $\widehat{\varphi}_2 \circ \varphi_2$ and $\widehat{\varphi}_2 \circ \varepsilon \circ \varphi_1$ are both in $\mathrm{End}(E')$ and have the same degree (namely p^{2m}). Since $\mathrm{End}(E') = \mathbb{Z}$, we have $\widehat{\varphi}_2 \circ \varphi_2 = p^m$ and $\widehat{\varphi}_2 \circ \varepsilon \circ \varphi_1 = \pm p^m$, which implies that $\varphi_2 = \pm\varepsilon \circ \varphi_1$ and hence $\Pi_1 = \Pi_2$.) Therefore, $X(K)$ is indeed infinite.

Now only 5, 7, and p are ramified in $K/\mathbb{Q}$. By exercise 1.12, $E(K)_{\mathrm{tors}}$ is finite. Also, as we mentioned above, X is birationally equivalent to $X_0(37)$ over $\mathbb{Q}$, which is known to have genus 2, and composing a rational map from X to $X_0(37)$ with π_0 gives a nonconstant rational map $\pi : X \to E$ defined over $\mathbb{Q}$. Hence lemma 1.9 implies that $E(K)$ has infinite rank.

Thus, if E, K, and p are as above (including the hypothesis that $(\frac{-37}{p}) = +1$), then as χ varies over the irreducible characters of $\mathrm{Gal}(K/\mathbb{Q})$ such that d_χ is even (all but finitely many), the root numbers $w(E,\chi)$ should all be $+1$, $\mathrm{ord}_{s=1}(L(E,\chi,s))$ should be even, $m_\chi(E)$ should be positive for infinitely many χ's, and therefore the conjecture in (12) asserts that infinitely many of the functions $L(E,\chi,s)$ should have at least a double zero at $s = 1$. In the case where $(\frac{-37}{p}) = -1$, L. Howe has systematically calculated the root numbers $w(E,\chi)$ in [Ho]. Assuming just that $m_\chi(E) \geq 1$ when $w(E,\chi) = -1$, he finds the following lower bound for $\mathrm{rank}(E(L_m))$, where L_m is the subfield of K (or of $\mathbb{Q}(E'[p^m])$) such that $\mathrm{Gal}(L_m/\mathbb{Q}) \cong \mathrm{PGL}_2(\mathbb{Z}/p^m\mathbb{Z})$:

$$\mathrm{rank}_{\mathbb{Z}}(E(L_m)) \geq p^{2m} - p^{2m-1} - p - 1.$$

Note for comparison that $[L_m : \mathbb{Q}] = (p^2 - 1)p^{3m-2}$. The above method for constructing points on $E(K)$, which was first exploited by M. Harris (in [Ha]), will make a contribution to $\mathrm{rank}_{\mathbb{Z}}(E(L_m))$ of $(p+1)p^{m-1} + O(1)$ as $n \to \infty$. So in both cases there is a serious discrepancy between what the root number calculations might suggest for the ranks and what explicit, systematic constructions give.

Another interesting example to consider is the following. Let E be the same elliptic curve as before (defined in (13)), but now we take E' to be defined by the equation $y^2 = x^3 - x$. Then E' has conductor 32 and is an elliptic curve with complex multiplication. In fact, $\mathrm{End}(E') \cong \mathbb{Z}[i]$, where i corresponds to the automorphism $(x, y) \to (-x, iy)$ of E'. Now $37 = (6+i)(6-i)$ in $\mathbb{Z}[i]$. Let $\varphi \in \mathrm{End}(E')$ correspond to $6+i$. Then φ is an isogeny of E' to itself defined over $F = \mathbb{Q}(i)$ and its kernel is a subgroup of $E'(\overline{\mathbb{Q}})$ of order 37. Thus $(j(E'), j(E'))$ is a point on $X(\mathbb{Q})$, where X is again the curve defined by $f_{37}(x, y) = 0$. If $p \neq 37$, then just as before, for ever cyclic subgroup Π of $E'[p^\infty]$ of order p^m, we obtain a pair of elliptic curves $E'_\Pi = E'/\Pi$ and $E''_\Pi = E'/\varphi(\Pi)$. (Note that E'_Π and E''_Π are not necessarily isomorphic.) Then $(j(E'_\Pi), j(E''_\Pi))$ is a point on X defined over $\mathbb{Q}(E'[p^\infty])$ and, for the same reason as before, is actually defined over $K = \overline{\mathbb{Q}}^{\ker(\widetilde{\rho}_{E'})}$, where $\rho_{E'} : G_\mathbb{Q} \to \mathrm{Aut}(E'[p^\infty])$ gives the action of $G_\mathbb{Q}$ on $E'[p^\infty]$ and $\widetilde{\rho}_{E'}$ is the corresponding projective representation. We have $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{im}(\widetilde{\rho}_{E'})$, which is isomorphic to a subgroup of $PGL_2(\mathbb{Z}_p)$. This time $\mathrm{im}(\widetilde{\rho}_{E'})$ is much smaller and is not even of finite index in $PGL_2(\mathbb{Z}_p)$.

We can consider $E'[p^\infty]$ as a module over the ring $R_p = \mathrm{End}(E') \otimes_\mathbb{Z} \mathbb{Z}_p$ and the action of $\rho_{E'}(g)$ on $E'[p^\infty]$ is R_p-linear for every $g \in G_F$. From this fact, one can deduce that $\rho_{E'}(G_F)$ is isomorphic to a subgroup of $R_p^\times$ and hence is abelian. That is, $\mathrm{Gal}(F(E'[p^\infty])/F)$ is abelian. According to exercise 1.16, we have $F \subset \widetilde{F} \subset \mathbb{Q}(E'[p^\infty])$ and $F \subset F_\infty^{\mathrm{ac}} \subset K$, where $\widetilde{F}$ is the compositum of all $\mathbb{Z}_p$-extensions of F (so that $\mathrm{Gal}(\widetilde{F}/F) \cong \mathbb{Z}_p^2$) and F_∞^{ac} is the anticyclotomic $\mathbb{Z}_p$-extension of F. Furthermore, $[K : F_\infty^{\mathrm{ac}}] < \infty$. K is a union of dihedral extensions of $\mathbb{Q}$ and if χ is the character of an irreducible 2-dimensional representation of $\mathrm{Gal}(K/\mathbb{Q})$, then δ_χ is the nontrivial character of $\mathrm{Gal}(F/\mathbb{Q})$ and so $w(E, \chi) = \delta_\chi(-37) = -1$. That is, $\mathrm{ord}_{s=1}(L(E, \chi, s))$ is odd and $m_\chi(E)$ should be positive for all such χ. Using lemma 1.9, we can at least say that $E(K)$ has infinite rank. (Exercise 1.10 implies that $E(K)_{\mathrm{tors}}$ is finite. It is not hard to show that there are infinitely many distinct j-invariants $j(E'_\Pi)$ as Π varies (although it is possible for E'_{Π_1} and E'_{Π_2} to be isomorphic over $\mathbb{C}$ for distinct Π_1, Π_2). It follows that $X(K)$ is infinite.) Therefore, $m_\chi(E)$ is positive for infinitely many χ's.

It is interesting to apply lemma 1.9 to $K = \mathbb{Q}_\Sigma^{\mathrm{ab}}$, where Σ is any finite set of primes. Combined with theorem 1.3, we get the following result.

Theorem 1.10 *Suppose that X is a curve defined over $\mathbb{Q}$ with genus at least 2. Suppose also that there is a nonconstant rational map $\pi : X \to E$ defined over $\mathbb{Q}$, where E is a modular elliptic curve. Then $X(\mathbb{Q}_\Sigma^{\mathrm{ab}})$ is finite.*

The hypotheses are satisfied for example when X is defined by $x^4+y^4=1$, which has genus three and is a two-sheeted covering of the elliptic curve E defined by $y^2=1-x^4$.

Exercises.

In the following exercises, E denotes a fixed elliptic curve defined over $\mathbb{Q}$.

1.1 Suppose that A is any p-primary, abelian group. Let $z \in \mathbb{Z}_p$. Then $z = \operatorname*{Lim}_{n\to\infty} z_n$ for some sequence $\{z_n\}$ of integers. Show that if $a \in A$, then there exists an integer n_0 such that $a^{z_n} = a^{z_{n_0}}$ for all $n \geq n_0$. Show that if we define $a^z = a^{z_{n_0}}$, then A becomes a $\mathbb{Z}_p$-module. If A is given the discrete topology, show that the map $\mathbb{Z}_p \times A \to A$ defined by $(z,a) \to a^z$ is continuous. (If we use additive notation for A, then we would of course write za.)

1.2 Suppose that $A \cong (\mathbb{Q}_p/\mathbb{Z}_p)^r$ for some $r \geq 1$. Prove that the automorphism group of A is isomorphic to $\mathrm{GL}_r(\mathbb{Z}_p)$. (Two interesting examples are $A = \mu_{p^\infty}$ and $A = E[p^\infty]$.)

1.3 Let $K/\mathbb{Q}$ be a finite Galois extension. Let H be a subgroup of $G = \mathrm{Gal}(K/\mathbb{Q})$ and let $L = K^H$. The inclusion $E(L) \subset E(K)$ induces a $\mathbb{C}$-linear map

$$E(L) \otimes_{\mathbb{Z}} \mathbb{C} \to (E(K) \otimes_{\mathbb{Z}} \mathbb{C})^H.$$

Prove that this map is an isomorphism. Suppose now that H is a normal subgroup of G and that $\sigma : G \to \mathrm{GL}_d(\mathbb{C})$ is an irreducible representation such that $H \subset \ker(\sigma)$. Then σ can also be regarded as an irreducible representation σ' of $G/H = \mathrm{Gal}(L/\mathbb{Q})$. Show that the multiplicity of σ' in the (G/H)-representation space $E(L) \otimes_{\mathbb{Z}} \mathbb{C}$ is the same as the multiplicity of σ in the G-representation space $E(K) \otimes_{\mathbb{Z}} \mathbb{C}$.

1.4 Let $K/\mathbb{Q}$ be a finite Galois extension. For every irreducible character χ of $\mathrm{Gal}(K/\mathbb{Q})$, define $m_\chi(E)$ as in the text. (See (9).) Prove that if τ is any automorphism of the field $\mathbb{Q}(\chi)$ generated by the values of χ, then χ^τ is another irreducible character of $\mathrm{Gal}(K/\mathbb{Q})$ and $m_{\chi^\tau}(E) = m_\chi(E)$. (Note: It is conjectured that $\mathrm{ord}_{s=1}(L(E/\mathbb{Q},\chi^\tau,s)) = \mathrm{ord}_{s=1}(L(E/\mathbb{Q},\chi,s))$. Even in the case that $d_\chi = 1$, this is only known if $\mathrm{ord}_{s=1}(L(E/\mathbb{Q},\chi,s)) \leq 1$.)

1.5 Let K denote the compositum of all quadratic extensions of $\mathbb{Q}$. Prove that $E(K)_{\text{tors}}$ is finite.

1.6 Prove that there exist infinitely many quadratic fields F with the property that $\text{rank}_{\mathbb{Z}}(E(F)) > \text{rank}_{\mathbb{Z}}(E(\mathbb{Q}))$. (Hint: E is defined by an equation of the form $y^2 = f(x)$, where $f(x) \in \mathbb{Q}[x]$ and has degree 3. If p is any sufficiently large prime, show that p is ramified in $F/\mathbb{Q}$, where $F = \mathbb{Q}\left(\sqrt{f(\frac{1}{p})}\right)$, that $E(F)_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}$, and that $\text{rank}_{\mathbb{Z}}(E(F)) > \text{rank}_{\mathbb{Z}}(E(\mathbb{Q}))$.)

1.7 Let K be a Galois extension of $\mathbb{Q}$ such that $\text{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^n$ for some $n \geq 1$. Prove that

$$\text{rank}_{\mathbb{Z}}(E(K)) = \text{rank}_{\mathbb{Z}}(E(\mathbb{Q})) + \sum_F \text{rank}_{\mathbb{Z}}\left(E(F)/E(\mathbb{Q})\right)$$

where F varies over all quadratic subfields of K.

1.8 Let K denote the composition of all quadratic extensions of $\mathbb{Q}$. Show that $E(K)$ has infinite rank.

1.9 Let F_∞ be any $\mathbb{Z}_p$-extension of a number field F. Let F_n denote the n-th layer (so that $\text{Gal}(F_n/F)$ is cyclic of order p^n). Prove the congruence $\text{rank}_{\mathbb{Z}}(E(F_n)) \equiv \text{rank}_{\mathbb{Z}}(E(F_{n-1})) \pmod{\varphi(p^n)}$.

1.10 Let F be an imaginary quadratic field. Let L be any finite extension of F and let $K = F_\infty^{\text{ac}} L$, where F_∞^{ac} is the anticyclotomic $\mathbb{Z}_p$-extension of F for any prime p. Prove that $E(K)_{\text{tors}}$ is finite. (Hint: First show that any prime of F which is inert in $F/\mathbb{Q}$ must split completely in F_∞^{ac}/F.)

1.11 Let $G = \text{PGL}_2(\mathbb{Z}_p)$ where p is any prime. Show that for all $g \in G$, g and g^{-1} are conjugate in G. This implies that the character of any finite dimensional representation of G over $\mathbb{C}$ is real-valued. (Hint: If $A \in \text{GL}_2(\mathbb{Z}_p)$, show that A and $B = \det(A)A^{-1}$ are conjugate in $\text{GL}_2(\mathbb{Z}_p)$ by considering the equation $XA = BX$ for $X = \begin{bmatrix} x & y \\ z & -x \end{bmatrix}$.)

1.12 Suppose that E' is an elliptic curve defined over $\mathbb{Q}$. Let p be any prime. Suppose that $\widetilde{\rho}_{E'} : G_{\mathbb{Q}} \to \text{PGL}_2(\mathbb{Z}_p)$ is as described earlier. Let $K = \overline{\mathbb{Q}}^{\ker(\widetilde{\rho}_{E'})}$. Show that if E' has good, supersingular reduction at a prime $l \neq p$, then the residue field for any prime of K lying above l is finite. N. Elkies has proven that infinitely many such primes exist. Let E be any elliptic curve/$\mathbb{Q}$ (or even any abelian variety). Deduce that $E(K)_{\text{tors}}$ is finite.

1.13 Let F_∞/F be a $\mathbb{Z}_p$-extension. Assume that E is an elliptic curve defined over F. Prove that if $E(F)_{p\text{-prim}} = 0$, then $E(F_\infty)_{p\text{-prim}} = 0$.

1.14 Let F_∞/F be a $\mathbb{Z}_p$-extension. Suppose that λ is a prime of F and $\lambda \nmid p$. Show that λ is unramified in F_∞/F. (Hint: Let L be any finite abelian extension of F in which λ is tamely ramified. Show that the ramification index for λ in L/F divides $N(\lambda) - 1$. What can the corresponding inertia subgroup of $\mathrm{Gal}(F_\infty/F)$ be?)

1.15 Suppose that F_∞/F is a $\mathbb{Z}_p$-extension. We can write $E(F_\infty)_{\text{tors}} = A \times B$, where A is the subgroup of elements whose order is relatively prime to p and B is $E(F_\infty)_{p\text{-prim}}$. Assume that E has good reduction at p. Prove that A is finite. Show by example that B can be infinite. (Hint: For the first assertion, show that at least one prime of F lying over p is ramified in F_∞/F. For the second assertion, try $E : y^2 = x^3 - x$, $p \equiv 1 \pmod 4$, and $F = \mathbb{Q}(i)(E[p])$.

1.16 Let $R_p = \mathrm{End}(E') \otimes_{\mathbb{Z}} \mathbb{Z}_p$, where E' is the elliptic curve $y^2 = x^3 - x$ considered at the end of this section and p is any prime. Show that $R_p^\times \cong \mathbb{Z}_p^2 \times \Delta$, where Δ is a finite group. Show that $M = F(E'[p^\infty])$ cannot be just a finite extension of $F(\mu_{p^\infty})$ (which is a subfield). Deduce that $\widetilde{F}$ is a subfield of M and $[M : \widetilde{F}] < \infty$. Deduce that $\mathbb{Q}(E'[p^\infty])$ contains F and that $M = \mathbb{Q}(E'[p^\infty])$. If $K = \overline{\mathbb{Q}}^{\ker(\widetilde{\rho}_{E'})}$, show that K contains F_∞^{ac} and that $[K : F_\infty^{\text{ac}}] < \infty$.

2 Selmer groups.

Let K be any algebraic extension of $\mathbb{Q}$. Suppose that E is an elliptic curve defined over K. One of the principal ways in which one studies the Mordell-Weil group $E(K)$ is by using Galois cohomology. Fix $n \geq 2$. Then there is a natural injective homomorphism of $E(K)/nE(K)$ into $H^1(G_K, E[n])$ which is called the Kummer map. If K is a finite extension of $\mathbb{Q}$, then $H^1(G_K, E[n])$ turns out to be an infinite group. (See exercise 2.10.) But one can show that the image of $E(K)/nE(K)$ under the Kummer map is contained in a certain finite subgroup of $H^1(G_K, E[n])$ (called the n-Selmer group). In that way, one proves the weak Mordell-Weil theorem which asserts that $E(K)/nE(K)$ is finite when $[K : \mathbb{Q}] < \infty$. Using the theory of heights one then proves the Mordell-Weil theorem: $E(K) \cong \mathbb{Z}^r \times T$ *for some* $r \geq 0$ *and some finite group* T. So then $E(K)/nE(K) \cong (\mathbb{Z}/n\mathbb{Z})^r \times T/nT$ and, if one knows the structure of the n-Selmer group, one would be able to give an upper bound on r.

In these notes we will consider all n's at once, replacing $E(K)/nE(K) = E(K) \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z})$ by the direct limit $E(K) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z})$ and the n-Selmer group by a certain subgroup $\mathrm{Sel}_E(K)$ of $H^1(G_K, E(\overline{\mathbb{Q}})_{\mathrm{tors}})$ which is called the Selmer group for E over K. It fits into an exact sequence

$$0 \to E(K) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z}) \to \mathrm{Sel}_E(K) \to \text{Ш}_E(K) \to 0$$

where $\text{Ш}_E(K)$ is the so-called Tate-Shafarevich group for E over K. ($\text{Ш}_E(K)$ is a certain subgroup of $H^1(G_K, E(\overline{\mathbb{Q}}))$ which we will also soon define.) Now $E(K) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z}) \cong (\mathbb{Q}/\mathbb{Z})^r$ and therefore knowing the structure of $\mathrm{Sel}_E(K)$ would then give an upper bound on r.

We will give two equivalent definitions of $\mathrm{Sel}_E(K)$. After that, the main objective of this chapter will be to describe an alternative definition for the p-primary subgroup of $\mathrm{Sel}_E(K)$ which involves only the Galois module $E[p^\infty]$. (For any prime p, $E[p^\infty] = \bigcup_m E[p^m]$ is the p-primary subgroup of $E(\overline{\mathbb{Q}})_{\mathrm{tors}}$.) This alternative definition will be valid under the hypothesis that E has good, ordinary reduction at all primes of K lying over p. We will adopt the more usual notation for Galois cohomology groups, writing $H^i(L, \cdot)$ in place of $H^i(G_L, \cdot)$ and $H^i(K/L, \cdot)$ in place of $H^i(\mathrm{Gal}(K/L), \cdot)$ if K/L is a Galois extension.

First Definition: We define the Tate-Shafarevich group $Ш_E(K)$ by

$$Ш_E(K) = \ker\Bigg(H^1(K, E(\overline{K})) \longrightarrow \prod_v H^1(K_v, E(\overline{K}_v))\Bigg)$$

where v runs over all primes of K, archimedean and nonarchimedean. If K is a finite extension of $\mathbb{Q}$, then K_v is the completion of K at v. If K is an infinite algebraic extension of $\mathbb{Q}$, then K_v denotes the union of the completions at v of all finite extensions of $\mathbb{Q}$ contained in K. Thus K_v is always either $\mathbb{R}$ or $\mathbb{C}$ or an algebraic extension of $\mathbb{Q}_l$ (for some prime l). The map defining $Ш_E(K)$ is defined by using the restriction maps

$$H^1(K, E(\overline{K})) \longrightarrow H^1(K_v, E(\overline{K}_v))$$

noting that $E(\overline{K}) \subset E(\overline{K}_v)$ and G_{K_v} can be identified with a subgroup of G_K. (These identifications depend on choosing an embedding $\overline{K} \hookrightarrow \overline{K}_v$ consistent with the natural map $K \hookrightarrow K_v$. But the choice doesn't matter.) To define $\mathrm{Sel}_E(K)$, consider the map

$$\lambda : H^1(K, E(\overline{K})_{\mathrm{tors}}) \longrightarrow H^1(K, E(\overline{K}))$$

arising from the inclusion $E(\overline{K})_{\mathrm{tors}} \subset E(\overline{K})$. This map is surjective. (The reason for this is that the cokernel of the map λ is isomorphic to a subgroup of $H^1(K, E(\overline{K})/E(\overline{K})_{\mathrm{tors}})$. This group is trivial because $E(\overline{K})/E(\overline{K})_{\mathrm{tors}}$ is a uniquely divisible group.) Finally, the Selmer group is defined by

$$\mathrm{Sel}_E(K) = \lambda^{-1}(Ш_E(K)). \tag{15}$$

Second Definition: This is based on Kummer theory for E. Let L be a field of characteristic zero. Classical Kummer theory gives an isomorphism $L^\times/(L^\times)^n \xrightarrow{\sim} H^1(L, \mu_n)$ for any $n \geq 1$, where μ_n denotes the group of n-th roots of unity in $\overline{L}$. Taking the direct limit, one obtains an isomorphism

$$\kappa : L^\times \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} H^1(L, (\overline{L}^\times)_{\mathrm{tors}}).$$

Of course, $(\overline{L}^\times)_{\mathrm{tors}}$ is just the group of roots of unity in $\overline{L}^\times$. The map is defined as follows. Suppose that $\alpha = a \otimes r \in L^\times \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z})$, where $a \in L^\times$ and $r = \frac{m}{n} + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$. Since $\overline{L}^\times$ is a divisible group, we can choose $b \in \overline{L}^\times$

such that $b^n = a^m$. Define $\varphi_\alpha : G_L \to (\overline{L}^\times)_{\text{tors}}$ by $\varphi_\alpha(g) = g(b)/b$ for all $g \in G_L$. Then the cohomology class $[\varphi_\alpha]$ in $H^1(L, (\overline{L}^\times)_{\text{tors}})$ is well-defined and one defines

$$\kappa(\alpha) = [\varphi_\alpha].$$

The injectivity of κ is not hard to prove. The surjectivity is a consequence of Hilbert's Theorem 90: $H^1(L, \overline{L}^\times) = 0$. If L is any finite extension of $\mathbb{Q}$, then it is easy to see $L^\times \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z})$ is isomorphic to a countably infinite direct sum of copies of $\mathbb{Q}/\mathbb{Z}$. Thus $H^1(L, (\overline{L}^\times)_{\text{tors}})$ is quite big.

If E is an elliptic curve defined over L, then $E(\overline{L})$ is also a divisible group. Imitating Kummer theory for the multiplicative group $L^\times$, one defines the Kummer homomorphism

$$\kappa : E(L) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z}) \longrightarrow H^1(L, E(\overline{L})_{\text{tors}})$$

in the same way: Let $\alpha = P \otimes r \in E(L) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z})$, where $P \in E(L)$ and $r = \frac{m}{n} + \mathbb{Z}$. Choose $Q \in E(\overline{L})$ such that $nQ = mP$. Define a 1-cocycle $\varphi_\alpha : G_L \to E(\overline{L})_{\text{tors}}$ by $\varphi_\alpha(g) = g(Q) - Q$ for all $g \in G_L$. Then $[\varphi_\alpha]$ is well-defined and one defines $\kappa(\alpha) = [\varphi_\alpha]$. It is not hard to verify that the following sequence (which is called the Kummer sequence) is exact:

$$0 \longrightarrow E(L) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z}) \xrightarrow{\kappa} H^1(L, E(\overline{L})_{\text{tors}}) \xrightarrow{\lambda} H^1(L, E(\overline{L})) \longrightarrow 0. \tag{16}$$

If K is an algebraic extension of $\mathbb{Q}$, we will use the Kummer sequence for $L = K$ and also for the completions $L = K_v$ where v is any prime of K. In the following commutative diagram, the vertical maps are defined in obvious ways and the rows are exact.

$$\begin{tikzcd}
0 \arrow[r] & E(K) \otimes (\mathbb{Q}/\mathbb{Z}) \arrow[r, "\kappa"] \arrow[d, "a_v"] & H^1(K, E(\overline{K})_{\text{tors}}) \arrow[r, "\lambda"] \arrow[d, "b_v"] & H^1(K, E(\overline{K})) \arrow[r] \arrow[d, "c_v"] & 0 \\
0 \arrow[r] & E(K_v) \otimes (\mathbb{Q}/\mathbb{Z}) \arrow[r, "\kappa_v"] & H^1(K_v, E(\overline{K}_v)_{\text{tors}}) \arrow[r, "\lambda_v"] & H^1(K_v, E(\overline{K}_v)) \arrow[r] & 0
\end{tikzcd}$$

Suppose that $[\varphi] \in H^1(K, E(\overline{K})_{\text{tors}})$. According to the first definition, $[\varphi] \in \mathrm{Sel}_E(K)$ if and only if $c_v \circ \lambda([\varphi]) = 0$ for every prime v of K. Clearly, this is equivalent to requiring that $b_v([\varphi]) \in \mathrm{im}(\kappa_v)$ for all v. Therefore, we obtain the second definition of the Selmer group:

$$\mathrm{Sel}_E(K) = \ker \left(H^1(K, E(\overline{K})_{\text{tors}}) \to \prod_v (H^1(K_v, E(\overline{K}_v)_{\text{tors}}) / \mathrm{im}(\kappa_v)) \right).$$

That is, if $[\varphi] \in H^1(K, E(\overline{K})_{\text{tors}})$, then $[\varphi] \in \text{Sel}_E(K)$ if and only if $[\varphi|_{G_{K_v}}] \in \text{im}(\kappa_v)$ for every prime v of K.

Let p be a prime. The p-primary subgroup of $\mathbb{Q}/\mathbb{Z}$ is isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$. Therefore, for any field L, the p-primary subgroup of $E(L) \otimes (\mathbb{Q}/\mathbb{Z})$ is $E(L) \otimes (\mathbb{Q}_p/\mathbb{Z}_p)$. We will now let κ and κ_v denote the global and local Kummer maps restricted to the p-primary subgroups: If K is any algebraic extension of $\mathbb{Q}$, we have

$$\begin{aligned}
\kappa &: E(K) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \to H^1(K, E[p^\infty]), \\
\kappa_v &: E(K_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \to H^1(K_v, E[p^\infty]).
\end{aligned}$$

The p-primary subgroup of $\text{Sel}_E(K)$ is

$$\text{Sel}_E(K)_p = \ker \left(H^1(K, E[p^\infty]) \to \prod_v H^1(K_v, E[p^\infty]) / \text{im}(\kappa_v) \right). \tag{17}$$

Here v runs over all primes of K. Everything in this definition, except possibly $\text{im}(\kappa_v)$, depends just on the G_K-module $E[p^\infty]$. Most of the rest of this chapter concerns describing $\text{im}(\kappa_v)$ in a way which also involves just the Galois module $E[p^\infty]$.

The first remark to be made is that $\text{im}(\kappa_v)$ is divisible. This is obvious since $E(K_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p)$ is divisible. If $v \nmid p$, we will show that $E(K_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$ and so $\text{im}(\kappa_v) = 0$. That is, if $[\varphi] \in H^1(K_v, E[p^\infty])$, then the local condition at v defining $\text{Sel}_E(K)_p$ is simply that $[\varphi|_{G_{K_v}}]$ is trivial in $H^1(K_v, E[p^\infty])$.

Theorem 2.1 *(i) Let E be an elliptic curve defined over an algebraic extension K_v of $\mathbb{Q}_l$ where l is a prime, $l \neq p$. Then $E(K_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$. (ii) Let E be an elliptic curve defined over $K_v = \mathbb{C}$ or $K_v = \mathbb{R}$. Then $E(K_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$. Thus, whenever $v \nmid p$, we have $\text{im}(\kappa_v) = 0$.*

Proof. Part (ii) is rather easy. Since $K_v = \mathbb{R}$, $E(K_v) \cong S$ or $S \times \mathbb{Z}/2\mathbb{Z}$, where $S = \mathbb{R}/\mathbb{Z}$. Now S is divisible by p and so $S \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$. Also, if T is any finite group, then $T \otimes \mathbb{Q}_p/\mathbb{Z}_p$ is easily seen to be trivial. Hence $E(K_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$. If $K_v = \mathbb{C}$, then $E(K_v) \cong S \times S$ and so again we have $E(K_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$.

Now assume that K_v is a finite extension of $\mathbb{Q}_l$, where l is a prime, $l \neq p$. There is a theorem of E. Lutz (Proposition 6.3 of [Si1]) which states that

$$E(K_v) \cong \mathbb{Z}_l^{[K_v:\mathbb{Q}_l]} \times T$$

where T is a finite group. Since $l \neq p$, $\mathbb{Z}_l$ is p-divisible, and so we have $\mathbb{Z}_l \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$. Again, $T \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$, and therefore it follows that $E(K_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$. If K_v is an infinite algebraic extension of $\mathbb{Q}_l$, then we have $K_v = \bigcup L_v$, where L_v runs over all finite extensions of $\mathbb{Q}_l$ contained in K_v. Since $E(L_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$ for each such L_v, it clearly follows that $E(K_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$ too. ■

If K_v is an algebraic extension of $\mathbb{Q}_p$, then the situation is considerably more subtle. Suppose first that K_v is a finite extension of $\mathbb{Q}_p$. Then the theorem of Lutz states that

$$E(K_v) \cong \mathbb{Z}_p^{[K_v:\mathbb{Q}_p]} \times T,$$

where T is a finite group. Since $\mathbb{Z}_p \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \cong \mathbb{Q}_p/\mathbb{Z}_p$, we have

$$\operatorname{im}(\kappa_v) \cong E(K_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{[K_v:\mathbb{Q}_p]}. \tag{18}$$

In contrast, it turns out that

$$H^1(K_v, E[p^\infty]) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{2[K:\mathbb{Q}_p]} \times \text{ (a finite group)}.$$

Using a terminology that we define later, we would say that $\operatorname{im}(\kappa_v)$ has $\mathbb{Z}_p$-corank $[K_v : \mathbb{Q}_p]$ and that $H^1(K_v, E[p^\infty])$ has $\mathbb{Z}_p$-corank $2[K_v : \mathbb{Q}_p]$.

Assume that E has good, ordinary reduction at v. Thus, the reduction of E at v is an elliptic curve $\widetilde{E}$ defined over the residue field k_v for v and $\widetilde{E}(\overline{k}_v)$ has elements of order p. More precisely, it turns out that $\widetilde{E}[p^\infty] \cong \mathbb{Q}_p/\mathbb{Z}_p$. There is a reduction map $E(\overline{K}_v) \to \widetilde{E}(\overline{k}_v)$ which is equivariant for the action of the Galois groups: G_{K_v} acts on $E(\overline{K}_v)$ in the obvious way. There is a natural homomorphism $G_{K_v} \to G_{k_v}$ whose kernel is the inertia subgroup I_{K_v} of G_{K_v}, and G_{K_v} acts on $\widetilde{E}(\overline{k}_v)$ through the above homomorphism together with the obvious action of G_{k_v} on $\widetilde{E}(\overline{k}_v)$. In particular, there is a natural G_{K_v}-equivariant homomorphism

$$\pi : E[p^\infty] \to \widetilde{E}[p^\infty].$$

It is known that π is surjective and $\ker(\pi) \cong \mathbb{Q}_p/\mathbb{Z}_p$. The action of G_{k_v} on $\widetilde{E}[p^\infty]$ is given by a character $\psi : G_{k_v} \to \mathbb{Z}_p^\times$. We can regard ψ as a character of G_{K_v} which is trivial on I_{K_v}. The action of G_{K_v} on $\ker(\pi)$ is given by a character $\varphi : G_{K_v} \to \mathbb{Z}_p^\times$. Thus the action ρ_E of G_{K_v} on $E[p^\infty]$ is "triangular", that is $\rho_E = \begin{bmatrix} \varphi & * \\ 0 & \psi \end{bmatrix}$. The action of G_{K_v} on μ_{p^∞} is also given by a character $\chi : G_{K_v} \to \mathbb{Z}_p^\times$ and the Weil pairing implies that $\det(\rho_E) = \chi$. Hence $\varphi\psi = \chi$.

We will denote $\ker(\pi)$ by $\mathcal{F}[p^\infty]$. The motivation for this notation is that there is a formal group $\mathcal{F}$ associated to E, the kernel of the reduction map $E(\overline{K}_v) \to \widetilde{E}(\overline{k}_v)$ coincides with the group $\mathcal{F}(\overline{\mathfrak{m}}_v)$ of the formal group (where $\overline{\mathfrak{m}}_v$ is the maximal ideal in the ring of integers of $\overline{K}_v$), and $\ker(\pi)$ is just the p-primary subgroup of $\mathcal{F}(\overline{\mathfrak{m}}_v)$. In fact, for the proof of Lutz' theorem, one uses the logarithm for the formal group $\mathcal{F}$ to compare $\mathcal{F}(\mathfrak{m}_v)$ with a compact subgroup of the additive group of K_v.

Consider the map $\varepsilon_v : H^1(K_v, \mathcal{F}[p^\infty]) \to H^1(K_v, E[p^\infty])$ which is induced by the inclusion $\mathcal{F}[p^\infty] \subset E[p^\infty]$. Here is a description of $\mathrm{im}(\kappa_v)$.

Theorem 2.2 *Assume that K_v is a finite extension of $\mathbb{Q}_p$ and that E has good, ordinary reduction at v. Then* $\mathrm{im}(\kappa_v) = \mathrm{im}(\varepsilon_v)_{\mathrm{div}}$.

Proof. Recall that $\mathrm{im}(\kappa_v)$ is isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^{[K_v:\mathbb{Q}_p]}$. To prove theorem 2.2, all we have to show is that $\mathrm{im}(\kappa_v) \subseteq \mathrm{im}(\varepsilon_v)$ and that $\mathrm{im}(\varepsilon_v) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{[K_v:\mathbb{Q}_p]} \times$ (a finite group). The first statement is not hard to prove. The exact sequence

$$0 \to \mathcal{F}[p^\infty] \to E[p^\infty] \to \widetilde{E}[p^\infty] \to 0$$

induces an exact sequence of cohomology groups

$$H^0(K_v, E[p^\infty]) \longrightarrow H^0(K_v, \widetilde{E}[p^\infty]) \longrightarrow H^1(K_v, \mathcal{F}[p^\infty]) \xrightarrow{\varepsilon_v} H^1(K_v, E[p^\infty]) \xrightarrow{\pi_v} H^1(K_v, \widetilde{E}[p^\infty]) \longrightarrow H^2(K_v, \mathcal{F}[p^\infty]).$$

Thus $\mathrm{im}(\varepsilon_v) = \ker(\pi_v)$ and so the inclusion $\mathrm{im}(\kappa_v) \subset \mathrm{im}(\varepsilon_v)$ would follow if we show that $\pi_v \circ \kappa_v$ is the zero map. Let $[\varphi] \in \mathrm{im}(\kappa_v)$. Then there exists a $Q \in E(\overline{K}_v)$ so that $\varphi(g) = g(Q) - Q$ for all $g \in G_{K_v}$. Denote the image of Q under the reduction map $E(\overline{K}_v) \to \widetilde{E}(\overline{k}_v)$ by $\widetilde{Q}$, we have $\pi_v([\varphi]) = [\widetilde{\varphi}] \in H^1(K_v, \widetilde{E}[p^\infty])$ where $\widetilde{\varphi}(g) = g(\widetilde{Q}) - \widetilde{Q}$ for all $g \in G_{K_v}$. That is $\widetilde{\varphi}$ is a 1-coboundary for $\widetilde{E}(\overline{k}_v)$; its cohomology class is trivial in $H^1(K_v, \widetilde{E}(\overline{k}_v))$.

But $\widetilde{E}(\overline{k}_v)$ is a torsion group and its p-primary subgroup $\widetilde{E}[p^\infty]$ is a direct summand. Hence it is clear that $\widetilde{\varphi}$ is a 1-coboundary for $\widetilde{E}[p^\infty]$, and so $[\widetilde{\varphi}] = \pi_v([\varphi])$ is indeed trivial. This proves that $\mathrm{im}(\kappa_v) \subset \mathrm{im}(\varepsilon_v)$.

Since $\mathrm{im}(\kappa_v)$ is divisible, we must just show that $[\mathrm{im}(\varepsilon_v) : \mathrm{im}(\kappa_v)]$ is finite to prove theorem 2.2. Some terminology will be helpful. Let A be any p-primary abelian group. We can regard A as a $\mathbb{Z}_p$-module. (See exercise 1.1.) We put the discrete topology on A. Then its Pontryagin dual $\widehat{A} = \mathrm{Hom}_{\mathrm{cont}}(A, \mathbb{Q}_p/\mathbb{Z}_p)$ is a compact $\mathbb{Z}_p$-module. (See exercise 2.1.) We say that A is a cofinitely generated $\mathbb{Z}_p$-module if $\widehat{A}$ is finitely generated as a $\mathbb{Z}_p$-module. We then define $\mathrm{corank}_{\mathbb{Z}_p}(A)$ to be the rank of $\widehat{A}$ as a $\mathbb{Z}_p$-module. Thus, if A is cofinitely generated as a $\mathbb{Z}_p$-module, then $\widehat{A} \cong \mathbb{Z}_p^r \times T$ for some $r \geq 0$ and some finite group T. Therefore, $A \cong \widehat{\widehat{A}}$ must be isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^r \times \widehat{T}$ and has $\mathbb{Z}_p$-corank r. Then $A_{\mathrm{div}} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^r$ (which we then say is $\mathbb{Z}_p$-cofree) and $[A : A_{\mathrm{div}}] < \infty$.

By (18), it follows that $\mathrm{im}(\kappa_v)$ is $\mathbb{Z}_p$-cofree and has $\mathbb{Z}_p$-corank equal to $[K_v : \mathbb{Q}_p]$. We must explain why $\mathrm{im}(\varepsilon_v)$ is $\mathbb{Z}_p$-cofinitely generated and has the same $\mathbb{Z}_p$-corank. Now the order of $\ker(\varepsilon_v)$ is bounded above by the order of $H^0(K_v, \widetilde{E}[p^\infty]) = \widetilde{E}(k_v)_p$ which is finite. Hence it suffices to show that $H^1(K_v, \mathcal{F}[p^\infty])$ is $\mathbb{Z}_p$-cofinitely generated and has $\mathbb{Z}_p$-corank $[K_v : \mathbb{Q}_p]$. We will base the proof of this on some theorems of Tate concerning Galois cohomology over local fields. However, in chapter 3 we will give a self-contained proof of what we need by using standard techniques of Iwasawa theory.

Suppose that A is a discrete G_{K_v}-module and that $A \cong (\mathbb{Q}_p/\mathbb{Z}_p)^r$ as a $\mathbb{Z}_p$-module. Here is a helpful but nontrivial result. We include also the case where K_v is a finite extension of $\mathbb{Q}_l$ with $l \neq p$.

Corank Lemma. *(1) Let K_v be a finite extension of $\mathbb{Q}_p$. Then $H^1(K_v, A)$ is $\mathbb{Z}_p$-cofinitely generated and its corank is equal to*

$$r[K_v : \mathbb{Q}_p] + \mathrm{corank}_{\mathbb{Z}_p}(H^0(K_v, A)) + \mathrm{rank}_{\mathbb{Z}_p}(H^0(K_v, \widehat{A}(1)).$$

(2) Assume that K_v is a finite extension of $\mathbb{Q}_l$ where $l \neq p$. Then $H^1(K_v, A)$ is $\mathbb{Z}_p$-cofinitely generated and its corank is equal to

$$\mathrm{corank}_{\mathbb{Z}_p}(H^0(K_v, A)) + \mathrm{rank}_{\mathbb{Z}_p}(H^0(K_v, \widehat{A}(1)).$$

Applying this to $A = \mathcal{F}[p^\infty] \cong \mathbb{Q}_p/\mathbb{Z}_p$ will give the desired result. We have $r = 1$, and $H^0(K_v, \mathcal{F}[p^\infty])$ is a subgroup of $H^0(K_v, E[p^\infty]) = E(K_v)_p$, which is finite. Now $\widehat{A} = \mathrm{Hom}_{\mathrm{cont}}(A, \mathbb{Q}_p/\mathbb{Z}_p)$ and $\widehat{A}(1)$ is the Tate twist: $\widehat{A}(1) = \mathrm{Hom}_{\mathrm{cont}}(A, \mu_{p^\infty})$. The action of G_{K_v} on $\mathcal{F}[p^\infty]$ is by a character $\varphi : G_{K_v} \to \mathbb{Z}_p^\times$. Therefore $\widehat{A}(1)$ is isomorphic to $\mathbb{Z}_p$ and G_{K_v} acts by $\chi\varphi^{-1} = \psi : G_{K_v} \to \mathbb{Z}_p^\times$. The character ψ, which gives the action of G_{K_v} on $\widetilde{E}[p^\infty]$ is clearly nontrivial. (The inertia group I_{K_v} acts trivially, but a Frobenius automorphism acts nontrivially.) It follows that if $A = \mathcal{F}[p^\infty]$, then $H^0(K_v, \widehat{A}(1)) = 0$. The first part of the Corank Lemma implies that $H^1(K_v, \mathcal{F}[p^\infty])$, and hence $\mathrm{im}(\varepsilon_v)$, has $\mathbb{Z}_p$-corank $[K_v : \mathbb{Q}_p]$ as needed. Theorem 2.2 follows.

Right now we will justify the Corank Lemma by using results of Tate about Galois cohomology over local fields. We let A be any G_{K_v}-module which is isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^r$ for some $r \geq 1$. First we show that $H^1(K_v, A)$ is $\mathbb{Z}_p$-cofinitely generated. The exact sequence

$$0 \to A[p] \to A \xrightarrow{p} A \to 0$$

induces a surjective map $H^1(K_v, A[p]) \to H^1(K_v, A)[p]$. Let L_v be a finite Galois extension of K_v such that G_{L_v} acts trivially on $A[p]$. The restriction map $H^1(K_v, A[p]) \to H^1(L_v, A[p])$ has a finite kernel. Also,

$$H^1(L_v, A[p]) = \mathrm{Hom}(\mathrm{Gal}(M_v/L_v), A[p])$$

where M_v is the maximal extension of L_v such that $\mathrm{Gal}(M_v/L_v)$ is an elementary abelian p-group. Since L_v has only finitely many extensions of degree p, it is not hard to see that M_v/L_v is a finite extension, and hence $H^1(L_v, A[p])$ must be finite. So $H^1(K_v, A[p])$ and therefore $H^1(K_v, A)[p]$ are finite. This implies that $H^1(K_v, A)$ is cofinitely generated as a $\mathbb{Z}_p$-module.

Let M be a finite G_{K_v}-module. Assume that $|M| = p^a$. Let $\widehat{M}(1) = \mathrm{Hom}(M, \mu_{p^\infty})$, which is another G_{K_v}-module of the same order. The results of Tate are

(i) $\displaystyle\prod_{j=0}^{2} |H^j(K_v, M)|^{(-1)^j} = \begin{cases} p^{-a[K_v:\mathbb{Q}_p]} & \text{if } v|p \\ 1 & \text{if } v \nmid p \end{cases}$

(ii) *$H^2(K_v, M)$ is the Pontryagin dual of $H^0(K_v, \widehat{M}(1))$ and hence has the same order.*

One can extend these results to infinite G_{K_v}-modules such as A by writing $A = \bigcup_n A[p^n]$ and applying the above results to $M = A[p^n]$ for all $n \geq 0$. One obtains

(i) $\sum_{j=0}^{2}(-1)^j \operatorname{corank}_{\mathbb{Z}_p}(H^j(K_v, A)) = \begin{cases} -[K_v : \mathbb{Q}_p] \operatorname{corank}_{\mathbb{Z}_p}(A) & \text{if } v|p \\ 0 & \text{if } v \nmid p \end{cases}$

(ii) $H^2(K_v, A)$ *is the Pontryagin dual of* $H^0(K_v, \widehat{A}(1))$ *and hence we have* $\operatorname{corank}_{\mathbb{Z}_p}(H^2(K_v, A)) = \operatorname{rank}_{\mathbb{Z}_p}(H^0(K_v, \widehat{A}(1))$.

The Corank Lemma follows immediately from these statements. Later (in theorem 3.11) we will give a self-contained proof for the case $A \cong \mathbb{Q}_p/\mathbb{Z}_p$ needed in the proof of theorem 2.2 by using an "Iwasawa-theoretic" approach. It is based on the fact that G_{K_v} acts on A by a character $\alpha : G_{K_v} \to \mathbb{Z}_p^\times$. Thus one can "trivialize" the Galois module A by taking an extension L_v/K_v such that the action of G_{K_v} on A factors through $\operatorname{Gal}(L_v/K_v)$ and such that L_v is a $\mathbb{Z}_p$-extension of some finite extension of K_v. Then we can use the restriction map and the fact that $H^1(L_v, A) = \operatorname{Hom}(\operatorname{Gal}(L_v^{\mathrm{ab}}/L_v), A)$.

It will be important to have information about $[\operatorname{im}(\varepsilon_v) : \operatorname{im}(\kappa_v)]$. This is not hard to obtain. It is clear that an upper bound on this index is given by $|H^1(K_v, \mathcal{F}[p^\infty])/H^1(K_v, \mathcal{F}[p^\infty])_{\mathrm{div}}|$. Now for $m \gg 0$, we have

$$H^1(K_v, \mathcal{F}[p^\infty])_{\mathrm{div}} = p^m H^1(K_v, \mathcal{F}[p^\infty]).$$

Choose such an m and consider the exact sequence

$$0 \longrightarrow A[p^m] \longrightarrow A \xrightarrow{p^m} A \longrightarrow 0$$

where $A = \mathcal{F}[p^\infty]$. This induces an exact sequence of cohomology groups

$$H^1(K_v, A) \xrightarrow{p^m} H^1(K_v, A) \longrightarrow H^2(K_v, A[p^m])$$

and hence $[\operatorname{im}(\varepsilon_v) : \operatorname{im}(\kappa_v)]$ is bounded above by $|H^2(K_v, A[p^m])|$ for any sufficiently large m. The order of this group equals $|H^0(K_v, \widehat{A[p^m]}(1))|$. The Weil pairing $E[p^m] \times E[p^m] \to \mu_{p^m}$ induces another nondegenerate pairing $A[p^m] \times \widetilde{E}[p^m] \to \mu_{p^m}$. That is, $\operatorname{Hom}(A[p^m], \mu_{p^m}]) \cong \widetilde{E}[p^m]$ as G_{K_v}-modules. It follows that $H^0(K_v, \widehat{A[p^m]}(1)) = \widetilde{E}(k_v)_p$ for $m \gg 0$. Therefore, $\operatorname{im}(\varepsilon_v)/\operatorname{im}(\kappa_v)$ is cyclic and we have

$$|\operatorname{im}(\varepsilon_v)/\operatorname{im}(\kappa_v)| \leq |\widetilde{E}(k_v)_p|. \tag{19}$$

It turns out that equality holds and the two groups are even isomorphic, but we will not need this.

We have proved the following result.

Theorem 2.3 *If K_v is a finite extension of $\mathbb{Q}_p$ and if E is an elliptic curve/K_v with good, ordinary reduction, then* $\operatorname{im}(\kappa_v)$ *has finite index in* $\operatorname{im}(\varepsilon_v)$ *and* $\operatorname{im}(\varepsilon_v)/\operatorname{im}(\kappa_v)$ *is a cyclic group whose order divides* $|\widetilde{E}(k_v)_p|$, *where k_v is the residue field of v. In particular, if $p \nmid |\widetilde{E}(k_v)|$, then* $\operatorname{im}(\kappa_v) = \operatorname{im}(\varepsilon_v)$.

If v is a prime of K where E has good reduction and if the characteristic of the residue field k_v divides $|\widetilde{E}(k_v)|$, then v is called an anomalous prime for E. For a fixed E, anomalous primes seem rather rare, although it seems likely that infinitely many such primes should exist. There is a nice discussion of this question for the curves $y^2 = x^3 + D$ in the introduction of [Ma1]. Obviously, E has ordinary reduction at any anomalous prime v for E. See exercise 2.12 for more about this property.

We will now compare the images of κ_v and ε_v for infinite extensions of $\mathbb{Q}_p$ under certain restrictive hypotheses. One hypothesis concerns the so-called profinite degree of an infinite extension K/F. This is defined as the least common multiple of the degrees $[L : F]$, where L varies over all finite extensions of F contained in K. This should be interpreted as a formal product Πl^{a_l} over all primes l, where $0 \le a_l \le \infty$. If l^∞ "divides" this product, then the power of l dividing $[L : F]$ is unbounded as L varies. The main result is the following.

Theorem 2.4 *Assume that K_v is an extension of $\mathbb{Q}_p$ with finite residue field k_v. Assume also that the profinite degree of $K_v/\mathbb{Q}_p$ is divisible by p^∞. Then* $\operatorname{im}(\kappa_v) = \operatorname{im}(\varepsilon_v)$. *In particular, this is true if K_v is a ramified $\mathbb{Z}_p$-extension of F_v, where F_v is a finite extension of $\mathbb{Q}_p$.*

Proof. By the same argument as in the proof of theorem 2.2, we still have $\operatorname{im}(\kappa_v) \subset \operatorname{im}(\varepsilon_v)$. We will show that $\operatorname{im}(\varepsilon_v)$ is a divisible group and that $\operatorname{im}(\varepsilon_v)/\operatorname{im}(\kappa_v)$ is finite. This clearly implies the equality. The fact that $\operatorname{im}(\varepsilon_v)/\operatorname{im}(\kappa_v)$ is finite follows from the observations in the previous paragraph. For we can write K_v as a union of finite extensions of $\mathbb{Q}_p : K_v = \bigcup_n F_v^{(n)}$. We let $\kappa_v^{(n)}$, $\varepsilon_v^{(n)}$ denote the two maps to $H^1(F_v^{(n)}, E[p^\infty])$ that we are considering, but over the ground field $F_v^{(n)}$. We have

$$H^1(K_v, E[p^\infty]) = \varinjlim_n H^1(F_v^{(n)}, E[p^\infty])$$

where the direct limit is defined by the natural restriction maps. We then have

$$\mathrm{im}(\varepsilon_v) = \varinjlim \mathrm{im}(\varepsilon_v^{(n)}), \quad \mathrm{im}(\kappa_v) = \varinjlim \mathrm{im}(\kappa_v^{(n)}),$$

and therefore $\mathrm{im}(\varepsilon_v)/\,\mathrm{im}(\kappa_v)$ is finite because it is a direct limit of the finite groups $\mathrm{im}(\varepsilon_v^{(n)})/\,\mathrm{im}(\kappa_v^{(n)})$ whose orders are uniformly bounded by $|\widetilde{E}(k_v)_p|$.

We will show that $H^1(K_v, \mathcal{F}[p^\infty])$, is divisible, from which it follows that $\mathrm{im}(\varepsilon_v)$ is divisible too. It suffices to prove that $H^1(K_v, A)$ is divisible whenever A is a divisible p-primary G_{K_v}-module. This follows from the fact that G_{K_v} has p-cohomological dimension 1. That is, if M is any finite p-primary G_{K_v}-module, then $H^n(K_v, M) = 0$ for all $n \geq 2$. To deduce that $H^1(K_v, A)$ is divisible, consider the exact sequence

$$0 \to A[p] \to A \to A \to 0$$

which induces an exact sequence of cohomology groups

$$H^1(K_v, A) \xrightarrow{p} H^1(K_v, A) \to H^2(K_v, A[p]).$$

Since the last group is zero, $H^1(K_v, A)$ is p-divisible. It must then be divisible since it is a p-primary group.

It is worth reviewing why G_{K_v} has p-cohomological dimension 1. The only hypothesis needed for this is that K_v is an extension of $\mathbb{Q}_l$ such that $[K_v : \mathbb{Q}_l]$ is divisible by p^∞ and l is any prime. This hypothesis implies that the p-primary subgroup of the Brauer group of K_v is zero. (The reason for this is that $\mathrm{Br}(K_v) = \varinjlim \mathrm{Br}(F_v^{(n)})$ where as before the $F_v^{(n)}$'s are finite extensions of $\mathbb{Q}_l$ such that $K_v = \bigcup_n F_v^{(n)}$. But in most treatments of local class field theory one proves that any element of $\mathrm{Br}(F_v^{(n)})$ of order p^m becomes trivial over any finite extension of degree divisible by p^m. Since the profinite degree of K_v over $F_v^{(n)}$ is divisible by p^∞, it follows that the p-primary subgroup of the direct limit is zero.) Therefore, $H^2(K_v, \overline{K}_v^\times)_p = 0$. Of course, the same argument applies to any algebraic extension of K_v and therefore $H^2(H, \overline{K}_v^\times) = 0$ for every closed subgroup H of G_{K_v}. Now consider the exact sequence of G_{K_v}-modules

$$1 \to \mu_p \to \overline{K}_v^\times \xrightarrow{p} \overline{K}_v^\times \to 1.$$

This induces an exact sequence

$$H^1(H, \overline{K}_v^\times) \to H^2(H, \mu_p) \to H^2(H, \overline{K}_v^\times)$$

for any closed subgroup H of G_{K_v}. The first term is zero by Hilbert's Theorem 90 and the second term is zero by the above remark. Hence $H^2(H, \mu_p) = 0$. Letting H be a Sylow pro-p subgroup P of G_{K_v}, it follows that $H^2(P, \mathbb{Z}/p\mathbb{Z}) = 0$. This implies that $H^2(P, M) = 0$ for any finite P-module M of p-power order (since the composition factors as a P-module must be isomorphic to $\mathbb{Z}/p\mathbb{Z}$). Since the restriction map $H^2(K_v, M) \to H^2(P, M)$ is injective, we have $H^2(K_v, M) = 0$ for any G_{K_v}-module M of p-power order, which suffices to show that G_{K_v} has p-cohomological dimension 1.

Exercises.

2.1 Let A be a p-primary abelian group which is given the discrete topology. The Pontryagin dual of A is defined by

$$\widehat{A} = \mathrm{Hom}(A, \mathbb{Q}_p/\mathbb{Z}_p)$$

which is topologized with the "compact-open" topology (where $\mathbb{Q}_p/\mathbb{Z}_p$ is given the discrete topology). Show that $\widehat{A}$ is a pro-p group (i.e. a projective limit of finite p-groups) and hence is compact. Similarly, if X is an abelian pro-p group, show that its Pontryagin dual $\widehat{X} = \mathrm{Hom}_{\mathrm{cont}}(X, \mathbb{Q}_p/\mathbb{Z}_p)$ is a discrete p-primary group (again with the "compact-open" topology). Show that $\widehat{\mathbb{Z}}_p \cong \mathbb{Q}_p/\mathbb{Z}_p$ and $\widehat{(\mathbb{Q}_p/\mathbb{Z}_p)} \cong \mathbb{Z}_p$ as topological groups.

2.2 Suppose that $G = \langle \sigma \rangle$ is a finite, cyclic group of order m and that A is an abelian group (written with additive notation) on which G acts. Then $H^1(G, A) = \ker(N)/\operatorname{im}(\sigma - 1)$, where $N : A \to A$ is the norm map defined by $N(a) = \sum_{i=0}^{m-1} \sigma^i(a)$ and $\sigma - 1 : A \to A$ is defined by $(\sigma - 1)(a) = \sigma(a) - a$ (both for all $a \in A$).

(a) Suppose that $\Gamma \cong \mathbb{Z}_p$ and let $\gamma \in \Gamma$ be chosen so that $\langle \gamma \rangle$ is a dense subgroup of Γ. (We say that γ is a topological generator of Γ.) Suppose that A is a finite, abelian p-group on which Γ acts continuously. (We put the discrete topology on A and require that the map $\Gamma \times A \to A$ defined by $(\gamma, a) \to \gamma(a)$ be continuous.) Let $\Gamma_n = \Gamma^{p^n}$ so that Γ/Γ_n is cyclic of order p^n. Then $H^1(\Gamma, A)$ can be defined as $\varinjlim_n H^1(\Gamma/\Gamma_n, A^{\Gamma_n})$.

Show that $H^1(\Gamma, A) = A/(\gamma - 1)A$.

(b) Suppose that A is a discrete, p-primary abelian group on which Γ acts continuously. Prove that $A = \bigcup_n A^{\Gamma_n}$. Defining $H^1(\Gamma, A)$ as above, show that $H^1(\Gamma, A) = A/(\gamma - 1)A$.

(c) Suppose that $A \cong (\mathbb{Q}_p/\mathbb{Z}_p)^r$ as a group and that Γ acts continuously on A. Prove that $H^0(\Gamma, A)$ and $H^1(\Gamma, A)$ have the same $\mathbb{Z}_p$-corank and that if $H^0(\Gamma, A)$ is finite, then $H^1(\Gamma, A) = 0$.

2.3 Let K_v be a finite extension of $\mathbb{Q}_l$ for some prime l. Let $A = \mathbb{Q}_p/\mathbb{Z}_p$ with a trivial action of G_{K_v}. Calculate $\mathrm{corank}_{\mathbb{Z}_p}(H^1(K_v, A))$ by using local class field theory. Verify the corank lemma in this case. More generally, verify the corank lemma if $A \cong \mathbb{Q}_p/\mathbb{Z}_p$ as a $\mathbb{Z}_p$-module and G_{K_v} acts on A by a character $\psi : G_{K_v} \to \mathbb{Z}_p^\times$ of finite order. (If ψ is nontrivial, the inflation-restriction sequence will help.)

2.4 Now take $A = \mu_{p^\infty}$. Calculate $\mathrm{corank}_{\mathbb{Z}_p}(H^1(K_v, A))$ by using Kummer theory. Verify the corank lemma in this case.

2.5 Let K_v be a finite extension of $\mathbb{Q}_l$, where l is a prime and $l \neq p$. Suppose that E is an elliptic curve defined over K_v which has good reduction. Then it is known that $K_v(E[p^\infty])/K_v$ is an unramified extension. Prove that $H^1(K_v^{\mathrm{unr}}/K_v, E[p^\infty]) = 0$, where K_v^{unr} denotes the maximal unramified extension of K_v. (Note that $\mathrm{Gal}(K_v^{\mathrm{unr}}/K_v) \cong \widehat{\mathbb{Z}} = \prod_q \mathbb{Z}_q$ where q varies over all primes. Use an argument involving the inflation-restriction sequence. Exercise 2.2 will be helpful.)

2.6 With the same assumptions as in exercise 2.5, show that $H^1(K_v, E[p^\infty])$ is finite, as predicted by the corank lemma. (Hint: Use the inflation-restriction sequence. It will be useful to know the structure of $\mathrm{Gal}(K_v^{\mathrm{tame}}/K_v)$, where

K_v^{tame} is the maximal tamely ramified extension of K_v. This can be described precisely by local class field theory.)

2.7 Using the corank lemma, determine $\text{corank}_{\mathbb{Z}_p}(H^1(K_v, E[p^\infty]))$ if E is an elliptic curve defined over a finite extension K_v of $\mathbb{Q}_p$.

2.8 Suppose that E is an elliptic curve defined over $\mathbb{Q}$ with the property that $\text{rank}_{\mathbb{Z}}(E(\mathbb{Q})) \geq 3$. Prove that $\ker(H^1(\mathbb{Q}, E[p^\infty]) \to \prod_l H^1(\mathbb{Q}_l, E[p^\infty]))$ is infinite for every prime p. (Hint: $H^1(\mathbb{Q}, E[p^\infty])$ contains a subgroup isomorphic to $E(\mathbb{Q}) \otimes (\mathbb{Q}_p/\mathbb{Z}_p)$. Study its image under the above global-to-local map. For $l \neq p$, $H^1(\mathbb{Q}_l, E[p^\infty])$ is finite by the corank lemma or by exercise 2.6. Note: It turns out that $\text{rank}_{\mathbb{Z}}(E(\mathbb{Q})) \geq 2$ suffices to give the same conclusion.)

2.9 Let E be an elliptic curve defined over a number field F. Let Σ be a finite set of primes of F containing all the archimedean primes, the primes dividing p, and the primes where E has bad reduction. Let F_Σ denote the maximal algebraic extension of F which is unramified outside Σ. Let K be any intermediate field: $F \subset K \subset F_\Sigma$. Let Σ_K denote the primes of K lying above those in Σ. Prove that

$$\text{Sel}_E(K)_p = \ker(H^1(F_\Sigma/K, E[p^\infty]) \to \prod_{\eta \in \Sigma_K} H^1(K_\eta, E[p^\infty])/\operatorname{im}(\kappa_\eta)).$$

The maps come from restriction maps when one chooses an embedding $F_\Sigma \hookrightarrow \overline{K}_\eta$ for each η.
(Hint: Exercise 2.5 is relevant.)

2.10 Let E be an elliptic curve defined over a finite extension K of $\mathbb{Q}$. Suppose that $n \geq 2$ and that p is any prime dividing n. Prove that $H^1(K, E[n])$ has infinitely many elements of order p. (Hint: Let $M = K(E[n])$, so that G_M acts trivially on $E[n]$. Use the inflation-restriction sequence to compare $H^1(K, E[n])$ with $H^1(M, E[n])^{\text{Gal}(M/K)}$.)

2.11 Let Σ be a finite set of primes of K containing all the primes where E has bad reduction and all the prime divisors of n, where $n \geq 2$. Let K_Σ be the maximal extension of K unramified outside the set Σ. Prove that $H^1(K_\Sigma/K, E[n])$ is finite.

2.12 Let $\widetilde{E}$ be an elliptic curve defined over a finite field k_v of characteristic p. Define $a_v = 1+|k_v|-|\widetilde{E}(k_v)|$. A theorem of Hasse (the Riemann hypothesis for the zeta function of $\widetilde{E}$ over k_v) states that $|a_v| \leq 2\sqrt{|k_v|}$. This means that the two roots α_v and β_v of the quadratic polynomial $X^2 - a_v X + |k_v|$ have absolute value $\sqrt{|k_v|}$. It is known that if $k_v^{(n)}$ denotes the extension of k_v of degree n, then $|\widetilde{E}(k_v^{(n)})| = 1 + |k_v^{(n)}| - (\alpha_v^n + \beta_v^n)$. (If $n = 1$, this is true by definition.)

(a) Prove that $\widetilde{E}$ is ordinary if and only if $p \nmid a_v$.

(b) Prove that if $\widetilde{E}$ is supersingular, $k_v = \mathbb{Z}/p\mathbb{Z}$, and $p \geq 5$, then $a_v = 0$.

(c) Prove that $\widetilde{E}(k_v)$ has an element of order p if and only if $a_v \equiv 1 \pmod{p}$. If $k_v = \mathbb{Z}/p\mathbb{Z}$ and $p \geq 7$, show that $a_v \equiv 1 \pmod{p} \iff a_v = 1$.

3 Λ-Modules.

Let $\Lambda = \mathbb{Z}_p[[T]]$, the ring of formal power series over $\mathbb{Z}_p$ in one variable. Λ is a Noetherian ring. If $g(T) = \sum_{i=0}^{\infty} b_i T^i \in \Lambda$, then $g(T)$ is invertible in Λ if and only if $b_0 \in \mathbb{Z}_p^{\times}$. This implies that Λ is a local ring with maximal ideal $\mathfrak{m} = (p, T)$. We have $\Lambda/\mathfrak{m} \cong \mathbb{Z}/p\mathbb{Z}$. In fact, $\Lambda/\mathfrak{m}^k$ is finite for every $k \geq 1$. We consider Λ as a topological ring by giving it the $\mathfrak{m}$-adic topology. (A base of neighborhoods of 0 is $\{\mathfrak{m}^k\}_{k \geq 1}$.) Then $\Lambda \cong \varprojlim \Lambda/\mathfrak{m}^k$ which makes Λ a compact topological ring. Λ is obviously not a PID, but nevertheless there is the following theorem reminiscent of the structure theory of modules over a PID.

Theorem 3.1 *Suppose that X is a finitely generated Λ-module. Then there exists a Λ-module homomorphism*

$$\varphi : X \to \Lambda^r \times \prod_{i=1}^{t} \Lambda/(f_i(T)^{e_i})$$

with a finite kernel and cokernel, where $r \geq 0$, $f_1(T), \ldots, f_t(T)$ are irreducible elements of Λ, and $e_1, \ldots, e_t$ are positive integers. The value of r, the prime ideals $(f_i(T))$, and the corresponding exponents e_i are uniquely determined by X.

Some of the Λ-modules that we will be interested in arise in the following way. Let F_∞/F be a $\mathbb{Z}_p$-extension, so that $\Gamma = \mathrm{Gal}(F_\infty/F)$ is isomorphic to $\mathbb{Z}_p$. Choose $\gamma_0 \in \Gamma$ such that $\gamma_0|_{F_1}$ is nontrivial. Then γ_0 generates a dense subgroup of Γ. Suppose that A is a p-primary, abelian group with the discrete topology and that Γ acts continuously on A. That is, there is a homomorphism $\Gamma \to \mathrm{Aut}(A)$ and the map $\Gamma \times A \to A$ defined by $(\gamma, a) \to \gamma(a)$ for all $\gamma \in \Gamma$, $a \in A$ is continuous. Then we can make both A and $\widehat{A} = \mathrm{Hom}(A, \mathbb{Q}_p/\mathbb{Z}_p)$ into Λ-modules. We already know how to make A and $\widehat{A}$ into $\mathbb{Z}_p$-modules. (See exercise 1.1.) We make them into $\mathbb{Z}_p[T]$-modules by defining $Ta = \gamma_0(a) - a$ for all $a \in A$. T is an endomorphism of A. In exercise 3.3, it is shown that T is "topologically nilpotent"' and so both A and $\widehat{A}$ can be made into Λ-modules.

Suppose that E is an elliptic curve defined over a field F. Then $A = H^1(F_\infty, E[p^\infty])$ is a p-primary abelian group and has a natural action of Γ.

We can then regard A as a Λ-module (with the discrete topology). If F is a finite extension of $\mathbb{Q}_l$ for any prime l, then $\widehat{A}$ is a finitely generated Λ-module. If F is a number field, then let Σ be a finite set of primes of F containing all archimedean primes, all primes dividing p, and all primes where E has bad reduction. Then $E[p^\infty]$ is a $\mathrm{Gal}(F_\Sigma/F)$-module, and $A = H^1(F_\Sigma/F_\infty, E[p^\infty])$ also has a natural action of Γ and can be regarded as a Λ-module. Again, $\widehat{A}$ turns out to be a finitely generated Λ-module. Also, $\mathrm{Sel}_E(F_\infty)_p$ is a Λ-submodule of $H^1(F_\Sigma/F_\infty, E[p^\infty])$ (just because it is Γ-invariant). There are many difficult, unsolved questions concerning the structure of these Λ-modules. We will state a few of them, using the following convenient terminology. If A is a discrete Λ-module as above, then we say that A is Λ-cotorsion if $\widehat{A}$ is Λ-torsion, A is Λ-cofinitely generated if $\widehat{A}$ is Λ-finitely generated, and we define $\mathrm{corank}_\Lambda(A)$ to be $\mathrm{rank}_\Lambda(\widehat{A})$.

Conjecture 3.2 *Suppose that F is a finite extension of $\mathbb{Q}$ and that E is any elliptic curve defined over F. Let Σ be chosen as above. Then*

$$\mathrm{corank}_\Lambda(H^1(F_\Sigma/F_\infty, E[p^\infty]) = [F : \mathbb{Q}].$$

In general, all that is known about this is that $\mathrm{corank}_\Lambda(H^1(F_\Sigma/F_\infty, E[p^\infty]) \geq [F : \mathbb{Q}]$ and that the equality is equivalent to the assertion that the Λ-module $H^2(F_\Sigma/F_\infty, E[p^\infty])$ is Λ-cotorsion.

Conjecture 3.3 *Suppose that F is a finite extension of $\mathbb{Q}$ and that E is an elliptic curve defined over F which has good, ordinary reduction at all primes of F lying over p. Suppose that F_∞/F is the cyclotomic $\mathbb{Z}_p$-extension. Then $\mathrm{Sel}_E(F_\infty)_p$ is Λ-cotorsion.*

This was conjectured by Mazur in [Ma1]. One case in which it is known to be true is when F is an abelian extension of $\mathbb{Q}$ and E is a modular elliptic curve defined over $\mathbb{Q}$. In this case, both conjectures 3.2 and 3.3 have been proven by Kato. Conjecture 3.3 should be true under the weaker hypothesis that E has either potentially ordinary or potentially multiplicative reduction at all primes of F (lying over p.) In general, the following conjecture (due to P. Schneider) gives the Λ-corank of $\mathrm{Sel}_E(F_\infty)_p$.

Conjecture 3.4 *Let F_∞/F be the cyclotomic $\mathbb{Z}_p$-extension of a number field F. Assume that E is an elliptic curve defined over F. Then*

$$\mathrm{corank}_\Lambda(\mathrm{Sel}_E(F_\infty)_p) = \sum_{v\,pss} [F_v : \mathbb{Q}_p]$$

where the sum is over all primes of F lying over p where E has potentially supersingular reduction.

This conjecture turns out to imply conjecture 3.2 (for the cyclotomic $\mathbb{Z}_p$-extension F_∞/F). One can prove that $\sum\limits_{v\,pss}[F_v : \mathbb{Q}_p]$ is a lower bound on $\mathrm{corank}_\Lambda(\mathrm{Sel}_E(F_\infty)_p)$, and therefore $\mathrm{Sel}_E(F_\infty)_p$ cannot be Λ-cotorsion if there is at least one prime of F lying over p where E has potentially supersingular reduction.

We will return now to various basic theorems concerning Λ and its module theory, partially proving theorem 3.1. We start with the following result.

Theorem 3.5 *Suppose that $g(T) \in \Lambda$, but $g(T) \notin p\Lambda$. If $g(T) = \sum\limits_{i=0}^{\infty} b_i T^i$, let d be the smallest integer such that $b_d \in \mathbb{Z}_p^\times$. Let $f(T) \in \Lambda$. Then there exists a polynomial $r(T) \in \mathbb{Z}_p[T]$ of degree $< d$, and an element $h(T) \in \Lambda$ such that*

$$f(T) = g(T)h(T) + r(T).$$

Furthermore, $h(T)$ and $r(T)$ are uniquely determined by $f(T)$ and $g(T)$.

Proof. The uniqueness is easy. If $g(T)h(T)+r(T) = g(T)h'(T)+r'(T)$, then $r'(T) - r(T) = s(T)$ is divisible by $g(T)$ in Λ. Let $\widetilde{\Lambda} = \Lambda/p\Lambda$ which can be thought of as $\mathbb{F}_p[[T]]$, where $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is the field with p elements. We will denote the image of an element $f(T) \in \Lambda$ under the canonical homomorphism $\Lambda \to \widetilde{\Lambda}$ by $\widetilde{f}(T)$. Assume that $s(T) \neq 0$. Then we can write $s(T) = p^m s_0(T)$, where $s_0(T) \notin p\Lambda$ and $m \geq 0$. Now p is a prime element of Λ because $\widetilde{\Lambda}$ is an integral domain. Since $g(T)$ divides $s(T)$, it then follows that $g(T)$ divides $s_0(T)$. But $\widetilde{s}_0(T)$ is a nonzero polynomial in $\widetilde{\Lambda}$ of degree $< d$ which is divisible by $\widetilde{g}(T)$ and therefore by T^d in $\widetilde{\Lambda}$. This is clearly impossible. Hence $s(T) = 0$ and so $r(T) = r'(T)$. This implies that $h(T) = h'(T)$ too.

We prove the existence by using the fact that $\widetilde{\Lambda}$ is a discrete valuation ring and has a simple division algorithm. If $\widetilde{f}(T) = \sum\limits_{i=0}^{\infty} \widetilde{a}_i T^i$ (where $\widetilde{a}_i \in \mathbb{F}_p$ for all i), then we can write $\widetilde{f}(T) = T^d(\sum\limits_{i=d}^{\infty} \widetilde{a}_i T^{i-d}) + \sum\limits_{i=0}^{d-1} \widetilde{a}_i T^i$. Since $\widetilde{g}(T)$ and T^d generate the same ideal in $\widetilde{\Lambda}$, we can write $\widetilde{f}(T) = \widetilde{g}(T)\widetilde{h}(T) + \widetilde{r}(T)$, where $\widetilde{h}(T) \in \widetilde{\Lambda}$ and $\widetilde{r}(T)$ is a polynomial in $\widetilde{\Lambda}$ of degree $< d$. Lifting back to Λ, we get a division algorithm modulo $p\Lambda$. That is, we can write

$$f(T) = g(T)h_1(T) + r_1(T) + pf_1(T)$$

where $h_1(T), f_1(T) \in \Lambda$ and $r_1(T)$ is a polynomial of degree $< d$. Applying this to $f_1(T)$ instead of $f(T)$, we then obtain

$$f(T) = g(T)h_2(T) + r_2(T) + p^2 f_2(T)$$

where again $h_2(T), f_2(T) \in \Lambda$, $r_2(T)$ is a polynomial of degree $< d$, and $h_2(T) \equiv h_1(T) \pmod{p\Lambda}$, $r_2(T) \equiv r_1(T) \pmod{p\mathbb{Z}_p[T]}$. Continuing, we obtain an equation for each $n \geq 1$:

$$f(T) = g(T)h_n(T) + r_n(T) + p^n f_n(T)$$

where $h_n(T) \in \Lambda$ and $h_{n+1}(T) \equiv h_n(T) \pmod{p^n\Lambda}$, $r_n(T) \in \mathbb{Z}_p[T]$ with degree $< d$ and $r_{n+1}(T) \equiv r_n(T) \pmod{p^n\mathbb{Z}_p[T]}$. Clearly, the limits exist in Λ and we can write $f(T) = g(T)h(T) + r(T)$ where $h(T) = \operatorname{Lim}_{n\to\infty} h_n(T)$, $r(T) = \operatorname{Lim}_{n\to\infty} r_n(T)$. Here $h(T) \in \Lambda$ and $r(T)$ is a polynomial of degree $< d$. This proves the existence. ∎

Corollary 3.6 *Let $g(T)$ be as in theorem 3.5. Then $\Lambda/(g(T))$ is isomorphic to $\mathbb{Z}_p^d$ as a $\mathbb{Z}_p$-module.*

Proof. This is clear because the map $f(T) + (g(T)) \to r(T)$ defines a $\mathbb{Z}_p$-module isomorphism of $\Lambda/(g(T))$ to $\{r(T) | r(T) \in \mathbb{Z}_p[T], \deg(r(T)) < d\}$. ∎

A polynomial $\sum_{i=0}^{d} c_i T^i \in \mathbb{Z}_p[T]$ is called a "distinguished polynomial" if $c_d = 1$ and $c_i \in p\mathbb{Z}_p$ for all $i < d$. (An equivalent condition is that the polynomial be monic and that all of its roots in $\overline{\mathbb{Q}}_p$ have positive valuation.)

Corollary 3.7 *Let $g(T)$ be as in theorem 3.5. Then there exists a unique distinguished polynomial $g_0(T)$ such that $g(T) = u(T)g_0(T)$, where $u(T) \in \Lambda^\times$. The degree of $g_0(T)$ is d.*

Proof. Multiplication by T defines an endomorphism of the $\mathbb{Z}_p$-module $\Lambda/(g(T))$. Since this is free with $\mathbb{Z}_p$-rank d, there is a monic polynomial $g_0(T)$ of degree d such that $g_0(T)$ annihilates $\Lambda/(g(T))$. Namely, take $g_0(T)$ to be the characteristic polynomial of T acting on this $\mathbb{Z}_p$-module. Thus, $(g_0(T)) \subset (g(T))$. Applying corollary 3.6 to $g_0(T)$, we see that $\Lambda/(g_0(T))$ is isomorphic to $\mathbb{Z}_p^{d_0}$ where $d_0 \leq d$. But there is a natural surjective homomorphism $\Lambda/(g_0(T)) \to \Lambda/(g(T))$ of $\mathbb{Z}_p$-modules. Hence $d_0 = d$ and this homomorphism must be an isomorphism. That is, $g_0(T)$ is distinguished of degree d and $(g_0(T)) = (g(T))$. Thus, $g(T) = u(T)g_0(T)$ as stated. It is clear that $\Lambda/(g(T))$ can be identified with $\mathbb{Z}_p[T]/(g_0(T))$ and that $g_0(T)$ as defined above is the minimal polynomial of the endomorphism T of $\Lambda/(g(T))$. This implies uniqueness because if $g(T) = u'(T)g_0'(T)$ where $g_0'(T)$ is a distinguished polynomial, then $g_0'(T)$ annihilates $\Lambda/(g(T))$ and hence $g_0(T)|g_0'(T)$ in $\mathbb{Z}_p[T]$. It is also clear from the above that $\deg(g_0(T)) = \deg(g_0'(T))$ and so $g_0(T) = g_0'(T)$. (Alternatively, one could see that $g_0(T)$ and $g_0'(T)$ have the same degree by reducing modulo $p\Lambda$.) ■

Theorem 3.8 *Let $g(T)$ be a nonzero element of Λ. Then we can write $g(T)$ uniquely in the form*

$$g(T) = p^m u(T) g_0(T)$$

where $m \geq 0$, $u(T) \in \Lambda^\times$, and $g_0(T)$ is a distinguished polynomial. Also, $g(T)$ is an irreducible element of Λ if and only if either $m = 1$ and $g_0(T) = 1$ or $m = 0$ and $g_0(T)$ is irreducible as an element of $\mathbb{Q}_p[T]$.

Proof. We can obviously write $g(T)$ as $g(T) = p^m g_1(T)$ where $g_1(T) \in \Lambda$, but $\notin p\Lambda$. Here m is unique. We can then apply corollary 3.7 to $g_1(T)$, obtaining the first assertion. Now obviously p is irreducible in Λ. On the other hand, if $g_0(T)$ is reducible in Λ, then by applying corollary 3.7, one would find that $g_0(T)$ can be factored as a product of distinguished polynomials of degree $< \deg(g_0(T))$. Hence $g_0(T)$ would be reducible in $\mathbb{Q}_p[T]$. Conversely, if $g_0(T)$ is reducible in $\mathbb{Q}_p[T]$, then it is reducible in $\mathbb{Z}_p[T]$ and its monic, irreducible factors are also distinguished. One can see this by reducing modulo $p\Lambda$. It is then clear that $g(T)$ is reducible in Λ. ■

Thus, up to multiplication by elements of $\Lambda^\times$, the irreducible elements of Λ are either p or any distinguished polynomial in $\mathbb{Z}_p[T]$ which is irreducible over $\mathbb{Z}_p$ or, equivalently, over $\mathbb{Q}_p$. Since $\mathbb{Z}_p[T]$ is a UFD, it is easy to deduce that Λ is also a UFD.

Now let X be any finitely generated, torsion Λ-module. We will give a partial proof of theorem 3.1. We let $Y = X_{\mathbb{Z}_p\text{-tors}}$. It is easy to see that Y is a Λ-submodule of X, and therefore is also finitely generated. This implies that Y has finite exponent, i.e., $p^m Y = 0$ for some $m \geq 0$. Also, X/Y is torsion-free as a $\mathbb{Z}_p$-module. Assume first that $Y = 0$. Let $g(T)$ be a nonzero annihilator of X. If we write $g(T) = p^m g'(T)$ where $m \geq 1$, then it is clear that $g'(T)$ annihilates X. Hence we can assume that $g(T) \notin p\Lambda$. Now if X has n generators, X will be a homomorphic image of $(\Lambda/(g(T)))^n$. It follows from corollary 3.6 that X is finitely generated as a $\mathbb{Z}_p$-module and, since $Y = 0$, X must be a free $\mathbb{Z}_p$-module: $X \cong \mathbb{Z}_p^\lambda$ for some $\lambda \geq 0$.

Consider the $\mathbb{Q}_p$-vector space $V = X \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ of dimension λ together with the endomorphism T. We can consider V as a module over $\mathbb{Q}_p[T]$, and since this ring is a PID, we have

$$V \cong \prod_{i=1}^{t} \mathbb{Q}_p[T]/(f_i(T)^{e_i})$$

where the $f_i(T)$'s are uniquely determined, monic irreducible polynomials over $\mathbb{Q}_p$ and the e_i's are uniquely determined nonnegative integers (everything up to order, of course). However, if we write $g(T) = u(T)g_0(T)$ where $g_0(T)$ is a distinguished polynomial, then $g_0(T)$ annihilates V and it follows that $f_i(T)|g_0(T)$ in $\mathbb{Q}_p[T]$ for each i. But this implies that each $f_i(T)$ is a distinguished polynomial in $\mathbb{Z}_p[T]$. Now X is a $\mathbb{Z}_p$-lattice in V and so is $X' = \prod_{i=1}^{t} \mathbb{Z}_p[T]/(f_i(T)^{e_i})$. It follows that for some $k \geq 0$, $p^k X \subset X'$. Clearly $p^k X$ is isomorphic to X. The index $[X' : p^k X]$ is obviously finite. Identifying $\mathbb{Z}_p[T]/(f_i(T)^{e_i})$ with $\Lambda/(f_i(T)^{e_i})$, we then obtain an injective Λ-module homomorphism

$$\varphi : X \to \prod_{i=1}^{t} \Lambda/(f_i(T)^{e_i})$$

where the $f_i(T)$'s are irreducible distinguished polynomials, and hence irreducible elements of Λ. The cokernel of φ is finite. This proves theorem 3.1 in the important special case where X is assumed to be $\mathbb{Z}_p$-torsion free. Note that

$$\mathrm{rank}_{\mathbb{Z}_p}(X) = \sum_{i=1}^{t} e_i \deg(f_i(T))$$

since, as we have seen, $f(T) = f_i(T)^{e_i}$ is a distinguished polynomial and $\Lambda/(f(T)) \cong \mathbb{Z}_p^{\deg(f)}$.

Two finitely generated, torsion Λ-modules X_1 and X_2 are said to be pseudo-isomorphic if there is a Λ-module homomorphism $\psi : X_1 \to X_2$ such that $\ker(\psi)$ and $\operatorname{coker}(\psi)$ are both finite. We then write $X_1 \sim X_2$. It turns out that this is an equivalence relation. Also, if X is any finitely generated, torsion Λ-module, then it is not hard to show that $X \sim Y \times X/Y$, where $Y = X_{\mathbb{Z}_p\text{-tors}}$ as before. Thus, to prove theorem 3.1 for X, it would suffice to show that Y is pseudo-isomorphic to a direct sum of finitely many Λ-modules of the form $\Lambda/(p^{\mu_j})$, where $\mu_j \geq 1$. For a complete proof of theorem 3.1, including the cases where $Y \neq 0$ or where $\operatorname{rank}_\Lambda(X) > 0$, we refer the reader to [Wa] or to [Bo]. The proofs found in those references are quite different—one involving a matrix reduction argument, the other a much more conceptual and general module-theoretic approach.

Suppose now that X is an arbitrary finitely generated, torsion Λ-module. In theorem 3.1, we would have $r = 0$ and we can assume that each $f_i(T)$ is taken to be either p or an irreducible, distinguished polynomial. Then the characteristic ideal of X is defined to be the ideal generated by the polynomial $f_X(T) = \prod_{i=1}^{t} f_i(T)^{e_i}$. Letting $Y = X_{\mathbb{Z}_p\text{-tors}}$ as before, we can apply our previous observations to the Λ-module X/Y. If we let $\lambda_X = \deg(f_X(T))$, then the invariant λ_X also has the following interpretations:

$$\lambda_X = \operatorname{rank}_{\mathbb{Z}_p}(X/Y) = \dim_{\mathbb{Q}_p}(X \otimes_{\mathbb{Z}_p} \mathbb{Q}_p).$$

We also define an invariant $\mu = \mu_X$ by $f_X(T) \in p^\mu\Lambda$, but $\notin p^{\mu+1}\Lambda$. That is, μ_X is the sum of the e_i's over all i's such that $f_i(T) = p$. In fact, $\mu_X = \mu_Y$ depends only on the structure of $Y = X_{\mathbb{Z}_p\text{-tors}}$ as a Λ-module. Assume that $p^m Y = 0$. For each j, $0 \leq j \leq m,$, let $Y[p^j]$ denote the kernel of the map $Y \xrightarrow{p^j} Y$, multiplication by p^j. Then for $1 \leq j \leq m$, $Y[p^j]/Y[p^{j-1}]$ can be considered as a $\widetilde{\Lambda}$-module, where recall that $\widetilde{\Lambda} = \Lambda/p\Lambda$ is the ring $\mathbb{F}_p[[T]]$. The above $\widetilde{\Lambda}$-modules are finitely generated. Then μ_X has the following interpretation:

$$\mu_X = \sum_{j=1}^{m} \operatorname{rank}_{\widetilde{\Lambda}}(Y[p^j]/Y[p^{j-1}]).$$

Since a finitely generated, torsion $\widetilde{\Lambda}$-module is finite, it is clear that $\mu_X > 0$ if and only if $X_{\mathbb{Z}_p\text{-tors}}$ is infinite. Other equivalent statements are that $X[p]$ is infinite or that X/pX is infinite. If $\mu_X = 0$, then X is a finitely generated $\mathbb{Z}_p$-module.

Our last general theorem concerning Λ-modules is the following very useful result which allows us to obtain information about X from certain quotients.

Theorem 3.9 *Let X be an abelian pro-p group on which Γ acts continuously. We regard X as a Λ-module. Then*

(1) $X = 0 \Longleftrightarrow X/TX = 0 \Longleftrightarrow X/\mathfrak{m}X = 0.$

(2) X is finitely generated as a Λ-module if and only if $X/\mathfrak{m}X$ is finite dimensional as an $\mathbb{F}_p$-vector space. The minimal number of generators of X as a Λ-module is $\dim_{\mathbb{F}_p}(X/\mathfrak{m}X)$.

(3) If X/TX is finite, then X is a torsion Λ-module.

Proof. Part (1) is the subject of exercise 3.2. For part (2), it is obvious that if X is finitely generated, then $\dim_{\mathbb{F}_p}(X/\mathfrak{m}X)$ is finite. To prove the converse, let $d = \dim_{\mathbb{F}_p}(X/\mathfrak{m}X)$ and pick $x_1, \ldots, x_d \in X$ so that their images in $X/\mathfrak{m}X$ form a basis over $\mathbb{F}_p$. Let $Y = \Lambda x_1 + \cdots + \Lambda x_d$, the Λ-submodule generated by $x_1, \ldots, x_d$. Since Λ is compact, Y is a closed subgroup of X. Hence X/Y is a pro-p group. But one can easily verify that $\mathfrak{m}(X/Y) = X/Y$. By part (1), this implies that $X/Y = 0$ and so $X = Y$. That is, X is generated as a Λ-module by the d elements $x_1, \ldots, x_d$.

Now assume that X/TX is finite. Then $X/\mathfrak{m}X$ is finite and so Λ is finitely generated as a Λ-module. Let $x_1, \ldots, x_d$ be a set of generators. Suppose that X/TX has exponent p^k. Then $p^k x_i \in TX$ for $1 \leq i \leq d$. Therefore we can write

$$p^k x_i = \sum_{j=1}^{d} T a_{ij}(T) x_j$$

for $1 \leq i \leq d$, where the $a_{ij}(T)$'s are elements of Λ. That is,

$$\sum_{j=1}^{d} (p^k \delta_{ij} - T a_{ij}(T)) x_j = 0$$

for each i. Let A be the $d \times d$ matrix $[p^k \delta_{ij} - T a_{ij}(T)]$. Let A^* be its adjoint matrix so that $A^* A = \det(A) I_d$. Let $g(T) = \det(A)$, which must be a nonzero element of Λ because $g(0) = p^{dk}$. We have $g(T) x_i = 0$ for each i and therefore $g(T)$ annihilates X. This proves (3). ■

Suppose now that G is any profinite group. That is, $G = \varprojlim G_n$, where the G_n's are finite groups. For simplicity, we will take the indexing set to be the set of nonnegative integers, although this is not essential. We also may assume that the homomorphisms $\varphi_{m,n} : G_m \to G_n$ for $m \geq n \geq 0$ which define the inverse limit are surjective. Then one obtains induced $\mathbb{Z}_p$-algebra homomorphisms

$$\psi_{m,n} : \mathbb{Z}_p[G_m] \to \mathbb{Z}_p[G_n].$$

Here, if $\mathcal{G}$ is any group, then $\mathbb{Z}_p[\mathcal{G}]$ denotes the group ring for $\mathcal{G}$ over $\mathbb{Z}_p$. The maps $\psi_{m,n}$ are surjective. One then defines the completed group ring for G over $\mathbb{Z}_p$ as

$$\mathbb{Z}_p[[G]] = \varprojlim \mathbb{Z}_p[G_n],$$

where the inverse limit is defined by the maps $\psi_{m,n}$. Now $\mathbb{Z}_p[G_n]$ is a compact topological ring, a $\mathbb{Z}_p$-algebra isomorphic to $\mathbb{Z}_p^{|G_n|}$ as a $\mathbb{Z}_p$-module. It follows that $\mathbb{Z}_p[[G]]$ is also a compact topological ring. Alternatively, one can define $\mathbb{Z}_p[[G]]$ as an inverse limit of the finite rings $(\mathbb{Z}/p^k\mathbb{Z})[G_n]$, each with the discrete topology, where $k \geq 1$, $n \geq 0$. For each n, there is a continuous, surjective, $\mathbb{Z}_p$-algebra homomorphism $\psi_n : \mathbb{Z}_p[[G]] \to \mathbb{Z}_p[G_n]$. Also, the ordinary group algebra $\mathbb{Z}_p[G]$ for G over $\mathbb{Z}_p$ can be identified with a subring of $\mathbb{Z}_p[[G]]$ in a natural way and turns out to be dense. This and other elementary properties of $\mathbb{Z}_p[[G]]$ are the subject of exercise 3.11.

We are interested in the special case $G = \Gamma \cong \mathbb{Z}_p$. Then we can take $G_n = \Gamma/\Gamma^{p^n}$, which is cyclic of order p^n. If γ_0 is a topological generator of Γ, then $\gamma_0^{(n)} = \gamma_0\Gamma^{p^n}$ generates G_n for each $n \geq 0$. The next result shows that the rings $\mathbb{Z}_p[[\Gamma]]$ and $\Lambda = \mathbb{Z}_p[[T]]$ can be identified. The identification is not canonical, but depends on the choice of γ_0.

Theorem 3.10 *There is a unique isomorphism*

$$\varepsilon : \Lambda \to \mathbb{Z}_p[[\Gamma]]$$

of topological $\mathbb{Z}_p$-algebras such that $\varepsilon(T) = \gamma_0 - 1$.

Proof. $\Lambda = \mathbb{Z}_p[[T]]$ is a compact $\mathbb{Z}_p$-algebra. For each $n \geq 0$, let $\omega_n = (1+T)^{p^n} - 1$, which is easily seen to be a distinguished polynomial of degree p^n. By corollary 3.6, $\Lambda/(\omega_n)$ is isomorphic to $\mathbb{Z}_p^{p^n}$ as a $\mathbb{Z}_p$-module. More precisely, by theorem 3.5, it is clear that $\{(1+T)^i + (\omega_n)\}_{0\le i<p^n}$ is a $\mathbb{Z}_p$-module basis for $\Lambda/(\omega_n)$. Also $(1+T)^{p^n} \equiv 1 \pmod{(\omega_n)}$. Hence we can define an isomorphism

$$\Lambda/(\omega_n) \to \mathbb{Z}_p[\Gamma/\Gamma^{p^n}]$$

of $\mathbb{Z}_p$-algebras by mapping $1+T+(\omega_n)$ to $\gamma_0^{(n)}$. Thus we obtain continuous, surjective, $\mathbb{Z}_p$-algebra homomorphisms $\Lambda \to \mathbb{Z}_p[\Gamma/\Gamma^{p^n}]$ for all $n \ge 0$ which map T to $\gamma_0^{(n)} - 1$. This induces a continuous, $\mathbb{Z}_p$-algebra homomorphism

$$\varepsilon : \Lambda \to \mathbb{Z}_p[[\Gamma]].$$

The image of ε is dense, but since Λ is compact, this image is also closed. Hence ε is surjective. It is clear that $\varepsilon(T) = \gamma_0 - 1$ and that this uniquely determines the map ε (assuming it is a continuous, $\mathbb{Z}_p$-algebra homomorphism). Also, $\ker(\varepsilon) \subset \bigcap_n (\omega_n)$, which is trivial. Hence ε is injective. The compactness of Λ implies that ε is a homeomorphism too. ■

The final topic of this section is to study the structure of certain specific Λ-modules in order to prove the following special case of the corank lemma of chapter 2. The argument is somewhat long, but is a good illustration of standard techniques of Iwasawa theory.

Theorem 3.11 *Let K_v be a finite extension of $\mathbb{Q}_p$. Suppose that A is a G_{K_v}-module and that $A \cong \mathbb{Q}_p/\mathbb{Z}_p$ as a group. Then $H^1(K_v, A)$ is a cofinitely generated $\mathbb{Z}_p$-module and* $\mathrm{corank}_{\mathbb{Z}_p}(H^1(K_v,A)) = [K_v : \mathbb{Q}_p] + \delta_A(K_v)$*, where $\delta_A(K_v) = 1$ if $A \cong \mathbb{Q}_p/\mathbb{Z}_p$ or $A \cong \mu_{p^\infty}$ as G_{K_v}-modules and $\delta_A(K_v) = 0$ otherwise.*

Note that $H^0(K_v, A)$ is either finite or all of A. The latter occurs only when $A \cong \mathbb{Q}_p/\mathbb{Z}_p$ as G_{K_v}-modules (i.e., the action of G_{K_v} on A is trivial). Also, $\widehat{A}(1) \cong \mathrm{Hom}(A, \mu_{p^\infty})$ and $H^0(K_v, \widehat{A}(1))$ is either trivial or all of $\widehat{A}(1)$, which is isomorphic to $\mathbb{Z}_p$ as a group. The latter occurs only when $A \cong \mu_{p^\infty}$ as G_{K_v}-modules. Thus

$$\delta_A(K_v) = \mathrm{corank}_{\mathbb{Z}_p}(H^0(K_v, A)) + \mathrm{rank}_{\mathbb{Z}_p}(H^0(K_v, \widehat{A}(1)))$$

and so the above theorem is just the content of the corank lemma when $r = 1$ and $v|p$. The two cases where $\delta_A(K_v) = 1$ are rather straightforward and are the subject of exercises 2.3 and 2.4. Therefore, we will assume that $\delta_A(K_v) = 0$ in the following proof.

Proof. The action of G_{K_v} on A is given by a homomorphism $\psi : G_{K_v} \to \mathbb{Z}_p^\times$. If ψ has finite order, then it factors through $\Delta = \mathrm{Gal}(F/K_v)$ where F is a finite extension of K_v. The corank lemma in this case is the subject of exercise 2.3. The argument just depends on local class field theory over F and studying the action of Δ on $F^\times$. It is straightforward and so we will now assume that $\mathrm{im}(\psi)$ is infinite. Let $F_\infty = \overline{K}_v^{\ker(\psi)}$ so that $G = \mathrm{Gal}(F_\infty/K_v)$ acts faithfully on A. Also, $G \cong \mathrm{im}(\psi)$, which is a subgroup of $\mathbb{Z}_p^\times$. Hence $G \cong \Delta \times \Gamma$, where $\Gamma \cong \mathbb{Z}_p$ and Δ is a finite group of order dividing $p-1$ if p is odd and of order 1 or 2 if $p = 2$. Let $F_0 = F_\infty^\Gamma$ so that $\Delta = \mathrm{Gal}(F_0/K_v)$ and $\Gamma = \mathrm{Gal}(F_\infty/F_0)$. That is, F_∞/F_0 is a $\mathbb{Z}_p$-extension. For $n \geq 0$, we let $F_n = F_\infty^{\Gamma^{p^n}}$. Then $F_\infty = \bigcup_n F_n$ and F_n/F_0 is cyclic of degree p^n. The inflation-restriction sequence

$$0 \to H^1(G, A) \xrightarrow{i} H^1(K_v, A) \xrightarrow{r} H^1(F_\infty, A)^G \longrightarrow H^2(G, A)$$

is exact and will allow us to study $H^1(K_v, A)$ by studying $H^1(F_\infty, A)^G$ instead.

If p is odd, then $H^2(G, A) = 0$ and so r is surjective. This follows easily from the facts that $|\Delta|$ is not divisible by p and Γ is a free pro-p group and hence has p-cohomological dimension 1. If $p = 2$ and $|\Delta| = 1$, then, for the same reason, $H^2(G, A) = 0$ and so r is surjective in this case too. But if $|\Delta| = 2$, then it is not hard to verify that $H^2(G, A) \cong \mathbb{Z}/2\mathbb{Z}$. Thus, $\mathrm{coker}(r)$ is finite or order ≤ 2 and is usually trivial. Now $\ker(r) = \mathrm{im}(i)$ also turns out to be finite of order ≤ 2 and is usually trivial. If $|\Delta| = 1$, then $G = \Gamma$ and one can apply exercise 2.2(c) to see that $H^1(G, A) = 0$. This is a consequence of the assumption that $H^0(K_v, A)$ is finite. If p is odd and $|\Delta| > 1$, then $A^\Delta = 0$. It is then even easier to see that $H^1(G, A) = 0$ (using a simple inflation-restriction argument). But if $p = 2$ and $|\Delta| = 2$, then A^Δ has order 2 and one finds that $H^1(G, A) \cong \mathbb{Z}/2\mathbb{Z}$. The above remarks show that

$$\mathrm{corank}_{\mathbb{Z}_p}(H^1(K_v, A)) = \mathrm{corank}_{\mathbb{Z}_p}(H^1(F_\infty, A)^G).$$

But $H^1(F_\infty, A) = \mathrm{Hom}_{\mathrm{cont}}(G_{F_\infty}, A)$ since G_{F_∞} acts trivially on A. Let $X = \mathrm{Gal}(M_\infty/F_\infty)$, where M_∞ denotes the maximal, abelian pro-p extension of F_∞. That is, M_∞ is the compositum of all finite, abelian p-extensions of F_∞. Then we have $H^1(F_\infty, A) = \mathrm{Hom}_{\mathrm{cont}}(X, A)$. From here on, we will omit the subscript cont, taking the requirement of continuity as understood.

Note that M_∞ is a Galois extension of K_v and that $\mathrm{Gal}(M_\infty/K_v)$ can be regarded as a group extension of the quotient group $\mathrm{Gal}(F_\infty/K_v) = G$ by the closed, normal subgroup $X = \mathrm{Gal}(M_\infty/F_\infty)$. Hence there is a natural action of G on X (by inner automorphisms). Then we have $H^1(F_\infty, A)^G = \mathrm{Hom}_G(X, A)$. Now X is a $\mathbb{Z}_p$-module on which G acts $\mathbb{Z}_p$-linearly and continuously. Let X^ψ denote the maximal quotient of X on which G acts by ψ. Then we have

$$\mathrm{corank}_{\mathbb{Z}_p}(H^1(K_v, A)) = \mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Hom}(X^\psi, A)) = \mathrm{rank}_{\mathbb{Z}_p}(X^\psi)$$

since $A \cong \mathbb{Q}_p/\mathbb{Z}_p$ as a group. The rest of the argument involves studying X as a G-module.

All of the characters of Δ have values in $\mathbb{Z}_p^\times$. If p is odd, so that $p \nmid |\Delta|$, then one has a decomposition of X by the characters of Δ (often referred to as the Δ-decomposition):

$$X = \bigoplus_{\chi \in \widehat{\Delta}} X^\chi.$$

Here $X^\chi = \{x \in X | \delta(x) = \chi(\delta)x \text{ for all } \delta \in \Delta\} = e_\chi X$, where e_χ is the idempotent for χ in $\mathbb{Z}_p[\Delta]$. If $p = 2$ and $|\Delta| = 2$, which is the only case where $|\Delta|$ is divisible by p, then we define X^χ as the maximal quotient of X on which Δ acts by χ. Now Δ acts on A by the character $\chi = \psi|_\Delta$, which we denote by ψ_Δ. Then $\mathrm{Hom}_\Delta(X, A) = \mathrm{Hom}(X^{\psi_\Delta}, A)$. Furthermore, Γ acts on A by the character $\psi_\Gamma : \Gamma \to 1 + p\mathbb{Z}_p$, where $\psi_\Gamma = \psi|_\Gamma$. If Y is any $\mathbb{Z}_p$-module on which Γ acts and if $\kappa : \Gamma \to 1 + p\mathbb{Z}_p$ is a continuous homomorphism, then we let Y^κ denote $Y/(\gamma_0 - \kappa(\gamma_0))Y$, which is the maximal quotient of Y on which Γ acts by the character κ. Here γ_0 is a fixed topological generator of Γ. In fact, we have $X^\psi = (X^{\psi_\Delta})^{\psi_\Gamma}$ and so it follows that

$$\mathrm{corank}_{\mathbb{Z}_p}(H^1(K_v, A)) = \mathrm{rank}_{\mathbb{Z}_p}(X^{\psi_\Delta}/(\gamma_0 - \psi_\Gamma(\gamma_0))X^{\psi_\Delta}).$$

We determine this rank by considering X^{ψ_Δ} as a Λ-module.

The Galois group X is an abelian, pro-p group. Applying exercise 3.3 to the discrete, p-primary Γ-module $\mathrm{Hom}(X, \mathbb{Q}_p/\mathbb{Z}_p)$, one can regard X as a Λ-module. We will prove the following statements about X which were proved by Iwasawa in [Iw].

(a) X is a finitely generated Λ-module.

(b) X has Λ-rank equal to $[K_v : \mathbb{Q}_p]|\Delta|$. More precisely, for each character χ of Δ, X^χ has Λ-rank equal to $[K_v : \mathbb{Q}_p]$.

(c) If F_∞ contains the group μ_{p^∞} of p-power roots of unity, then the Λ-torsion submodule $X_{\Lambda\text{-}\mathrm{tors}}$ is isomorphic to $T_p(\mu_{p^\infty})$, the Tate module of μ_{p^∞}. Otherwise, $X_{\Lambda\text{-}\mathrm{tors}} = 0$.

The key ingredient in proving these statements is local class field theory which gives the structure of $\mathrm{Gal}(M_n/F_n)$, where M_n denotes the maximal abelian pro-p extension of F_n. We have

$$\mathrm{Gal}(M_n/F_n) \cong \mathbb{Z}_p^{[F_n:\mathbb{Q}_p]+1} \times \mu_{F_n}$$

where μ_{F_n} denotes the group of p-power roots of unity in F_n. This comes from the reciprocity map $F_n^\times \to \mathrm{Gal}(F_n^{\mathrm{ab}}/F_n)$, which is injective and has dense image, together with the well-understood structure of $F_n^\times$ (which can be studied by using the p-adic log map). Note that $[F_n : \mathbb{Q}_p] = [K_v : \mathbb{Q}_p]|\Delta|p^n$ for $n \geq 0$. Furthermore, Δ can be identified with a subgroup of $\mathrm{Gal}(F_n/K_v)$ and so acts on $\mathrm{Gal}(M_n/F_n)$. We can consider the Δ-decomposition

$$\mathrm{Gal}(M_n/F_n) = \bigoplus_{\chi \in \widehat{\Delta}} \mathrm{Gal}(M_n/F_n)^\chi$$

and, since the reciprocity map is Δ-equivariant, one finds that the $\mathbb{Z}_p$-rank of $\mathrm{Gal}(M_n/F_n)^\chi$ is equal to $[K_v : \mathbb{Q}_p]p^n$ if χ is nontrivial and is equal to $[K_v : \mathbb{Q}_p]p^n{+}1$ if χ is trivial. The extra 1 could be thought of as corresponding to $\mathrm{Gal}(F_\infty/F_n) \cong \mathbb{Z}_p$ since $F_\infty \subset M_n$ and Δ acts trivially on $\mathrm{Gal}(F_\infty/F_n)$. Thus, we actually have that $\mathrm{rank}_{\mathbb{Z}_p}(\mathrm{Gal}(M_n/F_\infty)^\chi) = [K_v : \mathbb{Q}_p]p^n$ for all $n \geq 0$ and all characters χ of Δ.

The field M_n is just the maximal abelian extension of F_n contained in M_∞ and therefore $\mathrm{Gal}(M_\infty/M_n)$ is the closure of the commutator subgroup $\mathrm{Gal}(M_\infty/F_n)'$ of $\mathrm{Gal}(M_\infty/F_n)$. Consider the exact sequence

$$1 \to X \to \mathrm{Gal}(M_\infty/F_n) \to \mathrm{Gal}(F_\infty/F_n) \to 1.$$

If $g \in \mathrm{Gal}(F_\infty/F_n)$ and $x \in X$, recall that the action of g on x is defined by $g(x) = \widetilde{g}x\widetilde{g}^{-1}$, where $\widetilde{g} \in \mathrm{Gal}(M_\infty/F_n)$ is chosen so that $\widetilde{g}|_{F_\infty} = g$. Thus, $g(x)x^{-1} = \widetilde{g}x\widetilde{g}^{-1}x^{-1}$ is a commutator in $\mathrm{Gal}(M_\infty/F_n)$. We will leave it to the reader (in exercise 3.12) to prove the useful fact that

$$\mathrm{Gal}(M_\infty/F_n)' = \{\gamma_0^{p^n}(x)x^{-1} | x \in X\}$$

and that this is a closed subgroup of $\mathrm{Gal}(M_\infty/F_n)$. Switching to the usual additive notation for the Λ-module X, we therefore have

$$\mathrm{Gal}(M_\infty/M_n) = (\gamma_0^{p^n} - 1)X = \omega_n X \quad \text{and} \quad \mathrm{Gal}(M_n/F_\infty) = X/\omega_n X$$

for all $n \geq 0$, where, as previously, $\omega_n = (1+T)^{p^n} - 1$.

Statement (a) is now an immediate consequence of theorem 3.9, part 2 because $\omega_0 = T$ and X/TX is isomorphic to the finitely generated $\mathbb{Z}_p$-module $\mathrm{Gal}(M_0/F_\infty)$. This implies that $X/\mathfrak{m}X$ is finite. Statement (b) is a consequence of exercise 3.6.. For the first part, we note that the above remarks imply that $\mathrm{rank}_{\mathbb{Z}_p}(X/\omega_n X) = [F_n : \mathbb{Q}_p] = rp^n$, where $r = [K_v : \mathbb{Q}_p]|\Delta|$. To obtain the second part, note that the isomorphism $X/\omega_n X \cong \mathrm{Gal}(M_n/F_\infty)$ is Δ-equivariant. It follows that $(X/\omega_n X)^\chi \cong X^\chi/\omega_n X^\chi$ is isomorphic to $\mathrm{Gal}(M_n/F_\infty)^\chi$ and so, for each $\chi \in \widehat{\Delta}$ and $n \geq 0$, we have

$$\mathrm{rank}_{\mathbb{Z}_p}(X^\chi/\omega_n X^\chi) = [K_v : \mathbb{Q}_p]p^n.$$

Using exercise 3.6 again, we have $\mathrm{rank}_\Lambda(X^\chi) = [K_v : \mathbb{Q}_p]$ as stated.

The Λ-torsion submodule of X is a little more subtle to study. First we recall that G_{F_∞} has p-cohomological dimension 1, as was explained at the end of chapter 2. Consequently, as also explained at the end of chapter 2, it follows that $H^1(F_\infty, \mathbb{Q}_p/\mathbb{Z}_p)$ is a divisible group. That is, $\widehat{X} = \mathrm{Hom}(X, \mathbb{Q}_p/\mathbb{Z}_p)$ is divisible and so X is torsion-free as a $\mathbb{Z}_p$-module. In particular, it follows that X has no nonzero, finite Λ-submodules. Let $Y = X_{\Lambda\text{-}\mathrm{tors}}$ and let $W = X/Y$. Then W is a torsion-free Λ-module. This easily implies that we have an exact sequence

$$0 \to Y/\omega_n Y \to X/\omega_n X \to W/\omega_n W \to 0$$

for all $n \geq 0$. Now $\mathrm{rank}_\Lambda(W) = [K_v : \mathbb{Q}_p]|\Delta|$ and so it follows that $W/\omega_n W$ has $\mathbb{Z}_p$-rank $[K_v : \mathbb{Q}_p]|\Delta|p^n$, which is the same as the $\mathbb{Z}_p$-rank of $X/\omega_n X$. This implies that $Y/\omega_n Y$ must be finite and isomorphic to a subgroup of $(X/\omega_n X)_{\mathbb{Z}_p\text{-}\mathrm{tors}} = \mu_{F_n}$. If μ_{F_n} has bounded order as $n \to \infty$ (i.e., if μ_{p^∞} is not contained in F_∞), then so does $Y/\omega_n Y$. It follows that $Y = \varprojlim Y/\omega_n Y$ is itself finite and therefore we must have $Y = 0$. This proves the second part of statement (c).

For the first part of (c), note again that $Y = \varprojlim Y/\omega_n Y$. Since $Y/\omega_n Y$ is cyclic for all n, it is clear that if Y is infinite, then $Y \cong \mathbb{Z}_p$ as a $\mathbb{Z}_p$-module. Now, by exercise 3.5, it follows that the $\mathbb{Z}_p$-torsion subgroup of $W/\omega_n W$ has bounded order as $n \to \infty$. Hence if μ_{F_n} has unbounded order (i.e., if $\mu_{p^\infty} \subset F_\infty$), then $Y/\omega_n Y$ must have unbounded order too. Since $Y/\omega_n Y$ is isomorphic to a subgroup of μ_{F_n}, it follows that $Y \cong \varprojlim \mu_{F_n} = T_p(\mu_{p^\infty})$ as stated.

It is now easy to complete the proof of theorem 3.11. We proved before that $\mathrm{corank}_{\mathbb{Z}_p}(H^1(K_v, A)) = \mathrm{rank}_{\mathbb{Z}_p}(X^{\psi_\Delta}/g(T)X^{\psi_\Delta})$, where $g(T) = T - b$ with $b = \psi_\Gamma(\gamma_0) - 1 \in p\mathbb{Z}_p$. Thus $g(T)$ is a distinguished polynomial of degree 1. Statements (a), (b), (c) imply that X^{ψ_Δ} is pseudo-isomorphic to either $\Lambda^{[K_v:\mathbb{Q}_p]}$ or to $Y \times \Lambda^{[K_v:\mathbb{Q}_p]}$, where $Y = T_p(\mu_{p^\infty})$. The latter occurs if $\mu_{p^\infty} \subset F_\infty$ and ψ_Δ is the character giving the action of Δ on μ_{p^∞}. Now $\Lambda/g(T)\Lambda$ has $\mathbb{Z}_p$-rank 1 by corollary 3.6 (which is rather obvious in this case). If $\mu_{p^\infty} \not\subset F_\infty$, it then follows that $H^1(K_v, A)$ indeed has $\mathbb{Z}_p$-corank equal to $[K_v : \mathbb{Q}_p]$. If $\mu_{p^\infty} \subset F_\infty$, then $G = \mathrm{Gal}(F_\infty/K_v)$ acts on $T_p(\mu_{p^\infty})$ by a character χ. We are assuming $\psi \neq \chi$. If $\psi_\Delta \neq \chi_\Delta$, then $Y = 0$. If $\psi_\Delta = \chi_\Delta$, then $Y = T_p(\mu_{p^\infty})$, but $\psi_\Gamma \neq \chi_\Gamma$ and so it follows that $Y/g(T)Y$ is finite. In either case, we again find that $X^{\psi_\Delta}/g(T)X^{\psi_\Delta}$ has $\mathbb{Z}_p$-rank $[K_v : \mathbb{Q}_p]$. ■

Exercises

3.1 Let A be a finite, abelian p-group on which Γ acts continuously. Prove that $T^n A = 0$ for $n \gg 0$. Prove that $\mathfrak{m}^n A = 0$ when $n \gg 0$, where $\mathfrak{m}$ denotes the maximal ideal of Λ.

3.2 Let A be a discrete p-primary, abelian group on which Γ acts continuously. Prove that $A = \bigcup_n A^{\Gamma_n}$ (where $\Gamma_n = \Gamma^{p^n}$ for all $n \geq 0$). Prove that $A = 0 \iff A^\Gamma = 0 \iff A[p]^\Gamma = 0$. Use this to prove part (1) of theorem 3.9 by taking $A = \mathrm{Hom}_{\mathrm{cont}}(X, \mathbb{Q}_p/\mathbb{Z}_p)$.

3.3 Let A be as in exercise 3.2. We know how to make A into a $\mathbb{Z}_p$-module. Prove that if $a \in A$, then $T^n a = 0$ for $n \gg 0$. Using this, show that A can be made into a Λ-module. Let $X = \widehat{A}$. Show that if $x \in X$, then $T^n x \to 0$ in X. Using this, make X into a Λ-module.

3.4 Let Z be a finitely generated Λ-module. Show that Z is finite if and only if $\mathfrak{m}^n Z = 0$ for some $n \geq 0$. Prove that every finitely generated Λ-module X contains a Λ-submodule Z which is finite and contains all other finite Λ-submodules of X. Prove that if $f(T) \in \Lambda$, then $\Lambda/(f(T))$ contains no nonzero, finite Λ-submodules. Deduce that the kernel of the map occurring in theorem 3.1 must be the maximal finite Λ-submodule Z of X.

3.5 Suppose that X is a Λ-submodule of Λ^r and that $H = \Lambda^r/X$ is finite. For $n \geq 1$, let $\omega_n = (1+T)^{p^n} - 1$. Prove that $H \cong (X/\omega_n X)_{\mathbb{Z}_p\text{-tors}}$ as a Λ-module if $n \gg 0$. It follows that the finite Λ-module H is uniquely determined by the isomorphism class of X.

3.6 Suppose that X is a finitely generated Λ-module with the property that $\mathrm{rank}_{\mathbb{Z}_p}(X/\omega_n X) = rp^n + O(1)$ as $n \to \infty$. Prove that $\mathrm{rank}_\Lambda(X) = r$. Now assume in addition that $X/TX \cong \mathbb{Z}_p^r$. Prove that $X \cong \Lambda^r$ as a Λ-module.

3.7 In this problem, let $X = \Lambda/(f(T))$, where $f(T)$ is a nonzero element of Λ.

(a) Suppose that $X/\omega_n X$ is finite for all $n \geq 0$. Prove that

$$|X/\omega_n X| = u \prod_{\zeta^{p^n}=1} f(\zeta - 1).$$

where $u \in \mathbb{Z}_p^\times$. (Hint: Multiplication by $f(T)$ defines a $\mathbb{Z}_p$-linear map $\Lambda/(\omega_n) \to \Lambda/(\omega_n)$. The cokernel of this map is $X/\omega_n X$ and its order is the determinant, up to a p-adic unit.)

(b) If $f(T) = p^m$, then part (a) implies that $(X/\omega_n X) = p^{mp^n}$ for all $n \geq 0$. Assume that $f(T)$ is a distinguished polynomial of degree d. Assume that $X/\omega_n X$ is finite for all $n \geq 0$. Prove that $|X/\omega_n X| = p^{dn+c}$ for all $n \gg 0$, where c is some constant.

(c) Assume that X is a finitely generated torsion Λ-module and that $X/\omega_n X$ is finite for all n. Let $\mu = \mu_X$, $\lambda = \lambda_X$ as defined in this chapter. Using theorem 3.1, prove that $|X/\omega_n X| = p^{\mu p^n + \lambda n + O(1)}$ as $n \to \infty$.

3.8 Assume that A is a discrete, p-primary abelian group on which Γ acts continuously. Assume also that A^Γ has order p. Prove that either A is finite or that $\widehat{A} \cong \Lambda/(f(T))$, where $f(T)$ is an irreducible element of Λ. Deduce that if A is infinite, then either A has exponent p or A is $\mathbb{Z}_p$-cofree of finite $\mathbb{Z}_p$-corank.

3.9 Assume that A is a discrete, p-primary abelian group on which Γ acts continuously. Assume that A^Γ is finite and that $A^{\Gamma_{n+1}} = A^{\Gamma_n}$ for some $n \geq 0$. Prove that $A = A^{\Gamma_n}$.

3.10 (a) Let F_∞/F be a $\mathbb{Z}_p$-extension. Suppose that E is an elliptic curve defined over F and that $E(F_1)_p = E(F)_p$. Prove that $E(F_\infty)_p = E(F)_p$.

(b) Let E be an elliptic curve defined over $\mathbb{Q}$ with the following properties: E has good reduction at 2 and $\widetilde{E}(\mathbb{F}_2)$ has order 4, E has good reduction at 7, and $E(\mathbb{Q})_{\mathrm{tors}}$ has order 8. Let $\mathbb{Q}_\infty$ be the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$. Show that $E(\mathbb{Q}_\infty)_{\mathrm{tors}} = E(\mathbb{Q})_{\mathrm{tors}}$. (Note: The hypotheses are satisfied by the elliptic curve $y^2 + xy = y^3 - 115x + 392$ considered in chapter 1.)

3.11 (a) Let G be a profinite group. Consider the natural map

$$\mathbb{Z}_p[G] \to \mathbb{Z}_p[[G]].$$

Prove that this map is injective and that its image is dense.

(b) Suppose that G and H are profinite groups and that there is a continuous, surjective homomorphism $\varphi : G \to H$. Prove that the induced homomorphism $\mathbb{Z}_p[[G]] \to \mathbb{Z}_p[[H]]$ is also surjective.

(c) Assume that G is a pro-p group (i.e., an inverse limit of finite p-groups). Prove that $\mathbb{Z}_p[[G]]$ is a local ring.

3.12 In the notation of the proof of theorem 3.11, show that

$$\mathrm{Gal}(M_\infty/F_n)' = \{\gamma_0^{p^n}(x)x^{-1} | x \in X\}$$

and that this is a closed subgroup of $\mathrm{Gal}(M_\infty/F_n)$.

4 Mazur's Control Theorem.

The main result of this section is the following theorem of Mazur concerning the Galois theoretic behavior of Selmer groups. We suppose that F is a finite extension of $\mathbb{Q}$ and that E is an elliptic curve defined over F.

Theorem 4.1 *Assume that p is a prime and that E has good, ordinary reduction at all primes of F lying over p. Assume that $F_\infty = \bigcup_n F_n$ is a $\mathbb{Z}_p$-extension of F. Then the natural maps*

$$\mathrm{Sel}_E(F_n) \to \mathrm{Sel}_E(F_\infty)^{\mathrm{Gal}(F_\infty/F_n)}$$

have finite kernels and cokernels. Their orders are bounded as $n \to \infty$.

Of course, as before, F_n denotes the unique subfield of F_∞ containing F such that $[F_n : F] = p^n$. After proving this theorem, we will derive various corollaries, including theorem 1.4

Our proof of theorem 4.1 is based on the description of the images of the local Kummer homomorphisms presented in section 2, specifically theorems 2.1–2.4. We will also prove a special case of conjecture 3.3. Let E be any elliptic curve defined over F. Let K be an algebraic extension of F. For every prime η of K, we let

$$\mathcal{H}_E(K_\eta) = H^1(K_\eta, E[p^\infty])/\,\mathrm{im}(\kappa_\eta).$$

Let $\mathcal{P}_E(K) = \prod\limits_\eta \mathcal{H}_E(K_\eta)$, where η runs over all primes of K. Thus,

$$\mathrm{Sel}_E(K)_p = \ker\left(H^1(K, E[p^\infty]) \to \mathcal{P}_E(K)\right),$$

where the map is induced by restricting cocycles to decomposition groups. Also, we put

$$\mathcal{G}_E(K) = \mathrm{im}\left(H^1(K, E[p^\infty]) \to \mathcal{P}_E(K)\right).$$

Let $F_\infty = \bigcup_n F_n$ be an arbitrary $\mathbb{Z}_p$-extension of F. Consider the following commutative diagram with exact rows.

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Sel}_E(F_n)_p \arrow[r] \arrow[d, "s_n"] & H^1(F_n, E[p^\infty]) \arrow[r] \arrow[d, "h_n"] & \mathcal{G}_E(F_n) \arrow[r] \arrow[d, "g_n"] & 0 \\
0 \arrow[r] & \mathrm{Sel}_E(F_\infty)_p^{\Gamma_n} \arrow[r] & H^1(F_\infty, E[p^\infty])^{\Gamma_n} \arrow[r] & \mathcal{G}_E(F_\infty)^{\Gamma_n}. &
\end{tikzcd}$$

Here $\Gamma_n = \mathrm{Gal}(F_\infty/F_n) = \Gamma^{p^n}$. The maps s_n, h_n, and g_n are the natural restriction maps. The snake lemma then gives the exact sequence

$$0 \to \ker(s_n) \to \ker(h_n) \to \ker(g_n) \to \mathrm{coker}(s_n) \to \mathrm{coker}(h_n).$$

Therefore, we must study $\ker(h_n)$, $\mathrm{coker}(h_n)$, and $\ker(g_n)$, which we do in a sequence of lemmas.

Lemma 4.2 *The kernel of h_n is finite and has bounded order as n varies.*

Proof. By the inflation-restriction sequence, $\ker(h_n) \cong H^1(\Gamma_n, B)$, where B is the p-primary subgroup of $E(F_\infty)$. If B is finite, which is usually the case, then we will have $H^1(\Gamma_n, B) = \mathrm{Hom}(\Gamma_n, B)$ for $n \gg 0$. Theorem 4.1 follows immediately. But it is not necessary to assume the finiteness of B. If γ denotes a topological generator of Γ, then $H^1(\Gamma_n, B) = B/(\gamma^{p^n}-1)B$. (See exercise 2.2.) Since $E(F_n)$ is finitely generated, the kernel of $\gamma^{p^n}-1$ acting on B is finite. Now B_{div} has finite $\mathbb{Z}_p$-corank. Hence (by exercise 2.2(c)), it follows that $(\gamma^{p^n}-1)B_{\mathrm{div}} = B_{\mathrm{div}}$ and so it is clear that

$$B_{\mathrm{div}} \subseteq (\gamma^{p^n}-1)B \subseteq B.$$

Thus, $H^1(\Gamma_n, B)$ has order bounded by $[B : B_{\mathrm{div}}]$, which is finite and independent of n. If B is finite, then $\ker(h_n)$ has the same order as $H^0(\Gamma_n, B)$, namely $|E(F_n)_p|$. ■

Lemma 4.3 $\mathrm{Coker}(h_n) = 0$.

Proof. By the inflation-restriction exact sequence, the sequence

$$H^1(F_n, E[p^\infty]) \to H^1(F_\infty, E[p^\infty])^{\Gamma_n} \to H^2(\Gamma_n, B)$$

is exact, where $B = H^0(F_\infty, E[p^\infty])$ again. But $\Gamma_n \cong \mathbb{Z}_p$ is a free pro-p group. Therefore Γ_n has p-cohomological dimension 1. Hence $H^2(\Gamma_n, B) = 0$ and so h_n is surjective as claimed. ■

Let v be any prime of F. We will let v_n denote any prime of F_n lying over v. To study $\ker(g_n)$, we focus on each factor in $\mathcal{P}_E(F_n)$ by considering

$$r_{v_n} : \mathcal{H}_E((F_n)_{v_n}) \to \mathcal{H}_E((F_\infty)_\eta)$$

where η is any prime of F_∞ lying above v_n. ($\mathcal{P}_E(F_\infty)$ has a factor for all such η's, but the kernels will be the same.) If v is archimedean, then v splits completely in F_∞/F, i.e., $F_v = (F_\infty)_\eta$ for all $\eta | v$. Thus, $\ker(r_{v_n}) = 0$. For nonarchimedean v, we consider separately $v \nmid p$ and $v | p$.

Lemma 4.4 *Suppose v is a nonarchimedean prime not dividing p. Then* $\ker(r_{v_n})$ *is finite and has bounded order as n varies. If E has good reduction at v or if v splits completely in F_∞/F, then* $\ker(r_{v_n}) = 0$ *for all n.*

Proof. Let Γ_v denote the decomposition subgroup of Γ for any nonarchimedean prime v. If Γ_v is trivial, then v splits completely in F_∞/F and hence the lemma is obvious because $F_v = (F_\infty)_\eta$ and $\ker(r_{v_n}) = 0$ for all n. Otherwise, Γ_v has finite index in Γ and so v is finitely decomposed in F_∞/F. We now assume this. By theorem 2.1, $\mathcal{H}_E(M_\eta) = H^1(M_\eta, E[p^\infty])$ for every algebraic extension M_η of F_v. Let $B_v = H^0(K, E[p^\infty])$, where $K = (F_\infty)_\eta$. Since v is unramified and finitely decomposed in F_∞/F, K is the unramified $\mathbb{Z}_p$-extension of F_v (in fact, the only $\mathbb{Z}_p$-extension of F_v). The group B_v is isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^e \times$ (a finite group), where $0 \le e \le 2$. Let $\Gamma_{v_n} = \mathrm{Gal}(K/(F_n)_{v_n})$, which is isomorphic to $\mathbb{Z}_p$, topologically generated by γ_{v_n}, say. Then, using exercise 2.2 again, we have

$$\ker(r_{v_n}) \cong H^1(\Gamma_{v_n}, B_v) \cong B_v/(\gamma_{v_n} - 1)B_v.$$

Since $E((F_n)_{v_n})$ has a finite p-primary subgroup, it is clear that $(\gamma_{v_n} - 1)B_v$ contains $(B_v)_{\mathrm{div}}$ (just as in the proof of lemma 4.2) and hence

$$|\ker(r_{v_n})| \le |B_v/(B_v)_{\mathrm{div}}|. \tag{20}$$

This bound is independent of n and v_n. We have equality if $n \gg 0$. Now assume that E has good reduction at v. Then, since $v \nmid p$, $F_v(E[p^\infty])/F_v$ is unramified. It is clear that $K \subseteq F_v(E[p^\infty])$ and that $\Delta = \mathrm{Gal}(F_v(E[p^\infty])/K)$ is a finite, cyclic group of order prime to p. One can then prove that $B_v = E[p^\infty]^\Delta$ is divisible. Therefore, $\ker(r_{v_n}) = 0$ as stated. ■

Now assume that $v|p$. For each n, we let f_{v_n} denote the residue field for $(F_n)_{v_n}$. It doesn't depend on the choice of v_n. Now either v splits completely in F_∞/F, v is ramified in F_∞/F, or v is unramified but finitely decomposed in F_∞/F. In the first two cases, the finite field f_{v_n} stabilizes and so f_η is finite, where η is any prime of F_∞ lying over v and f_η is the corresponding residue field. Let $\widetilde{E}$ denote the reduction of E at v. Then we have

Lemma 4.5 *Suppose that v is a prime dividing p. Assume that E has good, ordinary reduction at v. Then* $\ker(r_{v_n})$ *is finite and has bounded order as n varies.*

Proof. If v splits completely in F_∞/F, then $\ker(r_{v_n}) = 0$ for all n. Assume that v is ramified in F_∞/F. In this case, theorem 2.4 is applicable. Then r_{v_n} can be viewed as the composition of the following two maps:

$$\begin{aligned} a_{v_n} &: H^1((F_n)_{v_n}, E[p^\infty])/\operatorname{im}(\kappa_{v_n}) \longrightarrow H^1((F_n)_{v_n}, E[p^\infty])/\operatorname{im}(\varepsilon_{v_n}) \\ b_{v_n} &: H^1((F_n)_{v_n}, E[p^\infty])/\operatorname{im}(\varepsilon_{v_n}) \longrightarrow H^1((F_\infty)_\eta, E[p^\infty])/\operatorname{im}(\varepsilon_\eta). \end{aligned}$$

Here we are using the notation of chapter 2. Now a_{v_n} is clearly surjective. Hence

$$|\ker(r_{v_n})| = |\ker(a_{v_n})| \cdot |\ker(b_{v_n})|.$$

But $\ker(a_{v_n}) = \operatorname{im}(\varepsilon_{v_n})/\operatorname{im}(\kappa_{v_n})$ and, by theorem 2.3, the order of this group is bounded by $|\widetilde{E}(f_\eta)_p|$, which is finite. On the other hand, the exact sequence

$$0 \to \mathcal{F}[p^\infty] \to E[p^\infty] \to \widetilde{E}[p^\infty] \to 0$$

of Galois modules gives us the following commutative diagram:

$$\begin{tikzcd} 0 \arrow[r] & H^1((F_n)_{v_n}, E[p^\infty])/\operatorname{im}(\varepsilon_{v_n}) \arrow[r, "\pi_{v_n}"] \arrow[d, "b_{v_n}"] & H^1((F_n)_{v_n}, \widetilde{E}[p^\infty]) \arrow[d, "c_{v_n}"] \\ 0 \arrow[r] & H^1((F_\infty)_\eta, E[p^\infty])/\operatorname{im}(\varepsilon_\eta) \arrow[r, "\pi_\eta"] & H^1((F_\infty)_\eta, \widetilde{E}[p^\infty]). \end{tikzcd}$$

Therefore, $|\ker(b_{v_n})| \leq |\ker(c_{v_n})|$. Now

$$\ker(c_{v_n}) \cong H^1((F_\infty)_\eta/(F_n)_{v_n}, \widetilde{E}(f_\eta)_p) \cong \widetilde{E}(f_\eta)_p/(\gamma_{v_n} - 1)\widetilde{E}(f_\eta)_p$$

where γ_{v_n} is a topological generator of $\operatorname{Gal}((F_\infty)_\eta/(F_n)_{v_n})$. Thus $|\ker(c_{v_n})|$ is bounded above by $|\widetilde{E}(f_\eta)_p|$ and so we obtain

$$|\ker(r_{v_n})| \leq |\widetilde{E}(f_\eta)_p|^2 \tag{21}$$

if v is ramified in F_∞/F.

Finally, assume that v is unramified but finitely decomposed in F_∞/F. Then $(F_\infty)_\eta$ is the unramified $\mathbb{Z}_p$-extension of $F_v(21)$. In this case, $\ker(r_{v_n}) = 0$ for all n. We will sketch the argument. (Since f_η is infinite, we can't apply theorem 2.4.) The Kummer sequence (16) reduces this to showing that $H^1(L/M, E(L))$ is trivial whenever M is a finite extension of F_v and

L/M is a finite, unramified p-extension. Let l and m denote the residue fields of L and M, respectively. Then we have an exact sequence

$$0 \to \mathcal{F}(\mathfrak{m}_L) \to E(L) \to \widetilde{E}(l) \to 0,$$

where $\mathfrak{m}_L$ denotes the maximal ideal of L and $\mathcal{F}(\mathfrak{m}_L)$ the group of points on the formal group $\mathcal{F}$. It is enough to verify that $H^1(L/M, \mathcal{F}(\mathfrak{m}_L))$ and $H^1(L/M, \widetilde{E}(l))$ are both trivial. Now $\mathrm{Gal}(L/M) = \mathrm{Gal}(l/m)$. The vanishing of $H^1(L/M, \mathcal{F}(\mathfrak{m}_L)$ can be proved by using thte fact that $\mathcal{F}(\mathfrak{m}_L)$ has a filtration where the successive quotients are isomorphic to the additive group l and $H^1(l/m, l) = 0$. The vanishing of $H^1(L/M, \widetilde{E}(l)) = H^1(l/m, \widetilde{E}(l))$ follows from that of $H^1(m, \widetilde{E}(\overline{m}))$, where $\overline{m}$ denotes the algebraic closure of m, and this can be shown just as in exercise 2.5. ■

Let v be any prime of F. If v splits completely in F_∞/F, then $\ker(r_{v_n}) = 0$ and so these primes contribute nothing to $\ker(g_n)$. For all other primes v of F, the number of primes v_n of F_n lying above v is bounded as $n \to \infty$. If E has good reduction at v and $v \nmid p$, then $\ker(r_{v_n}) = 0$, and so these primes contribute nothing to $\ker(g_n)$. Thus there are only finitely many v's that need to be considered and, for each such v, there are only a bounded number of v_n's. For those v_n's, lemmas 4.4 and 4.5 imply that $|\ker(r_{v_n})|$ is bounded. Combining these observations, we have proved the following lemma.

Lemma 4.6 *The order of* $\ker(g_n)$ *is bounded as* n *varies.*

Lemma 4.2 implies that $\ker(s_n)$ is finite and has bounded order no matter what type of reduction E has at $v|p$. Lemmas 4.3 and 4.6 show that $\mathrm{coker}(s_n)$ is finite and of bounded order, assuming that E has good, ordinary reduction at all $v|p$. Thus, theorem 4.1 is proved.

Here is one corollary of theorem 4.1. It implies theorem 1.4 since the finiteness of $\mathrm{Sel}_E(F)_p$ is equilvalent to that of $E(F)$ and $\text{Ш}_E(F)_p$.

Corollary 4.7 *Suppose that* E *is an elliptic curve defined over* F *and that* p *is a prime such that* E *has good, ordinary reduction at all primes of* F *lying above* p*. Assume also that* $\mathrm{Sel}_E(F)_p$ *is finite. Then* $\mathrm{Sel}_E(F_\infty)_p$ *is* Λ*-cotorsion. Consequently,* $\mathrm{rank}_{\mathbb{Z}}(E(F_n))$ *is bounded as* n *varies.*

Proof. Under the above hypotheses, theorem 4.1 implies that $\mathrm{Sel}_E(F_\infty)_p^\Gamma$ is finite. Let $X = \mathrm{Hom}(\mathrm{Sel}_E(F_\infty)_p, \mathbb{Q}_p/\mathbb{Z}_p)$. Then X is a Λ-module and X/TX is finite. (Note that X/TX is the maximal quotient of X on which Γ acts trivially. Hence X/TX is the Pontryagin dual of $\mathrm{Sel}_E(F_\infty)_p^\Gamma$.) By theorem 3.9, it follows that X is a finitely generated, torsion Λ-module. Hence $\mathrm{Sel}_E(F_\infty)_p$ is indeed Λ-cotorsion. As we saw in chapter 3, $X/X_{\mathbb{Z}_p\text{-tors}} \cong \mathbb{Z}_p^\lambda$ for some $\lambda \geq 0$. This implies that

$$(\mathrm{Sel}_E(F_\infty)_p)_{\mathrm{div}} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^\lambda.$$

Using theorem 4.1 again (giving the finiteness of the kernels), it follows that $(\mathrm{Sel}_E(F_n)_p)_{\mathrm{div}} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{t_n}$ where $t_n \leq \lambda$. Now

$$E(F_n) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{\mathrm{rank}_{\mathbb{Z}}(E(F_n))}$$

is a subgroup of $(\mathrm{Sel}_E(F_n)_p)_{\mathrm{div}}$ and therefore we obtain the inequality $\mathrm{rank}_{\mathbb{Z}}(E(F_n)) \leq \lambda$ for all $n \geq 0$. ■

The next result gives sufficient conditions for $\mathrm{Sel}_E(F_\infty)_p$ to be trivial.

Corollary 4.8 *Suppose that E is an elliptic curve defined over F and that p is a prime such that E has good, ordinary reduction at all primes of F lying over p. Assume that $\mathrm{Sel}_E(F)_p = 0$, that none of the primes of F over p are anomalous for E, and that $E(F_v)_p = 0$ for all primes v of F where E has bad reduction. Then $\mathrm{Sel}_E(F_\infty)_p = 0$.*

Proof. By lemma 4.3, $\mathrm{coker}(h_0) = 0$. Assume that $v|p$. If v is unramified in F_∞/F, then $\ker(r_v) = 0$. If v is ramified in F_∞/F, then the residue field f_η for a prime η of F_∞ above v is a finite p-extension of f_v, the residue field for v. Since $\widetilde{E}(f_\eta)_p^{\mathrm{Gal}(f_\eta/f_v)} = \widetilde{E}(f_v)_p = 0$, it follows that $\widetilde{E}(f_\eta)_p = 0$. Hence, by (21), $\ker(r_v) = 0$. Assume now that v is a prime of F where E has bad reduction (and so $v \nmid p$). If η is a prime of F_∞ lying above v, then $\mathrm{Gal}((F_\infty)_\eta/F_v)$ is either trivial or isomorphic to $\mathbb{Z}_p$. Since $E((F_\infty)_\eta)^{\mathrm{Gal}((F_\infty)_\eta/F_v)} = E(F_v) = 0$, it follows that $E((F_\infty)_\eta) = 0$. Thus the group B_v occurring in the proof of lemma 4.4 is trivial. Therefore, it is clear that $\ker(r_v) = 0$. Combining these remarks, we see that $\ker(g_0) = 0$. Therefore, $\mathrm{coker}(s_0) = 0$. That is, the map $\mathrm{Sel}_E(F)_p \to \mathrm{Sel}_E(F_\infty)_p^\Gamma$ is surjective. The hypothesis that $\mathrm{Sel}_E(F)_p = 0$ implies that $\mathrm{Sel}_E(F_\infty)_p^\Gamma = 0$. Therefore $X/TX = 0$, where $X = \mathrm{Hom}(\mathrm{Sel}_E(F_\infty)_p, \mathbb{Q}_p/\mathbb{Z}_p)$. By theorem 3.9, $X = 0$ and so $\mathrm{Sel}_E(F_\infty)_p = 0$ too. ■

Remark. The hypothesis for the primes v where E has bad reduction can be weakened. It suffices to assume that $B_v = H^0((F_\infty)_\eta, E[p^\infty])$ is divisible.

This is equivalent to assuming that the Tamagawa factor c_v for E/F_v is not divisible by p. (See exercise 4.6).

The next result concerns the growth of the order of $Ш_E(F_n)_p$, assuming that this group is finite for all n. The hypothesis that $E(F_n)$ is finite for all n is not necessary, but it simplifies the argument. For a more general result, see theorem 1.10 in [Gre2], which is proved at the end of section 3 of that article.

Corollary 4.9 *Assume that E is an elliptic curve defined over F and that E has good, ordinary reduction at all primes of F lying above p. Let F_∞/F be a $\mathbb{Z}_p$-extension. Assume that both $E(F_n)$ and $Ш_E(F_n)_p$ are finite for all $n \geq 0$. Then there exist integers $\lambda, \mu \geq 0$ depending only on E and F_∞/F such that $|Ш_E(F_n)_p| = p^{\lambda n + \mu p^n + O(1)}$ as $n \to \infty$.*

Proof. Let $X = \mathrm{Hom}(\mathrm{Sel}_E(F_\infty)_p, \mathbb{Q}_p/\mathbb{Z}_p)$. Then $\mathrm{Sel}_E(F_n)_p$ is finite for all $n \geq 0$ and therefore so is $\mathrm{Sel}_E(F_\infty)_p^\Gamma$. Now $|\mathrm{Sel}_E(F_\infty)_p^{\Gamma_n}| = |X/\omega_n X|$, where $\omega_n = (1+T)^{p^n} - 1$. This is because $X/\omega_n X$ is the maximal quotient of X on which Γ_n acts trivially. Hence $X/\omega_n X \cong \mathrm{Hom}(\mathrm{Sel}_E(F_\infty)_p^{\Gamma_n}, \mathbb{Q}_p/\mathbb{Z}_p)$ is just the Pontryagin dual of $\mathrm{Sel}_E(F_\infty)_p^{\Gamma_n}$ and so has the same order. By theorem 4.1, $|\mathrm{Sel}_E(F_n)_p|/|X/\omega_n X| = p^{t_n}$, where $|t_n|$ is bounded as n varies. Corollary 4.7 implies that X is a torsion Λ-module. The stated result follows from exercise 3.7(c). The integers λ and μ are just the Iwasawa invariants of the Λ-module X: $\lambda = \lambda_X$, $\mu = \mu_X$. ■

Remark. Under the hypotheses of corollary 4.9, the integers λ and/or μ can be positive. Examples where $\mu > 0$ were found by Mazur and are discussed in his paper [Ma1]. One such example is outlined in exercises 4.1–4.5. Other examples and results about λ and μ can be found in section 5 of [Gre2], e.g. corollary 5.6, propositions 5.7, 5.10, and various examples where λ and μ can be calculated precisely.

Theorem 1.6 shows that it is possible for $\mathrm{rank}(E(F_n))$ to be unbounded in a $\mathbb{Z}_p$-extension $F_\infty = \bigcup_n F_n$ even if E has good, ordinary reduction at the primes over p. But, as suggested by the comment after that theorem, there is some regularity to the growth of the rank. This is explained by the following result.

Corollary 4.10 *Suppose again that E is an elliptic curve defined over F which has good, ordinary reduction at all primes of F lying over p. Let*

F_∞/F be a $\mathbb{Z}_p$-extension. Let $r = \mathrm{corank}_\Lambda(\mathrm{Sel}_E(F_\infty)_p)$. Then

$$\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}_E(F_n)_p) = rp^n + O(1)$$

as $n \to \infty$. In particular, if $Ш_E(F_n)_p$ is finite for all n, then $\mathrm{rank}(E(F_n)) = rp^n + O(1)$ *as $n \to \infty$.*

Proof. Let $X = \mathrm{Hom}(\mathrm{Sel}_E(F_\infty)_p, \mathbb{Q}_p/\mathbb{Z}_p)$. We know that X is a finitely generated Λ-module. According to theorem 3.1 and corollary 3.6, X is pseudo-isomorphic to $\Lambda^r \times Y \times Z$, where Y is a free $\mathbb{Z}_p$-module of finite rank and Z is a torsion group of bounded exponent. As in the proof of corollary 4.9, $X/\omega_n X$ is the Pontryagin dual of $\mathrm{Sel}_E(F_\infty)_p^{\Gamma_n}$ and so

$$\mathrm{rank}_{\mathbb{Z}_p}(X/\omega_n X) = \mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}_E(F_\infty)_p^{\Gamma_n}).$$

By theorem 4.1, $\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}_E(F_\infty)_p^{\Gamma_n}) = \mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}_E(F_n)_p)$. Now $\Lambda/\omega_n\Lambda$ has $\mathbb{Z}_p$-rank p^n. (It can be identified with the group ring $\mathbb{Z}_p[\Gamma/\Gamma_n]$.) Also, $Y/\omega_n Y$ has bounded $\mathbb{Z}_p$-rank and $Z/\omega_n Z$ is finite. It is then clear that $\mathrm{rank}_{\mathbb{Z}_p}(X/\omega_n X) = rp^n + O(1)$ as $n \to \infty$ and this implies the first statement. Under the assumption that $Ш_E(F_n)_p$ is finite, $E(F_n) \otimes (\mathbb{Q}_p/\mathbb{Z}_p)$ has finite index in $\mathrm{Sel}_E(F_n)_p$ and so has the same $\mathbb{Z}_p$-corank. The $\mathbb{Z}_p$-corank of $E(F_n) \otimes (\mathbb{Q}_p/\mathbb{Z}_p)$ is equal to $\mathrm{rank}(E(F_n))$, giving the second statement. ∎

What happens if E doesn't have good, ordinary reduction at the primes of F lying over p? If E has potentially, ordinary reduction at all primes of F over p (i.e., good, ordinary reduction at those primes over some finite extension of F), then theorem 4.1 is still valid. The proof requires only some small modifications. The situation is more interesting if E is only assumed to have (potentially) ordinary or multiplicative reduction at the primes of F above p. The conclusion of theorem 4.1 should conjecturally still hold if F_∞ is the cyclotomic $\mathbb{Z}_p$-extension of F. This can be proved if $F = \mathbb{Q}$, but the proof needs the rather deep result that the Tate period q_E for E (assuming that E has multiplicative reduction at p) is not of the form $q_E = \zeta p^a$, where ζ is a root of unity. This was only established recently by Barré-Sirieix, Diaz, Gramain and Philibert who proved that q_E is actually transcendental if E has an algebraic j-invariant. (See section 3 of [Gre2] for a more thorough discussion.) For arbitrary $\mathbb{Z}_p$-extensions, theorem 4.1 would not in general be true under the above assumption.

Now let's assume that E has supersingular (or potentially supersingular) reduction for at least one prime of F lying over p. If F_∞/F is a $\mathbb{Z}_p$-extension which is ramified at such a prime, then one can show that $\mathrm{Sel}_E(F_\infty)_p$ has positive Λ-corank. If $r = \mathrm{corank}_\Lambda(\mathrm{Sel}_E(F_\infty)_p)$, then, as shown in the proof of corollary 4.10, $\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}_E(F_\infty)_p^{\Gamma_n}) = rp^n + O(1)$ as $n \to \infty$. Assume that $\mathrm{rank}(E(F_n))$ is bounded and that $Ш_E(F_n)_p$ is finite for all n. (Theorems 1.5 and 1.8 provide many cases where this assumption is known to hold.) Then $\mathrm{Sel}_E(F_n)_p$ would have bounded $\mathbb{Z}_p$-corank as $n \to \infty$ and so the conclusion in theorem 4.1 would fail to be true. In fact, the cokernel of the map $\mathrm{Sel}_E(F_n)_p \to \mathrm{Sel}_E(F_\infty)_p^{\Gamma_n}$ would have unbounded $\mathbb{Z}_p$-corank. (The kernel would still be finite and of bounded order by lemma 4.2.)

It is lemma 4.5 which is not valid if E has supersingular reduction at a prime v of F lying over p. For any $n \geq 0$, consider the map

$$r_{v_n} : \mathcal{H}_E((F_n)_{v_n}) \to \mathcal{H}_E((F_\infty)_\eta).$$

As discussed in chapter 2, if $d_n = [(F_n)_{v_n} : \mathbb{Q}_p]$, then $H^1((F_n)_{v_n}, E[p^\infty])$ has $\mathbb{Z}_p$-corank $2d_n$ and $\mathrm{im}(\kappa_{v_n})$ has $\mathbb{Z}_p$-corank d_n. Therefore, $\mathcal{H}((F_n)_v) = H^1((F_n)_v, E[p^\infty])/\mathrm{im}(\kappa_{v_n})$ has $\mathbb{Z}_p$-corank equal to d_n. This is true no matter what reduction type E has at the prime v. Assume that E has supersingular (or potentially supersingular) reduction at v. Assume also that $(F_\infty)_\eta/F_v$ is a ramified $\mathbb{Z}_p$-extension (i.e., the inertia subgroup of $\Gamma = \mathrm{Gal}(F_\infty/F)$ for v is nontrivial). Under these assumptions, it turns out surprisingly that $\mathrm{im}(\kappa_\eta) = H^1((F_\infty)_\eta, E[p^\infty])$. That is, $\mathcal{H}_E((F_\infty)_\eta) = 0$. Thus, even though the $\mathbb{Z}_p$-corank of $\mathcal{H}_E((F_n)_{v_n})$ is unbounded, the direct limit of these groups under the restriction maps is zero. Hence $\ker(r_{v_n}) = \mathcal{H}_E((F_n)_{v_n})$ for all $n \geq 0$.

The difference between the ordinary and supersingular cases shows up rather clearly in theorem 1.6, especially in the more precise statements (3) and (4). According to (4), under the assumption that F is an imaginary quadratic field and that $\mathrm{End}(E) \otimes \mathbb{Q} \cong F$, we have

$$\mathrm{rank}(E(F_n^{\mathrm{ac}})) = 2{\sum_{j=1}^{n}}' \varphi(p^j) + O(1).$$

if E has supersingular reduction at p. Here $\sum'$ denotes the sum over those j's with a fixed parity (depending on the parity of $\mathrm{ord}_{s=1}(L(E/\mathbb{Q}, s))$. Compare this with corollary 4.10. Another interesting result is the following recent theorem of Kurihara which should be compared with corollary 4.9.

Theorem 4.11 *Suppose that E is a modular elliptic curve defined over $\mathbb{Q}$ which has good, supersingular reduction at a prime $p \geq 5$. Assume that $L(E,1)/\Omega_E$ and the Tamagawa factors for all primes where E has bad reduction are not divisible by p. Assume also that $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong GL_2(\mathbb{Z}/p\mathbb{Z})$. Let $\mathbb{Q}_\infty = \bigcup_n \mathbb{Q}_n$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. Then $\text{Ш}_E(\mathbb{Q}_n)_p$ is finite and its order is p^{t_n} where*

$$t_n = {\sum_{j=1}^{n-1}}' p^j - \left[\frac{n}{2}\right]$$

for $n > 0$. Here $\sum'$ denotes the sum over integers $j \equiv n-1 \pmod 2$.

Exercises

In exercises 4.1–4.5, we consider the elliptic curve $E = X_0(11)$, which is defined by $y^2 + y = x^3 - x^2 - 10x - 20$.

4.1 In Cremona's tables, one fines that E has two $\mathbb{Q}$-isogenies of degree 5 and that $E(\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z}$. Deduce that $E[5] \cong \mu_5 \times \mathbb{Z}/5\mathbb{Z}$ as a $G_\mathbb{Q}$-module.

4.2 Let $\Sigma = \{\infty, 5, 11\}$. One can consider $H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, \mu_5)$ as a Λ-module, where $\mathbb{Q}_\infty$ denotes the cyclotomic $\mathbb{Z}_5$-extension of $\mathbb{Q}$. Show that the μ-invariant of $H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, \mu_5)\widehat{}$ is 1. (Hint: Use Kummer theory and consider the units of the fields $\mathbb{Q}_n$. The fact that the class number of $\mathbb{Q}_n$ is not divisible by 5 is helpful)

4.3 Show that E has good, ordinary reduction at $p = 5$. Show that $\mu_5 \subset \ker(E[5^\infty] \to \widetilde{E}[5^\infty])$. (Note: To define the reduction map, one must choose an embedding $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_5$.)

4.4 There is a natural map

$$\varepsilon : H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, \mu_5) \to H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[5^\infty]).$$

Show that $\ker(\varepsilon)$ is finite and that $\mathrm{im}(\varepsilon) \subset \mathrm{Sel}_E(\mathbb{Q}_\infty)_5$. The Λ-module $\mathrm{Sel}_E(\mathbb{Q}_\infty)\widehat{}_5$ is Λ-torsion by corollary 4.7. Show that its μ-invariant is positive.

4.5 A theorem of Kato turns out to imply that $\text{Ш}_E(\mathbb{Q}_n)$ is finite for all n. Prove that $\dim_{\mathbb{Z}/p\mathbb{Z}}(\text{Ш}_E(\mathbb{Q})[p]) \geq p^n - c$ for all n, where c is some constant.

References

[BeDa] M. Bertolini, H. Darmon, Nontriviality of families of Heegner points and ranks of Selmer groups over anticyclotomic towers, *Jour. Ramanujan Math. Soc.* **13** (1998), 15–24.

[C-W] J. Coates, A. Wiles, On the conjecture of Birch and Swinnerton-Dyer, *Invent. Math.* **39** (1977), 223–251.

[Cre] J. E. Cremona, Algorithms for Modular Elliptic Curves, Cambridge University Press (1992).

[Gre1] R. Greenberg, On the Birch and Swinnerton-Dyer Conjecture, *Invent. Math.* **72** (1983), 241–265.

[Gre2] R. Greenberg, Iwasawa theory for elliptic curves, in *Lecture Notes in Math.*, Vol. 1716.

[Ha] M. Harris, Systemic growth of Mordell-Weil groups of abelian varieties in towers of number fields, *Invent. Math.* **51** (1979), 123–141.

[Ho] L. Howe, Twisted Hasse-Weil L-functions and the result of Mordell-Weil groups, *Canadian J. Math.* **49** (1997), 749–771.

[Iw] K. Iwasawa, On $\mathbb{Z}_l$-extensions of algebraic number fields, *Ann. of Math.* **98** (1973), 246–326.

[Ku] P. F. Kurcanov, Elliptic curves of infinite rank over Γ-extensions, *Mat. Sbornik* **90** (1973), 320–329.

[Ma1] B. Mazur, Rational points of abelian varieties with values in towers of number fields, *Invent. Math.* **18** (1972), 183–266.

[Ma2] B. Mazur, Modular curves and arithmetic, *Proceedings of the International Congress of Mathematicians*, Warsaw, 1983, 185–211.

[Ri] K. Ribet, Torsion points of abelian varieties in cyclotomic extensions, *Enseign. Math.* **27** (1981), 315–319.

[Ro1] D. Rohrlich, On L-functions of elliptic curves and cyclotomic towers, *Invent. Math.* **75** (1984), 404–423.

[Ro2] D. Rohrlich, On L-functions of elliptic curves and anticyclotomic towers, *Invent. Math.* **75** (1984), 383–408.

[Ro3] D. Rohrlich, L-functions and division towers, *Math. Ann.* **281** (1988), 611–632.

[Ro4] D. Rohrlich, D. Rohrlich, Galois theory, elliptic curves, and root numbers, *Comp. Math.* **100** (1996), 311–349.

[Ro5] D. Rohrlich, Realization of some Galois representations of low degree in Mordell-Weil groups, *Math. Research Letters* **4** (1997), 123–30.

[Si1] J. Silverman, The Arithmetic of Elliptic Curves, *Graduate Texts in Math.* **106**, Springer-Verlag 1986.

[Si2] J. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, *Graduate Texts in Math.* **151**, Springer-Verlag 1994.