Aprameyo Pal

Mazur's Control Theorem for Elliptic Curves

Thesis Advisor: Jean Robert Belliard

Introduction

In this thesis we discuss some of the ideas related to Iwasawa theory of Elliptic Curves. Starting in the late 1950's Iwasawa proved a number of results and formulated some important conjectures concerning the behaviour of ideal class groups in the tower of subfields of a $\mathbb{Z}_p$-extension (See [8] , [16]). Inspired by Iwasawa's idea, Mazur formulated an analogous theory in 1960's and 1970's which is mostly contained in [12]. Around the same time Manin wrote an article [11] in which he simplified some of Mazur's ideas using Galois cohomology. All along one of the main motivation was to study a new approach to study the behaviour of Mordeil-Weil group of Elliptic curves (More generally Abelian Varieties) and the Birch-Swinnerton dyer conjecture.

One of the central theorems proven in Mazur's article [12] is his control theorem, which asserts that the Selmer group for an abelian variety behaves well Galois theoretically in a $\mathbb{Z}_p$-extension for any prime p where the abelian variety has good, ordinary reduction. This theorem has various corollaries including the Conjecture 4.2. In this thesis we follow Greenberg's idea [6] which is different from Manin's article [11] and Mazur [12]. Here we use the explicit structure theoretic-classification of the Iwasawa modules i.e $\Lambda = \mathbb{Z}_p[[T]]$ modules. We restrict ourselves to the case of Elliptic Curves with good, ordinary reduction at p. Although almost all the arguments will work for Abelian varieties. But for the other type of reductions like multiplicative and supersingular, we would have needed more arguments.

Section 1 and Section 2 recalls some basic results from Structure of Iwasawa algebras and in the end of Section 2, the main classification theorem is proved. In Section 3, we define Selmer group and Tate-Safarevich group and we give a description of the p-primary part of the selmer group for E over finite extensions of $\mathbb{Q}$ and (for some certain infinite extensions) in terms of the galois cohomology for the group $E[p^\infty]$, the p-torsion points on E.

In section 4, we mention some important Λ-modules and some important conjectures about the structure of those modules. Then we prove some special case of Corank lemma which was used in Section 3 using Iwasawa theory. Finally in Section 5, we prove Mazur's control theorem for Elliptic curves with good, ordinary reduction at p, which we state now:

Mazur's Control Theorem:
Let F be a finite extension of $\mathbb{Q}$ and E an elliptic curve over F. Assume p is a prime and E has good, ordinary reduction over all primes lying over p. Assume that $F_\infty = \bigcup_n F_n$ is a $\mathbb{Z}_p$-extension of F. Then the natural maps

$$Sel_E(F_n)_p \to Sel_E(F_\infty)_p^{Gal(F_\infty/F_n)}$$

have finite kernels and cokernels of bounded orders as $n \to \infty$

Here F_n denotes the unique subfield of F_∞ containing F such that ($[F_n : F] = p^n$) and $Sel_E(F_n)_p$ denotes the set of F_n-rational points of the p-Selmer group defined in Section 3.

In Appendix 1, we list some important results from Galois Cohomology which is extensively used in the text and give a full proof of Corank lemma. In appendix 2, we recall some important properties from Elliptic curves including Formal groups.

1 Group rings and power series

Let $\mathcal{O}$ be the ring of integral elements in $\mathbb{Q}_p$. Like for example for a Dirichlet character χ, $\mathcal{O} = \mathcal{O}_\chi = \mathbb{Z}_p[\chi(1), \chi(2), ...]$. Let $\mathfrak{p}$ be the maximal ideal of $\mathcal{O}$, since $\mathcal{O}$ is a local ring. Let π be a generator of $\mathfrak{p}$, so $(\pi) = \mathfrak{p}$.

Let $\mathbb{Z}_p$ be the p-adic group of integers and Γ be a multiplicative topological group isomorphic to $\mathbb{Z}_p$. Now $\mathbb{Z}$ is dense in $\mathbb{Z}_p$ and 1 generates $\mathbb{Z}$. So if γ correponds to 1 under the isomorphism then the cyclic subgroup generated by γ is dense inside Γ. Since the closed subgroups of $\mathbb{Z}_p$ are of the form $p^n\mathbb{Z}_p$, the closed subgroups of Γ are of the form Γ^{p^n}. Then $\Gamma_n = \Gamma/\Gamma^{p^n}$ is a cyclic group of order p^n generated by the coset of γ.

Consider the group ring $\mathcal{O}[\Gamma_n]$. Clearly there is a surjection from

$$\mathcal{O}[T] \to \mathcal{O}[\Gamma_n].$$

$$T \longmapsto \gamma - 1$$

Now clearly $((1+T)^{p^n} - 1) \subseteq$ kernel. We get the other way inclusion by using the rank equality. So we get:

$$\mathcal{O}[\Gamma_n] \simeq \mathcal{O}[T]/((1+T)^{p^n} - 1)$$

If $m \geq n \geq 0$ there is a natural map $\phi_{m,n} : \mathcal{O}[\Gamma_m] \to \mathcal{O}[\Gamma_n]$induced by the map $\Gamma_m \to \Gamma_n$. As $((1+T)^{p^n} - 1)$ divides $((1+T)^{p^m} - 1)$ if $m \geq n \geq 0$ we get a natural map of the polynomial rings corresponing to $\phi_{m,n}$. In fact we get one inverse system. So taking the inverse limit of the group rings $\mathcal{O}[\Gamma_n]$ with respect to $\phi_{m,n}$ we get the profinite group ring $\mathcal{O}[[\Gamma]]$.
As an element $\alpha \in \mathcal{O}[\Gamma]$ gives a sequence α_n such that $\phi_{m,n}(\alpha_m) = \alpha_n$ so $\mathcal{O}[\Gamma] \subseteq \mathcal{O}[[\Gamma]]$.
But $\mathcal{O}[[\Gamma]]$ contains more elements. So to get a better idea about the elemnets insides $\mathcal{O}[[\Gamma]]$ we look at the polynomial rings.
Now since $\mathcal{O}[\Gamma_n] \simeq \mathcal{O}[T]/((1+T)^{p^n} - 1)$, we have

$$\mathcal{O}[[\Gamma]] \simeq \varprojlim \mathcal{O}[T]/((1+T)^{p^n} - 1).$$

Our aim will be to prove the following theorem

Theorem 1.1 $\mathcal{O}[[\Gamma]] \simeq \mathcal{O}[[T]]$ *the isomorphism induced by* $\gamma \longmapsto 1 + T$.

For proving this theorem we will prove that

$$\mathcal{O}[[T]] \simeq \lim_{\leftarrow} \mathcal{O}[T]/((1+T)^{p^n}-1)$$

So initially we will study some properties of the power series ring $\mathcal{O}[[T]]$

Proposition 1.2 *Let $f,\ g \in \mathcal{O}[[T]]$ and assume $f = a_0 + a_1T + ...$,with $a_i \in p$ for $0 \leq i \leq n-1$, but $a_n \in \mathcal{O}^*$.Then we can uniquely write*

$$g = qf + r$$

where $q \in \mathcal{O}[[T]]$ and where $r \in \mathcal{O}[T]$ is a polynomial of degree atmost n-1.

Proof. Let α and τ be the projections on the beginning and tail end of the power series, given by

$$\alpha : \sum_{k=0}^{\infty} a_k T^k \to \sum_{k=0}^{n-1} a_k T^k$$

$$\tau : \sum_{k=0}^{\infty} a_k T^k \to \sum_{k=n}^{\infty} a_k T^{k-n}$$

Now we have two very important properties of τ
i) $\tau(hT^n) = h$ for any $h \in \mathcal{O}[[T]]$
ii) $\tau(h) = 0 \iff h$ is a polynomial of degree $\leq n-1$
So by property ii) our claim is equivalent to prove that $\tau(g) = \tau(qf)$.
Now taking f with the assumptions we can write f as following:

$$f = \alpha(f) + \tau(f)T^n$$

So

$$qf = q\alpha(f) + q\tau(f)T^n$$

Hence our problem reduces to solve the equation

$$\tau(g) = \tau(q\alpha(f)) + \tau((q\tau(f)T^n)$$

Using property *i)* which reduces to

$$\tau(g) = \tau(q\alpha(f)) + q\tau(f) \tag{1}$$

Now $\tau(f)$ is invertible in $\mathcal{O}[[T]]$ as the constant term is a_n which is a unit in $\mathcal{O}[[T]]$.
Putting $Z = q\tau(f)$, we get the equivalent to a)

$$\tau(g) = \tau\Big(Z\frac{\alpha(f)}{\tau(f)}\Big)+Z = \Big(I + \tau \circ \frac{\alpha(f)}{\tau(f)}\ \Big)Z$$

The only unknown in the equation is Z , so to find Z we have to invert $I + \tau \circ \frac{\alpha(f)}{\tau(f)}$.
Note that

$$\tau \circ \frac{\alpha(f)}{\tau(f)} : \mathcal{O}[[T]] \to \mathfrak{p}\mathcal{O}[[T]]$$

as $\frac{\alpha(f)}{\tau(f)} \in \mathfrak{p}\mathcal{O}[[T]]$. So by taking suitable norm, we can prove that $I + \tau \circ \frac{\alpha(f)}{\tau(f)}$ is a invertible operator. In fact explicitly it is easy to see that $Z = \sum_{k=0}^{\infty}(-1)^k\pi^k(\tau(\alpha(f)/(\pi\tau(f))))(\tau(g))$ is the inverse. So we get both the existence and uniqueness, which finishes the proof.

■

Definition 1.3 *$P(T) \in \mathcal{O}[T]$ is called distinguished if $P(T) = T^n + a_{n-1}T^{n-1} + ... + a_0$ with $a_i \in p$ for $0 \leq i \leq n-1$*

Theorem 1.4 *(p-adic Weierstrass Preparation Theorem)*
Let

$$f(T) = \sum_{k=0}^{\infty} a_k T^k \in \mathcal{O}[T]$$

and assume for some n we have $a_i \in \mathfrak{p}$ for $0 \leq i \leq n-1$, but $a_n \in \mathcal{O}^*$ Then f may be uniquely written in the form $f(T) = P(T)U(T)$, where $U(T) \in \mathcal{O}[[T]]$ is a unit and $P(T)$ is a distinguished polynomial of degree n.

More genereally , if $f(T)$ is nonzero then we may write uniquely

$$f(T) = \pi^{\mu}P(T)U(T)$$

with P and u as above and $\mu \in \mathbb{Z}_{\geq 0}$

Proof. If we just factor as large a power of π as possible from the coefficients of $f(T)$ then the second part follows easily from the first part.
Now for proving the first part let us take $g(T) = T^n$ in propositinon 1.2, then

$$T^n = q(T)f(T) + r(T),$$

with $\deg r \leq n-1$
Since $q(T)f(T) \equiv q(T)(a_nT^n$+higher terms $)(\text{mod } \pi)$, we must have $r(T) \equiv 0(\text{mod}\pi)$

Therefore $P(T) = T^n - r(T)$ is a distinguished polynomial of degree n. Let q_i be the coefficients of the polynomial $q(T)$ then comparing the coefficients of T^n in $f(T)q(T) = T^N - r(T)$ we get

$$a_0 q_n + a_1 q_{n-1} + ... + a_n q_o = 1$$

So,we get $a_n q_0 \equiv 1(\text{mod}\pi)$. Therefore $q_0 \in \mathcal{O}^*$ so $q(T)$ is a unit. Let$U(T) = 1/q(T)$ then $f(T) = P(T)U(T)$ as desired. Now every distinguised polynomial of degree n can be written in the form $P(T) = T^n - r(T)$ so we may transform back the equaton $f(T) = P(T)U(T)$ to

$$T^n = U(T)^{-1} f(T) + r(T)$$

then the uniqueness statement of the proposition 1.2 implies the uniqueness of P and U.

■

Corollary 1.5 *Let $f(T) \in \mathcal{O}[[T]]$ be nonzero. Then there are only finitely many $x \in \mathbb{C}_\text{ı}, |x| \leq 1$ with f(x) = 0*

Proof. Let $f(x) = 0$. Then from Theorem 1.4, $f(T) = \pi^\mu P(T)U(T)$. Since $U(T)$ is invertible, $U(x) \neq 0$. So we get $P(x) = 0$, but as a polynomial it can only have finitely many roots. We get the deired result.

■

Corollary 1.6 *Let P(T)$\in \mathcal{O}[T]$ be a distinguished polynomial and let $g(T) \in \mathcal{O}[T]$ be arbitrary. Then if $g(T)/P(T) \in \mathcal{O}[[T]]$ then $g(T)/P(T) \in \mathcal{O}[T]$.*

Proof. Let $g(T) = f(T)P(T)$ for some $f(T) \in \mathcal{O}[[T]]$. Let $x \in \mathbb{C}_p$ be a zero of $P(T)$. Then

$$0 = P(x) = x^n + (\text{multiple of } \pi)$$

So by p-adic valuation $|x| \leq 1$ hence $f(x)$ will converge so $g(x) = 0$. Now we can divide both $g(T)$ and $P(T)$ by $(T - x)$ and working in a larger ring if necessary, continuing this process we find that $P(T)$ divides $g(T)$ as polynomials .

■

Now we return to the proof of the main theorem. We have to prove that

$$\mathcal{O}\left[[T]\right] \simeq \lim_{\leftarrow} \mathcal{O}\left[T\right]/((1+T)^{p^n}-1)$$

First of all, $P_n(T) = (1+T)^{p^n} - 1$ is a distinguished polynomial. The ideal $(\pi, T) \supseteq (p, T)$ is a maximal ideal of $\mathcal{O}[T]$ and also gives the maximal ideal of $\mathcal{O}[[T]]$. Now,

$$P_{n+1}(T)/P_n(T) = (1+T)^{p^n(p-1)} + (1+T)^{p^n(p-2)} + \ldots\ldots\ldots + 1 \subseteq (p, T)$$

as clearly $P_0(T) \subseteq (p, T)$ by induction we have $P_n(T) \subseteq (p, T)^{n+1}$
By proposition 1.2 we have a natural map from $\mathcal{O}[[T]] \to \mathcal{O}[T] mod P_n(T)$ for each n given by $f(T) \to f_n(T)$ where $f(T) = q_n(T)p_n(T) + f_n(T)$ and $deg f_n \leq p^n$
Now if we have $m \geq n \geq 0$, then

$$f_m(T) - f_n(T) = (q_n - P_m q_m / P_n)P_n$$

By corollary 1.6, we have $f_m \equiv f_n (mod P_n)$ as polynomials so

$$(f_0, f_1, \ldots\ldots) \in \lim_{\leftarrow} \mathcal{O}\left[T\right]/P_n(T)$$

sowe get a map from the power series ring to the inverse limit. Now if $f_n = 0$ for every n then P_n divides f for all n. So $f \in \bigcap_{n=o}^{\infty}(p, T)^{n+1}$ which is zero so the map is injective.
Now for surjection let us pick any $(f_0, f_1, \ldots\ldots)$ is in the inverse limit, so for $m \geq n \geq 0, f_m \equiv f_n (mod P_n)$ therefore $(mod(p, T)^{n+1})$ then the coefficients of the terms form Cauchy sequence with respect to the (p, T)-adic topology for which $\mathcal{O}[[T]]$ is compact. So $\lim f_n$ exists. Let $\lim f_n = f$
But letting $m \to \infty$

$$q_{m,n} = (f_m - f_n)/P_n \to (f - f_n)/P_n$$

As $q_{m,n} \in \mathcal{O}[T]$ then the limit must be in $\mathcal{O}[[T]]$.Therefore

$$f = (P_n)(\lim_m q_{m,n}) + f_n$$

So we have $f \mapsto (f_0, f_1, \ldots\ldots)$ and that gives the surjection of the map.

■

2 The structure of Λ-Modules

In this section we will classify all Λ modules using the tools developed in the previous chapter.

Lemma 2.1 *$\Lambda = \mathbb{Z}_p[[T]]$ is a Unique Factorizaton Domain.*

Proof. By the p-adic Weistrass theorem, if $f(T) \in \Lambda$ is nonzero, then we may write uniquely

$$f(T) = p^{\mu} P(T) U(T)$$

with $\mu \geq 0$, $P(T)$ distinguished and $U(T) \in \Lambda^*$. Also if know f is a polynomial then so is U. There is a divison algorithm for distinguished polynomials: if $f(T) \in \Lambda$ and $P(T)$ is distinguished then (uniquely)

$$f(T) = q(T)P(T) + r(T)$$

with $r(T) \in \mathbb{Z}_p[T]$, deg $r(T) <$ deg $P(T)$ (We take deg $0 = -\infty$). From the above discussion it follows that the irreducible elements of Λ are p and the irreducible distinguished polynomials. Therefore Λ is a unique factorization domain.

■

Lemma 2.2 *Suppose $f, g \in \Lambda$ are relatively prime then the ideal (f, g) has finite index in Λ*

Proof. Let $h \in (f, g)$ be a polynomial of minimal degree. By Lemma 2.1 we may assume that, $h = p^s H$ with $H = 1$ or H is distinguished. Suppose $H \neq 1$. As f and g are relatively prime we may assume that H does not divide f. Now using the divison algorithm

$$f = Hq + r,$$

with deg $r <$ deg $H =$ deg h

so, $p^s f = hq + p^s r$. But deg $(p^s r) <$ deg h and $p^s r \in (f, g)$ we have a contradiction by our assumption on minimality of h. So we have $H = 1$ and $h = p^s$. Now interchanging g and f or dividing by unit we may assume that f is not divisible by p and distinguished. So we have,

$$(f, g) \supseteq (p^s, f)$$

By divison algorithm any element of Λ is congruent mod f to a polynomial of degree less than deg$f$. Since there are only finitely many such polynomials mod p^s, (p^s, f) has finite index.
Now there is a canonical surjection $\Lambda/(p^s, f) \to \Lambda/(f, g)$, hence $\Lambda/(f, g)$ is finite. ■

Lemma 2.3 *Suppose f,$g \in \Lambda$ are relatively prime*
1) the natural map

$$\Lambda/(fg) \xrightarrow{\phi} \Lambda/(f) \bigoplus \Lambda/(g)$$

is an injection with finite cokernel
2)there is an injection

$$\Lambda/(f) \bigoplus \Lambda/(g) \longrightarrow \Lambda/(fg)$$

with finite cokernel.

Proof. 1) The canonical map is $a(\text{mod } fg) \rightarrow (a \text{ mod } f, a \text{ mod } g)$. So if $f \mid a$ and $g \mid a$ then as Λ is a UFD and f,g are relatively prime, we get $fg \mid a$. So that this map is an injection.

Now our claim is $im(\phi) = \{(a \text{ mod } f, b \text{ mod } g) : a - b \in (f, g)\}$

Clearly if $(a \text{ mod } f, b \text{ mod } g) \in im(\phi)$ then $\exists c$ such that $c \equiv a \text{ mod } f, c \equiv b \text{ mod } g$, and hence $a - b \in (f, g)$.

Conversely, consider $(a \text{ mod } f, b \text{ mod } g)$. If $a - b \in (f, g)$ then $a - b = fA + gB$ for some A, B in Λ. Let

$$c = a - fA = b + gB.$$

then

$$c \equiv a \text{ mod } f, c \equiv b \text{ mod } g,$$

So (a, b) is in the image and the claim is proved.

Hence any element of cokernel can be written as $(0 \text{ mod } f, r + s \text{ mod } g)$ where $r \in \Lambda, s \in (f, g)$.
From the previous lemma $\Lambda/(f, g)$ is finite. Let $r_1, r_2, ...r_n \in \Lambda$ are the representatives for $\Lambda/(f, g)$, it follows that

$$[(0 \text{ mod } f, r_j \text{ mod } g) \mid 1 \leq j \leq n]$$

is a set of representatives for the cokernel of this map. So the cokernel is finite.

2) from part 1) we have

$$\Lambda/(fg) \simeq M \subseteq \Lambda/(f) \bigoplus \Lambda/(g) := N$$

with M of finite index in N. Let P be any distinguished polynomial in Λ relatively prime to fg. Let $(x, y) \in N$

$$\text{then } (P^i)(x,y) \equiv (P^j)(x,y) \bmod M$$

for some i less than j. Since $1 - P^{j-i} \in \Lambda^*$
we have

$$P^i(x,y) \in M$$

so we get $P^k \in N \subseteq M$for some k. Hence there is a map

$$N \to M \simeq \Lambda/(fg)$$

by multiplication by P^k . Let $P^k(x,y) = 0$ in M but $M \subseteq N$ so we can think $P^k(x,y) = 0$ in N then $f \mid P^k x, g \mid P^k y$. but we have gcd $(P, fg) = 1$ so $f \mid x$ and $g \mid y$ so $(x,y) = 0$ in N therefore the map is injective.

The image contains the ideal (P^k, fg) which has finite index by lemma 2. Now $p^k\Lambda/(fg\Lambda) \subseteq \Lambda/(fg\Lambda)$. Hence there is a surjection $\Lambda/(fg, p^k) \twoheadrightarrow$ *cokernel* which proves that the cokernel is finite.

■

Lemma 2.4 *The prime ideals of* Λ *are 0,*(p,T)*,* (p) *and the ideals* $(P(T))$ *where* $P(T)$ *is irreducible and distinguished. The ideal* (p,T) *is the unique maximum ideal of* Λ*.*

Proof. Clearly the ideals listed above are prime ideals. Let $\wp \neq 0$ be prime.Let $h \in \wp$ be a polynomial of minimal degree. We can choose h such that $h = p^s H$ with $H = 1$ or H distinguished. Since $\wp$ is prime $p \in \wp$ or $H \in \wp$. So if $H \neq 1 \in \wp$ then H must be irreducible by the minimality of its choice. So we get $(f) \subseteq \wp$ where $f = p$ or f is irreducible and distinguished. Let us assume that $(f) \neq \wp$ otherwise it is already in the list. So there exists $g \in \wp$ such that $f \nmid g$. So f, g are relatively prime since f is irreducible. Now we have $(f,g) \subseteq \wp$ and from lemma 2.2 the ring $\Lambda/(f,g)$ is finite . So $\wp$ has finite index in Λ. Now $\Lambda/\wp$ is a finite $\mathbb{Z}_p$ module so $p^N \in \wp$ for large N hence $p \in \wp$ since $\wp$ is prime (We will always get this. If $f = p$ then clearly we have this otherwise if f and g are relatively prime then as in the proof of lemma 2.2 we get $p^s \in (f,g) \subseteq \wp$). Also $T^i \equiv T^j \bmod \wp$ for some i less than j.But $1 - T^{j-1} \in \Lambda^*$ so $T^i \in \wp$ therefore $T \in \wp$ so $(p,T) \subseteq \wp$ but $\Lambda/(p,T) \simeq \mathbb{Z}/p\mathbb{Z}$ so (p,T) is maximal and $\wp = (p,T)$, since all the prime ideals are contained in (p,T) this is the only maximal ideal.

■

Lemma 2.5 *Let* $f \in \Lambda$ *with* $f \in \Lambda - \Lambda^*$ *Then* $\Lambda/(f)$ *is infinite.*

Proof. Assuming $f \neq 0$ it suffices to prove it for $f = p$ or f distinguished. If f is distinguished then by Division algorithm all polynomials of degree less than f (which is clearly infinite) provide a system of representatives of $\Lambda/(f)$. And if $f = p$ then $\Lambda/(f) = \mathbb{F}_p[[T]]$ which again is infinite.

■

Lemma 2.6 *Λ is a noetherian ring.*

Since the generators of an ideal can be be thought of polynomials then by Hilbert Basis Theorem Λ is noetherian

■

Definition 2.7 *Two $\Lambda-$ modules M and $M^{'}$ are said to be pseudo - isomorphic ($M \sim M^{'}$) if there is a homomorphism $M \to M^{'}$ with finite kernel and co-kernel. In other words there is an exact sequence of Λ modules*

$$0 \to A \to M \to M^{'} \to B \to 0$$

with A and B finite Λ modules

Warning ($M \sim M^{'}$)does not necessarily imply ($M^{'} \sim M$)

Now we want to study the structure of finitely generated Λ modules. Inspired by the classification of finitely generated modules over principal ideal domain, we get the following classification upto pseudo-isomorphism .

Theorem 2.8 *Let M be a finitely generated Λ module. Then*

$$M \sim \Lambda^r \oplus (\bigoplus_{i=1}^{s} \Lambda/(p^{n_i})) \oplus (\bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{m_j}))$$

where $r, s, t, n_i, m_j \in \mathbb{N}$ and f_j is distinguished and irreducible.

We will follow the same line of proof as in the case of PID theorem i.e. via admissible row and column operations. But here we have pseudo-isomorphism. So we will increase our list of admissible operations.

Suppose M has generators $u_1, u_2, u_3, ..., u_n$ with elementary relations

$$\lambda_{1,i}u_1 + \lambda_{2,i}u_2 + ... + \lambda_{n,i}u_n = 0, \lambda_{i,j} \in \Lambda$$

Now the relations are finitely generated since they form a submodule of Λ^n and Λ is noetherian. So we can represent the module M by a matrix whose rows are of the form $(\lambda_{1,i}, ..., \lambda_{n,i})$ where $\sum_1^n \lambda_i u_i = 0$ is a relation of M. Let us denote R this matrix.

In other words as M is finitely generated with the generators say u_1, u_2, $u_3, ..., u_n$ then we have a canonical surjection φ:$\Lambda^n \to M$ just sending $e_i \to u_i$. So we have $\Lambda^n/\ker\varphi \simeq M$. Now $\ker\varphi$ is the module of relations and it is finitely generated, say the generators are $r_1, r_2, r_3, ..., r_m$. Hence there is a canonical surjection f:$\Lambda^m \to \Lambda^n$ such that image$f$ =$\ker\varphi$ and image$f$ is given by a matrix R . So image$f$ $= A\Lambda^m$. Therefore $\Lambda^n/R\Lambda^m = \Lambda^n/\ker\varphi = M$. This matrix R is the presentation matrix of M and M is said to be represented by R.

Now we will review the basic admissible row and column operations.
Operation A. Rows or columns of R can be permuted
Operation B. A multiple of row or column) can be added to another row or column
Operation C. Rows or columns can be multiplied by units in Λ

Now we will see three more operations which arise from pseudo-isomorphism.

Operation 1 *If R contains a row $(\lambda_1, p\lambda_2...., p\lambda_n)$ with $p \nmid \lambda_1$ then R can be changed to matrix R' whose first row is $(\lambda_1, ..., \lambda_n)$ and the remaining rows are rows of R with the first element multiplied by p.*

$$\begin{pmatrix} \lambda_1 & p\lambda_2 & \cdots \\ \alpha_1 & \alpha_2 & \cdots \\ \beta_1 & \beta_2 & \cdots \end{pmatrix} \to \begin{pmatrix} \lambda_1 & \lambda_2 & \cdots \\ p\alpha_1 & \alpha_2 & \cdots \\ p\beta_1 & \beta_2 & \cdots \end{pmatrix}$$

As a special case if $\lambda_2 = ...\lambda_n = 0$ then we may multiply $\alpha_1, \beta_1, ...$ by an arbitrary power of p

Proof. By assumption on R we have the relation

$$\lambda_1 u_1 + p(\lambda_2 u_2 + ... + \lambda_n u_n) = 0$$

Let $M' = M \oplus v\Lambda$ with a new generator v modulo the additional relations

$$(-u_1, pv) = 0, (\lambda_2 u_2 + \lambda_3 u_3 + ... + \lambda_n u_n, \lambda_1 v) = 0$$

now we have a natural map $M \to M^{'}$ by $m \to (m, 0)$. Supose $m \to 0$ then m lies in the module generated by relations , so

$$(m, 0) = a(-u_1, pv) + b(\lambda_2 u_2 + \lambda_3 u_3 + ... + \lambda_n u_n, \lambda_1 v)$$

with $a, b \in \Lambda$.
Equating both sides, we get $ap = -b\lambda_1$ but by assumption $p \nmid \lambda_1$ so $p \mid b$ and $\lambda_1 \mid a$. In the other component, we get

$$\begin{aligned} m &= -\frac{a}{\lambda_1}(\lambda_1 u_1) - \frac{a}{\lambda_1} p(\lambda_2 u_2 + \lambda_3 u_3 + ... + \lambda_n u_n) \\ &= \frac{a}{\lambda_1}(0) = 0 \end{aligned} \tag{2}$$

So the canonical map is an injection. Now in $M^{'}$, pv and $\lambda_1 v$ are in the image of M. So the ideal (p, λ_1) will annihilate $M^{'}/M$. So $M^{'}/M$ becomes $\Lambda/(p, \lambda_1)$ module . Now from lemma 2.2 as p and λ_1 are relatively prime, the ring $\Lambda/(p, \lambda_1)$ is finite. $M^{'}$ is also finitely generated so we get $M^{'}/M$ is finite. Hence

$$M \sim M^{'}$$

It remains to prove that $M^{'}$ has the required relation matrix. $M^{'}$ has generators $v, u_2, ...u_n$. Now any relation $\alpha_1 u_1 + ... + \alpha_n u_n = 0$ becomes $p\alpha_1 v + ... + \alpha_n u_n = 0$, as $(-u_1, pv) = 0$. So we get that the first column is multiplied by p. Now from the 2nd relation $(\lambda_2 u_2 + \lambda_3 u_3 + ... + \lambda_n u_n, \lambda_1 v) = 0$ we have $\lambda_1 v + \lambda_2 u_2 + \lambda_3 u_3 + ... + \lambda_n u_n = 0$. So the new module has the desired relation matrix (here we did not consider the redundant row $(p\lambda_1, ..., p\lambda_2)$).

■

Operation 2 *If all elements in the first column of R are divisible by p^k and if there is a row $(p^k\lambda_1, ..., p^k\lambda_n)$ with $p \nmid \lambda_1$,then we may change to the matrix $R^{'}$ which is the same as R except that $(p^k\lambda_1, ..., p^k\lambda_n)$ is replaced by $(\lambda_1, ..., \lambda_n)$. In pictures*

$$\begin{pmatrix} p^k\lambda_1 & p^k\lambda_2 & \cdots \\ p^k\alpha_1 & \alpha_2 & \cdots \end{pmatrix} \to \begin{pmatrix} \lambda_1 & \lambda_2 & \cdots \\ p^k\alpha_1 & \alpha_2 & \cdots \end{pmatrix}$$

Proof. Let $M^{'} = M \oplus v\Lambda$ with a new generator v modulo the additional relations

$$(p^k u_1, -p^k v) = 0, (\lambda_2 u_2 + \lambda_3 u_3 + ... + \lambda_n u_n, \lambda_1 v) = 0$$

As before $p \nmid \lambda_1$ implies that there is a canonical injection $M \to M^{'}$ and $p^k v$ and $\lambda_1 v$ is in the image of M so the ideal (p^k, λ_1) annihilates $M^{'}/M$ so we get by the same argument as before $M^{'}/M$ is finite. So

$$M \sim M^{'}.$$

Here we dont have that $M^{'}$ have the relation matrix $R^{'}$. But from the relation $p^k(u_1 - v) = 0$ and using p^k divides the first coefficient of all the relations involving u_1 we get that $M^{'}$ can be decomposed as

$$M^{'} = M^{''} \oplus \Lambda(u_1 - v)$$

where $M^{''}$ is generated by $v, u_2, ...u_n$ and the relations are generated by $(\lambda_1, ..., \lambda_n)$ and R i.e $R^{'}$.

Now there is a canonical surjection $\Lambda \to \Lambda(u_1 - v)$ which has the kernel generated by p^k (As $p^k(u_1 - v) = 0$). So we have

$$\Lambda(u_1 - v) = \Lambda/(p^k)$$

Hence we get

$$M \sim M^{''} \oplus \Lambda/(p^k).$$

In Theorem 2.8, we have the terms like $\Lambda/(p^k)$ upto pseudo-isomorphism. So we have already proceeded towards the classification and can continue the classification ignoring this term. Therefore after elementary operations we can deal with $M^{''}$.

■

Operation 3 *If R contains a row $(p^k\lambda_1, ..., p^k\lambda_n)$ and for some λ with $p \nmid \lambda$, $(\lambda\lambda_1, ..., \lambda\lambda_n)$ is also a relation (not necessarily contained in R i.e not necessarily elementary relation), then R may be changed to $R^{'}$ where $R^{'}$ is the same as R with $(p^k\lambda_1, ..., p^k\lambda_n)$ replaced by $(\lambda_1, ..., \lambda_n)$.*

Proof. We have a canonical surjection $M \to M^{'}$ where $M^{'} = M/(\lambda_1 u_1 + ...\lambda_n u_n)$. From our assumption the kernel is annihilated by the ideal (λ, p^k). Also kernel is finitely generated as M is finitely generated and the kernel is a module over $\Lambda/(\lambda, p^k)$ which is finite. So the kernel is finite and

$$M \sim M^{'}$$

$M^{'}$ is generated by $v_1, v_2, ...v_n$ where $v_i =$ image of u_i under the map for all $1 \leq i \leq n$. So by definition $M^{'}$ has the relation matrix $R^{'}$. Hence the proof is done.

■

With these admissible operations we return to the proof of the theorem.

Proof of Theorem 2.8 Let $f \neq 0$ and $f \in \Lambda$ then

$$f(T) = p^{\mu} P(T) U(T)$$

with P distinguished and $U \in \Lambda^*$. Let

$$\deg_w f = \text{deg } P(T), \text{ if } \mu = 0 \text{ otherwise} = \infty.$$

This is called Weierstrass degree of f. Now suppose that a matrix R is given then

$$\deg^{(k)}(R) = \text{mindeg}_w(a'_{ij}) \text{ for } i, j \geq k$$

where a'_{ij} ranges over all the relation matrices obtained from R via admissible operations. If the matrix R has the form

$$\begin{pmatrix} \lambda_{11} & \cdots 0 & \cdots & 0 \\ & \ddots & & \\ 0 & \cdots \lambda_{r-1,r-1} & \cdots & 0 \\ * & \cdots * & \cdots & * \\ * & \cdots * & \cdots & * \end{pmatrix} = \begin{pmatrix} D_{r-1} & 0 \\ A & B \end{pmatrix}$$

with λ_{kk} distinguished polynomials and

$$\deg \lambda_{kk} = \deg_w \lambda_{kk} = \deg^{(k)}(R), \text{ for } 1 \leq k \leq r-1$$

then we say that R is in $(r-1)$ normal form.

We will first assume the following claim to be proven later.

Claim. If the submatrix $B \neq 0$ then R may be transformed via admissible operations into R' which is in r normal form and has the same first $(r-1)$ diagonal elements.

So if we start with a relation matrix R and $r = 1$ by the claim we may successively change R to obtain the following form of the matrix

$$\begin{pmatrix} \lambda_{11} & & 0 \\ & \ddots & \\ & & \lambda_{rr} \\ A & & 0 \end{pmatrix}$$

where each λ_{jj} is distinguished and degλ_{jj} =deg$^{(j)}(R)$ for $j \leq r$. So if we can prove that A is zero matrix then we are done. Now by the divison algorithm and operation B we can assume

$$\lambda_{ij} = 0 \text{ or } \deg\lambda_{ij} < \deg \lambda_{jj} \text{ for } i \neq j.$$

Suppose $\lambda_{ij} \neq 0$ for some $i \neq j$. Now since deg $_w\lambda_{jj}$ is minimal, we get $p \mid \lambda_{ij}$ so we have a nonzero realtion $(\lambda_{i1}, ...\lambda_{ir}, 0, 0, ...0)$ which is divisible by p. Let $\lambda = \lambda_{11}.....\lambda_{rr}$ then $p \nmid \lambda$ since λ_{jj}s are distinguished and

$$(\lambda\lambda_{i1}/p, ...\lambda\lambda_{ir}/p, 0, 0, ...0)$$

is also a relation since $\lambda_{jj}u_j = 0$. Now operation 3 gives us that we may assume p does not divide λ_{ij} for some j as we can successively change the row $(\lambda_{i1}, ...\lambda_{ir}, 0, 0, ...0)$ by removing the p. so,

$$\deg\ _w\lambda_{jj} \leq \deg\ \lambda_{ij} < \deg\ \lambda_{jj} = \deg\ ^{(j)}(R).$$

This is impossible. So we have $\lambda_{ij} = 0$ for all $i \neq j$ which implies $A = 0$. This in terms of Λ modules imply that we have

$$M \sim \Lambda/(\lambda_{11}) \oplus ..... \oplus \Lambda/(\lambda_{rr}) \oplus \Lambda^{n-r}.$$

We recall that in Operation 2, we ignored elements of the type $\Lambda/(p^k)$. Now we can put back the factors $\Lambda/(p^k)$ and we get

$$M \sim \Lambda/(\lambda_{11} \oplus ..... \oplus \Lambda/(\lambda_{rr}) \oplus \Lambda^{n-r} \oplus (\bigoplus_{i=1}^{s} \Lambda/(p^{n_i})).$$

We can think of λ_{ii} to be irreducible (we get this just decomposing λ_{ii} into irreducibles and then using the lemma 3) which finishes the proof of Theorem 1.

■

Proof of Claim. By the special case of operation 1 we can say that a large power of p divides each λ_{ij} with $i \geq r$ and $j \leq r-1$ i.e $p^N \mid A$ with N large enough such that $p^N \nmid B$. Now using operation 2 we can assume that $p \nmid B$ We may also assume that B contains an entry λ_{ij} such that

$$\deg_w\lambda_{ij} = \deg^{(r)}(R) < \infty.$$

We may assume that λ_{ij} is distinguised (if $\lambda_{ij} = P(T)U(T)$ then by we can multiply λ_{ij} by U^{-1}). Now the first $(r-1)$ rows have zero in the jth column so they do not change. Again using the zeros and operation A we get $\lambda_{ij} = \lambda_{rr}$.
Now by divison algorithm and operation B we can assume that λ_{rj} is such that

$$\deg \lambda_{rj} < \deg \lambda_{rr},\ j \neq r,$$

and

$$\deg\lambda_{rj} < \deg \lambda_{jj},\ j < r.$$

No from definition of $(r-1)$ normal form λ_{rr} has minimal Weierstrass degree in B so we must have $p \mid \lambda_{rj}$ for $j > r$. Again by operation 1 we can assume that $p^N \mid \lambda_{rj}$ for $j < r$.
Let $\lambda_{rj} \neq 0$ for some $j > r$. By operation 1 we can assume there is some j with $p \nmid \lambda_{rj}$ then

$$\deg_w \lambda_{rj} = \deg \lambda_{rj} < \deg \lambda_{rr} = \deg {}_w\lambda_{rr}$$

which is impossible. So $\lambda_{rj} = 0$ for $j > r$.
Let $\lambda_{rj} \neq 0$ for some $j < r$.By operation 1 we can assume that there is some j with $p \nmid \lambda_{rj}$ then

$$\deg_w \lambda_{rj} \leq \deg \lambda_{rj} < \deg \lambda_{jj} = \deg {}_w\lambda_{jj}$$

But deg $\lambda_{jj} = \deg^{(j)}(R)$, which contradicts definition of $\deg^{(j)}(R)$. Therefore $\lambda_{rj} = 0$ for $j < r$. Hence we get $\lambda_{rj} = 0$ for all $j \neq r$ and our claim is proven.

■

3 Selmer groups

Let K be any algebraic extension over $\mathbb{Q}$ and E be an elliptic curve over K. One of the most interesting object associated with E is the Mordell-Weil group of $E(K)$. Mordell-Weil group of $E(K)$ is studied in different ways. We have chosen here the approach via Galois cohomology.
Fix $n \geq 2$. We have a canonical exact sequence

$$0 \to E[n] \to E(\overline{K}) \xrightarrow{n} E(\overline{K}) \to 0.$$

Where $\overline{K}$ denotes the algebraic closure of K and $E[n]$ denotes the n torsion points. So from this we get an exact cohomological sequence

$$E[n]^{G_K} \hookrightarrow E(\overline{K})^{G_K} \to E(\overline{K})^{G_K} \to H^1(G_K, E[n]) \to H^1(G_K, E(\overline{K})) \to \dots$$

where G_K is the absolute galois group $Gal(\overline{K}/K)$.
Now $E(\overline{K})^{G_K} = E(K)$, so we get a canonical injection (which is called Kummer map)

$$E(K)/nE(K) \hookrightarrow H^1(G_K, E[n]) \tag{3}$$

Now If K is a finite extension of $\mathbb{Q}$ then $H^1(G_K, E[n])$ becomes infinite but under Kummer map it can be shown $E(K)/nE(K)$ is contained in a finite subgroup of $H^1(G_K, E[n])$(called n-Selmer group) . So then using theory of heights one can prove the Mordell-Weil theorem

$$E(K) \cong \mathbb{Z}^r \times T, \tag{4}$$

for some $r \geq 0$ and some finite group T. Hence

$$E(K)/nE(K) \cong (\mathbb{Z}/n\mathbb{Z})^r \times T/nT$$

and clearly if one knows n-Selmer group then one can give upper bound to r.
From (4) we get

$$E(K) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z}) \cong (\mathbb{Q}/\mathbb{Z})^r$$

Now $E(K)/nE(K) = E(K) \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z})$, so passing to direct limits we get $E(K) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z})$ and an injection $E(K) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z}) \hookrightarrow H^1(G_K, E(\overline{\mathbb{Q}})_{tors})$. One can show that $E(K) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z})$ is a subgroup of $Sel_E(K)$ and we will get an exact sequence

$$0 \to E(K) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z}) \to Sel_E(K) \to Ш_E(K) \to 0$$

Therefore knowing the structure of $Sel_E(K)$ will give an upper bound on r. We will give two equivalent definitions of $Sel_E(K)$ and describe an alternative

definition for the p-primary subgroup of $Sel_E(K)$ which involves only Galois module $E[p^\infty]$ under the assumption that E has good ordinary reduction at all primes of K lying over p. (for any prime p, $E[p^\infty] = \cup_m E[p^m]$ is the p primary subgroup of $E(\overline{\mathbb{Q}})_{tors}$)).

We adopt two more usual notations for Galois cohomological groups, writing $H^i(L,.)$ in place of $H^i(G_L,.)$ and $H^i(K/L,.)$ in place of $H^i(Gal(K/L),.)$ if K/L is a galois extension.

Definition 3.1 *(First definition)*

Let v runs over all primes of K, archimedean and non-archimedean. 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 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).
Now we have the natural map $K \hookrightarrow K_v$. So we can choose an embedding $\overline{K} \hookrightarrow \overline{K_v}$ (The choice does not matter) and by identifying G_{K_v} with the decomposition group we get G_{K_v} identified with a subgroup of G_K. Now $G_{K_v} \hookrightarrow G_K$ induces $H^1(K, E(\overline{K})) \to H^1(K_v, E(\overline{K}))$ and noting that $E(\overline{K}) \subset E(\overline{K_v})$ induces $H^1(K_v, E(\overline{K})) \to H^1(K_v, E(\overline{K_v}))$ and then composing we get

$$H^1(K, E(\overline{K})) \to H^1(K_v, E(\overline{K_v})).$$

Now we define the Tate- Safarevich group $Ш_E(K)$ by

$$Ш_E(K) = ker\left(H^1(K, E(\overline{K})) \to \prod_v H^1(K_v, E(\overline{K_v}))\right)$$

Now we have the canonical inclusion $E(\overline{K})_{tors} \hookrightarrow E(\overline{K})$ which induces

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

Lemma 3.2 *λ is surjective .*

Proof: coker(λ) is isomorphic to a subgroup of $H^1(K, E(\overline{K})/E(\overline{K})_{tors})$. Now $E(\overline{K})/E(\overline{K})_{tors}$ is a uniquely divisible group, so $H^1(K, E(\overline{K})/E(\overline{K})_{tors})$ is also uniquely divisible group. But we know $H^1(G, E(\overline{K})/E(\overline{K})_{tors})$ is torsion group for every finite group G and passing to the direct limits we get that $H^1(K, E(\overline{K})/E(\overline{K})_{tors})$ is torsion group. (See Appendix 1, Theorem 6.4) So we get $H^1(K, E(\overline{K})/E(\overline{K})_{tors})$ is zero. So coker(λ) is zero proving that λ is surjective.
Now we define Selmer group by

$$Sel_E(K) = \lambda^{-1}(Ш_E(K))$$

Definition 3.3 *(Second definition)*

Let E be an elliptic curve over L then $E(\overline{L})$ is also a divisible group. Then imitating Kummer theory for the multiplicative group $L^\times$, we define Kummer homomorphism:

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

in the following way:
Let $\alpha = P \otimes r \in E(L) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z})$ where $P \in E(L)$ and $r = \frac{m}{n} + \mathbb{Z}$.
Now since $E(\overline{L})$ is divisible we can choose $Q \in E(\overline{L})$ such that $nQ = mP$. Then define a 1-cocycle $\varphi_\alpha : G_L \to E(\overline{L})_{tors}$ by $\varphi_\alpha = g(Q) - Q$ for all $g \in G_L$. First of all φ_α is defined as $g(Q)-Q \in E(\overline{K})_{tors}$ since $n(g(Q)-Q) = g(nQ) - nQ = g(mP) - mP = mg(P) - mP = mP - mP = 0$, since G_L fixes L.
So $[\varphi_\alpha]$ is well-defined and one defines $\kappa(\alpha) = [\varphi_\alpha]$. Now we get the following sequence:
$0 \longrightarrow E(L) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z}) \xrightarrow{\kappa} H^1(L, E(\overline{L})_{tors}) \xrightarrow{\lambda} H^1(L, E(\overline{L})) \longrightarrow 0$

Lemma 3.4 *The above sequence is exact.*

Proof : We already know λ is surjective, so we only have to prove that κ is injective and $im(\kappa) = ker(\lambda)$.

Injectivity of κ : If $\kappa(\alpha) = [\varphi_\alpha] = 0$, which gives φ_α is a 1-coboundary in $Z^1(L, E(\overline{L})_{tors})$, the 1-cocycle elements and $Q \in E(\overline{L})_{tors}$. Then $\exists n_1$ such that $n_1 Q = 0$ which gives $n_1 mP = n_1 nQ = 0$. So we get $P \in E(L)_{tors}$ and $n_1 mP = 0$, but $P \otimes r = P \otimes n_1 mr = n_1 mp \otimes r = 0 \otimes r = 0$ since $r \in \mathbb{Q}/\mathbb{Z}$. So $\alpha = 0$ proving that κ is injective.

Exactnes at $H^1(L, E(\overline{L})_{tors}$: We have defined λ by composing $G_L \to E(\overline{L})_{tors} \hookrightarrow E(\overline{L})$. Now clearly $\lambda \circ \kappa = 0$ since φ_α becomes 1-coboundary in $Z^1(L, E(\overline{L}))$ since $Q \in E(\overline{L})$. So the image κ is included in ker λ.
For the converse, let $[\varphi] \in H^1(L, E(\overline{L})_{tors})$. We have $\lambda([\varphi]) = 0$ which means there exists $Q \in E(\overline{L})$ such that $G_L \xrightarrow{\varphi} E(\overline{L})_{tors}$ is defined by $\varphi(g) = g(Q) - Q$. As $g(Q) - Q \in E(\overline{L})_{tors}$, there exists n such that $n(g(Q) - Q) = 0$. Since $E(\overline{L})$ is divisible we can choose m and $P \in E(\overline{L})$ such that $mnQ = P$. Now $gP - P = g(mnQ) - mnQ = m[n(g(Q) - Q)] = 0$ for all $g \in G_L$. Then if we take $r = \frac{1}{mn} + \mathbb{Z}$ and $\alpha = P \otimes r$ we get $\kappa(\alpha) = [\varphi]$. So image $\kappa \supseteq$ ker λ. ■

Remark: From (3) so we get a canonical injection (which is called Kummer map)

$$E(K)/nE(K) \hookrightarrow H^1(G_K, E[n])$$

and then passing to direct limit we obtain an injection $E(K) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z}) \hookrightarrow H^1(G_K, E(\overline{\mathbb{Q}})_{tors})$. This can be shown easily this map is the map κ described above. So in this way also we can obtain κ is injective.

Now following the same procedure for the completetions $L = K_v$ where v is any prime of K , we get the following commutative diagram where the vertical rows are defined in obvious ways and the rows are exact.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\kappa} & H^1(K, E(\overline{K})_{tors}) & \xrightarrow{\lambda} & H^1(K, E(\overline{K})) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle a_v} & & \downarrow{\scriptstyle b_v} & & \downarrow{\scriptstyle c_v} & & \\ 0 & \longrightarrow & E(K_v) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\kappa_v} & H^1(K_v, E(\overline{K_v})_{tors}) & \xrightarrow{\lambda_v} & H^1(K_v, E(\overline{K_v})) & \longrightarrow & 0 \end{array}$$

Let $[\varphi] \in H^1(K, E(\overline{K})_{tors})$. Now from the first definition of $Sel_E(K)$, $[\varphi] \in Sel_E(K)$ if and only if $c_v \circ \lambda([\varphi]) = 0$ for every prime v of K. But from the commutavity of the diagram $c_v \circ \lambda([\varphi]) = \lambda_v \circ b_v([\varphi])$ and $\mathrm{im}(\kappa_v) = \ker(\lambda_v)$. So we get $c_v \circ \lambda([\varphi]) = 0 \iff b_v([\varphi]) \in \mathrm{im}(\kappa_v)$ for all v. So we get the second definition of Selmer group:

$$Sel_E(K) = ker\Big(H^1(K, E(\overline{K})_{tors}) \to \textstyle\prod_v H^1(K_v, E(\overline{K_v})_{tors})/im(\kappa_v) \Big)$$

That is if $[\varphi] \in H^1(K, E(\overline{K})_{tors})$ then $[\varphi] \in Sel_E(K) \iff [\varphi|_{G_{K_v}}] \in im(\kappa_v)$ for every prime v of K.
Let p be a prime. Now we will follow the same line of argument to obtain the p-primary subgroup of $Sel_E(K)$. The p-primary subgroup of $\mathbb{Q}/\mathbb{Z}$ is isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$. So for any field L, the p-primary subgroup of $E(L) \otimes (\mathbb{Q}/\mathbb{Z})$ can be identified with $E(L) \otimes (\mathbb{Q}_p/\mathbb{Z}_p)$. Suppose κ and κ_v denotes the global and local Kummer maps restricted to the p-primary subgroups. So if K is any algebraic extension of $\mathbb{Q}$ then we get:

$$\kappa : E(K) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \to H^1(K, E[p^\infty])$$

$$\kappa_v : E(K_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \to H^1(K_v, E[p^\infty])$$

So proceeding with this κ and κ_v and imitating the previous argument we get the p-primary subgroup of $Sel_E(K)$ is:

$$Sel_E(K)_p = ker\Big(\ H^1(K, E[p^\infty]) \to \prod_v H^1(K_v, E[p^\infty])/im(\kappa_v) \Big)$$

where v runs over all the primes of K. Now in this definition of $Sel_E(K)_p$ everything except possibly $im(\kappa_v)$ depends on G_{K_v}-module $E[p^\infty]$. We will try to describe $im(\kappa_v)$ involving only the galois module $E[p^\infty]$.

Remark: Since $E(K_v)\otimes(\mathbb{Q}_p/\mathbb{Z}_p)$ is divisible $im(\kappa_v)$ is also divisible. Now we will show that if $v \nmid p$ then $E(K_v)\otimes(\mathbb{Q}_p/\mathbb{Z}_p) = 0$ and so $im(\kappa_v)$ is also zero.

Theorem 3.5 *i) Suppose that E is an elliptic curve defined over $K_v = \mathbb{C}$ or $K_v = \mathbb{R}$. Then $E(K_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$.*

ii) Suppose E is an ellitic curve defined over an algebraic extension K_v of $\mathbb{Q}_l$ where l is a prime , $l \neq p$, then $E(K_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$.
Thus , whenever $v \nmid p$, we have $im(\kappa_v) = 0$.

Proof:i) If $K_v = \mathbb{R}$ then $E(K_v) \cong \mathbb{R}/\mathbb{Z}$ or $\mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Now $\mathbb{R}/\mathbb{Z} \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$. Also if T is any finite group then clearly $T \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$. So we get $E(K_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$. If $K_v = \mathbb{C}$ then $E(K_v) \cong \mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$ and by similar argument we get $E(K_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$.

ii) If K_v is a finite extension of $\mathbb{Q}_l$ where l is a prime and $l \neq p$. Then from (Appendix 2, Theorem 7.4) we get the structure of $E(K_v)$:

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

where T is a finite group. Now $\mathbb{Z}_l$ is p-divisible since $l \neq p$. So $\mathbb{Z}_l \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$ and we have $T \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$ for any finite group T. It follows that $E(K_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$.
Now if K_v is an infinite algebraic extension of $\mathbb{Q}_l$ then $K_v = \bigcup L_v$ where L_v runs over all finite extensions of $\mathbb{Q}_l$ which is contained in K_v. But we have $E(L_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$ for each L_v. So we have $E(K_v) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$ and we are done.

■

Now when $v \mid p$ then K_v is an algebraic extension of $\mathbb{Q}_p$ and the situation becomes more subtle.
Let us assume first that K_v is a finite extension then again from the theorem (Appendix 2, Theorem 7.4) , we get

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

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

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

Assume that E has good, ordinary reduction at v. Thus the reduction of E at v is an elliptic curve $\tilde{E}$ defined over the residue field k_v for v. Now as E has good, ordinary reduction at v we get $\tilde{E}(\overline{k_v})[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$ for every $r \geq 0$. So more precisely, we get

$$\tilde{E}[p^\infty] \cong \varinjlim(\mathbb{Z}/p^r\mathbb{Z}) \cong \mathbb{Q}_p/\mathbb{Z}_p.$$

Now the canonical reduction map $E(\overline{K_v}) \to \tilde{E}(\overline{k_v})$ is G_{K_v} equivariant in the following sense:
G_{K_v} acts naturally on $E(\overline{K_v})$. There is a natural homomorphism $G_{K_v} \to G_{k_v}$ whose kernel is the inertia subgroup I_{K_v} and G_{K_v} acts on $\tilde{E}(\overline{k_v})$ by the above homomorphism with the canonical action of G_{k_v} on $\tilde{E}(\overline{k_v})$.
So restricting we get a natural G_{K_v}-equivariant homomorphism :

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

Now from (Appendix 2,Lemma 7.5) we get that π is surjective and $ker(\pi) \cong \mathbb{Q}_p/\mathbb{Z}_p$.
The action of G_{k_v} on $\tilde{E}[p^\infty]$ is given by a character $\psi : G_{k_v} \to \mathbb{Z}_p^\times$ since $Aut(\mathbb{Q}_p/\mathbb{Z}_p) \cong \mathbb{Z}_p^\times$. But we can extend ψ as a character of G_{K_v} whose kernel contains I_{K_v}. The action of G_{K_v} on $ker(\pi)$ is given by a character $\varphi : G_{K_v} \to \mathbb{Z}_p^\times$ again for same reason. So we get the action ρ_E of G_{K_v} on $E[p^\infty]$is triangular, that is $\rho_E = \begin{pmatrix} \varphi & \star \\ 0 & \psi \end{pmatrix}$. Now 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 from Weil Pairing (See [19], page 95, Section 8) we get that $\det(\rho_E) = \chi$. Hence $\varphi\psi = \chi$.

Let us denote $ker(\pi)$ by $\mathcal{F}[p^\infty]$. The motivation for this notation is clear since this the p-primary part of the formal group $\mathcal{F}(\overline{\mathfrak{m}_v})$ which is explained in more details in (Appendix 2, lemma 7.5). Now we have a natural inclusion : $\mathcal{F}[p^\infty] \hookrightarrow E[p^\infty]$ which induces

$$\varepsilon_v : H^1(K_v, \mathcal{F}[p^\infty]) \to H^1(K_v, E[p^\infty])$$

Now we get the description of $im(\kappa_v)$ from the following theorem.

Theorem 3.6 *Let K_v be a finite extension of $\mathbb{Q}_p$ and assume that E has good, ordinary reduction at v, then $im(\kappa_v) = im(\varepsilon_v)_{div}$.*

Proof: Now we know $im(\kappa_v) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{[K_v:\mathbb{Q}_p]}$. So to prove the theorem it is sufficient to show that $im(\kappa_v) \subseteq im(\varepsilon_v)$ and $im(\varepsilon_v) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{[K_v:\mathbb{Q}_p]} \times T$, where T is a finite group.

Let us prove the first condition $im(\kappa_v) \subseteq im(\varepsilon_v)$:
Consider the exact sequence

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

which induces an exact sequence of cohomology groups :

$$\begin{array}{ccccc} H^0(K_v, E[p^\infty]) & \longrightarrow & H^0(K_v, \tilde{E}[p^\infty]) & \longrightarrow & H^1(K_v, \mathcal{F}[p^\infty]) \\ & & & & \downarrow{\scriptstyle \varepsilon_v} \\ H^2(K_v, \mathcal{F}[p^\infty]) & \longleftarrow & H^1(K_v, \tilde{E}[p^\infty]) & \xleftarrow{\pi_v} & H^1(K_v, E[p^\infty]) \end{array}$$

Now from the diagram we get $im(\varepsilon_v) = ker(\pi_v)$. So if we can show that $\pi_v \circ \kappa_v = 0$ as a map then $im(\kappa_v) \subseteq im(\varepsilon_v)$ will follow.
Let $[\varphi] \in im(\kappa_v)$. Now we have the exact sequence

$$0 \longrightarrow E(L) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z}) \xrightarrow{\kappa_v} H^1(L, E(\overline{L})_{tors}) \xrightarrow{\lambda_v} H^1(L, E(\overline{L})) \longrightarrow 0$$

So $im(\kappa_v) = ker(\lambda_v)$ and then we get $\exists\, Q \in E(\overline{K_v})$ such that $\varphi(g) = g(Q) - Q$ for all $g \in G_{K_v}$. Let $\tilde{Q}$ is the image of Q under the reduction map $E(\overline{K_v}) \to \tilde{E}(\overline{k_v})$. Now, $\pi_v([\varphi]) = [\tilde{\varphi}] \in H^1(K_v, \tilde{E}[p^\infty]$ where $\tilde{\varphi}(g) = g(\tilde{Q}) - \tilde{Q}$ for all $g \in G_{K_v}$. So $\tilde{\varphi}$ is a 1-coboundary for $\tilde{E}(\overline{k_v})$ and then $[\tilde{\varphi}] = 0$ in $H^1(K_v, \tilde{E}(\overline{k_v})$. But $\tilde{E}(\overline{k_v})$ is a torsion group and so its p-primary subgroup $\tilde{E}[p^\infty]$ is a direct summand. So we get $\tilde{E}(\overline{k_v}) \cong \tilde{E}[p^\infty] \oplus E_1$ where E_1 is a subgroup. So we can write $\tilde{Q} = \tilde{Q}_1 + \tilde{Q}_2$ where $\tilde{Q}_1 \in \tilde{E}[p^\infty]$ and $\tilde{Q}_2 \in E_1$. This direct sum is G_{K_v} equivariant so we get $\tilde{\varphi}(g) = g(\tilde{Q}) - \tilde{Q} = (g(\tilde{Q}_1) - \tilde{Q}_1) + (g(\tilde{Q}_2) - \tilde{Q}_2)$. So we get $\tilde{\varphi}(g) : G_{K_v} \to \tilde{E}[p^\infty]$ such that $\tilde{\varphi}(g) = g(\tilde{Q}_1) - \tilde{Q}_1$. So $\tilde{\varphi}$ is a 1-coboundary for $E[p^\infty]$ and $[\tilde{\varphi}] = 0$ in $H^1(K_v, E[p^\infty])$. This proves that $im(\kappa_v) \subseteq im(\varepsilon_v)$.

■

We know already that $im(\kappa_v)$ is divisible so to finish the proof of theorem 2, it is enough to show $[im(\varepsilon_v) : im(\kappa_v)]$ is finite. Now some terminologies will be helpful.

Terminologies:

Let A be any p-primary group. Then we can regard A as $\mathbb{Z}_p$ module. Now if we put discrete topology on A then it can be shown easily that its Pontryagin dual $\widehat{A} = Hom_{cont}(A, \mathbb{Q}_p/\mathbb{Z}_p)$ is a compact $\mathbb{Z}_p$ module. We say A is a cofinitely generated $\mathbb{Z}_p$ module if $\widehat{A}$ is finitely generated as a $\mathbb{Z}_p$ module. We then define $corank_{\mathbb{Z}_p}(A) = rank_{\mathbb{Z}_p}(\widehat{A})$.
So if A is cofinitely generated as a $\mathbb{Z}_p$ module then we get $\widehat{A} \cong \mathbb{Z}_p^r \times T$ for some $r \geq 0$ and some finite group T. So $A \cong \widehat{\widehat{A}} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^r \times \widehat{T}$ and has $\mathbb{Z}_p$-corank r. Then $A_{div} = (\mathbb{Q}_p/\mathbb{Z}_p)^r$(we say that A_{div} is $\mathbb{Z}_p$-cofree) and $[A : A_{div}] < \infty$.

We obtain $im(\kappa_v)$ is $\mathbb{Z}_p$-cofree and has $\mathbb{Z}_p$-corank $[K_v : \mathbb{Q}_p]$. So for proving $[im(\varepsilon_v) : im(\kappa_v)]$ is finite, it is enough to show that $im(\varepsilon_v)$ is $\mathbb{Z}_p$-cofinitely generated and has the same $\mathbb{Z}_p$-corank.

Now $|ker(\varepsilon_v)|$ is bounded above by the order of the finite group $H^0(K_v, \tilde{E}[p^\infty]) = \tilde{E}(k_v)_p$. So it is sufficient to show that $H^1(K_v, \mathcal{F}[p^\infty])$ is $\mathbb{Z}_p$-cofinitely generated and has $\mathbb{Z}_p$-corank $[K_v : \mathbb{Q}_p]$.

Proof of this can be done in two different ways. We will prove here using some theorems of Tate concerning Galois cohomology over local fields and the second proof can be done using standard techniques in Iwasawa theory which will be the topic of whole next chapter.
Suppose A is a discrete G_{K_v} module and $A \cong (\mathbb{Q}_p/\mathbb{Z}_p)^r$ as a $\mathbb{Z}_p$ module. Let us denote Tate twist by $\widehat{A}(1)$ where $\widehat{A}(1) = Hom(A, \mu_{p^\infty})$. Then $\widehat{A}(1)$ is a free $\mathbb{Z}_p$ module of rank r.

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 we have*

$$corank_{\mathbb{Z}_p}(A) = r[K_v : \mathbb{Q}_p] + corank_{\mathbb{Z}_p}(H^0(K_v, A)) + rank_{\mathbb{Z}_p}(H^0(K_v, \widehat{A}(1)))$$

2) Let K_v be a finite extension of $\mathbb{Q}_l$ where $l \neq p$. Then $H^1(K_v, A)$ is $\mathbb{Z}_p$-cofinitely generated and we have

$$corank_{\mathbb{Z}_p}(A) = corank_{\mathbb{Z}_p}(H^0(K_v, A)) + rank_{\mathbb{Z}_p}(H^0(K_v, \widehat{A}(1)))$$

Now we will apply the Corank lemma to $A = \mathcal{F}[p^\infty] \cong \mathbb{Q}_p/\mathbb{Z}_p$ which will finish the proof of Theorem 3.6. We have $r = 1$ and $H^0(K_v, \mathcal{F}[p^\infty])$ is a subgroup of $H^0(K_v, \tilde{E}[p^\infty]) = \tilde{E}(k_v)_p$ which is finite. So $corank_{\mathbb{Z}_p}(H^0(K_v, \mathcal{F}[p^\infty]) = 0$.

Now we want to prove that $rank_{\mathbb{Z}_p}(H^0(K_v, \hat{A}(1)))$ is also zero for $A = \mathcal{F}[p^\infty]$. Our claim is $H^0(K_v, \hat{A}(1)) = 0$ which is equivalent to prove that the action of G_{K_v} on $\hat{A}(1)$ is non-trivial.
Using the notations introduced earlier we have ,
G_{K_v} acts on $A = \mathcal{F}[p^\infty]$ by a character $\varphi : G_{K_v} \to \mathbb{Z}_p^\times$. G_{K_v} acts on $E[p^\infty]$ by a character $\psi = \chi\varphi^{-1} : G_{K_v} \to \mathbb{Z}_p^\times$. G_{K_v} acts on μ_{p^∞} by a character $\chi : G_{K_v} \to \mathbb{Z}_p^\times$
The character ψ which gives the action of G_{K_v} on $E[p^\infty]$ is clearly nontrivial. Since the inertia group I_{K_v} acts trivially but a Frobenius automorphism acts nontrivially. Now $\widehat{A}(1) = Hom(A, \mu_{p^\infty})$ has a natural G_{K_v} action induced by the actions on A and μ_{p^∞}. We have to show that this action is nontrivial. Now the action of G_{K_v} on $\hat{A}(1)$ is given in the following way:
Let $h \in \widehat{A}(1)$ then

$$g.h(a) = g.h(g^{-1}.a) = \chi(g).(h((\varphi(g))^{-1}.a) = \chi(g).(\varphi(g))^{-1}(h(a))$$

$$= \chi\varphi^{-1}(g).(h(a)) = \psi(g).(h(a))$$

but as ψ acts non-trivially so we get action of G_{K_v} on $\hat{A}(1)$ is non-trivial which gives $H^0(K_v, \widehat{A}(1)) = 0$. So from first part of the corank lemma we get that $im(\varepsilon_v)$ has $\mathbb{Z}_p$-corank $[K_v : \mathbb{Q}_p]$. So Theorem 3.6 is proved.

■

Now the Corank Lemma can be proved by using results of Tate concerning Galois Cohomology over local fields. This is done in details in Appendix 1. But we need some results of Tate to have some important information about $[im(\varepsilon_v) : im(\kappa_v)]$, which are listed below:

Proposition 3.7 *Let A be as above then we have. $H^2(K_v, A)$ is the Pontryagin Dual of $H^0(K_v, \hat{A}(1))$ and then*

$$corank_{\mathbb{Z}_p}(H^2(K_v, A) = rank_{\mathbb{Z}_p}(H^0(K_v, \hat{A}(1)))$$

.

Theorem 3.8 *If K_v is a finite extension of $\mathbb{Q}_p$ and if E is an elliptic curve over K_v with good, ordinary reduction at v then $im(\kappa_v)$ has finite index in $im(\varepsilon_v)$ and the quotient $im(\varepsilon_v)/im(\kappa_v)$ is a cyclic group whose order divides $|\tilde{E}(k_v)_p|$, where k_v is the residue field of v. So in particular, if $p \nmid |\tilde{E}(k_v)|$ then $im(\varepsilon_v) = im(\kappa_v)$.*

Proof. Clearly $[im(\varepsilon_v) : im(\kappa_v)]$ is bounded above by $|H^1(K_v, \mathcal{F}[p^\infty])/H^1(K_v, \mathcal{F}[p^\infty])_{div}|$. Now for $m \gg 0$, we have

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

Choosing such m and considering the exact sequence

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

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

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

So we get $im(\varepsilon_v)/im(\kappa_v) \hookrightarrow H^2(K_v, A[p^m])$ and so $[im(\varepsilon_v) : im(\kappa_v)]$ is bounded by $|H^2(K_v, A[p^m])|$ for any sufficiently large m . Now from the above result of Tate, $|H^2(K_v, A[p^m])| = |H^0(K_v, \widehat{A[p^m]}(1))|$.
The Weil pairing $E[p^m] \times E[p^m] \to \mu_{p^m}$ induces another non-degenrate Galois equivariant pairing (See [19], page 95, Section 8)

$$A[p^m] \times \tilde{E}[p^m] \to \mu_{p^m}$$

So we get, $Hom(A[p^m], \mu_{p^m}) \cong \tilde{E}[p^m]$ as G_{K_v} - modules. Then using this we get,

$$H^0(K_v, \widehat{A[p^m]}(1)) = Hom(A[p^m], \mu_{p^\infty})^{G_{K_v}} \cong \tilde{E}(k_v)_p$$

Now $\tilde{E}(k_v)_p$ is a cyclic group so as $im(\varepsilon_v)/im(\kappa_v)$ is a subgroup of $\tilde{E}(k_v)_p$ we get all the statements of our theorem.

■

We will now compare $im(\varepsilon_v)$and $im(\kappa_v)$ for infinite extensions of $\mathbb{Q}_p$ under some restrictions. Let us first define the 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. So we can interpret this as a formal product $\prod l^{a_l}$ over all primes l where $0 \leq a_l \leq \infty$. If l^∞ divides this product that means the power of l dividing $[L : F]$ is unbounded as l varies.

Theorem 3.9 *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 $im(\varepsilon_v) = im(\kappa_v)$. In particular, if K_v is a ramified $\mathbb{Z}_p$ extension of F_v where F_v is a finite extenion of $\mathbb{Q}_p$, this condition is satisfied.*

Proof: By the same argument as in theorem 3.6, we still have $im(\varepsilon_v) \subseteq im(\kappa_v)$. Now to prove $im(\varepsilon_v) = im(\kappa_v)$, it is sufficient to show that $im(\varepsilon_v)$ is divisible group and $im(\varepsilon_v)/im(\kappa_v)$ is finite.
Now to prove that $im(\varepsilon_v)$ is divisible we will use that G_{K_v} has p-cohomological dimension 1 (which follows from the next lemma). Now if $H^1(K_v, \mathcal{F}[p^\infty])$ is divisible then $im(\varepsilon_v)$ is divisible. So it is sufficient to prove that $H^1(K_v, A)$ is divisible whenever A is a divisible p-primary G_{K_v}-module. Now if M is any finite $p-$primary G_{K_v} module, then $H^n(K_v, M) = 0$ for all $n \geq 2$ since G_{K_v} has p-cohomological dimension 1. Now consider the exact sequence:

$$0 \longrightarrow A[p] \longrightarrow A \xrightarrow{p} A \longrightarrow 0.$$

which induces an exact sequence of cohomology groups

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

Now $H^2(K_v, A[p]) = 0$ so $H^1(K_v, A)$ is $p-$divisible. But it is a p-primary group so it is divisible.

Let us write $K_v = \cup_n F_v^{(n)}$ where $F_v^{(n)}$ are the finite extensions of $\mathbb{Q}_p$. we denote $\kappa_v^{(n)}, \varepsilon_v^{(n)}$ the two maps to $H^1(F_v^{(n)}, E[p^\infty])$ that we are considering over $F_v^{(n)}$. 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,

$$im(\varepsilon_v) = \varinjlim_n im(\varepsilon_v^{(n)}), \qquad im(\kappa_v) = \varinjlim_n im(\kappa_v^{(n)})$$

So $im(\varepsilon_v)/im(\kappa_v)$ is finite as it is a direct limit of the finite groups $im(\varepsilon_v^{(n)})/im(\kappa_v^{(n)})$ whose orders are uniformly bounded by $|\tilde{E}(k_v)_p|$ (From Theorem 3.8).

■

Lemma 3.10 *G_{K_v} has p-cohomological dimension 1.*

Proof: Here we only need 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. From this assumption we get that p-primary part of the Brauer group of K_v is zero. Therefore $H^2(K_v, \overline{K_v}^\times)_p = 0$. By applying the same argument on any algebraic extension of K_v we get

$H^2(H, \overline{K_v}^\times) = 0$ for every closed subgroup H of G_{K_v}. Now consider the exact sequence

$$1 \longrightarrow \mu_p \longrightarrow \overline{K_v}^\times \xrightarrow{p} \overline{K_v}^\times \longrightarrow 1$$

which induces an exact sequence of cohomology groups

$$H^1(H, \overline{K_v}^\times) \longrightarrow H^2(H, \mu_p) \longrightarrow H^2(H, \overline{K_v}^\times)$$

for any closed subgroup H of G_{K_v}. Now the first term is zero by Hilbert's theorem 90 and the third term is zero by the above remark. So, $H^2(H, \mu_p) = 0$. Now let H be a Sylow p-subgroup P of G_{K_v}. Then $H^2(P, \mathbb{Z}/p\mathbb{Z}) = 0 \Longrightarrow H^2(P, M) = 0$ for any finite P module of p-power order.(Since then M decomposes as a P module in isomorphic copies of $\mathbb{Z}/p\mathbb{Z}$).
Now we have 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. That sufices to show that G_{K_v} has p-cohomological dimension 1.

■

Remarks: 1) Suppose that E has multiplicative reduction at v and K_v is any algebraic extension of $\mathbb{Q}_p$. Then $im(\varepsilon_v) = im(\kappa_v)$, where

$$\varepsilon_v : H^1(K_v, \mathcal{F}[p^\infty]) \to H^1(K_v, E[p^\infty])$$

which is induced by the inclusion $\mathcal{F}[p^\infty] \hookrightarrow E[p^\infty]$.
This can be proved either adapting the earlier arguments to this case or by using classical Kummer theory for $\overline{K_v}^\times$ together with Tate parametrization.

2) Suppose E has good, supersingular reduction at v, then it is still possible to describe $im(\kappa_v)$ in a way which depends only on the G_{K_v}-module $E[p^\infty]$. This description involves Fontaine's ring B_{cris}, and we have chosen in the present text to avoid this theory.

4 Some important Λ-modules

Our main aim in this section is to prove the corank lemma for $A = \mathbb{Q}_p/\mathbb{Z}_p$. But before that we will see some important Λ-modules which arise in the related context.

1) Let F_∞/F be a $\mathbb{Z}_p$ extension so that $\Gamma = Gal(F_\infty/F) \cong \mathbb{Z}_p$. Let γ_0 be a fixed generator of Γ. Suppose A is a p-primary, abelian discrete group and Γ acts continuously on A. Let $\widehat{A} = Hom(A, \mathbb{Q}_p/\mathbb{Z}_p)$. We know that A and $\widehat{A}$ are $\mathbb{Z}_p$-modules. Now defining $Ta = \gamma_0(a) - a$ for all $a \in A$, A and $\widehat{A}$ become $\mathbb{Z}_p[T]$-module. T is an endomorphism in A. Then it can be shown that T is topologically nilpotent and so both A and $\widehat{A}$ can be thought of as Λ-modules.

2) Let E be an elliptic curve over 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 consider A as a Λ-module (with 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.

3)Let F be a number field and 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 $Gal(F_\Sigma/F)$-module and $A = H^1(F_\Sigma/F_\infty, E[p^\infty])$ also has a natural action of Γ and can be thought of as a Λ-module. Again $\hat{A}$ becomes a finitely generated Λ-module. Now $Sel_E(F_\infty)_p$ is a Λ-submodule of $H^1(F_\Sigma/F_\infty, E[p^\infty])$.

Now we will state some conjectures concerning the structure of these Λ-modules. We will need some terminologies which is defined below.

Terminologies: 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 $corank_\Lambda(A) = rank_\Lambda(\widehat{A})$.

Conjecture 4.1 *Suppose F is a finite extension of $\mathbb{Q}$ and that E is an elliptic curve over F. Let Σ is chosen as above. Then*

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

See [6], Chapter 3. In general all that is known in this context is that

$$corank_\Lambda(H^1(F_\Sigma/F_\infty, E[p^\infty])) \geq [F : \mathbb{Q}]$$

and the equality is equivalent to show that $H^2(F_\Sigma/F_\infty, E[p^\infty])$ which is a Λ-module is Λ-cotorsion.

Conjecture 4.2 *(Mazur) Suppose F is a finite extension of $\mathbb{Q}$ and 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 $Sel_E(F_\infty)_p$ is Λ-cotorsion.*

This was conjectured by Mazur [12]. We have one more conjecture (Due to P. Schneider) (See [3])which gives the Λ-corank of $Sel_E(F_\infty)_p$.

Conjecture 4.3 *(P. Schneider) 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*

$$corank_\Lambda(Sel_E(F_\infty)_p) = \sum_{v\, pss} [F_v : \mathbb{Q}_p].$$

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

Now we will prove the final goal of this chapter.

Theorem 4.4 *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 $corank_{\mathbb{Z}_p}(H^1(K_v, A)) = [K_v : \mathbb{Q}_p] + \delta_A(K_v)$ 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}-module and $\delta_A(K_v) = 0$ otherwise.*

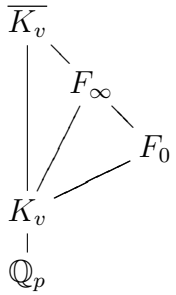
Note: $H^0(K_v, A)$ (or $H^0(K_v, \widehat{A}(1))$ is either trivial or all of A (or $\widehat{A}(1)$). The latter occurs only when $A \cong \mathbb{Q}_p/\mathbb{Z}_p$ (or $A \cong \mu_{p^\infty}$) as a G_{K_v}-module. We know that $\widehat{A}(1) \cong \mathbb{Z}_p$ as a group so we get

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

So the above theorem is the corank lemma for $r = 1$ and $v \mid p$.
The two cases when $\delta_A(K_v) = 1$ can be proved by using standard Local class field theory. So now here we will assume $H^0(K_v, A)$ and $H^0(K_v, \widehat{A}(1))$ is finite and $\delta_A(K_v) = 0$

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 again this can be done by local clas field

theory. So let us assume that $im(\psi)$ is infinite. Let $F_\infty = \overline{K_v}^{ker(\psi)}$. So $G = Gal(F_\infty/K_v)$ acts faithfully on A and $G \cong im(\psi)$, which is a subgroup of $\mathbb{Z}_p^\times$. Hence $G \cong \Delta \times \Gamma$ where $\Gamma = \psi^{-1}(1 + p\mathbb{Z}_p) \cong \mathbb{Z}_p$ and Δ is a finite group of order dividing $p-1$ if p is odd and of order 1 or 2 if p is 2 . Now as $F_0 = F_\infty^\Gamma$ we have $\Delta = Gal(F_0/K_v)$ and $\Gamma = Gal(F_\infty/F_0)$. So F_∞/F is a $\mathbb{Z}_p$ extension . If we define $F_n = F_\infty^{\Gamma^{p^n}}$ for $n \geq 0$ then $F_\infty = \cup_n F_n$ and F_n/F_o is cyclic of order p^n.
So we have the following field extension diagram:



Consider the following exact sequence from the five term exact sequence theorem (Appendix 1 , Theorem 6.3)

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

Our aim is to study $H^1(K_v, A)$ by studying $H^1(F_\infty, A)^G$. For that we need to prove that $coker(r)$ and $ker(r)$ is finite .

Proof of $coker(r)$ is finite :

Γ is a free pro-p group so has p-cohomological dimension 1. If p is odd then $|\Delta|$ is not divisible by p. So we get that $H^2(G, A) = 0$. So r is surjective and $coker(r) = 0$. If $p = 2$ and $\Delta = 1$ then also by same reasoning r is surjective. If $|\Delta| = 2$, then it can be shown that $H^2(G, A) \cong H^2(\Gamma, A) \times H^2(\Delta, A)$. So $H^2(G, A) = \mathbb{Z}/2\mathbb{Z}$ (As $H^2(\Gamma, A) = 0$ and $|\Delta| = 2$). Thus $coker(r)$ is finite of order ≤ 2.

Proof of $ker(r)$ is finite :

First of all from the exact sequence $ker(r) = im(i)$. So for proving finiteness of $ker(r)$ it is enough to prove finiteness for $H^1(G, A)$.
If $|\Delta| = 1$, then $G = \Gamma$ and since we are assuming $H^0(K_v, A)$ is finite from the lemma 6.11 Appendix 1 , we get that $H^1(G, A) = 0$. Now if p is odd and

$|\Delta| > 0$, then $A^{\Delta} = 0$, then by the following inflation-restriction sequence

$$0 \longrightarrow H^1(\Gamma, A^{\Delta}) \longrightarrow H^1(G, A) \longrightarrow H^1(\Delta, A)^{\Gamma}$$

we get that $H^1(G, A) = 0$ (also $H^1(\Gamma, A^{\Delta}) = 0$ as $A^{\Delta} = 0$ and $H^1(\Delta, A)^{\Gamma} = 0$ as $|\Delta|$ is coprime to p). But if $p = 2$ and $|\Delta| = 2$, then A^{Δ} has order 2 and again from the above exact sequence one finds that $|H^1(G, A)| \leq 4$ (As both $H^1(\Gamma, A^{\Delta})$ and $H^1(\Delta, A)^{\Gamma}$ has cardinality less than or equal to 2).

therefore we get the finiteness of $ker(r)$.

By the above results we get that

$$corank_{\mathbb{Z}_p}(H^1(K_v, A)) = corank_{\mathbb{Z}_p}(H^1(F_\infty, A)^G)$$

Since G_{F_∞} acts trivially on A we get $H^1(F_\infty, A) = Hom(G_{F_\infty}, A)$(Here in every case it is understood that we take the continuous maps) . Now let M_∞ denote the maximal , abelian pro-p extension of F_∞ i.e. M_∞ is the compositum of all finite , abelian p-extensions of F_∞ . If we denote $X = Gal(M_\infty/F_\infty)$ then we get

$$H^1(F_\infty, A) = Hom(G_{F_\infty}, A) = Hom(X, A)$$

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

$$corank_{\mathbb{Z}_p}(H^1(K_v, A)) = corank_{\mathbb{Z}_p}(Hom(X_\psi, A)) = rank_{\mathbb{Z}_p}(X_\psi)$$

Since $A \cong \mathbb{Q}_p/\mathbb{Z}_p$ as a group. We will finish the proof by carefully studying the properties of X as a G-module.
All of the characters of Δ have values in $\mathbb{Z}_p^{\times}$. If p is odd, then $p \nmid |\Delta|$, and one has a decomposition of X by the characters of Δ

$$X = \bigoplus_{\chi \in \widehat{\Delta}} X_\chi$$

where $X_\chi = \{x \in X | \delta(x) = \chi(\delta)x \text{ for all } \delta \in \Delta)\} = e_\chi X$, where e_χ is the idempotent for χ in $\mathbb{Z}_p[\Delta]$.
If $p = 2$ and $|\Delta| = 2$ which is the only case when p divides $|\Delta|$, then we

define X_χ by the maximal quotient of X on which Δ acts by χ .
Δ acts on A by the charater $\chi = \psi|_\Delta$ (denoted by ψ_Δ) . Then

$$Hom_\Delta(X, A) = Hom(X_{\psi_\Delta}, A)$$

Furthermore if Y is any $\mathbb{Z}_p$-module and if $\kappa : \Gamma \to 1 + p\mathbb{Z}_p$ is a continuous homomorphism, then the maximal quotient of Y on which Γ acts by the character κ (denoted by Y_κ) is equal to $Y/(\gamma_0 - \kappa(\gamma_0))Y$. Here γ_0 is a fixed topological generator of Γ. By definition Γ acts on A by the character $\psi_\Gamma : \Gamma \to 1 + \mathbb{Z}_p$, where $\psi_\Gamma = \psi|_\Gamma$. In fact as $G \cong \Delta \times \Gamma$ we have $X_\psi = (X_{\psi_\Delta})_{\psi_\Gamma}$. So we get that

$$corank_{\mathbb{Z}_p}(H^1(K_v, A)) = rank_{\mathbb{Z}_p}(X_{\psi_\Delta}/(\gamma_0 - \psi_\Gamma(\gamma_0))X_{\psi_\Delta})$$

Let A be a discrete p-primary abelian group on which Γ acts continuously. Then using the fact that, if $a \in A$ then $T^n a = 0$ for $n \gg 0$, we can consider A as a Λ-module. X is an abelian, pro-p group. Then applying the above fact to the discrete, p-primary Γ-module $Hom(X, \mathbb{Q}_p/\mathbb{Z}_p)$, we can consider X as a Λ-module.
We will use the classification of Λ modules(chapter 2) and the following results of Iwasawa(See [9])
i) X is a finitely generated Λ-module .
ii) 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 $[K_v : \mathbb{Q}_p]$.
iii) If F_∞ contains the group μ_{p^∞} of p-power roots of unity, then the Λ-torsion submodule $X_{\Lambda-tors}$ is isomorphic to $T_p(\mu_{p^\infty})$, the Tate module of μ_{p^∞}. Otherwise $X_{\Lambda-tors} = 0$.

Now we will finish the proof of the theorem. We have already proved that

$$corank_{\mathbb{Z}_p}(H^1(K_v, A)) = rank_{\mathbb{Z}_p}(X_{\psi_\Delta}/f(T)X_{\psi_\Delta})$$

where $f(T) = T - b$ with $b = \psi_\Gamma(\gamma_0) - 1 \in p\mathbb{Z}_p$. So $f(T)$ is a distinguished polynomial of degree 1 . From the satements i), ii) ,iii) using the classification of Λ-modules (Chapter 2, Theorem 2.8), we obtain that X_{ψ_Δ} is pseudo-isomorphic to $\Lambda^{[K_v:\mathbb{Q}_p]}$ or $Y \times \Lambda^{[K_v:\mathbb{Q}_p]}$, where $Y = T_p(\mu_{p^\infty})$ (According as $F_\infty \not\supseteq \mu_{p^\infty}$ or $F_\infty \supset \mu_{p^\infty}$).
As $f(T)$ has degree 1, by the factorization theorem (Chapter 1, Proposition 1.2) we get that $\Lambda/f(T)\Lambda$ has $\mathbb{Z}_p$-rank 1. So if $F_\infty \not\supseteq \mu_{p^\infty}$ then $H^1(K_v, A)$ has $\mathbb{Z}_p$-corank equal to $[K_v : \mathbb{Q}_p]$.
If $\mu_{p^\infty} \subset F_\infty$, then $G = Gal(F_\infty/K_v)$ acts on $T_p(\mu_{p^\infty})$ by a character χ. We are assuming $\psi \neq \chi$. Now if $\psi_\Delta \neq \chi_\Delta$,then considering action of both the

characters on any element y in Y we get that, $\xi^a y = \xi^b y$, $a \neq b$, where ξ is a root of unity. This gives $y = 0$ as $(\xi^{a-b} - 1) \in \mathbb{Z}_p^\times$ (See [20], Proposition 2.2.8). So we get $Y = 0$.
If $\psi_\Gamma \neq \chi_\Gamma$, we have $Y/f(T)Y \cong \Lambda/(T-p, T-b)$ where $p \neq b$ as $\psi_\Gamma(\gamma_0) \neq \chi_\Gamma(\gamma_0)$. As $(T-p)$ and $(T-b)$ are co-prime we get $Y/f(T)Y$ is finite by Lemma 2.2(Chapter 2). In both cases we again find that $X_{\psi_\Delta}/f(T)X_{\psi_\Delta}$ has $\mathbb{Z}_p$-corank $[K_v : \mathbb{Q}_p]$.

■

5 Mazur's Control Theorem

Let F be a finite extension of $\mathbb{Q}$ and E an elliptic curve over F.

Theorem 5.1 *Assume p is a prime and E has good, ordinary reduction over all primes lying over p. Assume that $F_\infty = \bigcup_n F_n$ is a $\mathbb{Z}_p$-extension of F. Then the natural maps*

$$Sel_E(F_n)_p \to Sel_E(F_\infty)_p^{Gal(F_\infty/F_n)}$$

have finite kernels and cokernels of bounded orders as $n \to \infty$

Here as before, F_n denotes the unique subfield of F_∞ containing F such that $[F_n : F] = p^n$. We will prove the theorem with the explicit description of the local Kummer homomorphism of chapter 3. But before proving the theorem, we will introduce some notations.

Notations:

Let E be any elliptic curve defined over F. Let K be an algebraic extension of F. For every prime of η of K, we let

$$H_E(K_\eta) = H^1(K_\eta, E[p^\infty])/im(\kappa_\eta)$$

where κ_η is the local kummer map

$$\kappa_\eta : E(K_\eta) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \to H^1(K_\eta, E[p^\infty])$$

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

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

where the map is induced from $G_{K_\eta} \hookrightarrow G_K$.
Also we define

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

Proof of the Theorem : From the definition of $Sel_E(F_n)_p$ we get the exact sequence

$$0 \to Sel_E(F_n)_p \to H^1(F_n, E[p^\infty]) \to \mathcal{G}_E(F_n) \to 0$$

Now taking the inductive limit over the natural restriction maps, we get another exact sequence

$$0 \to Sel_E(F_\infty)_p \to H^1(F_\infty, E[p^\infty]) \to \mathcal{G}_E(F_\infty) \to 0$$

Let $\Gamma_n = Gal(F_\infty/F_n) = \Gamma^{p^n}$. Then taking the Γ_n invariants we get the following exact sequence

$$0 \to Sel_E(F_\infty)_p^{\Gamma_n} \to H^1(F_\infty, E[p^\infty])^{\Gamma_n} \to \mathcal{G}_E(F_\infty)^{\Gamma_n}$$

Considering the above two exact sequences we get the following commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & Sel_E(F_n)_p & \longrightarrow & H^1(F_n, E[p^\infty]) & \longrightarrow & \mathcal{G}_E(F_n) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle s_n} & & \downarrow{\scriptstyle h_n} & & \downarrow{\scriptstyle g_n} & & \\
0 & \longrightarrow & Sel_E(F_\infty)_p^{\Gamma_n} & \longrightarrow & H^1(F_\infty, E[p^\infty])^{\Gamma_n} & \longrightarrow & \mathcal{G}_E(F_\infty)^{\Gamma_n} & &
\end{array}$$

where the maps s_n, h_n, g_n are the natural restriction maps. So by the snake lemma we get the following exact sequence :

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

Therefore to finish the proof of the theorem, we have to prove finiteness and boundedness of $ker(h_n), ker(g_n), coker(h_n)$, which are proved in the following lemmas.

Lemma 5.2 *$coker(h_n) = 0$.*

Proof: By the inflation-restriction sequence (from five term exact sequence) we get the following exact sequnce

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

where $B = E[p^\infty]^{G_{F_\infty}}$. Now $\Gamma_n \cong \mathbb{Z}_p$, which is a free pro-p group . So Γ_n has p-cohomological dimension 1 . Hence $H^2(\Gamma_n, B) = 0$ (as B is a p-primary group) and so h_n is surjective.

■

Lemma 5.3 *$ker(h_n)$ is finite and has bounded order as $n \to \infty$*

Proof: Again by the same inflation -restriction exact sequence

$$0 \longrightarrow H^1(\Gamma_n, B) \longrightarrow H^1(F_n, E[p^\infty]) \xrightarrow{h_n} H^1(F_\infty, E[p^\infty])^{\Gamma_n} \longrightarrow H^2(\Gamma_n, B)$$

where $B = E[p^\infty]^{G_{F_\infty}}$. So we obtain $ker(h_n) = H^1(\Gamma_n, B)$. If γ denotes the topological generator of Γ then, by the Lemma 6.11 (in Appendix 1) we get that $H^1(\Gamma_n, B) = B/(\gamma^{p^n} - 1)B$. Now B_{div} has finite $\mathbb{Z}_p$-corank (Since $E[p^\infty]$ has finite $\mathbb{Z}_p$-corank). $H^0(\Gamma_n, B_{div}) = B_{div}^{\Gamma_n}$ which is equal to the divisible part of p-primary subgroup of $E(F_n)$. But by Mordeil-weil theorem $E(F_n)$ is finitely generated , so $H^0(\Gamma_n, B_{div})$ is finite. Again by the Lemma 6.11 (in Appendix 1), we get that $H^1(\Gamma_n, B_{div}) = B_{div}/(\gamma^{p^n} - 1)B_{div} = 0$. Hence $(\gamma^{p^n} - 1)B_{div} = B_{div}$. We get that

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

As B is a cofinitely genrated $\mathbb{Z}_p$-module, $[B : B_{div}]$ is finite. Clearly $H^1(\Gamma_n, B)$ is bounded by $[B : B_{div}]$ which is finite and independent of n, which finishes our proof.

■

Lemma 5.4 *The order of $ker(g_n)$ is bounded as n varies.*

Proof: We will prove this lemma by carefully considering some cases. Let v be any prime of F. Let v_n be any prime of F_n lying over v. We will study $ker(g_n)$ by considering each factor of $\mathcal{P}_E(F_n)$ with the maps

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

where η is any prime of F_∞ lying over v_n. This map r_{v_n} is induced from the canonical reduction

$$H^1((F_n)_{v_n}, E[p^\infty]) \xrightarrow{res} H^1((F_\infty)_\eta, E[p^\infty])$$

where res is the reduction map and r_{v_n} is well-defined as $res(im(\kappa_{v_n})) \subseteq im(\kappa_\eta)$.

Now if v is archimedean then v splits completely in F_∞/F so $F_v = (F_\infty)_\eta$ for all $\eta \mid v$. Then clearly $ker(r_{v_n}) = 0$. Now for non-archimedean v we consider two cases separately, $v \nmid p$ and $v \mid p$.

Case I

v is a nonarchimedean prime and $v \nmid p$. Then $ker(r_{v_n})$ is finite and has bounded order as n varies. Moreover if E has good reduction at v or v splits completely in F_∞/F then $ker(r_{v_n}) = 0$.

Proof: Let Γ_v denote the decomposition group of Γ for any non-archimedean prime v. If $\Gamma_v = 0$ then v splits completely in F_∞/F and then as above $F_v = (F_\infty)_\eta$ for all $\eta \mid v$ and $ker(r_{v_n}) = 0$.
Otherwise Γ_v has a finite index in Γ and so v is finitely decomposed in Γ. Now we are assuming $v \nmid p$, so by Theorem 3.5(Chapter 3)we get that $im(\kappa_\eta) = 0$ and $\mathcal{H}_E(M_\eta) = H^1(M_\eta, E[p^\infty])$ for every algebraic extension M_η of F_v . Now as $v \nmid p$, v is unramified and by assumption it is finitely decomposed in F_∞/F. So $(F_\infty)_\eta$ is the $\mathbb{Z}_p$-unramified extension of F_v (the only $\mathbb{Z}_p$-extension of F_v). So $\Gamma_{v_n} := Gal((F_\infty)_\eta/(F_n)_{v_n}) \cong \mathbb{Z}_p$. Let us assume that Γ_{v_n} is generated by a topological generator γ_{v_n}. Then the inflation-restriction exact sequence gives

$$0 \longrightarrow H^1(\Gamma_{v_n}, B_v) \longrightarrow H^1((F_n)_{v_n}, E[p^\infty]) \xrightarrow{r_{v_n}} H^1((F_\infty)_\eta, E[p^\infty]),$$

where $B_v = E[p^\infty]^{G_{(F_\infty)_\eta}}$. We get $ker(r_{v_n}) = H^1(\Gamma_{v_n}, B_v)$. Now $B_v \cong (\mathbb{Q}_p/\mathbb{Z}_p)^e \times$(finite group) where $0 \leq e \leq 2$. Again by the Lemma 6.11(Appendix 1) we get that $H^1(\Gamma_{v_n}, B_v) \cong B_v/(\gamma_{v_n} - 1)B_v$. By following the same lines of arguements as in Lemma 5.3, we get that $(\gamma_{v_n} - 1)B_v$ contains $(B_v)_{div}$. So we obtain

$$|ker(r_{v_n})| \leq |B_v/(B_v)_{div}|$$

This bound is independent of n and of v_n.
Now assume that E has good reduction at v. Then since $v \nmid p$, $F_v(E[p^\infty])/F_v$ is unramified. Let $F_{v,n} := F_v(1/p^n E(F_v))$ then $F_{v,\infty} = \cup_n F_{v,n} = F_v(E[p^\infty])$. Then from (Silverman , proposition VIII.1.5) $F_{v,n}$ are abelian, p extension. So

$$Gal(F_{v,\infty}/F_v) \cong \varprojlim_n Gal(F_{v,n}/F_v)$$

and $Gal(F_{v,\infty}/F_v)$ is a infinite pro-p group. Since $F_{v,\infty}/F_v$ is unramified, $Gal(F_{v,\infty}/F_v)$ is a quotient of $G_{f_v} \cong \widehat{\mathbb{Z}}$, where f_v denote the residue field of F_v. Now as $Gal(F_{v,\infty}/F_v)$ is pro-p, it is a quotient of the maximal pro-p quotient of $\widehat{\mathbb{Z}} = \mathbb{Z}_p$, which is either finite or whole. As $Gal(F_{v,\infty}/F_v)$ is infinite, we get $Gal(F_{v,\infty}/F_v) = \mathbb{Z}_p$. Since $(F_\infty)_\eta$ is the only $\mathbb{Z}_p$-extension of F_v , we get, $(F_\infty)_\eta \cong F_v(E[p^\infty])$.
So we get $B_v = E[p^\infty]$ and then $ker(r_{v_n}) = H^1(\Gamma_{v_n}, E[p^\infty]) = 0$ again by the same kind of reasoning using Lemma 6.11(Appendix 1).

Case II

Suppose v is a non-archimedean prime dividing p .Assume that E has good, ordinary reduction at at v. Then $ker(r_{v_n})$ is finite and has bounded order as $n \to \infty$.

Proof: We will divide the case in three subcases. Either v splits completely in F_∞/F or v is ramified in F_∞/F or v is unramified but finitely decomposed in F_∞/F.
Now if v splits completely then again we have $ker(r_{v_n}) = 0$.
If v is ramified in F_∞/F then f_η is finite, where f_η is the residue field of $(F_\infty)_\eta$ and η is any prime of F_∞ lying over v. In this case we can apply Theorem 3.9(Chapter 3). So we have $im(\kappa_\eta) = im(\varepsilon_\eta)$. We also have $im(\kappa_{v_n}) \subseteq im(\varepsilon_{v_n})$. Therefore we can think of r_{v_n} as composition of the following two maps

$$a_{v_n} : H^1((F_n)_{v_n}, E[p^\infty])/im(\kappa_{v_n}) \longrightarrow H^1((F_\infty)_\eta, E[p^\infty])/im(\varepsilon_{v_n})$$

$$b_{v_n} : H^1((F_n)_{v_n}, E[p^\infty])/im(\varepsilon_{v_n}) \longrightarrow H^1((F_\infty)_\eta, E[p^\infty])/im(\varepsilon_\eta)$$

Where the notations are as defined in Chapter 3. Clearly a_{v_n} is surjective. So we have

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

But $ker(a_{v_n}) = im(\varepsilon_{v_n})/im(\kappa_{v_n})$ and by Theorem 3.8(Chapter 3) we get the order of this group is bounded by $|\tilde{E}(f_\eta)_p|$ which is finite.
On the other hand, from the exact sequence of galois modules

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

We get the following commutative diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & H^1((F_n)_{v_n}, E[p^\infty])/im(\varepsilon_{v_n}) & \xrightarrow{\pi_{v_n}} & H^1((F_n)_{v_n}, \tilde{E}[p^\infty]) \\ & & \downarrow{\scriptstyle b_{v_n}} & & \downarrow{\scriptstyle c_{v_n}} \\ 0 & \longrightarrow & H^1((F_\infty)_\eta, E[p^\infty])/im(\varepsilon_\eta) & \xrightarrow{\pi_\eta} & H^1((F_\infty)_\eta, \tilde{E}[p^\infty]) \end{array}$$

So from the diagram we get that $|\ker(b_{v_n})| \leq |\ker(c_{v_n})|$. Now again by the inflation - restriction sequence we get

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

again by the Lemma 6.11 (Appendix 1) where γ_{v_n} is any topological generator of $Gal((F_\infty)_\eta/(F_n)_{v_n}) \cong \mathbb{Z}_p$. Therefore $|\ker(c_{v_n})|$ is bounded by $|\tilde{E}(f_\eta)_p|$. So we obtain, if v is ramified in F_∞/F,

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

which is finite and independent of n.

Finally in the last case we 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. In this case our aim is to prove $ker(r_{v_n}) = 0.$ for all n. Firstly we will prove that it is enough to prove the following claim.

Claim: $H^1(L/M, E(L)) = 0$ whenever M is a finite extension of F_v and L/M is a finite, unramified p-extension.

Assuming the claim we get $ker(res) = 0$ by the inflation-restriction sequence where res is the following map

$$H^1((F_n)_{v_n}, E[p^\infty]) \xrightarrow{res} H^1((F_\infty)_\eta, E[p^\infty])$$

$ker(r_{v_n}) = 0$ is equivalent to proving

$$im(\kappa_\eta) \cap res(H^1((F_n)_{v_n}, \tilde{E}[p^\infty])) = res(im(\kappa_{v_n}))$$

from the following diagram, where every map is injective

$$\begin{array}{ccc} E((F_n)_{v_n}) \otimes \mathbb{Q}_p/\mathbb{Z}_p & \xrightarrow{\kappa_{v_n}} & H^1((F_n)_{v_n}, \tilde{E}[p^\infty]) \\ \downarrow{\scriptstyle b_{v_n}} & & \downarrow{\scriptstyle res} \\ E((F_\infty)_\eta) \otimes \mathbb{Q}_p/\mathbb{Z}_p & \xrightarrow{\kappa_\eta} & H^1((F_\infty)_\eta, \tilde{E}[p^\infty]) \end{array}$$

Clearly $res(im(\kappa_{v_n})) \subseteq im(\kappa_\eta) \cap res(H^1((F_n)_{v_n}, \tilde{E}[p^\infty]))$.
For the other way inclusion, firstly we note that from the inflation-restriction sequence image of res lies in $H^1((F_\infty)_\eta, \tilde{E}[p^\infty])^{G_{v_n}} = H^1((F_\infty)_\eta, \tilde{E}[p^\infty])^{\Gamma_{v_n}}$ where $\Gamma_{v_n} = Gal((F_\infty)_\eta/(F_n)_{v_n}) \cong \mathbb{Z}_p$.
So enough to show $res(im(\kappa_{v_n})) \supseteq im(\kappa_\eta)^{\gamma_{v_n}} \cap res(H^1((F_n)_{v_n}, \tilde{E}[p^\infty]))$. As res is injective, using the explicit description of Kummer map from Chapter 3 we get that it is enough to prove that $(E((F_\infty)_\eta) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{\Gamma_{v_n}} \subseteq E((F_n)_{v_n}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$.

Let $P \otimes \frac{1}{p^k} \in (E((F_\infty)_\eta) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{\Gamma_{v_n}}$. Then from the definition of $\mathbb{Q}_p/\mathbb{Z}_p$ we can think $P \otimes \frac{1}{p^k} \in (E((F_\infty)_\eta/p^k E((F_\infty)_\eta)^{\Gamma_{v_n}}$.
Consider the following exact sequence

$$0 \longrightarrow p^k E((F_\infty))_\eta \longrightarrow E((F_\infty)_\eta \longrightarrow (E((F_\infty)_\eta/p^k E((F_\infty)_\eta) \longrightarrow 0$$

which gives the cohomological exact sequence

$$0 \longrightarrow (p^k E((F_\infty))_\eta)^{\Gamma_{v_n}} \longrightarrow E((F_n)_{v_n} \xrightarrow{\alpha} (E((F_\infty)_\eta/p^k E((F_\infty)_\eta)^{\Gamma_{v_n}}$$
$$\downarrow$$
$$H^1(\Gamma_{v_n}, p^k E((F_\infty))_\eta)$$

where α is the canonical map obtained from the previous exact sequence. We have $P \otimes Im(\alpha) \in coker(\alpha)$. Since

$$H^1(\Gamma_{v_n}, p^k E((F_\infty))_\eta) = \varinjlim_m (\Gamma_{v_n}/\Gamma_{v_n,m}, p^k E(F_n))$$

Hence, $H^1(\Gamma_{v_n}, p^k E((F_\infty))_\eta)$ is a torsion subgroup and so is $coker(\alpha)$. So there exists s such that
$p^s(P \otimes \frac{1}{p^k}) \in Im(\alpha)$
$\implies \exists Q \in E((F_n)_{v_n}),$ such that $p^s(P \otimes \frac{1}{p^k}) = \alpha(Q)$
$\implies P \otimes \frac{1}{p^k} = Q \otimes \frac{1}{p^s}$
So we get, $(E((F_\infty)_\eta) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{\Gamma_{v_n}} \subseteq E((F_n)_{v_n}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$.

Now we will prove the claim. Let l and m be the residue fields of L and M respectively. Then we have the following 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 $\mathcal{F}(\mathfrak{m}_L)$ denotes the group of points on the formal group $\mathcal{F}$. For proving the claim it is enough to verify $H^1(L/M, \mathcal{F}(\mathfrak{m}_L)) = 0$ and $H^1(L/M, \widetilde{E}(l)) = 0$.

Now $H^1(L/M, \mathcal{F}(\mathfrak{m}_L)) = H^1(L/M, \mathcal{O}_L)$ as $\mathcal{F}(\mathfrak{m}_L)$ and $\mathcal{O}_L$ have same Galois group filtration ($\mathcal{F}(\mathfrak{m}_L^n)/\mathcal{F}(\mathfrak{m}_L^{n+1}) \cong \mathfrak{m}_L^n/\mathfrak{m}_L^{n+1} \cong \pi^n\mathcal{O}_L/\pi^{n+1}\mathcal{O}_L \cong \mathcal{O}_L/\pi\mathcal{O}_L$ where $\pi \in \mathcal{O}_M$ is the uniformizer) (See Appendix 2 , Proposition 7.1). Since L/M is unramified extension we have $\mathcal{O}_L \cong \mathcal{O}_M[Gal(L/M)] \cong \mathcal{O}_L \otimes \mathbb{Z}_p[Gal(L/M)] \cong \mathbb{Z}_p[Gal(L/M)]^s$ which is clearly cohomologically trivial. So $H^1(L/M, \mathcal{F}(\mathfrak{m}_L)) = 0$.

$H^1(L/M, \widetilde{E}(l)) = H^1(l/m, \widetilde{E}(l))$. $H^1(l/m, \widetilde{E}(l)) = H^1(l/m, \widetilde{E}(l)[p^\infty])$ as l/m is a p-extension. Let $\widetilde{m}$ be a $\mathbb{Z}_p$-extension of m containing l (we can find one as l/m is a p-extension) then from the inflation-restriction sequence we get

$$H^1(l/m, \widetilde{E}(l)[p^\infty]) \hookrightarrow H^1(\Gamma_m, \widetilde{E}(\widetilde{m})[p^\infty])$$

where $\Gamma_m \cong Gal(\widetilde{m}/m) \cong \mathbb{Z}_p$. But $(\widetilde{E}(\widetilde{m}[p^\infty]))^{\Gamma_m} = E(m)[p^\infty]$ is finite which gives $H^1(\Gamma_m, \widetilde{E}(\widetilde{m})[p^\infty]) = 0$. Thus $H^1(l/m, \widetilde{E}(l)[p^\infty]) = 0$.

Now we will finish the proof of the Lemma. We have to prove finiteness and boundedness of the following map

$$g_n : \mathcal{G}_E(F_n) \to \mathcal{G}_E(F_\infty)^{\Gamma_n}$$

Now we have

$$ker(g_n) \subseteq \prod_{v_n} ker(r_{v_n}) = \prod_{v} \prod_{v_n|v} ker(r_{v_n})$$

where v_n and v run over all primes of F_n and F correspondingly. If v is archimedean then $ker(r_{v_n}) = 0$, and they dont contribute to the kernel. So we will consider only the non-archimedean primes. We will assume that v does not split completely in F_∞/F as for those primes also $ker(r_{v_n}) = 0$. We have two cases $v \nmid p$ and $v \mid p$.

There are only finitely many primes dividing p and for every such v by case II, we have $ker(r_{v_n})$ is finite and independent of n (We have assumed that E has good , ordinar reductions at all $v \mid p$). Hence

$$|\prod_{v|p} \prod_{v_n|v} ker(r_{v_n})| < \infty$$

and it is independent of n.

If $v \nmid p$, then if E has good reduction over v we have $ker(r_{v_n}) = 0$ otherwise $ker(r_{v_n})$ is finite and independent of n. But E can have bad reduction at only finitely many points. So

$$|\prod_{v\nmid p} \prod_{v_n|v} ker(r_{v_n})| < \infty$$

and it is independent of n.
Thus we get that $ker(g_n)$ is finite and bounded as n varies.

■

Now we will finish the proof of Theorem 5.1. $ker(s_n)$ is finite and has bounded order as n varies, follows from Lemma 5.3. $coker(s_n)$ is finite and bounded as n varies follows from Lemma 5.2 and Lemma 5.4, under the assumption that E has good, ordinary reduction at all $v \mid p$. So Theorem 5.1 is proved.

■

6 Appendix 1

Some important results from Galois cohomology

Cup Product:
If A and B are two G-modules then $A \otimes_{\mathbb{Z}} B$ is also a G-module(by $\sigma(a \otimes b) = \sigma a \otimes \sigma b$) and we obtain for every pair $p, q \geq 0$ a bilinear map

$$\mathcal{C}^p(G, A) \times \mathcal{C}^q(G, B) \xrightarrow{\cup} \mathcal{C}^{p+q}(G, A \otimes B) \tag{5}$$

by

$$(a \cup b)(\sigma_0, \ldots, \sigma_{p+q}) = a(\sigma_0, \ldots, \sigma_p) \otimes b(\sigma_p, \ldots \sigma_{p+q})$$

where $\mathcal{C}^n(G, A)$ consists of the continuous functions $x : G^{n+1} \to A$ such that

$$x(\sigma\sigma_0, \ldots, \sigma\sigma_n) = \sigma x(\sigma_0, \ldots, \sigma_n)$$

Proposition 6.1 *$\partial(a \cup b) = (\partial a) \cup b + (-1)^p (a \cup \partial b)$, where $\partial = \partial^n$ is the usual alternating sum.*

Proof: Reference:-(See [13], Chapter 1.4, page 35)

From this proposition it follows that $a \cup b$ is a cocycle if both a and b are cocycles and a coboundary if one of the cochains a and b is a coboundary and the other a cocycle. Therefore the pairing (5) induces a bilinear map

$$H^p(G, A) \times H^q(G, B) \xrightarrow{\cup} H^{p+q}(G, A \otimes B), \qquad (\alpha, \beta) \longmapsto \alpha \cup \beta$$

This map is called the *Cup-Product*.

Some basic results: At first we will define some very canonical and important homomorphisms between cohomology groups then we will state some results.

Inflation: Let H be a normal closed subgroup of G and A be a G-module. Then A^H is a G/H-module . The projection and the injection

$$G \to G/H, \qquad A^H \hookrightarrow A$$

induces a homomorphism

$$inf_G^{G/H} : H^n(G/H, A^H) \to H^n(G, A)$$

called inflation .

Restriction: Let H be any closed subgroup of G then the following two homomorphisms

$$H \hookrightarrow G, \qquad A \xrightarrow{id} A$$

induces homomorphism between cohomology groups

$$res^G_H : H^n(G, A) \to H^n(H, A)$$

Theorem 6.2 *Let H be a normal subgroup of G and let A be a G-module . Then the sequence*

$$0 \longrightarrow H^1(G/H, A^H) \xrightarrow{Inf} H^1(G, A) \xrightarrow{res} H^1(H, A)$$

is exact.

Proof: See ([1], Chapter 4.5, page - 100)

Transgression:Let H be a normal subgroup of G and A a G-module. Then there is a canonical homomorphism

$$tg : H^1(H, A)^{G/H} \to H^2(G/H, A^H)$$

called transgression, which is given as follows:
If $x : H \to A$ is an inhomogeneous 1-cocycle in a class $[x] \in H^1(H, A)^{G/H}$, then there exists a 1-cochain $y : G \to A$ such that $y|_H = x$ and that $(\partial y)(\sigma_1, \sigma_2)$ is contained in A^H and depends only on the cosets $\sigma_1 H, \sigma_2 H$, i.e may be regarded as a cocycle of G/H. And for each cochain y,

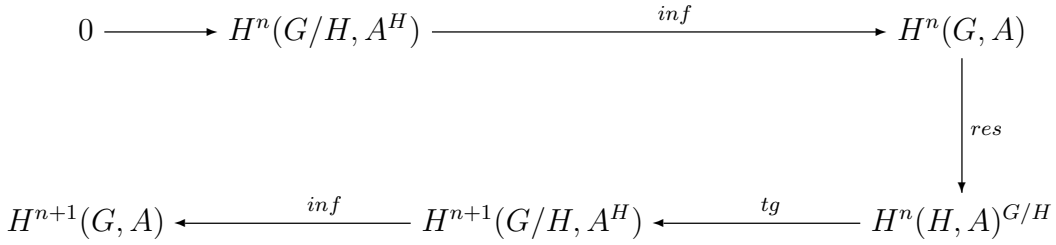
$$tg[x] = [\partial y]$$

Reference:(See [13], Theorem 1.6.5, page 62)

Theorem 6.3 *(Five term exact sequence) Let H be a closed normal subgroup of G and let A be a G module . We then have an exact sequence*

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^1(G/H, A^H) & \xrightarrow{inf} & H^1(G, A) & & \\ & & & & \downarrow{\scriptstyle res} & & \\ H^2(G, A) & \xleftarrow{inf} & H^2(G/H, A^H) & \xleftarrow{tg} & H^1(H, A)^{G/H} & & \end{array}$$

Moreover , if $H^n(H,A)=0$ for $i=1,\dots n-1$, we have an exact sequence



Proof:
(See [13], Theorem 1.6.6, page 64)

Remark: Proof of this theorem is very long but it follows trivially from Spectral Sequence, which will come later in the chapter.

Theorem 6.4 *Let G be a profinite group and U an open subgroup.Then for every G-module A such that $\hat{H}^n(U,A)=0$ we have*

$$(G:U)\hat{H}^n(G,A)=0$$

In particular, if G is finite then $\hat{H}^n(G,A)$ is annihilated by the order $|G|$. If moreover, A is finitely generated as a $\mathbb{Z}$ module, then $\hat{H}^n(G,A)$ is finite.

Recall for $n=0$, $\hat{H}^n(G,A)=A^G/N_GA$ and for $n\geq 1$, $\hat{H}^n(G,A)=H^n(G,A)$.
So we get that for arbitrary profinite groups G the cohomology groups $H^n(G,A)$, $n\geq 1$ are torsion groups since

$$H^n(G,A)=\varinjlim_{U} H^n(G/U,A^U)$$

where U through the open normal subgroups of G and applying the previous theorem we get our conclusion.

Now we will mention some very important spectral sequences which are widely used in cohomology of number fields.

Hochschild - Serre spectral sequence:
Let G be a profinite group, H a closed normal subgroup of G and A a G-module. Then there is a canonical spectral sequence

$$E_2^{pq}=H^p(G/H,H^q(H,A))\Rightarrow H^{p+q}(G,A)$$

It is called Hochschild - Serre spectral sequence.
Reference: ([13] , Theorem 2.1.5, page 82)

Corollary 6.5 *As a corollary using the property of spectral sequence we get the Five term exact sequence theorem .*

First we will state two important definitions.

Definition 6.6 $H^n(G,A)^* = Hom(H^n(G,A), \mathbb{Q}/\mathbb{Z})$

Definition 6.7 *Let G be a profinite group, H a closed subgroup and A a G-module, then we define*

$$D_n(H,A) = \varinjlim_{U \supseteq H} H^n(U,A)^*$$

where U runs throught the open subgroups of G containing H.

Definition 6.8

$$D_n(A) = D_n(\{1\},A) = \varinjlim_{U \supseteq H} H^n(U,A)^*$$

Tate spectral sequence:
If $cd(G,A) \leq n$ (where cd stands for cohomological dimension) then for every normal subgroup H , there is a cohomological spectral sequence

$$E_2^{pq} = H^p(G/H, D_{n-q}(H,A)) \Rightarrow H^{n-(p+q)}(G,A)^*$$

This is called Tate spectral sequence.

Reference: ([13] , Theorem 2.1.11 , page 89)

Tate spectral sequence is used to prove the Tate duality theorems. For local fields we have the following central theorem of Tate:

Theorem 6.9 *(Tate Duality) Let K be a p-adic local field. Let A be a finite G_K module and let $\hat{A}(1) = Hom(A, \mu_{p^\infty})$ .Then the cup-product*

$$H^i(K, \hat{A}(1)) \times H^{2-i}(K, A) \xrightarrow{\cup} H^2(K, \mu_{p^\infty}) \cong \mathbb{Q}/\mathbb{Z}$$

induces for $0 \leq i \leq 2$ an isomorphism of finite abelian groups

$$H^i(K, \hat{A}(1)) \xrightarrow{\sim} H^{2-i}(K, A)^*$$

Reference: ([13], Theorem 7.2.6, page 327)

Now there is one more very important invariant which is associated with the cohomology of local fields. This is Euler-Poincare Characteristic.
Let K be a local field and p be its residue characteristic. If A is a finite G_K-module of order prime to char(K) (in the case char$(K) > 0$). Then we define **Euler-Poincare characteristic** of A

$$\chi(K, A) = \prod_{j=0}^{2} |H^j(K, A)|^{(-1)^j}$$

Now we have the following theorem of Tate

Theorem 6.10 *(Tate)*
For every finite G_K-module A of order a prime to char(K) , we have

$$\chi(K, A) = \| \ a \ \|_K$$

where $\| \quad \|_K$ is the normalized absolute value of K.

Proof: The theorem's statement is very simple but very hard to proof.
reference:([13], Theorem 7.3.1, page 339)

Now we will prove Corank lemma which was used in chapter 3.

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 we have

$$corank_{\mathbb{Z}_p}(A) = r[K_v : \mathbb{Q}_p] + corank_{\mathbb{Z}_p}(H^0(K_v, A)) + rank_{\mathbb{Z}_p}(H^0(K_v, \hat{A}(1)))$$

2) Let K_v be a finite extension of $\mathbb{Q}_l$ where $l \neq p$. Then $H^1(K_v, A)$ is $\mathbb{Z}_p$-cofinitely generated and we have

$$corank_{\mathbb{Z}_p}(A) = corank_{\mathbb{Z}_p}(H^0(K_v, A)) + rank_{\mathbb{Z}_p}(H^0(K_v, \hat{A}(1)))$$

Proof: Let M be a finite G_{K_v}-module. Assume that $|M| = p^a$. Let $\widehat{M}(1) = Hom(M, \mu_{p^\infty})$. Now $\widehat{M}(1)$ is also a G_{K_v}-module order p^a. Now from Theorem 6.10, taking $A = M$ and taking the canonical absolute value in K_v we get
if $v|p$

$$\prod_{j=0}^{2} |H^j(K, A)|^{(-1)^j} = p^{-a[K_v:\mathbb{Q}_p]}$$

otherwise when $v \nmid p$

$$\prod_{j=0}^{2} |H^j(K, A)|^{(-1)^j} = 1$$

And applying Theorem 6.9 to M and K_v we get that ,

$$H^2(K_v, M) \text{ is the Pontryagin dual of } H^0(K_v, \widehat{M}(1)).$$

Now we can extend these results to infinite G_{K_v}-modules. Let $A = \bigcup_n A[p^n]$ and then applying the above results to $M = A[p^n]$ for all $n \geq 0$ which are finite, we get
when $v|p$

$$\sum_{j=0}^{2} (-1)^j corank_{\mathbb{Z}_p}(H^j(K_v, A)) = -[K_v : \mathbb{Q}_p] corank_{\mathbb{Z}_p}(A) \tag{6}$$

and when $v \nmid p$

$$\sum_{j=0}^{2} (-1)^j corank_{\mathbb{Z}_p}(H^j(K_v, A)) = 0 \tag{7}$$

and

$H^2(K_v, A)$ is the Pontryagin dual of $H^0(K_v, \widehat{A}(1))$ and hence we have

$$corank_{\mathbb{Z}_p}(H^2(K_v, A) = rank_{\mathbb{Z}_p}(H^0(K_v, \widehat{A}(1))) \tag{8}$$

So using (6), (7) and (8) we get the corank lemma in both cases.

■

Here we will mention one more lemma which is very useful.

Lemma 6.11 *Suppose that $G =< \sigma >$ is a finite, cyclic group of order m and that A is an abelian group (writen with additive notion) on which G acts. Then $H^1(G, A) = ker(N)/im(\sigma - 1)$, where $N : A \longrightarrow A$ is the norm map defined by*

$$N(a) = \sum_{i=0}^{m-1} \sigma^i(a)$$

and $\sigma - 1 : A \longrightarrow A$ is defined by $(\sigma - 1)(a) = \sigma(a) - a$ (both for all $a \in A$). a) Suppose $\Gamma \cong \mathbb{Z}_p$ and let $\gamma \in \Gamma$ be chosen so that $< \gamma >$ is a dense subgroup 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 $\Gamma \times A \longrightarrow A$ defined by $(\gamma, a) \longrightarrow \gamma(a)$ 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 $\varinjlim H^1(\Gamma/\Gamma_n, A^{\Gamma_n})$. 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 $A = \cup_n A^{\Gamma_n}$. 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 $H^1(\Gamma, A) = 0$.

Proof: Part a) and b) follows just by simple calculation using the structure of $H^1(G, A)$ described initially in the lemma.

c) Suppose $A \cong (\mathbb{Q}_p/\mathbb{Z}_p)^r$. We have $H^0(\Gamma, A) = A^\Gamma$ and $H^1(\Gamma, A) = A/(\gamma - 1)A$. Now we have the following excat sequence

$$H^0(\Gamma, A) \hookrightarrow A \xrightarrow{\gamma - 1} A \longrightarrow H^1(\Gamma, A) \longrightarrow 0.$$

By dualizing we get $\text{corank}(H^0(\Gamma, A)) = \text{corank}(H^1(\Gamma, A))$. So if $H^0(\Gamma, A)$ is finite, then $H^1(\Gamma, A)$ is finite also. But as $(\mathbb{Z}_p)^r$ has no non-trivial finite subgroup, $(\mathbb{Q}_p/\mathbb{Z}_p)^r$ has no finite non-trivial quotient which gives $H^1(\Gamma, A) = 0$.

■

7 Appendix 2

Some Important Results from Elliptic Curves

Firstly we will recall some results concerning Formal Groups.

Let R be a ring.

Definition. A (*one-parameter commutative*) formal group $\mathcal{F}$ defined over R is a power series $F(X,Y) \in R[[X,Y]]$ satisfying:
(a) $F(X,Y) = X + Y +$ (terms of degree ≥ 2).
(b) $F(X,F(Y,Z)) = F(F(X,Y),Z)$ (associativity).
(c) $F(X,Y) = F(Y,X)$ (commutativity).
(d) There is a unique power series $i(T) \in R[[T]]$ such that $F(T,i(T)) = 0$ (inverse).
(e) $F(X,0) = X$ and $F(0,Y) = Y$.

We call $F(X,Y)$ the formal group law of $\mathcal{F}$.

Formal group of Elliptic Curve:
Let E be an elliptic curve given by a Weierstrass equation with coefficients in R.

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

always remembering that there is the extra point at infinity $O = [0,1,0]$. Now we make a change of variables, so let

$$z = -\frac{x}{y} \qquad w = -\frac{1}{y}$$

the origin at O on E is now the point $(z,w) = (0,0)$ and z is a local uniformizer at O (i.e z has a zero of order 1 at O). The usual Weierstrass equation becomes

$$w = z^3 + a_1zw + a_2z^2w + a_3w^2 + a_4zw^2 + a_6w^3 (= f(z,w)).$$

Now if we substitute this equation into itself recursively then we get w as a power series in z.
Since $x = \frac{z}{w}$ and $y = -\frac{1}{w}$ we can obtain Laurent series for x and y by substituting the power series for $w(z)$. Then we can form a power series $F(z_1,z_2)$ (z_1 and z_2 are two points on E) which gives the addition law of z_1 and z_2.

Reference: [19], Chapter IV.1

The formal group associated to E , denoted by $\widehat{E}$ is given by the power series $F(z_1, z_2)$.

Let R be a complete local ring, $\mathcal{M}$ be the maximal ideal of R, k be the residue field, and $\mathcal{F}$ a formal group over R, with formal group law $F(X, Y)$.

Definition: The group associated to $\mathcal{F}/R$, denoted $\mathcal{F}(\mathcal{M})$, is the set $\mathcal{M}$ with the group operations

$$\begin{array}{ccc} x \oplus_{\mathcal{F}} y = F(x, y) & \text{(addition)} & \text{for } x, y \in \mathcal{M}, \\ \ominus_{\mathcal{F}} x = i(x) & \text{(inverse)} & \text{for } x \in \mathcal{M}. \end{array}$$

Proposition 7.1 *(a) For each $n \geq 1$, the map*

$$\mathcal{F}(\mathcal{M}^n)/\mathcal{F}(\mathcal{M}^{n+1}) \to \mathcal{M}^n/\mathcal{M}^{n+1}$$

induced by the identity map on sets is an isomorphism of groups.

(b)Let p be the characteristc of k ($p = 0$ is allowed). Then every torsion element of $\mathcal{F}(\mathcal{M})$ has order a power of p.

Reference: See [19], Chapter 4, Proposition 3.2 Now let K be a local field, complete with respect to a discrete valuation v, R be the ring of integers of K, $\mathcal{M}$ the maximal ideal of R, π a uniformizer for R (i.e $\mathcal{M} = \pi R$) and k be the residue field of R i.e $k = R/\mathcal{M}$.

Let $\widetilde{E}(k)$ be the elliptic curve defined over k obtained by reducing modulo π. Now the curve $\widetilde{E}/k$ may or may not be singular. But in any case the set of non-singular points, denoted by $\widetilde{E}_{ns}(k)$ forms a group. We define two subgroups of $E(K)$ as follows:

$$E_0(K) = \{P \in E(K) : \widetilde{P} \in \widetilde{E}_{ns}(k)\}$$

$$E_1(K) = \{P \in E(K) : \widetilde{P} = 0\}$$

Then we get the following exact sequence of abelian groups:

$$0 \to E_1(K) \to E_0(K) \to \widetilde{E}_{ns}(k) \to 0$$

Reference: [19] , Proposition 6.2.1.

Now from the following proposition we get more explicit description of $E_1(K)$.

Proposition 7.2 *Let E/K be given by a minimal Weierstrass equation, let $\widehat{E}/R$ be the formal group associated to E and let $w(z) \in R[[z]]$ be the power series described above. Then the map*

$$\widehat{E}(M) \to E_1(K)$$

$$z \to (\frac{z}{w(z)}, -\frac{1}{w(z)})$$

is an isomorphism.

Reference: See [19], Chapter 6, Proposition 2.2

Then the above exact sequence becomes

$$0 \to \widehat{E}(M) \to E_0(K) \to \widetilde{E}_{ns}(k) \to 0 \tag{9}$$

Moreover if E has good reduction i.e $\widetilde{E}/k$ is non-singular then $E_0(K) = E(K)$ and $\widetilde{E}_{ns}(k) = \widetilde{E}(k)$. Then (9) becomes

$$0 \to \widehat{E}(M) \to E(K) \to \widetilde{E}(k) \to 0 \tag{10}$$

We will mention one more important proposition which will imply Lutz's Theorem.

Proposition 7.3 *Let K be a finite extension of $\mathbb{Q}_p$ (so char(K) = 0 and k is a finite field). Then $E(K)$ contains a subgroup of finite index which is isomorphic to R^+ (taken additively).*

Reference: See [19], Chapter 6, Proposition 6.3
Now we will have the Lutz's theorem

Theorem 7.4 *$E(K) \cong \mathbb{Z}_p^{[K:\mathbb{Q}_p]} \times$ (finite group)*

Proof: (Clear from the above proposition and structure of R^+)

In the end we will prove one more very important lemma on p-primary part of Formal groups. We will continue with the notations described in Section 3.

Lemma 7.5 *The natural map*

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

is surjective and $ker(\pi) \cong \mathbb{Q}_p/\mathbb{Z}_p$.

Proof: We will use the exact sequence obtained in (9).

$$0 \to \widehat{E}(M) \to E(K) \to \widetilde{E}(k) \to 0$$

which induces the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \widehat{E}(M) & \longrightarrow & E(K) & \longrightarrow & \widetilde{E}(k) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle [p]} & & \downarrow{\scriptstyle [p]} & & \downarrow{\scriptstyle [p]} & & \\ 0 & \longrightarrow & \widehat{E}(M) & \longrightarrow & E(K) & \longrightarrow & \widetilde{E}(k) & \longrightarrow & 0 \end{array}$$

where $[p]$denotes the canonical multiplication map by p. So by snake lemma we get

$$\widehat{E}[p^\infty] \hookrightarrow E[p^\infty] \to \widetilde{E}[p^\infty] \to \widehat{E}(M)/[p]\widehat{E}(M) \to 0$$

So if we can prove $\widehat{E}(M)/[p]\widehat{E}(M) = 0$ then the first part of the lemma will be proved.
Now $[p] : \widehat{E}(M) \longrightarrow \widehat{E}(M)$ is defined by sending $y \mapsto f(y)$ where $y \in \widehat{E}(M)$ and $f(T) \in \mathcal{O}_K[[T]], f = p.g(T) + T^{p^h}(h(T))$, $h(T)$ is invertible and h is the height of $\widehat{E}(M)$ (See Reference: See [19], Chapter 4, Corollary 4.4 and Section 7). So proving $\widehat{E}(M)/[p]\widehat{E}(M) = 0$ is equivalent to find a x such that $f(x) - y = 0$. But $f(T) - y$ is of weierstrass degree p^h therefore $f(T) - y = P(T)U(T)$ where $P(T)$ is distinguished of degree p^h. Therefore $f(T) - y$ has non-zero solution which proves the frist part of the lemma.
Now $E[p^\infty] \cong (\mathbb{Q}_p/\mathbb{Z}_p)^2$ since $E(\mathbb{C}) \cong (\mathbb{Q}/\mathbb{Z})^2$. This gives $ker(\pi) \cong \mathbb{Q}_p/\mathbb{Z}_p$.

■

References

[1] J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic number theory*, London, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], 1986, Reprint of the 1967 original.

[2] J. Coates, R. Greenberg, K. A. Ribet, and K. Rubin, *Arithmetic theory of elliptic curves*, Lecture Notes in Mathematics, vol. 1716, Springer-Verlag, Berlin, 1999, Lectures from the 3rd C.I.M.E. Session held in Cetraro, July 12–19, 1997, Edited by C. Viola.

[3] John Coates, Peter Schneider, and Ramdorai Sujatha, *Links between cyclotomic and* GL_2 *Iwasawa theory*, Doc. Math. (2003), no. Extra Vol., 187–215 (electronic), Kazuya Kato's fiftieth birthday.

[4] A. Fröhlich, *Formal groups*, Lecture Notes in Mathematics, No. 74, Springer-Verlag, Berlin, 1968.

[5] R Greenberg, *Iwasawa theory for elliptic curves*, Arithmetic theory of elliptic curves (Cetraro, 1997), Lecture Notes in Math., vol. 1716, Springer, Berlin, 1999, pp. 51–144.

[6] Ralph Greenberg, *Introduction to Iwasawa theory for elliptic curves*, Arithmetic algebraic geometry (Park City, UT, 1999), IAS/Park City Math. Ser., vol. 9, Amer. Math. Soc., Providence, RI, 2001, pp. 407–464.

[7] Dale Husemoller, *Elliptic curves*, Graduate Texts in Mathematics, vol. 111, Springer-Verlag, New York, 1987, With an appendix by Ruth Lawrence.

[8] K Iwasawa, *On* $\mathbf{Z}_l$*-extensions of algebraic number fields*, Ann. of Math. (2) **98** (1973), 246–326.

[9] Kenkichi Iwasawa, *Local class field theory*, Oxford Science Publications, The Clarendon Press Oxford University Press, New York, 1986, Oxford Mathematical Monographs.

[10] Serge Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.

[11] Ju. I. Manin, *Cyclotomic fields and modular curves*, Uspehi Mat. Nauk **26** (1971), no. 6(162), 7–71.

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

[13] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2000.

[14] Paulo Ribenboim, *L'arithmétique des corps*, Hermann, Paris, 1972.

[15] J.-P. Serre, *A course in arithmetic*, Springer-Verlag, New York, 1973, Translated from the French, Graduate Texts in Mathematics, No. 7.

[16] J-Pierre Serre, *Classes des corps cyclotomiques (d'après K. Iwasawa)*, Séminaire Bourbaki, Vol. 5, Soc. Math. France, Paris, 1995, pp. Exp. No. 174, 83–93.

[17] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg.

[18] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.

[19] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original.

[20] Lawrence C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997.