AN INTRODUCTION TO IWASAWA THEORY FOR ELLIPTIC CURVES

Abstract. We present the first few sections of Greenberg's article "Introduction to Iwasawa Theory for Elliptic Curves". In the process, we review the construction of $\mathbb{Z}_p$-extensions of the rational numbers, discuss Iwasawa's result on the growth of the class group in towers of cyclotomic extensions, and analyze the notion of a Selmer group of an elliptic curve defined over a number field.

Part I

$\mathbb{Z}_p$-Extensions. Let p be a prime number. Denote $K_n = \mathbb{Q}(\zeta_{p^{n+1}})$ as the splitting field of the polynomial $x^{p^{n+1}} - 1$ over $\mathbb{Q}$. The Galois group is known explicitly from the isomorphism

$$\begin{array}{ccc} \big(\mathbb{Z}/p^{n+1}\,\mathbb{Z}\big)^\times & \xrightarrow{\sim} & \mathrm{Gal}\big(K_n/\mathbb{Q}\big) \\ a \mod p^{n+1} & \longrightarrow & \big[\sigma_a : \zeta_{p^{n+1}} \mapsto \zeta_{p^{n+1}}^a\big] \end{array}$$

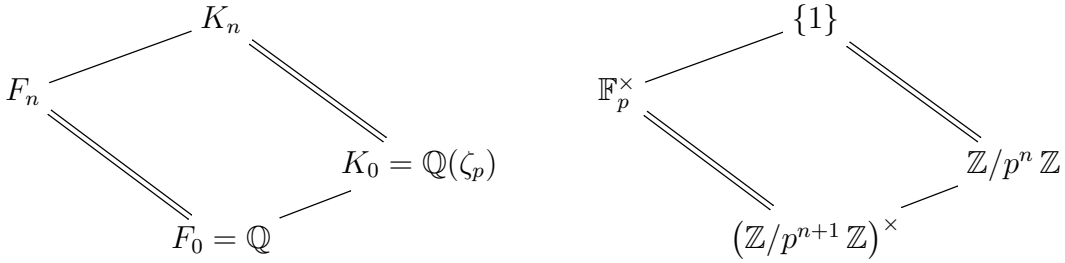
We have two short exact sequences of interest: one coming from the *Teichmüller Character*

$$\begin{array}{ccccccccc} \{0\} & \longrightarrow & \mathbb{Z}/p^n\,\mathbb{Z} & \longrightarrow & \big(\mathbb{Z}/p^{n+1}\,\mathbb{Z}\big)^\times & \xrightarrow{\omega} & \mathbb{F}_p^\times & \longrightarrow & \{1\} \\ & & a \bmod p^n & \longrightarrow & 1 + p\,a \bmod p^{n+1} & & & & \\ & & & & b \bmod p^{n+1} & \xrightarrow{\omega} & b^{p^n} \bmod p^{n+1} & & \end{array}$$

and another coming from surjecting onto the *Sylow p-Subgroup.*

$$\begin{array}{ccccccccc} \{1\} & \longrightarrow & \mathbb{F}_p^\times & \longrightarrow & \big(\mathbb{Z}/p^{n+1}\,\mathbb{Z}\big)^\times & \longrightarrow & \mathbb{Z}/p^n\,\mathbb{Z} & \longrightarrow & \{0\} \\ & & & & b \bmod p^{n+1} & \longrightarrow & b^{p-1} \bmod p^{n+1} & & \end{array}$$

Here $\mathbb{Z}/p^n\,\mathbb{Z}$ is an additive subgroup of the multiplicative group $\big(\mathbb{Z}/p^{n+1}\,\mathbb{Z}\big)^\times$. Let $F_n = \mathbb{Q}(\alpha_n)$ be the field generated by the resolvent $\alpha_n = \sum_{a \in \mathbb{F}_p^\times} \zeta_{p^{n+1}}^a$, so that we have the field diagram



where the bold lines denote the groups $\mathrm{Gal}\big(F_n/F_0\big) \simeq \mathrm{Gal}\big(K_n/K_0\big) \simeq \mathbb{Z}/p^n\,\mathbb{Z}$. Upon denoting $K_\infty = \bigcup_{n \geq 0} K_n$ and $F_\infty = \bigcup_{n \geq 0} F_n$ as the respective composite fields, we have the Galois groups

$$\mathrm{Gal}\big(F_\infty/\mathbb{Q}\big) \simeq \mathrm{Gal}\big(K_\infty/\mathbb{Q}(\zeta_p)\big) \simeq \mathbb{Z}_p.$$

We call both $K_\infty = \mathbb{Q}(\zeta_{p^\infty})$ and F_∞ *cyclotomic $\mathbb{Z}_p$-extensions of* $\mathbb{Q}$. In general, given a field $F_0 = F$, we wish to create a tower $F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n \subseteq \cdots$ such that $\mathrm{Gal}\big(F_n/F_0\big) \simeq \mathbb{Z}/p^n\,\mathbb{Z}$. If we denote $F_\infty = \bigcup_{n\geq 0} F_n$, then $\mathrm{Gal}\big(F_\infty/F\big) \simeq \mathbb{Z}_p$.

Remark. One can create more exotic extensions than $\mathbb{Z}_p$. The multiplicative group $\mathbb{G}_m$ over the field $K = \mathbb{Q}$ yields the finite extension $K_n = \mathbb{Q}\big(\mathbb{G}_m[p^{n+1}]\big) = \mathbb{Q}(\zeta_{p^{n+1}})$, so that $\mathrm{Gal}\big(K_n/K\big) \simeq \big(\mathbb{Z}/p^{n+1}\,\mathbb{Z}\big)^\times$. Hence $\mathrm{Gal}\big(K_\infty/K\big) \simeq GL_1(\mathbb{Z})$. We say that the compositum $K_\infty = \mathbb{Q}(\zeta_{p^\infty})$ is a $GL(1)$-extension of $\mathbb{Q}$. More generally, given an abelian variety E of dimension d over a number field K, denote the finite extension $K_n = K\big(E[p^{n+1}]\big)$. Then $\mathrm{Gal}\big(K_n/K\big) \hookrightarrow GL_{2d}\big(\mathbb{Z}/p^{n+1}\,\mathbb{Z}\big)$ coming from the action on the Tate module, so that the compositum $K_\infty = K\big(E[p^\infty]\big)$ is contained in an $GL(2d)$-extension of K.

Relation with Fermat's Last Theorem. The following was first conjectured in 1635 by Pierre de Fermat (August 17, 1601 – January 12, 1665).

> **Conjecture (Fermat, 1635).** For integral exponents $n > 2$, the integer solutions a, b, and c to the equation $a^n + b^n = c^n$ must satisfy $a\,b\,c = 0$.

As noted in `Wikipedia`, "[this] famous Last Theorem was first discovered by [Fermat's] son in the margin on his father's copy of an edition of Diophantus, and included the statement that the margin was too small to include the proof." Indeed, to prove such a conjecture, one need only consider the odd prime exponents p. If not n is not divisible by any odd prime, then $n = 2^{m+2}$ is a power of 2, and one can write

$$x^4 + y^4 = z^4 \qquad \text{where} \qquad \begin{cases} x = a^{2^m} \\ y = b^{2^m} \\ z = c^{2^m} \end{cases} \qquad \Longrightarrow \qquad x\,y\,z = \big(a\,b\,c\big)^{2^m}.$$

Fermat himself showed (albeit posthumously) that $x\,y\,z = 0$ using the Method of Infinite Descent, so that $a\,b\,c = 0$. On the other hand, if n is divisible by an odd prime p, then one can write

$$x^p + y^p = z^p \qquad \text{where} \qquad \begin{cases} x = a^{n/p} \\ y = b^{n/p} \\ z = c^{n/p} \end{cases} \qquad \Longrightarrow \qquad x\,y\,z = \big(a\,b\,c\big)^{n/p}.$$

In 1770, Leonhard Euler (April 15, 1707 – September 18, 1783) proved the conjecture for $p = 3$; in 1825, Peter Dirichlet (February 13, 1805 – May 5, 1859) proved it for $p = 5$; and in 1839, Gabriel Lamé (July 22, 1795 – May 1, 1870) proved in for $p = 7$. In fact, in 1847, Lamé attempted to prove the conjecture for all odd primes p by factoring over the ring $\mathbb{Z}[\zeta_p]$. The idea was to write $\prod_{j=1}^{p}(x + \zeta_p^j\,y) = z^p$, then conclude that each factor $x + \zeta_p^j\,y = \alpha_j^p$ for some element $\alpha_j \in \mathbb{Z}[\zeta_p]$. Unfortunately, Ernst Kummer (January 29, 1810 – May 14, 1893) had shown some years before that unique factorization fails in this ring – and therefore such a conclusion was not valid. In 1850, Kummer showed the following.

> **Theorem (Kummer, 1850).** Assume that p is an odd prime that does not divide the order of the class group of $\mathbb{Z}[\zeta_p]$. Then the conjecture is valid.

Using his theory of ideal class groups for the cyclotomic field $K = \mathbb{Q}(\zeta_p)$, he was able to show that each ideal $\left(x + \zeta_p^j\, y\right) \mathcal{O}_K = \mathfrak{a}_j^p$ for some ideal $\mathfrak{a}_j$ in $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$. The assumption allowed him to conclude $\mathfrak{a}_j = \alpha_j\, \mathcal{O}_K$ for some element $\alpha_j \in \mathbb{Z}[\zeta_p]$ because $\mathfrak{a}_j^p = z^p\, \mathcal{O}_K$ is a principal ideal, so that each factor $x + \zeta_p^j\, y = \alpha_j^p$. He was able to formulate a contradiction from this point.

Remark. Any odd prime p satisfying the assumption in the theorem is called a *regular prime*; any prime that divides the order of the class group $\mathbb{Z}[\zeta_p]$ is called an *irregular prime*. Kummer calculated that the only irregular primes $p < 165$ are $p = 37$, 59, 67, 101, 103, 131, or 149. It is known that there are infinitely many irregular primes; it is not known whether there are infinitely many regular primes, but it appears that approximately $e^{-1/2} \approx 61\%$ of primes are regular. Hence Kummer settled many cases of the conjecture – but unfortunately not infinitely many cases.

Iwasawa's Results. Let me explain more about the class group mentioned above. Let K be a number field with ring of integers $\mathcal{O}_K$; in practice, we will choose $K = \mathbb{Q}(\zeta_{p^{n+1}})$ and $\mathcal{O}_K = \mathbb{Z}[\zeta_{p^{n+1}}]$. Recall that we say $\mathfrak{a}$ is a *(fractional) ideal of* K if $\mathfrak{a}$ is a nonzero, finitely generated $\mathcal{O}_K$-submodule of K. Equivalently, it is a nonzero subset of K such that $x\,\mathfrak{a} \subseteq \mathcal{O}_K$ for some nonzero $x \in \mathcal{O}_K$. A (fractional) ideal $\mathfrak{a}$ of K is said to be *principal* if $\mathfrak{a} = \alpha\, \mathcal{O}_K$ for some nonzero $\alpha \in K$. The following is a standard result from Algebraic Number Theory.

Proposition.

- The collection $\mathbf{I}_K$ of (fractional) ideals $\mathfrak{a}$ of K forms an abelian group under multiplication. Explicitly,

$$\mathfrak{a} \cdot \mathfrak{b} = \left\{ \sum_{i=1}^{n} \alpha_i\, \beta_i \,\middle|\, \alpha_i \in \mathfrak{a},\, \beta_i \in \mathfrak{b} \right\} \quad \text{and} \quad \mathfrak{a}^{-1} = \left\{ x \in K \,\middle|\, x\,\mathfrak{a} \subseteq \mathcal{O}_K \right\}.$$

- The collection $\mathbf{P}_K$ of principal ideals $\alpha\, \mathcal{O}_K$ forms an abelian subgroup of $\mathbf{I}_K$.
- The *(ideal) class group* $C\ell(\mathcal{O}_K) = \mathbf{I}_K / \mathbf{P}_K$ of K is a is finite group. Moreover, we have an exact sequence

$$\begin{array}{ccccccccc} \{1\} & \longrightarrow & \mathcal{O}_K^\times & \longrightarrow & K^\times & \longrightarrow & \mathbf{I}_K & \longrightarrow & C\ell(\mathcal{O}_K) \longrightarrow \{1\} \\ & & & & & & \alpha & \longrightarrow & \alpha\, \mathcal{O}_K \end{array}$$

We call the order $h_K = \left|C\ell(\mathcal{O}_K)\right| = \left|\mathbf{I}_K : \mathbf{P}_K\right|$ of the (ideal) class group the *class number*. The following explains the usefulness of considering regular primes.

Corollary. Assume that $\mathfrak{a} \in \mathbf{I}_K$ satisfies $\mathfrak{a}^d \in \mathbf{P}_K$ for some d relatively prime to h_K. Then $\mathfrak{a} \in \mathbf{P}_K$.

We explain why. Since the class group has finite order h_K, we see that $\mathfrak{a}^{h_k} \in \mathbf{P}_K$. Write $r\, h_K + s\, d = 1$ for some integers r and s. But then $\mathfrak{a} = \left(\mathfrak{a}^{h_K}\right)^r \cdot \left(\mathfrak{a}^d\right)^s \in \mathbf{P}_K$. In the specific case where $K = \mathbb{Q}(\zeta_p)$, we choose $d = p$: if p is a regular prime, then it is relatively prime to $h_K = \left|C\ell(\mathbb{Z}[\zeta_p])\right|$. If $\mathfrak{a}^p = z^p\, \mathcal{O}_K$ then $\mathfrak{a}^p \in \mathbf{P}_K$, so $\mathfrak{a} \in \mathbf{P}_K$, showing that $\mathfrak{a} = \alpha\, \mathcal{O}_K$ is principal.

The conclusion here is we can prove the conjecture when we know about the elements of p-power order in the (ideal) class group $C\ell(\mathbb{Z}[\zeta_p])$. In the 1950's, Kenkichi Iwasawa (September 11, 1917 – October 26, 1998) studied precisely this group. Allow me to state the precise

result. Denote $K_n = \mathbb{Q}(\zeta_{p^{n+1}})$ so that $\mathcal{O}_{K_n} = \mathbb{Z}[\zeta_{p^{n+1}}]$ is its ring of integers. We can compute the group $\mathbf{I}_{K_n}$ of (fractional) ideals, the subgroup $\mathbf{P}_{K_n}$ of principal ideals, and the quotient group $C\ell(\mathbb{Z}[\zeta_{p^{n+1}}]) = \mathbf{I}_{K_n}/\mathbf{P}_{K_n}$ as the (ideal) class group. Let e_n denote the exponent of p which exactly divides the order of the (ideal) class group, that is, $p^{e_n} = \big|C\ell\big(\mathbb{Z}[\zeta_{p^{n+1}}]\big)[p^\infty]\big|$ in terms of the subgroup

$$C\ell(\mathcal{O}_K)[p^\infty] = \left\{ \overline{\mathfrak{a}} \in \mathbf{I}_K/\mathbf{P}_K \;\middle|\; \mathfrak{a}^{p^n} \in \mathbf{P}_K \text{ for some } n \geq 1 \right\} \subseteq C\ell(\mathcal{O}_K).$$

Iwasawa's main result is that the exponent e_n does not grow too "quickly."

> **Theorem (Iwasawa, 1950's).** There exist integers μ, λ, and ν, only dependent on p, such that $e_n = \mu\, p^n + \lambda\, n + \nu$ for "sufficiently large" n.

In fact, Iwasawa showed that $\mu = \nu = 0$.

Remark. One can attempt to replace $K_n = \mathbb{Q}(\zeta_{p^{n+1}})$ with an arbitrary $\mathbb{Z}_p$-extension of number fields. Indeed, we have seen that this example can be constructed via the multiplicative group $\mathbb{G}_m$ over $K = \mathbb{Q}$. Given a number field $F_0 = F$, we can always create a tower of number fields $F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n \subseteq \cdots$ such that we have the group $\mathrm{Gal}\big(F_n/F_0\big) \simeq \mathbb{Z}/p^n\,\mathbb{Z}$. We can define the group $\mathbf{I}_{F_n}$ of (fractional) ideals, the subgroup $\mathbf{P}_{F_n}$ of principal ideals, and the quotient group $C\ell(\mathcal{O}_{F_n}) = \mathbf{I}_{F_n}/\mathbf{P}_{F_n}$ as the (ideal) class group. Write $p^{e_n} = \big|C\ell(\mathcal{O}_{F_n})[p^\infty]\big|$. The main question is whether there exist integers μ, λ, and ν, only dependent on the extension F_∞/F, such that $e_n = \mu\, p^n + \lambda\, n + \nu$ for "sufficiently large" n. We'll discuss this throughout the seminar!

Part II

Class Field Theory. In order to generalize Iwasawa's ideas for elliptic curves, we discuss a different way to view the (ideal) class group. We recall a result shown by Johann Peter Gustav Lejeune Dirichlet (February 13, 1805 – May 5, 1859).

> **Theorem (Dirichlet, 1846).** Let L be a number field with ring of integers $\mathcal{O}_L$. Then $U(L) = \mathcal{O}_L^\times$ is a finitely generated abelian group under multiplication. More precisely, $U(L) \simeq U(L)_{\mathrm{tors}} \times \mathbb{Z}^r$ where $U(L)_{\mathrm{tors}}$ is a finite group of roots of unity and $r = \mathrm{rank}_{\mathbb{Z}}\big(U(L)\big) = r_1 + r_2 - 1$ is a nonnegative integer in terms of
>
> $$L \otimes_{\mathbb{Q}} \mathbb{R} = \underbrace{\mathbb{R} \times \cdots \times \mathbb{R}}_{r_1 \text{ copies}} \times \underbrace{\mathbb{C} \times \cdots \times \mathbb{C}}_{r_2 \text{ copies}}.$$

This is known as Dirichlet's Unit Theorem. The set $U(L) = \mathcal{O}_L^\times$ is called the unit group of L; this is a subgroup of the multiplicative group $\mathbb{G}_m(L) = L^\times$. For each positive integer n, the map $\alpha \mapsto \alpha^n$ induces a short exact sequence

$$\{1\} \longrightarrow \mu_n \longrightarrow U(\overline{L}) \xrightarrow{\;n\;} U(\overline{L}) \longrightarrow \{1\}.$$

Each of these groups can be viewed as a $\mathbb{Z}$-module with action by $G_L = \mathrm{Gal}(\overline{L}/L)$, and hence action by the decomposition group $G_{L_v} = \mathrm{Gal}(\overline{L}_v/L_v)$ corresponding to a choice of embedding $\overline{L} \hookrightarrow \overline{L}_v$ for each place v. This induces the following exact diagram coming from

group cohomology:

$$\begin{array}{ccccccccc}
\{1\} & \longrightarrow & \dfrac{\mathcal{O}_L^\times}{\left(\mathcal{O}_L^\times\right)^n} & \xrightarrow{\ \kappa\ } & H^1\big(G_L,\ \mu_n\big) & \longrightarrow & H^1\big(G_L,\ U(\overline{L})\big)[n] & \xrightarrow{\ n\ } & \{0\} \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \{1\} & \longrightarrow & \displaystyle\prod_v H^1\big(G_{L_v},\ U(\overline{L}_v)\big) & \xrightarrow{\ \sim\ } & \displaystyle\prod_v H^1\big(G_{L_v},\ U(\overline{L}_v)\big) & &
\end{array}$$

Here, κ is the Kummer map which sends α to that cohomology class $\xi : \sigma \mapsto \big(\sigma \sqrt[n]{\alpha}\big) / \sqrt[n]{\alpha}$. We review a fundamental result which culminates in the study of Local Class Field Theory.

> **Theorem.** Let $U(L) = \mathcal{O}_L^\times$ denote the unit group of a number field L. There exists a map $\lambda^{-1} : C\ell(\mathcal{O}_L) \to H^1\big(G_L,\ U(\overline{L})\big)$ which induces an isomorphism
>
> $$C\ell(\mathcal{O}_L) \simeq \ker\left[H^1\big(G_L,\ U(\overline{L})\big) \to \prod_v H^1\big(G_{L_v},\ U(\overline{L}_v)\big)\right].$$

This requires some explanation because it is not a standard result in the literature. Let H denote the Hilbert class field of L, and denote $G_{H/L} = \mathrm{Gal}(H/L)$ as its Galois group. The map $\alpha \mapsto \alpha\,\mathcal{O}_H$ induces the short exact sequence

$$\{1\} \longrightarrow U(H) \longrightarrow \mathbb{G}_m(H) \longrightarrow \mathbf{P}_H \longrightarrow \{1\}$$

of $G_{H/L}$-modules, which yields the exact sequence

$$\mathbb{G}_m(L) \longrightarrow H^0\big(G_{H/L},\ \mathbf{P}_H\big) \xrightarrow{\ \lambda^{-1}\ } H^1\big(G_{H/L},\ U(H)\big) \longrightarrow H^1\big(G_{H/L},\ \mathbb{G}_m(H)\big).$$

Every fractional ideal $\mathfrak{a}$ of L becomes principal in H, so that $\mathfrak{a}\,\mathcal{O}_H = \alpha\,\mathcal{O}_H$; hence the $G_{H/L}$-invariant ideals $H^0\big(G_{H/L},\ \mathbf{P}_H\big) = \mathbf{I}_L$. Hilbert's Theorem 90 asserts $H^1\big(G_{H/L},\ \mathbb{G}_m(H)\big) = \{0\}$, so that $H^1\big(G_{H/L},\ U(H)\big) \simeq \mathbf{I}_L/\mathbf{P}_L = C\ell(\mathcal{O}_L)$. Since H/L is an unramified extension, and the short exact sequence

$$\{1\} \longrightarrow U(\overline{L}_v) \longrightarrow \mathbb{G}_m(\overline{L}_v) \xrightarrow{\ \mathrm{ord}_v\ } \mathbb{Q} \longrightarrow \{0\}$$

comes from those ramified extensions, the composition

$$C\ell(\mathcal{O}_L) \xrightarrow{\ \lambda^{-1}\ } H^1\big(G_{H/L},\ U(H)\big) \xrightarrow{\ \mathrm{Inf}\ } H^1\big(G_L,\ U(\overline{L})\big) \longrightarrow H^1\big(G_{L_v},\ U(\overline{L}_v)\big)$$

must be trivial for each place v. (I am thankful to Jiu-Kang Yu for assisting with this argument.)

Selmer Groups for Number Fields. This result motivates a definition. We define the n-Selmer group of a number field L as the abelian group

$$\mathrm{Sel}^{(n)}(L) = \ker\left[H^1\big(G_L,\ \mu_n\big) \to \prod_v H^1\big(G_{L_v},\ U(\overline{L}_v)\big)\right]$$

so that we have the following exact diagram:

$$\begin{array}{ccccccccc}
\{1\} & \longrightarrow & \dfrac{\mathcal{O}_L^\times}{\left(\mathcal{O}_L^\times\right)^n} & \xrightarrow{\kappa} & \mathrm{Sel}^{(n)}(L) & \xrightarrow{\lambda} & C\ell(\mathcal{O}_L)[n] & \longrightarrow & \{1\} \\
 & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \lambda^{-1}} & & \\
\{1\} & \longrightarrow & \dfrac{\mathcal{O}_L^\times}{\left(\mathcal{O}_L^\times\right)^n} & \xrightarrow{\kappa} & H^1\big(G_L,\ \mu_n\big) & \longrightarrow & H^1\big(G_L,\ U(\overline{L})\big)[n] & \xrightarrow{n} & \{0\} \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \{1\} & \longrightarrow & \displaystyle\prod_v H^1\big(G_{L_v},\ U(\overline{L}_v)\big) & \xrightarrow{\sim} & \displaystyle\prod_v H^1\big(G_{L_v},\ U(\overline{L}_v)\big) & &
\end{array}$$

As the quotient $\mathcal{O}_L^\times/\left(\mathcal{O}_L^\times\right)^n$ and class group $C\ell(\mathcal{O}_L)$ are finite groups, the n-Selmer group $\mathrm{Sel}^{(n)}(L)$ is a finite group as well. In what follows, we would like to find a similar short exact sequence which does not assume $L/\mathbb{Q}$ is finite nor depend on a choice of positive integer n.

Remark. If L is a number field containing the nth roots of unity μ_n, then Kummer Theory asserts that $H^1\big(G_L,\ \mu_n\big) \simeq L^\times/\left(L^\times\right)^n$. In this case, the n-Selmer group can be realized as

$$\mathrm{Sel}^{(n)}(L) \simeq \left\{ \overline{\alpha} \in \frac{L^\times}{\left(L^\times\right)^n} \;\middle|\; \alpha\,\mathcal{O}_L = \mathfrak{a}^n \text{ for some } \mathfrak{a} \in \mathbf{I}_L \right\}.$$

This definition appears in Franz Lemmermeyer's paper *Selmer Groups and Quadratic Reciprocity*, which appeared online at `http://arxiv.org/abs/1108.5674v1`.

Elliptic Curves. Continue to let L be a number field, and consider an elliptic curve E defined over L. That is, we consider the abelian variety

$$E: \quad y^2 + a_1\,x\,y + a_3\,y = x^3 + a_2\,x^2 + a_4\,x + a_6$$

of dimension $d = 1$, where each coefficient $a_i \in L$. Then the set

$$E(L) = \left\{ (x_1 : x_2 : x_0) \in \mathbb{P}^2(L) \;\middle|\; \begin{array}{r} x_2^2\,x_0 + a_1\,x_1\,x_2\,x_0 + a_3\,x_2\,x_0^2 \\ = x_1^3 + a_2\,x_1^2\,x_0 + a_4\,x_1\,x_0^2 + a_6\,x_0^3 \end{array} \right\}$$

is an abelian group. In 1908, Jules Henri Poincaré (April, 29 1854 – July 17, 1912) conjectured bit more:

> **Theorem (Mordell, 1922; Weil, 1928).** $E(L)$ is a finitely generated abelian group under addition. That is, $E(L) \simeq E(L)_{\mathrm{tors}} \times \mathbb{Z}^r$ where $E(L)_{\mathrm{tors}}$ is a finite group, and $r = \mathrm{rank}_{\mathbb{Z}}\big(E(L)\big)$ is a nonnegative integer.

This was shown in 1922 by Louis Joel Mordell (January 28, 1888 – March 12, 1972) for $L = \mathbb{Q}$, then generalized in 1928 to arbitrary number fields L (and abelian varieties of arbitrary dimension d) by André Weil (May 6, 1906 – August 6, 1998). The proof relies on the fact that the quotient group $E(L)/n\,E(L)$ is finite.

We've seen that the unit group $U(L) = \mathcal{O}_L^\times$ and the Mordell-Weil group $E(L)$ are both finitely generated abelian groups, so we make a general observation. Say that $\Gamma \simeq \Gamma_{\mathrm{tors}} \times \mathbb{Z}^r$.

For any positive integer n, we have the quotient

$$\frac{\Gamma}{n\,\Gamma} \simeq \frac{\Gamma_{\text{tors}}}{n\,\Gamma_{\text{tors}}} \times \left(\frac{\mathbb{Z}}{n\,\mathbb{Z}}\right)^r \simeq \Gamma \otimes_{\mathbb{Z}} \left(\frac{\mathbb{Z}}{n\,\mathbb{Z}}\right) \simeq \Gamma \otimes_{\mathbb{Z}} \left(\frac{\frac{1}{n}\,\mathbb{Z}}{\mathbb{Z}}\right)$$

as a finite group. Note that we have different structures depending on whether we take the inverse limit or the direct limit:

$$\varprojlim_n \frac{\Gamma}{p^n\,\Gamma} \simeq \Gamma \otimes_{\mathbb{Z}} \mathbb{Z}_p \qquad \text{yet} \qquad \varinjlim_n \frac{\Gamma}{p^n\,\Gamma} \simeq \Gamma \otimes_{\mathbb{Z}} \big(\mathbb{Q}_p/\mathbb{Z}_p\big).$$

Both are $\mathbb{Z}_p$-modules, but only the one on the left is finitely generated. We'll return to the modules

$$\varprojlim_n \frac{\mathcal{O}_L^\times}{\big(\mathcal{O}_L^\times\big)^{p^n}} \simeq \mathcal{O}_L^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p \qquad \text{and} \qquad \varprojlim_n \frac{E(L)}{p^n\,E(L)} \simeq E(L) \otimes_{\mathbb{Z}} \mathbb{Z}_p.$$

Towers of Number Fields. We would like to know if we can generalize the Mordell-Weil Theorem to extensions larger than number fields – such as those extensions $K/\mathbb{Q}$ which are algebraic. To this end, we have the following deep result.

> **Theorem.** Denote $K = \mathbb{Q}_\Sigma^{\text{ab}}$ as the compositum of those finite, abelian extensions L of $\mathbb{Q}$ which are unramified outside a finite set $\Sigma = \{p_1,\, p_2,\, \ldots,\, p_n\}$ of primes p_i. Let E be an elliptic curve defined over $\mathbb{Q}$.
>
> - $E(K)_{\text{tors}}$ is a finite group.
> - $\text{rank}_{\mathbb{Z}}\big(E(L)\big)$ is uniformly bounded.
> - $E(K)$ is a finitely generated abelian group.

The first statement was shown in 1981 by Kenneth Alan Ribet (June 28, 1948 –). The second was shown in a series of papers and preprints in the 1980's by Kazuya Kato (January 17, 1952 –) and David Ephraim Rohrlich (?? –). (We also need the result that elliptic curves E over $\mathbb{Q}$ are modular.) We show the third statement following a proof due to Barry Charles Mazur (December 19, 1937 –). Let L be a finite, abelian extension of $\mathbb{Q}$, unramified outside of Σ, such that $\text{rank}_{\mathbb{Z}}\big(E(L)\big)$ is maximal. Then the quotient group $E(K)/E(L)$ is torsion, so that for each $P \in E(K)$ we can find a positive integer m such that $[m]P \in E(L)$. Hence we have a well-defined perfect pairing

$$\text{Gal}(K/L) \times \frac{E(K)}{E(L)} \longrightarrow E(K)_{\text{tors}} \qquad \text{which sends} \qquad \big(\sigma,\ P\big) \ \mapsto\ \sigma(P) - P.$$

But this induces a group homomorphism $E(K)/E(K)_{\text{tors}} \to E(L)$ defined by $P \mapsto [t]P$ where $t = \big|E(K)_{\text{tors}}\big|$. Now the Mordell-Weil Theorem asserts that $E(L)$ is finitely generated, so that $E(K)$ must be as well.

Remark. Here is a special case of this result. Let $K_\infty = \mathbb{Q}(\zeta_{p^\infty})$ be the compositum of the cyclotomic fields $K_n = \mathbb{Q}(\zeta_{p^{n+1}})$. Since each K_n is a finite, abelian extension of $\mathbb{Q}$ which is unramified outside of $\Sigma = \{p\}$, we see that $K_\infty = \mathbb{Q}_\Sigma^{\text{ab}}$ in this case. The result above implies that, for any given elliptic curve E over $\mathbb{Q}$, there exists some nonnegative integer n_0 such that

$$\text{rank}_{\mathbb{Z}}\big(E(K_n)\big) = \text{rank}_{\mathbb{Z}}\big(E(K_{n_0})\big) \qquad \text{for all } n \geq n_0.$$

Selmer Groups for Elliptic Curves. Let E be an elliptic curve over $\mathbb{Q}$. Recall that the Mordell-Weil Theorem for number fields L used the statement that, for any positive integer n, the quotient $E(L)/n\,E(L)$ is finite. We discuss how to generalize this to algebraic extensions K over $\mathbb{Q}$.

With $\overline{K}$ as the algebraic closure of K, we have the following short-exact sequence of abelian groups:

$$\{O_E\} \longrightarrow E[n] \longrightarrow E(\overline{K}) \xrightarrow{[n]} E(\overline{K}) \longrightarrow \{O_E\}.$$

Each of these groups can be viewed as a $\mathbb{Z}$-module with action by $G_K = \mathrm{Gal}(\overline{K}/K)$, and hence action by the decomposition group $G_{K_v} = \mathrm{Gal}(\overline{K}_v/K_v)$ corresponding to a choice of embedding $\overline{K} \hookrightarrow \overline{K}_v$ for each place v. This induces the following exact diagram coming from Galois cohomology:

$$\begin{array}{ccccccccc}
\{O_E\} & \longrightarrow & \dfrac{E(K)}{n\,E(K)} & \xrightarrow{\kappa} & \mathrm{Sel}_E^{(n)}(K) & \xrightarrow{\lambda} & Ш_E(K)[n] & \xrightarrow{[n]} & \{0\} \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
\{O_E\} & \longrightarrow & \dfrac{E(K)}{n\,E(K)} & \xrightarrow{\kappa} & H^1\big(G_K,\ E[n]\big) & \xrightarrow{\lambda} & H^1\big(G_K,\ E(\overline{K})\big)[n] & \xrightarrow{[n]} & \{0\} \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \{O_E\} & \longrightarrow & \displaystyle\prod_v H^1\big(G_{K_v},\ E(\overline{K}_v)\big) & \xrightarrow{\sim} & \displaystyle\prod_v H^1\big(G_{K_v},\ E(\overline{K}_v)\big) & &
\end{array}$$

Here we replace $E(K)/n\,E(K) \simeq E(K) \otimes_{\mathbb{Z}} \left(\frac{1}{n}\,\mathbb{Z}\,/\mathbb{Z}\right)$ to find the direct limits

$$\varinjlim_n \frac{E(K)}{n\,E(K)} \simeq E(K) \otimes_{\mathbb{Z}} \big(\mathbb{Q}/\mathbb{Z}\big) \qquad \text{and} \qquad \varinjlim_n \frac{E(K)}{p^n\,E(K)} \simeq E(K) \otimes_{\mathbb{Z}} \big(\mathbb{Q}_p/\mathbb{Z}_p\big).$$

This can be summarized as the following.

Proposition. We have the short exact sequences

$$\begin{array}{ccccccccc}
\{O_E\} & \longrightarrow & E(K) \otimes_{\mathbb{Z}} \big(\mathbb{Q}_p/\mathbb{Z}_p\big) & \xrightarrow{\kappa} & \mathrm{Sel}_E(K)_p & \xrightarrow{\lambda} & Ш_E(K)[p^\infty] & \longrightarrow & \{0\} \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
\{O_E\} & \longrightarrow & E(K) \otimes_{\mathbb{Z}} \big(\mathbb{Q}/\mathbb{Z}\big) & \xrightarrow{\kappa} & \mathrm{Sel}_E(K) & \xrightarrow{\lambda} & Ш_E(K) & \longrightarrow & \{0\}
\end{array}$$

in terms of the p-primary Selmer group

$$\mathrm{Sel}_E(K)_p = \varinjlim_n \mathrm{Sel}_E^{(p^n)}(K) = \ker\left[H^1\big(G_K,\ E[p^\infty]\big) \to \prod_v H^1\big(G_{K_v},\ E(\overline{K})\big)\right]$$

and the Tate-Shafarevich group

$$Ш_E(K) = \ker\left[H^1\big(G_K,\ E(\overline{K})\big) \to \prod_v H^1\big(G_{K_v},\ E(\overline{K})\big)\right].$$

Remark. A similar result holds for the class group. Recall that if we denote $U(K) = \mathcal{O}_K^\times$ as the unit group of K, then the map $\alpha \mapsto \alpha^n$ induces a short exact sequence

$$\{1\} \longrightarrow \mu_n \longrightarrow U(\overline{K}) \xrightarrow{\ n\ } U(\overline{K}) \longrightarrow \{1\}.$$

The following becomes clear.

Proposition. We have the short exact sequences

$$\begin{array}{ccccccccc}
\{1\} & \longrightarrow & \mathcal{O}_K^\times \otimes_{\mathbb{Z}} \left(\mathbb{Q}_p/\mathbb{Z}_p\right) & \xrightarrow{\ \kappa\ } & \mathrm{Sel}(K)_p & \xrightarrow{\ \lambda\ } & C\ell(\mathcal{O}_K)[p^\infty] & \longrightarrow & \{0\} \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
\{1\} & \longrightarrow & \mathcal{O}_K^\times \otimes_{\mathbb{Z}} \left(\mathbb{Q}/\mathbb{Z}\right) & \xrightarrow{\ \kappa\ } & \mathrm{Sel}(K) & \xrightarrow{\ \lambda\ } & C\ell(\mathcal{O}_K) & \longrightarrow & \{0\}
\end{array}$$

in terms of the p-primary Selmer group

$$\mathrm{Sel}(K)_p = \varinjlim_n \mathrm{Sel}^{(p^n)}(K) = \ker\left[H^1\big(G_K,\ \mu_{p^\infty}\big) \to \prod_v H^1\big(G_{K_v},\ U(\overline{K})\big)\right]$$

Generalized Selmer Groups. We conclude the presentation by offering a general definition for Selmer groups and Tate-Shafarevich groups. Let $K/\mathbb{Q}$ be an algebraic extension, and Γ be a divisible abelian group, that is, a group for which the sequence

$$\{O_\Gamma\} \longrightarrow \Gamma[n] \longrightarrow \Gamma \xrightarrow{\ n\ } \Gamma \longrightarrow \{O_\Gamma\}$$

is exact for each positive integer n. We will assume that $\sigma(P \oplus Q) = \sigma(P) \oplus \sigma(Q)$ for all $P, Q \in \Gamma$ and $\sigma \in \mathrm{Gal}(\overline{K}/K)$, so that the sequence above holds as $\mathrm{Gal}(\overline{K}/K)$-modules. Using the arguments above, we have the short exact sequences

$$\begin{array}{ccccccccc}
\{O_\Gamma\} & \longrightarrow & \Gamma(K) \otimes_{\mathbb{Z}} \left(\mathbb{Q}_p/\mathbb{Z}_p\right) & \xrightarrow{\ \kappa\ } & \mathrm{Sel}_\Gamma(K)_p & \xrightarrow{\ \lambda\ } & Ш_\Gamma(K)[p^\infty] & \longrightarrow & \{0\} \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
\{O_\Gamma\} & \longrightarrow & \Gamma(K) \otimes_{\mathbb{Z}} \left(\mathbb{Q}/\mathbb{Z}\right) & \xrightarrow{\ \kappa\ } & \mathrm{Sel}_\Gamma(K) & \xrightarrow{\ \lambda\ } & Ш_\Gamma(K) & \longrightarrow & \{0\}
\end{array}$$

in terms of the K-rational points $\Gamma(K) = H^0\big(\mathrm{Gal}(\overline{K}/K),\ \Gamma\big)$, the p-primary Selmer group

$$\mathrm{Sel}_\Gamma(K)_p = \ker\left[H^1\big(G_K,\ \Gamma[p^\infty]\big) \to \prod_v H^1\big(G_{K_v},\ \Gamma\big)\right]$$

and the Tate-Shafarevich group

$$Ш_\Gamma(K) = \ker\left[H^1\big(G_K,\ \Gamma\big) \to \prod_v H^1\big(G_{K_v},\ \Gamma\big)\right].$$

Clearly, these assumptions are true for $\Gamma = U(\overline{\mathbb{Q}})$, the units in $\overline{\mathbb{Z}}$, and for $\Gamma = E(\overline{\mathbb{Q}})$ relative to an elliptic curve E defined over $\mathbb{Q}$.

Questions. Denote $K_n = \mathbb{Q}(\zeta_{p^{n+1}})$.

- Is $Ш_\Gamma(K_n)$ a finite group? Is $p^{e_n} = \left|Ш_\Gamma(K_n)[p^\infty]\right|$ finite integer?
- Do there exist integers μ, λ, and ν, only dependent on p, such that $e_n = \mu\, p^n + \lambda\, n + \nu$ for "sufficiently large" n?

Kenkichi Iwasawa solved these questions for $C\ell(\mathcal{O}_K) = Ш_U(K_n)$. We will find that Barry Mazur's Control Theorem will help in answering these questions for $Ш_E(K_n)$.