Selmer groups

Lectures at Baskerville

August 2022

Chris Wuthrich

Contents

Introduction and notations

These notes are the draft for my lectures at Baskerville Hall in August 2022. They contain more detail than what will be presented during the 3 lectures there. Prerequisites for these notes is material from [28].

Throughout the notes, the following notations will be used.

- E is an elliptic curve.
- F will stand for a general perfect field.
- K is a number field and $\mathcal{O}_K$ its ring of integers.
- K_v will stand for the completion of K at a place v and $\mathbb{F}_v$ for its residue field. $\mathcal{O}_v$ is the ring of integers in K_v and $\mathfrak{m}_v$ its maximal ideal.
- Σ is a finite set of places in K and $\mathcal{O}_\Sigma$ is the ring of Σ-integers in K.
- $H^i(F, \cdot)$ is the i-th Galois cohomology for the absolute Galois group G_F of F.
- $\mu[n]$ is the Galois module of n-th roots of unity.
- For any abelian group A, we denote by A/n the quotient A/nA; even when the group is written multiplicatively. For instance $\mathbb{Q}^\times/2$ is the group $\mathbb{Q}^\times$ modulo its squares.

1 First lecture

Ernst Sejersted Selmer (1920-2006)

1.1 Example

Let E be the elliptic curve

$$E\colon\ y^2 + y = x^3 + x^2 - 9x - 15$$

defined over the number field $K = \mathbb{Q}(\zeta)$ with $\zeta^2+\zeta+1 = 0$. This curve is chosen so that $E(K)_{\text{tors}} = {}^{\mathbb{Z}}/_{3\mathbb{Z}}\, S \oplus {}^{\mathbb{Z}}/_{3\mathbb{Z}}\, T$ with $S = (5, 9)$ and $T = (-2+\zeta, 2+\zeta)$. It has good reduction outside the primes $\mathfrak{p}_1$ and $\mathfrak{p}_2$ above 19, which are generated by $\pi_1 = 3-2\zeta$ and $\pi_2 = 5+2\zeta$ respectively.

For any field F such that E is an elliptic curve over F with $E[3] \subset E(F)$ and $\gcd\bigl(\text{char}(F), n\bigr) = 1$, we define the following map

$$\kappa\colon \quad \begin{aligned} E(F) &\longrightarrow {}^{F^\times}\!/_{\cube} \times {}^{F^\times}\!/_{\cube} \\ P = (x,y) &\longmapsto \bigl(-4x + y + 11,\ (2+3\zeta)\,x + y + (5+6\zeta)\bigr) \end{aligned}$$

where $\cube$ stands for the set of cubes in $F^\times$. Using the notation introduced above we will write $F^\times/3$ now for this quotient. Though this definition does not make sense for the point $P = O$ as it has no x and y-coordinates and for the points where either of the two linear terms is zero. Actually, $-4x + y + 11 = 0$ is an equation for the tangent to E at S and the other term is an equation for the tangent at T. Since S and T are 3-torsion points on a Weierstrass equations, they are inflection points; therefore the first term vanishes only for $P = S$ and the second only for $P = T$. If we correct the definition of κ by

$$\kappa(O) = (1,1), \qquad \kappa(S) = \kappa(-S)^2 \qquad \text{and} \qquad \kappa(T) = \kappa(-T)^2$$

we have a well-defined map.

Later, in Lemma 3 and Lemma 4, we will show that κ is a group homomorphism with kernel $3E(F)$. We continue to write κ for the injective map from $E(F)/3$.

For any prime $\mathfrak{p}$, denote by $v_{\mathfrak{p}}$ the valuation at this prime. We will use the same notation for the induced homomorphism : $K^\times/3 \times K^\times/3 \to \mathbb{Z}/3 \times \mathbb{Z}/3$ in both arguments.

Lemma 1

Let $\mathfrak{p}$ be a prime not dividing 3 and not equal to $\mathfrak{p}_1$ or $\mathfrak{p}_2$. Then the map $v_{\mathfrak{p}} \circ \kappa\colon E(K)/3 \to \mathbb{Z}/3 \times \mathbb{Z}/3$ is zero.

Proof. By assumption the equation of E defines a reduces curve $\tilde{E}$ over the residue field $\mathbb{F}_\mathfrak{p}$ with $E[3] \subset E(\mathbb{F}_\mathfrak{p})$. We can compare the maps κ for the field K and $\mathbb{F}_\mathfrak{p}$:

$$\begin{tikzcd}
E(K)/3 \arrow[r, "\kappa"] \arrow[d] & K^\times/3 \times K^\times/3 \\
\tilde{E}(\mathbb{F}_\mathfrak{p})/3 \arrow[r, "\tilde{\kappa}"] & \mathbb{F}_\mathfrak{p}^\times/3 \times \mathbb{F}_\mathfrak{p}^\times/3
\end{tikzcd}$$

If $P \in E(K)$ is such that $\tilde{P} \notin \{O, S, T\}$, then the formula for κ and $\tilde{\kappa}$ are the same. Therefore the valuation of both parts of $\kappa(P)$ will be 0.

If $\tilde{P} = O$, then $P = (x, y)$ belongs to the kernel of reduction and hence $v_\mathfrak{p}(x) = -2m$ and $v_\mathfrak{p}(y) = -3m$ for some integer m. It is clear that $v_\mathfrak{p}(-4x + y + 11) = -3m \equiv 0 \pmod 3$ and similar for the second term.

If $\tilde{P} = T$, then $Q = P - T$ is such that $\tilde{Q} = O$. Then $\kappa(P) = \kappa(Q)\kappa(T) = \kappa(Q) \cdot \kappa(-T)^2$ and by the first two cases both $\kappa(Q)$ and $\kappa(-T)$ have valuation divisible by n. The case $\tilde{P} = S$ is treated the same way. □

Let $\mathfrak{q}$ be the unique prime above 3; it is generated by $\pi = 2 + \zeta$. Set $\Sigma = \{\mathfrak{q}, \mathfrak{p}_1, \mathfrak{p}_2\}$. Define the subgroup $\mathscr{H} \leqslant K^\times/3$ by

$$\mathscr{H} = \left\{ a \in K^\times \;\middle|\; v_\mathfrak{p}(a) \equiv 0 \pmod 3 \; \forall \mathfrak{p} \notin \Sigma \right\} \Big/ \text{⧉}.$$

In [28] it is denoted $K(\Sigma, 3)$, we will later use the notation $H^1(\mathcal{O}_\Sigma, \mu[3])$. Since $\mathcal{O}_K$ is a unique factorisation domain and its units are just $\mu[6]$, it is easy to determine that $\mathscr{H}$ is a $\mathbb{F}_3$-vector space of dimension 4 with basis ζ, π, π_1, π_2.

The previous lemma implies that we have an injective map

$$\kappa \colon E(K)/3 \longrightarrow \mathscr{H} \times \mathscr{H}.$$

This already proves the weak Mordell-Weil theorem for this curve and bounds the rank of $E(K)$ to be at most 6, but we will push this further now. For each $\mathfrak{p} \in \Sigma$, we can compare κ with the local version over the completion $K_\mathfrak{p}$:

$$\kappa_\mathfrak{p} \colon E(K_\mathfrak{p})/3 \longrightarrow K_\mathfrak{p}^\times/3 \times K_\mathfrak{p}^\times/3.$$

It is clear that the image of κ belongs to the group

$$\left\{ (a, b) \in \mathscr{H} \times \mathscr{H} \;\middle|\; (a, b) \in \operatorname{Im} \kappa_\mathfrak{p} \; \forall \mathfrak{p} \in \Sigma \right\},$$

which we will later define to be the Selmer group $\mathrm{Sel}_3(E/K)$.

As an example of how the three extra conditions help to reduce the rank, we concentrate on $\mathfrak{p} = \mathfrak{p}_1$. The curve has split multiplicative reduction over $K_{\mathfrak{p}_1} \cong \mathbb{Q}_{19}$ with Tamagawa number $c_{\mathfrak{p}_1} = 3$. The 3-torsion point S has bad reduction, so it can be used to split the exact sequence

$$0 \longrightarrow E^0(K_{\mathfrak{p}_1}) \longrightarrow E(K_{\mathfrak{p}_1}) \longrightarrow E(K_{\mathfrak{p}_1})/E^0(K_{\mathfrak{p}_1}) \cong \mathbb{Z}/3 \longrightarrow 0.$$

Since the kernel of reduction $\hat{E}(\mathfrak{p}_1)$ is divisible by 3, we get an isomorphism $E^0(K_{\mathfrak{p}_1})/3 \cong \mathbb{F}_{\mathfrak{p}_1}^\times/3 \approx \mathbb{Z}/3$ by reduction. However T is divisible by 3 in $E(K_{\mathfrak{p}_1})$. Pick U such that $3U = T$; concretely we can take

$$U = \big(5 + 9 \cdot 19 + 13 \cdot 19^2 + 12 \cdot 19^3 + \mathrm{O}(19^4),\; 9 + 19 + 18 \cdot 19^2 + 16 \cdot 19^3 + \mathrm{O}(19^4)\big).$$

Therefore $E(K_{\mathfrak{p}_1})/3$ is of dimension 2 generated by U and S. The group $K_{\mathfrak{p}_1}^{\times}/3$ has dimension 2 as well, generated by ξ and π_1 where $\xi^3 = \zeta$. The image under $\kappa_{\mathfrak{p}_1}$ in $K_{\mathfrak{p}_1}^{\times}/3 \times K_{\mathfrak{p}_1}^{\times}/3$ is equal to the group generated by $\kappa(U) = (\xi\,\pi_1, 1)$ an $\kappa(S) = (\pi_1^2, 1)$. Hence $(a,b) \in \mathscr{H} \times \mathscr{H}$ satisfies $(a,b) \in \operatorname{Im} \kappa_{\mathfrak{p}_1}$ if and only if b is a cube in $K_{\mathfrak{p}_1}^{\times}$.

Writing $a = \zeta^{a_1} \cdot \pi^{a_2} \cdot \pi_1^{a_3} \cdot \pi_2^{a_4}$ and similar for b, the conditions turn out to be

$$\begin{aligned} (a,b) \in \kappa_{\mathfrak{p}_1} &\iff b_2 = b_3 = 0 \\ (a,b) \in \kappa_{\mathfrak{p}_2} &\iff a_2 + b_2 = a_4 + b_4 = 0 \\ (a,b) \in \kappa_{\mathfrak{q}} &\iff a_2 = b_2 = a_1 + a_3 + 2a_4 + 2b_1 + 2b_3 + b_4 = 0 \end{aligned}$$

Therefore $\mathrm{Sel}_3(E/K)$ is 3-dimensional, generated by $\kappa(S) = (\pi_1^2\,\pi_2^2, \zeta\,\pi_2)$ and $\kappa(T) = (\zeta^2\,\pi_2, \pi_2^2)$ and (ζ,ζ).

It remains to determine if $(\zeta,\zeta) \in \operatorname{Im} \kappa$. Suppose $P = (X : Y : Z)$ maps to (ζ,ζ), then there exist $U, V \in K^{\times}$ such that

$$\begin{gathered} -4\,X + Y + 11\,Z = \zeta\,U^3 \\ (2 + 3\zeta)\,X + Y + (5 + 6\zeta)\,Z = \zeta\,V^3. \end{gathered}$$

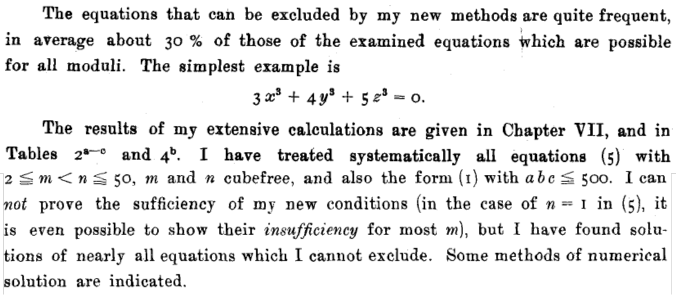
We will see soon that the tangent at $-S - T \in E[3]$ will also have that property, meaning that there is a $W \in K^{\times}$ such that

$$(-1 - 3\zeta)\,X + Y + (-1 - 6\zeta)\,Z = \zeta\,W^3.$$

Moreover $(U : V : W)$ will be a point on the curve

$$C_{(\zeta,\zeta)}: \qquad \zeta\,U^3 + (3 - 2\zeta)\,V^3 + (-3 - 5\zeta)\,W^3 + (-6 - 6\zeta)\,UVW.$$

It turns out that $(2 - \zeta : 1 : 1)$ is a solution in $C_{(\zeta,\zeta)}(K)$. The corresponding point is $P = (-2 - 2\zeta : -1 : 1 + \zeta) = (-2, \zeta)$, obtained by solving the above three linear equation. It must have infinite order in $E(K)$. We conclude that $E(K)$ is isomorphic to $\mathbb{Z}/3 \oplus \mathbb{Z}/3 \oplus \mathbb{Z}$. (Using heights one could also verify that S, T, and P generate the Mordell-Weil group. And, yes, there are much easier ways to verify this information.)



The equations that can be excluded by my new methods are quite frequent, in average about 30 % of those of the examined equations which are possible for all moduli. The simplest example is

$$3\,x^3 + 4\,y^3 + 5\,z^3 = 0.$$

The results of my extensive calculations are given in Chapter VII, and in Tables 2^{a-c} and 4^{b}. I have treated systematically all equations (5) with $2 \leqq m < n \leqq 50$, m and n cubefree, and also the form (1) with $a\,b\,c \leqq 500$. I can *not* prove the sufficiency of my new conditions (in the case of $n = 1$ in (5), it is even possible to show their *insufficiency* for most m), but I have found solutions of nearly all equations which I cannot exclude. Some methods of numerical solution are indicated.

from [27] (1951)

1.2 Complete n-descent

Let E be an elliptic curve over a field F and let $n \geqslant 2$. We suppose that $E[n] \subset E(F)$ and that $\gcd\bigl(\mathrm{char}(F), n\bigr) = 1$. For each n-torsion point T, we pick a function

$g_T \in F(E)$ with divisor $\mathrm{div}(g_T) = [n]^*(T) - [n]^*(O)$. Next, there is a function $f_T \in F(E)$ with divisor $\mathrm{div}(f_T) = n(T) - n(O)$ such that $f_T \circ [n] = g_T^n$. (See III.8 in [28].) This determines f_T up to multiplication by an n-th power in $F^\times$. We define

$$\begin{array}{rrcll} \kappa_T : & E(F) & \longrightarrow & F^\times/n & \\ & P & \longmapsto & f_T(P) & \text{if } P \notin \{O, T\} \\ & O & \longmapsto & 1 & \\ & T & \longmapsto & \kappa_T(-T)^{-1} & \end{array}$$

which works if $n > 2$. For $n = 2$ see Prop X.1.4 in [28]. For $n = 3$, $f_T(P) = 0$ defines the inflection tangent at T like in the above example.

Lemma 2

For all $S, T \in E[n]$, we have $\kappa_{-T} = \kappa_T \circ [-1]$ and $\kappa_{S+T} = \kappa_S \cdot \kappa_T$.

The proof is left to hard-working students in ☞ Exercise A.

Lemma 3

For each $T \in E[n]$, the map κ_T is a group homomorphism.

Proof. Let $P, Q \in E(F)$. We wish to show $\kappa_T(P+Q) \overset{?}{=} \kappa_T(P) \cdot \kappa(Q)$. If P or Q is O it is obvious.

Suppose first $Q = -P$. Then $\kappa_T(P) \cdot \kappa_T(-P) = \kappa_T(P) \cdot \kappa_{-T}(P) = \kappa_{T-T}(P) = 1$.

Next suppose that neither of P, Q or $P+Q$ belongs to $\{O, T\}$. Let ℓ_P be the equation of a line through $-P$ and T. Set

$$G(P, Q) = \frac{\ell_P(Q)}{x(Q) - x(T-P)},$$

which is a function $E \times E \longrightarrow \mathbb{P}^1$ defined over F whose divisor is

$$\mathrm{div}(G) = (P+Q=0) - (P+Q=T) + (Q=T) - (Q=O) + (P=T) - (P=0).$$

There exists a constant $c \in F^\times$ such that

$$c \cdot G(P, Q)^n = \frac{f_T(P+Q)}{f_T(P) \cdot f_T(Q)}$$

as functions in $(P, Q) \in E \times E$. Composition with $[n]$ shows that c is an n-to power in $F^\times$:

$$c \cdot G(nP, nQ)^n = \frac{f_T(nP+nQ)}{f_T(nP) \cdot f_T(nQ)} = \left(\frac{g_T(P+Q)}{g_T(P) \cdot g_T(Q)}\right)^n$$

as functions in (P, Q).

Finally, the special case $P = T$ or $Q = T$ can be deduced from the above. For instance $\kappa(Q+T)\,\kappa(-T) = \kappa(Q)$ implies that $\kappa(Q)\,\kappa(T) = \kappa(Q+T)$. □

Fix a basis S, T of $E[n]$.

Lemma 4

The kernel of the homomorphism

$$\kappa = \kappa_S \times \kappa_T : E(F) \longrightarrow F^\times/n \times F^\times/n$$

is $n\,E(F)$.

Proof. $n\,E(F) \subset \ker\kappa$: If $P = nQ$ for a $Q \in E(F)$, then $f_T(P) = f_T(nQ) = g_T(Q)^n$ is an n-th power for all $P \neq O, T$.

$\ker\kappa \subset n\,E(F)$: Let $P \neq O$ such that $\kappa(P) = (1,1)$. It follows from Lemma 2 that $\kappa_T(P) = 1$ for all $T \in E[n]$.

Pick $Q \in E(\bar{F})$ such that $nQ = P$. Let σ be an element in the absolute Galois group G_F of F. Set $\xi_\sigma = \sigma(Q) - Q$ and our aim is to show that it is equal to O. First

$$n\,\xi_\sigma = n\,\sigma(Q) - nQ = \sigma(nQ) - nQ = \sigma(P) - P = O$$

which shows that $\xi_\sigma \in E[n]$. By assumption, there is a $u \in F$ such that $f_T(P) = u^n$, which happens to be 0 if $P = T$. As before $u^n = f_T(P) = g_T(Q)^n$, which shows that there is $\zeta \in \mu[n] \subset F$ with $g_T(Q) = u\,\zeta \in F$. By definition of the Weil pairing (III.8 in [28]), we have

$$\begin{aligned} e_n(\xi_\sigma, T) &= \frac{g_T(X+\xi_\sigma)}{g_T(X)} && \text{as a function in } X \\ &= \frac{g_T\big(\sigma(Q)\big)}{g_T(Q)} && \text{by taking } X = Q \\ &= \frac{\sigma\big(g_T(Q)\big)}{g_T(Q)} = 1 && \text{as } g_T(Q) \in F. \end{aligned}$$

Since this holds for all $T \in E[n]$, the non-degeneracy of the Weil-pairing implies that $\xi_\sigma = O$ and therefore $Q \in E(F)$. □

Now, we suppose that E is an elliptic curve over a number field K. Let Σ be a finite set of primes containing all places above prime divisors of n and all places where E has bad reduction.

Lemma 5

For each $T \in E[n]$, the valuation of $\kappa_T(P)$ at $\mathfrak{p} \notin \Sigma$ is zero in ${}^{\mathbb{Z}}/_{n\mathbb{Z}}$ for all $P \in E(K)$.

Proof. The cases $\tilde{P} \neq O$ can be treated the same way as in the proof of Lemma 1. Hence we will concentrate on the function f_T on the formal group $\hat{E}$ over the completion $K_\mathfrak{p}$ associated to a minimal equation for E. See Chapter IV in [28]. Since g_T has a simple pole at O, we can write $g_T = c\,t^{-1} + \mathrm{O}(t^0)$ as a power series in $t = -x/y$ with $c \neq 0$. By assumption, f_T has no other zero or pole in $\hat{E}$ than at O. Therefore $f_T = a\,t^{-n} \cdot u$ for a unit power series $u = 1 + \mathrm{O}(t) \in \mathcal{O}_v[[t]]^\times$ and $a \neq 0$. The composition with $[n] = n\,t + \mathrm{O}(t^2)$ gives $a\,n^{-n} = c^n$ and hence a is a n-th power in $K_\mathfrak{p}^\times$. As a consequence the valuation of $f_T(P)$ for any $P \in \hat{E}(\mathfrak{p})$ is a multiple of n. □

(This is usually proved differently, see Proposition VIII.1.5 in [28].)

Theorem 6

Let E be an elliptic curve over a number field K such that $E[n] \subset E(K)$. Then $E(K)/n$ is finite.

Proof. By Lemma 4, we now that $E(K)/n$ is isomorphic to the image of κ in $K^{\times}/n \times K^{\times}/n$. However the previous lemma shows that the image of κ lies in $\mathscr{H} \times \mathscr{H}$ where $\mathscr{H}$ is the subgroup of $K^{\times}/n$ consisting of all elements with valuation divisible by n at primes outside Σ. The group $\mathscr{H}$ fits into the short exact sequence of finite groups

$$\begin{tikzcd} 0 \arrow[r] & \mathcal{O}_{\Sigma}^{\times}/n \arrow[r] & \mathscr{H} \arrow[r] & \mathrm{Cl}(\mathcal{O}_{\Sigma})[n] \arrow[r] & 0 \end{tikzcd}$$

where $\mathcal{O}_{\Sigma}$ is the ring of Σ-integers in K. The finiteness of the class group and Dirichlet's theorem for the units imply now that $\mathscr{H}$ is finite. □

A quick remark on the earlier example. Lemma 2 explains why the correctly scaled equation of the tangent at $-S-T$ also gives a $\zeta^2 \cdot \zeta^2$ times a cube for $\kappa(P) = (\zeta, \zeta)$. We still need to justify how we get the equation for the curve $C_{(a,b)}$ for $(a,b) \in \mathscr{H} \times \mathscr{H}$. With the methods as above, one shows that one can scale the equation of the line through S and T to obtain a function $h_{S,T}$ such that $f_S \cdot f_T \cdot f_{-S-T} = h_{S,T}^3$ in $K(E)^{\times}$. In the example above this is $h_{S,T} = -X + Y - 4Z$. Hence there is a $\omega \in \mu[3]$ such that $h_{S,T}(P) = \omega\, abUVW$. One can adjust the variable U by ω to assume that $\omega = 1$. Now one has four linear forms, f_T, f_S, f_{-S-T} and $h_{S,T}$, hence they must be linearly dependent. In the example above, we find

$$C_{(a,b)}: \qquad a\,U^3 + (-5-3\zeta)\,b\,V^3 + (-2+3\zeta)\,a^2b^2\,W^3 + 6\,ab\,UVW = 0.$$

Remark. This method of finding an upper bound to the rank can be generalised to the case when $E[n]$ is no longer in $E(K)$. One can construct as above a map $\kappa\colon E(K)/n \to R^{\times}/n$ where R is the algebra $\mathrm{Maps}_{G_K}(E[n], \bar{K})$ which is such that $\mathrm{Spec}(R) = E[n]$. The algebra split into a product of number fields one for each Galois orbit in $E[n]$. However, the map is injective only if n is prime. See [24, 8] and the notes [29] of a short course by Stoll for how to do explicit n-descent in general.

Also we should add that this is only one way to work with the Selmer group; there is a second “indirect” method already used by Birch and Swinnerton-Dyer [2] and explained well in [9] which is the basis of the implementation for `mwrank`. This method uses the theory of (co)-invariants for forms and tries to find the curves $C_{(a,b)}$ associated to E directly. Apart from the computational use of this method, it is crucial in the work of Bhargava and Shankar [1].

2 Second lecture

Serge Lang (1927-2005)

2.1 Enters Galois cohomology

Let E be an elliptic curve over a field F; we no longer suppose $E[n] \subset E(F)$ now. We are going to use Galois cohomology $H^i(F,\cdot)$ now as in Appendix B in [28] or [21]. ☞ Exercise B.

Let $P \in E(F)$. As before, we pick $Q \in E(\bar{F})$ such that $nQ = P$. Then

$$\sigma \mapsto \xi_\sigma = \sigma(Q) - Q$$

represents a class in $H^1\big(F, E[n]\big)$:

$$\sigma(\xi_\tau) + \xi_\sigma - \xi_{\sigma\tau} = \sigma\big(\tau(Q) - Q\big) + \sigma(Q) - Q - \sigma\tau(Q) + Q = O.$$

A different choice of Q results in a different cocycle, but the difference is a coboundary. Hence there is a well-defined map

$$\kappa\colon E(K) \to H^1\big(F, E[n]\big).$$

Why do we denote it again by κ? Well, in the case that $E[n] \subset E(F)$ they are linked as follows. Pick a basis S, T of $E[n]$. As a consequence of what we did in the proof of Lemma 4, one can easily show that the diagram

$$\begin{tikzcd}
E(F) \arrow[r, "\kappa"] \arrow[d, "\kappa_S \times \kappa_T"'] & H^1\big(F, E[n]\big) \arrow[d, "\cong"] \\
F^\times/n \times F^\times/n \arrow[r, "\delta", "\cong"'] & H^1\big(F, \mu[n]\big) \times H^1\big(F, \mu[n]\big)
\end{tikzcd}$$

commutes, where the right hand vertical map is induced by $E[n] \to \mu[n] \times \mu[n]$ sending R to $\big(e_n(R,S), e_n(R,T)\big)$, and where the bottom horizontal map is the Kummer map from Hilbert's Satz 90.

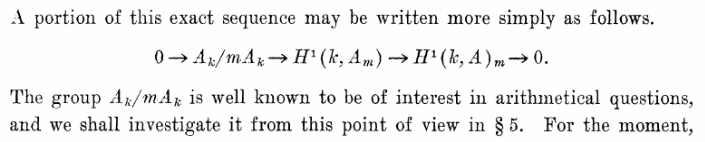
Back to the general case without assumption on $E[n]$. Let us be even more general: Suppose $\phi\colon E \to E'$ is an isogeny defined over F; the previous case is recovered when using $\phi = [n]$ of degree n^2. The long exact sequence for

$$\begin{tikzcd}
0 \arrow[r] & E[\phi] \arrow[r] & E \arrow[r, "\phi"] & E \arrow[r] & 0
\end{tikzcd}$$

gives the short exact sequence

$$\begin{tikzcd}
0 \arrow[r] & E'(F)/\phi\big(E(F)\big) \arrow[r, "\kappa"] & H^1\big(F, E[\phi]\big) \arrow[r, "\lambda"] & H^1(F, E)[\phi] \arrow[r] & 0,
\end{tikzcd}$$

which to my knowledge appeared first in by Lang and Tate.



A portion of this exact sequence may be written more simply as follows.

$$0 \to A_k/mA_k \to H^1(k, A_m) \to H^1(k, A)_m \to 0.$$

The group A_k/mA_k is well known to be of interest in arithmetical questions, and we shall investigate it from this point of view in § 5. For the moment,

from [15]

Suppose now that E is an elliptic curve over a number field K. Write res_v for the reduction of Galois cohomology from K to K_v and let κ_v denote the above map κ for the field K_v.

Definition. We define the **Selmer group** by

$$\mathrm{Sel}_\phi(E/K) = \left\{ \xi \in H^1\big(K, E[\phi]\big) \;\middle|\; \mathrm{res}_v(\xi) \in \mathrm{Im}\,\kappa_v \ \forall v \right\}$$

consisting of all elements in $H^1\big(K, E[\phi]\big)$ that are locally in the image of the Kummer map κ_v. Further we define the **Tate-Shafarevich** group $\text{Ш}(E/K)$ as the following kernel:

$$\text{Ш}(E/K) = \ker\left(H^1(K, E) \to \prod_v H^1(K_v, E) \right)$$

where the product runs over all places v in K.

The two are linked by the short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & E'(K)/\phi\big(E(K)\big) \arrow[r, "\kappa"] & \mathrm{Sel}_\phi(E/K) \arrow[r, "\lambda"] & \text{Ш}(E/K)[\phi] \arrow[r] & 0. \end{tikzcd}$$

Theorem 7

Let $\phi\colon E \longrightarrow E'$ be an isogeny defined over a number field K. Then the Selmer group $\mathrm{Sel}_\phi(E/K)$ is a finite group.

See Theorem X.4.2 in [28]. The crucial step is to show that the Selmer group lies inside the group $H^1(K, E[\phi]; \Sigma)$ of cocycles that are unramified outside Σ, which is a finite group that I like to denote by $H^1(\mathcal{O}_\Sigma, E[\phi])$ for some reason. In the case $E[n] \subset E(F)$ treated above this is the group $\mathscr{H} \times \mathscr{H}$ and $\mathscr{H}$ itself is $H^1(F, \mu[n]; \Sigma) = H^1(\mathcal{O}_\Sigma, \mu[n])$.

2.2 Geometric interpretation

Let E be an elliptic curve over a field F and let $\phi\colon E' \longrightarrow E$. The following interpretation is due to Châtelet [7].

Definition. A **ϕ-covering** of E defined over F is a morphism $\pi\colon C \longrightarrow E'$ defined over F of smooth projective curves such that there exists an isomorphism $\theta\colon C \dashrightarrow E$ defined over $\bar{F}$ such that $\pi = \phi \circ \theta$, i.e. the diagram

$$\begin{tikzcd} C \arrow[dr, "\pi"] \arrow[dd, dashed, "\theta"'] & \\ & E' \\ E \arrow[ur, "\phi"'] & \end{tikzcd}$$

commutes

In terms of twisting, a ϕ-covering is a twist of $\phi\colon E \longrightarrow E'$. In particular π is of the same degree as ϕ. See [8]. A morphism of ϕ-covering is a E'-morphism. The trivial ϕ-covering is $\phi\colon E \longrightarrow E'$ with $\theta = \mathrm{id}_E$.

Theorem 8

There is a bijection between $H^1\bigl(F, E[\phi]\bigr)$ and the set of isomorphism classes of ϕ-coverings of E defined over F.

The proof is analogous to Theorem X.3.6 in [28]. The bijection is set up as follows. First, if $\pi\colon C \longrightarrow E'$ is a ϕ-covering and $\sigma \in G_F$, then one can show that the map $\sigma(\theta)\circ\theta^{-1}\colon E \longrightarrow E$ is equal to the translation by a point $\xi_\sigma \in E[\phi]$. This is, surprise, surprise, a 1-cocycle.

Conversely, using a given cocycle ξ one can define a new G_F-action on the function field $F(E)^\times$ by setting $(\sigma * f)(P) = \sigma(f)(P+\xi_\sigma)$. The new field is the function field of a smooth projective curve C over F with a map to E. The rest of the proof is checking that everything works.

The curve C inherits an action by E and it can be viewed as a principal homogeneous space as in Section X.3 in [28]. This explains the map $\lambda\colon H^1\bigl(F, E[\phi]\bigr) \longrightarrow H^1\bigl(F, E\bigr)[\phi]$. If $P \in E'(F)$, then $\kappa(P) \in H^1\bigl(F, E[\phi]\bigr)$ is represented by the ϕ-covering $\tau_P \circ \phi\colon E \longrightarrow E'$ where τ_P is the translation by P on E'. In particular, an ϕ-covering is in the image of $E'(F)/\phi(E(F))$ if and only if $C(F) \neq \varnothing$.

In the starting example, the curve $C_{(a,b)}$ associated to a general $(a,b) \in \mathscr{H}\times\mathscr{H}$ comes with the degree 3 map $\pi\colon C_{(a,b)} \longrightarrow E$ sending $(U:V:W)$ to

$$\Bigl(-2a\,U^3 - 2\zeta b\,V^3 + (2+2\zeta)a^2b^2\,W^3 : \\ -a\,U^3 + (11+3\zeta)b\,V^3 + (8-3\zeta)a^2b^2\,W^3 : \\ a\,U^3 + (-1-\zeta)b\,V^3 + \zeta a^2b^2\,W^3\Bigr).$$

It is a $\hat\phi$-covering for the isogeny $\hat\phi$ dual to $\phi\colon E \longrightarrow E'$ which has $T-S$ in the kernel. These were the sort of descents that Selmer did in his work [27] in the 50ies.

2.3 Interpretation as extensions

Let ξ be a cocycle representing an element in $H^1\bigl(F, E[n]\bigr)$. We are going to associate to ξ a short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \mu[n] \arrow[r] & W_\xi \arrow[r] & E[n] \arrow[r] & 0 \end{tikzcd}$$

of G_F-modules. As a group W_ξ is just the direct sum $\mu[n]\oplus E[n]$, but the Galois action is twisted as follows:

$$\sigma(\zeta, T) = \Bigl(\sigma(\zeta)\cdot e_n\bigl(\xi_\sigma, \sigma(T)\bigr),\ \sigma(T)\Bigr)$$

for all $\sigma \in G_F$, $\zeta \in \mu[n]$ and $T \in E[n]$.

Lemma 9

This defines a group action of G_F on W_ξ.

Proof. Let σ and $\tau \in G_F$. Then

$$\begin{aligned}\sigma\big(\tau(\zeta, T)\big) &= \sigma\Big(\tau(\zeta)\cdot e_n\big(\xi_\tau, \tau(T)\big),\ \tau(T)\Big)\\ &= \Big(\sigma\big(\tau(\zeta)\big)\cdot\sigma\big(e_n\big(\xi_\tau,\tau(T)\big)\big)\cdot e_n\big(\xi_\sigma,\sigma(\tau(T))\big),\ \sigma\big(\tau(T)\big)\Big)\\ &= \Big(\sigma\tau(\zeta)\cdot e_n\big(\sigma(\xi_\tau),\sigma\tau(T)\big)\cdot e_n\big(\xi_\sigma,\sigma\tau(T)\big),\ \sigma\tau(T)\Big)\\ &= \Big(\sigma\tau(\zeta)\cdot e_n\big(\sigma(\xi_\tau)+\xi_\sigma,\sigma\tau(T)\big),\ \sigma\tau(T)\Big)\\ &= \Big(\sigma\tau(\zeta)\cdot e_n\big(\xi_{\sigma\tau},\sigma\tau(T)\big),\ \sigma\tau(T)\Big) = (\sigma\tau)(\zeta,T)\end{aligned}$$ □

Two extensions of $E[n]$ by $\mu[n]$ are isomorphic if there is an isomorphism of exact sequences as in

$$\begin{tikzcd} 0 \arrow[r] & \mu[n] \arrow[r] \arrow[d, "\mathrm{id}"] & W_1 \arrow[r] \arrow[d, "\cong"] & E[n] \arrow[r] \arrow[d, "\mathrm{id}"] & 0 \\ 0 \arrow[r] & \mu[n] \arrow[r] & W_2 \arrow[r] & E[n] \arrow[r] & 0 \end{tikzcd}$$

Proposition 10

There is a bijection between $H^1(F, E[n])$ and isomorphism classes of extensions of G_F-modules of $E[n]$ by $\mu[n]$.

The set in the theorem is usually denoted by $\mathrm{Ext}^1_{G_F}(E[n], \mu[n])$. One can replace $\mu[n]$ by $\mathbb{G}_m$ if one wishes as in [8].

Lemma 11

Let $\xi \in H^1(F, E[n])$. The connecting homomorphism

$$\partial\colon H^1(F, E[n]) \to H^2(F, \mu[n]) = \mathrm{Br}(F)[n]$$

sends a class represented by the cocycle η to the 2-cocycle

$$(\xi \cup \eta)_{\sigma,\tau} = e_n\big(\xi_\sigma, \sigma(\eta_\tau)\big).$$

This is called the cup-pairing

$$\cup\colon H^1(F, E[n]) \times H^1(F, E[n]) \to \mathrm{Br}(F)[n].$$

2.4 Local dualities

John Tate (1925–2019)

Theorem 12

Let E be an elliptic curve over a p-adic field K_v and let $n > 1$. Then the pairing

$$\cup\colon H^1(K_v, E[n]) \times H^1(K_v, E[n]) \longrightarrow \mathrm{Br}(K_v)[n] \xrightarrow[\cong]{\mathrm{inv}_v} {}^{\mathbb{Z}}/_{n\mathbb{Z}}$$

is a perfect, symmetric bilinear pairing.

This result is due to Tate [32] and it holds in general for G_{K_v}-modules which have a non-degenerate pairing $M \times M' \longrightarrow \mu[n]$, like the Weil pairing. See also [21, 7.2.6].

If $E[n] \subset E(K_v)$ and ξ corresponds to $(a, b) \in K_v^\times/n \times K_v^\times/n$ and η to (a', b') for a choice S and T of a basis of $E[n]$, then I believe that

$$e(S,T)^{\xi \cup \eta} = \{a, b'\} \cdot \{a', b\}$$

where $\{,\}$ is the Hilbert norm symbol in K_v. See [30]. For the general case when $E[n] \not\subset E(K_v)$ see Section 2 in [10].

There is another pairing also due to Tate

$$\langle\ ,\ \rangle\!\rangle_v : E(K_v)/n \times H^1(K_v, E)[n] \longrightarrow \mathrm{Br}(K_v)[n] \cong {}^{\mathbb{Z}}/_{n\mathbb{Z}}$$

that we construct now.

First, if $D = \sum_i m_i(P_i)$ is a divisor of degree 0 on a curve C and $f \in F(C)^\times$ whose divisor has disjoint support from that of D, then we write

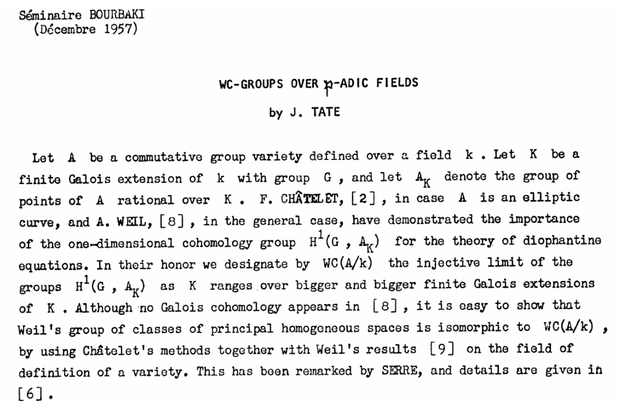
$$f(D) = \prod_i f(P_i)^{m_i}$$

which is invariant under multiplying f by a constant.

We are given $P \in E(K_v)$ and ξ a cocycle in $H^1(K_v, E)$. Pick a K_v-rational divisor of degree 0, like $(P) - (O)$, whose sum is P. Then, for each $\sigma \in G_{K_v}$, we pick a divisor $B_\sigma \in \mathrm{Div}^0(E)$ with sum ξ_σ whose support is disjoint from the support of D. Then there is a function $f_{\sigma,\tau}$ with divisor $\sigma(B_\tau) + B_\sigma - B_{\sigma\tau}$ for each pair $\sigma, \tau \in G_{K_v}$. We set $\langle P, \xi \rangle\!\rangle_v \in \mathrm{Br}(K_v)$ to be equal to the 2-cocycle sending (σ, τ) to $f_{\sigma,\tau}(P)^{-1}$.

Theorem 13

$\langle\ ,\ \rangle\!\rangle_v$ is a perfect bilinear pairing.



Séminaire BOURBAKI
(Décembre 1957)

WC-GROUPS OVER $\mathfrak{p}$-ADIC FIELDS

by J. TATE

Let A be a commutative group variety defined over a field k . Let K be a finite Galois extension of k with group G , and let A_K denote the group of points of A rational over K . F. CHÂTELET, [2] , in case A is an elliptic curve, and A. WEIL, [8] , in the general case, have demonstrated the importance of the one-dimensional cohomology group $H^1(G , A_K)$ for the theory of diophantine equations. In their honor we designate by WC(A/k) the injective limit of the groups $H^1(G , A_K)$ as K ranges over bigger and bigger finite Galois extensions of K . Although no Galois cohomology appears in [8] , it is easy to show that Weil's group of classes of principal homogeneous spaces is isomorphic to WC(A/k) , by using Châtelet's methods together with Weil's results [9] on the field of definition of a variety. This has been remarked by SERRE, and details are given in [6] .

from [32]

One can show that the two pairings are compatible in the sense that

$$\langle \kappa(P), \xi \rangle_v = \langle P, \lambda(\xi) \rangle\!\rangle_v \quad \forall P \in E(K_v), \xi \in H^1(K_v, E[n]).$$

See for instance Proposition 2.1 in [11]. ☞ Exercise C.

Other local results that can be of use:

$$\begin{aligned} H^2(K_v, E[n]) &\cong \operatorname{Hom}(E(K_v)[n], \mathbb{Z}/n) \\ H^i(K_v, E[n]) &= 0 \qquad \text{for all } i \geqslant 3 \\ H^2(K_v, E) &= 0 \end{aligned}$$

If E has good reduction and n is coprime to the residue characteristic, then the image of κ can also be described as

$$H^1_{\mathrm{ur}}(K_v, E[n]) = \ker\Big(H^1(K_v, E[n]) \to H^1(I_v, E[n])\Big)$$

where I_v is the inertia group. Instead the description of the image of κ for n dividing the residual characteristic in terms of $E[n]$ alone is harder, but possible using p-adic Hodge theory. As a consequence, it is possible to define Selmer groups for any Galois module. This is parallel to the fact that the L-function of E/K is also determined by the action of G_K on the torsion points alone.

2.5 Global dualities

For a number field K, we have an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \operatorname{Br}(K) \arrow[r] & \bigoplus_v \operatorname{Br}(K_v) \arrow[r, "\sum \mathrm{inv}_v"] & {}^{\mathbb{Q}}/_{\mathbb{Z}} \arrow[r] & 0. \end{tikzcd}$$

Lemma 14

Let ξ and η be two elements in $\mathrm{Sel}_n(E/K)$. Then $\xi \cup \eta = 0 \in \mathrm{Br}(K)$.

Proof. Let W_ξ be the G_K-module extending $E[n]$ by $\mu[n]$ corresponding to ξ. Consider the commuting digram

$$\begin{tikzcd}
H^1(K, E[n]) \arrow[r, "\xi\cup\cdot"] \arrow[d] & \mathrm{Br}(K) \arrow[d, tail] \\
\prod H^1(K_v, E[n]) \arrow[r, "\mathrm{res}_v(\xi)\cup\cdot"] & \prod_v \mathrm{Br}(K_v)
\end{tikzcd}$$

The image of η in the bottom right corner for each finite v is

$$\mathrm{res}_v(\eta) \cup \mathrm{res}_v(\xi) = \langle \mathrm{res}_v(\eta), \mathrm{res}_v(\xi)\rangle_v = \langle\!\langle Q_v, \lambda\,\mathrm{res}_v(\xi)\rangle\!\rangle_v = \langle\!\langle Q_v, 0\rangle\!\rangle_v = 0$$

where $\kappa(Q_v) = \mathrm{res}_v(\eta)$. Since the right hand map is injective, we conclude that $\xi \cup \eta = 0$. □

Oh, well, that is disappointing. But it may explain why the Cassels-Tate pairing is a little harder to define.

Ian Cassels (1922–2015)

Let ξ and η be two elements in $\text{Ш}(E/K)[n]$. We can lift ξ to an element in $\mathrm{Sel}_n(E/K)$ and represent it as an n-covering $C \longrightarrow E$. Since C is isomorphic to E over $\bar{K}$, we have $\mathrm{Pic}^0(C) \cong E$. For each $\sigma \in G_K$, pick a divisor $B_\sigma \in \mathrm{Div}^0(C)$ representing the class corresponding to $\eta_\sigma \in E[n]$. There is a function $f_{\sigma,\tau} \in K(C)^\times$ with divisor $\sigma(B_\tau) + B_\sigma - B_{\sigma\tau}$. Since $\xi \in \text{Ш}(E/K)$, the curve C has a K_v-rational point Q_v for all v. Define the pairing

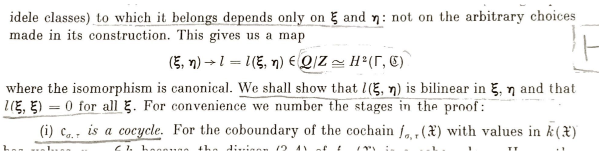
$$\begin{aligned}
[\cdot,\cdot]\colon \text{Ш}(E/K)[n] \times \text{Ш}(E/K)[n] &\longrightarrow {}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \\
(\xi, \eta) &\longmapsto \sum_v \mathrm{inv}_v\bigl(\sigma, \tau \mapsto f_{\sigma,\tau}(Q_v)\bigr) \in {}^{\mathbb{Q}}\!/_{\mathbb{Z}}
\end{aligned}$$

Note it is a bit surprising that the choice of Q_v does not matter, but that is because $\mathrm{res}_v(\eta) = 0$ implies that f comes from a constant 2-cocycle in $\mathrm{Br}(K_v)$.

Theorem 15

This pairing $[\cdot,\cdot]$ is bilinear and alternating. The kernel on each side is $n\text{Ш}(E/K)$. It extends to a pairing $\text{Ш}(E/K)\times\text{Ш}(E/K) \longrightarrow {}^{\mathbb{Q}}\!/_{\mathbb{Z}}$ whose kernel is the subgroup of divisible elements.

This is due to Cassels [4] (IV) and it was generalised by Tate [31]. See also [21, 11, 12, 20] and [5, 10] for concrete implementations.


idele classes) to which it belongs depends only on ξ and η: not on the arbitrary choices made in its construction. This gives us a map

$$(\xi, \eta) \to l = l(\xi, \eta) \in Q/Z \cong H^2(\Gamma, \mathfrak{C})$$

where the isomorphism is canonical. We shall show that $l(\xi, \eta)$ is bilinear in ξ, η and that $l(\xi, \xi) = 0$ for all ξ. For convenience we number the stages in the proof:

(i) $\mathfrak{c}_{\sigma,\tau}$ *is a cocycle.* For the coboundary of the cochain $f_{\sigma,\tau}(\mathfrak{X})$ with values in $\bar{k}(\mathfrak{X})$

from [4] IV

Another important result within global cohomology is an exact sequence due to Cassels [4] (VII), which was generalised by Poitou [23] and Tate [31], see [21, 8.6.13].

Theorem 16

Let E/K be an elliptic curve and $n > 1$. Let Σ be a finite set containing all bad places, all those dividing n and all infinite places. Consider the map

$$\mathrm{res}\colon \operatorname{Sel}_n(E/K) \to \bigoplus_{v\in\Sigma} E(K_v)/n.$$

The image of this map res is dual to the cokernel of $H^1(\mathcal{O}_\Sigma, E[n]) \to \bigoplus_{v\in\Sigma} H^1(K_v, E)[n]$ under the pairing $\langle\cdot,\cdot\rangle\!\rangle_v$. The kernel of res is dual to the kernel of the restriction $H^2(\mathcal{O}_\Sigma, E[n]) \to \bigoplus_{v\in\Sigma} H^2(K_v, E[n])$.

Usually this is summarise in one long exact sequence of finite groups

$$\begin{tikzcd}
0 \arrow[r] & E(K)[n] \arrow[r] & \bigoplus_{v\in\Sigma} E(K_v)[n] \arrow[r] & H^2(\mathcal{O}_\Sigma, E[n])^\vee \arrow[dll, rounded corners] & \\
 & \operatorname{Sel}_n(E/K) \arrow[r] & \bigoplus_{v\in\Sigma} E(K_v)/n \arrow[r] & H^1(\mathcal{O}_\Sigma, E[n])^\vee \arrow[r] & \operatorname{Sel}_n(E/K)^\vee \arrow[r] & 0
\end{tikzcd}$$

where $A^\vee = \operatorname{Hom}(A, {}^{\mathbb{Q}}\!/\!_{\mathbb{Z}})$ is the Pontryagin dual.

There are many interesting applications of these duality statements.

- Cassels originally used it to verify a conjecture by Selmer saying that the "second descent" reduces the rank bound by an even number. More precisely, if $\phi\colon E \to E'$ is an isogeny of degree p defined over a number field. Then the image of the map δ in

$$\begin{tikzcd}
0 \arrow[r] & E(K)[\phi] \arrow[r] & E(K)[n] \arrow[r] & E'(K)[\hat\phi] \arrow[dll, rounded corners] & \\
 & \operatorname{Sel}_\phi(E/K) \arrow[r] & \operatorname{Sel}_n(E/K) \arrow[r] & \operatorname{Sel}_{\hat\phi}(E'/K) \arrow[dll, rounded corners, "\delta"] & \\
 & Ш(E/K)/\hat\phi(Ш(E'/K)) \arrow[r] & Ш(E/K)/n \arrow[r] & Ш(E'/K)/\phi(Ш(E/K)) \arrow[r] & 0
\end{tikzcd}$$

  has even dimension.

- Cassels showed that the Birch and Swinnerton-Dyer conjecture is invariant under isogenies, which was among the first theoretical results supporting the conjecture.

- Also the fact that the order of $Ш(E/K)$ should be a square lead Birch and Swinnerton-Dyer to include its order in the leading term formula, despite only having some knowledge about its 2-torsion part.

- The pairing is also useful in explicit computation as it allows to verify that $Ш(E/K)[p]$ is non-trivial and hence to lower the rank bound without having to do a p^2-descent.

- In fact all known non-trivial elements of $Ш(E/K)[n]$ are ultimately proven to have no rational points in this manner as the Brauer-Manin obstruction is a reformulation of this method in the case of elliptic curves.

- Not surprisingly the parity results, showing that the parity of the ranks of the Selmer groups agree with the analytic rank module 2, rely on the duality.

- Generalisations are crucial in the method of Euler systems and in the modularity theorem in the Taylor-Wiles method.

- . . .

3 Third lecture

3.1 Local norms

Let K_v be a p-adic field and let L_w/K_v be a finite Galois extension of group G. Let E/K_v be an elliptic curve. Analogous to class field theory, we may ask what is

$$D_v = E(K_v)/N\bigl(E(L_w)\bigr).$$

Using Tate's modified group cohomology, we may write $D_v = \hat{H}^0\bigl(G, E(L_w)\bigr)$.

Proposition 17

Assume that L_w/K_v is unramified and that $d = |G|$ is coprime to 6. Then D_v is a cyclic group of order $\gcd(d, c_v)$ where c_v is the Tamagawa number of E/K_v. Moreover the group $E^0(K_v)$ of points with good reduction are all in the image of the norm map.

Proof. Since the extension is unramified the type of reduction and the Tamagawa number will not change in the extension.

By Theorem 2 on page 21 in [6], $\hat{H}^0(G, \mathcal{O}_w) = 0$ as the trace map $\mathcal{O}_w \to \mathcal{O}_v$ is surjective on the ring of integers in unramified extensions. There is an integer $r > 0$ such that $\hat{E}(\mathfrak{m}_w^r)$ is isomorphic to $\mathcal{O}_w$ as a G-module; and hence $\hat{H}^0\bigl(G, \hat{E}(\mathfrak{m}_w^r)\bigr) = 0$. Also $\hat{H}^0\bigl(G, \mathbb{F}_w\bigr)$ is trivial, so the norm map is surjective on the quotient of $\hat{E}(\mathfrak{m}_w^{r-1})$ by $\hat{E}(\mathfrak{m}_w^r)$. We conclude that $\hat{H}^0\bigl(G, \hat{E}(\mathfrak{m}_v^{r-1})\bigr) = 0$ and, by induction, that $\hat{H}^0\bigl(G, \hat{E}(\mathfrak{m}_w)\bigr) = 0$.

To conclude that the norm map $E^0(L_w) \to E^0(K_v)$ is surjective, we only need to show that $\hat{H}^0\bigl(G, \tilde{E}^0(\mathbb{F}_w)\bigr)$ is trivial. If the reduction is bad, it follows because trace and norm are surjective on finite fields. If the reduction is good, it is a consequence of a theorem by Schmidt [25], later generalised by Lang [14], that the norm is surjective. But ☞ Exercise E and Exercise X.6 in [28].

Therefore we have $\hat{H}^0\bigl(G, E(L_w)\bigr) = \hat{H}^0\bigl(G, E(L_w)/E^0(L_w)\bigr)$. If the reduction is additive or non-split multiplicative, then this is zero, because the order of the group $E(L_w)/E^0(L_w)$ is the Tamagawa number which is then a divisor or 12 and hence coprime to the order of G. In the split multiplicative case, it is cyclic of order c_v. Since the action of G is trivial on it, the group $\hat{H}^0\bigl(G, E(L_w)\bigr)$ is cyclic of order $\gcd\bigl(|G|, c_v\bigr)$. □

From the proof one sees that it isn't hard to extend this sort of computation to many more situations. If d is divisible by 3, for instance, we only have to exclude that the reduction is of type IV or IV*.

Lemma 18

Suppose L_w/K_v is totally ramified, that E has good reduction, and that $\gcd(|G|, p) = 1$, i.e., it is tamely ramified. Then D_v is isomorphic to $\tilde{E}(\mathbb{F}_v)/|G|$.

Proof. The group $\hat{E}(\mathfrak{m}_w)$ is a pro-p-group, so $\hat{H}^i\bigl(G, \hat{E}(\mathfrak{m}_v)\bigr) = 0$ as we assumed p to be coprime to the order of G. Since the reduction is good, we get $D_v \cong \hat{H}^0\bigl(G, \tilde{E}(\mathbb{F}_w)\bigr)$. The extension is totally ramified, meaning $\mathbb{F}_w = \mathbb{F}_v$ and G acts trivially on $\tilde{E}(\mathbb{F}_w)$ completes the proof. □

Now to the totally and wild case which is a result due to Lubin and Rosen [16] and much harder to prove.

Proposition 19

Assume L_w/K_v is a totally ramified extension of p-adic fields whose Galois group has order $d = p^m$. Suppose that the curve E/K_v has good ordinary reduction. Then D_v is a finite group whose order divides $\left(\#\tilde{E}(\mathbb{F}_v)[p^\infty]\right)^2$.

3.2 Selmer groups as Galois modules

Let E/K be an elliptic curve over a number field. Let L/K be a Galois extension with group G, which is a p-group for a prime $p > 3$. Let Σ be a finite set of places as before, but impose that also all ramified places belong to Σ. We suppose

$$E(K)[p] = 0.$$

Lemma 20

$E(L)[p] = 0$.

Proof. Assume $E(L) \neq \{O\}$. The size of G-orbits on the set $E(L)[p]$ must be powers of p. The orbit $\{O\}$ is of size 1. Since the order of the set $E(L)[p]$ is a multiple of p, there has to be other fixed points in $E(L)[p]$. But that contradicts the assumption $E(K)[p] = 0$. □

It is obvious that $E(L)^G = E(K)$. But beware:

Proposition 21

For any n that is a power of p, we have an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & E(K)/n \arrow[r, "\alpha"] & (E(L)/n)^G \arrow[r] & H^1(G, E(L))[n] \arrow[r] & 0. \end{tikzcd}$$

Proof. By Lemma 20, the sequence

$$\begin{tikzcd} 0 \arrow[r] & E(L) \arrow[r, "{[n]}"] & E(L) \arrow[r] & E(L)/n \arrow[r] & 0 \end{tikzcd}$$

is exact, now the long exact sequence concludes the proof. □

Theorem 22

Let L/K be a Galois extension whose degree is a power of p and let n be a power of p and suppose $E(K)[p] = 0$. Then the map

$$\beta\colon \operatorname{Sel}_n(E/K) \longrightarrow \operatorname{Sel}_n(E/L)^G$$

is injective and the cokernel is dual to the cokernel of

$$\operatorname{Sel}_n(E/K) \longrightarrow \bigoplus_{v\in\Sigma} E(K_v)/n \longrightarrow \bigoplus_{v\in\Sigma} D_v/n.$$

Proof. It follows from the inflation–restriction–transgression sequence that we have an isomorphism

$$H^1\big(\mathcal{O}_\Sigma, E[n]\big) \cong H^1\big(\mathcal{O}_{\Sigma(L)}, E[n]\big)^G.$$

where $\Sigma(L)$ is the set of places in L above those in Σ. Consider the diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Sel}_n(E/L)^G \arrow[r] & H^1\big(\mathcal{O}_{\Sigma(L)}, E[n]\big)^G \arrow[r] & \Big(\bigoplus_w H^1(L_w, E)[n]\Big)^G & \\
0 \arrow[r] & \mathrm{Sel}_n(E/K) \arrow[r] \arrow[u, "\beta"] & H^1\big(\mathcal{O}_\Sigma, E[n]\big) \arrow[r] \arrow[u, "\cong"] & \bigoplus_v H^1(K_v, E)[n] \arrow[r, "\mathrm{res}^\vee"] \arrow[u, "\oplus\rho_v"] & \mathrm{Sel}_n(E/K)^\vee
\end{tikzcd}$$

It follows that β is injective. The local restriction map $\rho_v \colon H^1\big(K_v, E\big[n\big]\big) \to H^1\big(L_w, E\big)[n]$ is dual to the norm map $E(L_w)/n \to E(K_v)/n$. So the kernel of $\oplus_v \rho_v$ is $\bigoplus D_v/n$. A little diagram chase similar to the snake lemma, shows that the cokernel of β is dual to the cokernel of the map from $\mathrm{Sel}_n(E/K)$ to the group $\bigoplus D_v/n$. □

Let us deduce some consequences in the case that G is cyclic of order p and $n = p$. First $H^1\big(G, E(L)\big) = H^1\big(G, E(L) \otimes \mathbb{Z}_p\big)$. It has the advantage that $E(L) \otimes \mathbb{Z}_p$ is a free $\mathbb{Z}_p$-module of the same rank as $E(L)$.

It is known that any free $\mathbb{Z}_p$-module with a G-action is a direct sum of copies of the following three indecomposable $\mathbb{Z}_p[G]$-lattices:

- $\mathbb{Z}_p$ with trivial action,
- the group ring $\mathbb{Z}_p[G]$, and
- the augmentation kernel $A = \ker\big(\mathbb{Z}_p[G] \to \mathbb{Z}_p\big)$.

In particular although $\mathbb{Z}_p \oplus A$ and $\mathbb{Z}_p[G]$ have both rank p, they are not isomorphic modules: Indeed $H^1\big(G, \mathbb{Z}_p\big) = H^1\big(G, \mathbb{Z}_p[G]\big) = 0$ but $H^1\big(G, A\big) = {}^{\mathbb{Z}}/_{p\mathbb{Z}}$. Hence if $E(L) \otimes \mathbb{Z}_p = \mathbb{Z}_p^a \oplus A^b \oplus \mathbb{Z}_p[G]^c$, then $H^1\big(G, E(L)\big) = \mathbb{F}_p^b$ and $a + b = \operatorname{rank} E(K)$.

Now consider the diagram

$$\begin{tikzcd}
0 \arrow[r] & \Big(E(L)/p\Big)^G \arrow[r] & \mathrm{Sel}_p(E/L)^G \arrow[r] & \Big(Ш(E/L)[p]\Big)^G & \\
0 \arrow[r] & E(K)/p \arrow[r] \arrow[u, "\alpha"] & \mathrm{Sel}_p(E/K) \arrow[r] \arrow[u, "\beta"] & Ш(E/K)[p] \arrow[r] \arrow[u, "\gamma"] & 0
\end{tikzcd}$$

and the snake lemma provides the exact sequence

$$0 \longrightarrow \ker\gamma \longrightarrow H^1\big(G, E(L)\big) \longrightarrow \operatorname{coker}\beta \longrightarrow \operatorname{coker}\gamma.$$

In particular if an element of $Ш(E/K)$ capitulates in L/K then a component isomorphic to A must appear in $E(L) \otimes \mathbb{Z}_p$.

Proposition 23

Suppose L/K is cyclic of degree p. If $E(K)$ has rank 0 and $Ш(E/K)[p]$ is trivial, then the rank of $E(L)$ is at most $(p-1)\cdot\sum_v \dim_{\mathbb{F}_p} D_v$.

See ☞ Exercise D.

Proof. First $D_v = \hat{H}^0\big(G, E(L_w)\big)$ is p-torsion so $D_v/p = D_v$. By assumption the kernel of γ must be trivial and, $a+c=0$. Hence the dimension b of $H^1\big(G, E(L)\big)$ in the above exact sequence is at most $\sum_v \dim_{\mathbb{F}_p} D_v$. Therefore $E(L) \cong A^b$ has rank bounded by $(p-1)\sum_v \dim_{\mathbb{F}_p} D_v$. □

Corollary 24

Let E be an elliptic curve over $\mathbb{Q}$ and let p be a prime such that E has rank 0, there is no p-torsion in $Ш(E/\mathbb{Q})$ or in $E(\mathbb{Q})$, and no Tamagawa number is divisible by p. Then $E(L)$ has rank 0 for any cyclic extension L/K of degree p, provided E has good ordinary reduction with $p \nmid \#\tilde{E}(\mathbb{F}_v)$ at all ramified places v.

There are plenty of examples now. For instance the curve with Cremona label 11a1 must have rank zero over $\mathbb{Q}(\zeta_{107})^+$. That fact can also be deduced from Iwasawa theory using modular symbols, instead any sort of descent would be infeasible.

The map β also appears in Iwasawa theory. The following is known as the control theorem, originally due to Mazur [19].

Theorem 25

Let L/K be a $\mathbb{Z}_p$-extension with group Γ and suppose E has good ordinary reduction at all ramified places. Then

$$\varinjlim_m \mathrm{Sel}_{p^m}(E/K) \to \varinjlim_m \mathrm{Sel}_{p^m}(E/L)^\Gamma$$

has a finite kernel and cokernel.

Proof. In the case $E(K)[p]=0$, this follows from Theorem 22 together with the fact that $\varinjlim D_v/p^m$ is finite and bounded for all places and all intermediate extensions in L/K, thanks to Propositions 17 and 19. The case $E(K)\neq 0$ is not much harder, but omitted here. □

3.3 p-adic heights

Let L/K be a Galois extension with an abelian group G. Let E/K be an elliptic curve. We will construct a pairing on parts of the Selmer group with values in G. Let $n>1$, though only divisors of $|G|$ are interesting.

Let $\xi, \eta \in \mathrm{Sel}_n(E/K)$. While ξ can be arbitrary, we have to assume some conditions on η: Pick for each v, a point $Q_v \in E(K_v)$ such that $\kappa(Q_v) = \mathrm{res}_v(\eta)$.

We will suppose that Q_v is a norm from $E(L_w) \to E(K_v)$ for all w. By Proposition 17 this only imposes restrictions on ramified and bad primes. We write $\mathrm{Sel}_n^0(E/K)$ for the subgroup of $\mathrm{Sel}_n(E/K)$ of η that satisfy this condition.

Associate to ξ the extension W_ξ. Consider the following diagram

$$\begin{tikzcd}
H^1(K,\mu[n]) \arrow[r] \arrow[d] & H^1(K,W_\xi) \arrow[r] \arrow[d] & H^1(K,E[n]) \arrow[r] \arrow[d] & \mathrm{Br}(K)[n] \\
\prod_v H^1(K_v,\mu[n]) \arrow[r] & \prod H^1(K_v,W_\xi) \arrow[r] & \prod H^1(K_v,E[n]) \arrow[r] & 0
\end{tikzcd}$$

where the products run over all places in v (though a large enough finite set would be enough). The zero at the bottom right comes from Theorem 13 as $\lambda \circ \mathrm{res}_v(\xi) = 0$ as in the proof of Lemma 14. From that Lemma 14 we see that η can be lifted to an element $\tilde{\eta} \in H^1(K, W_\xi)$. By assumption, we can find a point $R_w \in E(L_w)$ for every place w in L such that $N(R_w) = Q_v$. We can lift $\kappa(R_w)$ to $\zeta_w \in H^1(L_w, W_\xi)$. The map corresponding to the norm map on cohomology is the corestriction $\mathrm{cor}\colon H^1(L_w,\cdot) \to H^1(K_v,\cdot)$. By construction $\mathrm{res}_v(\tilde{\eta}) - \mathrm{cor}(\zeta_w)$ lies in the image of the first map in the bottom row. Let $\epsilon_v \in H^1(K_v,\mu[n]) \cong K_v^\times/n$ be a lift. One can show that this yields an idèle ϵ, we define $[\![\xi,\eta]\!] = \psi_G(\epsilon)$ where $\psi_G\colon \mathbb{A}_K^\times \to G$ is the reciprocity map from global class field theory.

Lemma 26

The above defines a bilinear pairing

$$[\![\cdot,\cdot]\!]\colon \mathrm{Sel}_n(E/K) \times \mathrm{Sel}_n^0(E/K) \longrightarrow G/n.$$

It is symmetric on $\mathrm{Sel}_n^0(E/K)$.

Here is a first special case: Suppose L/K is the Hilbert class field; in which case G identifies with the class group of K. For a point $P \in E(K)$, we can write $x(P)\,\mathcal{O}_K$ as $\mathfrak{a}_P \cdot \mathfrak{e}_P^{-2}$ for integral ideals $\mathfrak{a}_P$ and $\mathfrak{e}_P$.

Proposition 27

Suppose L/K is the Hilbert class field. Let $P, Q \in E(K)$ and suppose that Q has good reduction at all bad places. Then there exists an ideal $\mathfrak{d}$ such that $[\![\kappa(P),\kappa(Q)]\!]$ is the class of the ideal $\mathfrak{e}_{P+Q}\,\mathfrak{e}_P^{-1}\,\mathfrak{e}_Q^{-1}\mathfrak{d}$ in $\mathrm{Cl}(K)/n$.

(This should be true, but maybe I am off by a factor ±1 or ±2.) The argument to show this is to notice that the local contribution in this pairing for all finite places is equal to the exponential of the local height function $\hat{\lambda}_{E,v}$ as discussed in Silverman's lectures. This is linked directly to the denominator ideal of x. The ideal $\mathfrak{d}$ can taken to be trivial if a global minimal equation exists. See [13].

Since everything in sight splits when n is the product of coprime integers, we may suppose that $n = p^m$ for some prime p and $m \geqslant 1$ and that L/K is an extension of degree p^m. In fact, we choose L/K to be the subextension of that degree in a $\mathbb{Z}_p$-extension L_∞/K. Such an extension is unramified outside the places above p. We will now suppose that E has good ordinary reduction at all those ramified places. Let $E^\bullet(K)$ be the subgroup of $E(K)$ of all points that have good reduction everywhere and that are sufficiently close to O at all ramified places so that it will lie in the image of the local norm map for the completion of L_∞. By Proposition 19, this is a finite index subgroup.

Proposition 28

Suppose L/K is inside a $\mathbb{Z}_p$-extension, E and $n = p^m$ as above. Then the pairing $[\![\cdot,\cdot]\!] \colon E(K) \times E^\bullet(K) \longrightarrow G$ extends to the p-adic height pairing $E(K) \times E(K) \to \mathbb{Q}_p$ for this $\mathbb{Z}_p$-extension.

The pairings are compatible and glue to a pairing on $E(K) \times E^\bullet(K)$ with values in $\operatorname{Gal}(L_\infty/K) \approx \mathbb{Z}_p$. Since $E^\bullet(K)$ has finite index, one can linearly extend it to a pairing with values in $\mathbb{Q}_p$. If the extension is the unique cyclotomic $\mathbb{Z}_p$-extension of K, then the local contributions at unramified places is the p-adic analogue of the function $\hat{\lambda}_{E,v}$, meaning that all appearances of $\log$ there are replaced by the p-adic logarithm $\log_p$. The contribution at ramified places is the p-adic logarithm composed with a canonical p-adic σ-function. The ordinary assumption is crucial here as explained in [17].

The regulator of this pairing appears in the formulation of the leading term formula for the p-adic L-function as discussed in [18]. The Galois cohomological description of this analytic height pairing was first given by Schneider [26] and Perrin-Riou [22]. See [3] for how to write the usual real-valued height pairing using extensions in a very similar way.

4 Exercises

A) Prove lemma 2 using a function $h_{S,T}$ with divisor $(S+T) - (S) - (T) + (O)$.

B) (i) Let G be a finite group and let M be a free $\mathbb{Z}$-module with an linear action by G such that $M^G = 0$. Show that $H^1(G, M) = \left(M \otimes {}^{\mathbb{Q}}\!/_{\mathbb{Z}}\right)^G$.

(ii) Use this to calculate $H^1(G, M)$ when $G = D_4$ is the dihedral group of order 8 and M is $\mathbb{Z}^2$ with the obvious action, say by the matrices $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$.

(iii) Let A be the set of elements $\sum_{g\in G} a_g\, g \in \mathbb{Z}[G]$ such that $\sum_{g \in G} a_g = 0$. Calculate $H^1(G, A)$.

C) (i) Let E be an elliptic curve over a p-adic field K_v. Show that

$$\#E(K_v)/n = \#E(K_v)[n] \cdot \#\mathcal{O}_v/n.$$

Hint: Show that the function $\natural \colon A \mapsto \#A/n \cdot \left(\#A[n]\right)^{-1}$ is multiplicative in exact sequences of abelian groups.

(ii) Let $p \neq \ell$ be two primes. Determine the size of $H^1(\mathbb{Q}_\ell, E)[p]$ and $H^1(\mathbb{Q}_\ell, E[p])$

(iii) Calculate the size of $H^1(K_{\mathfrak{q}}, E[3])$ in the original example.

D) Let $E/\mathbb{Q}$ be an elliptic curve and let $L/\mathbb{Q}$ be a cyclic extension of degree $p > 3$. Assume $E(\mathbb{Q})[p] = 0$, that $E(\mathbb{Q})$ has rank 0 and that $\text{Ш}(E/\mathbb{Q})[p] = 0$.

Show that if $\operatorname{rank} E(L) < (p-1)\sum \dim_{\mathbb{F}_p} D_v$ as in Proposition 23, then $Ш(E/L)[p]$ is non-trivial.

Use this an the information available on the lmfdb over $\mathbb{Q}$ and over $L = \mathbb{Q}(\zeta_{11})^+$ to prove that 5 divides the order of $Ш(E/L)$ for the curve with Cremona label 11a2 (and lmfdb label 11.a1).

E) Let E be an elliptic curve over a finite field F with q elements and let L/F be the extension of degree f. Let $\phi\colon E \to E$ be the q-power Frobenius sending $(X : Y : Z)$ to $(X^q : Y^q : Z^q)$.

(i) Show that the endomorphism $1 + \phi + \phi^2 + \cdots + \phi^{f-1}$ is not 0.

(ii) Deduce from this that the norm map $E(L) \to E(F)$ is surjective.

(iii) Let $\xi \in H^1\bigl(L/F, E(L)\bigr)$. Show that ξ is a coboundary. Hint: Pick a point $Q \in E(\bar{F})$ such that $(\phi - 1)(Q) = \xi_\sigma$ where $\sigma \in \operatorname{Gal}(L/F)$ is the Frobenius.

(iv) Prove that there are no pointless curves of genus 1 over F.

References

[1] Manjul Bhargava and Arul Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Ann. of Math. (2) **181** (2015), no. 1, 191–242. *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0*, Ann. of Math. (2) **181** (2015), no. 2, 587–621.

[2] B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on elliptic curves. I*, J. Reine Angew. Math. **212** (1963), 7–25.

[3] Spencer Bloch, *A note on height pairings, Tamagawa numbers, and the Birch and Swinnerton-Dyer conjecture*, Invent. Math. **58** (1980), no. 1, 65–76.

[4] J. W. S. Cassels, *Arithmetic on curves of genus* 1. *I. On a conjecture of Selmer*, J. Reine Angew. Math. **202** (1959), 52–99. *II. A general result*, J. Reine Angew. Math. **203** (1960), 174–208. *III. The Tate-Šafarevič and Selmer groups*, Proc. London Math. Soc. (3) **12** (1962), 259–296. *IV. Proof of the Hauptvermutung*, J. Reine Angew. Math. **211** (1962), 95–112. *V. Two counterexamples*, J. London Math. Soc. **38** (1963), 244–248. *VI. The Tate-Šafarevič group can be arbitrarily large*, J. Reine Angew. Math. **214(215)** (1964), 65–70. *VII. The dual exact sequence*, J. Reine Angew. Math. **216** (1964), 150–158.

[5] J. W. S. Cassels, *Second descents for elliptic curves*, J. Reine Angew. Math. **494** (1998), 101–127, Dedicated to Martin Kneser on the occasion of his 70th birthday.

[6] J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic number theory*, London Mathematical Society, London, 2010, Papers from the conference held at the University of Sussex, Brighton, September 1–17, 1965, Including a list of errata.

[7] François Châtelet, *Points rationnels et classification des courbes de genre un*, C. R. Acad. Sci. Paris **206** (1938), 1532, See also: Jean-Louis Colliot-Thélène, *Les grands thèmes de François Châtelet*, Enseign. Math. (2) **34** (1988), no. 3-4, 387–405.

[8] J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon, and M. Stoll, *Explicit n-descent on elliptic curves. I. Algebra*, J. Reine Angew. Math. **615** (2008), 121–155. *II. Geometry*, J. Reine Angew. Math. **632** (2009), 63–84. *III. Algorithms*, Math. Comp. **84** (2015), no. 292, 895–922.

[9] John E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997, Available at `https://johncremona.github.io/book/fulltext/index.html`.

[10] Tom Fisher and Rachel Newton, *Computing the Cassels-Tate pairing on the 3-Selmer group of an elliptic curve*, Int. J. Number Theory **10** (2014), no. 7, 1881–1907.

[11] Tom A. Fisher, *The Cassels-Tate pairing and the Platonic solids*, J. Number Theory **98** (2003), no. 1, 105–155.

[12] Matthias Flach, *A generalisation of the Cassels-Tate pairing*, J. Reine Angew. Math. **412** (1990), 113–127.

[13] Jean Gillibert and Christian Wuthrich, *The class group pairing and p-descent on elliptic curves*, Proc. Lond. Math. Soc. (3) **106** (2013), no. 2, 345–374.

[14] Serge Lang, *Algebraic groups over finite fields*, Amer. J. Math. **78** (1956), 555–563.

[15] Serge Lang and John Tate, *Principal homogeneous spaces over abelian varieties*, Amer. J. Math. **80** (1958), 659–684.

[16] Jonathan Lubin and Michael I. Rosen, *The norm map for ordinary abelian varieties*, J. Algebra **52** (1978), no. 1, 236–240.

[17] B. Mazur and J. Tate, *The p-adic sigma function*, Duke Math. J. **62** (1991), no. 3, 663–688.

[18] B. Mazur, J. Tate, and J. Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), no. 1, 1–48.

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

[20] Adam Morgan and Alexander Smith, *The Cassels-Tate pairing for finite Galois modules*, 2021, Preprint, available at https://arxiv.org/abs/2103.08530.

[21] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, Grundlehren der Mathematischen Wissenschaften, vol. 323, Springer, 2000, A newer version (with different numberings of theorems) is available at http://www.mathi.uni-heidelberg.de/~schmidt/NSW2e/.

[22] Bernadette Perrin-Riou, *Groupe de Selmer d'une courbe elliptique à multiplication complexe*, Compositio Math. **43** (1981), no. 3, 387–417.

[23] George Poitou, *Propriétés globales des modules finis*, Cohomologie galoisienne des modules finis; Travaux et Recherches Mathématiques, No. 13, Dunod, Paris, 1967, Séminaire de l'Institut de Mathématiques de Lille, sous la direction de G. Poitou, pp. 255–277.

[24] Edward F. Schaefer and Michael Stoll, *How to do a p-descent on an elliptic curve*, Trans. Amer. Math. Soc. **356** (2004), no. 3, 1209–1231.

[25] F. K. Schmidt, *Analytische Zahlentheorie in Körpern der Charakteristik p*, Math Z. **33** (1931), 1–32.

[26] Peter Schneider, *p-adic height pairings. I*, Invent. Math. **69** (1982), no. 3, 401–409.

[27] Ernst S. Selmer, *The Diophantine equation $ax^3+by^3+cz^3=0$*, Acta Math. **85** (1951), 203–362 (1 plate). *The diophantine equation $ax^3+by^3+cz^3=0$. Completion of the tables*, Acta Math. **92** (1954), 191–197. *A conjecture concerning rational points on cubic curves*, Math. Scand. **2** (1954), 49–54. *The Diophantine equation $\eta^2=\xi^3-D$. A note on Cassels' method*, Math. Scand. **3** (1955), 68–74.

[28] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.

[29] Michael Stoll, *Descent on elliptic curves*, Explicit methods in number theory, Panor. Synthèses, vol. 36, Soc. Math. France, Paris, 2012, Available at http://www.mathe2.uni-bayreuth.de/stoll/talks/short-course-descent.pdf, pp. 51–80.

[30] P. Swinnerton-Dyer, *Two descent from Fermat to now*, Mathematisches Institut, Georg-August-Universität Göttingen: Seminars Summer Term 2004, Universitätsdrucke Göttingen, Göttingen, 2004, pp. 95–102.

[31] John Tate, *Duality theorems in Galois cohomology over number fields*, Proc. Internat. Congr. Mathematicians (Stockholm, 1962), Inst. Mittag-Leffler, Djursholm, 1963, pp. 288–295.

[32] John Tate, *WC-groups over p-adic fields*, Séminaire Bourbaki, Vol. 4, Soc. Math. France, 1995, pp. Exp. No. 156, 265–277.