ELLIPTIC CURVES AND FORMAL GROUPS

Lubin, Serre, Tate

July 1964

Abstract

These are lecture notes by Jonathan Lubin, Jean-Pierre Serre and John Tate which are part of "*Lecture notes prepared in connection with the seminars held at the Summer Institute on Algebraic Geometry*, Whitney Estate, Woods Hole, Massachusetts, July 6 – July 31, 1964". The TeX version was prepared by Robert Harley from scanned copies made available by Felipe Voloch and Jane Ross, and from remarks by the authors.

1. Serre discussed his result on the action of Galois groups on the points of finite order on elliptic curves over number fields and local fields [4]. The local results in case of non-degenerate reduction can be obtained by methods to be discussed in this seminar.

2. Lubin discussed results from [2] on the endomorphism rings of formal Lie groups on one parameter over $\mathfrak{p}$-adic integer rings. If A is a commutative ring with identity, *a one-parameter formal Lie group over* A is a power series $F(x,y) \in A[[x,y]]$ such that

1. $F(x,y) \equiv x+y \mod \deg 2$
2. $F(F(x,y),z) = F(x,F(y,z))$
3. $F(x,y) = F(y,x)$

If F and G are two such formal groups an *A-homomorphism of F into G* is a power series $f(x) \in A[[x]]$ such that f has no constant term and $f(F(x,y)) = G(f(x),f(y))$.

The set of all such homomorphisms is called $\mathrm{Hom}_A(F,G)$ and is an abelian group under the addition $(f+g)(x) = G(f(x),g(x))$; the group $\mathrm{End}_A(F) = \mathrm{Hom}_A(F,F)$ is a ring. If $f \in \mathrm{End}_A(F)$, we denote by $c(f)$ its first-degree coefficient.

Proposition 1 *If A is an integral domain of characteristic zero, and F is a formal group over A, the map*

$$c: \ \mathrm{End}_A(F) \to A$$

is an injective ring-homomorphism

In the case we are interested in, where A is a $\mathfrak{p}$-adic integer ring, i.e., a complete rank-one valuation ring of characteristic zero, with residue class field of characteristic $p > 0$, $c(\mathrm{End}_A(F))$ is closed in A so that the endomorphism ring always contains $\mathbb{Z}_p$, the p-adic integers.

Proposition 2 *If F is a formal Lie group defined over the $\mathfrak{p}$-adic integer ring $\mathfrak{o}$, and F^*, the formal group defined over $k = \mathfrak{o}/\mathfrak{p}$ by reducing all the coefficients of F modulo $\mathfrak{p}$, is such that F^* is not k-isomorphic to the additive formal group $x + y$, then $\mathrm{End}_{\mathfrak{o}}(F)$ is injected into $\mathrm{End}_k(F^*)$ by the reduction map $f \mapsto f^*$.*

We know that over the algebraic closure K of k, $\mathrm{End}_K(F^*)$ is isomorphic to the unique maximal order in the central division algebra D_h of rank h^2 and invariant $1/h$ over $\mathbb{Q}_p$. Here h is the height of F^* as defined by Lazard [1].

Thus since $\mathrm{End}_{\mathfrak{o}}(F)$ is a commutative subring of $\mathrm{End}_K(F^*)$, its fraction field must be isomorphic to a subfield of D_h and so the degree of this field over $\mathbb{Q}_p$ must divide h.

A consequence of this is that if F is defined over $\mathfrak{o}$, there is a finite extension $\mathfrak{o}'$ of $\mathfrak{o}$ such that for any larger $\mathfrak{o}''$, $\mathrm{End}_{\mathfrak{o}''}(F) = \mathrm{End}_{\mathfrak{o}'}(F)$. We call this $\mathrm{End}_{\mathfrak{o}'}(F)$ the absolute endomorphism ring of F, and denote it $\mathrm{End}(F)$.

If F is defined over a $\mathfrak{p}$-adic integer ring $\mathfrak{o}$, the height of F is defined to be the height of F^*, the formal group defined over $k = \mathfrak{o}/\mathfrak{p}$.

If F is of height $h < \infty$ over $\mathfrak{o}$, F is *full* if

1. $\mathrm{End}(F)$ is integrally closed in its fraction field K.
2. $[K : \mathbb{Q}_p] = h$.

It turns out that for every local field K there is a full formal group whose endomorphism ring is the ring of integers of K.

3. Lubin discussed results from [3], and some other conjectures about points of finite order on formal groups.

If F is a formal group of height $h < \infty$ defined over $\mathfrak{o}$, and $\mathcal{O}$ is the ring of integers in any complete extension $\mathcal{L}$ of $L =$ the fraction field of $\mathfrak{o}$, and if $\mathcal{P}$ is the maximal ideal of $\mathcal{O}$, then $\mathcal{P}$ can be made into a group by means of: $\alpha + \beta = F(\alpha, \beta)$. Clearly the only elements of this group of finite order are of order p^n for some n: if we call $[\lambda]_F$ the endomorphism of F corresponding to the p-adic integer λ, then assuming that we have $\alpha \in \mathcal{P}$ such that $[m]_F(\alpha) = 0$ for $p \nmid m$, since $[\frac{1}{m}]_F \in \mathrm{End}_{\mathfrak{o}}(F)$, $([\frac{1}{m}]_F \circ [m]_F)(\alpha) = 0$ and so $\alpha = 0$.

Now since F is of height h, the endomorphism $[p]_F$ is a power series whose first unit coefficient is in degree p^h. Thus the first unit coefficient of $[p^r]_F(x)$ is in degree p^{rh}. And a Weierstrass preparation type argument shows that $[p^r]_F(x) = P(x) \cdot U(x)$ where $P(x)$ is a monic polynomial of degree p^{rh} such that all coefficients of degree less than p^{rh} are in $\mathfrak{p}$, and where $U(x)$ is a power series with unit constant term. Thus in a sufficiently large $\mathcal{O}$, there are exactly p^{rh} elements $\alpha \in \mathcal{P}$ such that $[p^r]_F(\alpha) = 0$.

We can form the "Tate group" of F:

$$T(F) = \varprojlim_n T_{p^n}(F)$$

where $T_{p^n}(F)$ is the group of all α in the algebraic closure of L such that $[p^n]_F(\alpha) = 0$; the projective limit is taken with respect to the maps $[p^{m-n}]_F : T_{p^m} \to T_{p^n} \quad (m > n)$.

Then $T(F)$ is a free $\mathbb{Z}_p$-module of rank h. It is also an $\mathrm{End}_{\mathfrak{o}}(F)$-module. Let us assume that $c(\mathrm{End}(F)) \subset \mathfrak{o}$ so that K, the fraction-field of $c(\mathrm{End}(F))$, is a subfield of L. Call $\mathcal{L}$ the field gotten by adjoining to L all roots of $[p^n]_F$ (all n). Then $G = \mathrm{Gal}(\mathcal{L}/L)$ has a faithful representation $G \hookrightarrow \mathrm{End}_{\mathbb{Z}_p}(T(F)) \cong \mathrm{GL}(h, \mathbb{Z}_p) \subset \mathrm{GL}(h, \mathbb{Q}_p)$ but also the action of G on $T(F)$ commutes with $\mathrm{End}(F)$ so $T(F) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is an $\mathrm{End}(F) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong K$-module of rank $s = h/r$ where r is the $\mathbb{Z}_p$-rank of $\mathrm{End}(F)$. One may ask whether G is open in $\mathrm{GL}(s, K)$, or, at any rate, whether the commuting algebra of G in $\mathrm{End}(T(F)) \otimes \mathbb{Q}_p$ is reduced to K. We have no indication of the truth or falsity of this[1], except in the case $s = 1$, where it is true, and can be used to give an explicit reciprocity law in local class field theory in the following way:

As mentioned before, for each finite extension K of $\mathbb{Q}_p$, with ring of integers $\mathfrak{o}$, there is a full formal group F defined over $\mathfrak{o}$ whose absolute endomorphism ring is isomorphic to $\mathfrak{o}$. Then $T(F)$ is a free $\mathfrak{o}$-module of rank 1 and so $G = \mathrm{Gal}(\mathcal{L}/K) \hookrightarrow \mathrm{GL}(1, \mathfrak{o}) = \mathfrak{o}^*$. A simple counting argument shows that in fact this map is onto. The field $\mathcal{L}$ is a totally ramified abelian extension of K and in fact a maximal such, and the action of $\mathfrak{o}^*$ on $\mathcal{L}$ given by the

[1] Now known to be true from theorems of Serre ("*Sur les groupes de Galois attachés aux groupes p-divisibles*" in "Proceedings of the Conference on Local Fields, NUFFIC Summer School, Driebergen, Netherlands, 1966", Springer-Verlag) and of Shankar Sen ("*Lie algebras of Galois groups arising from Hodge-Tate modules*" in Annals of Mathematics (2) **97** (1973), pp. 160–170).

above isomorphism turns out to be the inverse of that furnished by the reciprocity law of local class field theory: specifically, if $[\,p^n\,](\alpha) = 0$ for some n, and $u \in \mathfrak{o}^*$,

$$(u, \mathcal{L}/K)\,(\alpha) = [\,u^{-1}\,]_F\,(\alpha)\,.$$

By patching this together with the Frobenius mapping on the maximal unramified extension of K, we get an explicit reciprocity formula for the maximal abelian extension of K.

4. Lubin discussed unpublished results of Lubin-Tate on moduli of formal groups. Let Φ be a formal group of height $h < \infty$ defined over the residue class field $k = \mathfrak{o}/\mathfrak{p}$. Such a Φ is k-isomorphic to one satisfying $\Phi(x, y) \equiv x + y \mod \deg p^h$, and we will assume this condition satisfied for the sake of convenience. Let $t = (t_1, \ldots, t_{h-1})$ be a family of $h - 1$ independent transcendentals. By methods of Lazard [1] it is easy to construct a formal group $\Gamma(t_1, \ldots, t_{h-1})\,(x, y)$ with coefficients in the polynomial ring $\mathfrak{o}[\,t_1, \ldots, t_{h-1}\,]$ such that

(i) $\Gamma^*(0, \ldots, 0)\,(x, y) = \Phi(x, y)$

(ii) $\Gamma(0, \ldots, 0, t_i, \ldots, t_{h-1})\,(x, y) \equiv x + y + t_i\, C_{p^i}(x, y) \mod \deg\ p^i\!+\!1\,.$

Choose such a Γ. Let A be a local $\mathfrak{o}$-algebra with maximal ideal M. If we specialize the t_i to elements $\alpha_i \in M$, we obtain a group law $\Gamma(\alpha)\,(x, y)$ defined over A which reduces mod M to Φ, i.e. such that $\Phi = (\Gamma(\alpha))^*$. (Here we are identifying $k = \mathfrak{o}/\mathfrak{p}$ with its canonical image in A/M).

Theorem 1 *Suppose A is separated and complete for the M-adic topology. Let F be a formal group over A such that $\Phi = F^*$. Then there exist $\alpha_i \in M$, $1 \le i \le h - 1$, and an A-isomorphism $\phi :\ F \simeq \Gamma(\alpha)$ such that $\phi^* =$ identity. Moreover, the point $\alpha = (\alpha_1, \ldots, \alpha_{h-1})$ and ϕ are unique.*

In other words, the functor which associates with each complete local $\mathfrak{o}$-algebra A the set of isomorphism classes of formal groups F over A reducing to Φ mod M (allowable isomorphisms being those A-isomorphisms reducing to identity mod M) is representable by the "universal" group law $\Gamma(t)$ over the algebra $\mathfrak{o}\,[[\,t_1, \ldots, t_{h-1}\,]]$. As usual, there results an operation of $\operatorname{Aut}\Phi$ on $\mathfrak{o}\,[[\,t\,]]$, whose study should be interesting. In case $h = 2$ we have used it to construct an elliptic curve E over $\mathfrak{o}$ whose formal group has complex multiplication, although E does not.

5. Tate discussed a mixed group-sheaf cohomology. Let S be a ground scheme, X a group scheme over S, and B a commutative group scheme over S. Suppose X operates on B in an evident sense. Let $\mathcal{U}$ be an open covering of X. With the aid of the group law $X \times X \to X$, one can associate with $\mathcal{U}$ a certain open cover $\mathcal{U}^{(p)}$ of $X^p = X \times X \times \cdots \times X$ (p times), for each p. One can then define a double complex $C^{\bullet\bullet}(\mathcal{U}, X, B)$ in which an element of $C^{p,q}$ is a family of morphisms from the intersections of $(q+1)$ open sets in the covering $\mathcal{U}^{(p)}$ into B. The differentiation $C^{p,q} \to C^{p,q+1}$ is as in the Čech sheaf cohomology, while the differentiation $C^{p,q} \to C^{p+1,q}$ is defined by formulas as for the coboundary in the standard inhomogenous cochain complex in group cohomology. Passing to the associated single complex and cohomology we get groups $\mathrm{H}^n(\mathcal{U}, X, B)$. For example, $\mathrm{H}^2(\mathcal{U}, X, B)$ describes the group-scheme extensions of X by B which, as fiber spaces, are trivial on the covering $\mathcal{U}$. Passing to the limit over $\mathcal{U}$, we get groups $\mathrm{H}^n(X, B)$.

6. Tate discussed results of Serre-Tate on the lifting[2] of abelian varieties from characteristic p, the main idea[3] being that to lift A is equivalent to lifting consistently the finite subschemes $\mathrm{Ker}(A \xrightarrow{p^n} A)$ for all n. Let R be an Artinian local ring with residue field $k = R/\mathfrak{m}$. Let I be an ideal in $\mathfrak{m}$ such that $\mathfrak{m} I = 0$. Put $R' = R/I$. We wish to "lift" things from R' to R.

(i) *Lifting homomorphisms of groups.* Let B be a group scheme smooth over R, and let X be a group scheme flat over R. Assume X and B are commutative for simplicity. Let

$$B' = B \otimes_R R', \quad X' = X \otimes_R R', \quad \widetilde{B} = B \otimes_R k, \quad \text{etc.}$$

Let $t(\widetilde{B})$ be the tangent space to the origin on $\widetilde{B}$. The tensor product $t(\widetilde{B}) \otimes I$ is a finite dimensional vector space over k. Let $W(t(\widetilde{B}) \otimes I)$ denote the corresponding group scheme over k, isomorphic to the direct product of $(\dim \widetilde{B})(\dim_k I)$ copies of the additive group $\mathbb{G}_a$.

Theorem 2 *There is an exact sequence*

$$0 \to \mathrm{Hom}_k(\widetilde{X}, W(t(\widetilde{B}) \otimes I)) \to \mathrm{Hom}_R(X, B) \to \mathrm{Hom}_{R'}(X', B') \xrightarrow{\delta} \mathrm{H}^2(\widetilde{X}, W(t(\widetilde{B}) \otimes I)).$$

Here the Homs are *group* homomorphisms. The H^2 is that defined in the preceding section, and the image of δ is contained in the symmetric part of H^2, and hence can be viewed as in $\mathrm{Ext}^1(\widetilde{X}, W)$. The theorem is proved by means of an exact sequence of complexes as in §5.

$$0 \to C^{\bullet\bullet}(\mathcal{U}, \widetilde{X}, W) \to C^{\bullet\bullet}(\mathcal{U}, X, B) \to C^{\bullet\bullet}(\mathcal{U}, X', B') \to 0,$$

where $\mathcal{U}$ is an affine open covering of X. The exactness follows from the fact that on an affine set, a morphism $X' \to B'$ can be lifted to $X \to B$.

[2] The term "raising" was used in the original notes.

[3] Serre remarks that he covered the case of varieties with full p-torsion as described in 7.(iv) and 8, whereas the main idea of section 6 and its application in 7.(iii) are in fact entirely due to Tate.

Of course the interesting point is the δ: the obstruction to lifting a homomorphism of commutative groups lies in $\mathrm{Ext}(\widetilde{X}, W)$. A geometric description of that extension could certainly be given (and might enable one to avoid the mixed group-sheaf cohomology of §5). It would also be interesting to examine the relations between this and the group extensions given by Greenberg's functor (assuming k perfect); if $I = \mathfrak{m}$, it seems that Greenberg's extension is obtained from the other by a suitable power of Frobenius.

(ii) *Lifting abelian varieties.* Suppose now that k is of characteristic $p \neq 0$. The main theorem can be formulated by saying that there is an *equivalence of categories* $C_1 \to C_2$, where:

> (C_1) is the category of abelian schemes over R.
>
> (C_2) is the category of pairs (Φ, X), where Φ is an abelian scheme over k, and where X is a lifting to R of Φ^*. For this to make sense, we must say what A^* is if A is an abelian scheme over R (or k):
>
> $$A^* = \lim_{n\to\infty} A_{p^n}, \text{where } A_{p^n} = \mathrm{Ker}(p^n : A \to A).$$

Of course the kernel A_{p^n} is taken as a group scheme (finite and flat over R (or k)). Concerning A^* one considers it as an ind-object; the notion of a lifting to R of Φ^* is therefore equivalent to that of a sequence of liftings of the Φ_{p^n} to group schemes X_n flat over R, together with injections $X_n \to X_{n+1}$ lifting the canonical inclusions $\Phi_{p^n} \subset \Phi_{p^{n+1}}$. In what follows we shall pretend that A^* (or Φ^*) is a true group scheme—it is clear that this will not lead to serious worries.

The functor $C_1 \to C_2$ is clear; it associates with each abelian scheme A over R the pair $(\widetilde{A}, A^*)$ where $\widetilde{A}$ is the reduction of A (mod $\mathfrak{m}$), which is an abelian variety over k. Clearly, A^* is a lifting of $\widetilde{A}^*$. The marvellous thing is that it is an equivalence of categories! In other words, if one knows the reduction $\widetilde{A}$ of an abelian scheme A, all that is lacking to determine A is a lifting of the ind-group scheme $\widetilde{A}^*$, which is quite an innocent thing (see below).

The proof of the theorem which was sketched in the seminar used the exact sequence of (i) above together with known facts about the existence of liftings of abelian schemes. However, with better foundations, the theorem should result formally from:

Lemma 1 *One has* $\mathrm{Ext}^i(\Phi, \mathbb{G}_a) \xrightarrow{\sim} \mathrm{Ext}^i(\Phi^*, \mathbb{G}_a)$ *for all* i.

(In fact, these groups are zero for $i \neq 1$, and for $i = 1$, they are k-vector spaces of dimension dim A). The lemma would result from the fact that Φ/Φ^* is uniquely divisible by p, hence all its Exts with $\mathbb{G}_a$ are zero.

7. Serre discussed applications of the preceding.

(iii) *The case where Φ has no point of order p.* In this case one can identify Φ^* with the *formal group* attached to Φ. Thus, to lift Φ is the same as to lift its formal group. In case $\dim \Phi = 1$ (Φ an elliptic curve with Hasse inv. $= 0$) the lifting of the formal group has been discussed by Lubin in section 4 above.

(iv) *The case where Φ has the maximum number of points of order p.* [This is the case which Serre has treated previously (unpublished) by using the Greenberg functor. The present theory gives new proofs, more satisfying in certain respects.] We suppose k *perfect* (this seems essential, and not only due to our natural taste for Galois theory). Let $n = \dim \Phi$. The hypothesis made on Φ amounts to saying that Φ_p is the direct sum of an étale k-group of order p^n and an infinitesimal k-group of "order" p^n. The first is a $(\mathbb{Z}/p\mathbb{Z})^n$ twisted by Galois, and the second a $(\mu_p)^n$ twisted analogously. More generally one has a canonical decomposition:

$$\Phi^* = \Phi^*_m + \Phi^*_{\text{ét}}\,.$$

Now it is clear that $\Phi^*_{\text{ét}}$ has a unique lifting to R (Hensel). It is the same (for example by Cartier duality or by the results of Dieudonné) for Φ^*_m. One sees therefore immediately *that there is a canonical way to lift* Φ^*, namely the direct sum of the liftings of Φ^*_m and $\Phi^*_{\text{ét}}$, and there results, by the general theory a *canonical lifting of the abelian variety* Φ. It is easy to see that one even obtains in this way a *functor* from the category of the Φ to the category C_1, a functor which is inverse to the reduction functor (N.B. this inverse is defined only on the Φ having the maximum number of points of order p). If one passes to the limit over R, one finds *a priori* a *formal abelian scheme* lifting Φ canonically, but Mumford explained to us how, using the canonicalness, one can prove that it is in reality an abelian scheme.

Before discussing the canonical liftings in more detail, let us say a word about the other liftings. We suppose for simplicity for k is algebraically closed. It is almost evident that each lifting of Φ^*, call it A^*, is an extension.

$$0 \to A^*_m \to A^* \to A^*_{\text{ét}} \to 0$$

where A^*_m and $A^*_{\text{ét}}$ are the canonical liftings of Φ^*_m and $\Phi^*_{\text{ét}}$. To suppose k algebraically closed allows us to identify these latter groups with the groups ($\mathbb{G}_m$-formal)^n, and $(\mathbb{Q}_p/\mathbb{Z}_p)^n$, these groups being taken over R in the obvious sense. It is then an exercise to show that an R-extension of $\mathbb{Q}_p/\mathbb{Z}_p$ by $\mathbb{G}_m$-formal is characterized by an element of the group $R^*_1 = 1 + \mathfrak{m}$, the multiplicative group of elements of R congruent to 1 modulo the maximal ideal $\mathfrak{m}$.

Passing to the limit over R, one sees that this result continues to hold if one is over a complete noetherian local ring R with residue field k. Of course one is no longer sure that one has true abelian schemes, but in any case, one has formal schemes. Therefore one can say that the formal variety of moduli has as its points the systems of n^2 Einseinheiten; it has moreover a canonical group structure.

The abelian schemes, or formal schemes, whose moduli (in the preceding sense) are of *finite order* deserve the name *quasi-canonical*. In case R is a discrete valuation ring, such a scheme is isogenous to a canonical scheme; the situation is not clear in the general case.

Continuing to assume R a discrete valuation ring of characteristic zero, there is a simple characterization of the quasi-canonical schemes: these are those for which the module $V_p = T_p \otimes \mathbb{Q}_p$ *splits* as a module over the p-adic Lie algebra of the Galois group. In this way one arrives at a justification of theorem 1, page 9 of [4].

8. Serre discussed the canonical lifting of elliptic curves. The problem considered is the following. Let k be perfect, and let E be an elliptic curve with invariant $j \in k$ and with Hasse invariant $\neq 0$ (i.e., having the maximum number of points of order p); by the preceding discussion, there is a canonical lifting of E to the ring $W(k)$ of Witt vectors. The j of that lifting is therefore a function

$$\theta : \ k - \mathrm{Ker}(\mathrm{Hasse}) \to W(k)$$

How does one calculate θ ?

Let s be the Frobenius automorphism of $W(k)$, given by $(x_0, x_1, \ldots) \mapsto (x_0^p, x_1^p, \ldots)$. Let $T_p\,(j, j')$ be the classical equation relating the modular invariants of two elliptic curves having an isogeny of degree p between themselves, an equation with coefficients in $\mathbb{Z}$, symmetric in j, j'.

Theorem 3

(i) *Let* $\lambda \in k - \mathrm{Ker}(\textit{Hasse})$, *and let* $x = \theta(\lambda) \in W(k)$. *One has*

$$(*) \qquad T_p\,(x, s(x)) = 0, \quad \textit{and} \quad x \equiv \lambda \pmod{p}$$

(ii) *If* $\lambda \in k - \mathbb{F}_{p^2}$, *the system* $(*)$ *has a unique solution.*

(Combining (i) and (ii) one sees therefore that $(*)$ characterizes $x = \theta(\lambda)$, provided that $\lambda \notin \mathbb{F}_{p^2}$).

To prove (i) one applies the functor "canonical lifting" to the Frobenius isogeny: $E \to E^{(p)}$. The canonical lifting of $E^{(p)}$ is obtained from that of E by applying the automorphism s. Its modular invariant $s(x)$ is therefore related to the invariant x of the lifting of E by the equation $T_p\,(x, s(x)) = 0$, hence (i). The assertion (ii) is proved in a standard way by successive approximations. The hypothesis $\lambda \notin \mathbb{F}_{p^2}$ intervenes in order to be sure that a certain partial derivative of T_p does not vanish.

Just for fun, here is a numerical example: for $p = 2$, $\lambda = 1$, the canonical lifting $\theta(\lambda)$ is equal to $-3^3 5^3$.

References

[1] M. Lazard. *Sur les groupes de Lie formels à un paramètre.* Bull. Soc. Math. France **83** (1955), pp. 251–274.

[2] J. Lubin. *One-parameter formal Lie groups over $\mathfrak{p}$-adic integer rings.* Annals of Math. (2) **80** (1964), pp. 464–484. See also : Annals of Math. (2) **84** (1966), p. 372.

[3] J. Lubin and J. Tate. *Formal complex multiplication in local fields.* Annals of Math. (2) **81** (1965), pp. 380–387.

[4] J.-P. Serre. *Groupes de Lie ℓ-adiques attachés aux courbes elliptiques.* Colloque de Clermont-Ferrand, CNRS, April 1964, pp. 239–256.