1. Galois groups and Galois representations

2. Geometric Galois representations

2.1. Tate modules.

2.2. The cyclotomic character.

2.3. The Tate module of an elliptic curve.

REMARK 2.4. Let E be an elliptic curve over a finite extension F of $\mathbb{Q}_\ell$. When $\ell = p$ or when E has bad reduction, the Galois representation $V_p(E)$ is more complicated, in particular it is ramified, but essentially completely known. We describe below some results without proofs (see Silverman's book).

(i) If $\ell = p$ and E has good reduction, an extension of the arguments of Prop. **??** would show that there is a G_F-equivariant exact sequence

$$0 \to T_p(E_0(\widehat{\overline{F}})) \to T_p(E(\overline{F})) \to T_p(\overline{E}(\overline{k}_F)) \to 0.$$

The latter Tate-module has actually $\mathbb{Z}_p$-rank 1 or 0, in which case we say that $\overline{E}$ is ordinary or supersingular respectively. On can show that the first case occurs if and only if the integer

$$a := |k_F| + 1 - |\overline{E}(k_F)|$$

is prime to p. In this case, the eigenvalue of frob_{k_F} on $T_p(\overline{E}(\overline{k}_F))$ is the (unique) root of $X^2 - aX + |k_F|$ that belongs to $\mathbb{Z}_p^\times$. In the supersingular case, $E(\overline{F})[p]$ is an (absolutely) irreducible $\mathbb{F}_p[G_F]$-module and $V_p(E)$ will be described more precisely in the lectures of Berger. In all cases, $V_p(E)$ is a crystalline representation of G_F, whose Fontaine functor D_{cris} is known explicitely.

(ii) We say that E has *split multiplicative reduction* if E has an integral Weierstrass equation whose reduction $\overline{E}$, the plane curve over k_F obtained by reducing that equation modulo π_F, has a unique singular point which is furthermore a double point whose two tangents are defined over k_F. In this case a theorem of Tate ensures that there exists a unique $q_E \in F^\times$ and a $\mathbb{Z}[G_F]$-equivariant isomorphism

$$E(\overline{F}) \xrightarrow{\sim} \overline{F}^\times / q_E^{\mathbb{Z}}.$$

The "Tate-period" q_E has the property that $v(q_E) = -v(j(E)) > 0$. This describes explicitely $T_p(E)$ in terms of q_E in this case, for all prime p. In particular, there is an exact sequence of $\mathbb{Z}_p[G_F]$-modules

$$0 \to \mathbb{Z}_p(1) \to T_p(E) \to \mathbb{Z}_p \to 0,$$

which is non-split even after inverting p, and even mod p if q_E is not a p-th power in $F^\times$. In particular, $T_p(E)$ is tamely ramified if $\ell \neq p$ (i.e. $\rho_{E,p}(P_F) = \{1\}$). This result of Tate is especially important as for any E, there exists a finite extension F'/F such that $E \times_F F'$ has either good or split multiplicative reduction.

Let us give an application of all of this to the computation of $\rho_{E,p}$ in some example. Recall the two following elementary results from group theory:

(a)(Dickson) If a subgroup $G \subset \mathrm{GL}_2(\mathbb{F}_p)$ has its order divisible by p and if G acts irreducibly on $\mathbb{F}_p^2$ (for instance, contains an element with irreducible characteristic polynomial), then $G \supset \mathrm{SL}_2(\mathbb{F}_p)$.

(b) (Serre) If G is a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$ whose image in $\mathrm{GL}_2(\mathbb{F}_p)$ contains $\mathrm{SL}_2(\mathbb{F}_p)$, and if $p \geq 5$, then $G \supset \mathrm{SL}_2(\mathbb{Z}_p)$.

Dickson's result follows from the fact that the transvections in $\mathrm{SL}_2(\mathbb{F}_p)$ are the elements of order p, and that any two non-proportional transvections generate $\mathrm{SL}_2(\mathbb{F}_p)$. For a proof of Serre's result, see Serre "Abelian ℓ-adic representations".

Example 2.5. *Consider the elliptic curve* $E : y^2 + y = x^3 - x^2$ *over* $\mathbb{Q}$. *Then* $\rho_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_p)$ *is surjective if* $p \equiv 3 \bmod 4$ *and* $p \geq 7$.

Proof — Indeed, $\det \rho_{E,p}$ is the p-adic cyclotomic character, hence surjective, so by (b) it is enough to show that the reduction mod p of $\rho_{E,p}$ satisfies the assumptions of (a) above.

Note first that $\Delta = 11$ so E has good reduction outside 11. Moreover, $|\overline{E}(\mathbb{F}_2)| = 5 = 1 + 2 - (-2)$, so $\det(1 - T\rho_{E,p}(frob_2)) = 1 + 2T + 2T^2$. For $p \equiv 3 \bmod 4$, this polynomial is irreducible over $\mathbb{F}_p$ as its discriminant -4 is not a square in $\mathbb{F}_p$.

Moreover, E has split multiplicative reduction at 11. Indeed, modulo 11 we have $x^3 - x^2 + 1/4 \equiv (x+3)^2(x+4) \bmod 11$, so E mod 11 is $Y^2 = X^2(X+1)$ up to changing Weierstrass coordinates, and the tangents at $(0,1)$ are $Y = \pm X$. As $j(E) = -2^{12}/11$, the Tate-period of $E \times \mathbb{Q}_{11}$ is a uniformizer, hence it is never a p-th power in $\mathbb{Q}_{11}$, so $\rho_{E,p}(I_{\mathbb{Q}_{11}})$ mod p is cyclic of order p for each p by Tate's theorem, and we are done. □

Not that this funishes examples of Galois extensions of $\mathbb{Q}$ whose Galois group is $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ for each $n \geq 1$, in particular non solvable, whenever $p = 3k + 4 \geq 7$.

Actually, a lot is know about the image of $\rho_{E,p}$ for a general elliptic curve over $\mathbb{Q}$. Let us simply say that if E has no CM, a theorem of Serre ensures that this image is always open, and equals the whole of $\mathrm{GL}_2(\mathbb{Z}_p)$ for almost all prime p. Actually, for the curve E of the proposition, this occurs for all $p \neq 5$. For $p = 5$, there are exactly three homothety classes of $G_{\mathbb{Q}}$-stable lattices in $V_5(E)$, the reduction mod 5 of $T_5(E)$ being non-split. The two other elliptic curves over $\mathbb{Q}$ which are isogenous to E, and corresponding to these lattices, are the curves $y^2 + y = x^3 - x^2 - 7820x - 263580$ and $y^2 + y = x^3 - x^2 - 10x - 20$ (this last one having a split 5-torsion). See Serre's paper : Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. 15 (1972), no. 4, 259–331.

References : As an elementary and useful reference for this paragraph, see Silverman's book "The arithmetic of ellictic curves". See also Serre "Abelian ℓ-adic representations", and Katz-Mazur "Arithmetic moduli of elliptic curves". For tables of elliptic curves, see the home page of John Cremona : `http://www.warwick.ac.uk/staff/J.E.Cremona/ftp/data/INDEX.html` (the notation for an elliptic curve is usually $[a_1, a_2, a_3, a_4, a_6]$ as in (**??**)), Pari GP is often useful as well.

2.6. Tate modules of Jacobians and general geometric Galois representations. The construction of the Tate-module of an elliptic curve directly generalizes, following Weil, to any abelian variety over F, in which case its dimension is twice the dimension of the abelian variety if $p \in F^*$: see for instance Mumford's book on abelian varieties for the study of the multiplication by N on an abelian variety. Each algebraic curve has an natural associated abelian variety, its Jacobian, whose Tate-module can actually be defined from scratch as follows.

Let C be a projective smooth algebraic curve over F, and assume that $C \times_F \overline{F}$ is connected. The geometric Weil divisor group $\mathrm{Div}(C)$ is the free abelian group over the set $C(\overline{F})$. It has a natural *degree* linear map $\deg : \mathrm{Div}(C) \to \mathbb{Z}$ sending a point to 1, the kernel of which is denoted by $\mathrm{Div}^0(C)$. There is a natural group homomorphism $\mathrm{div} : \overline{F}(C)^\times \to \mathrm{Div}^0(C)$ associating to any rational function $f \in \overline{F}(C)^\times$ its divisor $\mathrm{div}(f)$ counting its poles and zeros with their multiplicities. Consider the abelian group

$$\mathrm{Pic}^0(C)(\overline{F}) = \mathrm{Div}^0(C)/\mathrm{div}(\overline{F}(C)^\times).$$

Note that the action of G_F on $C(\overline{F})$ gives $\mathrm{Div}(C)$ a structure of discrete G_F-module, that preserves $\mathrm{Div}^0(C)$ and $\mathrm{div}(\overline{F}(C)^\times)$, hence $\mathrm{Pic}^0(C)(\overline{F})$ is a discrete G_F-module as well. If E is an elliptic curve, then the map $E(\overline{F}) \to \mathrm{Pic}^0(E)(\overline{F})$, $P \mapsto [P]-[O]$, is a $\mathbb{Z}[G_F]$-module homomorphism essentially by definition of the group law on $E(\overline{F})$. As a consequence this map is surjective, and it is actually even bijective (Abel's theorem) as a relation $[P]-[O] = \mathrm{div}(f)$ would imply that $f : E \times_F \overline{F} \xrightarrow{\sim} \mathbb{P}^1_{\overline{F}}$.

THEOREM 2.7. *(Weil) Let $A = \mathrm{Pic}^0(C)(\overline{F})$. For $N \in F^\times$, then $|A[N]| = N^{2g}$ where g is the genus of the curve $C \times_F \overline{F}$. In particular $T_p(A) \simeq \mathbb{Z}_p^{2g}$, if $p \in F^*$.*

Let us set $T_p(C) := T_p(\mathrm{Pic}^0(C)(\overline{F}))$, this definition is coherent with the previous one for elliptic curves by the remarks above. The properties of these more general Tate-modules are actually quite similar to the ones we have seen for elliptic curves.

All these constructions of Galois representations are actually special cases of a much more general construction defined by Grothendieck called *étale cohomology*, which makes sense for any scheme of finite type over F and even more (see Grothendieck's SGA 4 or Milne's *étale cohomology*). If X is such a scheme, and if we set $X_{F'} = X \times_F F'$ if $F \to F'$ is a field embedding, he defined for $p \in F^\times$ a finite type $\mathbb{Z}_p$-module

$$H^i_{et}(X_{\overline{F}}, \mathbb{Z}_p) = \operatorname{proj\,lim}_m H^i_{et}(X_{\overline{F}}, \mathbb{Z}/p^m\mathbb{Z})$$

which has a natural continuous $\mathbb{Z}_p$-linear action of G_F. We also write $H^i_{et}(X_{\overline{F}}, \mathbb{Q}_p) = H^i_{et}(X_{\overline{F}}, \mathbb{Z}_p)[1/p]$. These cohomology groups vanish for $i \notin \{0, \dots, 2d\}$, where $d = \dim(X)$.

EXAMPLES:

(i) When $X = \mathbb{G}_m = \mathbb{A}^1 \backslash \{0\}$, then $H^1_{\mathrm{et}}(X_{\overline{F}}, \mathbb{Z}_p) = \mathbb{Z}_p(-1)$ is the $\mathbb{Z}_p$-dual of $T_p(\overline{F}^\times)$.

(ii) When $X = E$ is an elliptic curve over F (or more generally an abelian variety over F), then $T_p(E)$ is also naturally isomorphic[1] to the $\mathbb{Z}_p$-dual of $H^1_{\mathrm{et}}(E_{\overline{F}}, \mathbb{Z}_p)$.

(iii) When $C = X$ is a projective smooth algebraic curve over F, the *Kummer exact sequence* gives a canonical isomorphism $H^1_{\mathrm{et}}(C_{\overline{F}}, \mathbb{Z}_p) \overset{\sim}{\rightarrow} T_p(C)(-1)$. Still in this case, Weil constructed a non-degenerated, $\mathbb{Z}_p[G_F]$-equivariant, symplectic pairing $T_p(C) \times T_p(C) \rightarrow \mathbb{Z}_p(1)$, thus again $H^1_{\mathrm{et}}(C_{\overline{F}}, \mathbb{Z}_p) = \mathrm{Hom}_{\mathbb{Z}_p}(T_p(C), \mathbb{Z}_p)$.

(iv) If $X_{\overline{F}}$ is connected and proper of dimension d, then $H^0_{et}(X_{\overline{F}}, \mathbb{Z}_p) = \mathbb{Z}_p$ (trivial G_F-action) and $H^{2d}_{et}(X_{\overline{F}}, \mathbb{Z}_p) = \mathbb{Z}_p(-d)$ (Tate twist).

Assume from now on that X is proper smooth over F. The étale cohomology groups satisfy various wonderful properties with respect to changing the base field F, which are very similar to the properties we encountered for Tate-modules of elliptic curves.

(i) (*Change of algebraically closed field*) First of all, if $F \rightarrow F'$ is any field embedding, then

$$H^i_{et}(X_{\overline{F}}, \mathbb{Z}_p)_{|G_{F'}} \overset{\sim}{\rightarrow} H^i_{et}(X_{\overline{F'}}, \mathbb{Z}_p).$$

(ii) (*Comparison with Betti cohomology*) If $F = \overline{F} = \mathbb{C}$, then $H^i_{et}(X, \mathbb{Z}_p)$ is canonically isomorphic to $H^i_{\mathrm{Betti}}(X(\mathbb{C}), \mathbb{Z}) \otimes \mathbb{Z}_p$.

(iii) (*Finite fields*) If F is a finite field of characteristic $\ell \neq p$, the Grothendieck-Lefschetz trace formula shows that

$$|X(F)| = \sum_{i=0}^{2\dim(X)} (-1)^i \mathrm{trace}(\mathrm{Frob}_F | H^i_{et}(X_{\overline{F}}, \mathbb{Q}_p)).$$

(hence the rationality of the Zeta-function X). Moreover, Deligne has shown that the characteristic polynomial of Frob_F on each $H^i_{et}(X_{\overline{F}}, \mathbb{Q}_p)$ belongs to $\mathbb{Z}[t]$, and that its roots are *effective q-Weil numbers of weight i*, i.e. algebraic integers x whose complex absolute value is $q^{i/2}$ in any embedding $\mathbb{Q}(x) \rightarrow \mathbb{C}$, where $q = |F|$. We recover in particular this way the results of Weil and Hasse recalled for elliptic curves. For general curves, all of this was due to Weil.

Assume that $X_{\overline{F}}$ is connected. Note that if F' is any finite extension of F in $\overline{F}$, then it follows from the Grothendieck-Lefschetz formula above and Deligne's result that the term corresponding to $i = 2\dim(X)$ dominates in the formula for $|X(F')|$, so that $|X(F')| = |F'|^{\dim(X)} + o(|F'|^{\dim(X)})$ for $|F'| \rightarrow \infty$ (Lang-Weil estimates).

It is conjectured that Frob_F is always a semi-simple endomorphism of $H^i_{et}(X_{\overline{F}}, \mathbb{Q}_p)$ (this is known when X is an abelian variety, by the work of Weil).

(iv) (*Local fields*) If F is a finite extension of $\mathbb{Q}_\ell$ with $\ell \neq p$, and if X is the generic fiber of a proper smooth scheme $\mathcal{X}$ over $\mathcal{O}_F$, we say that X has good reduction over F. In this case, Grothendieck's *base change theorems* show

[1] Actually, for any X then $H^1_{\mathrm{et}}(X_{\overline{F}}, \mathbb{Z}_p) = \mathrm{Hom}(\pi_1(X_{\overline{F}}), \mathbb{Z}_p)$ where $\pi_1(X_{\overline{F}})$ is Grothendieck's étale fundamental group. The point is then that any étale covering of an elliptic curve is again an elliptic curve, hence is dominated by $[N]$ for some integer $N \geq 1$ (note that this is clear over $\mathbb{C}$).

> that the G_F-representation $H^i_{et}(X_{\overline{F}}, \mathbb{Z}_p)$ is unramified, i.e. factors through $G_F/I_F = G_{k_F}$, and that we have an isomorphism of $\mathbb{Z}_p[G_{k_F}]$-modules
>
> $$H^i_{et}(\overline{X}_{\overline{k_F}}, \mathbb{Z}_p) \overset{\sim}{\rightarrow} H^i_{et}(X_{\overline{F}}, \mathbb{Z}_p)$$
>
> where $\overline{X} = \mathcal{X} \times_{\mathcal{O}_F} k_F$ over k_F. In particular, the G_{k_F}-module $H^i_{et}(\overline{X}_{\overline{k_F}}, \mathbb{Z}_p)$ is independent on the choice of $\mathcal{X}$ as above such that $\mathcal{X} \times_{\mathcal{O}_F} F \simeq X$. Note that this directly generalizes, in a very simple way, the paragraph about integral models of elliptic curves. When X has not necessarily good reduction, but still $\ell \neq p$, then the restriction of $H^i_{et}(X_{\overline{F}}, \mathbb{Q}_p)$ to the inertia group I_F satisfies no specific restriction : it can contain any continous representation of I_F that extends to G_F. When $\ell = p$, the story is quite different, and it is known that $H^i_{et}(X_{\overline{F}}, \mathbb{Q}_p)$ is de Rham in the sense of Fontaine, which is a very restrictive condition; when X has good reduction over F, it is even crystalline (see Berger's lectures for these notions and for the story of these results : Fontaine, Messing, Faltings, Kato, Tsuji).

When F is a number field and when X is proper smooth over F, it easy to see that X_{F_v} has good reduction over F_v for almost all finite places $v \in S(F)$, thus the Galois representation $H^i_{\mathrm{et}}(X_{\overline{F}}, \mathbb{Z}_p)$ is unramified outside p and the places of bad reduction of X, and encaptures the collection of traces of Frob_v on $H^i_{\mathrm{et}}(\overline{X}_v \times_{k_{F_v}} \overline{k_{F_v}}, \mathbb{Z}_p)$ for almost all v.

There are several mostly open conjectures about the G_F-representation $H^i_{\mathrm{et}}(X_{\overline{F}}, \mathbb{Q}_p)$ when F is a number field. For instance, it is believed that it is semi-simple. Another famous conjecture of Tate asserts that the G_F-invariant subspace of $H^{2i}_{et}(X_{\overline{F}}, \mathbb{Q}_p)(i)$ is generated over $\mathbb{Q}_p$ by the cohomology classes associated to the algebraic cycles on X of codimension i. There are several other important conjectures related to motives and L-functions that will unfortunately not be discussed here, and for which we refer to Tate's paper at the Corvallis conference on L-functions, and to the proceedings of the Seattle conference on Motives. When $F/\mathbb{Q}_\ell$ is a local field and X has bad reduction, an important open problem in the analysis of the action of G_F on $H^i_{\mathrm{et}}(X_{\overline{F}}, \mathbb{Q}_p)$ is the so-called *weight-monodromy* conjecture (even when $\ell \neq p$).

Definition 2.8. *Let L be a finite extension of $\mathbb{Q}_p$, F a number field, and $\rho : G_F \rightarrow \mathrm{GL}_n(L)$ a Galois representation.*

– We say that ρ is (strongly) geometric if there exists some proper smooth scheme X over F such that ρ is a subquotient of $H^i_{\mathrm{et}}(X_{\overline{F}}, \mathbb{Q}_p)(m) \otimes_{\mathbb{Q}_p} L$ for some $i \geq 0$ and some $m \in \mathbb{Z}$.

– We say that ρ is weakly geometric if ρ is unramified outside some finite set $S \subset S(F)$ and if $\rho_{|G_{F_v}}$ is de Rham for each $v \in S(F)_p$.

As we saw, geometric implies weakly geometric. The other direction is the so-called Fontaine-Mazur conjecture.

Conjecture 2.9. *(Fontaine-Mazur) Weakly geometric Galois representations are geometric.*

(Langlands) Any irreducible geometric Galois representation of G_F of dimension n is attached to a cuspidal algebraic automorphic representation of $\mathrm{GL}_n(\mathbb{A}_F)$ *(and conversely).*

We will not say anything about the meaning of the second statement here (we shall say a bit more later for $n = 2$). Both conjectures are known when $n = 1$, in which case it follows from Class field theory and the theory of complex multiplication of abelian varieties. We shall discuss the case $n = 2$ in the next chapter. A striking consequence of the Fontaine-Mazur conjecture is that if ρ is weakly geometric, then the a priori p-adic numbers $\mathrm{trace}(\rho(\mathrm{Frob}_v))$, for $v \notin S$, are algebraic numbers (even sums of Weil numbers!). Moreover, it implies that there are only countably many weakly geometric Galois representations, and in particular, no non-trivial continuous families of such.

Exercise 1. Let F be a finite field and let p be a prime invertible in F. Show that the p-adic cyclotomic character has an open image in $\mathbb{Z}_p^*$. Under which condition is it surjective ?

Exercise 2. Let F be a finite extension of $\mathbb{Q}_p$. Show that there is a number field E such that $E \times_{\mathbb{Q}} \mathbb{Q}_p = F$. Using the global reciprocity map rec_E, show that if χ is the p-adic cyclotomic character of F, then $\chi \circ \mathrm{rec}_F$ is the composite of the norm $F^\times \rightarrow \mathbb{Q}_p^\times$ with the character $\mathbb{Q}_p^\times \rightarrow \mathbb{Z}_p^\times$ sending p to 1 and which is the identity on $\mathbb{Z}_p^\times$.

Exercise 3. Consider the elliptic curve $E : y^2 + xy + y = x^3 - x^2 - x$, for which $\Delta = 17$ and $j = 3^3.11^3/17$. Show that $\rho_{E,p}$ is surjective for $p \equiv 3, 5, 6 \bmod 7$ and $p \geq 5$.

Exercise 4. Show[2] that there are exactly 5 elliptic curves over $\mathbb{F}_2$, namely $y^2 + y = x^3$, $y^2 + y = x^3 + x + 1$, $y^2 + y = x^3 + x$, $y^2 + xy = x^3 + x$, $y^2 + xy = x^3 + x^2 + x$, with respective number of points over $\mathbb{F}_2$: 3, 1, 5, 4 and 2.

Exercise 5. Fix a finite set P of primes and choose for each $p \in P$ an elliptic curve E_p over $\mathbb{F}_p$. Show that there is an elliptic curve E over $\mathbb{Q}$ such that for each $p \in P$, E has good reduction over $\mathbb{Q}_p$ and $\overline{E}_{\mathbb{Q}_p} \simeq E_p$.

Exercise 6. Show that for each finite set P of primes, say different from 2 and 17, there are two non-isomorphic irreducible Galois representations $G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathbb{Q}_5)$, arising from the Tate-module of some elliptic curves over $\mathbb{Q}$, which are unramified at the primes in P and with the same trace of Frob_ℓ for each $\ell \in P$.

Exercise 7. Admit that for each prime ℓ there is an elliptic curve E over $\mathbb{F}_\ell$ such that $|E(\mathbb{F}_\ell)| = 1 + \ell$ (it is a special case of the footnote of Ex. 4). Show that for each prime p, there is an elliptic curve E over $\mathbb{Q}$ such that the representation $G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathbb{F}_p)$ on $E(\overline{\mathbb{Q}})[p]$ is surjective (for instance, construct by a variant of Ex. 6 an E which has split multiplicative reduction at some prime ℓ and with suitable good reduction at some other prime ℓ'). In particular, there is a Galois extension of $\mathbb{Q}$ with Galois group $\mathrm{GL}_2(\mathbb{F}_p)$.

Exercise 8. Show that for p an odd prime, and E an elliptic curve over $\mathbb{Q}_p$, there is some $g \in G_{\mathbb{Q}_p}$ that does not act on $E(\overline{\mathbb{Q}}_p)[p]$ has an homothety. Deduce that if E is an elliptic curve over $\mathbb{Q}$, then $E(\overline{\mathbb{Q}})[p]$ cointains at most two $G_{\mathbb{Q}}$-stable lines if p is odd. What if $p = 2$?

Problem 9. (Algebraic Hecke characters) Let F be a number field. A Hecke-character is a continuous morphism $\eta : F^\times \backslash \mathbb{A}_F^\times \rightarrow \mathbb{C}^\times$. If η is such a character, and if $v \in S(F)$, we denote by $\eta_v : F_v^\times \rightarrow \mathbb{C}^\times$ the restriction of η to F_v^*, it is a continuous character.

[2] By theorems of Tate and Honda, for any prime p and any integer a such that $a^2 \leq 4p$, there exists an elliptic curve E over $\mathbb{F}_p$ such that $|E(\mathbb{F}_p)| = p + 1 - a$. This elliptic curve E is not unique up to isomorphism in general, but it is up to isogeny (over $\mathbb{F}_p$).

– Show that $\eta_v(\mathcal{O}_{F_v}^\times) = 1$ for almost all v, hence that the equality $\eta((x_v)) = \prod_v \eta_v(x_v)$ makes sense and holds for all idèles (x_v).

We say that η is algebraic if for each $\sigma \in \mathrm{Hom}(F,\mathbb{C})$ there is an (necessarily unique) integer a_σ such that if $v \in S(F)_\infty$ is the place induced by σ, then $\eta_v(z) = \sigma(z)^{a_\sigma}\overline{\sigma(z)}^{a_{\overline{\sigma}}}$ if v is complex, and $\eta_v(z) = \epsilon_v(z)z^{a_\sigma}$ for some finite order character $\epsilon_v : F_v^\times \to \{\pm 1\}$ if v is real. The a_σ are called the weights of η. Assume that η is algebraic.

– Show that the subfield of $\mathbb{C}$ generated by the $\eta_v(z)$ for each finite place v and each $z \in F_v^\times$ is a number field (called the coefficient field of *η).*

– (Weil) Fix some pair of field embeddings $\iota_\infty : \overline{\mathbb{Q}} \to \mathbb{C}$ and $\iota_p : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_p$. They define a bijection $\iota_p\iota_\infty^{-1} : \mathrm{Hom}(F,\mathbb{C}) \xrightarrow{\sim} \mathrm{Hom}(F,\overline{\mathbb{Q}}_p)$, so that we may view the a_σ as indexed by this latter set as well. Denote moreover by $v_\sigma \in S(F)_p$ the place above p defined by the element $\sigma \in \mathrm{Hom}(F,\overline{\mathbb{Q}}_p)$. Show that the continuous character $\mathbb{A}_F^\times \to \overline{\mathbb{Q}}_p^\times$ defined by the formula

$$\eta_\lambda((z_v)) = \prod_{v\in S(F)_\mathbb{R}} \epsilon_v(z_v) \prod_{v\in S(F)_f} \iota_p\iota_\infty^{-1}(\eta_v(z_v)) \prod_{\sigma\in\mathrm{Hom}(F,\overline{\mathbb{Q}}_p)} \sigma(z_{v_\sigma})^{a_\sigma}$$

is trivial over kernel of the global reciprocity map rec_F, hence defines a continuous character $\eta_\iota : G_F \to \overline{\mathbb{Q}}_p^\times$. Show that η_ι is unramified outside the finite set $S_p(F) \cup S_\infty(F) \cup \{v \in S(F)_f, \eta_v(\mathcal{O}_{F_v}^\times) \neq 1\}$.

– Define the Norm $|.| : \mathbb{A}_F^\times \to \mathbb{R}^\times$ by the formula $|(x_v)| = \prod_{v\in S(F)} |x_v|_v$. Show that $|.|$ is an algebraic Hecke character. Show that $a_\sigma = 1$ for all σ, that the coefficient field of $|.|$ is $\mathbb{Q}$, and that its associated p-adic Galois character is the p-adic cyclotomic characters.

– If F is a totally real field, show that any algebraic Hecke character of F has the form $|.|^m\eta$ where $m \in \mathbb{Z}$ and where η has finite image (such characters are called Artin Hecke-characters, they are obviously algebraic).

Problem 10. Let E be the elliptic curve $y^2 = x^3 - x$ over $F = \mathbb{Q}(i)$ with $i^2 = -1$ ($\Delta = 2^8$), and fix some prime p.*

– Show that $(x,y) \mapsto (-x,iy)$ defines an endomorphism $[i]$ of E such that $[i]^2 = [-1]$ and that $T_p(E)$ is free of rank 1 over $\mathbb{Z}_p[i] := \mathbb{Z}_p[X]/(X^2+1)$.

– Show that the action of G_F on $E(\overline{F})$ commutes with $[i]$, and that $\rho_{E,p}$ factors through a Galois representation $G_F \to \mathbb{Z}_p[i]^\times$. In particular, $\rho_{E,p}(G_F)$ is abelian.

– (*) Show that there is an algebraic Hecke character η of F with weights 0 and 1 such that $\rho_{E,p} \circ \mathrm{rec}_F$ is a Galois representation attached to η.

– Show that any finite abelian extension of F is contained in the field generated by the (x,y)-coordinates of the N-torsion points of $E(\overline{F})$ for some $N \geq 1$.

3. Modular Galois representations

3.1. Modular forms. We review now the theory of modular forms. Here are some classical references : Shimura "Arithmetic theory of automorphic functions", Ogg "Modular forms and Dirichlet series", Miyake "Modular forms", Serre "Cours d'arithmétique". Part of this theory is easier to understand when we introduce the language of automorphic representations of GL_2 (see e.g. Bump's or Gelbart's books), we shall not adopt this point of view here (but maybe later when we shall deal with quaternion algebras).

3.1.1. *The Poincaré upper half-plane.* Let $\mathbb{H} = \{\tau \in \mathbb{C}, \mathrm{Im}(\tau) > 0\}$ be the Poincaré upper-half plane. The natural projective action of $\mathrm{GL}_2(\mathbb{C})$ on $\mathbb{P}^1(\mathbb{C})$ induces an action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathbb{H}$, and even of $\mathrm{GL}_2(\mathbb{R})^+ = \{g \in \mathrm{GL}_2(\mathbb{R}), \det(g) > 0\}$, given explicitely by the classical formula $\left(\begin{array}{cc} a & b \\ c & d \end{array}\right)\tau = \frac{a\tau+b}{c\tau+d}$. If $k \in \mathbb{Z}$, $f : \mathbb{H} \to \mathbb{C}$, and $\gamma = \left(\begin{array}{cc} a & b \\ c & d \end{array}\right) \in \mathrm{GL}_2(\mathbb{R})^+$, we set

$$(f|_k\gamma)(\tau) = (c\tau + d)^{-k} f(\gamma\tau) \det(\gamma)^{k/2}.$$

One checks at once that this defines a right action[3] of $\mathrm{GL}_2(\mathbb{R})^+$ on the space $\mathcal{O}(\mathbb{H})$ of holomorphic functions on $\mathbb{H}$, hence an action of its discrete subgroup $\mathrm{SL}_2(\mathbb{Z})$ as well by restriction.

For $N \geq 1$, recall that $\Gamma_1(N) \subset \mathrm{SL}_2(\mathbb{Z})$ is the finite index subgroup whose elements are upper unipotent modulo N, i.e. of the form $\left(\begin{array}{cc} a & b \\ c & d \end{array}\right)$ with $c = 0 \bmod N$ and $a = d = 1 \bmod N$. It is torsion-free when $N \geq 4$ and acts freely on $\mathbb{H}$ in this case. The group $\Gamma_1(N)$ is normalized by the slightly bigger subgroup $\Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$ whose elements only satisfy $c = 0 \bmod N$, and $\gamma \mapsto d \bmod N$ induces a group isomorphism $\Gamma_0(N)/\Gamma_1(N) \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^\times$. We shall view this way any (Dirichlet) character $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ as a character of $\Gamma_0(N)$.

3.1.2. *Modular forms.* A (holomorphic) modular form of level N, weight k, and character ε, is a holomorphic function f on $\mathbb{H}$ such that (i) and (ii) below hold :

(MF1) $f|_k\gamma = \varepsilon(\gamma)f$ for all $\gamma \in \Gamma_0(N)$,

(MF2) f is *holomorphic at the cusps* : for all $\sigma \in \mathrm{SL}_2(\mathbb{Z})$, the function $f|_k\sigma$ has an expansion as a power series in $e^{2i\pi\tau/M}$ for some integer $M \geq 1$, with only ≥ 0 exponents.

Lemma 3.2. *(MF2) is equivalent to the similar property where $\sigma \in \mathrm{SL}_2(\mathbb{Z})$ is replaced by $\sigma \in \mathrm{GL}_2(\mathbb{Q})^+$.*

Proof — Remark that any element in $\mathbb{P}^1(\mathbb{Q})$ may be written $\gamma(\infty)$ for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$: write $x = a/b$ with $(a, b) = 1$ and use a Bezout relation to define a γ such that $\gamma(\infty) = x$. It follows that

$$\mathrm{GL}_2(\mathbb{Q})^+ = \mathrm{SL}_2(\mathbb{Z}).B$$

where B is the subgroup of upper triangular matrices in $\mathrm{GL}_2(\mathbb{Q})^+$. If f has an expansion as a power series in $e^{2i\pi\tau/M}$ for some integer $M \geq 1$, with only ≥ 0 exponents, then so does $f(a\tau + b)$ for $a \in \mathbb{Q}^\times$ and $b \in \mathbb{Q}$ (increasing M if necessary). The first part of the lemma follows. □

Note that if (MF1) is satisfied, then (MF2) above only has to be checked for σ in a system of representative of the finite set of orbits

$$\Gamma_1(N)\backslash\mathrm{GL}_2(\mathbb{Q})^+/B = \Gamma_1(N)\backslash\mathbb{P}^1(\mathbb{Q}),$$

[3] For $k = 0$ it is the natural induces action on $\mathcal{O}(\mathbb{H})$. For $k \neq 0$, the reason for this is that the map $\mathrm{GL}_2(\mathbb{R})^+ \to \mathcal{O}(\mathbb{H})^\times$, $\gamma \mapsto (\tau \mapsto \frac{\det(\gamma)^{1/2}}{c\tau+d})$ defines a 1-cocycle of $\mathrm{GL}_2(\mathbb{R})^+$ on $\mathcal{O}(\mathbb{H})$. This is an easy computation, which is obvious for its square, which is the Jacobian cocycle: for $\gamma = \left(\begin{array}{cc} a & b \\ c & d \end{array}\right) \in \mathrm{GL}_2(\mathbb{R})^+$, $\frac{\partial\gamma\tau}{\partial\tau} = \frac{\det(\gamma)}{(c\tau+d)^2}$.

called *the cusps* of $\Gamma_1(N)$.

Modular forms of level N, weight k, character ε form a complex sub-vectorspace of $\mathcal{O}(\mathbb{H})$ denoted by $M_k(N,\varepsilon)$. When in (MF2) we replace "≥ 0 exponents" by "> 0 exponents", we say that f is a *cuspform*. Cuspforms form a sub-vector space $S_k(N,\varepsilon) \subset M_k(N,\varepsilon)$.

Definition 3.3. *As* $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_1(N)$*,* $f(\tau+1) = f(\tau)$ *for* $f \in M_k(N)$*, so* $f(\tau) = \sum_{n\geq 0} a_n q^n$ *where* $q := e^{2i\pi\tau}$*. This specific expansion is called the q-expansion of* f*.*

Note that $a_0 = 0$ if f is a cuspform, the converse being true in general only if $N = 1$ as $\mathrm{SL}_2(\mathbb{Z})$ has only one cusp.

An important fact is that $M_k(N,\varepsilon)$ *is finite dimensional.* This may be proved for instance by integrating df/f, for $f \in M_k(N,\varepsilon)$, on the boundary of a fundamental domain of $\Gamma_1(N)$ acting on $\mathbb{H}$ (a finite union of transformations of the well-known domain for $\mathrm{SL}_2(\mathbb{Z})$) and noticing that if f vanishes say at ∞ to a sufficiently high order explicit in terms of N and k, then $f = 0$ (see e.g. Serre "Cours d'arithmétique" for this point of view detailled when $N = 1$). More conceptualy, form each k and N there is a line bundle L_k on the compact Riemann surface $\Gamma_1(N)\backslash(\mathbb{H}\coprod\mathbb{P}^1(\mathbb{Q}))$ whose sections are exactly the modular forms of weight k level N (ε varying). It follows from the computation of this line bundle and Riemann-Roch's formula that there are explicit formulas formulas for the dimension of $S_k(N,\varepsilon)$ whenever $k \geq 2$ (see Shimura's book for $\oplus_\varepsilon S_k(N,\varepsilon)$, there is a formula due to Cohen-Oesterle for the individual summands).

One can show that $S_k(N,\varepsilon)$ has an explicit complement in $M_k(N,\varepsilon)$ generated by *Eisenstein series* (see Miyake's book), so that the really mysterious part of $M_k(N,\varepsilon)$ is $S_k(N,\varepsilon)$. As $-1 \in \Gamma_0(N)$, note that $M_k(N,\varepsilon) = 0$ if $\varepsilon(-1) \neq (-1)^k$. Moreover, we can show that $M_k(N,\varepsilon) = 0$ if $k \leq 0$, so we assume from now on $k > 0$.

In Serre's *Cours d'arithmetique*, you will find a detailed study of the case $N = 1$ (hence $\varepsilon = 1$ as well). The first nonzero cuspform is Ramanujan's famous Δ function, which is a generator of $S_{12}(1)$, and whose q-expansion is $\Delta = q\prod_{n\geq 1}(1-q^n)^{24}$. As another example, $S_2(11,\varepsilon) = 0$ if $\varepsilon \neq 1$ and $S_2(11,1) = \mathbb{C}f$ where $f = q\prod_{n\geq 1}(1-q^n)^2(1-q^{11n})^2$ (see Shimura's book).

3.3.1. *Hecke operators.* The vector space $M_k(N,\varepsilon)$ is equipped with a natural collection of endomorphisms called Hecke operators. In particular, for each prime ℓ with $(\ell, N) = 1$, we have an operator T_ℓ defined as follows. Let $\Delta(N,\ell) \subset M_2(\mathbb{Z})$ be the subset of matrices with determinant ℓ and congruent to $\begin{pmatrix} 1 & * \\ 0 & \ell \end{pmatrix}$ modulo N.

Lemma 3.4. $\Delta(N,\ell) = \Gamma_1(N)\begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix}\Gamma_1(N) = \coprod_{i=0}^{\ell}\Gamma_1(N)x_i$*, where* $x_i = \begin{pmatrix} 1 & i \\ 0 & \ell \end{pmatrix}$ *if* $i < \ell$ *and* $x_\ell = \delta\begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}$ *where* $\delta \in \Gamma_0(N)$ *is any element mapping to* $\ell \in (\mathbb{Z}/N\mathbb{Z})^\times$*.*

Proof — Note first that we have the inclusions

$$\Delta(N,\ell) \supset \Gamma_1(N)\begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix}\Gamma_1(N) \supset \coprod_{i=0}^{\ell} \Gamma_1(N)x_i.$$

Indeed, the first one is obvious, as well as the second one for the x_i with $i < \ell$. For x_ℓ remark that we may assume that the d-coefficient of δ is divisible by ℓ as the reduction mod ℓ : $\Gamma_1(N) \to \mathrm{SL}_2(\mathbb{F}_\ell)$ is well-known to be surjective for $(N,\ell) = 1$ (see Exercise 2), in which case we even have $x_\ell \in \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix}\Gamma_1(N)$ and we are done.

As a consequence, we may deduce the case $N \geq 1$ to $N = 1$ just by taking the intersection with $\Delta(N,\ell)$. Indeed, if $u \in \Delta_1(N,\ell)$ and $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ are such that $\gamma u \in \Delta_1(N,\ell)$, then we see that $\gamma \in \Gamma_1(N)$.

Consider now the right action of $\mathrm{GL}_2(\mathbb{Q})^+$ on $\mathbb{Z}$-lattices in $\mathbb{Q}^2$ given by $\gamma.\Lambda = {}^t\gamma(\Lambda)$. Then $\mathrm{SL}_2(\mathbb{Z})$ is the stabilizer of $\mathbb{Z}^2$. As $|\mathbb{Z}^2/g(\mathbb{Z}^2)| = |\det(g)|$ for any $g \in M_2(\mathbb{Z})$, the orbit $\Delta(1,\ell).\mathbb{Z}^2$ is exactly the set of sublattices of $\mathbb{Z}^2$ of index ℓ. As ℓ is prime, there are $\ell + 1$ such lattices, which are the $x_i.\mathbb{Z}^2$ for $i = 0, \ldots, \ell$, and we are done. □

Definition 3.5. *Fix $k \in \mathbb{Z}$. If $f : \mathbb{H} \to \mathbb{C}$, we set $T_\ell(f) := \ell^{k/2-1}(\sum_{i=0}^{\ell} f|_k x_i)$.*

Lemma 3.6. *T_ℓ preserves $M_k(N,\varepsilon)$ and $S_k(N,\varepsilon)$. On q-expansions:*

$$T_\ell(\sum_{n\geq 0} a_n q^n) = \sum_{n\geq 0} a_{\ell n} q^n + \varepsilon(\ell)\ell^{k-1}\sum_{n\geq 0} a_n q^{\ell n}.$$

Moreover, T_ℓ and $T_{\ell'}$ commute each other.

Proof — $\Delta(N,\ell)$ is stable by left and right translations by $\Gamma_1(N)$, and by conjugation by $\Gamma_0(N)$. Any coset $\Gamma_1(N)x_i$ is then set to another one by any right translation of an element of $\Gamma_1(N)$, or conjugation by an element of $\Gamma_0(N)$. It follows that if f satisfies (MF1) then so does $T_\ell(f)$. It follows from lemma 3.2 that if f satisfies (MF2) (resp. is a cuspform), then so does $T_\ell(f)$, hence the first statement.

By definition, $(f|_k x_i)(\tau) = \ell^{-k/2} f(\frac{\tau+i}{\ell})$ if $i < \ell$, $(f|_k x_\ell) = \ell^{k/2}\epsilon(\ell)f(\ell\tau)$ if $i = \ell$. The expression for T_ℓ follows then from the relation $\sum_{i=0}^{\ell-1} e^{2i\pi n(\tau+i)/\ell} = 0$ for $(n,\ell) = 1$, $\ell\, q^{n/\ell}$ otherwise. One checks on the q-expansion that T_ℓ and $T_{\ell'}$ commute. □

(The T_ℓ are actually normal, hence semi-simple, for some natural adjunction defined by mean of the *Peterson* product on cuspforms.) A nonzero form $f \in M_k(N,\varepsilon)$ which is a common eigenvector for all the T_ℓ-operators is called an *eigenform.* If f is such a form, and if we write $T_\ell(f) = a_\ell f$ for each ℓ, one can show that the subfield of $\mathbb{C}$ generated by the a_ℓ is a number field, called *the coefficient field of f* (see below when $k = 2$). If f is a cuspform which is "normalized", i.e. whose coefficient a_1 of q in its q-expansion satisfies $a_1 = 1$, then we see from the formula for T_ℓ that $a_\ell(f) = a_\ell$ for each ℓ with $(\ell, N) = 1$: the Hecke eigenvalues can be read off from the q-expansion (see Exercise 4).

Exercise 1. Show that the characteristic polynomial of a finite order element of $\mathrm{SL}_2(\mathbb{Z})$ has the form $X^2 + tX + 1$ where $-2 \leq t \leq 2$. Deduce that $\Gamma_1(N)$ is torsion free if, and only if, $N \geq 4$. What about $\Gamma_0(N)$?

Exercise 2*. Show that for each integer $N \geq 1$, the reduction map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is surjective. As an application, compute the index of $\Gamma_1(N)$ inside $\mathrm{SL}_2(\mathbb{Z})$.

Exercise 3. (Diamond operators) Define $M_k(N)$ as the space of holomorphic functions on $\mathbb{H}$ such that $f|_k\gamma = f$ for all $\gamma \in \Gamma_1(N)$. Show that $(\gamma, f) \mapsto f|_k\gamma$ defines a right action of $\Gamma_0(N)/\Gamma_1(N)$ on $M_k(N)$ and that $M_k(N) = \oplus_\varepsilon M_k(N, \varepsilon)$.

If $d \in (\mathbb{Z}/N\mathbb{Z})^\times$, and $f \in M_k(N)$, we usually write $f|_k\langle d\rangle$ for $f|_k\gamma$ where $\gamma \in \Gamma_0(N)$ is any element with image $d \in (\mathbb{Z}/N\mathbb{Z})^\times$.

Exercise 4. (Statements of Atkin-Lehner theory) For $d \geq 1$ consider the element

$$s = \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q})^+.$$

For $N \geq 1$ and $d|N$, remark that $s\Gamma_1(N)s^{-1} \subset \Gamma_1(N/d)$. Deduce that for $d|N$, $f(\tau) \mapsto f(d\tau)$ defines an injective linear map $u_{d,\varepsilon'} : M_k(N/d, \varepsilon') \to M_k(N, \varepsilon)$, where ε is the composite of ε' and the natural map $(\mathbb{Z}/N\mathbb{Z})^\times \to (\mathbb{Z}/\frac{N}{d}\mathbb{Z})^\times$. How does $u_{d,\varepsilon'}$ act on q-expansions ? Show that for ℓ prime to N, T_ℓ commutes with $u_{d,\varepsilon'}$.

An element of $M_k(N, \varepsilon)$ which lies in the image of $\oplus_{d|N,\varepsilon'} u_{d,\varepsilon'}$ is called an *old form.* A nonzero eigenform $f \in S_k(N, \varepsilon)$ which is not old is called a new form. A theorem of Atkin-Lehner asserts that for each such newform f, *the biggest subspace* $M_k(N)[f] \subset M_k(N)$ *containing* f *and which is a common eigenspace for the* T_ℓ *operators for all but finitely many* ℓ *with* $(\ell, N) = 1$ *has dimension* 1. A newform f has the property that $a_1(f) \neq 0$, in particular $M_k(N)[f] = \mathbb{C}f$ contains unique newform *normalized* so that $a_1(f) = 1$. Last but not least, for each nonzero eigenform $f \in S_k(N, \varepsilon)$, there is a newform g of some level $N'|N$ with the same eigenvalue of T_ℓ for all ℓ prime to N.

Exercise 5. For $N \geq 1$, consider the element

$$w_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q})^+.$$

Show that $w_N\Gamma_1(N)w_N^{-1} = \Gamma_1(N)$. Deduce that the map $f(\tau) \mapsto N^{-k/2}f(-1/N\tau)\tau^{-k}$ induces an isomorphism $M_k(N, \varepsilon) \simeq M_k(N, \varepsilon^{-1})$, whose square is multiplication by $(-1)^k$. Does it commute with T_ℓ for $(\ell, N) = 1$?

3.7. Galois representations attached to modular eigenforms. Let $f \in S_k(N, \varepsilon)$ be an eigenform of weight $k \geq 1$, and write $T_\ell(f) = a_\ell f$ for each prime ℓ which is prime to N. Let E be the coefficient field of f, choose some prime p as well as some p-adic place $\lambda \in S(E)_p$.

THEOREM 3.8. *(Eichler-Shimura, Igusa, Deligne, Ribet) There is a unique irreducible Galois representation* $\rho_{f,\lambda} : G_\mathbb{Q} \to \mathrm{GL}_2(E_\lambda)$ *which is unramified outside* $Np\infty$*, and such that*

$$\det(1 - T\rho_{f,\lambda}(\mathrm{Frob}_\ell)) = 1 - a_\ell T + \varepsilon(\ell)\ell^{k-1}T^2$$

for each prime ℓ *not dividing* Np.

This theorem is fundamental in algebraic number theory, however its proof requires a huge amount of mathematics. The existence of $\rho_{f,\lambda}$ is due to Eichler-Shimura, completed by Igusa, when $k = 2$, to Deligne when $k > 2$ and to Deligne-Serre when $k = 1$. By construction, it is a geometric Galois representation (Eichler-Shimura, Deligne, Sholl). See Appendix A for a sketch of the proof of Eichler-Shimura. The irreducibility assertion is due to Ribet. By the property of $\rho_{f,\lambda}$, we see that

$$\det(\rho_{f,\lambda}) = \varepsilon\chi^{1-k}$$

where χ is the p-adic cyclotomic character. As $\varepsilon(-1) = (-1)^k$, $\det(\rho_{f,\lambda}(c_\infty) = -1$. When $k = 1$ (and only in this case by the computation above of the determinant), Deligne and Serre showed that $\rho_{f,\lambda}$ has a finite image (hence comes from an Artin representation). The determination of $\rho_{f,\lambda|G_{\mathbb{Q}_\ell}}$ for $\ell|N$ or $\ell = p$ is also essentially achieved[4]. It is best formulated in terms of the local Langlands correspondence and the representation of $\mathrm{GL}_2(\mathbb{Q}_\ell)$ associated to f in the case $\ell \neq p$ (Langlands, Carayol); when $\ell = p$ it may described in terms of the p-adic local Langlands correspondence (Faltings, Saito, Breuil, Emerton).

Definition 3.9. *Let $L/\mathbb{Q}_p$ be a finite extension of $\mathbb{Q}_p$. A Galois representation $G_\mathbb{Q} \to \mathrm{GL}_2(L)$ is modular if it is isomorphic to some $\rho_{f,\lambda}$ as above.*

Let $\mathbb{F}_q$ be a finite field. A Galois representation $G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{F}_q)$ is modular if it is isomorphic to the residual representation of a modular Galois representation $\rho_{f,\lambda}$.

(In both definition, we authorize to enlarge the coefficient field if necessary: for instance if L is a finite extension of E_λ, we agree that $\rho_{f,\lambda} \otimes_{E_\lambda} L$ is modular.)

In the past years, several wonderful conjectures about modular Galois representations have been proved, chronologically :

(i) (*Taniyama-Shimura-Weil conjecture*) If E is an elliptic curve over $\mathbb{Q}$, then $V_p(E)^\vee = V_p(E)(-1)$ is modular for each p. It has been proved by Wiles, Taylor-Wiles, Breuil-Conrad-Diamond-Taylor. In this case, the associated modular form f has weight 2 and coefficient field $\mathbb{Q}$. This allowed Wiles to complete the proof of Fermat's last theorem, thanks to previous works of Frey, Hellegouarch and Ribet.

(ii) (*Serre's conjecture*) Any Galois representation $G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{F}_q)$ which is odd (i.e. c_∞ has determinant -1) is modular. This was conjectured by Serre and has been proved by Khare, Khare-Wintenberger, using works of many people.

(iii) (*Fontaine-Mazur conjecture for* GL_2) Any weakly geometric p-adic Galois representation $\rho : G_\mathbb{Q} \to \mathrm{GL}_2(L)$ which is odd, and such that $\rho_{|G_{\mathbb{Q}_p}}$ has distinct Hodge-Tate weights, is modular up to a Tate-twist. This has been reently proved by Kisin and Emerton, again using works of many people, notably the advances in the p-adic Langlands program by Breuil, Colmez and others.

Of course, (iii) implies (i). This kind of statement is called a *modularity theorem.* One general advantage of modular representations is that they can be counted (for instance, we know explicitely $\dim M_k(N, \varepsilon)$), moreover they are easy to manipulate (this will be very clear when we shall deal with congruences). However, the most well-known advantage is that their L-functions are easily shown to be entire (Hecke), something which is conjectured for any geometric Galois representation not containing $\mathbb{Q}_p(m)$ but completely out of reach in general. For instance, before knowing (i) it was not possible to define unconditionnaly the order at $s = 1$ of the L-function of an arbitrary elliptic curve over $\mathbb{Q}$, which was very annoying regarding the Birch-Swinnerton conjecture.

[4] It is, for instance, up to semi-simplification, and even up to *Frobenius semi-simplification* when $\ell \neq p$.

There are many people working on extending the various aspects of these results to higher dimensional Galois representations, or over base fields different from $\mathbb{Q}$, mostly using general automorphic forms and Shimura varieties. It is not the place however to describe these advances.