Geometric and modular Galois representations

1. Galois groups and Galois representations

1.1. First definitions. Let F be a field, $\overline{F}$ a separable algebraic closure of F, and $G_F := \mathrm{Gal}(\overline{F}/F)$ the absolute Galois group of F, *i.e.* the group of F-linear field automorphisms of $\overline{F}$.

For each finite Galois extension K of F inside $\overline{F}$, a basic fact from field theory is that the restriction induces a *surjective* group homomorphism $G_F \to \mathrm{Gal}(K/F)$, so that G_F is isomorphic to the projective limit of the $\mathrm{Gal}(K/F)$ where K runs over all the extensions as above. In particular, G_F is a compact, totally disconnected, topological group for the product (or "Krull") topology: the subgroups of the form $\mathrm{Gal}(\overline{F}/K)$ with $F \subset K \subset \overline{F}$ a finite extension are open, and form a fundamental system of neighborhoods of $1 \in G_F$.

Recall Galois theory: the map $K \subset \overline{F} \mapsto \mathrm{Gal}(\overline{F}/K) \subset G_F$ is a bijection between (possibly infinite) extensions of F inside $\overline{F}$ and closed subgroups of G_F, the inverse bijection being $H \mapsto \overline{F}^H$.

A Galois representation of F is a continuous representation

$$\rho : G_F \to \mathrm{GL}_n(A)$$

where A is some topological, separated, commutative ring.[1]

The normal subgroup $\mathrm{Ker}\,\rho = \rho^{-1}(\{1\})$ is closed, hence of the form $\mathrm{Gal}(\overline{F}/F(\rho))$ for a unique Galois extension $F(\rho)$ of F inside $\overline{F}$. We sometimes call $F(\rho)$ the *extension of F cut out by ρ*, its Galois group $\mathrm{Gal}(F(\rho)/F) \simeq \rho(G_F)$ is a closed subgroup of $\mathrm{GL}_n(A)$. From this perspective, *finding A-valued Galois representations first amounts to finding (possibly infinite) Galois extensions K/F whose Galois group may be realized as a closed subgroup of* $\mathrm{GL}_n(A)$. When A is discrete, note that $\mathrm{Ker}\,\rho$ is an open subgroup, so $F(\rho)$ is a finite extension of F.

We will typically consider the following kind of rings A:

(i) Finite fields, or more generally, finite rings, like $\mathbb{F}_q$ (the finite field with q elements) or $(\mathbb{Z}/p^3\mathbb{Z})[X,Y]/(X^4,(X+Y)^2,Y^7)$. We shall always equip them with the discrete topology.

(ii) $A = \mathbb{C}$ the field of complex numbers, equipped with its usual topology, in which case we talk about *Artin representation.* As there exists a neighborhood of $1 \in \mathrm{GL}_n(\mathbb{C})$ containing no non-trivial subgroup (see the exercices), an Artin representation also factors through the Galois group of a finite Galois extension of F.

(iii) A is a finite extension of $\mathbb{Q}_p$, or more generally a finite dimensional $\mathbb{Q}_p$-algebra. In this case, A is endowed with its natural topology of normed vector space over $\mathbb{Q}_p$, for which it is a topological $\mathbb{Q}_p$-algebra. When A is a field, we talk about p-adic Galois representations.

[1] We usually equip $M_n(A) \times A \simeq A^{n^2+1}$ with the direct product topology and view $\mathrm{GL}_n(A)$ as the closed subset $\{(x,y), \det(x)y = 1\}$.

(iv) Affinoid algebras over $\mathbb{Q}_p$. These are the natural coefficients when considering families of representations with coefficients of type (iii), which are exactly the zero dimensional affinoid algebras. We will say more about them in due time.

(v) Any other interesting topological ring !

For our purposes in this course, we will be mostly interested in p-adic Galois representation $G_F \to \mathrm{GL}_n(L)$ where L is a finite extension of $\mathbb{Q}_p$, and in families of such representations. In the remaining part of this paragraph, we introduce the first natural invariants of such representations : the *residual* representation.

If L is a finite extension of $\mathbb{Q}_p$, we denote by $\mathcal{O}_L$ its ring of p-adic integers, by π_L a uniformizer of $\mathcal{O}_L$, and by $k_L = \mathcal{O}_L/(\pi_L)$. In the following statement, G_F could be replaced by any profinite group.

Lemma 1.2. *Let L be a finite extension of $\mathbb{Q}_p$ and $\rho : G_F \to \mathrm{GL}_n(L)$ a Galois representation. There are $\mathcal{O}_L$-lattices $\Lambda \subset L^n$ which are stable by G_F. The semi-simplification of the representation of G_F on $\Lambda/\pi_L\Lambda \simeq k_L^n$ does not depend on the choice of Λ.*

Recall that the semi-simplification of a representation of a group G on a finite dimensional vector space V over a field k is the direct sum of all the Jordan-Hölder constituents of the $k[G]$-module V. We usually denote it by V^{ss}. In this definition, we take multiplicities into account: $\dim_k V = \dim_k V^{\mathrm{ss}}$. The representation V is semi-simple iff $V \simeq V^{\mathrm{ss}}$ as $k[G]$-modules. Concretely, if (V_i) is an increasing filtration of sub-representations of V such that V_{i+1}/V_i is irreducible, then $V^{\mathrm{ss}} \simeq \oplus_i V_{i+1}/V_i$.

Proof — As G_F is compact and ρ is continuous, $G = \rho(G_F)$ is a compact subgroup of $\mathrm{GL}_n(L)$. Let Λ be any $\mathcal{O}_L$-lattice inside L^n. Then $\{g \in \mathrm{GL}_n(L), g(\Lambda) = \Lambda\}$ is an open subgroup of $\mathrm{GL}_n(L)$, hence its intersection H with G is an open subgroup of G. In particular, $\Lambda' = \sum_{g\in G} g(\Lambda)$ is a finite sum over a set of representative of G/H, hence is a lattice as $\mathcal{O}_L$ is a DVR, G-stable by construction.

Note that if Λ is a G-stable lattice, so is $\Lambda' = \pi_L^i\Lambda$ for $i \in \mathbb{Z}$, and the multiplication by π_L^i induces a $k_L[G]$-isomorphism $\Lambda/\pi_L\Lambda \xrightarrow{\sim} \Lambda'/\pi_L\Lambda'$. Let now Λ_1 and Λ_2 be two G-stable lattices. Then so are the $L_i := \Lambda_1 + \pi_L^i\Lambda_2$ for $i \in \mathbb{Z}$. Note that $L_i = \Lambda_1$ for $i \gg 0$, $L_i = \pi_L^i\Lambda_2$ for $-i \gg 0$, and $\pi_L L_i \subset L_{i+1} \subset L_i$ for each $i \in \mathbb{Z}$. It follows that we may assume that $\pi_L\Lambda_1 \subset \Lambda_2 \subset \Lambda_1$. We have an exact sequence of $k[G]$-modules

$$0 \to \Lambda_2/\pi_L\Lambda_1 \to \Lambda_1/\pi_L\Lambda_1 \to \Lambda_1/\Lambda_2 \to 0.$$

On the other hand, $\Lambda_2 \subset \Lambda_1 \subset \pi_L^{-1}\Lambda_2$, so the $k_L[G]$-module $\Lambda_2/\pi_L\Lambda_2 \simeq \pi_L^{-1}\Lambda_2/\Lambda_2$ is as well an extension of $\pi_L^{-1}\Lambda_2/\Lambda_1 \simeq \Lambda_2/\pi_L\Lambda_1$ by Λ_1/Λ_2. □

Definition 1.3. *Let L be a finite extension of $\mathbb{Q}_p$ and $\rho : G_F \to \mathrm{GL}_n(L)$ a Galois representation. We denote by $\bar{\rho} : G_F \to \mathrm{GL}_n(k_L)$ the semi-simple representation defined by the previous lemma. It is called the residual representation of ρ.*

An alternative proof for the second-part of the lemma is to appeal to a classical result of Brauer-Nesbitt : two finite-dimensional k-representations V_1 and V_2 of a group G have isomorphic semi-simplifications if and only if for all $g \in G$ we have $\det(1 - tg|V_1) = \det(1 - tg|V_2) \in k[t]$:

LEMMA 1.4. *Let k be a field, R a k-algebra (unital, associative, but non necessarily commutative), and let $M_1, \ldots, M_r$ be finitely many non-isomorphic simple R-modules which are finite dimensional over k. There is an element $e_i \in R$ such that $e_{i|M_i} = \mathrm{id}_{M_i}$ and $e_i(M_j) = 0$ for $j \neq i$.*

In particular, if M and N are two semi-simple R-modules of finite dimension over k, then $M \simeq N$ as R-module if and only if $\det(1 - ta_{|M}) = \det(1 - ta_{|N})$ for all $a \in R$ (Brauer-Nesbitt). When k has characteristic 0, or when $d = \dim(M) = \dim(N)$ satisfies $d! \in k^\times$, it is enough to assume that $\mathrm{trace}(a|M) = \mathrm{trace}(a|N)$ for all $a \in R$.

Proof — We may replace R by its image in $\mathrm{End}_k(\oplus_i M_i)$, so we may assume that R is finite dimensional over k, and even semi-simple as it has a faithful semi-simple module. Wedderburn-Artin theory shows that $R \simeq \prod_i M_{d_i}(D_i^{\mathrm{opp}})$ where $D_i = \mathrm{End}_R(M_i)$ is a division k-algebra (Schur's lemma) and $d_i = \dim_{D_i}(M_i)$. The diagonal element $(0, .., 1, .., 0)$ with 1 at place i and 0 elsewhere in this composition does the trick. To check the second statement, let M_i be the simple constituents of $M \oplus N$ and denote by m_i and n_i the respective multiplicity of M_i in M and N. If $e_i \in A$ is as in the first part, then the equality of characteristic polynomials, or of traces in the second case, applied to e_i shows that $n_i = m_i$. □

We shall be mostly interested in $G_{\mathbb{Q}}$, or in G_F for a number field F. To give interesting examples of Galois representations, it is necessary to review a bit the structure of these Galois groups.

Exercise 1. Let $|||.|||$ be a triple norm on $M_n(\mathbb{C})$. Show that $U = \{M, |||M - 1||| < 1\}$ is an open subset of $\mathrm{GL}_n(\mathbb{C})$ and that the unique subgroup of $\mathrm{GL}_n(\mathbb{C})$ inside U is $\{1\}$. (Observe first that if $M \in U$, each eigenvalue λ of M satisfies $|\lambda - 1| < 1$.)

Exercise 2. Let $\rho : G_F \to \mathrm{GL}_n(\overline{\mathbb{Q}}_p)$ be a continuous representation. Show that $\rho(G_F) \subset \mathrm{GL}_n(L)$ for some finite extension L of $\mathbb{Q}_p$ inside $\overline{\mathbb{Q}}_p$ (use Baire's theorem).

Exercise 3. Let $G \subset \mathrm{GL}_n(\mathbb{Z}_p)$ be a subgroup. Show that G has a unique stable lattice in $\mathbb{Q}_p^n$ (up to homotheties) if, and only if, G acts irreducibly on $\mathbb{F}_p^n$.

Exercise 4. Let $G \subset \mathrm{GL}_2(\mathbb{Z}_p)$ be the subgroup of matrices which are upper triangular modulo p. Show that up to homotheties, G has exactly two stable lattices in $\mathbb{Q}_p^2$, and that the two residual representations are non isomorphic. Generalize to dimension n.

Exercise 5^*. Show that $G \subset \mathrm{GL}_n(\mathbb{Q}_p)$ has only finitely many stable lattices in $\mathbb{Q}_p^n$ (up to homotheties) if, and only if, G acts irreducibly on $\mathbb{Q}_p^n$.

Open problem (to the author). Let $\rho_n : \mathrm{GL}_2(\mathbb{Z}_p) \to \mathrm{GL}_{n+1}(\mathbb{Q}_p)$ be the n-th symmetric power of the standard representation ρ_1, what is the number $\ell(p, n)$ of homothety classes of $\mathbb{Z}_p$-lattices of $\mathbb{Q}_p^{n+1}$ which are stable by $\mathrm{GL}_2(\mathbb{Z}_p)$? Much easier subproblem : show that $\ell(p, n) = 1$ if and only if $n < p$, and compute $\ell(p, p)$.

1.5. The local-global structure of the Galois group of a number field. When F is a finite field with q elements, $G_F \simeq \widehat{\mathbb{Z}}$, a canonical topological generator of G_F being the *arithmetic Frobenius* element $\mathrm{frob}_F : x \mapsto x^q$. The *geometric Frobenius* is by definition the inverse of the arithmetic Frobenius, and will be denoted by $\mathrm{Frob}_F \in G_F$.

When F is a finite extension of $\mathbb{Q}_p$, the structure of G_F is rather well-known. There is a natural filtation of G_F by closed normal subgroups, called the ramification filtration (see Serre's *Corps locaux*, or maybe Berger and Fargues lectures). The first subgroup of this filtration is the inertia group

$$I_F = \mathrm{Gal}(\overline{F}/F^{\mathrm{ur}})$$

where $F^{\mathrm{ur}} \subset \overline{F}$ is the maximal unramified extension of F. Explicitely, F^{ur} is the abelian extension generated by all roots of unity of order prime to p. As is well known, the natural map $G_F/I_F \to \mathrm{Gal}(\overline{k_F}/k_F)$ is an isomorphism, so we shall view Frob_{k_F} as an element of G_F/I_F. The subgroup I_F has a unique pro-p-Sylow subgroup $P_F \subset I_F$ called the wild inertia subgroup, and $I_F/P_F \simeq \prod_{\ell \neq p} \mathbb{Z}_\ell$. Explicitely, I_F/P_F is the Galois group of the extension F^{t} of F^{ur} generated by the $\pi_F^{1/n}$ where n is prime to p (this does not depend on the choice of π_F). The subgroup P_F is normal in G_F and the action by conjugation of Frob_{k_F} on I_F/P_F is the multiplication by q, where $q = |k_F|$. Local class field theory provides a canonical *reciprocity* map

$$\mathrm{rec}_F : F^\times \to G_F^{\mathrm{ab}}$$

sending π_F to the geometric Frobenius in G_F/I_F and sending $\mathcal{O}_F^\times$ isomorphically onto the image of I_F in G_F^{ab}. Thus the reciprocity map induces an isomorphism $\widehat{F^\times} \to G_F^{\mathrm{ab}}$, where $\widehat{F^\times}$ is the completion of $F^\times$ with respect to all the open subgroups of finite index. For instance, $\widehat{\mathbb{Q}_p^\times} \simeq \widehat{\mathbb{Z}} \times \mathbb{Z}_p^\times \simeq G_{\mathbb{Q}_p}^{\mathrm{ab}}$. For other properties of the reciprocity map, see Serre's *Corps locaux* or Neukirch's *Class field theory*.

For sake of completeness, recall that as $\mathbb{C}$ is algebraically closed we have $G_{\mathbb{C}} = \{1\}$ and $G_{\mathbb{R}} = \mathbb{Z}/2\mathbb{Z}$. We convene that $\mathbb{C}/\mathbb{R}$ is ramified and set $I_{\mathbb{R}} = G_{\mathbb{R}}$. In these cases, we define

$$\mathrm{rec}_{\mathbb{R}} : \mathbb{R}^\times \to G_{\mathbb{R}}^{\mathrm{ab}} = G_{\mathbb{R}}$$

as the morphism with kernel $\mathbb{R}_{>0}^\times$, and $\mathrm{rec}_{\mathbb{C}}$ is the trivial morphism $\mathbb{C}^* \to G_{\mathbb{C}}$.

When F is a number field, the structure of G_F is not so well known. Recall that the Kronecker-Weber theorem asserts that the naural surjection $G_{\mathbb{Q}} \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{cycl}}/\mathbb{Q}) = \widehat{\mathbb{Z}}^\times$ induces an isomorphism $G_{\mathbb{Q}}^{\mathrm{ab}} \simeq \widehat{\mathbb{Z}}^\times$. Here are two famous open problems:

CONJECTURE 1.6. *(Shafarevic) The closed subgroup of $G_{\mathbb{Q}}$ generated by the commutators is a free pro-finite group over countably many generators.*

(Galois inverse problem) Any finite group is a quotient of $G_{\mathbb{Q}}$.

In some sense, these conjectures say that $G_{\mathbb{Q}}$ is not so interesting as an abstract group. On the other hand, $G_{\mathbb{Q}}$ has an extra "local-global" structure that usually carries a deep arithmetic information.

Denote by $S(F)$ the set of places (or equivalence classes of valuations) of the number field F. If S is a subset of $S(F)$ we shall write S_f for the subset of finite places in F, S_∞ for the subset of archimedean places, and we shall use various other suggestive notations like $S_p \subset S$ for the subset of places above the prime p, or $S_{\mathbb{R}} \subset S$ for the subset of real places in S. For each $v \in S(F)$, denote by F_v the completion of F with respect to v. Let $\iota_v : \overline{F} \to \overline{F_v}$ be a field embedding extending $F \to F_v$.

It defines a continuous group homomorphism $\iota_v^* : G_{F_v} \to G_F$, the conjugacy class of which in G_F does not depend on the choice of ι_v. The local-global structure alluded above is this collection of conjugacy classes of morphisms $G_{F_v} \to G_F$ for all $v \in S(F)$.

If $S \subset S(F)$ we denote by $F_S \subset \overline{F}$ the maximal algebraic extension unramified outside S, *i.e.* such that $\iota_v(F_S) \subset F_v^{\rm ur}$ for each $v \notin S$ and each ι_v. Set

$$G_{F,S} = \mathrm{Gal}(F_S/F).$$

By definition, $G_{F,S}$ is the quotient of G_F by the closed normal subgroup generated by the I_{F_v} for all $v \notin S$. For each $v \notin S$, the maps $\iota_v^* : G_{F_v} \to G_{F,S}$ factor through $G_{k_{F_v}}$, hence $G_{F,S}$ contains a canonical conjugacy class:

$$\mathrm{Frob}_v := \bigcup_{\iota_v} \iota_v^*(\mathrm{Frob}_{k_v}) \subset G_{F,S}.$$

We sometimes view Frob_v as an element of $G_{F,S}$ well defined up to conjugacy. For each $v \in S_{\mathbb{R}}$, the maps $\iota_v^* : G_{\mathbb{R}} = G_{F_v} \to G_{F,S}$ send the order two element of $G_{\mathbb{R}}$ to a conjugacy class of *complex conjugations* in $G_{F,S}$ (even in G_F) denoted c_v.

We say that a Galois representation $\rho : G_F \to \mathrm{GL}_n(A)$ is unramified outside S if $\rho(I_{F_v}) = 1$ for each $v \notin S$, or which is the same if it factors through $G_{F,S}$. We also say that ρ is unramified outside some integer N (resp. $N\infty$) if it is unramified outside the set S of places of F dividing N (resp. N or ∞). In this case, it makes notably sense to consider for each $v \notin S$ the characteristic polynomial of $\mathrm{Frob_v} \in G_{F,S}$.

From now on, S will always denote a *finite* subset of $S(F)$. There are several wonderful questions and conjectures about the groups $G_{F,S}$.

CONJECTURE 1.7. *(Shafarevic) Is $G_{F,S}$ topologically finitely generated ?*

("finite" Fontaine-Mazur) Any Galois representation $\rho : G_{\mathbb{Q},S} \to \mathrm{GL}_n(\mathbb{Q}_p)$ such that $\rho(I_{\mathbb{Q}_p})$ is finite has finite image.

The general conjecture of Fontaine-Mazur will be dicussed a bit later. Here are some well-known but important positive results on the $G_{F,S}$.

THEOREM 1.8. *(Minkowski) $G_{\mathbb{Q},\{\infty\}} = \{1\}$.*

(Hermite) For each number field F and any prime p, $\mathrm{Hom}(G_{F,S}, \mathbb{F}_p)$ is a finite dimensional $\mathbb{F}_p$-vector space.

(Cebotarev) The union of the conjugacy classes of Frob_v for all $v \notin S$ is dense in $G_{F,S}$.

Of course Hom means "continuous group homomorphisms" here. The first part of the theorem says that for each number field $F \neq \mathbb{Q}$, there is at least one prime ramified in F. The second part of the theorem follows from Hermite's classical result in geometry of numbers that for each integer $n \geq 1$, there is only finitely many number fields of degree n which are unramified outside S. Note that Cebotarev theorem also holds if we restricts to a density one subset of primes $v \in S(F)\backslash S$.

PROPOSITION 1.9. *Let $L/\mathbb{Q}_p$ be a finite extension and let ρ_1 and ρ_2 be two semi-simple p-adic Galois representations $G_{F,S} \to \mathrm{GL}_n(L)$. Then $\rho_1 \simeq \rho_2$ if, and only if, for each $v \notin S$ we have $\mathrm{trace}(\rho_1(\mathrm{Frob}_v)) = \mathrm{trace}(\rho_2(\mathrm{Frob}_v))$.*

We leave as an exercise to prove a similar statement if L is a finite field (if $p = \mathrm{char}(L) > 0$ and $p \le n$, use the full characteristic polynomial).

Proof — Assume that the trace equality holds for all $v \notin S$. So the $T_i = \mathrm{trace}(\rho_i) : G_{F,S} \to L$ are two continuous functions that coincide over the dense subset of conjugacy classes of Frob_v for $v \notin S$, thus they are equal. We conclude by lemma 1.4 applied to $k = L$, $R = L[G_{F,S}]$, $M = \rho_1$ and $N = \rho_2$. □

Let us end this paragraph by describing the abelianization of G_F when F is a number field. Recall that the idèles $\mathbb{A}_F^\times$ of F is the subgroup of $\prod_{v \in S(F)} F_v^\times$ whose elements (x_v) satisfy $x_v \in \mathcal{O}_{F_v}^\times$ for almost all v (i.e. all but maybe finitely many). It is a locally compact topological space for the product topology. We have a diagonal embedding $F^\times \to \mathbb{A}_F^\times$ with discrete image, as well as closed embeddings $F_v^\times \to \mathbb{A}_F^\times$, $x \mapsto (1, \dots, 1, x, 1, \dots)$ (at place v) for each v. As Galois number fields are unramified outside finitely many primes, the collection of maps $\mathrm{rec}_{F_v} : F_v^\times \to G_{F_v}^{\mathrm{ab}}$, together with the ι_v^*, define a continuous map

$$\mathrm{rec}_F : \mathbb{A}_F^\times \longrightarrow G_F^{\mathrm{ab}}$$

called the global reciprocity map (as the target is abelian, the conjugacy class of morphisms ι_v^* is a well-defined and unique morphism for each v). The main theorem of global class field theory shows that rec_F *is surjective and its kernel is the closed subgroup generated by* $F^\times$ *and the connected components of* 1 *in* $F_v^\times$ *for each archimedean* $v \in S(F)$. In particular, an exercise on idèles (do it!) shows that:

THEOREM 1.10. *(Global class field theory)* rec_F *induces an exact sequence*

$$1 \longrightarrow U_F \backslash (\{\pm 1\}^{S(F)_{\mathbb{R}}} \times \prod_{v \in S(F)_f} \mathcal{O}_{F_v}^\times) \longrightarrow G_F^{\mathrm{ab}} \longrightarrow \mathrm{Cl}(\mathcal{O}_F) \longrightarrow 1$$

where U_F *is the closure of* $\mathcal{O}_F^\times$ *inside the left hand side, diagonally embedded*[2]*, and where* $\mathrm{Cl}(\mathcal{O}_F)$ *is the ideal class group of* $\mathcal{O}_F$.

COROLLARY 1.11. $G_{F,S}^{\mathrm{ab}}$ *sits in a similar sequence with* $S(F)$ *replaced by* S *everywhere.*

For many results about local and global Galois groups, see Serre's *Corps locaux*, Neukirch's *Class field theory* and the book *Cohomology of number fields*, by Neukirch, Schmidt and Wingberg. Class field theory gives a description of all the 1-dimensional Galois representations. (There are however still two unknown: the position of U_F inside the idèles ("Leopold's conjecture") and the finite group $\mathrm{Cl}(\mathcal{O}_F)$.) Generalization of this picture to the higher dimensional Galois representations is one of the main aim of algebraic number theory, mostly contained in the theory of automorphic forms and in the Langlands program in its various aspects.

Exercise 1. Let $F \to F'$ *be a field embedding. Let* $i, j : \overline{F} \to \overline{F'}$ *be two extensions of this embedding and* $i^*, j^* : G_{F'} \to G_F$ *be the associated group homomorphisms. Show that there exists some* $h \in G_F$ *such that* $h i^*(g) h^{-1} = j^*(g)$ *for all* $g \in G_{F'}$.

Exercise 2. Show that the algebraic numbers over $\mathbb{Q}$ *are dense in* $\overline{\mathbb{Q}}_p$ *for the* p*-adic topology. Deduce that the morphisms* $G_{F_v} \to G_F$ *are injective.*

[2]For $v \in S(F)_{\mathbb{R}}$, the map $F_v^\times \to \{\pm 1\}$ we are thinking about is the one giving the sign of an element.

Exercice 3. Let F'/F be a finite Galois extension of number fields. Let P be a prime of $\mathcal{O}_F$ and $v \in S(F)$ the associated finite place. Show that the image of the maps $G_{F_v} \to G_F \to \mathrm{Gal}(F'/F)$ are exactly the decomposition groups at the primes of F' above P, the image of I_{F_v} being the associated inertia groups.

Exercise 4. Let $\rho : G_{\mathbb{Q},S} \to \mathrm{GL}_n(\mathbb{C})$ be an Artin representation and $M = \mathbb{Q}(\rho)$. Show that $p \notin S$ splits completely in M if, and only if, $\mathrm{trace}(\rho(\mathrm{Frob}_p)) = n$.

Exercise 5. Using Theorem 1.10, show that there is no cyclic extension of degree 3 of $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$ which is unramified outside the primes above 2 and ∞. Deduce that there is no surjective Galois representation[3] $G_{\mathbb{Q},\{\infty,2\}} \to \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$.

Exercise 6. Using corollary 1.11, show that $\mathrm{rec}_{\mathbb{Q}}$ induces an isomorphism $\prod_{p\in S_f} \mathbb{Z}_p^* \to \mathrm{G}_{\mathbb{Q},S}^{\mathrm{ab}}$. Determine Frob_ℓ for $\ell \notin S$ via this isomorphism. Let $\mathbb{Q}_S^{\mathrm{cycl}} \subset \overline{\mathbb{Q}}$ be the field generated by all the roots of unity of order n such that n has all its prime divisors in S, show that the natural surjection $G_{\mathbb{Q},S}^{\mathrm{ab}} \to \mathrm{Gal}(\mathbb{Q}_S^{\mathrm{cycl}}/\mathbb{Q})$ is an isomorphism (Kronecker-Weber theorem).

Exercise 7. (Burnside basis theorem) If G is a profinite group and p is a prime, denote by $G(p)$ the maximal pro-p-quotient of G, i.e. the projective limit of the G/H with H open of index a power of p. Show that $G(p)$ is is topologically finitely generated if, and only if, $\dim_{\mathbb{F}_p} \mathrm{Hom}(G, \mathbb{Z}/p\mathbb{Z}) < \infty$, in which case this latter dimension is the minimal number of topological generators of $G(p)$. Deduce that $G_{F,S}(p)$ is topologically finitely generated, and that for p odd, $G_{\mathbb{Q},\{\infty,p\}}(p) \simeq \mathbb{Z}_p$.

(Hint: Reduce first to the case where $G = G(p)$ is a pro-p-group, and even to the case where G is a finite p-group. Show then by induction on $|G|$ that the maximal subgroups of G are normal and of index p.)

Exercise 8. Let $S = S(F)_p \cup S(F)_\infty$, $r_1 = |S(F)_{\mathbb{R}}|$ and $2r_2 = |S(F)_{\mathbb{C}}|$. Show that $G_{F,S}^{\mathrm{ab}}(p) \simeq \mathbb{Z}_p^r \times \Delta$ for some finite abelian p-group Δ and where $r \geq r_2 + 1$. Show that $r = 1$ if $F = \mathbb{Q}$ or if F is a quadratic real field, and that $r = 2$ if F is an imaginary quadratic field. It is believed that $r = r_2 + 1$ in all cases (Leopold's conjecture).

Open problem (to the author). What is the pro-order of $\mathrm{Frob}_v \in G_{\mathbb{Q},S}$, for $v \notin S$? Easy problem : assume that $\infty \in S$, show that $c_\infty \in G_{\mathbb{Q},S}$ has order 2 iff $|S| \geq 2$. Let us mention here the following result of Clozel and the author : if $|S| \geq 3$ and $S \supset \{\infty, p\}$ then $\iota_p^* : G_{\mathbb{Q}_p} \to G_{\mathbb{Q},S}$ is injective.

2. Geometric Galois representations

Artin representations of G_F are always defined over some number fields, hence give rise to a collection of p-adic Galois representations for all primes p. We review now some other important examples of p-adic Galois representations that are associated to algebraic varieties over F.

[3]A theorem of Tate ensures that there is no irreducible Galois representation $G_{\mathbb{Q},\{\infty,2\}} \to \mathrm{GL}_2(\mathbb{F}_{2^m})$ for all $m \geq 1$. It is believed that for any $n \geq 1$ and any prime p, there is only finitely many Galois representations $G_{\mathbb{Q},\{\infty,p\}} \to \mathrm{GL}_n(\overline{\mathbb{F}}_p)$. This would follow from variants to GL_n of Serre's conjecture.

2.1. Tate modules. An especially nice class are the ones arising from Tate modules of commutative algebraic groups over F, that we briefly review now.

Let A be an abelian group. If $N \geq 1$ is an integer, we denote by $A[N]$ the subgroup of elements $a \in A$ such that $Na = 0$. If N and M are co-prime, Bezout's theorem ensures that $A[MN] = A[M] \oplus A[N]$. If p is a prime, we denote by $T_p(A)$ the projective limit of the $A[p^n]$ for $n \geq 1$ and for the transition maps given by multiplication by $p : A[p^{n+1}] \to A[p^n]$, and $V_p(A) = T_p(A)[1/p]$. The abelian group $T_p(A)$ is a $\mathbb{Z}_p$-module in a natural way, called *the p-adic Tate module of A*.

In the following examples, there will be some integer $h \geq 1$ such that $|A[p^n]| = p^{nh}$ for all $n \geq 1$. It is an exercise on finite abelian groups to check that in this case,

$$\forall n \geq 1,\ \ A[p^n] \simeq (\mathbb{Z}/p^n\mathbb{Z})^h,\ \ T_p(A) \simeq \mathbb{Z}_p^h, \ \text{ and } \ T_p(A)/p^nT_p(A) \xrightarrow{\sim} A[p^n].$$

Furthermore, A will be a *discrete G_F-module, i.e.* a $\mathbb{Z}[G_F]$-module such that the stabilizer in G_F of any $a \in A$ is an open subgroup of G_F. This implies that $T_p(A)$ defines a Galois representation $G_F \to \mathrm{GL}_h(\mathbb{Z}_p)$, its reduction modulo p beeing $A[p] \simeq \mathbb{F}_p^h$. Similarily, if $A[N] \simeq (\mathbb{Z}/N\mathbb{Z})^h$ it defines a Galois representation $G_F \to \mathrm{GL}_h(\mathbb{Z}/N\mathbb{Z})$ (*the N-torsion representation associated to A*). The residual representation of $V_p(A)$ is the semi-simplification of $A[p]$.

2.2. The cyclotomic character. Apply this to the multiplicative group

$$A = \mathbb{G}_m(\overline{F}) = \overline{F}^\times,$$

in which case we also set $\mu_N(\overline{F}) = A[N]$. Of course, $|\mu_N(\overline{F})| = N$ if $N \in F^\times$ and $\mu_p(\overline{F}) = 0$ if $pF = 0$. Thus $T_p(A) = 0$ if $pF = 0$, $T_p(A) \simeq \mathbb{Z}_p$ otherwise, and $\mu_N(\overline{F}) \simeq \mathbb{Z}/N\mathbb{Z}$ if $N \in F^\times$. Using the obvious action of G_F on A, we obtain for $p \in F^\times$ a continous character

$$\chi : G_F \to \mathrm{Aut}_{\mathbb{Z}_p}(T_p(A)) = \mathbb{Z}_p^\times$$

called the *p-adic cyclotomic character of G_F*. For $N \in F^\times$, the *mod N cyclotomic character* is the character $G_F \to (\mathbb{Z}/N\mathbb{Z})^\times$ defined by $\mu_N(\overline{F})$. By construction, $F(\chi) = \cup_{n\geq 1} F(\mu_{p^n}(\overline{F})) \subset \overline{F}$.

When $F = \mathbb{R}$, χ is the non-trivial character of $G_\mathbb{R} = \mathbb{Z}/2\mathbb{Z}$.

When F is a finite field of characteristic $\ell \neq p$, this Galois representation of $G_F = \widehat{\mathbb{Z}}$ is the one mapping Frob_F to $|F|^{-1} \in \mathbb{Z}_p^*$ by definition of Frob_F.

When F is a finite extension of $\mathbb{Q}_\ell$ and $(N, \ell) = 1$, then $X^N - 1$ is separable over k_F so $A[N] = \mu_N(\overline{F}) \subset F^{\mathrm{ur}}$, and χ factors through a character of $G_F/I_F = G_{k_F}$ whenever $p \in F^*$. As the reduction "mod π_F" induces an bijection $\mu_N(\overline{F}) \xrightarrow{\sim} \mu_N(\overline{k_F})$ for $N \in F^\times$, we see that this latter character *is* nothing but the p-adic cyclotomic character of G_{k_F}. The case $\ell = p$ is subtler; a useful way to describe χ is in terms of the reciprocity map: $\chi \circ \mathrm{rec}_F : F^* \to \mathbb{Q}_p^*$ is the composition of the norm $F^* \to \mathbb{Q}_p^*$ with the character sending p to 1 and which is the identity on $\mathbb{Z}_p^*$ (see the exercises).

When F is a number field, the bijections $\mu_N(\overline{F}) \xrightarrow{\sim} \mu_N(\overline{F_v})$ ensure that for each $v \in S(F)$, $\chi_{|G_{F_v}}$ is the p-adic cyclotomic character of G_{F_v}. In particular, *χ is the unique character $G_F \to \mathbb{Z}_p^\times$ unramified outside (the primes dividing) p, ∞, such that for a finite place v not dividing p, ∞, we have $\chi(\mathrm{Frob}_v) = |k_{F_v}|^{-1} \in \mathbb{Z}_p^\times$.* A simple but interesting application of this is the following classical result.

PROPOSITION 2.3. *(Gauss) For each integer $N \geq 1$, the N-th cyclotomic polynomial is irreducible over $\mathbb{Q}$.*

Proof — Indeed, $\chi_N : G_{\mathbb{Q}} \to (\mathbb{Z}/N\mathbb{Z})^\times$ is unramified outside the primes ℓ dividing N and ∞, and for such an ℓ, $\chi_N(\mathrm{Frob}_\ell) = \ell^{-1} \in (\mathbb{Z}/N\mathbb{Z})^\times$. As those elements generate $(\mathbb{Z}/N\mathbb{Z})^\times$ when ℓ varies, χ_N is surjective, thus $\mathbb{Q}(\chi_N) = \mathbb{Q}(e^{2i\pi/N})$ has degree $\varphi(N)$ over $\mathbb{Q}$, and the result follows. □

DEFINITION 2.4. *(Tate twist) If V is a Galois representation of G_F on a $\mathbb{Q}_p$-vectorspace, and if $i \in \mathbb{Z}$, we denote by $V(i)$ the representation V twisted by the character χ^i.*

2.5. The Tate module of an elliptic curve. Assume now that E is an elliptic curve over F, that is a projective, geometrically connected, and smooth, algebraic curve over F of genus 1, equipped with a rational point $O \in E(F)$. As is well-known, E may be embedded as a non-singular cubic of $\mathbb{P}^2_F$ in such a way that the projective line at infinity meets O as a triple (flex) point. The affine part of E has then a *Weierstrass equation* of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in F. \tag{2.1}$$

The non-singularity of this plane curve is expressed in the non-vanishing of its *discriminant*, which some explicit element[4] $\Delta \in \mathbb{Z}[a_1, \ldots, a_6]$. Conversely, any plane curve defined by such an equation with non-zero Δ defines an elliptic curve over F, by taking the closure in $\mathbb{P}^2_F$. The Weierstrass equation is non-unique however.[5]

Recall that the relation "*$P+Q+R = O$ if, and only if, there is a projective line in $\mathbb{P}^2$ whose intersection with E is P, Q, R (with multiplicities)*" defines an abelian group structure on $A = E(\overline{F})$ with identity element O. This abelian group is a discrete G_F-module. The addition in A actually comes from an F-morphism $E \times E \to E$, hence so does the multiplication by N, often denoted by $[N] : E \to E$, for any integer $N \geq 1$. It can be shown that $[N]$ is finite of degree N^2, étale if $N \in F^*$. We shall content ourselves with the following proposition here.

PROPOSITION 2.6. *$A[N] \simeq (\mathbb{Z}/N\mathbb{Z})^2$ if $N \in F^\times$ and $T_p(A) \simeq \mathbb{Z}_p^2$ if $p \in F^*$.*

Proof — We only have to show the assertion on $A[N]$. Remark first that if F is algebraically closed, and if $F \to F'$ is a field embedding, then $E(F)[N]$ is finite if and only if $E(F')[N]$ is finite, in which case they are equal, as $E(F)[N]$ is (the F-points of) the closed F-subvariety $[N]^{-1}(\{O\})$ of E. When $F = \mathbb{C}$ the abelian group $E(\mathbb{C})$ is a compact complex torus $\mathbb{C}/\Lambda$ by Weierstrass theory, so $A[N] \simeq \frac{1}{N}\Lambda/\Lambda \simeq (\mathbb{Z}/N\mathbb{Z})^2$. By the remark above, this concludes the proof when F is any field that embeds into $\mathbb{C}$, and in particular when F is finitely generated

[4]Following Silverman, $\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$ where $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$, $b_6 = a_3^2 + 4a_6$ and $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$. The important property of Δ is that the Weierstrass plane curve, viewed as a scheme over $\mathbb{Z}[a_1, \ldots, a_6]$, is smooth exactly over $\mathbb{Z}[a_1, \ldots, a_6][\Delta^{-1}]$. When $a_1 = a_3 = a_2 = 0$, to which we can always reduce when 6 is invertible, we essentially have the usual formula $\Delta = -16(4a_4^3 + 27a_6^2)$.

[5]Using the Riemann-Roch theorem, we may show that it is unique up to changes of coordinates of the form $x = u^2x' + r$ and $y = u^3y' + su^2x' + t$ where $u, r, s, t \in F$ and $u \neq 0$, see Silverman's book Chap. III.

over $\mathbb{Q}$. For a general F of characteristic 0, remark that E is always defined over its finitely generated subfield $F_0 = \mathrm{Frac}(\mathbb{Z}[a_1, \dots, a_6])$, hence we are done by applying the remark again (this method is called "Lefschetz principle"). Let us postpone the case where F has positive characteristic. □

Assume that F is complete for some discrete valuation v, let $\mathcal{O}$ be its valuation ring and k its residue field. An *integral* Weierstrass equation for E is an equation as in (2.1) such that $a_i \in \mathcal{O}$ for each i. We say that E has good reduction over F if, up to a projective linear change of coordinates in $\mathbb{P}^2_F$, E possesses an integral Weierstrass equation with $\Delta \in \mathcal{O}^\times$. We assume now that this is the case, and we fix such an integral Weierstrass equation. Denote by $\overline{E}$ the elliptic curve[6] over k obtained by reducing this equation modulo the maximal ideal of $\mathcal{O}$. The natural reduction map $\mathbb{P}^2(\mathcal{O}) = \mathbb{P}^2(F) \to \mathbb{P}^2(k)$ induces a natural reduction map $E(F) \to \overline{E}(k)$.

Proposition 2.7. *(Good reduction case) This map is a surjective group homomorphism. Denote by $E_0(F)$ its kernel and by m_F the maximal ideal of F. The map $(x, y) \mapsto x/y$ induces a group isomorphism $E_0(F) \xrightarrow{\sim} m_F$ if we endow this last set with the formal group law defined by E.*

In particular, for each integer $N \geq 1$ in $\mathcal{O}^\times$, $[N] : E_0(F) \to E_0(F)$ is bijective and the reduction map induces an isomorphism $E(F)[N] \xrightarrow{\sim} \overline{E}(k)[N]$.

Proof — As $\Delta \in \mathcal{O}^\times$, the integral Weierstrass model of E is smooth over $\mathcal{O}$, hence $E(F) = E(\mathcal{O}) \to \overline{E}(k)$ is surjective by Hensel's lemma. The reduction map is a group homomorphism by definition of the group law, as we may always re-scale any line in $\mathbb{P}^2$ so that its coefficients are in $\mathcal{O}$ and one of them in $\mathcal{O}^\times$.

Consider now the change of projective linear coordinates on $\mathbb{P}^2_{\mathcal{O}}$ sending O to $(0, 0) \in \mathbb{A}^2$ given by $(z, w) = (-x/y, 1/y)$; the Weierstrass equation becomes

$$w = z^3 + a_1 zw + a_2 z^2 w + a_3 w^2 + a_4 z w^2 + a_6 w^3.$$

It follows that if $z \in m_F$ then there is one, and only one, $w \in F$ such that $(z, w) \in E_0(F)$, in which case $w \in m_F$ as well, namely

$$w = z^3(1 + a_1 z + (a_1^2 + a_2)z^2 + \cdots) \in \mathbb{Z}[a_1, \dots, a_6][[z]].$$

This shows that the coordinate $z : E_0(F) \xrightarrow{\sim} m_F$ is bijective. The group law is easily "computed" in terms of the coordinate z: if R is the polynomial ring $\mathbb{Z}[a_1, \dots, a_6]$, there exists an element

$$\mathcal{F}(u, v) \in R[[u, v]],\ \mathcal{F}(u, v) \equiv u + v \bmod (u, v)^2,$$

such that whenever $P_i = (z_i, w_i) \in E_0(F)$, $i = 1, 2, 3$ such that $P_1 + P_2 = P_3$, then $z_3 = \mathcal{F}(z_1, z_2)$. It follows that for each integer $N \geq 1$, there is an element $\mathcal{F}_N \in R[[z]], \mathcal{F}_N(z) \equiv Nz \bmod (z^2)$, such that $[N] : E_0(F) \to E_0(F)$ is $z \mapsto \mathcal{F}_N(z)$. (See Silverman's book Chap. IV §1 for some details about the computations abovem as well as Fargues lectures for wonderful things about formal groups.)

Assume now that $N \in \mathcal{O}^\times$. The subset $\mathcal{O}^\times z + z^2\mathcal{O}[[z]] \subset \mathcal{O}[[z]]$ being a group for the composition of power series, it follows that $[N]$ is bijective on $E_0(F)$. In particular, $E(F)[N] \to \overline{E}(k)[N]$ is injective. If $P \in \overline{E}(k)[N]$, we have seen that

[6] This curve actually is well-defined as the minimal Weierstrass equation is unique of to changes of coordinates with $(u, r, s, t) \in \mathcal{O}_F^4$ and $u \in \mathcal{O}_F^\times$.

there is some $Q \in E(F)$ that lifts P. So $[N]Q \in E_0(F)$, hence has the form $[N]R$ for some $R \in E_0(F)$, hence $Q - R \in E_0(F)[N]$ lifts P. □

Proof — (End of proof of proposition 2.6). When F is algebraically closed of characteristic $p > 0$, we may view F as the residue field of the Witt vectors $W(F)$ of F, and we may lift (anyhow) a Weierstrass equation to $W(F)$. For instance, if F is the algebraic closure of a finite field of characteristic p, then $W(F)$ is isomorphic to the p-adic completion of $\mathcal{O}_{\mathbb{Q}_p^{\mathrm{ur}}}$. Note that the discriminant of this integral Weierstrass equation is non-zero mod p, hence in $W(F)^\times$.

Changing the notations, assume now that F is complete for a discrete valuation $v : F^\times \to \mathbb{Z}$ such that $v(p) = 1$, with algebraically closed residue field k, and that E has good reduction over F, with residue curve any given elliptic curve $\overline{E}$ over k. By the characteristic 0 case, there is a finite extension L of F such that $E(L)[N] = E(\overline{F})[N] \simeq (\mathbb{Z}/N\mathbb{Z})^2$. Proposition 2.7 ensures that the reduction map

$$E(L)[N] \to \overline{E}(k)[N]$$

is an isomorphism, and we are done. □

We usually set $T_p(E) := T_p(A)$. For $p \in F^\times$, the Galois representation

$$\rho_{E,p} : G_F \to \mathrm{Aut}_{\mathbb{Z}_p}(T_p(E)) \simeq \mathrm{GL}_2(\mathbb{Z}_p)$$

is usually extremely interesting, in the sense that it tells a lot about the elliptic curve E.[7]

For instance if F is finite with q elements and p is prime to q, then a theorem of Weil asserts that

$$|E(F)| = q + 1 - \mathrm{trace}(\rho_{E,p}(\mathrm{Frob}_F^{-1})) \quad \text{and} \quad \det(\rho_{E,p}(\mathrm{Frob}_F^{-1})) = q.$$

A theorem of Hasse says that $|\mathrm{trace}(\rho_{E,p}(\mathrm{Frob}_F^{-1}))| \leq 2\sqrt{q}$. For a general F, the Weil-pairing shows that $\det(\rho_{E,p})$ is the p-adic cyclotomic character of G_F.

Let F be a finite extension of $\mathbb{Q}_\ell$. When E has good reduction over F, Prop. 2.7 shows that $E(\overline{F})[N] \subset E(F^{\mathrm{ur}})$ whenever $N \in \mathcal{O}_F^*$, in which case the reduction mod π_F induces a group isomorphism $E(\overline{F})[N] \xrightarrow{\sim} E(\overline{k_F})[N]$. In particular, if $p \in \mathcal{O}_F^\times$ and E has good reduction over F, then $\rho_{E,p}$ is unramified and factors through a representation of G_{k_F} which is exactly $\rho_{\overline{E},p}$.

If $F \to F'$ is any field embedding and $N \in F^*$, then $E(\overline{F})[N] = E(\overline{F'})[N]$ so it is clear that $T_p(E)_{|G_{F'}} = T_p(E \times_F F')$ for any p. As a consequence, the analysis above shows that when F is a number field, *the datum of $\rho_{E,p}$ is exactly the same as the one of the collection of $|\overline{E}(k_{F_v})|$ for almost all $v \in S(F)$*, as expressed by the following statement.

THEOREM 2.8. *Let S be the finite set of primes v of F such that either $v \in S_p(F) \cup S_\infty(F)$, or E has bad reduction at F_v.*

The Galois representation $\rho_{E,p} : G_F \to \mathrm{GL}_2(\mathbb{Q}_p)$ is semi-simple, unramified outside S, and for all $v \notin S$ we have $\mathrm{trace}(\rho_{E,p}(\mathrm{Frob}_v^{-1})) = |k_{F_v}| + 1 - |\overline{E}(k_{F_v})|$. *It*

[7] Not always, however, for instance it does not say anything if F is algebraically closed. It is typically interesting if F is of finite type over its prime subfield.

is the unique Galois representation with these properties. It is irreducible if E has no complex multiplication.

This follows from the analysis above and Prop.1.9, except the fact that $V_p(E)$ is a semi-simple, irreducible is the non-CM case, G_F-representation. This actually comes from other ideas, and is rather specific to number fields. Briefly, if E is CM then V_p is easily seen to be semi-simple. Assume E is not CM. It is enough to check that $T_p(E)$ has only finitely many G_F-stable $\mathbb{Z}_p$-lattices up to homothety. It is a general fact that for each such lattice Λ there exists an elliptic curve E' over F and an isogeny $E' \to E$ such that Λ is the image of $T_p(E')$ via this isogeny. It turns out that E and E' have good reduction at the same finite places (this can be read off from $V_p(E) = V_p(E')$, by the Neron-Ogg-Shafarevic criterion). But up to isomorphisms, there are only finitely many elliptic curves over F with good reduction outside a fixed finite set S: this is Shafarevic's theorem see e.g. Serre's *Abelian ℓ-adic representations* Chap. IV 1.4.