# Junior Algebraic Geometry Seminar, Spring 2019/20

*Galois representations and modular forms*

## Deligne's construction of Galois representations

In broad strokes the (global arithmetic) Langlands conjecture (for $\mathrm{GL}_n$) attempts to relate two classes of disparate objects. On the one hand we have automorphic representations—objects of harmonic analysis. On the other hand we have Galois representations—objects of arithmetic. The Langlands conjecture then roughly posits that there should be a natural bijection between these two classes of objects which preserves natural data on both sides.

Well before Langlands started to formalize the program that would bear his name surprising connections between analytic and arithmetic objects were being observed by Japanese mathematicians (e.g. Taniyama and Shimura). They realized that there was a close connection between modular forms (of which automorphic representations are generalizations of) and elliptic curves or, essentially equivalently, the Tate modules of elliptic curves (which are Galois representations). Much work on this subject was performed in the '60s and '70s with one of the major landmarks being Deligne's general association in [Del71] of an elliptic curve/Galois representation to a modular form (with some assumptions).

More explicitly associated to modular forms, elliptic curves, and Galois representations are analytic objects called *L-functions* which, roughly, encode analytically important numerical invariants of the respective objects. One can then understand Deligne's result as the claim that associated to a (weight 2) modular form $f$ (with certain extra properties) there is an elliptic curve $E_f$, and a fortiori a Galois representation $\rho_f$, with the property that we have an equality of $L$-functions

$$L(f,s) = L(E_f,s) = L(\rho_f,S)$$

(although truthfully he really only shows an equality of *partial L-functions* with the full equality only being later shown by Carayol et al.). Deligne was motivated by a desire to use his recent results onf the Weil conjecture to prove the longstanding Ramanujan conjecture.

The goal of this seminar is to cover enough material to rigorously understand the statement of Deligne's result as well as give a full account of his construction. Time permitting we then discuss applications of this result (e.g. the Ramanujan conjecture) and future directions (e.g. the modularity conjecture of Wiles et al. and the Langlands program at large).

## References

There is no fully contained account of the background material for the results in [Del71]. A very broad overview of the construction is given in [Sai]. That said the best approximation for a comprehensive account are various chapters in [Sai13] and [Sai14]. In general we will jump around between a large set of notes and books. There will be ancillary references listed below in case the reader would like to compare sources.

## Talks

The outlines below are only loose guidelines.

*1. Introduction and overview* This will be a talk given by Alex Youcis which will discuss the above outline in more detail giving motivation for the objects that are involved.

**Galois representations**

*2. Galois representations (I)*

(1) Recall the definition of number fields, the integer ring of a number field, the notion of a place of a number field, and the completion of a number field at a place. See [KKSK00, §6.2-§6.3].

(2) Define globbal fields, local fields, and recall the classification of local fields. See [KKSK00, §6.2].
(3) Discuss the relationship between Galois groups of number fields and the Galois groups of their completions (the ‘decomposition group’). See [KKSK00, §6.3] and more specifically [KKSK00, Lemma 6.72].
(4) Let $F$ be a $p$-adic field and $G_F := \mathrm{Gal}(\overline{F}/F)$ its absolute Galois group. Define the inertia subgroup $I_F \subseteq G_F$ and wild inertia subgroup $P_F \subseteq I_F$ of $F$. See [Clab].
(5) Discuss the structure of $G_F/I_F$ and $I_F/P_F$. Discuss the notion of an unramified and tamely ramified extension of $F$. Define a Frobenius element in $G_F$.
(6) Discuss the classification of unramified extensions of a local field. See [Clab].
(7) Explain the definition of a Frobenius element in the Galois group of a number field and explain Cebotarev density. See [KKSK00, Proposition 5.11] and [KKSK00, §6.3(a)] as well as [Len].

*Additional references:* [Lor07, §2 - §25], [Claa], [Mar77], [CF67], and [Neu13].

*3. Galois representations (II)*

(1) Define a Galois representation and, more generally, what a Galois module is (i.e. for a field $F$ and a topological ring $R$ a *Galois $R$-module* is a topological $R$-module $M$ with a homomorphism $G_F \longrightarrow \mathrm{Aut}_R(M)$ such that the induced action map $G_F \times M \longrightarrow M$ is continuous). See [Wie, Definition 1.2.1].
(2) Define $\ell$-adic representations and Artin representations. See [Wie, Definition 1.1.3].
(3) Give concrete examples of Galois representations: a concrete example of an Artin representation (e.g. see [BK, Example 1.19]), the $\ell$-adic cyclotomic character of a field $F$ (e.g. see [Bel, §2.3.1]), the $\ell$-adic Tate module of an elliptic (e.g. see [Bel, §2.4] or [BK, Pg. 71]), and if you have the time/the desire the example from [You, Appendix 2].
(4) Discuss the general formalism of étale cohomology as a Galois representation and discuss the basic properties such a theory satisfies in the smooth proper case. See [Bel, §3.1].
(5) Explain why all Artin representations have finite image. In fact, show that if $G$ is any real/complex Lie group then any continuous homomorphism $\rho : G_F \longrightarrow G$ has finite image . Sketch: since $G$ satisfies the “no small subgroups property” (see [Gun]) there exists a neighborhood $U$ of the identity $e \in G$ such that $U$ contains no non-trivial subgroups. Note that $\rho^{-1}(U)$ is an open subset of $G_F$ which, since $G_F$ has a neighborhood basis of the identity consisting of compact open subgroups (since it’s profinite), there exists some compact open subgroup $K \subseteq \rho^{-1}(U)$. Since $\rho(K) \subseteq U$ is a subgroup we deduce by construction that $\rho(K) = \{e\}$ and thus $K \subseteq \ker\rho$. But, $G_F/K$ is finite as desired.
(6) Define what it means for an Galois representation $\rho : G_F \longrightarrow \mathrm{GL}_n(K)$, where $F$ is a $p$-adic local field and $K$ is an arbitrary topological field, to be (potentially) unramified and (potentially) semi-stable. See [FO, Definition 1.22]—there they assume that $K = \mathbf{Q}_\ell$ but this is not necessary. Explain Grothendieck’s $\ell$-adic monodromy theorem and sketch the proof. See [FO, Theorem 1.24].
(7) (OPTIONAL) If you have enough time explain the classification of $\ell$-adic representations in terms of Weil–Deligne representations as in [FO, Proposition 1.28].

*Additional references:* [Kre] and [Tay04].

*4. Galois representations (III)*

(1) Define what it means for a Galois representation $\rho$ to be semi-simple and define the semi-simplification $\rho^{\mathrm{ss}}$ of $\rho$. See the discussion in [Kre, §1.1] and [Wie, §2.1].
(2) Discuss the Brauer–Nesbitt theorem (see [Wie, Theorem 2.4.6]) but since we are mostly interested in $\ell$-adic representations discuss also the simpler version in this case (see [Wie, Proposition 2.4.3]).
(3) Let $F$ be a number field and $\rho : G_F \longrightarrow \mathrm{GL}_n(K)$ be a Galois representation where $K$ is a characteristic 0 topological field. Assume that $\rho$ is unramified almost everywhere (i.e. that $\rho \mid G_{F_v}$ is unramified for almost every finite place $v$) and let $S$ be the set of unramified finite places. Explain why the subset $\{\mathrm{tr}\,\rho(\mathrm{Frob}_v)\}_{v\in S} \subseteq K$ determines uniquely the representation $\rho^{\mathrm{ss}}$. More explicitly, explain why if $\rho'$ is a second representation such that for all but finitely many finite places $v$ of $F$ one has that $\rho$ and $\rho'$ are both unramified and $\mathrm{tr}(\rho(\mathrm{Frob}_v)) = \mathrm{tr}(\rho'(\mathrm{Frob}_v))$ then $\rho^{\mathrm{ss}} \cong (\rho')^{\mathrm{ss}}$. See [BK, Theorem 3.19].

(4) As an example of this idea, explain why there does not exist a Galois character $\chi : G_{\mathbf{Q}} \longrightarrow \mathbf{Q}_\ell^\times$ such that $\chi(\mathrm{Frob}_p) = p$ for all $p \neq 11$ and $\chi(\mathrm{Frob}_{11}) = 1$.
(5) Define the $L$-function of an Artin representation (see [BK, §3.2 Artin Representations], state Artin's theorem (see [BK, Theorem 3.11]) without proof, and state Artin's conjecture (see [BK, Conjecture 3.13]).
(6) Compute an example of the $L$-function of an Artin representation of a number field (e.g. see [BK, Example 1.19]).
(7) Define the $L$-factors of an $\ell$-adic representation of a number field $F$ at finite places $v$ of $F$ not dividing $\ell$. See [BK, Pg. 69].
(8) Describe the (finite part of the) $L$-function of the tate module an elliptic curve $E$ over $\mathbf{Q}$, prove the claim for places of good reduction, and sketch the proof at places of bad reduction. Explain the relationship between $L(V_\ell(E)^\vee, s)$ and $\zeta(\mathcal{E}, s)$ where $\mathcal{E}$ is a minimal Weierstrass model of $E$ over $\mathrm{Spec}(\mathbf{Z})$. See [Kre, §1.4] and ask me about the second part.

*Alternative references:* [Tay04] and [Blo].

### Modular curves

*5. Elliptic curves (I)*

(1) Define elliptic curves $\mathcal{E}$ of a general base scheme $S$ and morphisms of elliptic curves. See [Hid12, Definition 2.2.1].
(2) Identify an elliptic curve $\mathcal{E}$ over $S$ with $\mathrm{Pic}^0_{\mathcal{E}/S}$ and thus provide $\mathcal{E}$ with a group structure. See [Hid12, Theorem 2.2.1].
(3) Prove that the analytification map $E \mapsto E^{\mathrm{an}}$ provides an equivalence of categories:

$$\left\{\begin{matrix}\text{Elliptic curves}\\ \text{over } \mathbf{C}\end{matrix}\right\} \longrightarrow \left\{\begin{matrix}\text{1-dimensional compact}\\ \text{complex Lie groups}\end{matrix}\right\}$$

and moreover that every 1-dimensional complex Lie group is of the form $\mathbf{C}/\Lambda$ where $\Lambda \subseteq \mathbf{C}$ is a lattice. Sketch: the analytification map is fully faithful by GAGA and the fact that the image consists of 1-dimensional compact complex Lie groups is clear. Conversely, use Riemann's existence theorem (i.e. that every compact Riemann surface is algebraizable) to deduce that your 1-dimensional compact complex Lie group $G$ is of the form $G = X^{\mathrm{an}}$ for some $X$. Use GAGA to deduce that $X$ is a proper group variety. Deduce it must be an elliptic curve. For the statement about lattices use the surjectivity of the exponential map $\exp : \mathfrak{g} \longrightarrow G$ together with the fact that $\mathfrak{g}$ is abelian (since it's one-dimensional) to dedue that $G$ is a quotient of $\mathfrak{g} \cong \mathbf{C}$. Since $G$ is compact and $\ker \exp$ is discrete (by the identity theorem from complex analysis) deduce that $\ker \exp$ is lattice.

**NB:** For this latter lattice claim one can also argue by the universal cover. It's up to you.
(4) State that if $E$ is an elliptic curve over a field $k$ and $n$ is an integer with $\gcd(n, \mathrm{char}(k)) = 1$ then $E[n]$ is a finite étale group scheme of order $n^2$ and, in fact, $E[n]_{k^{\mathrm{sep}}} \cong (\mathbf{Z}/n\mathbf{Z})^2$. Prove this claim when $\mathrm{char}(k) = 0$. Sketch: show that it suffices to show the claim over a finitely generated $\mathbf{Q}$-subextension $K$ of $k$. Embed $K$ in to $\mathbf{C}$ to reduce the claim to $k = \mathbf{C}$. Use part (3) of this talk.
(5) Explain the fact that if $f : \mathcal{E} \longrightarrow \mathcal{E}'$ is a map of elliptic schemes over $S$ which is non-constant on fibers and $f(0_{\mathcal{E}}) = 0_{\mathcal{E}'}$ then $f$ is a locally free group homomorphism. See [Hid12, Corollary 2.2.2], [Sta18, Tag039B], and use (4).
(6) Let $\mathcal{E}$ be an elliptic scheme over $S$. Show that Zariski locally on $S$ the elliptic curve $\mathcal{E}$ can be put in Weierstrass form. See [Hid12, §2.2.5].

*Additional references:* [KM85, Chapter 2], [Sai13], [Sai14], [EvdGB], [Cona], and [Mum74].

*6. Elliptic curves (II)*

(1) Let $F$ be a $p$-adic local field. Define what it means for $E$ to have (potentially) good reduction and bad reduction. See [Sai13, Definition 1.5] and [Sai13, Proposition 1.24] (note that one can replace $\mathbf{Z}_{(p)}$ in this proposition with $\mathcal{O}_F$).

(2) State the Neron–Ogg–Shafarevich theorem and explain the proof of "good reduction $\implies$ unramified Tate module". See [Gat].
(3) Define what it means for an elliptic curve over $F$ to have additive/multiplicative reduction. See [Sai13, Definition 1.5] (note that one can replace $\mathbf{Q}$ in his definition with $F$).
(4) Define a generalized elliptic scheme and discuss its relationship to multiplicative reduction. See [Sai13, §1.5].
(5) Give an example of an elliptic curve with good reduction and one with multiplicative reduction and one with neither.
(6) Show that for an elliptic curve $E$ over a field $k$ of characteristic $p > 0$ the group scheme $E[p]$ is never an étale group scheme. In fact, show that $E[p]^\circ$ is never trivial. See [Sai14, §8.1].
(7) Define what it means for an elliptic $E$ over $S$, an $\mathbf{F}_p$-scheme, to be ordinary/supersingular. See [Sai14, §8.1].
(8) Explain the several equivalent conditions on what it means for an elliptic curve over a characteristic $p$ field to be supersingular/ordinary. See [Sai14, Proposition 8.2] and [Sai14, Proposition 8.5].
(9) Give examples of ordinary and supersingular elliptic curves. See [Sai14, Example 8.6].
(10) Define the $L$-function of an elliptic curve over a number field $F$. See [BK, §1.4.2].
(11) Discuss the example in [BK, Example 1.20].

*Additional references:* [Hid12] and [KM85, Chapter 2].

*7. Modular curves (I)*

(1) Define what a coarse and fine moduli space is.See [Sai13, Definition 2.7]. See also [Hid12, §2.3.2] or [Ols16, Chapter 11] for coarse moduli spaces.
(2) Give examples of a coarse moduli space and a fine moduli space. For example, explain why $\mathbb{A}^1_k$ is the coarse moduli space for the functor of isomorphism classes of elliptic curves over $k$ (See [Sai14, Lemma 8.30] and the subsequent question). Also, explain why the moduli space of Weierstrass forms has a fine moduli space (see [Hid12, §2.2.6] and [Ber13, §4.1.2]).
(3) Define the modular curves $Y_0(N)$, $Y_1(N)$, and $Y(N)$. See [Sai13, §2.2-§2.3] (note that Saito only discusses $Y(N)$ and $Y_1(N)$ using the symbol $\mathcal{M}$ for the functors that the $Y_?(N)$ (perhaps coarsely) represent). See also [Conb, §9]. Additionally see [Hid12, §2.6]/[Hid12, §2.9.4] (where he uses the symbols $\mathcal{E}$ instead of $Y$) and [DS05, Chapter 7]. You should only work here over $\mathbf{Z}[\frac{1}{N}]$ to not worry about more sophisticated notions of level structures.
(4) Define the compactified modular curves $X(N)$, $X_0(N)$, and $X_1(N)$. See [Sai13, Definition 2.8] and [Sai13, Definition 2.20] (note he uses $\overline{M}$ to denote the functors associated to these modular curves). See also [DS05, Chapter 7].

*Additional references:* [KM85, Chapter 3], [KM85, Chapter 8], [Conb], and [Loe].

*8. Modular curves (II)*

(1) Define the notion of a modular form of level $\Gamma_0(N)$ with $\mathbf{Q}$-coefficients. See [Sai13, Definition 2.12(2)].
(2) Given the example of the $\Delta$-form. See [Del71, Introduction].
(3) Define the Hecke operators on the system of modular curves $X_0(N)$ and explain what the induced action on the space of modular forms are. See [Sai13, §2.6].
(4) Explain the $q$-expansion of a modular form. See [Sai13, §2.7].
(5) Explain what a normalized Hecke eigencuspform is (see [Sai13, Definition 2.42](3)—note that he calls such things *primary forms*).
(6) Define a modular form/normalized Hecke eigencuspform of level $\Gamma_0(N)$ with coefficients in $K$ a field of characteristic 0. See [Sai13, Definition 2.42].
(7) Define the $L$-function of a normalized Hecke eigencuspform. See [Sai13, Equation (2.47)].
(8) Explain the strong multiplicity one property for modular forms. See [Sai13, Theorem 2.49] as well as [BD, Theorem 5.13]
(9) Explain the relationship between 'arithmetic modular forms' (as defined above) and 'analytic modular forms'. See [Sai13, §2.11].

*Additional references:* [DS05] and [Ste].

*9. Modular curves (III)*

(1) Discuss the notion of a cyclic group scheme over **Z**. See [Sai14, §8.2] and particularly [Sai14, Definition 8.13]. See also [KM85, §1.4].
(2) Define the notion of a section of exact order $N$. See [Sai14, Definition 8.20]. See [KM85, §1.4] and [KM85, §1.8].
(3) Define the $Y(N)$, $Y_1(N)$, and $Y_0(N)$ over **Z**. See [Sai14, §8.4-8.5] and [Sai14, §8.8]. See also [KM85, Chapter 3]
(4) Discuss extensions of these ideas to compactified modular curves. See [Sai14, §8.9]. See also [KM85, Chapter 8].

*Additional references:* [Hid12].

**Modular curves (IV)**

(1) Define the curves $Y_{0,*}(N)$, $Y_{1,*}(N)$, and $Y_{1,0}(N)$. See [Sai14, Definition 8.35][Sai14, Definition 8.75].
(2) Define the compactifications of these curves. See [Sai14, §8.9].
(3) Explain the result [Sai14, Theorem 8.32] and prove it. Be sure to draw many pictures.
(4) Explain the result [Sai14, Proposition 8.73] and prove it. Be sure to draw many pictures.

*Additional references:* [DS05, Chapter 8].

**Deligne's construction**

*10. Deligne's construction (I)*

(1) Discuss Hecke algebras both over a field and integrally. See [Sai13, §2.10] and [Sai14, §9.1].
(2) State rigorously Deligne's result. See [Sai14, Theorem 9.13] and [Sai14, Corollary 9.14].
(3) Explain Deligne's result in terms of partial $L$-functions.
(4) Explain the proof of Deligne's theorem. See [Sai14, Theorem 9.16] and its proof.

*Additional references:* [Del71] and [DS05, §9.5].

*11. Deligne's construction (II)*

(1) State the Ramanujan conjecture and discuss its significance. See [Gow] and [Del71].
(2) Explain the proof of the Ramanujan conjecture. See [Del71, §5.1].
(3) Discuss Deligne's construction as part of the greater Modularity Conjecture and discuss the result of Wiles et al. See [DS05, §9.6].
(4) Discuss the construction of Deligne and the result of Wiles in the larger context of the Langlands program. See [Kna97] and discuss with Alex.

## References


[BD] Peter Bruin and Sander Dahmen, *Modular forms*, http://www.few.vu.nl/~sdn249/modularforms16/Notes.pdf.
[Bel] Joel Bellaiche, *Galois representations*, http://people.brandeis.edu/~bergdall/spring2k8galoisreps.pdf.
[Ber13] José Bertin, *Algebraic stacks with a view toward moduli stacks of covers*, Arithmetic and Geometry Around Galois Theory, Springer, 2013, pp. 1–148.
[BK] Peter Bruin and Arno Kret, *Galois representations and automorphic forms*, https://www.math.leidenuniv.nl/~pbruin/GaloisReps.pdf.
[Blo] Adam Block, *Artin l-functions*, http://www.columbia.edu/~abb2190/ArtinLFunctions.pdf.
[CF67] John William Scott Cassels and Albrecht Frölich, *Algebraic number theory: proceedings of an instructional conference*, Academic Pr, 1967.
[Claa] Pete L. Clark, *Algebraic number theory ii: Valuations, local fields and adeles*, http://math.uga.edu/~pete/8410FULL.pdf.

[Clab] ———, *Lecture notes on local fields*, http://math.uga.edu/~pete/local.pdf.
[Cona] Brian Conrad, *Abelian varieties*, https://www.mit.edu/~fengt/249C.pdf.
[Conb] ———, *Modular curves*, http://virtualmath1.stanford.edu/~conrad/248BPage/handouts/modularcurves.pdf.
[Del71] Pierre Deligne, *Formes modulaires et representations $\ell$-adiques*, Séminaire Bourbaki vol. 1968/69 Exposés 347-363, Springer, 1971, pp. 139–172.
[DS05] Fred Diamond and Jerry Michael Shurman, *A first course in modular forms*, vol. 228, Springer, 2005.
[EvdGB] Bas Edixhoven, Gerard van der Geer, and Moonen Ben, *Abelian varieties*, http://gerard.vdgeer.net/AV.pdf.
[FO] Jean-Marc Fontaine and Yi Ouyang, *Theory of $p$-adic galois representations*, https://www.math.u-psud.fr/~fontaine/galoisrep.pdf.
[Gat] Pietro Gatti, *The neron-ogg-shafarevich criterion*, http://algant.eu/documents/theses/gatti.pdf.
[Gow] W.T. Gowers, *The work of pierre deligne*, https://www.abelprize.no/c57681/binfil/download.php?tid=57753.
[Gun] Murat Gungor, *"no small subgroups" argument*, MathOverflow, URL:https://mathoverflow.net/q/103783 (version: 2012-08-02).
[Hid12] Haruzo Hida, *Geometric modular forms and elliptic curves (2nd edition)*, World Scientific, 2012.
[KKSK00] Kazuya Kato, Nobushige Kurokawa, Takeshi Saitō, and Masato Kurihara, *Number theory: introduction to class field theory*, vol. 186, American Mathematical Soc., 2000.
[KM85] Nicholas M Katz and Barry Mazur, *Arithmetic moduli of elliptic curves*, no. 108, Princeton University Press, 1985.
[Kna97] AW Knapp, *Introduction to the langlands program*, Proceedings of symposia in pure mathematics, vol. 61, AMERICAN MATHEMATICAL SOCIETY, 1997, pp. 245–302.
[Kre] Arno Kret, *Galois representations*, https://www.math.leidenuniv.nl/scripties/KretMaster.pdf.
[Len] Henrik Lenstra, *The chebotarev density theorem*, http://websites.math.leidenuniv.nl/algebra/Lenstra-Chebotarev.pdf.
[Loe] David Loeffler, *Modular curves*, https://warwick.ac.uk/fac/sci/maths/people/staff/david_loeffler/teaching/modularcurves/lecture_notes.pdf.
[Lor07] Falko Lorenz, *Algebra: Volume ii: Fields with structure, algebras and advanced topics*, Springer Science & Business Media, 2007.
[Mar77] Daniel A Marcus, *Number fields*, vol. 8, Springer, 1977.
[Mum74] David Mumford, *Abelian varieties*, vol. 2, Oxford university press Oxford, 1974.
[Neu13] Jürgen Neukirch, *Algebraic number theory*, vol. 322, Springer Science & Business Media, 2013.
[Ols16] Martin Olsson, *Algebraic spaces and stacks*, vol. 62, American Mathematical Soc., 2016.
[Sai] Takeshi Saito, *Galois representations and modular forms*, https://www.ms.u-tokyo.ac.jp/~t-saito/talk/eepr.pdf.
[Sai13] Takeshi Saitō, *Fermat's last theorem: basic tools*, vol. 243, American Mathematical Soc., 2013.
[Sai14] Takeshi Saito, *Fermat's last theorem: The proof*, vol. 245, American Mathematical Soc., 2014.
[Sta18] The Stacks Project Authors, *Stacks Project*, http://stacks.math.columbia.edu, 2018.
[Ste] William Stein, *Modular forms: A computational approach*, https://wstein.org/books/modform/stein-modform.pdf.
[Tay04] Richard Taylor, *Galois representations*, Annales de la Faculté des sciences de Toulouse: Mathématiques, vol. 13, 2004, pp. 73–119.
[Wie] Gabor Wiese, *Galois representations*, http://math.uni.lu/~wiese/notes/GalRep.pdf.
[You] Alex Youcis, *Weil-deligne representations and p-adic hodge theory: motivation*, https://alex-youcis.github.io/weilnotes.pdf.