NOTES ON THE GLOBAL LANGLANDS CONJECTURES

KEVIN BUZZARD

Abstract. Notes on what the statement of the global Langlands conjectures for number fields looks like, with particular attention paid to basic definitions which undergraduates could understand and implement in Lean.

1. Intimidating introduction

The Langlands Philosophy is a big web of conjectures and ideas and currently a very active area of research. At its vaguest, it says that a theory called the theory of automorphic representations can be completely explained via representations of something called the "global Langlands group". Unfortunately actually giving a *definition* of the global Langlands group is a major open problem in the area. As you can imagine, such a conjecture is difficult to work with – for example it is essentially impossible to disprove the conjecture, and it can also be difficult to find in the literature a complete concrete list of properties which this group is supposed to have; in this form it is almost a "conjectural conjecture".

I was quite annoyed by this fact about 15 years ago, and with professor Gee we attempted to write down a concrete statement where everything was actually well-defined. Instead of using the global Langlands group we used a Galois group which had a rigorous and unambiguous definition. Instead of complex representations we used p-adic representations – our vector spaces were defined over the algebraic closure of the p-adic numbers (which is still an algebraically closed field of characteristic zero, so all the usual 3rd year rep theory theorems apply to it). But most importantly, instead of trying to explain all automorphic representations, we only attempted to explain a subset of them, namely the so-called "L-algebraic" representations. In this section let me give some kind of explanation as to what our version of the conjecture looks like.

We start off with a number field K (e.g. the rational numbers) and a so-called "connected reductive group G over K" (e.g. the group GL_n). Attached to K is a gigantic ring $\mathbb{A}_K$ called the *adeles* of K with a topology, and an *automorphic representation* of G is a (typically infinite-dimensional) representation of $G(\mathbb{A}_K)$ satisfying some properties. Note that of course we don't teach much about infinite-dimensional representations of groups in the Imperial undergraduate degree – but this doesn't matter, because the plan is not to prove theorems about these groups, but just write down definitions.

The conjecture that Gee and I make is that associated to an automorphic representation π of G over K which is "L-algebraic" (that's just one more condition on the representation) there should be a family of p-adic Galois representations ρ_λ taking values in the L-group of G. Example: the L-group of GL_n is just basically GL_n again, so this is just a fancy way of talking about n-dimensional representations of a certain Galois group. Furthermore, if ρ_λ is the Galois representation attached to π then ρ_λ and π should be "compatible" in the sense that if you're given π then you can work out some stuff (e.g. some numbers, or homomorphisms, or matrices, or whatever) and given ρ you can work out some numbers/matrices/whatever in a totally different way, and if π and ρ match up then all these numbers/matrices/whatever attached to π and ρ should match up too.

My paper with Gee is here and it is completely intimidating for an undergraduate or MSc student.

The purpose of this document is to massively un-intimidate all of the nonsense above, until it becomes stuff which an undergraduate can reasonably work on as a project.

2. Connected reductive groups

It's not necessary to understand connected reductive groups over number fields to understand the Langlands conjectures, because we could just stick to the case where the group is GL_n and the number field is $\mathbb{Q}$, and the conjectures are already hugely interesting and open in this case if $n \geq 2$ (although Wiles made great progress on them in the 1990s and deduced Fermat's Last Theorem as a consequence). But here are some of the ideas behind the general definition of a connected reductive group. In fact there is no point sticking to number fields here, the theory of connected reductive groups works over any field (and in fact over any commutative ring, but let's stick to fields).

Let K be a field (if you like you can stick to $K = \mathbb{Q}$, it's already interesting and deep). The first thing you need to know about connected reductive groups over K is that they're not actually groups. They are "affine group varieties", so it's really an abuse of notation to call them groups; their complex points are groups, but they are more data than this (for example GL_n isn't a group by itself, but $\mathrm{GL}_n(\mathbb{C})$ is a group as is $\mathrm{GL}_n(L)$ for any field L). If you're doing the algebraic geometry course here then you'll know what an affine variety is by now, but if you don't then here's the main thing you need to know: whatever an affine variety over a field K is, it is completely determined by its *coordinate ring*, which is a K-algebra. A K-algebra is just a fancy way of saying "a commutative ring equipped with a ring homomorphism from K"; examples include polynomial rings $K[X_1, X_2, \ldots, X_n]$ and quotients $K[X_1, X_2, \ldots, X_n]/I$ of these by ideals; such K-algebras are called *finitely-generated*. Lean has the theory of K-algebras, indeed `[Algebra K A]` means that A is a K-algebra.

If an affine variety is just a K-algebra in disguise, what's the point of them? Well, the funky thing about the dictionary between affine varieties and K-algebras is that if X and Y are affine varieties over K and their corresponding coordinate rings are A and B, then to give a map of affine varieties from X to Y is the same thing as giving a K-algebra homomorphism from B to A, and not from A to B; the arrows all go the wrong way around.

So a "connected reductive group" should really be called a "connected reductive group variety". Let's now forget about connected and reductive, and let's talk about group varieties.

This phenomenon that maps go the other way when you translate between the language of varieties and the language of K-algebras has quite a weird consequence. I've told you that an affine variety X over K is basically the same thing data (just packed up differently) as a K-algebra A. But if we want to give the variety a group structure then this involves giving a multiplication map $X \times X \to X$, an identity element of X, and an inverse map $X \to X$, and when we translate this back down into ring theory we get a bunch of maps all going the wrong way. For example, on K-algebras A corresponding to group varieties the "multiplication map" isn't a map from $A \times A$ to A, it's a map $A \to A \otimes_K A$, the tensor product of A with itself. And the identity is a K-algebra map $A \to K$. And then the group axioms are totally weird statements about these maps, which look like the usual group axioms but backwards. Whatever is going on?

What is going on is that making the affine variety X into a group is the same thing as making the commutative K-algebra A into something called a *commutative Hopf algebra*. You can read about Hopf algebras on Wikipedia. But let's not jump the gun: before we talk about Hopf algebras, let's talk about bialgebras.

2.1. **Project: the theory of bialgebras.**

A *monoid* is a slighly simpler thing than a group. It has multiplication and identity, but it might not have inverses. This means that there are loads more monoids than groups, and that monoids are (a) simpler to work with but (b) much harder to classify (but this is OK, we don't want to classify them). The axioms for a monoid are the axioms for a group which don't mention inverses: they are $a \times (b \times c) = (a \times b) \times c$ and $1 \times a = a \times 1 = a$. The inverse axioms aren't there because they don't make sense. The naturals, integers, rationals, reals and complexes are all monoids under multiplication; they all have a 0 and 0 doesn't have an inverse, but this doesn't matter because monoids don't need inverses. A group is a monoid with some extra stuff (inverses), so a group variety is a monoid variety with extra stuff, so let's first discuss how to formalise monoid varieties. And this is easier than you think because the hard work (the key definition) has already been done.

A *commutative bialgebra* over a field K is a commutative K-algebra A (i.e., a commutative ring A equipped with a ring homomorphism from K to A) equipped with two K-algebra maps called comultiplication $A \to A \otimes_K A$ and counit $A \to K$, satisfying some axioms. You can read these axioms on the Wikipedia page for bialgebras. The axioms look intimidating, but if you write them down and then look at them backwards then they become the usual axioms for monoids. The idea now is that if L is any field containing K, then the set of K-algebra maps from A to L naturally becomes a monoid, and putting this monoid structure on this set is a nice challenge.

The mathematics looks like this: fix a field L containing K and let G (it's not a group, it's a monoid, but let's call it G anyway) be the set of K-algebra maps from A to L. The identity element of G is obtained by taking the counit map $A \to K$ and composing with the map $K \to L$. The multiplication map is defined in the following way: if ϕ and ψ are two K-algebra maps $A \to L$ then their product is the K-algebra map from A to L defined by first applying the comultiplication (to get to $A \otimes_K A$) and then applying $\phi \otimes \psi$ (to get to $L \otimes_K L$) and then applying multiplication on L (to get to L). The monoid axioms can be deduced from the axioms of a bialgebra, which are essentially exactly the monoid axioms but with all the arrows written the wrong way around.

Putting this monoid structure on these maps would be a very nice project. I have worked through the proofs of the axioms on paper and they are all 4-line calculations which in Lean would just involve a bunch of rewriting (to move brackets around) and applying axioms of a bialgebra.

2.2. **Project: Hopf algebras.**

To get from a monoid variety to a group variety we have to add inverses. The "coinverse" map on the bialgebra side of things turns a bialgebra into a Hopf algebra. Right now mathlib doesn't have Hopf algebras, but I am actively working on this: see here for the state of things. Right now the most natural thing to do would be to literally copy this file into the FLT project and then import it into another file and work on the second file.

One nice literature reference for Hopf algebras is chapter III of Christian Kassel's 'Quantum Groups'. Take a look at Prop III.3.1, Def III.3.2, and Theorem III.3.4, and you should be able to deduce the following three things about Hopf algebras:

(1) The coinverse map S on a bialgebra is unique, if it exists.
(2) In a Hopf algebra we have $S(ab) = S(b)S(a)$.
(3) If A is a commutative Hopf algebra then S is a bijection.

The mathematics here is not hard (if you're not intimidated by tensor products); this project (to prove one or more of these results) is just straight algebra and can be done independently of the monoid exercise in the previous subsection.

2.3. **Project: Group varieties and Hopf algebras.**

Assuming the two previous projects, one can then put them together and start working on group varieties, which of course are a prerequisite for the general theory of connected reductive group varieties.

If A is a commutative Hopf algebra then the coinverse map, or antipode map or whatever you want to call it, translates into the inverse map on the K-algebra maps $A \to L$ which we've put a monoid structure on in the previous section; this beefs the monoid structure up into a group structure.

Concretely this means putting a group structure on the K-algebra maps $A \to L$ for all fields L containing K. In fact all of this generalises: one could observe that we never assumed that K and L were fields and everything works for K and L commutative rings and L just assumed to be a K-algebra. Finally one can go full abstract (which is the generality which `mathlib` would want), and show that Hopf algebras over K are antiequivalent to the category of group objects in the category of affine schemes over K. This sounds very fancy but it's just lots of buzzwords saying obvious things: it's one of those situations where the question looks intimidating because it goes on about equivalences of categories, but once you write down the axioms it turns out that they all translate down into concrete statements about K-algebras with proofs which are just a few lines of calculations.

3. Compatible systems of Galois representations

Given an L-algebraic automorphic representation for a connected reductive group G over a number field K, the Langlands Philosophy conjectures the existence of a compatible family of ℓ-adic Galois representations taking values in the L-group of G. What does all this gobble-de-gook mean?

3.1. **Project: families of ℓ-adic Galois representations.**

Let's let K be any field, but instead of working with a general G let's specialise to the case where $G = \mathrm{GL}_n$. I want to define a *family of ℓ-adic Galois representations*, but before I do that I need to talk about the ℓ-adic numbers (here ℓ is a prime). The ℓ-adic numbers are just some field $\mathbb{Q}_\ell$, like the real numbers are a field. Lean's maths library already has them, and the *only thing* you need to know about them is that they're a field with a metric on, just like the real numbers are. You don't need to know the definition of the ℓ-adic numbers or any theorems about them – you can just use them (like you used the real numbers when you were at school without ever having seen a formal definition of them via Cauchy sequences or whatever).

Next we need the concept of an algebraic closure. Again this is something you don't need to know too much about; if K is any field then there's a typically bigger field called the *algebraic closure* $\overline{K}$ of K, with the property that all non-constant polynomials with coefficients in K have all their roots in $\overline{K}$. Example: the algebraic closure of $\mathbb{R}$ is $\mathbb{C}$, and hence a polynomial like X^2+1 with coefficients in $\mathbb{R}$ but no roots in $\mathbb{R}$ will factor into linear factors over $\mathbb{C}$. Again, Lean has algebraic closures and all you need to know about them is that if K is a field then $\overline{K}$ is a field and a K-algebra.

OK so what is a family of ℓ-adic Galois representations? First, we need a number field E (that is, a subfield of $\mathbb{C}$ which is finite-dimensional over $\mathbb{Q}$, or more abstractly any field E containing a copy of $\mathbb{Q}$ such that E is finite-dimensional over $\mathbb{Q}$). And second, for every prime number ℓ and for every field homomorphism $\lambda : E \to \overline{\mathbb{Q}}_\ell$ (the algebraic closure of the ℓ-adic numbers), we are given a continuous group homomorphism $\rho_\lambda : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$. Here $\overline{K}$ denotes an algebraic closure of K, and $\mathrm{Gal}(\overline{K}/K)$ is defined to be the group of isomorphisms $\overline{K} \cong \overline{K}$ which restrict to the identity function on K (the group law is composition of functions). This group has a topology, and the topology is already in mathlib.

Mathlib also has the ℓ-adic numbers $\mathbb{Q}_\ell$, and the concept of algebraic closure as I mentioned already. So whilst a lot of this stuff above looks daunting, it's already there and it's just a case of writing everything down in the right order. The only issue (i.e., the only thing which isn't in mathlib already) will be putting a topology on $\mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$. The way to do it is probably to put a distance function on $\overline{\mathbb{Q}}_\ell$ (not hard; I can explain how, there's an explicit formula), and then to *assume* that this distance function is a metric (this is much harder, so just sorry it: I have a post-doc working on this proof) and then the induced topology on $\overline{\mathbb{Q}}_\ell$ gives rise to a topology on $\mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ (not hard). Once you have a group structure and a topology on both sides, you can talk about continuous group homomorphisms, and that's the definition.

The weird thing about this definition is that these representations are all completely unrelated to each other as ℓ varies. The concept we're really interested in is *compatible* families of ℓ-adic Galois representations, and before we can define these, we need to talk about Frobenius elements.

3.2. **Project: Frobenius elements.** A *valuation* (sometimes called a *nonarchimedean norm*) on a field F is a function v from F to $\mathbb{R}_{\geq 0}$ satisfying four axioms: (1) $v(0)=0$; (2) $v(1)=1$; (3) $v(ab)=v(a)v(b)$; (4) $v(a+b) \leq \max\{v(a), v(b)\}$. Valuations are in mathlib. Two valuations v_1 and v_2 are *equivalent* if there's some real number $0<\rho$ such that $v_1(f)=v_2(f)^\rho$ for all $f \in F$; we usually think of equivalent valuations as being "equal" but as you might guess, Lean is a bit fussy about this.

An example of a valuation is the p-adic valuation (or p-adic norm) on $\mathbb{Q}$; let's define it step by step. First let's define it on primes; set $v(p)=p^{-1}$ and $v(q)=1$ for all primes $q \neq p$. Now using axiom (3) and the fact that every positive integer is uniquely the product of primes, we can figure out $v(n)$ for all positive integers n. Now using the fact that $v(x^{-1}) = v(x)^{-1}$ we can figure out $v(x)$ for every positive rational x. Finally we set $v(0) = 0$ and $v(-x) = v(x)$ and this defines the valuation uniquely (one has to check axiom 4 but all this is already in mathlib, I think).

Given a valuation on a field, one can define the valuation subring $R = \{f \in F \mid v(f) \leq 1\}$, a subring of F, which has a maximal ideal $m = \{f \in F \mid v(f) < 1\}$, and the quotient is a field called the residue field of v.

I claim that given a prime number p, there exists an extension of the p-adic norm on $\mathbb{Q}$ to a valuation w on $\overline{\mathbb{Q}}$; the proof is probably a standard application of Zorn's lemma although I haven't thought it through. Furthermore I claim that there is a field isomorphism $F_p : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$ called the *Frobenius element* which satisfies firstly that $w(F_p(x)) = w(x)$ for all $x \in \overline{\mathbb{Q}}$, and secondly that the induced ring homomorphism from the residue field of w to itself is the map sending t to t^p. This proof can be sorried (it is a pretty simple argument *assuming* that you are on top of the Galois theory course and the algebraic number theory course, but we don't need to worry about it). The element F_p is not at all unique; it depends on w and even then there is lots of ambiguity in the choice. We won't worry about this, all we want is a definition of F_p and the fact that it raises things to the pth power on the residue field.

3.3. Project: Frobenius elements for number fields.

All this generalises from $\mathbb{Q}$ to general number fields. If K is a number field, then for P a maximal ideal of the integers $\mathcal{O}$ of K there is a story exactly like the above; there is a P-adic valuation on K, there is an extension to $\overline{K}$, and there's a Frobenius element F_P in $\mathrm{Gal}(\overline{K}/K)$ which induces the map $t \mapsto t^q$ where q is the size of the residue field $\mathcal{O}/P$. Again, you don't have to prove anything here, the important thing is getting the statements down correctly, so we have access to Frobenius elements.

3.4. Compatible families of Galois representations.

I defined a family of representations ρ_λ of $\mathrm{Gal}(\overline{K}/K)$ above. Let's stick to $K = \mathbb{Q}$ at first. The family is *compatible* if there is a finite set of prime numbers S and, for each prime p *not* in S a monic degree n polynomial $H_p \in E[X]$ with the following property: for every prime $\ell \neq p$ and every $\lambda : E \to \overline{\mathbb{Q}}_\ell$, the associated member ρ_λ of the family has the property that the characteristic polynomial of $\rho_\lambda(F_p)$ is H_p. In words, we're saying that the ρ_λ all have the same characteristic polynomials on these random Frobenius elements. You might want to deduce from this that all the ρ_λ are isomorphic, but this is not in general the case; they're all continuous with respect to completely different and inompatible topologies, so they can't be.

All this definition works pretty much verbatim if you change $\mathbb{Q}$ to a general number field K; then S becomes a finite set of prime ideals of the integers of K.

3.5. Unramified Galois representations.

TODO

3.6. From GL_n to a general connected reductive G.

TODO

4. Automorphic representations

The Langlands philosophy says that one should be able to associate a compatible family of ℓ-adic Galois representations to an *automorphic representation* so another key definition will be to define these.

There are two cases: an easy case, where the real Lie group $G(\mathbb{R})$ is compact; then no analysis is needed. And then the general case. TODO

Email address: k.buzzard@imperial.ac.uk

Department of Mathematics, Imperial College London