Where to Find Galois Representations, and Why

S. M.-C.

3 October 2016

Abstract

Starting from prime numbers, we'll discuss one of the motivating problems in number theory, and how it connects to Galois theory and then to Galois representations. This sets us up for a gentle view of what the Langlands program is all about. As an example we'll discuss the simplest case, Langlands for GL_1, also known as class field theory. (Knowledge of abstract algebra will be helpful.)

[I'm gonna make tons of simplifying assumptions in this talk. In particular: everything is Galois, and ignore ramified primes.]

As a number theorist I'm interested in prime numbers. Certainly including the usual $\{2, 3, 5, \ldots\}$, but in fact a slightly broader notion of prime number.

The familiar primes $\{2, 3, 5, \ldots\}$ are specific to the ring $\mathbb{Z}$ of integers in the field of rational numbers $\mathbb{Q}$. (If you don't know what rings and fields are, this is the example to keep in mind: rings are like integers, fields are like fractions.) In addition to the rational numbers, the number theorist is interested in other *number fields*, i.e. things got by adding an *algebraic number* (i.e. root of a polynomial with rational coefficients) to $\mathbb{Q}$. Every number field has its own "integers", just like the integers $\mathbb{Z}$ in $\mathbb{Q}$. (Since $\mathbb{Q}$ is the "rational" numbers, we'll call $\mathbb{Z}$ the *rational primes*.)

For example, $\sqrt{-1}$ is an algebraic number, because it's a root of $x^2 + 1$. Thus we can form a number field by adding it to the rationals: $\mathbb{Q}(\sqrt{-1})$, which consists of numbers of the form $\frac{a}{b} + \frac{c}{d}\sqrt{-1}$ ($\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$). The integers in this number field are $\mathbb{Z}[\sqrt{-1}]$, which consists of numbers of the form $a + b\sqrt{-1}$ ($a, b \in \mathbb{Z}$). This is the example I'll carry along today, but keep in mind that we can ask the same question for any number field: $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\cos(\pi/7))$, etc.

Just as $\mathbb{Z}$ has primes, so does $\mathbb{Z}[\sqrt{-1}]$ have primes. And as with $\mathbb{Z}$, we can ask: what are the primes in $\mathbb{Z}[\sqrt{-1}]$? (The precise meaning of "prime" changes from "prime element" to "prime ideal", but if you're not familiar then there's no harm of continuing to think of it in precisely the same way.)

This is the motivating question I want to discuss today.

Question 1. Every number field has its corresponding integers. What are the primes?

Some of the primes will be the same as rational primes; for example, 3 is a prime in $\mathbb{Z}$, and it turns out that 3 is also a prime in $\mathbb{Z}[\sqrt{-1}]$. Some primes will be different; for example, $2 + \sqrt{-1}$ is a prime in $\mathbb{Z}[\sqrt{-1}]$ which is not a prime in $\mathbb{Z}$.

Now, let me be more specific about the Question. We can't even list all the rational primes; how could we hope to find all primes in some number field? Quite right. My goal is not to list all the primes of a number field. Rather, I want to understand how the primes of a number field relate to the rational primes.

Question 2. How do the primes in a number field relate to the rational primes?

Consider: every rational integer (i.e. element of $\mathbb{Z}$) is also an integer in our number field (i.e. element of $\mathbb{Z}[\sqrt{-1}]$). Thus every rational prime is also an integer in our number field; an *integer*, but it may or may not remain *prime*.

As it turns out, 3 is still prime in $\mathbb{Z}[\sqrt{-1}]$. But 5 is no longer prime: it factors $5 = (2 + \sqrt{-1})(2 - \sqrt{-1})$. Also 7 remains prime, 11 remains prime, 13 factors as $13 = (3 + 2\sqrt{-1})(3 - 2\sqrt{-1})$, and so on.

Furthermore, every prime of $\mathbb{Z}[\sqrt{-1}]$ is (either a rational prime or) a factor of a rational prime. Indeed, one can check that if $a + b\sqrt{-1}$ is a prime, then $(a + b\sqrt{-1})(a - b\sqrt{-1}) = a^2 + b^2$ is a rational prime. It is also true, and believable from the previous fact, that every rational prime factors into at most two primes in $\mathbb{Z}[\sqrt{-1}]$.

The same is true in any number field, that every prime is a factor of a rational prime, and that rational primes factor into at most some number of primes (this number is the degree of the number field). By understanding "the relationship between primes in a number field and rational primes" I mean "understanding how rational primes factor in a number field". And we can start with an even simpler question: which rational primes are totally split?

As with any question in algebra, symmetry is waiting in the wings, and now's the time to bring it out. Every number field has a group of symmetries, namely its automorphisms as a field. This is called its *Galois group*. It is named for Évariste Galois, the young Frenchman who first used it to great effect (in studying when a polynomial is "solvable by radicals"), and whose picture you see on the advertisement for this lecture. (It's a nice picture—he looks very mischevious.)

Since the Galois group is the group of symmetries of our number field, and we're trying to study our number field, one is justified in believing it will play an important role. We engage the services of our Galois group in the following way: if π is a prime in our number field, then acting on π by any symmetry of our number field (i.e. element of the Galois group) produces another prime in our number field (possibly the same one). Thus the Galois group acts on the set of primes in our number field.

Furthermore, field automorphisms have to fix 1, so they have to fix any rational integer $1 + \cdots + 1$, and in particular they have to fix any rational prime. Thus the Galois group acts on the set of primes dividing any fixed rational prime. We wanted to understand how a prime factors in a number field; now we have a group acting on this factorization, and that is a good sign.

That's been a lot, we need desperately to return to our example of the number field $\mathbb{Q}(\sqrt{-1})$ and its integers $\mathbb{Z}[\sqrt{-1}]$. First of all, what is the Galois group? In addition to the identity, there's only one other symmetry (let's call it σ) exchanging $\sqrt{-1}$ with $-\sqrt{-1}$, i.e. $\sigma : a + b\sqrt{-1} \mapsto a - b\sqrt{-1}$. The Galois group consists of these two symmetries. And in the examples we wrote down above, it's evident that (the identity fixes everything and) σ exchanges the two prime factors of each rational prime that factors.

This is a good start, but we can make a stronger connection between primes and the Galois group. For every rational prime p we can associate a symmetry, an element of the Galois group, which we call Frob_p (Frob for Frobenius), which will tell us a whole bunch about how the prime factors. (Actually Frob_p is only well-defined up to conjugation, but it's fine to think of it as an element).

I think it's necessary to give some suggestion as to what Frob_p is, but it's a bit complicated, so I authorize you to ignore completely what I'm about to say.

[Recall that modulo p, it's true that $(x + y)^p \equiv x^p + y^p$. Thus p-powering is a morphism modulo p, and it is called the Frobenius morphism. Now, if π is a prime of $\mathcal{O}_K$ dividing a prime p of $\mathbb{Z}$, then $\mathcal{O}/\pi$ is an extension of $\mathbb{Z}/p = \mathbb{F}_p$, and it has a distinguished automorphism: p-powering, i.e. the Frobenius. Now Frob_p is an element of the Galois group of K that fixes π and reduces to the p-power Frobenious mod π.]

Now I insist that you return to attention, because here's what you really need to know about Frob_p.

- It's an element of the Galois group associated to the rational prime p.
- For intuition, it's "like p-powering".
- Frob_p is the identity precisely when p is totally split. (This is not so hard to see from the definition of Frob_p, but I won't explain it.)
- More specific things I won't go into.

The point: Frob_p is a way of encoding in our Galois group very specific information about the factorization of p.

Back to our example. Recall that our Galois group has the two elements $\{\mathrm{id}, \sigma\}$ where $\sigma : \sqrt{-1} \to -\sqrt{-1}$. For each rational prime p, Frob_p is either id or σ. In fact our intuition that Frob_p is "like p-powering" is delightfully accurate: Frob_p is the element of the Galois group given by $\sqrt{-1} \mapsto (\sqrt{-1})^p$. Since all primes p are odd, we can rewrite

$$(\sqrt{-1})^p = (\sqrt{-1})^{p-1}\sqrt{-1} = (-1)^{\frac{p-1}{2}}\sqrt{-1} = \begin{cases} \sqrt{-1} & \text{if } p \equiv 1 \bmod 4 \\ -\sqrt{-1} & \text{if } p \equiv 3 \bmod 4 \end{cases}.$$

(Here is an example of where we're ignoring things: not all primes are odd. But it's an accurate representation of the true situation in the sense that all but finitely many primes are odd, and what we're ignoring only ever includes finitely many primes.)

It's impossible to ignore any longer our motivating question in the case of $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Z}[\sqrt{-1}]$. Recall the question: we want to know what all the primes of $\mathbb{Z}[\sqrt{-1}]$ are, in the sense of understanding how primes of $\mathbb{Z}$ factor in $\mathbb{Z}[\sqrt{-1}]$. Now observe the answer.

1. A prime either remains prime or factors into two primes (up to finitely many exceptions; in this case the only exception is 2).
2. A prime p factors into two primes (i.e. is totally split) when $\mathrm{Frob}_p = \mathrm{id}$, and remains prime when $\mathrm{Frob}_p = \sigma$.
3. $\mathrm{Frob}_p = \mathrm{id}$ when $p \equiv 1 \bmod 4$, and $\mathrm{Frob}_p = \sigma$ when $p \equiv 3 \bmod 4$.

Thus $p \equiv 1 \bmod 4$ factor into two primes, and $p \equiv 3 \bmod 4$ remain prime. That is, the primes of $\mathbb{Z}[\sqrt{-1}]$ consist of the rational primes $p \equiv 3 \bmod 4$ and two primes for each $p \equiv 1 \bmod 4$.

We could have arrived at the conclusion sooner in this example. But the theory we're developing is essential for the general case, and despite knowing the answer, we'll continue to illustrate the theory with this example.

What made the question so easy in this case was the ease with which we could write down Frob_p. In general it is not at all easy to determine Frob_p. How can we proceed?

As another general principle, when dealing with groups we can almost always expect representation theory to be useful. A *representation* of a group G is an action of G on a vector space, or equivalently, a morphism $G \to \mathrm{GL}_n(\mathbb{C})$. (We could replace $\mathbb{C}$ with any field, and this is often a good idea, but today we'll stick with $\mathbb{C}$.)

Representation theory is a whole field in itself, so there's no time to get into it, but one of the main morals is this: if you understand the representations, you understand the group. So a possible way to approach our problem is to look for representations of our Galois groups, and in particular try to understand what happens to Frob_ps.

In fact, let's take it a step further. Remember that each number field has its own symmetries, its own Galois group. Instead of considering them all individually, we can collect them all into a single *absolute Galois group* and then study this object. By taking the union of all number fields, we get a big extension of the rational number, an algebraic closure. The group of symmetries of this thing, i.e. its Galois group, is the absolute Galois group $G_{\mathbb{Q}}$ of $\mathbb{Q}$. Just as the algebraic closure is made up of number fields, the absolute Galois group is made up of the Galois groups of number fields in a very precise way. More precisely, the Galois groups of number fields are precisely the (continuous) finite quotients of the absolute Galois group.

Because of the precise relationship between the absolute Galois group $G_{\mathbb{Q}}$ and the Galois groups of number fields, if we understand the representations of $G_{\mathbb{Q}}$ then we understand the representations of all Galois groups of number fields. More precisely, every representation $G_{\mathbb{Q}} \to \mathrm{GL}_n \mathbb{C}$ factors through $G_{\mathbb{Q}} \to \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{GL}_n \mathbb{C}$ where $\mathrm{Gal}(K/\mathbb{Q})$ is the Galois group of some number field. In this sense the representations of $G_{\mathbb{Q}}$ are precisely all o the representations of Galois groups of number fields. So our motivating question we've carried since the beginning now has the following form.

Question 3. What are the representations of $G_{\mathbb{Q}}$, and how does each Frob_p behave?

Finally: a *Galois representation* is a representation of $G_{\mathbb{Q}}$. Everything we've just gone through is one big reason *why* number theorists want to find Galois representations.

Now we turn to the second question: *where*? This is what the Langlands program is all about. The Langlands philosophy is that Galois representations should be connected to representation theory of other groups we understand better.

$$\{\text{automorphic representations}\} \longleftrightarrow \{\text{Galois representations}\}$$

Automorphic representations are complicated to define, but the key point that I want to convey is that they happen on groups that are easier to understand. On the right side the group is $G_{\mathbb{Q}}$, which is so messed up that it's hard to even write down an element of it. On the left hand side there are many groups, but they're things like matrix groups, like GL_n, whose elements are just matrices, and whose representation theory is much better understood.

Let's illustrate this with an example. (This is also the point when I'll stop trying to stay accessible to people without abstract algebra.) The simplest group that can appear on the left hand side is GL_1, the group of one-by-one invertible matrices. In this case the Langlands correspondence is given by a little piece of number theory called class field theory dating all the way back to the '30s.

Class field theory revolves around the Artin map:

$$\theta : \mathbb{A}^\times / \mathbb{Q}^\times \to G_{\mathbb{Q}}^{\mathrm{ab}}.$$

On the right is the abelianization of $G_{\mathbb{Q}}$, i.e. the biggest abelian quotient. On the left is the *idèle class group*, which is something of a monster. Essentially $\mathbb{A}^\times$ is a product over $\mathbb{R}^\times$ and all p-adic fields $\mathbb{Q}_p^\times$, and then we mod out by $\mathbb{Q}^\times$. The details don't matter for us, the point is that the idèle class group is more intrinsic than the absolute Galois group (or its abelianization). And the content of class field theory is that the Artin map is not-quite-but-very-nearly-an-isomorphism. (It's an isomorphism of profinite completions.)

To understand this as Langlands for GL_1 we first rewrite the left hand side of the Artin map.

$$\theta : \mathrm{GL}_1(\mathbb{A}) / \mathrm{GL}_1(\mathbb{Q}) \to G_{\mathbb{Q}}^{\mathrm{ab}}.$$

It turns out that an automorphic representation of GL_1 is simply a 1-dimensional representation of $\mathrm{GL}_1(\mathbb{A}) / \mathrm{GL}_1(\mathbb{Q})$.

The Artin map allows us to link Galois representations and automorphic representations. Let $G_{\mathbb{Q}} \to \mathrm{GL}_1(\mathbb{C})$ be a 1-dimensional Galois representation. Since the image is abelian it factors $G_{\mathbb{Q}} \to G_{\mathbb{Q}}^{\mathrm{ab}} \to \mathrm{GL}_1(\mathbb{C})$. Then composing with the Artin map we get an automorphic representation $\mathbb{A}^\times/\mathbb{Q}^\times \to G_{\mathbb{Q}}^{\mathrm{ab}} \to \mathrm{GL}_1(\mathbb{C})$. The not-quite-but-very-nearly-an-isomorphism property shows that the 1-dimensional representations of $G_{\mathbb{Q}}$ are not-quite-but-very-nearly the same as automorphic representations of GL_1.

Furthermore, while Frob_p is difficult to write down on the Galois side, on the automorphic side it is much easier. Recall that $\mathbb{A}^\times = \mathrm{GL}_1(\mathbb{A})$ is some kind of product over $\mathbb{R}^\times$ and $\mathbb{Q}_p^\times$. The thing sent to Frob_p by the Artin map is simply the element with a p in the $\mathbb{Q}_p$ slot and 1 elsewhere.

$$\begin{aligned} \theta : \mathrm{GL}_1(\mathbb{A})/\mathrm{GL}_1(\mathbb{Q}) &\to G_{\mathbb{Q}}^{\mathrm{ab}} \\ (1, \ldots, 1, p, 1, \ldots) &\mapsto \mathrm{Frob}_p \end{aligned}$$

This realizes the Langlands philosophy for GL_1: we have a connection between automorphic representations of GL_1 and (some of the) representations of $G_{\mathbb{Q}}$, and we can characterize what happens to Frob_p.

This is only the very slightest idea of what Langlands is really about; I still don't know it that well myself. But to give an idea, GL_1 can be replaced by any connected reductive group, $\mathbb{Q}$ can be replaced by any number field, or by still other fields for other versions of Langlands, and there are other aspects besides matching up representations, and much more.