My thesis for the layman

Kimball Martin

August 12, 2004

These are notes written to explain, informally, what my thesis (entitled *Four-dimensional Galois representations of solvable type and automorphic forms*) is about for all my friends who have asked. I tried to write at the level of popular science for a general Caltech undergrad. Questions and suggestions are, as always, welcome.

1 Fields

Let's consider a simple example first. I hope you know what $\mathbb{R}$ (the real numbers) and $\mathbb{C}$ (the complex numbers) are. If not, you may as well stop reading now. They are examples of *fields*, i.e., number systems which contain 0 and 1 and for which you can add, subtract, multiply or divide any two numbers in the system and get another number in the system. (I am assuming that addition and multiplication satisfy all the usual rules you're familiar with from elementary school, i.e., the commutative [$a+b=b+a$, $ab=ba$], associative [$a+(b+c)=(a+b)+c$, $(ab)c=a(bc)$] and distributive [$a(b+c)=ab+ac$] laws. One can define more general number systems by getting rid of some of these properties.) For example, the integers aren't a field because you can't divide, and the non-negative reals aren't because you can't subtract. However the rational numbers $\mathbb{Q}$ are a field. In fact, they are the smallest field contained in $\mathbb{R}$.

A field is considered an algebraic structure since you can do algebra on it, just like with the real or rational numbers. An important tool to study algebraic structures is to look at their "symmetries," or *automorphisms*. An automorphism of an algebraic structure is essentially just a relabeling of all its elements which preserves its structure. Say F is a field. Then we think of an automorphism ϕ of F as a function $\phi : F \to F$ such that $\phi(a+b) = \phi(a) + \phi(b)$ and $\phi(ab) = \phi(a)\phi(b)$. One sees that from this definition, ϕ preserves the additive and multiplicative structures of the field (and these are the only structures that a field has). You can easily show (well, I can anyway) that the additive and multiplicative identities must also be preseved by ϕ, i.e., $\phi(0) = 0$ and $\phi(1) = 1$.

An *extension of fields E over F* (which I'll also write as E/F) is a field E which contains the field F. For example $\mathbb{C}/\mathbb{R}$ is such an extension, as well as $\mathbb{R}/\mathbb{Q}$ and $\mathbb{C}/\mathbb{Q}$. The first extension is much "smaller" than the latter two extensions. By this I mean the following. You may be familiar with the fact that $\mathbb{C}$ is two-dimensional over $\mathbb{R}$, i.e., any element z of $\mathbb{C}$ can be described by two real parameters x and y in $\mathbb{R}$, namely $z = x + iy$. We say the *degree* of $\mathbb{C}/\mathbb{R}$ is two. On the other hand, if you try to do the same thing with $\mathbb{R}/\mathbb{Q}$ ore $\mathbb{C}/\mathbb{Q}$, you'll find that these extensions have infinite degree. For example, if you want to describe an arbitrary real number x in terms of rationals $r_1, r_2, \ldots$, you need to do something like $x = r_1 + \sqrt{2}r_2 + \sqrt[3]{2}r_3 + \cdots + \sqrt{3}r_? + \cdots + \pi r_? + \pi^2 r_? + \cdots$. The fact that I needed to put question marks in the subscripts for the r's might clue you in that the degree of $\mathbb{R}/\mathbb{Q}$ is not just infinite, but uncountably so.

Formally, the degree of an extension E/F is the dimension of E as a vector space over F. In other words, the degree (when finite) is the smallest number n such that we can write any z in E in terms of n elements of F, i.e., $z = x_1 z_1 + x_2 z_2 + \cdots + x_n z_n$. Here each x_i is in F and each z_i is a *fixed* element of E. As the x_i independently range over F, the z values should range over all of E. So this sort of means if you paste F together to itself n-times in the right way, you essentially get E. Thus the degree really is a way of quantifying the size of E/F. If the degree of E/F is finite, then we say the extension E/F is *finite*.

2 What is number theory, anyway?

The fields of most interest to number theorists (classically, at least) are *number fields*, i.e., finite extensions of $\mathbb{Q}$. I'll vaguely say what the reason is. Perhaps it would be good if you knew what number theory was about first. The principal goal in number theory is to determine the integer solutions to polynomial equations, such as $y^2 = x^3 + 2$, $z^2 = u^4 + v^4$ and $x^n + y^n = z^n$. In many cases, it turns out to be easier to first determine the rational solutions to an equation, since the rationals have more structure than the integers (namely division). Number theorists discovered that it was often helpful to use larger fields to find solutions in smaller ones. Here's a quick example.

Suppose we want to solve $x^2 + y^2 = 5$. One approach is to just try all possible values for x and y, but we want to make things a little more challenging for ourselves. (Otherwise, we'll never get any theorems and never understand the structure of things.) Let $\mathbb{Q}(i)$ denote the numbers of the form $a + bi$ where a and b are rational and $i^2 = -1$. (Note $\mathbb{Q}(i)$ is a field of degree two over $\mathbb{Q}$.) We can factor the left side of our equation in $\mathbb{Q}(i)$ to get $(x + iy)(x - iy) = 5$. We couldn't do this sort of thing if we only stuck to $\mathbb{Q}$. Now just as there are prime numbers in $\mathbb{Q}$, we also have a notion of primes in $\mathbb{Q}(i)$ (see the next paragraph). So we can factor 5 into primes of $\mathbb{Q}(i)$. Then $(x+iy)$ and $(x-iy)$ have to be appropriate products of these primes and we can see which ones work out. (Just think about how you would solve $rs = 5$ in integers. Well, since 5 is prime in $\mathbb{Q}$, the only possibilities are $r = \pm 5$, $s = \pm 1$ and $r = \pm 1$, $s = \pm 5$.) Note that 5 is not prime in $\mathbb{Q}(i)$, even though it is in $\mathbb{Q}$, since $5 = 1 + 4 = (1 + 2i)(1 - 2i)$. Basic algebraic number theory tells me that $(1 + 2i)$ and $(1 - 2i)$ are primes in $\mathbb{Q}(i)$. So 5 factors as $5 = 1 \cdot 5 = (1 + 2i)(1 - 2i)$ Thus $x + iy$ and $x - iy$ have to equal either 1 and 5 or $(1 + 2i)$ and $(1 - 2i)$. Well, only the latter can happen for x, y rational and we see that the integer solutions are $x = \pm 1$, $y = \pm 2$ or $x = \pm 2$, $y = \pm 1$. (Observe that I could have done all this with integers instead of rationals, but I won't tell you my clandestine reasons for using fields.)

While it was wholly unnecessary to introduce $\mathbb{Q}(i)$ to solve $x^2 + y^2 = 5$, you might imagine that such an approach is actually the more elegant way to go in more complicated situations. The fundamental point here is that solving equations in number theory boils down to questions about primes. I didn't actually tell you what I meant by primes and there are some serious technicalities. The basic idea is this. In the usual integers $\mathbb{Z}$, we have units (i.e., numbers of absolute value 1, which are just ± 1 for $\mathbb{Z}$), primes and composites. Any composite number can be written uniquely (up to trivial modifications) as a product of primes and units. The primes $2, 3, 5, 7, \ldots$ can't be factored any further using non-units. Now any number field also has something called a ring of integers, and this contains the usual integers (also called the rational integers) $\mathbb{Z}$. In the case of $\mathbb{Q}(i)$, the ring of integers is the set $\mathbb{Z}[i]$ of numbers of the form $a + bi$ where a and b are in $\mathbb{Z}$. In general, the ring of integers isn't so simple. And another crazy thing that happens is you don't always have unique factorization in the ring of integers like in $\mathbb{Z}$, but you do have unique factorization of "ideal numbers," which is beyond what I want to talk about. In the case of $\mathbb{Q}(i)$ you do have unique factorization in the ring of integers and you can define primes as the non-units in $\mathbb{Z}[i]$ which cannot be factored further into non-units. For a general number field, you have to define primes in terms of these "ideal numbers."

You may now be wondering, why number theory? I have often wondered that myself. I don't know and I'm not sure anyone else does either, but it seemed like a good idea at the time. I think principally because it's fun and interesting of its own right, but you, the non-mathematician, may only want to know about applications (which is, in my mind, a pity). Most applications of number theory that I know of are in computer science and modern physics. (Actually, most are in other fields of math. I would say number theory and calculus have been the two main driving forces in the development of modern mathematics.) Often the applications aren't discovered until much after the theory. In computer science, number theory is important to both cryptography and coding theory. There's a lot of solving polynomial equations (mod 2) and the current standard public-key encryption system (RSA) relies entirely on the supposition that factoring large numbers is hard. A lot of number theory has gone into convincing us that it is so and determining how big you need to make your key to ensure it's secure.

In terms of physics, let's think of the following. To determine the five Platonic solids, you find some necessary equations that they must satisfy and the solids are determined by the *integer* solutions to these equations. Similarly, to determine possible shapes of electron orbitals, for example, you need to determine *integer* solutions to certain equations. Now this is a simple example that doesn't require advanced number theory, but it illustrates the principle whereby the determination of some structure with discrete possibilities leads to a question of finding integer solutions to equations. I think that there are important applications of

number theory (or at least of methods developed therein) in particle physics and string theory, maybe even in relativity, but I'm still just learning about that.

3 What is a Galois representation?

Well, since you asked, I'll tell you. It's a representation of a Galois group, of course!

Okay, now that you've mastered all the subtleties of that definition, let's return to the notion of an automorphism. Let E/F be an extension of fields. Then the *Galois group*, $\mathrm{Gal}(E/F)$, is the *group* of automorphisms of E which fix each element of F. For example $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ has two elements: the identity (i.e., the trivial automorphism which fixes every element of $\mathbb{C}$) and complex conjugation. It's easy to check that these are automorphisms. In general, for a "nice" extension E/F (such as $\mathbb{C}/\mathbb{R}$ or $\mathbb{Q}(i)/\mathbb{Q}$), the size of $\mathrm{Gal}(E/F)$ is the degree of the extension E/F. Being a group means that you can compose any two automorphisms and get another one and that each automorphism has an inverse. In $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$, the inverse of complex conjugation is, well, complex conjugation. Similarly the Galois group of $\mathbb{Q}(i)/\mathbb{Q}$ contains exactly two elements: the trivial automorphism and complex conjugation.

The Galois group tells you lots of important things about the extension E/F. In particular, you can use $\mathrm{Gal}(E/F)$ to study the primes of E and F (more precisely, to study how primes in F decompose into primes in E, as $5 = (1+2i)(1-2i)$ in our example above). A *representation* of a group is essentially a way of looking at that group as a set of matrices.[1] For example, consider $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$. Write the trivial automorphism as e and complex conjugation as c. Then $e(a+bi) = a+bi$ and $c(a+bi) = \overline{a+bi} = a-bi$. We can write this in matrix form as

$$e(a+bi) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} = a+bi,$$

and

$$c(a+bi) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ -b \end{pmatrix} = a-bi,$$

where the column vector $\begin{pmatrix} a \\ b \end{pmatrix}$ represents $a+bi$. So we can think of e and c as the 2×2 matrixes $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. More formally, I can define a function ρ from $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$ to the 2×2 matrices (with complex coefficients, say) by

$$\rho(e) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \rho(c) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Then I say that ρ is a (Galois) representation of $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$. So I've contained all the information about this Galois group within this representation. [In general, an *n-dimensional representation* is a just map ρ from a group G into the set of $n \times n$ invertible matrices which preserves the composition (or multiplication) law, i.e., $\rho(ab) = \rho(a)\rho(b)$; it need not be one to one. There are lots of representations (the "irreducible" ones are given by the character table of a group, if you've learnt that in organic chemistry or elsewhere), some of which tell you everything about the group and some don't. In fact, there's always the trivial representation ρ_0 which sends every group element to the identity matrix, and that doesn't tell you much at all.]

4 The Langlands Program

Tagline: Attach automorphic representations to Galois representations.

In the early 1900's, Emil Artin defined an object called an L-function in terms of a Galois representation. These L-functions are analytic objects, maps from $\mathbb{C}$ to $\mathbb{C}$, where as the Galois representation is a very algebraic object. The L-function attached to a Galois representation ρ is denoted $L(s,\rho)$. (100 points for anyone who can tell me what the L-stands for—no one seems to know, but the terminology goes back to L. Dirichlet.) Dirichlet had previously introduced the notion of L-functions in a simpler setting to prove a

[1] Now I'll assume you know what a matrix is and what matrix multiplication is. If you don't, go find out, at least for 2×2 matrices.

wonderful theorem which essentially says that in any arithmetic progression, there are an infinite number of primes. More precisely, if a and b are positive integers with no common factors, then the set of numbers

$$a + b, a + 2b, a + 3b, a + 4b, a + 5b, \ldots$$

contains infinitely many primes. Even though it is a simple statement that mathematicians believed to be true for a long time, they remained unable to prove it until Dirichlet's very ingenious use of L-functions. With even more modern techniques, we can in fact say precisely what percentage of numbers in an arithmetic progression are prime.

Artin conjectured that for "non-trivial, irreducible" Galois representations, $L(s, \rho)$ is *entire*, i.e., continuous and infinitely differentiable at each point in the complex plane. This would give some information on primes, but it's really hard to prove this analytic fact from this algebraic object. The general strategy is to attach to each Galois representation something called an "automorphic representation," which is an also analytic object with an analytic L-function. We say a Galois representation is attached to an automorphic representation if they have the "same" L-function. These L-functions of automorphic representations (of a certain type) are entire, so this correspondence between algebraic objects and analytic objects would give Artin's conjecture as a special case. This correspondence was conjectured in a general setting by Langlands (the "Langlands program"), and the precise statement of these conjectures took many years to formulate. It has far-reaching consequences and is one of the most important areas of current mathematical research by connecting seemingly fundamentally different areas of mathematics (analytic and algebraic).

This "Langlands correspondence" (for GL_n) was established for one-dimensional representations and "most" two-dimensional representations. The two-dimensional case plays an important role in the Wiles's famous proof of Fermat's Last Theorem. Not much is known in other dimensions, except some results in four-dimensions by my advisor, Dinakar Ramakrishnan. For my thesis, I looked at other four-dimensional cases and tried to classify the "simpler" ones (the ones of *solvable type*), using completely different methods than what Dinakar did (I mostly used finite group theory). In certain cases (which weren't known before), I was able to establish this correspondence. See me or my thesis for more details.

As a final remark, I realize that I didn't mention the last term in the title of my thesis, i.e., the term *automorphic form*. To be honest, I don't think that term even appears anywhere else in my thesis (apart from the references, perhaps) so you can probably forget about it. The idea is that automorphic forms correspond to automorphic representations, so you can talk about whichever one you want.