THIS WEEK'S FINDS IN MATHEMATICAL PHYSICS - WEEK 201

JOHN BAEZ

Lately James Dolan and I have been studying number theory. I used to *hate* this subject: it seemed like a massive waste of time. Newspapers, magazines and even lots of math books seem to celebrate the idea of people slaving away for centuries on puzzles whose only virtue is that they're easy to state but hard to solve. For example: are any odd numbers the sum of all their divisors? Are there infinitely many pairs of primes that differ by 2? Is every even number bigger than 2 a sum of two primes? Are there any positive integer solutions to

$$x^n + y^n = z^n$$

for $n > 2$? My response to all these was: WHO CARES?!

Sure, it's noble to seek knowledge for its own sake. But working on a math problem just because it's *hard* is like trying to drill a hole in a concrete wall with your nose, just to prove you can! If you succeed, I'll be impressed – but I'll still wonder why you didn't put all that energy into something more interesting.

Now my attitude has changed, because I'm beginning to see that behind these silly hard problems there lurks an actual *theory*, full of deep ideas and interesting links to other branches of mathematics, including mathematical physics. It just so happens that now and then this theory happens to crack another hard nut.

I'd known for a while that something like this must be true: after all, when Andrew Wiles proved Fermat's Last Theorem, even the newspapers admitted this was just a spinoff of something more important, namely a special case of the Taniyama-Shimura Conjecture. They said this had something to do with elliptic curves and modular forms, which are very nice geometrical things that show up all over in complex analysis and string theory. Unfortunately, the actual statement of this conjecture seemed impenetrable – it didn't resonate with things I understood.

In fact, the Taniyama-Shimura Conjecture is part of a big *network* of problems that are more interesting but harder to explain than the flashy ones I listed above: problems like the Extended Riemann Hypothesis, the Weil Conjecture (now solved), the Birch-Swinnerton-Dyer Conjecture, and bigger projects like the Langlands Program and developing the theory of "motives". And these problems rest on top of a solid foundation of beautiful stuff that's already known, like Galois theory and class field theory, and stuff about modular forms and L-functions.

As I'm gradually beginning to understand little bits of these things, I'm getting really excited about number theory ..., so I'm dying to *explain* some of it! But where to start? I have to start with something basic that underlies all the fancy stuff. Hmm, I think I'll start with Galois theory.

As you may have heard, Galois invented group theory in the process of showing you can't solve the quintic equation

$$ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$$

by radicals. In other words, he showed you can't solve this equation by means of some souped-up version of the quadratic formula that just involves taking the coefficients a, b, c, d, e, f and adding, subtracting, multiplying, dividing and taking nth roots.

The basic idea is something like this. In general, a quintic equation has 5 solutions – and there's no "best one", so your formula has got to be a formula for all five. And there's a puzzle: how do you give one formula for five things?

Well, think about the quadratic formula! It has that "plus or minus" in it, which comes from taking a square root. So, it's really a formula for *both* solutions of the quadratic equation. If there were a formula for the quintic that worked like this, we'd have to get all 5 solutions from different choices of nth roots in this formula.

Galois showed this can't happen. And the way he did it used *symmetry*! Roughly speaking, he showed that the general quintic equation is completely symmetrical under permuting all 5 solutions, and that this symmetry group – the group of permutations of 5 things – can't be built up from the symmetry groups that arise when you take nth roots.

The moral is this: you can't solve a problem if the answer has some symmetry, and your method of solution doesn't let you write down an answer that has this symmetry!

An old example of this principle is the medieval puzzle called "Buridan's Ass". Placed equidistant between two equally good piles of hay, this donkey starves to death because it can't make up its mind which alternative is best. The problem has a symmetry, but the donkey's method of solution doesn't, so it's stuck.

Buridan's ass would also get stuck if you asked it for *the* solution to the quadratic equation. Galois proof of the unsolvability of the quintic by radicals is just a more sophisticated variation on this theme. (Of course, you *can* solve the quintic if you strengthen your methods.)

A closely related idea is "Curie's principle", named after Marie's husband Pierre. This says that if your problem has a symmetry and it is a unique solution, the solution must be symmetrical.

For example, if some physical system has rotation symmetry and it has a unique equilibrium state, this state must be rotationally invariant.

Now, in the case of a ferromagnet below its "Curie temperature", the equilibrium state is *not* rotationally invariant: the little magnetized electrons line up in some specific direction! But this doesn't contradict Curie's principle, since there's not a unique equilibrium state – there are lots, since the electrons can line up in any direction.

Physicists use the term "spontaneous symmetry breaking" when any *one* solution of a symmetric problem is not symmetrical, but the whole set of them is. This is precisely what happens with the quintic, or even the quadratic equation.

While these general ideas about symmetry apply to problems of all sorts, their application to number theory kicks in when we apply them to *fields*. A "field" is a gadget where you can add, subtract, multiply and divide by anything nonzero, and a bunch of familiar laws of arithmetic hold, which I won't bore you with here. The three most famous fields are the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$. However, there are lots of other interesting fields.

Number theorists are especially fond of algebraic number fields. An "algebraic number" is a solution to a polynomial equation whose coefficients are rational numbers. You get an "algebraic number field" by taking the field of rational numbers, throwing in finitely many algebraic numbers, and then adding, subtracting, multiplying and dividing them to get more numbers until you've got a field.

For example, we could take the rationals, throw in the square root of 2, and get a field consisting of all numbers of the form $a+b\sqrt{2}$ where a and b are rational. Notice: if we add, multiply, subtract or divide two numbers like this, we get another number of this form. So this is really a field – and it's called $\mathbb{Q}(\sqrt{2}\,)$, since we use round parentheses to denote the result of taking a field and "extending" it by throwing in some extra numbers.

More generally, we could throw in the square root of any integer n, and get an algebraic number field called $\mathbb{Q}(\sqrt{n}\,)$, consisting of all numbers $a+b\sqrt{n}$ where a and b are rational. If $\sqrt{n}$ is rational then this field is just $\mathbb{Q}$, which is boring. Otherwise, we call it a "quadratic number field".

Even more generally, we could take the rationals and throw in a solution of any quadratic equation with rational coefficients. But it's easy to see that this doesn't give anything beyond fields like $\mathbb{Q}(\sqrt{n}\,)$. And that's the real reason we call these the "quadratic number fields".

There are also "cubic number fields", and "quartic number fields", and "quintic number fields", and so on. And others, too, where we throw in solutions to a whole bunch of polynomial equations!

Now, it turns out you can answer lots of classic but rather goofy-sounding number theory puzzles like "which integers are a sum of two squares?" by converting them into questions about algebraic number fields. And the good part is, the resulting questions are connected to all sorts of other topics in math – they're not just glorified mental gymnastics! So, from a modern viewpoint, a bunch of classic number theory puzzles are secretly just tricks to get certain kinds of people interested in algebraic number fields.

But right now I *don't* want to explain how we can use algebraic number fields to solve classic but goofy-sounding number theory puzzles. In fact, I want to downplay the whole puzzle aspect of number theory.

Instead, I hope you're reeling with horror at thought of this vast complicated wilderness of fields containing $\mathbb{Q}$ but contained in $\mathbb{C}$. First there's a huge infinite thicket of algebraic number fields ... and then, there's an ever scarier jungle of fields that contain transcendental numbers like π and e! I won't even talk about *that* jungle, it's so dark and scary. Physicists usually zip straight past this whole wilderness and work with C.

But in fact, if you stop and carefully examine all the algebraic number fields and how they sit inside each other, you'll find some incredibly beautiful patterns. And these patterns are turning out to be related to Feynman diagrams, topological quantum field theory, and so on ....

However, before we can talk about all that, we need to understand the basic tool for analyzing how one field fits inside another: Galois theory!

A function from a field to itself that preserves addition, subtraction, multiplication and division is called an "automorphism". It's just a *symmetry* of the field. But now, suppose we have a field K which contains some smaller field k. Then we

define the "Galois group of K over k" to be the group of all automorphisms of K that act as the identity on k. We call this group $\mathrm{Gal}(K/k)$ for short.

The classic example, familiar to all physicists, is the Galois group of the complex numbers, $\mathbb{C}$, over the real numbers, $\mathbb{R}$. This group has two elements: the identity transformation, which leaves everything alone, and complex conjugation, which switches i and $-i$. Since the only group with 2 elements is $\mathbb{Z}/2$, we have $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \mathbb{Z}/2$.

Where does complex conjugation come from? It comes from the fact that $\mathbb{C}$ from $\mathbb{R}$ by throwing in a solution of the quadratic equation $x^2 = -1$. We say $\mathbb{C}$ is a "quadratic extension of $\mathbb{R}$". But as soon as we throw in one solution of this equation, we inevitably throw in another, namely its negative – and there's no way to tell which is which. And complex conjugation is the symmetry that switches them!

Note: we know that i and $-i$ are different, but we can't tell which is which! This sounds a bit odd at first. It's a bit hard to explain precisely in ordinary language, which is part of why Galois had to invent group theory. But it's fun to try to explain it in plain English ... so let me try. The complex numbers have two solutions to $x^2 = -1$. By convention, one of them is called "i", and the other is called "$-i$". Having made this convention, there's never any problem telling them apart. But we could reverse our convention and nothing would go wrong. For example, if the ghost of Galois wafted into your office one moonless night and wrote "$-i$" in all your math and physics books wherever there had been "i", everything in these books would still be true!

Here's another way to think about it. Suppose we meet some extraterrestrials and find that they too have developed the complex numbers by taking the real numbers and adjoining a square root of -1, only they call it "@". Then there would be no way for us to tell if their "@" was our "i" or our "$-i$". All we can do is choose an arbitrary convention as to which is which.

Of course, if they put their "@" in the lower halfplane when drawing the complex plane, we might feel like calling it "$-i$" ... but here we are secretly making use of a convention for matching their complex plane with ours, and the *other* convention would work equally well! If they drew their real line *vertically* in the complex plane, it would be more obvious that we need a convention to match their complex plane with ours, and that there are two conventions for doing this, both perfectly self-consistent.

If you've studied enough physics, this extraterrestrial scenario should remind you of those thought experiments where you're trying to explain to some alien civilization the difference between left and right ... by means of radio, say, where you're *not* allowed to refer to specific objects you both know – so it's cheating to say "imagine you're on Earth looking at the Big Dipper and the handle is pointing down; then Arcturus is to the right."

If the laws of physics didn't distinguish between left and right, you couldn't explain the difference between left and right without "cheating" like this, so the laws of physics would have a symmetry group with two elements: the identity and the transformation that switches left and right. As it turns out, the laws of physics *do* distinguish between left and right – see "week 73" for more on that. But that's another story. My point here is that the Galois group of $\mathbb{C}$ over $\mathbb{R}$ is a similar sort

of thing, but built into the very fabric of mathematics! And that's why complex conjugation is so important.

I could tell you a nice long story about how complex conjugation is related to "charge conjugation" (switching matter and antimatter) and also "time reversal" (switching past and future). But I won't!

Here's another example of a Galois group that physicists should like. Let $\mathbb{C}(z)$ be the field of rational functions in one complex variable z – in other words, functions like $f(z) = P(z)/Q(z)$ where P and Q are polynomials in z with complex coefficients. You can add, subtract, multiply and divide rational functions and get other rational functions, so they form a field. And they contain C as a subfield, because we can think of any complex number as a *constant* function. So, we can ask about the Galois group of $\mathbb{C}(z)$ over $\mathbb{C}$. What's it like?

It's the Lorentz group!

To see this, it's best to think of rational functions as functions not on the complex plane but on the "Riemann sphere" – the complex plane together with one extra point, the "point at infinity". The only conformal transformations of the Riemann sphere are "fractional linear transformations":

$$T(z) = \frac{az + b}{cz + d}.$$

So, the only symmetries of the field of rational functions that act as the identity on constant functions are those coming from fractional transformations, like this:

$$f \longmapsto f^T, \quad \text{where } f^T(z) = f(T(z)).$$

If you don't follow my reasoning here, don't worry – the details aren't hard to fill in, but they'd be distracting here.

The last step is to check that the group of fractional linear transformations is the same as the Lorentz group. You can do this algebraically, but you can also do it geometrically by thinking of the Riemann sphere as the "heavenly sphere": that imaginary sphere the stars look like they're sitting on. The key step is to check this remarkable fact: if you shoot past the earth near the speed of light, the constellations will look distorted by a Lorentz transformation - but if you draw lines connecting the stars, all the *angles* between these lines will remain the same; only their *lengths* will get messed up!

Moreover, it's obvious that if you rotate your head, both angles and lengths on the heavenly spehere are preserved. So, any rotation or Lorentz boost gives an angle-preserving transformation of the heavenly sphere – that is, a conformal transformation! And this must be a fractional linear transformation.

Summarizing, the Galois group of $\mathbb{C}(z)$ over $\mathbb{C}$ is the Lorentz group, or more precisely, its connected component, $\mathrm{SO}_0(3,1)$: $\mathrm{Gal}(\mathbb{C}(z)/\mathbb{C}) = \mathrm{SO}_0(3,1)$.

We've talked about the Galois group of $\mathbb{C}(z)$ over $\mathbb{C}$ and the Galois group of $\mathbb{C}$ over $\mathbb{R}$. What about the Galois group of $\mathbb{C}(z)$ over $\mathbb{R}$? Unsurprisingly, this is the group of transformations of the Riemann sphere generated by fractional linear transformations *and* complex conjugation. And physically, this corresponds to taking the connected component of the Lorentz group and throwing in *time reversal*! So you see, complex conjugation is related to time reversal. But I promised not to go into that ....

I've been talking about Galois groups that physicists should like, but you're probably wondering where the number theory went! Well, it's all part of the same big

story. In number theory we're especially interested in Galois groups like $\mathrm{Gal}(K/k)$ where K is some algebraic number field and k is some subfield of K. For starters, consider this example: $\mathrm{Gal}(\mathbb{Q}(\sqrt{n}\,)/\mathbb{Q})$, where $\sqrt{n}$ is irrational. I've already hinted at what this group is! $\mathbb{Q}(\sqrt{n}\,)$ has $\sqrt{n}$ in it, so it also has $-\sqrt{n}$ in it, and there's an automorphism that switches these two while leaving all the rational numbers alone, namely $a + b\sqrt{n} \longmapsto a - b\sqrt{n}$ $(a, b \in \mathbb{Q})$.

So, we have: $\mathrm{Gal}(\mathbb{Q}(\sqrt{n}\,))/\mathbb{Q}) = \mathbb{Z}/2$ just like the Galois group of $\mathbb{C}$ over $\mathbb{R}$.

To get some bigger Galois groups, let's take $\mathbb{Q}$ and throw in a "primitive nth root of unity". Hmm, I may need to explain what that means. There are n different nth roots of 1 – but unlike the two square roots of -1, these are not all created equal! Only some are "primitive".

For example, among the 4th roots of unity we have 1 and -1, which are actually square roots of unity, and i and $-i$, which aren't. A "primitive nth root of unity" is an nth root of 1 that's not a kth root for any $k < n$. If you take all the powers of any primitive nth root of unity, you get *all* the nth roots of unity. So, if we take some primitive nth root of unity, call it $1^{1/n}$ for lack of a better name, and extend the rationals by this number, we get a field $\mathbb{Q}(1^{1/n})$ which contains all the nth roots of unity. Since the nth roots of unity are evenly distributed around the unit circle, this sort of field is called a "cyclotomic field", for the Greek word for "circle cutting". In fact, one can apply Galois theory to this field to figure out which regular n-gons one can construct with a ruler and compass!

But what's the Galois group $\mathrm{Gal}(\mathbb{Q}(1^{1/n})/\mathbb{Q})$ like? Any symmetry in this group must map $1^{1/n}$ to some root of unity, say $1^{m/n}$ – and once you know which one, you completely know the symmetry. But actually, this symmetry must map $1^{1/n}$ to some *primitive* root of unity, so m has to be relatively prime to n. Apart from that, though, anything goes – so the size of $\mathrm{Gal}(\mathbb{Q}(1^{1/n})/\mathbb{Q})$ is just the number of m less than n that are relatively prime to n. And if you think about it, these numbers relatively prime to n are just the same as elements of $\mathbb{Z}/n$ that have multiplicative inverses! So if you think some more, you'll see that $\mathrm{Gal}(\mathbb{Q}(1^{1/n})/\mathbb{Q}) = (\mathbb{Z}/n)^\times$ where $(\mathbb{Z}/n)^\times$ is the "multiplicative group" of $\mathbb{Z}/n$ – that is, the elements of $\mathbb{Z}/n$ that have multiplicative inverses, made into a group via multiplication!

This group can be big, but it's still abelian. Can we get some nonabelian Galois groups from algebraic number fields?

Sure! Let's say you take some polynomial equation with rational coefficients, take *all* its solutions, throw them into the rationals – and keep adding, subtracting, multiplying and dividing until you get some field K. This K is called the "splitting field" of your polynomial.

But here's the interesting thing: if you pick your polynomial equation at random, the chances are really good that it has n different solutions if the polynomial is of degree n, and that *any* permutation of these solutions comes from a unique symmetry of the field K. In other words: barring some coincidence, all roots are created equal! So in general we have $\mathrm{Gal}(K/\mathbb{Q}) = S_n$, where S_n is the group of all permutations of n things.

Sometimes of course the Galois group will be smaller, since our polynomial could have repeated roots or, more subtly, algebraic relations between roots – as in the cyclotomic case we just looked at.

But, we can already start to see how to prove the unsolvability of the general quintic! Pick some random 5th-degree polynomial, let K be its splitting field, and

note $\mathrm{Gal}(K/\mathbb{Q}) = S_5$. Then, show that if we build up an algebraic number field by starting with $\mathbb{Q}$ and repeatedly throwing in nth roots of numbers we've already got, we just can't get S_5 as its Galois group over the rationals! We've already seen this in the case where we throw in a square root of n, or an nth root of 1. The general case is a bit more work. But instead of giving the details, I'll just mention a good textbook on Galois theory for beginners:

• Ian Stewart, Galois Theory, 3rd edition, Chapman and Hall, New York, 2004.

Ian Stewart is famous as a popularizer of mathematics, and it shows here – he has nice discussions of the history of the famous problems solved by Galois theory, and a nice demystification of the Galois' famous duel. But, this is a real math textbook – so you can really learn Galois theory from it! Make sure to get the 3rd edition, since it has more examples than the earlier ones.

Having given Ian Stewart the dirty work of explaining Galois theory in the usual way, let me say some things that few people admit in a first course on the subject.

So far, we've looked at examples of a field k contained in some bigger field K, and worked out the group $\mathrm{Gal}(K/k)$ consisting of all automorphisms of K that fix everything in k.

But here's the big secret: this has NOTHING TO DO WITH FIELDS! It works for ANY sort of mathematical gadget! If you've got a little gadget k sitting in a big gadget K, you get a "Galois group" $\mathrm{Gal}(K/k)$ consisting of symmetries of the big gadget that fix everything in the little one.

But now here's the cool part, which is also very general. Any subgroup of $\mathrm{Gal}(K/k)$ gives a gadget containing k and contained in K: namely, the gadget consisting of all the elements of K that are fixed by everything in this subgroup.

And conversely, any gadget containing k and contained in K gives a subgroup of $\mathrm{Gal}(K/k)$: namely, the group consisting of all the symmetries of K that fix every element of this gadget.

This was Galois' biggest idea: we call this a GALOIS CORRESPONDENCE. It lets us use *group theory* to classify gadgets contained in one and containing another. He applied it to fields, but it turns out to be useful much more generally.

Now, it would be great if the Galois corresondence were always a perfect $1-1$ correspondence between subgroups of $\mathrm{Gal}(K/k)$ and gadgets containing k and contained in K. But, it ain't true. It ain't even true when we're talking about fields!

However, that needn't stop us. For example, we can restrict ourselves to cases when it *is* true. And this is where the Fundamental Theorem of Galois Theory comes in! It's easiest to state this theorem when k and K are algebraic number fields, so that's what I'll do. In this case, there's a $1-1$ correspondence between subgroups of $\mathrm{Gal}(K/k)$ and extensions of k contained in K if:

i) K is a "finite" extension of k. In other words, K is a finite-dimensional vector space over k.

ii) K is a "normal" extension of k. In other words, if a polynomial with coefficients in k has no roots in k, but one root in K, then all its roots are in K.

For general fields we also need another condition, namely that K be a "separable" extension of k. But this is automatic for algebraic number fields, so let's not worry about it.

At this point, if we had time, we could work out a bunch of Galois groups and see a bunch of patterns. Using these, we could see why you can't solve the general

quintic using radicals, why you can't trisect the angle or double the cube using ruler-and-compass constructions, and why you can draw a regular pentagon using ruler and compass, but not a regular heptagon. Basically, to prove something is impossible, you just show that some number can't possibly lie in some particular algebraic number field, because it's the root of a polynomial whose splitting field has a Galois group that's "fancier" than the Galois group of that algebraic number field.

For example, ruler-and-compass constructions produce distances that lie in "iterated quadratic extensions" of the rationals – meaning that you just keep throwing in square roots of stuff you've got. Doubling the cube requires getting your hands on the cube root of 2. But the Galois group of the splitting field of $x^3 = 2$ has size divisible by 3, while an iterated quadratic extension has a Galois group whose size is a power of 2. Using the Galois correspondence, we see there's no way to stuff the former field into the latter.

But you can read about this in any good book on Galois theory, so I'd rather dive right into that thicket I was hinting at earlier: the field of ALL algebraic numbers! The roots of any polynomial with coefficients in this field again lie in this field, so we say this field is "algebraically closed". And since it's the smallest algebraically closed field containing $\mathbb{Q}$, it's called the "algebraic closure of $\mathbb{Q}$", or $\overline{\mathbb{Q}}$ for short.

This field $\overline{\mathbb{Q}}$ is huge. In particular, it's an infinite-dimensional vector space over $\mathbb{Q}$. So, condition i) in the Fundamental Theorem of Galois Theory doesn't hold. But that's no disaster: when this happens, we just need to put a topology on the group $\mathrm{Gal}(K/k)$ and set up the Galois correspondence using *closed* subgroups of $\mathrm{Gal}(K/k)$. Using this trick, every algebraic number field corresponds to some closed subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

So, for people studying algebraic number fields, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is like the holy grail. It's the symmetry group of the algebraic numbers, and the key to how all algebraic number fields sit inside each other! But alas, this group is devilishly complicated. In fact, it has literally driven men mad. One of my grad students knows someone who had a breakdown and went to the mental hospital while trying to understand this group!

(There may have been other reasons for his breakdown, too, but as readers of E. T. Bell's book "Men in Mathematics" know, the facts should never get in the way of a good anecdote.)

If $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ were just an infinitely tangled thicket, it wouldn't be so tantalizing. But there are things we can understand about it! To describe these, I'll have to turn up the math level a notch ...

First of all, an extension K of a field k is called "abelian" if $\mathrm{Gal}(K/k)$ is an abelian group. Abelian extensions of algebraic number fields can be understood using something called class field theory. In particular, the Kronecker-Weber theorem says that every finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field. So, they all sit inside a field called $\mathbb{Q}_{\mathrm{cyc}}$, which is gotten by taking the rationals and throwing in *all* nth roots of unity for *all* n. Since $\mathrm{Gal}(\mathbb{Q}(1^{1/n})/\mathbb{Q}) = (\mathbb{Z}/n)^\times$ we know from Galois theory that $\mathrm{Gal}(\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q})$ must be a big group containing all the groups $(\mathbb{Z}/n)^\times$ as closed subgroups. It's easy to see that $(\mathbb{Z}/n)^\times$ is a quotient group of $(\mathbb{Z}/m)^\times$ if m is divisible by n; this lets us take the "inverse limit" of all the groups $(\mathbb{Z}/m)^\times$ – and that's $\mathrm{Gal}(\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q})$. This inverse limit is also the multiplicative group of the ring $\widehat{\mathbb{Z}}$, the inverse limit of all the rings $\mathbb{Z}/n$. $\widehat{\mathbb{Z}}$ is also called

the "profinite completion of the integers", and I urge you to play around with it if you never have! It's a cute gadget.

In short: $\mathrm{Gal}(\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q}) = \widehat{\mathbb{Z}}$, and if we stay inside $\mathbb{Q}_{\mathrm{cyc}}$, we're in a zone where the pattern of algebraic number fields can be understood. This stuff was worked out by people like Weber, Kronecker, Hilbert and Takagi, with the final keystone, the Artin reciprocity theorem, laid in place by Emil Artin in 1927. In a certain sense $\mathbb{Q}_{\mathrm{cyc}}$ is to $\overline{\mathbb{Q}}$ as homology theory is to homotopy theory: it's all about *abelian* Galois groups, so it's manageable.

People now use $\mathbb{Q}_{\mathrm{cyc}}$ as a kind of base camp for further expeditions into the depths of $\overline{\mathbb{Q}}$. In particular, since $\mathbb{Q}$ is contained in $\mathbb{Q}_{\mathrm{cyc}}$ and $\mathbb{Q}_{\mathrm{cyc}}$ is contained in $\overline{\mathbb{Q}}$, we get an exact sequence of Galois groups:

$$1 \longrightarrow \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}_{\mathrm{cyc}}) \longrightarrow \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Gal}(\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q}) \longrightarrow 1.$$

So, to understand $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ we need to understand $\mathrm{Gal}(\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q})$, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}_{\mathrm{cyc}})$ and how they fit together! The last two steps are not so easy. Shafarevich has conjectured that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}_{\mathrm{cyc}})$ is the profinite completion of a free group, say F^*. This would give

$$1 \longrightarrow F^* \longrightarrow \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \widehat{\mathbb{Z}} \longrightarrow 1$$

but I have no idea how much evidence there is for Shafarevich's conjecture, or how much people know or guess about this exact sequence.

More recently, Deligne has turned attention to a certain "motivic" version of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, which is a proalgebraic group scheme. This sort of group has a *Lie algebra*, which makes it more tractable. And there are a bunch of fascinating conjectures about this Lie algebra is related to the Riemann zeta function at odd numbers, Connes and Kreimer's work on Feynman diagrams, Drinfeld's work on the Grothendieck-Teichmüller group, and more!

I really want to understand this stuff better – right now, it's a complete muddle in my mind. When I do, I will report back to you. For now, though, let me give you some references.

For two very nice but very different introductions to algebraic number fields, try these:

• H. P. F. Swinnerton-Dyer, A Brief Guide to Algebraic Number Theory, Cambridge U. Press, Cambridge 2001.

• Juergen Neukirch, Algebraic Number Theory, Engl. transl. Norbert Schappacher, Springer, Berlin, 1986.

Both assume you know some Galois theory or at least can fake it. Neukirch's book is good for the all-important analogy between Galois groups and fundamental groups, which I haven't even touched upon here! Swinnerton-Dyer's book has the virtue of brevity, so you can see the forest for the trees. Both have a friendly, slightly chatty style that I like.

For Shafarevich's conjecture, try this:

• Iwasawa, On solvable extensions of algebraic number fields, Ann. Math. 58 (1953) 548–572.

For Deligne's motivic analogue, try this:

• Pierre Deligne, Le groupe fondamental de la droite projective moins trois points, in Galois Groups over $\mathbb{Q}$, MSRI Publications 16 (1989), 79–313.

This stuff has a lot of relationships to 3d topological quantum field theory, braided monoidal categories, and the like ... and it all goes back to the Grothendieck-Teichmüller group. To learn about this group try this book, and especially this article in it:

• Leila Schneps, The Grothendieck-Teichmüller group: a survey, in *The Grothendieck Theory of Dessins D'Enfants*, London Math. Society Notes 200, Cambridge U. Press, Cambridge 1994, pp. 183–204.

To hear and watch some online lectures on this material, try:

• Leila Schneps, The Grothendieck-Teichmüller group and fundamental groups of moduli spaces, MSRI lecture available at
`http://www.msri.org/publications/ln/msri/1999/vonneumann/schneps/1/`
Grothendieck-Teichmüller group and Hopf algebras, MSRI lecture available at
`http://www.msri.org/publications/ln/msri/1999/vonneumann/schneps/2/`

For a quick romp through many mindblowing ideas which touches on this material near the end:

• Pierre Cartier, A mad day's work: from Grothendieck to Connes and Kontsevich – the evolution of concepts of space and symmetry, Bulletin of the AMS, 38 (2001), 389–408. Also available at `http://www.ams.org/joursearch/index.html`

For even more mindblowing ideas along these lines:

• Jack Morava, The motivic Thom isomorphism, talk at the Newton Institute, December 2002, also available at `math.AT/0306151`

Quote of the week:

"Paris, 1 June – A deplorable duel yesterday has deprived the exact sciences of a young man who gave the highest expectations, but whose celebrated precosity was lately overshadowed by his political activities. The young Evariste Galois ... was fighting with one of his old friends, a young man like himself, like himself a member of the Society of Friends of the People, and who was known to have figured equally in a political trial. It is said that love was the cause of the combat. The pistol was the chosen weapon of the adversaries, but because of their old friendship they could not bear to look at one another and left their decision to blind fate."
Le Precursor, June 4 1832