Number Theory II: What is an algebraic number and why should I care?

Kiran Kedlaya
Berkeley Math Circle, December 10, 2000

1 Basic facts

I'll answer half of the title question immediately. For the purposes of this talk, an *algebraic number* is a complex number which is the root of a polynomial with integer coefficients. An *algebraic integer* is an algebraic number which is the root of a monic polynomial with integer coefficients.

I'll say more about why you should care later. For now, let me just give a bunch of examples to convince you that algebraic numbers crop up all over the place.

- A rational number is an algebraic number; a rational number is an algebraic integer if and only if it is an integer. For clarity, I'll refer to the usual integers as the *rational integers*.
- For any rational number p/q, the root of unity $e^{2\pi ip/q}$ satisfies the polynomial $x^q - 1 = 0$, and so is an algebraic integer.
- A *Gaussian integer*, a number of the form $a + bi$, is an algebraic integer.
- For any rational number p/q, the numbers $\cos(2\pi p/q)$ and $\sin(2\pi p/q)$ are algebraic integers, and $\tan(2\pi p/q)$ is an algebraic number. Can you explicitly write down polynomials that these are roots of? (These polynomials turn out to have lots of interesting properties.)
- Given a recurrence relation $x_{n+k} = a_1 x_{n+k-1} + \cdots + a_k x_n$ with (rational) integer coefficients, all solutions can be expressed in terms of some algebraic integers. For example, the n-th Fibonacci number can be written as
$$\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{-5}}{2}\right)^n - \left(\frac{1-\sqrt{-5}}{2}\right)^n\right].$$
- The eigenvalues of a matrix with (rational) integer entries are algebraic integers. This is one way algebraic numbers come up in topology, group theory, algebraic geometry, combinatorics, etc.

Here are some basic facts about algebraic numbers. These may not be obvious at first; I'll mention two ways to prove them in a moment.

1. The set of algebraic numbers is closed under addition, subtraction, multiplication and division. The set of algebraic integers is closed under addition, subtraction and multiplication, but not division.

2. The root of a polynomial whose coefficients are algebraic numbers (resp., algebraic integers) is one also.

The first method involves symmetric polynomials, which are interesting enough in their own right that I'll discuss them in some detail.

Theorem 1. *Let P be a symmetric polynomial (with integer coefficients) in $x_1, \ldots, x_n$. Then P can be expressed as a polynomial (with integer coefficients) in the elementary symmetric functions $\sigma_1, \ldots, \sigma_n$ given by*

$$t^n + \sigma_1 t^{n-1} + \cdots + \sigma_n = (t + x_1) \cdots (t + x_n).$$

For example, $\sigma_1 = x_1 + \cdots + x_n$, $\sigma_2 = \sum_{i<j} x_i x_j$, and so on.

The proof of this is a successive elimination argument of a form quite common in computational algebraic geometry. It's related to something called a "Gröbner basis".

Proof. The idea is to deal with the terms of P "from the outside in". That is, we first deal with terms which are as "unbalanced" as possible.

We can write

$$P = \sum_{a_1 \geq \cdots \geq a_n} \sum_{\text{sym}} c_{a_1,\ldots,a_n} x_1^{a_1} \cdots x_n^{a_n}.$$

We put an ordering on n-tuples by saying that $(a_1, \ldots, a_n) > (b_1, \ldots, b_n)$ if and only if $na_1 + (n-1)a_2 + \cdots + a_n > nb_1 + (n-1)b_2 + \cdots + b_n$. Now sort the terms in decreasing order by $na_1 + (n-1)a_2 + \cdots + a_n$. Choose the biggest term $(a_1, \ldots, a_n)$ and notice that the polynomial

$$\sigma_1^{a_1 - a_2} \cdots \sigma_{n-1}^{a_{n-1} - a_n} \sigma_n^{a_n}$$

has the same largest term, and the coefficient of that term is 1. So subtract off $c_{a_1,\ldots,a_n}$ times this product, and repeat. □

I'll demonstrate why this is a useful fact by showing that the product of two algebraic integers is an algebraic integer. Given two algebraic integers which are the roots of the monic polynomials P and Q with rational integer coefficients, let $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n$ be the roots of P and Q, respectively. Now consider the polynomial

$$\prod_{i=1}^{m} \prod_{j=1}^{n} (x - \alpha_i \beta_j).$$

Now $\prod_{j=1}^{n} (x - \alpha_i \beta_j)$ can be viewed as a symmetric polynomial in $\beta_1, \ldots, \beta_n$, if I treat x and α_i as constant. (More precisely, if I look at all terms with a fixed power of x and α_i, these together form a symmetric polynomial in the β_i). By the theorem, this polynomial is a polynomial in the elementary symmetric functions of the β_i, which by assumption are integers. So we now have a polynomial in x and α_i with integer coefficients; we now take the product over the α_i and repeat the argument.

The second, more modern method, uses some linear algebra. The main idea is that α is an algebraic number if and only if $1, \alpha, \alpha^2, \ldots$ lie in a finite dimensional vector space over $\mathbb{Q}$. So to show that $\alpha\beta$ is algebraic given that α and β are, suppose α satisfies a polynomial of degree m and β satisfies a polynomial of degree n over $\mathbb{Q}$. Then all of the products $\alpha^i\beta^j$ lie in the vector space spanned by $\alpha^k\beta^l$ for $k < m, l < n$. In particular, all of the $(\alpha\beta)^i$ lie in a finite dimensional vector space, so $\alpha\beta$ is algebraic.

2 Unique and nonunique factorization

It's easier to study algebraic numbers as part of a larger structure than on their own. So we define a *number field* to be the smallest set containing $\mathbb{Q}$ plus some finite set $\alpha_1, \ldots, \alpha_n$ of algebraic numbers, which is also closed under addition, subtraction, multiplication and division. We'll usually denote this number field $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$. We define a *ring of integers* to be the set of algebraic integers in a number field.

WARNING: it's not always obvious what the ring of integers in a number field is. Take the example $\mathbb{Q}(\sqrt{D})$ (D positive or negative). If $D \equiv 1 \pmod 4$, then $(1 + \sqrt{-D})/2$ is an algebraic integer; more generally, the integers in the number field are $(a + b\sqrt{-D})/2$ for a, b rational integers of the same parity. If $D \equiv 2, 3 \pmod 4$, then the only integers in the number field are the obvious ones $a + b\sqrt{-D}$ for a, b rational integers.

One nice property about the rational integers is unique factorization. Is unique factorization true for other rings of integers? Sometimes yes, sometimes no.

To make that precise, we'll need some more definitions. define a *unit* to be an algebraic integer whose reciprocal is also an algebraic integer. (For example, roots of unity are units, but there are other units too; we'll see some later.) We call an element α of a ring of integers *irreducible* if whenever you write $\alpha = \beta\gamma$ as the product of two elements of the ring, one of β or γ is a unit. (I didn't say "prime" because I'm saving that word for later). We say a ring of integers has *unique factorization* if whenever an element of a ring of integers is expressed as a product of irreducible elements, that expression is unique up to changing the order and multiplying by units.

For example, the Gaussian integers have unique factorization, because they admit an analogue of the Euclidean division algorithm.

Theorem 2. *Given Gaussian integers p and q with $q \neq 0$, there exist Gaussian integers r and s with $p = qr + s$ and $|s| < |q|$.*

Proof. Draw the square with vertices $0, q, iq, (1 + i)q$. Then p is congruent to a Gaussian integer z inside (or on the boundary of) the square. Also, the open discs of radius $|q|$ centered at $0, q, iq, (1 + i)q$ cover the square completely, so z is within $|q|$ of one corner of the square, say w. Now take $s = z - w$; then $|s| < |q|$ and $s \equiv p \pmod q$, so we can set $r = (p - s)/q$ and we're done. □

Corollary 1. *Every (rational) prime congruent to 1 modulo 4 is the sum of two squares; moreover, this expression is unique up to order and signs.*

Proof. If $p \equiv 1 \pmod 4$, then there exist x and y such that $x^2 + y^2$ is divisible by p but not by p^2. Apply the Euclidean algorithm in the Gaussian integers (left for you to write down!) to $x + iy$ and p; the result will be a Gaussian integer $r + si$ with $r^2 + s^2 = p$. Uniqueness is also left to you. □

EXERCISE: Find some other rings of integers which have unique factorization. (For starters, try $\mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[(1 + \sqrt{-3})/2]$.

On the other hand, consider this example in $\mathbb{Z}[\sqrt{-5}]$:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

None of 2, 3, or $1 \pm \sqrt{-5}$ can be written as a nontrivial product of two elements of $\mathbb{Z}[\sqrt{-5}]$, so this ring doesn't have unique factorization. What to do?

Kummer realized that one could find an algebraic integer in a bigger ring that would allow you to break up such problem factorizations. (For example, if we toss in $\sqrt{2}$, then it divides both $1 + \sqrt{-5}$ and 2.) However, it turns out that it's a little better to work not with these "ideal numbers", as Kummer called them, but with the collection of their multiples.

Definition: an *ideal* in a ring of integers R is a subset S such that

1. for $x, y \in S$, $x + y \in S$;
2. if $x \in S$ and $r \in r$, then $xr \in S$.

Example: If $R = \mathbb{Z}$, then an ideal is an arithmetic progression containing 0. More general example: the *principal ideal* generated by $r \in R$ consists of all multiples of r. But not all ideals have this form!

Because of the way an ideal is defined, we can work "modulo" an ideal, that is, it makes sense to write $a \equiv b \pmod I$ because this equivalence respects addition and multiplication. If I is nonzero, then the number of equivalence classes modulo I is finite; we call this number the *norm* of the ideal.

An ideal I is *prime* if $xy \in I$ implies $x \in I$ or $y \in I$. For example, if $R = \mathbb{Z}$ and $I = (n)$, then I is prime if and only if n is prime. In general, if I has prime norm, it is a prime ideal, but the converse is not true; we only know that I has prime power norm. For example, the ideal (3) in $\mathbb{Z}[i]$ is prime, but its norm is 9.

The arithmetic on $\mathbb{Z}[i]/(3)$ is not the same as on $\mathbb{Z}/(9)$, though! The main distinction is that in $\mathbb{Z}[i]/(3)$, everything not congruent to 0 mod (3) has a multiplicative inverse. (Thus $\mathbb{Z}[i]/(3)$ is an example of a *finite field*.)

The big theorem about prime ideals is the recovery of unique factorization.

Theorem 3. *Every nonzero ideal in a ring of integers has a unique prime factorization.*

Corollary 2. *If every ideal of a ring of integers R is principal, then R has unique factorization. (Note: the converse is also true.)*

Two ideals I and J in the ring of integers R of a number field K are *equivalent* if there exists $k \in K$ such that $kI = J$. (Note that k need not lie in R. If you prefer a definition within R: I and J are equivalent if there exist nonzero $i, j \in R$ such that $iI = jJ$.) This equivalence is respected by multiplication.

Theorem 4 (Minkowski). *The number of equivalence classes of ideals in a ring of integers is finite.*

This number is called the *class number* of the number field.

Theorem 5 (Gauss). *For $n > 3$ not divisible by 4, the number of primitive (having no common factor) triples (x, y, z) of integers such that $x^2 + y^2 + z^2 = n$ is equal to 12 times the class number of $\mathbb{Q}(\sqrt{-n})$ if $n \equiv 1, 2 \pmod 4$, or 24 times the class number of $\mathbb{Q}(\sqrt{-n})$ if $n \equiv 3 \pmod 4$.*

Note: Gauss didn't express this theorem in terms of number fields, but in terms of binary quadratic forms $ax^2+bxy+cy^2$ whose discriminant b^2-4ac equals $-4n$, if $n \equiv 1, 2 \pmod 4$, or $-n$, if $n \equiv 3 \pmod 4$. Two forms are equivalent if you can get from one to the other by making a variable substitution of the form $u = px + qy, v = rx + sy$ where p, q, r, s are integers with $ps - qr = 1$.

EXERCISE: Prove that the number of equivalence classes of forms equals the class number of $\mathbb{Q}(\sqrt{-n})$.

3 Diophantine equations

One important use of algebraic numbers is to answer questions about Diophantine equations. We have already seen one example of this (representing an integer as the sum of two squares); let's consider a few more examples.

The equation $x^2 - Dy^2 = 1$ is (mis)named "Pell's equation". Over $\mathbb{Q}(\sqrt{-D})$, we can factor the left side and rewrite the equation as

$$(x + y\sqrt{D})(x - y\sqrt{D}) = 1.$$

This makes clear the multiplicative structure of the set of solutions: if (a, b) and (c, d) are solutions, then

$$\begin{aligned} 1 &= (a + b\sqrt{D})(c + d\sqrt{D})(a - b\sqrt{D})(c - d\sqrt{D}) \\ &= [(ac + bdD) + (ad + bc)\sqrt{D}][(ac + bdD) - (ad + bc)\sqrt{D}] \\ &= (ac + bdD)^2 - D(ad + bc)^2. \end{aligned}$$

Moreover, we can sort all solutions into increasing order by $x + y\sqrt{D}$ (which is an increasing function of x for $x \geq 0$, given that $x^2 - Dy^2 = 1$). Now it's easy to see that all solutions in positive integers are "powers" of the smallest solution, assuming that any solutions exist.

There are several ways to show that solutions exist. One method uses continued fractions and has been known at least for 1000 years (it occurs in an old Indian text); it is probably the best method for explicitly computing solutions.

ASIDE: What does this have to do with algebraic numbers? What we've done is to classify the algebraic integers in the field $\mathbb{Q}(\sqrt{D})$ whose products with their conjugates equal 1. An analogous classification can be made for an arbitrary number field, which solves the Pell equation along the way.

What about the equation $x^2 - Dy^2 = n$ when $n \neq 1$? The situation is more complicated, so one needs to know a bit more to make progress. For example, given that $\mathbb{Q}(\sqrt{2})$ has unique factorization, one can prove the following. (Note the resemblance to the proof that a prime $p \equiv 1 \pmod 4$ is the sum of two squares.)

Theorem 6. *For n a squarefree integer, the equation $x^2 - 2y^2 = n$ has a solution in integers if and only if it has a solution modulo n.*

Proof. By multiplicativity, it suffices to show that $x^2 - 2y^2 = n$ has a solution for $n = -1$, $n = 2$, and $n = p$ for p an odd prime such that 2 is congruent to a square modulo p. For $n = -1$, use $1^2 - 2 \cdot 1^2 = -1$; for $n = 2$, use $2^2 - 2 \cdot 1^2 = 2$.

Now suppose p is an odd prime such that 2 is congruent to a square modulo p. Find x, y such that $x^2 - 2y^2$ is divisible by p but not by p^2 (if it is divisible by p^2, fix that by replacing x with $x + p$). Now form the ideal $(x + y\sqrt{D}, p)$. Its norm divides p^2 and $x^2 - 2y^2$, so it must be p. □

Incidentally, one can replace 2 by any integer D such that $\mathbb{Q}(\sqrt{D})$ has unique factorization, provided that $x^2 - Dy^2 = -1$ has a solution. It turns out (but is by no means obvious!) that unique factorization implies that D is prime, and it is believed (but not proved) that $\mathbb{Q}(\sqrt{D})$ has unique factorization for about 75% of the primes D. Moreover, existence of a solution of $x^2 - Dy^2 = 1$ then implies $D \equiv 1 \pmod 4$, but not every prime congruent to 1 modulo 4 will work (try $D = 5$).

For an example of a different flavor, let us find the solutions of the equation $x^2 + 2 = y^3$. In the ring $\mathbb{Z}[\sqrt{-2}]$, which has unique factorization, this factors as

$$(x + \sqrt{-2})(x - \sqrt{-2}) = y^3.$$

Note that x must be odd: if x were even, then $x^2 + 2$ would be divisible by 2 but not by 4, so could not be a perfect cube. Therefore the ideals $(x + \sqrt{-2})$ and $(x - \sqrt{-2})$ are relatively prime, and each must be the cube of an ideal. That is, $x + \sqrt{-2}$ and $x - \sqrt{-2}$ are equal to a unit (which can only be ± 1) times a a cube. In particular, we have

$$x + \sqrt{-2} = (a + b\sqrt{-2})^3 = (a^3 - 6ab^2) + (3a^2b - 2b^3)\sqrt{-2}.$$

In particular, $3a^2b - b^3 = 1$. Since this is a multiple of b, we must have $b = \pm 1$. If $b = 1$, then $3a^2 - 2 = 1$, so $a = 1$ and $x = 5$. If $b = -1$, then $-3a^2 + 2 = 1$, which is impossible.

ASIDE: We didn't actually need unique factorization: the argument still would go through if we just knew that the number field had class number not divisible by 3.

Additional examples:

1. One can prove the law of quadratic reciprocity by working with number fields containing roots of unity. (Quadratic reciprocity will be described in Oaz's talk.)

2. Lamé gave a proof of Fermat's Last Theorem for p-th powers assuming that the number field $\mathbb{Q}(e^{2\pi i/p})$ has unique factorization. Unfortunately, this only holds for finitely many primes p. Fortunately, Kummer gave a proof that also works if the class number of $\mathbb{Q}(e^{2\pi i/p})$ is not divisible by p. Unfortunately, no one has proved that there are infinitely many such p. Fortunately, numerical evidence and heuristics suggest that about 60% of primes have this property. (More fortunately, Fermat's Last Theorem has now been proved by Wiles et al.)

4 Read all about it!

There are tons of books on algebraic number theory out there (some of which don't assume very much from classical number theory). Some titles that come to mind (with commentary):

- Esmonde and Murty, *Problems in Algebraic Number Theory* (beware of the many small errors, hopefully to be corrected in a future edition)
- Ireland and Rosen, *A Classical Introduction to Modern Number Theory* (a pretty good read, I'm told)
- Lang, *Algebraic Number Theory* (not an easy read, assumes undergraduate algebra)
- Marcus, *Number Fields* (mostly does examples)
- Neukirch, *Algebraic Number Theory* (not to be confused with his other books, which are very difficult reading)
- Pollard and Diamond, *The Theory of Algebraic Numbers* (the avoidance of abstract algebra makes this an easy read but obscures certain points)