Introduction

Dinesh S. Thakur

We will begin with an explanation of some of the original motivations for the study of cyclotomic fields and lay out the plan for this workshop. Many concepts just mentioned here will get explained in detail later.

In school and college, starting from (the set of) counting numbers $\mathbf{N}$, we are led successively first to $\mathbf{Z}$, $\mathbf{Q}$ by the need of solving equations involving simple additions and multiplications, then to $\mathbf{R}$ by looking at lengths or using limit operations, infinite sums etc.. Finally we are taught the magic of the passage from $\mathbf{R}$ to $\mathbf{C}$, where by forcing or decreeing a solution i to one equation $x^2 + 1 = 0$, we can solve all the polynomial equations. This is the so-called Fundamental theorem of algebra.

On the other hand, if starting from $\mathbf{N}$, we allow only algebraic operations (additions and multiplications) and hence the polynomial equations, but not the infinite or limiting processes, then we are led to (the set of) algebraic numbers $\overline{\mathbf{Q}}$. The countable (thus of measure zero) set $\overline{\mathbf{Q}}$ is much smaller than $\mathbf{C}$.

Historically, the slow emergence of the algebraic numbers had at least three different motivating sources: (1) Basic number theory study of Diophantine equations (basically polynomial equations with integral coefficients, where we also limit ourselves to integral solutions) such as Fermat equation $x^n + y^n = z^n$, arising as a natural generalization of Pythagoras equation for the right-angled triangle sides, (2) Basic geometry study of 'cyclotomy' which means division of a circle, i.e., attempt of constructing regular polygons (by ruler and compass), (3) Study of representation of integers by quadratic forms with integral coefficients (linear forms are easy: representable numbers are the multiples of GCD of coefficients i.e, $\mathbf{Z}$ is a PID) and resulting emergence of 'reciprocity' laws.

Most of you know how to solve Pythagoras equation $x^2 + y^2 = z^2$ in integers, though some of you may have only seen its rational (i.e., dehomogenized) version (i.e., $a^2+b^2 = 1$ in rationals) as a $t = \tan(\theta/2)$ substitution in calculus which turns integrand involving rational functions of trigonometric functions of θ into one involving rational functions of t. (By school geometry, the straight line joining the point $(-1, 0)$ to the point (a, b), with polar co-ordinates $(1, \theta)$, on the unit circle around origin has slope $t = \tan(\theta/2)$. Solving $b = (a + 1)t$, $a^2 + b^2 = 1$, we get $t^2/1 = (1 - a^2)/(a + 1)^2$. Thus

$(1-t^2)/(1+t^2) = \cdots = a$ and $b = 2t/(1+t^2)$).

The usual algebra method is to reduce without loss of generality (by getting rid of common factors and by parity considerations) to $x^2 = z^2 - y^2 = (z+y)(z-y)$ where x, y, z are relatively prime, with x even and y, z odd. Then the unique factorization into primes implies that apart from the GCD, which is 2, both the factors are squares: $z+y = 2p^2$, $z-y = 2q^2$. Thus we are lead to the parametric solution $(x, y, z) = (2pq, p^2-q^2, p^2+q^2)$.

Fermat used this to show that there are no non-trivial integral solutions to $x^4 + y^4 = z^4$ (I will leave out easy GCD and parity considerations): By above, a nontrivial solution $x^4+y^4 = w^2$ leads to $x^2 = 2pq$, $y^2 = p^2-q^2$ and $w = p^2+q^2$. Now $y^2+q^2 = p^2$ again gives $q = 2ab$, $y = a^2-b^2$ and $p = a^2+b^2$. Thus, $x^2 = 2pq = 4ab(a^2+b^2)$ implies by unique factorization that $a = X^2$, $b = Y^2$ and $a^2+b^2 = W^2$, thus leading to a 'smaller' solution $X^4+Y^4 = W^2$ leading to an infinite descent of positive integers, a contradiction.

Hence, the natural attempt (tried by Euler, Cauchy, Kummer etc. and successful in some special cases, but not in general) to attack the general Fermat equation $x^n + y^n = z^n$ was to try infinite descent by using factorization $x^n + y^n = z^n = \prod(x + \zeta_n^i y)$ into 'cyclotomic' integers. Here n is odd and ζ_n is a primitive n-th root of unity, e.g., $\zeta_n = e^{2\pi i/n}$. If (there is the catch) the unique factorization held for these cyclotomic integers, then apart from small GCD, each factor would be n-th power and we may try manipulations as above to get an infinite descent. Soon, once we develop these ideas a little, we will go through the proof for $n = 3$. Later, once we develop the cyclotomic machinery, we will explain Kummer's successful attempt under the condition of 'regularity', which is weaker than unique factorization condition.

As other examples, we may want to attempt solving $x^3 = y^2 + 1$ in integers by factoring the right side as $(y+i)(y-i)$ into 'Gaussian integers'. (Exercise: Do this, assuming unique factorization into Gaussian integers $a + ib$ ($a, b \in \mathbf{Z}$ and go through rigorous details once more after we develop Gaussian integers). Try the same for $x^2 = y^2 + 5 = (y + \sqrt{-5})(y - \sqrt{-5})$ and you would see it would fail: the 'integer system' $a + b\sqrt{-5}$ does not have unique factorization. Of course, this is a wrong attempt and you should have tried $5 = x^2 - y^2 = (x+y)(x-y)$ instead to conclude $x = \pm 3$).

This shows that we need careful study of generalizations of concepts such as 'rational numbers', 'integers', 'primes' etc. As we see above, given a polynomial with integral coefficients, we needed to forcefully factor it by using generalized numbers: So algebraic numbers are just solutions of (non-trivial) polynomials with integral coefficients. (Easy theorem then is that $\overline{\mathbf{Q}}$: $\{$algebraic numbers$\}$ is algebraically closed, i.e., polynomial with algebraic coefficients have all roots algebraic).

What should be the algebraic integers? Those are the solutions of monic polynomials with integral coefficients: This fits with the degree one case. Another way to see why this is what we want is as follows: Want the set of algebraic integers to be closed under sums, products and conjugation (as all conjugates look the same from $\mathbf{Q}$ point of view) and hence the elementary symmetric functions of the roots, which are the coefficients of the minimal (monic) polynomial should have algebraic as well as rational and hence integral coefficients.

But, at least for the diophantine equations applications, we do not want to look at full $\overline{\mathbf{Q}}$ at once, otherwise we will have too much factorization such as $5 = (5^{1/2})^2 = (5^{1/4})^4$ and so on. So we adjoin only finitely many (which will turn out to be the same as one) algebraic numbers to $\mathbf{Q}$ at a time to get so-called number fields. Examples are $\mathbf{Q}$, $\mathbf{Q}(i)$, $\mathbf{Q}(\sqrt{-5})$, $\mathbf{Q}(\zeta_n)$ associated to equations above. If we write K for a number field, the ring of algebraic integers in it will be denoted by $\mathcal{O}_K$. We will see soon that in $\mathbf{Q}(\sqrt{-5})$, the failure of unique factorization is illustrated by $6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

Historically, there were three different (but basically the same at the end) ways to get back unique factorizations after modifying the concepts a little: 'Ideals' of Dedekind, 'ideal complex numbers' of Kummer and 'divisors' of Kronecker. We will use the ideals: The basic idea is that unique factorization fails because something is missing in the system of these generalized integers: For example, if instead of natural numbers, we just take those of the form $4n+1$, then $21\times 21 = 9\times 49$ is failure of unique factorization, which is restored once we add (missing) 3 and 7 in the system. When we are interested in divisibility questions, an algebraic integer enters the picture via the set of its integral multiples, so we introduce ideals which are sets of integral linear combinations of several algebraic integers (rather than just one). In other words, the set of multiples of 'something' should be closed under addition and multiplication by algebraic integers, so that ideals are such sets, i.e., $\mathcal{O}_K$ submodules of $\mathcal{O}_K$. Similarly, $\mathcal{O}_K$ submodules of K are called fractional (with the word 'fractional' being dropped sometimes, if clear from context) ideals.

We will learn basic operations on ideals and see that they have unique factorization property. But we were originally interested in algebraic numbers. So we have to study what we loose in the passage: An ideal generated by a single number is called a principal ideal and (group of non-zero fractional) ideals modulo the principal ones is called the class group. It will turn out to be finite. The numbers which are multiples of each other (i.e., they differ by 'units') give rise to the same principal ideal. The unit group will turn out to be finitely generated. So in some sense, what we loose is manageable.

So our goal in the *Dedekind domains* series in the first week is to study these notions of integers, ideals, factorizations of ideals, the structure theorems for the class group and unit group etc. This set-up is good for strong number field, function field analogies (they are thus studied together as global fields), which we will see (in the third week of the Summer School) are very useful in '*Iwasawa theory*', a theory developed by Iwasawa to study a number field (i.e., a finite extension of $\mathbf{Q}$) by studying a tower of its extensions via analytic and Galois theoretic tools.

The prototype of the *Galois theory* and cyclotomic theory was also developed by Gauss in his attempt to solve the second motivating problem: By ruler and compass we get lines (linear equations) and circles (quadratic equations) and their successive intersection points. Successive degree 2 extensions lead to degree 2^k extensions of $\mathbf{Q}$. Construction of a regular n-gon corresponds basically to $e^{2\pi i/n}$ whose minimal polynomial has degree $\phi(n)$. Also, $\phi(n) = 2^k$ easily implies $n = 2^r$ times product of distinct Fermat primes, i.e., the primes of the form $2^{2^s}+1$. So the construction is impossible for n not of this form. On the other hand to show the construction is possible for such n, we have to have good control on subfield structure of $\mathbf{Q}(\zeta_n)$ to realize it by successive ruler and compass construction. This is where Gauss developed Galois and cyclotomic theory he needed in this context. We will give some details later.

To understand how the usual integers factor into ideals in a number field, we need to understand how the usual primes factor into prime ideals in number fields. We will see that such prime decomposition laws are quite simple in cyclotomic fields, but not in general. The deeper reason behind this will turn out to be that the Galois groups of the cyclotomic fields are abelian (i.e., commutative). We will prove famous *Kronecker-Weber theorem* which says that any finite abelian extension of $\mathbf{Q}$ is contained in some $\mathbf{Q}(\zeta_n)$. So the study of cyclotomic extensions (which by definition are subfields of the basic cyclotomic extensions $\mathbf{Q}(\zeta_n)$ is the study of finite abelian extensions of $\mathbf{Q}$. Replacing the base $\mathbf{Q}$ by a number field leads to a neat generalization called *Class field theory.* We will only state and illustrate the main theorems.

We will then prove Kummer's results on *Fermat's last theorem* by using cyclotomic and *Kummer theory.* Here we already go a little beyond abelian theory. After extensive work by several mathematicians, the Fermat's last theorem was finally proved by Wiles (and Taylor) by going still further in handling number fields with non-abelian Galois groups. We will be content with showing historical continuity for motivation, central ideas, themes and some techniques.

Two important, but hard to compute, structures are class group and unit group. We will see that special values of simply defined analytic functions, called *zeta and L-functions*, reveal a lot of information on them. Concurrently with the Dedekind domains series, we will also have example oriented series on *quadratic and cyclotomic fields* to illustrate the theory and to build up an example base. We will see the importance in cyclotomic theory of index 2 and of degree 2 (quadratic) sub-extensions of the basic cyclotomic fields.

We said that we would deal with $\mathbf{Q}(\zeta_n)$ rather than $\overline{\mathbf{Q}}$ to deal with the n-th Fermat equation, but it turns out that we need to take further extensions, such as *Kummer extensions*, which are obtained by adjoining a n-th root of some number in a number field already containing ζ_n. We also motivated $\overline{\mathbf{Q}}$ by saying that in number theory we do not want analytic operations. But the truth is that we use all the tools we can get even to study rational or algebraic numbers and so we use not only $\mathbf{R}$, which is the completion of $\mathbf{Q}$ for the usual absolute values, but we study all possible *absolute values and completions*. These concepts of p-adic sizes and completions form a 'local' approach and then we also briefly study *local-global principles* such as *Hasse theorem* for quadratic forms.

Even at the school level, we study some analogies between integers and rational numbers on one hand and polynomials and rational functions on the other. These analogies are even better, more useful and deep when we only allow coefficients from a finite field to our rational functions. This, for example, forces only finitely many remainders (residue classes) when we divide, just as in the integer case. Again the basic Dedekind domains theory and zeta and L-functions can be developed. One of the main unsolved problems in number theory is Riemann hypothesis, whose function field analog, due to Artin, was proved by Weil. As we will see, Iwasawa theory got started when Iwasawa attempted to carry over the successful tools in function fields to number field case.

Apart from the size and group structure of the class group, the relations (called *Stickelberger relations*) with respect to Galois action on it also encode a lot of useful arithmetic information. They will be proved by studying the ideal factorization of the *Gauss and Jacobi sums.*

As for the third motivating question, Fermat, Euler and many other mathematicians played with the questions such as which natural numbers are of the form $x^2 + y^2$ or $x^2 + 5y^2$ etc. Factoring, as before, in $\mathbf{Q}(i)$ or $\mathbf{Q}(\sqrt{-5})$, this relates to the question of which numbers are norms (basically products of conjugates) from those number fields. Because of the multiplicativity of norms, it quickly reduces to the question of which primes are thus representable. If a prime p is $x^2 + y^2$, then $x^2 \equiv -1$ modulo p. This leads to the question when -1 is a square modulo p (for a given p, this is easy to check, but we want to characterize all such p's: they are primes of the form $4n + 1$ and 2) or more generally for which primes a given number is a quadratic residue. Playing with many examples, Euler quickly found, for example, that if p and q are primes of the form $4n+1$, then p is a square modulo q if and only if q is a square modulo p. This is an instance of quadratic reciprocity, which was generalized to any contexts such as *Power reciprocity* laws. We will see many proofs, most natural ones occuring in factorization laws. We will also give proofs of these using Gauss-Jacobi sums.

We have tried here to give a quick plan. It will make more sense as we go along and master the terminology through the lectures and more importantly, through the problem sessions and discussions.

Dinesh Thakur
Department of Mathematics
University of Arizona
Tucson, AZ 85721
USA
e-mail: thakur@math.arizona.edu