Basic definitions, and the irreducibility of the cyclotomic polynomials

November 24, 2013

In this class we're studying cyclotomic fields. For this first lecture, I just want to introduce you to the basic objects. So it'll be mostly definitions, plus a little bit of playing around. This will also give you a chance to refresh your memory on field theory. In the end we'll state and prove one real theorem, the "irreducibility of the cyclotomic polynomial". We'll give one proof in this lecture, and another in the next. Both will introduce characters and constructions which will be important for the future. (The future of our study of cyclotomic fields, at least.)

So, let's get going on those definitions. Recall that a field is a set F equipped with two binary operations $+$ and $\cdot$ which satisfy the usual rules of algebra (including being able to divide by nonzero elements of F). Primary examples: the field $\mathbb{Q}$ of rational numbers, the field $\mathbb{C}$ of complex numbers, and the finite fields $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ of integers (mod p), where p is a prime number.

Now, a *cyclotomic field* is a field generated over $\mathbb{Q}$ by some root of unity. We can think of these fields "abstractly", or imagine them sitting inside some fixed algebraic closure $\overline{\mathbb{Q}}$. For extra concreteness we could even take $\overline{\mathbb{Q}}$ to be the algebraic numbers, a subfield of $\mathbb{C}$.

Before diving into the study of these cyclotomic fields, it's probably good to step back and start by studying roots of unity in general.

Definition 0.1. *Let F be a field. A* root of unity *in F is an element $z \in F$ which satisfies $z^n = 1$ for some $n \in \mathbb{N}$.*

To be more precise, when $z^n = 1$ we call z an n^{th} *root of unity*. The set of n^{th} roots of unity (in a given field F) will be denoted $\{z^n = 1\}$. Now, the first remark to make is that the set $\{z^n = 1\}$ of n^{th} roots of unity is a group under multiplication. More precisely, it's a subgroup of $F^\times$, the nonzero elements of F under multiplication. This is me pausing while you check that. OK, now we're mostly interested in the case where $F = \overline{\mathbb{Q}}$. There the main claim about this group $\{z^n = 1\}$ is the following:

Proposition 0.2. *Let n be a natural number. The group $\{z^n = 1\}$ of n^{th} roots of unity in $\overline{\mathbb{Q}}$ is cyclic of order n.*

Concretely, what this means is that there exists an n^{th} root of unity, such that its k^{th} powers for $0 \leq k < n$ are distinct and give all the n^{th} roots of unity.

We'll give two truly different proofs of this proposition. Actually we'll often try to give multiple proofs in this class. Number theory has this strange quality where things seem to be true for many different reasons. This is especially the case for the interesting things.

Proof. The first proof is an abstract one. (It works even if $\overline{\mathbb{Q}}$ is replaced by any field which is separably closed and whose characteristic does not divide n.) It relies on the following lemma:

Lemma: For any field F, any finite subgroup of $F^\times$ is cyclic.

This lemma is really the crux of the matter, but we won't give a proof. It would be good to look at the one in Serre's *A Course in Arithmetic*. It's on page 4 and it's not long. It uses a counting argument to show that a generator has to exist, without specifying one explicitly.

Anyway, what the lemma says for us is that we only need to check that the set $\{z^n = 1\}$ has cardinality n. But, $\{z^n = 1\}$ is the set of roots of the polynomial $p(X) = X^n - 1$ of degree n. Thus, since $\overline{\mathbb{Q}}$ is algebraically closed, p will have exactly n roots provided that it is separable. Recalling the differential criterion for separability, we need to check that $p'(z) \neq 0$ whenever $p(z) = 0$, i.e. whenever $z^n = 1$. This is clear from the calculation $p'(X) = n \cdot X^{n-1}$. □

Proof. For the second proof, we take $\overline{\mathbb{Q}} \subset \mathbb{C}$. Thus we reduce to showing that the group of n^{th} roots of unity in $\mathbb{C}$ is cyclic of order n. (These roots will automatically lie in $\overline{\mathbb{Q}}$ because $z^n = 1$ is a polynomial equation.) Now, what's special about $\mathbb{C}$ is that we can represent its elements by points in the plane. For purposes of addition, it's best to use cartesian coordinates (x, y); but for purposes of multiplication — such as concerns roots of unity — it's better to use polar coordinates (r, θ).

In polar coordinates, the equation $z^n = 1$ corresponds to the pair of equations $r^n = 1$, $n \cdot \theta = 0$. The first equation has exactly one solution, $r = 1$ (roots of unity in $\mathbb{R}$ are easy; positive roots of unity in $\mathbb{R}$ are even easier!). The second equation has exactly n solutions, namely $\theta \in 2\pi \cdot \{0, \frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}\}$.

Conclusion: our group of n^{th} roots of unity $\{z^n = 1\}$ is cyclic of order n, and is in fact generated by the complex number with polar coordinates $(1, \frac{2\pi}{n})$. □

A fancier way of saying this is that the complex exponential map induces an isomorphism of abelian groups $exp : \mathbb{C}/2\pi i\mathbb{Z} \xrightarrow{\sim} \mathbb{C}^\times$, which thus restricts to an isomorphism on the n-torsion points of these respective groups. Pictorially, what we end up with is a description of the n^{th} roots of unity as the vertices of a regular n-gon centered at the origin, rotated so that one of the vertices is at $1 \in \mathbb{C}$.

A generator of $\{z^n = 1\}$ is called a *primitive n^{th} root of unity*. So the proposition we just proved says that primitive n^{th} roots of unity exist. Usually, we will denote a choice of primitive n^{th} root of unity by ζ_n. The second proof even gives a canonical choice, so we could be definitive and say that $\zeta_n = exp(2\pi i/n)$.

This raises an interesting point, though. The second proof produced this canonical choice of ζ_n, but it did so by embedding our algebraic field $\overline{\mathbb{Q}}$ into a field $\mathbb{C}$ which carries geometry/analysis. Though roots of unity are algebraic objects, the construction of this particular ζ_n was not algebraic. In fact there is no canonical algebraic way of specifying a primitive n^{th} root of unity — all of the choices are algebraically indistinguishable. We will make this precise and prove it at the end of this lecture: it's the Galois-theoretic reformulation of the irreducibility of the cyclotomic polynomials.

By the way, how many choices of ζ_n are there? That is, how many generators are there for this group $\{z^n = 1\}$? Well, this is a question in the language of group theory, so it will be invariant under isomorphism, meaning the answer will be the same for this cyclic group of order n as for any cyclic group of order n. In particular it will be the same as for $\mathbb{Z}/n\mathbb{Z}$, where the answer is $\phi(n)$, the number of integers $0 \leq k < n$ which are relatively prime to n. For example, if $n = p$ is prime, then $\phi(p) = p - 1$: excepting 1, every p^{th} root of unity is primitive.

So the picture for the n^{th} roots of unity in $\overline{\mathbb{Q}}$ is the following. There are $\phi(n)$ choices of generator for this group. Given any such choice ζ_n, every n^{th} root of unity z can be written uniquely as $z = \zeta_n^k$ for some $0 \leq k < n$. When k is relatively prime to n, we get exactly the primitive n^{th} roots of unity. In general, z will still be a primitive d^{th} root of unity for some uniquely determined $d|n$, namely d is the order of the subgroup generated by z.

Using these concepts we can refine our definition of cyclotomic fields.

Definition 0.3. *Let $n \in \mathbb{N}$. The n^{th}* cyclotomic field *is the subfield $\mathbb{Q}(\zeta_n)$ of $\overline{\mathbb{Q}}$, where ζ_n is any primitive n^{th} root of unity.*

From the above discussion it follows that the field $\mathbb{Q}(\zeta_n)$ does not depend on the choice of ζ_n, and that $\mathbb{Q}(\zeta_n)$ moreover contains the full group of n^{th} roots of unity. Furthermore, every cyclotomic field in our original sense is equal to $\mathbb{Q}(\zeta_n)$ for some n (not quite uniquely determined, as we're about to see in examples!).

Now let's do some examples. Hilbert said "Mann muß immer mit den einfachsten Beispielen anfangen". I don't agree, but out of deference to his wisdom let's do that anyway.

Example 1: When $n = 1$, there's only one n^{th} root of unity, namely $1 \in \overline{\mathbb{Q}}$. It's primitive. The 1^{st} cyclotomic field is $\mathbb{Q}(\zeta_1) = \mathbb{Q}$.

Example 2: Gee, thanks Hilbert. OK, let's move on to $n = 2$. There are 2 of them, ± 1. The primitive one is -1. The 2^{nd} cyclotomic field is.... again $\mathbb{Q}$.

Example 3: Apparently, Hilbert should've said that one must always begin with the 3rd simplest example. There are three 3^{rd} roots of unity. You can see them as the vertices of a triangle in the complex plane. The primitive ones are the two that aren't 1. Now, you might recall from trigonometry that sine and cosine of a 30 or 60 degree triangle can be written in terms of $\sqrt{3}$. So we've probably got a hope to calculate ζ_3 in terms of square roots. Actually, this is easy to do. A third root of unity satisfies $x^3 - 1 = 0$. But this equation is also satisfied by the non-primitive third root of unity, 1. To find an equation satisfied only by the primitive ones, we divide by $x - 1$. This gives

$$\frac{x^3 - 1}{x - 1} = 1 + x + x^2.$$

So the two ζ_3's are exactly the roots of this quadratic, meaning $\zeta_3 = \frac{-1 \pm \sqrt{-3}}{2}$. Thus $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$, a *quadratic field*. Something to ponder: is it a coincidence that we see the number same 3 both in ζ_3 and in $\sqrt{-3}$? Answer: No. We'll talk about this soon.

Example 4: We can similarly analyze the case $n = 4$. The fourth roots of unity are the roots of $x^4 - 1$. So, ± 1 and $\pm\sqrt{-1}$. The conclusion is that $\mathbb{Q}(\zeta_4) = \mathbb{Q}(\sqrt{-1})$. We could have also done as above: to rule out the non-primitive ± 1 (we know they're not primitive because they were already 2nd roots of unity), we divide $x^4 - 1$ by $x^2 - 1$, getting $x^2 + 1$.

Example 5: $n = 5$ is prime, so the only non-primitive fifth root of unity is 1. So, proceeding just as in the case $n = 3$, the polynomial whose roots are exactly the primitive 5th roots of unity is $(x^5 - 1)/(x - 1) = 1 + x + x^2 + x^3 + x^4$. Now, it may not be clear how to express the roots of this

polynomial in familiar terms. But in fact we'll soon see that they can be written in terms of nested square roots. The innermost square root will be $\sqrt{5}$. The upshot is that $\mathbb{Q}(\zeta_5)$ is a degree-4 extension of $\mathbb{Q}$, which contains $\mathbb{Q}(\sqrt{5})$ as a quadratic subfield.

This analysis of examples raises a number of general questions, but perhaps the most important to start with is, what is the degree of the n^{th} cyclotomic extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$? The answer is the main theorem of this lecture. It is due to Gauss.

Theorem 0.4. *Let $n \in \mathbb{N}$. The degree of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$.*

Recall that the degree of a field extension is, by definition, the dimension of the top field as a vector space over the bottom field. So the above claim is linear-algebraic: it says that the vector space generated by the powers of ζ_n over $\mathbb{Q}$ is of dimension $\phi(n)$. Note that the naive bound is $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] \leq n$, coming from the fact that ζ_n is a root of the degree-n polynomial $X^n - 1$, but actually it's not too difficult to see that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] \leq \phi(n)$, by "cutting down" the polynomial $X^n - 1$ as we did in analyzing the above examples. We'll see this more explicitly soon, but for now I just wanted to make the point that the real content in this theorem is that this last $\leq$ is in fact an $=$, i.e. the cyclotomic field $\mathbb{Q}(\zeta_n)$ is as big as it could be.

This is not something to be taken for granted: it really depends on the fact that our base field is $\mathbb{Q}$. The bound $[F(\zeta_n) : F] \leq \phi(n)$ would hold for any field, but only for certain fields is there equality. For instance, it follows from our above analysis of the case $n = 3$ that one has equality if $F = \mathbb{Q}$ or $\mathbb{Q}(\sqrt{3})$ or $\mathbb{Q}(\sqrt{7})$, but not if $F = \mathbb{Q}(\sqrt{-3})$, where the degree reduces to 1. Could this be predicted in advance? For which fields is there equality when $n = 7$?

Before proving the theorem, we'll try to get a better feel for it by giving two reinterprations. The first will be in terms of symmetry groups, and the second will be in terms of polynomials. So we'll have three ways of thinking of this theorem: the original (LinAlg), and then the two new ones (Gal) and (Poly). The equivalence of these three perspectives will also hold for a general field F instead of $\mathbb{Q}$ (though maybe F should be of characteristic not dividing n), so by giving them we still won't have done any work towards proving the above theorem, we'll just have understood the statement more deeply.

We start with the symmetry group reformulation (Gal). This is the $\mathcal{GALOIS\ PERSPECTIVE}$. I write it in script because it's a beautiful perspective, and I write it in capital letters because it's an important perspective. The Galois perspective on this theorem says that to prove the field $\mathbb{Q}(\zeta_n)$ is the right size, you just have to show that it has the right number of symmetries.

To be more precise, we consider the group of automorphisms of the field $\mathbb{Q}(\zeta_n)$, which also can be called the Galois group $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Since $\mathbb{Q}(\zeta_n)$ is generated by ζ_n, any automorphism σ is determined by what it does to ζ_n. On the other hand, the statement that ζ_n is a primitive n^{th} root of unity is a statement in the language of fields ($\zeta_n^n = 1$ but $\zeta_n^d \neq 1$ for $0 < d < n$), so it's preserved by any automorphism. What this means is that $\sigma(\zeta_n)$ must be another primitive n^{th} root of unity, i.e. it must be ζ_n^k for some uniquely determined $0 \leq k < n$ relatively prime to n.

In total, we see that associating $\sigma \mapsto k$ defines an injection from $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ to the set $\{0 \leq k < n, (k, n) = 1\}$ of size $\phi(n)$. Then the reformulation (Gal) says that this injection is actually a bijection. In other words, given any two primitive n^{th} roots of unity, we can find an automorphism of $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ which sends one to the other. This is the precise form of the "algebraic indistiguishability" of primitive n^{th} roots of unity we talked about earlier.

Actually, the above discussion, though completely correct, wasn't totally satisfactory. For instance, does this injection $\sigma \mapsto k$ depend on the choice of ζ_n? And $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is a group — what does this injection do to that structure? A good way to address both of these questions at once is to rephrase the definition of the injection as follows.

The field $\mathbb{Q}(\zeta_n)$ contains the multiplicative subgroup $\{z^n = 1\}$. So any automorphism of $\mathbb{Q}(\zeta_n)$ restricts to an automorphism of $\{z^n = 1\}$. This gives a group homomorphism $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to Aut(\{z^n = 1\})$. It's an injection because, again, $\mathbb{Q}(\zeta_n)$ is generated by n^{th} roots of unity. But what is $Aut(\{z^n = 1\})$? Well in fact, the automorphism group of any cyclic group of order n canonically identifies with $(\mathbb{Z}/n\mathbb{Z})^\times$, the units in the ring of integers (mod n). (Recall that a *unit* in a ring is an element which has a multiplicative inverse. For instance, the units of a field are the nonzero elements of the field; the units in $\mathbb{Z}/n\mathbb{Z}$ are represented by the $0 \leq k < n$ relatively prime to n.) This identification sends a $k \in (\mathbb{Z}/n\mathbb{Z})^\times$ to the automorphism $g \mapsto g^k$. The upshot is that we have an injective group homomorphism

$$Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$$

characterized by the fact that it sends σ to the k for which $\sigma(\zeta) = \zeta^k$ for any n^{th} root of unity ζ. The reformulation (Gal) of the theorem is that this map is surjective (or, an isomorphism).

Now we turn to the (Poly) reformulation. This reformulation will say that the n^{th} cyclotomic polynomial is irreducible. The n^{th} cyclotomic polynomial is the monic polynomial whose roots are exactly the primitive n^{th} roots of unity. It can be explicitly obtained by "cutting down" the polynomial $X^n - 1$ as we did in examples above, but the most convenient way to get at it is to just write it down:

$$\Phi_n(X) = \prod_{\zeta \text{ a primitive } n^{th} \text{ root of unity}} (X - \zeta).$$

This polynomial clearly has the defining property of the n^{th} cyclotomic polynomial. What may not be clear, unlike if we used the cutting down method, is that it has rational coefficients! But we can see this using Galois theory. As argued above, any field automorphism σ of $\overline{\mathbb{Q}}$ permutes the set of primitive n^{th} roots of unity. So if we apply σ to the above expression, we get the same expression back again, just the order of the factors has been permuted. So $\sigma\Phi_n(X) = \Phi_n(X)$; then, looking at the coefficients, we see that they all are fixed by σ for any σ; thus they all lie in $\mathbb{Q}$. Note that this argument does not require yet knowing that the above injection $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ is surjective! If it were not surjective, the only thing that would change is that we could further break this polynomial up into packets consisting of the different Galois orbits. So, anyway, $\Phi_n(X) \in \mathbb{Q}[X]$. In fact $\Phi_n(X) \in \mathbb{Z}[X]$; we'll probably see that later.

A good example is that when $n = p$ is a prime, $\Phi_p(X) = 1 + X + X^2 + \ldots + X^{p-1}$. This follows from the cutting down method: $\Phi_p(X)(X - 1)$ must be equal to $X^p - 1$ since they are both separable and monic and have the same roots. That's a simple argument, but it has real power: if we think of this equality $\Phi_p(X) = 1 + X + X^2 + \ldots + X^{p-1}$ in terms of the above definition of $\Phi_p(X)$, we see many nontrivial algebraic relations among the various primitive p^{th} roots of unity.

Now, finally, the (Poly) interpretation of the theorem is that $\Phi_n(X)$ is an irreducible polynomial, i.e. it can't be written as a product of two polynomials in $\mathbb{Q}[X]$ of lesser degree.

Again, the equivalence of the three interpretations (LinAlg), (Gal), (Poly) follows from general field theory. Instead of recalling the precise argument, let me just indicate how a failure of the theorem would

appear from each of the three perspectives. From the (LinAlg) perspective, it would manifest itself in a non-trivial dependence relation among fewer than $\phi(n)$ different powers of ζ_n. This corresponds, in the (Poly) perspective, to a smaller-degree polynomial satisfied by ζ_n. Such a polynomial, if taken to have minimal degree, would have to be a nontrivial divisor of $\Phi_n(X)$, by the division algorithm in $\mathbb{Q}[X]$. So we'd get a nontrivial factorization of $\Phi_n(X)$ in $\mathbb{Q}[X]$, which is how (Poly) would see the failure. But then there could never be any Galois automorphism which sends a root of one of the factors to a root of the others, because these would satisfy different algebraic relations. And that's how (Gal) would see the failure. It's also pretty easy to go backwards from (Gal) to (Poly) to (LinAlg) — or, using some "Artin tricks", to go directly between (Gal) and (LinAlg) — and that pretty much gives the equivalence.

Perhaps we've explored the statement enough that we can finally give a proof of it. But again, the proof has real content. Another measure of this is that there are in fact at least two totally different proofs. I'll call one the "p-adic" proof, and one the "ℓ-adic" proof. You don't need to take these names to have any meaning; I just want to flag how the proofs fit into bigger modern frameworks. As we'll see, the p-adic proof is most related to the (LinAlg) perspective, and the ℓ-adic proof is most related to the (Gal) perspective.

Today we'll give the p-adic proof. Actually, we'll only do the case where $n = p$ is prime. The method extends pretty easily to prime powers, and then another argument can be used to reduce from a general n to its separate prime powers. We may discuss such reduction methods later, but they're orthogonal to our discussion here.

Proof. We take the (LinAlg) perspective. So we're trying to show that the $\mathbb{Q}$-vector space $\mathbb{Q}(\zeta_p)$ has dimension $p-1$. The first step is to go from $\mathbb{Q}$ to $\mathbb{Z}$. Note that there's a natural abelian subgroup $\mathbb{Z}[\zeta_p] \subset \mathbb{Q}(\zeta_p)$: take the $\mathbb{Z}$-span of the powers of ζ_p instead of the $\mathbb{Q}$-span. This is actually a sub*ring*, since it's closed under multiplication, but for now let's just think of it as an abelian group under addition. This abelian group $\mathbb{Z}[\zeta_p]$ is finitely generated: indeed, the fact that $\zeta_p^p = 1$ shows that $\mathbb{Z}[\zeta_p]$ is generated by just the first $p-1$ powers of ζ_p.

Now, $\mathbb{Z}[\zeta_p]$ is also torsion-free as an abelian group, since it lives inside a $\mathbb{Q}$-vector space. Recall the theorem that every finitely generated torsion-free abelian group has a $\mathbb{Z}$-basis. Such a $\mathbb{Z}$-basis of $\mathbb{Z}[\zeta_p]$ necessarily also gives a $\mathbb{Q}$-basis of $\mathbb{Q}(\zeta_p)$, so we deduce

$$dim_{\mathbb{Q}}(\mathbb{Q}(\zeta_p)) = dim_{\mathbb{Z}}(\mathbb{Z}[\zeta_p]).$$

The advantage of passing from $\mathbb{Q}$ to $\mathbb{Z}$ like this is that from $\mathbb{Z}$ we can then pass to other, simpler fields: the finite fields $\mathbb{F}_p$. The ring $\mathbb{Z}$ is like glue holding these various fields together. To go from $\mathbb{Z}$ to $\mathbb{F}_p$, note that if M is a free abelian group of rank r, then certainly $M/p = M/pM$ is an $\mathbb{F}_p$-vector space of dimension r, since a basis of M gives a basis of M/p. (This is easiest to see if you think of a basis as specifying an isomorphism $M \simeq \mathbb{Z}^r$). So in total we have

$$dim_{\mathbb{Q}}(\mathbb{Q}(\zeta_p)) = dim_{\mathbb{Z}}(\mathbb{Z}[\zeta_p]) = dim_{\mathbb{F}_p}(\mathbb{Z}[\zeta_p]/p).$$

This gives the set-up for the p-adic proof: it suffices to show that $dim_{\mathbb{F}_p}(\mathbb{Z}[\zeta_p]/p) = p-1$.

Now, the heart of the proof is the identity

$$p = (1-\zeta_p)(1-\zeta_p^2)\dots(1-\zeta_p^{p-1}).$$

This follows by setting $X = 1$ in the identity $1 + X + X^2 + \dots + X^{p-1} = \Phi_p(X)$.

This is a remarkable identity. It's remarkable because p was supposed to be a prime number. But now we see that when we move from $\mathbb{Z}$ to the ring $\mathbb{Z}[\zeta_p]$, then p no longer looks like a prime number. In fact here we've exhibited a very long factorization of p: it has $p-1$ factors. That's the key to this proof: this length-$(p-1)$ factorization of p will translate into the statement $dim_{\mathbb{F}_p}(\mathbb{Z}[\zeta_p]/p) = p-1$ which gives the desired $dim_{\mathbb{Q}}(\mathbb{Q}(\zeta_p)) = p-1$.

But, philosophically, we have to rule out the possibility that we have just done the analog of writing $p = (-p)(-1)$, or something like that. Actually, we'll see that the above factorization is more like $27 = (-3)(3)(-3)$: a nontrivial factorization, but where all the factors are essentially the same.

By "essentially the same" we mean something different from the fact that there are Galois symmetries relating them (though that is also true)! We mean that each factor is a unit multiple of each other factor. Recall that a *unit* in a ring is an element that has a multiplicative inverse. Units are the things that don't really count for the purposes of factorizations. You don't get anywhere new using them, like $p = (-p)(-1)(1)$.

To prove that these factors are all unit multiples of each other, it suffices to show that each divides each other (in the ring $\mathbb{Z}[\zeta_p]$). This is because if $a|b$ and $b|a$ in a ring which lives in a field, then the quotients a/b and b/a are each others' inverses, and so are units. So we just need to show that $(1-\zeta_p^j)$ divides $(1-\zeta_p^k)$ for every $0 \leq j,k < p$. By rechoosing which primitive p^{th} root of unity we're calling ζ_p, we can assume $j = 1$. Then the identity

$$(1-\zeta_p^k) = (1-\zeta_p)(1+\zeta_p+\ldots+\zeta_p^{k-1})$$

verifies the claim.

A byproduct of this proof is that all the numbers $1+\zeta_p+\ldots+\zeta_p^{k-1}$ are units in the ring $\mathbb{Z}[\zeta_p]$. These numbers are called *cyclotomic units*. They are very special objects, but for now we actually want to just ignore them because they're units.

We summarize the above in the following statement:

Summary: In the ring $\mathbb{Z}[\zeta_p]$, there is a factorization $p = u \cdot \pi^{p-1}$ where u is a unit and $\pi = 1-\zeta_p$.

With this, actually, the proof is almost done. We're trying to find the dimension of $\mathbb{Z}[\zeta_p]/p$. But now we see that $\mathbb{Z}[\zeta_p]/p$ is the same as $\mathbb{Z}[\zeta_p]/(\pi^{p-1}\mathbb{Z}[\zeta_p])$. So there's a whole sequence of length $p-1$ of "modding outs" more drastic than modding out by p: we can mod out by π^k for any k from 0 to $p-1$. Thus we can prove the desired statement $dim_{\mathbb{F}_p}(\mathbb{Z}[\zeta_p]/p) = p-1$ if we just show that the dimension grows by one each time we mod out by a further power of π.

In other words (by the "third isomorphism theorem") we need to show that each successive quotient $(\pi^k\mathbb{Z}[\zeta_p])/(\pi^{k+1}\mathbb{Z}[\zeta_p])$ is one-dimensional. But multiplication by π gives an isomorphism between each of these successive quotients. So we can take $k = 0$, meaning it suffices to just see that $\mathbb{Z}[\zeta_p]/\pi$ is one-dimensional. But actually, the map $\mathbb{F}_p \to \mathbb{Z}[\zeta_p]/\pi$ sending 1 to 1 is an isomorphism. Indeed, the quotient by $\pi = 1-\zeta_p$ identifies ζ_p with 1, and thus also identifies each power of ζ_p with 1, which implies that the map is surjective. Thus if it weren't an isomorphism then $\mathbb{Z}[\zeta_p]/\pi$ would be 0, so π would be a unit, so $p = u\pi^{p-1}$ would be a unit, so we'd have $dim_{\mathbb{Q}}(\mathbb{Q}(\zeta_p)) = dim_{\mathbb{F}_p}(\mathbb{Z}[\zeta_p]/p) = 0$. But this is totally absurd, since $\mathbb{Q}(\zeta_p)$ contains $\mathbb{Q}$! □

As an aside, one reason to call this the p-adic proof is that it actually shows that the theorem holds

even if you replace $\mathbb{Q}$ by $\mathbb{Q}_p$, the p-adic numbers. But we're not talking about the p-adic numbers, at least not for now.

The above proof can be made much more efficient, though at the cost of not touching on some important ideas. Note that in the end what we really showed is that the powers of π form a basis. There are quicker ways of seeing that; search the net for "Eisenstein criterion" if you want a proof from the (Poly) perspective.

There is also a fourth and totally radical perspective on this theorem, which is the scheme theoretic one. The purpose of scheme theory is to make geometry out of rings. In our case, the scheme theory perspective claims that the extension of rings $\mathbb{Z}[\zeta_n]/\mathbb{Z}$ is like a ramified cover of topological spaces. One imagines $\mathbb{Z}$ as space populated by its primes, and similarly for $\mathbb{Z}[\zeta_n]$. The (Sch) restatement of the above theorem is that this is a connected cover of degree $\phi(n)$. In the above proof we saw this by looking above the prime p, where we saw "nilpotency" of order $p-1$, which implies that the cover must have degree $p-1$.