Theorem 1.1. Suppose $m$ is a primitive $m$th root of unity, then $\mathcal{O}_{\mathbb{Q}(\zeta_m)} = \mathbb{Z}[\zeta_m]$.

1. The ring of integers

Since $\zeta_m$ satisfies $x^m - 1 = 0$, we have $\mathbb{Z}[\zeta_m] \subset \mathcal{O}_{\mathbb{Q}(\zeta_m)}$. We can now prove the following theorem fairly easily:

Theorem 1.1. If $\zeta_m$ is a primitive $m$th root of unity, then $\mathcal{O}_{\mathbb{Q}(\zeta_m)} = \mathbb{Z}[\zeta_m]$.

To do so, we need the following lemma:

Lemma 1.2. Suppose $m = p^n$. Then in $\mathcal{O}_{\mathbb{Q}(\zeta_m)}$, we have:

(i) The elements $(1 - \zeta_m^i)/(1 - \zeta_m^i)$ all generate the same ideal for $(i, p) = 1$;

(ii) If $p > 2$, the element $1 + \zeta_m^i$ is a unit;

(iii) We have the ideal factorization $(p) = (1 - \zeta_m^i)^{(p-1)p^{n-1}}$

Proof. (i) We have $(1 - \zeta_m^i)/(1 - \zeta_m^i) = 1 + \zeta_m^i + \cdots + \zeta_m^{i-1} \in \mathbb{Z}[\zeta_m]$. On the other hand, if $ii' \equiv 1$ (mod $p^n$), we have $(1 - \zeta_m^{ii'})/(1 - \zeta_m^i) = (1 - \zeta_m^{ii'})/(1 - \zeta_m^i) = 1 + \zeta_m^i + \cdots + \zeta_m^{i-1} \in \mathbb{Z}[\zeta_m]$, so we find that $(1 - \zeta_m^i)$ and $(1 - \zeta_m^{i'})$ divide one another in $\mathbb{Z}[\zeta_n]$ and hence in $\mathcal{O}_{\mathbb{Q}(\zeta_m)}$. (ii) By (i), $1 + \zeta_m^i = (1 - \zeta_m^2)/(1 - \zeta_m^i)$ is a unit; hence in $\mathcal{O}_{\mathbb{Q}(\zeta_m)}$. (iii) We have $\Phi_p(x) = (x^{p^n} - 1)/(x^{p^{n-1}} - 1) = 1 + x^{p^{n-1}} + \cdots + x^{(p-1)p^{n-1}} = \prod_{i=1}^{p-1}(x - \zeta_m^i)$, so $\Phi_p(1) = p - 1$.

By (i), the right side generates the same ideal as $(1 - \zeta_m^i)^{(p-1)p^{n-1}}$.

We now prove the theorem.

Proof of the theorem. We first prove the case that $m = p^n$ for some $n$. It is enough to show that for every prime $q$, we have $\mathcal{O}_{\mathbb{Q}(\zeta_m)}/q = \mathbb{Z}[\zeta_m]/q$. Now, for $q \neq p$, we know that $\Phi_p(x)$ is separable mod $q$, so disc $\Phi_p(x) = D_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(1, \zeta_m, \ldots, \zeta_m^{(p-1)p^{n-1}})$ is a unit in $\mathbb{Z}(q)$, and it follows that $\mathcal{O}_{\mathbb{Q}(\zeta_m)}/q = \mathbb{Z}[\zeta_m]/q$. It remains only to consider the case that $q = p$. By (iii) above, we have that $(1 - \zeta_m^i)$ is the unique prime ideal lying above $p$, and we also observe by the degree formula that we must have $\mathcal{O}_{\mathbb{Q}(\zeta_m)}/(1 - \zeta_m^i) \cong \mathbb{Z}/(p)$. Thus, by the last theorem from last time, we have

$$\mathcal{O}_{\mathbb{Q}(\zeta_m)}/p = \mathbb{Z}[1, 1 - \zeta_m^i]/p = \mathbb{Z}[\zeta_m]/p.$$ 

This completes the proof for the $m = p^n$ case.

But for the general case, we induct on the number of prime factors; as in the proof of the irreducibility of $\Phi_m(x)$, we have that $(D_{\mathbb{Q}(\zeta_m)}, D_{\mathbb{Q}(\zeta_r)}) = 1$ if $p$ is prime to $r$, and then by the first theorem of the last lecture, we have

$$\mathcal{O}_{\mathbb{Q}(\zeta_m)} = \mathcal{O}_{\mathbb{Q}(\zeta_m, \zeta_r)} = \mathcal{O}_{\mathbb{Q}(\zeta_m)} \mathcal{O}_{\mathbb{Q}(\zeta_r)},$$

and since $\mathbb{Z}[\zeta_m, \zeta_r] = \mathbb{Z}[\zeta_m]\mathbb{Z}[\zeta_r]$, we are able to carry out the induction.
Example 1.3. This example is due to Dedekind. Let \( \alpha \) be a root of \( x^3 - x^2 - 2x - 8 \), and consider \( \mathbb{Q}(\alpha) \). One can show that \( \mathcal{O}_{\mathbb{Q}(\alpha)} \) is generated by \( \alpha \) and \( \frac{4}{\alpha} \). By analyzing \( \mathcal{O}_{\mathbb{Q}(\alpha)} \) modulo 2, one can show that it is not generated over \( \mathbb{Z} \) by any single element.

2. Fermat’s Last Theorem

We will now prove certain cases of Fermat’s Last Theorem, by studying the arithmetic of \( \mathbb{Z}[\zeta_p] \). We introduce the following (non-standard) terminology:

**Definition 2.1.** We say that an odd prime \( p \) is **h-regular** if \( p \) does not divide the class number (i.e., the order of the ideal class group) of \( \mathbb{Q}(\zeta_p) \). We say that \( p \) is **strongly h-regular** if it is h-regular, and if it satisfies the further property that for all units \( u \in \mathbb{Z}[\zeta_p]\times \) such that \( u \equiv m \pmod{p\mathbb{Z}[\zeta_p]} \) for some \( m \in \mathbb{Z} \), then \( u = u'^p \) for some \( u' \in \mathbb{Z}[\zeta_p] \).

**Remark 2.2.** We will see later, by class field theory, the fact (known as Kummer’s lemma) that a prime \( p \) being h-regular implies that it is strongly h-regular. We will also give an explicitly computable criterion for h-regularity in terms of Bernoulli numbers.

Fermat’s Last Theorem for prime exponents is classically broken up into two cases: case I is the situation that all terms are prime to \( p \), whereas in case II, one term may be divisible by \( p \). Case II is the harder one. While both cases begin with a factorization of the left side in \( \mathbb{Z}[\zeta_p] \), case I then shows that the factors are prime, and produces a linear relation among different powers of \( \zeta_p \) modulo \( p \). Case II involves subtler analysis, and an induction argument on the power of \( p \) dividing the appropriate term of the equation.

**Exercise 2.3.** Prove case I of Fermat’s Last Theorem for h-regular primes. That is, prove that if \( p \) is h-regular, there do not exist integer solutions to

\[
x^p + y^p = z^p
\]

with \( x, y, z \) prime to \( p \).

Our aim is to prove case II of Fermat’s Last Theorem for strongly h-regular primes.

**Theorem 2.4.** Let \( p \) be strongly h-regular. Then there are no non-zero integer solutions to

\[
x^p + y^p = z^p
\]

with \( p \) dividing (at least) one of \( x, y, z \).

**Proof.** Suppose to the contrary that a solution exists. We first note that we may assume that \( p | z \), but \( p \) is prime to \( x, y \); indeed, we may certainly assume that \( x, y, z \) have no common factors; because \( p \) is odd, we may write \( x^p + y^p + (-z)^p = 0 \), so the situation is symmetric in \( x, y, z \), and we assume that \( p | z \). But then, if \( p \) divided \( x \) or \( y \), it would have to divide all three, contradicting relative primality.

Let \( p^{n'} \) be the largest power of \( p \) dividing \( z \). We will prove by induction on \( n' \) that no such solution is possible. However, we will induct on the following slightly stronger statement: there do not exist \( \alpha, \beta, \gamma \in \mathbb{Z}[\zeta_p], u \in \mathbb{Z}[\zeta_p]\times \), and \( n \in \mathbb{N} \) such that

\[
\alpha^p + \beta^p + u(1-\zeta_p)^{pn} \gamma^p = 0,
\]
and \((1 - \zeta_p)\) does not divide \(\alpha\beta\gamma\). (Note that \(n\) here is \(n'(p-1)\).) Before beginning the induction, we make some general observations. If we had such a solution, we would obtain an identity of ideals:

\[
\prod_{j=0}^{p-1} \left( \alpha + \zeta_p^j \beta \right) = (1 - \zeta_p)^n \gamma^p. \tag{2.4.2}
\]

Note that \(\alpha + \zeta_p^j \beta \equiv \alpha + \beta \pmod{1 - \zeta_p}\), so since \(1 - \zeta_p\) must divide at least one factor on the left, it must in fact divide all of them.

We now observe that all the \(\alpha + \zeta_p^j \beta\) must be distinct modulo \((1 - \zeta_p^2)\). If we had \(\alpha + \zeta_p^j \beta \equiv \alpha + \zeta_p^{j'} \beta \pmod{1 - \zeta_p^2}\) for \(j' > j\), we would have \((1 - \zeta_p^2)\left(\zeta_p^j \beta \right)\) \(\in \mathbb{Z}[[\zeta_p]]\). Since \((1 - \zeta_p^{j'-j})\) is a unit multiple of \(1 - \zeta_p\), this would imply \((1 - \zeta_p)\beta\), contradicting our initial hypothesis.

Proof to be continued next time. \(\square\)