Cyclotomic fields

If m is a positive integer, we write $\zeta_m = e^{\frac{2i\pi}{m}}$ a primitive m^{th}-root of unit in $\mathbb{C}$. Recall that φ is Euleur's totient, such that $\varphi(m) = \prod_{p|m}^{r}(p-1)p^{v_p(m)-1}$.

Exercise 1. [Equality of cyclotomic fields]

1. Let m be an odd integer. Show that $\mathbb{Q}(\zeta_{2m}) = \mathbb{Q}(\zeta_m)$.
2. Show that if m is even and r is a multiple of m such that $\varphi(r) \leq \varphi(m)$ then $r = m$.
3. Show that the only roots of unity in $K = \mathbb{Q}(\zeta_m)$ are the powers of ζ_m if m is even, and the powers of ζ_{2m} if m is odd. *(Hint : When m is even, show that if ω is a primitive k^{th}-root of unity in K, then there exist $u, v \in \mathbb{Z}$ such that $\zeta_r = \zeta_m^u \omega^v$, where $r = lcm(k, m)$)*
4. Give necessary and sufficient conditions on m and n for $\mathbb{Q}(\zeta_m)$ to be equal to $\mathbb{Q}(\zeta_n)$.

Exercise 2. [Maximal real subfields of cyclotomic fields]

Let p be an odd prime number and $K = \mathbb{Q}(\zeta_p)$.

1. Show that $\{\zeta_p^i \mid -\frac{p-1}{2} \leq i \leq \frac{p-1}{2}, i \neq 0\}$ is an integral basis of $\mathcal{O}_K$.
2. Let $F = \mathbb{Q}(\zeta_p)^+ = K \cap \mathbb{R}$. Show that $F = \mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right)$.
3. Show that $\mathcal{O}_F = \mathbb{Z}\left[2\cos\left(\frac{2\pi}{p}\right)\right]$.

Remark : A totally imaginary number field K which is a quadratic extension of a totally real number field F is called a CM-field, for complex multiplication.

Exercise 3. [Kronecker's lemma]

Let K be a number field and $x \in \mathcal{O}_K$ such that $|\sigma(x)| \leq 1$ for every embedding $\sigma : K \hookrightarrow \mathbb{C}$. We will show that x is a root of unity.

1. Let $P_k = \prod_{\sigma:K\hookrightarrow\mathbb{C}}(X - \sigma(x^k))$. Show that $P_k \in \mathbb{Z}[X]$.
2. Show that the set $\{P_k \mid k \geq 1\}$ is finite.
3. Deduce that x is a root of unity.

Remark : Real algebraic integers of absolute value > 1 whose other conjugates have absolute value < 1 are called Pisot numbers, and they have remarkable diophantine properties. For instance, it is easy to see that their powers get closer and closer to integers.

Exercise 4. [Units of $\mathbb{Z}[\zeta_p]$]

Let p be an odd prime number and $u \in \mathbb{Z}[\zeta_p]^\times$.

1. Show that there exists $a \in \mathbb{Z}$ such that $\frac{u}{\overline{u}} = \pm\zeta_p^a$. *(Hint : Use Exercises 1 and 3.)*
2. Assume that $\frac{u}{\overline{u}} = -\zeta_p^a$. Show that $u \equiv \overline{u} \bmod (1-\zeta_p)$ and deduce that $u \equiv -u \bmod (1-\zeta_p)$.
3. Show $\mathbb{Z}[\zeta_p]/(1-\zeta_p)$ is an integral ring of characteristic p, and deduce a contradiction.
   Remark : This is often called Kummer's lemma.
4. Show that $u = \zeta_p^r v$ for some $r \in \mathbb{Z}$ and $v \in \mathcal{O}_{Q(\zeta_p)^+}^\times$.

Exercise 5. [Quadratic subfields of cyclotomic fields]

1. Let p be an odd prime number. Show that the only quadratic subfield $\mathbb{Q}(\zeta_p)$ is $\mathbb{Q}(\sqrt{p^*})$, where $p^* = \begin{cases} p \text{ if } p \equiv 1 \bmod 4 \\ -p \text{ if } p \equiv 3 \bmod 4 \end{cases}$. *(Hint : Use the discriminant.)*
2. Define the p^{th}-quadratic Gauss sum to be $G_p = \sum_{a \in \mathbb{Z}/p\mathbb{Z}^\times} \left(\frac{a}{p}\right) \zeta_p^a$, where $\left(\frac{a}{p}\right)$ is Legendre's symbol, defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ if } a \text{ is a square} \bmod p \\ -1 \text{ otherwise} \end{cases}.$$

   Show that $G_p^2 = p^*$.
3. Compute $(\zeta_8 + \zeta_8^{-1})^2$ and find every subfield of $Q(\zeta_8)$. What is the quadratic subfield of $\mathbb{Q}(\zeta_4)$?
4. Show that every quadratic field is contained in a cyclotomic field.

Remark : The Kronecker-Weber theorem, also called Kronecker's Jugendtraum (Kronecker's dream of youth), states that every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field. This is better explained by class field theory.

Exercise 6. [Fermat continued] Recall from TD 1 that we wanted to prove that the equation $(F)_p : x^p + y^p = z^p$ admits no non-trivial integer solution for $p \geq 5$ an odd prime.

We had assumed for a contradiction that (x, y, z) was a primitive solution of $(F)_p$ in $\mathbb{Z}^3$ satisfying $xyz \not\equiv 0 \bmod p$. Assuming $\mathbb{Z}[\zeta_p]$ is a factorial domain, we had established that $x + \zeta_p y = u\alpha^p$ for some $\alpha \in \mathbb{Z}[\zeta_p]$ and $u \in \mathbb{Z}[\zeta_p]^\times$.

1. Show that there exists $a \in \mathbb{Z}$ such that $\alpha^p \equiv a \bmod p$.
2. Show that there exists $k \in \{0, \ldots, p-1\}$ such that $x + \zeta_p y \equiv (x + \zeta_p^{-1} y)\zeta_p^k \bmod p$. *(Hint : Use Kummer's lemma.)*
3. By using the fact that ζ_p has degree $p-1$ over $\mathbb{Q}$, show that $k = 1$.
4. Deduce that $x \equiv y \bmod p$.
5. The same reasoning shows that $x \equiv -z \bmod p$. Deduce the contradiction $p \mid 3x^p$.

Remark : With a bit more work, one can also deduce a contradiction in the case $p \mid xyz$.