Exercise Sheet 8

Cyclotomic Fields, Legendre Symbol

1. The *Möbius function* $\mu : \mathbb{Z}^{\geqslant 1} \to \mathbb{Z}$ is defined by

$$\mu(n) \ := \ \begin{cases} (-1)^k & \text{if } n \text{ is the product of } k \geqslant 0 \text{ distinct primes,} \\ 0 & \text{otherwise.} \end{cases}$$

   (a) Show that for any integer $n \geqslant 1$ we have

$$\sum_{d|n} \mu(\tfrac{n}{d}) \ = \ \sum_{d|n} \mu(d) \ = \ \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1. \end{cases}$$

   (b) *Möbius inversion:* Let $(G, +)$ be an abelian group and let f and g be arbitrary functions $\mathbb{Z}^{\geqslant 1} \to G$. Use (a) to show that

$$\forall n \in \mathbb{Z}^{\geqslant 1} \colon \, g(n) = \sum_{d|n} f(d)$$

   if and only if

$$\forall n \in \mathbb{Z}^{\geqslant 1} \colon \, f(n) = \sum_{d|n} \mu(\tfrac{n}{d}) g(d).$$

   (c) Let $n \in \mathbb{Z}^{\geqslant 1}$ and let $\zeta \in \mathbb{C}$ be an n^{th} primitive root of unit. We define the n^{th} *cyclotomic polynomial* as

$$\Phi_n(X) := \prod_{d \in (\mathbb{Z}/n\mathbb{Z})^\times} (X - \zeta^d).$$

   Use (b) to show that

$$\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(\frac{n}{d})}.$$

   (d) Deduce that Φ_n has coefficients in $\mathbb{Z}$ and is irreducible in $\mathbb{Q}[X]$.

   (e) *Euler's phi function:* Deduce that

$$\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^\times| = \sum_{d|n} \mu(\tfrac{n}{d}) d.$$

2. Determine the possibilities for the group $\mu(K)$ of roots of unity in K for all number fields K of degree 4 over $\mathbb{Q}$.

3. Prove that for any odd prime number p the following are equivalent:
   (a) $p \equiv 1 \bmod (4)$.
   (b) p is totally split in $\mathbb{Z}[i]$.
   (c) $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.
4. Prove that every quadratic number field can be embedded in a cyclotomic field.
5. Prove the third case of Gauss's reciprocity law, i.e., that for any odd prime p

$$\left(\tfrac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

   Hint: Use that $(1+i)^2 = 2i$ to evaluate $(1+i)^p$ and prove that

$$\left(\tfrac{2}{p}\right)(1+i)i^{\frac{p-1}{2}} \equiv 1 + i(-1)^{\frac{p-1}{2}} \bmod (p).$$

6. Calculate the following Legendre symbols:
   (a) Calculate $\left(\frac{3}{p}\right)$ for any odd prime p.
   (b) Calculate $\left(\frac{-22}{71}\right)$.