Exercise sheet 5

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

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

   Here and below all sums are extended only over positive divisors.

   (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. Use (b) to show that the n^{th} *cyclotomic polynomial* satisfies

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

   (d) Deduce that Φ_n has coefficients in $\mathbb{Z}$.

   (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 every quadratic number field can be embedded in a cyclotomic field.

*4. (a) Determine the ring of integers of any subfield of $\mathbb{Q}(\mu_\ell)$ for any prime ℓ.

(b) Work out the result explicitly in the case $\ell = 7$.

5. *Second supplement to the quadratic reciprocity law:* Prove that for any odd prime ℓ we have $(\frac{2}{\ell}) = (-1)^{\frac{\ell^2-1}{8}}$.

Hint: Evaluate the sum $(1+i)^\ell$ modulo $\ell\mathbb{Z}[i]$ in two ways.

6. (a) Compute the Legendre symbol $\left(\frac{-22}{71}\right)$.

(b) Compute the Legendre symbol $\left(\frac{3}{p}\right)$ for any odd prime p.

(c) Find distinct two digits primes p and q, such that each is a quadratic residue modulo the other.