Solutions 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

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

Solution: All sums are extended only over positive divisors.

(a) The first equality follows by reordering the summands. Next write $n = p_1^{k_1} \cdots p_r^{k_r}$ with distinct primes p_i and exponents $k_i > 0$. Then the divisors of n are the numbers $d = p_1^{l_1} \cdots p_r^{l_r}$ for all choices of $0 \leqslant l_i \leqslant k_i$. If any $l_i > 1$, then $\mu(d) = 0$. Hence the divisors with $\mu(d) \neq 0$ are precisely the numbers $d = \prod_{s \in S} s$ for all subsets $S \subset \{p_1, \ldots, p_r\}$. We obtain

$$\sum_{d|n} \mu(d) = \sum_{S \subset \{p_1,\ldots,p_r\}} (-1)^{|S|} = \sum_{k=0}^{r} \binom{r}{k} (-1)^k = \begin{cases} (1-1)^r = 0 & \text{if } r > 0, \\ 1 & \text{if } r = 0. \end{cases}$$

(b) Suppose that the first condition holds. We calculate

$$\begin{aligned} \sum_{d|n} \mu(\tfrac{n}{d}) g(d) &= \sum_{d|n} \mu(\tfrac{n}{d}) \sum_{k|d} f(k) = \sum_{k|n} f(k) \sum_{d\colon k|d|n} \mu(\tfrac{n}{d}) \\ &= \sum_{k|n} f(k) \sum_{d\colon k|d|n} \mu(\tfrac{n/k}{d/k}) = \sum_{k|n} f(k) \sum_{d|\frac{n}{k}} \mu(\tfrac{n/k}{d}) = f(n). \end{aligned}$$

Suppose now that the second condition holds. We calculate

$$\sum_{d|n} f(d) = \sum_{d|n} \sum_{k|d} \mu(\tfrac{d}{k}) g(k) = \sum_{k|n} g(k) \sum_{d\colon k|d|n} \mu(\tfrac{d}{k}) = \sum_{k|n} g(k) \sum_{d\colon d|\frac{n}{k}} \mu(d) = g(n),$$

where the last equality follows from (a).

(c) For any $m \in \mathbb{Z}^{\geqslant 1}$ we have $X^m - 1 = \prod_{d|m} \Phi_d(X)$, because any m^{th} root of unity is a primitive d^{th} root of unity for precisely one $d|m$. Applying Möbius inversion (here written multiplicatively) to the map $f\colon \mathbb{Z}^{\geqslant 1} \to \mathbb{C}(X)^\times$ with $f(m) := \Phi_m(X)$ we obtain the desired result.

(d) By (c) the n^{th} cyclotomic polynomial can be written as $\Phi_n = P(X)/Q(X)$ for some polynomials $P, Q \in \mathbb{Z}[X]$ with constant terms ± 1. Thus we can expand it as a power series in $\mathbb{Z}[[X]]$ with constant term ± 1. But by definition Φ_n is a polynomial over $\mathbb{C}$; hence the power series expansion stops and Φ_n is a polynomial in $\mathbb{Z}[X]$.

Since $\Phi_n \in \mathbb{Q}[X]$ is monic with $\Phi_n(\zeta) = 0$ and $[\mathbb{Q}(\zeta)/\mathbb{Q}] = \varphi(n) = \deg \Phi_n$ it follows that Φ_n is the minimal polynomial of ζ over $\mathbb{Q}$ and thus irreducible. (Since ζ is an algebraic integer, this also implies that Φ_n has coefficients in $\mathbb{Z}$.)

(e) By (c), we have

$$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times| = \deg \Phi_n = \sum_{d|n} \deg\big((X^d - 1)^{\mu(\frac{n}{d})}\big) = \sum_{d|n} \mu(\tfrac{n}{d}) d.$$

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

   Solution: Let $n := |\mu(K)|$; then K contains the field of n^{th} roots of unity $\mathbb{Q}(\mu_n)$. Thus $\varphi(n) = [\mathbb{Q}(\mu_n)/\mathbb{Q}]$ divides $[K/\mathbb{Q}] = 4$. A quick computation shows that $\varphi(n)|4$ precisely for the values $n = 1, 2, 3, 4, 5, 6, 8, 10, 12$. Since always $\{\pm 1\} \subset \mu(K)$, this leaves only the values $n = 2, 4, 6, 8, 10, 12$. We claim that each of these actually occurs for a number field of degree 4 over $\mathbb{Q}$.

   For $n = 8, 10, 12$ the field $\mathbb{Q}(\mu_n)$ already has degree $\varphi(n) = 4$ over $\mathbb{Q}$.

   For $n = 6$ set $K := \mathbb{Q}(\sqrt{-3}, \sqrt{7})$. This has degree 4 over $\mathbb{Q}$, because its quadratic subfields $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{7})$ have distinct discriminants -3 and 28. The inclusion $\mathbb{Q}(\sqrt{7}) \subset K$ also implies that the discriminant of $K/\mathbb{Q}$ is divisible by 7. On the other hand K contains the primitive 6^{th} root of unity $\frac{1+\sqrt{-3}}{2}$. Thus 6 divides $|\mu(K)|$ and hence, by the above list $|\mu(K)| \in \{6, 12\}$. But $|\mu(K)| = 12$ would require that $K = \mathbb{Q}(\mu_{12})$, which is impossible, because 7 does not divide the discriminant of $\mathbb{Q}(\mu_{12})/\mathbb{Q}$. Thus $|\mu(K)| = 6$, as desired.

   For $n = 4$, see exercise 1 on sheet 5, where we proved that $\mu(\mathbb{Q}(\sqrt{5}, i))$ has order 4.

   Finally, for $n = 2$ note that any subfield of $\mathbb{R}$ contains only the roots of unity $\{\pm 1\}$. An example of such a field is $K := \mathbb{Q}(\sqrt{2}, \sqrt{3})$. This has degree 4 over $\mathbb{Q}$, because its quadratic subfields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ have distinct discriminants.

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 $a, b \in \mathbb{Z}$.

   Solution: (a) $\Leftrightarrow$ (b): By §8 Proposition 6 of the lecture course, the prime p splits in $\mathbb{Z}[i] = \mathcal{O}_{\mathbb{Q}(\mu_4)}$ if and only if the image of p in $(\mathbb{Z}/4\mathbb{Z})^\times$ has order 1. This is equivalent to $p \equiv 1 \bmod (4)$.

   (c) $\Rightarrow$ (b): If $p = a^2 + b^2$, we have $p = (a+bi)(a-bi) = (a+bi)\overline{(a+bi)}$. Since p is not a unit, this shows that neither of $a \pm bi$ is a unit. Thus p is not prime in $\mathbb{Z}[i]$. Being odd, it is also not ramified in $\mathbb{Z}[i]$. It only remains that p is split in $\mathbb{Z}[i]$, and then $p = (a+bi)(a-bi)$ is actually its prime factorization in $\mathbb{Z}[i]$.

   (b) $\Rightarrow$ (c): As $\mathbb{Z}[i]$ is a principal ideal domain, the prime p is totally split in $\mathbb{Z}[i]$ if and only if $p\mathbb{Z}[i] = p_1p_2\mathbb{Z}[i]$ for inequivalent prime elements p_1 and p_2 in $\mathbb{Z}[i]$. Since $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$ acts transitively on the primes above p, it follows that in this case $p_2\mathbb{Z}[i] = \bar{p}_1\mathbb{Z}[i]$. Writing $p_1 = a + bi$, we deduce that $(a^2+b^2)\mathbb{Z}[i] = (p_1\bar{p}_2)\mathbb{Z}[i] = p\mathbb{Z}[i]$. As both a^2+b^2 and p are positive, it follows that $a^2+b^2 = p$.

4. Prove that every quadratic number field can be embedded in a cyclotomic field.

   Solution: As usual write $K := \mathbb{Q}(\sqrt{d})$ for a squarefree integer $d = \pm p_1 \cdots p_r$ with distinct prime factors. Rewrite this in the form $d = \pm p_1^* \cdots p_r^*$ with $p_\nu^* := -p_\nu$ if $p_\nu \equiv 3 \bmod (4)$ and $p_\nu^* := p_\nu$ otherwise. Abbreviate $K_n := \mathbb{Q}(e^{\frac{2\pi i}{n}})$. Then, by §8 Proposition 7 from the lecture course, for all ν with p_ν odd we have $\sqrt{p_\nu^*} \in K_{p_\nu}$. We also have $\sqrt{-1} \in K_4$, and since $e^{\frac{2\pi i}{8}} = \frac{1+i}{\sqrt{2}}$ we have $\sqrt{2} = e^{\frac{2\pi i}{8}} + e^{-\frac{2\pi i}{8}} \in K_8$. Therefore $\sqrt{d} = \sqrt{\pm 1}\sqrt{p_1^*} \cdots \sqrt{p_r^*} \in K_{4d}$ and hence $K \subset K_{4d}$.

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

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

   Solution: See Theorem 8.6 in Chapter 1 of Neukirch.

6. Calculate the following Legendre symbols:

   (a) Calculate $\left(\frac{3}{p}\right)$ for any odd prime p.

   (b) Calculate $\left(\frac{-22}{71}\right)$.

Solution:

(a) If $p \neq \pm 3$, the law of quadratic reciprocity states that $\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}$. Note that $\left(\frac{p}{3}\right)$ and $(-1)^{\frac{p-1}{2}}$ depend only on the residue classes of p modulo 3 and 4, respectively. We calculate for $p \neq \pm 3$:

$$\left(\frac{p}{3}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \bmod (3), \\ -1 & \text{if } p \equiv 2 \bmod (3), \end{cases}$$

$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1 & p \equiv 1 \bmod (4), \\ -1 & p \equiv 3 \bmod (4). \end{cases}$$

The cases $p \equiv 0, 2 \bmod (4)$ cannot occur, since p is odd. Combining these results with $\left(\frac{3}{\pm 3}\right) = 0$, we obtain

$$\left(\frac{3}{p}\right) = \begin{cases} 0 & \text{if } p \equiv 3, 9 \bmod (12), \\ 1 & \text{if } p \equiv 1, 11 \bmod (12), \\ -1 & \text{if } p \equiv 5, 7 \bmod (12). \end{cases}$$

(b) It follows from the multiplicativity of the Legendre symbol that $\left(\frac{-22}{71}\right) = \left(\frac{-1}{71}\right)\left(\frac{2}{71}\right)\left(\frac{11}{71}\right)$. We have $\left(\frac{-1}{71}\right) = (-1)^{35} = -1$, and by exercise 5 we obtain $\left(\frac{2}{71}\right) = (-1)^{630} = 1$. Furthermore $\left(\frac{11}{71}\right)\left(\frac{71}{11}\right) = (-1)^{5 \cdot 35} = -1$ and

$$\left(\frac{71}{11}\right) = \left(\frac{5}{11}\right) = (-1)^{2 \cdot 5}\left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = 1.$$

Hence $\left(\frac{11}{71}\right) = -1$ and $\left(\frac{-22}{71}\right) = 1$.