Solutions 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

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

Solution:

(a) The first equality follows by substituting $d = n/d'$. 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

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

(b) If the first condition holds, we calculate

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

If the second condition holds, we calculate

$$\sum_{d|n} f(d) = \sum_{d|n} \sum_{k|d} \mu(\tfrac{d}{k}) g(k) = \sum_{k|n} g(k) \sum_{d\colon k|d|n} \mu(\tfrac{d}{k}) = \sum_{k|n} g(k) \sum_{e|\frac{n}{k}} \mu(e) \overset{(a)}{=} g(n).$$

(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. Viewing each as a power series in $\mathbb{Z}[[X]]$ with constant term ± 1, the quotient is therefore also 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 $\mathbb{Z}[X]$.

(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 it contains the two distinct quadratic subfields $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{7})$ with distinct discriminants -3 and 28. Also K contains the primitive 6^{th} root of unity $\frac{1+\sqrt{-3}}{2}$. Thus 6 divides $|\mu(K)|$; hence the above list shows that $|\mu(K)| \in \{6, 12\}$. Moreover, $|\mu(K)| = 12$ would require that $K = \mathbb{Q}(\mu_{12})$ and therefore $\mathbb{Q}(\sqrt{7}) \subset \mathbb{Q}(\mu_{12})$. But $\mathbb{Q}(\mu_{12}) = \mathbb{Q}(\sqrt{-1}, \sqrt{-3})$ only has the three quadratic subfields $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{3})$ with respective discriminants 4, -3, 12. Thus this case is impossible, and we have $|\mu(K)| = 6$, as desired.

For $n = 4$ we set likewise $K := \mathbb{Q}(\sqrt{-1}, \sqrt{7})$. This has degree 4 over $\mathbb{Q}$, because its quadratic subfields $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{7})$ have distinct discriminants 4 and 28. Also K contains a primitive 4^{th} root of unity.. Thus 4 divides $|\mu(K)|$; hence the above list shows that $|\mu(K)| \in \{4, 8, 12\}$. Here $|\mu(K)| = 12$ would require that $K = \mathbb{Q}(\mu_{12})$ and therefore $\mathbb{Q}(\sqrt{7}) \subset \mathbb{Q}(\mu_{12})$, which we have already excluded above. Similarly, $|\mu(K)| = 8$ would require that $K = \mathbb{Q}(\mu_8)$ and therefore $\mathbb{Q}(\sqrt{7}) \subset \mathbb{Q}(\mu_8)$. But $\mathbb{Q}(\mu_8) = \mathbb{Q}(\sqrt{-1}, \sqrt{2})$ only has the three quadratic subfields $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$ with respective discriminants 4, 8, -8. Thus this case is impossible, and we have $|\mu(K)| = 4$, as desired.

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 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. For any positive integer n abbreviate $K_n := \mathbb{Q}(e^{\frac{2\pi i}{n}})$. Then, in the lecture we proved that 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 $\sqrt{d} = \sqrt{\pm 1}\sqrt{p_1^*} \cdots \sqrt{p_r^*} \in K_{4|d|}$ and hence $K \subset K_{4|d|}$.

*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 $\ell = 7$.

   Solution:

   (a) Fix a primitive ℓ-th root of unity $\zeta \in \mathbb{C}$. Then for $K := \mathbb{Q}(\mu_\ell)$ we know already that $\mathcal{O}_K = \mathbb{Z}[\zeta] \cong \mathbb{Z}[X]/(\Phi_\ell)$ with $\Phi_\ell(X) = 1 + X + \ldots + X^{\ell-1}$. Thus $1, \zeta, \ldots, \zeta^{\ell-2}$ is a $\mathbb{Z}$-basis of $\mathcal{O}_K$. Since $1 + \zeta + \ldots + \zeta^{\ell-1} = \Phi_\ell(\zeta) = 0$, we can substitute the basis element 1 by the element $\zeta^{\ell-1}$ and deduce that the primitive ℓ-th roots of unity $\zeta, \zeta^2, , \ldots, \zeta^{\ell-1}$ form another $\mathbb{Z}$-basis of $\mathcal{O}_K$. In other words, any element of $\mathcal{O}_K$ can be written uniquely in the form

$$\sum_{j \in \mathbb{F}_\ell^\times} a_j \zeta^j \qquad (*)$$

with coefficients $a_j \in \mathbb{Z}$.

On the other hand, by the main theorem of Galois theory the subfields of K are the fixed fields K^H for all subgroups $H < \mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{F}_\ell^\times$. For any such H we then have $\mathcal{O}_{K^H} = \mathcal{O}_K \cap K^H$. But the element $(*)$ is invariant under H if and only if the coefficient a_j depends only on the coset $jH \subset \mathbb{F}_\ell^\times$. Thus

$$\mathcal{O}_{K^H} \;=\; \bigoplus_{[j] \in \mathbb{F}_\ell^\times / H} \mathbb{Z} \cdot \sum_{j' \in [j]} \zeta^{j'}. \qquad (**)$$

(b) The group $\mathbb{F}_7^\times$ is cyclic of order 6 and its subgroups are precisely 1, $\{\pm\overline{1}\}$, $\{\overline{1}, \overline{2}, \overline{4}\}$, and $\mathbb{F}_7^\times$.

i. For $H = 1$ we get $K^H = K$ and hence $\mathcal{O}_{K^H} = \mathcal{O}_K = \mathbb{Z}[\zeta]$.

ii. For $H = \mathbb{F}_\ell^\times$ we get $K^H = \mathbb{Q}$ and hence $\mathcal{O}_{K^H} = \mathbb{Z}$.

iii. For $H = \{\overline{1}, \overline{2}, \overline{4}\}$ the basis in $(**)$ consists of $\omega := \zeta + \zeta^2 + \zeta^4$ and $\omega' := \zeta^3 + \zeta^5 + \zeta^6$. Here

$$\omega + \omega' \;=\; \zeta + \zeta^2 + \zeta^4 + \zeta^3 + \zeta^5 + \zeta^6 \;=\; -1;$$

hence $\mathcal{O}_{K^H} = \mathbb{Z}[\omega]$. More precisely we have

$$\omega^2 \;=\; \zeta^2 + \zeta^4 + \zeta^8 + 2\zeta^3 + 2\zeta^5 + 2\zeta^6 \;=\; \omega + 2\omega' \;=\; -\omega - 2.$$

Thus $\omega^2 + \omega + 2 = 0$ and hence $\omega = \frac{-1 \pm \sqrt{-7}}{2}$. Indeed, since $-7 \equiv 1 \bmod (4)$, we already know that the ring of integers of $\mathbb{Q}(\sqrt{-7})$ is $\mathbb{Z}[\frac{-1 \pm \sqrt{-7}}{2}]$.

iv. For $H = \{\pm\overline{1}\}$ the basis in $(**)$ consists of $\eta := \zeta + \zeta^{-1}$ and $\eta' := \zeta^2 + \zeta^{-2}$ and $\eta'' := \zeta^3 + \zeta^{-3}$. Here

$$\begin{aligned} \eta^2 \;&=\; \zeta^2 + 2 + \zeta^{-2} \;=\; \eta' + 2 \qquad \text{and} \\ \eta + \eta' + \eta'' \;&=\; \zeta + \zeta^{-1} + \zeta^2 + \zeta^{-2} + \zeta^3 + \zeta^{-3} \;=\; -1; \end{aligned}$$

hence we have $\eta' = \eta^2 - 2$ and $\eta'' = 1 - \eta - \eta^2$ and therefore $\mathcal{O}_{K^H} = \mathbb{Z}[\eta]$. Moreover we have

$$\eta^3 \;=\; \zeta^3 + 3\zeta + 3\zeta^{-1} + 2\zeta^{-3} \;=\; \eta'' + 3\eta \;=\; 1 + 2\eta - \eta^2$$

and so $\eta^3 + \eta^2 - 2\eta - 1 = 0$. Thus

$$\mathcal{O}_{K^H} \;=\; \mathbb{Z}[\eta] \;\cong\; \mathbb{Z}[X]/(X^3 + X^2 - 2X - 1).$$

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

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

   Solution: We already know that $2^{\frac{\ell-1}{2}} \equiv \left(\frac{2}{\ell}\right) \mod \ell$. Thus on the one hand we have

   $$(1+i)^\ell \;=\; (1+i)((1+i)^2)^{\frac{\ell-1}{2}} \;=\; (1+i)(2i)^{\frac{\ell-1}{2}} \;\equiv\; (1+i)\left(\tfrac{2}{\ell}\right)i^{\frac{\ell-1}{2}} \mod \ell\mathbb{Z}[i].$$

   On the other hand, as the map $x \mapsto x^\ell$ is a ring homomorphism modulo ℓ, we get

   $$(1+i)^\ell \;\equiv\; 1+i^\ell \mod \ell\mathbb{Z}[i].$$

   Together this shows that

   $$(1+i)\left(\tfrac{2}{\ell}\right)i^{\frac{\ell-1}{2}} \;\equiv\; 1+i^\ell \mod \ell\mathbb{Z}[i].$$

   Here both sides are complex numbers of absolute value $\leqslant \sqrt{2}$. As every non-zero element of $\ell\mathbb{Z}[i]$ has absolute value $\geqslant \ell > 2\sqrt{2}$, this congruence is actually an equality. In other words we have

   $$\left(\tfrac{2}{\ell}\right) \;=\; \tfrac{1+i^\ell}{1+i} \cdot i^{\frac{1-\ell}{2}}.$$

   Here the right hand side depends only on ℓ modulo (8). Also ℓ is odd by assumption. By evaluating four cases the stated formula follows.

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.

   Solution:

   (a) The multiplicativity of the Legendre symbol shows that $\left(\frac{-22}{71}\right) = \left(\frac{-1}{71}\right)\left(\frac{2}{71}\right)\left(\frac{11}{71}\right)$. Here we have $\left(\frac{-1}{71}\right) = (-1)^{35} = -1$ by the first supplement to the quadratic reciprocity law, and $\left(\frac{2}{71}\right) = (-1)^{630} = 1$ by the second supplement. Furthermore by the quadratic reciprocity law itself we have $\left(\frac{11}{71}\right)\left(\frac{71}{11}\right) = (-1)^{5\cdot 35} = -1$ and so $\left(\frac{11}{71}\right) = -\left(\frac{71}{11}\right) = -\left(\frac{5}{11}\right)$. Likewise we have $\left(\frac{5}{11}\right)\left(\frac{11}{5}\right) = (-1)^{2\cdot 5} = 1$ and so $\left(\frac{5}{11}\right) = \left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = 1$. Therefore $\left(\frac{11}{71}\right) = -1$ and so $\left(\frac{-22}{71}\right) = (-1)\cdot 1 \cdot (-1) = 1$.
   (Indeed we have $7^2 = 49 \equiv -22 \mod (71)$.)

   (b) By definition we have $\left(\frac{3}{3}\right) = 0$. For any prime $p > 3$ the law of quadratic reciprocity states that $\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}$. Here $\left(\frac{p}{3}\right)$ and $(-1)^{\frac{p-1}{2}}$ depend only on the residue classes of p modulo 3 and 4, respectively. We thus compute

$p \bmod (12)$	$\left(\frac{p}{3}\right)$	$(-1)^{\frac{p-1}{2}}$	$\left(\frac{3}{p}\right)$
1	1	1	1
5	-1	1	-1
7	1	-1	-1
11	-1	-1	1

The answer is therefore

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

(c) If at least one of the primes is $\equiv 1 \bmod (4)$, the quadratic reciprocity law says that $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$. Then it only remains to guarantee that $\left(\frac{q}{p}\right) = 1$. Taking $p = 13$ and $q = 17$ we get $\left(\frac{17}{13}\right) = \left(\frac{4}{13}\right) = 1$, because 4 is a square.
(Indeed we have $2^2 = 4 \equiv 17 \bmod (13)$ and $8^2 = 64 \equiv 13 \bmod (17)$.)