Problem set 9 : Cyclotomic Extensions

---

(1) Determine $[\mathbb{Q}(\zeta_7, \zeta_3) : \mathbb{Q}(\zeta_3)]$.

(2) Determine a primitive element of a subfield K of $E = \mathbb{Q}(\zeta_{13})$ so that $[K : \mathbb{Q}] = 3$.

(3) Put $\zeta = \zeta_7$. Determine the degrees of $\zeta + \zeta^5$ and $\zeta + \zeta^5 + \zeta^8$ over $\mathbb{Q}$.

(4) Put $\zeta = \zeta_{11}$ and $\alpha = \zeta + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^9$. Show that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$.

(5) Let ν be a primitive element modulo p where p is a prime. Thus $\mathbb{F}_p^\times = (\nu)$. Let $\zeta = \zeta_p$. Using the list $\{\zeta^{\nu^0}, \zeta^{\nu^1}, \zeta^{\nu^2}, \ldots, \zeta^{\nu^{p-2}}\}$, show how to find the sum β of powers of ζ which determines a subfield $\mathbb{Q}(\beta)$ of $\mathbb{Q}(\zeta)$ so that $[\mathbb{Q}(\beta) : \mathbb{Q}] = d$ where $d \,|\, (p-1)$.

(6) Let K be finite extension of $\mathbb{Q}$. Show that K contains only a finite number of roots of unity.

(7) Suppose $A \in \mathbb{C}^{n\times n}$ and $A^k = I$. for some integer $k \in \mathbb{N}$. Show that A can be diagonalized. Prove that the matrix $A = \begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix}$ where $\alpha \in K$ and K is a field of chracteristic p satisfies $A^p = I$ and cannot be diagonalized if $\alpha \neq 0$.

(8) Show that $\Phi_n(x) = x^{\phi(n)}\Phi_n(1/x)$ and deduce that the coefficients of $\Phi_n(x)$ satisfy $a_k = a_{\phi(n)-k}$ for all $0 \le k \le \phi(n)$.

(9) Establish the following formulas:
   (a) $\Phi_n(x) = \Phi_m(x^{n/m})$ where m is the product of distinct prime factors of n.
   (b) $\Phi_{pn}(x) = \Phi_n(x^p)/\Phi_n(x)$ where p is coprime to n.
   (c) $\Phi_{2n}(x) = \Phi_n(-x)$ where $n \ge 1$ is an odd integer.

(10) Let ζ, η and ω denote the primitive fifteenth, fifth and cube roots of unity.
   (a) Describe all the automorphisms in $G := G(\mathbb{Q}(\zeta)/\mathbb{Q})$.
   (b) Show that G is isomorphic to a direct product of two cyclic groups. Construct this isomorphism.
   (c) Show that $\mathbb{Q}(\omega)$, $\mathbb{Q}(\zeta)$, $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\omega, \sqrt{5})$ are subfields of $\mathbb{Q}(\zeta)$.
   (d) Make the Galois correspondence between the subfields of $\mathbb{Q}(\zeta)$ and subgroups of G explicit.