Yale University Department of Mathematics
Math 370 Fields and Galois Theory
Spring 2019

Problem Set # 8 (due in class on Thursday April 4)

Problems with roots of unity:

1. For $n \geq 0$, let $\phi_n = \zeta_{2^{n+2}}$ and $\xi_n = \phi_n + \overline{\phi}_n$. Let $K_n = \mathbb{Q}(\phi_n)$ and $K_n^+ = \mathbb{Q}(\xi_n)$.

(a) Prove that $[K_n : K_n^+] = 2$ and $[K_n^+ : \mathbb{Q}] = 2^n$. You may use the fact that $[K_n : \mathbb{Q}] = 2^{n+1}$.

(b) Determine the quadratic equation that ϕ_n satisfies over K_n^+ in terms of ξ_n.

(c) Prove that $\xi_{n+1}^2 = 2 + \xi_n$, and hence that

$$\xi_n = \sqrt{2 + \sqrt{2 + \sqrt{\cdots + \sqrt{2}}}}$$

where there are n nested square roots. This provides an explicit presentation for the 2-power roots of unity, showing that they are constructible (which we already knew).

(d) Prove that $K_n/\mathbb{Q}$ is Galois with group $(\mathbb{Z}/2^{n+2}\mathbb{Z})^\times$ and that $K_n^+/\mathbb{Q}$ is Galois with group cyclic of order 2^n. **Hint.** Recall the isomorphism $(\mathbb{Z}/2^{n+2}\mathbb{Z})^\times \cong C_2 \times C_{2^n}$, where C_m is a (multiplicativly written) cyclic group of order m.

2. Let p be an odd prime number, $\zeta = \zeta_p$, and $K = \mathbb{Q}(\zeta)$. We know that $K/\mathbb{Q}$ is a Galois extension with (cyclic) group $G \cong (\mathbb{Z}/p\mathbb{Z})^\times$ and let $\sigma \in G$ be a generator. Let $H \subset G$ be the unique subgroup of index 2. Define

$$\eta_0 = \sum_{\tau \in H} \tau(\zeta), \qquad \eta_1 = \sum_{\tau \in G \smallsetminus H} \tau(\zeta).$$

These are called the **periods** of ζ with respect to H.

(a) Prove that $\sigma(\eta_0) = \eta_1$ and $\sigma(\eta_1) = \eta_0$ and that

$$\eta_0 = \sum_{a \text{ square}} \zeta^a, \qquad \eta_1 = \sum_{a \text{ nonsquare}} \zeta^a$$

where the sums are taken over the set of squares and nonsquares, respectively, in $(\mathbb{Z}/p\mathbb{Z})^\times$.

(b) Prove that $\eta_0 + \eta_1 = -1$, and more generally, that $\sum_{\tau \in G} \tau(\zeta^a) = -1$ for any a with $p \nmid a$.

(c) Let $g = \sum_{i=0}^{p-1} \zeta^{i^2}$ be the classical **Gauss sum**. Prove that

$$g = \sum_{i=0}^{p-2} (-1)^i \sigma^i(\zeta) = \eta_0 - \eta_1.$$

(d) Prove that $\tau(g) = g$ if $\tau \in H$ and $\tau(g) = -g$ if $\tau \in G \smallsetminus H$. Conclude, using the Galois correspondence, that $[\mathbb{Q}(g) : \mathbb{Q}] = 2$. Also conclude that $\overline{g} = g$ if -1 is a square modulo p and that $\overline{g} = -g$ if -1 is not a square modulo p, where the overline is complex conjugation. **Hint.** For the last part, recall that inversion is the same as complex conjugation for any root of unity.

(e) Prove that $g\overline{g} = p$. **Hint.** Massage $g\overline{g}$ to be the double sum $\sum_{k=0}^{p-2} (-1)^k \sum_{j=0}^{p-2} \sigma^j(\sigma^k(\zeta)/\zeta)$, then use part (b).

(f) Prove that $g^2 = (-1)^{(p-1)/2} p$.

(g) Finally, conclude that $\mathbb{Q}(\sqrt{(-1)^{(p-1)/2} p})$ is the unique quadratic subfield of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$.