Graduate Algebra
Homework 8

Due 2015-04-08

1. Suppose n is an odd integer. Show that $\Phi_{2n}(X) = \Phi_n(-X)$.

   Proof. Let $\zeta_m = e^{2\pi i/m}$. Note that $\zeta_{2n} = -\zeta_n$. Chinese remainder gives $(\mathbb{Z}/2n\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/n\mathbb{Z})^\times$ and so the primitive $2n$-th roots $= \{\zeta_{2n}^k | 1 \leq k \leq 2n, (k, 2n) = 1\} = \{-\zeta_n^k | 1 \leq k \leq 2n, (k, 2n) = 1\} = \{-\zeta_n^k | 1 \leq k \leq n, (k, n) = 1\}$. Thus

   $$\Phi_{2n}(X) = \prod (X - \zeta_{2n}^k) = \prod (X + \zeta_n^k) = (-1)^{\varphi(n)} \prod (-X - \zeta_n^k) = (-1)^{\varphi(n)} \Phi_n(-X)$$

   thus it suffices to show that $\varphi(n)$ is even. But n is odd and if p^m is the largest power of a prime divisor p of n then $\varphi(p^m) = (p-1)p^{m-1} \mid \varphi(n)$ by the Chinese remainder theorem. This is clearly even.

   Alternatively you may use the Mobius inversion formula for Φ_m to prove the relation by induction. $\square$

2. Let $K = \mathbb{Q}(i, \sqrt[8]{2})$ be the splitting field of $X^8 - 2$ over $\mathbb{Q}$. Show that $\mathrm{Gal}(K, \mathbb{Q}(i))$ is the cyclic group $\mathbb{Z}/8\mathbb{Z}$, $\mathrm{Gal}(K/\mathbb{Q}(\sqrt{2})) \cong D_8$ and $\mathrm{Gal}(K/\mathbb{Q}(i\sqrt{2})) \cong Q_8$. [Hint: You might find your job easier if you recall presentations for these groups.]

   Proof. Note that $\zeta_8 = (1+i)/\sqrt{2} \in K$ and so $K/\mathbb{Q}$ is Galois. Any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ takes $\alpha = \sqrt[8]{2}$ to $\zeta_8^a \alpha$ and i to $\pm i$.

   First, $K = \mathbb{Q}(i)\mathbb{Q}(\alpha)$ and since $\mathbb{Q}(i)/\mathbb{Q}$ is quadratic we deduce that $[K : \mathbb{Q}] = 16]$.

   $\mathrm{Gal}(K/\mathbb{Q}(i))$. Consider σ taking i to i and α to $\zeta_8\alpha$. Then $\sigma \in \mathrm{Gal}(K/\mathbb{Q}(i))$ and σ has order 8. But $[K : \mathbb{Q}(i)] = 8$ and so the Galois group is cyclic generated by σ.

   $\mathrm{Gal}(K/\mathbb{Q}(\sqrt{2}))$. Let σ take i to $-i$ and fix α and let τ fix i and take α to $i\alpha$. Clearly $\sigma, \tau \in \mathrm{Gal}(K/\mathbb{Q}(\sqrt{2}))$ and $\sigma^2 = 1$, $\tau^4 = 1$. Also $\sigma\tau\sigma = \tau^3$ (both fix i and take α to $-i\alpha$) and so $\langle \sigma, \tau \rangle \cong D_8$ is a subgroup of $\mathrm{Gal}(K/\mathbb{Q}(\sqrt{2}))$. Again both have order 8 so they are isomorphic.

   $\mathrm{Gal}(K/\mathbb{Q}(i\sqrt{2}))$. Let σ fix i and take α to $i\alpha$ and let τ take i to $-i$ and α to $\zeta_8\alpha$. Then it's easy to check that σ and τ fix $i\alpha^4 = i\sqrt{2}$. Also, $\sigma^2 = \tau^2$ both take i to i and α to $-\alpha$ as $\zeta = (1+i)/\alpha^4$. Finally, note that $\sigma\tau\sigma = \tau$ take i to $-i$ and α to $\zeta\alpha$. Finally $\sigma^4 = \tau^4 = 1$ and so $\langle \sigma\tau \rangle \cong Q_8$. Again comparing orders we get the isomorphism. $\square$

3. Let $p > 2$ be a prime and g a generator of $\mathbb{F}_p^\times$. Show that the subextensions $\mathbb{Q}(\zeta_p)/K/\mathbb{Q}$ are all of the form

   $$K_r = \mathbb{Q}\Big(\sum_{i=1}^{(p-1)/r} \zeta_p^{g^{ri}}\Big)$$

   where r ranges over the divisors of $p-1$. [Hint: Compute the Galois group of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/K_r)$. A straightforward problem.]

Proof. $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$. Suppose $a \in \mathbb{F}_p^\times$ fixes $\sum \zeta_p^{g^{ri}}$. Write $a = g^b$. Then $\sum \zeta_p^{g^{ri}} = \sum \zeta_p^{g^{ri+b}}$. Since $\{\zeta_p^{g^j} | 0 \le j < p-1\}$ is a basis of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ it follows that the sets $\{g^{ri} | 1 \le i \le (p-1)/r\}$ and $\{g^{ir+b} | 1 \le i \le (p-1)/r\}$ are equal. Immediately we deduce that $r \mid b$ and if $r \mid b$ then clearly g^b fixes K_r. Thus $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/K_r) \cong \langle g^r \rangle$. The result now follows from the fact that every subgroup of $\mathbb{F}_p^\times$ is cyclic of the form $\langle g^r \rangle$ for some r. $\square$