HW #6 (Solutions)

1) We have $f(x)=\prod_{i=1}^{n}(x-r_i)$, $f'(x)=\sum_{i=1}^{n}\left(\prod_{j\neq i,1\le j\le n}(x-r_j)\right)$

thus $f'(r_k)=\prod_{j\neq k,1\le j\le n}(r_k-r_j)$ since other terms contain r_k-r_k

$(-1)^{\frac{n(n-1)}{2}}\prod_{i=1}^{n}f'(r_i)=(-1)^{\frac{n(n-1)}{2}}\prod_{i=1}^{n}\prod_{j\neq i,1\le j\le n}(r_i-r_j)=\prod_{1\le i\neq j\le n}(r_i-r_j)=d$

Let $\Lambda_p(x)=x^{p-1}+x^{p-2}+\cdots+1$, We have $x^p-1=(x-1)\Lambda_p(x)$

Differentiate both sides and we have $px^{p-1}=\Lambda_p(x)+(x-1)\Lambda_p'(x)$.

The roots of $\Lambda_p(x)$ are ζ_p^i $1\le i\le p-1$

So $(\zeta_p^i-1)\Lambda_p'(\zeta_p^i)=p\cdot\zeta_p^{i(p-1)}$.

$$\prod_{i=1}^{p-1}(\zeta_p^i-1)\cdot\prod_{i=1}^{p-1}\Lambda_p'(\zeta_p^i)=p^{p-1}\cdot\zeta_p^{(p-1)\frac{p(p-1)}{2}}$$

$$(-1)^{\frac{p-1}{2}}=p^{p-1}\cdot\zeta_p^{\frac{p^2(p-1)}{2}}$$

Case I. $p=2$, $\zeta_2-1=-2$ $\zeta_2^{\frac{p^2(p-1)}{2}}=-1$

$$d=-1=-1^{2\cdot(1-1/2)}\cdot 2^{2-2}$$

Case II. $p>2$, In this case p is odd, $p-1$ is even

$$\zeta_p^{\frac{(p-1)p(p-1)}{2}}=(\zeta_p^p)^{\frac{(p-1)^2}{2}}=1$$

$$\prod_{i=1}^{p-1}(\zeta_p^i-1)=\sum_{k=0}^{p-1}(-1)^{p-k}\sum_{1\le i_1<\cdots<i_k\le p-1}\zeta_p^{i_1}\cdots\zeta_p^{i_k}$$

$$=\sum_{k=0}^{p-1}(-1)^{p-1-k}\cdot(-1)^k$$

$$=\sum_{k=0}^{p-1}1=p.$$

$$d=(-1)^{\frac{p(p-1)}{2}}\cdot\prod_{i=1}^{p-1}\Lambda_p'(\zeta_p^i)=(-1)^{\frac{p(p-1)}{2}}\cdot p^{p-1}/p=(-1)^{\frac{p(p-1)}{2}}\cdot p^{p-2}$$

---

2) $E=\mathbb{Q}(\sqrt{d})$ is a quadratic subfield of Λ_p.

Notice that $\mathrm{Aut}(\Lambda_p/\mathbb{Q})=\mathbb{Z}_p^*$ is cyclic, its subgroup of deg 2 is unique

$\Rightarrow$ the quadratic subfield of Λ_p is unique

When $p=4n+1$, $d=p^{p-2}>0$ $\sqrt{d}\in\mathbb{R}$, $E\subset\mathbb{R}$.

When $p=4n+3$, $d=-p^{p-2}<0$ $\sqrt{d}\in\mathbb{R}$, $E\not\subset\mathbb{R}$

---

3) Since L/F is normal, $L=\mathrm{Inv}N$, so $N\trianglelefteq G$. By Prob #1, we have

$\mathrm{Inv}(H\cap N)=f(K,L)=E$, so $H\cap N=\{1\}$

Also, $G=\mathrm{Aut}(K\cap L)=\langle H,N\rangle=HN$ (since $N\trianglelefteq G$), we have

a short exact sequence $1 \to N \xrightarrow{n \mapsto n} G \xrightarrow{} H \to 1$

$h_n \mapsto h$ well defined by $H \cap N = \{1\}$

So we get $G = N \rtimes H$.

If K/F and L/F are normal, we have $H \lhd G$, $N \lhd G$, so the short exact seq splits, then $G = H \times N$

P271 #4. We know that if $n = p_1^{e_1} \cdots p_k^{e_k}$, $\mathbb{Z}_n = \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}$

First consider $\mathbb{Z}_{p^e}$

Case I. $p = 2$ By thm 4.21 $Gal_{\mathbb{Q}}(\lambda_{2^{e+1}}) = \mathbb{Z}_2 \times \mathbb{Z}_{2^e}$ and we have a subf F of the SFE of $\lambda_{2^{e+1}}$. $Aut(F/\mathbb{Q}) \cong \mathbb{Z}_{2^e}$.

Case II. $p \neq 2$, $Gal_{\mathbb{Q}}(\lambda_{p^{e+1}}) = \mathbb{Z}_{p^{e+1}}^* = \mathbb{Z}_{p^e(p-1)}$ and $\mathbb{Z}_{p^e} < \mathbb{Z}_{p^e(p-1)}$, so we hav a subfield F of the SFE of $\lambda_{p^{e+1}}$. $Aut(F/\mathbb{Q}) \cong \mathbb{Z}_{p^e}$

In conclusion, for each $p_i^{e_i}$, we have F_i s.t. $Aut(F_i/\mathbb{Q}) \cong \mathbb{Z}_{p_i^{e_i}}$

Notice that $F_i \subset \mathbb{Q}(\zeta_{p_i^{e_i+1}})$ if $i \neq j$, $F_i \cap F_j = \mathbb{Q}$

Consider $F = \mathbb{Q}(\{F_i\})$ by P243 #2, we have $Aut(F/\mathbb{Q}) = \mathbb{Z}_{p_1^{e_1}} \times \cdots \mathbb{Z}_{p_n^{e_n}} = \mathbb{Z}_n$

4) For an algebraic $u \neq 0$, notice $\sin u = \frac{1}{2i}(e^{iu} - e^{-iu})$, $(e^{iu})^2 - 2i\sin u e^{iu} - 1 = 0$ so e^{iu} is also algebraic since the field of algebraic numbers is algebraic closed. This contradicts to Lindemann-Weierstrass Thm 515

5) $Gal_{\mathbb{Q}}(x^4+1) = Aut(\mathbb{Q}(\zeta_8)/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ by thm 4.21

$Gal_{\mathbb{Q}}(x^5+1) = Aut(\mathbb{Q}(\zeta_{10})/\mathbb{Q}) \cong \mathbb{Z}_{10}^* \cong \mathbb{Z}_4$ 515

Since $p^k \equiv_{(m)} 1$ $\xi^{p^k} - \xi = 0$, so $[\mathbb{Z}_p(\xi) : \mathbb{Z}_p] \leq k$.

OTOH, $\sigma : \xi \mapsto \xi^p \in Aut(\mathbb{Z}_p(\xi)/\mathbb{Z}_p)$ and $|\langle \sigma \rangle| = k$, so $[\mathbb{Z}_p(\xi) : \mathbb{Z}_p] \geq k$

515

6. a. We know from theorem 4.26 that the Frobenius automorphism generates the Galois group. It suffices to find the order of ω under the map $a \to a^p$. This is clearly the same as the order of $\bar{p}$ in the group $\mathbb{Z}_m^*$, as we want to know what is the smallest power of p greater than 1 such that $p^e = 1 \bmod m$.

   b. We know λ_m as $\phi(m)$ roots given by the mth primitive roots of unity, and the derivative test shows these roots are distinct. If the polynomial is irreducible, then the splitting field is a Galois extension and has degree $\phi(m)$. This is equal to the order of the Galois group, which is generated by the Frobenius automorphism, so the Frobenius automorphism must have order $\phi(m)$. By the reasoning above, $\bar{p}$ has full order in $\mathbb{Z}_m^*$ and generates it.

   Suppose $\bar{p}$ generates $\mathbb{Z}_m^*$. Then the Frobenius automorphism $a \to a^p$ has order equal to the degree of λ_m. The Frobenius automorphism is an automorphism of the splitting field that fixes the base field, and from the remarks at the top of page 236 we see $|G|$ is less than or equal to the degree of the splitting field. Since $|G| = \phi(m)$ and the degree of the splitting field is at most $\phi(m)$ (as adjoining one primitive root gets all mth roots of unity), we have equality.

   c. By the above λ_m is irreducible if and only if $\mathbb{Z}_4^*$ is generated by $\bar{p}$. When $p \neq 2$, this is the case if and only if p is 3 mod 4. It has 1 as a root when $p = 2$ and is reducible there.

   Again, λ_8 is irreducible if and only if $\mathbb{Z}_8^*$ is generated by $\bar{p}$. But this multiplicative group is never cyclic, so it is never the case it is irreducible (because when $p = 2$ it has 1 as a root, which can be factored out).

7. By the above problem, it suffices to determine if $\mathbb{Z}_{18}^*$, which has $\phi(18) = 6$ elements, is generated by $\bar{p}$. Observe that 5 is a generator, so the only generators are 5 and $5^5 = 11$.

   a. Here 23 is 5 mod 18 and hence a generator, so it is irreducible.

   b. Note 43 is 7 mod 18 and not a generator, so it is reducible.

   c. Note 73 is 1 mod 18 and clearly not a generator, so it is reducible.

8. Let $L = K(\alpha_1, \ldots, \alpha_n, t_1, \ldots, t_j)$ where the α_i are algebraic over K and the t_i are transcendental. Let T be a maximal subset of the t_i so that T is algebraically independent over K. Then T is a transcendence basis since $L/K(T)$ is algebraic. We now see that $L = K(T, \alpha_1, \ldots, \alpha_n)$, so it is finite dimensional over $K(T)$ since each α_i is algebraic. Let this finite dimension be d.

   Suppose K_α is not finitely generated and hence not finite. Then we can find $d+1$ algebraic elements α_i in L linearly independent over K. Then they are also linearly independent over $K(T)$. Suppose not. Then there is some linear combination $\sum c_i \alpha_i = 0$ with $c_i \in T$ and not all c_i contained in K. Suppose without loss of generality that some c_i term contains t_1 terms. Clearing denminators if needed, this shows that t_1 is algebraic over $K(T \backslash t_1)$. Then L is algebraic over $K(T/t_1)$, and we have produced a small transcendence basis. This is a contradiction, as transcendence degree is well-defined.

   But now we have $d+1$ elements of L linearly independent over $K(T)$, which is absurd.

9. a. Suppose first that n has no repeated prime factors and that the prime factors are p_i. Then every primitive nth root of unity can be written as a product of powers of p_ith roots of unity. That is, $\xi = \prod \xi_{p_i}^{e_i}$ for $e_i \in \mathbb{Z}_{p_i}^*$. Clearly all Galois conjugates are given by the e_i running through all possible values. It suffices to show this is a basis. By the proof of the tower theorem, it suffices to show that the primitive p_ith roots of unity form a basis for $\mathbb{Q}(\xi_{p_i}, \xi_{p_{i-1}}, \ldots, \xi_{p_1})$ over $\mathbb{Q}(\xi_{p_{i-1}}, \ldots, \xi_{p_1})$. Then the result follows by induction, since the base case is trivial. Note that this is equivalent to showing that ξ_{p_i} is a primitive element for the extension and the extension has degree $p-1$, since then $1, \xi_{p_i}, \ldots \xi_{p_i}^{p-2}$ will be a basis for the extension, which is equivalent to $\xi_{p_i}, \ldots \xi_{p_i}^{p-2}, \xi_{p_i}^{p-1}$ being a basis (since the sum of the primitive pth roots is 1). That it is a primitive element is obvious.

   If $m = \prod_1^i p_k$, then the top field is the splitting field for λ_m. This is irreducible and has degree $\phi(m) = \prod_1^i (p_k - 1)$. The lower field is the splitting field of λ_{m/p_i} and has degree $\prod_1^{i-1}(p_k - 1)$. Hence the extension has degree $p_i - 1$.

   b. Suppose that n has repeated prime factors, so that $n = \prod p_i^{e_i}$ where, without loss of generality, $e_1 > 1$. Then if ξ_n is a primitive nth root of unity, we have $\xi_n = \prod \xi_{p_i^{e_i}}^{j_i}$. Let $\omega_m = \xi_{p_1}^m \prod_{i>1} \xi_{p_i^{e_i}}^{j_i}$. Then

$$\omega_1(1 + \omega_{p_1} + \omega_{2p_1} + \ldots) = 0$$

   and each term is a primitive nth root of unity, since the exponent is in the multiplicative group mod $p_1^{e_1}$, so they are not linearly independent.

   An example makes this much clearer. If ξ is a 9th root of unity, we have $\xi(1 + \xi^3 + \xi^6) = 0$, since ξ^3 is a third root of unity, and if ω is a nth root of unity, $1 + \omega + \cdots + \omega^{n-1} = 0$. The above sum is just this repeated for the general case.