Math 901

Solutions to Homework # 3

1. Let $E$ be the splitting field of $f(x) = x^6 + 3 \in \mathbb{Q}[x]$ and let $\alpha \in E$ be a root of $f(x)$.

(a) Prove that $E = \mathbb{Q}(\alpha)$. (Hint: Note that $\frac{1+\sqrt{3}i}{2}$ is a primitive 6th root of unity.)

(b) Let $G$ be the Galois group of $E/\mathbb{Q}$. Determine, with justification, whether $G$ is abelian.

Solution: For part (a), the roots of $f(x)$ are $\omega^i \alpha$ for $i = 0, \ldots, 5$, where $\omega$ is a primitive 6th root of unity. Then $E = \mathbb{Q}(\omega, \alpha)$. But $(\alpha^3)^2 = -3$, so $\alpha^3 = \pm \sqrt{3}i$. Without loss of generality, assume $\alpha^3 = \sqrt{3}i$. Since $\frac{1+\sqrt{3}i}{2}$ is a primitive 6th root of unity, we see that $\omega \in \mathbb{Q}(\alpha)$. Hence, $E = \mathbb{Q}(\alpha)$.

For part (b), note that as $E = \mathbb{Q}(\alpha)$ and $x^6 + 3$ is irreducible over $\mathbb{Q}$ (by Eisenstein), we have $[E : \mathbb{Q}] = 6$. Thus $G = \text{Gal}(E/\mathbb{Q})$ has order 6. For each $i = 0, \ldots, 5$, let $\sigma_i : E \to E$ be given by $\sigma_i(\alpha) = \omega^i \alpha$. These are well-defined since $\alpha$ and $\omega^i \alpha$ are both roots of $x^6 + 3$. Thus, $G = \{\sigma_i \mid i = 0, \ldots, 5\}$. Note that for each $j \geq 0$:

$$\sigma_j(\omega) = \sigma_j(\frac{1+\sqrt{3}i}{2}) = \sigma_j(\frac{1 + \alpha^3}{2}) = \frac{1 + \sigma_j(\alpha)^3}{2} = \frac{1 + \omega^{3j} \alpha^3}{2} = \frac{1 + (-1)^j \sqrt{3}i}{2}.$$ 

Hence, $\sigma_j(\omega) = \omega^5$ if $j$ is odd and $\sigma_j(\omega) = \omega$ if $j$ is even. Now,

$$\sigma_2 \sigma_1(\alpha) = \sigma_2(\omega \alpha) = \sigma_2(\omega) \sigma_2(\alpha) = \omega \cdot \omega^2 \alpha = \omega^3 \alpha.$$ 

Also,

$$\sigma_1 \sigma_2(\alpha) = \sigma_1(\omega^2 \alpha) = \sigma_1(\omega)^2 \sigma_1(\alpha) = (\omega^5)^2 \cdot \omega \alpha = \omega^5 \alpha.$$ 

Hence, $\sigma_1 \sigma_2 \neq \sigma_2 \sigma_1$ and $G$ is not abelian.

2. Let $E/F$ be a finite Galois field extension with Galois group $G$. Let $\alpha \in E$ and $H$ the Galois group of $E/F(\alpha)$. Let $\sigma_1, \ldots, \sigma_n$ be a complete set of coset representatives for $H$ in $G$. (I.e., $n = [G : H]$ and $\sigma_i H \neq \sigma_j H$ for all $i \neq j$.) Prove that the minimal polynomial of $\alpha$ over $F$ is $\prod_{i=1}^n (x - \sigma_i(\alpha))$.

Solution: Let $f(x) = \prod_{i=1}^n (x - \sigma_i(x))$. Clearly, $f(x)$ is monic and $\deg f = [G : H] = [F(\alpha) : F]$. Let $\sigma_1$ be the coset representative for $H$; i.e., $\sigma_1 \in H$. Then $\sigma_1(\alpha) = \alpha,$
4. Let \( E/F \) be a finite Galois extension and \( K \) an intermediate field. Let \( G = \text{Gal}(E/F) \) and \( H = \text{Gal}(E/K) \). Prove that \( N_G(H) = \{ g \in G \mid g(K) = K \} \) and \( N_G(H)/H \cong \text{Aut}(K/F) \).

**Solution:** Suppose \( g \in N_G(H) \) and \( h \in H \). Since \( g^{-1}hg \in H \) then \( g^{-1}hg \) restricted to \( K \) is the identity map. For \( k \in K, k = (g^{-1}hg)(k) \), so \( g(k) = h(g(k)) \). Since this holds for all \( h \in H \), we see that \( g(k) \in E_H = K \) for all \( k \in K \). Thus, \( g(K) \subseteq K \). As \( K/F \) is algebraic, we have \( g(K) = K \). Conversely, suppose \( g(K) = K \). Let \( h \in H \). To show \( g^{-1}hg \in H \) it suffices to show that \( (g^{-1}hg)(k) = k \) for all \( k \in K \). But as \( g(k) \in K, h(g(k)) = g(k) \). Hence, \( g^{-1}h(g(k)) = (g^{-1}g)(k) = k \). Thus, \( g \in N_G(H) \).

For the second statement, define a map \( \phi : N_G(H) \to \text{Aut}(K/F) \) by restriction to \( K \). This map is well-defined by the first part of the problem. Clearly, \( \phi \) is a group homomorphism. Any \( \sigma \in \text{Aut}(K/F) \) can be extended to an element \( \tau \in G \). Then \( \phi(\tau) = \sigma \) and we have that \( \phi \) is surjective. Finally, \( \sigma \in \ker \phi \) if and only if \( \sigma \) fixes \( K \), which is if and only if \( \sigma \in H \). The desired isomorphism now follows.

5. Let \( K \subseteq E, F \subseteq L \) are fields and suppose \( E/K \) is finite and Galois. Prove that \( EF/F \) is Galois and \( \text{Gal}(EF/F) \) is isomorphic to a subgroup of \( \text{Gal}(E/K) \).

**Solution:** As \( E/K \) is finite and separable, \( E = K(\alpha) \). Let \( f(x) = \text{Min}(\alpha, K) \). Then \( E \) is the splitting field of \( f(x) \) over \( K \). Now \( EF = F(\alpha) \). As \( \alpha \) is separable over \( K \), \( \alpha \) is separable over \( F \). Thus, \( EF/F \) is separable. Also, \( EF \) is the splitting field for \( f(x) \) over \( F \), so \( EF/F \) is normal and hence Galois. Now define \( \phi : \text{Gal}(EF/F) \to \text{Gal}(E/K) \) by restriction to \( E \). Then \( \phi \) is a well-defined group homomorphism. If \( \sigma \in \ker \phi \) then \( \sigma \) restricted to \( E \) is the identity map. Since \( \sigma \) restricted to \( F \) is the identity map, we obtain that \( \sigma \) is the identity map on \( EF \). (See, for example, Problem \# 3 from Homework \# 1.) Thus, \( \ker \phi = \{ 1 \} \) and \( \phi \) is injective.
Let $F$ be a field and $f(x) \in F[x]$ a separable irreducible polynomial of prime degree. Let $\alpha$ be a root of $f(x)$ and suppose $f(x)$ has at least two roots in $E = F(\alpha)$. Prove that $E$ is the splitting field for $f(x)$ and that $E/F$ is cyclic. (Hint: Let $L$ be the normal closure of $E/F$, $G = \text{Gal}(L/F)$, and $H = \text{Gal}(L/E)$. Prove that $H \neq N_G(H)$.)

**Solution:** Let $\beta \neq \alpha$ be a root of $f(x)$ in $E = F(\alpha)$. As $f(x)$ is irreducible, $E = F(\beta)$ as well. Also, there exists an automorphism $\sigma$ of $E$ which fixes $F$ and sends $\alpha$ to $\beta$. Extend $\sigma$ to an element $\tau \in G$. As $\tau(E) = E$, $\tau \in N_G(H)$ by Problem #4. Moreover, as $\tau$ does not fix $E$, $\tau \not\in H$. Hence, $H$ is a proper subgroup of $N_G(H)$. Now, $[G : H] = [E : F] = p$ (the degree of $f(x)$), so $[G : N_G(H)] = 1$. Hence, $H$ is normal in $G$, which implies $E$ is normal over $F$. Hence, $E = L$ and $G$ has prime order.

Let $E$ be a finite extension of a finite field $F$. Prove that $\text{Tr}_E^F$ and $\text{N}_E^F$ are surjective (as maps from $E$ to $F$). (Recall from Math 818 that $E/F$ is a cyclic extension.)

**Solution:** As finite fields are perfect, $E/F$ is separable. Thus, $\text{Tr}_E^F$ is nonzero. As $\text{Tr}_E^F$ is a linear transformation of $F$-vector spaces from $E$ to $F$, and $F$ is one-dimensional, we see that $\text{Tr}_E^F$ is surjective. For the norm, clearly $\text{N}_E^F(\alpha) = 0$ if and only if $\alpha = 0$. Let $\phi$ be $\text{N}_E^F$ restricted to $E^* = E \setminus \{0\}$. It suffices to prove that $\phi : E^* \to F^*$ is surjective. As $\phi$ is a group homomorphism, it is enough to prove that $|E^*|/|K| = |F^*|$, where $K = \ker \phi$. Let $G = \langle \sigma \rangle$. By Hilbert’s Satz 90, $K = \{ \frac{\alpha}{\sigma(\alpha)} \mid \alpha \in E^* \}$. Now, $K$ is the image of the group homomorphism $f : E^* \to E^*$ given by $f(\alpha) = \frac{\alpha}{\sigma(\alpha)}$. Note that $\alpha \in \ker f$ if and only if $\sigma(\alpha) = \alpha$, which holds if and only if $\alpha \in F^*$ (as $F = E_\sigma$). Hence, $|K| = |E^*|/|F^*|$ and so $|E^*|/|K| = |F^*|$. 