Math 901

Solutions to Exam # 1

Section III

5. Let $E$ be the splitting field for $x^8 - 1$ over $\mathbb{Q}$. Find (explicitly) the elements of the Galois group of $E/\mathbb{Q}$ and find (with justification) primitive elements for each of the intermediate fields of $E/\mathbb{Q}$.

**Solution:** The roots of $x^8 - 1$ are just the 8th roots of unity. Let $\omega$ be a primitive 8th root of unity. Then $E = \mathbb{Q}(\omega)$. We also know from a result in class that $G = \text{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}_8^*$. Let $\phi$ be an element of $G$. Then $\phi$ is determined by $\phi(\omega)$. Further, $\phi(\omega)$ must be a primitive 8th root of unity, which are $\omega, \omega^3, \omega^5, \omega^7$. Since $|G| = 4$, all four primitive 8th roots of unity determine legitimate automorphisms of $E/\mathbb{Q}$. Let $\sigma$ be the element of $G$ defined by $\sigma(\omega) = \omega^3$ and $\tau$ the element of $G$ given by $\tau(\omega) = \omega^5$. Then $(\sigma\tau)(\omega) = (\tau\sigma)(\omega) = \omega^7$. Further, $\sigma^2 = \tau^2 = (\sigma\tau)^2 = 1$, the identity map on $E$. Thus, $G = \{1, \sigma, \tau, \sigma\tau\}$, the Klein-4 group. The intermediate fields of $E/\mathbb{Q}$ correspond to the subgroups of $G$. The nontrivial subgroups of $G$ are $\langle \sigma \rangle$, $\langle \tau \rangle$, and $\langle \sigma\tau \rangle$. Note that as $|\sigma| = 2$, $\omega + \sigma(\omega) = \omega + \omega^3 \in E_\sigma$. Thus, $\mathbb{Q}(\omega + \omega^3) \subseteq E_\sigma$. Further, $\omega$ is a root of $(x - \omega)(x - \omega^3) = x^2 - (\omega + \omega^3) - 1 \in \mathbb{Q}(\omega + \omega^3)[x]$. Hence, $[E : \mathbb{Q}(\omega + \omega^3)] \leq 2$. Since, $[E : E_\sigma] = |\sigma| = 2$, we see that $E_\sigma = \mathbb{Q}(\omega + \omega^3)$. In almost identical fashion, one can show that $E_{\sigma\tau} = \mathbb{Q}(\omega + \omega^7)$. For $\langle \tau \rangle$, notice that $\tau(\omega^2) = (\tau(\omega))^2 = \omega^{10} = \omega^2$. Thus, $\omega^2 \in E_\tau$. If one notices that $\omega^2 = \pm i$, then one sees that $[\mathbb{Q}(\omega^2) : \mathbb{Q}] = 2$ and hence $E_\tau = \mathbb{Q}(\omega^2)$. Alternatively, one can observe that $\omega$ is a root of $(x - \omega)(x + \omega) = x^2 - \omega^2 \in \mathbb{Q}(\omega^2)[x]$. Thus, as above, we have that $[E : \mathbb{Q}(\omega^2)] \leq 2$ and $E_\tau = \mathbb{Q}(\omega^2)$.

6. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree 7 and $E$ its splitting field. Let $G$ be the Galois group of $E/\mathbb{Q}$ and suppose $[E : \mathbb{Q}] = 21$. Prove that $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$ for every pair of distinct roots $\alpha, \beta$ of $f(x)$ (Hint: First argue that $G$ cannot be abelian.)

**Solution:** Let $\alpha \in E$ be a root of $f(x)$. Then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 7$. If $G$ is abelian, then every intermediate field of $E/\mathbb{Q}$ is normal over $\mathbb{Q}$, and so $\mathbb{Q}(\alpha)$ would be the splitting field of $f(x)$. This contradicts that $E$ is the splitting field and $[E : \mathbb{Q}] = 21$. So $G$ is nonabelian. Let $P$ be a Sylow 3-subgroup of $G$ and $Q$ a Sylow 7-subgroup of $G$. By Sylow’s Theorems, we have that $Q$ is normal in $G$. If $P$ is also normal, then $G$ would be cyclic, a contradiction. Hence, $P$ is not normal. Since $[G : P] = 7$ and $P \leq N_G(P) \neq G$, we must have $N_G(P) = P$. Now, suppose $L = \mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$ for two distinct roots $\alpha$ and $\beta$ of $f(x)$. Then $\text{Aut}(L/\mathbb{Q}) \neq \{1\}$, as there exists an automorphism of $L$ sending $\alpha$ to $\beta$. Let $H = \text{Gal}(E/L)$. Then $|H| = 3$, a Sylow 3-subgroup. By a homework problem (in fact, Problem # 3 on this exam), we have $N_G(H)/H \cong \text{Aut}(L/\mathbb{Q})$. But this contradicts that $N_G(H) = H$ for every Sylow 3-subgroup of $G$. Thus, $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$ for every pair of distinct roots $\alpha$ and $\beta$ of $f(x)$. 
7. Let $E/\mathbb{Q}$ be an algebraic field extension and suppose every irreducible polynomial in $\mathbb{Q}[x]$ has a root in $E$. Prove that $E$ is algebraically closed. (Hint: Use the primitive element theorem on an appropriate splitting field.)

**Solution:** Fix some algebraic closure $\overline{E}$ of $E$. It suffices to show that $\overline{E} = E$. Let $\alpha \in \overline{E}$. Then $\alpha$ is algebraic over $\mathbb{Q}$. Let $f(x) \in \mathbb{Q}[x]$ be the minimal polynomial of $\alpha$ over $\mathbb{Q}$ and $L$ the splitting field for $f(x)$ over $\mathbb{Q}$. Note that $\alpha \in L$. As $L/\mathbb{Q}$ is finite and separable (characteristic zero), there exists $\beta \in L$ such that $L = \mathbb{Q}(\beta)$ by the Primitive Element Theorem. Finally, let $h(x)$ be the minimal polynomial of $\beta$ over $\mathbb{Q}$. Note that since $L$ is normal over $\mathbb{Q}$, $h(x)$ splits in $L$ and in fact $L = \mathbb{Q}(\gamma)$ for every root $\gamma$ of $h(x)$. (Note that as $h(x)$ is irreducible, $[L : \mathbb{Q}] = [\mathbb{Q}(\beta) : \mathbb{Q}] = [\mathbb{Q}(\gamma) : \mathbb{Q}]$ for every root $\gamma$ of $h(x)$.) But by hypothesis, $h(x)$ has a root in $E$. Hence, $\alpha \in L \subseteq E$.

8. Let $E/\mathbb{Q}$ be a finite Galois extension whose Galois group is simple and nonabelian. Suppose there exists a prime $p$ and an element $\alpha \in E$ such that $\alpha^p \in \mathbb{Q}$. Prove that $\alpha \in \mathbb{Q}$. (Hint: Let $\beta = \alpha^p$. Then the minimal polynomial of $\alpha$ over $\mathbb{Q}$ divides $x^p - \beta$. Find the roots of this polynomial.)

**Solution:** Let $\beta = \alpha^p$ as in the hint. The roots of $f(x) = x^p - \beta$ are $\omega^i\alpha$, for $i = 0, \ldots, p-1$, where $\omega$ is a primitive $p$th root of unity. Let $g(x)$ be the minimal polynomial of $\alpha$ over $\mathbb{Q}$. If $\deg g(x) = 1$ then $\alpha \in \mathbb{Q}$ and we are done. So suppose $\deg g \geq 2$. As $g(x)$ divides $f(x)$, we must have $\omega^i\alpha$ is a root of $g(x)$ for some $i = 1, \ldots, p-1$. Since $E/\mathbb{Q}$ is normal and $g(x)$ has a root (namely, $\alpha$) in $E$, $g(x)$ splits in $E$. Thus, $\omega^i\alpha \in E$. Since $\alpha \in E$, we obtain that $\omega^i \in E$. Now, $\omega^i$ is also a primitive $p$th root of unity (as $\gcd(i, p) = 1$), so $\mathbb{Q}(\omega^i) = \mathbb{Q}(\omega)$ is a subfield of $E$. Since $\mathbb{Q}(\omega)$ is the splitting field for $x^p - 1$ over $\mathbb{Q}$, we have that $\mathbb{Q}(\omega)/\mathbb{Q}$ is a normal extension.

Then $H = \text{Gal}(E/\mathbb{Q}(\omega))$ is a normal subgroup of $G = \text{Gal}(E/\mathbb{Q})$. Since $G$ is simple, we must have $H = \{1\}$ or $H = G$.

Suppose first that $H = \{1\}$. Then $E = \mathbb{Q}(\omega)$. But then $G = \text{Gal}(\mathbb{Q}(\omega))/\mathbb{Q}) \cong \mathbb{Z}_p^*$, which is abelian, a contradiction.

Now suppose $H = G$. Then $\mathbb{Q}(\omega) = \mathbb{Q}$, which implies $p = 2$ (as $[\mathbb{Q}(\omega) : \mathbb{Q}] = \phi(p) = p - 1$). Then $\alpha$ is a root of $x^2 - \beta \in \mathbb{Q}[x]$. As we are assuming $\alpha \notin \mathbb{Q}$, we have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$. Thus, $\mathbb{Q}(\alpha)/\mathbb{Q}$ is a normal extension. Since $G$ is simple, there are no intermediate fields which are normal over $\mathbb{Q}$ except $E$ and $\mathbb{Q}$. Thus, we must have $E = \mathbb{Q}(\alpha)$. But then $|G| = 2$ and $G$ is abelian, a contradiction.

Hence, $\deg g = 1$ and $\alpha \in \mathbb{Q}$.