Let $K \subseteq L$ be fields, $f(x)$ be a polynomial in $K[x]$, $\sigma \in \text{Aut}_K L$, and $\ell \in L$. Suppose that $f(\ell) = 0$. Prove $f(\sigma(\ell)) = 0$. Give all details.

Let $f(x) = \sum_{j=0}^{n} k_j x^j$, with each $k_j \in K$. We have $0 = f(\ell)$. Apply the ring homomorphism $\sigma$ to both sides to get

$$0 = \sigma(0) = \sigma(f(\ell)) = \sigma \left( \sum_{j=0}^{n} k_j \ell^j \right) = \sum_{j=0}^{n} \sigma(k_j)(\sigma(\ell))^j.$$

The hypothesis also tells us that $\sigma(k_j) = k_j$ for all $j$; so

$$0 = \sum_{j=0}^{n} k_j(\sigma(\ell))^j = f(\sigma(\ell)).$$

2. Let $K \subseteq L$ be fields, $f(x)$ be an irreducible polynomial of $K[x]$, and $\alpha_1$ and $\alpha_2$ be elements of $L$ with $f(\alpha_1) = f(\alpha_2) = 0$. Prove that there exists a ring isomorphism $\sigma : K[\alpha_1] \to K[\alpha_2]$ with $\sigma(\alpha_1) = \alpha_2$ and $\sigma(k) = k$ for all $k \in K$. Give all details.

There is a surjective ring homomorphism $\phi_1 : K[x] \to K[\alpha_1]$ with $\phi_1(g(x)) = g(\alpha_1)$ for all $g(x) \in K[x]$. The kernel of $\phi_1$ is generated by the minimal polynomial $f(x)$ of $\alpha_1$. The first isomorphism theorem ensures the existence of a ring isomorphism with $\tilde{\phi}_1(\tilde{g}) = \phi_1(g) = g(\alpha_1)$ for all $g \in K[x]$. We repeat the above procedure to produce a ring isomorphism $\tilde{\phi}_2 : K[x]/(f(x)) \to K[\alpha_2]$, with $\tilde{\phi}_2(\tilde{g}) = g(\alpha_2)$ for all $g \in K[x]$. It follows that $\tilde{\phi}_2 \circ \tilde{\phi}_1^{-1} : K[\alpha_1] \to K[\alpha_2]$ is a ring isomorphism. It is clear that

$$\tilde{\phi}_2 \circ \tilde{\phi}_1^{-1}(\alpha_1) = \tilde{\phi}_2(\tilde{x}) = \alpha_2.$$
3. State the Fundamental Theorem of Galois Theory. Please give hypotheses and conclusions.

Let $K$ be a field with $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$, let $f(x)$ be a polynomial in $K[x]$, and let $F$ be the splitting field of $f$ over $K$. Then

a. $|\text{Aut}_K F| = \dim_K F$.

b. There is a one-to-one, inclusion reversing, correspondence between the subgroups $H$ of $\text{Aut}_K F$ and the intermediate fields $E$ with $K \subseteq E \subseteq F$. The correspondence is given as follows. If $H$ is a subgroup of $\text{Aut}_K F$, then the corresponding field is $F^H$, which is defined to be

$$\{ \alpha \in F \mid \sigma(\alpha) = \alpha, \text{ for all } \sigma \in H \}.$$ 

If $E$ is a field with $K \subseteq E \subseteq F$, then the corresponding group is

$$\text{Aut}_E F = \{ \sigma \in \text{Aut}_K F \mid \sigma(e) = e \text{ for all } e \in E \}.$$ 

c. If $F^H$ is one of the fields with $K \subseteq F^H \subseteq F$ for some subgroup $H$ of $\text{Aut}_K F$, then $\dim_{F^H} F = |H|$.

4. Let $F$ be the splitting field of $f(x) = x^3 - 2$ over $\mathbb{Q}$. Find all fields $K$ with $\mathbb{Q} \subseteq K \subseteq F$. Give complete details.

The roots of $f$ in $\mathbb{C}$ are $r_1 = \theta$, $r_2 = \omega \theta$, and $r_3 = \omega^2 \theta$, where $\theta = \sqrt[3]{2}$, and $\omega = e^{2\pi i/3}$. It follows that $K = \mathbb{Q}[\theta, \omega]$. The polynomial $f$ is irreducible over $\mathbb{Q}$ by the Eisenstein criteria; so, $f$ is the minimal polynomial of $\theta$ over $\mathbb{Q}$; and $\dim_{\mathbb{Q}} \mathbb{Q}[\theta] = 3$. We know that $\omega$ is a root of $g(x) = x^2 + x + 1$. Furthermore, $g(x)$ is irreducible over $\mathbb{Q}[\theta]$ because the only possible factorization would be a factorization into linear factors. We know that $g$ does not factor into linear factors over $\mathbb{Q}[\theta]$ because the roots of $g$ are $\omega$ and $\omega^2$. Neither of these roots are real numbers and $\mathbb{Q}[\theta] \subseteq \mathbb{R}$. It follows that $\dim_{\mathbb{Q}[\theta]} F = 2$. We now use problem 2 to produce an automorphism $\sigma$ of $F$ which fixes $\mathbb{Q}[\theta]$ and sends $\omega$ to $\omega^2$. We know that

$$6 = \dim_{\mathbb{Q}} F = \underbrace{\dim_{\mathbb{Q}} \mathbb{Q}[\omega]}_{2} \dim_{\mathbb{Q}[\omega]} F.$$ 

It follows that $f$ is the minimal polynomial of $\theta$ over $\mathbb{Q}[\omega]$. We use problem 2 again to produce an automorphism $\tau$ of $F$ which fixes $\mathbb{Q}[\omega]$ and sends $\theta$ to $\theta \omega$. We notice that on the roots of $f$: $r_1 = \theta$, $r_2 = \omega \theta$, $r_3 = \omega^2 \theta$, the action of $\sigma$ is $(2, 3)$ and the action of $\tau$ is $(1, 2, 3, 1, 3)$. The permutations $(2, 3)$ and $(1, 2, 3)$ generate all of $S_3$ and $\text{Aut}_\mathbb{Q} F$ is a subgroup of $S_3$. We conclude that $\sigma$ and $\tau$ generate $\text{Aut}_\mathbb{Q} F$ and $\text{Aut}_\mathbb{Q} F = S_3$. The subgroups of $S_3$ are $S_3$, $(1, 2, 3)$, $(1, 2)$, $(1, 3)$, $(2, 3)$, and $(1)$. The corresponding fields are:

$$F^{S_3} = \mathbb{Q}, \quad F^{(1, 2, 3)} = \mathbb{Q}[\omega], \quad F^{(1, 2)} = \mathbb{Q}[\omega^2 \theta], \quad F^{(1, 3)} = \mathbb{Q}[\omega \theta],$$

$$F^{(2, 3)} = \mathbb{Q}[\theta], \quad F^{(1)} = F.$$
5. We know that \( x^9 - 1 = (x^3 - 1)(x^6 + x^3 + 1) \). We also know that \( g(x) = x^6 + x^3 + 1 \) is irreducible over \( \mathbb{Q} \). (There is no need to re-prove these facts.) Let \( F \) be the splitting field of \( g(x) \) over \( \mathbb{Q} \). Find \( \text{Aut}_{\mathbb{Q}} F \). Be sure to tell me the elements of \( \text{Aut}_{\mathbb{Q}} F \) as well as the group structure. Give complete details.

The roots of \( g \) in \( \mathbb{C} \) are \( \zeta, \zeta^2, \zeta^4, \zeta^5, \zeta^7, \zeta^8 \). So, \( F = \mathbb{Q}[\zeta] \), and \( \dim_{\mathbb{Q}} F = 6 \). If \( \sigma \) is in \( \text{Aut}_{\mathbb{Q}} F \), then the entire action of \( \sigma \) is completely determined by the value of \( \sigma(\zeta) \). Problem 1 tells us that \( \sigma(\zeta) \) must be \( \zeta^j \) for \( j \in \{1, 2, 4, 5, 7, 8\} \). Problem 2 tells us that each of the six listed candidates for \( \sigma \) really is a ring isomorphism. So, we have learned that \( \text{Aut}_{\mathbb{Q}} F \) consists of the six functions \( \sigma_j(\zeta) = \zeta^j \) for \( j \in \{1, 2, 4, 5, 7, 8\} \). It is easy to see that \( \sigma_2 \) generates this group. Indeed,
\[
\sigma_2^2 = \sigma_4, \quad \sigma_2^3 = \sigma_8, \quad \sigma_2^4 = \sigma_7, \quad \sigma_2^5 = \sigma_5, \quad \sigma_2^6 = \sigma_1.
\]

We conclude that \( \text{Aut}_{\mathbb{Q}} F \) is the cyclic group of order six which is generated by the function \( \sigma_2 \).