Algebra Homework 4

Due Wednesday, February 6

1 Let p and q be distinct prime numbers, and let $\mathbb{Q} \subseteq E \subseteq \mathbb{C}$, where E is a finite degree extension of $\mathbb{Q}$. Assume that $\sqrt{p}, \sqrt{q} \in E$.

(a) Show that $X^2 - q$ is irreducible over $\mathbb{Q}[\sqrt{p}]$.

(b) Now assume that E is normal over $\mathbb{Q}$. Show that there exists $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ such that $\sigma(\sqrt{p}) = \sqrt{p}$ and $\sigma(\sqrt{q}) = -\sqrt{q}$.

(**Hint:** For (a), you know how $X^2 - q$ factors – can the required elements possibly lie in the field $\mathbb{Q}[\sqrt{p}]$? For (b), you are hoping for a transitive action on the roots of $X^2 - q$.)

Solution

(a) If $X^2 - q = (X - \sqrt{q})(X + \sqrt{q})$ is not irreducible over $\mathbb{Q}[\sqrt{p}]$, then $\sqrt{q} \in \mathbb{Q}[\sqrt{p}]$. This means that $\sqrt{q} = a + b\sqrt{p}$ with $a, b \in \mathbb{Q}$. Squaring this, we find that

$$2ab\sqrt{p} = q - a^2 - b^2 p \in \mathbb{Q}$$

which means that either a or b must be 0. If $a = 0$, then $q = b^2 p$; write $b = \frac{m}{n}$ with $(m, n) = 1$. Then $n^2 q = m^2 p$. Thus p divides n, so p^2 divides n^2; this shows that p divides m, which contradicts the assumption that $(m, n) = 1$. If $b = 0$, then $\sqrt{q} = a$, which we know can't happen (because $X^2 - q$ is irreducible over $\mathbb{Q}$ by the Eisenstein criterion).

(b) Since E is normal over $\mathbb{Q}$, which has characteristic 0, E is Galois over $\mathbb{Q}$. Thus E is a splitting field for some $f \in \mathbb{Q}[X]$ over $\mathbb{Q}$. It follows that E is a splitting field for f over $\mathbb{Q}[\sqrt{p}]$. Since $X^2 - q$ is irreducible over $\mathbb{Q}[\sqrt{p}]$, it follows that $G = \mathrm{Gal}(E/\mathbb{Q}[\sqrt{p}])$ acts transitively on the roots of $X^2 - q$. Let $\sigma \in G$ such that $\sigma(\sqrt{q}) = -\sqrt{q}$. Clearly $\sigma(\sqrt{p}) = \sqrt{p}$.

2 Let $p_1, \ldots, p_n$ be different prime numbers. Show that the real numbers $\sqrt{p_1}, \ldots, \sqrt{p_n}$ are linearly independent over $\mathbb{Q}$. (**Hint:** Let n be the smallest number such that there are different prime numbers $p_1, \ldots, p_n$ and nonzero coefficients $a_i \in \mathbb{Q}$ with $a_1\sqrt{p_1} + \cdots + a_n\sqrt{p_n} = 0$. Now show that n is *not* the smallest such n.)

Solution

Let n be the smallest possible number of primes that can give a counterexample, and suppose $a_1\sqrt{p_1} + \cdots + a_n\sqrt{p_n} = 0$. Let E be the splitting field in $\mathbb{C}$ for $f = \prod(X^2 - p_i)$; thus each $\sqrt{p_i} \in E$, and E is normal over $\mathbb{Q}$. It follows from Problem 1 that there is a $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ such that $\sigma(\sqrt{p_1}) = -\sqrt{p_1}$ and $\sigma(\sqrt{p_2}) = \sqrt{p_2}$. Thus

$$0 = a_1\sqrt{p_1} + \cdots a_n\sqrt{p_n} + \sigma(a_1\sqrt{p_1} + \cdots a_n\sqrt{p_n}) = 2a_2\sqrt{p_2} + b_3\sqrt{p_3} + \cdots b_n\sqrt{p_n}$$

and $2a_2 \neq 0$. This contradicts the minimality of n.

3 Let $F \subseteq E \subseteq L$ and let $G = \mathrm{Gal}(L/F)$.

(a) If E is normal over F, show that $\sigma(E) = E$ for all $\sigma \in G$.

(b) Assume that $|L : F| < \infty$ and that L is normal over F. If $\sigma(E) \subseteq E$ for all $\sigma \in G$, show that E is normal over F.

(**Hint:** For (b), notice that $|E : F| < \infty$.)

Solution

(a) Let $\alpha \in E$. Since E is normal, E is algebraic, so α has a minimal polynomial $f = m_{F,\alpha}$. For each $\sigma \in G$, $\sigma(\alpha)$ is a root of f. Since E is normal over F, f splits in E, so $\sigma(\alpha) \in E$. This proves that $\sigma(E) \subseteq E$. Since σ has an inverse, $\sigma(E) = E$.

(b) We can write $L = F[\alpha_1, \ldots, \alpha_n]$, and $f = \prod m_{F,\alpha_i}$. Since each m_{F,α_i} has a root in L, and L is normal, f splits in L, and so L is a splitting field for f. Now let $\alpha \in E$, and consider $g = m_{F,\alpha}$. Since L is a splitting field, $G = \mathrm{Gal}(L/F)$ acts transitively on the roots of g. Let β be some other root of g and let $\sigma \in G$ such that $\sigma(\alpha) = \beta$. Then

$$\beta = \sigma(\alpha) \in \sigma(E) = E,$$

so $\beta \in E$. This shows that g splits in E, so E is normal over F.

4 Let $\mathbb{Q} \subseteq E \subseteq \mathbb{C}$.

(a) If E is normal over $\mathbb{Q}$, show that $|E : E \cap \mathbb{R}| \leq 2$.

(b) Show that in general there is no bound on $|E : E \cap \mathbb{R}|$, even among fields such that $|E : \mathbb{Q}| < \infty$.

(**Hint:** Show that E is Galois over $\mathbb{Q}$; think about complex conjugation.)

Solution

(a) If $E \subseteq \mathbb{R}$, then $|E : E \cap \mathbb{R}| = 1$.

Thus, we may assume that $E \not\subseteq \mathbb{R}$. Since E is normal over $\mathbb{Q}$, which has characteristic zero, E is Galois over $\mathbb{Q}$. Let $\tau \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q})$ be complex conjugation; since E is normal over $\mathbb{Q}$, $\tau(E) = E$, so we can think of $\tau \in G = \mathrm{Gal}(E/\mathbb{Q})$. Obviously, τ generates a subgroup $H \subseteq G$ of order 2. Also $\mathrm{Fix}(H) = E \cap \mathbb{R}$. Since E is Galois over $\mathbb{Q}$,

$$|E : E \cap \mathbb{R}| = |\mathrm{Fix}(H)| = 2.$$

(b) Let $\zeta \in \mathbb{C}$ be a complex (that is, not real) p^{th} root of -1, where p is prime. Let $E = \mathbb{Q}[\zeta]$. Then $|E : \mathbb{Q}| = p$, and so we know that $|E : E \cap \mathbb{R}|$ must be either p or 1; since $E \not\subseteq \mathbb{R}$, it must be p.