Algebra 2, Homework 1 Solutions

Problem 1:
Let $F \subset E$ be an algebraic field extension and $R$ a ring such that $F \subset R \subset E$. Prove that $R$ is field.

It is enough to show that $r^{-1} \in R$ whenever $0 \neq r \in R$. Let $f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in F[x]$ be the minimal polynomial for $r$ over $F$. Since $f(x)$ is irreducible, we must have $a_n \neq 0$. Set $s = r^{n-1} + a_1r^{n-2} + \cdots + a_{n-1}$. Then $rs = f(r) - a_n = -a_n$, so $r^{-1} = -a_n^{-1}s \in R$.

Problem 2:
Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then $E$ has the $\mathbb{Q}$-basis $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$. Find $a, b, c, d \in \mathbb{Q}$ such that $(1 + \sqrt{2} + \sqrt{3})^{-1} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$.

One checks that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, from which it easily follows that $[E : \mathbb{Q}] = 4$ and $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis.

The equation $(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6})(1 + \sqrt{2} + \sqrt{3}) = 1$, with $a, b, c, d \in \mathbb{Q}$, is equivalent to

$$(a + 2b + 3c) + (a + b + 3d)\sqrt{2} + (a + c + 2d)\sqrt{3} + (b + c + d)\sqrt{6} = 1,$$

which gives $a + 2b + 3c = 1$, $a + b + 3d = 0$, $a + c + 2d = 0$, and $b + c + d = 0$. We obtain $a = \frac{1}{2}$, $b = \frac{1}{4}$, $c = 0$, and $d = -\frac{1}{4}$.

Problem 3:
Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.

(a) Show that $E/\mathbb{Q}$ is Galois.

This is true because $E$ is a splitting field over $\mathbb{Q}$ of the separable polynomial $f(x) = (x^2 - 2)(x^2 - 3)(x^2 - 5)$.

(b) Find $\text{Gal}(E/\mathbb{Q})$.

We first check that $\sqrt{5} \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Assume that $\alpha = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ satisfies $\alpha^2 = 5$, where $a, b, c, d \in \mathbb{Q}$. Then (1) $a^2 + 2b^2 + 3c^2 + 6d^2 = 5$, (2) $ab + 3cd = 0$, (3) $ac + 2bd = 0$, and (4) $ad + bc = 0$. If $d = 0$, then $ab = bc = ca = 0$, so $\alpha \in \mathbb{Q} \cup \mathbb{Q}\sqrt{2} \cup \mathbb{Q}\sqrt{3}$ which contradicts $\alpha^2 = 5$. We therefore have $d \neq 0$. Now (2) and (4) imply that $d(a^2 - 3c^2) = a(ad + bc) - c(ab + 3cd) = 0$, and since $\sqrt{3} \notin \mathbb{Q}$ this gives $a = c = 0$. It then follows from (3) that $b = 0$, so $\alpha \in \mathbb{Q}\sqrt{6}$, again contradicting $\alpha^2 = 5$. Since $\sqrt{5} \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$ we obtain $[E : \mathbb{Q}] = 8$.

The roots of $f(x)$ are $\{\pm\sqrt{2}, \pm\sqrt{3}, \pm\sqrt{5}\}$, and $G = \text{Gal}(E/\mathbb{Q})$ is a subgroup of the permutation group $\text{Sym}(\pm\sqrt{2}, \pm\sqrt{3}, \pm\sqrt{5})$. Since each element of $G$ also preserves the roots of each of the polynomials $x^2 - 2$, $x^2 - 3$, $x^2 - 5$, we must have $G \subset \text{Sym}(\pm\sqrt{2}) \times \text{Sym}(\pm\sqrt{3}) \times \text{Sym}(\pm\sqrt{5})$. Finally, since $|G| = 8$, we obtain $G = \text{Sym}(\pm\sqrt{2}) \times \text{Sym}(\pm\sqrt{3}) \times \text{Sym}(\pm\sqrt{5}) \cong \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$.

(c) Find $\alpha \in E$ such that $E = \mathbb{Q}(\alpha)$.

Set $\alpha = \sqrt{2} + \sqrt{3} + \sqrt{5}$. Using the above description of $G = \text{Gal}(E/\mathbb{Q})$, we obtain $\text{Gal}(E/\mathbb{Q}(\alpha)) = \{\sigma \in G \mid \sigma(\alpha) = \alpha\} = \{1\}$. It follows that $\mathbb{Q}(\alpha) = E$.
Problem 4:  
Let $E$ be a finite extension of $\mathbb{Q}$. Show that $E$ contains only finitely many roots of 1.

Set $n = [E : \mathbb{Q}]$ and let $\alpha \in E$ be a primitive $m$-th root of unity. Then $\phi(m) = [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq n$, where $\phi(m)$ is Euler’s phi function. Recall that $\phi(ab) = \phi(a)\phi(b)$ whenever $(a,b) = 1$, and $\phi(p^d) = (p-1)p^{d-1}$ for each prime $p$ and $d \geq 1$. These identities imply that $m \leq 2\phi(m)^2 \leq 2n^2$. Finally, since there are at most $m$ primitive $m$-th roots of 1, the total number of roots of 1 is at most

$$\sum_{m=1}^{2n^2} m = \binom{2n^2 + 1}{2}.$$ 

Problem 5: 
Let $K/F$ be a finite Galois extension such that $[K : F] = p^n$ where $p$ is a prime and $n \geq 1$. Show that:

(a) There exists a subextension $F \subset E \subset K$ such that $[E : F] = p$.
(b) Any such subextension $E$ is Galois over $F$.

By the Main Theorem of Galois theory, we need to prove that, if $G$ is any non-trivial $p$-group, then $G$ contains a subgroup of index $p$ and every such subgroup is normal. It follows from Sylow’s first theorem that $G$ has a subgroup of index $p$. Let $H \leq G$ be any subgroup of index $p$, and let $C \subset G$ be the center of $G$. Then $C \neq \{1\}$. If $C \not\subset H$, then $G$ is generated by $C$ and $H$, so $H$ is normal. Otherwise $H/C$ is a subgroup of index $p$ in $G/C$, and it follows by induction on $|G|$ that $H/C$ is normal in $G/C$, hence $H$ is normal in $G$.

Problem 6:  
Let $F \subset E \subset K$ be field extensions such that $K/F$ is Galois. Set $G = \text{Gal}(K/F)$ and $H = \text{Gal}(K/E)$. Show that $\text{Aut}_F(E) \cong N_G(H)/H$.

For each $\sigma \in G$ we have $\sigma(E) = E \iff \text{Gal}(K/\sigma(E)) = \text{Gal}(K/E) \iff \sigma H \sigma^{-1} = H \iff \sigma \in N_G(H)$. It follows that restriction of automorphisms gives a well defined group homomorphism

$$\phi : N_G(H) \to \text{Aut}_F(E).$$

The kernel of this homomorphism is $H = \text{Gal}(K/E)$. We must show that $\phi$ is surjective. Let $\sigma : E \to E$ be any element of $\text{Aut}_F(E)$. Since $K/F$ is Galois, $K$ is a splitting field over $F$ of some polynomial $f(x) \in F[x]$. Since $K$ is also a splitting field of $f(x)$ over $E$, and since $f(x)$ is preserved by $\sigma$, it follows that $\sigma$ can be extended to an automorphism of $K$.

Problem 7:  
Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree 4 with exactly two real roots. Show that $\text{Gal}(f(x)/\mathbb{Q})$ is either $S_4$ or $D_4$.

Write $f(x) = (x - \alpha)(x - \beta)(x - \gamma)(x - \tau)$ where $\alpha, \beta \in \mathbb{R}$ and $\gamma \in \mathbb{C} \setminus \mathbb{R}$. Then the splitting field of $f(x)$ over $\mathbb{Q}$ is $E = \mathbb{Q}(\alpha, \beta, \gamma)$, and $G = \text{Gal}(E/\mathbb{Q})$ is a subgroup of $S_4 = \text{Sym} \{\alpha, \beta, \gamma, \tau\}$. Consider the tower of extensions $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\alpha, \beta) \subset E$.

The first extension has degree 4, and the last extension has degree 2. If $\beta \notin \mathbb{Q}(\alpha)$, then the middle extension has degree 3, so $[E : \mathbb{Q}] = 24$ and $G = S_4$. 


Otherwise the middle extension is trivial and \(|G| = |E : \mathbb{Q}| = 8\). Since \(\mathbb{Q}(\alpha)/\mathbb{Q}\) is not a normal field extension, \(H = \text{Gal}(E/\mathbb{Q}(\alpha))\) is not a normal subgroup in \(G\). In particular, \(G\) is not Abelian, which implies that no element of \(G\) has order 8, and at least one element \(\sigma \in G\) has order greater than 2. Write \(H = \{1, \tau\}\) and \(S = \langle \sigma \rangle = \{1, \sigma, \sigma^2, \sigma^{-1}\}\). Since \([G : S] = 2\), \(S\) is a normal subgroup of \(G\). It follows that for each element \(\nu \in G\) we have \(\nu \sigma \nu^{-1} \in \{\sigma, \sigma^{-1}\}\). We deduce that \(\{1, \sigma^2\}\) is also a normal subgroup of \(G\), hence \(\tau \neq \sigma^2\), so \(G = \langle \sigma, \tau \rangle\) is generated by \(\sigma\) and \(\tau\). Finally, since \(G\) is not Abelian we must have \(\tau \sigma \tau^{-1} = \sigma^{-1}\), so \(\sigma\) and \(\tau\) satisfy the relations of the Dihedral group \(D_4\) (\(\sigma^4 = 1\), \(\tau^2 = 1\), and \(\tau \sigma \tau^{-1} = \sigma^{-1}\)).

**Problem 8:**

Let \(F\) be a perfect field and \(F \subset E\) an algebraic field extension, such that every non-constant polynomial \(f(x) \in F[x]\) has a root in \(E\). Show that \(E\) is algebraically closed. (Hint: Primitive element theorem.)

We first show that if \(f(x) \in F[x]\) is any polynomial, then \(E\) contains a splitting field for \(f(x)\) over \(F\). To see this, let \(K\) be any splitting field for \(f(x)\) over \(F\). Since \(F\) is perfect it follows that \(K/F\) is a finite separable extension, so there exists a primitive element \(\alpha \in K\) such that \(K = F(\alpha)\). Let \(g(x) \in F[x]\) be the minimal polynomial for \(\alpha\). By assumption we can find \(\alpha' \in E\) such that \(g(\alpha') = 0\). Then \(F(\alpha') \cong F[x]/(g(x)) \cong K\) is a splitting field for \(f(x)\) contained in \(E\).

To see that \(E\) is algebraically closed, it is enough to show that, if \(E \subset E'\) is any finite field extension, then \(E = E'\). Let \(\alpha \in E'\) be any element. Since \(\alpha\) is algebraic over \(F\), it has a minimal polynomial \(f(x) \in F[x]\). Since \(E\) contains a splitting field for \(f(x)\), it follows that all roots of \(f(x)\) are contained in \(E\), including \(\alpha\). This proves that \(E' = E\).