Graded

1. (14.2.28) Let $f(x) \in F[x]$ be an irreducible (and separable) polynomial of degree n over the field F, let L be the splitting field of $f(x)$ over F and let α be a root of $f(x)$ in L. If K is any Galois extension of F contained in L, show that the polynomial $f(x)$ splits into a product of m irreducible polynomials each of degree d over K, where $m = [F(\alpha) \cap K \colon F]$ and $d = [K(\alpha)\colon K]$. [If H is the subgroup of the Galois group of L over F corresponding to K then the factors of $f(x)$ over K correspond to the orbits of H on the roots of $f(x)$. Then use Exercise 9 of Section 4.1]

   Proof. Let $G = \mathrm{Gal}(L/F)$ and let $H = \mathrm{Gal}(L/K)$. Observe H is normal in G since K is Galois over F. Furthermore, observe that the claim to prove is clear when $\alpha \in K$: since K is Galois over F and $f(x)$ has a root in K then all of its roots are in K. So suppose further that $\alpha \notin K$.

   There is a transitive group action of G on the set of roots of $f(x)$ (all belonging to L) since L is Galois over F. Since H is a subgroup of G it also acts on the set of roots of $f(x)$, and denote its distinct orbits by $\mathcal{O}_1, \ldots, \mathcal{O}_r$; let α be in $\mathcal{O}_1$ by relabeling if needed.

   We show that these orbits are in correspondence with the irreducible monic factors of $f(x)$ over K: Observe that each orbit $\mathcal{O}_i$ is a collection of distinct Galois conjugates β_j of roots under H; it follows that $\prod(x-\beta_j)$ is irreducible (if it were not then we could partition $\mathcal{O}_i$ into two sets which are orbits of H, which is impossible by minimality of the orbit $\mathcal{O}_i$) and divides $f(x)$. Similarly, if $g_i(x)$ is an irreducible monic factor of $f(x)$ over K it is the minimal polynomial of one of its roots β_k. It follows that the other roots of $g_i(x)$ are Galois conjugates of β_k under H and thus the roots form one of the orbits of H. The degree of each of these factors is exactly the size of their corresponding orbit (i.e. the number of roots it has).

   Then apply Exercise 9 of Section 4.1 to see that G permutes the orbits of H transitively and each orbit has the same cardinality. In particular with $\alpha \in \mathcal{O}_1$ we have $|\mathcal{O}_1| = |H \colon H \cap G_\alpha|$, where $G_\alpha \leq G$ is the stabilizer of α in G, and $r = |G\colon HG_a|$.

   Observe that the fixed field of G_α is $F(\alpha)$: every element of $F(\alpha)$ is fixed by G_α since α is fixed by G_α, and since L is the field F adjoined with every root of $f(x)$, any element of L fixed by G_α is a rational function of only α over F. Use the Galois correspondence to see that $|\mathcal{O}_1| = |H\colon H \cap G_\alpha| = [KF(\alpha)\colon K] = [K(\alpha)\colon K]$ ($F \subseteq K$) and the number of orbits r is equal to $|G\colon HG_\alpha| = [K \cap F(\alpha)\colon F]$. Thus $f(x)$ splits into the product of $[K \cap F(\alpha)\colon F]$ many irreducible monic factors times a unit, where each factor has degree $[K(\alpha)\colon K]$. □

2. (14.4.4) For *any* Galois extension K of F, show the irreducible (and separable) polynomial $f(x) \in F[x]$ factors in $K[x]$ as in Exercise 28 of Section 2 (whether or not K is contained in the Galois closure L of $f(x)$). [Show first that the factorization of $f(x)$ over K is the same as its factorization over $L \cap K$. Then show the factors of $f(x)$ over $L \cap K$ correspond to the orbits of $H = \mathrm{Gal}(L/L \cap K)$ on the roots of $f(x)$ and use Exercise 9 of Section 4.1.]

   Proof. We show first that the factorization of $f(x)$ over K is the same as its factorization over $L \cap K$, where L is the splitting field of $f(x) \in F[x]$. We show that if $f(x)$ has factorization $q_1(x) \cdots q_r(x)$ of irreducibles over K then the same factorization holds over $L \cap K$. Take any $q_i(x)$ and observe that any root of $q_i(x)$ is a root of $f(x)$ so it is found in the splitting field L. As a result we can factorize $q_i(x)$ as the product $c\prod(x-\beta_j)$ in $L[x]$, where c is a unit and β_j is a distinct (since $f(x)$ is separable) root of $q_i(x)$. By expanding the product it follows that $q_i(x)$ is in $L[x]$, and so $q_i(x)$ is in $(L \cap K)[x]$. It follows by unique factorization that the factorization of $f(x)$ into $q_1(x)\cdots q_r(x)$ is the same in K and in $L \cap K$.

Let $G = \mathrm{Gal}(L/F)$ and $H = \mathrm{Gal}(L/L \cap K)$. Observe G acts transitively on the roots of $f(x)$ by permuting them, and the subgroup H acts on the roots of $f(x)$ as well. We show that H is normal in G by showing that $L \cap K$ is Galois over F: Since L, K are Galois over F they are both finite, separable, and normal extensions of F. Then the extension $L \cap K$ over F is finite since L and K are, and it is separable since L is separable (Subfields of separable extensions are seperable: Take any element $\alpha \in L \cap K$ and view it as an element of L, then the minimal polynomial of α over F is separable as desired.). The extension $L \cap K$ is normal since L and K are normal extensions (Intersections of normal extensions are normal: Take any irreducible polynomial $p(x) \in F[x]$ with root $\beta \in L \cap K$. Then with $\beta \in L$, $f(x)$ splits into linear factors over L, similarly over K. But by unique factorization of polynomials these factorizations must be the same so $f(x)$ splits into linear factors over $L \cap K$.).

Thus $L \cap K$ is a Galois extension over F contained in L as desired, and so H is normal in G. Use the previous exercise with $L \cap K$ in place of K and obtain the desired factorization of $f(x)$ over $(L \cap K)[x]$, which is the same factorization over $K[x]$ as shown above. $\square$

Additional Problems

1. (14.2.27) Let $\alpha = \sqrt{(2+\sqrt{2})(3+\sqrt{3})}$ (positive square roots for concreteness) and consider the extension $E = \mathbb{Q}(\alpha)$.

   (a) Show that $a = (2+\sqrt{2})(3+\sqrt{3})$ is not a square in $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. [If $a = c^2$, $c \in F$, then $a\varphi(a) = (2+\sqrt{2})^2(6) = (c\varphi(c))^2$ for the automorphism $\varphi \in \mathrm{Gal}(F/\mathbb{Q})$ fixing $\mathbb{Q}(\sqrt{2})$. Since $c\varphi(c) = N_{F/\mathbb{Q}(\sqrt{2})}(c) \in \mathbb{Q}(\sqrt{2})$ conclude that $\sqrt{6} \in \mathbb{Q}(\sqrt{2})$, a contradiction.]

   (b) Conclude from (a) that $[E\colon \mathbb{Q}] = 8$. Prove that the roots of the minimal polynomial over $\mathbb{Q}$ for α are the 8 elements $\pm\sqrt{(2\pm\sqrt{2})(3\pm\sqrt{3})}$.

   (c) Let $\beta = \sqrt{(2-\sqrt{2})(3+\sqrt{3})}$. Show that $\alpha\beta = \sqrt{2}(3+\sqrt{3}) \in F$ so that $\beta \in E$. Show similarly that the other roots are also elements of E so that E is a Galois extension of $\mathbb{Q}$. Show that the elements of the Galois group are precisely the maps determined by sending α to one of the eight elements in (b).

   (d) Let $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ be the automorphism which maps α to β. Show that since $\sigma(\alpha^2) = \beta^2$ that $\sigma(\sqrt{2}) = -\sqrt{2}$ and $\sigma(\sqrt{3}) = \sqrt{3}$. From $\alpha\beta = \sqrt{2}(3+\sqrt{3})$ conclude that $\sigma(\alpha\beta) = -\alpha\beta$ and hence $\sigma(\beta) = -\alpha$. Show that σ is an element of order 4 in $\mathrm{Gal}(E/\mathbb{Q})$.

   (e) Show similarly that the map τ defined by $\tau(\alpha) = \sqrt{(2+\sqrt{2})(3-\sqrt{3})}$ is an element of order 4 in $\mathrm{Gal}(E/\mathbb{Q})$. Prove that σ and τ generate the Galois group, $\sigma^4 = \tau^4 = 1$, $\sigma^2 = \tau^2$ and that $\sigma\tau = \tau\sigma^3$.

(f) Conclude that $\mathrm{Gal}(E/\mathbb{Q}) \cong Q_8$, the quaternion group of order 8.

Proof. (a) Suppose that $a = c^2$ for some $c \in F$. Then $a\varphi(a) = c^2\varphi(c^2) = (c\varphi(c))^2 = (2+\sqrt{2})(3+\sqrt{3})(2+\sqrt{2})(3-\sqrt{3}) = (2+\sqrt{2})^2(6)$; since $c\varphi(c)$ is equal to $N_{F/\mathbb{Q}(\sqrt{2})}(c) \in \mathbb{Q}(\sqrt{2})$ (the Galois group of $F/\mathbb{Q}(\sqrt{2})$ only has two elements), it follows that $(2+\sqrt{2})\sqrt{6} \in \mathbb{Q}(\sqrt{2})$, meaning $\sqrt{6} \in \mathbb{Q}(\sqrt{2})$, which is impossible. So a is not a square in F.

(b) The field extension $F/\mathbb{Q}$ is degree 4, and the field extension $F(\alpha)/F$ is degree 2 since α is not an element of F by (a) and α has minimal polynomial $x^2 - a \in F[x]$. Hence $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \alpha)$ is a degree 8 extension of $\mathbb{Q}$. Observe that $\alpha^2/(2+\sqrt{2}) - 3 = \sqrt{3}$ so that $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \alpha) = \mathbb{Q}(\sqrt{2}, \alpha) = E(\sqrt{2})$ We show that $E(\sqrt{2}) = E$ by contradiction. Suppose the degree of the extension is 2 (the minimal polynomial is $x^2 - 2$) and apply the automorphism sending $\sqrt{2} \mapsto -\sqrt{2}$ which fixes E to see that $\alpha^2 \mapsto (2-\sqrt{2})(3+\sqrt{3}) \neq \alpha^2$, which is a contradiction. Hence $E = E(\sqrt{2})$, and so E is a degree 8 extension of $\mathbb{Q}$.

Observe that $f(x) = \prod\left(x \pm \sqrt{(2\pm\sqrt{2})(3\pm\sqrt{3})}\right) = x^8 - 24x^6 + 144x^4 - 288x^2 + 144$ is a monic degree eight polynomial over $\mathbb{Q}$ with the eight roots $\pm\sqrt{(2\pm\sqrt{2})(3\pm\sqrt{3})}$ as desired. Since $[E \colon \mathbb{Q}] = 8$, it follows that this polynomial is irreducible, and so is the minimal polynomial for α.

(c) With $\alpha\beta = \sqrt{(2+\sqrt{2})(3+\sqrt{3})}\sqrt{(2-\sqrt{2})(3+\sqrt{3})} = \sqrt{2(3+\sqrt{3})^2} = \sqrt{2}(3+\sqrt{3})$, we have that $\beta = \sqrt{2}(3+\sqrt{3})/\alpha \in E$. We have similarly that $\gamma = \sqrt{(2+\sqrt{2})(3-\sqrt{3})} = (2+\sqrt{2})\sqrt{6}/\alpha$ and $\omega = \sqrt{(2-\sqrt{2})(3-\sqrt{3})} = [\alpha\sqrt{2}(3-\sqrt{3})]/[(2+\sqrt{2})\sqrt{6}]$. It follows that E is the splitting field for the irreducible separable polynomial $f(x)$, so E is a Galois extension of $\mathbb{Q}$. Since we can write each of the eight roots in terms of α, every automorphism in $\mathrm{Gal}(E/\mathbb{Q})$ permuting the roots of $f(x)$ is determined by where α is sent.

(d) With $\sigma(\alpha^2) = (2-\sqrt{2})(3+\sqrt{3}) = \beta^2$, observe that (since σ fixes $\mathbb{Q}$) $\sigma(\sqrt{2}) = -\sqrt{2}$ and σ fixes $\sqrt{3}$. Then with $\alpha\beta = \sqrt{2}(3+\sqrt{3})$ we have that $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta) = \beta\sigma(\beta) = -\sqrt{2}(3+\sqrt{3}) = -\alpha\beta$; by cancellation $\sigma(\beta) = -\alpha$. It follows that σ has order 4 ($\alpha \mapsto \beta \mapsto -\alpha \mapsto -\beta \mapsto \alpha$).

(e) The map τ sending α to γ is similarly of order 4: With $\alpha\gamma = (2+\sqrt{2})\sqrt{6}$ and $\tau(\alpha^2) = \gamma^2$, we have that τ sends $\sqrt{3}$ to $-\sqrt{3}$ and fixes $\sqrt{2}$. Thus $\tau(\alpha\gamma) = \tau(\alpha)\tau(\gamma) = \gamma\tau(\gamma) = -(2+\sqrt{2})\sqrt{6} = -\alpha\gamma$, so by cancellation $\tau(\gamma) = -\alpha$. Hence τ is of order 4 as desired.

Then we check that

$$\begin{aligned}
&\sigma \colon \alpha \mapsto \beta, \quad \tau \colon \alpha \mapsto \gamma,\\
&\sigma^2 = \tau^2 \colon \alpha \mapsto -\alpha,\\
&\sigma^3 \colon \alpha \mapsto -\beta, \quad \tau^3 \colon \alpha \mapsto -\gamma,\\
&\tau\sigma \colon \alpha \mapsto \omega,\\
&\tau\sigma^{-1} = \tau\sigma^3 = \sigma\tau \colon \alpha \mapsto -\omega,\\
&\mathrm{id}_E = \tau^4 = \sigma^4 \colon \alpha \mapsto \alpha
\end{aligned}$$

form the Galois group.

(e) Observe that the group above is given by the presentation $\langle \sigma, \tau \mid \sigma^4 = \mathrm{id}_E, \sigma^2 = \tau^2, \sigma\tau = \tau\sigma^{-1} \rangle$, which is Q_8, the quaternion group of order 8, up to isomorphism. $\square$

2. (14.3.6) Suppose $K = \mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{D_1}, \sqrt{D_2})$ with $D_1, D_2 \in \mathbb{Z}$, is a biquadratic extension and that $\theta = a + b\sqrt{D_1} + c\sqrt{D_2} + d\sqrt{D_1 D_2}$ where $a, b, c, d \in \mathbb{Z}$ are integers. Prove that the minimal polynomial $m_\theta(x)$ for θ over $\mathbb{Q}$ is irreducible of degree 4 over $\mathbb{Q}$ but is reducible modulo every prime p. In particular show that the polynomial $x^4 - 10x^2 + 1$ is irreducible in $\mathbb{Z}[x]$ but is reducible modulo every prime. [Use the fact that there are no biquadratic extensions over finite fields.]

Proof. Since $\mathbb{Q}(\theta)$ is a degree four extension of $\mathbb{Q}$, it follows that $m_\theta(x)$ is irreducible of degree 4. There are no biquadratic extensions of finite fields, since extensions of finite fields are necessarily cyclic. If we view $m_\theta(x)$ as an element of $\mathbb{F}_p[x]$ and suppose it is irreducible, then its splitting field is an extension of $\mathbb{F}_p$, which is $\mathbb{F}_{p^4}$ (if $f(x) \in \mathbb{F}_p[x]$ is irreducible of degree n then $\mathbb{F}_p[x]/(f(x)) \cong \mathbb{F}_{p^n}$). But $\mathrm{Gal}(\mathbb{F}_{p^4}/\mathbb{F}_p) \cong \mathbb{Z}/4\mathbb{Z}$, and we cannot find a suitable automorphism permuting the roots of $m_\theta(x)$ which has order 4 (the Klein 4-group has elements of order 2 and 1), which means the Galois group could not be cyclic as desired. Hence $m_\theta(x)$ is reducible mod p for any prime p. $\square$

3. (14.3.9) Let $q = p^m$ be a power of the prime p and let $\mathbb{F}_q = \mathbb{F}_{p^m}$ be the finite field with q elements. Let $\sigma_q = \sigma_p^m$ be the m^{th} power of the Frobenius automorphism σ_p, called the q-Frobenius automorphism.

(a) Prove that σ_q fixes $\mathbb{F}_q$.

(b) Prove that every finite extension of $\mathbb{F}_q$ of degree n is the splitting field of $x^{q^n} - x$ over $\mathbb{F}_q$, hence is unique.

(c) Prove that every finite extension of $\mathbb{F}_q$ of degree n is cyclic with σ_q as generator.

(d) Prove that the subfields of the unique extension of $\mathbb{F}_q$ of degree n are in bijective correspondence with the divisors d of n.

Proof. (a) For any element $a \in \mathbb{F}_q$, observe that a satisfies the polynomial $x^q - x$. It follows that $\sigma_q(a) = a^q = a$, so σ_q fixes $\mathbb{F}_q$ as desired.

(b) Observe that $x^{q^n} - x$ over $\mathbb{F}_q$ is separable (its derivative is -1), and that for any roots α, β we have that $\alpha\beta, \alpha^{-1}, (\alpha \pm \beta)$ are also roots (the first two are clear, for the third use the binomial theorem and the fact that we are working in characteristic p, or apply the Frobenius endomorphism directly). Hence the set $\mathbb{F}$ of these q^n roots form a field which is a subfield of the splitting field, meaning $\mathbb{F}$ is the splitting field of $x^{q^n} - x$ over $\mathbb{F}_q$. It follows that the degree of the extension is n since $\mathbb{F}$ has q^n elements. Conversely, let $\mathbb{F}$ be a degree n extension of $\mathbb{F}_q$ so that $\mathbb{F}$ has q^n elements, and its multiplicative group is cyclic with order $q^n - 1$. So each nonzero element of $\mathbb{F}$ satisfies the polynomial $x^{q^n - 1} - 1$, and so every element of $\mathbb{F}$ is a root of $x^{q^n} - x$; this polynomial is separable and has exactly q^n roots so $\mathbb{F}$ is the splitting field for this polynomial. Hence every finite extension of $\mathbb{F}_q$ of degree n is the unique splitting field of $x^{q^n} - x$ over $\mathbb{F}_q$.

(c) For $\mathbb{F}$ a degree n extension of $\mathbb{F}_q$, observe that σ_q is injective, hence surjective since $\mathbb{F}$ is finite. So σ_q is an automorphism of $\mathbb{F}$ fixing $\mathbb{F}_q$.

We expect there to be n automorphism of this form. We show that the cyclic group generated by σ_q is the Galois group: Observe that each power of σ_q is a distinct automorphism, and that σ_q^n is the identity map. Suppose the order of σ_q was less than n – this means that for some $i < n$, for every element $a \in \mathbb{F}$ we would have $a^{q^i} = a$, which means that every element of $\mathbb{F}$ satisfied the polynomial $x^{q^i} - x$ which only has q^i roots at most, while $\mathbb{F}$ has q^n elements, impossible. Hence σ_q generates the Galois group, which is cyclic of order n.

(d) By the Galois correspondence, subfields of the degree n extension $\mathbb{F}$ of $\mathbb{F}_q$ are in bijective correspondence with the subgroups of the Galois group, which is isomorphic to $\mathbb{Z}/n\mathbb{Z}$. But the subgroups of $\mathbb{Z}/n\mathbb{Z}$ are unique and cyclic of order d where d divides n. So each divisor d of n determines a unique subgroup, which by the Galois correspondence determines a unique subfield, and vice versa. □

4. (Conjugate Fields) Let K/F be Galois, and $E = K^H$ be the intermediate field corresponding to $H \subset \mathrm{Gal}(K/F)$ under the Galois correspondence.

   (a) For $\tau \in \mathrm{Gal}(K/F)$, show that $\tau(E)$ is the fixed field of $\tau H \tau^{-1}$.

   Proof. Observe that $\tau(E)$ is a field since τ is a field isomorphism of E with $\tau(E)$ (τ restricted to E is a nonzero field homomorphism with left and right inverses). We have that any element of $\tau(E)$ is of the form $\tau(e)$ for $e \in E$, and this element is fixed by any element $\tau h \tau^{-1} \in \tau H \tau^{-1}$: $(\tau h \tau^{-1})(\tau(e)) = \tau(h(e)) = \tau(e)$ (H fixes E). Conversely, if $k \in K$ is fixed by $\tau h \tau^{-1}$, then $h\tau^{-1}(k) = \tau^{-1}(k) = e$ for some $e \in E$. Thus $k = \tau(e)$. Hence $\tau(E)$ is the fixed field of $\tau H \tau^{-1}$. □

   (b) Take $F = \mathbb{Q}$, K the splitting field of $x^3 - 2$ over $\mathbb{Q}$, and H be a subgroup of order 2 in $\mathrm{Gal}(K/F) \cong S_3$. What are the conjugate fields of the fixed field E, i.e. what is

   $$\left\{\tau(K^H) \colon \tau \in \mathrm{Gal}(K/F)\right\}?$$

   Proof. Conjugate fields are in correspondence with conjugate subgroups. If H is generated by a 2-cycle τ, then the other conjugate subgroups are given by $\sigma H \sigma^{-1}$ and $\sigma^2 H \sigma^{-2}$ where σ is any 3-cycle (these are the other two subgroups of order 2 in S_3). It follows that the conjugate fields are $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\zeta_3 \sqrt[3]{2}), \mathbb{Q}(\zeta_3^2 \sqrt[3]{2})$ where ζ_3 is a primitive third root of unity (These are the subfields of $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ which are fixed by the order two subgroups of $\mathrm{Gal}(K/F) \cong S_3$; see pages 546 and 568 for the explicit automorphisms and field diagrams involved). □

Feedback

1. None.

2. Things are okay so far; same as usual I think.