(1) Let n be a square-free integer (i.e., every prime divides n at most once). Let $\mathbb{Q}$ be the rational numbers. Define

$$\mathbb{Q}(\sqrt{n}) = \{a + b\sqrt{n} \mid a, b \in \mathbb{Q}\},$$

which is the splitting field of $x^2 - n$ over $\mathbb{Q}$.

(a) If $b \neq 0$, show that $a + b\sqrt{n}$ satisfies a unique monic degree 2 polynomial with rational coefficients.

Proof. Define $f(x) = x^2 - 2ax + (a^2 - b^2 n)$. It is straightforward to verify that f has $a+b\sqrt{n}$ as a root. Since $\mathbb{Q}$ is a field, the kernel of the ring morphism $\gamma : \mathbb{Q}[x] \to \mathbb{Q}(\sqrt{n})$ mapping $x \mapsto a + b\sqrt{n}$ must be principal generated by the smallest degree monic polynomial it contains, which is necessarily unique. It is not hard to see that since $b, n \neq 0$ and n is square-free that $\ker \gamma$ contains no degree-0 or degree-1 polynomials, so that it must be generated by the monic polynomial f, which is of the next-highest degree 2. Hence, f is unique. $\square$

(b) Determine the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{n})$.
(Hint: The answer depends on whether or not $n \equiv 1 \pmod 4$)

Proof. Fix some square-free $n \in \mathbb{N}$. Let $\mathcal{O}_{\mathbb{Q}(\sqrt{n})}$ denote the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{n})$. By Gauss' Lemma, given $a, b \in \mathbb{Q}$, we have that $a + b\sqrt{n} \in \mathcal{O}_{\mathbb{Q}(\sqrt{n})}$ if and only if the minimal polynomial of $a + b\sqrt{n}$ in $\mathbb{Q}[x]$ is an integer polynomial[1]. By part (a), this is furthermore true if and only if $2a, a^2 - b^2 n \in \mathbb{Z}$. Suppose some $a, b \in \mathbb{Q}$ are given satisfying this condition.

Case 1: $a \in \mathbb{Z}$. In this case, necessarily $b \in \mathbb{Z}$ as well. Indeed, suppose $b = p/q$ in reduced form (so $\gcd(p, q) = 1$). Because p and q share no factors, neither do p^2 and q^2. Thus, in order for $p^2 n/q^2$ to be an integer, q^2 must be a factor of n, which is square-free, meaning $q = 1$. Hence b is an integer if a is.

Case 2: $a \notin \mathbb{Z}$. In this case, since we know it must be true that $2a \in \mathbb{Z}$, necessarily $a = m/2$ where m is odd. Furthermore, it must be true that $m^2/4 - b^2 n \in \mathbb{Z}$, which holds iff $m^2 - 4b^2 n \in 4\mathbb{Z}$. Write $b = p/q$ where p and q are coprime. Then since m is odd, so is m^2, meaning that $4b^2 n = 4p^2 n/q^2$ is likewise an odd integer. Then 4 must be a factor of q^2, so that q must be even. This further implies that p must be odd, as p and q are coprime. Note that $4p^2 n$ is divisible by no power of 2 larger than 8, as p is odd and n is square-free. Hence, $q^2 \leq 8$ and q is even, so $q = \pm 2$. Thus, it remains to find all $p \in \mathbb{Z}$ for which $m^2 - 4b^2 n = m^2 - 4p^2 n/4 = m^2 - p^2 n \in 4\mathbb{Z}$, i.e., those $p \in \mathbb{Z}$ for which $m^2 \equiv p^2 n \pmod 4$. Since m is odd, we can write $m = 2k + 1$, in which case $m^2 = 4k^2 + 4k + 1 \equiv 1 \bmod 4$. Hence, any $p \in \mathbb{Z}$ for which $p^2 n \equiv 1 \bmod 4$ suffices. In particular, neither p nor n can be even. Furthermore, since p is odd, $p^2 \equiv 1 \bmod 4$. Hence, the only way it can be true that $p^2 n \equiv 1 \bmod 4$ is if $n \equiv 1 \bmod 4$. Indeed, if $n \equiv 3 \bmod 4$, then we would have $p^2 n \equiv 3 \bmod 4$.

To recap, given $a, b \in \mathbb{Q}$, if a and b are integers, then for any square-free n $a + b\sqrt{n}$ is *always* integral over $\mathbb{Z}$.

If $n \not\equiv 1 \bmod 4$, then these are the only elements integral over $\mathbb{Z}$, in which case $\mathcal{O}_{\mathbb{Q}(\sqrt{n})} = \mathbb{Z}[\sqrt{n}]$.

If $n \equiv 1 \bmod 4$, then $a + b\sqrt{n} \in \mathcal{O}_{\mathbb{Q}(\sqrt{n})}$ if a and b are of the form $m/2$ and $p/2$, where m and p are either both even or both odd. In this case, $\mathcal{O}_{\mathbb{Q}(\sqrt{n})} = \mathbb{Z}\left[\frac{1+\sqrt{n}}{2}\right]$. $\square$

[1] Let $f \in \mathbb{Z}[x]$ be a monic polynomial of minimal degree which has $a + b\sqrt{n}$ as a root. Since f is irreducible in $\mathbb{Z}[x]$, by Gauss' Lemma it is irreducible in $\mathbb{Q}[x]$. Hence, f is a monic irreducible polynomial which has $a + b\sqrt{n}$ as a root, so that f must be the minimal polynomial of $a + b\sqrt{n}$.

(2) Let $\mathbf{k}$ be a field and consider the two rings

$$A = \mathbf{k}[x,y]/(y^2 - x^3), \qquad B = \mathbf{k}[x,y]/(y^2 - x^3 - x^2).$$

They are both domains (you don't have to prove this); show that in both cases the normalization is the subring of the field of fractions generated by the ring and y/x.

Hint: Show that adjoining y/x gives a ring which is isomorphic to a polynomial ring over $\mathbf{k}$ in 1 variable.

Proof. First, we define an embedding $A \to \mathbf{k}[t]$. It suffices to define a ring morphism $\mathbf{k}[x,y] \to \mathbf{k}[t]$ with kernel $(y^2 - x^3)$. Define $\varphi : \mathbf{k}[x,y] \to \mathbf{k}[t]$ to be the $\mathbf{k}$-linear map sending $x \mapsto t^2$ and $y \mapsto t^3$. Clearly $\ker\varphi \supseteq (y^2 - x^3)$. Now, suppose that $p \in \ker\varphi$. Viewing p as an element of $(k[x])[y]$, we can perform polynomial division to write $p = q(y^2 - x^3) + r$, where r is of degree of at most 1 (w.r.t. y). Write

$$r = \sum_{i=0}^{n} (a_i x^i + b_i x^i y).$$

Then by additivity, $r \in \ker\varphi$, as $q(y^2 - x^3) \in \ker\varphi$. Hence,

$$\varphi(r) = \sum_{i=0}^{n} (a_i t^{2i} + b_i t^{2i+3}) = 0,$$

which clearly holds if and only if $a_i = b_i = 0$ for all i, as the t^i for $i \geq 2$ are $\mathbf{k}$-linearly independent. In other words, $r = 0$, so that indeed we have $p \in (y^2 - x^3)$. Hence, $\ker\varphi = (y^2 - x^3)$.

Therefore, by the universal property of a quotient there exists an embedding $\widetilde{\varphi} : A \hookrightarrow \mathbf{k}[t]$ with image $\mathbf{k}[t^2, t^3]$. Note that $\mathbf{k}[t] \supseteq \mathbf{k}[t^2, t^3]$ is an integral extension, as t is a root of the monic polynomial $z^2 - t^2$ in $\mathbf{k}[t^2, t^3][z]$. Furthermore, note that $\operatorname{Frac}\mathbf{k}[t^2, t^3] = \operatorname{Frac}\mathbf{k}[t]$ (as $t^3/t^2 = t$ belogns to $\operatorname{Frac}\mathbf{k}[t^2, t^3]$), and $\mathbf{k}[t]$ is a UFD, so that it is integrally closed in its field of fractions. Hence, $\mathbf{k}[t]$ is the normalization of $\mathbf{k}[t^2, t^3] \cong A$. By the universal property of the fraction field, there exists a morphism $\psi : \operatorname{Frac} A \to \mathbf{k}(t)$ sending $p/q \mapsto \widetilde{\varphi}(p)/\widetilde{\varphi}(q)$ such that the following diagram commutes

$$\begin{tikzcd}
 & \mathbf{k}[t] \arrow[r, hook] & \mathbf{k}(t) \\
A \arrow[ur, hook, "\widetilde{\varphi}"] \arrow[dr, hook] & & \\
 & A[\frac{y}{x}] \arrow[r, hook] & \operatorname{Frac} A \arrow[uu, hook, dashed, "\psi"']
\end{tikzcd}$$

It is straightforward to see that given any $f(x, y, y/x) \in A[\frac{y}{x}]$, that $\psi(f) = f(t^2, t^3, t) \in \mathbf{k}[t]$. Furthermore, given any $f(t) \in \mathbf{k}[t]$, we have that $f(y/x) \in A[\frac{y}{x}]$ maps to f via ψ, so that $\psi|_{A[\frac{y}{x}]} : A[\frac{y}{x}] \to \mathbf{k}[t]$ is both injective and surjective (injective because ψ is a nontrivial morphism of fields), hence, an isomorphism. It follows that $A[\frac{y}{x}]$ is the normalization of A.

First, we define an embedding $B \to \mathbf{k}[t]$. It suffices to define a ring morphism $\mathbf{k}[x,y] \to \mathbf{k}[t]$ with kernel $(y^2 - x^3 - x^2)$. Define $\varphi : \mathbf{k}[x,y] \to \mathbf{k}[t]$ to be the $\mathbf{k}$-linear map sending $x \mapsto t^2 - 1$ and $y \mapsto t^3 - t$. A routine calculation yields that $y^2 - x^3 - x^2 \in \ker\varphi$. Now, suppose that $p \in \ker\varphi$. Vieweing p as an element of $(k[x])[y]$, we can perform polynomial division to write $p = q(y^2 - x^3 - x^2) + r$ where r is of degree at most 1 (w.r.t. y). Write

$$r = a(x) + y \cdot b(x),$$

where $a, b \in \mathbf{k}[x]$. Then by additivity, $r \in \ker\varphi$, as $q(y^2 - x^3 - x^2) \in \ker\varphi$. Hence,

$$\varphi(r) = a(t^2 - 1) + t(t^2 - 1)b(t^2 - 1) = 0.$$

Note that $a(t^2 - 1)$ will necessarily be an even-degree polynomial or a constant term, while $t(t^2 - 1)b(t^2 - 1)$ will be an odd-degree polynomial. Hence, the only way for it to be true that

$$a(t^2 - 1) + t(t^2 - 1)b(t^2 - 1) = 0$$

is if $a(t^2 - 1) = b(t^2 - 1) = 0$, which in turn is true if and only if $a = b = 0$. Hence, $r = 0$, so that $p = q(y^2 - x^3 - x^2) \in (y^2 - x^3 - x^2)$. Hence $\ker\varphi = (y^2 - x^3 - x^2)$.

Therefore, by the universal property of a quotient there exists an embedding $\widetilde{\varphi} : A \hookrightarrow \mathbf{k}[t]$ with image $\mathbf{k}[t^2-1, t(t^2-1)]$. Note that $\mathbf{k}[t] \supseteq \mathbf{k}[t^2-1, t(t^2-1)]$ is an integral extension, as t is a root of the monic polynomial $z^2 - (t^2-1) - 1 \in \mathbf{k}[t^2-1, t(t^2-1)][z]$. Furthermore, note that $\operatorname{Frac}\mathbf{k}[t^2-1, t(t^2-1)] = \operatorname{Frac}\mathbf{k}[t]$ (as $t(t^2-1)/(t^2-1) = t$ belongs to $\operatorname{Frac}\mathbf{k}[t^2-1, t(t^2-1)]$), and $\mathbf{k}[t]$ is a UFD, so that it is integrally closed in its field of fractions. Hence, $\mathbf{k}[t]$ is the normalization of $\mathbf{k}[t^2-1, t(t^2-1)] \cong A$. By the universal properry of the fraction field, there exists a morphism $\psi : \operatorname{Frac} A \to \mathbf{k}(t)$ sending $p/q \mapsto \widetilde{\varphi}(p)/\widetilde{\varphi}(q)$ such that the following diagram commutes.

$$\begin{tikzcd}
& \mathbf{k}[t] \arrow[r, hook] & \mathbf{k}(t) \\
A \arrow[ur, hook, "\widetilde{\varphi}"] \arrow[dr] & & \\
& A[\frac{y}{x}] \arrow[r, hook] & \operatorname{Frac} A \arrow[uu, dashed, "\psi"']
\end{tikzcd}$$

It is straightforward to see that given any $f(x, y, y/x) \in A[\frac{y}{x}]$, that $\psi(f) = f(t^2 - 1, t(t^2 - 1), t) \in \mathbf{k}[t]$. Furthermore, given any $f(t) \in \mathbf{k}[t]$, we have that $f(y/x) \in A[\frac{y}{x}]$ maps to f via ψ, so that $\psi|_{A[\frac{y}{x}]} : A[\frac{y}{x}] \to \mathbf{k}[t]$ is both injective and surjective (injective because ψ is a nontrivial morphism of fields), hence, an isomorphism. It follows that $A[\frac{y}{x}]$ is the normalization of A. $\square$

(3) (a) Let A be a ring and $f = t^n + a_1 t^{n-1} + \cdots + a_n$ be any monic polynomial with coefficients in A. Define the **splitting ring** $S_A(f)$ of f to be

$$S_A(f) = A[\xi_1, \ldots, \xi_n]/I$$

where $\xi_1, \ldots, \xi_n$ are variables, and I is generated by the coefficients of

$$(t - \xi_1) \cdots (t - \xi_n) - f(t)$$

thought of as a polynomial in t. Show that the natural map $A \to S_A(f)$ is integral (you don't need to prove it is injective, though that is true).

Proof. It suffices to show that each ξ_i is integral over A for $i = 1, \ldots, n$. Note that f is a monic polynomial with coefficients in A, so it further suffices to show that $f(\xi_i) = 0$. For $j = 1, \ldots, n$, let e_j be the coefficient of the $(n-j)^{\text{th}}$ term of $(t - \xi_1)\cdots(t - \xi_n)$. Then the generators of I are the elements $e_j - a_j$ for $j = 1, \ldots, n$, so that working modulo I,

$$f(\xi_i) = \xi_i^n + a_1\xi_i^{n-1} + \cdots + a_n = \xi_i^n + e_1\xi_i^{n-1} + \cdots + e_n = (\xi_i - \xi_1)\cdots(\xi_i - \xi_n) = 0,$$

so that indeed ξ_i is integral over A, f is integral. $\square$

(b) (Atiyah-Macdonald, Exercise 5.8.ii). Let A be a subring of B, and let C be the integral closure of A in B. Let f, g be monic polynomials in $B[x]$ such that $fg \in C[x]$. Then f, g are in $C[x]$.

Proof. Let $\deg f = n$ and $\deg g = m$. We start by constructing a ring B' over which f and g split completely into linear factors. Define B_1 to be the ring $B[t_1]/(f(t_1))$. Viewed as an element of $B_1[x]$, $f(x)$ has a root $\overline{t_1}$ in B_1. Furthermore, $f(x)$ is in the kernel of the quotient map $B_1[x] \twoheadrightarrow B_1[x]/(x - \overline{t_1})$, so that we can write $f(x) = (x - \overline{t_1})f_1(x)$ for some polynomial $f_1(x) \in B_1[x]$. In particular, note that $\deg f_1 = n - 1$. We can then construct B_2 to be the quotient ring $B_1[t_2]/(f_1(t_2))$, adjoining another root of f. Again $f_1(x)$ is clearly in the kernel of the quotient map $B_2[x] \twoheadrightarrow B_2[x]/(x - \overline{t_2})$, so that there exists a polynomial $f_2(x) \in B_2[x]$ of degree $n-2$ with $f_1(x) = (x - \overline{t_2})f_2(x)$. We can proceed in this manner until we have constructed B_n, in which f splits completely as $(x - \overline{t_1})(x - \overline{t_2})\cdots(x - \overline{t_n})$. In a similar manner, we can adjoin the roots of g to B_n one-by-one until we have obtained a ring B' over which both f and g split entirely into linear factors, say as

$$f = \Pi(x - \xi_i) \qquad \text{and} \qquad g = \Pi(x - \eta_j).$$

Each ξ_i and η_j is a root of fg and therefore is integral over C. Hence the coefficients of f and g, which are polynomials in the ξ_i's and η_j's respectively, are also integral over C, and therefore belong to C. Thus $f, g \in C[x]$. $\square$

(4) (Atiyah-Macdonald, Exercise 5.12). Let G be a finite group of automorphisms of a ring A, and let A^G denote the subring of G-invariants, that is of all $x \in A$ such that $\sigma(x) = x$ for all $\sigma \in G$. Prove that A is integral over A^G.

Proof. First, we show that A^G is a ring. Given $a, b \in A^G$ and $\sigma \in G$, we have by the fact that σ is a ring morphism that

$$\sigma(1) = 1, \qquad \sigma(ab) = \sigma(a)\sigma(b) = ab \qquad \text{and} \qquad \sigma(a - b) = \sigma(a) - \sigma(b) = a - b,$$

so that indeed $1, ab, a \pm b \in A^G$.

Let $a \in A$ and define $p := \prod_{\sigma \in G}(x - \sigma(a)) \in A[x]$. First, we claim that $p \in A^G[x]$. It suffices to show that $\tau(p) = p$ for all $\tau \in G$ (where we implicitly extend $\tau : A \to A$ to a map $A[x] \to A[x]$ simply sending $x \mapsto x$). Indeed, we have:

$$\tau(p) = \tau\left(\prod_{\sigma \in G}(x - \sigma(a))\right) = \prod_{\sigma \in G}(x - \tau(\sigma(a))) \stackrel{(*)}{=} \prod_{\sigma \in G}(x - \sigma(a)),$$

where $(*)$ follows by the fact that the group homomorphism $G \to G$ given by $\sigma \mapsto \tau \circ \sigma$ is an automorphism (as it has an inverse given by composition with τ^{-1}). Finally, clearly a

is a root of p, as since G is a group it contains the identity automorphism $\mathrm{id}_A : A \to A$, so that if $G = \{\mathrm{id}_A, \sigma_1, \dots, \sigma_n\}$, then

$$p(a) = (a - a)(a - \sigma_1(a)) \cdots (a - \sigma_n(a)) = 0.$$

Therefore a is indeed integral over A^G. □

Let S be a multiplicatively closed subset of A such that $\sigma(S) \subseteq S$ for all $\sigma \in G$, and let $S^G = S \cap A^G$. Show that the action of G on A extends to an action on $S^{-1}A$, and that $(S^G)^{-1}A^G \cong (S^{-1}A)^G$.

Proof. Define an action of G on $S^{-1}A$ by

$$\begin{aligned} G \times S^{-1}A &\to S^{-1}A \\ (\sigma, a/s) &\mapsto \sigma(a)/\sigma(s). \end{aligned}$$

Note that $\sigma(a)/\sigma(s)$ is indeed a valid element of $S^{-1}A$ as $\sigma(S) \subseteq S$. First, we show that this is well-defined. Suppose $a/s = b/t$ in $S^{-1}A$, so that there exists $x \in S$ such that

$$x(ta - sb) = 0.$$

Then

$$\sigma(x)(\sigma(t)\sigma(a) - \sigma(s)\sigma(b)) = \sigma(x(ta - sb)) = \sigma(0) = 0,$$

so that $\sigma(a)/\sigma(s) = \sigma(b)/\sigma(t)$ via the element $\sigma(x) \in S$. We further claim that each $\sigma \in G$ acts as a ring endomorphism on $S^{-1}A$. Indeed, it is multiplicative:

$$\sigma\left(\frac{a}{s} \cdot \frac{b}{t}\right) = \sigma\left(\frac{ab}{st}\right) = \frac{\sigma(ab)}{\sigma(st)} = \frac{\sigma(a)\sigma(b)}{\sigma(s)\sigma(t)} = \frac{\sigma(a)}{\sigma(s)} \cdot \frac{\sigma(b)}{\sigma(t)} = \sigma\left(\frac{a}{s}\right) \cdot \sigma\left(\frac{b}{t}\right),$$

and additive:

$$\sigma\left(\frac{a}{s} + \frac{b}{t}\right) = \sigma\left(\frac{ta + sb}{st}\right) = \frac{\sigma(ta + sb)}{\sigma(st)} = \frac{\sigma(t)\sigma(a) + \sigma(s)\sigma(b)}{\sigma(s)\sigma(t)} = \frac{\sigma(a)}{\sigma(s)} + \frac{\sigma(b)}{\sigma(t)} = \sigma\left(\frac{a}{s}\right) + \sigma\left(\frac{b}{t}\right).$$

Now, I claim $(S^G)^{-1}A^G \cong (S^{-1}A)^G$. Define a ring morphism $\varphi : A^G \to (S^{-1}A)^G$ by $a \mapsto a/1$. Note that indeed if $a \in A^G$, then $a/1 \in (S^{-1}A)^G$, as for all $\sigma \in G$ we have $\sigma(a/1) = \sigma(a)/\sigma(1) = a/1$. It is not hard to verify that this is a ring morphism:

$$\varphi(1) = \frac{1}{1} \qquad \text{and} \qquad \varphi(a + bc) = \frac{a + bc}{1} = \frac{a}{1} + \frac{b}{1} \cdot \frac{c}{1} = \varphi(a) + \varphi(b)\varphi(c).$$

Furthermore, φ sends every element in S^G to a unit in $(S^{-1}A)^G$, as given $s \in S^G$ we have

$$\varphi(s) \cdot \frac{1}{s} = \frac{s}{1} \cdot \frac{1}{s} = \frac{s}{s} = \frac{1}{1}.$$

Hence, by the universal property of localization, there exists a morphism $\widetilde{\varphi} : (S^G)^{-1}A^G \to (S^{-1}A)^G$ sending $a/s \mapsto \varphi(a)\varphi(s)^{-1} = (a/1)(1/s) = a/s$. We claim $\widetilde{\varphi}$ is an isomorphism.

First, we show that it is injective. Let $a/s \in (S^G)^{-1}A^G$ such that $\widetilde{\varphi}(a/s) = a/s$ is zero in $(S^{-1}A)^G$, so that there exists $t \in S$ with $ta = 0$. Define

$$t' := \prod_{\sigma \in G} \sigma(t),$$

then $t'a = 0$ as well, so that $a/s \in (S^G)^{-1}A^G$.

Finally, we claim that $\widetilde{\varphi}$ is surjective. Let $a/s \in (S^{-1}A)^G$ so that there exists $t \in S$ such that $ts\sigma(a) = t\sigma(s)a$. Set $t' = \prod_{\sigma \in G} \sigma(t)$. Define a' and s' similarly. Then □

(5) (Atiyah-Macdonald, Exercise 5.9). Let A be a subring of a ring B and let C be the integral closure of A in B. Prove that $C[x]$ is the integral closure of $A[x]$ in $B[x]$.

Proof. First, we show that $C[x] \supseteq A[x]$ is an integral extension. Let $f \in C[x]$. By Proposition 3.1.1, it suffices to show that there exists a subring C' of $B[x]$ that contains A and f such that C' is a finitely generated $A[x]$-module. Set $C' := C[x]$. Since C is a finitely generated A module, clearly $C[x]$ is a finitely generated $A[x]$ module, giving the desired result.

Secondly, we show that $C[x]$ is integrally closed in $B[x]$. Suppose $f \in B[x]$ is integral over $C[x]$, so that $-f$ is also integral over $C[x]$, meaning there exists $g_1, \dots, g_n \in C[x]$ such that

$$(-f)^n + g_1(-f)^{n-1} + \cdots + g_{n-1}(-f) + g_n = 0.$$

Then let r be an integer greater than the degree of f and each g_i, and let f_1 be the monic polynomial $x^r - f$. Then

$$(f_1 - x^r)^n + g_1(f_1 - x^r)^{n-1} + \cdots + g_{n-1}(f_1 - x^r) + g_n = 0.$$

Expanding, we have that there exists $h_1, \dots, h_n \in C[x]$ such that

$$f_1^n + h_1 f_1^{n-1} + \cdots + h_{n-1} f_1 + h_n = 0,$$

where in particular

$$h_n = g_n + g_{n-1}x^r + g_{n-2}x^{2r} + \cdots + g_2 x^{r(n-2)} + g_1 x^{r(n-1)} \in C[x].$$

Then

$$f_1^n + h_1 f_1^{n-1} + \cdots + h_{n-1} f_1 = -h_n \in C[x],$$

so that

$$f_1(f_1^{n-1} + h_1 f_1^{n-2} + \cdots + h_{n-2} f_1 + h_{n-1}) \in C[x],$$

so that by Question 3(b), $f_1 \in C[x]$, meaning $f = x^r - (x^r - f) \in C[x]$ by Corollary 3.1.2. $\square$