Exercises from Ch. 5: Algebraic Extensions, Lang

Matthew Gergley

Last Updated: February 12, 2026

Disclaimer: The proofs given are completed by myself. Thus, they are also reviewed by myself to ensure no logic flaws and incorrect arguments/deductions/conclusions. If you find any error in my proofs, please do not hesitate to contact me so we can discuss any potential errors and I can update the document as needed.

Exercises

Exercise 0.1. (Exercise 2)
Let $E = F(\alpha)$ where α is algebraic over F, of odd degree. Show that $E = F(\alpha^2)$.

Proof. Assume that $E = F(\alpha)$ where α is algebraic of odd degree. Hence, $[F(\alpha)\colon F] = 2k+1$ with $k \in \mathbb{Z}_{\geq 0}$. Observe that we have the following tower

$$F \subseteq F(\alpha^2) \subseteq F(\alpha)$$

since $\alpha^2 \in F(\alpha)$ ($F(\alpha)$ is closed). Let $f(X) = X^2 - \alpha^2 \in F(\alpha^2)[X]$. Hence, $f(\alpha) = 0$. Thus, $[F(\alpha)\colon F(\alpha^2)] \leq 2$. By the tower law,

$$[F(\alpha)\colon F] = \underbrace{[F(\alpha)\colon F(\alpha^2)]}_{\leq 2} \cdot [F(\alpha^2)\colon F]$$

We see that for the right hand side of this equation to be odd, we cannot have $[F(\alpha)\colon F(\alpha^2)] = 2$. Thus, $[F(\alpha)\colon F(\alpha^2)] = 1 \iff F(\alpha) = F(\alpha^2)$.

□

Exercise 0.2. (Exercise 3)
Let α and β be two elements which are algebraic over F. Let $f(X) = \mathrm{Irr}(\alpha, F, X)$ and $g(X) = \mathrm{Irr}(\beta, F, X)$. Suppose that $\deg f$ and $\deg g$ are relatively prime. Show that g is irreducible in the polynomial ring $F(\alpha)[X]$.

Proof. Set $x = \deg f$ and $y = \deg g$. BWOC assume that g is reducible in $F(\alpha)[X]$. Hence,

$$[F(\alpha, \beta)\colon F(\alpha)] = z < \deg g \quad (z \geq 1).$$

By the tower laws,

$$[F(\alpha, \beta)\colon F] = \underbrace{[F(\alpha, \beta)\colon F(\alpha)]}_{=z} \cdot \underbrace{[F(\alpha)\colon F]}_{=x}$$

and

$$[F(\alpha, \beta)\colon F] = [F(\alpha, \beta)\colon F(\beta)] \cdot \underbrace{[F(\beta)\colon F]}_{=y}$$

Set $l = [F(\alpha, \beta)\colon F(\beta)]$. Thus, $zx = yl$ $(y \big| zx)$. Since $(x, y) = 1$, there exists $u, v \in \mathbb{Z}$ such that

$$ux + vy = 1$$

Multiplying both sides by z,

$$(zx)u + (zy)v = z$$
$$ylu + zyv = z$$
$$y(ly + zv) = z$$

Hence, $y \big| z$, but $z < y$. Therefore, $g(X)$ is irreducible in $F(\alpha)[X]$.

□

Exercise 0.3. (Exercise 6)
Show that $\sqrt{2} + \sqrt{3}$ is algebraic over $\mathbb{Q}$, of degree 4.

Proof. We will show that $\sqrt{2} + \sqrt{3}$ is algebraic by finding some $f(X) \in \mathbb{Q}[X]$ such that $f(\sqrt{2} + \sqrt{3}) = 0$. Let $\alpha = \sqrt{2} + \sqrt{3}$. Then,

$$\begin{aligned} \alpha^2 &= 5 + 2\sqrt{6} \\ \alpha^2 - 5 &= 2\sqrt{6} \\ \alpha^4 - 10\alpha^2 + 25 &= 24 \\ \alpha^4 - 10\alpha^2 + 1 &= 0 \end{aligned}$$

Thus, take $f(X) = X^4 - 10X^2 + 1 \in \mathbb{Q}[X]$. By construction, $f(\alpha) = 0$ and thus α is algebraic over $\mathbb{Q}$. Moreover $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. But also

$$(\sqrt{2} + \sqrt{3})(\sqrt{2} - \sqrt{3}) = -1,$$

so $\sqrt{2} - \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$, and hence

$$\sqrt{2} = \frac{1}{2}((\sqrt{2} + \sqrt{3}) + (\sqrt{2} - \sqrt{3})) \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

and likewise $\sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Therefore, $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Thus, we have

$$[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4.$$

We found a polynomial $f(X)$ of degree 4 and thus conclude that we also have $f(X) = \mathrm{Irr}(\sqrt{2} + \sqrt{3}, \mathbb{Q}, X)$. □

Exercise 0.4. (Exercise 8)
Let $f(X) \in k[X]$ be a polynomial of degree n. Let K be its splitting field. Show that $[K\colon k]$ divides $n!$.

Proof. We proceed by induction. If $n = 1$, then k itself is the splitting field of $f(X)$ and $(1 =)[k\colon k] \big| 1!$. Suppose that we can find a splitting field of dimension dividing $\deg f\,!$ over k for all $f(X) \in k[X]$ such that $\deg f < n$.
First, suppose that $f(X)$ is irreducible over k. Consider the extension $k(a_1) \supseteq k$ where a_1 is a root of $f(X)$. Hence,

$$f(X) = (X - a_1)g(X) \in k(a_1)[X]$$

with $\deg g = n - 1$. Thus, by the inductive hypothesis, there is a splitting field E for $g(X)$ over $k(a_1)$ such that $[E\colon k(a_1)] \big| (n-1)!$. Then, $E = k(a_1)(a_2, \ldots, a_n)$ where $a_2, \ldots, a_n$ are the roots of $g(X)$. Since $f(X)$ splits over $E = k(a_1, \ldots, a_n)$, E is a splitting field for $f(X)$ over k. Since $[k(a_1)\colon k] = n$ (since $f(X)$ is irreducible over k), $[E\colon k] = n \cdot [E\colon k(a_1)]$, and this divides $n!$ because $[E\colon k(a_1)] \big| (n-1)!$.
Now, secondly, suppose $f(X)$ is reducible in $k[X]$, i.e. $f(X) = g(X)h(X)$, where $\deg g = m < n$ and $\deg h = l < n$, then by the inductive hypothesis there is a splitting field $E = k(a_1, \ldots, a_m)$ for $g(X)$ over k such that $[E\colon k] \big| m!$. Again, by the inductive hypothesis, there is a splitting field $L = k(b_1, \ldots, b_l)$ for $h(X)$ over E such that $[E\colon L] \big| l!$. Then, $k(a_1, \ldots, a_m, b_1, \ldots, b_l) = K$ is a splitting field for $f(X)$ over k and $[K\colon k] = [K\colon E] \cdot [E\colon k]$ which divides $m!k!$, which divides $n!$. (Observe that $n!/m!k! = n!/m!(n-m)!$ is an integer, nCm).

□

Exercise 0.5. (Exercise 9)
Find the splitting field of $X^{p^8} - 1$ over the field $\mathbb{Z}/p\mathbb{Z}$.

Proof. Let $f(X) = X^{p^8} - 1 \in \mathbb{Z}/p\mathbb{Z}[X]$. Since we are in characteristic p, $f(X) = X^{p^8} - 1 = (X-1)^{p^8}$. Thus, $f(X)$ splits over $\mathbb{Z}/p\mathbb{Z}$. Note that 1 is a root of multiplicity p^8, thus $f(X)$ is not separable.

□

Exercise 0.6. (Exercise 10)
Let α be a real number such that $\alpha^4 = 5$.

a Show that $\mathbb{Q}(i\alpha^2)$ is normal over $\mathbb{Q}$.

b Show that $\mathbb{Q}(\alpha + i\alpha)$ is normal over $\mathbb{Q}(i\alpha^2)$.

c Show that $\mathbb{Q}(\alpha + i\alpha)$ is not normal over $\mathbb{Q}$.

Proof.

a We have $\alpha^2 = \sqrt{5}$. Thus, we want to show $\mathbb{Q}(i\sqrt{5})/Q$ is normal. The irreducible polynomial of $i\alpha^2$ over $\mathbb{Q}$ is $\operatorname{Irr}(i\alpha^2, \mathbb{Q}, X) = X^2 + 5 = f(X)$. Then $f(\pm i\sqrt{5}) = 0$. Thus, $f(X) = (X + i\sqrt{5})(X - i\sqrt{5})$. Hence, $\mathbb{Q}(i\alpha^2)$ is the splitting field for $f(X)$. Therefore, $\mathbb{Q}(i\alpha^2)/\mathbb{Q}$ is normal.

b Let $f(X) = X^2 - 2i\sqrt{5} \in \mathbb{Q}(i\alpha^2)[X]$. Then $f(X) = (X + (\sqrt[4]{5} + i\sqrt[4]{5}))(X - (\sqrt[4]{5} + i\sqrt[4]{5}))$ in $\mathbb{Q}(\alpha + i\alpha)$. Hence, $\mathbb{Q}(\alpha + i\alpha)$ is the splitting field for $f(X)$. Thus, $\mathbb{Q}(\alpha + i\alpha)/\mathbb{Q}(i\alpha^2)$ is normal.

c Consider $X^4 + 20 \in \mathbb{Q}[X]$ (one can derive this from $\beta = \sqrt[4]{5} + i\sqrt[4]{5}$ and applying arithmetic to until you get something completely in $\mathbb{Q}$). Thus, $f(X) = (X^2 + 2i\sqrt{5})(X^2 - 2i\sqrt{5}) = (X + (\sqrt[4]{5} + i\sqrt[4]{5}))(X - (\sqrt[4]{5} + i\sqrt[4]{5}))(X^2 - 2i\sqrt{5})$. Observe that $X^2 - 2i\sqrt{5} = (X + (\sqrt[4]{5} - i\sqrt[4]{5}))(X - (\sqrt[4]{5} - i\sqrt[4]{5}))$, but $\pm(\sqrt[4]{5} - i\sqrt[4]{5})$ is not necessarily in $\mathbb{Q}(\sqrt[4]{5} + i\sqrt[4]{5}) = \mathbb{Q}(\alpha + i\alpha)$. We argue this. By way of contradiction, suppose $\alpha - i\alpha \in \mathbb{Q}(\alpha + i\alpha)$. Then $\alpha = \frac{1}{2}[(\alpha + i\alpha) + (\alpha - i\alpha)]$ and $i\alpha = \frac{1}{2}[(\alpha + i\alpha) - (\alpha - i\alpha)]$. This would imply that $i \in \mathbb{Q}(\alpha + i\alpha)$ which is impossible since $\mathbb{Q}(\alpha + i\alpha)$ is generated by a single complex number with $\alpha \in \mathbb{R} \setminus \{0\}$. Hence, $\alpha - i\alpha \notin \mathbb{Q}(\alpha + i\alpha)$. Thus, since this polynomial doesn't completely split over this extension despite having a root, we conclude that $\mathbb{Q}(\alpha + i\alpha)/\mathbb{Q}$ is not normal.

□

Exercise 0.7. (Exercise 12)
Let K be a finite field with p^n elements. Show that every element of K has a unique p-th root in K.

Proof. Define $\varphi\colon K \to K$ by $\varphi(x) = x^p$, a Frobenius mapping. Hence, φ is an embedding. Furthermore, since K is finite, φ is surjective, and thus $\varphi \in \operatorname{Aut}(K)$. By surjectivity, for all $y \in K$, there exists some $x \in K$ such that $\varphi(x) = x^p = y$. Thus, $\sqrt[p]{y} = x \in K$. The uniqueness of the p-th root follows immediately from the injectivity of φ.

□

Exercise 0.8. (Exercise 13)
If the roots of a monic polynomial $f(X) \in k[X]$ in some splitting field are distinct, and form a field, then $\operatorname{char} k = p$ and $f(X) = X^{p^n} - X$ for some $n \geq 1$.

Proof. Let $F = \{\alpha_1, \ldots, \alpha_q\}$ be the set of distinct roots of $f(X) \in k[X]$, which is a field by assumption, where $|F| = q = \deg f$. Since F is a field with a finite number of elements, $\operatorname{char} F = p$ for some prime p. The splitting field of $f(X)$ over k is, by definition, the smallest subfield that contains k and all the roots of $f(X)$. But F is already a field that contains all the roots, so $k(F) \subseteq F$. Trivially, $F \subseteq k(F)$ and thus $k(F) = F \supset k$. Therefore, since $\operatorname{char} F = p$, we have $\operatorname{char} k = p$, proving the first part. Consider the Frobenius map $\varphi\colon F \to F$ given by $\varphi(x) = x^p$. By definition, φ is an embedding and, furthermore, since F is finite, a surjection. Thus, $\varphi \in \operatorname{Aut}(F)$. Then, there exists some $n \geq 1$ such that $\varphi^n(x) = x^{p^n} = x$ for all $x \in F$. Hence, every element $x \in F$ satisfies the polynomial equation $X^{p^n} - X = 0$. Thus,

$$F \subseteq \{x \in k^a \colon x^{p^n} - x = 0\},$$

where k^a is an algebraic closure of k. The $\deg(X^{p^n} - X) = p^n$ and $\frac{d}{dx}\left[X^{p^n} - X\right] = -1 \neq 0$ which implies that $X^{p^n} - X$ is separable with exactly p^n distinct roots. By the above, F is a field containing

all the roots of $X^{p^n} - X$ and $|F| = q$, so we must have $q = p^n$. Hence, $F = \{x \in k^a \colon x^{p^n} - x = 0\}$. By definition, F was the set of roots of the monic polynomial $f(X) \in k[X]$ and it is also exactly the set of roots of $X^{p^n} - X$.
Therefore, $f(X)$ and $X^{p^n} - X$ are both monic and separable with the same set of roots, F. Hence, it follows that they must be equal. Thus, $f(X) = X^{p^n} - X \in k[X]$.

□

Exercise 0.9. (Exercise 14)
Let $\operatorname{char} K = p$. Let L be a finite extension of K, and suppose $[L \colon K]$ prime to p. Show that L is separable over K.

Proof. Let $L = K(\alpha_1, \ldots, \alpha_n)$ be a finite extension of K and thus L is also algebraic. Assume $([L \colon K], p) = 1$. Let $\alpha \in L$. By way of contradiction, suppose α is inseparable. Then the derivative of $\operatorname{Irr}(\alpha, K, X)$ is 0 and since $\operatorname{char} K = p$, this implies that the degree of the irreducible polynomial of α over K is divisible by p. Since $[K(\alpha) \colon K] = \deg \operatorname{Irr}(\alpha, K, X)$, we have $p \Big| [K(\alpha) \colon K]$. Furthermore, we have the following tower of fields,

$$K \subseteq K(\alpha) \subseteq L$$

Thus, $[L \colon K] = [L \colon K(\alpha)] \cdot [K(\alpha) \colon K]$. Therefore, $[K(\alpha) \colon K] \Big| [L \colon K]$. Then from $p \Big| [K(\alpha) \colon K]$, we obtain $[K(\alpha) \colon K] = pr$ with $r \in \mathbb{Z}$. Hence,

$$pr \Big| [L \colon K] \Rightarrow [L \colon K] = (pr)s = p(rs) \Rightarrow p \Big| [L \colon K] \quad (s \in \mathbb{Z})$$

This is a contradiction! We assumed $([L \colon K], p) = 1$. Thus, α is separable and since α was arbitrary, every $\alpha \in L$ is separable. Therefore, $L \supset K$ is separable.

□

Exercise 0.10. (Exercise 15)
Suppose $\operatorname{char} K = p$. Let $a \in K$. If a has no p-th root in K, show that $X^{p^n} - a$ is irreducible in $K[X]$ for all positive integers n.

Proof. Assume that $\operatorname{char} K = p$ and $a \in K$. Suppose that a has no p-th root in K, i.e., there is no $b \in K$ such that $b^p = a$. Let $n \geq 1$. By way of contradiction, suppose $f(X) = X^{p^n} - a$ is reducible in $K[X]$. Let α be a root of $f(X)$ in an algebraic closure K^a. Then $\alpha^{p^n} = a \in K$. Note that $f'(X) = 0$, so $f(X)$ is inseparable. In characteristic p, we have

$$X^{p^n} - a = (X - \alpha)^{p^n}$$

in $K^a[X]$. Thus $f(X)$ has a unique root α (of multiplicity p^n) in K^a.
Since $f(X)$ is reducible over K, there exist $g(X), h(X) \in K[X]$ with $\deg g, \deg h \geq 1$ such that $f(X) = g(X)h(X)$. Without loss of generality, suppose α is a root of $g(X)$ and $\deg g(X) = p^m$ with $m < n$ (since the degree of the minimal polynomial of α over K must divide p^n and be strictly less than p^n).
Define $\beta = \alpha^{p^m}$. Then

$$\beta^{p^{n-m}} = \left(\alpha^{p^m}\right)^{p^{n-m}} = \alpha^{p^n} = a.$$

So a is a p^{n-m}-th power in the extension $K(\alpha)/K$. But since $[K(\alpha) : K] = p^m$ and $n - m \geq 1$, and the Frobenius is purely inseparable, the assumption that $X^{p^n} - a$ is reducible forces a to become a lower p-power in a smaller purely inseparable extension.
Repeating this process (or using induction), we eventually obtain that a is a p-th power in K, i.e., there exists $b \in K$ with $b^p = a$. This contradicts the hypothesis that a has no p-th root in K.
Therefore $X^{p^n} - a$ is irreducible in $K[X]$ for every positive integer n. □

Exercise 0.11. (Exercise 16)
Let $\operatorname{char} K = p$. Let α be algebraic over K. Show that α is separable if and only if $K(\alpha) = K(\alpha^{p^n})$ for all positive integers n.

Proof. Let $\operatorname{char} K = p$ and α be algebraic over K with $\operatorname{Irr}(\alpha, K, X) = f(X)$ and $\deg f(X) = d = [K(\alpha)\colon K]$.
($\implies$) Assume α is separable over K. Then $f'(X) \neq 0$ and thus $p \nmid d$. Fix any $n \in \mathbb{Z}^+$ and set $\beta = \alpha^{p^n}$. Hence, $\beta \in K(\alpha)$ and thus $K(\beta) \subseteq K(\alpha)$. Observe that α is a root of $X^{p^n} - \beta \in K(\beta)[X]$. Thus, $g(X) = \operatorname{Irr}(\alpha, K(\beta), X)$ divides $X^{p^n} - \beta$ and since $\operatorname{char} K = p$, $\deg g(X) = p^k \leq p^n$. Hence, $[K(\alpha)\colon K(\beta)] = p^k \leq p^n$. From the tower,

$$K \subseteq K(\beta) \subseteq K(\alpha),$$

we have

$$[K(\alpha)\colon K] = [K(\alpha)\colon K(\beta)] \cdot [K(\beta)\colon K]$$

Thus, $[K(\alpha)\colon K(\beta)] \Big| [K(\alpha)\colon K]$. Hence, we have $p^k \big| d$, $p^k \leq p^n$, and $p \nmid d$. Thus, we must have $p^k = 1$. Therefore, $[K(\alpha)\colon K(\beta)] = 1 \Rightarrow K(\alpha) = K(\beta) = K(\alpha^{p^n})$.
($\impliedby$) Assume $K(\alpha) = K(\alpha^{p^n})$ with $n \in \mathbb{Z}^+$. By way of contradiction, suppose α is inseparable. Then $f'(X) = 0$ and thus $f(X) = g(X^p)$ for some $g(X) \in K[X]$ with $\deg g(X) = \frac{d}{p} \in \mathbb{Z}$. Since $[K(\alpha)\colon K] = d \geq 2$ ($d = 1$ is trivial), we have $\frac{d}{p} < d$. By definition, we have $f(\alpha) = 0$ and thus $g(\alpha^p) = 0$ and since $g(X)$ is irreducible, we must have $g(X) = \operatorname{Irr}(\alpha^p, K, X)$. Thus, $[K(\alpha^p)\colon K] = \deg g(X) = \frac{d}{p}$. By assumption, taking $n = 1$, $K(\alpha) = K(\alpha^p)$

$$d = [K(\alpha)\colon K] = [K(\alpha^p)\colon K] = \frac{d}{p}$$

Either from our previous remark of $\frac{d}{p} < d$ or from $d(p-1) = 0$, we see that there is clearly a contradiction. Thus, α is separable over K.

□

Exercise 0.12. (Exercise 17)
Prove that the following tow properties are equivalent:

a) Every algebraic extension of K is separable.

b) Either $\operatorname{char} K = 0$, or $\operatorname{char} K = p$ and every element of K has a p-th root in K.

Proof. ($a \implies b$) Assume that every algebraic extension of K is separable. There are two possible characteristics for K, either 0 or some prime p. If $\operatorname{char} K = 0$, then all irreducibles in $K[X]$ are separable. Thus, in this case, the implication is trivial. Now suppose $\operatorname{char} K = p$. By way of contradiction, suppose that there exists some $a \in K$ such that $\sqrt[p]{a} \notin K$. Then the polynomial $X^p - a \in K[X]$ is irreducible. Observe that $\frac{d}{dX}[X^p - a] = 0$, thus all the roots of $X^p - a$ are multiple. Hence $K(\alpha)$, with α a root of $X^p - a$, would be an algebraic extension that is not separable (α is a multiple root), contradicting our assumption. Thus, every element of K has a p-th root in K.
($b \impliedby a$) Assume $\operatorname{char} K = 0$. In characteristic 0, all irreducible polynomials over K are separable and thus every algebraic extension is separable. Now suppose $\operatorname{char} K = p$ and every element of K has a p-th root in K. Let α be any algebraic element over K. By *Exercise 16*, α is separable if and only if $K(\alpha) = K(\alpha^{p^n})$ for all $n \in \mathbb{Z}^+$. Since every element of K has a p-th root by assumption, $K(\alpha) = K(\alpha^{p^n})$ for all n. Hence, α is separable. By induction, every algebraic extension of K is separable.

□