.1 Field extensions, II

Exercise .1.1. Let k be a field, $f(x) \in k[x]$, and let F be the splitting field for $f(x)$ over k. Let $k \subseteq K$ be an extension such that $f(x)$ splits as a product of linear factors over K. Prove that there is a homomorphism $F \to K$ extending the identity on k.

Solution. Since f splits over F, we may write

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_r)$$

where $\alpha_i \in F$. But then since f splits over K, we may also write

$$f(x) = (x - \beta_1) \cdots (x - \beta_r)$$

where $\beta \in K$. Then we may consider the homomorphism $\varphi : F \to K$ which extends the identity on k and maps $\alpha_i \mapsto \beta_i$. Certainly this is a homomorphism. □

Exercise .1.2. Describe the splitting field of $x^6 + x^3 + 1$ over $\mathbb{Q}$. Do the same for $x^4 + 4$.

Solution. Note that $(x^6 + x^3 + 1)(x^3 - 1) = x^9 - 1$ so the roots of the polynomial are 9th roots of unity. Furthermore, they are not the roots of $x^3 - 1 = (x^2 + x + 1)(x - 1)$. Thus, the roots of the polynomial are $\zeta, \zeta^2, \zeta^4, \zeta^5, \zeta^7, \zeta^8$ where $\zeta = e^{2\pi i/9}$. Since these roots are all generated by ζ, we find that the splitting field of $x^6 + x^3 + 1$ is $\mathbb{Q}(\zeta)$.

Note that $x^4 + 4 = (x^2 - 2x + 2)(x^2 + 2x + 2)$. We can easily find the roots of these polynomials to be $1 \pm i, -1 \pm i$ respectively, so the splitting field is merely $\mathbb{Q}(i)$. □

Exercise .1.3. Find the order of the automorphism group of the splitting field of $x^4 + 2$ over $\mathbb{Q}$.

Solution. The splitting field of $x^4 + 2$ over $\mathbb{Q}$ is $\mathbb{Q}(i, \sqrt[4]{2})$. Let σ be an automorphism of this field which fixes $\mathbb{Q}$. Then $\sigma(\sqrt[4]{2})^4 = \sigma(\sqrt[4]{2}^4) = \sigma(2) = 2$ so $\sigma(\sqrt[4]{2})$ is a root of $x^4 - 2$. Furthermore, $\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1$ so $\sigma(i)$ is a root of $x^2 + 1$. Since there are four choices for the first and two choices for the second, the automorphism group has order 8. □

Exercise .1.4. Prove that the field $\mathbb{Q}(\sqrt[4]{2})$ is not the splitting field of any polynomial over $\mathbb{Q}$.

Solution. This is equivalent to showing that $F = \mathbb{Q}(\sqrt[4]{2})$ is not normal; that is, there is an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ with a root in F which does not split as a product of linear factors over F. Consider $f(x) = x^4 - 2$. This is irreducible over $\mathbb{Q}$ by Eisenstein and it factors over F as $(x - \sqrt[4]{2})(x + \sqrt[4]{2})(x^2 + \sqrt{2})$. The last factor does not have roots over F since its splitting field is $\mathbb{Q}(\sqrt[4]{2}, i)$. Thus, F is not the splitting field of any polynomial over $\mathbb{Q}$. □

Exercise .1.5. Let F be a splitting field for a polynomial $f(x) \in k[x]$, and let $g(x) \in k[x]$ be a factor of $f(x)$. Prove that F contains a unique copy of the splitting field of $g(x)$.

Solution. Since F is a splitting field for $f(x)$, we may write

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$$

where $\alpha_i \in F$. Furthermore, we have $f(x) = g(x) \cdot h(x)$ where $g, h \in k[x]$. Suppose WLOG that $\alpha_1, \ldots, \alpha_m$ are the roots of g in F. Then we may consider the algebraic extension $k(\alpha_1, \ldots, \alpha_m)$. Clearly this is a splitting field of $g(x)$ contained within F. Uniqueness follows from the minimality of F as a splitting field for $f(x)$. Indeed, if there were other roots of g in F, and hence other roots of f, then F would properly contain the splitting field of $f(x)$. □

Exercise .1.6. Let $k \subseteq F_1, k \subseteq F_2$ be two finite extensions, viewed as embedded in the algebraic closure $\overline{k}$ of k. Assume that F_1 and F_2 are splitting fields of polynomials in $k[x]$. Prove that the intersection $F_1 \cap F_2$ and the composite F_1F_2 (the smallest subfield of $\overline{k}$ containing both F_1 and F_2) are both also splitting fields over k. (Theorem 4.8 is likely going to be helpful.)

Solution. We show that $F_1 \cap F_2$ is finite and normal. Certainly if F_1 and F_2 are finite, then their intersection is finite, generated by the extension elements in both fields. Furthermore, suppose $f(x) \in k[x]$ is irreducible and has a root in $F_1 \cap F_2$. Then $f(x)$ splits as a product of linear factors over both F_1 and F_2. Thus, all of the roots of f are contained in both F_1 and F_2, hence in their intersection. A similar proof follows for F_1F_2. □

Exercise .1.7. Let $k \subseteq F = k(\alpha)$ be a simple algebraic extension. Prove that F is normal over k if and only if for every algebraic extension $F \subseteq K$ and every $\sigma \in \mathrm{Aut}_k(K)$, $\sigma(F) = F$.

Solution. Suppose F is normal. In particular, the minimal polynomial $p(x)$ of α splits into linear factors over F since it's irreducible over k. Let $\sigma \in \mathrm{Aut}_k(K)$. Then $\sigma(\alpha)$ is a root of p, hence $\sigma(\alpha) \in F$. Since k is fixed by σ, we find that $\sigma(F) = F$.

For the other direction, let $p(x)$ be irreducible over k and suppose F contains a root α of $p(x)$. Let K be the splitting field of $p(x)$ and let β be a different

root of $p(x)$. Then there is an automorphism $\sigma \in \mathrm{Aut}_k(K)$ which sends $\alpha \mapsto \beta$. Since $\sigma(F) = F$ and $\alpha \in F$, it must be the case that $\beta \in F$. Thus, $p(x)$ splits into linear factors over F. □

Exercise .1.8. Let p be a prime, and let k be a field of characteristic p. For $a, b \in K$, prove that $(a+b)^p = a^p + b^p$.

Solution. By the binomial theorem, we have

$$\begin{aligned}(a+b)^p &= \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k \\ &= a^p + b^p\end{aligned}$$

since for all $0 < k < p$ we have

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

has a factor of p since p is prime (so no term in the denominator cancels the p in the numerator). Since k has characteristic p, each of these coefficients is 0. The only remaining terms are $a^p + b^p$. □

Exercise .1.9. Using the notion of 'derivative' given in §4.2, prove that $(fg)' = f'g + fg'$ for all polynomials f, g.

Solution. Rather than messing with series and coefficients, we can first note the following:

$$\begin{gathered}(f+g)' = f' + g', \\ (cf)' = cf', \\ (xf') = f + f', c' = 0\end{gathered}$$

Let $A \subseteq R[x]$ be the set of polynomials f with the property that $(fg)' = f'g + fg'$ for all polynomials g.

If $f_1, f_2 \in A$, then for every polynomial g,

$$\begin{aligned}((f_1+f_2)g)' &= (f_1 g + f_2 g)' \\ &= (f_1 g)' + (f_2 g)' \\ &= f_1 g' + f_1' g + f_2 g' + f_2' g \\ &= (f_1 + f_2) g' + (f_1' + f_2') g \\ &= (f_1 + f_2) g' + (f_1 + f_2)' g\end{aligned}$$

so A is closed under addition.

Similarly,

$$\begin{aligned}((f_1f_2)g)' &= (f_1(f_2g))' \\ &= f_1'f_2g + f_1(f_2g)' \\ &= f_1'f_2g + f_1(f_2'g + f_2g') \\ &= (f_1'f_2 + f_1f_2')g + f_1f_2g'.\end{aligned}$$

That is, A is closed under multiplication. Finally, since A contains all constants and $x \in A$, we can conclude that $A = R[x]$. □

Exercise .1.10. Let $k \subseteq F$ be a finite extension in characteristic $p > 0$. Assume that p does not divide $[F : k]$. Prove that $k \subseteq F$ is separable.

Solution. Since F is finite, we have $k \subseteq F = k(\alpha_1, \ldots, \alpha_n)$. Let f_i be the minimal polynomial of α_i. Since $[F : k]$ is the product of the degrees of the minimal polynomials of each α_i and $p \nmid [F : k]$, it must be the case that $p \nmid \deg f_i$ for all i. In particular, f_i is not a polynomial in x^p, hence it is not inseparable over k. □

Exercise .1.11. Let p be a prime integer. Prove that the Frobenius homomorphism on $\mathbb{F}_p$ is the identity. (Hint: Fermat.)

Solution. Recall that that the Frobenius homomorphism is the map $x \mapsto x^p$. For all $x \in \mathbb{F}_p$ we find

$$x^p \equiv x \pmod{p}$$

so the homomorphism is the identity map. □

Exercise .1.12. Let k be a field, and assume that k is not perfect. Prove that there are inseparable irreducible polynomials in $k[x]$. (If char $k = p$ and $u \in k$, how many roots does $x^p - u$ have in $\overline{k}$?)

Solution. We may assume that char $k = p > 0$ since all fields of characteristic 0 are perfect. Then consider the polynomial $f(x) = x^p - u$. We find $f'(x) = px^{p-1} = 0$ (since k has characteristic p). Thus, $\gcd(f, f') = x^p - u \neq 0$ and f has a repeated root $\sqrt[p]{u}$ of multiplicity p. □

Exercise .1.13. Let k be a field of positive characteristic p, and let $f(x)$ be an irreducible polynomial. Prove that there exists an integer d and a *separable* irreducible polynomial $f_{\text{sep}}(x)$ such that

$$f(x) = f_{\text{sep}}(x^{p^d}).$$

The number p^d is called the *inseparable degree* of $f(x)$. If $f(x)$ is the minimal polynomial of an algebraic element α, the inseparable degree of α is defined to be the inseparable degree of $f(x)$. Prove that α is inseparable if and only if its inseparable degree is $\geq p$.

The picture to keep in mind is as follows: the roots of the minimal polynomial $f(x)$ of α are distributed into $\deg f_{\text{sep}}$ 'clumps', each collecting a number of coincident roots equal to the inseparable degree of α. We say that α is 'purely inseparable' if there is only one clump, that is, if all roots of $f(x)$ coincide (see Exercise 4.14).

Solution. Let d be the greatest integer such that $f(x)$ is a polynomial in x^{p^d}, say $f(x) = g(x^{p^d})$. Then g is irreducible (or else f wouldn't be) and is not a polynomial in x^p by the maximality of d, hence it is separable.

Suppose α is inseparable. That is, its minimal polynomial $f(x)$ is inseparable, hence a polynomial in x^p. Then the inseparable degree of α is $\geq p$. For the other direction, suppose the inseparable degree of α is $\geq p$. That is, $f(x)$ can be written as a polynomial in x^p. Thus, $f(x)$ is inseparable, hence α is inseparable. □

Exercise .1.14. Let $k \subseteq F$ be an algebraic extension, in positive characteristic p. An element $\alpha \in F$ is *purely inseparable* over k if $\alpha^{p^d} \in k$ for some $d \geq 0$. The extension is defined to be purely inseparable if every $\alpha \in F$ is purely inseparable over k.

Prove that α is purely inseparable if and only if $[k(\alpha) : k]_s = 1$, if and only if its degree equals its *inseparability* degree.

Solution. If α is purely inseparable, then $\alpha^{p^d} = a \in k$ for some $d \geq 0$. Consider the polynomial $f(x) = x^{p^d} - a \in k[x]$ which factors as $(x-\alpha)^{p^d} \in k(\alpha)[x]$. That is, $f(x)$ has exactly one root in $\overline{k}$, namely α. Thus, $[k(\alpha) : k]_s = 1$ as there is only one embedding of $k(\alpha)$ into $\overline{k}$.

Now suppose $[k(\alpha) : k]_s = 1$. That is, there is one embedding of $k(\alpha)$ into $\overline{k}$, so α is the unique root of its minimal polynomial $f(x)$. Since $f(x)$ is irreducible, it can be written as a separable polynomial g in x^{p^d} where p^d is the inseparability degree of α. Furthermore, since $f(x)$ only has one distinct root, g has degree 1. Thus, $\deg f = p^d$.

Finally, if the degree of α is equal to its inseparability degree then the minimal polynomial f of α has the form $x^{p^d} - a$ where p^d is the inseparability degree of α. In particular, $\alpha^{p^d} = a \in k$. □

Exercise .1.15. Let $k \subseteq F$ be an algebraic extension, and let $\alpha \in F$ be separable over k. For every intermediate field $k \subseteq E \subseteq F$, prove that α is separable over E.

Solution. Let f be the minimal polynomial of α over k. Since α is separable, we have $\gcd(f, f') = 1$. Note that for any intermediate extension $E \subseteq F$, the minimal polynomial g of α over E divides f. In particular, since f splits into linear factors over F, so do any factors of f. Hence, g is separable over F. □

Exercise .1.16. Let $k \subseteq E \subseteq F$ be algebraic field extensions, and assume that $k \subseteq E$ is separable. Prove that if $\alpha \in F$ is separable over E, then $k \subseteq E(\alpha)$ is a separable extensions. (Reduce to the case of finite extensions.)

Deduce that the set of elements of F which are separable over k form an intermediate field F_{sep}, such that every element $\alpha \in F, \alpha \notin F_{\text{sep}}$ is *inseparable* over k.

For $F = \overline{k}$, $\overline{k}_{\text{sep}}$ is called the *separable closure* of k.

Solution. Recall that an extension is separable iff $[E : k]_s = [E : k]$. That is, the number of embeddings of E into $\overline{k}$ is equal to the degree of the extension. Then it is easy to see that

$$[E(\alpha) : k]_s = [E(\alpha) : E]_s \cdot [E : k]_s = [E(\alpha) : E] \cdot [E : k] = [E(\alpha) : k]$$

so the extension $k \subseteq E(\alpha)$ is separable. □

Exercise .1.17. Let $k \subseteq F$ be an algebraic extension, in positive characteristic. With notation as in Exercises 4.14 and 4.16, prove that the extension $F_{\text{sep}} \subseteq F$ is purely inseparable. Prove that an extension $k \subseteq F$ is purely inseparable if and only if $F_{\text{sep}} = k$.

Solution. We may assume that $\text{char}k = p > 0$ since otherwise k is perfect and $F_{\text{sep}} = F$. Let $\alpha \in F$ and let $f(x) \in k[x]$ be the minimal polynomial of α. We may assume that $f(x)$ is not separable or else $\alpha^{p^0} \in F_{\text{sep}}$ and α is purely inseparable. Since f is inseparable, we can write $f(x) = g(x^p)$ for some $g(x) \in k[x]$. In particular, α^p is algebraic over F_{sep} of degree less than α, so $\alpha^{p^{n+1}} = (\alpha^p)^{p^n}$ is separable over F for some $n \geq 0$. It follows that the minimal polynomial of α over F_{sep} is $(x-\alpha)^{p^m}$ for some m, which is equivalent to saying that $\alpha^{p^m} \in F_{\text{sep}}$ so α is purely inseparable. □

Exercise .1.18. Let $k \subseteq F$ be a finite extension, in positive characteristic. Define the *inseparable degree* $[F : k]_i$ to be the quotient $[F : k]/[F : k]_s$.

- Prove that $[k(\alpha) : k]_i$ equals the inseparable degree of α_i as defined in Exercise 4.13.
- Prove that the inseparable degree is multiplicative: if $k \subseteq E \subseteq F$ are finite extensions, then $[F : k]_i = [F : E]_i[E : k]_i]$.
- Prove that a finite extension is purely inseparable if and only if its inseparable degree equals its degree.

- With notation as in Exercise 4.16, prove that $[F : k]_s = [F_{\text{sep}} : k]$ and $[F : k]_i = [F : F_{\text{sep}}]$. (Use Exercise 4.17.)

Solution. To do. □