Homework 3
Algebra

Joshua Ruiter

February 20, 2018

Lemma 0.1 (for Exercise 7)**.** *Let k be a field contained in a field K. Let E, F be finitely generated algebraic extensions of k in K, that is,*

$$E = k(\alpha_1, \dots, \alpha_m) \qquad F = k(\beta_1, \dots, \beta_n)$$

Then

$$EF = k(\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n)$$

Proof. Because $k \subset E \subset EF$ and $\alpha_1, \dots, \alpha_m \in E \subset EF$ and $\beta_1, \dots, \beta_n \in F \subset EF$, thus $\alpha_i, \beta_j \in EF$, so

$$k(\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n) \subset EF$$

On the other hand, we have the inclusions $E, F \subset k(\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n)$, and EF is the intersection of all fields containing E and F, so

$$EF \subset k(\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n)$$

Thus equality holds. □

Lemma 0.2 (for Exercise 7)**.** *Let $k \subset E \subset K$ be a tower of fields, and let $\alpha_1, \dots, \alpha_n \subset K$ be algebraic over k. Then*

$$[E(\alpha_1, \dots, \alpha_n) : E] \leq [k(\alpha_1, \dots, \alpha_n) : k]$$

Proof. First we do the case $n = 1$. We know that $[k(\alpha_1) : k] = \deg(\mathrm{Irr}(\alpha_1, k))$. Since the $k \subset E$, the irreducible polynomial of α_1 over E can't have larger degree than that of $\mathrm{Irr}(\alpha_1, k)$, so

$$\deg(\mathrm{Irr}(\alpha_1, E)) = [E(\alpha_1) : E] \leq [k(\alpha_1) : k]$$

Now suppose the result holds for $1, 2, \dots, n-1$. Define $k_i = k(\alpha_1, \dots, \alpha_i)$ and $E_i = E(\alpha_1, \dots, \alpha_i)$. Then we have towers

$$k \subset k_1 \subset k_2 \subset \dots \subset k_n$$
$$E \subset E_1 \subset E_2 \subset \dots \subset E_n$$

By the multiplicative tower law,

$$[E_n : E] = [E_n : E_{n-1}] \dots [E_2 : E_1][E_1 : E]$$
$$[k_n : k] = [k_n : k_{n-1}] \dots [k_2 : k_1][k_1 : k]$$

By the base case, $[E_{i+1} : E_i] \leq [k_{i+1} : k_i]$ for all i, applying this inequality repeatedly to the tower product gives the desired inequality. □

Proposition 0.3 (Exercise 7)**.** *Let E, F be finite extensions of a field k with E, F contained in a field K. Then*

$$[EF : k] \leq [E : k][F : k]$$

If $[E : k]$ and $[F : k]$ are relatively prime, then the above is an equality.

Proof. E and F are finitely generated algebraic extensions, so we can write them as

$$E = k(\alpha_1, \dots, \alpha_m) \qquad F = k(\beta_1, \dots, \beta_n)$$

And by a previous lemma, we can write the compositum as

$$EF = E(\beta_1, \dots, \beta_n) = F(\alpha_1, \dots, \alpha_m) = k(\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n)$$

By the previous lemma,

$$[E(\beta_1, \dots, \beta_n) : E] \leq [k(\beta_1, \dots, \beta_n) : k] \implies [EF : E] \leq [F : k]$$

Applying the tower law to $k \subset E \subset EF$, we have

$$[EF : k] = [EF : E][E : k] \leq [E : k][F : k]$$

By the tower law, both $[E : k]$ and $[F : k]$ divide $[EF : k]$. If $[E : k]$ and $[F : k]$ are relatively prime, then their product must also divide $[EF : k]$, so then $[E : k][F : k] \leq [EF : k]$. Thus if $[E : k], [F : k]$ are relatively prime, the inequality goes both ways and becomes and equality. □

Proposition 0.4 (Exercise 9)**.** *Let p be a prime. The splitting field fof $x^{p^8} - 1$ over $\mathbb{Z}/p\mathbb{Z}$ is $\mathbb{Z}/p\mathbb{Z}$.*

Proof. By the binomial theorem,

$$(x-1)^{p^8} = x^{p^8} + \binom{p^8}{1} x^{p^8-1}(-1)^1 + \dots + \binom{p^8}{p^8-1} x(-1)^{p^8-1} + (-1)^{p^8}$$

Since $\binom{p^8}{n}$ is divisible by p all but the first and last terms vanish in $\mathbb{Z}/p\mathbb{Z}[x]$, so

$$(x-1)^{p^8} = x^{p^8} + (-1)^{p^8}$$

If p is odd, then p^8 is odd and $(-1)^{p^8} = -1$. If p is even, then $p = 2$, so $-1 = 1$, so $(-1)^{p^8} = -1$. Thus

$$x^{p^8} - 1 = (x-1)^{p^8}$$

so x^{p^8} splits into linear factors over $\mathbb{Z}/p\mathbb{Z}$. □

Proposition 0.5 (Exercise 10)**.** *Let $\alpha \in \mathbb{R}$ such that $\alpha^4 = 5$. Then $\mathbb{Q}(i\alpha^2)$ is normal over $\mathbb{Q}$, and $\mathbb{Q}(\alpha + i\alpha)$ is normal over $\mathbb{Q}(i\alpha^2)$, but $\mathbb{Q}(\alpha + i\alpha)$ is not normal over $\mathbb{Q}$.*

Proof. Let $f(x) = x^2 + 5 \in \mathbb{Q}[x]$. Then f is irreducible over $\mathbb{Q}$, and $\mathbb{Q}(i\alpha^2)$ is the splitting field of f, since

$$f(x) = x^2 + 5 = (x - i\alpha^2)(x + i\alpha^2)$$

and $\mathbb{Q}(i\alpha^2) = \mathbb{Q}(i\alpha^2, -i\alpha^2)$. Thus $\mathbb{Q}(i\alpha^2)$ is a normal extension of $\mathbb{Q}$.

Now let $g(x) = x^2 - 2i\alpha^2 \in \mathbb{Q}(i\alpha^2)[x]$. Then

$$\begin{aligned} g(x) &= x^2 - 2i\alpha^2 = x^2 - (\alpha^2 + 2i\alpha^2 - \alpha^2) = x^2 - (\alpha^2 + 2i\alpha^2 + i^2\alpha^2) \\ &= x^2 - (\alpha + i\alpha)^2 = (x - (\alpha + i\alpha))(x + (\alpha + i\alpha)) \end{aligned}$$

Thus $\mathbb{Q}(\alpha + i\alpha)$ is the splitting field of g over $\mathbb{Q}(i\alpha^2)$, so $\mathbb{Q}(\alpha + i\alpha)$ is normal over $\mathbb{Q}(i\alpha^2)$.

Let $h(x) = x^4 + 20$. Then h is irreducible over $\mathbb{Q}$ by Eisenstein's criterion at the prime 5, and

$$(\alpha + i\alpha)^4 = -20 \implies h(\alpha + i\alpha) = 0$$

so $\alpha + i\alpha$ is a root of h. But h does not split into linear factors in $\mathbb{Q}(\alpha + i\alpha)$. It does factor over $\mathbb{Q}(\alpha + i\alpha, -\alpha + i\alpha)$ as

$$x^4 + 20 = (x - (\alpha + i\alpha))(x - (\alpha + i\alpha))(x - (-\alpha + i\alpha))(x + (-\alpha + i\alpha))$$

But $-\alpha + i\alpha \notin \mathbb{Q}(\alpha + i\alpha)$, so h does not split into linear factors over $\mathbb{Q}(\alpha + i\alpha)$. But it has a root in $\mathbb{Q}(\alpha + i\alpha)$, so this extension is not normal. □

Proposition 0.6 (Exercise 12)**.** *Let K be a finite field with p^n elements for some prime p. Then every element of K has a unique pth root in K.*

Proof. Define $\phi : K \to K$ by $x \mapsto x^p$. This is a field homomorphism, since

$$(a + b)^p = a^p + b^p$$

in characteristic p. Then $\ker \phi$ must be zero, since it is an ideal of a field. Thus ϕ is injective. But ϕ is a map between finite sets, so then it must also be surjective. Thus ϕ is a bijection, so for every $x \in K$ there is a unique y so that $y^p = x$. □

Proposition 0.7 (Exercise 15)**.** *Let p be a prime and let K be a field of characteristic p. Suppose $a \in K$ has no p-th root. Then for all $n \in \mathbb{N}$, the polynomial $f(x) = x^{p^n} - a$ is irreducible in $K[x]$.*

Proof. First we consider the case $n = 1$. Let F be a splitting field for f, and let $\alpha \in F$ be a root of f, so $\alpha^p = a$. Then F also has characteristic p, so

$$(x - \alpha)^p = x^p - \alpha^p = x^p - a = f(x)$$

Thus α is the only root of f, with multiplicity p. By unique factorization in $K[x]$, we can write f as a product of monic irreducible polynomials,

$$f(x) = q_1(x)q_2(x) \dots q_m(x)$$

where each $q_1(x)$ is a power of $(x-\alpha)$ by the above. Since each q_i is irreducible, each q_i is equal to $\mathrm{Irr}(\alpha, K)$, so

$$f(x) = (\mathrm{Irr}(\alpha, K))^m$$

We know that $\mathrm{Irr}(\alpha, K) = (x-\alpha)^j$ for some $j \in \mathbb{N}$, so $jm = p$. We know that a does not have a pth root in K, so $\alpha \notin K$, so $j \neq 1$. Then since p is prime, $j = p$, and $m = 1$, so $f = \mathrm{Irr}(\alpha, K)$, that is, f is irreducible.

Now assume the result is true for $1, 2 \ldots, n-1$ and assume $n \geq 2$. Let G be a splitting field for $g(x) = x^p - 1$ over K, and let $\alpha \in G$ be a root of g, so $\alpha^p = a$. By the hypothesis that a does not have a pth root in K, we know that $\alpha \notin K$. We claim that α does not have a pth root in $K(\alpha)$. If $\beta \in K(\alpha) = K[\alpha]$ were a pth root of α, then β would need to be a constant polynomial, so then $\beta \in K$ and $(\beta^p)^p = \alpha^p = a$, which contradicts the fact that a does not have a pth root in K. Thus α does not have a pth root in $K(\alpha)$. Now consider

$$\left(x^{p^{n-1}} - \alpha\right)^p = x^{p^n} - \alpha^p = x^{p^n} - a = f(x)$$

Since α does not have a pth root in $K(\alpha)$, by inductive hypothesis, $x^{p^{n-1}} - \alpha$ is irreducible over $K(\alpha)$. Form the splitting field for $x^{p^{n-1}} - \alpha$ over $K(\alpha)$, and let β be a root, $(\beta^{p^{n-1}} = \alpha)$. Then

$$(x-\beta)^{p^{n-1}} = x^{p^{n-1}} - \beta^{p^{n-1}} = x^{p^{n-1}} - \alpha$$

so the splitting field for $x^{p^{n-1}} - \alpha$ over $K(\alpha)$ is $K(\alpha, \beta)$. We know that $\beta \notin K(\alpha)$, since $x^{p^{n-1}} - \alpha$ is irreducible over $K(\alpha)$. We can now write f as

$$f(x) = \left(x^{p^{n-1}} - \alpha\right)^p = \left((x-\beta)^{p^{n-1}}\right)^p = (x-\beta)^p$$

over $K(\alpha, \beta)$. Thus the only roots of f over $K(\alpha, \beta)$ are β, and since $\beta \notin K$, this implies that f is irreducible over K. □

Lemma 0.8 (for Exercise 16)**.** *Let K be a field of characteristic p, and let $K \subset E$ be an algebraic extension. Let $\alpha \in E$. Then for any $n \in \mathbb{N}$,*

$$\left(K(\alpha)^{p^n}\right) K = K\left(\alpha^{p^n}\right)$$

(In case of confusion, the left side is a compositum of the fields $(K(\alpha))^{p^n}$ and K inside the algebraic closure of K.

Proof. $K(\alpha)$ contains α, so $K(\alpha)^{p^n}$ contains α^{p^n}, and the LHS compositum contains K, so the containment

$$\left(K(\alpha)^{p^n}\right) K \supset K\left(\alpha^{p^n}\right)$$

is clear. Let $\beta \in K(\alpha)^{p^n}$. Then $\beta = \eta^{p^n}$ for some $\eta \in K(\alpha) = K[\alpha]$. We can write η as a polynomial in α with coefficients $b_0, \ldots, b_m \in K$, then pull out the linear term and think of η as a binomial.

$$\eta = b_m \alpha^m + \ldots + b_1 \alpha + b_0$$

Then because $\mathrm{char}\, K = p$,

$$\eta^{p^n} = b_m^{p^n} (\alpha^m)^{p^n} + \ldots + b_1^{p^n} \alpha^{p^n} + b_0^{p^n} = b_m (\alpha^{p^n})^m + \ldots b_1^{p^n} \alpha^{p^n} + b_0^{p^n}$$

That is, $\eta^{p^n} \in K[\alpha^{p^n}] = K(\alpha^{p^n})$, so $\beta \in K(\alpha^{p^n})$. Thus we have the containment

$$(K(\alpha))^{p^n} \subset K\left(\alpha^{p^n}\right) \implies \left(K(\alpha)^{p^n}\right) K \subset K\left(\alpha^{p^n}\right)$$

This proves the desired equality. □

Proposition 0.9 (Exercise 16)**.** *Let K be a field of characteristic p, and let α be algebraic over K. Then α is separable if and only if $K(\alpha) = K(\alpha^{p^n})$ for all $n \in \mathbb{N}$.*

Proof. Suppose α is separable. Then $K(\alpha)$ is separable over K, so by Corollary 6.10 (Lang pg. 251), $(K(\alpha)^{p^n})K = K(\alpha)$. Using the previous lemma, $(K(\alpha)^{p^n})K = K(\alpha^{p^n})$, so we have

$$K(\alpha) = K(\alpha^{p^n})$$

for all $n \in \mathbb{N}$. Now suppose that $K(\alpha) = K(\alpha^{p^n})$ for all $n \in \mathbb{N}$. Then in particular, $K(\alpha) = K(\alpha^p) = K(\alpha)^p K$ (using the previous lemma), so by Corollary 6.10 again, $K(\alpha)$ is separable over K; hence α is separable (by definition). □

Lemma 0.10 (for Exercise 17)**.** *Let K be a field of characteristic zero. Then every algebraic extension of K is separable.*

Proof. Let $K \subset E$ be an algebraic extension, and let $\alpha \in E$, and let $f = \mathrm{Irr}(\alpha, K)$. By Proposition 6.1 (Lang pg. 247), f is separable, so α is separable. Then by Theorem 4.4 (Lang pg. 241), E is a separable extension. □

Lemma 0.11 (for Exercise 17)**.** *Let K be a field of characteristic p where p is prime, and suppose that every element of K has a p-th root in K. Then every algebraic extension of K is separable.*

Proof. Since every element of K has a p-th root in K, the injective homomorphism $K \to K$ given by $x \mapsto x^p$ is surjective. Thus $K^p = K$. Then by Corollary 6.12 (Lang pg. 252), every algebraic extension of K is separable. □

Lemma 0.12 (for Exercise 17)**.** *Let K be a field of characteristic p such that every algebraic extension of K is separable. Then every element of K has a p-th root in K.*

Proof. Let $\overline{K}$ be the algebraic closure of K, and let $\alpha \in K$. Define $f(x) = x^p - \alpha \in K[x]$, and let $\beta \in \overline{K}$ be a root of f. Then f splits linearly over $K(\beta)$ since

$$(x - \beta)^p = x^p - \beta^p = x^p - \alpha$$

Suppose $\beta \notin K$. Then $K(\beta)$ is an algebraic extension, so by hypothesis it is separable. But this contradicts the fact that f has a repeated root (namely β, with multiplicity p), so we must conclude that $\beta \in K$. Thus α has a p-th root in K. □

Proposition 0.13 (Exercise 17)**.** *Let K be a field. The following are equivalent:*

1. *Every algebraic extension of K is separable.*
2. *Either* $\mathrm{char}\, K = 0$ *or* $\mathrm{char}\, K = p$ *and every element of K has a p-th root in K.*

Proof. Lemmas 0.10 and 0.11 combine to give (2) $\implies$ (1). Lemma 0.12 is (1) $\implies$ (2). □