

ALGEBRA HW 9

CLAY SHONKWILER

1

Let $F = \mathbb{Z}/p\mathbb{Z}$, let $L = F(x, y)$ and let $K = F(x^p, y^p)$. Show that L is a finite field extension of K , but that there are infinitely many fields between K and L . Is $L = K[\alpha]$ for some $\alpha \in L$? Is L separable over K ?

Proof. Note that x satisfies the polynomial $Z^p - x^p \in K[Z]$, so the minimal polynomial of x over K must divide this polynomial. Since $Z^p - x^p = (Z - x)^p$, this polynomial is inseparable and, hence, the minimal polynomial of x must be separable as well, meaning it must be a polynomial in Z^p . However, this in turn implies that the minimal polynomial of x must be $Z^p - x^p$. Therefore, $[K(x) : K]_{\text{insep}} = p$. On the other hand, since the minimal polynomial of x has a unique root and since any K -embedding of $K(x)$ into \bar{K} must take x to one of the roots of its minimal polynomial, we see that there is only one such embedding; hence, $[K(x) : K]_{\text{sep}} = 1$, and so

$$[K(x) : K] = [K(x) : K]_{\text{insep}} = p.$$

Now, consider $L = K(x, y) = K(x)(y)$ as an extension of $K(x)$. Clearly, y satisfies the polynomial $Z^p - y^p \in K(x)[Z]$, so the minimal polynomial of y over $K(x)$ must divide $Z^p - y^p$. By the same argument as above, this implies that $[L : K(x)]_{\text{insep}} = p$ and, furthermore, since $Z^p - y^p = (Z - y)^p$, we see that $[L : K(x)]_{\text{sep}} = 1$, so $[L : K(x)] = [L : K(x)]_{\text{insep}} = p$. Finally, this means that

$$[L : K] = [L : K(x)][K(x) : K] = p^p,$$

so L is finite over K .

Define

$$\begin{aligned} K_1 &= K(x^{p+1} + y) \\ K_2 &= K(x^{2p+1} + y) \\ &\vdots \\ K_n &= K(x^{np+1} + y) \\ &\vdots \end{aligned}$$

Now, for any K_i ,

$$(x^{ip+1} + y)^p - (x^{p(ip+1)} + y^p) = (x^{p(ip+1)} + y^p) - (x^{p(ip+1)} + y^p) = 0$$

since we're in characteristic p , so $x^{ip+1} + y$ satisfies the polynomial $Z^p - (x^{p(ip+1)} + y^p) \in K[Z]$. Now, in \bar{K} (or even L),

$$f_i(Z) = Z^p - (x^{p(ip+1)} + y^p) = Z^p - (x^{ip+1} + y)^p = (Z - (x^{ip+1} + y))^p,$$

so this polynomial is inseparable. Since the minimal polynomial of $x^{ip+1} + y$ over K must divide this polynomial, it must also be inseparable and, therefore, a polynomial in Z^p . The only such polynomial is $Z^p - (x^{p(ip+1)} + y^p)$, we see that $f_i(Z)$ is the minimal polynomial of $x^{ip+1} + y$ over K and, hence,

$$[K_i : K]_{insep} = p.$$

Since the minimal polynomial of $x^{ip+1} + y$, $f_i(Z)$, has a unique root and any K -embedding of K_i must map x^{ip+1} to another root of its minimal polynomial, we see that there is only one K -embedding of K_i into \bar{K} , so $[K_i : K]_{sep} = 1$. Hence, K_i is purely inseparable over K , and so $[K_i : K] = p$. In particular, this means that $K_i \neq L$ for all $i \in \mathbb{N}$.

Now, suppose $K_i = K_j$ for some $i \neq j$. Then $x^{ip+1} + y, x^{jp+1} + y \in K_i = K_j$, so

$$(x^{ip+1} + y) - (x^{jp+1} + y) = x^{ip+1} - x^{jp+1} \in K_i = K_j.$$

Now, since $K_i \supset K$, we can divide by a multiple of x^p ; in particular,

$$\frac{x^{ip+1} - x^{jp+1}}{x^{ip}} = x - x^{(j-i)p+1} \in K_i = K_j.$$

Now, since $1, x^{(j-i)p} \in K \subset K_i$, we can divide by $1 - x^{(j-i)p}$:

$$\frac{x - x^{(j-i)p+1}}{1 - x^{(j-i)p}} = x \in K_i = K_j.$$

Hence, $x^{ip+1} \in K_i = K_j$, so $(x^{ip+1} + y) - x^{ip+1} = y \in K_i = K_j$, and so $K_i = L$. However, since this is impossible, we conclude that $K_i \neq K_j$ for all $i \neq j$, and so there are infinitely many distinct, non-trivial intermediate extensions $K \subset K_i \subset L$.

By the Primitive Element Theorem, since L is finite over K , $L = K[\alpha]$ if and only if there are only finitely many intermediate fields M such that $K \subset M \subset L$. Since we just saw that there are infinitely many such intermediate fields, we conclude that there is no such $\alpha \in L$ such that $L = K[\alpha]$. Furthermore, if L is separable over K , then the Primitive Element Theorem tells us that there is such a primitive element; since there isn't one, we conclude that L is not separable over K . \square

2

Let $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$ and let $\Phi_n(x)$ be the minimal polynomial of ζ_n over \mathbb{Q} .

(a): Find the roots of $\Phi_n(x)$. Show that $\deg \Phi_n(x) = \phi(n)$, where

$$\phi(n) = \#\{m \in \mathbb{Z} | 1 \leq m \leq n, (m, n) = 1\}.$$

Proof. We want to show that $\Phi_n(x) = \Psi_n(x)$, where

$$\Psi_n(x) := \prod_{\substack{1 \leq m \leq n \\ (m,n)=1}} (x - \zeta_n^m).$$

Now, if $\psi : \mathbb{Q}(\zeta_n) \hookrightarrow \bar{\mathbb{Q}}$, then ψ must fix \mathbb{Q} and is completely determined by $\psi(\zeta_n)$. Now, since $\zeta_n^n = 1$, it must be the case that

$$1 = \psi(1) = \psi(\zeta_n^n) = \psi(\zeta_n)^n,$$

so $\psi(\zeta_n)$ is an n th root of unity; that is, $\psi(\zeta_n) = \zeta_n^k$ for some $1 \leq k \leq n$. On the other hand, suppose $(k, n) \neq 1$. Then $n = kd$ for some $1 < d < n$, and so $(\zeta_n^k)^d = \zeta_n^n = 1$; that is, ζ_n^k is of order $d < n$. Since $\zeta_n^d \neq 1$, it cannot be the case that $\psi(\zeta_n) = \zeta_n^k$. Hence, the only possible images of ζ_n under embeddings of $\mathbb{Q}(\zeta_n) \hookrightarrow \bar{\mathbb{Q}}$ are ζ_n^m for $(m, n) = 1$. Since all conjugates of ζ_n must be roots $\Phi_n(x)$, we see that $\Phi_n(x)$ divides $\Psi_n(x)$.

On the other hand, suppose $(m, n) = 1$ and we define the map $\psi_m : \mathbb{Q}(\zeta_n) \rightarrow \mathbb{Q}(\zeta_n)$ by

$$\begin{aligned} 1 &\mapsto 1 \\ \zeta_n &\mapsto \zeta_n^m \end{aligned}$$

and extend as usual. Then ψ_m is certainly a homomorphism. On the other hand, since $m \in (\mathbb{Z}/n\mathbb{Z})^*$, m has a multiplicative inverse $m' \in (\mathbb{Z}/n\mathbb{Z})^*$, which is also relatively prime to n . Then $\psi_{m'} : \mathbb{Q}(\zeta_n) \rightarrow \mathbb{Q}(\zeta_n)$ given by

$$\begin{aligned} 1 &\mapsto 1 \\ \zeta_n &\mapsto \zeta_n^{m'} \end{aligned}$$

is also a homomorphism. Now, for $\alpha = a_1\zeta_n + \cdots + a_{n-1}\zeta_n^{n-1} + a_n \in \mathbb{Q}(\zeta_n)$,

$$\begin{aligned} \psi_{m'} \circ \psi_m(\alpha) &= \psi_{-m}(\psi_m(a_1\zeta_n) + \cdots + \psi_m(a_n)) \\ &= \psi_{m'}(a_1\zeta_n^m + \cdots + a_{n-1}\zeta_n^{m(n-1)} + a_n) \\ &= \psi_{m'}(a_1\zeta_n^m) + \cdots + \psi_{m'}(a_{n-1}\zeta_n^{m(n-1)}) + \psi_{m'}(a_n) \\ &= a_1\zeta_n^{mm'} + \cdots + a_{n-1}\zeta_n^{mm'(n-1)} + a_n \\ &= a_1\zeta_n + \cdots + a_{n-1}\zeta_n^{n-1} + a_n \\ &= \alpha, \end{aligned}$$

so $\psi_{m'} \circ \psi_m \equiv id$. A parallel computation shows that $\psi_m \circ \psi_{m'} \equiv id$, so we see that $\psi_{m'}$ is an inverse of ψ_m . Therefore, ψ_m is an isomorphism and, thus, is an embedding $\mathbb{Q}(\zeta_n) \hookrightarrow \bar{\mathbb{Q}}$. Since $\psi_m(\zeta_n) = \zeta_n^m$, this implies that ζ_n^m must be a root of $\Phi_n(x)$. Since our choice of $m < n$ such that $(m, n) = 1$ was arbitrary, we see that all such m must be roots of $\Phi_n(x)$ and, thus, $\Psi_n(x)$ must divide $\Phi_n(x)$.

Since each divides the other and each is monic, we conclude that $\Phi_n(x) = \Psi_n(x)$. Clearly, the degree of $\Phi_n(x)$ is $\phi(n)$. \square

(b): Show that $\prod_{\substack{d|n \\ d>0}} \Phi_d(x) = x^n - 1$, and deduce that $\sum_{\substack{d|n \\ d>0}} \phi(d) = n$.

Proof. Since the roots of $x^n - 1$ are precisely the n th roots of unity, we see that, in $\overline{\mathbb{Q}}$, we can factor $x^n - 1$ as

$$x^n - 1 = \prod_{j=1}^n (x - \zeta_n^j).$$

Thus, simply grouping appropriately and using the fact that $\Phi_d = \prod_{\substack{1 \leq m \leq d \\ (m,d)=1}} (x - \zeta_d^m)$, which we showed in (a) above, we see that

$$x^n - 1 = \prod_{j=1}^n (x - \zeta_n^j) = \prod_{\substack{d|n \\ d>0}} \prod_{\substack{1 \leq m \leq d \\ (m,d)=1}} (x - \zeta_d^m) = \prod_{\substack{d|n \\ d>0}} \Phi_d(x).$$

Obviously, $\deg(x^n - 1) = n$. On the other hand, since $x^n - 1 = \prod_{\substack{d|n \\ d>0}} \Phi_d(x)$,

$$n = \deg(x^n - 1) = \deg \left(\prod_{\substack{d|n \\ d>0}} \Phi_d(x) \right) = \sum_{\substack{d|n \\ d>0}} \deg \Phi_d(x) = \sum_{\substack{d|n \\ d>0}} \phi(d)$$

by the result proved above. \square

(c): Let $K_n = \mathbb{Q}(\zeta_n)$. What is $[K_n : \mathbb{Q}]$?

Answer: Since $\Phi_n(x)$ is the minimal polynomial of ζ_n ,

$$K_n \simeq \mathbb{Q}[x]/(\Phi_n(x)),$$

which is a degree $\phi(n)$ extension of \mathbb{Q} , since Φ_n is irreducible of degree $\phi(n)$. Hence, $[K_n : \mathbb{Q}] = \phi(n)$. \clubsuit

(d): Show that K_n is Galois over \mathbb{Q} .

Proof. Since \mathbb{Q} is characteristic 0, it suffices to show that K_n is normal over \mathbb{Q} . However, this is clear, because the roots of $\Phi_n(x)$ are simply powers of ζ_n , so $\Phi_n(x)$ splits in K_n ; that is, K_n is the splitting field of $\Phi_n(x)$ (and, in fact, of $x^n - 1$), so K_n is normal over \mathbb{Q} . \square

3

Let K be a field, and let x_1, \dots, x_n be transcendentals over K . For $i = 1, \dots, n$, let s_i be the i th symmetric polynomial in x_1, \dots, x_n .

(a): Show that $K(x_1, \dots, x_n)$ is the splitting field over $K(s_1, \dots, s_n)$ of the polynomial $Z^n - s_1 Z^{n-1} + s_2 Z^{n-2} - \dots + (-1)^n s_n$.

Proof. Consider the product

$$\prod_{i=1}^n (Z - x_i).$$

Then, when we multiply out this product, the coefficient on x^k will be $(-1)^k s_k$, so

$$\prod_{i=1}^n (Z - x_i) = Z^n - s_1 Z^{n-1} + s_2 Z^{n-2} - \dots + (-1)^n s_n.$$

Hence, we see that the roots of this polynomial are precisely the x_i , so $K(x_1, \dots, x_n)$ is the splitting field over $K(s_1, \dots, s_n)$ of this polynomial. \square

(b): Show that the extension $K(s_1, \dots, s_n) \subset K(x_1, \dots, x_n)$ is Galois.

Proof. Since the minimal polynomial of x_i must divide $Z^n - s_1 Z^{n-1} + s_2 Z^{n-2} - \dots + (-1)^n s_n$, which has all distinct roots, so the minimal polynomial of x_i is separable. Since this is true for all $i = 1, \dots, n$, we see that the extension $K(s_1, \dots, s_n) \subset K(x_1, \dots, x_n)$ is separable. On the other hand, since we saw in (a) that $K(x_1, \dots, x_n)$ is the splitting field of the polynomial $Z^n - s_1 Z^{n-1} + s_2 Z^{n-2} - \dots + (-1)^n s_n$, this extension is also normal and, therefore, Galois. \square

(c): Show that the Galois group is the symmetric group S_n .

Proof. First, note that any permutation $\sigma \in S_n$ corresponds to an automorphism ϕ_σ of $K(x_1, \dots, x_n)$ where $\phi_\sigma(x_i) = x_{\sigma(i)}$ and $\phi_\sigma|_K = id_K$, since the x_i are algebraically independent. Hence, if we can show that for each $\sigma \in S_n$, $\phi_\sigma|_{K(s_1, \dots, s_n)}$ is the identity map, then this will imply that there is a copy of S_n contained in G . However, this is clear, because, since s_i is symmetric for all i ,

$$\phi_\sigma(s_i) = s_i$$

for all $i = 1, \dots, n$ and all $\sigma \in S_n$. Thus, $S_n \subset G$. Note that this implies that $\#G \geq \#S_n = n!$.

On the other hand, consider the notation $L = K(s_1, \dots, s_n)$. Then $[L(x_1) : L] \leq n$, since the minimal polynomial of x_1 must divide $f(Z) = Z^n - s_1 Z^{n-1} + s_2 Z^{n-2} - \dots + (-1)^n s_n = (Z - x_1) \prod_{i=2}^n (Z - x_i)$. In turn, $[L(x_1, x_2) : L(x_1)] \leq n - 1$, since the minimal polynomial of x_2 over $L(x_1)$ divides $\frac{f(Z)}{Z - x_1}$, which has degree $n - 1$. Iterating in

this fashion, we see that $[L(x_1, \dots, x_k) : L(x_1, \dots, x_{k-1})] \leq n - k + 1$ and, in turn, that

$$[L(x_1, \dots, x_n) : L] = [L(x_1, \dots, x_n) : L(x_1, \dots, x_{n-1})] \cdots [L(x_1) : L] \leq 2 \cdot 3 \cdots (n-1) \cdot n = n!.$$

Since $L(x_1, \dots, x_n) = K(x_1, \dots, x_n)$ and since this is a Galois extension of L , we know that

$$\#G = [K(x_1, \dots, x_n)] \leq n!$$

Since we've shown that $n! \leq \#G \leq n!$, we conclude that, in fact, $\#G = n!$. Since $\#S_n = n!$ and $S_n \subset G$, this in turn implies that $G \simeq S_n$. \square

4

Let L be a normal field extension of K , and let K_0 be the maximal purely inseparable extension of K contained in L . View L as contained in a fixed algebraic closure \bar{K} of K .

(a): Let $\beta \in L$, and let $\beta_1, \dots, \beta_n \in \bar{K}$ be the distinct images of β under the K -embeddings $L \hookrightarrow \bar{K}$. Let $f(x) = \prod (x - \beta_i)$. Show that $f(x) \in K_0[x]$.

Proof. Since L is normal over K , every K -embedding $L \hookrightarrow \bar{K}$ is an automorphism of L , so it must be that case that all of the β_i are in L . Hence, $f(x) \in L[x]$. Now, as in Problem 3(a) above, the coefficients of $f(x)$ are just the elementary symmetric polynomials s_1, \dots, s_n in β_1, \dots, β_n . Furthermore, again as in 3(a), any K -automorphism of L simply permutes the β_i , so the s_i are fixed by any such automorphism. Thus, since $s_i \in L$ for each $i = 1, \dots, n$ and every s_i is fixed by every K -automorphism of L , we see that each s_i is purely inseparable over K and, therefore, must be contained in the maximal purely inseparable extension of K contained in L . Therefore, we conclude that $f(x) \in K_0[x]$. \square

(b): In part (a), show that $f(x)$ is the minimal polynomial of β over K_0 .

Proof. Since the identity map is certainly a K -automorphism of L , $\beta = \beta_i$ for some i . Hence, $f(\beta) = 0$, so the minimal polynomial of β over K_0 must divide $f(x) \in K_0[x]$. Now, note that if ψ is a K -automorphism of L , then $\psi|_{K_0}$ defines a K -embedding of K_0 into $L \subset \bar{K}$; since K_0 is purely inseparable, there is only one K -embedding $K_0 \hookrightarrow \bar{K}$, so we see that $\psi|_{K_0} \equiv id$. Therefore, ψ is also a K_0 -automorphism of L . Therefore, every K -conjugate of β is also a K_0 -conjugate of β , i.e. all the β_i are images of β under K_0 -embeddings $L \hookrightarrow \bar{K}_0 = \bar{K}$. Hence, since every conjugate of β must be a factor of its minimal polynomial over K_0 , we see that the minimal polynomial of β must be divisible by $f(x)$. Therefore, since

the minimal polynomial and f mutually divide each other and both are monic, we conclude that $f(x)$ is the minimal polynomial of β over K_0 . \square

(c): Conclude that L is separable over K_0 .

Proof. Since our choice of β in part (a) was arbitrary, we see that the minimal polynomial over K_0 of every element of L is separable, which implies that L is separable over K_0 . \square

5

Let $K = \mathbb{F}_p(t)$ and let $L = K[\sqrt[p]{t}]$, where p is an odd prime number.

(a): Find the maximal separable extension K' of K in L , and the maximal purely inseparable extension K_0 of K in L .

Answer: As we've seen, the minimal polynomial of $\sqrt[p]{t}$ over K is $x^p - t$. Let $\alpha = \sqrt[p]{t}$. Now, in L , we can factor this as

$$x^{2p} - t = (x^p - \sqrt{t})(x^p + \sqrt{t}) = (x^p - \alpha^p)(x^p + \alpha^p) = (x - \alpha)^p(x + \alpha)^p;$$

since $p \neq 2$, $\alpha \neq -\alpha$, so we see that there are two distinct roots of the minimal polynomial of α over K . Hence, there are two distinct embeddings $L \hookrightarrow \bar{K}$, and so $[L : K]_{\text{sep}} = 2$. Thus, if we can find an intermediate separable extension of degree 2, this must be the maximal separable extension K' of K in L . Our choice, is clear, however: since $\sqrt{t} = \alpha^p \in L$, consider $K[\sqrt{t}]$. \sqrt{t} has separable minimal polynomial

$$(x - \sqrt{t})(x + \sqrt{t}) = x^2 - t \in K[x],$$

so $K' = K[\sqrt{t}]$ is the maximal separable extension of K in L .

On the other hand, since $[L : K] = [L : K]_{\text{sep}}[L : K]_{\text{insep}}$ and $[L : K] = 2p$, $[L : K]_{\text{sep}} = 2$, we know that $[L : K]_{\text{insep}} = p$. Now, $\sqrt[p]{t}$ has minimal polynomial $x^p - t = (x - \sqrt[p]{t})^p$ over K , so we see that $K_0 = K[\sqrt[p]{t}]$ is purely inseparable. Since it is an extension of degree p , we conclude that it is the maximal purely inseparable extension of K in L .

♣

(b): Show *explicitly* in this example that L is the compositum of K' and K_0 , by expressing $\sqrt[p]{t}$ as a combination of elements from K' and K_0 .

Proof. Certainly, it suffices to show that we can express $\sqrt[p]{t}$ as a combination of elements from K' and K_0 . Now, $\sqrt{t} \in K'$ and $(\sqrt{t})^{\frac{p-1}{2}} \in K_0$, since p is odd and thus $p - 1$ is divisible by 2. In

turn, this implies that $\frac{1}{(\sqrt[p]{t})^{\frac{p-1}{2}}} \in K_0$. Now,

$$\frac{\sqrt{t}}{(\sqrt[p]{t})^{\frac{p-1}{2}}} = \frac{\sqrt[p]{t^p}}{\left(\sqrt[p]{t^2}\right)^{\frac{p-1}{2}}} = \frac{\sqrt[p]{t^p}}{\sqrt[p]{t^{p-1}}} = \sqrt[p]{\frac{t^p}{t^{p-1}}} = \sqrt[p]{t}.$$

Hence, we see that, indeed, $\sqrt[p]{t}$ is the combination of elements of K' and K_0 , so L is the compositum of K' and K_0 . \square

(c): What if instead $p = 2$?

Answer: If $p = 2$, then $\alpha \sqrt[2]{t} = -\sqrt[2]{t}$, and so the minimal polynomial for α ,

$$x^{2p} - t = (x - \alpha)^p(x + \alpha^p) = (x - \alpha)^{2p}$$

has only a single root. Since every K -embedding of L into \bar{K} must map α to a root of this polynomial, this implies that there is only a single such K -embedding, so L is purely inseparable over K . Hence, $K' = K$, $K_0 = L$ and it's trivially true that L is the compositum of K' and K_0 .

