

MATH 511B, SOLUTIONS TO HW 7

1. The polynomial $x^4 + 2$ is Eisenstein at 2, hence irreducible. To make life easy for ourselves, in this problem we consider all our extensions of \mathbb{Q} to be contained inside \mathbb{C} .

Let $\sqrt[4]{-2}$ denote the root of $x^4 + 2$ in the first quadrant of \mathbb{C} and let $K = \mathbb{Q}(\sqrt[4]{-2})$, a field of degree 4 over \mathbb{Q} . The splitting field of $x^4 + 2$ is obtained by adjoining i to K , so it remains to determine whether this is an extension of degree 2, or whether it is an extension of degree 1, i.e., whether or not K already contains i .

Suppose $\mathbb{Q}(\sqrt[4]{-2})$ contains i . Then it contains $\mathbb{Q}(\sqrt{-2}, i)$; by a previous problem set $\mathbb{Q}(\sqrt{-2}, i)$ has degree 4 over \mathbb{Q} , so we would have to have $\mathbb{Q}(\sqrt[4]{-2}) = \mathbb{Q}(\sqrt{-2}, i) = \mathbb{Q}(\sqrt{2}, i)$. If $\sqrt[4]{-2} \in \mathbb{Q}(\sqrt{2}, i)$, it can be written

$$\sqrt[4]{-2} = (a + b\sqrt{2}) + (c + d\sqrt{2})i.$$

Since $\arg(\sqrt[4]{-2}) = \pi/4$ we must have $c + d\sqrt{2} = a + b\sqrt{2}$, and

$$\sqrt[4]{-2} = (a + b\sqrt{2})(1 + i).$$

Raising both sides to the fourth power gives

$$-2 = (a + b\sqrt{2})^4(-4)$$

or

$$\frac{1}{2} = (a + b\sqrt{2})^4.$$

This implies that $(a + b\sqrt{2})^{-1}$ is a fourth root of 2, a contradiction since $x^4 - 2$ is irreducible hence cannot have a root in $\mathbb{Q}(\sqrt{2})$.

Therefore the splitting field of $x^4 + 2$ is $\mathbb{Q}(\sqrt[4]{-2}, i)$, an extension of \mathbb{Q} of degree 8.

2. Observe that $x^4 + x^2 + 1$ factors as $(x^2 + x + 1)(x^2 - x + 1)$, and that if ζ is a root of $x^2 - x + 1$ then $\zeta^6 = 1$ and ζ^2 is a root of $x^2 + x + 1$. It follows that the splitting field of $x^4 + x^2 + 1$ over \mathbb{Q} is obtained by adjoining a single root of $x^2 - x + 1$, and has degree 2 over \mathbb{Q} .

3. The polynomial $x^6 - 4$ factors as $(x^3 - 2)(x^3 + 2)$. We know from class that the splitting field of $x^3 - 2$ has degree 6 over \mathbb{Q} . But $r^3 = 2$ if and only if $(-r)^3 = -2$, so $x^3 + 2$ already splits over the splitting field of $x^3 - 2$. Therefore the splitting field of $x^6 - 4$ has degree 6 over \mathbb{Q} .

4. Let's do the easy direction first (the 'if' direction). If $K = F(\alpha_1, \dots, \alpha_n)$, let f_i be the minimal polynomial of α_i and put $f = f_1 \cdots f_n$. Then each f_i has a root in K and therefore splits in K , and K is the splitting field of f over F .

In the other direction, suppose that K is the splitting field of $f \in F[x]$, and fix an algebraic closure \overline{F} of F containing K . Suppose $g \in F[x]$ is irreducible with a

root $\alpha \in K$. Let β be any root of g in \overline{F} . Since g is irreducible, there exists a map of fields $\sigma : F(\alpha) \rightarrow \overline{F}$ fixing F and sending $\sigma(\alpha) = \beta$. By the extension theorem σ extends to a map $\sigma' : K \rightarrow \overline{F}$. Since $\sigma'(K)$ is isomorphic to K over F , it follows that $\sigma'(K)$ is a splitting field for f ; by the uniqueness of splitting fields we conclude $K = \sigma'(K)$. But $\beta = \sigma'(\alpha) \in \sigma'(K)$, so $\beta \in K$.

5. For (i), if K_i is the splitting field of f_i in K , then K_1K_2 is the splitting field of f_1f_2 . For (ii), suppose g is irreducible and has a root in $K_1 \cap K_2$. Then it has a root in K_1 , and also a root in K_2 . By the previous problem g splits in completely in K_1 , and also in K_2 ; therefore it splits completely in $K_1 \cap K_2$. Again by the previous problem, $K_1 \cap K_2$ is a splitting field.

6. It suffices to show that if $\alpha \in R \setminus \{0\}$ then $1/\alpha \in R$. Since $\alpha \in L$ and L/K is algebraic, the element α is algebraic over K , and in this case we know that $1/\alpha$ can be written as $1/\alpha = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}$ with the $c_i \in K$ and $n = [K(\alpha) : K]$. But $c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} \in R$, as desired.

For a counterexample when L/K isn't algebraic, let K be any field, let $L = K(t)$ with t an indeterminate, and take $R = K[t]$.

7. The interesting part of this problem is showing that there are infinitely many distinct fields lying between $\mathbb{F}_p(t, u)$ and $\mathbb{F}_p(t^p, u^p)$.

Solution 1: Here is one solution, which has the benefit of being extremely short and the drawback of not seeing the whole picture. For the latter, see solution 2 below. Let $K_\alpha = \mathbb{F}_p(t^p, u^p, t + \alpha u)$ where $\alpha \in \mathbb{F}_p(t^p, u^p)$. We wish to show that $K_\alpha \neq K_\beta$ if $\alpha \neq \beta$. Suppose $t + \beta u \in K_\alpha$. Then $(t + \beta u) - (t + \alpha u) = (\beta - \alpha)u \in K_\alpha$. Since $\beta - \alpha \in \mathbb{F}_p(t^p, u^p)$ we have $u \in K_\alpha$. But then $t = (t + \alpha u) - \alpha u \in K_\alpha$ as well, and so $\mathbb{F}_p(t, u) \subset K_\alpha$. This is a contradiction, and the claim follows.

Solution 2: The extension $\mathbb{F}_p(t, u)/\mathbb{F}_p(t^p, u^p)$ is purely inseparable of degree p^2 . Any extension lying strictly between $\mathbb{F}_p(t, u)$ and $\mathbb{F}_p(t^p, u^p)$ has degree p over $\mathbb{F}_p(t^p, u^p)$ and is of the form $\mathbb{F}_p(t^p, u^p, f(t, u))$ for some rational function $f(t, u) \in \mathbb{F}_p(t, u) \setminus \mathbb{F}_p(t^p, u^p)$. For $f, g \in \mathbb{F}_p(t, u) \setminus \mathbb{F}_p(t^p, u^p)$ we want a criterion that will often prove that $\mathbb{F}_p(t^p, u^p, f) \neq \mathbb{F}_p(t^p, u^p, g)$.

Suppose that $g \in \mathbb{F}_p(t^p, u^p, f)$. Since f has degree p over $\mathbb{F}_p(t^p, u^p)$ it follows that g may be written

$$g = a_0 + a_1f + \cdots + a_{p-1}f^{p-1}$$

with the $a_i \in \mathbb{F}_p(t^p, u^p)$. Differentiate both sides of this equation with respect to t . Since each a_i is a rational function in t^p , we have $\partial a_i / \partial t = 0$ for all i , and by the Leibniz rule we obtain

$$\frac{\partial g}{\partial t} = \left(\sum_{i=1}^{p-1} i a_i f^{i-1} \right) \frac{\partial f}{\partial t}.$$

Similarly

$$\frac{\partial g}{\partial u} = \left(\sum_{i=1}^{p-1} i a_i f^{i-1} \right) \frac{\partial f}{\partial u}.$$

Note that the factor on the right hand side is the same in both of these equations! It follows that f, g generate the same extension of $\mathbb{F}_p(t^p, u^p)$ only if the ratios $\frac{\partial f}{\partial t} / \frac{\partial f}{\partial u}$ and $\frac{\partial g}{\partial t} / \frac{\partial g}{\partial u}$ are equal. (At least when the denominators are both nonzero. One way to avoid having to deal with special cases like this is to say that f, g generate the same extension of $\mathbb{F}_p(t^p, u^p)$ only if $[\frac{\partial f}{\partial t} : \frac{\partial f}{\partial u}]$ and $[\frac{\partial g}{\partial t} : \frac{\partial g}{\partial u}]$ represent the same point in the projective space $\mathbb{P}^1(\mathbb{F}_p(t, u))$.)

To prove that there are infinitely many extensions lying between $\mathbb{F}_p(t, u)$ and $\mathbb{F}_p(t^p, u^p)$, it suffices to exhibit an infinite collection of elements $f \in \mathbb{F}_p(t, u)$ such that the ratios $\frac{\partial f}{\partial t} / \frac{\partial f}{\partial u}$ are all distinct. There are many ways to do this, but a particularly simple one is to consider $f_n = t^n + u$ where n is relatively prime to p . Then $\frac{\partial f_n}{\partial t} / \frac{\partial f_n}{\partial u} = nt^{n-1}$. Alternately, we can consider the subfields K_α from the first solution: if $f = t + \alpha u$ with $\alpha \in \mathbb{F}_p(t^p, u^p)$ then $\frac{\partial f_n}{\partial t} / \frac{\partial f_n}{\partial u} = 1/\alpha$.

It is natural to ask whether this argument has a converse. Indeed, we can prove:

Theorem: Suppose $f, g \in \mathbb{F}_p(t, u) \setminus \mathbb{F}_p(t^p, u^p)$. The pairs $[\frac{\partial f}{\partial t} : \frac{\partial f}{\partial u}]$ and $[\frac{\partial g}{\partial t} : \frac{\partial g}{\partial u}]$ represent the same point in the projective space $\mathbb{P}^1(\mathbb{F}_p(t, u))$ if and only if $\mathbb{F}_p(t^p, u^p, f) = \mathbb{F}_p(t^p, u^p, g)$. In other words, the extensions lying strictly between $\mathbb{F}_p(t, u)$ and $\mathbb{F}_p(t^p, u^p)$ are parameterized by the image of the map

$$\mathbb{F}_p(t, u) \setminus \mathbb{F}_p(t^p, u^p) \rightarrow \mathbb{P}^1(\mathbb{F}_p(t, u))$$

sending $f \mapsto [\frac{\partial f}{\partial t} : \frac{\partial f}{\partial u}]$.

Proof: Interchanging t and u if necessary, suppose without loss of generality that $u \notin \mathbb{F}_p(t^p, u^p, f)$. If we had $\partial f / \partial t = 0$ then f would lie in $\mathbb{F}_p(t^p, u)$, and so $\mathbb{F}_p(t^p, u^p, f) = \mathbb{F}_p(t^p, u)$; this contradicts our assumption on u , and therefore $\partial f / \partial t \neq 0$.

Now $\mathbb{F}_p(t, u) = \mathbb{F}_p(t^p, u^p)(f, u)$, and g may be written uniquely as

$$g = \sum_{0 \leq i, j < p} c_{ij} f^i u^j$$

with each $c_{ij} \in \mathbb{F}_p(t^p, u^p)$. Differentiating with respect to t yields

$$\frac{\partial g}{\partial t} = \left(\sum_{i,j} i c_{ij} f^{i-1} u^j \right) \frac{\partial f}{\partial t};$$

since $\partial f / \partial t \neq 0$ it follows by hypothesis on f and g that

$$\frac{\partial g}{\partial u} = \left(\sum_{i,j} i c_{ij} f^{i-1} u^j \right) \frac{\partial f}{\partial u}.$$

On the other hand, differentiating our expression for g with respect to u gives

$$\frac{\partial g}{\partial u} = \left(\sum_{i,j} j c_{ij} f^i u^{j-1} \right) + \left(\sum_{i,j} i c_{ij} f^{i-1} u^j \right) \frac{\partial f}{\partial u}.$$

Taking the difference gives

$$\sum_{0 \leq i, j < p} j c_{ij} f^i u^{j-1} = 0.$$

Since the elements $f^i u^j$ with $0 \leq i, j < p$ are a basis for $\mathbb{F}_p(t, u)$ over $\mathbb{F}_p(t^p, u^p)$, we deduce $c_{ij} = 0$ whenever $j \neq 0$. Thus $g = \sum c_{i0} f^i \in \mathbb{F}_p(t, u, f)$, as desired.

Finally, we have

Challenge: Determine which points in $\mathbb{P}^1(\mathbb{F}_p(t, u))$ have a representative $[r : s]$ such that $r = \partial f / \partial t$ and $s = \partial f / \partial u$ for some $f \in \mathbb{F}_p(t, u)$. Is it all of $\mathbb{P}^1(\mathbb{F}_p(t, u))$? (Equivalently: for which $c \in \mathbb{F}_p(t, u)$ does the differential equation $\frac{\partial f}{\partial u} = c \frac{\partial f}{\partial t}$ have a nonzero solution?)

8. Write $f = \sum a_i x^i$ and $g = \sum b_j x^j$. Then $fg = \sum_k \left(\sum_{i+j=k} a_i b_j \right) x^k$, hence

$$D(fg) = \sum_k \left(\sum_{i+j=k} (i+j) a_i b_j \right) x^{k-1}.$$

Now $D(g) = \sum j b_j x^{j-1}$, so

$$fD(g) = \sum_k \left(\sum_{i+j=k} j a_i b_j \right) x^{k-1}$$

and similarly

$$gD(f) = \sum_k \left(\sum_{i+j=k} i a_i b_j \right) x^{k-1}.$$

The result follows.

9. Let E be a splitting field of f over F . Then E is an extension of K in which f splits, so it contains a unique splitting field E' of f over K . By hypothesis f has distinct roots in E' . But since E is an extension of E' , the roots of f in E' coincide with the roots of f in E . Therefore f has distinct roots in E and is separable over F .

Alternately, note that the GCD of f and f' in $K[x]$ is identical to the GCD of f and f' in $F[x]$.

10. To see that $f = x^p - x - a$ is separable, note that its derivative f' is equal to -1 .

To prove the irreducibility of f , we first note that if r is any root of f , then $r^p = r + a$. Now if g is any polynomial over \mathbb{F}_p and if r is any root of g , then r^p is also a root of g : indeed $g(r^p) = g(r)^p = 0$. Therefore if g is an irreducible factor of f and r is a root of g (so also a root of f), $r^p = r + a$ is a root of g as well; inductively $r + na$ is a root of g for $n = 0, \dots, p-1$. It follows that g has at least p distinct roots, hence has degree at least p . We conclude that g must equal f , and f is irreducible.