

PS 9 Solutions

Math 256 Section 31

June 7, 2005

50.17) Let E be the splitting field of a set S of polynomials in $F[x]$. If $E = F$, then E is the splitting field of x over F . If $E \neq F$, then find a polynomial $f_1(x)$ in S that does not split in F , and form its splitting field, which is a subfield E_1 of E where $[E_1 : F] > 1$. If $E = E_1$, then E is the splitting field of $f_1(x)$ over F . If $E \neq E_1$, find a polynomial $f_2(x)$ in S that does not split in E_1 , and form its splitting field $E_2 \leq E$ where $[E_2 : E_1] > 1$. If $E = E_2$, then E is the splitting field of $f_1 f_2$ over F . If $E \neq E_2$, then continue the construction in the obvious way. E is a finite extension of F , so this process must eventually terminate with some $E_r = E$, which is the splitting field of $f_1 f_2 \dots f_r$ over F .

50.19) (\Rightarrow): Let $\alpha \in E \setminus F$. $\text{irr}(\alpha, F)$ splits in E since it has a zero (α) over F , so E contains all conjugates of α over F .

(\Leftarrow): Let σ an automorphism of \bar{F} fixing F . For each $\alpha \in E$, we must have $\sigma(\alpha) \in E$. So $\sigma(E) \subset E$. σ^{-1} is also an automorphism fixing F , so we see that $\sigma^{-1}(E) \subset E$. Thus $E \subset \sigma(E) \subset E$, so σ restricted to E is onto, and thus an automorphism of E . By Theorem 50.3, E is a splitting field.

51.11) Let K be a finite extension of E . We need that K is a separable extension of E . Let $\alpha \in K$. $[K : E] < \infty$, so α is algebraic over E , and as E is algebraic over F , we have that α is algebraic over F , so we may consider $\text{irr}(\alpha, F)$. F is perfect, so α is a zero of $\text{irr}(\alpha, F)$ of multiplicity 1. $\text{irr}(\alpha, E)$ divides $\text{irr}(\alpha, F)$, so α is a zero of $\text{irr}(\alpha, E)$ of multiplicity 1, so α is separable over E . Thus K is separable over E .

51.15) Let $f(x) = \sum a_i x^i$ and $g(x) = \sum b_i x^i$.

a) $D(f(x) + g(x)) = D(\sum (a_i + b_i)x^i) = \sum i(a_i + b_i)x^{i-1} = \sum ia_i x^{i-1} + \sum ib_i x^{i-1} = D(f(x)) + D(g(x))$

b) F

c) $F[x^p]$

51.16) a) $D(af(x)) = D(\sum aa_i x^i) = \sum ia a_i x^{i-1} = a \sum ia_i x^{i-1} = aD(f(x))$

b) (outline only) If $\deg(fg) = 0$ then $f, g \in F$, so $f' = g' = 0$. Assume for $n < k$, prove for $n = k > 0$. Write $f(x) = h(x) + a_r x^r$, where $\deg(h) < \deg(f)$

and $a_r \neq 0$ and similarly for g . Multiply, take derivatives, apply the induction hypothesis, and simplify.

c) Induct on m . $m = 1$: $D((f(x))^1) = (f(x))^0 f'(x)$ reduces to $D(f(x)) = f'(x)$. Assume for $m < k$. For $m = k$: $D(f(x)^k) = D(f(x)f(x)^{k-1}) = f(x)[(k-1)f(x)^{k-2}f'(x)] + f'(x)f(x)^{k-1} = [f(x)(k-1)f(x)^{k-2} + f(x)^{k-1}]f'(x) = kf(x)^{k-1}f'(x)$

51.17) $f(\alpha) = 0$, so in $\overline{F}[x]$, let $f(x) = (x - \alpha)^\nu g(x)$ where $g(\alpha) \neq 0$ and $\nu \geq 1$. Then by exercise 16, $f'(x) = (x - \alpha)^\nu g'(x) + \nu(x - \alpha)^{\nu-1}g(x)$. Since $\nu \geq 1$, $f'(\alpha) = 0^\nu g'(\alpha) + \nu 0^{\nu-1}g(\alpha) = \nu 0^{\nu-1}g(\alpha)$. This is zero iff $\nu > 1$.

51.18) Suppose α is a zero of an irreducible polynomial, $f \in F[x]$. $\deg f'(x) < \deg f(x)$ so $f'(\alpha) \neq 0$, so by exercise 17, α is a zero of multiplicity 1. All zeros have the same multiplicity, so all have multiplicity 1, so $f(x)$ is separable.

51.19) (\Rightarrow): If every exponent of q is divisible by p , then $q(x) = g(x^p)$ for some polynomial g over F . Then $g(x) = (x - \alpha^p)h(x)$ in $\overline{F}[x]$. If $q(\alpha) = 0$ then $g(\alpha^p) = 0$ so we may factor to get $g(x) = (x - \alpha^p)h(x)$ in $\overline{F}[x]$. Then $q(x) = (x^p - \alpha^p)h(x^p) = (x - \alpha)^p h(x^p)$, so α is a root of multiplicity at least p , so q is not separable.

(\Leftarrow): Following the argument for exercise 18, we see that $q'(\alpha) \neq 0$ unless $q' = 0$. $q' = 0$ iff each exponent of each term in q is divisible by p . If this is not the case, then $q'(\alpha) \neq 0$ so α has multiplicity 1 by exercise 17 and so q is a separable polynomial.