MATH 259: Homework #4

Jesse Farmer

27 April 2005

1. *Suppose L/E and E/F are field extensions. Let $\alpha \in L$ be algebraic over F. Prove or disprove that $[E(\alpha) : E]$ divides $[F(\alpha) : F]$.*

   I am almost certain this is false, but don't know how to show it.

2. *Find a splitting field $F/\mathbb{Q}$ for each of the following polynomials. Also find the degree and a primitive element for each extension.*

   (a) $x^4 - 5x^2 + 6$

   This polynomial is reducible into $(x^2 - 2)(x^2 - 3)$, so that $\mathbb{Q}(\sqrt{3}, \sqrt{2})$ is a splitting field over $\mathbb{Q}$. From previous assignments it follows that $[\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}] = 6$ and $\mathbb{Q}(\sqrt{3}, \sqrt{2}) = \mathbb{Q}(\sqrt{3} + \sqrt{2})$ so that $\sqrt{2} + \sqrt{3}$ is a primitive element.

   (b) $x^4 - 5$

   This polynomial factors over $\mathbb{C}$ as $(x - \sqrt[4]{5})(x + \sqrt[4]{5})(x - i\sqrt[4]{5})(x + i\sqrt[4]{5})$. Hence the splitting field is $\mathbb{Q}(i, \sqrt[4]{5})$ since any strictly smaller field extension of $\mathbb{Q}$ will not contain one of the generators, and the two generators are linearly independent over $\mathbb{Q}$. Since the minimal polynomial of i over $\mathbb{Q}(\sqrt[4]{5})$ is still $x^2 + 1$, the degree of the extension is 8.

   From one of the following exercises it follows that $\mathbb{Q}(i, \sqrt[4]{5}) = \mathbb{Q}(i + \sqrt[4]{5})$, since over the splitting field we have $i - \alpha_i \neq \sqrt[4]{5} - \beta_j$ for all i, j where α_i, β_j are roots of generators' respective minimal polynomials, except for the case where $\alpha_i = i$ and $\beta_j = \sqrt[4]{5}$.

3. *Find a splitting field E of $x^3 - 5$ over $\mathbb{F}_7$, $\mathbb{F}_{11}$, and $\mathbb{F}_{13}$. In each case determine $|E|$.*

   Since any finite field extension of $\mathbb{F}_p$ is of the form $\mathbb{F}_{p^n}$ for some n, and these fields are constructed as the splitting field of the polynomial $x^{p^n} - x$, it suffices to find a field extension of $\mathbb{F}_p$ such that every root of $x^3 - 5$ is a root of $x^{p^n} - x$ where n is the smallest such positive integer. Reducing this polynomial it therefore suffices to find a smallest $n \in \mathbb{N}$ such that $x^{p^n - 1} - 1 = 0$ modulo p. In all the cases below equality denotes congruence modulo p, for the respective primes in consideration. Let $f(x) = x^3 - 5$.

   For $\mathbb{F}_7$ there are no roots contained in the field itself since every cube modulo 7 is congruent to either 1 or 6. Let α be a root of f so that $\alpha^3 = 5$. Then for $n = 2$, $\alpha^{48} = 5^{16} = 2$ modulo 7. However, for $n = 3$, this becomes $\alpha^{342} = 5^{114} = 1$ modulo 7. Hence the splitting field of f over $\mathbb{F}_7$ is $\mathbb{F}_{343}$.

   For $\mathbb{F}_{11}$ there is a root in the field, namely $\alpha = 3$, but no other roots. Consider $n = 2$. Then if α is a root of f, $\alpha^{120} = 5^{40} = 1$ modulo 11. Hence the splitting field of f over $\mathbb{F}_{11}$ is $\mathbb{F}_{121}$.

   For $\mathbb{F}_{13}$ there are two roots in the field, namely, $\alpha = 7$ and $\alpha = 11$, but no other roots. Again, consider $n = 2$. Then if α is a root of f, $\alpha^{168} = 5^{56} = 1$ modulo 13. Hence the splitting field of f over $\mathbb{F}_{13}$ is $\mathbb{F}_{169}$.

4. *Let F be a field and $f, g \in F[x]$ with $\deg f, \deg g > 0$. Show that $\gcd(g, f) \neq 1$ if and only if f and g have a common root α, with $\alpha \in E$ for some field extension E/F.*

If f and g have a common root α in some field extension E/F then the minimal polynomial of α, h, has $\deg h > 0$ and $h \mid g$ and $h \mid f$. Hence h is a common divisor, and $\gcd(g, f) \neq 1$.

Conversely, if $\gcd(f, g) \neq 1$ then there exists a polynomial $h \in F[x]$ with $\deg h > 0$ which divides both f and g. Let E be the splitting field of h over F. Then for any root $\alpha \in E$ of h, $f(\alpha) = g(\alpha) = h(\alpha) = 0$, i.e., f and g share a common root.

5. *Let $F(\alpha)/F$ be a simple extension with α separable over F. Suppose* $\operatorname{char} F = p > 0$. *Show that* $F(\alpha) = F(\alpha^p)$.

   Since α is separable, $F(\alpha)/F$ is a separable extension. Consider $F(\alpha)/F(\alpha^p)$. Let f be the minimal polynomial of α over $F(\alpha^p)$. Then α is a root of $g(x) = x^p - \alpha^p$. Since $\operatorname{char} F = p$, $g(x) = (x - \alpha)^p$ over $F(\alpha)$. But then $f \mid g$, and f has no multiple roots since $F(\alpha)/F(\alpha^p)$ is also a separable extension. Hence $f(x) = x - \alpha \in F(\alpha^p)[x]$ and $\alpha \in F(\alpha^p)$.

6. Let F be a field and $x^p - a$, $x^p - b$, p a prime, be two irreducible polynomials in $F[x]$. Suppose that $\operatorname{char} F \neq p$. Let $E = F(\alpha, \beta)$ with $\alpha^p = a$, $\beta^p = b$, and $[E : F] = p^2$. Show that $\alpha + \beta$ is a primitive element of E/F.

   Let $F_1 = F(\alpha)$. Then $F_1(\beta) = F_1(\alpha + \beta) = E$ and $p^2 = [E : F] = [E : F_1][F_1 : E]$ which implies $[E : F_1] = p$. Assume for contradiction that $F(\alpha + \beta) \neq E$. Then $\alpha + \beta \notin F$ since that would imply $\alpha + \beta \in F_1$ and hence $\beta \in F_1$, contradicting that $[E : F_1] = p$.

   Then $[E : F(\alpha, \beta)] > 1$ so that $p^2 = [E : F(\alpha, \beta)][F(\alpha, \beta) : F]$ implies that $[F(\alpha, \beta) : F] = p$. Let f be the minimal polynomial of $\alpha + \beta$ over F. Since $[F_1(\alpha + \beta) : F_1] = p$, it is also the minimal polynomial of $\alpha + \beta$ over F_1. Define $g(x) = (x - \alpha)^p - b$. Then $g(\alpha + \beta) = 0$ and $f \mid g$. Write $f = gh$ for some $h \in F_1[x]$. Since $\deg g = \deg f$, $\deg h = 1$, but as g is monic it must be that $h = 1$. Hence $g = f$, which means that, in fact, $g \in F[x]$. But the coefficient of x^{p-1} in g is $-p\alpha$ by calculation. Since $\operatorname{char} F \neq p$, it follows that $\alpha \in F$, contradicting the fact that $x^p - a$ is irreducible.

   Therefore $F(\alpha + \beta) = F(\alpha, \beta)$.

7. *Let E/F be a field extension and $\alpha, \beta \in E$ be algebraic over F with minimal polynomials f, g of degree m and n, respectively. Write $f = \prod_{i=1}^{m}(x - \alpha_i)$ and $g = \prod_{i=1}^{n}(x - \beta_i)$ with $\alpha_1 = \alpha$ and $\beta_1 = \beta$. If $\alpha - \alpha_i \neq \beta - \beta_j$ for all i, j show that $F(\alpha, \beta) = F(\alpha + \beta)$.*

   From the proof that separable extensions are simple, we know that if $c \in F$ satisfies $g(c(\alpha - \alpha_i) + \beta)$ for all $2 \leq i \leq m$ then $F(\alpha, \beta) = F(\alpha + \beta)$. But for $c = 1$ this becomes $\alpha - \alpha_i + \beta \neq \beta_j$ for any j with $1 \leq j \leq n$, and i with $1 \leq i \leq m$.

   However, the hypothesis in the statement of the exercise seems to be backwords. Namely, we want $\alpha - \alpha_i \neq \beta_j - \beta$, rather than the condition given.

8. *Deduce from the previous exercise that* $\mathbb{Q}(\sqrt[3]{p}, \sqrt[3]{q}) = \mathbb{Q}(\sqrt[3]{p} + \sqrt[3]{q})$ *where p, q are prime.*

   The minimal polynomial of $\sqrt[3]{p}$ is $x^3 - p$, which splits into

$$(x - \sqrt[3]{p})\left(\frac{\sqrt[3]{p} + i\sqrt{3}\sqrt[3]{p}}{2}\right)\left(\frac{\sqrt[3]{p} - i\sqrt{3}\sqrt[3]{p}}{2}\right)$$

   For p, q distinct primes, these factors satisfy the conditions of the previous exercise (as no cube root of two distinct primes will ever be rational multiples of one another) and therefore $\mathbb{Q}(\sqrt[3]{p}, \sqrt[3]{q}) = \mathbb{Q}(\sqrt[3]{p} + \sqrt[3]{q})$.

9. *Let F be a field and E/F the splitting field of $x^n - 1$. Define $\mu_n = \{\zeta \in E \mid \zeta^n = 1\}$. If* $\operatorname{char} F = 0$ *or* $\operatorname{char} F = p \nmid n$ *show that μ_n is a cyclic subgroup of E^* of order n.*

   In general μ_n is a cyclic group (of some order) since if $\alpha, \beta \in \mu_n$ then $(\alpha\beta)^n = \alpha^n\beta^n = 1$, and it is known that any subgroup of the multiplicative group of a field is cyclic. Consider the polynomial $x^n - 1$. Its derivative is nx^{-1}, which has a zero only at $x = 0$ for fields of characteristic 0 or fields of prime characteristic p which do not divide n. Hence, for such fields, every root of $x^n - 1$ is distinct and the splitting field of $x^n - 1$ has order n. That is, μ_n is a cyclic subgroup of E^* of order n.