MATH 259: Homework #1

Jesse Farmer

04 April 2005

1. *Show that $p(x) = x^3 + 9x + 6$ is irreducible in $\mathbb{Q}[x]$. Let θ be a root of $p(x)$. Find the inverse of $1 + \theta$ in $\mathbb{Q}(\theta)$.*

   p is irreducible by Eisenstein's theorem. Note that $1 + \theta$ is a root of

   $$p(1 - x) = (1 - x)^3 + 9(1 - x) + 6 = x^3 - 3x^2 + 12x - 4$$

   Therefore, by Example 5 on pp. 516, it follows that

   $$(1 + \theta)^{-1} = \frac{(\theta + 1)^2 - 3(\theta + 1) + 12}{4} = \frac{\theta^2 + \theta - 10}{4}$$

2. *Show that $x^3 - 2x - 2$ is irreducible over $\mathbb{Q}$ and let θ be a root. Compute $(1+\theta)(1+\theta+\theta^2)$ and $\frac{1+\theta}{1+\theta+\theta^2}$ in $\mathbb{Q}(\theta)$.*

   Let $p(x) = x^3 - 2x - 2$. Since $\deg p = 3$, it is reducible if and only if it has a rational root, but neither $\pm 2, \pm 1$ are roots. So, by the rational roots theorem p has no roots and is therefore irreducible. Any root θ of p satisfies $\theta^3 = 2\theta + 2$, so

   $$(1 + \theta)(1 + \theta + \theta^2) = 1 + 2\theta + 2\theta^2 + \theta^3 = 3 + 4\theta + 2\theta^2$$

3. *Prove directly that the map $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ is an isomorphism of $\mathbb{Q}(\sqrt{2})$.*

   This map is a bijection since it is its own left and right inverse. Denote this map by φ, then

   $$\varphi(a + b + (c + d)\sqrt{2}) = a + b - (c + d)\sqrt{2} = a - c\sqrt{2} + b - d\sqrt{2} = \varphi(a + b\sqrt{2}) + \varphi(c + d\sqrt{2})$$

   and

   $$\varphi(ac + 2bd + (ad + bc)\sqrt{2}) = ac + 2bc - (ad + bc)\sqrt{2} = (a - b\sqrt{2})(c - d\sqrt{2}) = \varphi(a + b\sqrt{2})\varphi(c + d\sqrt{2})$$

   Therefore φ is, indeed, an isomorphism.

4. *Show that if α is a root of $a_n x^n + \cdots + a_1 x + a_0$ then $a_n\alpha$ is a root of the monic polynomial $x^n + a_{n-1}x^{n-1} + a_n a_{n-2} x^{n-2} + \cdots + a_n^{n-2} a_1 x + a_n^{n-1} a_0$.*

   Let the latter polynomial be denoted by $f(x)$ and the former by $g(x)$ then

   $$f(a_n\alpha) = (a_n\alpha)^n + \sum_{i=0}^{n-1} a_n^{n-1-i} a_i (a_n\alpha)^i = a_n^n \alpha^n + \sum_{i=0}^{n-1} a_n^{n-1} a_i \alpha^i = a_n^{n-1} g(\alpha) = 0$$

5. *Suppose the degree of the extension K/F is a prime p. Show that any subfield E of K containing F is either K or F.*

   In this case, $F \subset E \subset K$. Let $[K : F] = p$ be prime, and $[K : E] = n$, $[E : F] = m$. Then we know that $p = mn$, which implies that either $m = 1$ or $n = 1$, i.e., either $K = E$ or $F = E$.

6. *Prove that if $[F(\alpha) : F]$ is odd then $F(\alpha) = F(\alpha^2)$.*

   $\alpha^2 \in F(\alpha)$, so $F(\alpha^2)$ is a field extension of $F(\alpha)$. Hence we have $F \subset F(\alpha^2) \subset F(\alpha)$. Then if $[F : F(\alpha)]$ is odd both $[F(\alpha) : F(\alpha^2)]$ and $[F(\alpha^2) : F]$ must be odd. Assume for contradiction that $\alpha \notin F(\alpha^2)$. Then the polynomial $x^2 - \alpha^2$ is irreducible over $F(\alpha^2)$, and is therefore the minimal polynomial for α over $F(\alpha)^2$. However, this implies that $[F(\alpha) : F(\alpha^2)] = 2$, contradicting the fact that $[F(\alpha) : F]$ is odd. Hence $\alpha \in F(\alpha^2)$, and $F(\alpha^2) = F(\alpha)$.

7. *Determine the degree of $\mathbb{Q}(\sqrt{3 + 2\sqrt{2}})$ over $\mathbb{Q}$.*

   Note that $(1 + \sqrt{2})^2 = 3 + 2\sqrt{2}$, so that $\sqrt{3 + 2\sqrt{2}} = 1 + \sqrt{2}$. This has a minimal polynomial of degree two, viz., $x^2 - 2x - 1$, so $\mathbb{Q}(\sqrt{3 + 2\sqrt{2}})$ has degree 2 over $\mathbb{Q}$.

8. *Suppose $F = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$ where $\alpha_i^2 \in \mathbb{Q}$ for $1 \le i \le n$. Prove that $\sqrt[3]{2} \notin F$.*

   If $\sqrt[3]{2} \in F$ then $\mathbb{Q}(\sqrt[3]{2})$ would be a subfield of F. However $[F : \mathbb{Q}]$ is a power of 2, since, if any minimal polynomial over $\mathbb{Q}$ becomes reduced in once of the larger field extensions, its degree would simply become 1. This is a contradiction since $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ and certainly cannot divide any power of 2.

9. *Let f be an irreducible polynomial of degree n over a field F and $g \in F[x]$. Prove that every irreducible factor of the composite polynomial $f \circ g$ has degree divisible by n.*

   Let α be any root of $f \circ g$ (in its splitting field, say). It is sufficient to prove that $[F(\alpha) : F]$ is divisible by n for all such α. Since f is irreducible and $g(\alpha)$ is a root of f, it follows that $[F((g(\alpha)) : F] = n$. But $F(g(a))$ is a subfield of $F(\alpha)$, and hence $n \mid [F(\alpha) : F]$ since

   $$[F(\alpha) : F] = [F(\alpha) : F(g(\alpha))] \cdot [F(g(\alpha)) : F]$$

10. *Let E/F be a field extension and $\alpha_i \in E$ algebraic over F for $1 \le i \le n$. Show that*

    $$[F(\alpha_1, \dots, \alpha_n) : F] \le \prod_{i=1}^{n} m_i$$

    where m_i is the degree of the minimal polynomial of α_i over F.

    We can write

    $$[F(\alpha_1, \dots, \alpha_n) : F] = \prod_{i=1}^{n} [F(\alpha_1, \dots, \alpha_i) : F(\alpha_1, \dots, \alpha_{i-1})]$$

    where $F(\alpha_0)$ is defined as F. Each $[F(\alpha_1, \dots, \alpha_i) : F(\alpha_1, \dots, \alpha_{i-1})]$ is bounded by m_i, since α_i has a minimal polynomial of degree m_i over F, and so that same polynomial has α_i as a root when its coefficients are in $F(\alpha_1, \dots, \alpha_{i-1})$. It could, of course, be the case that what was the minimal polynomial is now reducible over $F(\alpha_1, \dots, \alpha_{i-1})$, which is why strict equality might not hold. The inequality follows immediately.

11. *Suppose $[E : F] = p$, where p is a prime. Show that for every $\alpha \in E \setminus F$, $E = F(\alpha)$.*

    Let $\alpha \in E \setminus F$, then $F \subset F(\alpha) \subset E$. Note that it is sufficient to show that $[E : F(\alpha)] = 1$, since any finite extension is algebraic and hence is an extension by an element with degree 1. If $[E : F]$ is prime, then $[E : F(\alpha)][F(\alpha) : F]$ is also prime. Since $\alpha \notin F$, F is strictly contained in F, and hence $[E : F(\alpha)] = 1$, so that $E = F(\alpha)$.

12. *Let $[E : F] = n$ and $\alpha \in E$. Show that* $\deg f \mid n$ *where f is the minimal polynomial of α over F.*

    Note that $F(\alpha) \subset E$ since $\alpha \in E$. Then $[F(\alpha) : F] = \deg f$, and therefore $n = m \cdot \deg f$, where $m = [E : F(\alpha)]$.

13. *Let $E = F(\alpha)$ where α is algebraic over F. Let F' be a subfield of E contained in F, and let g be the minimal polynomial of α over F', and f the minimal polynomial of α over F. Let $[E : F] = n$ and $m = \deg g$. Show that $f = gh$ for some $h \in F'[x]$ and n is a multiple of m.*

We can treat f as a polynomial in $F'[x]$ since $F \subset F'$. It follows then that there exists some h such that $f = gh + r$ where $\deg r < \deg g$. Since $f(\alpha) = g(\alpha) = 0$, it follows that $r(\alpha) = 0$. But as g is the minimal polynomial of α over F', r must be identically 0, and hence $f = gh$. That n is a multiple of m follows from the equality $n = [E : F] = [E : F'][F' : E] = m[F' : E]$.

14. *Let E/F be a field extension and $\alpha \in E$ be algebraic over F. Let F' be a subfield of E contained in F. Let $f \in F[x]$ be an irreducible polynomial such that $f(\alpha) = 0$ and $\deg f = n$. Show that f is irreducible in $F'[x]$ if and only if $[F'(\alpha) : F'] = n$.*

    Let g be the minimal polynomial of α over F'. Then $[F'(\alpha) : F'] = \deg g$. If f is irreducible over F', then $f = c \cdot g$ for some constant $c \in F'^{*}$, so that $\deg f = \deg g = n$. Conversely, if $[F'(\alpha) : F'] = n$, then $\deg g = n$. If f were reducible over F' then there would exist an irreducible polynomial of degree less than n with α as a root, contradicting the minimality of g.

15. *Let F, F', E be subfields of a field L. Suppose $[E : F] = n$ and $F \subset F'$ with $[F' : F] = m$. Suppose m, n are relatively prime. Let $EF' = F'E$ denote the subfield of L generated by $F' \cup E$. Show that $[F'E : F] = mn$. Compute $[F'E : F']$.*

    Write $F' = F(\beta_1, \ldots, \beta_s)$ and $E = F(\alpha_1, \ldots, \alpha_r)$. Then

    $$EF' = F(\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s)$$

    . In particular one sees that,

    $$[F(\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_{s-i}) : F(\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_{s-i-1})] \leq [F(\beta_1, \ldots, \beta_{s-i}) : F(\beta_1, \ldots, \beta_{s-i-1})]$$

    This is because any polynomial irreducible over $F(\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_{s-i-1})]$ is certainly irreducible over $F(\beta_1, \ldots, \beta_{s-i-1})$. However, as previously, the product of all the elements on the left-hand side of the inequality is equal to $[EF' : E]$, while the product of those on the right-hand side is equal to $[F' : F] = m$. Hence $[EF' : F] = [EF' : E][E : F] \leq mn$. Writing

    $$[EF' : F] = [EF' : E][E : F] = [EF' : F'][F' : F]$$

    shows that both m and n divide $[EF' : F]$. Since m and n are relatively prime it follows that $mn \mid [EF' : F]$, and therefore that $[EF : F] = mn$. It follows that $[EF' : F'] = n$ and $[EF' : E] = m$.

16. *In the above, let $E = F(\alpha)$ and $[E : F] = n$. Let $f \in F[x]$ be the minimal polynomial of α over F. Show that f is irreducible over F'.*

    In this case, $EF' = F'(\alpha)$, and from a previous problem we know f is irreducible over F' if and only if $[F'(\alpha) : F] = n$. But as $[F' : F]$ is relatively prime to n by hypothesis, exactly that follows from the previous problem. Hence f is irreducible over F'.

17. *Let $E = F(\alpha)$ be a subfield of L and F' a subfield of L such that $F \subset F'$ with $[F' : F] = 2$. Let $f \in F[x]$ be an irreducible sextic with $f(\alpha) = 0$. Show that f is irreducible over F' or f is a product of irreducible cubics in $F'[x]$.*