PMAT 431, Fall 2004

Solution to Assignment 5

1. Section 6.2 #32: Let p and q in $\mathbb{C}$ satisfy $\sqrt{p} \notin \mathbb{Q}$ and $\sqrt{q} \notin \mathbb{Q}(\sqrt{p})$.

   (a) Show that $\mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\sqrt{p} + \sqrt{q})$.

   (b) Use Theorem 5 to find a basis of $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ over $\mathbb{Q}$.

   (c) Deduce that $x^4 - 2(p+q)x^2 + (p-q)^2$ is the minimal polynomial of $\sqrt{p} + \sqrt{q}$ over $\mathbb{Q}$.

   Solution.

   (a). Write $E = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ and $u = \sqrt{p} + \sqrt{q}$. We have $u^2 = (p+q) + 2\sqrt{pq}$, so

   $$u^3 = (\sqrt{p} + \sqrt{q})(p+q) + 2(\sqrt{p} + \sqrt{q})\sqrt{pq} = (p+3q)\sqrt{p} + (3p+q)\sqrt{q}.$$

   Substituting $\sqrt{q} = u - \sqrt{p}$ leads to $u^3 = (3p+q)u + 2(q-p)\sqrt{p}$. Hence $2(q-p)\sqrt{p}$ is in $\mathbb{Q}(u)$ so, since $p \neq q$, $\sqrt{p} \in \mathbb{Q}(u)$. Then $\sqrt{q} = u - \sqrt{p} \in \mathbb{Q}(u)$, so $E \subseteq \mathbb{Q}(u)$. $\mathbb{Q}(u) \subseteq E$ is clear.

   (b). Write $L = \mathbb{Q}(\sqrt{p})$. Since $x^2 - p$ is irreducible over $\mathbb{Q}$, $\{1, \sqrt{p}\}$ is a $\mathbb{Q}$-basis of L. We have $E = \mathbb{Q}(\sqrt{p}, \sqrt{q}) = L(\sqrt{q})$ and we claim $\{1, \sqrt{q}\}$ is an L-basis of E. For this it suffices to show that $x^2 - q$ is irreducible over L, that is it has no root in L. But $\pm\sqrt{q}$ are the only roots of $x^2 - q$ in $\mathbb{R}$, so it suffices to show $\sqrt{q} \notin L$. But this is true by assumption. Hence, this shows $\{1, \sqrt{q}\}$ is an L-basis of E. By Theorem 5, $\{1, \sqrt{p}, \sqrt{q}, \sqrt{pq}\}$ is a $\mathbb{Q}$-basis of E.

   (c). We have $u^2 = (p+q) + 2\sqrt{pq}$, so $[u^2 - (p+q)]^2 = 4pq$. This gives

   $$u^4 - 2(p+q)u^2 + (p+q)^2 = 4pq, \qquad \text{that is} \qquad u^4 - 2(p+q)u^2 + (p-q)^2 = 0.$$

   Thus $f(u) = 0$ where $f(x) = x^4 - 2(p+q)x^2 + (p-q)^2$. If $m(x)$ is the minimal polynomial of u over $\mathbb{Q}$, this shows $m(x) | f(x)$. But $\deg[m(x)] = [\mathbb{Q}(u) : \mathbb{Q}] = [E : \mathbb{Q}] = 4$ by (b), so we have $m(x) = f(x)$ as required (both are monic).

2. Section 6.3 #3: If $2 \neq 0$ in the field F, show that the splitting field E of $x^4 + 1$ over F is a simple extension of F and factor $x^4 + 1$ completely in $E[x]$. What happens if $2 = 0$ in F?

   Solution. Let $u \in E$ be a root of $x^4 + 1$. Then $-u$ is a root, distinct from u because $2 \neq 0$. Thus u^{-1} and $-u^{-1}$ are distinct roots, and if either equals $\pm u$ then $u^{-2} = (\pm u)^2 = u^2$, so $u^4 = 1$, a contradiction (since $2 \neq 0$). Hence $E = F(u)$ and $x^4 + 1 = (x-u)(x+u)(x-u^{-1})(x+u^{-1})$. If $2 = 0$ then $x^4 + 1 = (x+1)^4$ splits over F itself.

3. Section 6.3 #4(d): Find the splitting field E of $f(x) = x^3 - x + 1$ over $F = \mathbb{Z}_3$.

   Solution. $f(x)$ is irreducible over $\mathbb{Z}_3$—no root. If u is a root in E then $f(x) = (x-u)(x^2 + ux + (u^2 - 1))$. Now $-2 = 1$ in $\mathbb{Z}_3$ so $x^2 + ux + u^2 = (x-u)^2$. Hence $f(x) = (x-u)[(x-u)^2 - 1] = (x-u)(x-(u+1))(x-(u-1))$, so $E = \mathbb{Z}_3(u)$.

4. Section 6.3 #14: Let p be a prime and let $w = e^{2\pi i/p}$, a pth root of unity. Show that $\mathbb{Q}(w)$ is the splitting field of $x^p - 1$ over $\mathbb{Q}$, and that $[\mathbb{Q}(w) : \mathbb{Q}] = p - 1$. [Hint: Example 13 §4.2.]

   Solution. The roots of $x^p - 1$ are $1, w, w^2, \ldots, w^{p-1}$ (Theorem 4) so $\mathbb{Q}(w)$ is the splitting field. We have $x^p - 1 = (x-1)\Phi_p(x)$ where $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ is the pth cyclotomic polynomial. Then Φ_p is irreducible over $\mathbb{Q}$ by Example 13 §4.2. Since w is a root of Φ_p, $[\mathbb{Q}(w) : \mathbb{Q}] = p - 1$ by Theorem 4 §6.2.

5. Section 6.4 #22: (a) Let f be a monic irreducible polynomial of degree n in $\mathbb{Z}_p[x]$. Show that $f(x)$ divides $x^{p^n} - x$ in $\mathbb{Z}_p[x]$. [Hint: Theorem 3 §6.2 and Exercise 8 §4.1.]

   (b) Show that the degree of each monic irreducible divisor $f(x)$ of $x^{p^n} - x$ is a divisor of n. [Hint: Theorem 5.]

   (c) Factor $x^8 - x$ into irreducibles in $\mathbb{Z}_2[x]$.

   Solution. Write $h(x) = x^{p^n} - x$.

   (a). Let $K \supseteq \mathbb{Z}_p$ be a field containing a root u of f. Since f is irreducible, it is the minimal polynomial of u over $\mathbb{Z}_p$. If $E = \mathbb{Z}_p(u)$ then $[E : \mathbb{Z}_p] = n$ and so $|E| = p^n$. Then u is a root of $h(x)$ so $f(x) | h(x)$ in $E[x]$, say $h = qf$. But $h = q_0 f + r$ in $\mathbb{Z}_p[x]$ by the division algorithm, so this holds in $E[x]$. By the uniqueness in $E[x]$, we get $q = q_0 \in \mathbb{Z}_p[x]$ and $r = 0 \in \mathbb{Z}_p[x]$.

   (b). Let $h(x) = f(x)g(x)$. Write $K = GF(p^n)$. Then K is the splitting field of h and so splits f. So let $u \in K$ be a root of f and write $E = \mathbb{Z}_p(u)$. Since f is irreducible, $[E : \mathbb{Z}_p] = m$ where $m = \deg\ f$. Hence $|E| = p^m$ so $E \subseteq K$ implies $m | n$ by Theorem 5.

   (c). Since $h(x) = x^8 - x = x^{2^3} - x$, the irreducible divisors are of degree 1 or 3 by (b). Then

   $$x^8 - x = x(x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) = x(x-1)(x^3 + x + 1)(x^3 + x^2 + 1).$$