MATH 259: Homework #2

Jesse Farmer

13 April 2005

1. *Let E/F be a field extension with $f, g \in F[x]$, both irreducible over F. Let $\alpha, \beta \in E$ be such that $f(\alpha) = g(\beta) = 0$. Show that f is irreducible in $F(\beta)[x]$ if and only if g is irreducible in $F(\alpha)[x]$.*

   By the symmetry of the proposition it is sufficient to prove this statement in one direction only. Let $n = \deg f$ and $m = \deg g$. If g is irreducible over $F(\alpha)$ then $[F(\alpha, \beta) : F(\alpha)] = m$ and $[F(\alpha, \beta) : F] = mn$. But then $mn = [F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\beta)][F(\beta) : F] = [F(\alpha, \beta) : F(\beta)]m$, so that $[F(\alpha, \beta) : F(\beta)] = n$ and therefore f is irreducible over $F(\beta)$.

2. *Let E/F be a field extension with $[E : F] = p$, a prime. Show that for all $\alpha \in E \setminus F$, $F(\alpha) = E$.*

   Since $\alpha \in E \setminus F$ we have $F \subsetneq F(\alpha) \subseteq E$, so that $[F(\alpha) : F] \neq 1$. Then

   $$p = [E : F] = [E : F(\alpha)][F(\alpha) : F]$$

   Since $[F(\alpha) : F] \neq 1$ and p is prime it follows that $[E : F(\alpha)] = 1$ and therefore $E = F(\alpha)$.

3. *Compute the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$.*

   The minimal polynomial is $x^4 - 10x + 1$, which has $\sqrt{2} + \sqrt{3}$ and is irreducible by applying Eisentein to the polynomial at $x = y + 1$.

4. *Let p, q be primes. Show that $\mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\sqrt{p} + \sqrt{q}) = \mathbb{Q}(\sqrt{p} + 2\sqrt{q})$.*

   The polynomial $x^4 - 2(p+q) + (p-q)^2$ is a minimal polynomial for $\sqrt{p} + \sqrt{q}$ over $\mathbb{Q}$. Since $\mathbb{Q}(\sqrt{p} + \sqrt{q}) \subseteq \mathbb{Q}(\sqrt{p}, \sqrt{q})$ and they have the same degree over $\mathbb{Q}$, it follows that they must be equal. Similarly, the minimal polynomial of $\sqrt{p} + 2\sqrt{q}$ is $x^4 - 2(p + 4q) + (p - 4q)^2$. This is a subfield of $\mathbb{Q}(\sqrt{p}, \sqrt{2})$, also, and has degree 4 over $\mathbb{Q}$. Therefore all three quadratic fields are equal.

5. (a) *Let E/F be a quadratic extention of F and suppose $ch(F) \neq 2$. Show that there exists an $\alpha \in F$ such that $\alpha^2 = d \in F$ and $\alpha \notin F$ and $E = F(\alpha)$.*

   Pick some $\alpha \in E \setminus F$, which is possible since $[E : F] = 2$. Since E/F is a finite extension it is also algebraic, and therefore α is a root of the polynomial

   $$f(x) = x^2 + bx + c$$

   for some $b, c \in F$. We know from previous lectures that the quadratic formula is defined for fields with $\mathrm{ch}(F) \neq 2$. That is,

   $$\alpha = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

   Since $\mathrm{ch}(F) \neq 2$, it follows that $4c = 0$ if and only if $c = 0$ and so $\sqrt{b^2 - 4c}$ is a number whose square is in F, but which is not in F itself. To see that $F(\alpha) = F' := F(\sqrt{b^2 - 4c})$ is clear: $F(\alpha) \subset F'$ from the quadratic equation, and the opposite inclusion is true since $\sqrt{b^2 - 4c} = \pm(b + 2\alpha)$. From the second problem it follows that, in fact, $F' = E = F(\sqrt{b^2 - 4c})$.

(b) *Let E/F be a quadratic extension with $ch(F) \neq 2$. Let $E = F(\alpha) = F(\beta)$ with $\alpha^2 = d \in F$ and $\beta^2 = h \in F$. Then $\beta = \alpha \cdot c$ for some $c \in F^*$. Consversely, if $\beta = \alpha \cdot c$ for $c \in F^*$ then $F(\beta) = F(\alpha) = E$.*

The converse is immediate as it implies that $\alpha = \beta \cdot c^{-1} \in F(\beta)$ and $\beta = \alpha \cdot c \in F(\alpha)$. To show the opposite implication write $\alpha = x\beta + y$ for some $x, y \in F$. $x \in F^*$ since, if $x = 0$ then $\alpha \in F$. So it is sufficient to show that $y = 0$. But $\alpha^2 = (x\beta)^2 + 2xy\beta + y^2$, so that $2xy\beta \in F$. As $\beta \in E \setminus F$ and $x \neq 0$, the only way this is possible is if $y = 0$, and hence $\alpha = \beta \cdot c$, or $\beta = \alpha \cdot c^{-1}$.

(c) *Let $F/\mathbb{Q}$ be a quadratic field with $F \subset \mathbb{C}$. Show that $F = \mathbb{Q}(\sqrt{n})$ whewre $n = p_1 \cdots p_n$, $p_i \neq p_j$ are prime if $F \subset \mathbb{R}$. Otherwise, if $F \not\subset \mathbb{R}$, then $F = \mathbb{Q}(\sqrt{-n})$ for n as above.*

From the first part it follows that $\mathbb{Q}(\sqrt{\frac{m}{n}}) = \mathbb{Q}(\sqrt{mn})$ since $\sqrt{\frac{m}{n}} \cdot n = \sqrt{mn}$. Hence it suffices to consider the case of $\mathbb{Q}(\sqrt{n})$ where $n \in \mathbb{Z}$. If $F \subset \mathbb{R}$ then clearly $n \in \mathbb{Z}_+$. Assuming it is not a perfect square, since then $F = \mathbb{Q}$, we can reduce the powers of any prime dividing n to 1 since $p^{\lfloor \frac{k}{2} \rfloor}\sqrt{p^{k-2\lfloor \frac{k}{2} \rfloor}} = \sqrt{p^k}$, where $k - 2\lfloor \frac{k}{2} \rfloor = 1$ if k is odd and 0 otherwise. Hence $\mathbb{Q}(\sqrt{n}) = \mathbb{Q}(\sqrt{p_1 \cdots p_j})$ where each p_i is a prime divisor of n and $p_i \neq p_j$ if $i \neq j$.

(a) *Let $A = \{p_1, \dots, p_n\}$ be distinct primes. Let $E_i = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_i})$. Show for any two such subsets $B = \{p_{i_1}, \dots, p_{i_s}\}$ and $C = \{p_{j_1}, \dots, p_{j_r}\}$ of A that*

$$\mathbb{Q}(\sqrt{p_{i_1} \cdots p_{i_s}}) = \mathbb{Q}(\sqrt{p_{j_1} \cdots p_{j_r}})$$

if and only if $B = C$. Show that if M_n is the set of all quadratic fields of this form, where $p_{i_k} < p_{i_{k+1}}$ (i.e., we discount permutations of the primes) then $|M_n| = 2^n - 1$.

Obviously if $B = C$ then the two quadratic fields are equal. If $B \neq C$ then we can write

$$n\sqrt{p_{i_1} \cdots p_{i_s}} = m\sqrt{p_{j_1} \cdots p_{j_r}}$$

for some $m, n \in \mathbb{Z}_+$ by the previous part. Squaring both sides and cancelling any common prime numbers among B and C leaves us with $\sqrt{p_{k_1} \cdots p_{k_t}} = \frac{m}{n}$, which is impossible if $t > 0$. It must therefore be the case that $\frac{m}{n} = 1$ and that $B = C$.

So see that $|M_n| = 2^n - 1$, encode the membership of the various p_i as a binary number, with a 1 in the i^{th} position if p_i is among the p_{j_k} in C. Each n-digit binary number represents a unique quadratic extension by the above, and hence $|M_n| = 2^n - 1$, which is the number of n-digit binary numbers.

(b) *With notation as above, show that the number of quadratic subfields of E_n is $2^n - 1$, i.e., M_n includes all the quadratic subfields.*

The same technique works here, after noting that if $E_i = E_j$ then $j = i$, since the square root of no prime is a rational multiple of another. Hence there is a bijection between subfields of E_k and k-digit binary numbers. In particular, the number of subfields of E_n is $2^n - 1$.

6. *Deduce from the previous exercise that $[\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n}) : \mathbb{Q}] = 2^n$.*

   This follows immediately since $[E_i : E_{i-1}] = 2$ for $1 \leq i \leq n$, where $E_0 = \mathbb{Q}$.

7. *Determine the splitting field and its degree over $\mathbb{Q}$ for $x^4 - 2$.*

   The splitting field for this polynomial is $\mathbb{Q}(i, \sqrt[4]{2})$. The degree is computed in exactly the same as the following exercise.

8. *Determine the splitting field and its degree over $\mathbb{Q}$ for $x^4 + 2$.*

   The splitting field of this polynomial is $\mathbb{Q}(i, \sqrt[4]{2})$ and it has degree 8. This can be seen as $\pm\sqrt[4]{2}$ are clearly a root of this polynomial, factoring this into two degree 2 polynomials over $\mathbb{Q}(\sqrt[4]{2})$. Adjoining i, which has a minimal polynomial of degree 2 over $\mathbb{Q}(\sqrt[4]{2})$, gives roots to these two polynomials and hence this is the splitting field, with degree $4 \cdot 2 = 8$ over $\mathbb{Q}$.

9. *Determine the splitting field and its degree over* $\mathbb{Q}$ *for* $x^4 + x^2 + 1$.

   The splitting field of this polynomial over $\mathbb{Q}$ is $\mathbb{Q}\left(\frac{1+i\sqrt{3}}{2}\right)$, which has a minimal polynomial of degree 2 over $\mathbb{Q}$ and therefore the splitting field has degree 2. Note that this polynomial is reducible over $\mathbb{Q}$ already since $x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 + x - 1)$.

10. *Determine the splitting field and its degree over* $\mathbb{Q}$ *for* $x^6 - 4$.

    Similarly, adjoining $\sqrt[3]{2}\zeta$ where ζ is a primitive third root of unity to $\mathbb{Q}$ splits this polynomial, which itself already factors over $\mathbb{Q}$ into $x^3 + 2$ and $x^3 - 2$. As $\sqrt[3]{2}\zeta$ has a minimal polynomial of degree 3, so does the splitting field over $\mathbb{Q}$.