MATH 259: Homework #3

Jesse Farmer

20 April 2005

1. *Let E/F be a field extension with $\alpha, \beta \in E$ such that $[F(\alpha) : F] = m$ and $[F(\beta) : F] = p$, where p is prime and $1 \leq p < m$.*

   (a) *Show that $[F(\alpha, \beta) : F] = mp$.*
   Since $F(\alpha)$ and $F(\beta)$ are subfields of $F(\alpha, \beta)$,
   $$kp = [F(\alpha, \beta) : F(\beta)][F(\beta) : F] = [F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\alpha)][F(\alpha) : F] = jm$$
   for some $j, k \in \mathbb{N}$. Since $p < m$, p cannot divide m it must be that so $p \mid j$. Moreover, $m < p$ implies $k < j$ so that $j \mid p$ and hence $j = p$. Therefore $jm = mp = [F(\alpha, \beta) : F]$.

   (b) *Suppose* $\operatorname{char} F \neq p$. *Show that $F(\alpha, \beta) = F(\alpha + \beta)$.*
   We have $F(\alpha, \beta) = F(\alpha)(\alpha + \beta) = F(\alpha)(\beta)$. From the previous part $[F(\alpha, \beta) : F(\alpha)] = p$, so that $[F(\alpha)(\alpha + \beta) : F(\alpha)] = p$, also.

   (c) *For distinct primes p, q compute $[\mathbb{Q}(\sqrt[q]{p}, \sqrt[p]{q}) : \mathbb{Q}]$ and show that $\mathbb{Q}(\sqrt[q]{p}, \sqrt[p]{q}) = \mathbb{Q}(\sqrt[q]{p} + \sqrt[p]{q})$.*
   The minimal polynomials of $\sqrt[q]{p}$ and $\sqrt[p]{q}$ over $\mathbb{Q}$ are $x^q - p$ and $x^p - q$, which are easily seen to be irreducible by Eisenstein. Therefore $[Q(\sqrt[q]{p} : \mathbb{Q}] = q$ and $[Q(\sqrt[p]{q} : \mathbb{Q}] = p$. Since $p \neq q$ either $p < q$ or $q < p$, so by the first part $[\mathbb{Q}(\sqrt[q]{p}, \sqrt[p]{q}) : \mathbb{Q}] = pq$. The second statement follows directly from (b) since $\operatorname{char} \mathbb{Q} = 0$.

   (d) *Show that $\mathbb{Q}(\sqrt[p]{2}, \sqrt[q]{2}) = \mathbb{Q}(\sqrt[p]{2} + \sqrt[q]{2})$ when p and q are distinct primes.*
   The minimal polynomials of $\sqrt[p]{2}$ and $\sqrt[q]{2}$ are $x^p - 2$ and $x^q - 2$, which are irreducible by Eisenstein. Since $p \neq q$ it must be the case that $p < q$ or $q < p$, so by the first part $[\mathbb{Q}(\sqrt[p]{2}, \sqrt[q]{2}) : \mathbb{Q}] = pq$. Then, again, by the second part, $\mathbb{Q}(\sqrt[p]{2}, \sqrt[q]{2}) = \mathbb{Q}(\sqrt[p]{2} + \sqrt[q]{2})$.

2. *Let $E/\mathbb{Q}$ and $E'/\mathbb{Q}$ be field extensions and $\sigma : E \to E'$ a ring homomorphism. Show that $\sigma \mid_{\mathbb{Q}} = 1_{\mathbb{Q}}$, i.e., σ is a $\mathbb{Q}$-monomorphism.*

   This follows directly from known properties of ring homormorphisms, namely, that they fix both the multiplicative and additive identities and preserve multiplicative and additive inverses. Since E, E', and $\mathbb{Q}$ share the same identities by hypothesis it follows that $\sigma(1) = 1$ and $\sigma(-1) = -1$ so that $\sigma(m) = m$ for all $m \in \mathbb{Z}$ (since $\mathbb{Z}$ is generated by 1 or -1). But then $1 = \sigma(1) = \sigma(nn^{-1}) = n\sigma(n^{-1})$, for $n \in \mathbb{Z}$. Hence
   $$\sigma\left(\frac{p}{q}\right) = \frac{p}{q}$$
   for all $p, q \in \mathbb{Z}$, $q \neq 0$. Again, since $\sigma(0) = 0$ it follows that σ fixes all of $\mathbb{Q}$, i.e., σ is a $\mathbb{Q}$ monomorphism.

3. *Let E/F be a finite normal field extension and F' a field such that $F \subset F' \subset E$. Let $g \in F'[x]$ be irreducible with $g(\alpha) = 0$ for some $\alpha \in E$. Show that $g = c\prod(x - \alpha_i)$ for $c \in F'^*$, $\alpha_i \in E$, $1 \leq i \leq d = \deg g$.*

   Let f be the minimal polynomial of α over h. Then f splits into linear factors over E. Since α is a root of g there exists some $h \in F'[x]$ such that $f = gh$. But then since f splits into linear factors in E and E is a UFD, gh must split and, in particular, g must split times perhaps a leading coefficient in F'^*.

4. *Let M be a field and E_1, E_2, F subfields of M with $F \subset E_1$ and $F \subset E_2$. Assume E_1/F and E_2/F are both normal extensions. If they are also finite show that $(E_1E_2)/F$ and $(E_1 \cap E_2)/F$ are finite normal extensions.*

   If E_1/F and E_2/F are finite and normal then there exist polynomials $f_1, f_2 \in F[x]$ such that E_1/F and E_2/F are the splitting fields of f_1 and f_2, respectively. Then the product of these two polynomials splits in E_1E_2, and no smaller field can do so since E_1E_2 is by definition the smallest field containing both E_1 and E_1. Hence E_1E_2 is a splitting field for f_1f_2, and is therefore normal.

   If f is an irreducible polynomial with a root in $E_1 \cap E_2$ then by the normality of E_1 all of its roots are in E_1. Similarly, all of its roots are in E_2, also, and hence all of its roots are in $E_1 \cap E_2$. But then f certainly splits over $E_1 \cap E_2$ so that $(E_1 \cap E_2)/F$ is a normal extension.

5. *Let E/F be an algebraic (not necessarily finite) extension and let $\sigma : E \to E$ be an F-monomorphism. Show that* $\operatorname{im}\sigma = E$.

   Let $Z(f) = \{\alpha \in E \mid f(\alpha) = 0\}$. Since E/F is algebraic every $x \in E$ is in at least one $Z(f)$, namely, $Z(g)$ where g is the minimal polynomial of x over F. Then $E = \bigcup_{f \in F[x]} Z(f)$. To show that $\sigma(E) = E$ it therefore suffices to show that $\sigma(Z(f)) = Z(f)$. Let $\alpha \in Z(f)$, then there exists some constants in F such that

$$\alpha^n + \cdots + a_1\alpha + a_0 = 0$$

   Applying σ to this gives

$$\sigma(\alpha)^n + \cdots + a_1\sigma(\alpha) + a_0 = 0$$

   since σ is an F-monomorphism. Therefore $f(\sigma(\alpha)) = 0$ and $\sigma(\alpha) \in Z(f)$. Since σ is injective it has a left inverse, and the same argument applies to show that $\sigma^{-1}(Z(f)) \subset Z(f)$ so that $Z(f) \subset \sigma(Z(f))$. Then

$$\sigma(E) = \sigma\left(\bigcup_{f \in F[x]} Z(f)\right) = \bigcup_{f \in F[x]} \sigma(Z(f)) = \bigcup_{f \in F[x]} Z(f) = E$$

6. *Let E/F be a splitting field of $f \in F[x]$ where $\deg f = n \geq 1$. Show that $[E : F] \mid n!$.*

   This is obviously true for $n = 1$, so consider the $n - 1$ case. First assume f is irreducible. Then let $\alpha \in E$ be a root of f. Since f is irreducible it has the same degree as the minimal polynomial of α over F, and therefore $[F(\alpha) : F] = n$. But by the inductive hypothesis $[E : F(\alpha)] \mid (n-1)!$ so that

$$[E : F] = [E : F(\alpha)][F(\alpha) : F] \mid n(n-1)! = n!$$

   If f is reducible then write $f = f_1f_2$ where f_1 is irreducible over F and $\deg f_1 = m$. Let E' be the splitting field of f_1 over F. Then $E' \subset E$. Then $[E' : F] \mid m!$ and $[E : E'] \mid (n-m)!$ by the inductive hypothesis, so that $[E : F] \mid m!(n-m)! \mid n!$.

7. (a) *Compute* $\operatorname{Aut}(\mathbb{Q}(\sqrt[3]{2}))$.

   Any element of $\mathbb{Q}(\sqrt[3]{2})$ can be written as $a + b\sqrt[3]{4} + c\sqrt[3]{2}$ for $a, b, c \in \mathbb{Q}$. Since any homomorphism of $\mathbb{Q}(\sqrt[3]{2})$ fixes $\mathbb{Q}$ it must be that, for $\sigma \in \operatorname{Aut}(\mathbb{Q}(\sqrt[3]{2}))$,

$$\sigma(a + b\sqrt[3]{4} + c\sqrt[3]{2}) = a + b\sigma(\sqrt[3]{4}) + c\sigma(\sqrt[3]{2})$$

   Since $\sigma(\sqrt[3]{2}^3) = \sigma(2) = 2$, $\sigma(\sqrt[3]{2})^3 = 2$. But the only real number that satisfies this, and hence the only number in $\mathbb{Q}(\sqrt[3]{2})$, is $\sqrt[3]{2}$. Therefore $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$. From this $\sigma(\sqrt[3]{4})$ is completely determined as $2 = \sigma(\sqrt[3]{2})\sigma(\sqrt[3]{4})$, so that $\sigma(\sqrt[3]{4}) = \sqrt[3]{4}$. Therefore the only automorphism of $\mathbb{Q}(\sqrt[3]{2})$ is the identity map.

(b) *Is* $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ *normal?*

This extension is not normal because the irreducible polynomial x^3-2 has a root in $\mathbb{Q}(\sqrt[3]{2})$ but does not split over $\mathbb{Q}(\sqrt[3]{2})$, viz.,

$$x^3-2=(x-\sqrt[3]{2})(x^2+\sqrt[3]{2}x+\sqrt[3]{4})$$

The quadratic factor on the right hand side is irreducible over $\mathbb{Q}(\sqrt[3]{2})$.

(c) *Show that if* $[E:F]=2$ *then* E/F *is normal.*

If $[E:F]=2$ then there exists some $\alpha\in E$ such that $E=F(\alpha)$, and the minimal polynomial of α has degree 2. Call this polynomial f. Then f has at least one linear factor, viz., $x-\alpha$, and the remaining factor must also be linear by degree considerations. Therefore E/F is a splitting field for f, and hence normal.

(d) *Let* $F=\mathbb{Q}$, $F'=\mathbb{Q}(\sqrt{2})$, *and* $E=\mathbb{Q}(\sqrt[4]{2})$. *Show that* E/F' *and* F'/F *are finite normal, but* E/F *is not.*

Both E/F and F'/F are obviously finite. F'/F is normal since it is the splitting field of x^2-2 over $\mathbb{Q}$. Similarly, E/F' is normal since it is the splitting field of $x^2-\sqrt{2}$ over $\mathbb{Q}(\sqrt{2})$. E/F, however, is not normal, as x^4-2 has two roots in E, but does does not split over E. That is,

$$x^4-2=(x^2-\sqrt{2})(x^2+\sqrt{2})=(x-\sqrt[4]{2})(x+\sqrt[4]{2})(x^2+\sqrt{2})$$

and x^4-2 cannot be factored further.

8. (a) *Let* E/F *be a finite extension and* $E=F(\alpha_1,\dots,\alpha_r)$. *Let* f_i *be the minimal polynomial of* α_i *and define* $f=\prod f_i$. *Let* N/E *be a splitting field of* f *over* E. *Show that* N/F *is a normal extension.*

Since N/E is a finite extension which splits f it is also normal. Any irreducible polynomial $g\in F[x]$ is also a polynomial in $E[x]$, irreducible over F. If g is reducible over E then it can be factored into the product of irreducible polynomials over E, each of which splits in N by hypothesis. Since everything in consideration is a UFD, it follows that g splits into linear factors and therefore N/F is normal.

(b) *With* E *as above, let* M/F *be a finite normal extension with* $F\subset E\subset M$. *Let* $f=\prod f_i$ *so that* $f=\prod_{i=1}^n(x-\alpha_i)$, $n\geq r$. *Let* $N=F(\alpha_1,\dots,\alpha_n)$. *Show that* $|\mathrm{HomAlg}_F(E,M)|=|\mathrm{HomAlg}_F(E,N)|$.

Since each f_i has a root in M and M is normal, each f_i splits and hence their product, f, must split, too. But as N is the smallest field over which f splits, it must be that $N\subset M$. Hence any F-monomorphism from E into N is also an F-monomorphism into M by inclusion.

If $\sigma:E\hookrightarrow M$ is an F-monomorphism then $f(\sigma(\alpha_i))=0$, as in the fifth exercise. Hence $\sigma(\alpha_i)\in N$ and $\sigma(E)=F(\sigma(\alpha_1),\dots,\sigma(\alpha_r))\subset N$. So any such σ is in fact a monomorphism into N. Therefore $|\mathrm{HomAlg}_F(E,M)|=|\mathrm{HomAlg}_F(E,N)|$ and, in fact, the sets are equal.

(c) *With* E/F *and* f *in (a), let* N/E *and* N'/E *be splitting fields of* f *over* E. *Show that* $|\mathrm{HomAlg}_F(E,N)|=|\mathrm{HomAlg}_F(E,N')|$

Between two splitting fields N/E and N'/E of the same polynomial f there exists an isomorphism, say, τ, which fixes F. Then define a map by $\sigma\mapsto\tau\circ\sigma$. This is surjective since for any $\sigma:E\to N'$, $\tau^{-1}\circ\sigma:E\to N$ maps to σ. It is injective since if $\tau\circ\sigma_1=\tau\circ\sigma_2$ then $(\tau\circ sigma_1)(x)=(\tau\circ\sigma_1)(x)$ for all x, which implies that $\sigma_1(x)=\sigma_2(x)$ for all x by the injectivity of τ.

Therefore $|\mathrm{HomAlg}_F(E,M)|=|\mathrm{HomAlg}_F(E,N)|$.

(d) *With* E/F *as in (a), let* M/F *and* M'/F *be finite normal extensions with* $F\subset E\subset M$ *and* $f\subset E\subset M'$. *Show that* $|\mathrm{HomAlg}_F(E,M)|=|\mathrm{HomAlg}_F(E,M')|$.

By above there exist N/E, N'/E splitting fields of f with $N\subset M$ and $N'\subset M'$. Using the previous parts, it follows that

$$|\mathrm{HomAlg}_F(E,M)|=|\mathrm{HomAlg}_F(E,N)|=|\mathrm{HomAlg}_F(E,N')|=|\mathrm{HomAlg}_F(E,M')|$$