Solutions to Homework 8

1. Let L_1 and L_2 be two finite extensions of k inside of an extension L/k.

(*i*) Prove $[L_1L_2 : k] \leq [L_1 : k][L_2 : k]$.

(*ii*) Assume that $[L_1 : k]$ and $[L_2 : k]$ are relatively prime. Show that $[L_1L_2 : k] = [L_1 : k][L_2 : k]$. If we instead assume that $L_1 \cap L_2 = k$, then does the equality necessarily hold?

(*iii*) As an application of (*ii*), if $\alpha \in L$ is algebraic over k with $[k(\alpha) : k]$ relatively prime to $[L_1 : k]$, prove that $[L_1(\alpha) : L_1] = [k(\alpha) : k]$, and conclude that minimal polynomial for α over k is irreducible over L_1 and hence serves as the minimal polynomial for α over L_1.

(*i*) Since $[L_1L_2 : k] = [L_1L_2 : L_1][L_2 : k]$, it suffices to show $[L_1L_2 : L_1] \leq [L_2 : k]$. Let $\{e_i\}$ be a k-basis of L_2. Since the L_j's are finite algebraic over k, L_1L_2 consists of polynomials in elements of L_2 with coefficients in L_1, so L_1L_2 is spanned by the $\{e_i\}$ over L_1 (but possibly with linear dependence relations).

(*ii*) Since $[L_i : k]$ divides $[L_1L_2 : k]$, we see that $[L_1 : k][L_2 : k]$ divides $[L_1L_2 : k]$, so $[L_1 : k][L_2 : k] \leq [L_1L_2 : k]$. By Exercise 4.2 below, we have the reverse inequality. If we consider $L_i = \mathbf{Q}(a_i)$ with a_1 and a_2 two distinct cube roots of 2 in $\mathbf{C}$, so $a_1 = a_2\omega$ with ω a non-trivial cube root of 1, we see that $L_1L_2 = \mathbf{Q}(a_1, \omega)$ is a splitting field of $X^3 - 2$, and this has degree 6 over $\mathbf{Q}$, by the first part. Since $\mathbf{Q}(a_1) \neq \mathbf{Q}(a_2)$ (why?), we conclude that $\mathbf{Q}(a_1) \cap \mathbf{Q}(a_2) = \mathbf{Q}$ by degree considerations, so this furnishes a counterexample to the last part.

(*iii*) By previous parts, $[L_1(\alpha) : k] = [k(\alpha) : k][L_1 : k]$, so $[L_1(\alpha) : L] = [k(\alpha) : k]$. Thus, the minimal polynomial f for α over K is a monic in $K[X] \subseteq L[X]$ which has the same degree as the minimal polynomial for α over L, and vanishes at α. Thus, f is also the minimal polynomial for α over L.

2. (*i*) Let L_1 and L_2 be two quadratic extensions of k. Assume k does not have characteristic 2, so $L_i = k(a_i)$ with $a_i^2 = b_i \in k^\times$. Show that $L_1 \simeq L_2$ as extensions of k if and only if b_1/b_2 is a square in $k^\times$. Use this to give a complete list (without repetitions) of all quadratic extensions of $\mathbf{Q}$, up to isomorphism.

(*ii*) Consider the identification ι between isomorphism classes of quadratic extensions of k and the *group* $k^\times/k^{\times 2}$, as explained in (*i*). If L_1 and L_2 are two quadratic distinct extensions of k inside of an extension L/k, show that the composite L_1L_2 is a degree 4 extension of k and the non-trivial subextensions over k are L_1, L_2, and the field corresponding to the 'product' of L_1 and L_2 under ι.

(*i*) The 'if' is clear, since $b_1 = (b_1/b_2)b_2$. As for 'only if', suppose b_2 is a square in $k(\sqrt{b_1})$, so for some $x, y \in k$, $(x + ya_1)^2 = b_2$. This says that $b_2 = x^2 + b_1y^2$ and $2xya_1 = 0$. Since $2 \in k^\times$, $xy = 0$. Because $b_2 \notin k^{\times 2}$, we can't have $y = 0$, so $x = 0$ and $b_1/b_2 = y^2 \in k^{\times 2}$.

(*ii*) Say $L_i = k(\sqrt{b_i})$. Then $L_1L_2 = k(\sqrt{b_1}, \sqrt{b_2})$ is of degree 4 over k since the degree divides 4 and is at least 2, so if the composite degree weren't 4, we would have $L_1 = L_1L_2 = L_2$, a contradiction. The composite contains the quadratic subfield $k(\sqrt{b_1b_2})$, which we see is distinct from L_1 and L_2 since $L_1 \neq L_2$ and each $L_i \neq k$. This corresponds to the 'product' under ι.

It remains to check that L_1L_2 contains no other quadratic subfields over k. Say $k(\sqrt{b})$ lies in L_1L_2, with $b \in k^\times$ a non-square. Since $L_1(\sqrt{b})$ lies between $L_1 = k(\sqrt{b_1})$ and the quadratic extension L_1L_2, $L_1(\sqrt{b}) = L_1$ or $L_1(\sqrt{b}) = L_1L_2 = L_1(\sqrt{b_2})$. In the first case, $k(\sqrt{b}) = k(\sqrt{b_1})$. Consider the second case, so b/b_2 is a square in L_1, say $b/b_2 = (x + y\sqrt{b_1})^2 = x^2 + y^2b_1 + 2xy\sqrt{b_1}$. This forces $2xy = 0$, so x or y vanishes. Thus, $k(\sqrt{b}) = k(\sqrt{b_1b_2})$ or $k(\sqrt{b}) = k(\sqrt{b_2})$, respectively.

3. Let $f \in k[T, X]$, with f not divisible by any non-constants in $k[T]$ or $k[X]$. Show that f is irreducible when viewed in $k(X)[T]$ if and only if it is irreducible when viewed in $k(T)[X]$.

By Gauss' Lemma, both cases are equivalent to f being irreducible in $k[T, X]$ (since f has positive degree both in T and X, and no non-constant elements of $k[T, X]$ which are units in $k[T]$ or $k[X]$ can divide f, by hypothesis).

4. For each of the following extensions L/k, determine $[L : k]$ and find a basis for L as a k-vector space:

$k = \mathbf{Q}$, $L = \mathbf{Q}(a, b)$ with $a^2 = 6$, $b^3 = 2$

$k = \mathbf{C}(T)$, L is the splitting field of $X^n - T$ over k

$k = \mathbf{F}_p(T)$, L is the splitting field of $X^p - T$ over k, with p a prime (same p in both places!).

For the first one, the degree is 6 (by Exercise 1) and a basis is the set of $a^i b^j$ with $i = 0, 1$ and $j = 0, 1, 2$ (by the *proof* of the multiplicativity formula). In the second case, once we adjoin a single solution x to $X^n = T$, then we already have all of the others, since $X^n - 1$ splits completely over $\mathbf{C}$ (and hence over $\mathbf{C}(T)$). Since $X^n - T$ is irreducible over $\mathbf{C}(T)$ by Exercise 2, $[L : k] = n$ and a basis consists of x^i with $0 \le i < n$. A similar argument applies to any field in which $X^n - 1$ splits completely. This applies in particular to $n = p$ and the base field $\mathbf{F}_p(T)$, settling the final case.

5. Let L/K be a field extension, and $\alpha \in K$ be algebraic over L. Consider the multiplication map $m_\alpha : K(\alpha) \to K(\alpha)$ on the finite-dimensional K-vector space $K(\alpha) = K[\alpha]$. Using a matrix for this relative to a suitable basis, prove that the characteristic polynomial of this linear map is the minimal polynomial of α over K. In terms of this minimal polynomial, what are the trace and determinant of this map?

Let $f = X^d + a_{d-1}X^{d-1} + \cdots + a_0$ be the minimal polynomial of α over K. Since $K(\alpha) \simeq K[X]/f$ over K, $\{\alpha^i\}$ with $0 \le i < d$ is an ordered K-basis of $K(\alpha)$. With respect to this ordered basis, the matrix for T_α is

$$M = \begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -a_{d-1} \end{pmatrix}$$

In order to show that $\det(\lambda I - M) = f(\lambda)$, we expand along the right column. Be careful about powers of -1. The trace is $-a_{d-1}$ and the determinant is $(-1)^d$ times the constant term, which is to say $(-1)^d a_0$.

6. Prove that $f(X) = X^3 + 3X + 1$ is irreducible over $\mathbf{Q}$. If we let α denote a root of f in some extension, use the fact that f vanishes at α and $f(X-1)$ vanishes at $\alpha + 1$ to express $1/\alpha$ and $1/(\alpha+1)$ as quadratic polynomials in α with $\mathbf{Q}$ coefficients.

We can apply the rational root theorem (or apply Eisenstein to $f(X-1) = X^3 - 3X^2 + 6X - 3$ with $p = 3$) to prove irreducibility over $\mathbf{Q}$. Using the relation $f(\alpha) = 0$, we see that $\alpha \ne 0$ and $-(\alpha^2 + 3) = \alpha^{-1}$. Since $f(X-1)$ vanishes on $\beta = \alpha + 1 \ne 0$, we can express β^{-1} as a rational polynomial in β. Using $\beta = \alpha + 1$ then yields $\beta^{-1} = (1/3)\alpha^2 - (1/3)\alpha + 4/3$.

7. Prove that $X^4 - 5X^2 + 6$ and $X^4 + 5X^2 + 6$ are reducible over $\mathbf{Q}$ with splitting fields of degree 4 which you should describe concretely (give a basis and express in the form $\mathbf{Q}(\alpha)$ for suitable α).

Prove also that $X^4 - 5$ is irreducible over $\mathbf{Q}$ but with splitting field of degree 8 over $\mathbf{Q}$ which you should describe in terms of some field generators and a basis.

Since $X^4 - 5X^2 + 6 = (X^2 - 3)(X^2 - 2)$ and $2/3$ is not a square in $\mathbf{Q}$ (by a variety of arguments), by Exercise 1 we see that the splitting field is $\mathbf{Q}(a, b)$ with $a^2 = 3$ and $b^2 = 2$, and $\mathbf{Q}(a) \ne \mathbf{Q}(b)$, so the extension has degree 4. Since $(a+b)^2 = 5 + 2ab$, if $\mathbf{Q}(a+b)$ is not the entire splitting field, then $\mathbf{Q}(a+b) = \mathbf{Q}(ab) = \mathbf{Q}(\sqrt{6})$. But then $a + b$ is a $\mathbf{Q}$-linear combination of 1 and ab, contradicting the fact that 1, a, b, and ab are a basis of the splitting field over $\mathbf{Q}$. The case of $X^4 + 5X^2 + 6$ is done similarly.

Now consider $X^4 - 5$. This is irreducible over $\mathbf{Q}$ by Eisenstein, so if a is a root in a splitting field, then $\mathbf{Q}(a)/\mathbf{Q}$ has degree 4. From our knowledge of $\mathbf{C}$, this polynomial has four distinct roots in a splitting field, so the roots are of the form $a\zeta$, with ζ a set of 4 distinct roots of $X^4 = 1$. Taking ratios of roots of $X^4 - 5$, we see that a splitting field is a composite of subfields $\mathbf{Q}(a)$ and $\mathbf{Q}(\zeta)$ with $\zeta^4 = 1$ and $\zeta \ne 1, -1$ — that is, $\zeta^2 + 1 = 0$. Now $\zeta \notin \mathbf{Q}(a)$, since $\mathbf{Q}(a)$ admits a real embedding, yet $X^2 + 1$ has no roots in $\mathbf{R}$. So the splitting field $\mathbf{Q}(a, \zeta)$ is quadratic over $\mathbf{Q}(a)$ and therefore has degree 8 over $\mathbf{Q}$.

If you are interested, you might suspect $a + \zeta$ could be a primitive generator for the splitting field over $\mathbf{Q}$. To prove this without Galois theory, one way to is to somehow verify that $(a + \zeta)^i$ for $0 \le i \le 7$ are linearly independent over $\mathbf{Q}$. This can be done by expanding these all in terms of the basis $a^n \zeta^m$ ($0 \le n \le 3$, $0 \le m \le 1$) of the splitting field over $\mathbf{Q}$ and then computing the relevant 8 by 8 determinant is non-zero. Quite painful.