Shashank Singh
sss1@andrew.cmu.edu
21-373 Honors Algebraic Structures, Fall 2011
Assignment 8
Due: Monday, November 21

The following lemma is used in the below proofs.

Lemma 1: Let E be a field, and let F be a field extension of E. Then, if $a \in F$ is agebraic of degree $m \in \mathbb{N}$ over E, then $[E(a) : E] = m$.

Proof: Since a is algebraic of degree m, for $S = \{1, a, \dots, a^{m-1}\}$, S is linearly independent, as otherwise, since $\exists$ a non-trivial linear combination $q_0 + q_1 a + \dots + q_{m-1}a^{m-1}$ of elements in S, $\exists Q \in E[x]$ of degree $k < m$ such that $Q(a) = 0$. Therefore, $[E(a) : E] \geq m$.

Suppose, for sake of contradiction, that $[E(a) : E] > m$, so that, for $n = [E(a) : E] - m$, $n > 0$. Then, as shown in lecture, for $B = \{1, a, \dots, a^{m+n}\}$, B is a basis of $E(a)$. Since a is algebraic over E of degree m, $\exists P \in E[x]$ of degree m such that $P(a) = 0$. Let $p_0, p_1, \dots, p_m$ be the coefficients of P, so that $P(a) = p_0 + p_1 a + \dots + p_m a^m = 0$. Then, $1 = -(p_0)^{-1}(p_1 a + p_2 a^2 + \dots + p_m a^m$, contradicting the linear independence of B. Thus, $[E(a) : E] \leq m$.

Therefore, $[E(a) : E] = m$. ■

Exercise 50: Suppose $u \in E(x_1, x_2, \dots, x_n)$ is algebraic in E. Then, for some $P, Q \in E[x]$ such that $\frac{P}{Q}$ in reduced form, $u = \frac{P}{Q}$. Furthermore, for some $k \in \mathbb{N}$, $0 = r_0 + r_1 u + \dots + r_k u^k = r_0 + r_1 \frac{P}{Q} + \dots + r_k \left(\frac{P}{Q}\right)^k$. Thus, $\left(\frac{P}{Q}\right)^k = -r_k^{-1}\left(r_0 + r_1\frac{P}{Q} + \dots + r_{k-1}\left(\frac{P}{Q}\right)^{k-1}\right)$, so that $P^k = -r_k^{-1}\left(r_0 Q^k + r_1 P Q^{k-1} + \dots + r_{k-1}P^{k-1}Q\right)$. Thus, P divides $r_k^{-1}Q^k$. Since $\frac{P}{Q}$ is in reduced form, P and Q have no common factors, so that P divides r_k^{-1}. Thus, P is a constant. Furthermore, $Q^k = -r_0^{-1}\left(r_1 P Q^{k-1} + \dots + r_{k-1}P^{k-1}Q + r_k P^k\right)$, so that Q divides $r_0^{-1}P^k$. Since P and Q have no common factors, Q divides r_0^{-1} so that Q is also constant. Thus, $\frac{P}{Q}$ is constant, so that $u = \frac{P}{Q} \in E$. Thus, if u is algebraic in E, then $u \in E$, so that the contrapositive, that every element of $E(x_1, \dots, x_n)\backslash E$ is transcendental, holds. ■

Exercise 51: Let E be a field, let F be a field extension, let $a, b \in F$ be algebraic over E of degrees m and n respectively, with $(m, n) = 1$.

By Lemma 1 above, $[E(a) : E] = m$, and $[E(b) : E] = n$. Note that $E(a, b)$ is a field extension both of $E(a)$ and of $E(b)$, which are in turn field extensions of E. Thus, by Lemma 29.5, m and n both divide $[E(a, b) : E]$. Since $(m, n) = 1$, so that m and n share no prime factors thus the product of the prime factorizations of m and n divides $[E(a, b) : E]$, so that $[E(a, b) : E] \geq mn$.

Suppose, for sake of contradiction, that $[E(a, b) : E] > mn$, so that, for $k = [E(a, b) : E] - m$, $l = [E(a, b) : E] - n$, either $k > 0$ or $l > 0$. Then, as shown in lecture, for

$$B = \{1, a, \dots, a^{m+k}, 1b, ab, \dots, a^{m+k}b, \dots, 1b^{n+l}, ab^{n+l}, \dots, a^{m+k}b^{n+l}\},$$

B is a basis of $E(a)$. Since a is algebraic of degree m over E, $\exists P \in E[x]$ of degree m such that $P(a) = 0$. Since b is algebraic of degree n over E, $\exists Q \in E[x]$ of degree n such that $Q(b) = 0$. Let $p_0, p_1, \dots, p_m$ be the coefficients of P and let $q_0, q_1, \dots, q_n$ be the coefficients of Q, so that $P(a) = p_0 + p_1 a + \dots + p_m a^m = 0$ and $Q(b) = q_0 + q_1 b + \dots + q_n b^n = 0$. Then, $1 = -(p_0)^{-1}(p_1 a + p_2 a^2 + \dots + p_m a^m$ and $1 = -(q_0)^{-1}(q_1 b + q_2 b^2 + \dots + q_n b^n$. In either case, since either $k > 0$ or $l > 0$, this contradicts the linear independence of B. Thus, $[E(a) : E] \leq m$.

Therefore, $[E(a, b) : E] = mn$. ■

Exercise 52: Let E be a field, and let F be a field extension of E.

i: Suppose $u \in F$ is algebraic over E. Then, $\exists P \in E[x]$ such that $P(u) = 0$. Let n be the degree of P, and let $p_0, p_1, \ldots, p_n$ be the coefficients of P, so that $p_0 + p_1 u + \ldots + p_n u^n = 0$. Subtracting odd terms gives $-(p_1 u + p_3 u^3 + \ldots + p_k u^k) = p_0 + p_2 u^2 + \ldots + p_j u^j$, where one of k, u is n, and the other is $n-1$, depending on whether n is even or odd. Then, squaring both sides of the equation gives $q_2 u^2 + q_6 u^6 + \ldots + q_{2k} u^{2k} = q_0 + p_4 u^2 + \ldots + p_{2j} u^{2j}$ for some $q_0, q_2, \ldots, q_{2n} \in E$, so that $q_0 + q_2 u^2 + \ldots + q_{2n} u^{2n} = 0$. Thus, u^2 is a root of $q_0 + q_2 u + \ldots q_{2n} u^n$, so that u^2 is algebraic. ■

ii: Suppose $v \in F$ of algebraic of odd degree over E (in particular, let v be algebraic of degree $m \in \mathbb{N}$ over E). Clearly, $E(v^2) \subseteq E(v)$, since any field containing v contains v^2. Suppose $p \in E(v)$, so that $p = e_0 + e_1 v + \ldots + e_{m-1} v^{m-1}$ for some $e_0, e_1, \ldots, e_{m-1} \in E$ (as $\{1, v, v^2, \ldots, v^{m-1}\}$ is a basis of $E(v)$. Let $a = e_0 + e_2 v^2 + \ldots + e_{m-2} v^{m-2}$, $b = e_1 + e_3 v^2 + \ldots + e_{m-1} v^{m-2}$, so that $a, b \in E(v^2)$. Then, subtracting odd terms gives $a = vb$. Since m is odd, $b \neq 0$ (as, otherwise, there would be a polynomial P of degree $(m-1)$ with $P(v) = 0$), so, since $ab^{-1} = v$, $v \in E(v^2)$. Therefore, $p \in E(v^2)$, so $E(v) \subseteq E(v^2)$ and thus $E(v) = E(v^2)$.

By Lemma 1 above, if v is algebraic of degree m over E, $[E(v) : E] = m$. Since $E(v^2) = E(v)$, $[E(v^2) : E] = m$, so that v^2 is algebraic of degree m over E (in particular, v^2 is algebraic of odd degree over E). ■

iii: It is possible to have w algebraic of even degree over E and $E(v) = E(v^2)$. For instance, let $w = \omega = \frac{-1+i\sqrt{3}}{2}$, and let $E = \mathbb{R}$. Clearly, w is not of degree 1 over $\mathbb{R}$, since $w \notin \mathbb{R}$. However, $w^2 + w + 1 = 0$, so w is algebraic of degree 2 over E. Since $w = -1 - w^2$, $\mathbb{R}(w) = \mathbb{R}(w^2)$. ■

Exercise 53: Let E be a field, and let F be a field extension of E. Suppose $u, v \in F$ with v algebraic (in particular, of degree $m \in \mathbb{N}$, over $E(u)$, and v transcendental over E. Then, for some $e_0, e_1, \ldots, e_m \in E(u)$, $e_0 + e_1 v + \ldots + e_m v^m = 0$. Since $e_0, e_1, \ldots, e_m \in E(u)$, $e_0 = p_{0,0} + p_{0,1} u + \ldots + p_{0,n} u^n, e_1 = p_{1,0} + p_{1,1} u + \ldots + p_{1,n} u^n, \ldots, e_m = p_{m,0} + p_{m,1} u + \ldots + p_{m,n} u^n$. Let $f_0 = p_{0,0} + p_{1,0} v + \ldots + p_{m,0} v^m, f_1 = p_{0,1} + p_{1,1} v + \ldots + p_{m,1} v^m, \ldots, f_m = p_{0,m} + p_{1,m} v + \ldots + p_{m,m} v^m$. Then, $f_0, f_1, \ldots, f_m \in E(v)$, and $f_0 + f_1 u + \ldots + f_n u^n = 0$. Furthermore, since v is transcendental over E, $f_0 \neq 0$. Thus, u is algebraic over $E(v)$. ■

Exercise 54: Let E be a field, and let $F = E(x)$. Let $u = \frac{x^3}{x+1}$, and let $K = E(u)$. Let $v = x$. Then, since any field containing x contains $\frac{x^3}{x+1}$, $K(v) = E(x) = F$. Since x is a root of $u + uy - y^3 \in E(u) = K$, by Lemma 1 above, $[F : K] \leq 3$. It remains to show that there does not exist a polynomial P of degree 1 or 2 such that $P(u) = 0$, so that $[F : K] \geq 3$, and thus $[F : K] = 3$.

The following lemma is used in the solution of Exercise 56:

Lemma 2: Let E be a field, let $P \in E[x]$ be of degree $n \geq 1$, and let F be a splitting field extension for P over E. If the roots of P are distinct (that is, they are all of multiplicity 1), and no root is in E, $[F : E] = n!$.

Proof: If $n = 1$, then P is already linear, so that E is itself a splitting field for P, and $[E : E] = 1$ which divides n. Suppose, as an inductive hypothesis, that, for some $k \in \mathbb{N}$, the above lemma holds $\forall n \leq k$. Let P be a polynomial of degree $(k+1)$, with distinct factors $f_1, f_2, \ldots, f_{k+1} \notin E$. Let F_k be a splitting field of $P/(f_{k+1})$, and let F_{k+1}. Then, $[F_{k+1} : F_k] = k + 1$. Since $[F_k : E] = k!$, $[F_{k+1} : E] = [F_k : E][F_{k+1} : F_k] = k!(k+1) = (k+1)!$. Thus, by the Principle of Mathematical Induction, the above lemma holds $\forall n \in \mathbb{N}$.

Exercise 56: Order the roots of P $f_1, f_2, \ldots, f_n$ such that, for some $k \in \mathbb{N}$, $\forall n \in \mathbb{N}$, $i \leq k$ if and and only if $f_i \notin E$ and, $\forall j \in \mathbb{N}$ with $i \neq j \leq k$, $f_i \neq f_j$. That is, pick an ordering such that each of the roots not in E appears exactly once within the first k terms. By Lemma 2 above, a splitting field extension F' of $(x - f_1)(x - f_2) \ldots (x - f_k)$ is such that $[F' : E] = k!$. Furthermore, it is a splitting field of P, since all other factors of P are either already in E or are among $f_0, f_1, \ldots, f_k$, so that they can be factored into linear terms. Thus, since $k!$ divides $n!$ (as $k \leq n$), $[F : E]$ divides $n!$.