21-373, Algebraic Structures, Department of Mathematical Sciences, Carnegie Mellon University
Fall 2011: (Math Studies Section) Monday, Wednesday, Friday, 10:30 am, Porter Hall 226B.
Luc TARTAR, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

32- Friday November 18, 2011.

Lemma 32.1: If E is a field, if F is a field extension of E, and if $a \in F$ is algebraic over E, there is a unique irreducible monic (in the sense that the coefficient of highest degree is 1) polynomial $P_a \in E[x]$ such that $P_a(a) = 0$, and one calls it the *minimal polynomial* for a over E.[1] One has $E(a) = E[a]$, which is isomorphic to $E[x]/(P_a)$, and a basis of $E(a)$ (as an E-vector space) is $\{1, a, \ldots, a^{d-1}\}$ with $d = deg(P_a)$, so that $[E(a):E] = d$.
Proof: Let J be the ideal of polynomials $P \in E[x]$ such that $P(a) = 0$. One has $J \neq \{0\}$, since a is algebraic over E, and J is generated by a polynomial of minimum degree $d \geq 1$, and choosing it to be monic defines P_a. If $d = 1$, then $a \in E$, P_a is the polynomial $x - a$, and $E(a) = E[a] = E$. If $d \geq 2$, P_a must be irreducible, since if $P_a = Q_1 Q_2$ with $deg(Q_1), deg(Q_2) \geq 1$, then either $Q_1(a) = 0$ or $Q_2(a) = 0$ (since $0 = P_a(a) = Q_1(a)\,Q_2(a)$), contradicting the definition of d.

That P_a is unique comes from the fact that $Q(a) = 0$ implies that Q is a multiple of P_a, and if Q is irreducible it must then be $c\,P_a$ with $c \in F^*$, and if Q is monic, it implies $c = 1$.

Then, $1, a, \ldots, a^{d-1}$ are E-linearly independent, again because of the definition of d, and $E[a] = \{f(a) \mid f \in E[x], deg(f) \leq d-1\}$ is actually a field (so that it is $E(a)$): indeed if $f \in E[x]$ with $f \neq 0$ and $deg(f) \leq d-1$, then the *gcd* of f and P_a is 1, so that there exist $g, h \in E[x]$ with $1 = g\,f + h\,P_a$ (since $E[x]$ is a PID, and the *gcd* is well defined), which implies $f(a)\,g(a) = 1$, and every non-zero element in $E[a]$ then has a multiplicative inverse in $E[a]$ (since one may assume that $deg(g) \leq d-1$ by replacing g by its remainder in the Euclidean division by P_a, and changing accordingly what h is).

Remark 32.2: The notation P_a may be misleading, since it does not mention what E is, so let us use the notation P_a^E for the sake of this observation. If K is an intermediate field, i.e. $E \subset K \subset F$, and if $a \in F$ is algebraic over E, then it is algebraic over K, since $P_a^E \in E[x]$ implies $P_a^E \in K[x]$, but P_a^E may be reducible in $K[x]$, in which case P_a^K will be a divisor of P_a^E, hence $deg(P_a^K) \leq deg(P_a^E)$ in general.

Notation 32.3: If R_1, R_2 are two rings, then if σ is a ring-homomorphism from R_1 into R_2, one also denotes σ the corresponding ring-homomorphism from $R_1[x]$ into $R_2[x]$, which sends $P = \sum_j c_j x^j$ to $\sigma\,P = \sum_j \sigma(c_j)\,x^j$. Of course, if σ is an isomorphism from R_1 onto R_2, it induces an isomorphism from $R_1[x]$ onto $R_2[x]$.

Lemma 32.4: Let E_1, E_2 be two (isomorphic) fields, and σ an isomorphism from E_1 onto E_2. If F_1 is a field extension of E_1 and $a_1 \in F_1$ is algebraic over E_1 with minimal polynomial P_{a_1}, if F_2 is a field extension of E_2 and $a_2 \in F_2$ is algebraic over E_2, with minimal polynomial P_{a_2}, and if $\sigma\,P_{a_1} = P_{a_2}$, then there is a unique isomorphism τ from $E_1(a_1)$ onto $E_2(a_2)$ extending σ and satisfying $\tau(a_1) = a_2$.
Proof: Remark that if $a_1 \in E_1$, then $P_{a_1} = x - a_1$, so that $\sigma\,P_{a_1} = x - \sigma(a_1)$, and the hypothesis is that $a_2 = \sigma(a_1)$, and then $E_1(a_1) = E_1$, $E_2(a_2) = E_2$ and $\tau = \sigma$.

Assume that $a_1 \notin E_1$, so that P_{a_1} has degree $d > 1$. If $f = c_0 + c_1 x + \ldots + c_n x^n \in E_1[x]$, then $\sigma\,f = \sigma(c_0) + \sigma(c_1)x + \ldots + \sigma(c_n)x^n \in E_2[x]$. Since the desired isomorphism τ must satisfy $\tau(c) = \sigma(c)$ for all $c \in E_1$, and $\tau(a_1) = a_2$, it must satisfy $\tau\big(f(a_1)\big) = \sigma\,f(a_2)$ for all $f \in E_1[x]$, and one observes that this definition makes sense, i.e. if $b \in E_1(a_1)$ can be written as $b = f(a_1) = g(a_1)$ for two polynomials $f, g \in E_1[x]$, the two definitions of $\tau(b)$ using either f or g are equal: indeed, $f - g$ must be a multiple of P_{a_1}, but $f - g = P_{a_1} Q$ implies $\sigma\,f - \sigma\,g = \sigma\,(f - g) = \sigma\,P_{a_1}\,\sigma\,Q = P_{a_2}\,\sigma\,Q$, so that $\sigma\,f - \sigma\,g$ being a multiple of P_{a_2}, their values at a_2 coincide, i.e. $\sigma\,f(a_2) = \sigma\,g(a_2)$.

[1] In linear algebra, the term minimal polynomial is used with a slightly different meaning: for a field K one considers the (non-commutative) ring of $n \times n$ matrices A with entries in K (or the endomorphisms of a K-vector space V of dimension n), and for such a matrix A one considers the polynomials $P \in K[x]$ satisfying $P(A) = 0$; they form an ideal, generated by a monic polynomial P_{min} of minimal degree, called the minimal polynomial of A, which has no reason to be irreducible (since the ring of matrices has zero-divisors). The Cayley–Hamilton theorem asserts that $P_{char}(A) = 0$, where the characteristic polynomial is defined by $P_{char}(\lambda) = det(A - \lambda\,I)$, so that the minimal polynomial divides P_{char}, hence has degree $\leq n$.

Remark 32.5: The application mentioned in Remark 31.5 consists in taking $E' = E$ and $\sigma = id$, so that it says that if a_1 and a_2 belong to two (possibly different) field extensions F_1, F_2 of E, and have the same minimal polynomial P, then $E(a_1) \subset F_1$ and $E(a_2) \subset F_2$ are isomorphic by an isomorphism τ whose restriction to E is identity.

Lemma 32.6: If E is a field, if F is any field extension of E, and if A is any (non-empty) finite subset of elements of F which are algebraic over E, then $E(A)$ is a finite field extension of E.
Proof: By induction on $n = |A|$. If $K = E(a_1, \ldots, a_{n-1})$ is a finite field extension of E, then a_n being algebraic over E is also algebraic over K, so that $K(a) = K[a]$, and one has $[K(a_n) : K] \le d_n$, the degree of the minimal polynomial for a_n in E (which is the order of a_n as an algebraic element over E), because the degree of the minimal polynomial for a_n over K is $\le d_n$; since $E(a_1, \ldots, a_n) = K(a_n)$, one deduces that $[E(a_1, \ldots, a_n) : E(a_1, \ldots, a_{n-1})] \le d_n$, hence $[E(a_1, \ldots, a_n) : E]$ is $\le$ the product of the orders of the elements of A.

Lemma 32.7: If D is a field, if E is an algebraic extension of D, and if F is an algebraic extension of E, then F is an algebraic extension of D.
Proof: If $z \in F$, it is algebraic over E, so that $P(z) = 0$ for a monic irreducible polynomial $P = c_0 + c_1 x + \ldots + x^n$, with $c_0, \ldots, c_{n-1} \in E$. Since $c_0, \ldots, c_{n-1}$ are algebraic over D, $E_0 = D(c_0, \ldots, c_{n-1}) \subset E$ is a finite field extension of D by Lemma 32.6, and then z is algebraic over E_0 because P has its coefficients in E_0, and P is irreducible over E_0, so that adding the root z to E_0 gives a field E_1 with $[E_1 : E_0] = n$, and one deduces that $[E_1 : D] = n\,[E_0 : D] < +\infty$, so that z is algebraic over D.

Lemma 32.8: If E is a field and F is any field extension field of E, then $\mathcal{A}_E(F) = \{z \in F \mid z \text{ algebraic over } E\}$ is a subfield of F.
Proof: For $a, b \in F$ algebraic over E, $E(a, b)$ is a finite field extension of E by Lemma 32.6, hence an algebraic extension of E. In consequence, $a + b$ and $a\,b$ are algebraic over E, as well as a^{-1} if $a \ne 0$, since they belong to $E(a, b)$.

Remark 32.9: Directly, all powers of a are E-linear combinations of $1, \ldots, a^{\alpha-1}$ with $\alpha = order(a)$, and all powers of b are E-linear combinations of $1, \ldots, b^{\beta-1}$ with $\beta = order(b)$, so that all powers of $a+b$ and of $a\,b$ are E-linear combinations of $a^i b^j$ with $0 \le i \le \alpha - 1, 0 \le j \le \beta - 1$, showing that $a + b$ and $a\,b$ are algebraic over E, because $1, a+b, \ldots, (a+b)^{\alpha\,\beta}$ are E-linearly dependent, as well as $1, a\,b, \ldots, (a\,b)^{\alpha\,\beta}$, since they are $\alpha\,\beta+1$ elements in an E-vector space generated by $\alpha\,\beta$ elements. This shows that $order(a+b) \le order(a)\,order(b)$, and $order(a\,b) \le order(a)\,order(b)$.

Furthermore, if $a \ne 0$ is algebraic over E, then $c_0 + c_1 a + \ldots + c_{\alpha-1} a^{\alpha-1} + a^\alpha = 0$, with $c_0 \ne 0$, and multiplying by $c_0^{-1} a^{-\alpha}$ one has $c_0^{-1} + c_0^{-1} c_{\alpha-1} a^{-1} + \ldots + c_0^{-1} c_1 (a^{-1})^{\alpha-1} + (a^{-1})^\alpha = 0$, showing that a^{-1} is algebraic over E, with $order(a^{-1}) \le order(a)$, hence $order(a^{-1}) = order(a)$.

Remark 32.10: Since $\mathbb{Q} \subset \mathbb{C}$, and $\mathbb{C}$ is algebraically closed, every polynomial $P \in \mathbb{Q}[x]$ has roots in $\mathbb{C}$, which are algebraic over $\mathbb{Q}$, and by Lemma 32.8, the set of all (complex) algebraic numbers $K = \mathcal{A}_{\mathbb{Q}}(\mathbb{C})$ is a field, which is an algebraic extension of $\mathbb{Q}$ by definition of K; this field is algebraically closed, since if $P \in K[x]$ had no root in K it would have a root in a finite extension of K, which would be an algebraic extension of $\mathbb{Q}$ by Lemma 32.7, i.e. it would be a root of $P_1 \in \mathbb{Q}[x]$, so that it would belong to K by definition of K.

It is true that for any field E there exists an algebraic extension F of E which is algebraically closed, but one difficulty for proving this result is that one cannot define the "set" of all "algebraic elements over E", since one can only say which elements of a *given* field extension F are algebraic over E.