21-238, Math Studies Algebra 2, Department of Mathematical Sciences, Carnegie Mellon University
Spring 2012: Monday, Wednesday, Friday, 10:30 am, Doherty Hall 1211.
Luc TARTAR, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

39- Monday April 30, 2012.

Lemma 39.1: Let F be a finite extension of E with $[F:E]=n$, and let $\overline{E}$ be an algebraic closure of E. Then, there are at least 1 and at most n homomorphisms σ from F into $\overline{E}$ satisfying $\sigma\,|_E= id_E$;[1] there are n if and only if F is a separable extension of E.
Proof: One proves a slightly stronger result by induction on n, suggested by the method of proof: if σ is an isomorphism from E onto E', and $\overline{E'}$ is an algebraic closure of E', there are at least 1 and at most n homomorphisms τ from F into $\overline{E'}$ satisfying $\tau\,|_E=\sigma$, and there are n if and only if F is a separable extension of E.

If $n=1$, there is nothing to prove. If $n>1$, one chooses $\alpha\in F\setminus E$, with monic irreducible polynomial $P\in E[x]$; an homomorphism ρ from $E(\alpha)$ into $\overline{E'}$ with $\rho\,|_E=\sigma$ is determined by $\rho(\alpha)$, which must be a root β of $\sigma(P)\in E'[x]$ in $\overline{E'}$ (and $\sigma(P)$ splits over $\overline{E'}$ since it is an algebraic closure of E'), so there are s possibilities for ρ with $1\le s\le deg(P)=[E(\alpha):E]$, and one obtains an isomorphism ρ from $E(\alpha)$ onto $E'(\beta)$ with $\beta=\rho(\alpha)$; by induction, for each of these ρ there are t extensions to an homomorphism τ from F into $\overline{E'}$, with $1\le t\le[F:E(\alpha)]$, which makes $1\le s\,t\le[E(\alpha):E]\,[F:E(\alpha)]=[F:E]=n$.

Suppose that F is a separable extension of E, then one argues by induction that there are exactly n extensions: there are $s=deg(P)=[E(\alpha):E]$ extensions ρ by separability, and by induction there are $t=[F:E(\alpha)]$ extensions from ρ to τ, since F is a separable extension of $E(\alpha)$.

Suppose that F is not a separable extension of E, and choose $\alpha\in F\setminus E$ which is not a separable element, so that $s<deg(P)$ and since $t\le[F:E(\alpha)]$ one obtains $s\,t<n$ for the number of extensions τ.

Lemma 39.2: If α is separable over E, then $E(\alpha)$ is a separable extension of E.
Proof: By the proof of Lemma 39.1 there are $[E(\alpha):E]$ extensions of id_E into an homomorphism from $E(\alpha)$ into an algebraic closure $\overline{E}$ of E, and by the conclusion of Lemma 39.1 it means that $E(\alpha)$ is a separable extension of E.

Lemma 39.3: If G is a (possibly infinite) separable extension of F and F is a (possibly infinite) separable extension of E, then G is a separable extension of E.
Proof: Let $\alpha\in G\backslash F$, so that its monic irreducible polynomial $P\in F[x]$ is separable; let $F_0=E(\beta_1,\ldots,\beta_m)\subset F$ be a finite extension of E containing the coefficients of P, so that P is irreducible in $F_0[x]$, and assume that one has proved that P is separable in $F_0[x]$, so that α is separable over F_0, and by Lemma 39.2 $F_0(\alpha)$ is a separable extension of F_0.

Since β_1 is separable over E by hypothesis, $E(\beta_1)$ is a separable extension of E by Lemma 39.2. For $i=2,\ldots,m$, β_i is separable over E by hypothesis, so that it is separable over $E(\beta_1,\ldots,\beta_{i-1})$, and $E(\beta_1,\ldots,\beta_i)$ is then a separable extension of $E(\beta_1,\ldots,\beta_{i-1})$ by Lemma 39.2, and since $F_0(\alpha)$ is a separable extension of $F_0=E(\beta_1,\ldots,\beta_m)$, one will prove by induction on the number of steps (here $m+1$) that $F_0(\alpha)$ is a separable extension of E: since $\alpha\in F_0(\alpha)$ it will then be separable over E, and varying α will show that G is a separable extension of E.

The crucial step in the induction is to show that if $E(\beta)$ is a separable extension of E and $\widetilde{E}$ is a finite and separable extension of $E(\beta)$, then $\widetilde{E}$ is a separable extension of E. By Lemma 39.1 there are $[E(\beta):E]$ homomorphisms σ from $E(\beta)$ into $\overline{E}$ which extend id_E, and a given σ is an isomorphism of $E(\beta)$ onto its image $E(\gamma)\subset\overline{E}$ (with γ depending upon σ); by Lemma 39.1 there are $[\widetilde{E}:E(\beta)]$ homomorphisms τ from $\widetilde{E}$ into $\overline{E(\gamma)}=\overline{E}$ which extend σ, so that there are $[\widetilde{E}:E(\beta)]\,[E(\beta):E]=[\widetilde{E}:E]$ homomorphisms from $\widetilde{E}$ into $\overline{E}$ which extend id_E, and by Lemma 39.1 it implies that $\widetilde{E}$ is a separable extension of E.

For proving that P is separable in $F_0[x]$, one notices that P has no repeated root in a splitting field extension $\widetilde{F}$ for P over F. Then, let $\widetilde{F_0}\subset\widetilde{F}$ be the field generated by F_0 and the roots of P, which is a splitting field extension for P over F_0; if P was not separable in $F_0[x]$ it would imply that P has a

[1] An homomorphism σ from a field E into a ring with identity satisfying $\sigma(1)=1$ is automatically injective, i.e. is a monomorphism (since for $a\neq 0$ one has $\sigma(a)\,\sigma(a^{-1})=1$, implying $\sigma(a)\neq 0$, hence for $b\neq a$ one has $\sigma(b)-\sigma(a)=\sigma(b-a)\neq 0$).

repeated root in $\widetilde{F_0}$, but since $\widetilde{F}$ is an extension of $\widetilde{F_0}$, this would imply that P has a repeated root in $\widetilde{F}$, a contradiction.

Lemma 39.4: If F is an extension of E, then the set of $\alpha \in F$ which are separable over E is an intermediate field.
Proof: Let α, β be separable over E, then α is separable over $E(\beta)$, so that $E(\alpha, \beta)$ is a separable extension of $E(\beta)$, and since $E(\beta)$ is a separable extension of E by Lemma 39.2, one deduces that $E(\alpha, \beta)$ is a separable extension of E by Lemma 39.3; then, $\alpha + \beta$, $\alpha\,\beta$, and β^{-1} if $\beta \neq 0$ are particular elements of $E(\alpha, \beta)$, which are then separable over E.

Definition 39.5: A *separable closure* of E is the field of separable elements over E in an algebraic closure $\overline{E}$ of E.

Definition 39.6: A field E is *perfect* if all (irreducible) polynomials $P \in E[x]$ are separable (and it is the case in characteristic 0).

Lemma 39.7: If E is finite, then E is perfect.
Proof: Assume that E has characteristic p, and let P be irreducible. If $P' \neq 0$, then P is separable. If $P' = 0$, then $P = \sum_{j=0}^m c_j x^{j\,p}$, but using the Frobenius automorphism (Lemma 27.2) one has $c_j = b_j^p$ some some $b_j \in E$, and then $P = \sum_{j=0}^m b_j^p x^{j\,p} = \big(\sum_{j=0}^m b_j x^j\big)^p$, contradicting irreducibility.

Lemma 39.8: If F is an algebraic extension of a finite field E, then F is perfect.
Proof: Let $P \in F[x]$ be irreducible, and let E_1 be the field generated over E by the coefficients of P; since each coefficient is algebraic over E, E_1 is a finite extension of E, and it is then a finite field. Then, since $P \in E_1[x]$, one sees by Lemma 39.7 and Definition 39.6 that P is separable.

Definition 39.9: For k a field, ℓ a field extension of k, and X a subset of ℓ, one denotes $k(X)$ the subfield of ℓ generated by k and X, and then the *algebraic closure of X (and k)*, denoted $acl(X)$, is the set of elements of ℓ which are algebraic over $k(X)$.

Lemma 39.10: The operation *acl* of Definition 39.9 has the following properties:

a) $X \subset acl(X)$ and $acl\big(acl(X)\big) = acl(X)$ for all $X \subset \ell$; $X \subset Y \subset \ell$ implies $acl(X) \subset acl(Y)$.

b) $acl(X) = \bigcup_{J \text{ finite } \subset X} acl(J)$.

c) If $a \in acl(X \cup \{b\}) \setminus acl(X)$, then $b \in acl(X \cup \{a\}) \setminus acl(X)$.

Proof: One has $X \subset k(X) \subset acl(X)$, and $X_1 \subset X_2$ implies $k(X_1) \subset k(X_2)$; then, if $k_1 \subset k_2$ are subfields of ℓ, $acl(k_1) \subset acl(k_2)$ since $z \in acl(k_1)$ means $z \in \ell$ and $P(z) = 0$ for some non-zero $P \in k_1[x]$, which then satisfies $P \in k_2[x]$. If k is a subfield of ℓ and $K = acl(k)$, then $z \in \ell$ algebraic over K means $Q(z) = 0$ for some non-zero $Q \in K[x]$; the coefficients of Q are algebraic elements over k, so they belong to a finite extension of k, but z belonging to a finite extension of K is then itself in a finite extension of k, so that it is algebraic over k, hence belongs to K, proving $acl\big(acl(k)\big) = acl(k)$.

The characterization of $z \in acl(X)$ is that it satisfies a polynomial equation with coefficients in $k(X)$, and reduction to the same denominator shows that it satisfies a polynomial equation with coefficients in $k[X]$, but these elements of $k[X]$ are polynomials in a finite number of elements $x_1, \ldots, x_r \in X$ which form a finite subset J and $z \in acl(J)$; this proves $acl(X) \subset \bigcup_{J \text{ finite } \subset X} acl(J)$, but since $acl(J) \subset acl(X)$ for all J, one has equality.

If $a \in acl(X \cup \{b\}) \setminus acl(X)$, then it implies that $b \notin acl(X)$, since $acl(X \cup \{b\})$ would be $acl\big(acl(X)\big) = acl(X)$; a satisfies a polynomial equation $\sum_{i=1}^m P_i(x_1, \ldots, x_n, b)\, a^i = 0$, and at least one P_i uses b, or one would have $a \in acl(X)$; reordering the sum in powers of b shows that $b \in acl(\{x_1, \ldots, x_n, a\}) \subset acl(X \cup \{a\})$.

Remark 39.11: An important observation is that properties a), b) and c) of Lemma 39.10 are analogous to the properties of the operation *span* in linear algebra, the difference being that in linear algebra one restricts attention to homogeneous polynomials of degree ≤ 1.[2] Actually, the theory of independence, bases, and dimension in linear algebra can be developed on the basis of just these three properties alone, so that there are parallel definitions and facts in our setting.

[2] Polynomials of degree 1 are said to be *affine* functions, and they are called *linear* only if they are homogeneous (of degree 1), i.e. with zero constant term.

Definition 39.12: $X \subset \ell$ is *algebraically independent over k* if and only if for every $x \in X$ one has $x \notin acl(X \setminus \{x\})$: in a more symmetric way, X is algebraically independent over k if and only if for every finite list $a_1, \ldots, a_n \in X$ and every $P \in k[x_1, \ldots, x_n]$, $P(a_1, \ldots, a_n) = 0$ implies $P = 0$. It implies that every element of an algebraically independent set over k (in particular, every element of a transcendence basis for ℓ over k) is transcendental over k.

$X \subset \ell$ is a *transcendence basis for ℓ over k* if and only if it is algebraically independent over k, and $acl(X) = \ell$. Notice that X is empty if and only if ℓ is an algebraic extension of k.

Lemma 39.13: X is a *transcendence basis for ℓ over k* if and only if it is maximal among subsets of ℓ which are algebraically independent over k.

Every subset of ℓ which is algebraically independent over k is included into a transcendence basis for ℓ over k.

Proof: If $acl(X) = \ell$, then all elements of $\ell \setminus X$ are algebraic over $k(X)$, so that if one adds to X an element from $\ell \setminus X$ the set obtained is no longer algebraically independent over k, i.e. X is maximal among subsets of ℓ which are algebraically independent over k. If X is algebraically independent over k and if $acl(X) \neq \ell$, then there exists $y \in \ell \setminus acl(X)$, such that $X \cup \{y\}$ is algebraically independent over k, hence X cannot be maximal among subsets of ℓ which are algebraically independent over k.

If $X_i \subset \ell$ is a chain of algebraically independent sets over k, i.e. totally ordered by inclusion, then $X_* = \bigcup_{i \in I} X_i$ is an algebraically independent set over k, since any finite set from X_* is included in a common X_i; by Zorn's lemma, applied to the algebraically independent sets over k which contain a given subset A (itself algebraically independent over k), one finds a maximal X containing A.