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

40- Wednesday May 2, 2012.

Lemma 40.1: If a transcendence basis $X = \{x_1, \ldots, x_m\}$ for ℓ over k has m elements, then any $m+1$ elements $y_1, \ldots, y_{m+1} \in \ell$ are automatically algebraically dependent over k.

In the general case, any two transcendence bases for ℓ over k have the same cardinality, which is called the *transcendence degree* of the extension.

Proof: By induction on m, for all fields k and field extensions ℓ: it is true for $m = 0$ (corresponding to ℓ being an algebraic extension of k), so that one assumes the result proved up to $m-1$. Since it follows from the induction hypothesis if all y_i are algebraic over $k(x_1, \ldots, x_{m-1})$, one may assume that y_{m+1} is not algebraic over $k(x_1, \ldots, x_{m-1})$, but since it is algebraic over $k(x_1, \ldots, x_m)$, one deduces that x_m is algebraic over $k(x_1, \ldots, x_{m-1}, y_{m+1})$; writing $K = k(y_{m+1})$, x_m is algebraic over $K(x_1, \ldots, x_{m-1})$, and then $y_1, \ldots, y_m$ being algebraic over $k(x_1, \ldots, x_{m-1}, x_m)$ are algebraic over $K(x_1, \ldots, x_{m-1})$, so that they are algebraically dependent over K by the induction hypothesis:[1] it means that $y_1, \ldots, y_m$ satisfy a non-zero polynomial equation with coefficients in K, which is made of rational fractions in y_{m+1}, and using a common denominator one transforms it into a non-zero polynomial equation for $y_1, \ldots, y_m, y_{m+1}$.

If $Y = \{y_1, \ldots, y_n\}$ is another transcendence basis for ℓ over k having n elements, one deduces that $n \leq m$, hence $n = m$ by exchanging the roles of X and Y.

In the general case, if X is an infinite transcendence basis for ℓ over k (i.e. $card(X) \geq \aleph_0$), then the preceding finite case shows that any other transcendence basis Y for ℓ over k must be infinite. Any element of ℓ, hence any element $x \in X$ belongs to $acl(B_x)$ for a finite subset $B_x \subset Y$;[2] using the axiom of choice, one may consider a mapping $f : x \mapsto B_x$, but it may fail to be injective; however, since the number of x being sent to the same finite subset $B \subset Y$ is $\leq |B|$ by the first part, putting a well order on X by Zermelo's axiom (equivalent to the axiom of choice), one may define a mapping $g : x \mapsto (B_x, n)$ where n is the rank of x in the finite set $f^{-1}(B_x)$, and g is injective, showing that $cardinal(X) \leq cardinal\big(\mathbb{N} \times \mathcal{P}_{finite}(Y)\big) = cardinal(Y)$, where $\mathcal{P}_{finite}(Y)$ denotes the set of finite subsets of Y;[3] similarly, $cardinal(Y) \leq cardinal(X)$, hence $cardinal(Y) = cardinal(X)$ by the Schröder–Bernstein theorem.[4,5]

Lemma 40.2: If k is a field, $R = k[x_1, x_2]$ the ring of polynomials in two indeterminates with coefficients in k, which is an Integral Domain, and K the field of fractions of R, i.e. $K = k(x_1, x_2)$, then K is an extension of k of transcendence degree 2. Examples of bases are $\{x_1, x_2\}$, $\{x_1 + x_2, x_1 x_2\}$, and $\{x_1^2, x_2^2\}$, with different subfields generated by the three bases.

Proof: If x_1 and x_2 were algebraically dependent, there would exist a non-zero P in two variables (with coefficients in k) with $P(x_1, x_2) = 0$, i.e. all its coefficients would be 0. The subfield generated is K.

If $s = x_1 + x_2$ and $p = x_1 x_2$ were not algebraically independent, there would exist coefficients in k, not all zero, such that $\sum_{i,j} c_{i,j} (x_1 + x_2)^i (x_1 x_2)^j = 0$; one then looks at terms of higher total degree by maximizing $i + 2j$ for the non-zero coefficients, so there maybe some cancellations, but if among these terms

[1] With k replaced by K and ℓ replaced by the subfield L of elements in ℓ which are algebraic over $K(x_1, \ldots, x_{m-1})$, so that $\{x_1, \ldots, x_{m-1}\}$ is a transcendence basis of L.

[2] If $Z = \bigcup_{x \in X} B_x$, then all elements of X are algebraic over $k(Z)$, so that all elements of ℓ are algebraic over $k(Z)$, and this implies $Z = Y$, since a strictly smaller set than Y cannot be a transcendence basis for ℓ over k.

[3] $\mathcal{P}_{finite}(S)$ has the same cardinal than S for any infinite set S, and $\mathbb{N} \times S$ has the same cardinal than S for any infinite set S.

[4] Friedrich Wilhelm Karl Ernst SCHRÖDER, German mathematician, 1841–1902. He worked in Darmstadt, and in Karlsruhe, Germany. The Schröder–Bernstein theorem is partly named after him (CANTOR stated it without giving a proof, which BERNSTEIN provided in 1898, and SCHRÖDER obtained it independently the same year).

[5] Felix BERNSTEIN, German mathematician, 1878–1956. He worked at Georg-August-Universität, Göttingen, Germany. The Schröder–Bernstein theorem is partly named after him (CANTOR stated it without giving a proof, which BERNSTEIN provided in 1898, and SCHRÖDER obtained it independently the same year).

one looks for those with maximum degree in x_1 one maximizes i, and that selects exactly one coefficient, which must then not be there. Since $x_1^2 - x_1 s + p = 0$, and $x_2^2 + x_2 s - p = 0$, x_1 and x_2 are algebraic (of degree 2) over $k(s,p)$, so that $\{s,p\}$ is a transcendence basis. $k(s,p)$, the subfield generated, is that of symmetric rational fractions.

$y_1 = x_1^2$ and $y_2 = x_2^2$ are clearly algebraically independent, and the relation shows that x_1 and x_2 are algebraic (of degree 2) over $k(y_1,y_2)$, so that $\{x_1^2, x_2^2\}$ is a transcendence basis. $k(y_1,y_2)$, the subfield generated, is that of rational fractions invariant by changing x_1 into $-x_1$, and by changing x_2 into $-x_2$.

Lemma 40.3: If X and Y are algebraically independent sets over k having the same cardinality, then $k(X)$ and $k(Y)$ are isomorphic.
Proof: If f is a bijection from X onto Y, the isomorphism from $k(x_i, i \in X)$ onto $k(x_j, j \in Y)$ is characterized by sending x_i onto $x_{f(i)}$ for all $i \in X$, and this extends in a unique way to polynomials, $k[x_i, i \in X]$ becoming isomorphic to $k[x_j, j \in Y]$, and then it extends in a unique way to rational fractions, $k(x_i, i \in X)$ becoming isomorphic to $k(x_j, j \in Y)$.

Lemma 40.4: Let K be an algebraically closed field, let P be its prime subfield, and let B be a transcendence basis for K over P. Then, K is an algebraic closure of $P(B)$.
Proof: If $a \in K$ was not algebraic over $P(B)$, then it would be algebraically independent of B, and could be added to B, contradicting the maximality of B, hence all elements of K are algebraic over $P(B)$.

Lemma 40.5: Let $E_0 = \mathbb{Q}$, $E_m = \mathbb{Q}(x_1,\ldots,x_m)$ for $m \ge 1$, and $E_\infty = \bigcup_{m\ge 1} E_m = \mathbb{Q}(x_j, j \in \mathbb{N})$; let $\overline{E_\infty}$ be an algebraic closure of E_∞, and define $\overline{E_m}$ as the set of $a \in \overline{E_\infty}$ which are algebraic over E_m, for $m = 0,1,\ldots$. Then, if K is a *countable* algebraically closed field of characteristic 0, it is isomorphic to one of the $\overline{E_m}$ for $m \ge 0$, or to $\overline{E_\infty}$ (and to only one of them).
Proof: Let P be the prime subfield of K, which is isomorphic to $\mathbb{Q}$. One chooses a transcendence basis B for K over P, which must be finite (possibly empty if K is an algebraic extension of P) or countably infinite, since K is countable; the case where B is finite with $m \ge 0$ elements gives K isomorphic to $\overline{E_m}$, while the case where B is (countably) infinite gives K isomorphic to $\overline{E_\infty}$.

Remark 40.6: If $E = \mathbb{Z}_p$, and F is a finite extension of E with $[F\!:\!E] = n$, then $|F| = p^n$, F is a splitting field extension for the separable polynomial $x^{p^n} - x$, and the Galois group $Aut_E(F)$ is cyclic of order n, and generated by the Frobenius automorphism φ: $a \mapsto a^p$. The subfields correspond to subgroups of the cyclic group, and there is exactly one subgroup of order d for each divisor d of n, generared by φ^e if $d\,e = n$, and the fixed field has size p^e and is $\big\{a \in F \mid a^{p^e} = a\big\}$.

Lemma 40.7: For $E = \mathbb{Z}_p$, let F be an algebraic closure of E, and let $K_n = \{a \in F \mid a^{p^n} = a\}$ (with $K_1 = E$), which is a subfield of F with p^n elements, the unique of that size. One has $K_m \subset K_n$ if and only if m divides n, and $F = \bigcup_{n\ge 1} K_n$.
Proof: Since F is algebraically closed, $P = x^{p^n} - x$ splits over F, and since $P' = -1$ it has no repeated root, so that it has p^n distinct roots. If an intermediate field K is finite, then it is a finite extension of E, and must have order p^k for some $k \ge 1$; K^* being a multiplicative group of size $p^k - 1$ one has $a^{p^k - 1} = 1$ for all $a \in K^*$, i.e. $a^{p^k} = a$ for all $a \in K$, so that $K = K_k$. By Remark 40.6 the only subfields of K_n are K_m with m dividing n. Every $a \in F$ is algebraic over E by definition of an algebraic closure, so that $E(a)$ is a finite extension of E, and must then coincide with one K_n, showing that $F = \bigcup_{n\ge 1} K_n$.

Remark 40.8: Describing which subgroups of $Aut_E(F)$ are in correspondence with intermediate fields uses closed sets for a particular topology, so that it is useful to review some basic notions of topology.

A *topological space* $(X,\mathcal{T})$ is a space X equipped with a *topology* $\mathcal{T}$, i.e. a family of subsets called *open* subsets satisfying two axioms: any union of open sets is open, and any finite intersection of open sets is open.[6] A subset is then called *closed* if and only if its complement is open. A *basis* $\mathcal{B}$ of a topological space $(X,\mathcal{T})$ is a subset $\mathcal{B} \subset \mathcal{T}$ such that any open set $U \in \mathcal{T}$ is a union $U = \bigcup_{i\in I} B_i$, with $B_i \in \mathcal{B}$ for all $i \in I$; a family $\mathcal{C}$ of subsets is a basis for a topology (where the open sets are by definition all the unions of elements

[6] One usually says explicitly that $\emptyset$ and X must be open, but this corresponds to a union of open sets indexed by the empty set, and an intersection of open sets indexed by the empty set.

from $\mathcal{C}$) if and only if it satisfies the axiom that for all $C_1, C_2 \in \mathcal{C}$ and $c \in C_1 \cap C_2$ there exists $C_3 \in \mathcal{C}$ such that $c \in C_3 \subset C_1 \cap C_2$.

For a subset $Y \subset X$ the *interior* Y° of Y is the largest open subset A such that $A \subset Y$, the *closure* $\overline{Y}$ of Y is the smallest closed subset B such that $Y \subset B$, and the *boundary* ∂Y of Y is $\overline{Y} \setminus Y^\circ$. A subset Y is *dense* if $\overline{Y} = X$. The *connected component* of a point $a \in X$ is the smallest subset A containing a which is both open and closed; a topological space is said to be *connected* if the only subsets which are both open and closed are $\emptyset$ and X.

If $(X_1, \mathcal{T}_1)$ and $(X_2, \mathcal{T}_2)$ are two topological spaces, a mapping f from X_1 into X_2 is *continuous at* $a \in X_1$ if and only if for every open set $V \in \mathcal{T}_2$ containing $b = f(a)$ there exists an open set $U \in \mathcal{T}_1$ containing a such that $f(U) \subset V$; f is *continuous* from X_1 into X_2 if and only if it is continuous at every point of X_1, or equivalently if and only if for every open set $W \in \mathcal{T}_2$ the inverse image $f^{-1}(W)$ is open (i.e. $\in \mathcal{T}_1$), or equivalently if and only if for every closed set $Z \subset X_2$ the inverse image $f^{-1}(Z)$ is closed in X_1. A topology $\mathcal{T}_1$ on X is *finer than* another topology $\mathcal{T}_2$ on X (or $\mathcal{T}_2$ is *coarser than* $\mathcal{T}_1$) if $\mathcal{T}_2 \subset \mathcal{T}_1$, i.e. the identity from X equipped with the topology $\mathcal{T}_1$ onto X equipped with the topology $\mathcal{T}_2$ is continuous; the finest topology on X is the *discrete topology* for which all subsets are open, and the coarsest topology on X is that for which the only open sets are $\emptyset$ and X. For a subset $Y \subset X$, the *relative topology* on Y is that for which the open sets are the intersections $A \cap Y$ for $A \in \mathcal{T}$, i.e. the coarsest topology on Y which makes the injection of Y into X continuous. The *product topology* on $X_1 \times X_2$ is that for which $A \subset S_1 \times S_2$ is open if and only if A is a union of products of open sets, i.e. a basis is made of the products of an open set in X_1 by an open set in X_2; for a general product $P = \prod_{i \in I} X_i$ where X_i has topology $\mathcal{T}_i$, the product topology on P has a basis made of the products $A = \prod_{i \in I} A_i$ with $A_i \in \mathcal{T}_i$ for all $i \in I$ and $A_i = X_i$ except for i in a finite subset J of I, i.e. it is the coarsest topology which makes all the projections π_i from P onto X_i continuous. If f is continuous from a connected space X_1 into X_2, then $f(X_1)$ is connected.

A group G is a *topological group* if it has a topology such that $(x, y) \mapsto x\, y$ is continuous from $G \times G$ into G, and $x \mapsto x^{-1}$ is continuous from G into G.

A topology is T_1 if for all $a, b \in X$ with $a \neq b$ there exists an open set A such that $a \in A$ and $b \notin A$, i.e. every point is closed. A topology is T_2 or *Hausdorff* if for all $a, b \in X$ with $a \neq b$ there exists two disjoint open sets A, B such that $a \in A$ and $b \in B$, i.e. the diagonal is closed in $X \times X$. A topology is T_3 or *regular* if for all $A \subset X$ closed and $b \in X$ with $b \notin A$ there exists an open set A_+ such that $A \subset A_+$ and $b \notin A_+$. A topology is T_4 or *normal* if for all disjoint closed sets A, B there exist two disjoint open sets A_+, B_+ such that $A \subset A_+$ and $B \subset B_+$.

A topological space is *compact* if and only if for every *open covering* of X (i.e. $X = \bigcup_{i \in I} U_i$ with all U_i open) there exists a finite *subcovering* (i.e. $X = \bigcup_{j \in J} U_j$ for a finite $J \subset I$), or equivalently if and only if X has the *finite intersection property*, i.e. if a family of closed set $F_i, i \in I$ is such that $\bigcap_{j \in J} F_j \neq \emptyset$ for all finite subsets $J \subset I$, then $\bigcap_{i \in I} F_i \neq \emptyset$. Any closed subset of a compact space is compact. In a Hausdorff space, every compact subset is closed. A compact Hausdorff space is normal. If f is continuous from a compact space X_1 into X_2, then $f(X_1)$ is compact; if moreover X_2 is a compact Hausdorff space, then the image by f of a closed set in X_1 is a closed set in X_2, so that if f is also a bijection, then its inverse f^{-1} is continuous, i.e. it is an *homeomorphism*: on a compact Hausdorff space one cannot replace the topology by a strictly finer topology and still have a compact space, and one cannot replace the topology by a strictly coarser topology and still have a Hausdorff space.

A *metric space* (X, d) has a topology defined by a *metric* (or *distance*) d, which is a mapping from $X \times X$ into $\mathbb{R}$ such that $d(y, x) = d(x, y) \geq 0$ for all $x, y \in X$, $d(x, y) = 0$ if and only if $y = x$, and satisfying the *triangle inequality* $d(x, z) \leq d(x, y) + d(y, z)$ for all $x, y, z \in X$: for $x \in X$ and $r > 0$ the *open ball* $B_x(r)$ is $\{y \in X \mid d(x, y) < r\}$, and a basis of the topology is given by the family of open balls. A sequence x_n converges to x_∞ if $d(x_n, x_\infty)$ tends to 0 as n tends to ∞. For $A \subset X$, the closure $\overline{A}$ is the set of points b for which there exists a sequence a_n which converges to b and is such that $a_n \in A$ for all n. A mapping f from X_1 (with metric d_1) into X_2 (with metric d_2) is continuous at a if it transforms sequences converging to a into sequences converging to $f(a)$, or equivalently, for every $\varepsilon > 0$ there exists $\delta > 0$ such that $d_1(x, a) < \delta$ implies $d_2\big(f(x), f(a)\big) < \varepsilon$. A metric space X (with metric d) is compact if and only if for every sequence $x_n \in X$ there exists a subsequence $y_n = x_{g(n)}$ which converges.[7]

[7] For $(X, \mathcal{T})$, $x_n \to x_\infty$ means that for every open set $U \ni x_\infty$, one has $x_n \in U$ for n large enough.