TRANSCENDENCE DEGREE

ALEX WRIGHT

1. Introduction

We can describe the size of a field extension E/F using the idea of dimension from linear algebra.

$$[E : F] = \dim_F(E)$$

But this doesn't say enough about the size of really big field extensions.

$$[F(x_1) : F] = [F(x_1, ..., x_n) : F] = \infty$$

So we will define a new notion of the size of a field extension E/F, called transcendence degree. It will have the following two important properties.

$$tr.deg(F(x_1, ..., x_n)/F) = n$$

and if E/F is algebraic,

$$tr.deg(E/F) = 0$$

The theory of transcendence degree will closely mirror the theory of dimension in linear algebra.

2. Review of Field Theory

Definition. *$\alpha \in E$ is algebraic over $F \subset E$ if there is a non zero polynomial $p(x) \in F[x]$ such that $p(\alpha) = 0$. E/F is said to be algebraic if all $\alpha \in E$ are algebraic over F.*

Recall that $\alpha \in E$ is algebraic iff there is an intermediate field $F \subset L \subset E$ such that $\alpha \in L$ and $[L : F] < \infty$.

Lemma. *If $\alpha_1, ..., \alpha_n \in E$ are algebraic over F then*

$$[F(\alpha_1, ..., \alpha_n) : F] < \infty$$

and E/F is an algebraic extension.

It is in fact also true that if $\alpha_i, i \in I$ are infinitely many elements contained in some extensions E of F, and each α_i is algebraic over F, then $F(\alpha_i : i \in I)/F$ is algebraic. We will use this fact latter on.

Date: December 2006.

Theorem. *If K/L and L/M are algebraic extensions, then K/M is algebraic too.*

Proof. *Take $\alpha \in K$. Pick $p(x) = a_0 + ... + a_n x^n \in L[x], p(x) \neq 0$ so that $p(\alpha) = 0$. Now α is algebraic over $M(a_0, ..., a_n)$ But, by the KLM Theorem and the previous lemma,*

$$\begin{aligned} & [M(\alpha, a_0, ..., a_n) : M] \\ \leq\; & [M(\alpha, a_0, ..., a_n) : M(a_0, ..., a_n)][M(a_0, ..., a_n) : M] \\ \leq\; & n[M(a_0, ..., a_n) : M] \\ <\; & \infty \end{aligned}$$

so α is contained in a finite degree extension of M. Hence α is algebraic over M. Since every element of K is algebraic over M, by definition K/M is algebraic.

3. Algebraic (In)dependence

Let E/F be a field extension, and $S \subset E$.

Definition. *S is algebraically independent over F if for all non zero polynomials $p(x_1, ..., x_n) \in F[x_1, ..., x_n]$, and $s_1, ..., s_n \in S$ (all distinct), we have $p(s_1, ..., s_n) \neq 0$. S is algebraically dependent over F if it is not algebraically independent.*

Example (1). *If E/F is an algebraic extension and $\alpha \in E$ then $\{\alpha\}$ is algebraically dependent.*

Example (2). *In $F(x_1, ..., x_n)/F$, $\{x_1, ..., x_n\}$ is algebraically independent.*

Lemma. *If $S \subset E$ is algebraically independent, then S is maximal iff E is algebraic over $F(S)$.*

Proof. *If α is algebraic over $F(S)$, then α satisfies some non zero polynomial equation with coefficients in $F(S)$.*

$$\frac{p_0(s_1, ..., s_n)}{q_0(s_1, ..., s_n)} + \frac{p_1(s_1, ..., s_n)}{q_1(s_1, ..., s_n)}\alpha + ... + \frac{p_m(s_1, ..., s_n)}{q_m(s_1, ..., s_n)}\alpha^m = 0$$

Here the $p_i \in F[x_1, ..., x_n]$, and $s_1, ..., s_n \in S$. Clearing denominators we get that α satisfies

$$r_0(s_1, ..., s_n) + ... + r_m(s_1, ..., s_n)\alpha^m = 0$$

where $r_0 = p_0 q_1 q_2 ... q_m \in F[x_1, ..., x_n]$ etc. Thus $S \cup \{\alpha\}$ is not algebraically independent. This proves that if $E/F(S)$ is algebraic, then S is maximal. (We cannot add any $\alpha \in E$ to it.)

Conversely, suppose S is maximal. Take $\alpha \in E, \alpha \notin S$. $S \cup \{\alpha\}$ is not algebraically independent, so we can find a non zero polynomial $p \in F[x_0, x_1, ..., x_n]$ and $s_1, ..., s_n \in S$ such that $p(\alpha, s_1, ..., s_n) = 0$. Since S is algebraically independent, α must actually appear in this expression. Grouping powers of α we get

$$p(\alpha, s_1, ..., s_n) = p_0(s_1, ..., s_n) + ... + p_m(s_1, ..., s_n)\alpha^m = 0$$

Thus α is algebraic over $F(S)$. This shows that all $\alpha \notin S$ are algebraic over $F(S)$. Of course all $\alpha \in S$ are also algebraic over $F(S)$. Thus $E/F(S)$ is algebraic.

Lemma. *Let A be a set. If E/F has an algebraically independent set of cardinality $|A|$ then $F(x_\alpha : \alpha \in A)$ can be embedded into E.*

Proof. *Let $S = \{s_\alpha : \alpha \in A\}$ be an algebraically independent subset of E of cardinality $|A|$. We can define a map*

$$\phi : F[x_\alpha : \alpha \in A] \to E$$

by saying $\phi|_F$ is the identity and $\phi(x_\alpha) = s_\alpha$. Since S is algebraically independent, the kernel of ϕ is trivial, and ϕ is an injection. Thus we can take

$$\Phi : F(x_\alpha : \alpha \in A) \to E : \frac{p(x_{\alpha_1}, ..., x_{\alpha_n})}{q(x_{\alpha_1}, ..., x_{\alpha_n})} \mapsto \frac{\phi(p)}{\phi(q)}$$

as the desired injection of $F(x_\alpha : \alpha \in A)$ into E.

We will end up defining the transcendence degree of E/F as the size of an algebraically independent subset of E. To prove this is well defined, we need to prove the following result, which mirrors the proof that the size of a vector space basis is unique.

Theorem (Exchange Lemma)**.** *Let E/F be a field extension. If E is algebraic over $F(a_1, ..., a_n)$, and $\{b_1, ..., b_m\}$ is an algebraically independent set, then $m \leq n$.*

Proof. *b_1 is algebraic over $F(a_1, ..., a_n)$. So there is a non-zero polynomial p such that $p(b_1, a_1, ..., a_n) = 0$. b_1 must appear somewhere in the polynomial, so must some a_i. Without loss of generality, we can assume a_1 appears in $p(b_1, a_1, ..., a_n)$. So a_1 is algebraic over $F(b_1, a_1, ..., a_n)$. Now $F(b_1, a_1, ..., a_n)$ is algebraic over $F(b_1, a_2, ..., a_n)$, and E is algebraic over $F(b_1, a_1, ..., a_n)$, so E must be algebraic over $F(b_1, a_2, ..., a_n)$.*

Once we have that E is algebraic over $F(b_1, ..., b_r, a_{r+1}, ..., a_n)$, we again "exchange" an a_i for a b_j. b_{r+1} is algebraic over the field $F(b_1, ..., b_r, a_{r+1}, ..., a_n)$. So there is a non-zero polynomial p such that $p(b_1, ..., b_{r+1}, a_{r+1}, ..., a_n) = 0$. Since the b_i's are algebraically independent, one of the a_i's must appear in this expression. By re-numbering *we can get that a_{r+1} appears in this expression. Hence again we will get that E is algebraic over $F(b_1, ..., b_{r+1}, a_{r+2}, ..., a_n)$. When this process terminates we see that E is algebraic over $F(b_1, ..., b_n)$ (or, if $m < n$, $F(b_1, ..., b_m, a_{m+1}, ..., a_n)$). Hence $m \leq n$.*

Corollary. *If E/F has a maximal, finite, algebraically independent set $\{s_1, ..., s_n\}$ then any other maximal algebraically independent set also has size n.*

Proof. *E is algebraic over $F(s_1, ..., s_n)$. So by applying the lemma, we see that any other maximal algebraically independent set has at most n elements. And if $\{t_1, ..., t_m\}$ is another maximal algebraically independent set, by applying the lemma on $F(t_1, ..., t_m)$ we get that $n \leq m$. Thus $m = n$.*

In fact it is true that if E/F has two maximal algebraically independent sets S and T then $|S| = |T|$. This is analogous to the fact that the cardinality of a vector space basis is unique, even when it is infinite. The proof of this fact is difficult, and we will not need this result. The interested reader can find a proof in Hungerford's Algebra, page 315.

Theorem. *Every extension E/F has a maximal algebraically independent subset.*

Proof. *This is the same proof that every vector space has a basis. If E/F is algebraic, $\emptyset$ is a maximal algebraically independent subset. Otherwise, look at $\mathcal{S}$, set of algebraically independent subsets of E. If $\mathcal{C}$ is a chain of increasing sets in $\mathcal{S}$, then $\cup\mathcal{C} \in \mathcal{S}$. Hence by Zorn's Lemma, $\mathcal{S}$ has a maximal element S. S is a maximal algebraically independent set.*

This same proof in fact can be adapted to prove the following.

Theorem. *Every algebraically independent subset T of E can be extended to a transcendence base of $E/F/$*

Proof. *Set $\mathcal{S}$ as the set of algebraically independent subsets of E that contain T and proceed as above.*

This fact should be compared with the fact that in Linear Algebra, every linearly independent set can be extended to a basis.

Transcendence Degree

Definition. *A maximal algebraically independent subset $S \subset E$ is called a transcendence base for E/F.*

So by an earlier lemma, S is a transcendence base for E/F iff S is algebraically independent and E is algebraic over $F(S)$.

This should be compared to the statement that S is a basis for a vector space V iff the vectors of S are linearly independent and S spans V.

Definition. *The transcendence degree of E/F is the size of a transcendence base. It is denoted $tr.deg(E/F)$.*

Example. $tr.deg(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = 0$

Example. $tr.deg(F(x_1, ..., x_n)/F) = n$

Definition. *An extension E/F is called purely transcendental if it has a transcendence base S such that $E = F(S)$.*

Example. *$F(x_1, ..., x_n)/F$ is purely transcendental but $\mathbb{Q}(\sqrt{2}, x)/\mathbb{Q}$ is not (why?).*

Theorem. *Every field extension E/F is a purely transcendental extension followed by an algebraic extension.*

Proof. *Take a transcendence base S for E/F. Then $F(S)/F$ is purely transcendental and $E/F(S)$ is algebraic.*

Theorem. *Let E/F be a field extension. Suppose $S \subset E$ and E is algebraic over $F(S)$, then there is a transcendence base T for E/F with $T \subset S$.*

Proof. *Let T be a maximal algebraically independent subset of S. Every element of S is algebraic over $F(T)$, so $F(S)$ is algebraic over $F(T)$. E is algebraic over $F(S)$, so in fact we have that E is algebraic over $F(T)$.*

This is similar to how we can find a vector space basis in any spanning set. We now have so many comparisons between transcendence degree and dimension that we can create the following table.

Dimension	**Transcendence Degree**
S is linearly independent	S is algebraically independent
S spans E	E is algebraic over $F(S)$
Every vector space has a basis	Every extension has a transc. base

There are many applications of transcendence bases. A classic is the following.

Theorem. *$\mathbb{Q}[x_1, ..., x_n]$ is not isomorphic to $\mathbb{Q}[x_1, ..., x_m]$ if $n \neq m$.*

Proof. *If these two rings were isomorphic, their fraction fields would also be isomorphic.*

$$\mathbb{Q}(x_1, ..., x_n) \cong \mathbb{Q}(x_1, ..., x_m)$$

The field on the left has transcendence degree n, and the one on the right has transcendence degree m, so these fields can be isomorphic only if $m = n$.

Transcendence degree can also be used to show that $\mathbb{C}$ has proper sub-fields which are isomorphic to $\mathbb{C}$. (In contrast, there are no proper sub-fields of $\mathbb{R}$ which are isomorphic to $\mathbb{R}$.) And more surprisingly, transcendence degree can be used to show that any algebraically closed field of cardinality $|\mathbb{C}|$ is in fact isomorphic to $\mathbb{C}$. The theory of transcendence degree is also used to prove that you can extend certain field homomorphism to larger fields.

References

[1] Lang, Serg. Algebra. Addison-Wesley Publishing Company.

[2] Hungerford, Thomas. Algebra. Springer.

E-mail address: `amwright@uwaterloo.ca`