# Commutative Algebra – Lecture 12: Algebras and Affine Fields (Oct. 16, 2013)

Stephen Melczer

October 16, 2013

## 1 Finishing up another proof of Theorem A

Recall that last time we had

**Proposition** (Special case of Noether normalization). *Let $R = F[a_1, \dots, a_n]$ be an affine algebra and suppose that $R$ is algebraic over $F[a_1]$. Then there exists $b \in R$ such that $R = F[b, a_2, \dots, a_n]$ and $R$ is integral over $F[b]$.*

Before our alternate proof, we need two observations. First,

**Lemma 1.** *Suppose $C \subset R$ with $c \in C$ invertible in $R$ and $c^{-1}$ integral over $C$. Then $c^{-1} \in C$.*

*Proof.* Since $c^{-1}$ is integral over $C$ we have

$$\left(c^{-1}\right)^n + \sum_{i=0}^{n-1} a_i \left(c_{-1}\right)^i = 0,$$

where the $a_i$ are in $C$. Multiplying by $c^{n-1}$ gives

$$c^{-1} = \sum_{i=0}^{n-1} (-a_i) c^{n-i-1},$$

and $n - i - 1 \geq 0$ for $0 \leq i \leq n-1$. □

Second,

**Proposition.** *Suppose $R$ is a domain and $C$ is a subring of $R$ such that $R$ is integral over $C$. Then $R$ is a field if and only if $C$ is a field.*

*Proof.* The forward implication follows from the previous lemma. For the reverse, take $a \in R$ with $a \neq 0$. Then $C[a] \subset R$ and $C[a]$ is a field since we assumed $C$ is a field and $a$ is integral. Thus, $a^{-1} \in C[a] \subset R$ and $R$ is a field. □

Here is our old friend, which we will now prove without the Artin-Tate lemma.

**Theorem 1.1** (Main Theorem A). *An affine algebra $R = F[a_1, \ldots, a_n]$ is a field if and only if $R$ is algebraic over $F$.*

*Proof.* Our old proof of the reverse implication did not use the Artin-Tate lemma. For the forward, we may again show by induction that $R$ is algebraic over the field of fractions of $F[a_1]$ and thus, clearing denominators, we may assume that $R$ is algebraic over $F[a_1]$.

By the special case of Noether normalization, there exists $b \in R$ such that $R$ is integral over $F[b]$ and $R = F[b, a_2, \ldots, a_n]$. But $R$ is a field, so by the previous proposition $F[b]$ is a field. Thus, $b$ is algebraic over $F$ and by the transitivity of integral extensions we are done. □

# 2 Dependence Relations

## 2.1 Introduction to dependence relations

Our first step is a language for general dependence relations.

**Definition 2.1.** A *strong abstract dependence relation (s.a.d.r.)* on a set $V$ is a relation $\delta$ between elements of $V$ and subsets of $V$, written $v\delta S$ satisfying (AD1–AD4)

(AD1) $v \in S$ implies $v\delta S$

(AD2) Suppose that $v\delta S$ and suppose that $S_1 \subset V$ such that for all $s \in S$, $s\delta S_1$, then $v\delta S_1$

(AD3) (Steinitz exchange property) $v\delta(S \cup \{s\})$ and $v \not\delta S$ then $s\delta(S \cup \{v\})$

(AD4) $v\delta S$ implies there exists $S_0 \subset S$ with $|S_0| < \infty$ with $v\delta S_0$

Let's see how this captures linear dependence. Let $V$ be a vector space, and take $v\delta S$ to mean that $v$ is in the span of $S$. Let's check the axioms:

(AD1) If $v \in S$ then $v$ is trivially in the span of $S$.

(AD2) Suppose that $v \in \mathrm{Span}(S)$. Then write

$$v = \sum_{I \in I} \alpha_i s_i,$$

for $\alpha_i \in F$, $s_i \in S$, and $I$ a finite index set. Then if each $s_i \in \mathrm{Span}(S_1)$ we can write $s_i = \sum_{j \in J} \beta_{ij} t_j$ for $t_i \in S_0$ and $J$ some finite index set, so $v = \sum_{j \in J} \sum_{i \in I} \alpha_i \beta_{ij} t_j$ which is in the span of $S_1$.

(AD3) Say $v$ is in the span of $S \sup\{s\}$ so $v = \sum \alpha_i s_i + \beta s$ with $\alpha_i, \beta \in F$ and $s_i \in S$. Then $\beta \neq 0$ since $v \notin \mathrm{Span}(S)$ so $s = (1/\beta)v - \sum(\alpha_i/\beta)s_i$ which is in the span of $S \cup \{v\}$.

(AD4) Say $v \in \mathrm{Span}(S)$. Then $v = \sum \alpha_i s_i$ with $s_i \in S$. But this sum is finite, so let $S_0$ be the set of the $s_i$ in the finite sum. Then $S_0$ is finite and $v$ is in its span.

Thus, linear dependence is an example of a s.a.d.r. Can we get linear algebra results?

## 2.2 Dependences in linear algebra

**Definition 2.2.** Let $\delta$ be a s.a.d.r. on $V$. We say that $S \subset V$ is independent if $s \not\delta (S \setminus \{s\})$ for all $s \in S$, and say that $S \subset V$ is dependent if it is not independent.

First, we show that we can extend an independent set by including an elements that does not depend on it.

**Lemma 2.** *Let $\delta$ be a s.a.d.r. on $V$. Suppose that $S$ is an independent subset of $V$ and $v \not\delta S$. Then $S \cup \{v\}$ is independent.*

*Proof.* Suppose that the result doesn't hold. Since $v \not\delta S$ there must exist $s \in S$ such that $s\delta((S \cup \{v\}) \setminus \{s\})$. But this is equivalent to $s\delta((S \setminus \{s\}) \cup \{v\})$, so by the Steinitz exchange property $v\delta((S \setminus \{s\}) \cup \{s\})$, a contradiction. □

We now wish to look at what it means to be a basis.

**Definition 2.3.** Let $\delta$ be a s.a.d.r. on $V$. A base of $V$ is a maximal independent subset of $V$.

To begin, we prove that any independent set can be extended to a basis.

**Proposition.** *Let $\delta$ be a s.a.d.r. on $V$, and $S$ be an independent subset of $V$. Then $S$ is contained in a base of $V$.*

*Proof.* Let $\mathcal{S}$ be the set of all independent subsets of $V$ which contain $S$. Let $S_1 \subset S_2 \subset \cdots$ be a chain in $\mathcal{S}$. Consider the union $U$ of the $S_i$. Clearly $S \subset U$. Furthermore, suppose that $U$ is not independent, i.e., there exists some $v \in U$ with $v\delta(U \setminus \{v\})$. By AD4, there exists a finite $T \subset U \setminus \{v\}$ with $v\delta T$. But as $T$ is finite, at some point in the chain we have an $S_j$ with $T \subset S_j$ and $v \in S_j$, contradicting $S_j$ being independent. Since $S \in \mathcal{S}$, Zorn's Lemma implies that $\mathcal{S}$ contains a maximal element. □

We also see that every element of $V$ depends on a basis, by maximality.

**Proposition.** *Let $\delta$ be a s.a.d.r. on $V$ and let $B$ be a base of $V$. Then for all $v \in V$, $v\delta B$.*

*Proof.* By maximality and our lemma about extending by a single element. □

Next we show that all bases have the same cardinality.

**Proposition.** *Let $\delta$ be a s.a.d.r. on $V$. Any two bases of $V$ have the same cardinality.*

*Proof.* We haven't talked about cardinals, so we will only prove it in the finite case. Let $B, B'$ be bases, and write $B = \{b_1, \ldots, b_t\}$. By symmetry it suffices to show that $|B| \leq |B'|$.

We claim that there exists $b'_1, \ldots, b'_k \in B'$ such that $\{b'_1, \ldots, b'_k, b_{k+1}, \ldots, b_t\}$ is independent. If $k = 0$ then the result holds. Now suppose we know that $\{b'_1, \ldots, b'_{k-1}, b_k, \ldots, b_t\}$ is independent. Then $b_k \not\delta \{b'_1, \ldots, b'_{k-1}, b_{k+1}, \ldots, b_t\}$, but $b_k \delta B'$. By AD2 with $B'$ as $S$ and $\{b'_1, \ldots, b'_{k-1}, b_{k+1}, \ldots, b_t\}$ as $S_1$, we see that there exists some $b'_k \in B'$ such that $b'_k \not\delta \{b'_1, \ldots, b'_{k-1}, b_{k+1}, \ldots, b_t\}$ and by our previous lemma $\{b'_1, \ldots, b'_{k-1}, b'_k, b_{k+1}, \ldots, b_t\}$ is independent. This proves the claim, and applying the claim with $t = k$ proves the theorem. □

## 2.3 Algebraic dependence

Now lets apply these ideas to algebraic dependence.

**Definition 2.4.** Let $R$ be an $F$-algebra. Say $a_1, \ldots, a_n \in R$ are algebraically independent over $F$ if $\psi : F[\lambda_1, \ldots, \lambda_n] \to F[a_1, \ldots, a_n]$ given by $\lambda_i \mapsto a_i$ is one-to-one. If $a_1, \ldots, a_n$ are not independent, we say they are algebraically dependent.

Let $R$ be an $F$-algebra and a domain – then we say that $a\delta S$ if $a$ is algebraic over $F[S]$.

**Proposition.** *Suppose $S$ is algebraically independent over $F$. Then $a\delta S$ if and only if $S \cup \{a\}$ is an algebraic dependence over $F$.*

*Proof.* First, suppose that $S \cup \{a\}$ is algebraically dependent. Then there exists $f \in F[\lambda_1, \ldots, \lambda_{n+1}]$ such that $f(s_1, \ldots, s_n, a) = 0$ for $s_i \in S$. Since $S$ is algebraically independent $\lambda_{n+1}$ must appear in $f$. Let $g(\lambda_{n+1}) = f(s_1, \ldots, s_n, \lambda_{n+1})$, so $g \in F[S][\lambda_{n+1}]$ is still a nontrivial polynomial with $g(a) = 0$. Thus, $a$ is algebraic over $F[S]$ so $a\delta S$.

Finally, say $a\delta S$. Then there exists $g \in F[S][\lambda]$ such that $g(a) = 0$. The coefficients of $g$ involve only finitely many $s_i \in S$ – call these $s_1, \ldots, s_n$. If we view $g \in F[\lambda_1, \ldots, \lambda_n, \lambda]$ with $g(s_1, \ldots, s_n, a) = 0$ so $S \cup \{a\}$ is algebraically dependent over $F$. □

We are able to apply our general results above, due to the following proposition.

**Proposition.** *This $\delta$ be a s.a.d.r.*

*Proof.* AD1 Take $v \in S$. Then $v$ is algebraic over $F[S]$ as it satisfies $\lambda - v$.

AD3 Take $v$ algebraic over $F[S \cup \{s\}]$ but $v$ not algebraic over $F[S]$. Then there exists $f \in F[S \cup \{s\}][\lambda]$ with $f(v) = 0$. But $s$ appears non-trivially in $f$ since $v \not\delta S$. If we view $f \in F[S][\lambda', \lambda]$ with $f(s, v) = 0$ then we have $f \in F[S \cup \{v\}][\lambda']$ with $f(s) = 0$ and $f$ is non-trivial in $F[S \cup \{v\}]$.

AD4 Say $v$ is algebraic over $F[S]$ so $f(v) = 0$ for some $f \in F[S][\lambda]$. Only finitely many elements of $S$ appear in the coefficients of $f$, call this set $S_0$. Then $f \in F[S_0][\lambda]$ so $v\delta S_0$.

AD2 Suppose $v\delta S$ and $S_1$ is such that $s\delta S$ for all $s \in S$. By AD4, there exists $S_0 \subset S$ finite with $v\delta S_0$. Then $v$ is algebraic over $F[S_0]$, and each $s_i \in S_0$ is algebraic over $F[S_1]$. Let $K$ be the field of fractions of $F[S_0]$. Let $L$ be the field of fractions of $F[S_1]$.

We have transitivity of algebraic extensions for fields. Note that each $s_i \in S_0$ is algebraic over $L$ and $v$ is algebraic over $K$. So by transitivity $v$ is algebraic over $L$. Then there exists $f \in L[\lambda]$ with $f(v) = 0$. Clear denominators to get $f \in F[S_1]$ with $g(v) = 0$, so $v\delta S_1$.

□

This leads to the following definition.

**Definition 2.5.** Let $R$ be an $F$-algebra and domain. Let $B$ be a base with respect to $\delta$. We say that $B$ is a transcendence base, and that the size of $B$ is the transcendence degree of $R$ (which is well defined by our work above). This is written $tr.deg_F(R)$.

## References

[1] L.H. Rowen, *Graduate Algebra: Commutative View*, American Mathematical Society, 2006.