Commutative Algebra – Lecture 10: Algebras and Affine Fields (Oct. 11, 2013)

Navid Alaei

December 9, 2013

1 Theorem A, Artin-Tate Lemma, and Integral Extensions

Recall that last time we stated Theorem A concerning characterization of affine domains.

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.*

To this end, we stated, and proved, two main lemmas to help with the proof of Theorem (1.1);

Lemma 1. *Suppose R is an F-algebra and $a \in R$. If the field of fractions K of $F[a]$ is affine over F, then a is algebraic over F, and thus $K = F[a]$.*

Lemma 2. *Suppose R is an algebra over a commutative ring K, which as a K-module is free with base $B = \{b_j : j \in J\}$ for some index set J. If H is a subring of K over which B spans R, then $H = K$.*

In order to prove theorem (1.1), we need one last lemma.

Lemma 3 (Artin-Tate)**.** *Suppose $R = F[a_1, \ldots, a_n]$ is an affine F-algebra, and K a subfield of R, with R a finite dimensional vector space over K. Then K is affine over F.*

Note: *Before we prove the Artin-Tate lemma, recall that we have already established that if $R = F[a_1, \ldots, a_n]$ is algebraic over F, then R is a field. So Artin-Tate lemma will facilitate the proof of the forward direction. We proceed by induction on n. When $n = 1$, we know from field theory that $F[a_1]$ is a field if and only if a_1 is a algebraic over F (see Remark 4.7 in [1] for more details). Now suppose that the result is valid for all positive integers up to and including $n - 1$. Suppose $R = F[a_1, \ldots, a_n]$ is a field. Let K denote the field of fractions of $F[a_1]$ (inside R). Then we may write $R = K[a_2, \ldots, a_n]$, which by our induction hypothesis is algebraic over K, and thus finite dimensional as a K-vector space. Hence, it is sufficient to show that K is algebraic over F. By Lemma (1), this boils down to showing that K is affine over F. This is precisely what the Artin-Tate lemma allows us to conclude.*

Proof. Since R is finite dimensional as a K-vector space, there exists $b_1, \dots, b_m \in R$ such that $\{b_1, \dots, b_m\}$ forms a basis for R over K. By definition of a basis, we may find $\alpha_{ijk}, \beta_{uk} \in K$ such that

$$b_i b_j = \sum_{k=1}^{m} \alpha_{ijk} b_k, \qquad a_u = \sum_{k=1}^{m} \beta_{uk} b_k, \tag{1}$$

for each $1 \leq i, j \leq m$ and $1 \leq u \leq n$. Now consider

$$H = F[\alpha_{ijk}, \beta_{uk} : 1 \leq i, j \leq m, 1 \leq u \leq n] \subseteq K.$$

Set $R_0 := Hb_1 + \cdots + Hb_m$, and observe that (1) implies that R_0 is indeed closed under multiplication, and therefore is a subalgebra of R containing $a_1, \dots, a_n$. As $R_0 \subseteq R$ and contains the generators of R we must have $R_0 = R$. Applying Lemma (2) finishes the proof. □

REMARK: *Note that the assumption that $R = F[a_1, \dots, a_n]$ is a domain is crucial in Theorem A. For instance, let F be a field and consider $F \times F = F[(0,1),(1,0)]$. Then this is an affine algebra generated by algebraic elements $(1,0),(0,1)$, but is not a field, since $(1,0) \cdot (1,0) = (0,0)$.*

We now introduce the notion of *integrality*, and then use it to give an alternate proof of Theorem A. Before we do, recall that an element x of an arbitrary C-algebra R is called **algebraic** over C if x is a root of a polynomial $f(\lambda) \in C[\lambda]$.

Definition 1.2 (Integral Extension)**.** Suppose R is a C-algebra. We say that $r \in R$ is **integral** over C if $f(r) = 0$ for some ***monic*** $f(\lambda) \in C[\lambda]$. We also say that R is an **integral extension** of C if every element in R is integral over C. If this is the case, then R is said to be **integral over** C.

REMARK: *Observe that begin integral implies algebraic and these notions coincide when C is a field. The converse, however, is not true. For instance, $\sqrt{2}/2$ is algebraic over $\mathbb{Z}$ but is not integral. Indeed, let $f(\lambda) = 2\lambda^2 - 1 \in \mathbb{Z}[\lambda]$, and note $f(\sqrt{2}/2) = 0$ so that the minimal polynomial, $m(\lambda) \in \mathbb{Z}[\lambda]$, for $\sqrt{2}/2$ must have degree at most 2. But $m(\lambda)$ is clearly not of degree one, and thus must equal $f(\lambda)$. As $f(\lambda)$ is not monic, $\sqrt{2}/2$ is not integral over $\mathbb{Z}$.*

It is important to note that integrality is, in fact, the right notion which generalizes the notion of algebraicity to extensions of arbitrary commutative rings.

Lemma 4. *Suppose R is a C-algebra and $r \in R$ is algebraic over C; i.e., $\sum_{j=0}^{n} c_j r^j = 0$ for some $c_0, \dots, c_n \in C$, and $n \geq 1$. Then $c_n r$ is integral over C.*

Proof. Consider the monic polynomial $\lambda^n + \sum_{j=0}^{n-1} c_n^{n-1-j} c_j \lambda^n \in C[\lambda]$. Evaluating at $c_n r$

gives

$$
\begin{aligned}
(c_n r)^n + \sum_{j=0}^{n-1} c_n^{n-1-j} c_j (c_n r)^j &= (c_n r)^n + c_n^{n-1} c_0 + c_n^{n-1} c_1 r + \cdots + c_{n-1}(c_n r)^{n-1} \\
&= c_n^n r^n + c_n^{n-1}(c_0 + c_1 r + \cdots + c_{n-1} r^{n-1}) \\
&= c_n^{n-1}(c_n r^n + c_0 + c_1 r + \cdots + c_{n-1} r^{n-1}) \\
&= 0,
\end{aligned}
$$

where the last equality follows from the assumption that r is algebraic. □

Theorem 1.3. *Suppose R is a C-algebra and $r \in R$ is given. Then the following are equivalent.*

1. *r is integral over C.*
2. *$C[r]$ is finitely generated as a C-module.*
3. *There is a faithful $C[r]$-module M which is finitely generated as a C-module.*

Proof. To begin, observe that (2) immediately implies (3). To show that (1) implies (2), note that if r is integral over C, then there exists $n \geq 1$, and suitable elements $c_0, \ldots, c_{n-1} \in C$ such that $r^n = -(c_0 + c_1 r + \cdots + c_{n-1} r^{n-1})$. But then it's evident that $C[r] = C + Cr + \cdots + Cr^{n-1}$. Lastly, it remains to show that (3) implies (1). To ease the notation, let $M = Cr_1 + Cr_2 + \cdots + Cr_k$, for some $r_1, \ldots, r_k \in R$. Fix $r \in M$ and note $xr_j \in M$ for all $1 \leq j \leq k$. Hence, there exists elements $c_{ij} \in C$ such that

$$
rr_i = \sum_{j=0}^{k} c_{ij} r_j, \tag{2}
$$

holds for each $1 \leq i \leq k$. Let A be the $k \times k$ matrix whose $(i,j)^{\text{th}}$ entry is given by c_{ij}, and let $\mathbf{v} = [r_1, \ldots, r_k]^T$, where T denotes the transpose operator. By (2), we obtain

$$
(x\mathbf{I}_k - A)\mathbf{v} \begin{bmatrix} r - c_{11} & -c_{12} & \cdots & -c_{1k} \\ -c_{21} & r - c_{22} & \cdots & -c_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ -c_{rk1} & -c_{k2} & \cdots & r - c_{kk} \end{bmatrix} \cdot \begin{bmatrix} r_1 \\ r_2 \\ \vdots \\ r_r \end{bmatrix} = \mathbf{0},
$$

where $\mathbf{I}_k$ denotes the $k \times k$ identity matrix. This means

$$
(\det A)\mathbf{v} = (\text{adj } A)(A\mathbf{v}) = 0. \tag{3}
$$

In particular, the left hand side of (3) immediately gives $(\det A) r_j = 0$ for each $j = 1, \ldots, k$. But then

$$
(\det A) M = (\det A) \sum_{j=1}^{k} C r_j = 0. \tag{4}
$$

Since M is faithful, its annihilator is trivial and so (4) implies $\det A = 0$. Noting that $\det A$ is a monic polynomial in r, we obtain the desired result. □

Theorem (1.3) has many striking implications.

Corollary. *If R is C-algebra which is finitely generated as a C-module, then R is an integral extension of C.*

Proof. Given $r \in R$, note $C[r] \subseteq R$ and one may view R (naturally) as a $C[r]$-module. Now apply Theorem (1.3). □

Lemma 5. *Suppose $C \subseteq L \subseteq R$ are rings with C and L commutative. Then*

1. *If L is finitely generated as a C-module and R is finitely generated as an L-module, then R is finitely generated as a C-module.*

2. *If $r \in R$, and if L and $C[r]$ are both finitely generated as a C-module, then $L[r]$ is also finitely generated as a C-module.*

Proof. For (1), note we may pick $\ell_1, \ldots, \ell_n \in L$ and $r_1, \ldots, r_m \in R$ such that $L = C\ell_1 + \cdots + C\ell_n$ and $R = Lr_1 + \cdots + Lr_m$. We claim that $R = C\ell_1 r_1 + \cdots + C\ell_n r_m$. Indeed, note $x \in R$ if and only if there exist $\beta_1 \ldots, \beta_m \in L$ such that $x = \sum_{i=1}^m \beta_i r_i$. Similarly $\beta_i \in L$ $(1 \le i \le m)$ if and only if there are $\alpha_1, \ldots, \alpha_n \in C$ such that $\beta_i = \sum_{k=1}^n \alpha_{ik}\ell_k$. Hence, we may write

$$x = \sum_{i=1}^{m} \left(\sum_{k=1}^{n} \alpha_{ik}\ell_k \right) r_i = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} \alpha_{ik}\ell_k r_i \right),$$

as desired. For part (2), note

$$C[r] := \left\{ \sum_{j=0}^{n} c_j r^j : c_j \in C, n \ge 0 \right\}, \quad L[r] := \left\{ \sum_{j=0}^{n} \alpha_j r^j : \alpha_j \in L, n \ge 0 \right\}.$$

Now we know we can write $L = C\ell_1 + \cdots + C\ell_k$ and $C[r] = Cd_1, \ldots, Cd_m$ for some $\ell_1, \ldots, \ell_k \in L$ and $d_1, \ldots, d_m \in C[r]$. This means that every power of r is spanned by some subset of $\{d_1, \ldots, d_m\}$. Consequently, one may write $L[r] = Ld_1 + \cdots + Ld_m$; i.e., $L[r]$ is finitely generated as an L-module and L is finitely generated as a C-module. Applying part (1) gives the desired result. □

Corollary. *If $r_1, \ldots, r_n \in R$ are integral over C, then $C[r_1, \ldots, r_n]$ is finitely generated as a C-module, and thus is an integral extension of C.*

Proof. This follows trivially by induction on n in view of Lemma (5) and the corollary preceding it. □

Recall from field theory that if $F \supseteq M \supseteq L$ is a tower of filed extensions such that F is algebraic over L, then F is algebraic over M and M is algebraic over L. Similarly, an analogous result holds for integral extensions.

Proposition (Transitivity of Integral Extensions)**.** *If R is integral over W and W is integral over C, then R is integral over C.*

Proof. Fix $r \in R$ and note there exists monic $f(\lambda) = \lambda^n + \sum_{j=0}^{n-1} w_j r^j \in W[\lambda]$ with $f(r) = 0$. Consider $W_0 = [w_0, \ldots, w_{n-1}]$ and note the generators of W_0 are integral over C by our original assumption, and thus the W_0 is finitely generated as a C-module, by our second corollary. Hence, r is integral over W_0 from which it follows, by part (1) of (5), that $C[w_0, \ldots, w_{n-1}, r]$ is finitely generated as a C-module. The result is now trivial. □

In order to give an alternate proof of Theorem A, we require three last results. We shall present the first one here and leave the other two for next class.

Theorem 1.4 (Special Case of Noether Normalization)**.** *Suppose an affine algebra $R = F[a_1, \ldots, a_n]$ is algebraic over $F[a_1]$. Then there exists a suitable choice of $b \in R$ such that $R = F[b, a_2, \ldots, a_n]$ and R is integral over $F[b]$.*

Proof. We proceed by induction on n. When $n = 1$, the result is trivial since we may take $b = a_1$. Now suppose $n = 2$. We must show that if $R = F[a_1, a_2]$ is affine and algebraic over $F[a_1]$, then there exists a $d \in R$ for which $R = F[d, a_2]$ and R is integral over $F[d]$. Equivalently, we wish to show that there exists $d \in R$ with a_2 is integral over $F[d]$. To begin, note that since R is algebraic over $F[a_1]$, there exists polynomials $g_j(\lambda_1) = \sum_{k=0}^{m_j} \alpha_{kj} \lambda_1^k \in F[\lambda_1]$, for each $0 \le j \le n$ and with $\alpha_{m_j j} \neq 0$, such that

$$\sum_{j=0}^{n} g_j(a_1) a_2^j = 0. \tag{5}$$

Setting

$$f(\lambda_1, \lambda_2) = \sum_{j=0}^{n} g_j(\lambda_1)\lambda_2^j = \sum_{j=0}^{n} \left(\sum_{i=0}^{m_j} \alpha_{ij} \lambda_1^i \right) \lambda_2^j \in F[\lambda_1, \lambda_2],$$

we see that (5) is equivalent to $f(a_1, a_2) = 0$. In order to ensure that a_2 is also integral over $F[a_1]$, we must have that $f(\lambda_1, \lambda_2)$ is monic in λ_2. Define

$$h(\lambda_1, \lambda_2) := f(\lambda_1 + \lambda_2^{n+1}, \lambda_2), \qquad \text{and} \qquad d = a_1 - a_2^{n+1}.$$

Note $h(d, a_2) = f(a_1, a_2) = 0$. Now consider the expression for $h = f(\lambda_1 + \lambda_2^{n+1}, \lambda_2)$; namely

$$\sum_{j=0}^{n} \left(\sum_{i=0}^{m_j} \alpha_{ij} (\lambda_1 + \lambda_2^{n+1})^i \right) \lambda_2^j. \tag{6}$$

It is evident that the highest order term of h in λ_2 is obtained by choosing the largest j for which m_j is greatest; i.e., if we let j' denote the the largest j with respect to having the largest value m_j, then the leading coefficient of h in λ_2 is given by

$$\alpha_{m_{j'} j'} \lambda_2^{(n+1)m_{j'} + j'}.$$

By construction, the value $(n+1)m_{j'}+j'$ is unique so that the leading term in λ_2 cannot vanish by cancellation through another term. Lastly, since we are working over a field F, all coefficients are invertible; it is no loss generality to assume h is monic. Since $h(d, a_2) = 0$, this shows that a_2 is integral over $F[d]$. But note this forces $a_1 = d + a_2^{n+1}$ to be integral over $F[d]$. Combining these observations, we conclude that R is integral over $F[d]$. This verifies the case for $n = 2$. WE WILL FINISH OFF THE INDUCTION NEXT TIME! $\square$

References

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