18.705 Commutative Algebra
Fall 2008

Theorem (Refined Noether Normalization Lemma). *Let k be a field, R a finitely generated k-algebra, and $\mathfrak{a}_1 \subset \cdots \subset \mathfrak{a}_r \subsetneqq R$ a chain of proper ideals. Then there exist algebraically independent elements $t_1, \dots, t_n$ of R such that*

(a) *R is module finite over $k[t_1, \dots t_n]$;*

(b) *for $1 \le i \le r$, there is an $h(i)$ such that $\mathfrak{a}_i \cap k[t_1, \dots t_n] = \big(t_1, \dots, t_{h(i)}\big)$.*

Proof (Cf. [Bourbaki, "Commutative Algebra," Thm. 1, p. 344].) By hypothesis, $R = S/\mathfrak{b}_0$ where S is a polynomial ring $k[T_1, \dots, T_m]$. Say $\mathfrak{a}_i = \mathfrak{b}_i/\mathfrak{b}_0$. Then it suffices to prove the assertion for S and $\mathfrak{b}_0 \subset \mathfrak{b}_1 \subset \cdots \subset \mathfrak{b}_r$. Thus we may assume R is the polynomial algebra $k[T_1, \dots, T_m]$. The proof proceeds by induction on r.

First, suppose $r = 1$ and $\mathfrak{a}_1$ is a principal ideal generated by a nonzero element t_1. Then $t_1 \notin k$ because $\mathfrak{a}_1 \ne R$. Write $t_1 = \sum a_{(j)} T_1^{j_1} \cdots T_m^{j_m}$ where (j) denotes $(j_1, \dots, j_m) \in \mathbb{Z}^m_{\ge 0}$ and $a_{(j)} \in k$ is nonzero. We are going to choose positive integers s_i for $2 \le i \le m$ such that T_1 is integral over $R' := k[t_1, t_2, \dots, t_m]$ where $t_i := T_i - T_1^{s_i}$. Then clearly, (a) follows.

Note that T_1 satisfies the equation,

$$t_1 - \sum a_{(j)} T_1^{j_1} (t_2 + T_1^{s_2})^{j_2} \cdots (t_m + T_1^{s_m})^{j_m} = 0.$$

Set $e(j) := j_1 + s_2 j_2 + \cdots + s_m j_m$. Take $s_i := \ell^i$ where ℓ is an integer greater than all of the j_i. Then the $e(j)$ are distinct. Let $e(j')$ be largest $e(j)$. Then the above equation can be written in the form

$$a_{(j')} T_1^{e(j')} + \sum_{v < e(j')} Q_v T_1^v = 0$$

where $Q_v \in R'$, and hence, T_1 is integral over R'. Thus (a) holds.

By the theory of transcendence bases [Artin, "Algebra," Ch. 13, § 8, pp. 525–527], the elements $t_1, \dots, t_m$ are algebraically independent. Let $x \in \mathfrak{a}_1 \cap R'$. Then $x = t_1 x'$ where $x' \in R \cap k(t_1, \dots, t_m)$. Furthermore, $R \cap k(t_1, \dots t_m) = R'$ because R' is normal as it is a polynomial algebra. Hence $\mathfrak{a}_1 \cap R' = t_1 R'$. Thus (b) holds in case $r = 1$ and $\mathfrak{a}_1$ is principal.

Second, suppose $r = 1$ and $\mathfrak{a}_1$ is arbitrary. If $\mathfrak{a}_1 = 0$, then we may take $t_i := T_i$. So assume $\mathfrak{a}_1 \ne 0$. The proof proceeds by induction on m. The case $m = 1$ follows from the first case (but is simpler) because $k[T_1]$ is a principal ring. Let $t_1 \in \mathfrak{a}_1$ be nonzero. By the first case, there exist elements $u_2, \dots, u_m$ such that $t_1, u_2, \dots u_m$ are algebraically independent and satisfy (a) and (b) with respect to R and $t_1 R$. By induction, there exist elements $t_2, \dots, t_m$ satisfying (a) and (b) with respect to $k[u_2, \dots, u_m]$ and $\mathfrak{a}_1 \cap k[u_2, \dots, u_m]$.

Set $R' := k[t_1, \dots, t_m]$. Since R is module finite over $k[t_1, u_2, \dots, u_m]$ and the latter is module finite over R', the former is module finite over R'. Hence (a) holds, and $t_1, \dots, t_m$ are algebraically independent. Moreover, by hypothesis,

$$\mathfrak{a}_1 \cap k[t_2, \dots, t_m] = (t_2, \dots, t_h)$$

for some $h \le m$. So $\mathfrak{a}_1 \cap k[t_1, \dots, t_m] \supset (t_1, \dots, t_h)$.

Conversely, given $x \in \mathfrak{a}_1 \cap R'$, write $x = \sum_{i=0}^d Q_i t_1^i$ where $Q_i \in k[t_2, \dots, t_m]$. Since $t_1 \in \mathfrak{a}_1$, we have $Q_0 \in \mathfrak{a}_1 \cap k[t_2, \dots, t_m]$, so $Q_{(0)} \in (t_2, \dots, t_h)$. Hence $x \in (t_1, \dots, t_h)$. Thus $\mathfrak{a}_1 \cap R' = (t_1, \dots, t_h)$. Thus (b) holds for $r = 1$.

Finally, suppose the theorem holds for $r-1$. Let $u_1, \ldots, u_m$ be algebraically independent elements of R satisfying (a) and (b) for the sequence $\mathfrak{a}_1 \subset \cdots \subset \mathfrak{a}_{r-1}$, and set $s := h(r-1)$. By the second case, there exist elements $t_{s+1}, \ldots, t_m$ satisfying (a) and (b) for $k[u_{s+1}, \ldots, u_m]$ and $\mathfrak{a}_r \cap k[u_{s+1}, \ldots, u_m]$. Then

$$\mathfrak{a}_r \cap k[t_{s+1}, \ldots, t_m] = \big(t_{s+1}, \ldots, t_{h(r)}\big)$$

for some $h(r)$. Set $t_i := u_i$ for $1 \le i \le s$. Set $R' := k[t_1, \ldots, t_m]$. Then R is module finite over $k[u_1, \ldots, u_m]$ by hypothesis, and $k[u_1, \ldots, u_m]$ is module finite over R' by hypothesis. Hence R is module finite over R'. Thus (a) holds, and $t_1, \ldots, t_m$ are algebraically independent over k.

Fix i with $1 \le i \le r$. Set $\ell := h(i)$. Then $t_1, \ldots, t_\ell \in \mathfrak{a}_i$. Given $x \in \mathfrak{a}_i \cap R'$, write $x = \sum Q_{(v)} t_1^{v_1} \cdots t_\ell^{v_\ell}$ with $(v) = (v_1, \ldots, v_\ell) \in \mathbb{Z}^\ell_{\ge 0}$ and $Q_{(v)} \in k[t_{\ell+1}, \ldots, t_m]$. Then $Q_{(0)}$ lies in $\mathfrak{a}_i \cap k[t_{\ell+1}, \ldots, t_m]$. The latter is equal to zero. It is zero if $i \le r-1$ because it lies in $\mathfrak{a}_i \cap k[u_{\ell+1}, \ldots, u_m]$, which is equal to zero. and $\mathfrak{a}_r \cap k[t_{s+1}, \ldots, t_m]$ is equal to $(t_{s+1}, \ldots, t_\ell)$ by hypothesis. So $\mathfrak{a}_r \cap k[t_{\ell+1}, \ldots, t_m] = 0$. Thus $Q_{(0)} = 0$. Hence $x \in \big(t_1, \ldots, t_{h(i)}\big)$. Thus $\mathfrak{a}_i \cap R'$ is contained in $\big(t_1, \ldots, t_{h(i)}\big)$. So the two are equal. Thus (b) holds, and the theorem is proved.

Remark (*Another proof*). Suppose k is infinite. Then in the proof of the first case, we can take $t_i := T_i - a_i T_1$ for suitable $a_i \in k$. Namely, say $t_1 = H_d + \cdots + H_0$ where H_i is homogeneous of degree i in $T_1, \ldots, T_m$ and $H_d \neq 0$. Since k is infinite, there exist $a_i \in k$ such that $H_d(1, a_2, \ldots, a_m) \neq 0$. Since $H_d(1, a_2, \ldots, a_m)$ is the coefficient of T_1^d in

$$H_d(T_1, t_2 + a_2 T_1, \ldots, t_m + a_m T_1),$$

after collecting like powers of T_1, the equation

$$t_1 - H_d(T_1, t_2 + a_2 T_1, \ldots, t_m + a_m T_1) - \cdots - H_0(T_1, t_2 + a_2 T_1, \ldots, t_m + a_m T_1) = 0$$

becomes an equation of integral dependence of degree d for T_1 over $k[t_1, \ldots, t_m]$.