COMMUTATIVE ALGEBRA HOMEWORK VII

BATCHELDER, KELLER, MOORHEAD

Problem 3 An element $u \in A$ is *integral* over an ideal $I \lhd A$ if u satisfies a monic polynomial

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \tag{$\dagger$}$$

with a_{n-j} in I^j.

(a) Show that u is integral over I iff $(I + (u))^n = I(I + (u))^{n-1}$.
(b) Show that u is integral over I iff there is a f.g. A-module M such that $uM \subseteq IM$, and whenever $aM = 0$ then au is nilpotent.

Solution

(a) Suppose u is integral over I. Since $I \subseteq I + (u)$ we always have the containment

$$I(I + (u))^{n-1} \subseteq (I + (u))(I + (u))^{n-1} = (I + (u))^n.$$

To show containment in the other direction, let $x \in (I + (u))^n$. Then x is of the form

$$x = (b_1 + r_1 u)(b_2 + r_2 u) \cdots (b_n + r_n u)$$

where $b_i \in I$ and $r_i \in A$ for all i. If we expand this product, we have one term of the form ru^n where $r = r_1 r_1 \cdots r_n \in A$ and the remaining terms are all of the form $b_j u^i$ where $b_j \in I^j$ and $i + j = n$. Terms of this latter form are in the ideal $I(I + (u))^{n-1}$ since $b_j \in I^j \subseteq I(I + (u))^{j-1}$ and $u^i \in (I + (u))^i$ so we have

$$b_j u^i \subseteq I(I + (u))^{j-1}(I + (u))^i = I(I + (u))^{i+j-1} = I(I + (u))^{n-1}.$$

Since ideals are closed under finite sums, to show $x \in I(I + (u))^{n-1}$ it remains only to show that $ru^n \in I(I + (u))^{n-1}$. Indeed, since ideals are closed under left multiplication by elements from the ring, it suffices to show that $u^n \in I(I + (u))^{n-1}$. Since u is integral over I, we have a dependence relation

$$u^n + a_{n-1}u^{n-1} + \cdots + a_1 u + a_0 = 0$$

where $a_{n-j} \in I^j$. Then we have

$$u^n = -a_{n-1}u^{n-1} - a_{n-2}u^{n-2} \cdots - a_1 u - a_0.$$

Each term on the right is clearly in $I(I + (u))^{n-1}$ by the fact that $a_{n-j} \in I^j$ so their sum u^n must also be in $I(I + (u))^{n-1}$. Then $x \in I(I + (u))^{n-1}$ and we have that $(I + (u))^n \subseteq I(I + (u))^{n-1}$ and hence $(I + (u))^n \subseteq I(I + (u))^{n-1}$ as required.

To show the converse implication, suppose $(I+(u))^n = I(I+(u))^{n-1}$. Then since $u^n \in (I+(u))^n$ we must have $u^n \in I(I+(u))^{n-1}$. In other words

$$u^n = c_0(c_1 + r_1 u)(c_2 + r_2 u) \cdots (c_{n-1} - r_{n-1} u)$$

where $r_i \in A$ and $c_i \in I$ for all I. When we expand the RHS each term will be of the form $b_j u^i$ where $b_j \in I^{j+1}$ and $i + j = n-1$. Then by collecting like powers of u we have that the coefficient of u^i is a sum of elements of I^{j+1}, hence lies in I^{j+1}. Then we have

$$u^n = a'_0 + a'_1 u + a'_2 u^2 + \cdots + a'_{n-1} u^{n-1}$$

where $a'_j \in I^{j+1}$. Alternatively,

$$u^n - a'_{n-1} u^{n-1} - a'_{n-2} u^{n-2} - \cdots - a'_1 u - a_0 = 0.$$

Set $a_i = -a'_i \in I^{j+1} = I^{n-i}$ since $i + j = n - 1$. Then we have

$$u^n + a_{n-1} u^{n-1} + \cdots + a_1 u + a_0$$

where $a_i \in I^{n-i}$. Then u satisfies the polynomial

$$x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

where $a_i \in I^{n-i}$, and therefore u is integral over I. This completes the proof. □

(b) Suppose that $u \in A$ is integral over I. Then u satisfies the following dependence relation,

$$u^n + a_{n-1} u^{n-1} + \cdots + a_1 u + a_0 = 0$$

where $a_{n-j} \in I^j$. Then there exist $s_{jk} \in I$ such that $a_{n-j} = \prod_{k=1}^{j} s_{jk}$. Let G_j be the set $\{s_{jk} : 1 \le k \le j\}$ and $G = \bigcup_{j=1}^{n} G_j$. Let $J =< G >$ be the ideal generated by G. Then J is finitely generated, and u is integral over J as we have ensured that $a_{n-j} \in J^j$.

Let $M = (J + (u))^{n-1}$. Then $uM \subseteq (J+(u))^n = JM$ as $u \in (J + (u))$ and u is integral over J. $J \subseteq I$ implies that $JM \subseteq IM$, hence $uM \subseteq IM$. Now suppose that $aM = 0$. As $u \in (J+(u))$, we then have that a annihilates u^{n-1}. Then $0 = au^{n-1} = a^{n-1}u^{n-1} = (au)^{n-1}$, hence au is nilpotent.

Now suppose that there is a f.g. A-module M such that $uM \subseteq IM$, and whenever $aM = 0$ then au is nilpotent. Let $v_1, v_2, \ldots, v_k$ be a generating set for M. Then since $uM \subseteq IM$ we have in particular $uv_1, uv_2, \ldots, uv_k \in IM$. Then for all $1 \le i \le k$ we have $uv_i = a_i v'_i$ for some $a_i \in I$ and some $v'_i \in M$. Expanding each v'_i in terms of the generators gives the system of equations

$$\begin{aligned}
uv_1 &= a_1(r_{11}v_1 + r_{12}v_2 + \cdots + r_{1k}v_k) \\
uv_2 &= a_2(r_{21}v_1 + r_{22}v_2 + \cdots + r_{2k}v_k) \\
&\vdots \\
uv_k &= a_k(r_{k1}v_1 + r_{k2}v_2 + \cdots + r_{kk}v_k)
\end{aligned}$$

where $r_{ij} \in A$ for all $1 \le i, j \le k$. Let v be the column vector $v = [v_1\ v_2\ \cdots\ v_k]^T$. Then in matrix form we can express this system as $(u\mathbf{1})v = Bv$ where $\mathbf{1}$ is the identity matrix in $M_k(A)$ and $B \in M_k(A)$ is the matrix with entry $b_{ij} = a_i r_{ij} \in I$ in the ith row, jth column. Equivalently, we have

$$(\star) \qquad (u\mathbf{1} - B)v = 0$$

By the Caley-Hamilton Theorem, the $k \times k$ matrix $C = u\mathbf{1} - B$ must satisfy its own characteristic polynomial, which we will denote by

$$p_C(x) = d_0 + d_1 x + \cdots + d_k x^k.$$

Then we have

$$d_0\mathbf{1} + d_1C + d_2C^2 + \cdots + d_kC^k = 0$$

or equivalently

$$C[d_1 + d_2C + \cdots + d_kC^{k-1}] = d_0\mathbf{1}.$$

We now observe that $d_0 = \pm\det(C)$ and choose either D or $-D$ to be the matrix $d_1 + d_2C + \cdots + d_kC^{k-1}$ so that $DC = \det(C)\mathbf{1}$. Then multiplying both sides of $(\star)$ by D gives

$$\det(u\mathbf{1} - B)\mathbf{1}v = 0$$

so the element $a = \det(u\mathbf{1} - B) \in A$ annihilates each v_i and hence annihilates M. Then by our hypothesis, au is nilpotent. Then $a^\ell u^\ell = (au)^\ell = 0$ for some ℓ. Let

$$p_B(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{k-1}x^{k-1} + x^k$$

be the characteristic polynomial for B. Note that since all the entries of B are in I, p_B satisfies $c_i \in I^{k-i}$. We also have that $a = \det(u\mathbf{1} - B) = p_B(u)$.

Now we note that given two monic polynomials in x, both of which have the property that the coefficient of x_i is contained the ideal I^{d-i} where d is the degree of the polynomial whence the coefficient came, then the product of these two polynomials will also have this property. This is easily extended to finite products. Hence, since $p_B(x)$ and x^ℓ are both polynomials with this property, we have that $q(x) = x^\ell[p_B(x)]^\ell$ is also a polynomial with this property. Finally, $q(u) = u^\ell[p_B(u)]^\ell = u^\ell a^\ell = 0$, and therefore u is integral over I. The result follows. $\square$