18.705 Commutative Algebra
Lecture 1

Andrew V. Sutherland
Adapted from the 2018 lecture notes of Jack Jeffries (§1.1-1.4)

September 10, 2026

A motivating question

Let G be a group acting on a (commutative, unital) ring R.

Definition

The invariant ring of the action of G on R is the subring

$$R^G := \{r \in R : g(r) = r \text{ for all } g \in G\}.$$

R^G is a subring of R because each $g \in G$ is a ring homomorphism.
If $G = \langle g_1, \ldots, g_m \rangle$ then $r \in R^G$ if and only if $g_i(r) = r$ for $1 \leq i \leq m$.

Question

Let $R = K[x_1, \ldots, x_n]$ with K a field. Is there a finite set $\{f_1, \ldots, f_k\} \subset R^G$ such that every $f \in R^G$ is a polynomial in $f_1, \ldots, f_k$ with coefficients in K?

We will give a precise answer to this question (yes for finite G, no in general).

Example: the symmetric group

Let the symmetric group S_n act on $R = K[x_1, \ldots, x_n]$ via $\sigma(x_i) = x_{\sigma(i)}$.

For $n = 3$ the polynomial $f = x_1^2 + x_2^2 + x_3^2$ is invariant,
but the polynomial $g = x_1^2 + x_1x_2 + x_2^2 + x_3^2$ is not.

Theorem (Fundamental theorem of symmetric polynomials)

$R^{S_n} = K[e_1, \ldots, e_n]$, *where* $e_1, \ldots, e_n$ *are the elementary symmetric polynomials* $e_i := \sum_{|I|=i} \prod_{j \in I} x_j$ *(the sum is over subsets* $I \subseteq \{1, \ldots, n\}$*).*

So every symmetric polynomial is a polynomial in $e_1, \ldots, e_n$; e.g., $f = e_1^2 - 2e_2$.

In fact the e_i are algebraically independent, so R^{S_n} is a polynomial ring in n variables.
We will see that this is very much the exception rather than the rule.

Example: roots of unity

Let K be a field containing a primitive dth root of unity ζ_d,
and let $G = \langle g \rangle$ be cyclic of order d acting on $R = K[x_1, \ldots, x_n]$ via $g(x_i) = \zeta_d x_i$.

Write $f \in R$ as a sum $f = f_0 + \cdots + f_r$ of homogeneous pieces, with f_i of degree i.
Then $g(f_i) = \zeta_d^i f_i$, so $g(f) = f$ if and only if $f_i = 0$ whenever $d \nmid i$. Thus

$$R^G = \{f \in R : \text{every term of } f \text{ has degree divisible by } d\},$$

the dth Veronese ring. For $d = 2$ (so $\operatorname{char} K \neq 2$) this is the ring of even polynomials.

R^G is generated as a K-algebra by the **finite** set of monomials of degree d,
since each monomial of degree ℓd is a product of ℓ monomials of degree d (check!).

For $n = d = 2$, $R^G = K[x^2, xy, y^2] \simeq K[u, v, w]/(uw - v^2)$ is not a polynomial ring.

Example: a finite subgroup of $\mathrm{GL}_2(\mathbb{C})$

Let $R = \mathbb{C}[x, y]$ and let $G = \langle A, B \rangle \leq \mathrm{GL}_2(\mathbb{C})$ act on R via its action on $\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right]$, where $A = \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Then G is the quaternion group Q_8.

Some invariants: $x^2y^2,\ x^4 + y^4,\ xy(x^4 - y^4),\ x^4y^4,\ x^2y^2(x^4 + y^4),\ \ldots$

On the basis $1, x, y, x^2, xy, y^2$ of $\mathbb{C}[x, y]_{\leq 2}$ the matrix of A is $\mathrm{diag}(1, i, -i, -1, 1, -1)$, so A fixes only the span of 1 and xy, and $B(xy) = -xy$; no invariants of degree 1,2.

One can similarly find all invariants of degree $\leq d$ for any fixed d, but the problem grows with d and it cannot tell us whether finitely many invariants generate R^G.

Infinite groups: $\mathrm{SL}_2(\mathbb{C})$ acts on a 2×3 matrix X of indeterminates via $X \mapsto gX$. Since $\det g = 1$ its 2×2 minors are invariant, and in fact they generate $\mathbb{C}[X]^{\mathrm{SL}_2(\mathbb{C})}$.

Finitely generated algebras

Definition

An A-algebra is a ring R with a ring homomorphism $\varphi\colon A \to R$. A subset $\Lambda \subseteq R$ generates R as an A-algebra if the only subring of R containing $\varphi(A) \cup \Lambda$ is R itself.

Equivalently, every $r \in R$ is a polynomial in elements of Λ with coefficients in $\varphi(A)$; equivalently, the homomorphism $A[x_\lambda : \lambda \in \Lambda] \to R$ sending $x_\lambda \mapsto \lambda$ is surjective.

Definition

$\varphi\colon A \to R$ is algebra-finite (R is a finitely generated A-algebra, or of finite type) if R is generated as an A-algebra by finitely many $f_1, \ldots, f_k \in R$.
We may then write $R = A[f_1, \ldots, f_k]$ (there may be relations among the f_i).

Thus R is finitely generated over A if and only if $R \simeq A[x_1, \ldots, x_k]/I$ for some k.

Since $\varphi = (A \twoheadrightarrow \varphi(A) \hookrightarrow R)$ and surjections are trivially algebra-finite, it suffices to consider inclusions $A \subseteq R$, equivalently, ring extensions R/A.

Algebra-finiteness

Our question: for $R = K[x_1, \ldots, x_n]$ with a G-action, is $K \subseteq R^G$ algebra-finite?

- Yes for S_n (generated by the e_i) and Veronese rings (by degree-d monomials).

Non-example: $\mathbb{Z} \subseteq \mathbb{Q}$ is not algebra-finite: $\mathbb{Z}[a_1/b_1, \ldots, a_k/b_k] \subseteq \mathbb{Z}[1/(b_1 \cdots b_k)] \neq \mathbb{Q}$.

Let $A \subseteq B \subseteq C$ be rings. It follows from the definitions that

- $A \subseteq B$ and $B \subseteq C$ algebra-finite $\Rightarrow A \subseteq C$ algebra-finite;
- $A \subseteq C$ algebra-finite $\Rightarrow B \subseteq C$ algebra-finite;
- but $A \subseteq C$ algebra-finite $\not\Rightarrow A \subseteq B$ algebra-finite.

Example

Let $K \subseteq B := K[x, xy, xy^2, \ldots] \subseteq C := K[x, y]$. A finitely generated K-subalgebra of B lies in $K[x, xy, \ldots, xy^m]$ for some m, whose monomials have y-exponent at most m times their x-exponent, so it does not contain xy^{m+1}.
Thus B is not a finitely generated K-algebra, but C obviously is.

Finitely generated modules

Via $\varphi\colon A \to R$, the ring R is an A-module with $a \cdot r := \varphi(a)r$ (restriction of scalars).

Recall that $\Gamma \subseteq M$ generates M if no proper submodule of M contains Γ.
Equivalently, every $m \in M$ is an A-linear combination $\sum_i a_i\gamma_i$ of elements $\gamma_i \in \Gamma$;
equivalently, the map $A^{\oplus\Gamma} \to M$ that sends the basis vector $e_\gamma \mapsto \gamma$ is surjective.

We write $M = \sum_{\gamma\in\Gamma} A\gamma$ to indicate that Γ generates M.

Definition

$\varphi\colon A \to R$ is module-finite (often just finite) if R is a finitely generated A-module.

Module-finite $\Rightarrow$ algebra-finite, since linear combinations are polynomial expressions.
The converse is far from true.

As before, surjections are module-finite, so it suffices to consider inclusions $A \subseteq R$.

Module-finiteness

Examples:

- For fields $K \subseteq L$, module-finite means $[L : K] < \infty$.
- $\mathbb{Z} \subseteq \mathbb{Z}[i]$ is module-finite: $\mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i$, and $\{1, i\}$ is a basis, so $\mathbb{Z}[i]$ is free.
- $R \subseteq R[x]$ is algebra-finite but not module-finite: $R[x]$ is free with basis $1, x, x^2, \ldots$
- $K[x] \subseteq K[x, 1/x]$ is not module-finite: every element has the form $f(x)/x^n$, so any finitely generated $K[x]$-submodule lies in some $x^{-N}K[x] \neq K[x, 1/x]$.

Lemma

Suppose $R \subseteq S$ is module-finite.
If N is finitely generated as an S-module then N is finitely generated as an R-module.
In particular, a composition of module-finite maps is module-finite.

Proof: If $S = \sum_{i=1}^{r} Ra_i$ and $N = \sum_{j=1}^{s} Sb_j$ then $N = \sum_{i,j} Ra_ib_j$.

Integral elements

Definition

Let $\varphi\colon A \to R$ be a ring homomorphism. An element $r \in R$ is integral over A if

$$r^n + \varphi(a_{n-1})r^{n-1} + \cdots + \varphi(a_1)r + \varphi(a_0) = 0$$

for some $a_0, \ldots, a_{n-1} \in A$. We say R is integral over A if every $r \in R$ is.

Integral $\Rightarrow$ algebraic, but not conversely ($1/2 \in \mathbb{Q}$ is algebraic over $\mathbb{Z}$ but not integral).

As before, integrality depends only on $\varphi(A) \subseteq R$, so we may assume $A \subseteq R$.

In field theory, finite extensions and algebraic elements are closely related.
The next two results show that the situation for rings is similar,
with "finite" replaced by "module-finite" and "algebraic" by "integral".

Integral implies module-finite

Proposition

Let $A \subseteq R$ be rings.

1. *If $r \in R$ is integral over A then $A[r]$ is module-finite over A.*
2. *If $r_1, \ldots, r_k \in R$ are integral over A then $A[r_1, \ldots, r_k]$ is module-finite over A.*

Proof: (1) $A[r] = \sum_{i<n} Ar^i$, since $r^m = -r^{m-n}(a_{n-1}r^{n-1} + \cdots + a_0)$ for $m \geq n$.
(2) $A \subseteq A[r_1] \subseteq \cdots \subseteq A[r_1, \ldots, r_k]$ is a composition of module-finite maps, since each r_i is integral over $A[r_1, \ldots, r_{i-1}]$ (via the same monic equation).

This is the origin of the term "ring": the powers of r wrap around.

Module-finite implies integral

Lemma (Determinant trick)

Let R be a ring and $B \in \mathrm{M}_n(R)$. Then $\mathrm{adj}(B)B = \det(B)I_n$,
where $\mathrm{adj}(B)_{ij} := (-1)^{i+j}\det(\widehat{B}_{ji})$ and $\widehat{B}_{ji}$ is B with row j and column i deleted.

It is a polynomial identity in the b_{ij}, so it suffices to check it in $\mathbb{Z}[b_{11}, \ldots, b_{nn}]$; this is a domain, so we may work in its fraction field, where it is linear algebra.

Theorem

If $A \subseteq R$ is module-finite then R is integral over A.

Proof: To the blackboard!

On the blackboard: module-finite implies integral

Theorem. If $A \subseteq R$ is module-finite then R is integral over A.

Proof. Write $R = \sum_{i=1}^{k} A r_i$ and fix $r \in R$. For each i we have $r r_i \in R$, so we can write

$$r r_i = \sum_{j=1}^{k} a_{ij} r_j \qquad (a_{ij} \in A).$$

Let $C = (a_{ij}) \in) A^{k \times k}$, let $I = 1_{A^{k \times k}}$, and let $v = (r_1, \dots, r_k)^{\mathsf{T}} \in R^k$. We have $(rI - C)\, v = 0$.

Multiplying on the left by $\operatorname{adj}(rI_k - C)$ and applying the determinant trick gives $\det(rI - C)\, v = 0$. Considering the first entry $r_1 = 1$ of v gives $\det(rI - C) = 0$.

Now $f(t) := \det(tI - C) \in A[t]$ is monic of degree k (the only term of degree k in t comes from the diagonal), and $f(r) = \det(rI - C) = 0$ shows that r is integral over A. □

Remark. This is the Cayley–Hamilton theorem for the"multiplication by r" map on the A-module R.

Presented on the blackboard; not part of the projected slides.

Module-finite = integral + algebra-finite

Corollary

R is module-finite over $A \iff R$ is integral and algebra-finite over A.

Proof: ($\Rightarrow$) module generators are algebra generators, and apply the theorem.
($\Leftarrow$) apply the proposition to $R = A[r_1, \ldots, r_k]$ with each r_i integral.

Corollary

If $R = A[\Lambda]$ with every $\lambda \in \Lambda$ integral over A, then R is integral over A.

Proof: Each $r \in R$ lies in $A[L]$ for some finite $L \subseteq \Lambda$, which is integral.

Definition

The integral closure of A in R is the set of elements of R that are integral over A.
It is a subring of R (apply the corollary with Λ the set of integral elements).

Examples and non-examples of module-finite ring extensions

Some examples

1. $\mathbb{C}[x,y] \subseteq \mathbb{C}[x,y,z]/(x^2+y^2+z^2)$ is module-finite, since z is integral.

2. $\mathbb{C}[u,v] \subseteq S := \mathbb{C}[u,v,w]/(u^2+vw)$ is not integral, hence not module-finite: in $\mathrm{Frac}(S) = \mathbb{C}(u,v)$ we have $w = -u^2/v \notin \mathbb{C}[u,v]$, but every element of $\mathbb{C}(u,v)$ that is integral over the UFD $\mathbb{C}[u,v]$ lies in $\mathbb{C}[u,v]$ (rational root theorem). (This S is isomorphic to the previous one, but $\mathbb{C}[u,v]$ maps to $\mathbb{C}[x,y+iz]$.)

3. $K[x] \subseteq K[x, x^{1/2}, x^{1/3}, \ldots] \subseteq \overline{K(x)}$ is integral (generated by integral elements) but not algebra-finite (prove it!), hence not module-finite.

As with algebra-finiteness, module-finiteness is transitive, and $A \subseteq C$ module-finite implies $B \subseteq C$ module-finite for $A \subseteq B \subseteq C$, but not $A \subseteq B$ module-finite.

Invariant rings are module-finite extensions

Proposition

Let K be a field, R a finitely generated K-algebra, and G a finite group of automorphisms of R that fix K. Then $R^G \subseteq R$ is module-finite.

Proof: It suffices to show that R is algebra-finite and integral over R^G.
Algebra-finite: since $K \subseteq R^G$, generators of R over K are generators of R over R^G.
Integral: for $r \in R$, each $g \in G$ permutes the factors of $F_r(t) := \prod_{h \in G}(t - h(r))$, so $F_r \in R^G[t]$; it is monic of degree $|G|$ and $F_r(r) = 0$.

We now have $K \subseteq R^G \subseteq R$ with $K \subseteq R$ algebra-finite and $R^G \subseteq R$ module-finite.
We want $K \subseteq R^G$ to be algebra-finite, but nothing we have shown so far implies this:
$A \subseteq C$ algebra-finite and $B \subseteq C$ module-finite $\not\Rightarrow A \subseteq B$ algebra-finite in general.

We need one more finiteness condition (on A)...

Noetherian rings

Definition

A ring R is Noetherian if every ascending chain of ideals $I_1 \subseteq I_2 \subseteq \cdots$ eventually stabilizes: there exists N such that $I_n = I_{n+1}$ for all $n \geq N$.

Proposition

The following are equivalent for a ring R:

1. *R is Noetherian;*
2. *every nonempty set of ideals of R has a maximal element (under inclusion);*
3. *every ascending chain of finitely generated ideals of R eventually stabilizes;*
4. *every generating set of an ideal I of R contains a finite generating set for I;*
5. *every ideal of R is finitely generated.*

Proof: On blackboard: $(1) \Leftrightarrow (2)$ and $(1) \Rightarrow (3) \Rightarrow (4) \Rightarrow (5) \Rightarrow (1)$.

On the blackboard: characterizations of Noetherian rings

Proposition. The following are equivalent: (1) R is Noetherian; (2) every nonempty set of ideals has a maximal element; (3) every ascending chain of finitely generated ideals eventually stabilizes; (4) every generating set of an ideal I contains a finite generating set for I; (5) every ideal is finitely generated.

Proof. (1) $\Rightarrow$ (2): Suppose a nonempty set $\mathcal{S}$ of ideals has no maximal element. Pick $I_1 \in \mathcal{S}$; since I_1 is not maximal in $\mathcal{S}$ there is $I_2 \in \mathcal{S}$ with $I_1 \subsetneq I_2$; since I_2 is not maximal there is $I_3 \in \mathcal{S}$ with $I_2 \subsetneq I_3$; and so on. This gives a strictly ascending chain of ideals, contradicting (1).

(2) $\Rightarrow$ (1): Given $I_1 \subseteq I_2 \subseteq \cdots$, the set $\{I_n\}$ has a maximal element I_N, and $I_n = I_N$ for all $n \geq N$.

(1) $\Rightarrow$ (3): Trivial, since finitely generated ideals are ideals.

(3) $\Rightarrow$ (4): Let $I = (\Lambda)$ and suppose no finite subset of Λ generates I. Then for every finite $L \subseteq \Lambda$ we have $(L) \subsetneq I$, so some $\lambda \in \Lambda$ does not lie in (L) (otherwise $\Lambda \subseteq (L)$ and $I = (L)$). Starting from $L_0 = \emptyset$ and repeatedly adjoining such a λ yields a strictly ascending chain $(L_0) \subsetneq (L_1) \subsetneq (L_2) \subsetneq \cdots$ of finitely generated ideals, contradicting (3).

(4) $\Rightarrow$ (5): Every ideal I is generated by $\Lambda = I$, and by (4) some finite subset of I generates I.

(5) $\Rightarrow$ (1): Given $I_1 \subseteq I_2 \subseteq \cdots$, the union $I = \bigcup_n I_n$ is an ideal (any two of its elements lie in a common I_n), so $I = (a_1, \ldots, a_m)$ by (5). Each a_j lies in some I_{n_j}; with $N = \max_j n_j$ we get $I \subseteq I_N \subseteq I_n \subseteq I$ for all $n \geq N$, so the chain stabilizes. $\square$

Presented on the blackboard; not part of the projected slides.

Examples and non-examples of Noetherian rings

Noetherian rings:

- Any field K (its only ideals are (0) and (1)).
- Any PID, such as $\mathbb{Z}$, $K[x]$, or $\mathbb{C}\{z\} := \{f \in \mathbb{C}[[z]] : f \text{ converges near } 0\}$. Every ideal of $\mathbb{C}\{z\}$ is (z^n) for some n: every nonzero $f \in \mathbb{C}\{z\}$ is $z^n g(z)$ with $g(0) \neq 0$, and any such g is a unit in $\mathbb{C}\{z\}$.

Non-Noetherian rings:

- $K[x_1, x_2, \ldots]$: the chain $(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \cdots$ does not stabilize.
- $K[x, x^{1/2}, x^{1/3}, \ldots]$: the chain $(x) \subsetneq (x^{1/2}) \subsetneq (x^{1/3}) \subsetneq \cdots$ does not stabilize. Similarly for the ring $\bigcup_{n \geq 1} \mathbb{C}[[z^{1/n}]]$ of Puiseux series with nonnegative exponents.
- $\mathcal{C}(\mathbb{R}, \mathbb{R})$, the ring of continuous functions on $\mathbb{R}$: the ideals $I_n := \{f : f|_{[-1/n, 1/n]} \equiv 0\}$ form a strictly ascending chain. Same for $\mathcal{C}^\infty(\mathbb{R}, \mathbb{R})$, but not for analytic functions, where every I_n is (0).

Noetherian modules

Definition

An R-module M is Noetherian if every ascending chain of submodules of M stabilizes.

The analogues of (1)–(5) for modules are equivalent (same proof);
in particular, Noetherian modules are finitely generated.
R is a Noetherian ring if and only if R is a Noetherian R-module,
in which case so is R/I (its ideals correspond to ideals of R containing I).

Lemma

Let $N \subseteq M$ be a submodule. Then M is Noetherian if and only if N and M/N are.

Proposition

If R is Noetherian, an R-module is Noetherian if and only if it is finitely generated.
In particular, every submodule of a finitely generated R-module is finitely generated.

The Hilbert Basis Theorem

Theorem (Hilbert Basis Theorem)

If A is a Noetherian ring then so are $A[x_1, \ldots, x_n]$ and $A[[x_1, \ldots, x_n]]$.

Proof: To the blackboard! (if time, or see notes).

Corollary

Every finitely generated algebra over a Noetherian ring is Noetherian.
In particular, every finitely generated algebra over a field is Noetherian.

Similarly, every module-finite extension R of a Noetherian ring A is Noetherian (an ascending chain of ideals of R is a chain of A-submodules of R).

The converse of the corollary is false: $\mathbb{C}\{z\}$ and $\mathbb{C}[[z]]$ are Noetherian but not algebra-finite over $\mathbb{C}$: their $\mathbb{C}$-dimension is uncountable, unlike that of $\mathbb{C}[x_1, \ldots, x_n]/I$.

On the blackboard: proof of the Hilbert Basis Theorem

Theorem. If A is a Noetherian ring then so are $A[x_1, \ldots, x_n]$ and $A[[x_1, \ldots, x_n]]$.

Proof. Since $A[x_1, \ldots, x_n] = A[x_1, \ldots, x_{n-1}][x_n]$ (and likewise for power series), by induction on n it suffices to show that $A[x]$ is Noetherian, i.e., that every ideal $I \subseteq A[x]$ is finitely generated.

Let $J \subseteq A$ be the set of leading coefficients of elements of I and 0. This is an ideal of A. Since A is Noetherian, $J = (a_1, \ldots, a_m)$. Choose $f_i \in I$ with leading coefficient a_i and put $N := \max_i d_i$.

If $f \in I$ has degree $e \geq N$ and leading coefficient $a = \sum_i c_i a_i$ (with $c_i \in A$), then $f - \sum_i c_i x^{e-d_i} f_i \in I$ has degree $< e$. Repeating this, every $f \in I$ can be written as $f = g + h$ with $h \in (f_1, \ldots, f_m)$ and $g \in I \cap M$, where $M := \sum_{j<N} Ax^j$.

Now M is a finitely generated A-module and A is Noetherian, so the A-submodule $I \cap M$ is finitely generated, say by $g_1, \ldots, g_s$. Therefore $I = (g_1, \ldots, g_s, f_1, \ldots, f_m)$ is finitely generated. $\square$

The proof for $A[[x]]$ is similar.

Presented on the blackboard; not part of the projected slides.

The Artin–Tate lemma and Noether's finiteness theorem

Theorem (Artin–Tate lemma)

Let $A \subseteq B \subseteq C$ be rings with A Noetherian, C module-finite over B, and C algebra-finite over A. Then B is algebra-finite over A.

Proof: To the blackboard! (if time, or see notes).

Theorem (Noether)

Let K be a field, R a finitely generated K-algebra, and G a finite group of automorphisms of R that fix K. Then R^G is a finitely generated K-algebra.

Proof: Apply Artin–Tate to $K \subseteq R^G \subseteq R$: K is Noetherian, $K \subseteq R$ is algebra-finite by hypothesis, and $R^G \subseteq R$ is module-finite by the proposition on invariant rings.

This answers our motivating question for finite G.
(For infinite G the answer can be no: Nagata's counterexample to Hilbert's 14th.)

On the blackboard: proof of the Artin–Tate lemma

Theorem (Artin–Tate lemma). Let $A \subseteq B \subseteq C$ be rings with A Noetherian, C module-finite over B, and C algebra-finite over A. Then B is algebra-finite over A.

Proof. Write $C = A[f_1, \dots, f_r]$ and $C = \sum_{i=1}^{s} B g_i$, and assume wlog that $g_1 = 1$. Since each f_i and each product $g_i g_j$ lies in C, there are elements $b_{ij}, b_{ijk} \in B$ such that

$$f_i = \sum_{j=1}^{s} b_{ij} g_j \qquad \text{and} \qquad g_i g_j = \sum_{k=1}^{s} b_{ijk} g_k.$$

Let $B_0 := A[\{b_{ij}\} \cup \{b_{ijk}\}] \subseteq B$. Then B_0 is a finitely generated A-algebra, hence Noetherian by the corollary to the Hilbert Basis Theorem.

Claim: $C = \sum_{i=1}^{s} B_0 g_i$. Every $c \in C$ is a polynomial in the f_i with coefficients in A, hence (substituting $f_i = \sum_j b_{ij} g_j$) a polynomial in the g_j with coefficients in B_0. Using $g_i g_j = \sum_k b_{ijk} g_k$ repeatedly, every monomial in the g_j of degree ≥ 2 reduces to a B_0-linear combination of $g_1, \dots, g_s$, and monomials of degree ≤ 1 are already of this form because $g_1 = 1$. This proves the claim.

So C is a finitely generated module over the Noetherian ring B_0, and therefore its B_0-submodule B is also finitely generated, say $B = \sum_{l=1}^{m} B_0 c_l$. In particular $B = B_0[c_1, \dots, c_m]$ is algebra-finite over B_0, and B_0 is algebra-finite over A by construction, so B is algebra-finite over A by transitivity. □

Presented on the blackboard; not part of the projected slides.