THE HILBERT BASIS THEOREM

Here is some terminology (which is standard in EGA but less standard in popular commutative algebra books). Let A be a ring (as always, commutative with multiplicative identity) and fix an A-algebra B. Note that there is an obvious A-module structure on B.

We say B is *finite* over A if the A-algebra B is finitely generated as an A-module. In other words there is a surjective map of A-modules

$$A^m \twoheadrightarrow B.$$

Here, as always, the two headed right arrow " $\twoheadrightarrow$ " denotes a surjective map. A^m is the direct sum of m-copies of A.

We say that B is a *finite type* algebra over A if B is finitely generated as an A-algebra, i.e. B is finite type over A if the natural map $A \to B$ giving B its A-algebra structure is a composite of ring homomorphisms of the form

$$A \xrightarrow{\text{natural}} A[X_1, \dots, A_n] \twoheadrightarrow B.$$

In other words, we have elements $b_1, \dots, b_n$ in B such that every element of B can be written as a polynomial of the form $\sum_{\boldsymbol{\nu}} a_{\boldsymbol{\nu}} b_1^{\nu_1} \dots b_n^{\nu_n}$, with $\boldsymbol{\nu} = (\nu_1, \dots, \nu_n)$ varying in n-tuples of non-negative integers, $a_{\boldsymbol{\nu}}$ varying in A and such that all but a finite number of the $a_{\boldsymbol{\nu}}$ are zero.

It is clear that if B is finite over A, then it is of finite type over A.

1. Noetherian rings and modules

Our conventions are the usual commutative algebra conventions. For example, modules M over a ring A satisfy $1 \cdot m = m$ for all $m \in M$. Note that ideals are the same as A-submodules of A, with A regarded as an A-module in an obvious way.

Recall that a ring A is called Noetherian is if it satisfies any of the following conditions:

(a) Every ideal of A is finitely generated.
(b) Every ascending chain of ideals

$$I_1 \subset I_2 \subset \dots \subset I_n \subset \dots$$

stabilises, i.e. there is an n such that $I_n = I_{n+m}$ for all $m \geq 0$.
(c) Every nonempty set of ideals of A contains a maximal element with respect to inclusion.

See [Ku, pp.10–11, Prop. 2.2] for a proof. Or simpler still, supply one yourself since the proofs are easy.

Recall that a module M over A is said to be Noetherian if it satisfies any of the following equivalent conditions:

(a) Every submodule of M is finitely generated.
(b) Every ascending chain of submodules of M

$$M_1 \subset M_2 \subset \dots \subset M_n \subset \dots$$

stabilises.

(c) Every nonempty set of submodules of M contains a maximal element with respect to inclusion.

The proof is *mutatis mutandis* the same as the proof of the case when $M = A$ above.

1.0.1. It is clear that the homomorphic image B of a Noetherian ring A is also Noetherian. Similarly if A is a ring and M a Noetherian A-module, then every quotient of M by a submodule is again Noetherian.

2. **The Hilbert basis theorem**

Actually there are two Hilbert basis theorems, one for rings and the other for modules.

2.1. **The theorem for rings.** Here is the statement for rings (see also [Ku, p.11, Prop. 2.3 and Cor. 2.4]) :

Theorem 2.1.1. (Hilbert Basis for Rings) *Let A be a Noetherian ring and B a finite type A-algebra. Then B is a Noetherian ring.*

Proof. Using 1.0.1 we see that it is enough to prove that every polynomial ring $A[X_1, \ldots, X_n]$ over A is Noetherian, and by induction, we are reduced to the case where $B = A[X]$, the polynomial ring in one variable over A. We will prove the contrapositive of the required statement, namely we will prove that if $A[X]$ is not Noetherian then A is not Noetherian.

So suppose $A[X]$ is not Noetherian. Let I be an ideal in $A[X]$ which is not finitely generated. Pick $f_1 \in I$ of lowest degree. Suppose we have picked elements $f_1, \ldots, f_n$ in I. Now pick an element f_{n+1} in $I \smallsetminus \langle f_1, \ldots, f_n \rangle$ of lowest degree. This gives us a sequence of elements $\{f_n\}$ in B. Let n_k be the degree of f_k. Note that the $n_k \leq n_{k+1}$ for all $k \geq 1$. Let $a_k \in A$ be the leading coefficient of f_k, i.e. a_k is the coefficient of X^{n_k} in f_k. We have a chain of ideals in A

$$(*) \qquad \langle a_1 \rangle \subset \langle a_1, a_2 \rangle \subset \ldots \langle a_1, \ldots, a_k \rangle \subset \ldots$$

We claim the chain never stabilises. Suppose $\langle a_1, \ldots, a_k \rangle = \langle a_1, \ldots, a_{k+1} \rangle$ for some $k \geq 1$. Then we have $\alpha_1, \ldots, \alpha_k \in A$ such that $a_{k+1} = \sum_{i=1}^{k} \alpha_i a_i$. Let

$$g = f_{k+1} - \sum_{i=1}^{k} \alpha_i X^{n_{k+1} - n_i} f_i.$$

Then $g \in I \smallsetminus \langle f_1, \ldots, f_k \rangle$ for $f_{k+1} = g + \sum_{i=1}^{k} \alpha_i X^{n_{k+1} - n_i} f_i$ and $f_{k+1} \notin \langle f_1, \ldots, f_k \rangle$. However the degree of g is strictly less than the degree of f_{k+1}, a contradiction. Thus the chain in $(*)$ does not stabilise, and hence A is not Noetherian. $\square$

2.2. **The theorem for modules.** The version for modules is as follows (see also [Ku, pp.14–15, Prop. 2.17]):

Theorem 2.2.1. (Hilbert Basis for Modules) *Let A be a Noetherian ring and M a finitely generated A-module. Then M is a Noetherian.*

Proof. Since M is finitely generated, we have a surjective map $A^n \twoheadrightarrow M$ of A-modules, where A^n is the direct sum of n-copies of A. By the remark in 1.0.1 we are reduced to the case $M = A^n$. The case $n = 1$ is trivially true by definition of a Noetherian ring. So assume $n > 1$ and A^{n-1} is Noetherian.

Suppose U is a submodule of A^n. We have to show that U is finitely generated. Let $\pi\colon A^n \to A$ be the map $(a_1, \ldots, a_n) \mapsto a_1$. The kernel of π can be identified with A^{n-1}. In greater detail, we have a short exact sequence of A-modules

$$0 \longrightarrow A^{n-1} \xrightarrow{\sigma} A^n \xrightarrow{\pi} A \longrightarrow 0$$

with the map $\sigma\colon A^{n-1} \to A^n$ being $(a_1, \ldots, a_{n-1}) \mapsto (0, a_1, \ldots, a_{n-1})$. Let $I = \pi(U)$. Then I is an ideal in A. Let K be the kernel of the map $\pi|_U$. We then have a commutative diagram with exact rows

$$\begin{array}{ccccccccc}
0 & \longrightarrow & K & \longrightarrow & U & \xrightarrow{\pi} & I & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A^{n-1} & \xrightarrow[\sigma]{} & A^n & \xrightarrow[\pi]{} & A & \longrightarrow & 0
\end{array}$$

The downward arrows in the middle and the right are the canonical inclusions and the downward arrow on the left is the induced map from K to A^{n-1}. The last mentioned map is also an injective map, for $K = U \cap \sigma(A^{n-1})$ and the arrow we are discussing is the composite $K \subset \sigma(A^{n-1}) \xrightarrow{\sigma^{-1}} A^{n-1}$. In other words K can be regarded as a submodule of A^{n-1}. By induction K is finitely generated. By the Hilbert basis theorem for rings, I is finitely generated. It follows, by looking at the exact sequence on the top row of our commutative diagram, that U is finitely generated. Indeed if $x_1, \ldots, x_d$ are generators of K, and $y_1, \ldots, y_m$ generators for I, and $u_1, \ldots u_m \in U$ elements such that $\pi(u_i) = y_i$ for $i = 1, \ldots, m$, then $x_1, \ldots, x_d, u_1, \ldots, u_m$ are generators of U. □

References

[Ku] E. Kunz *Introduction to Commutative Algebra and Algebraic Geometry*, Birkhaüser, Boston, Basel, Berlin, 1985.

[SP] The Stacks project authors, *TheStacks project*, https://stacks.math.columbia.edu, 2021.