Noetherian rings and modules

Proposition. *Let R be a ring and M an R-module. Then the following are equivalent:*

1. *Every submodule of M is finitely generated (fg).*
2. *M satisfies ACC (the* **ascending chain condition***), i.e., if $M_i \subseteq M$ are submodules and*

$$M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n \subseteq \cdots$$

then there exists a positive integer N such that $M_N = M_{N+i}$ for all $i \geq 0$. We say every ascending chain of submodules of M **stabilizes.** *(Equivalently, there exists no infinite chain*

$$M_1 < M_2 < \cdots < M_n < \cdots.)$$

3. *M satisfies the* **Maximum Principle***, i.e., if $S \neq \emptyset$ is a collection of submodules of M then S contains a maximal element, that is a module $M_o \in S$ such that if $M_o \subseteq N$ with $N \in S$ then $N = M_o$.*

An R-module M satisfying any (hence all) of these equivalent conditions is called a **noetherian R-module**.

Proof. 1) $\to$ 2): Let

$$\mathcal{C}: \quad M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n \subseteq \cdots$$

be a chain of submodules of M. Then $M' := \bigcup_{i=1}^{\infty} M_i \subseteq M$ is a submodule. By 1), it is finitely generated, so $M' = \sum_{i=1}^{n} Rx_i$ for some $x_i \in M'$. By definition, $x_i \in M_{j_i}$ some j_i. Let s be the maximum of the finitely many j_i's. Then $M' = M_s$. It follows that $M_s = M' = M_{s+i}$ for all $i \geq 0$.

2) $\to$ 3). Let $\emptyset \neq S$ be a collection of submodules of M. Let $M_1 \in S$. If M_1 is not maximal, there exists an $M_2 \in S$ with $M_1 < M_2$. Inductively, if M_i is not maximal, there exists an $M_{i+1} \in S$ with $M_i < M_{i+1}$. By ACC, the sequence

$$M_1 < M_2 < \cdots < M_i < \cdots$$

must terminate.

3) $\to$ 1). Let $N \subseteq M$ be a submodule. Let

$$S := \{M_i \mid M_i \subseteq N \text{ is a fg submodule }\}.$$

Then $(0) \in S$ so $S \neq \emptyset$. By assumption, there exists a maximal element $M' \in S$. If $N \neq M'$ then there exists $x \in N \setminus M'$. But M' fg means that $M' + Rx \subseteq N$ is also fg, so $M' + Rx \in S$. This contradicts the maximality of M'. Hence $N = M'$ is fg. $\square$.

Remark. Let $R = F[t_1, \dots, t_n, \dots]$ (infinitely many t_i). Let $M = R$ as an R-module. Then M is fg since cyclic but the ideal $(t_1, \dots t_n, \dots)$ is clearly not fg, so R is not a noetherian R-module. Thus, in general, submodules of fg modules need not be fg.

Definition. Let R be a commutative ring. We say that R is a **noetherian ring** if R is a noetherian R-module.

Remark. R is a noetherian ring if and only if every ideal of R is fg if and only if every ideal of R satisfy ACC.

Example. Every PID is noetherian.

We need another noetherian R-module result.

Proposition. *Let $N \subseteq M$ be R-modules. Then M is an R-noetherian if and only if N and M/N are R-noetherian. Thus if we have an exact sequence*

$$0 \to M' \to M \to M'' \to 0$$

of R-modules and if two of the modules M, M', M'' are R-noetherian then they all are.

Proof. $\to$: If $N_o \subseteq N$ is a submodule then $N_o \subseteq M$ is a submodule hence fg. Thus N is R-noetherian. By the Correspondence Principle, a (countable) chain of submodules in M/N has the form $M_1/N \subseteq M_2/N \subseteq \cdots$ where $N \subseteq M_1 \subseteq M_2 \subseteq \cdots$ is a chain of submodules of M. Thus there exists an r such that $M_r = M_{r+j}$ for all $j \geq 0$ and hence $M_r/N = M_{r+j}/N$ for all $j \geq 0$.

$\leftarrow$ is left as an exercise (cf., analogous solvable groups result). $\square$

Corollary. *If M, N are noetherian R-modules, so is $M \oplus N$.*

Proof. $(M \oplus N)/N \cong M$ and N are noetherian. $\square$

Theorem. *Let R be a noetherian ring. If M is a fg R-module then M is R-noetherian.*

Proof. Suppose $M = \sum_{i=1}^{n} Rx_i$. Let $\phi : R^n \to M$ be the R-epimorphism given by $e_i \mapsto x_i$, where $\{e_1, \cdots, e_n\}$ is the standard basis for R^n. Since R is R-noetherian so is R^n by the Corollary, and hence so is $M \cong R^n/\ker\phi$. $\square$

Proposition. *If $\phi : R \to S$ is a ring epimorphism and R is a noetherian ring then S is a noetherian ring.*

Proof. Let $\mathfrak{A} \subseteq S$ be an ideal. Then $\phi^{-1}(\mathfrak{A}) \subseteq R$ is an ideal hence fg. Thus $\mathfrak{A} = \phi(\phi^{-1}(\mathfrak{A}))$ is fg. $\square$

Hilbert Basis Theorem. *If R is a noetherian ring so is $R[t_1, \ldots, t_n]$.*

Proof. By induction on n, it suffices to show that $R[t]$ is noetherian whenever R is. Let $\mathfrak{A} \subseteq R[t]$ be an ideal. We must show that $\mathfrak{A}$ is fg. Let

$$I_n = \{r \in R \,|\, r = 0 \text{ or } r = \text{lead}(f),\ f \in \mathfrak{A},\ \deg f = n\}.$$

(Here lead(f) is the leading coefficient of f.) Clearly, $I_n \subseteq R$ is an ideal for all n. If $f \in \mathfrak{A}$ then $tf \in \mathfrak{A}$ and lead$(f) =$ lead(tf). Thus $I_n \subseteq I_{n+1}$ for all n. Since R is noetherian, there exists an n such that $I_n = I_{n+i}$ for all $i \geq 0$. Moreover, every I_j is fg. Let $I_j = (a_{1j}, \ldots, a_{m_j j})$ for $0 \leq j \leq n$ for some $1 \leq m_j < \infty$. By definition, there exist $f_{ij} \in \mathfrak{A}$ such that deg $f_{ij} = j$ and lead$(f_{ij}) = a_{ij}$. Note that $f_{io} = a_{io}$ for all i.

Claim. $\mathfrak{A} = \left\langle f_{ij} \,|\, 1 \leq i \leq m_j, \quad 0 \leq j \leq n \right\rangle$ and hence $\mathfrak{A}$ is fg.

Let $f \in \mathfrak{A}$, lead$(f) = a$, and deg $f = d$. So $f = at^d + \cdots$. If $d = 0$ then $f = a$ lies in $I_o = (f_{1o}, \ldots, f_{m_o o})$ and we are done. We proceed by induction on d.
Suppose that $d > 0$. If $d < n$, write $a = \sum_{i=1}^{m_d} r_i a_{id}$ some $r_i \in R$. Then $g = f - \sum_{i=1}^{m_d} r_i f_{id}$ lies in $\mathfrak{A}$ and deg $g < d$. By induction, $g \in \left\langle f_{ij} \,|\, 1 \leq i \leq m_j, \quad 0 \leq j \leq n \right\rangle$ and hence so does f. Thus we may assume that $d \geq n$. Since $I_d = I_n$, we have $a = \sum_{i=1}^{m_n} r_i a_{in}$ some $r_i \in R$.

Then $g = f - \sum_{i=1}^{m_n} r_i t^{d-n} f_{in}$ lies in $\mathfrak{A}$ and deg $g <$ deg $f = d$ and again we are done by induction on deg. $\square$

Remarks. 1. Noetherian domains need not be UFD's, since $\mathbf{Z}[\sqrt{-5}]$ is an example of such.
2. $F[t_1, \ldots, t_n, \ldots]$ is a UFD but is not noetherian.

Definition. Let $R \subseteq S$ be commutative rings. We say that S is a **fg (commutative) R-algebra** (or an **affine R-algebra** when R is a field) if there exist $x_1, \ldots, x_n \in S$ such that $S = R[x_1, \ldots x_n]$ as rings (not necessarily a polynomial ring).

Remark. $R[t]$ is a fg commutative R-algebra but definitely not a fg R-module. (Why?)

Corollary. *Let S be a fg commutative R-algebra. If R is noetherian so is S.*

Proof. Let $S = R[x_1, \ldots, x_n]$. Since $R[t_1, \ldots, t_n]$ is noetherian and we have a ring epimorphism $R[t_1, \ldots, t_n] \to R[x_1, \ldots, x_n]$ via $f(t_1, \ldots, t_n) \mapsto f(x_1, \ldots, x_n)$, all ideals of S are fg by the Correspondence Principle. $\square$

Remark. The proof (or definition) shows that S is a fg commutative R-algebra if and only if there exists and epimorphism $R[t_1, \ldots, t_n] \to R[x_1, \ldots, x_n]$ fixing R.

Lemma. (Artin-Tate) *Let $R \subseteq S \subseteq T$ be rings. Suppose that R is noetherian and T is a fg commutative R-algebra. Suppose that as a S-module T is fg. Then S is an affine R-algebra.*

Proof. Let $T = R[x_1, \ldots x_n]$ as an R-algebra for some $x_i \in T$. Let $T = \sum_{i=1}^{m} Sy_i$ as an S-module for some $y_i \in T$. Then

(i). $x_i = \sum_{j=1}^{m} a_{ij} y_j$ for some $a_{ij} \in S$ and

(ii). $y_i y_j = \sum_{k=1}^{m} b_{ijk} y_k$ for some $b_{ijk} \in S$ (since T is a ring).

Let $S_o = R[a_{ij}, b_{ijk} \,|\, i, j, k]$, a fg R-algebra. Then $R \subseteq S_o \subseteq S \subseteq T$.

Claim. T is a fg S_o-module.

Let $f \in T$ so $f = \sum c_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}$ for some $c_{i_1,\ldots,i_n} \in R$. Applying (i) and (ii) repeatedly shows that $f \in \sum_{i=1}^{m} S_o y_i$. Thus $T = S_o y_1 + \cdots + S_o y_m$ as claimed.

Since S_o is a fg R-algebra, it is noetherian by the Hilbert Basis Theorem. Thus T, being a fg S_o-module, is a noetherian S_o-module. Consequently, $S \subseteq T$ is a fg S_o-module. It follows immediately that S is a fg R-algebra. $\square$

Zariski's Lemma. *Let F be a field and E a ring containing F. Suppose that E is an affine F-algebra. If E is a field then E is a finite dimensional F-vector space (i.e., a fg F-module).*

Proof. Suppose that $E = F[x_1, \ldots, x_m]$. Recall that $F(x_1, \ldots, x_i)$ denotes the quotient field of $F[x_1, \ldots, x_i]$. Since E is a field, $E = F(x_1, \ldots, x_m)$. Suppose that E is not a finite dimensional F-vector space. By relabeling the x_i, we may assume that $F(x_1, \ldots, x_i)$ is not a finite dimensional $F(x_1, \ldots x_{i-1})$-vector space for $1 \leq i \leq r$, some r, and E is a finite dimensional $F(x_1, \ldots, x_r)$-vector space. (If $K \subseteq L \subseteq M$ are fields, it is easy to check (do so) that M is a finite dimensional K-vector space if and only if M is a finite dimensional L-vector space and L is a finite dimensional K-vector space.) Let $K = F(x_1, \ldots, x_r)$. We have $E = K(x_{r+1}, \ldots, x_m)$ is a fg K-module and F is a noetherian ring (since a field). Thus the lemma implies that K is a fg F-algebra. Write $K = F[y_1, \ldots, y_n]$ for some $y_i \in K$. It is easy to check that if $L \subseteq M$ are fields and $x \in M$ has the property that $L[x]$ is not a finite dimensional F-vector space then $L[x] \cong L[t]$ and $L(x) \cong L(t)$ as rings.

(Exercise.) It follows that $K \cong F(t_1, \ldots, t_r)$ and $F[x_1, \ldots, x_r] \cong F[t_1, \ldots, t_r]$ as rings. Thus we can write

$$y_i = \frac{f_i(x_1, ..., x_r)}{g_i(x_1, ..., x_r)}$$

for some $f_i, g_i \in F[t_1, \ldots, t_r]$, $g_i \neq 0$, $1 \leq i \leq n$. Let $g = g_1 \cdots g_n$ in $F[t_1, \ldots, t_r]$. Thus $g(x_1, ..., x_r) \in F[x_1, \ldots, x_r]$. We know $F[t_1, \ldots, t_r]$ contains infinitely many irreducibles. In particular, there exists an irreducible $f \in F[t_1, \ldots, t_r]$ such that $f \not| g$. Thus $f(x_1, ..., x_r) \not| g(x_1, ..., x_r)$ in $F[x_1, \ldots, x_r]$. But

$$\frac{1}{f(x_1, ..., x_r)} \in K = F[y_1, \ldots, y_n] = F\Big[\frac{f_1(x_1, ..., x_r)}{g_1(x_1, ..., x_r)}, \ldots, \frac{f_n(x_1, ..., x_r)}{g_n(x_1, ..., x_r)}\Big].$$

By clearing denominators, we may choose $N \geq 0$ such that

$$\frac{g(x_1, ..., x_r)^N}{f(x_1, ..., x_r)} \in F[f_1(x_1, ..., x_r), \ldots, f_n(x_1, ..., x_r)].$$

Then $\dfrac{g(x_1, ..., x_r)^N}{f(x_1, ..., x_r)}$ lies in $F[x_1, \ldots, x_r]$, i.e., $f | g^N$ in $F[t_1, \ldots, t_r]$, a contradiction. □

Definition. Let $R = F[t_1, \ldots, t_n]$ and $\mathfrak{A} \subseteq R$ an ideal. Then the set

$$Z(\mathfrak{A}) = \{a = (a_1, ..., a_n) \in F^n \mid f(a) = 0 \text{ for all } f \in \mathfrak{A}\}$$

is called the **variety** defined by $\mathfrak{A}$ over F.

Hilbert Nullstellensatz. (Weak Form) *Let F be an algebraically closed field. Let $R = F[t_1, \ldots, t_n]$. Let $\mathfrak{A} \subseteq R$ be an ideal. Then $Z(\mathfrak{A}) = \emptyset$ if and only if $\mathfrak{A} = R$. If $\mathfrak{A} < R$ then there exist $f_1, ..., f_r \in R$ such that $a \in Z(\mathfrak{A})$ if and only if $f_i(a) = 0$ for all i, $1 \leq i \leq r$. In particular, if $f_1, ..., f_r \in F[t_1, \ldots, t_n]$ do not generate the unit ideal in $F[t_1, \ldots, t_n]$ then there exists a point $a \in F^n$ such that $f_1(a0 = 0, ..., f_r(a) = 0$.*

Proof. The last statement follows immediately from the Hilbert Basis Theorem. Certainly if $\mathfrak{A} = R$ then there exists no $a \in F^n$ a solution to $1 \in R$. Suppose that $\mathfrak{A} < R$. Then there exists a maximal ideal $\mathfrak{m} \in R$ such that $\mathfrak{A} \subseteq \mathfrak{m}$. Let $^{-} : R \to R/\mathfrak{m}$. Let $E = R/\mathfrak{m} = F[\bar{t}_1, \ldots, \bar{t}_n]$. R is an affine F-algebra hence so is E. By Zariski's Lemma, E is a finite dimensional F-vector space. Since F is algebraically closed, this means that $E = F$. Indeed let $x \in E$. Then $F[x]$ is a finite dimensional F-vector space so $1, x, x^2, \ldots, x^n$ must be linear dependent over F for some n, i.e., x is a root of some non-zero polynomial $f \in F[t]$. But any such f factors completely over F, since all the roots of f lie in F. So $E = F$. Consequently the point $(\bar{t}_1, \ldots, \bar{t}_n) \in E^n = F^n$ lies in $Z(\mathfrak{A})$, since $\mathfrak{A} \subseteq \mathfrak{m}$, i.e., $\overline{\mathfrak{A}} = \overline{\mathfrak{m}} = 0$ □

Remark. In the above, $Z((f_1, \ldots, f_r))$ is the intersection of the 'hypersurfaces'

$$f_1 = 0, \ldots, f_r = 0 \quad \text{in} \quad F^n.$$

Remark. That F is algebraically closed is essential. Indeed $f(t_1, ..., t_n) = t_1^2 + \cdots + t_n^2 + 1$ has no solution in $\mathbf{R}^n$ yet $(f) < \mathbf{R}[t_1, \ldots, t_n]$. Can you state what the above argument shows when F is not algebraically closed?

Hilbert Nullstellensatz. (Strong Form) *Let F be an algebraically closed field. Let $R = F[t_1, \ldots, t_n]$. Let $f, f_1, ..., f_r \in R$. Let $\mathfrak{A} = (f_1, ..., f_r) \subseteq R$. Suppose that $f(a) = 0$ for all $a \in Z(\mathfrak{A})$. Then there exists an integer m such that $f^m \in \mathfrak{A}$, i.e., $f \in \sqrt{\mathfrak{A}}$. In particular, if $\mathfrak{A}$ is a prime ideal then $f \in \mathfrak{A}$.*

Proof. (Rabinowitch Trick). Let $S = R[t]$. Let $\mathfrak{B} = (f_1, ..., f_r, 1 - tf) \subseteq S$. If $\mathfrak{B} < S$ then there exists a point $(a_1, ..., a_{n+1}) \in Z(\mathfrak{B})$. Thus $f_i(a_1, ..., a_n) = 0$ for all i and $1 - a_{n+1}f(a_1, ..., a_n) = 0$. In particular, $(a_1, ..., a_n)$ lies in $Z(\mathfrak{A})$. By hypothesis, this means that $f(a_1, ..., a_n) = 0$ which in turn implies that $1 = 0$, a contradiction. Thus $\mathfrak{B} = S$. So we can write

$$1 = \sum_{i=1}^{r} g_i f_i + g \cdot (1 - tf)$$

for some $g, g_i \in S$. Substituting $\dfrac{1}{f}$ for t and clearing denominators yields the result. □