I. Noetherianity

Recall that a commutative ring R is called Noetherian if any ascending chain of ideals in R

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$$

stabilizes, i.e. if there exists an integer N for which $I_n = I_N$ whenever $n \geq N$.

Lemma 1: Any field is Noetherian.

Proof: If k is a field then the only ideals in k are 0 and k itself. ∎

Def$^{\underline{n}}$: A commutative ring R is called a principle ideal domain (PID) if R is a domain and if each ideal $I \subseteq R$ is generated by a single element, i.e. if there exists $a \in I$ for which $I = (a)$.

Note here that

$$(a) = \{ b \in R : b \text{ is divisible by } a \}.$$

Lemma 2: Any PID is Noetherian.

Proof: Let R be a PID and consider an

ascending chain of ideals $I_0 \subseteq I_1 \subseteq \dots$ in R. Let I be the ideal

$$I = \bigcup_{m \geq 0} I_m = \sum_{m \geq 0} I_m$$

and take $a \in I$ with $I = (a)$. By construction there is some N for which $a \in I_N$, so that $I_N = (a) = I$ and subsequently $I_n = I_N$ for all $n \geq N$. ∎

Example: $\mathbb{Z}$ is a PID. Indeed, for any nonzero ideal $I \subseteq \mathbb{Z}$ take a minimal positive integer a with $a \in I$. We claim $I = (a)$. Indeed, for any $b \in I$ we have $b = t \cdot a + r$ for an integer t and an integer r with $0 \leq r < a$. Since $r = b - ta \in I$ we conclude by minimality of a that $r = 0$, and hence that $b = t \cdot a$. So $b \in (a)$, and we conclude $I = (a)$.

Example: For k a field, $k[x]$ is a PID. Indeed, for any nonzero ideal $I \subseteq k[x]$ take $p(x) \in I$ a nonzero element of minimal degree. By multiplying by a unit in k we can assume that $p(x)$ is monic. For any $f(x) \in I$ we can write

$$f(x) = t(x) \cdot p(x) + r(x)$$

with $r(x)$ of degree $<$ deg $p(x)$. (This is easy to see by induction on the degree of $f(x)$.) Hence

$$r(x) = f(x) - t(x) \cdot p(x) \in I$$

and by minimality of $p(x)$ we conclude $r(x) = 0$. Hence $f(x) \in (p(x))$, and we conclude $I = (p(x))$.

Corollary 8: $\mathbb{Z}$ is Noetherian, and for any field k the polynomial ring $k[x]$ is Noetherian.

II. Polynomial rings are Noetherian

For any comm. ring R we can consider the polynomial ring $R[x]$, which is explicitly the free R-module $R[x] = \bigoplus_{i \geq 0} R \cdot x^i$ equipped with the expected product

$$\left(\sum_{i=1}^{m} a_i \cdot x^i\right) \cdot \left(\sum_{j=1}^{n} b_j x^j\right) = \sum_k \left(\sum_{i+j=k} a_i b_j\right) x^k.$$

We define recursively
$$R[x_1,\dots,x_n] = (R[x_1,\dots,x_{n-1}])[x_n].$$

Theorem 4: For any commutative Noetherian ring R, and any $n \geq 1$, the polynomial ring
$$R[x_1,\dots,x_n]$$
is also Noetherian.

Proof: It suffices to prove the result at $n=1$, i.e. to prove Noetherianity of $R[x]$ given Noeth. of R.

Take an ascending chain of ideals
$$I_0 \subseteq I_1 \subseteq \cdots \quad \text{in } R[x] \qquad (*)$$
and for each $m \geq 0$ let
$$I_m(d) = \left\{ a \in R : \begin{array}{l} \text{a polynomial of the form} \\ ax^d + \text{lower deg terms} \\ \text{is in } I_r \end{array} \right\}.$$

Note that each $I_m(d)$ is an ideal in R, and that we have inclusions
$$I_{m+1}(d) \supseteq I_m(d), \quad I_m(d+1) \supseteq I_m(d).$$
The latter inclusion comes from multiplying by x in I_m.

Consider the ascending sequence

$$I_0(0) \subseteq I_1(1) \subseteq I_2(2) \subseteq \cdots$$

and for each d, $I_0(d) \subseteq I_1(d) \subseteq I_2(d) \subseteq \cdots$.

By Noeth. of R we can find N at which

$$I_n(n) = I_N(N) \text{ whenever } n \geq N$$

and, for each d, we find m_d with

$$I_m(d) = I_{m_d}(d) \text{ whenever } m \geq m_d.$$

Take now

$$M = \max\{N, m_0, m_1, \ldots m_N\}$$

to get $I_m(d) = I_M(d)$ whenever $m \geq M$ across all d.

We claim that $I_m = I_M$ whenever $m \geq M$, thus stabilizing the original sequence $(*)$. To see this, let's assume not, take $m > M$ with $I_M \subsetneq I_m$, and choose $f(x)$ of minimal degree with

$$f(x) \in I_m \setminus I_M.$$

Since $f(x) \neq 0$ necessarily, we can write

$$f(x) = ax^d + \text{lower degree terms}$$

for some nonzero $a \in R$. Since $I_m(d) = I_M(d)$ however, we can choose $g(x)$ in I_M of the form

$$g(x) = ax^d + \text{lower degree}.$$

This gives $f(x) - g(x)$ of degree $< d$

while $f(x) - g(x) \in I_m \setminus I_M$, since $f(x) \notin I_M$.
However this contradicts minimality of $f(x)$.

So we see that, indeed, $I_m = I_M$ when $m \geq M$, and thus stabilize our original sequence. We conclude that $R[x]$ is in fact Noetherian. ∎

Corollary 5: The integral polynomial rings

$$\mathbb{Z}[x_1, \ldots, x_n]$$

are all Noetherian, and for any field k the polynomial rings $k[x_1, \ldots, x_n]$ are all Noetherian.

– III. Finitely generated algebras

Theorem 6: For any commutative ring k, and commutative k-algebra A, any choice of elements

$$a_1, a_2, \ldots, a_n \in A$$

specifies a unique k-algebra map

$$\phi : k[x_1, \ldots, x_n] \to A$$

with $\phi(x_i) = a_i$ for all $i = 1, \ldots, n$.

Proof: As for uniqueness, given two such alg maps

ϕ and ϕ' we have via bilinearity and splitting over products

$$\phi(p(x_1,\dots,x_n)) = p(\phi x_1, \dots, \phi x_n) = p(a_1,\dots,a_n)$$
$$= \phi'(p(x_1,\dots,x_n))$$

at all p in $k[x_1,\dots,x_n]$. Hence $\phi = \phi'$.

For existence we first consider the case $k[x]$ of polynomials in a single variable. In this case $k[x]$ is the (noncommutative) free algebra and we have the proposed map $\phi : k[x] \to A$ with $\phi(x) = a$ [Theorem 1, Genrel], and for $K = k[x]$ the map ϕ gives A the structure of a K-algebra. Considering $K_r = k[x_1,\dots,x_r]$ for $r \leq n$,

$$K_r = K_{r-1}[x],$$

we now observe by induction the existence of an alg map $\phi : k[x_1,\dots,x_n] \to A$ with prescribed values $\phi(x_i) = a_i$. ∎

Def$^{\underline{n}}$: For a field, or more generally a commutative ring k, we say a commutative k-alg A is finitely generated if A admits a finite subset $\{a_1,\dots,a_n\} \subseteq A$ for which the associated k-alg map $k[x_1,\dots,x_n] \to A$, $x_i \mapsto a_i$, is surjective. Equivalently, A is finitely generated if A admits some surjective algebra map

$$k[x_1, \ldots, x_n] \to A.$$

Remark: We also call finitely generated k-algebras finite type k-algebras.

Remark: Being of finite type is a property, not a structure. We do not care to choose any particular set of algebra generators $a_1, \ldots, a_n \in A$.

Theorem 7: Let k be a PID, or more generally any comm. Noeth. ring. Any finite type k-algebra is Noetherian.

Proof: Let A be of finite type, and consider a surjective algebra map

$$\phi : k[x_1, \ldots, x_n] \to A.$$

Then we have

$$\{\text{Ideals in } A\} = \{A\text{-submodules in } A\}$$
$$= \{k[x_1, \ldots, x_n]\text{-submodules in } A\},$$

via surjectivity of ϕ. But by Theorem 4 the poly ring $k[x_1, \ldots, x_n]$ is Noetherian, so that submodules in A satisfy the ACC. Hence A is Noetherian. ∎

Corollary 8: For k a field, any finite type k-algebra is Noetherian. Also, any finite type $\mathbb{Z}$-algebra is Noetherian.

IV Noetherianity and finite generation

We call an ideal I in a ring R finitely generated if

$$I = (x_1, \dots, x_t) = \left\{ \sum_{i=1}^{t} a_i x_i : a_i \in R \right\}$$

for some finite collection of elements $x_i \in I \subseteq R$.

Theorem 9: For a commutative ring R the following are equivalent

i) R is Noetherian

ii) Any ideal in R is finitely generated.

iii) Every submodule of a finitely generated R-module is also finitely generated.

Proof: First observe that an R-module M is finitely generated if and only if any <u>exhaustive</u>

ascending chain of submodules, i.e. chain $M_0 \subseteq M_1 \subseteq \cdots$ with $M = \bigcup_{i \geq 0} M_i$, stabilizes. Indeed, if $M = R \cdot \{m_1, \ldots, m_n\}$ then we can find some M_N with

$$m_1, \ldots, m_n \in M_N$$

by exhaustion, giving $M_N = M$. Conversely, if M is <u>not</u> finitely generated take a minimal generating set $\{m_\lambda : \lambda \in \Lambda\}$ for M and choose an unbounded function

$$f : \Lambda \to \mathbb{Z}_{\geq 0}.$$

Then for $M_i = R \cdot \{m_\lambda : f(\lambda) \leq i\}$ we obtain an ascending, exhaustive chain of submodules which does not stabilize.

Anyway! If R is Noetherian then every finitely generated R-module M is Noetherian [Thm 6, Findim], as is any submodule in such finitely generated M [Cor 7, Findim]. So we see (i) $\Rightarrow$ (iii), and restricting to the case $M = R$ we see (i) $\Rightarrow$ (ii) as well as (iii) $\Rightarrow$ (ii). For (ii) $\Rightarrow$ (i), suppose ideals in R are all finitely generated and consider an ascending chain of ideals

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots \quad \text{in } R.$$

Then for the ideal $I = \bigcup_{n\geq 0} I_n$ we can find generators $I = (x_1, \ldots, x_t)$ and take N sufficiently large to obtain

$$x_1, \ldots, x_t \in I_N \Rightarrow I = I_N \Rightarrow I_n = I_n$$

for all $n \geq N$. Thus R is Noetherian. ∎

Corollary 10: For any field k, or $k = \mathbb{Z}$, any finite type k-algebra R admits a finite presentation

$$k[x_1, \ldots, x_n] \big/ (f_1, \ldots, f_t) \xrightarrow{\sim} A . \qquad (*)$$

Proof: Any surjective algebra map $k[x_1, \ldots, x_n] \to A$ has kernel $I \subseteq k[x_1, \ldots, x_n]$ an ideal in $k[x_1, \ldots, x_n]$. Since $k[x_1, \ldots, x_n]$ is Noetherian, by Theorem 4, this ideal is finitely generated $I = (f_1, \ldots, f_t)$, giving such an expression $(*)$. ∎

~ V Factorization

Def$^{!}$: An element a in a commutative domain R is called irreducible if a is a non-unit and in any factorization $a = a_1 \cdot a_2$ one of a_1 or a_2 is a unit.

Two units p and q are said to be associates if $p = u \cdot q$ for a unit $u \in R^{\times}$.

A commutative domain R is called a unique factorization domain if each nonzero non-unit $a \in R$ factors into a product of irreducibles

$$a = p_1 \cdots p_r,$$

and this factorization is unique up to permuting the order and taking associates.

Lemma 11: For nonzero elem a, b in a commutative domain R $(a) = (b)$ if and only if $b | a$ and, in any factoring $a = u \cdot b$, u is a unit.

Proof: We have $a = ub$ and $b = u'a$ by assumption, giving $a = u \cdot u' \cdot a \Rightarrow (1 - u \cdot u') \cdot a = 0$. Since R is a domain this forces $u \cdot u' = 1$. ∎

Lemma 12: In any PID R,

i) Every nonzero nonunit $a \in R$ is divisible by an irreducible element.

ii) Every nonzero nonunit $a \in R$ factors into a finite product of irreducibles $a = p_1 p_2 \cdots p_r$.

Proof of (ii): Factor a as

$$a = b_1 \cdot a_1 \quad \text{with} \begin{cases} a_1, b_1 \text{ nonunits if } a \text{ not irred.} \\ a_1 = 1 \text{ if } a \text{ is irreducible.} \end{cases}$$

Similarly, factor

$$a_1 = b_2 \cdot a_2 \quad \text{w/} \begin{cases} a_2, b_2 \text{ nonunit if } b_1 \text{ red nonunit} \\ a_2 = 1 \quad \text{else}, \end{cases}$$

etc. In this way we produce a collection of divisors

$$\cdots a_t \mid a_{t-1} \mid a_{t-2} \mid \cdots \mid a$$

and corresponding ascending sequence of ideals

$$(a) \subseteq (a_1) \subseteq (a_2) \subseteq \cdots .$$

Since every PID is Noetherian (Lemma 2) this chain stabilizes at some minimal index N,

$$(a_N) = (a_n) \quad \text{for all } n \geq N.$$

We have $a_N = b_{N+1} \cdot a_{N+1}$ and, since $(a_N) = (a_{N+1})$, $a_{N+1} = b'_{N+1} \cdot a_N$. Hence $a_N = (b'_{N+1} \cdot b_{N+1}) \cdot a_N \Rightarrow (1 - b'_{N+1} \cdot b_{N+1}) \cdot a_N = 0$. Since R is a domain, and all $a_N \neq 0$, we conclude that b_{N+1} is a unit.

If a_N were not a unit then by construction b_{N+1} would not be a unit. So we conclude a_N is a unit, which again by construction and min. of N implies a_{N-1} is an irreducible divisor of a. ∎

Proof of (ii): If a admits no such finite expression then we can take successive irreducible divisors $a = p_1 \cdot a_1$, $a_1 = p_2 \cdot a_2$, $a_3 = p_4 \cdot a_4$, etc. giving an ascending sequence of ideals

$(a) \subseteq (a_1) \subseteq (a_2) \subseteq \cdots$.

By Noetherianity $(a_N) = (a_{N+1})$ at some large N, which implies via the factorization $a_N = p_{N+1} a_{N+1}$ and Lemma 11 that p_{N+1} is a unit. But this was specifically not the case, since by assumption p_{N+1} is irreducible. So we reach a contradiction, and conclude that a admits a finite factoring as a product of irreducibles. ∎

Lemma 13: For an irreducible element p in a PID R, if $p \mid a \cdot b$ then either $p \mid a$ or $p \mid b$.

Proof: Suppose $p \mid a \cdot b$ and that $p \nmid a$. We have $(p, a) = (d)$ for some $d \in R$ by PID-ness, giving $p = c \cdot d$. If d is not a unit, this implies c a unit by irred. of p. Hence $(d) = (p)$, and we conclude $p \mid a$ since $a \in (d)$, a contradiction. Hence d is a unit and $1 \in (d)$. This gives

$1 \in (p, a) \Rightarrow 1 = c_1 \cdot p + c_2 \cdot a$ for some c_i in R. Thus

$$p \mid (c_1 \cdot p \cdot b + c_2 \cdot a \cdot b) = (c_1 p + c_2 \cdot a) \cdot b = b. \quad \blacksquare$$

Proposition 14: Any PID is a unique factorization domain.

Proof: Take a nonzero nonunit a w/ factorizations into irreducibles

$$p_1 p_2 \cdots p_r = a = q_1 q_2 \cdots q_s, \quad \text{w/ } s \geq r \text{ say}.$$

Then $p_1 \mid q_1 \cdots q_r$ and by Lemma 13 $p_1 \mid q_i$ for some i. After permuting we may assume $i = 1$, $p_1 \mid q_1$. Then by irreducibility

$$q_1 = u_1 \cdot p_1 \quad \text{for a unit } u_1.$$

We divide by p_1 now (legal since we're in a domain) to get

$$p_2 \cdots p_r = u_1 q_2 \cdots q_s.$$

If $p_2 \mid u_1$ then $u_2 = a \cdot p_2 \Rightarrow 1 = u_2^{-1} \cdot a \cdot p_2 \Rightarrow$ p_2 a unit, which is nonsense. So $p_2 \mid q_2 \cdots q_s$ and after permuting we get

$$p_3 \cdots p_r = (u_1 u_2) \cdot q_3 \cdots q_s.$$

Continuing in this fashion we get

$$1 = \begin{cases} (u_1 \cdots u_r)\, q_{r+1} \cdots q_s & \text{if } s > r \\ u_1 \cdots u_r & \text{if } s = r. \end{cases}$$

In the first case we conclude that q_s is invertible, which is crap! Hence $s = r$, and after reordering,

$$p_i = u_i \cdot q_i \quad \text{for each } i. \quad \blacksquare$$

Theorem 15: If K is a unique fact. domain then $K[x]$ is a unique fact. domain.

Proof: Omitted (see Stacks project). $\blacksquare$

Corollary 16: For each $n \geq 1$,

$$\mathbb{Z}[x_1, \ldots, x_n] \text{ is a UFD,}$$

and for any field k, $k[x_1, \ldots, x_n]$ is a UFD.

Remark: Quotients of UFDs are not UFDs in general, since they are usually not domains. However, even when Q/I is a domain, there's no reason for the quotient to have unique factorization.

So, this is really *just* a result for polynomial rings.