

The ascending tree condition

Fred Richman
Florida Atlantic University

23 December 2001

Abstract

A strengthening of the ascending chain condition allows a choice-free constructive development of the theory of Noetherian modules. Related topics in the theory of PID's and elementary divisor rings are also explored.

The theory of finitely generated modules over a Noetherian ring admits a satisfactory constructive development by considering finitely presented modules over a coherent Noetherian ring [5]. From a classical point of view, every finitely generated module over a Noetherian ring is finitely presented—in particular, every Noetherian ring is coherent—so this also provides an adequate classical theory. From a constructive point of view, being finitely presented, rather than finitely generated, is a stronger property that must be assumed even if the ring is a field. The definition of Noetherian used in [5] was the **ascending chain condition** on finitely generated ideals, in the form

If $I_1 \subset I_2 \subset I_3 \subset \cdots$ is a chain of finitely generated ideals, then there exists n such that $I_n = I_{n+1}$.

With this definition one can, for example, prove the **Hilbert basis theorem**: If R is a coherent Noetherian ring, then so is the polynomial ring $R[X]$.

What role do (countable) choice axioms play in this development? In order to apply the ACC you have to construct a countable chain. This often requires choice. For example, to prove that a quotient of a Noetherian module is Noetherian, you lift a chain of finitely generated ideals from the quotient to the module. Because there is no canonical way to do that, unless the kernel

is finitely generated, you have to invoke choice. Similar problems appear in showing that an extension of a Noetherian module by a Noetherian module is Noetherian.

The question arises as to whether these invocations of choice can be avoided. One interesting way to avoid choice is to replace the ACC by **Noetherian induction**:

If C is a set of finitely generated ideals with the property that a finitely generated ideal I is in C whenever all finitely generated ideals that strictly contain I are in C , then every finitely generated ideal is in C .

Such a theory was successfully developed by Jacobsson and L\"ofwall [4] including a proof of the Hilbert basis theorem. They required the ring to be **strongly discrete** (have a membership algorithm): if I is a finitely generated ideal, and x is an element, then either $x \in I$ or $x \notin I$. This seems necessary and is reasonable for a theory that emphasizes strict inclusion of ideals. I have yet to learn to love this approach although I have tried, off and on, for many years.

In this paper I present an alternative way to avoid choice by modifying the chain condition. Instead of ascending chains, indexed by the natural numbers, we allow increasing functions on trees. The result is the **ascending tree condition**.

1 The ATC

An **acceptable index set** is a nonempty set A , with a binary relation $a < b$, such that for each $a \in A$ there is $b \in A$ with $a < b$. We will be interested in families of subsets I_a , indexed by A , which are **increasing**, that is, if $a < b$, then $I_a \subset I_b$. We say that an increasing family **halts** if there exist $a < b$ in A with $I_a = I_b$.

By a **tree** we will mean a partially ordered set T with a least element 0 such that for each $t \in T$

- the set $\{s \in T : s \leq t\}$ is a finite chain, and
- there exists $s \in T$ such that $s > t$.

So every tree is an acceptable index set. The set \mathbf{N} of natural numbers is a tree. A more complicated example is the set of finite sequences of natural numbers partially ordered by extension.

A set \mathcal{C} of subsets of a set satisfies the **ascending chain condition** (the **ACC**) if any increasing family of elements of \mathcal{C} , indexed by the natural numbers \mathbf{N} , halts. It satisfies the **ascending tree condition** (the **ATC**) if any increasing family of elements, indexed by a tree, halts. Of course ATC implies ACC. The point of using ATC, rather than ACC, is to avoid appeals to countable choice axioms. If you allow such appeals, then the two conditions are equivalent.

Theorem 1 *In the presence of the axiom of dependent choices, ATC is equivalent to ACC.*

Proof. Let T be a tree and I_t an increasing family of subsets indexed by T . By the axiom of dependent choices, we can construct a sequence $t_1 < t_2 < t_3 < \dots$ in T . Define an increasing family I'_n , indexed by \mathbf{N} , by $I'_n = I_{t_n}$. By ACC, there exists n such that $I_{t_n} = I_{t_{n+1}}$. ■

It is often easier to construct an increasing family using an acceptable index set rather than a tree. That is the point of considering acceptable index sets. The following theorem shows that the two associated notions of Noetherian are equivalent.

Theorem 2 *If a set \mathcal{C} of subsets of a set satisfies the ATC, then any increasing family of elements of \mathcal{C} , indexed by an acceptable index set, halts.*

Proof. Let I_a be an increasing family of elements of \mathcal{C} indexed by an acceptable index set A , and let $a_0 \in A$. Let T be the set of nonempty finite sequences $a_0 < a_1 < \dots < a_n$ in A ordered by extension. Note that T is a tree with least element the one-element sequence a_0 . We get an increasing family J_t indexed by T upon setting $J_{(a_0, \dots, a_n)} = I_{a_n}$. So there exist $s < t$ in T such that $J_s = J_t$. If the last elements of s and t are a and b respectively, then $a < b$ and $I_a = I_b$. ■

The halting terminology is meant to be suggestive. We can think of an increasing chain I_n in \mathcal{C} as being generated by successive steps of an algorithm, the condition that the algorithm halts being $I_n = I_{n+1}$. An increasing family indexed by a tree can be thought of as being generated by a *nondeterministic* algorithm with the same halting condition. There is a strong suggestion here of Brouwer's free choice sequences. A family indexed by a tree is essentially a slight modification of Brouwer's notion of a *spread* [3].

2 Noetherian modules

Define a **Noetherian module** to be a module that satisfies the ATC on finitely generated submodules. Clearly submodules of Noetherian modules are Noetherian.

Theorem 3 *Quotients of Noetherian modules are Noetherian.*

Proof. Let $\varphi : B \rightarrow C$ be an epimorphism with B Noetherian. Let C_n be an increasing family of finitely generated submodules of C indexed by a tree N . Let I consist of pairs (n, A) with $n \in N$ and A a finitely generated submodule of B that maps onto C_n . Set $(n, A) < (n', A')$ if $n < n'$ and $A \subset A'$. Then I is an acceptable index set. Consider the family $F_{(n,A)} = A$ indexed by I . As B is Noetherian, there exist $n < n'$ and A such that A maps onto both C_n and $C_{n'}$, so $C_n = C_{n'}$. ■

The obvious attempts to prove this theorem using ACC instead of ATC require choice unless $\ker \varphi$ is finitely generated.

Theorem 4 *If a module B maps onto a Noetherian module C with Noetherian kernel A , then B is Noetherian.*

Proof. Let F_n be an increasing family of finitely generated submodules of B indexed by a tree N . Denote the map from B onto C by φ . If $m < n$, and $\varphi(F_m) = \varphi(F_n)$, then $F_n = F_m + K$ for some finitely generated submodule K of A . Consider the set J consisting of triples (m, n, K) such that $m < n$ and $K \subset A$ is a finitely generated submodule such that $F_n = F_m + K$. Define $(m, n, K) < (m', n', K')$ if $n < m'$ and $K \subset K'$.

We show that J is an acceptable index set. Suppose $n_0 \in N$ and K_0 is a finitely generated submodule of $A \cap F_{n_0}$. The set $N' = \{n \in N : n > n_0\}$ is an acceptable index set with a transitive order. Consider the increasing family $\varphi(F_n) \subset C$ indexed by N' . As C is Noetherian, there exist m and n with $n_0 < m < n$ and $\varphi(F_m) = \varphi(F_n)$. There is a finitely generated submodule K of A , containing K_0 , so that $F_n = F_m + K$. So J is nonempty, and is an acceptable index set. Set

$$G_{(m,n,K)} = K.$$

Then G is an ascending family of finitely generated submodules of A indexed by J . As A is Noetherian, there exist (m, n, K) and (m', n', K') in J with $m < n < m' < n'$ and $K = K'$. So $K' = K \subset F_{m'}$ whence $F_{m'} = F_{n'}$. ■

It follows that finite-rank free modules over a Noetherian ring are Noetherian. With just ACC, you seem to need strong discreteness and coherence to prove this without choice.

The Noetherian induction principle implies ATC.

Theorem 5 *A strongly discrete module that admits Noetherian induction is Noetherian.*

Proof. To show that every increasing family F , indexed by a tree N , halts, we proceed by Noetherian induction on F_0 . Choose $j > 0$ in N . If $F_j = F_0$, then F halts. If $F_j \neq F_0$, then define F' to be the restriction of F to the subtree $N' = \{i \in N : i = j \text{ or } i > j\}$. Note that j is the 0 element of N' . Then F' is an increasing family indexed by the tree N' such that $F'_0 = F_j$ strictly contains F_0 . So F' halts by the Noetherian induction hypothesis. Therefore F also halts. ■

3 The Hilbert basis theorem

Let R be a ring and consider the polynomial ring $R[X]$, where X commutes with elements of R . Denote by $R[X]_n$ the set of polynomials of degree less than n (a rank- n free R -module). Let $L_n(I)$ be the left ideal in R obtained by projecting $I \cap R[X]_n$ onto the last coordinate of $R[X]_n$ (the coefficient of X^{n-1}). Let $L(I) = \bigcup_{n=1}^{\infty} L_n(I)$.

Theorem 6 *If R is coherent, and I is a left ideal in $R[X]$, then $L_m(I)$ is finitely generated for each $m \leq n$ if and only if $I \cap R[X]_n$ is finitely generated.*

Proof. Suppose $I \cap R[X]_n$ is finitely generated. If $m \leq n$, then $I \cap R[X]_m = (I \cap R[X]_n) \cap R[X]_m$. As R is coherent, if $I \cap R[X]_n$ is finitely generated, then so is $I \cap R[X]_m$. But $L_m(I)$ is a homomorphic image of $I \cap R[X]_m$.

Conversely, suppose $L_m(I)$ is finitely generated for each $m \leq n$. Then there is a finitely generated submodule M of $I \cap R[X]_n$ such that $L_m(I) = L_m(M)$ for each $m \leq n$. We show that $M = I \cap R[X]_n$. Indeed, if $f \in I \cap R[X]_m$, then we can find $g \in M$ such that $f - g \in I \cap R[X]_{m-1}$, and induction finishes the proof. ■

Heinzer and Papick [1] define the **Kaplansky Property, (KP)**:

For each finitely generated ideal I of $R[X]$, the ideals $L_n(I)$, and the ideal $L(I) = \bigcup_{n=1}^{\infty} L_n(I)$, are finitely generated.

In view of Theorem 6, a key lemma [5, VIII Lemma 1.1] for the constructive proof of the Hilbert basis theorem shows that a coherent Noetherian ring satisfies KP. We give a shortened proof of the heart of that lemma.

Theorem 7 *Suppose, for each n , that $R[X]_n$ is a coherent R -module satisfying the ACC on finitely generated submodules. Then R satisfies KP.*

Proof. Let I be a finitely generated left ideal of $R[X]$. Let M_0 be the R -submodule of $R[X]_n$ generated by a set of generators of I . Let $M_{i+1} = M_i + (XM_i) \cap R[X]_n$, which is finitely generated because $R[X]_{n+1}$ is coherent. If $M_{i+1} = M_i$, then $M_j = M_i$ for all $j > i$. Such an i exists because $R[X]_n$ satisfies the ACC on finitely generated submodules. Let $M = M_i$. We will show that $M = I \cap R[X]_n$ and that $L(I) = L_n(I)$.

Now $I = \sum_{k=0}^{\infty} X^k M$. We will show by induction that

$$\left(\sum_{k=0}^t X^k M \right) \cap R[X]_n = M \text{ and } L_{n+t}(I) = L_n(I).$$

This is true for $t = 0$. Suppose it's true for $t - 1$. Let $f = \sum_{k=0}^t X^k m_k$ with $m_k \in M$ for each k . The last coefficient of $f \in R[X]_{n+t}$, is the last coefficient of $m_t \in R[X]_n$ which is in $L_n(I)$. If $f \in R[X]_n$, then

$$f = X \sum_{k=0}^{t-1} X^k m_{k+1} + m_0 \in R[X]_n$$

so

$$X \sum_{k=0}^{t-1} X^k m_{k+1} \in R[X]_n \text{ and } \sum_{k=0}^{t-1} X^k m_{k+1} \in M$$

whence $f \in M$. ■

A few remarks about Theorem 7 are in order. Extensions of finitely generated coherent modules are coherent [5, III Theorem 2.5] so $R[X]_n$ is coherent if $R[X]_1 = R$ is. If R is Noetherian (ATC), then $R[X]_n$ has the ACC on finitely generated submodules, but without choice we don't know

how to derive this from the weaker assumption of ACC on R . However, if R is also coherent and strongly discrete, then we can establish ACC by induction for $R[X]_n$ without choice because intersections remain finitely generated and strong discreteness allows us to choose the *first* place where a chain pauses.

The standard constructive treatments of the Hilbert basis theorem require that the ring also be coherent. So we need to prove inheritance of coherence from R to $R[X]$ in order to iterate. It is desirable to show that strong discreteness is also inherited. That is the content of [5, VIII Lemma 1.3]. Although the ring R there was assumed to satisfy the ACC on finitely generated left ideals, the proof actually shows the following reformulation:

Theorem 8 (MRR VIII.1.3) *If R is a coherent ring satisfying KP, then $R[X]$ is a coherent ring. If, in addition, R is strongly discrete, then so is $R[X]$.*

It remains to consider the inheritance by $R[X]$ of the Noetherian condition on R —the Hilbert basis theorem proper. Choice is used heavily in the proof in [5, VIII Theorem 1.5]. Using ATC eliminates this.

Theorem 9 *If R is a coherent Noetherian ring, then so is $R[X]$.*

Proof. A left ideal I in $R[X]$ is said to be **supported by n** if it is generated by a finite subset of $R[X]_n$. Let I_t be an ascending family of finitely generated ideals of $R[X]$ indexed by a tree T . If I_t is supported by n , then there are $r > s > t$ such that $I_r \cap R[X]_n = I_s \cap R[X]_n$. So the index set T' consisting of pairs $r < s$ in T with $(r < s) < (u < v)$ if $s < u$ and there is n so that I_s is supported by n and $I_u \cap R[X]_n = I_v \cap R[X]_n$ is acceptable. The family of finitely generated ideals $I_{(r < s)} = L(I_s)$ indexed by T' is increasing. As R is Noetherian, there exist $r < s < u < v$ in T and n so that I_s is supported by n and $I_u \cap R[X]_n = I_v \cap R[X]_n$, with $L(I_s) = L(I_v)$. So $L(I_u) = L(I_v)$ and I_v is supported by n whence $I_u = I_v$. ■

4 PID's

A principle ideal domain is a Noetherian Bézout domain, so a modification of the definition of Noetherian will have repercussions for PID's. One test to see if you have the right notion of a PID is to show that every PID is an

elementary divisor ring. It suffices to diagonalize 2-by-2 matrices. Given a matrix

$$\begin{pmatrix} a & b \\ \bullet & \bullet \end{pmatrix}$$

construct s and t so that $d_1 = sa + tb$ divides both a and b . Then multiply by a matrix of determinant 1 on the right to get:

$$\begin{pmatrix} a & b \\ \bullet & \bullet \end{pmatrix} \begin{pmatrix} s & -b/d_1 \\ t & a/d_1 \end{pmatrix} = \begin{pmatrix} d_1 & 0 \\ \bullet & \bullet \end{pmatrix}. \quad (*)$$

Now making a similar move on the left we get a matrix of the form

$$\begin{pmatrix} d_2 & \bullet \\ 0 & \bullet \end{pmatrix}.$$

where the ideal (d_1) is contained in (d_2) . Note that if $(d_1) = (d_2)$, then d_1 divides the entry below it in $(*)$, so we can diagonalize by making that entry zero with an elementary row operation.. Alternating back and forth, we generate a sequence of elements d_1, d_2, d_3, \dots so that $(d_1) \subset (d_2) \subset (d_3) \subset \dots$. If $(d_n) = (d_{n+1})$ for some n , as guaranteed by ACC, then we can diagonalize.

The choice problem arises from the fact that the s and t in $sa + tb = \gcd(a, b)$ are not unique, so we need choice to form the infinite sequence d_1, d_2, d_3, \dots . The ideal generated by $sa + tb$ is unique, but s and t enter into the construction of the new matrix. One could of course define a Bézout domain in terms of a *function* from $R \times R$ to $R \times R$ taking (a, b) to (s, t) , rather than simply requiring the existence of (s, t) for each (a, b) , but this seems unnatural in classical terms. Generally, I think it is desirable to take over classical definitions verbatim as much as possible.

If we have ATC instead of ACC, this proof goes through without choice. The index set here is the set of finite sequences $(s_1, t_1), (s_2, t_2), \dots (s_n, t_n)$ in $R \times R$ that do the row and column operations. The ideal indexed by such a sequence is the ideal generated by the upper left corner of the matrix after performing the n indicated operations. Note how this can be thought of as a nondeterministic algorithm for diagonalizing the matrix.

I had thought that this analysis of the proof that a PID is an elementary divisor ring sufficed to establish the superiority of ATC over ACC in a choiceless environment. In fact, it turns out that I was just looking at the

wrong proof. Helmer [2] also worries about using ACC to prove that a ring is an elementary divisor ring, presumably for different reasons. He defines a Bézout domain to be **adequate** if, given a and c , we can write $a = rs$ such that

1. $(r, c) = 1$, and
2. $(s, t) = 1$ if $(t, c) = 1$.

The two conditions say that you can construct a factor r of a that is maximal with respect to being relatively prime to c . Call an adequate ring **superadequate** if, instead of 2, it satisfies the stronger and simpler condition

- 2'. s divides c^n for some n .

Theorem 10 *A Bézout domain with ACC is superadequate.*

Proof. Suppose $a = rs$ with $(r, c) = 1$. Let $s_0 = s$ and $s_{i+1} = s_i / (s_i, c)$. Note that if we set $I_i = (s_i)$, then $I_{i+1} = I_i : (c)$. When the ideals I_i pause we have $(s_n, c) = 1$ and we set $r' = rs_n$ and $s' = s/s_n$. Clearly s' divides c^n .

■

An apparently weaker condition suffices to get an elementary divisor ring. Call a Bézout domain **subadequate** if, given d and $(s_1, s_2) = 1$, we can write $d = d_1d_2$ with $(s_1d_1, s_2d_2) = 1$. This is implied by adequate: Given a and $(t, c) = 1$, we can write $a = rs$ with $(tr, sc) = 1$. The notion of subadequate arises naturally when one tries to construct an element of maximal order in the module presented by a 2-by-2 matrix (a_{ij}) , that is, the module with generators x_1 and x_2 , and relations $a_{11}x_1 + a_{12}x_2 = 0$ and $a_{21}x_1 + a_{22}x_2 = 0$.

Theorem 11 *Any subadequate Bézout domain is an elementary divisor ring.*

Proof. It suffices to show that if M is a simply presented R -module with generators x_1 and x_2 , then M is a direct sum of two cyclic modules. As R is coherent, so is M [5, III Theorem 2.5]. As M is coherent, the annihilators of elements of M are principle, as are the annihilators of elements of M/Rm for any $m \in M$. Let Rr_i be the annihilator of x_i and write $r_i = ds_i$ with $(s_1, s_2) = 1$.

By hypothesis, we can write $d = d_1d_2$ so that $(s_1d_1, s_2d_2) = 1$. Then $r_i = d_1d_2s_i$. The annihilator of d_1x_2 is Rd_2s_2 , and the annihilator of d_2x_1

is Rd_1s_1 , so the annihilator of $d_2x_1 + d_1x_2$ is Rs_1ds_2 , the least common multiple of the annihilators of x_1 and x_2 . Thus the annihilator of $d_2x_1 + d_1x_2$ annihilates M . Choose a_1 and a_2 so that $a_1d_1 - a_2d_2 = 1$. Then $d_2x_1 + d_1x_2$ and $a_1x_1 + a_2x_2$ generate M . So we may assume that the annihilator of x_1 annihilates M , that is, $r_1M = 0$.

Let $R\lambda = \{r \in R : rx_2 \in Rx_1\}$. Then λ divides r_2 because $r_2x_2 = 0 \in Rx_1$. If $\lambda x_2 = \mu x_1$, then r_1 divides $(r_2/\lambda)\mu$ because $(r_2/\lambda)\mu x_1 = r_2x_2 = 0$. But r_2 divides r_1 , because $r_1x_2 = 0$, so λ divides μ . Then x_1 and $x_2 - (\mu/\lambda)x_1$ are generators that exhibit M as a direct sum of two cyclic modules. ■

References

- [1] HEINZER, WILLIAM J. AND IRA J. PAPICK, Remarks on a remark of Kaplansky, *Proc. Amer. Math. Soc.*, **105** (1989) 1–9.
- [2] HELMER, OLAF, The elementary divisor theorem for certain rings without chain condition, *Bull. Amer. Math. Soc.* **49** (1943), 225–236.
- [3] HEYTING, AREND, *Intuitionism, an introduction*, North-Holland 1956.
- [4] JACOBSSON, CARL AND CLAS LÖFWALL, Standard bases for general coefficient rings and a new constructive proof of Hilbert’s basis theorem, *J. Symbolic Comput.* **12** (1991), 337–371.
- [5] MINES, RAY, FRED RICHMAN AND WIM RUITENBURG, *A course in constructive algebra*, Springer Verlag 1988.