Noetherian rings

Perdry – Schuster

(work in progress)

Castro Urdiales, MAP 2006

Noetherian rings (classical definition)

ACC If $(a_i)_{i\in\mathbb{N}}$ is an weakly increasing sequence, there exists some index $n \in \mathbb{N}$ such that $a_n = a_{n+1} = a_{n+2} = \cdots$

A ring R is said to be Noetherian if the poset $(\mathcal{J}_\mathsf{R}, \subseteq)$ of all ideals of R satisfies ACC.

Equivalently, all ideals of R admit a finite basis.

Noetherian rings (classical definition)

ACC If $(a_i)_{i \in \mathbb{N}}$ is an weakly increasing sequence, there exists some index $n \in \mathbb{N}$ such that $a_n = a_{n+1} = a_{n+2} = \cdots$

A ring R is said to be Noetherian if the poset $(\mathcal{J}_{\mathsf{R}}, \subseteq)$ of all ideals of R satisfies ACC.

Equivalently, all ideals of R admit a finite basis.

The key result of the theory of Noetherian rings is the following theorem.

Noether's theorem If R is a Noetherian ring, then so is R[X].

From the constructive point of view...

...what does that mean?

First thing to do: Replace the set of all ideals of the ring R by the set of finitely generated ideals.

From the constructive point of view...

...what does that mean?

First thing to do: Replace the set of all ideals of the ring R by the set of finitely generated ideals.

Even with this restriction, the rings $\mathbb{Z}$ or $\mathbb{Q}$ fail to be Noetherian.

From the constructive point of view...

...what does that mean?

First thing to do: Replace the set of all ideals of the ring R by the set of finitely generated ideals.

Even with this restriction, the rings $\mathbb{Z}$ or $\mathbb{Q}$ fail to be Noetherian.

It is worth remarking that the proof of Noether's Theroem is constructive; the point is that the only ring which verifies constructively the hypotheses is the trivial ring $\{0\}$.

We need a new definition for Noetherian.

The key criteria for a good new definition of Noetherian rings are the following:

- It must be, from the point of view of classical mathematics, equivalent to the classical definition.
- It must hold, from the constructive point of view, at least for fields and for most usual Noetherian rings.
- One must be able to prove constructively that if it holds for a ring R, it is inherited by $R[X]$.

Richman/Seidenberg

In 1974, Fred Richman and Abraham Seidenberg gave the following version of the ascending chain condition.

RS If $(a_i)_{i\in\mathbb{N}}$ is a weakly increasing sequence, there exists some index $n \in \mathbb{N}$ such that $a_n = a_{n+1}$.

From the classical viewpoint the two conditions ACC and RS are equivalent.

Richman/Seidenberg

In 1974, Fred Richman and Abraham Seidenberg gave the following version of the ascending chain condition.

RS If $(a_i)_{i\in\mathbb{N}}$ is a weakly increasing sequence, there exists some index $n \in \mathbb{N}$ such that $a_n = a_{n+1}$.

From the classical viewpoint the two conditions ACC and RS are equivalent.

Definition Let R be a ring; the set of finitely generated ideals of R is denoted $\mathcal{J}_{\mathsf{R}}$. The ring R is said to be RS–Noetherian if the poset $(\mathcal{J}_{\mathsf{R}}, \subseteq)$ satisfies RS.

The key result If R is coherent and RS–Noetherian, so is R[X]. Moreover, if R is strongly discrete, so is R[X].

A ring R is coherent if for all $a_1, \ldots, a_n \in \mathsf{R}$, the kernel of the map

$$\begin{array}{ccc} \mathsf{R}^n & \longrightarrow & \mathsf{R} \\ (x_1, \ldots, x_n) & \mapsto & a_1 \cdot x_1 + \cdots + a_n \cdot x_n \end{array}$$

is finitely generated. This submodule of R^n is the syzygy module of the ideal $\langle a_1, \ldots, a_n \rangle \in \mathcal{I}_{\mathsf{R}}$.

The ring R is said to be strongly discrete if, given $a_1, \ldots, a_n$ and x in R, one can decide whether $x \in \langle a_1, \ldots, a_n \rangle$ or not.

Note that in classical math both of these statements hold for any Noetherian ring.

A property of Noetherian rings

Theorem Let I be an ideal in a Noetherian ring R. There exists finitely many prime ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_q$ containing I, s.t. if $\mathfrak{P}$ is a prime ideal containing I, there exists i s.t. $I \subseteq \mathfrak{P}_i \subseteq \mathfrak{P}$.

A property of Noetherian rings

Theorem Let I be an ideal in a Noetherian ring R. There exists finitely many prime ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_q$ containing I, s.t. if $\mathfrak{P}$ is a prime ideal containing I, there exists i s.t. $\mathsf{I} \subseteq \mathfrak{P}_i \subseteq \mathfrak{P}$.

Classical Algebra

Let $\mathfrak{F}$ be the family of all ideals not satisfying this property. R is Noetherian, so if $\mathfrak{F}$ is nonempty we can choose a maximal element I in $\mathfrak{F}$. I is in $\mathfrak{F}$, so it is not prime; take $a, b \in \mathsf{R}$ s.t. $ab \in \mathsf{I}$ and $a, b \notin \mathsf{I}$.

A property of Noetherian rings

Theorem Let I be an ideal in a Noetherian ring R. There exists finitely many prime ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_q$ containing I, s.t. if $\mathfrak{P}$ is a prime ideal containing I, there exists i s.t. $\mathsf{I} \subseteq \mathfrak{P}_i \subseteq \mathfrak{P}$.

Classical Algebra

Let $\mathfrak{F}$ be the family of all ideals not satisfying this property. R is Noetherian, so if $\mathfrak{F}$ is nonempty we can choose a maximal element I in $\mathfrak{F}$. I is in $\mathfrak{F}$, so it is not prime; take $a, b \in \mathsf{R}$ s.t. $ab \in \mathsf{I}$ and $a, b \notin \mathsf{I}$.

The ideals $\mathsf{I} + a\mathsf{R}$ and $\mathsf{I} + b\mathsf{R}$ are strictly greater than I, hence not in $\mathfrak{F}$; there exists finitely many primes $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ and $\mathfrak{P}_{r+1}, \ldots, \mathfrak{P}_q$ containing each, with the property stated in the lemma.

A property of Noetherian rings

Theorem Let I be an ideal in a Noetherian ring R. There exists finitely many prime ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_q$ containing I, s.t. if $\mathfrak{P}$ is a prime ideal containing I, there exists i s.t. $\mathsf{I} \subseteq \mathfrak{P}_i \subseteq \mathfrak{P}$.

Classical Algebra

Let $\mathfrak{F}$ be the family of all ideals not satisfying this property. R is Noetherian, so if $\mathfrak{F}$ is nonempty we can choose a maximal element I in $\mathfrak{F}$. I is in $\mathfrak{F}$, so it is not prime; take $a, b \in \mathsf{R}$ s.t. $ab \in \mathsf{I}$ and $a, b \notin \mathsf{I}$.

The ideals $\mathsf{I} + a\mathsf{R}$ and $\mathsf{I} + b\mathsf{R}$ are strictly greater than I, hence not in $\mathfrak{F}$; there exists finitely many primes $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ and $\mathfrak{P}_{r+1}, \ldots, \mathfrak{P}_q$ containing each, with the property stated in the lemma.

Any prime ideal $\mathfrak{P}$ above I contains $\mathsf{I} + a\mathsf{R}$ or $\mathsf{I} + b\mathsf{R}$, so contains one of the $\mathfrak{P}_1, \ldots, \mathfrak{P}_q$; this is a contradiction, so $\mathfrak{F}$ is empty.

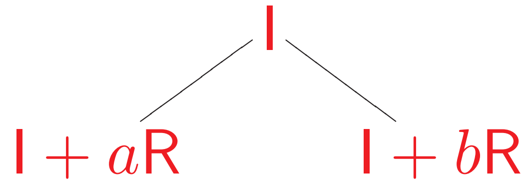
Computer Algebra

We say that we have a strong primality test in R if we can decide whether a finitely generated ideal I of R is prime or not, and if not, to produce $a, b \in$ R s.t. $ab \in$ I and $a, b \notin$ I.

Computer Algebra

We say that we have a strong primality test in R if we can decide whether a finitely generated ideal I of R is prime or not, and if not, to produce $a, b \in \mathsf{R}$ s.t. $ab \in \mathsf{I}$ and $a, b \notin \mathsf{I}$.

Algorithm Let I be an ideal. If I is prime, let $\mathfrak{P}_1 = \mathsf{I}$ and we are done. If not, let $a, b \in \mathsf{R}$ s.t. $ab \in \mathsf{I}$ and $a, b \notin \mathsf{I}$. Begin to construct the following tree:

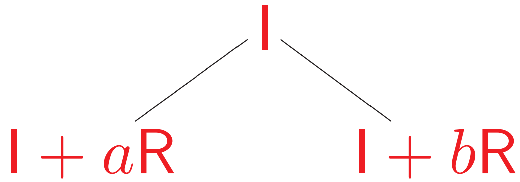


and apply the test to each leaf of the tree.

Computer Algebra

We say that we have a strong primality test in R if we can decide whether a finitely generated ideal I of R is prime or not, and if not, to produce $a, b \in$ R s.t. $ab \in$ I and $a, b \notin$ I.

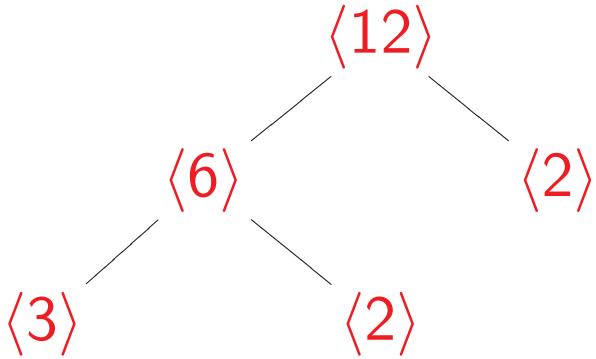
Algorithm Let I be an ideal. If I is prime, let $\mathfrak{P}_1 =$ I and we are done. If not, let $a, b \in$ R s.t. $ab \in$ I and $a, b \notin$ I. Begin to construct the following tree:



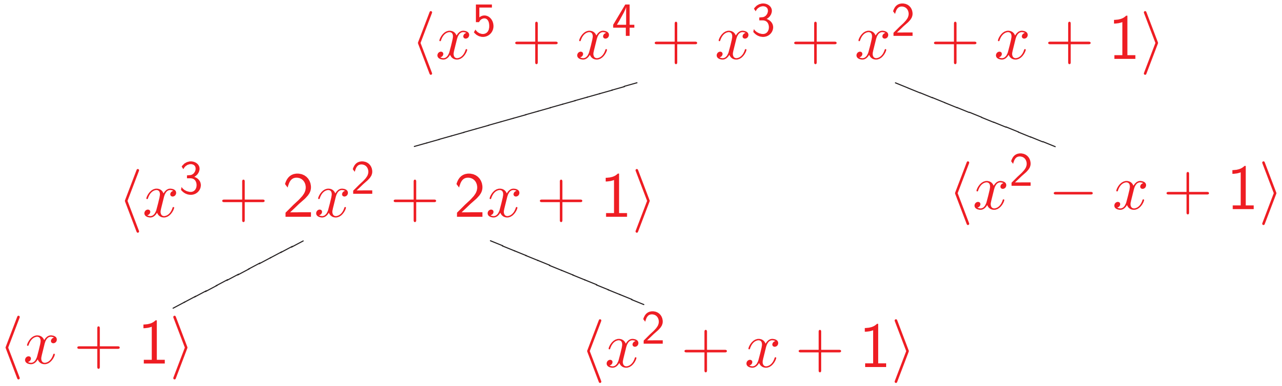
and apply the test to each leaf of the tree.

In this way, we construct a binary tree, with nodes labelled by ideals of R, such that, along each branch of it, there is an increasing sequence of ideals. Then each branch is finite; so the tree is finite. The ideals labelling the leaves of this tree are the minimal primes containing I.

Examples Ideals of $\mathbb{Z}$:



and ideals of $\mathbb{Q}[x]$:



Constructive Algebra

The Richman/Seidenberg theory of Noetherian rings allows to prove, for a wide class of rings, that the branches of our binary tree are finite.

We now need to use Fan Theorem to conclude that the tree is finite!

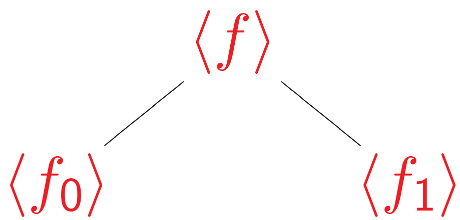
Constructive Algebra

The Richman/Seidenberg theory of Noetherian rings allows to prove, for a wide class of rings, that the branches of our binary tree are finite.

We now need to use Fan Theorem to conclude that the tree is finite!

In the case $\mathsf{R} = \mathbb{Q}[x]$ this can be proved directly by induction on the degree of the polynomial generating the ideal.

If $\mathsf{I} = \langle f \rangle$, and $n = \deg f$, the tree starts like



with $\deg f_0 < n$ and $\deg f_1 < n$. By induction, the two subtrees starting by $\langle f_0 \rangle$ and $\langle f_1 \rangle$ are finite, and so is this tree.

The same proof can be done for ideals of $\mathbb{Z}$, replacing the degree by $\langle a \rangle \mapsto \mid a \mid$.

A possible solution: strongly Noetherian rings

Definition Let $(\mathsf{E}, \leq)$ be a poset. A subset H of E is hereditary if

$$\forall x, \left(\{y \,:\, y < x\} \subseteq \mathsf{H} \Longrightarrow x \in \mathsf{H} \right).$$

The poset E is well-founded if the only hereditary subset of E is $\mathsf{H} = \mathsf{E}$.

A totally ordered well-founded set is well-ordered.

A possible solution: strongly Noetherian rings

Definition Let $(\mathsf{E}, \leq)$ be a poset. A subset H of E is hereditary if

$$\forall x, \left(\{y \ : \ y < x\} \subseteq \mathsf{H} \Longrightarrow x \in \mathsf{H} \right).$$

The poset E is well-founded if the only hereditary subset of E is $\mathsf{H} = \mathsf{E}$.

A totally ordered well-founded set is well-ordered.

Example The sets $(\mathbb{N}, \leq)$ is well-ordered. The sets $(\mathbb{N}^d, \leq_{\mathsf{lex}})$ are well ordered. If $(\mathsf{E}, \leq)$ is well-ordered then so is $\mathsf{E} \cup \{+\infty\}$.

A possible solution: strongly Noetherian rings

Definition Let $(\mathsf{E}, \leq)$ be a poset. A subset H of E is hereditary if

$$\forall x, \ (\{y \ : \ y < x\} \subseteq \mathsf{H} \Longrightarrow x \in \mathsf{H}) .$$

The poset E is well-founded if the only hereditary subset of E is $\mathsf{H} = \mathsf{E}$.

A totally ordered well-founded set is well-ordered.

Example The sets $(\mathbb{N}, \leq)$ is well-ordered. The sets $(\mathbb{N}^d, \leq_{\mathsf{lex}})$ are well ordered. If $(\mathsf{E}, \leq)$ is well-ordered then so is $\mathsf{E} \cup \{+\infty\}$.

Definition Let $(\mathsf{E}, \leq)$ be a poset; the condition $\mathsf{STRONG}(\mathsf{E})$ holds if there exists (explicitly) an increasing map ϕ from $(\mathcal{I}_{\mathsf{R}}, \subseteq)$ to a well-ordered set $(\mathsf{E}, \leq)$.

Definition A strongly discrete and coherent ring R is strongly Noetherian if the poset $\mathsf{STRONG}(\mathcal{I}_{\mathsf{R}}, \supseteq)$ holds.

Remark If R is a strongly Noetherian ring, then the poset $(\mathcal{I}_{\mathsf{R}}, \supseteq)$ is well-founded.

Examples

- The ring $\mathbb{Z}$ is strongly noetherian: each finitely generated ideal is principal, so we map $\mathcal{I}_{\mathbb{Z}}$ to $\mathbb{N} \cup \{+\infty\}$, by $(0) \mapsto +\infty$ and for $a \neq 0$, $(a) \mapsto |\, a \,|$.
- Let F be a (discrete) field. The ring F[X] is strongly Noetherian; again, we map $\mathcal{I}_{\mathsf{F[X]}}$ to $\mathbb{N} \cup \{+\infty\}$, by $(0) \mapsto +\infty$ and for $f \neq 0$, $(f) \mapsto \deg f$.

Examples

- The ring $\mathbb{Z}$ is strongly noetherian: each finitely generated ideal is principal, so we map $\mathcal{I}_{\mathbb{Z}}$ to $\mathbb{N} \cup \{+\infty\}$, by $(0) \mapsto +\infty$ and for $a \neq 0$, $(a) \mapsto |\, a\,|$.
- Let F be a (discrete) field. The ring F[X] is strongly Noetherian; again, we map $\mathcal{I}_{\mathsf{F[X]}}$ to $\mathbb{N} \cup \{+\infty\}$, by $(0) \mapsto +\infty$ and for $f \neq 0$, $(f) \mapsto \deg f$.

Application In a strongly noetherian ring, we can use induction on $\phi(\mathsf{I})$. This applies to our tree problem.

Examples

- The ring $\mathbb{Z}$ is strongly noetherian: each finitely generated ideal is principal, so we map $\mathcal{I}_{\mathbb{Z}}$ to $\mathbb{N} \cup \{+\infty\}$, by $(0) \mapsto +\infty$ and for $a \neq 0$, $(a) \mapsto |\, a \,|$.
- Let F be a (discrete) field. The ring $\mathsf{F[X]}$ is strongly Noetherian; again, we map $\mathcal{I}_{\mathsf{F[X]}}$ to $\mathbb{N} \cup \{+\infty\}$, by $(0) \mapsto +\infty$ and for $f \neq 0$, $(f) \mapsto \deg f$.

Application In a strongly noetherian ring, we can use induction on $\phi(\mathsf{I})$. This applies to our tree problem.

The key result If R is a coherent, strongly discrete and strongly Noetherian ring, so is $\mathsf{R[X]}$.

An other possible solution: a restricted fan condition

Let E be a poset. A finitely branching tree T with nodes labelled by elements of a poset E is said to be non-increasing (resp. decreasing) in E if the labelling $\phi : T \longrightarrow E$ is a non-increasing (resp. decreasing) map.

An other possible solution: a restricted fan condition

Let E be a poset. A finitely branching tree T with nodes labelled by elements of a poset E is said to be non-increasing (resp. decreasing) in E if the labelling $\phi : T \longrightarrow E$ is a non-increasing (resp. decreasing) map.

Such a tree is said to have depth lower than N (where N is a natural number) if along each branch of length greater than N, there are two consective nodes labelled with the same element of E.

An other possible solution: a restricted fan condition

Let E be a poset. A finitely branching tree T with nodes labelled by elements of a poset E is said to be non-increasing (resp. decreasing) in E if the labelling $\phi : T \longrightarrow E$ is a non-increasing (resp. decreasing) map.

Such a tree is said to have depth lower than N (where N is a natural number) if along each branch of length greater than N, there are two consective nodes labelled with the same element of E.

We say that FAN(E) holds if, and only if, every non-increasing finitely branching tree T labelled with has a finite depth.

Note that in the particular case of a decreasing tree T in E, FAN(E) implies that all branches of the tree have length smaller than N.

Fan-Noetherian rings

Definition A strongly discrete coherent ring R is FAN-Noetherian if $\mathrm{FAN}(\mathcal{I}_R, \supseteq)$ holds.

Fan-Noetherian rings

Definition A strongly discrete coherent ring R is FAN-Noetherian if $\mathrm{FAN}(\mathcal{I}_R, \supseteq)$ holds.

The key result If R is a coherent, strongly discrete and FAN-Noetherian ring, so is $R[X]$.

Fan-Noetherian rings

Definition A strongly discrete coherent ring R is FAN-Noetherian if $\mathrm{FAN}(\mathcal{I}_R, \supseteq)$ holds.

The key result If R is a coherent, strongly discrete and FAN-Noetherian ring, so is $R[X]$.

...the proofs of all these "key results" are very similar.

Is it possible to save some work here?

Acceptable properties

Let $(\mathsf{E}_i, \leq_i)_{i \in \mathsf{I}}$ be a family of posets, indexed by a poset $(\mathsf{I}, \leq)$. We denote by $\sum_{i \in \mathsf{I}} \mathsf{E}_i$ the disjoint union of the E_i's ordered by

$$x \in \mathsf{E}_i \preceq y \in \mathsf{E}_j \iff i < j \text{ or } i = j \wedge x \leq_i y\,.$$

Acceptable properties

Let $(\mathsf{E}_i, \leq_i)_{i \in \mathsf{I}}$ be a family of posets, indexed by a poset $(\mathsf{I}, \leq)$. We denote by $\sum_{i \in \mathsf{I}} \mathsf{E}_i$ the disjoint union of the E_i's ordered by

$$x \in \mathsf{E}_i \preceq y \in \mathsf{E}_j \iff i < j \text{ or } i = j \wedge x \leq_i y\,.$$

Let $\mathcal{P}$ be a property of posets (is E is a poset, $\mathcal{P}(\mathsf{E})$ may or may not hold constructively). It is an acceptable property if the following hold:

Acceptable properties

Let $(\mathsf{E}_i, \leq_i)_{i \in \mathsf{I}}$ be a family of posets, indexed by a poset $(\mathsf{I}, \leq)$. We denote by $\sum_{i \in \mathsf{I}} \mathsf{E}_i$ the disjoint union of the E_i's ordered by

$$x \in \mathsf{E}_i \preceq y \in \mathsf{E}_j \iff i < j \text{ or } i = j \wedge x \leq_i y \,.$$

Let $\mathcal{P}$ be a property of posets (is E is a poset, $\mathcal{P}(\mathsf{E})$ may or may not hold constructively). It is an acceptable property if the following hold:

- $\mathcal{P}(\mathsf{E}) \Longrightarrow \textsc{rs}(\mathsf{E})$.
- If there is an increasing map from E to F and $\mathcal{P}(\mathsf{F})$ holds, then $\mathcal{P}(\mathsf{E})$ holds.
- If $(\mathsf{E}_i, \leq_i)_{i \in \mathsf{I}}$ if family of posets, such that $\mathcal{P}(\mathsf{I})$ holds and for all i, $\mathcal{P}(\mathsf{E}_i)$ holds. Then $\mathcal{P}(\sum_{i \in \mathsf{I}} \mathsf{E}_i)$ holds.
- $\mathcal{P}(\mathbb{N})$ holds constructively.

The key of all key results

Let $\mathcal{P}$ be an acceptable property. A ring R is $\mathcal{P}$-noetherian if $\mathcal{P}(\mathcal{I}_{\mathsf{R}}, \supseteq)$ holds.

The key of all key results

Let $\mathcal{P}$ be an acceptable property. A ring R is $\mathcal{P}$-noetherian if $\mathcal{P}(\mathcal{I}_R, \supseteq)$ holds.

If R is a coherent, strongly discrete and $\mathcal{P}$-Noetherian ring, so is $R[X]$.

The ideas of the proof

Let M be a coherent R-module and N a R-submodule of M. There is an increasing map from $\mathcal{J}_{\mathsf{M}}$ to $\mathcal{J}_{\mathsf{M}/\mathsf{N}} \times \mathcal{J}_{\mathsf{N}}$ (ordered by the product order).

For all $\mathsf{I} \in \mathcal{J}_{\mathsf{R}[\mathsf{X}]}$ we define $n(\mathsf{I})$ as the smallest integer such that $\mathsf{I} \cap \mathsf{R}[\mathsf{X}]_{n(\mathsf{I})}$ generates I as an ideal.

Let Θ be the following map

$$\begin{array}{rccc} \Theta \ : & \mathcal{J}_{\mathsf{R}[\mathsf{X}]} & \longrightarrow & \mathcal{J}_{\mathsf{R}} \times \overleftarrow{\sum_{n \geq 1}} \mathcal{J}_{\mathsf{R}[\mathsf{X}]_n} \\ & \mathsf{I} & \longmapsto & \left(\mathrm{LC}(\mathsf{I}), \mathsf{I} \cap \mathsf{R}[\mathsf{X}]_{n(\mathsf{I})}\right) \ . \end{array}$$

This is a decreasing map – the value set being ordered lexicographically.