Positive-existential definability in Noetherian rings

Laurent Moret-Bailly

IRMAR, Université de Rennes 1
Member of the Eurpoean network *Arithmetic Algebraic Geometry*

ICMS workshop
Number Theory and Computability
June 2007

Summary

Conventions:

- Rings are commutative with unit.
- If R is a ring, we shall consider definability over R with respect to the language $L(R)$ which is the language of rings $(+, ., 0, 1)$, augmented with:

Conventions:

- Rings are commutative with unit.
- If R is a ring, we shall consider definability over R with respect to the language $L(R)$ which is the language of rings $(+, ., 0, 1)$, augmented with:

Conventions:

- Rings are commutative with unit.
- If R is a ring, we shall consider definability over R with respect to the language $L(R)$ which is the language of rings $(+, ., 0, 1)$, augmented with:

Conventions:

- Rings are commutative with unit.
- If R is a ring, we shall consider definability over R with respect to the language $L(R)$ which is the language of rings $(+, ., 0, 1)$, augmented with:
  - one constant for each element of R

Conventions:

- Rings are commutative with unit.
- If R is a ring, we shall consider definability over R with respect to the language $L(R)$ which is the language of rings $(+, ., 0, 1)$, augmented with:
  - one constant for each element of R
  - the logical constant FALSE.

Special subsets:

If R is a ring and $n \in \mathbb{N}$, then:

- *basic algebraic subsets* of R^n are defined by finite systems of polynomial equations, with coefficients in R:

$$\{t \in R^n \mid F_1(t) = \cdots = F_r(t) = 0\}$$

- *algebraic subsets* of R^n are finite unions of basic algebraic subsets
- *constructible subsets* of R^n are finite Boolean combinations of (basic) algebraic subsets
- *positive-existential subsets* of R^n are projections of algebraic subsets of some R^{n+p}
- *existential subsets* of R^n are projections of constructible subsets of some R^{n+p}.

Special subsets:

If R is a ring and $n \in \mathbb{N}$, then:

- *basic algebraic subsets* of R^n are defined by finite systems of polynomial equations, with coefficients in R:

$$\{t \in R^n \mid F_1(t) = \cdots = F_r(t) = 0\}$$

- *algebraic subsets* of R^n are finite unions of basic algebraic subsets
- *constructible subsets* of R^n are finite Boolean combinations of (basic) algebraic subsets
- *positive-existential subsets* of R^n are projections of algebraic subsets of some R^{n+p}
- *existential subsets* of R^n are projections of constructible subsets of some R^{n+p}.

Special subsets:

If R is a ring and $n \in \mathbb{N}$, then:

- *basic algebraic subsets* of R^n are defined by finite systems of polynomial equations, with coefficients in R:

$$\{t \in R^n \mid F_1(t) = \cdots = F_r(t) = 0\}$$

- *algebraic subsets* of R^n are finite unions of basic algebraic subsets
- *constructible subsets* of R^n are finite Boolean combinations of (basic) algebraic subsets
- *positive-existential subsets* of R^n are projections of algebraic subsets of some R^{n+p}
- *existential subsets* of R^n are projections of constructible subsets of some R^{n+p}.

Special subsets:

If R is a ring and $n \in \mathbb{N}$, then:

- *basic algebraic subsets* of R^n are defined by finite systems of polynomial equations, with coefficients in R:

$$\{t \in R^n \mid F_1(t) = \cdots = F_r(t) = 0\}$$

- *algebraic subsets* of R^n are finite unions of basic algebraic subsets
- *constructible subsets* of R^n are finite Boolean combinations of (basic) algebraic subsets
- *positive-existential subsets* of R^n are projections of algebraic subsets of some R^{n+p}
- *existential subsets* of R^n are projections of constructible subsets of some R^{n+p}.

Special subsets:

If R is a ring and $n \in \mathbb{N}$, then:

- *basic algebraic subsets* of R^n are defined by finite systems of polynomial equations, with coefficients in R:

$$\{t \in R^n \mid F_1(t) = \cdots = F_r(t) = 0\}$$

- *algebraic subsets* of R^n are finite unions of basic algebraic subsets
- *constructible subsets* of R^n are finite Boolean combinations of (basic) algebraic subsets
- *positive-existential subsets* of R^n are projections of algebraic subsets of some R^{n+p}
- *existential subsets* of R^n are projections of constructible subsets of some R^{n+p}.

Remarks:

- One can replace “projections” by “images by polynomial maps”.
- If R is a domain, all algebraic sets are basic.
- (Positive-)existential sets are those defined by (positive-)existential formulas in the language $L(R)$.
- The reason for the logical constant FALSE is to make the empty subset of R^n positive-existential when R is the zero ring!

Remarks:

- One can replace "projections" by "images by polynomial maps".
- If R is a domain, all algebraic sets are basic.
- (Positive-)existential sets are those defined by (positive-)existential formulas in the language $L(R)$.
- The reason for the logical constant FALSE is to make the empty subset of R^n positive-existential when R is the zero ring!

Remarks:

- One can replace "projections" by "images by polynomial maps".
- If R is a domain, all algebraic sets are basic.
- (Positive-)existential sets are those defined by (positive-)existential formulas in the language $L(R)$.
- The reason for the logical constant FALSE is to make the empty subset of R^n positive-existential when R is the zero ring!

Remarks:

- One can replace “projections” by “images by polynomial maps”.
- If R is a domain, all algebraic sets are basic.
- (Positive-)existential sets are those defined by (positive-)existential formulas in the language $L(R)$.
- The reason for the logical constant FALSE is to make the empty subset of R^n positive-existential when R is the zero ring!

Remarks:

- One can replace “projections” by “images by polynomial maps”.
- If R is a domain, all algebraic sets are basic.
- (Positive-)existential sets are those defined by (positive-)existential formulas in the language $L(R)$.
- The reason for the logical constant FALSE is to make the empty subset of R^n positive-existential when R is the zero ring!

  (for a nonzero ring, FALSE is equivalent to $1 = 0$)

"Existential" vs. "positive-existential":

Clearly, every positive-existential set is existential.

The converse is true (for given R) if and only if R is "good" in the following sense:

Definition

A ring R is good if

$$R \setminus \{0\} \text{ is positive-existential in } R$$

"Existential" vs. "positive-existential":

Clearly, every positive-existential set is existential.

The converse is true (for given R) if and only if R is "good" in the following sense:

Definition

A ring R is good if

$$R \setminus \{0\} \text{ is positive-existential in } R$$

"Existential" vs. "positive-existential":

Clearly, every positive-existential set is existential.

The converse is true (for given R) if and only if R is "good" in the following sense:

Definition

A ring R is good if

$$R \setminus \{0\} \text{ is positive-existential in } R$$

and is bad otherwise.

Problem:

find useful classes of good (resp. bad) rings

Some examples of good rings:

- Every finite ring is good.
- Every field is good (nonzero = invertible).
- $R_1 \times R_2$ is good iff both R_1 and R_2 are.
- $\mathbb{Z}$ is good:

Some examples of good rings:

- Every finite ring is good.
- Every field is good (nonzero = invertible).
- $R_1 \times R_2$ is good iff both R_1 and R_2 are.
- $\mathbb{Z}$ is good:

Some examples of good rings:

- Every finite ring is good.
- Every field is good (nonzero = invertible).
- $R_1 \times R_2$ is good iff both R_1 and R_2 are.
- $\mathbb{Z}$ is good:

Some examples of good rings:

- Every finite ring is good.
- Every field is good (nonzero = invertible).
- $R_1 \times R_2$ is good iff both R_1 and R_2 are.
- $\mathbb{Z}$ is good:

Some examples of good rings:

- Every finite ring is good.
- Every field is good (nonzero = invertible).
- $R_1 \times R_2$ is good iff both R_1 and R_2 are.
- $\mathbb{Z}$ is good:

Some examples of good rings:

- Every finite ring is good.
- Every field is good (nonzero = invertible).
- $R_1 \times R_2$ is good iff both R_1 and R_2 are.
- $\mathbb{Z}$ is good: for $t \in \mathbb{Z}$, we have

$$t \neq 0 \quad \Leftrightarrow \quad (\exists x)(\exists y)\ t^2 = (1+2x)(1+3y)$$

Some examples of good rings:

- Every finite ring is good.
- Every field is good (nonzero = invertible).
- $R_1 \times R_2$ is good iff both R_1 and R_2 are.
- $\mathbb{Z}$ is good: for $t \in \mathbb{Z}$, we have

$$\begin{aligned} t \neq 0 \quad &\Leftrightarrow \quad (\exists x)(\exists y)\ t^2 = (1+2x)(1+3y) \\ &\Leftrightarrow \quad (\exists w)(\exists x)(\exists y)\ tw = (1+2x)(1+3y). \end{aligned}$$

Some examples of good rings:

- Every finite ring is good.
- Every field is good (nonzero = invertible).
- $R_1 \times R_2$ is good iff both R_1 and R_2 are.
- $\mathbb{Z}$ is good: for $t \in \mathbb{Z}$, we have

$$
\begin{aligned}
t \neq 0 \quad \Leftrightarrow \quad & (\exists x)(\exists y)\ t^2 &= (1+2x)(1+3y) \\
\Leftrightarrow \quad & (\exists w)(\exists x)(\exists y)\ tw &= (1+2x)(1+3y).
\end{aligned}
$$

- In fact, the last formula shows that every ring of algebraic integers is good.

Some examples of bad rings:

- If p is a prime, $\mathbb{Z}_p$ is bad
- More generally, infinite compact topological rings are bad (examples: $\mathbb{F}_p[[t]]$, $\mathbb{F}_p^{\mathbb{N}}$).
- Infinite products of nonzero rings are bad.
- If R is a nonzero ring, and I is an infinite set, then $R[(X_i)_{i \in I}]$ is bad.

Some examples of bad rings:

- If p is a prime, $\mathbb{Z}_p$ is bad
- More generally, infinite compact topological rings are bad (examples: $\mathbb{F}_p[[t]]$, $\mathbb{F}_p^{\mathbb{N}}$).
- Infinite products of nonzero rings are bad.
- If R is a nonzero ring, and I is an infinite set, then $R\,[\,(X_i)_{i\in I}]$ is bad.

Some examples of bad rings:

- If p is a prime, $\mathbb{Z}_p$ is bad (every positive-existential set is p-adically compact).
- More generally, infinite compact topological rings are bad (examples: $\mathbb{F}_p[[t]]$, $\mathbb{F}_p^{\mathbb{N}}$).
- Infinite products of nonzero rings are bad.
- If R is a nonzero ring, and I is an infinite set, then $R\,[\,(X_i)_{i\in I}]$ is bad.

Some examples of bad rings:

- If p is a prime, $\mathbb{Z}_p$ is bad (every positive-existential set is p-adically compact).
- More generally, infinite compact topological rings are bad (examples: $\mathbb{F}_p[[t]]$, $\mathbb{F}_p^{\mathbb{N}}$).
- Infinite products of nonzero rings are bad.
- If R is a nonzero ring, and I is an infinite set, then $R[(X_i)_{i\in I}]$ is bad.

Some examples of bad rings:

- If p is a prime, $\mathbb{Z}_p$ is bad (every positive-existential set is p-adically compact).
- More generally, infinite compact topological rings are bad (examples: $\mathbb{F}_p[[t]]$, $\mathbb{F}_p^{\mathbb{N}}$).
- Infinite products of nonzero rings are bad.
- If R is a nonzero ring, and I is an infinite set, then $R\,[\,(X_i)_{i\in I}]$ is bad.

Some examples of bad rings:

- If p is a prime, $\mathbb{Z}_p$ is bad (every positive-existential set is p-adically compact).
- More generally, infinite compact topological rings are bad (examples: $\mathbb{F}_p[[t]]$, $\mathbb{F}_p^{\mathbb{N}}$).
- Infinite products of nonzero rings are bad.
- If R is a nonzero ring, and I is an infinite set, then $R\,[\,(X_i)_{i\in I}]$ is bad.

Main result for Noetherian domains:

"Most" Noetherian domains are good:

Theorem

Let R be a Noetherian domain.

Main result for Noetherian domains:

"Most" Noetherian domains are good:

Theorem

Let R be a Noetherian domain.

Main result for Noetherian domains:

"Most" Noetherian domains are good:

Theorem

Let R be a Noetherian domain.

If R is not local Henselian, then R is good.

Main result for Noetherian domains:

"Most" Noetherian domains are good:

Theorem

Let R be a Noetherian domain.

If R is not local Henselian, then R is good.

What about other Noetherian rings?

Main result for Noetherian domains:

"Most" Noetherian domains are good:

Theorem

Let R be a Noetherian domain.

If R is not local Henselian, then R is good.

What about other Noetherian rings?

What about the Henselian case?

Other good Noetherian rings:

Proposition

Let R be a Noetherian ring.

Other good Noetherian rings:

Proposition

Let R be a Noetherian ring.

Assume that every quotient domain of R is good.

Other good Noetherian rings:

Proposition

Let R be a Noetherian ring.

Assume that every quotient domain of R is good.

Then R is good. More generally, every ring of fractions $S^{-1}R$ is good.

Corollary

Artin rings are good.

Corollary

Let R be a Noetherian Jacobson ring

Corollary

Artin rings are good.

Proof: every quotient domain of an Artin ring is a field.

Corollary

Let R be a Noetherian Jacobson ring

Corollary

Artin rings are good.

Proof: every quotient domain of an Artin ring is a field.

Corollary

Let R be a Noetherian Jacobson ring.

Corollary

Artin rings are good.

Proof: every quotient domain of an Artin ring is a field.

Corollary

Let R be a Noetherian Jacobson ring
(every prime ideal is an intersection of maximal ideals).

Corollary

Artin rings are good.

Proof: every quotient domain of an Artin ring is a field.

Corollary

Let R be a Noetherian Jacobson ring.

Then every ring of fractions $S^{-1}R$ is good.

Corollary

Artin rings are good.

Proof: every quotient domain of an Artin ring is a field.

Corollary

Let R be a Noetherian Jacobson ring.

Then every ring of fractions $S^{-1}R$ is good.

In particular, if k is a field, every k-algebra essentially of finite type is good.

Local Henselian rings

Let R be local with maximal ideal $\mathfrak{m}$.

Recall that R is Henselian if:

Local Henselian rings

Let R be local with maximal ideal $\mathfrak{m}$.

Recall that R is Henselian if:

for every $F \in R[X]$, every simple root of F in $R/\mathfrak{m}$ lifts to a (unique) root of F in R.

Local Henselian rings

Let R be local with maximal ideal $\mathfrak{m}$.

Recall that R is Henselian if:

for every $F \in R[X]$, every simple root of F in $R/\mathfrak{m}$ lifts to a (unique) root of F in R.

Examples:

Local Henselian rings

Let R be local with maximal ideal $\mathfrak{m}$.

Recall that R is Henselian if:

for every $F \in R[X]$, every simple root of F in $R/\mathfrak{m}$ lifts to a (unique) root of F in R.

Examples:

- complete local rings (by Hensel's lemma)

Local Henselian rings

Let R be local with maximal ideal $\mathfrak{m}$.

Recall that R is Henselian if:

for every $F \in R[X]$, every simple root of F in $R/\mathfrak{m}$ lifts to a (unique) root of F in R.

Examples:

- complete local rings (by Hensel's lemma)
- $\widetilde{\mathbb{Q}} \cap \mathbb{Z}_p$.

Local Henselian rings tend to be bad:

Local Henselian rings tend to be bad:

Assume R is Noetherian, local and Henselian (not necessarily a domain).

Local Henselian rings tend to be bad:

Assume R is Noetherian, local and Henselian (not necessarily a domain).
If $\dim R = 0$ then R is good, so we assume $\dim R > 0$.

Local Henselian rings tend to be bad:

Assume R is Noetherian, local and Henselian (not necessarily a domain).
If $\dim R = 0$ then R is good, so we assume $\dim R > 0$.
Then:

Theorem

Local Henselian rings tend to be bad:

Assume R is Noetherian, local and Henselian (not necessarily a domain).
If $\dim R = 0$ then R is good, so we assume $\dim R > 0$.
Then:

Theorem

If R is excellent, then R is bad.

Local Henselian rings tend to be bad:

Assume R is Noetherian, local and Henselian (not necessarily a domain).
If $\dim R = 0$ then R is good, so we assume $\dim R > 0$.
Then:

Theorem

If R is excellent, then R is bad.

Remarks:

- All complete local rings, and all Noetherian rings "occurring naturally" in algebraic geometry and number theory, are excellent.

Local Henselian rings tend to be bad:

Assume R is Noetherian, local and Henselian (not necessarily a domain).
If $\dim R = 0$ then R is good, so we assume $\dim R > 0$.
Then:

Theorem

If R is excellent, then R is bad.

Remarks:

- All complete local rings, and all Noetherian rings "occurring naturally" in algebraic geometry and number theory, are excellent.
- There is a (non-excellent) Henselian discrete valuation ring which is good.

Rings of analytic functions:

Theorem

Let X be a reduced irreducible Stein analytic space.

Rings of analytic functions:

Theorem

Let X be a reduced irreducible Stein analytic space

(e.g. a polydisk)

Rings of analytic functions:

Theorem

Let X be a reduced irreducible Stein analytic space.

Then the ring $\mathcal{H}(X)$ of holomorphic functions on X is good.

Some elementary facts:

- If I is a finitely generated ideal of R and R/I is good, then $R \setminus I$ is positive-existential in R.

- ("Weil restriction") If some nonzero finite free R-algebra is good, then R is good.

Some elementary facts:

- If I is a finitely generated ideal of R and R/I is good, then $R \setminus I$ is positive-existential in R.
- ("Weil restriction") If some nonzero finite free R-algebra is good, then R is good.

The "Two Ideals" Lemma

(generalizing results of A. Shlapentokh and J. Demeyer)

Lemma

Let R be a Noetherian domain, and let $\mathfrak{p}$ and $\mathfrak{q}$ be two prime ideals of R. Assume that:

Then R is good.

The "Two Ideals" Lemma

(generalizing results of A. Shlapentokh and J. Demeyer)

Lemma

Let R be a Noetherian domain, and let $\mathfrak{p}$ and $\mathfrak{q}$ be two prime ideals of R. Assume that:

- $\mathfrak{p} \cap \mathfrak{q}$ *contains no nonzero prime.*

Then R is good.

The "Two Ideals" Lemma

(generalizing results of A. Shlapentokh and J. Demeyer)

Lemma

Let R be a Noetherian domain, and let $\mathfrak{p}$ and $\mathfrak{q}$ be two prime ideals of R. Assume that:

- $\mathfrak{p} \cap \mathfrak{q}$ *contains no nonzero prime*
  (e.g. $\mathfrak{p}$ has height 1 and $\mathfrak{p} \not\subset \mathfrak{q}$).

Then R is good.

The "Two Ideals" Lemma

(generalizing results of A. Shlapentokh and J. Demeyer)

Lemma

Let R be a Noetherian domain, and let $\mathfrak{p}$ and $\mathfrak{q}$ be two prime ideals of R. Assume that:

- $\mathfrak{p} \cap \mathfrak{q}$ *contains no nonzero prime.*
- $R/\mathfrak{p}$ *and* $R/\mathfrak{q}$ *are good.*

Then R is good.

The "Two Ideals" Lemma

(generalizing results of A. Shlapentokh and J. Demeyer)

Lemma

Let R be a Noetherian domain, and let $\mathfrak{p}$ and $\mathfrak{q}$ be two prime ideals of R. Assume that:

- $\mathfrak{p} \cap \mathfrak{q}$ *contains no nonzero prime.*
- $R/\mathfrak{p}$ *and* $R/\mathfrak{q}$ *are good.*

Then R is good.

Explicitly, for $t \in R$, we have $t \neq 0$ if and only if
(some multiple of t)=(some $x \notin \mathfrak{p}$)(some $y \notin \mathfrak{q}$)

The "Two Ideals" Lemma

(generalizing results of A. Shlapentokh and J. Demeyer)

Lemma

Let R be a Noetherian domain, and let $\mathfrak{p}$ and $\mathfrak{q}$ be two prime ideals of R. Assume that:

- *$\mathfrak{p} \cap \mathfrak{q}$ contains no nonzero prime.*
- *$R/\mathfrak{p}$ and $R/\mathfrak{q}$ are good.*

Then R is good.

Explicitly, for $t \in R$, we have $t \neq 0$ if and only if
(some multiple of t)=(some $x \notin \mathfrak{p}$)(some $y \notin \mathfrak{q}$)
and the conditions $x \notin \mathfrak{p}$ and $y \notin \mathfrak{q}$ are positive-existential.

Corollary

If k is a good (Noetherian) domain, then $k[X]$ is good.

Proof: Apply the lemma with $R = k[X]$, $\mathfrak{p} = (X)$, $\mathfrak{q} = (X - 1)$: then

- $\mathfrak{p} \cap \mathfrak{q} = X(X - 1)R$ contains no nonzero prime,
- $R/\mathfrak{p}$ and $R/\mathfrak{q}$ are both isomorphic to k.

Remark: the Noetherian assumption is in fact not needed.

Corollary

If k is a good (Noetherian) domain, then $k[X]$ is good.

Proof: Apply the lemma with $R = k[X]$, $\mathfrak{p} = (X)$, $\mathfrak{q} = (X - 1)$: then

- $\mathfrak{p} \cap \mathfrak{q} = X(X - 1)R$ contains no nonzero prime,
- $R/\mathfrak{p}$ and $R/\mathfrak{q}$ are both isomorphic to k.

Remark: the Noetherian assumption is in fact not needed.

Corollary

If k is a good (Noetherian) domain, then $k[X]$ is good.

Proof: Apply the lemma with $R = k[X]$, $\mathfrak{p} = (X)$, $\mathfrak{q} = (X - 1)$: then

- $\mathfrak{p} \cap \mathfrak{q} = X(X - 1)R$ contains no nonzero prime,
- $R/\mathfrak{p}$ and $R/\mathfrak{q}$ are both isomorphic to k.

Remark: the Noetherian assumption is in fact not needed.

One cannot apply the “Two Ideals” lemma directly if (for example) R is a one-dimensional local domain.

In such cases, one can try to replace R by a finite free R-algebra which has “more” primes.

For instance, if $R = \mathbb{Z}_{(2)}$, the ring $S = R[X]/(X^2 + X + 2)$ is free of rank 2 over R and has two maximal ideals ($X^2 + X + 2$ has two simple roots mod 2).

The lemma then implies that S is good, hence so is R by Weil restriction.

One cannot apply the “Two Ideals” lemma directly if (for example) R is a one-dimensional local domain.

In such cases, one can try to replace R by a finite free R-algebra which has “more” primes.

For instance, if $R = \mathbb{Z}_{(2)}$, the ring $S = R[X]/(X^2 + X + 2)$ is free of rank 2 over R and has two maximal ideals ($X^2 + X + 2$ has two simple roots mod 2).

The lemma then implies that S is good, hence so is R by Weil restriction.

One cannot apply the "Two Ideals" lemma directly if (for example) R is a one-dimensional local domain.

In such cases, one can try to replace R by a finite free R-algebra which has "more" primes.

For instance, if $R = \mathbb{Z}_{(2)}$, the ring $S = R[X]/(X^2 + X + 2)$ is free of rank 2 over R and has two maximal ideals ($X^2 + X + 2$ has two simple roots mod 2).

The lemma then implies that S is good, hence so is R by Weil restriction.

One cannot apply the “Two Ideals” lemma directly if (for example) R is a one-dimensional local domain.

In such cases, one can try to replace R by a finite free R-algebra which has “more” primes.

For instance, if $R = \mathbb{Z}_{(2)}$, the ring $S = R[X]/(X^2 + X + 2)$ is free of rank 2 over R and has two maximal ideals ($X^2 + X + 2$ has two simple roots mod 2).

The lemma then implies that S is good, hence so is R by Weil restriction.

One cannot apply the “Two Ideals” lemma directly if (for example) R is a one-dimensional local domain.

In such cases, one can try to replace R by a finite free R-algebra which has “more” primes.

For instance, if $R = \mathbb{Z}_{(2)}$, the ring $S = R[X]/(X^2 + X + 2)$ is free of rank 2 over R and has two maximal ideals ($X^2 + X + 2$ has two simple roots mod 2).

The lemma then implies that S is good, hence so is R by Weil restriction.

One cannot apply the “Two Ideals” lemma directly if (for example) R is a one-dimensional local domain.

In such cases, one can try to replace R by a finite free R-algebra which has “more” primes.

For instance, if $R = \mathbb{Z}_{(2)}$, the ring $S = R[X]/(X^2 + X + 2)$ is free of rank 2 over R and has two maximal ideals ($X^2 + X + 2$ has two simple roots mod 2).

The lemma then implies that S is good, hence so is R by Weil restriction.

One cannot apply the “Two Ideals” lemma directly if (for example) R is a one-dimensional local domain.

In such cases, one can try to replace R by a finite free R-algebra which has “more” primes.

For instance, if $R = \mathbb{Z}_{(2)}$, the ring $S = R[X]/(X^2 + X + 2)$ is free of rank 2 over R and has two maximal ideals ($X^2 + X + 2$ has two simple roots mod 2).

The lemma then implies that S is good, hence so is R by Weil restriction.

Note: the trick does not work if $R = \mathbb{Z}_2$

One cannot apply the "Two Ideals" lemma directly if (for example) R is a one-dimensional local domain.

In such cases, one can try to replace R by a finite free R-algebra which has "more" primes.

For instance, if $R = \mathbb{Z}_{(2)}$, the ring $S = R[X]/(X^2 + X + 2)$ is free of rank 2 over R and has two maximal ideals ($X^2 + X + 2$ has two simple roots mod 2).

The lemma then implies that S is good, hence so is R by Weil restriction.

Note: the trick does not work if $R = \mathbb{Z}_2$ because S is no longer a domain!

One cannot apply the “Two Ideals” lemma directly if (for example) R is a one-dimensional local domain.

In such cases, one can try to replace R by a finite free R-algebra which has “more” primes.

For instance, if $R = \mathbb{Z}_{(2)}$, the ring $S = R[X]/(X^2 + X + 2)$ is free of rank 2 over R and has two maximal ideals ($X^2 + X + 2$ has two simple roots mod 2).

The lemma then implies that S is good, hence so is R by Weil restriction.

Note: the trick does not work if $R = \mathbb{Z}_2$ because S is no longer a domain!

Of course, this method can be used in other situations:

The "Doubling Lemma"

Lemma

Let R be a Noetherian domain with fraction field K. Let $\mathfrak{p} \subset R$ be a nonzero prime ideal.

Exclude the case where R is local with maximal ideal $\mathfrak{p}$.

Then there exists a polynomial

$$F = X^2 + aX + b \in R[X]$$

such that $a \notin \mathfrak{p}$, $b \in \mathfrak{p}$, and F is irreducible in $K[X]$.

In particular, the R-algebra $S := R[X]/(F)$ has the following properties:

- *S is a domain,*
- *S is free of rank 2 as an R-module,*
- *S has two prime ideals above $\mathfrak{p}$, with quotients both isomorphic to $R/\mathfrak{p}$.*

The "Doubling Lemma"

Lemma

Let R be a Noetherian domain with fraction field K. Let $\mathfrak{p} \subset R$ be a nonzero prime ideal.

Exclude the case where R is local with maximal ideal $\mathfrak{p}$.

Then there exists a polynomial

$$F = X^2 + aX + b \in R[X]$$

such that $a \notin \mathfrak{p}$, $b \in \mathfrak{p}$, and F is irreducible in $K[X]$.

In particular, the R-algebra $S := R[X]/(F)$ has the following properties:

- *S is a domain,*
- *S is free of rank 2 as an R-module,*
- *S has two prime ideals above $\mathfrak{p}$, with quotients both isomorphic to $R/\mathfrak{p}$.*

The "Doubling Lemma"

Lemma

Let R be a Noetherian domain with fraction field K. Let $\mathfrak{p} \subset R$ be a nonzero prime ideal.

Exclude the case where R is local with maximal ideal $\mathfrak{p}$.

Then there exists a polynomial

$$F = X^2 + aX + b \in R[X]$$

such that $a \notin \mathfrak{p}$, $b \in \mathfrak{p}$, and F is irreducible in $K[X]$.

In particular, the R-algebra $S := R[X]/(F)$ has the following properties:

- *S is a domain,*
- *S is free of rank 2 as an R-module,*
- *S has two prime ideals above $\mathfrak{p}$, with quotients both isomorphic to $R/\mathfrak{p}$.*

The "Doubling Lemma"

Lemma

Let R be a Noetherian domain with fraction field K. Let $\mathfrak{p} \subset R$ be a nonzero prime ideal.

Exclude the case where R is local with maximal ideal $\mathfrak{p}$.

Then there exists a polynomial

$$F = X^2 + aX + b \in R[X]$$

such that $a \notin \mathfrak{p}$, $b \in \mathfrak{p}$, and F is irreducible in $K[X]$.

In particular, the R-algebra $S := R[X]/(F)$ has the following properties:

- *S is a domain,*
- *S is free of rank 2 as an R-module,*
- *S has two prime ideals above $\mathfrak{p}$, with quotients both isomorphic to $R/\mathfrak{p}$.*

The "Doubling Lemma"

Lemma

Let R be a Noetherian domain with fraction field K. Let $\mathfrak{p} \subset R$ be a nonzero prime ideal.

Exclude the case where R is local with maximal ideal $\mathfrak{p}$.

Then there exists a polynomial

$$F = X^2 + aX + b \in R[X]$$

such that $a \notin \mathfrak{p}$, $b \in \mathfrak{p}$, and F is irreducible in $K[X]$.

In particular, the R-algebra $S := R[X]/(F)$ has the following properties:

- *S is a domain,*
- *S is free of rank 2 as an R-module,*
- *S has two prime ideals above $\mathfrak{p}$, with quotients both isomorphic to $R/\mathfrak{p}$.*

The non-local case

Combining the Two Ideals Lemma, the Doubling Lemma, and an induction on dimension, one obtains:

Proposition

Let R be a Noetherian domain, $\mathfrak{p}$ a prime ideal of R.
Exclude the case where R is local with maximal ideal $\mathfrak{p}$.
If $R/\mathfrak{p}$ is good, then R is good.

Corollary

Every non-local Noetherian domain is good.

Proof: apply the proposition to any maximal ideal of R.

The non-local case

Combining the Two Ideals Lemma, the Doubling Lemma, and an induction on dimension, one obtains:

Proposition

Let R be a Noetherian domain, $\mathfrak{p}$ a prime ideal of R.
Exclude the case where R is local with maximal ideal $\mathfrak{p}$.
If $R/\mathfrak{p}$ is good, then R is good.

Corollary

Every non-local Noetherian domain is good.

Proof: apply the proposition to any maximal ideal of R.

The non-local case

Combining the Two Ideals Lemma, the Doubling Lemma, and an induction on dimension, one obtains:

Proposition

Let R be a Noetherian domain, $\mathfrak{p}$ a prime ideal of R.

Exclude the case where R is local with maximal ideal $\mathfrak{p}$.

If $R/\mathfrak{p}$ is good, then R is good.

Corollary

Every non-local Noetherian domain is good.

Proof: apply the proposition to any maximal ideal of R.

The non-Henselian case

If R is a local, non-Henselian Noetherian domain, there exists a finite R-algebra S which is a non-local domain, hence good.

The non-Henselian case

If R is a local, non-Henselian Noetherian domain, there exists a finite R-algebra S which is a non-local domain, hence good.

The non-Henselian case

If R is a local, non-Henselian Noetherian domain, there exists a finite R-algebra S which is a non-local domain, hence good.

The non-Henselian case

If R is a local, non-Henselian Noetherian domain, there exists a finite R-algebra S which is a non-local domain, hence good.

Using Weil restriction, one concludes that R is also good.

The non-Henselian case

If R is a local, non-Henselian Noetherian domain, there exists a finite R-algebra S which is a non-local domain, hence good.

Using Weil restriction, one concludes that R is also good.

(Some care is needed because S is not necessarily a free R-module).

Approximation properties and the Henselian case

Notation:

Assume

- R is a ring,
- S is a finite system of polynomial equations with coefficients in R,
- A is an R-algebra.

Then we denote by $\mathrm{sol}(S, A)$ the set of A-valued solutions of S.

Notation:

Assume

- R is a ring,
- S is a finite system of polynomial equations with coefficients in R,
- A is an R-algebra.

Then we denote by $\mathrm{sol}(S, A)$ the set of A-valued solutions of S.

Let R be a ring and I an ideal of R. We say that (R, I) satisfies the infinitesimal Hasse principle (IHP) if:

For each polynomial system S as before,

if $\mathrm{sol}(S, R/I^q) \neq \emptyset$ for each $q \geq 0$,

then $\mathrm{sol}(S, R) \neq \emptyset$.

Let R be a ring and I an ideal of R. We say that (R, I) satisfies the infinitesimal Hasse principle (IHP) if:

For each polynomial system S as before,

if $\mathrm{sol}(S, R/I^q) \neq \emptyset$ for each $q \geq 0$,

then $\mathrm{sol}(S, R) \neq \emptyset$.

Remarks on IHP:

Assume R is local and Noetherian, with maximal ideal I, and $\widehat{R}$ is the I-adic completion of R.

Then (IHP) is equivalent to either of:

- the approximation property: for each system S, $\mathrm{sol}(S, R)$ is I-adically dense in $\mathrm{sol}(S, \widehat{R})$,
- the strong approximation property (Pfister-Popescu; Becker-Denef-Lipshitz-van den Dries).

Remarks on IHP:

Assume R is local and Noetherian, with maximal ideal I, and $\widehat{R}$ is the I-adic completion of R.

Then (IHP) is equivalent to either of:

- the approximation property: for each system S, $\mathrm{sol}(S, R)$ is I-adically dense in $\mathrm{sol}(S, \widehat{R})$,
- the strong approximation property (Pfister-Popescu; Becker-Denef-Lipshitz-van den Dries).

Remarks on IHP:

Assume R is local and Noetherian, with maximal ideal I, and $\widehat{R}$ is the I-adic completion of R.

Then (IHP) is equivalent to either of:

- the approximation property: for each system S, $\mathrm{sol}(S, R)$ is I-adically dense in $\mathrm{sol}(S, \widehat{R})$,
- the strong approximation property (Pfister-Popescu; Becker-Denef-Lipshitz-van den Dries).

Remarks on IHP:

Assume R is local and Noetherian, with maximal ideal I, and $\widehat{R}$ is the I-adic completion of R.

Then (IHP) is equivalent to either of:

- the approximation property: for each system S, $\mathrm{sol}(S, R)$ is I-adically dense in $\mathrm{sol}(S, \widehat{R})$,
- the strong approximation property (Pfister-Popescu; Becker-Denef-Lipshitz-van den Dries).

Moreover, these properties are satisfied if R is excellent (Popescu).

The connection with bad rings:

Proposition

Let R be a Noetherian ring, I an ideal of R. The following are equivalent:

1. (R, I) *satisfies the IHP,*
2. *for all n in $\mathbb{N}$, every positive-existential subset of R^n is I-adically closed.*

(The proof is easy, directly from the definitions).

The connection with bad rings:

Proposition

Let R be a Noetherian ring, I an ideal of R. The following are equivalent:

1. *(R, I) satisfies the IHP,*
2. *for all n in $\mathbb{N}$, every positive-existential subset of R^n is I-adically closed.*

(The proof is easy, directly from the definitions).

Corollary

Let R be a Noetherian ring, I an ideal of R. Assume that (R, I) satisfies the IHP and I is not nilpotent. Then R is bad.

Corollary

Let R be a Noetherian ring, I an ideal of R. Assume that (R, I) satisfies the IHP and I is not nilpotent. Then R is bad.

Proof: since I is not nilpotent,

Corollary

Let R be a Noetherian ring, I an ideal of R. Assume that (R, I) satisfies the IHP and I is not nilpotent. Then R is bad.

Proof: since I is not nilpotent,
the I-adic topology on R is not discrete.

Corollary

Let R be a Noetherian ring, I an ideal of R. Assume that (R, I) satisfies the IHP and I is not nilpotent. Then R is bad.

Proof: since I is not nilpotent,
the I-adic topology on R is not discrete.
Hence, $R \setminus \{0\}$ is not closed,

Corollary

Let R be a Noetherian ring, I an ideal of R. Assume that (R, I) satisfies the IHP and I is not nilpotent. Then R is bad.

Proof: since I is not nilpotent,
the I-adic topology on R is not discrete.
Hence, $R \setminus \{0\}$ is not closed,
and therefore not positive-existential.

Corollary

Assume R is

- *Noetherian,*
- *local,*
- *Henselian,*
- *positive-dimensional (i.e. not Artinian),*
- *excellent.*

Then R is bad.