# Formalizing Elementary Divisor Rings in Coq

Cyril Cohen **Anders Mörtberg**

University of Gothenburg

May 27, 2014

# Introduction

Goal: Generalize the theory of linear algebra over fields (vector spaces) to rings ($R$-modules)

We want to **formalize** using type theory:

- algorithms,
- correctness proof, and
- theory.

# Type theory

- Alternative foundations of mathematics to set theory
- Well suited for computer implementation and formalization
- Coq proof assistant: Functional programming language with dependent types

# Formalizing linear algebra in type theory

- G. Gonthier: *Point-free set-free concrete linear algebra* (2011)
- Formalize the theory of finite dimensional vector spaces using matrices
- At the heart of the formalization is an implementation of Gaussian elimination
- Mathematical components library (SSReflect): Coq formalization of the four color theorem and Feit-Thompson theorem

# Formalizing linear algebra in type theory

We generalize this to rings where any matrix is equivalent to a matrix in Smith normal form:

- Gaussian elimination $\Rightarrow$ Smith normal form algorithms
- Finite dimensional vector spaces $\Rightarrow$ Finitely presented modules

# Elementary divisor rings

**Elementary divisor rings** are commutative rings where every matrix is equivalent to a matrix in Smith normal form:

$$\begin{pmatrix} d_1 & & 0 & \cdots & \cdots & 0 \\ & \ddots & & & & \vdots \\ 0 & & d_k & 0 & \cdots & 0 \\ \vdots & & 0 & 0 & & \vdots \\ \vdots & & \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & \cdots & 0 \end{pmatrix}$$

where $d_i \mid d_{i+1}$ for $1 \leqslant i < k$

# Linear algebra over elementary divisor rings

Given $M$ we get invertible $P$ and $Q$ such that $PMQ = D$ where $D$ is in Smith normal form.

Using this we can compute a matrix $L$ such that:

$$XM = 0 \leftrightarrow \exists Y.X = YL$$

*i.e.* we can compute the kernel of $M$.

In particular we get that elementary divisor rings are **coherent**

# Finitely presented modules

We restrict to finitely presented modules as these are used in applications (control theory, algebraic topology...) and in computer algebra systems like SINGULAR and HOMALG.

# Finitely presented modules

We restrict to finitely presented modules as these are used in applications (control theory, algebraic topology...) and in computer algebra systems like SINGULAR and HOMALG.

An $R$-module $\mathcal{M}$ is **finitely presented** if it is finitely generated and there is a finite number of relations between these.

$$R^{m_1} \xrightarrow{M} R^{m_0} \xrightarrow{\pi} \mathcal{M} \longrightarrow 0$$

$M$ is a matrix representing the $m_1$ relations among the $m_0$ generators of the module $\mathcal{M}$.

# Finitely presented modules: example

The $\mathbb{Z}$-module $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ is given by the presentation:

$$\mathbb{Z} \xrightarrow{\begin{pmatrix} 0 & 2 \end{pmatrix}} \mathbb{Z}^2 \longrightarrow \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

as if $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ is generated by $(e_1, e_2)$ there is one relation, namely $0e_1 + 2e_2 = 0$.

# Finitely presented modules: morphisms

A morphism between finitely presented $R$-modules is given by the following commutative diagram:

$$\begin{array}{ccccccc} R^{m_1} & \xrightarrow{M} & R^{m_0} & \longrightarrow & \mathcal{M} & \longrightarrow & 0 \\ \downarrow{\scriptstyle \varphi_R} & & \downarrow{\scriptstyle \varphi_G} & & \downarrow{\scriptstyle \varphi} & & \\ R^{n_1} & \xrightarrow{N} & R^{n_0} & \longrightarrow & \mathcal{N} & \longrightarrow & 0 \end{array}$$

As elementary divisor rings are coherent we get algorithms for computing the kernel of morphisms

# Deciding isomorphism of finitely presented modules

It is in general not possible to decide if two presentation matrices represent isomorphic $R$-modules

# Deciding isomorphism of finitely presented modules

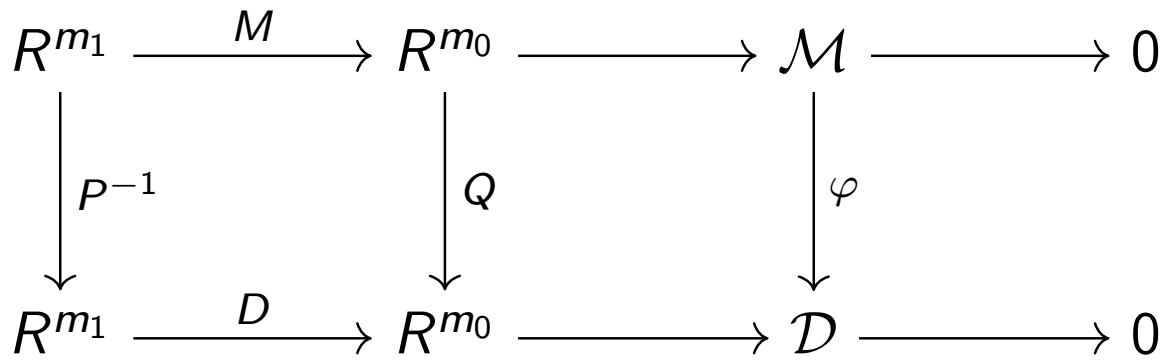
It is in general not possible to decide if two presentation matrices represent isomorphic $R$-modules

If $R$ is an elementary divisor ring this is possible:

- Compute the Smith normal form of the presentation matrices
- Compare the diagonals up to multiplication by units

# Deciding isomorphism of finitely presented modules

Given $M$ we get invertible $P$ and $Q$ such that $PMQ = D$:




Now $\varphi$ is an isomorphism as $P$ and $Q$ are invertible.

# Principal ideal domains

Classical result: Principal ideal domains (*i.e.* integral domains where every ideal is principal) are elementary divisor rings

# Principal ideal domains

Classical result: Principal ideal domains (*i.e.* integral domains where every ideal is principal) are elementary divisor rings

Principal ideal domain = Bézout domain + Noetherian

# Principal ideal domains

Classical result: Principal ideal domains (*i.e.* integral domains where every ideal is principal) are elementary divisor rings

Principal ideal domain = Bézout domain + Noetherian

**Bézout domains** are integral domains where for any two elements $a$ and $b$ there exists $x$ and $y$ such that $ax + by = gcd(a, b)$.

# Principal ideal domains

Classical result: Principal ideal domains (*i.e.* integral domains where every ideal is principal) are elementary divisor rings

Principal ideal domain = Bézout domain + Noetherian

**Bézout domains** are integral domains where for any two elements $a$ and $b$ there exists $x$ and $y$ such that $ax + by = gcd(a, b)$.

A ring is **Noetherian** if every ideal is finitely generated, which is equivalent (using classical logic) to saying that any ascending chain of ideals stabilizes.

# Constructive principal ideal domains

We say that $a$ divides $b$ strictly if

$$a \mid b \quad \wedge \quad b \nmid a$$

# Constructive principal ideal domains

We say that $a$ divides $b$ strictly if

$$a \mid b \quad \wedge \quad b \nmid a$$

Using this we can define **constructive principal ideal domains** as Bézout domains where strict divisibility is well-founded.

This can be seen as a constructive version of the ascending chain condition for principal ideals.

# Constructive principal ideal domains

We say that $a$ divides $b$ strictly if

$$a \mid b \quad \wedge \quad b \nmid a$$

Using this we can define **constructive principal ideal domains** as Bézout domains where strict divisibility is well-founded.

This can be seen as a constructive version of the ascending chain condition for principal ideals.

Can we drop the condition that strict divisibility is well-founded and generalize the result to arbitrary Bézout domains?

# Bézout domains

**Problem:** It is an open problem whether all Bézout domains are elementary divisor rings.

# Bézout domains

**Problem:** It is an open problem whether all Bézout domains are elementary divisor rings.

**Solution:** Consider extensions to Bézout domains that makes it possible for us to prove that they are elementary divisor rings. The extensions we consider are:

1. Adequacy,
2. gdco operation and
3. Krull dimension $\leq 1$.

# Kaplansky's results

I. Kaplansky: *Elementary Divisors and Modules* (1948)

He shows that the computation of Smith normal form of matrices over Bézout domains can be reduced to the case of $2 \times 2$ matrices.

The proof is concrete and constructive: We have implemented and proved correct the algorithm underlying the proof in Coq.

# The Kaplansky condition

A Bézout domain is an elementary divisor ring if and only if it satisfies the **Kaplansky condition**:

$$\text{for all } a, b, c \in R \text{ with } gcd(a, b, c) = 1$$
$$\text{there exists } p, q \in R \text{ with } gcd(pa, pb + qc) = 1$$

Hence it suffices to prove that the extensions to Bézout domains imply the Kaplansky condition in order to get that they are elementary divisor rings.

# Intuition behind the Kaplansky condition

Consider a $2 \times 2$ matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with coefficients in a Bézout domain $R$.

# Intuition behind the Kaplansky condition

Consider a $2 \times 2$ matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with coefficients in a Bézout domain $R$.

It is straightforward to show that it is equivalent to a matrix:

$$\begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}$$

for some $a', b', c' \in R$.

# Intuition behind the Kaplansky condition

Consider a $2 \times 2$ matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with coefficients in a Bézout domain $R$.

It is straightforward to show that it is equivalent to a matrix:

$$\begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}$$

for some $a', b', c' \in R$.

Without loss of generality we can assume that $gcd(a', b', c') = 1$. Furthermore, such a matrix can be put in Smith normal form if and only if there exists $p, q \in R$ with $\gcd(pa', pb' + qc') = 1$.

# Helmer: Adequate rings

O. Helmer: *The Elementary Divisor Theorem for certain rings without chain conditions* (1942)

A Bézout domain[1] $R$ is **adequate** if there for any $a, b \in R$ exists $r \in R$ such that

1. $r \mid a$,
2. $r$ is coprime with $b$, and
3. for all non unit $d$ such that $dr \mid a$ we have that $d$ is not coprime with $b$.

In the paper Helmer proves that this class of rings are elementary divisor rings, however Kaplansky has a simpler proof using the Kaplansky condition in his 1948 paper.

[1] Interestingly Helmer calls these "Prüfer rings"

# gdco domains

Adequacy resembles very much the notion of a "gdco operation" that takes $a, b \in R$ and computes the greatest divisor of $a$ coprime to $b$.

We call Bézout domains with such an operation **gdco domains** and we have proved that these satisfy the Kaplansky condition.

We have also proved that both adequacy and well-founded strict divisibility implies the existence of a gdco operation. Hence we get that both of these are elementary divisor rings.

# Krull dimension $\leq 1$

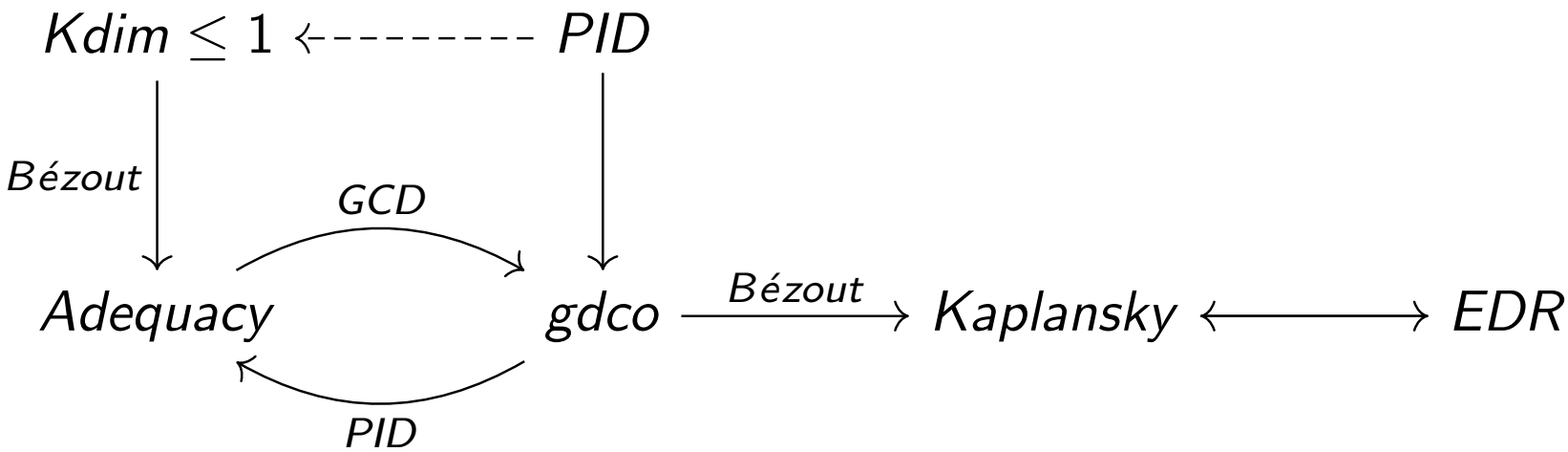
Classically Krull dimension is defined as the supremum of the length of all chains of prime ideals, this can be defined constructively using an inductive definition.

Concretely an integral domain $R$ is of **Krull dimension** $\leq 1$ if for any $a, u \in R$ there exists $v \in R$ and $m \in \mathbb{N}$ such that

$$a \mid u^m(1 - uv)$$

We have proved that Bézout domains of Krull dimension $\leq 1$ are adequate.

# Summary


Kdim ≤ 1
PID
Bézout
GCD
Adequacy
gdco
Bézout
Kaplansky
EDR
PID

# Conclusions

We have formalized proofs that elementary divisor rings are a good setting for developing linear algebra in type theory.

We have also formalized that Bézout domains extended with either

- adequacy,
- *gdco* operation,
- Krull dimension $\leq 1$, or
- well-founded strict divisibility

are elementary divisor rings and explored the connections between these extensions.

Thanks for your attention!