Formalization of Rings with Explicit Divisibility in Type Theory

Anders Mörtberg
mortberg@chalmers.se

Introduction

- SSReflect
- Rings with explicit divisibility
  - GCD domains
  - Bézout domains
  - Euclidean rings
- Smith normal form
  - Constructive PIDs

SSReflect

- Extension to Coq
- George Gonthier: formalization of the four color theorem
- Cayley-Hamilton theorem, decidability of ACF...

- Feit-Thompson theorem (part of the classification of finite simple groups)

SSReflect

- Small Scale Reflection
- New tactics and tacticals
- Library of mathematical theories

DvdRing

- A ring R has *explicit divisibility* if it has a divisibility test that give witnesses:

$$a \mid b \leftrightarrow \exists x.\, b = xa$$

- $\mathbb{Z}$ and $k[x]$ where k is a field (e.g. $\mathbb{Q}$)

DvdRing

- Demo!

GCD domains

- GCD domain: Every pair of elements have a greatest common divisor

$$\forall a\, b. \exists g \,.\, g \mid a \wedge g \mid b \wedge \forall g' \,.\, g' \mid a \wedge g' \mid b \to g' \mid g$$

Properties of GCD domains

Definition

The gcd of the coefficients of $p \in R[x]$ is called the *content* of p, written $cont(p)$

Definition

$p \in R[x]$ is *primitive* if $cont(p) = 1$

Theorem

Gauss lemma: $cont(pq) = cont(p)cont(q)$

Theorem

Every polynomial $p \in R[x]$ *can be written as* $p = cont(p)q$ *with* q *primitive*

Properties of GCD domains

- Using this one can give an algorithm for computing the gcd of $p, q \in R[x]$
- Give a proof that if R is a GCD domain then $R[x]$ also is
- Don't use field of fractions!
- Can compute gcd in $\mathbb{Z}[x_1, \ldots, x_n]$ and $k[x_1, \ldots, x_n]$

Bézout domains

- Non-Noetherian analogue of principal ideal domains
- PID: Every ideal is principal
  - Quantification over all ideals
- Bézout domain: Every finitely generated ideal is principal
- Equivalent definition:

$$\forall a\, b. \exists x\, y.\; ax + by = gcd(a, b)$$

Euclidean rings

- Euclidean norm, $f : R \to \mathbb{N}$
- Euclidean division: $\forall a\, b.\, \exists q\, r.\, a = bq + r$ and either $f(r) < f(b)$ or $r = 0$
- Examples: $\mathbb{Z}$ with absolute value and $k[x]$ with degree

Bézout domains and Euclidean rings

Theorem

Every Euclidean ring is a Bézout domain

Theorem

Every Bézout domain is a GCD domain

Theorem

$\mathbb{Z}$ *is a Euclidean ring*

Theorem

$k[x]$ *is a Euclidean ring*

Smith normal form

- Generalization of Gauss elimination algorithm
- Elements from a PID and not just a field
- Compute homology groups of simplicial complexes
  - "Homology is a rigorous mathematical method for detecting and categorizing holes in a shape." - Wikipedia

Smith normal form

- Let A be a nonzero $m \times n$ matrix over a PID. There exists invertible $m \times m$ and $n \times n$ matrices S,T such that

$$SAT = \begin{pmatrix} \alpha_1 & 0 & 0 & & \cdots & & 0 \\ 0 & \alpha_2 & 0 & & \cdots & & 0 \\ 0 & 0 & \ddots & & & & 0 \\ & & & \alpha_r & & & \vdots \\ \vdots & & & & 0 & & \\ & & & & & \ddots & \\ 0 & & & \cdots & & & 0 \end{pmatrix}$$

and $\alpha_i \mid \alpha_{i+1}$, $1 \leq i < r$

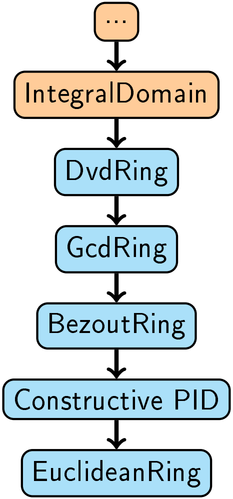
Smith normal form

- Open question for Bézout domains
- Need constructive approximation of PIDs

Constructive PIDs

- Mines, Richman, Ruitenburg: Bézout domains such that if we have a sequence $u(n)$ with $u(n+1) \mid u(n)$ then there exists k such that $u(k) \mid u(k+1)$
- In type theory this can be represented as that strict divisibility is well founded

Summary



...
IntegralDomain
DvdRing
GcdRing
BezoutRing
Constructive PID
EuclideanRing

Conclusions and further work

- Have: Divisibility theory in SSReflect
  - Formalized algorithms for $\mathbb{Z}$ and $k[x]$
- Todo: R GCD domain implies $R[x]$ GCD domain
- Have: Smith normal form algorithm in Haskell
- Todo: Formalize Smith normal form algorithm

Questions?

This work has been partially funded by the FORMATH project, nr. 243847, of the FET program within the 7th Framework program of the European Commission