Constructive Algebra in Functional Programming and Type Theory

Anders Mörtberg

Linear algebra

- Solving systems of linear equations

$$\begin{cases} 3x + 2y - z & = 1 \\ 2x - 2y + 4z & = -2 \\ -x + \frac{1}{2}y - z & = 0 \end{cases}$$

- Many methods to solve: Gauss elimination, Cramers rule, etc...
- Solution lies in a field, e.g. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

What about $\mathbb{Z}$?

$$\begin{cases} x + 3y - 2z & = 5 \\ 3x + 5y + 6z & = 7 \\ 2x + 4y + 3z & = 8 \end{cases}$$

- $\mathbb{Z}$ is not field, what about other integral domains?

Abstract algebra

- Study properties and patterns of mathematical concepts
- Generalize and consider problems for algebraic structures instead of concrete instances
- Algebraic theories: monoids, groups, rings, fields, vector spaces, modules...

Constructive algebra

- Advanced algebra rely on nonconstructive reasoning
- Example: The existence of maximal and prime ideals
- Question: How much of classical algebra can be made constructive?

Generalized linear algebra

- Drop assumption of field
- Coherent rings - Solve homogeneous systems
- Given a vector M there exist a matrix L such that $ML = 0$ and

$$MX = 0 \quad \leftrightarrow \quad \exists Y.\ X = LY$$

Representation in Haskell

```
class IntegralDomain a ⇒ Coherent a where
  solve :: Vector a → Matrix a
```

```
propCoherent :: (Coherent a, Eq a) ⇒ Vector a → Bool
propCoherent m = (solve m) `isSolution` m
```

Properties of coherent rings

- Coherence $\rightarrow$ $MX = 0$ where $M \in R^{n \times m}$ solvable
- Ideal intersection computable $\longleftrightarrow$ Coherence
- To prove coherence show how to compute $I \cap J$

Three coherence proofs

- Bézout domains
- Prüfer domains
- Polynomial rings

Noetherianity

- Noetherian: **All** ideals are finitely generated
- Not suitable for constructive mathematics since it relies on quantification over all subsets of the ring

Bézout domains

- Non-Noetherian principal ideal domains
- All **finitely generated** ideals are principal
- Examples: $\mathbb{Z}$, $k[x]$

Implementation

```
class IntegralDomain a ⇒ BezoutDomain a where
  toPrincipal :: Ideal a → (Ideal a,[a],[a])
```

- $(\langle t \rangle, us, vs) = \text{toPrincipal } \langle a_1, \ldots, a_n \rangle$

$$\begin{aligned} t &= a_1 u_1 + \cdots + a_n u_n \\ a_i &= t v_i \end{aligned}$$

Coherence

- Given ideals $I = \langle a \rangle$ and $J = \langle b \rangle$

$$I \cap J = \langle lcm(a, b) \rangle$$

- $I \cap J$ computable $\rightarrow$ Coherent!

Examples in $\mathbb{Z}$

- Compute principal ideal from $\langle 4, 6 \rangle$

```
> toPrincipal (Id [4,6])
(<2>,[-1,1],[2,3])
```

- Intersection of $\langle 2 \rangle$ and $\langle 3 \rangle$

```
> Id [2] `intersectionB` Id [3]
<6>
```

Examples in $\mathbb{Z}$

- Solving the system

$$\begin{cases} x + 3y - 2z & = 0 \\ 3x + 5y + 6z & = 0 \end{cases}$$

```
> solveMxN (M [Vec [1,3,-2], Vec [3,5,6]])
[ 7,0]
[-3,0]
[-1,0]
```

- The solution (except for the trivial) is

$$\begin{aligned} x &= 7 \\ y &= -3 \\ z &= -1 \end{aligned}$$

Prüfer domains

- Non-Noetherian Dedekind domains
- Simple first order description

$$\forall x\, y.\, \exists u\, v\, w. \quad ux = vy \wedge (1-u)y = wx$$

- Examples: Bézout domains, algebraic extensions and curves

Implementation

```
class IntegralDomain a ⇒ PruferDomain a where
  calcUVW :: a → a → (a,a,a)


propCalcUVW :: (PruferDomain a, Eq a) ⇒ a → a → Bool
propCalcUVW x y = u <*> x              ≡ v <*> y &&
                  (one <-> u) <*> y ≡ w <*> x
  where (u,v,w) = calcUVW x y
```

Examples

- $\mathbb{Z}[\sqrt{-5}]$: $a + b\sqrt{-5}$ where $a, b \in \mathbb{Z}$
- $k[x, y]$ with $y^2 = 1 - x^4$: $a + b\sqrt{1 - x^4}$ with $a, b \in k[x]$

Sketch of coherence proof

- Principal localization matrix for the ideal $\langle x_1, \ldots, x_n \rangle$

$$\begin{cases} \sum a_{ii} & = 1 \\ a_{lj} x_i & = a_{li} x_j \quad \forall i, j, l \in \{1, \ldots, n\} \end{cases}$$

- Property

$$\langle x_1, \ldots, x_n \rangle \langle a_{1j}, \ldots, a_{nj} \rangle = \langle x_j \rangle$$

Sketch of coherence proof

- Property

$$IJ = (I \cap J)(I + J)$$

- Implies

$$IJ(I + J)^{-1} = \langle a \rangle (I \cap J)$$

Polynomial ring

- $k[x_1, \ldots, x_n]$
- $\frac{1}{2}xz + xy^2 - x^2z^3 \in \mathbb{Q}[x, y, z]$

Gröbner bases

- Division in $k[x_1, \ldots, x_n]$ depend on the order of divisors

$$\begin{aligned} x^2/[x+y, x] &= (x-y)(x+y) + 0 \cdot x + y^2 \\ x^2/[x, x+y] &= x \cdot x + 0 \cdot (x+y) + 0 \end{aligned}$$

- Gröbner bases are the "well behaved" ideals in $k[x_1, \ldots, x_n]$. Division of any element in the ideal by the generators give the same result regardless of the order of the divisors.

- Buchberger algorithm

Coherence of $k[x_1, \ldots, x_n]$

- Let I and J be ideals in $k[x_1, \ldots, x_n]$
- Introduce t greater than all $x_1, \ldots, x_n$
- Compute using Gröbner bases:

$$(tI + (1-t)J) \cap k[x_1, \ldots, x_n] = I \cap J$$

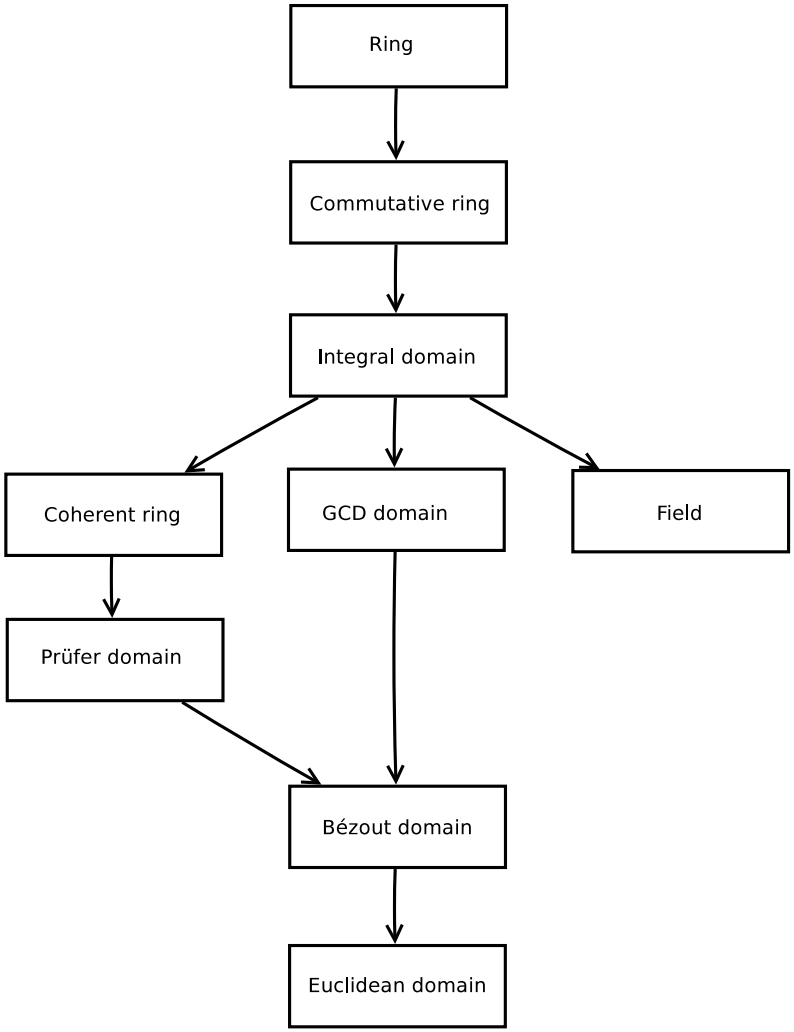
Examples

- Intersection in $k[x, y]$

$$\langle x^2 y \rangle \cap \langle x y^2 \rangle$$

```
> Id [x^2*y] `intersectionMP` Id [x*y^2]
<x^2y^2>
```

Implementation



Discussion

- Limitations
- Further work
- Conclusions

Questions?