Krull's Principal Ideal Theorem

Thierry Coquand and Henri Lombardi

Intuitionistic algebra

Wraith (ICM'78), if a theorem of algebra can be formulated in the form

$$\phi_1, \dots, \phi_n \vdash \phi$$

with $\phi_1, \dots, \phi_n, \phi$ *geometric algebra* then it is intuitionistically valid

Only some non constructive general argument

Some partial constructive results; use formal description of *coherent* spaces (spectrum of distributive lattices)

Intuitionistic algebra

Here we analyse a statement

$$R\ \ Noetherian, \phi_1, \dots, \phi_n \vdash \phi$$

We use a definition of Noetherian, which is *invariant by change of base*

We consider the space of *minimal prime ideals* which is *not* coherent

Krull's dimension

R commutative ring, generalised space of functions

Points of $Sp(R)$: irreducible subvarietes

The *Krull dimension* is the supremum of the lengths of chains of distincts prime ideals

Considered to be the "right" definition, for Noetherian rings

Spectrum, constructively

The spectrum of R can be described as a formal space

Propositional atoms $D(a)$

$$D(a) = \{P \in Sp(R) \mid a \notin P\}$$

- $\vdash\ D(1)$
- $D(0)\ \vdash$
- $D(a+b)\ \vdash\ D(a), D(b)$
- $D(ab)\ \vdash\ D(a)$
- $D(a), D(b)\ \vdash\ D(ab)$

Constructible Topology

Theorem: we have

$$D(a_1),\ \ldots,\ D(a_n) \vdash D(b_1), \ldots, D(b_m)$$

iff the ideal generated by the b_j meets the multiplicative monoid generated by the a_i.

Constructible topology: we add new symbols $V(a)$

- $\vdash D(a), V(a)$
- $D(a),\ V(a) \vdash$

Krull dimension, constructively

The theory of chains $P_0 \supseteq \cdots \supseteq P_n$ is the theory C_n with atomic propositions $D_i(a)$, $i \leq n$

- $\vdash \; D_i(1)$
- $D_i(0) \; \vdash$
- $D_i(a+b) \; \vdash \; D_i(a), D_i(b)$
- $D_i(ab) \; \vdash \; D_i(a)$
- $D_i(a), D_i(b) \; \vdash \; D_i(ab)$
- $D_i(a) \vdash D_{i+1}(a)$

Krull dimension

Theorem: The Krull dimension of R is $\leq n$ iff we have for any $a_0, \dots, a_n$

$$D_0(a_0), \dots, D_n(a_n) \vdash D_0(a_1), \dots, D_{n-1}(a_n)$$

in the theory of chains $P_0 \supseteq \cdots \supseteq P_n$ iff for any $a_0, \dots, a_n$ there exists $b_0, \dots, b_n$ and $p_0, \dots, p_n$ such that

$$a_0^{p_0}(a_2^{p_2} \cdots (a_n^{p_n}(1 + b_n a_n) + \cdots + b_2 a_2) + b_0 a_0) = 0$$

Krull dimension

We have a *complete* description of the theory of chains C_n.

Theorem: If R is strongly discrete, coherent and noetherian, each theory C_n is decidable.

More generally if we have a coherent space $X = Sp(T)$ ($=$ distributive lattice) we can describe the lattice for the space of *chains* of points of X

Krull's Principal Ideal Theorem

"probably the most important single theorem in the theory of Noetherian ring" (Kaplansky)

Hopefully an abstract theorem that has powerful concrete applications

Theorem: If R is *Noetherian* and P is minimal over $\langle x\rangle$ there cannot be any non trivial chain $P \supset Q_1 \supset Q_2$

I will describe the intuitionistic version (not the proof)

Minimal Prime Ideals

Describe the space $mSp(R)$ of *minimal* prime ideals for the Zariski topology

Same atomic propositions $D(a)$ and same axioms as before

We add the *infinitary* axioms

$$\vdash \ D(a), \ \bigvee_{a^n u=0} D(u)$$

The subspace $mSp(R)$ of $Sp(R)$ is no longer coherent.

Minimal Prime Ideals

We can write the theory of minimal prime ideals over x

- $D(x) \vdash$
- $\vdash\ D(a), \bigvee_{u(a^n - bx)=0} D(u)$

Noetherian rings

Let $G(a_0, \ldots, a_{n-1})$ to mean that there exists $i < n$ such that $a_i \in \langle a_0, \ldots, a_{i-1} \rangle$. (If $a_0, \ldots, a_{n-1}$ is the empty sequence $G()$ is the absurd proposition $\perp$.)

R is Noetherian iff for any predicate P on finite sequences such that

1. $G(\sigma) \to P(\sigma)$
2. $P(\sigma) \to P(\sigma a)$
3. $((\forall a)\, P(\sigma a)) \to P(\sigma)$

P holds on all sequences.

Noetherian rings

Classically this is equivalent to the usual definition.

Similar to bar induction: G is a bar

This definition is *invariant by change of base*

We can prove $R[X]$ Noetherian if R Noetherian without extra hypothesis on R

Krull's Principal Ideal Theorem

We consider the theory of chains $M \supseteq Q_0 \supseteq Q_1$ with M *minimal* over x

- $D(x) \vdash$
- $\vdash\ D(a), \bigvee_{u(a^n - bx)=0} D(u)$

Theorem: In this theory we have, for any $a_0, a_1 \in R$

$$D_0(a_0),\ D_1(a_1) \vdash\ D(a_0),\ D_0(a_1)$$