KRULL'S PRINCIPAL IDEAL THEOREM

THIERRY COQUAND, HENRI LOMBARDI

Introduction

The purpose of this note is to present a possible constructive version of Krull's principal ideal theorem. This theorem is qualified by Kaplansky [4] as being "probably the most important single theorem in the theory of Noetherian rings". Historically, it corresponds to one of the high point in the development of abstract algebra.

One motivation for analysing this proof is the following. It is known [5], in a non constructive way, that if we have a theorem classically valid of the form

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

where $\phi_1, \dots, \phi_n, \phi$ are *geometric formulae* then this theorem is also valid intuitionistically. Furthermore the work in [2] indicates a method for transforming a given classical argument of such a statement into an intuitionistic one. This seems to be related crucially to the fact that geometrical statements are invariant under change of base.

Krull's principal ideal theorem is a good example of a classical proof of a statement of the form

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

where $\phi_1, \dots, \phi_n, \phi$ are geometric formulae. The proof we present may indicate a general method for transforming a classical proof of such a statement in an intuitionistic argument. The key seems to be that it is possible to find an intuitionistic definition of "Noetherian", classically equivalent to the usual definition, which is invariant under change of base. We present such an invariant definition, which is enough to state and prove Krull's principal ideal theorem constructively.

1. Krull's Principal Ideal Theorem

We analyse the following version of the Principal Ideal Theorem. We write $\langle u \rangle$ the principal ideal generated by an element u of a ring, and $\langle u_1, \dots, u_n \rangle$ the ideal generated by a finite sequence $u_1, \dots, u_n$.

Theorem 1.1. *If R is a Noetherian local ring, of maximal ideal M, and M is minimal among primes of R containing $x \in M$ then for any $f \in M$ there exists n and k such that $x^k f^n \in \langle f^{n+1} \rangle$.*

We introduce the following notation. Let I_n be the ideal

$$I_n = \{u \in A \mid (\exists k)\ x^k u \in \langle f^n \rangle\}$$

Notice that the ideals I_n form a descending chain $I_0 \supseteq I_1 \supseteq \dots$ and that the theorem states that there exists n such that $f^n \in I_{n+1}$. Since we have clearly $f^n \in I_{n+1}$ iff $I_n = I_{n+1}$, the theorem states that there exists n such that $I_n = I_{n+1}$.

Proof. The fact that M is minimal over $\langle x \rangle$ can be expressed by that if $u \in M$ there exists k such that $u^k \in \langle x \rangle$. Since R is Noetherian, M is finitely generated and hence we can find p such that $M^p \subseteq \langle x \rangle$.

We claim that for any k it is possible to find N such that for any sequence of decreasing ideals $J_0 \supset J_1 \supseteq \dots$ and any sequence $u_0 \in J_0, \dots, u_{N-1} \in J_{N-1}$ there exists $i < N$ such that $u_i \in J_{i+1} + M^k$.

Date: March 29, 2001.

Indeed, for $k = 1$ we can take $N = 2$ because either $u_1 \in M$ or u_1 is invertible and hence we can find R such that $u_0 = au_1$ and then $u_0 \in J_1$.

Suppose that we have found N for k and take any sequence of length $\geq L = NK$

$$u_0 \in J_0, \ldots, u_{L-1} \in J_{L-1}$$

where K is such that any sequence of elements in M^k/M^{k+1} of length $\geq K$ is not independent, seeing M^k/M^{k+1} as a vector space over the field R/M. If we assume M to be generated by q elements we can take $K = 1 + q^k$. By induction hypothesis, we can extract a subsequence $u_{n_0}, \ldots, u_{n_{K-1}}$ $u_{n_i} \in J_{n_i+1} + M^k$. Write $u_{n_i} = v_i + m_i$. By choice of K we have a relation of the form

$$m_i - \Sigma_{j>i} \alpha_j m_j \in M^{k+1}$$

and it follows from this that $u_{n_i} \in J_{n_i+1} + M^{k+1}$ as desired.

Since $M^p \subseteq \langle x \rangle$ it follows from this result that we can find N such that for any sequence

$$u_0 \in I_0, \ldots, u_{N-1} \in I_{N-1}$$

there exists $n < N$ such that $u_n \in \langle x \rangle + I_{n+1}$. Notice next that if

$$u = ax + v \quad u \in I_n \quad v \in I_{n+1}$$

then we have k such that

$$x^k u \in \langle f^n \rangle \qquad x^k v \in \langle f^{n+1} \rangle$$

and then $ax^{k+1} \in \langle f^n \rangle$ so that $a \in I_n$.

We can then define N infinite sequences $u_i(k) \in I_i,\ i < N$ starting from $u_i(0) = f^i \in I_i$ such that $u_i(k+1) = u_i(k)$ for all $i < N$ except one j for which we have

$$u_j(k) = x u_j(k+1) \pmod{I_{j+1}}$$

By the box principle, we find in this way $n < N$ and an infinite sequence $f^n = v_0,\ v_1, \ldots$ of elements in I_n such that

$$v_l = x v_{l+1} \pmod{I_{n+1}}$$

Since R is Noetherian we have eventually $v_l \in \langle v_0, \ldots, v_{l-1} \rangle$ and then, since $x \in M$ we get $v_l = 0 \pmod{I_{n+1}}$ and hence $f^n = v_0 = 0 \pmod{I_{n+1}}$ as desired. □

This proof is essentially the original one of Krull, as presented for instance in [3]. The differences with the proof in [3] are as follow:

- In [3] one introduces $Q_1 \subseteq Q \subseteq M$ with $f \in Q - Q_1$, $x \in M - Q$ and the ideals

  $$Q^{(n)} = \{u \in R \mid (\exists s \notin Q)\, su \in Q^n\}$$

  In our presentation, $u \in Q$ is replaced by its approximation $u \in \langle f \rangle$ while $s \notin Q$ is replaced by $s \in \{x^k \mid k \geq 0\}$. In this way, $Q^{(n)}$ becomes the ideal

  $$I_n = \{u \in R \mid (\exists k)\, x^k u \in \langle f^n \rangle\}.$$

- In [3] using Jordan-Holder's theorem, one notices that for any decreasing sequence of ideals $J_0 \supseteq J_1 \supseteq \ldots$ the corresponding sequence $J_0 + M^k \supseteq J_1 + M^k \supseteq \ldots$ is stationnary. We have replaced this step by a more explicit step, essentially in order to facilitate the connection with the next constructive proof of Krull's principal ideal theorem.

2. Constructive Proof, First Version

From now on, we work constructively.

Given a ring R we let $G(a_0, \ldots, a_{n-1})$ to mean that there exists $i < n$ such that $a_i \in (a_0, \ldots, a_{i-1})$. If $a_0, \ldots, a_{n-1}$ is the empty sequence $G()$ is the absurd proposition $\perp$. We define now intuitionistically R to be 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. Notice that, by the second clause, this is the same as saying that P holds on the empty sequence $()$. Let us call a predicate that satisfies the clause $1., 2., 3.$ to be *hereditary.*

The importance of this definition of Noetherian is that it is invariant by change of base. We shall comment on this in the next section. It is possible to show with this definition that if R is noetherian then so is $R[X]$ without coherence conditions.

We shall need the following lemma.

Lemma 2.1. *If R is Noetherian and $P(\sigma_0, \dots, \sigma_{m-1})$ is a property of m finite sequences of elements of R such that*

1. $G(\sigma_i) \to P(\sigma_0, \dots, \sigma_{m-1})$
2. $P(\sigma_0, \dots, \sigma_{m-1}) \to P(\sigma_0, \dots, \sigma_i a, \dots, \sigma_{m-1})$
3. $[(\forall a)\, P(\sigma_0 a, \dots, \sigma_{m-1}) \wedge \cdots \wedge (\forall a)\, P(\sigma_0, \dots, \sigma_{m-1} a)] \to P(\sigma_0, \dots, \sigma_{m-1})$

then P holds for all m finite sequences.

Proof. We do the argument for $m = 2$. We have by assumption

1. $G(\sigma_i) \to P(\sigma_0, \sigma_1)$
2. $P(\sigma_0, \sigma_1) \to P(\sigma_0, \sigma_1 a)$ and $P(\sigma_0, \sigma_1) \to P(\sigma_0 a, \sigma_1)$
3. $[(\forall a)\, P(\sigma_0 a, \sigma_1) \wedge (\forall a)\, P(\sigma_0, \sigma_1 a)] \to P(\sigma_0, \sigma_1)$

We consider the property $Q(\sigma) = (\forall \sigma_1)\, P(\sigma, \sigma_1)$ We claim that this property is hereditary. This follows from the fact that if we assume $(\forall a)\, Q(\sigma a)$ then the property $R(\sigma_1) = P(\sigma, \sigma_1)$ is hereditary. Hence Q and P hold universally. □

Let R be a ring, and M an ideal such that any element in R either is in M or is invertible. We assume $x \in M$ such that for any $u \in M$ there exists k such that $u^k \in \langle x \rangle$. We assume furthermore that R is Noetherian.

Theorem 2.2. *Let $f \in M$ and define I_n to be the ideal*

$$I_n = \{u \in A \mid (\exists k)\, x^k u \in \langle f^n \rangle\}$$

The predicate

$$H(\sigma) = G(\sigma) \vee [(\exists n)\, f^n \in I_{n+1}]$$

is hereditary.

Since R is Noetherian, this implies that $H()$ holds and hence $f^n \in I_{n+1}$ for some n.

Proof. We assume

$$(\forall a)\, H(a_0, \dots, a_{n-1}, a)$$

and we prove $C = H(a_0, \dots, a_{n-1})$. Notice that we have

$$G(a_0, \dots, a_{n-1}, a) = a \in \langle a_0, \dots, a_{n-1} \rangle \vee G(a_0, \dots, a_{n-1})$$

and hence we can rewrite the hypothesis as

$$(\forall a)\, [C \vee a \in \langle a_0, \dots, a_{n-1} \rangle]$$

We follow now the proof of theorem 1.1. We don't know that M is finitely generated, but we can do "as if" M is generated by $a_0, \dots, a_{n-1}$ that are given explicitely. We compute hence p such that

$$(\forall u \in M^p)\, [C \vee u \in \langle x \rangle]$$

Similarly, we find explicitely N such that for any decreasing sequence of ideals $J_k,\ k < N$ and any sequence $u_k \in J_k,\ k < N$ we have

$$C \vee (\exists k < N)\, [u_k \in J_{k+1} + M^p]$$

We introduce now the following predicate $Q_k(u_1, \dots, u_p)$ meaning that we have

$$f^k = x u_1 \pmod{I_{k+1}}, \dots, u_{p-1} = x u_p \pmod{I_{k+1}}$$

We define $Q_k()$ to be the true proposition T. Following the proof of theorem 1.1 we see that we have

$$[\wedge_{k<N} Q_k(\sigma_k)] \to C \vee (\exists i < N)\,(\exists a)\,Q_i(\sigma a)$$

We can now use lemma 2.1 with the predicate

$$P(\sigma_0, \dots, \sigma_{N-1}) = [\wedge_{k<N} Q_k(\sigma_k)] \to C$$

and we conclude that P holds on all N sequences. In particular if we apply P on the empty sequences we get that C holds, as desired. $\square$

Let us outline the algorithm implicit in this argument, first in the case where R is strongly discrete, that is where we can decide the appartenance of an element a to a given finitely generated ideal $\langle a_0, \dots, a_{n-1}\rangle$. In such a case the predicate G is decidable. The steps in the algorithm will then be indexed by a finite sequence $a_0, \dots, a_{n-1}$ of elements in M satisfying the negation of G. For this sequence, *either* we can follow the proof of theorem 1.1 and compute m such that $f^m \in I_{m+1}$ *or* we find explicitely $a \in M$ such that a *is not* in $\langle a_0, \dots, a_{n-1}\rangle$. We start then a new step of the algorithm with the new sequence $a_0, \dots, a_{n-1}, a$. This stops eventually because R is Noetherian and a sequence avoiding G cannot grow indefinitely.

Essentially the same algorithm goes on in the general case, but now we cannot decide $u \in \langle a_0, \dots, a_{n-1}\rangle$ any more. When such a question is raised, we proceed *as if* a was not in $\langle a_0, \dots, a_{n-1}\rangle$. If later we discover an explicit relation $a \in \langle a_0, \dots, a_{n-1}\rangle$ we backtrack at this stage and proceed according with this new information.

Of course, this is only an informal description. The proof above, being constructive, can itself be seen as an algorithm (with its own justification of termination).

However, this constructive formulation of Krull's principal ideal theorem is not optimal. For one thing, membership to M is assumed to be decidable, and one would like to have a version without this assumption. Another point is that it seems hard to derive the general version of the principal ideal theorem from this unary version. We shall present a better constructive version of Krull's principal ideal theorem. In the next section, we recall some results of [1], presented in a form suitable for formulating this refined version.

3. Spectrum as Theory and Constructive Krull Dimension

To any ring R we can associate its space of prime ideals $Sp(R)$ known as the *spectrum* of R, with two different topologies. The first one if the *Zariski topology* where the basic open subsets are of the form

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

The second one is the *constructible topology* where the basic open subsets are generated by $D(a)$, $a \in R$ and

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

so that a basic open subset in general is of the form

$$D(a) \cap V(b_1) \cap \cdots \cap V(b_n)$$

Both topologies are spectral: all basic open subsets are compact. Furthermore, the constructible topology is Hausdorff.

It is possible to have a constructive description of both topologies, as a point-free space (or locale), with Zariski or with the constructible topology. The Zariski topology can be elegantly described as the following theory for a generic prime ideal P

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

The fact that this theory is finitary corresponds to the fact that Zariski topology is spectral. It is also related to the fact that the dynamical proofs considered in [2] are finitely branching trees.

It can be shown [1] that 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.

Classically, both descriptions are equivalent: we have

$$D(a) \vdash \bigvee D(a_i)$$

iff a belongs to the radical of the ideal generated by the a_i iff

$$D(a) \subseteq \bigcup D(a_i)$$

in the space $Sp(R)$. Constructively, we think of the basic open subset $D(a) = a \notin R$ as an atomic proposition, syntactically given, and not as a set of points.

In order to get constructible topology we add a new predicate $V(a)$ with the axioms

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

There also, derivations are finitely branching trees.

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

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

In this setting, we can now formulate one of the main result of [1] as follows.

Theorem 3.1. *The Krull dimension of R is $\leq n$ iff we have for any $a_0,\ldots,a_n$*

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

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

$$a_0^{p_0}(a_2^{p_2}\cdots(a_n^{p_n}(1+b_na_n)+\cdots+b_2a_2)+b_0a_0)=0$$

We notice that this constructive approach of the spectrum is really in the spirit of Hilbert's program: we replace the semantical description of the spectrum as a set of points (models) by a syntactical notion of theory. The fact that the Krull dimension of a ring if $\leq n$ is then expressed as a derivability statement in a theory.

So far, all the theories we have considered were finitary. In order to describe constructively minimal prime ideals, we shall need to allow possibly infinitary disjunction, and the derivations will be well-founded, but not necessarily finite, trees.

4. Constructive Proof, Second Version

We now give a description of the formal space $mSp(R)$ of *minimal* prime ideals for the Zariski topology. The basic open subsets are still of the form $D(a)$, thought of as the proposition $a \notin M$ but we add the new axioms, which are no longer finitary

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

Let us describe more in details this topology. The basic open subsets $p, q, r, \ldots$ are of the form

$$p = D(a) = \{M \in mSp(R)\ \mid\ a \notin M\}$$

We have then

$$p \cap D(b) = D(ab)$$

We can describe inductively when a basic open subset $p = D(a)$ is covered by a family of basic open subsets $p_i = D(a_i)$, $i \in I$, that is we give a direct inductive definition of

$$p \vdash \bigvee p_i$$

This happens iff

- a belongs to the radical of some $\langle a_i \rangle$ or
- for some $b_1, \ldots, b_m$ such that a belomgs to the radical of $\langle b_1, \ldots, b_m \rangle$ we have

  $$p \cap D(b_j) \vdash \bigvee p_i$$

  for all j or
- for some $b \in R$ we have

  $$p \cap D(b) \vdash \bigvee p_i \qquad \text{and} \qquad p \cap D(u) \vdash \bigvee p_i$$

  for all u, n such that $ub^n = 0$

If we fix an element x of R we introduce the space $mSp_x(R)$ of minimal primes over x, which could be defined as $mSp(R/(x))$. We change the infinitary clause to

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

and we add the new clause

$$D(x) \vdash$$

We can now state a constructive version of Krull's principal ideal theorem

Theorem 4.1. *If R is Noetherian then in the theory of minimal prime over x we have, for any $f \in R$*

$$\vdash D(f), \bigvee_{uf^n(x^k - af)=0} D(u)$$

that is the collection of basic open subsets $D(f)$ and $D(u)$, $uf^n(x^k - af) = 0$, form a covering of the space $mSp_x(R)$.

Notice that this theorem is stronger than the previous one theorem 2.2. We don't assume given any minimal prime ideal over x, but we say that the conclusion

$$D(f) \vee \bigvee_{uf^n(x^k - af)=0} D(u)$$

is provable in the theory of minimal prime ideal over x. Another difference is that we do not assume M to be decidable, but M is here described only by the theory of its complement.

Actually, it is quite direct to show that we have conservativity of assuming M decidable in the following sense.

Lemma 4.2. *The entailment*

$$p,\, V(b_1),\, \ldots,\, V(b_m) \vdash \bigvee p_i$$

is provable in the theory $mSp_x(R)$ extended with

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

iff

$$p \vdash D(b_1),\, \ldots,\, D(b_m),\, \bigvee p_i$$

is provable in the theory $mSp_x(R)$.

So the collection of basic open subsets

$$D(f),\ D(u),\quad uf^n(x^k - af) = 0$$

covers $mSp_x(R)$ for the Zariski topology iff it covers it for the constructible topology.

The proof can then be given by following the proof of theorem 2.2, but working now with predicates that have as values the opens of the space $X = mSp_x(R)$. Let $P : R \to O(X)$ be such a predicate, we then have, for any $a \in R$

$$P\, hereditary \to P(a)$$

simply because, for any basic open p of X such that

$$p \vdash P\, hereditary$$

the predicate $p \vdash P(x)$, that is the predicate that expresses that $P(x)$ contains the basic open p, is hereditary. Hence since R is Noetherian, we have $p \vdash P(a)$ for all $a \in R$[1].

The following is a direct consequence of theorem 4.1, which expresses that if M is minimal over x there cannot be a proper chain of two prime ideals inside M.

Corollary 4.3. *In the theory of chains $M \supseteq Q_0 \supseteq Q_1$, with M minimal over x we have, if R is Noetherian, for any $a_0, a_1 \in R$*

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

We deduce from this result the following fact about theories. Let T a theory that contains the theory of chains $Q_0 \supseteq Q_1 \supseteq Q_2$. We suppose that the predicate $D(a)$ is not on the theory T and that we have for some given a_0, a_1, x

$$T, D(a), D_1(a_0),\ D_2(a_1) \vdash D_0(a), D(x), D_0(a_0),\ D_1(a_1)$$

for all $a \in R$. If R is noetherian, this implies

$$T, D_1(a_0),\ D_2(a_1) \vdash D_0(a_0),\ D_1(a_1)$$

Using this application, the theorem generalises to give the final version of the Principal Ideal Theorem.

Theorem 4.4. *If R is a Noetherian ring, and $x_1, \ldots, x_n \in R$, then in the theory of chains $M \supseteq Q_0 \supseteq \cdots \supseteq Q_n$ with M minimal over $\langle x_1, \ldots, x_n \rangle$, for any $a_0, \ldots, a_n \in R$ we have*

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

Proof. □

Corollary 4.5. *Let R be a noetherian local ring. Let us denote by $x \notin M$ the predicate "x is invertible". Let $x_1, \ldots, x_n \in \mathrm{Rad}(R) = \{y : (\forall z \in R)\, 1 + xz \notin M\}$. Assume that we have*

$$\forall a \in R\ \left(a \notin M\ \vee\ (\exists m \in \mathbb{N})\, (\exists a_1, \ldots, a_n \in R)\, a^m = a_1x_1 + \cdots + a_nx_n\right).$$

Then the Krull dimension of R is $\leq n$ with the constructive meaning given in [1].

References

[1] Coquand Th., Lombardi H. *Constructions cachées en algèbre abstraite (3) Dimension de Krull, Going Up, Going Down*, preprint

[2] Coste M., Lombardi H., Roy M.-F. *Dynamical method in algebra : Effective Nullstellensätze* to appear in Annals of Pure and Applied Logic.

[3] Eisenbud D. *Commutative algebra. With a view toward algebraic geometry.* Graduate Texts in Mathematics, 150. Springer-Verlag, New York, 1995.

[4] Kaplansky, I. *Commutative Rings.* Allyn and Bacon, Inc., Boston, Mass. 1970

[5] Wraith, G. *Intuitionistic algebra: some recent developments in topos theory.* Proceedings of the International Congress of Mathematicians (Helsinki, 1978), pp. 331–337, Acad. Sci. Fennica, Helsinki, 1980.

[1] This argument can be interpreted as saying that R is Noetherian in the sheaf model over X, and shows that the notion of being Noetherian is invariant under change of bases.

Department of Computer Science, Chalmers University of Technology and Gothenburg University, SE-412 96 Göteborg, Sweden. E-mail: coquand@cs.chalmers.se