Hidden constructions in abstract algebra (1) Integral dependance

Henri Lombardi [1]

December 2000

Abstract

We give an elementary method, hidden in a theorem of abstract algebra, for constructing integral dependance relations. We apply this method in order to give a constructive proof of a theorem of Kronecker.

MSC 2000 : 13B21, 03F65, 13F30

KeyWords : Valuation ring, Integral dependance relations, Constructive Mathematics.

A French version of this paper is available: send an email to the author.

Introduction

In this paper all rings are commutative with unity.

We continue here the work using the philosophy developed in papers [2, 4, 6, 7, 8, 9, 10].

Let us recall the following theorem due to Kronecker (cf. [5, 3]).

Theorem (Kronecker) *Let A be a commutative ring and inside $A[X]$*

$$f(X) = \sum_i f_i X^i = g(X)h(X) = \left(\sum_j g_j X^j\right)\left(\sum_k h_k X^k\right)$$

Then each $g_j h_k$ is integral over the ring generated by the f_i's.

Here are two interesting corollaries.

Corollaries

a) Let A be a normal ring, K its total quotient ring, and $f(X) \in A[X]$. Assume that $f(X) = g(X)h(X)$ in $K[X]$ and that the A-module generated by the coefficients of h contains 1. Then $g(X) \in A[X]$.

b) Let A a be a Prüfer ring, $g(X)$, $h(X) \in A[X]$ and $f(X) = g(X)h(X)$. The product of the ideals generated respectively by the coefficients of g and those of h is the ideal generated by the coefficients of f.

[1] Equipe of Mathématiques, UMR CNRS 6623, UFR des Sciences et Techniques, Université of Franche-Comté, 25030 BESANCON cedex, FRANCE, email: lombardi@math.univ-fcomte.fr

Kronecker's theorem, (or some variants), is needed for some constructive treatments of divisor theory (cf. [5, 11]). A constructive proof by Hurwitz is given in [5]. It would be also interesting to study the variants contained in [11].

In [3], this theorem is proved in an explicit way by using an abstract non-constructive proof and by making a suitable transformation of the proof. Using corollary 4.7 in [4], it is also possible to transform the abstract proof in order to give a constructive one. In the two cases, this transformation of an abstract proof in an explicit computation is directly inspired by logical methods. This is elegant, but not so easy to understand.

We present here another method, which has close relations with the two previous ones. This method is purely algebraic. Perhaps it gives less head hache.

1 The principle of the method

We consider a subring A of a ring B and an element x of B. We search for an integral dependance relation for x over A. The usual classical abstract argument uses a valuative criterion. One considers an arbitrary homomorphism $\varphi : B \to K$ where K is a valued field, V being its valuation ring, with $\varphi(A) \subset V$, and one shows that these hypotheses imply $\varphi(x) \in V$. The valuative criterion allows us to conclude that x is integral over A.

In the case where B is an integral domain, the valuative criterion can be expressed in the following form: the intersection of valuation rings of $\mathrm{Frac}(B)$ containing A is equal to the integral closure of A in $\mathrm{Frac}(B)$.

The idea of our method is the following one. We examine carefully the classical proof, and we consider the valuation ring V as an ideal object, which helps our steps. We replace ideal computations inside V by concrete computations inside suitable extensions of A. Indeed we see in the classical proof that certain computations can be made inside V by applying the principle: $\forall \alpha, \beta \in K$ such that $\alpha\beta = 1$, α is in V or β is in the maximal ideal of V. This principle is always applied to elements α, β that are given by the proof itself.

We repeat the same proof, and we replace each disjunction

"α is in V or β is in the radical (the maximal ideal) of V",

by the consideration of two new rings $C_1 = C[\alpha]$ and $C_2 = C[\beta]_{1+\beta C[\beta]}$, where C is some extension of the ring A, previously computed when following the proof step by step. So

"α is in C_1 and β is in the radical of C_2".

When the initial proof is unfolded in such a way as a tree, we have constructed at the end a finite number (finite since the proof is finite) of extensions A_i. Over each A_i the integral dependance relation is constructed. And the method of construction of the A_i's allows the gluing of these "local" integral dependance relations in a "global" integral dependance relation over A.

In fact, in order for everything to run well through our successive extensions of the ring A, we need a new category, slightly different from the category of commutative rings. We want an element we have forced to be in the radical never to go out of the radical when making a new ring extension. In this "good category" (from a computational point of view) objects are pairs (A, J) where A is a commutative ring and J is an ideal contained in the radical of A, and arrows from (A, J) to (A', J') are homomorphisms $f : A \to A'$ such that $f(J) \subset J'$. We find usual rings when $J = 0$ and local rings with local morphisms when A is local and J is the maximal ideal.

Such a pair (A, J) can be seen as an incomplete specification for a local ring $A_{\mathcal{P}}$ where $\mathcal{P}$ is a maximal ideal of A.

In this paper we use pairs $(A[\alpha_1, \dots, \alpha_n], \langle \gamma_1, \dots, \gamma_m \rangle)$. These pairs could be seen as incomplete specifications for valuation rings of K containing A.

Nevertheless, there is no need to use the good category explicitly and we work with a simplified version, sufficient to run a constructive proof.

In all papers of the series “Hidden constructions in abstract algebra” (Constructions cachées en algèbre abstraite) we use the idea of replacing abstract objects by incomplete specifications of these objects. For the existence of abstract objects, some use of nonconstructive devices is needed. Nevertheless, classical proofs that use these abstract objects can be reread as concrete proofs about incomplete specifications of these objects.

In this paper the method can also be seen, in fact, as a complete explicitation of computations that are used implicitely in the method of dynamical evaluation given in [4].

2 Gluing integral dependance relations

The “good category” leads to the following definition.

Definition 1 *Let J be an ideal in a subring A of a ring B and $x \in B$. We say that x is integral over (A, J) when we have an integral dependance relation*

$$(1 + j)x^{n+1} = a_1x^n + a_2x^{n-1} + \cdots + a_nx + a_{n+1}$$

where $j \in J$ and all $a_i \in A$.

Let us remark that x is integral over A with the usual meaning if and only if it is integral over $(A, \{0\})$ (or over $(A, \mathrm{Rad}(A))$) with the meaning of the above definition. Symetrically, x is integral over the pair (A, J) iff it is integral over the ring A_{1+J} with the usual meaning.

The concrete content of the valuative criterion can be found by a close inspection of any proof of this criterion, and is given by the following theorem. This theorem allows us to work with the method explained in the section 1.

The proof uses the resultant of two univariate polynomials. Once more, this shows that “éliminer l’élimination” is a very bad idea.

Theorem 2 *Let J be an ideal in a subring A of a ring B and $x \in B$. Let $\alpha, \beta \in B$ such that $\alpha\beta = 1$, if x is integral over $(A[\alpha], JA[\alpha])$ and over $(A[\beta], \beta A[\beta] + JA[\beta])$ then x is integral over (A, J).*

Proof We write the hypotheses, and we find the conclusion by eliminating α and β. Let us see more precisely how this computation works. The fact that x is integral over $(A[\alpha], JA[\alpha])$ corresponds to an integral dependance relation

$$a(\alpha, x) = (1 + j_1(\alpha))x^n + a_{n-1}(\alpha)x^{n-1} + \cdots + a_1(\alpha)x + a_0(\alpha) = 0 \qquad (1)$$

where j_1 has coefficients in J and $a_0, \dots, a_{n-1}$ have coefficients in A. Let s be a bound on the degrees.
The fact that x is integral over $(A[\beta], \beta A[\beta] + JA[\beta])$ corresponds to an integral dependance relation

$$b(\beta, x) = (1 + j_2 + \beta b_m(\beta))x^m + b_{m-1}(\beta)x^{m-1} + \cdots + b_1(\beta)x + b_0(\beta) = 0 \qquad (2)$$

where $j_2 \in J$ and $b_0, \dots, b_{m-1}, \beta b_m$ are polynomials in β of degrees $\leq r$ and have coefficients in A. We multiply (1) by β^s in order to eliminate α and we obtain

$$c(\beta, x) = (\beta^s + j_3(\beta))x^n + c_1(\beta)x^{n-1} + \cdots + c_{n-1}(\beta)x + c_n(\beta) = 0 \qquad (3)$$

where j_3 has degree $\leq s$ and coefficients in J and $c_1, \dots, c_n$ have degrees $\leq s$ and coefficients in A. Now we see the LHS in (2) and (3) as polynomials in β whose coefficients are polynomials in x. So (2) is rewritten

$$d(x, \beta) = d_r(x)\beta^r + d_{r-1}(x)\beta^{r-1} + \cdots + d_1(x)\beta + d_0(x) = 0 \qquad (4)$$

where $d_0, \dots, d_r$ have degrees $\leq m$ and coefficients in A and

$$d_0(x) = (1 + j_2)x^m + d_{0,m-1}x^{m-1} + \cdots + d_{0,0} \qquad j_2 \in J$$

In a similar way (3) is rewritten

$$e(x, \beta) = e_s(x)\beta^s + e_{s-1}(x)\beta^{s-1} + \cdots + e_1(x)\beta + e_0(x) = 0 \qquad (5)$$

where $e_0, \dots, e_s$ have degrees $\leq n$ and coefficients in A,

$$e_s(x) = (1 + j_{3,s})x^n + e_{s,n-1}x^{n-1} + \cdots + e_{s,0} \qquad j_{3,s} \in J$$

and for $\ell < s$

$$e_\ell(x) = j_{3,\ell}x^n + e_{\ell,n-1}x^{n-1} + \cdots + e_{\ell,0} \qquad j_{3,\ell} \in J$$

In ring A the T-polynomials $d(x, T)$ and $e(x, T)$ have a common zero β, so the resultant (w.r.t. T) is zero (since it annihilates the vector $(1, \beta, \dots, \beta^{r+s})$). The resultant is the determinant of some Sylvester matrix: its pattern is $(r + s)\times(r + s)$, its first r columns are filled with the coefficients of $e(x, T)$ and the s last ones with those of $d(x, T)$.

$$\begin{pmatrix}
e_s(x) & 0 & \cdots & \cdots & 0 & d_r(x) & 0 & \cdots & 0 \\
\vdots & e_s(x) & \ddots & & \vdots & \vdots & d_r(x) & & \vdots \\
 & & \ddots & & & & & & \\
\vdots & & & & & & & \ddots & 0 \\
e_1(x) & & & & & & & & d_r(x) \\
e_0(x) & & & \ddots & & \vdots & & & \vdots \\
 & \ddots & & & e_s(x) & d_1(x) & & & \\
\vdots & \ddots & & & \vdots & d_0(x) & & & \\
 & & & & & 0 & \ddots & & \\
 & & & & & \vdots & \ddots & & \\
\vdots & & \ddots & \ddots & \vdots & & & \ddots & \vdots \\
0 & \cdots & & 0 & e_0(x) & 0 & \cdots & 0 & d_0(x)
\end{pmatrix}$$

When we express this determinant we get a polynomial $h(x)$ of degree $\leq rn+sm$ with coefficients in A. The coefficient h_{rn+sm} of x^{rn+sm} may be viewed as a sum of two terms. The first one is the leading coefficient inside the product $e_s(x)^r d_0(x)^s$ (given by the diagonal of the matrix). The second one is a sum given by the non-diagonal products. As the only non-zero product using all the $e_s(x)$ on the diagonal is the product of all diagonal elements, any other non-zero product contains at least one $e_\ell(x)$ with $\ell < s$, and this $e_\ell(x)$ has its coefficient of degree n in J. So this coefficient h_{rn+sm} is equal to

$$h_{rn+sm} = (1 + j_{3,s})^r \cdot (1 + j_2)^s + j_4 = 1 + j$$

with $j_4, j \in J$. We are done. $\square$

3 Constructive rereading of the abstract proof of Kronecker's theorem

Hurwitz has given a constructive proof of Kronecker's theorem (cf. [5]). We are interested here by the constructive deciphering of the abstract proof (the usual one today).

This abstract proof is the following one. One considers the case where the g_j's and h_k's in Kronecker's theorem are independent variables, the degrees of g and h being fixed (m and n). One considers $A = \mathbf{Z}[f_i]$, $B = \mathrm{Frac}(\mathbf{Z}[g_j, h_k])$. One shows that each $g_j h_k$ is integral over A by showing that it is in all valuation rings V of B containing A. So one considers the following index j_0: g_{j_0} divides all the g_j, but no g_ℓ with $\ell > j_0$ divides g_{j_0}. In other words

$$\forall j \leq m \;\; g_j/g_{j_0} \in V, \qquad \forall \ell > j_0 \;\; g_\ell/g_{j_0} \in m_V$$

In a similar way one considers the index k_0 such that

$$\forall k \leq n \;\; h_k/h_{k_0} \in V, \qquad \forall \ell > k_0 \;\; h_\ell/h_{k_0} \in m_V$$

We get $g_j h_k \in g_{j_0} h_{k_0} V$ for all j, k. We let $i_0 = j_0 + k_0$ and we write

$$f_{i_0} = g_{j_0} h_{k_0} + \sum_{j_0 < \ell \leq m} g_\ell h_{i_0 - \ell} + \sum_{k_0 < \ell \leq n} h_\ell g_{i_0 - \ell} = g_{j_0} h_{k_0}(1 + \mu)$$

where $\mu \in m_V$. This implies that $(1 + \mu)$ is a unit. As $f_{i_0} \in V$ we get $g_{j_0} h_{k_0} \in V$, which ends the proof.

It is now easy to decipher constructively this proof by using theorem 2. We want to show that $g_j h_k$ is integral over $(A, \{0\})$. In the abstract proof, the determination of indices j_0 and k_0 is made by using many times the axiom

if $\alpha\beta = 1$, then α is in V or β is in m_V

where α is some $g_j/g_{j'}$ or some $h_k/h_{k'}$.

E.g., with $n = 3$, in order to find the good g_{j_0}, and denoting $x \preceq y$ for x divides y ($y/x \in V$) and $x \prec y$ for x divides strictly y ($y/x \in m_V$), we shall make the following disjunctions.

First disjunction. 0: $g_0 \prec g_1$ or 1: $g_1 \preceq g_0$

Branch 0. 00: $g_0 \prec g_2$ or 01: $g_2 \preceq g_0$

Branch 00. 000: $g_0 \prec g_3$ (final result g_0) or 001: $g_3 \preceq g_0$ (final result g_3)

Branch 01. 010: $g_2 \prec g_3$ (final result g_2) or 011: $g_3 \preceq g_2$ (final result g_3)

Branch 1. 10: $g_1 \prec g_2$ or 11: $g_2 \preceq g_1$

Branch 10. 100: $g_1 \prec g_3$ (final result g_1) or 101: $g_3 \preceq g_1$ (final result g_3)

Branch 11. 110: $g_2 \prec g_3$ (final result g_2) or 111: $g_3 \preceq g_2$ (final result g_3)

We look at this search of indexes j_0 and k_0, and each time that the axiom is used, we replace a pair (ring, ideal)

$$(A[\gamma_1, \ldots, \gamma_r], \langle \gamma_{i_1}, \ldots, \gamma_{i_s} \rangle)$$

by two pairs

$$(A[\gamma_1, \ldots, \gamma_r, \alpha], \langle \gamma_{i_1}, \ldots, \gamma_{i_s} \rangle) \quad \text{and} \quad (A[\gamma_1, \ldots, \gamma_r, \beta], \langle \gamma_{i_1}, \ldots, \gamma_{i_s}, \beta \rangle).$$

This gives a tree. At each node there is an extension of $(A, \{0\})$. At the root there is $(A, \{0\})$. At each leaf there is a pair

$$(A[(g_j/g_{j_0})_{0 \leq j \leq m}, (h_k/h_{k_0})_{0 \leq k \leq n}], \langle (g_\ell/g_{j_0})_{j_0 < \ell \leq m}, (h_\ell/h_{k_0})_{k_0 < \ell \leq n} \rangle)$$

For a pair (A', J) that corresponds to such a leaf, we have

$$f_{i_0} = g_{j_0}h_{k_0} + \sum_{j_0<\ell\leq m} g_\ell h_{i_0-\ell} + \sum_{k_0<\ell\leq n} h_\ell g_{i_0-\ell} = g_{j_0}h_{k_0}(1+\mu)$$

where $\mu \in J$. This is in fact a (very simple) integral dependance relation of $g_{j_0}h_{k_0}$ over (A', J) since $\mathbf{Z}[f_{i_0}] \subset A \subset A'$. Since all the g_jh_k are in $g_{j_0}h_{k_0}A'$ they are all integral over (A', J).
Now, considering two given indexes (j, k) we see we have constructed an integral dependance relation for g_jh_k over each pair (ring,ideal) at all the leaves of the tree. Using theorem 2 systematically we glue all these integral dependance relations and we get the integral dependance relation of g_jh_k over $(A, \{0\})$.

4 Gluing integral dependance relations and valuative criterion

Now we show that theorem 2, (we recall it here), is closely related, in classical mathematics, to the valuative criterion (we recall it here).

Theorem 2 *Let J be an ideal in a subring A of a ring B and $x \in B$. Let $\alpha, \beta \in B$ such that $\alpha\beta = 1$, if x is integral over $(A[\alpha], JA[\alpha])$ and over $(A[\beta], \beta A[\beta] + JA[\beta])$ then x is integral over (A, J).*

Theorem 3 (Valuative criterion) *Let J be an ideal in a subring A of a ring B and $x \in B$. Then x is integral over (A, J) if and only if for all homomorphism $\varphi : B \to K$ in a valued field K such that $\varphi(A) \subset V$ and $\varphi(J) \subset m_V$ we have $\varphi(x) \in V$.*

This valuative criterion is in classical mathematics an immediate consequence (via the completeness theorem of Gödel, which is a consequence of Zorn's lemma and third excluded principle) of proposition 4.14 (c) in [4]. This proposition implies indeed as a particular case the following fact: the dynamical evaluation ot the triple (J, A, B) as (m_V, V, K) (in a valued field) shows that $x \in A$ if and only if x is integral over (A, J).

Proof that 3 implies 2 Let us assume that x is integral over $(A[\alpha], JA[\alpha])$ and over $(A[\beta], \beta A[\beta] + JA[\beta])$ as in the hypotheses of theorem 2. Let $\varphi : B \to K$ an arbitrary homomorphism in a valued field K such that $\varphi(A) \subset V$ and $\varphi(J) \subset m_V$.
We have $\varphi(\alpha)\varphi(\beta) = 1$ in K, so $\varphi(\alpha) \in V$ or $\varphi(\beta) \in m_V$.
In the first case, since x is integral over $(A[\alpha], JA[\alpha])$, $\varphi(x)$ is integral over $(\varphi(A[\alpha]), \varphi(J)\varphi(A[\alpha]))$, so it is a fortiori integral over (V, m_V), so it is in V.
In the second case, the same reasoning shows that $\varphi(x)$ is integral over $(\varphi(A[\beta]), \varphi(\beta)\varphi(A[\beta]) + \varphi(J)\varphi(A[\beta]))$, so it is a fortiori integral over (V, m_V).
So the valuative criterion applies, and x is integral over (A, J). □

We need Zorn's lemma in the reverse way.

Proof that 2 implies 3 when B is a domain It is sufficient to consider the case where B is a field. Let x be an element of B such that it is not integral over (A, J). Let us consider the couples (A', J') where A' is a subring of B containing A, J' is an ideal of A' containing J and x is not integral over (A', J'). This set is not empty since it contains (A, J). It has a natural order given by

$$(A', J') \leq (A'', J'') \text{ if and only if } A' \subset A'' \text{ and } J' \subset J''$$

By Zorn's lemma, there exists a maximal pair (V, m) in this set. Let us show that V is a valuation ring of B and m is its maximal ideal. Let $\alpha \in B$, $\beta = 1/\alpha$. We want to show that $\alpha \in V$ or $\beta \in m$.

Since x is not integral over (V, m), theorem 2 gives:

$$x \text{ is not integral over } (V[\alpha], mV[\alpha]) \text{ or } x \text{ is not integral over } (V[\beta], \beta V[\beta] + mV[\beta])$$

Since the couple (V, m) is maximal, it is equal to one of the above. This means that $\alpha \in V$ or $\beta \in m$. □

Finally, let us remark that Gödel's completeness theorem does not use the full strength of the Third Excluded Principle and Choice. In the case of formal theories with a countable presentation, it can be easily seen that Gödel's completeness theorem is a consequence of a combination of countable choice and of the non-constructive principle **LLPO**, meaning that each real number is ≥ 0 or ≤ 0 (see e.g. [1]).

Conclusion

Our constructive proof is obtained by a simple rereading of arguments inside an abstract proof, without adding any new ingredient. Using this rereading method gives a priori less algorithmic efficiency than in other constructive proofs. Our method has not been thought of in order to give good algorithmic bounds. It has been thought of in order to bring good news: abstract methods in algebra are in fact constructive.

We think that this kind of method is able to realize a kind of Hilbert's program for large parts of abstract algebra: giving constructive semantics for abstract objects and getting constructive proofs for concrete results when they are obtained through abstract non-constructive methods.

In this paper finite extension-trees of the pair $(A, \{0\})$ constitute the constructive semantics for the consideration of all valuation rings inside the quotient field of A. The deciphering of the abstract proof is based on theorem 2 which is the constructive form of the valuative criterion. And the constructive proof of this theorem is hidden in any abstract proof of the valuative criterion. So the constructive proof is really hidden in the abstract one.

References

[1] Bishop E., Bridges D.: *Constructive Analysis*. Springer-Verlag (1985). 7

[2] Coquand T., Lombardi H. *Constructions cachees en algèbre abstraite (3) Dimension de Krull, Going Up, Going Down*. Preprint 2001. 1

[3] Coquand T., Persson H. *Valuations and Dedekind's Prague Theorem*. J. Pure Appl. Algebra 155 (2001), no. 2-3, 121–129. 1, 2

[4] Coste M., Lombardi H., Roy M.-F. *Dynamical method in algebra : Effective Nullstellensätze*. To appear in Annals of Pure and Applied Logic. 1, 2, 3, 6

[5] Edwards H. M. *Divisor theory*. Birkhaüser. Boston MA. 1990. 1, 2, 5

[6] Lombardi H. *Le contenu constructif d'un principe local-global avec une application à la structure d'un module projectif de type fini*. Publications Mathématiques de Besançon. Théorie des nombres. Fascicule (1997), 94–95 & 95–96. 1

[7] Lombardi H. *Relecture constructive de la théorie d'Artin-Schreier.* Annals of Pure and Applied Logic **91**, (1998), 59–92. 1

[8] Lombardi H. *Dimension de Krull, Nullstellensätze et Évaluation dynamique*. To appear in Math. Zeitschrift. 1

[9] Lombardi H., Quitté C. *Hidden constructions in abstract algebra (2) Horrocks theorem, from local to global)*. Preprint 1999. 1

[10] Lombardi H. *Platitude, localisation et anneaux de Prüfer, une approche constructive.* Preprint 1999. 1

[11] Weyl H. *Algebraic Theory of Numbers.* Princeton landmarks in mathematics, (1998). (first edition 1940) 2