Kolchin Seminar, March 15, 2003

STANDARD BASES IN COMMUTATIVE AND DIFFERENTIAL ALGEBRA

E.V. PANKRATIEV

Moscow team

Professors and researchers:
A. Mikhalev, E. Pankratiev, M. Kondratieva,
A. Astrelin
Post-graduate students:
V. Mityunin, A. Semenov,
O. Golubitsky (New Brunswick)
Students:
A. Zobnin, A. Ovchinnikov, etc.

`http://shade.msu.ru/~difalg`

(1) Standard bases in polynomial ideals
- Gröbner bases
- involutive bases
- characteristic sets (Wu's method)

(2) differential modules
(3) Ritt-Kolchin algorithm
(4) Carra-Ferro and Ollivier approach
(5) Mansfield's results
(6) Rosenfeld-Gröbner method
(7) Hubert approach

1. Standard bases in polynomial ideals

Gröbner bases.

Monomial orderings. Let $R = k[x_1, \dots, x_m]$ be the ring of polynomials in variables $x_1, \dots, x_m$ over a field k. By $T = T(X)$ we denote the commutative semigroup (the semigroup of monomials) generated by elements of X. For $\theta \in T$, $\theta = x_1^{e_1} \dots x_m^{e_m}$, define the degree of θ as $\deg \theta = e_1 + \dots + e_m$. Suppose that the monomials are ordered so that $\forall\ \theta \in T$

$$1 \leq \theta, \tag{1}$$

$$\theta_1 < \theta_2 \implies \theta\theta_1 < \theta\theta_2. \tag{2}$$

Such an ordering is called admissible.

- lexicographic ordering;
- total degree then lexicographic ordering;
- total degree then inverse lexicographic.

Notation. For any two monomials θ_1, θ_2, we can define their least common multiple $\theta = \phi_1\theta_1 = \phi_2\theta_2$. An admissible ordering being given, we can define for any polynomial f its leading monomial $\mathrm{Lm}(f)$, its highest coefficient $\mathrm{Hcoeff}(f)$, and its highest term $\mathrm{Hterm}(f) = \mathrm{Hcoeff}(f) \cdot \mathrm{Lm}(f)$.

For any two polynomials $f_1, f_2 \in R$, we define their S-polynomial $S(f_1, f_2) = \mathrm{Hcoeff}(f_2)\phi_1 f_1 - \mathrm{Hcoeff}(f_2)\phi_2 f_2$, where $\phi_1 \cdot \mathrm{Lm}(f_1) = \phi_2 \cdot \mathrm{Lm}(f_2) = \mathrm{LCM}(\mathrm{Lm}(f_1), \mathrm{Lm}(f_2))$.

Suppose that a polynomial $f \in R$ contains a term $c\phi$, where $\phi \in T$, $0 \neq c = c(f, \phi) \in k$, which is divisible by $\mathrm{Lm}(g)$: $\phi = \psi \cdot \mathrm{Lm}(g)$. Then we define the reduction relation $f \underset{g}{\to} h$, where $h = f - c(f, \phi) \cdot \psi \cdot g / \mathrm{Hcoeff}(g)$. We write $f \underset{G}{\to} h$ if there is $g \in G$ such that $f \underset{g}{\to} h$. For a reduction relation $\to$, we can define its transitive closure $\xrightarrow{+}$, its reflexive-transitive closure $\xrightarrow{*}$, and its symmetrical-reflexive-transitive closure $\overset{*}{\leftrightarrow}$.

Main Theorem.

Theorem 1. *Let I be an ideal of the ring $R = k[x_1, \dots, x_m]$, $<$ an admissible ordering of monomials T, $G \subset I$ an autoreduced set. Without loss of generality, we may assume that* $\mathrm{Hcoeff}(g_i) = 1$ *for any $g_i \in G$. Then the following conditions are equivalent:*

(1) *G is an autoreduced set of minimal rank in the ideal I;*
(2) *any $f \in I$ admits a G-representation;*
(3) $\mathrm{Lm}(G)$ *generates* $\mathrm{Lm}(I)$*;*
(4) $f \in I \iff f \underset{G}{\xrightarrow{*}} 0$*;*

The following conditions are necessary for preceding ones and, if G generates I, they are also sufficient:

(4) *if $f \underset{G}{\xrightarrow{*}} f'$, $f \underset{G}{\xrightarrow{*}} f''$ where f' and f'' are irreducible, then $f' = f''$;*
(5) $S(f, f') \underset{G}{\xrightarrow{*}} 0$ *for any $f, f' \in G$;*
(6) *if $f, f' \in G$, then in G there are polynomials $f = f_0, \dots, f_i, \dots, f_r = f'$ such that*

$$\mathrm{LCM}\{\mathrm{Lm}(f_i) : i = 0, \dots, s\} = \mathrm{LCM}(\mathrm{Lm}(f), \mathrm{Lm}(f')) \qquad (3)$$

and $S(f_{i-1}, f_i) \underset{G}{\xrightarrow{*}} 0$ *for any $i = 1, \dots, r$.*

Completion Algorithm. The general form of an algorithm for determining a Gröbner basis based is the following:

input: a set of polynomials $G = \{g_1, \dots, g_l\}$.
output: the Gröbner basis $G = \{g_1, \dots, g_k\}$ of the ideal (G).

```
begin
for any pair $(g_i, g_j)$
        if not criterion$(g_i, g_j)$ then
          compute the normal form $NF(S(g_i, g_j))$ of $S(g_i, g_j)$
          if $NF(S(g_i, g_j)) \neq 0$ then
            $G = G \cup \{NF(S(g_i, g_j))\}$
end
```

Normal form algorithm and normal G-representation. The strategies for choosing the current pair in the completion algorithm and their influence on the complexity of the algorithm are investigated in detail in many papers. Here, we would like to emphasize the role of the normal form algorithm. It is natural to reformulate the definitions of Gröbner bases in terms of normal form algorithms.

Definition 1. Let a reduction relation $\underset{G}{\rightarrow}$ on the ring R be given and suppose that we have a computable function $\mathrm{Sel} : R \to R$ such that $f \underset{G}{\rightarrow} \mathrm{Sel}(f)$ for any reducible $f \in F$. Consider the computable function S defined recursively by the formula

$$S(f) := \begin{cases} f, & \text{if } f \text{ is irreducible} \\ S(\mathrm{Sel}(f)), & \text{if } f \text{ is reducible.} \end{cases}$$

We call an S of this kind a *normal reduction process* or a *normal-form algorithm* for $\underset{G}{\rightarrow}$ and denote it as $\underset{G}{\Longrightarrow}$. For example, we can choose the terms being reduced in descending order and for a fixed term we try apply the reducing elements in the order, they are listed in G. Similarly, a finite set G being fixed, for any partial one-valued function $\mathrm{Sel} : T \to G$ such that $\mathrm{Sel}(\theta)$ is defined $\iff$ $\exists g \in G$ such that $\mathrm{Lm}(g)|\theta$ and in this case $\mathrm{Lm}(\mathrm{Sel}(\theta))|\theta$, we can define a normal G-representation as a G-representation whose terms are consistent with this function.

Theorem 2. *Let I be an ideal of the ring $R = k[x_1, \ldots, x_m]$, $<$ an admissible ordering of monomials T, $G \subset I$ a subset of I. Without loss of generality, we may assume that* $\mathrm{Hcoeff}(g_i) = 1$ *for any $g_i \in G$. Then, for any normal-form algorithm, G is a Gröbner basis of I iff one of the following equivalent conditions holds*

$2'$. *any $f \in I$ admits a normal G-representation;*

$4'$. *for any $f \in I$, we have $f \overset{*}{\underset{G}{\Longrightarrow}} 0$;*

The following conditions are necessary for preceding ones and, if G generates I, they are also sufficient:

$5'$. $S(f, f') \overset{*}{\underset{G}{\Longrightarrow}} 0$ *for any $f, f' \in G$;*

$6'$. *if $f, f' \in G$, then in G there are polynomials*

$$f = f_0, \ldots, f_i, \ldots, f_r = f'$$

which satisfy condition (3) *and are such that* $S(f_{i-1}, f_i) \xRightarrow[G]{*} 0$ *for any* $i = 1, \dots, r$.

Involutive bases.

Involutive divisions.

Definition 2. We say that an involutive division L is specified on the monoid T if, for any finite subset $U \subset T$ and for any monomial $u \in U$, a submonoid $L(u, U)$ of T is specified such that

(1) if $w \in L(u, U)$ and $v|w$, then $v \in L(u, U)$;
(2) if $u, v \in U$ and $uL(u, U) \cap vL(v, U) \neq \emptyset$, then $u \in vL(v, U)$ or $v \in uL(u, U)$;
(3) if $v \in U$ and $v \in uL(u, U)$, then $L(v, U) \subseteq L(u, U)$;
(4) if $V \subseteq U$, then $\forall\ u \in V\ L(u, U) \subseteq L(u, V)$.

The generators of the monoid $L(u, U)$ are called *multiplicative variables* for u. If $w \in uL(u, U)$, then we write $u\big|_L w$ and the monomial u is called an *(L-) involutive divisor of the monomial* w, and the monomial w is called an *(L-) involutive multiple* of u. In this case, we write the equality $w = uv$ as $w = u \times v$, otherwise as $w = u \cdot v$, and the monomial v is called *nonmultiplicative* for u.

Example 1. (1) $M(x_1^{i_1} \dots x_k^{i_k}) = \{x_k, \dots, x_m\}$ (*the right Pommaret division*).
(2) $M(x_k^{i_k} \dots x_m^{i_m}) = \{x_1, \dots, x_k\}$ (*the left Pommaret division*),
(3) $M(x_1^{i_1} \dots x_m^{i_m}) = \{x_k\ :\ i_k = \max_{n=1}^{m} i_n\}$.
(4) Let $U \subset T$ be a finite set. For any $1 \leq i \leq m$, we partition U into groups labeled by nonnegative integers $d_1, \dots, d_i$:

$$[d_1, \dots, d_i] = \{u \in U \mid d_j = \deg_j(u),\ 1 \leq j \leq i\}.$$

The variable x_i is multiplicative for $u \in U$ if $i = 1$ and $\deg_1(u) = \max\{\deg_1(v) \mid v \in U\}$, or $i > 1$, $u \in [d_1, \dots, d_{i-1}]$ and $\deg_i(u) = \max\{\deg_i(v) \mid v \in [d_1, \dots, d_{i-1}]\}$.

Involutive bases.

Definition 3. We say that a polynomial f is *involutively reducible to* g *by polynomial* h *at a monomial* m, present in f, and without mentioning the monomial m we write $f \xrightarrow[\text{inv } h]{} g$, if f is reducible to g in the usual sense and $\mathrm{Lm}(h)\big|_L m$. The relation $\xrightarrow[\text{inv } G]{}$ for an arbitrary set G of polynomials, as well as its transitive $\xrightarrow[\text{inv } G]{+}$ and reflexive-transitive $\xrightarrow[\text{inv } G]{*}$ closures are defined in the natural way. If a reduction relation is given, the a *normal-form* is defined. In this case it is called *involutive*. A *nonmultiplicative prolongation of a polynomial* is defined as its product by a variable which is nonmultiplicative for its leading monomial.

Definition 4. Let $R = K[x_1, \dots, x_m]$ be a polynomial ring, $X = \{x_1, \dots, x_m\}$, I be an ideal of R, $G \subset I$ be a finite set, and $\big|_L$ be an involutive division on the set of monomials T. The set G is called an *involutive basis* if the ideal I if, for any nonzero $f \in I$ there is an *involutive representation*:

$$f = \sum_{i=1}^{r} c_i \theta_i g_{j(i)}, \quad 0 \neq c_i \in K,\ \theta_i \in T(M(\mathrm{Lm}(g_i))),\ g_{j(i)} \in G. \tag{4}$$

Theorem 3. *Let $R = K[x_1, \dots, x_m]$ be a polynomial ring in the variables $X = \{x_1, \dots, x_m\}$, I be an ideal of R, $G \subset I$ be a finite set, and $\big|_L$ be an involutive division on the set of monomials T. Suppose that $\mathrm{Hcoeff}(g_i) = 1$ for any $g_i \in G$. Then, the following conditions are equivalent:*

(1) *G is an involutive basis of the ideal I;*
(2) *$\mathrm{Lm}(G)$ involutively generates $\mathrm{Lm}(I)$;*
(3) *for any $f \in I$, we have $f \xrightarrow[\textit{inv } G]{*} 0$;*
(4) *if $f - f' \in I$ and f, f' are involutively irreducible, then $f = f'$;*
(5) *if $f \in I$ and f is involutively irreducible, then $f = 0$.*

The following conditions are necessary for preceding ones and, if G generates I, they are also sufficient:

(6) *if $f \in G$ and $x_i \in NM(\mathrm{Lm}(f))$, then $x_i f$ admits an involutive representation;*
(7) *$x_i f \xrightarrow[\textit{inv } G]{*} 0$ for any $f \in G$ and $x_i \in NM(\mathrm{Lm}(f))$.*

Characteristic sets (Wu's method). This method is the closest to the methods used in differential algeba. Its specific features:

- in any polynomial, a leading variable (leader) is chosen;
- reduction relation is replaced by pseudoreduction relation;
- the variables are divided into "leaders" and "nonleaders";
- the results are divided into those valid "in general" and "in particular cases".

Applications of standard bases.

- Consistemsy of systems of algebraic equations;
- Hilbert functions;
- geometrical applications (Wu's method).

Problems under consideration.

- Comparison of Gröbner bases and involutive bases;
- numerical experiments: sequential and parallel methods (Mityunin *et al.*);
- "good" involutive divisions: comparison of "admissible" and "continuous" divisions (Semenov), projections of involutive divisions (Shemyakova);
- classification of admissible monomial orderings, investigation of orderings of differential monomials (Zobnin, Ovchinnikov);

- study of monomial orderings preserving Gröbner bases (Zobnin);
- passage from one involutive bases to another one (involutive Gröbner walk) (Golubitsky)

Differential modules. Let $\mathcal{F}$ be a differential field with a set $\Delta = \{\delta_1, \dots, \delta_m$ of derivation operators, $D = \mathcal{F}[\delta_1, \dots, \delta_m]$ be the ring of linear differential operators over $\mathcal{F}$ and M be a finitely generated (left) D-module. The theory of standard bases (Gröbner, involutive bases and characteristic sets) can be applied to submodules of M. In particular, the Hilbert polynomials (differential dimension polynomials) can be computed.

However, in this case, the Hilbert polynomials are not invariant with respect to changes of variables. For any submodule there exist a minimal differential dimension polynomial, but its determination is a difficult problem.

2. Standard bases in differential algebra

Considering the ring of differential polynomials $\mathcal{R} = \mathcal{F}\{y_1, \dots, y_n\}$ over a differential field $\mathcal{F}$ with a set of derivation operators $\Delta = \{\delta_1, \dots, \delta_m\}$. To construct a theory of standard bases in this ring, we should

(1) standardize the main definitions;
(2) determine the set of ideals under consideration;
(3) develop algorithmic procedures.

Problems arise when introducing definitions

- reduction procedure;
- autoreduced sets $\mathcal{A}$ (whether $\{1\}$ is an autoreduced set);
- coherent autoreduced sets (several nonequivalent definitions),
- characteristic sets of a differential ideal.

The possibilities for the class of ideals under consideration:

- differential ideals;
- radical (perfect) differential ideals;
- prime differential ideals;
- regular differential ideals;
- etc.

The main tool used for investigation of differential ideals is the theory of autoreduced (characteristic) sets developed by J. Ritt and E. Kolchin. It is known that, for a prime differential ideal I, if an autoreduced set $\mathcal{A}$ satisfies property (1) (is minimal), then properties (4) (normal simplifier) and (5) (coherence) are also fulfilled. The problem is how to construct the primary decomposition of a perfect differential ideal $I = \{\mathcal{A}\}$? This problem is very hard.

Definitions and notation. We introduce an admissible order on the set of derivatives $\Theta = \{\delta_1^{i_1} \dots \delta_m^{i_m} y_j\}$, where $i_1, \dots, i_m \geq 0$, $1 \leq j \leq n$. For any differential polynomial $f \in \mathcal{R}$, the highest derivative $\theta \in \Theta$ present in f is called the *leader* of f (we write $\theta = L_f$). By $S_f = \partial f / \partial L_f$ we denote the *separant* of f and by I_f we denote the *initial* of f (the leading coefficient of f considered as a polynomial in L_f), and we denote $H_f = S_f I_f$. The relation of differential reduction $f \underset{g}{\rightarrow} f_1$ allows one to eliminate form f the proper derivatives of L_g as well as the powers of L_g higher than or equal to those present in g. However, in this process, we should multiply f by some powers of S_g and I_g; hence, we cannot obtain in this way a relation satisfying property (4) (a canonical simplifier).

Consider a perfect differential ideal $I = \{\mathcal{A}\}$ generated (as a perfect differential ideal) by one irreducible ordinary differential polynomial $\mathcal{A} = \{f\}$. The primary decomposition of I consists in this case of a general component, for which $\mathcal{A}$ is the minimal autoreduced set, and, possibly, singular components. As a rule, f does not generate the general component as the differential ideal $\{\mathcal{A}\}$. M.V. Kondratieva proposed a partial method for determining the generators of this prime differential ideal and for constructing the primary decomposition. She also obtained the following sufficient condition for the perfect differential ideal $I = \{\mathcal{A}\}$ to be prime.

Theorem 4. *Let* $f = y^{(k)}y^{(s)} + y^{(k+1)} + y^{(k)} * g(y, y', \ldots y^{(s+1)})$, *where* $s > k + 1$. *Then,* $[f] : H_f^{\infty} = \{f\}$.

Ritt-Kolchin algorithm.

Input: $\Phi = \{f_1, \ldots, f_r\}$ is a finite set of Δ-polynomials
Output: $\mathcal{A}$ is a coherent autoreduced set of Δ-polynomials
$[\mathcal{A}] \subseteq [\Phi] \subseteq [\mathcal{A}] : H_{\mathcal{A}}^{\infty}$

```
Begin
$\mathcal{A} := \mathcal{A}(\Phi)$
if $\mathcal{A} = \{f\},\ f \in \mathcal{F}$ then
                    return
else
                    $G := \Phi \setminus \mathcal{A}$
                    $W := \emptyset$
                    for any $g \in G$
                        $r :=$ remainder of $g$ with respect to $\mathcal{A}$
                        if $r \neq 0$ then
                          $W := W \cup \{r\}$
                    for any pair $f_i, f_j \in \mathcal{A}$
                        $r :=$ remainder of $S_\Delta(f_i, f_j)$ with respect to $\mathcal{A}$
                        if $r \neq 0$ then
                          $W := W \cup \{r\}$
                    if $W \neq \emptyset$ then
                        $\Phi := \Phi \cup W$
                        Algorithm RK1 $(\Phi, \mathcal{A})$
End
```

Carra-Ferro and Ollivier approach. F. Ollivier and Carra-Ferro endow the set of differential monomials with an admissible order and defines derivation operations on the set of differential monomials (note that a derivation operation applied to a differential monomial in the ring of differential polynomials gives a differential polynomial). Then, he defines a standard basis of a differential ideal as a set satisfying property 3 of Theorem 1 for differential ideals. The main deficiency of this definition is that, as a rule, such a basis is infinite. For example, the standard basis in this sense for the differential ideal $[y^2]$ in the ring of ordinary differential polynomials $C\{y\}$ is infinite.

Mansfield's results. Constructing the theory of differential Gröbner bases, E. Mansfield considers autoreduced differential systems satisfying some additional conditions, namely, CNI (Coherent with Null Intersection), SPR ($S(G)$ is Pseudo-Reduced), and GAC (G is Almost Complete).

Rosenfeld-Gröbner method. Other generalizations of the Buchberger algorithm deal with some classes of differential ideals different from the prime ones. The most fruitful algorithm used in constructive differential algebra is proposed by Boulier, Lazard, Ollivier, and Petitot, and is known as the Rosenfeld–Gröbner algorithm. This algorithm represents a perfect differential ideal as an intersection of *regular* differential ideals. In contrast to the primary decomposition, this representation depends on the ranking of differential indeterminates.

Some numerical experiments. In a series of numerical experiments, the systems of Euler equations in two and three space variables were considered for different rankings by N. Makarevich. It was found out that not only the computation time and the memory used depend on the ranking, but also the number of components is different for different rankings. For some rankings, we did not succeed in determining the regular representation. The most interesting fact is that, for all cases where we did not succeed in determining the regular representation for three space variables, we did not also succeed in determining such a representation for two space variables.

Hubert approach. Another class of differential ideal was introduced by E. Hubert. It is known that, for prime differential ideals, the conditions 4 and 5 are equivalent. Hubert proposed to consider the differential ideals for which these conditions are equivalent, She called such ideals characterizable. Note that the definition of a characterizable ideal depends on the ranking of differential polynomials (there are differential ideal characterizable for one ranking and noncharacterizable for another one).

Differential Gröber walk. It is important to know how to pass from a characteristic set with respect to a ranking of the differential polynomials to the characteristic set with respect to another ranking. A method for solving this problem is proposed by O. Golubitsky. This is a generalization of the algorithm for passing from the Gröbner basis of a polynomial ideal with respect to an admissible ordering of monomials to the Gröbner basis of the same ideal with respect to another ordering.

MOSCOW STATE UNIVERSITY