THE TEACHING OF MATHEMATICS
2013, Vol. XVI, 1, pp. 22–28

POLYNOMIAL DIVISION AND GRÖBNER BASES

Samira Zeada

Abstract. Division in the ring of multivariate polynomials is usually not a part of the standard university math curriculum. However, the algorithm is elementary and it has very important consequences for algebraic computations. In this paper, the algorithm is explained and illustrated with some examples, and the importance of the choice of monomial ordering is stressed. The notion of Gröbner basis is introduced and explained on examples. The paper can be used by math students and teachers as a brief description of this very important topic and introduction for reading more detailed textbooks.

MathEduc Subject Classification: H25, H75
AMS Subject Classification: 97H20
Key words and phrases: multivariate polynomial division; Gröbner basis.

The most important algorithm in the polynomial ring is the division algorithm, which is responsible for many nice properties of rings of integers $\mathbb{Z}$ and polynomials $K[x]$ over a field K. Classical division algorithm for integers goes back to ancient times, and its main properties are described in Euclid's "Elements", including the important Euclidean algorithm for determining the greatest common divisor of two numbers. The corresponding division algorithm for polynomials is possible due to the existence of a natural ordering of monomials $1 < x < x^2 < \cdots < x^n < x^{n+1} < \cdots$ which corresponds to natural ordering of their powers, i.e., of integers: $0 < 1 < 2 < \cdots < n < n+1 < \cdots$. All math students are (or at least, should be) familiar with this division and its properties, including the Euclidean algorithm for polynomials. However, in the multivariate polynomial ring there is no such natural linear ordering. Therefore, there is no natural division algorithm in the ring of polynomials with many variables $K[x_1, \ldots, x_n]$. There are various conventions, leading to a number of different possible "orderings" of monomials and division algorithms. Certainly it is not enough to compare the (total) degree of multivariate monomials, since this would leave us unclear as to whether $x^3y^2z < x^3yz^2$ or $x^3y^2z > x^3yz^2$. It is clear that ordering of monomials is equivalent to ordering of their power exponents: there is a correspondence between a monomial $x^\alpha = x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}$ and its multiindex or exponent $\alpha = (\alpha_1, \ldots \alpha_n) \in \mathbb{N}_0^n$ (the set of nonnegative integers will be denoted by $\mathbb{N}_0$). Monomial orderings are a particular concern in computation and the results of certain important algorithms, such as the division algorithm, can vary depending on which monomial ordering is chosen.

Definition. Let K be a field. A *monomial ordering* on $K[x_1, \ldots, x_n]$ is any partial order relation $<$ on $\mathbb{N}_0^n$ (or equivalently, any partial order relation on the set of monomials $x^\alpha = x_1^{\alpha_1}x_2^{\alpha_2}\ldots x_n^{\alpha_n}$, $\alpha = (\alpha_1, \cdots, \alpha_n) \in \mathbb{N}_0^n$) such that:

1. $<$ is a total (linear) ordering on $\mathbb{N}_0^n$ (this means that every two elements are comparable);

2. if $\alpha < \beta \in \mathbb{N}_0^n$ and $\gamma \in \mathbb{N}_0^n$ then $\alpha + \gamma < \beta + \gamma$ (the additive property);

3. $<$ is a well-ordering on $\mathbb{N}_0^n$ (this means that every nonempty subset of $\mathbb{N}_0^n$ has a smallest element under $<$).

LEMMA. *The element $o = (0, \dots 0) \in \mathbb{N}_0^n$ is necessarily the smallest element in $\mathbb{N}_0^n$ under any such ordering.*

Proof. If $\alpha < o$ then, since $\alpha \in \mathbb{N}_0^n$, the additive property implies that $\alpha + \alpha < o + \alpha$ or $2\alpha < \alpha$. We could repeat this argument to conclude that $o > \alpha > 2\alpha > 3\alpha > \dots$. But then the set $\{0, \alpha, 2\alpha, \dots\}$ does not have a smallest element and the ordering is not a well-ordering.

Note that we have defined a monomial ordering as an ordering on n-tuples $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}_0^n$. Since there is a one-to-one relationship between the monomials in $K[x_1, \dots x_n]$ and $\mathbb{N}_0^n$ so that monomial $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ corresponds to n-tuple α (its exponent), the ordering $<$ on $\mathbb{N}_0^n$ gives us an ordering on monomials in $K[x_1, \dots, x_n]$. This is, if $\alpha < \beta$ then $x^\alpha < x^\beta$. Obviously, the additive property changes to multiplicative property in this case. The monomial ordering in one variable case can also be thought of simply as divisibility. That is, x is smaller than x^2, since x divides x^2. One can easily see that divisibility is not a monomial ordering in $K[x_1, \dots, x_n]$ for $n > 1$, since divisibility cannot help us to decide in general whether one monomial is greater than another. In the terms of exponents, divisibility corresponds to addition: $x^\alpha \mid x^\beta \Leftrightarrow \exists \gamma : \beta = \alpha + \gamma$. This implies, but is not equivalent to $\alpha < \beta$. We must have some way of ordering these variables.

Examples of monomial orderings

1. Lexicographic order

Let $\alpha = (\alpha_1, \dots, \alpha_n)$ and $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{N}_0^n$. We say that $\alpha <_{lex} \beta$ if, in the difference $\beta - \alpha \in \mathbb{Z}^n$, the left-most nonzero entry is positive. So, we say $x^\alpha <_{lex} x^\beta$ if $\alpha <_{lex} \beta$. It is important to realize that there are many *lex* orders, corresponding to how variables are ordered. So far, we have used *lex* order with $x_1 > x_2 > \cdots > x_n$. But given any linear ordering of the variables $x_1, \dots, x_n$, there is a corresponding *lex* order. For example, if the variables are x and y, then we get one *lex* order with $x < y$ and another with $y < x$. In the general case of n variables, there are $n!$ *lex* orders.

2. Graded lexicographic order

Let $\alpha, \beta \in \mathbb{N}_0^n$. We say that $\alpha <_{grlex} \beta$ if $|\alpha| = \sum_{i=1}^n \alpha_i < |\beta| = \sum_{i=1}^n \beta_1$ or $|\alpha| = |\beta|$. and $\alpha <_{lex} \beta$. The number $|\alpha|$ is called the degree of α.

3. Graded reverse lexicographic order

Let $\alpha, \beta \in \mathbb{N}_0^n$. We say that $\alpha <_{grevlex} \beta$ if $|\alpha| = \sum_{i=1}^n \alpha_i < |\beta| = \sum_{i=1}^n \beta_1$ or $|\alpha| = |\beta|$ and in $\beta - \alpha \in \mathbb{Z}^n$ the right-most nonzero entry is negative.

4. Matrix ordering

Let $\alpha, \beta \in \mathbb{N}_0^n$ and let $A \in GL(n, \mathbb{R})$ be an invertible matrix over real numbers. We define a relation $<_A$ on $\mathbb{N}_0^n$ by the condition

$$\alpha <_A \beta \Longleftrightarrow A \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} <_{lex} A \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}.$$

This is a total ordering since A is invertible. It is monomial if for all $\alpha \in \mathbb{N}_0^n$ the first nonzero term of $A \begin{pmatrix} \alpha_1 & \cdots & \alpha_n \end{pmatrix}^\top$ is positive (because the monomial 1 is the minimal element on $M = \{ x^\alpha : \alpha \in \mathbb{N}_0^n \}$, the set of monomials in $K[x_1, \ldots, x_n]$).

Here are some examples of matrix orderings.

The matrix associated with lexicographic ordering in three variables is $E = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, *deglex* is given by $\begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$, and *degrevlex* is given by $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}$. The matrix associated with the given monomial ordering is clearly not uniquely determined.

Definition. Let $f = \sum_\alpha a_\alpha x^\alpha$ be a nonzero polynomial in $K[x_1, \ldots, x_n]$ and let $<$ be a monomial order. Then: the multidegree of f is $multdeg(f) = \max\{\alpha \in \mathbb{N}_0^n : a_\alpha \neq 0\}$ (the maximum is taken with respect to $<$); the leading coefficient of f is $LC(f) = a_{multdeg(f)} \in K$; the leading monomial of f is $LM(f) = x^{multdeg\ (f)}$ (with coefficient 1); the leading term of f is $LT(f) = LC(f) \cdot LM(f)$.

A division algorithm for polynomials

In the division algorithm for polynomials in one variable, for the input of a divisor and a dividend we are guaranteed a unique and well defined output of a quotient and remainder. However, in the case of multivariate polynomials, the "quotients" and remainder depend on the monomial ordering and on the order of the divisors in the division. The division algorithm in the multivariable case allows us to divide $f \in K[x_1, \ldots, x_n]$ by $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$, so that we can express f in the form $f = q_1 f_1 + \cdots + q_s f_s + r$. The strategy is to repeatedly cancel the leading term of f by subtracting off an appropriate multiple of one of the f_i. However, the result of the division algorithm fails to be unique for multivariate polynomials because there may be a choice of divisor at each step.

The division algorithm is described in what follows.

1. Start with $q_1 = q_2 = \cdots = q_i = r = 0$.
2. If $f = 0$, stop. Otherwise, for each $i = 1, \ldots, s$ check if $LT(f_i)$ divides $LT(f)$. If so, replace f by $f - \frac{LT(f)}{LT(f_i)}$, add $\frac{LT(f)}{LT(f_i)}$ to q_i and then return to the beginning of 2). If $LT(g_i)$ does not divide $LT(f)$ for any i, continue to 3.

3. Add $LT(f)$ to r, replace f by $f - LT(f)$, and then return to the beginning of 2.

This algorithm always terminates, because we have built in the definition of a monomial order that it is well-ordered, and the multidegree of f is reduced in each iteration.

Recall that an ideal I in a commutative ring R is an additive subgroup in R which has the ideal property: $a \in R, b \in I \Rightarrow ab \in I$. The ideal $I = \langle b_1, \ldots, b_n \rangle \subset R$ generated by $b_1, \ldots, b_n \in R$ is the set of all elements of the form $a_1 b_1 + \cdots + a_n b_n$, where $a_1, \ldots, a_n \in R$. Now, if the remainder when f is divided by $f_1, \ldots, f_s$ is zero, then clearly f is in the ideal generated by f_i. However, as examples show, the converse does not hold.

THEOREM (Division algorithm in $K[x_1, \ldots, x_n]$). *Fix a monomial order $<$ on $\mathbb{N}_0^n$, and let $G = (f_1, \ldots, f_s)$ be an ordered s-tuple of polynomials in $K[x_1, \ldots, x_n]$. Then every $f \in K[x_1, \ldots x_n]$ can be written as $f = q_1 f_1 + \cdots + q_s f_s + r$ where $q_i, r \in K[x_1, \ldots, x_n]$, and either $r = 0$ or r is a linear combination, with coefficients in K of monomials none of which is divisible by any of $LT(f_1), \ldots, LT(f_s)$. We call r a remainder of f in division by G. Furthermore, if $q_i f_i \neq 0$ then we have multdeg(f) = multdeg$(q_i f_i)$.*

DEFINITION. We write f^G for the remainder in the division of f by the (ordered) list of polynomials $G = \{g_1, \ldots, g_j\}$.

EXAMPLE. If $G = (x^3y^2 - y^2z, xy^2 - yz)$, then using *lex* order on monomials $(x^5y^3)^G = yz^3$ since by the division algorithm we have

$$x^5y^3 = \left(x^2y\right)\left(x^3y^2 - y^2z\right) + \left(xyz + z^2\right)\left(xy^2 - yz\right) + yz^3$$

EXAMPLE. We will divide $f = x^3y^2 + xy + x + 1$ by $f_1 = x^3 + 1$ and $f_2 = y^2 + 1$ using *lex* order with $y < x$. Then according to our algorithm we get the following:

$$\begin{array}{rll}
(x^3y^2 + xy + x + 1) & : (x^3 + 1) \quad = y^2 & \\
-(x^3y^2 + y^2) & & \\
xy + x - y^2 + 1 & : (y^2 + 1) \quad = -1 & \rightarrow xy + x \\
-(-y^2 - 1) & & \\
2 & & \rightarrow xy + x + 2
\end{array}$$

The graphical representation used above for the division process is standard. After dividing f by the leading term of f_1, we get the polynomial $xy + x - y^2 + 1$ with no terms that are divisible by the leading term of f_1. Furthermore, the first low terms, xy and x are not divisible by the leading term of f_2, and so these go to the remainder column $\underline{r}$. We are left with $-y^2 + 1$ and we divide this by the leading term of f_2. We obtain $q_1 = y^2$. After dividing by the leading term of f_2, we get the 2, and so this term is sent to the remainder column and we have a total remainder $xy + x + 2$. Thus we obtain $q_2 = -1$ and

$$x^3y^2 + xy + x + 1 = y^2(x^3 + 1) + (-1)\left(y^2 + 1\right) + (xy + x + 2).$$

EXAMPLE. Let $f_1 = x^2y - 2x,\ f_2 = y^3 + 4 \in K[x, y]$. We will use *lex* order with $y < x$.

Let $f = x^2y^3 - 2xy^2 \in K[x, y]$. Our first case will be $f = (f_1, f_2)$. Then, by the procedure described above we obtain $x^2y^3 - 2xy^2 = y^2\left(x^2y - 2x\right) + 0\left(y^3 + 4\right) + 0$. If, however, we take $f = (f_2, f_1)$ in the second case, then we obtain $x^2y^3 - 2xy^2 = x^2\left(y^3 + 4\right) + 0\left(x^2y - 2x\right) - 2xy^2 - 4x^2$. So we can see that the two cases in the example produce two different remainders, 0 and $-2xy^2 - 4x^2$, respectively, due to a switch in the order of polynomials in f.

The need for a well defined remainder upon division is one of the motivations for the definition of "Gröbner" basis.

Monomial ideals and Gröbner basis

As we have seen, in general we do not obtain a uniquely determined remainder from the division algorithm. However, the subsequent definition of a Gröbner basis will have the quality that the division of f by G yields the same remainder, no matter how the elements of G are ordered in the division. Since we will show that every ideal I has a Gröbner basis, we are able to resolve the ideal membership problem with a necessary and sufficient condition for a polynomial f to be a member of an ideal I, namely that division of f by the Gröbner basis of I returns a remainder of 0.

DEFINITION. A monomial ideal is an ideal generated by a set of monomials.

This is, I is a monomial ideal, if there is a subset $A \subset \mathbb{N}_0^n$ such that I consists of all polynomials which are finite sums of the form $\sum_{\alpha \in A} h_\alpha x^\alpha$, where $h_\alpha \in K[x_1, \ldots, x_n]$. We write $I = \langle x^\alpha : \alpha \in A \rangle$. For example $I = \left\langle x^5y^2z, x^2yz^2, xy^3z^2 \right\rangle \subset K[x, y, z]$ is a monomial ideal. For all monomial ideals we have the fact that if x^β lies in I, then x^β is divisible by x^α for some $\alpha \in A$. Furthermore, for every polynomial f in a monomial ideal I, we can say that every term of f lies in I and that f is a K-linear combination of the monomials in I.

DEFINITION. Let $I \subset K[x_1, \ldots, x_n]$ be a nonzero ideal.

1. Let $LT(I)$ be the set of leading terms of element of I:

$$LT(I) = \{\, cx^\alpha : \text{there exists } f \in I \text{ with } LT(f) = cx^\alpha \,\}$$

2. We denote by $\langle LT(I) \rangle$ the ideal generated by the elements of $LT(I)$.

Note that if we are given a finite generating set for I, say $I = \langle g_1, \ldots, g_s \rangle$, then $\langle LT(g_1), \ldots, LT(g_s) \rangle$ and $\langle LT(I) \rangle$ are not always the same.

EXAMPLE. Let $I = \langle f_1, f_2 \rangle$ where $f_1 = x^3 - 2xy$ and $f_2 = x^3y - 2y^2 + x$, and use *lex* ordering on the monomials in $K[x, y]$. Then

$$f_3 := y\left(x^3 - 2xy\right) - \left(x^3y - 2y^2 + x\right) = -2xy^2 + 2y^2 - x$$

So $f_3 \in I$ and $LT(f_3) = -2xy^2 \in LT(I)$, but not in $\langle LT(f_1), LT(f_2)\rangle$ since it is not divisible by the leading terms of f_1 or f_2.

We want to obtain ideals that have the property that $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_s)\rangle$, i.e., that the ideal of the leading terms is generated by the leading terms of the original ideal's generators. We want to eliminate cases like the above by making sure that our basis generates all of $\langle LT(I)\rangle$. This motivates the following definition.

DEFINITION. Let a monomial ordering on $K[x_1, \ldots, x_n]$ be fixed. A finite subset $G = \{g_1, \ldots, g_s\}$ of an ideal I is said to be a Gröbner basis of the ideal I if $\langle LT(g_1), \ldots, LT(g_s)\rangle = LT(I)$.

As a corollary to the Hilbert Basis Theorem applied to $\langle LT(I)\rangle$ we have the following.

COROLLARY. *Let I be a nonzero polynomial ideal, then I has a Gröbner basis.*

While this corollary proves the existence of a Gröbner basis, its proof is not constructive and offers us little insight as to how to actually obtain one. We would like to obtain a generating set such that all that leading terms of the polynomials in the set generate the leading terms of the ideal I. This fails when there is a cancellation of leading terms of the kind in the previous example. To better determine when this cancellation occurs, Buchberger constructed a special polynomial that produces new leading terms.

DEFINITION. Let $f, g \in K[x_1, \ldots, x_n]$ be nonzero polynomials.

1. If multidegrees $multdeg(f) = \alpha$ and $multdeg(g) = \beta$, then let $\gamma = (\gamma_1, \ldots, \gamma_n)$ where $\gamma_i = \max(\alpha_i, \beta_i)$ for each i. We call x^γ the least common multiple of $LT(f)$ and $LT(g)$.
2. The S-polynomial (S stands for "syzygy", from Latin *syzygia* "conjunction", or Greek $\sigma\upsilon'\zeta\upsilon\gamma o\varsigma$ – *syzygos,* "yoked together") of f and g is the combination $S(f,g) = \frac{x^\gamma}{LT(f)} f - \frac{x^\gamma}{LT(g)} g$.

EXAMPLE. Let $f = x^4yz + x^2y^3z + xz$ and $g = 2x^2y^2z + xy^2 + xz^3$ in $Q[x, y, z]$ with the lexicographic ordering on monomials. Then $\gamma = (4, 2, 1)$ and we have:

$$S(f,g) = \frac{x^4y^2z}{x^4yz} f - \frac{x^4y^2z}{2x^2y^2z} g = yf - \frac{1}{2}x^2g = -\frac{1}{2}x^3y^2 - \frac{1}{2}x^3z^3 + x^2y^4z + xyz.$$

Notice the cancellation of the leading terms occurred by the construction of the S-polynomial. Once a basis contains all the possible S-polynomials of polynomials in the ideal generating set, there are no extra polynomials in $\langle LT(I)\rangle$ that are not in $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_s)\rangle$. This leads to a very important criterion.

THEOREM (Buchberger's criterion). *Let I be a polynomial ideal. Then a basis $G = \{g_1, \ldots, g_s\}$ for I is a Gröbner basis for I if and only if for all pairs $i \neq j$, the remainder on division of $S(g_i, g_j)$ by G is zero.*

THEOREM (Buchberger's algorithm). *Let $I = \langle f_1, \ldots, f_s \rangle \neq (0)$ be a polynomial ideal. Then a Gröbner basis for I can be constructed in a finite number of steps.*

Buchberger's algorithm proceeds like this. Let $F = (f_1, \ldots, f_s)$ be a list of the polynomials defining I. For each pair of polynomials f_i, f_j in F calculate their S-polynomial S, and divide it by the polynomials $f_1, \ldots, f_s$ in F obtaining S^F. If $S^F \neq 0$, add $S^F$to F and start again with $F = F \cup \{S^F\}$. Repeat the process until all S-polynomials of polynomials in F have remainder 0 after division by F. This process ends after a finite number of steps.

The Gröbner basis is determined by choice of a term order. Once we have chosen it, we can apply Buchberger's algorithm to obtain a Gröbner basis in that term order. Here are some examples of computing the Gröbner basis of an ideal with respect to different monomial orders.

EXAMPLE. Let $I = \langle x^2 + xy^2, x^2 - y^3, y^3 - y^2 \rangle$. First, let $<_{lex}$ be the lexicographic order with $y < x$ as our term order. Using Buchberger's algorithm we get a Gröbner basis for I, $G = (x^2 + xy^2, x^2 - y^3, y^3 - y^2, xy^2 + y^2)$ in one step. Second, let $<_{grlex}$ be the graded lexicographic order. For the same I by using Buchberger's algorithm we get a different Gröbner basis $G = (xy^2 + x^2, -y^3 + x^2, y^3 - y^2, x^3 + x^2y, x^2y + xy^2, -x^2 + y^2)$ in three steps.

EXAMPLE. For $I = \langle xy + y^2, x^2y + xy^2 + x^2 \rangle$, the Gröbner basis with respect to the *lex* order with $y < x$ is $G = \big(xy + y^2, x^2y + x^2 + xy^2, -x^2, -y^3\big)$, but the Gröbner bases with respect to the *lex* order with $x < y$ is $G = \big(y^2 + xy, xy^2 + x^2y + x^2, -x^2\big)$.

REFERENCES

[1] W. W. Adams, P. Loustaunau, *An Introduction to Gröbner Bases*, Graduate Studies in Mathematics, vol. 3, AMS, Providence RI, 1994.

[2] I. A. Ajwa, Zhuojun Liu, P. S. Wang, *Gröbner bases algorithm*, ICM Technical Report ICM-199502-00, 2003, 1–15.

[3] D. Cox, J. Little, D. O'Shea, *Ideals, Varieties, and Algorithms*, Springer, New York, 1997.

[4] L. Robbiano, *Term orderings on the polynomial ring*, EUROCAL' 85, vol. 2 (Linz, 1985), Lecture Notes in Computer Science, vol. 204, Springer, Berlin, 1985, pp. 513–517.

[5] M. Roczen, *First steps with Gröbner bases*, Preprint (`www-irm.mathematik.hu-berlin.de/~roczen/papers/eforie.pdf`).

[6] B. Sturmfels, *Gröbner Bases and Convex Polytopes*. University Lecture Series, vol. 8, AMS, Providence RI, 1996.

University of Belgrade – Faculty of Mathematics, Serbia