Groebner bases (standard bases)

Alexey Muranov

10th April 2025

1 Preliminaries and definition

Let $(M, \prec)$ be a totally ordered monoid whose (strict) order relation $(\prec)$ satisfies the following two conditions:

(1) $(\prec)$ is a well-order, that is, every nonempty subset of M has the least element with respect to $(\prec)$,

(2) $(\prec)$ is compatible with the multiplication, that is, if $x, y, z \in M$ and $x \prec y$, then $xz \prec yz$ and $zx \prec zy$.

It follows from these two conditions that the identity element $1 \in M$ is the least element of M: $1 \preceq x$ for every $x \in M$. Indeed, let x be the least element of M. Then either $x = 1$, or $1 \succ x \succ x^2 \succ \cdots$, but the relation $x \succ x^2$ is impossible if x is minimal.

In addition to the total order $(\prec)$, consider the divisibility preorder $(|)$ on M: "$x|y$" means that there exist $z, w \in M$ such that $y = zxw$.

It follows from the stated properties of $(\prec)$ that the divisibility relation $(|)$ is a subrelation (restriction) of $(\preceq)$. In particular, $(|)$ is a partial order: if $x|y$ and $y|x$, then $x = y$. Moreover, it follows that the divisibility relation is a well-founded partial order (that is, every subset of M has an element that is not divisible by any other element of that subset).

In the present note, elements of M shall be called *monomials*, though this is not a standard usage of the term.

Let $\mathbf{k}$ be a field. The goal is to define *Groebner bases* of two-sided ideals of the (associative but not necessarily commutative) unitary ring $\mathbf{k}M$.

Elements of M shall be identified with the corresponding elements of $\mathbf{k}M$ in all contexts where this does not cause confusion.

Notation. For every nontrivial element $p \in \mathbf{k}M$, let $\operatorname{lm}(p)$ denote its *leading monomial*, that is, the greatest element of M in the "monomial decomposition" of p.

Notation. If S is a subset of $\mathbf{k}M$, let $\operatorname{lm}(S)$ denote the set of the leading monomials of all the nontrivial elements of S:

$$\operatorname{lm}(S) \stackrel{\text{def}}{=} \{\, \operatorname{lm}(p) \mid p \in S,\ p \neq 0 \,\}.$$

Proposition. *If I is a two-sided ring ideal of $\mathbf{k}M$, then $\operatorname{lm}(I)$ is a two-sided semigroup ideal of M.*

Definition. If I is a two-sided ideal of $\mathbf{k}M$, then the elements of $M \setminus \operatorname{lm}(I)$ shall be called *normal* monomials with respect to I.

Remark. The monomials called *normal* in this note are more commonly known as *standard*. Calling them "normal" can be justified by considering a certain *algebraic rewriting system* on $\mathbf{k}M$ associated to I, with respect to which the normal monomials will generate the linear subspace of *normal forms*.

Notation. If I is a two-sided ideal of $\mathbf{k}M$, the linear subspace of $\mathbf{k}M$ spanned by the corresponding normal monomials shall be denoted $N(I)$.

Proposition. *If I is a two-sided ideal of $\mathbf{k}M$, then*

$$\mathbf{k}M = I \oplus N(I).$$

Proof. It is clear that $I \cap N(I) = \{0\}$.

To prove that $I + N(I) = \mathbf{k}M$, suppose that this is not the case and consider an element $p \in \mathbf{k}M \setminus (I + N(I))$ such that $\operatorname{lm}(p)$ is the least possible. The possibilities that $\operatorname{lm}(p) \in \operatorname{lm}(I)$ or that, otherwise, $\operatorname{lm}(p) \notin \operatorname{lm}(I)$ both lead to a contradiction with the minimality of $\operatorname{lm}(p)$. Indeed, if $\operatorname{lm}(p) \in \operatorname{lm}(I)$, then there exists $q \in p + I$ such that $\operatorname{lm}(q) \prec \operatorname{lm}(p)$, and if $\operatorname{lm}(p) \notin \operatorname{lm}(I)$, then there exists $q \in p + N(I)$ such that $\operatorname{lm}(q) \prec \operatorname{lm}(p)$. ☐

Definition. If I is a two-sided ideal of $\mathbf{k}M$, and p is an element of $\mathbf{k}M$, let the *remainder* of p modulo I, denoted $\operatorname{rem}_I(p)$, be the unique element $r \in N(I)$ such that $p - r \in I$.

Thus,

$$\operatorname{rem}_I \colon \mathbf{k}M \to N(I)$$

is the linear projection of $\mathbf{k}M$ onto $N(I)$ such that

$$\ker(\operatorname{rem}_I) = I.$$

The notion of a *Groebner basis* of I can be motivated by the problem of computing $\operatorname{rem}_I(p)$ for a given p in practice. The set of all elements of I, as well as the set of all *monic* elements of I, are Groebner bases of I, but using a small finite Groebner basis, if such exists, may be preferable over using an infinite or a large one.

Notation. For any subset S of M, let $\operatorname{divmin}(S)$ denote the set of minimal elements of S with respect to the divisibility relation.

For example, $\operatorname{divmin}(M) = \{1\}$.

Since the divisibility order on M is well-founded, every semigroup ideal K of M is generated by $\operatorname{divmin}(K)$ (as a two-sided semigroup ideal).

Proposition. *Let I be a two-sided ideal of* $\mathbf{k}M$*, and G a subset of I such that*

$$\operatorname{divmin} \operatorname{lm}(I) \subset \operatorname{lm}(G).$$

Then G generates I (as a two-sided ideal).

Proof. Suppose, on the contrary, that the two-sided ideal $\langle G \rangle$ generated by G does not contain all elements of I.

Let p be an element of $I \setminus \langle G \rangle$ such that $\operatorname{lm}(p)$ be the least possible with respect to $(\prec)$. Let g be an element of G such that $\operatorname{lm}(g) | \operatorname{lm}(p)$, and let $x, y \in M$ be such that $\operatorname{lm}(p) = x \operatorname{lm}(g) y$. Let α be the element of $\mathbf{k}$ such that the leading *terms* of p and of $\alpha x g y$ be the same, and let $q = p - \alpha x g y$. Then $q \in I \setminus \langle G \rangle$ and $\operatorname{lm}(q) \prec \operatorname{lm}(p)$, in contradiction with the choice of p. $\square$

Remark. If I is a two-sided ideal of $\mathbf{k}M$, $G \subset I$, and $\operatorname{divmin} \operatorname{lm}(I) \subset \operatorname{lm}(G)$, then there is a subset $G_0 \subset G$ such that $\operatorname{divmin} \operatorname{lm}(I) = \operatorname{lm}(G_0)$. This subset G_0 generates I too.

Definition. A *Groebner basis* of a two-sided ideal I of $\mathbf{k}M$ is a subset $G \subset I$ such that

$$\operatorname{divmin} \operatorname{lm}(I) \subset \operatorname{lm}(G).$$

The *reduced Groebner basis* of I is the set

$$\{\, x - \operatorname{rem}_I(x) \mid x \in \operatorname{divmin} \operatorname{lm}(I) \,\},$$

which is clearly a Groebner basis of I.