Blueprint of Groebner Basis Theory in LEAN

Lihong Zhi's Team

May 9, 2025

Chapter 1

Definitions

Definition 1 (`leadingTerm`)**.** Given a nonzero polynomial $f \in k[x]$, let

$$f = c_0 x^m + c_1 x^{m-1} + \cdots + c_m,$$

where $c_i \in k$ and $c_0 \neq 0$ [thus, $m = \deg(f)$]. Then we say that $c_0 x^m$ is the **leading term** of f, written

$$\mathrm{LT}(f) = c_0 x^m.$$

Definition 2 (`IsRemainder`)**.** Fix a monomial order $>$ on $\mathbb{Z}^n_{\geq 0}$, and let $F = (f_1, \ldots, f_s)$ 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

$$f = a_1 f_1 + \cdots + a_s f_s + r,$$

where $a_i, r \in k[x_1, \ldots, x_n]$, and either $r = 0$ or r is a linear combination, with coefficients in k, of monomials, none of which is divisible by any of $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$. We will call r a **remainder** of f on division by F.

Definition 3 (`IsGroebnerBasis`)**.** Fix a monomial order on the polynomial ring $k[x_1, \ldots, x_n]$.A finite subset $G = \{g_1, \ldots, g_t\}$ of an ideal $I \subseteq k[x_1, \ldots, x_n]$, with $I \neq \{0\}$, is said to be a **Gröbner basis** (or standard basis) if

$$\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle = \langle \mathrm{LT}(I) \rangle.$$

Using the convention that $\langle \emptyset \rangle = \{0\}$, we define the empty set $\emptyset$ to be the Gröbner basis of the zero ideal $\{0\}$.

Definition 4 (`sPolynomial`)**.** The S-polynomial of f and g is the combination

$$S(f, g) = \frac{x^\gamma}{\mathrm{LT}(f)} \cdot f - \frac{x^\gamma}{\mathrm{LT}(g)} \cdot g.$$

Chapter 2

Lemmas

Lemma 5 (`finset_subset_preimage_of_finite_image`)**.** *Let $f : \alpha \to \beta$ be a function and $s \subseteq \alpha$ a subset with finite image $f(s)$. Then there exists a finite subset $s' \subseteq_{fin} s$ such that:*

- *$s' \subseteq s$ (subset relation)*
- *$f(s') = f(s)$ (image equality)*
- *$|s'| = |f(s)|$ (cardinality preservation)*

Proof. □

Lemma 6 (`subset_finite_subset_subset_span`)**.**

Proof. □

Theorem 7 (`Submodule.fg_span_iff_fg_span_finset_subset`)**.**

Proof. □

Lemma 8 (`zero_le`)**.** *a Partially Ordered Set, a 0*

Proof. □

Lemma 9 (`degree_mem_support_iff`)**.**

Proof. □

Lemma 10 (`IsRemainder_def'`)**.** *Let $p \in R[\mathbf{X}]$, $G'' \subseteq R[\mathbf{X}]$ be a set of polynomials, and $r \in R[\mathbf{X}]$. Then r is a remainder of p modulo G'' with respect to monomial order m if and only if there exists a finite linear combination from G'' such that:*

1. *The support of the combination is contained in G''*
2. *p decomposes as the sum of this combination and r*
3. *For each $g' \in G''$, the degree of $g' \cdot (coefficient\ of\ g')$ is bounded by $\deg_m(p)$*
4. *No term of r is divisible by any leading term of non-zero elements in G''*

Proof. □

Lemma 11 (`IsRemainder_def''`)**.** *Let $p, r \in k[x_i : i \in \sigma]$, and let $G' \subseteq k[x_i : i \in \sigma]$ be a finite set. We say that r is a* generalized remainder *of p upon division by G' if the following two conditions hold:*

1. *For every nonzero $g \in G'$ and every monomial $x^s \in \mathrm{supp}(r)$, there exists some component $j \in \sigma$ such that*
$$\mathrm{multideg}(g)_j > s_j.$$
2. *There exists a function $q : G' \to k[x_i : i \in \sigma]$ such that:*

```
- For every $g \in G'$,
      $$
      \operatorname{multideg}''(q(g)g) \leq \operatorname{multideg}''(p);
      $$
- The decomposition holds:
      $$
      p = \sum_{g \in G'} q(g)g + r.
      $$
```

Proof. □

Lemma 12 (`lm_eq_zero_iff`)**.** *Let $p \in R[\mathbf{X}]$ be a multivariate polynomial. Then the leading term of p vanishes with respect to monomial order m if and only if p is the zero polynomial:*

$$\mathrm{LT}_m(p) = 0 \iff p = 0$$

Proof. □

Lemma 13 (`leadingTerm_image_sdiff_singleton_zero`)**.** *For any set of polynomials $G'' \subseteq R[\mathbf{X}]$ and monomial order m, the image of leading terms on the nonzero elements of G'' equals the image on all elements minus zero:*

$$\mathrm{LT}_m(G'' \setminus \{0\}) = \mathrm{LT}_m(G'') \setminus \{0\}$$

Proof. □

Lemma 14 (`leadingTerm_image_insert_zero`)**.**

Proof. □

Lemma 15 (`isRemainder_of_insert_zero_iff_isRemainder`)**.** *Let $p \in R[\mathbf{X}]$ be a polynomial, $G'' \subseteq R[\mathbf{X}]$ a set of polynomials, and $r \in R[\mathbf{X}]$ a remainder. Then the remainder property is invariant under inserting the zero polynomial:*

$$\mathsf{IsRemainder}_m\, p\, (G'' \cup \{0\})\, r \iff \mathsf{IsRemainder}_m\, p\, G''\, r$$

Proof. □

Lemma 16 (`isRemainder_sdiff_singleton_zero_iff_isRemainder`)**.** *Let $p \in R[\mathbf{X}]$ be a polynomial, $G'' \subseteq R[\mathbf{X}]$ a set of polynomials, and $r \in R[\mathbf{X}]$ a remainder. Then the remainder property is invariant under removal of the zero polynomial:*

$$\mathsf{IsRemainder}_m\, p\, (G'' \setminus \{0\})\, r \iff \mathsf{IsRemainder}_m\, p\, G''\, r$$

Proof. □

Lemma 17 (`sPolynomial_antisymm`)**.** *the S-polynomial of f and g is antisymmetric:*

$$\mathrm{Sph}\, fg = -\mathrm{Sph}\, gf$$

Proof. □

Lemma 18 (`sPolynomial_eq_zero_of_left_eq_zero`)**.** *For any polynomial $g \in \mathrm{MvPolynomial}\,\sigma R$ and monomial order m, the S-polynomial with zero as first argument vanishes:*

$$\mathrm{Sph}\,0g = 0$$

Proof. □

Lemma 19 (`sPolynomial_eq_zero_of_right_eq_zero'`)**.** *For any polynomial $g \in \mathrm{MvPolynomial}\,\sigma R$ and monomial order m, the S-polynomial with zero as second argument vanishes:*

$$\mathrm{Sph}\,f0 = 0$$

Proof. □

Theorem 20 (`div_set'`)**.** *Let $G'' \subseteq R[\mathbf{X}]$ be a set of polynomials where every nonzero element has a unit leading coefficient:*

$$\forall g \in G'',\ (\mathrm{IsUnit}(\mathrm{LC}_m(g)) \vee g = 0)$$

Then for any polynomial $p \in R[\mathbf{X}]$, there exists a remainder r satisfying:

$$\mathsf{IsRemainder}_m\, p\, G''\, r$$

where $\mathrm{LC}_m(g)$ denotes the leading coefficient of g under monomial order m.

Proof. □

Theorem 21 (`div_set''`)**.** *Let k be a field, and let $G'' \subseteq k[x_i : i \in \sigma]$ be a set of polynomials. Then for any $p \in k[x_i : i \in \sigma]$, there exists a generalized remainder r of p upon division by G''.*

Proof. □

Lemma 22 (`Ideal.fg_span_iff_fg_span_finset_subset`)**.** *A subset $s \subseteq R$ has finitely generated span if and only if: $\exists$ finite $s' \subseteq s$ such that $\mathsf{span}(s) = \mathsf{span}(s')$*

Proof. □

Lemma 23 (`span_singleton_zero`)**.** *For any ring R, the span of the zero singleton set equals the zero submodule:*

$$\mathsf{span}_R\{(0 : R)\} = \bot$$

Proof. □

Lemma 24 (`span_insert_zero`)**.** *For any subset $s \subseteq R$ of a ring R, inserting zero does not change the linear span:*

$$\mathsf{span}_R(\{0\} \cup s) = \mathsf{span}_R(s)$$

Proof. □

Lemma 25 (`span_sdiff_singleton_zero`)**.** *For any subset $s \subseteq R$ of a ring R, removing zero does not change the linear span:*

$$\mathsf{span}_R(s \setminus \{0\}) = \mathsf{span}_R(s)$$

Proof. □

Lemma 26 (`leadingTerm_ideal_span_monomial`)**.** *Let $G'' \subseteq R[x_1, \ldots, x_n]$ be a set of polynomials such that*

$$\forall p \in G'',\ \text{leadingCoeff}(p) \in R^\times.$$

Then,

$$\langle \text{lt}(G'') \rangle = \left\langle x^{\deg(p)} \mid p \in G'' \right\rangle,$$

Proof. □

Lemma 27 (`leadingTerm_ideal_sdiff_singleton_zero`)**.**

Proof. □

Lemma 28 (`leadingTerm_ideal_insert_zero`)**.**

Proof. □

Lemma 29 (`IsGroebnerBasis_erase_zero`)**.**

Proof. □

Lemma 30 (`IsGroebnerBasis_union_singleton_zero`)**.**

Proof. □

Lemma 31 (`leadingTerm_ideal_span_monomial'`)**.**

$$\langle \text{lt}(G) \rangle = \langle \{x^t : t \in \{\text{multideg}(p) : p \in G \setminus \{0\}\}\} \rangle$$

Proof. □

Lemma 32 (`mem_ideal_of_remainder_mem_ideal`)**.** *Let $G'' \subseteq R[x_1, \ldots, x_n]$, let $I \subseteq R[x_1, \ldots, x_n]$ be an ideal, and let $p, r \in R[x_1, \ldots, x_n]$. Suppose that:*

- *$G'' \subseteq I$,*
- *$r \in I$,*
- *r is the remainder of p upon division by G''.*

Then,

$$p \in I.$$

Proof. □

Lemma 33 (`remainder_mem_ideal_iff`)**.** *Let R be a commutative ring, and let $G'' \subseteq R[x_1, \ldots, x_n]$, $I \subseteq R[x_1, \ldots, x_n]$ be an ideal, and $p, r \in R[x_1, \ldots, x_n]$. Assume that:*

- *$G'' \subseteq I$,*
- *r is the remainder of p upon division by G''.*

Then,

$$r \in I \quad \iff \quad p \in I.$$

Proof. □

Lemma 34 (remainder_sub_remainder_mem_ideal). *Let $I \subseteq k[x_i : i \in \sigma]$ be an ideal, and let $G \subseteq I$ be a finite subset. Suppose that r_1 and r_2 are generalized remainders of a polynomial p upon division by G. Then,*

$$r_1 - r_2 \in I.$$

Proof. □

Lemma 35 (IsRemainder_term_not_mem_leading_term_ideal).

Proof. □

Lemma 36 (IsRemainder_term_not_mem_leading_term_ideal').

Proof. □

Lemma 37 (IsRemainder_monomial_not_mem_leading_term_ideal).

Proof. □

Lemma 38 (IsRemainder_monomial_not_mem_leading_term_ideal').

Proof. □

Theorem 39 (exists_groebner_basis). *Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal. Then there exists a finite subset $G = \{g_1, \ldots, g_t\}$ of I such that G is a Gröbner basis for I.*

Proof. □

Theorem 40 (groebner_basis_isRemainder_zero_iff_mem_span). *Let $G = \{g_1, \ldots, g_t\}$ be a Gröbner basis for an ideal $I \subseteq k[x_1, \ldots, x_n]$ and let $f \in k[x_1, \ldots, x_n]$. Then $f \in I$ if and only if the remainder on division of f by G is zero.*

Proof. □

Theorem 41 (groebner_basis_isRemainder_zero_iff_mem_span').

Proof. □

Theorem 42 (groebner_basis_zero_isRemainder_iff_mem_span).

Proof. □

Lemma 43 (groebner_basis_zero_isRemainder_iff_mem_span').

Proof. □

Lemma 44 (remainder_zero).

Proof. □

Theorem 45 (IsGroebnerBasis_iff). *Let $G = \{g_1, \ldots, g_t\}$ be a finite subset of $k[x_1, \ldots, x_n]$. Then G is a Gröbner basis for the ideal $I = \langle G \rangle$ if and only if for every $f \in I$, the remainder of f on division by G is zero.*

Proof. □

Theorem 46 (span_groebner_basis). *Let $G = \{g_1, \ldots, g_t\}$ be a Gröbner basis for an ideal $I \subseteq k[x_1, \ldots, x_n]$. Then G is a basis for the vector space I over k.*

Proof. □

Lemma 47 (`sPolynomial_decomposition`). *Let* $f, h_1, \dots, h_m \in k[\mathbf{x}] \setminus \{0\}$*, and suppose*

$$f = c_1 h_1 + \cdots + c_m h_m, \quad \text{with } c_i \in k.$$

If

$$\operatorname{lm}(h_1) = \operatorname{lm}(h_2) = \cdots = \operatorname{lm}(h_i) > \operatorname{lm}(f),$$

then

$$f = \sum_{1 \le i < j \le m} c_{i,j} S(h_i, h_j), \quad c_{i,j} \in k.$$

Furthermore, if $S(h_i, h_j) \neq 0$*, then* $\operatorname{lm}(h_i) > \operatorname{lm}(S(h_i, h_j))$.

Proof. □

Lemma 48 (`sPolynomial_degree_lt`). $h_1, h_2 \in k[\mathbf{x}], lm(h_1) = lm(h_2), S(h_1, h_2) \neq 0$*, then* $lm(S(h_1, h_2)) < lm(h_1)$.

Proof. □

Theorem 49 (`buchberger_criterion`). *A basis* $G = \{g_1, \dots, g_t\}$ *for an ideal* I *is a Gröbner basis if and only if* $S(g_i, g_j) \to_G 0$ *for all* $i \neq j$.

Proof.

□