THE ALGEBRAIC GEOMETRY ALGEBRAIC TOPOLOGY DUMP

ERNEST YEUNG ERNESTYALUMNI@GMAIL.COM

From the beginning of 2016, I decided to cease all explicit crowdfunding for any of my materials on physics, math. I failed to raise *any* funds from previous crowdfunding efforts. I decided that if I was going to live in *abundance*, I must lose a scarcity attitude. I am committed to keeping all of my material **open-sourced**. I give all my stuff *for free*.

In the beginning of 2017, I received a very generous donation from a reader from Norway who found these notes useful, through *PayPal*. If you find these notes useful, feel free to donate directly and easily through PayPal, which won't go through a 3rd. party such as indiegogo, kickstarter, patreon. Otherwise, under the *open-source MIT license*, feel free to copy, edit, paste, make your own versions, share, use as you wish.

gmail : ernestyalumni
linkedin : ernestyalumni
twitter : ernestyalumni

Contents

Abstract. Everything about Algebraic Geometry, Algebraic Topology

Date: 5 mars 2017.
Key words and phrases. Algebraic Geometry, Algebraic Topology.

Part 1. Reading notes on Cox, Little, O'Shea's *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*

1. Geometry, Algebra, and Algorithms

1.1. **Polynomials and Affine Space.** fields are important is that linear algebra works over *any* field

Definition 1 (2). *set of all polynomials in $x_1, \dots, x_n$ with coefficients in k, denoted $k[x_1, \dots, x_n]$*

polynomial f *divides* polynomial g provided $g = fh$ for some $h \in k[x_1, \dots, x_n]$

$k[x_1, \dots, x_n]$ satisfies all field axioms except for existence of multiplicative inverses; commutative ring, $k[x_1, \dots, x_n]$ *polynomial ring*

Exercises for 1. **Exercise 1.** $\mathbb{F}_2$ commutative ring since it's an abelian group under addition, commutative in multiplication, and multiplicative identity exists, namely 1. It is a field since for $1 \neq 0$, the multiplicative identity is 1.

Exercise 2.

(a)
(b)
(c)

1.2. **Affine Varieties.**

1.3. **Parametrizations of Affine Varieties.**

1.4. **Ideals.**

1.5. **Polynomials of One Variable.**

2. Groebner Bases

2.1. **Introduction.**

2.2. **Orderings on the Monomials in $k[x_1, \dots, x_n]$.**

2.3. **A Division Algorithm in $k[x_1, \dots, x_n]$.**

Part 2. Reading notes on Cox, Little, O'Shea's *Using Algebraic Geometry*

Using Algebraic Geometry. David A. Cox. John Little. Donal O'Shea. Second Edition. Springer. 2005. ISBN 0-387-20706-6 QA564.C6883 2004

7. Introduction

7.1. Polynomials and Ideals.

monomial

(1)
$$x_1^{\alpha_1} \dots x_n^{\alpha_n} \tag{1.1}$$

total degree of x^α is $\alpha_1 + \dots + \alpha_n \equiv |\alpha|$

field k, $k[x_1 \dots x_n]$ collection of all polynomials in $x_1 \dots x_n$ with coefficients k.

polynomials in $k[x_1 \dots x_n]$ can be added and multiplied as usual, so $k[x_1 \dots x_n]$ has structure of commutative ring (with identity)
however, only nonzero constant polynomials have multiplicative inverses in $k[x_1 \dots x_n]$, so $k[x_1 \dots x_n]$ not a field
however set of rational functions $\{f/g | f, g \in k[x_1 \dots x_n], \, g \neq 0\}$ is a field, denoted $k(x_1 \dots x_n)$

so
$$f = \sum_\alpha c_\alpha x^\alpha$$
where $c_\alpha \in k$
so
$$f \in k[x_1 \dots x_n] = \{ f | f = \sum_\alpha c_\alpha x^\alpha , x^\alpha = x_1^{\alpha_1} \dots x_n^{\alpha_n} , c_\alpha \in k \}$$

f homogeneous if all monomials have same total degrees

polynomial f is homogeneous if all monomials have the *same total degree*

Given a collection of polynomials $f_1 \dots f_s \in k[x_1 \dots x_n]$, we can consider all polynomials which can be built up from these by multiplication by arbitrary polynomials and by taking sums

Definition 2 (1.3)**.** *Let $f_1 \dots f_s \in k[x_1 \dots x_n]$*
Let $\langle f_1 \dots f_s \rangle = \{ p_1 f_1 + \dots + p_s f_s | p_i \in k[x_1 \dots x_n]$ for $i = 1 \dots s\}$

Exercise 1.
(a) $x^2 = x \cdot (x - y^2) + y \cdot (xy)$
(b)
$$p \cdot (x-y^2) = px - py^2$$
and for $pxy = (py)x$
(c)
$$p(y)(x-y^2) = p(y)x - p(y)y^2 \notin \langle x^2, xy \rangle$$

Exercise 2.
$$\sum_{i=1}^s p_i f_i + \sum_{j=1}^s q_j f_j = \sum_{i=1}^s (p_i + q_i) f_i , \quad p_i + q_i \in k[x_1 \dots x_n]$$
$\langle f_1 \dots f_s \rangle$ closed under sums in $k[x_1 \dots x_n]$

If $f \in \langle f_1 \dots f_s \rangle$,
$p \in k[x_1 \dots x_n]$

$$p \cdot f = p \sum_{i=1}^s q_j f_j = \sum_{i=1}^s p q_j f_j , \quad p q_j \in k[x_1 \dots x_n] \text{ so}$$
$$p \cdot f \in \langle f_1 \dots f_s \rangle$$

Done.

The 2 properties in Ex. 2 are defining properties of ideals in the ring $k[x_1 \dots x_n]$

Definition 3 (1.5)**.** *Let $I \subset k[x_1 \dots x_n]$, $\quad I \neq \emptyset$*
I ideal if
(a) $f + g \in I, \quad \forall f, g \in I$
(b) $pf \in I, \quad \forall f \in I$, *arbitrary* $p \in k[x_1 \dots x_n]$

Thus $\langle f_1 \dots f_s \rangle$ is an ideal by Ex. 2.

we call it the ideal generated by $f_1 \dots f_s$.

Exercise 3. Suppose $\exists$ ideal J, $f_1 \dots f_s \in J$ s.t. $J \subset \langle f_1 \dots f_s \rangle$
if $f \in \langle f_1 \dots f_s \rangle$, $f = \sum_{i=1}^s p_i f_i$, $\quad p_i \in k[x_1 \dots x_n]$

$\forall \, i = 1 \dots s$, $p_i f_i \in J$ and so $\sum_{i=1}^s p_i f_i \in J$, by def. of J as an ideal.

$$\langle f_1 \dots f_s \rangle \subseteq J \qquad \Longrightarrow J = \langle f_1 \dots f_s \rangle$$
$\Longrightarrow \langle f_1 \dots f_s \rangle$ is smallest ideal in $k[x_1 \dots x_n]$ containing $f_1 \dots f_s$

Exercise 4. For $I = \langle f_1 \dots f_s \rangle$
$J = \langle g_1 \dots g_t \rangle$

$I = J$ iff $s = t$ and $\forall f \in I$, $f = \sum_{i=1}^t q_i g_i$ and if $0 = \sum_{i=1}^t q_i g_i$, $q_i = 0$, $\forall i = 1 \dots t$, and if $0 = \sum_{i=1}^s p_i f_i$, $p_i = 0$, $\forall i = 1 \dots s$

Definition 4 (1.6).
$$\sqrt{I} = \{g \in k[x_1 \dots x_n] | g^m \in I \text{ for some } m \geq 1\}$$

e.g. $x + y \in \sqrt{\langle x^2 + 3xy, 3xy + y^2 \rangle}$
in $\mathbb{Q}[x, y]$ since

$$(x+y)^3 = x(x^2 + 3xy) + y(3xy + y^2) \in \langle x^2 + 3xy, 3xy + y^2 \rangle$$

- (Radical Ideal Property) $\forall$ ideal $I \subset k[x_1 \dots x_n]$, $\sqrt{I}$ ideal, $\sqrt{I} \supset I$
- **(Hilbert basis Thm.)** $\forall$ ideal $I \subset k[x_1 \dots x_n]$
  $\exists$ finite generating set,
  i.e. $\exists \{f_1 \dots f_2\} \subset k[x_1 \dots x_n]$ s.t. $I = \langle f_1 \dots f_s \rangle$
- (Division Algorithm in $k[x]$) $\forall f, g \in k[x]$ (EY : in 1 variable)
  $\forall f, g \in k[x]$ (in 1 variable)
  $f = qg + r$, $\exists!$ quotient q, $\exists$ remainder r

7.2.

7.3. Gröbner Bases.

Definition 5 (3.1). *Gröbner basis for $I \equiv G = \{g_1 \dots g_k\} \subset I$ s.t. $\forall f \in I$, $LT(f)$ divisible by $LT(g_i)$ for some i*

- (Uniqueness of Remainders) let ideal $I \subset k[x_1 \dots x_n]$
  division of $f \in k[x_1 \dots x_n]$ by Grö bner basis for I, produces $f = g + r$, $g \in I$, and no term in r divisible by any element of LT(I)

7.4. **Affine Varieties.** affine n-dim. space over k $\quad k^n = \{(a_1 \dots a_n) | a_1 \dots a_n \in k\}$
$\forall$ polynomial $f \in k[x_1 \dots x_n]$, $(a_1 \dots a_n) \in k^n$
$f : k^n \to k$
$f(a_1 \dots a_n)$ s.t. $x_i = a_i$ i.e.

if $f = \sum_\alpha c_\alpha x^\alpha$ for $c_\alpha \in k$, then
$f(a_1 \dots a_n) = \sum_\alpha c_\alpha a^\alpha \in k$, where $a^\alpha = a_1^{\alpha_1} \dots a_n^{\alpha_n}$

Definition 6 (4.1). *affine variety $\mathbf{V}(f_1 \dots f_s) = \{(a_1 \dots a_n) | (a_1 \dots a_n) \in k^n, f_1(x_1 \dots x_n) = \dots = f_s(x_1 \dots x_n) = 0\}$ subset $V \subset k^n$ is affine variety if $V = V(f_1 \dots f_s)$ for some $\{f_i\}$, polynomial $f_i \in k[x_1 \dots x_n]$*

- (Equal Ideals Have Equal Varieties) If $\langle f_1 \dots f_s \rangle = \langle g_1 \dots g_t \rangle$ in $k[x_1 \dots x_n]$, then $\mathbf{V}(f_1 \dots f_s) = \mathbf{V}(g_1 \dots g_t)$

so, recap
if $\langle f_1 \dots f_s \rangle = \langle g_1 \dots g_t \rangle$ in $k[x_1 \dots x_n]$,
then $V(f_1 \dots f_s) = V(g_1 \dots g_t)$

Recall Hilbert basis Thm. $\forall$ ideal $I \subset k[x_1 \dots x_n]$
$$I = \langle f_1 \dots f_s \rangle$$
$\implies$ if $I = J$, then $V(I) = V(J)$
think of V defined by I, rather than $f_1 = \dots = f_s = 0$

Exercise 3.
Recall Def. 1.5 Let $I \subset k[x_1 \dots x_n]$

I ideal if $f + g \in I \quad \forall f, g \in I$
$pf \in I, \quad \forall f \in I$ arbitrary $p \in k[x_1 \dots x_n]$

Let $f, g \in I(V)$
$$(f+g)(a_1 \dots a_n) = f(a_1 \dots a_n) + g(a_1 \dots a_n) = 0 + 0 = 0 \qquad f + g \in I(V)$$
$$pf(a_1 \dots a_n) = p(a_1 \dots a_n) f(a_1 \dots a_n) = 0 \qquad pf \in I(V)$$
Then $I(V)$ an ideal.
$V = V(x^2)$ in $\mathbb{R}^2$
$I = \langle x^2 \rangle$ in $\mathbb{R}[x, y]$, $\quad I = \{px^2 | p \in k[x, y]\}$
$I \subset I(V)$, since $px^2 = 0$ for $x^2 = 0$, $(0, b)$, $\quad b \in \mathbb{R}$
But $p(x, y) = x \in I(V)$, as
$$I(V) = \{f \in k[x_1 \dots x_n] | f(a_1 \dots a_n) = 0, \forall (a_1 \dots a_n) \in V\}$$
$p(0, b) = x = 0$
But $x \notin I$

Exercise 4. $I \subset \sqrt{I}$
Recall Def. 1.6 $\sqrt{I} = \{g \in k[x_1 \dots x_n] | g^m \in I \text{ for some } m \geq 1\}$
$\forall f \in I$, $f = f^1$, $m = 1$, so $f \in \sqrt{I}$, $\quad I \subset \sqrt{I}$
Hilbert basis thm., $\forall$ ideal $I \subset k[x_1 \dots x_n]$ s.t. $I = \langle f_1 \dots f_s \rangle$
$\{{}^{V(I) = \{(a_1 \dots a_n) | (a_1 \dots a_n) \in k^n, f_1(a_1 \dots a_n) = \dots = f_s(a_1 \dots a_n) = 0}\}$
$\mathbf{I}(\mathbf{V}(I)) = \{f \in k[x_1 \dots x_n] | f(a_1 \dots a_n) = 0 \quad \forall (a_1 \dots a_n) \in V(I)\}$
Let $g \in \sqrt{I}$, $\quad g^m \in I$, $\quad g^m = g^{m-1} g$
$g^m(a_1 \dots a_n) = 0 = g^{m-1}(a_1 \dots a_n) g(a_1 \dots a_n) = 0$. Then $g(a_1 \dots a_n) = 0$ or $g^{m-1}(a_1 \dots a_m) = 0$
as $g^m \in I$, and $V(I)$ is s.t. $f_1(a_1 \dots a_n) = \dots = f_s(a_1 \dots a_n) = 0$ for $I = \langle f_1 \dots f_s \rangle$

- (Strong Nullstellensatz) if k algebraically closed (e.g. $\mathbb{C}$), I ideal in $k[x_1 \dots x_n]$, then
$$\mathbf{I}(\mathbf{V}(I) = \sqrt{I}$$
- (Ideal-variety correspondence) Let k arbitrary field
$$I \subset I(V(I))$$
$$V(I(V)) = V \quad \forall V$$

Additional Exercises for Sec.4. Exercise 6.

8. Solving Polynomial Equations

8.1.

8.2. **Finite-Dimensional Algebras.** Gröbner basis $G = \{g_1 \dots g_t\}$ of ideal $I \subset k[x_1 \dots x_n]$,
recall def.: Gröbner basis $G = \{g_1 \dots g_t\} \subset I$ of ideal I, $\quad \forall f \in I$, LT(f) divisible by LT(g_i) for some i
$f \in k[x_1 \dots x_n]$ divide by G produces $f = g + r$, $g \in I$, r not divisible by any LT(I) uniqueness of r
$f \in k[x_1 \dots x_n]$ divide by G,
Recall from Ch. 1, divide $f \in k[x_1 \dots x_n]$ by G, the division algorithm yields

$$f = h_1 g_1 + \dots + h_t g_t + \overline{f}^G \qquad (2) \quad (2.1)$$

where remainder $\overline{f}^G$ is a linear combination of monomials $x^\alpha \notin \langle \text{LT}(I) \rangle$
since Gröbner basis, $f \in I$ iff $\overline{f}^G = 0$
$\forall f \in k[x_1 \dots x_n]$, we have coset $[f] = f + I = \{f + h | h \in I\}$ s.t. $[f] = [g]$ iff $f - g \in I$
We have a 1-to-1 correspondence
$$\text{remainders} \leftrightarrow \text{cosets}$$
$$\overline{f}^G \leftrightarrow [f]$$

algebraic

$$\overline{f}^G + \overline{g}^G \leftrightarrow [f]+[g]$$
$$\overline{\overline{f}^G \cdot \overline{g}^G} \leftrightarrow [f]\cdot[g]$$

$B = \{x^\alpha | x^\alpha \notin \langle \text{LT}(I)\rangle\}$ is a basis of A, basis monomials, standard monomials

20141023 EY's take

$\forall [f] \in A = k[x_1 \dots x_n]/I, \quad [f] = p_i b_i; \quad b_i \in B = \{x^\alpha | x^\alpha \notin \langle \text{LT}(I)\rangle\}$

For $I = \langle G \rangle$

e.g. $G = \{x^2 + \frac{3}{2}xy + \frac{1}{2}y^2 - \frac{3}{2}x - \frac{3}{2}y, xy^2 - x, y^3 - y\}$

$\langle \text{LT}(I)\rangle = \langle x^2, xy^2, y^3\rangle$

e.g. $B = \{1, x, y, xy, y^2\}$

$[f]\cdot[g] = [fg]$

e.g. $f = x$, $g = xy$, $[fg] = [x^2 y]$

now $f = h_1 g_1 + \dots + h_t g_t + \overline{f}^G$

8.3.

8.4. Solving Equations via Eigenvalues and Eigenvectors.

9. Resultants

10. Computation in Local Rings

10.1. Local Rings.

Definition 7 (1.1)**.**

$$k[x_1 \dots x_n]_{\langle x_1 \dots x_n\rangle} \equiv \{\frac{f}{g} | \text{ rational functions } \frac{f}{g} \text{ of } x_1 \dots x_n \text{ with } g(p) \neq 0 \text{ at } p\}$$

main properties of $k[x_1 \dots x_n]_{\langle x_1 \dots x_n\rangle}$

Proposition 1 (1.2)**.** *Let $R = k[x_1 \dots x_n]_{\langle x_1 \dots x_n\rangle}$. Then*

(a) *R subring of field of rational functions $k(x_1 \dots x_n) \supset k[x_1 \dots x_n]$*
(b) *Let $M = \langle x_1 \dots x_n \rangle \subset R$ (ideal generated by $x_1 \dots X_n$ in R)*
Then $\forall \frac{f}{g} \in R \backslash M$, $\frac{f}{g}$ unit in R (i.e. multiplicative inverse in R)
(c) *M maximal ideal in R*

Exercise 1. if $p = (a_1 \dots a_n) \in k^n$, $R = \{\frac{f}{g} | f, g \in k[x_1 \dots x_n], g(p) \neq 0\}$

(a) R subring of field of rational functions $k(x_1 \dots x_n)$
(b) Let M ideal generated by $x_1 - a_1 \dots x_n - a_n$ in R
Then $\forall \frac{f}{g} \in R\backslash M$, $\frac{f}{g}$ unit in R (i.e. multiplicative inverse in R)
(c) M maximal ideal in R

Proof. let $p = (a_1 \dots a_n) \in k^n$
let $g_1(p) \neq 0$, $g_2(p) \neq 0$

$$\frac{f_1}{g_1} + \frac{f_2}{g_2} = \frac{f_1 g_2 + f_2 g_1}{g_1 g_2} \qquad g_1(p)g_2(p) \neq 0 \text{ so } \frac{f_1}{g_1} + \frac{f_2}{g_2} \in R$$
$$\frac{f_1}{g_1} \cdot \frac{f_2}{g_2} = \frac{f_1 f_2}{g_1 g_2} \qquad g_1(p)g_2(p) \neq 0 \text{ so } \frac{f_1}{g_1}\frac{f_2}{g_2} \in R$$

$f = \frac{f}{1} \in R, \quad \forall f \in k[x_1 \dots x_n]$, so $k[x_1 \dots x_n] \subset R$

EY : 20141027, to recap,

Let $V = k^n$

Let $p = (a_1 \dots a_n)$

single pt. $\{p\}$ is (an example of) a variety

$I(\{p\}) = \{x_1 - a_1 \dots x_n - a_n\rangle \subset k[x_1 \dots x_n]$

$R \equiv k[x_1 \dots x_n]_{\langle x_1 - a_1 \dots x_n - a_n\rangle}$

$$R = \{\frac{f}{g} | \text{ rational function } \frac{f}{g} \text{ of } x_1 \dots x_n,\ g(p) \neq 0,\ p = (a_1 \dots a_n)\ \}$$

Prop. 1.2. properties

(a) R subring of field of rational functions $k(x_1 \dots x_n) \qquad k(x_1 \dots x_n) \subset R$
(b) $M = \langle x_1 \dots a_1 \dots x_n - a_n\rangle \subset R$. ideal generated by $x_1 - a_1 \dots x_n - a_n$
Then $\forall \frac{f}{g} \in R\backslash M$, $\frac{f}{g}$ unit in R ($\exists$ multiplicative inverse in R)
(c) M maximal ideal in R.
in R we allow denominators that are not elements of this ideal $I(\{p\})$

Definition 8 (1.3)**.** *local ring is a ring that has exactly 1 maximal ideal*

Proposition 2 (1.4)**.** *ring R with proper ideal $M \subset R$ is local ring if $\forall \frac{f}{g} \in R\backslash M$ is unit in R*

localization Ex. 8, Ex. 9

parametrization

Exercise 2.

$$x = x(t) = \frac{-2t^2}{1+t^2}$$
$$y = y(t) = \frac{2t}{1+t^2}$$

$k[t]_{\langle t \rangle} \qquad \frac{-2t^2}{1+t^2}$ rational function of t. $1 + t^2 \neq 0$

if $k = \mathbb{C}$ or $\mathbb{R}$

Consider set of convergent power series in n variables

$$k\{x_1 \dots x_n\} = \{\sum_{\alpha \in \mathbb{Z}^n_{\geq 0}} c_\alpha x^\alpha | c_\alpha \in k, \text{ series converges in some open } U \ni 0 \in k^n\ \} \tag{3}$$ (1.5)

Consider set $k[[x_1 \dots x_n]]$ of formal power series

$$k[[x_1 \dots x_n]] = \{\sum_{\alpha \in \mathbb{Z}^n_{\geq 0}} c_\alpha x^\alpha | c_\alpha \in k\} \text{ series need not converge} \tag{4}$$ (1.6)

variety V

□ $\quad k[x_1 \dots x_n]/\mathbf{I}(V) \qquad$ variety V

10.2. **Multiplicities and Milnor Numbers.** if I ideal in $k[x_1 \dots x_n]$, then denote $Ik[x_1 \dots x_n]_{\langle x_1 \dots x_n \rangle}$ ideal generated by I in larger ring $k[x_1 \dots x_n]_{\langle x_1 \dots x_n \rangle}$

Definition 9 (2.1). *Let I 0-dim. ideal in $k[x_1 \dots x_n]$, so $V(I)$ consists of finitely many pts. in k^n.*
Assume $(0 \dots 0) \in V(I)$
multiplicity of $(0 \dots 0) \in V(I)$ is

$$dim_k k[x_1 \dots x_n]_{\langle x_1 \dots x_n \rangle} / Ik[x_! \dots x_n]_{\langle x_1 \dots x_n \rangle}$$

generally, if $p = (a_1 \dots a_n) \in V(I)$
multiplicity of p, $m(p) = \dim k[x_1 \dots x_n]_M / Ik[x_1 \dots x_n]_M$

$$\dim k[x_1 \dots x_n]_M / Ik[x_1 \dots x_n]_M$$

localizing $k[x_1 \dots x_n]$ at maximal ideal $M = I(\{p\}) = \langle x_1 - a_1 \dots x_n - a_n \rangle$

11.

12.

13. Polytopes, Resultants, and Equations

14. Polyhedral Regions and Polynomials

14.1. **Integer Programming.** Prop. 1.12.

Suppose 2 customers A, B ship to same location
A: ship 400 kg pallet taking up $2\,m^3$ volume
B: ship 500 kg pallet taking up $3\,m^3$ volume

shipping firm trucks carry up to 3700 kg, up to $20\,m^3$

B's product more perishable, paying \$ 15 per pallet

A pays \$ 11 per pallet
How many pallets from A, B each in truck to maximize revenues?

$$\begin{aligned} 4A + 5B &\leq 37 \\ 2A + 3B &\leq 20 \\ A, B &\in \mathbb{Z}^*_{\geq 0} \end{aligned} \quad (1.1) \tag{5}$$

maximize $11A + 15B$

integer programming.
max. or min. value of some linear function

$$l(A_1 \dots A_n) = \sum_{i=1}^n c_i A_i$$

on set $(A_1 \dots A_n) \in \mathbb{Z}^n_{\geq 0}$ s.t.
3. Finally, by introducing additional variables; rewrite linear constraint inequalities as equalities. The new variables are called "slack variables"

$$(1.4) \qquad a_{ij} A_j = b_i, \quad A_j \in \mathbb{Z}_{\geq 0} \tag{6}$$

introduce indeterminate z_i, $\forall$ equation in (1.4)

$$z_i^{a_{ij} A_j} = z_i^{b_i}$$

m constraints

$$\prod_{i=1}^m z_i^{a_{ij} A_j} = \prod_{i=1}^m z_i^{b_i} = \left(\prod_{i=1}^m z_i^{a_{ij}} \right)^{A_j}$$

Proposition 3 (1.6). *Let k field, define $\varphi : k[w_1 \dots w_n] \to k[z_1 \dots z_m]$ by*

$$\varphi(w_j) = \prod_{i=1}^m z_i^{a_{ij}} \qquad \forall\, j = 1 \dots n$$

and

$$\varphi(g(w_1 \dots w_n)) = g(\varphi(w_1) \dots \varphi(w_n))$$

$\forall$ general polynomial $g \in k[w_1 \dots w_n]$
Then $(A_1 \dots A_n)$ integer pt. in feasible region iff $\varphi : w_1^{A_1} \dots w_n^{A_n} \mapsto z_1^{b_1} \dots z_m^{b_m}$

Exercise 3.
Now

$$\varphi(w_j) = \prod_{i=1}^m z_i^{a_{ij}}$$
$$z_i^{a_{ij} A_j} = z_i^{b_i}$$

If $(A_1 \dots A_n)$ an integer pt. in feasible region, $a_{ij} A_j = b_i$

$$z_i^{a_{ij} A_j} = z_i^{b_i} = \prod_{j=1}^n z_i^{a_{ij} A_j} \Longrightarrow \prod_{j=1}^n \prod_{i=1}^m (z_i^{a_{ij}})^{A_j} = \prod_{i=1}^m z_i^{b_i} = \prod_{j=1}^n \varphi(w_j)^{A_j} = \prod_{j=1}^n \varphi(w_j)^{A_j} = \varphi \left(\prod_{j=1}^n w_j^{A_j} \right) = \prod_{i=1}^m z_i^{b_i}$$

since $\varphi(g(w_1 \dots w_n)) = g(\varphi(w_1) \dots \varphi(w_n))$

If $\varphi : \prod_{j=1}^n w_j^{A_j} \mapsto \prod_{i=1}^m z_i^{b_i}$

$$\varphi \left(\prod_{j=1}^n w_j^{A_j} \right) = \prod_{j=1}^n (\varphi(w_j))^{A_j} = \prod_{i=1}^m z_i^{b_i} = \prod_{j=1}^n \left(\prod_{i=1}^m z_i^{a_{ij}} \right)^{A_j} \Longrightarrow \prod_{j=1}^n z_i^{a_{ij} A_j} = z_i^{b_i}$$

or $a_{ij} A_j = b_i$. So $(A_1 \dots A_n)$ integer pt.

Exercise 4.

$$\prod_{i=1}^m z_i^{b_i} = \prod_{i=1}^m \prod_{j=1}^n z_i^{a_{ij} A_j} = \prod_{j=1}^n \left(\prod_{i=1}^m z_i^{a_{ij}} \right)^{A_j} = \prod_{j=1}^n \varphi(w_j)^{A_j} = \varphi \left(\prod_{j=1}^n w_j^{A_j} \right)$$

So if given $(b_1 \dots b_m) \in \mathbb{Z}^m$, and for a given a_{ij}, $a_{ij} A_j = b_i$

For $m \leq n$, then a_{ij} is surjective, so $\exists\, A_j$ s.t. $\prod_{i=1}^m z_i^{b_i} = \varphi \left(\prod_{j=1}^n w_j^{A_j} \right)$

Proposition 4 (1.8)**.** *Suppose* $f_1 \dots f_n \in k[z_1 \dots z_m]$ *given*
Fix monomial order in $k[z_1 \dots z_n, w_1 \dots w_n]$ *with elimination property:*
$\forall$ *monomial containing 1 of* z_i *greater than any monomial containing only* w_j

Let $\mathcal{G}$ *Gröbner basis for ideal*

$$I = \langle f_1 - w_1 \dots f_n - w_n \rangle \subset k[z_1 \dots z_m, w_1 \dots w_n]$$

$\forall f \in k[z_1 \dots z_m]$, *let* $\overline{f}^{\mathcal{G}}$ *be remainder on division of* f *by* $\mathcal{G}$
Then

(a) *polynomial* f *s.t.* $f \in k[f_1 \dots f_n]$ *iff* $g = \overline{f}^{\mathcal{G}} \in k[w_1 \dots w_n]$

(b) *if* $f \in k[f_1 \dots f_n]$ *as in part (a),*
$g = \overline{f}^{\mathcal{G}} \in k[w_1 \dots w_n]$
then $f = g(f_1 \dots f_n)$ *, giving an expression for* f *as polynomial in* f_j

(c) *if* $\forall f_i, f$ *monomials,* $f \in k[f_1 \dots f_n]$,
then g *also a monomial.*

14.2. **Integer Programming and Combinatorics.**

15. Algebraic Coding Theory

16. The Berlekamp-Massey-Sakata Decoding Algorithm

References

[1] David A. Cox. John Little. Donal O'Shea. **Using Algebraic Geometry**. Second Edition. Springer. 2005. ISBN 0-387-20706-6 QA564.C6883 2004
[2] David Cox, John Little, Donal O'Shea. **Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra**, Fourth Edition, Springer