Introduction to Algebraic Geometry

Rostislav Horčík

Version 1.11

Chapter 1

Polynomial rings and affine varieties

1.1 Commutative rings and fields

Definition 1.1.1 An algebra $(R, +, \cdot, 0, 1)$ is called a *commutative ring* if the following conditions are satisfied:

1. $(a + b) + c = a + (b + c)$ and $(ab)c = a(bc)$ for all $a, b, c \in R$,
2. $a + b = b + a$ and $ab = ba$ for all $a, b \in R$,
3. $a(b + c) = ab + ac$ for all $a, b, c \in R$,
4. $a + 0 = a \cdot 1 = a$ for all $a \in R$,
5. Given $a \in R$, there is $b \in R$ such that $a + b = 0$.

We will often omit the word commutative since all the considered rings in this course are commutative.

Typical example is set of integers $\mathbb{Z}$ endowed with the usual addition and multiplication.

Definition 1.1.2 A commutative ring R is called a *field* if for all $a \in R \setminus \{0\}$ there is $b \in R$ such that $ab = 1$.

Typical examples are real numbers $\mathbb{R}$, rational numbers $\mathbb{Q}$ and complex numbers $\mathbb{C}$.

Definition 1.1.3 Let R be a ring. The group of *units* $R^\times$ is the set

$$R^\times = \{a \in R \mid (\exists b \in R)(ab = 1)\}.$$

Proposition 1.1.4 *The set $R^\times$ forms an Abelian group under the multiplication from R.*

PROOF: Let $a, c \in R^\times$. Then there are $b, d \in R$ such that $ab = 1$ and $cd = 1$. Thus $(ac)(bd) = (ab)(cd) = 1 \cdot 1 = 1$, i.e. $ac \in R^\times$. Further, we have trivially $1 \in R^\times$. Finally, if follows from the definition of $R^\times$ that for each $a \in R^\times$ the corresponding $b \in R$ such that $ab = 1$ is the inverse of a and clearly $b \in R^\times$ as well. □

Example 1.1.5 $\mathbb{Z}^\times = \{1, -1\}$. Let k be a field then $k^\times = k \setminus \{0\}$.

Definition 1.1.6 A commutative ring R is an *integral domain* if whenever $a, b \in R$ and $ab = 0$, then either $a = 0$ or $b = 0$.

Observation 1.1.7 *Let R be an integral domain and $a, b, c \in R$, $c \neq 0$. Then $ac = bc$ implies $a = b$.*

PROOF: $0 = ac - bc = (a - b)c$ implies $a - b = 0$. □

Definition 1.1.8 Let R, S be rings. A mapping $\phi\colon R \to S$ is a *ring homomorphism* if $\phi(1) = 1$, $\phi(a + b) = \phi(a) + \phi(b)$ and $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$ for all $a, b \in R$. If in addition ϕ is one-to-one and onto, then ϕ is called a *ring isomorphism*.

Definition 1.1.9 Let R be an integral domain. The field of fractions k of R is the collection of fractions a/b with $a, b \in R$, $b \neq 0$, and with the usual rules for addition and multiplication, i.e.

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \qquad \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

Note that since R is an integral domain and $b, d \neq 0$, we have $bd \neq 0$. In addition, two of these fractions a/b and a'/b' represent the same element in k if $ab' = a'b$.

Moreover, the subset $\{a/1 \mid a \in R\}$ forms an integral domain which is isomorphic to R.

1.2 Ideals

Definition 1.2.1 Let R be a commutative ring. A subset $I \subseteq R$ is said to be an *ideal* if it satisfies:

1. $0 \in I$,
2. if $a, b \in I$, then $a + b \in I$,
3. if $a \in I$ and $b \in R$, then $b \cdot a \in I$.

If $I \neq R$ then I is called a *proper* ideal.

Lemma 1.2.2 *Ideals are closed under arbitrary intersections. If $I_0 \subseteq I_1 \subseteq \cdots$ is an ascending chain of ideals, then $\bigcup_{i \in \mathbb{N}} I_i$ is an ideal.*

PROOF: Let $\{I_\lambda \mid \lambda \in \Lambda\}$ be a family of ideals indexed by the elements of Λ. Then clearly $\bigcap_{\lambda \in \Lambda} I_\lambda$ is an ideal. Let $I_0 \subseteq I_1 \subseteq \cdots$ be an ascending chain of ideals and let $I = \bigcup_{i \in \mathbb{N}} I_i$. Then clearly $0 \in I$. If $a, b \in I$ then there is $i \in \mathbb{N}$ such that $a, b \in I_i$. Thus $a + b \in I_i \subseteq I$. Similarly, if $a \in I$ then $a \in I_i$ for some i. Hence $b \cdot a \in I_i \subseteq I$ for any $b \in R$. □

Definition 1.2.3 Let R be a commutative ring and $S \subseteq R$. The smallest ideal containing S is called the *ideal generated by S* (it is just the intersection of all ideals containing S). We denote it by $\langle S \rangle$.

Let $a_1, \ldots, a_n \in R$. We write $\langle a_1, \ldots, a_n \rangle$ instead of $\langle \{a_1, \ldots, a_n\} \rangle$.

Lemma 1.2.4 *Let R be a commutative ring and $\{a_1, \ldots, a_n\} \subseteq R$. Then*

$$\langle a_1, \ldots, a_n \rangle = \left\{ \sum_{i=1}^{n} b_i \cdot a_i \mid b_1, \ldots, b_n \in R \right\}.$$

In particular, if $a \in R$, then

$$\langle a \rangle = \{ b \cdot a \mid b \in R \}.$$

PROOF: First, we check that $I = \{\sum_{i=1}^n b_i \cdot a_i \mid b_1, \ldots, b_n \in R\}$ is an ideal. Since $\sum_{i=1}^n 0 \cdot a_i = 0$, we have $0 \in I$. If $b = \sum_{i=1}^n b_i \cdot a_i \in I$ and $c = \sum_{i=1}^n c_i \cdot a_i \in I$ for some $b_i, c_i \in R$. Then $b + c = \sum_{i=1}^n (b_i + c_i) a_i \in I$. Let $d \in R$. Then $db = \sum_{i=1}^n (db_i) \cdot a_i \in I$. Thus I is an ideal.

Since I contains all the generators a_i, we have $\langle a_1, \ldots, a_n \rangle \subseteq I$. On the other hand, all elements of the form $\sum_{i=1}^n b_i \cdot a_i$, where $b_1, \ldots, b_n \in R$, belong to $\langle a_1, \ldots, a_n \rangle$. Thus $I = \langle a_1, \ldots, a_n \rangle$. □

Definition 1.2.5 The ideal generated by a single element is called *principal*. A proper ideal I is called *prime* if $ab \in I$ implies $a \in I$ or $b \in I$.

Proposition 1.2.6 *The following conditions on a ring R are equivalent:*

1. *every ideal in R is finitely generated;*

2. *every ascending chain of ideals $I_0 \subseteq I_1 \subseteq \cdots$ becomes constant, i.e. for some m, $I_m = I_{m+1} = \cdots$;*

3. *every non-empty set of ideals in R has a maximal element (i.e. an element not properly contained in any other ideal in the set).*

PROOF: ($1 \Rightarrow 2$): If $I_0 \subseteq I_1 \subseteq \cdots$ is an ascending chain, then $I = \bigcup_{i \in \mathbb{N}} I_i$ is again an ideal, and hence has a finite set $\{a_1, \ldots, a_n\}$ of generators. For some m, all $a_i \in I_m$. Thus $I_m = I_{m+1} = \cdots = I$.

($2 \Rightarrow 3$): If (3) is false, then there is a non-empty set S of ideals with no maximal element. Thus there must be a strictly increasing sequence $I_0 \subseteq I_1 \subseteq \cdots$ that never becomes constant.

($3 \Rightarrow 1$): Let I be an ideal, and let S be the set of ideals $J \subseteq I$ that are finitely generated. Let $J' = \langle a_1, \ldots, a_r \rangle$ be the maximal element of S. If $J' \neq I$, then there is $a \in I$ and $a \notin J'$. But $J' \subsetneq \langle a_1, \ldots, a_r, a \rangle \subseteq I$ (a contradiction). □

Definition 1.2.7 A ring R is *Noetherian* if it satisfies the conditions of the proposition.

1.3 Principal ideal domains and unique factorization

Definition 1.3.1 An integral domain R is called *principal ideal domain* (PID) if each its ideal is principal.

Theorem 1.3.2 *Let R be a PID. Then R is Noetherian.*

PROOF: Trivial, since each ideal is finitely generated. □

Definition 1.3.3 Let R be an integral domain.

1. An elements $a, b \in R$ are said to be *associates* if there is a unit $u \in R^\times$ such that $a = ub$. We denote this fact $a \sim b$.

2. An element $a \in R$ divides $b \in R$ (denoted $a|b$) if $b = ac$ for some $c \in R$.

3. A non-zero non-unit element $a \in R$ is *irreducible* if it does not factor, i.e. $a = bc$ implies b or c is a unit.

4. A non-zero non-unit element $a \in R$ is *prime* if it generates a prime ideal, i.e. $a|bc$ implies $a|b$ or $a|c$.

5. Let $a, b \in R$. We say that $c \in R$ is a *greatest common divisor* (gcd) of a and b if $c|a$, $c|b$, and if any element $d \in R$ which divides both a and b also divides c.

Lemma 1.3.4 *1. If a is prime then a is irreducible.*

2. If a is prime and $a|c_1c_2\cdots c_n$, then $a|c_i$ for some i. If each c_j is irreducible, then a and c_i are associates for some i.

3. If $a \sim b$, then a is irreducible (prime) iff b is irreducible (prime). In other words, if a is irreducible (prime) and u is a unit, then au is irreducible (prime).

4. A greatest common divisor is unique up to a unit.

PROOF:

1. Suppose $a = bc$. Then $a|bc$, i.e. $a|b$ or $a|c$ since a is prime. Assume that $a|b$. Then $b = ad$. Consequently, $a = adc$ which implies $dc = 1$. Thus c is a unit.

2. By induction on n. For $n = 1, 2$ it holds. For $n > 2$ we have $a|(c_1 \cdots c_{n-1})c_n$. Thus $a|c_n$ or $a|c_1 \cdots c_{n-1}$. Assume that each c_j is irreducible. We have $a|c_i$ for some i, i.e. $c_i = ad$. Since c_i is irreducible, we get that d is a unit (a is not unit).

3. Let a be irreducible and u a unit. If $au = cd$ then $a = u^{-1}cd$. Thus either $u^{-1}c$ or d is a unit. If d is a unit, we are done. If $u^{-1}c$ is a unit, then $vu^{-1}c = 1$ for some v. Thus c is a unit.

   Let a be prime. If $au|cd$ then $cd = auq$, i.e. $a|cd$. Thus $a|c$ or $a|d$, say $a|c$. Then $c = ax = (au)(u^{-1}x)$, i.e. $au|c$.

4. Let c and c' be two gcd of a and b. Then $c|c'$ and $c'|c$, i.e. $c' = cx$ and $c = c'y$ for some x, y. Thus $c = c'y = cxy$ which implies $1 = xy$. Consequently, x is a unit and $c \sim c'$.

□

Definition 1.3.5 An integral domain R is called a *unique factorization domain* (UFD) if every non-zero non-unit element has unique factorization into irreducible elements, i.e. if $a = p_1 \cdots p_n = q_1 \cdots q_m$, then $n = m$ and there is a permutation σ such that p_i and $q_{\sigma(i)}$ are associates. In other words, we can reorder the factors q_i in such a way that $p_i \sim q_i$ for all i.

Observe that if R is a UFD and $a = p_1 \cdots p_m$ is a factorization into irreducible elements, then some of the irreducible factors p_i can be associates. We can group them together and write $a = up_1^{s_1} \cdots p_n^{s_n}$ where $u \in R^\times$ and $s_1, \ldots, s_n \in \mathbb{N}$.

Example 1.3.6 The set $\mathbb{Z}$ is a UFD since each integer can be uniquely expressed as a product of primes.

Lemma 1.3.7 *Let R be a PID and $a, b \in R$. Let $\langle a, b\rangle = \langle c\rangle$. Then $c = \gcd(a, b)$.*

PROOF: Since $a \in \langle c\rangle$, we have $c|a$. Similarly $c|b$. Let $d|a$ and $d|b$, i.e. $a = dy$ and $b = dz$ with $y, z \in R$. Since $c \in \langle a, b\rangle$, we get $c = wa + tb$ with $w, t \in R$. Then $c = wdy + tdz = d(wy + tz)$, i.e. $d|c$. □

Lemma 1.3.8 *Let R be a PID. Then a is irreducible iff a is prime.*

PROOF: ($\Leftarrow$) Follows from Lemma 1.3.4.

($\Rightarrow$) Suppose that a is irreducible and $a|bc$. If a does not divide b then $\gcd(a, b) = 1$. Since $\langle 1\rangle = \langle a, b\rangle$, we can write $1 = xa + yb$ with some $x, y \in R$. Then $c = xac + ybc$. Since $a|bc$, we get $a|c$. □

Theorem 1.3.9 *Every PID R is a UFD.*

PROOF: First, we prove that a finite factorization into irreducible elements exists. Consider all principal ideals $\langle d\rangle$ where d does not factor into a finite product of irreducibles. Since R is Noetherian, there is a maximal such ideal $\langle c\rangle$. The element c must be reducible otherwise it would have a factorization. Thus $c = ab$ where neither a nor b is a unit. Since each $\langle a\rangle$ and $\langle b\rangle$ contains $\langle c\rangle$ properly (if e.g. $\langle a\rangle = \langle c\rangle$, then $a \sim c$ and $b \sim 1$), each a and b factors into finite product of irreducibles. This gives a finite factorization of c (a contradiction).

Secondly, we deal with the uniqueness. Let $p_1 \cdots p_n = q_1 \cdots q_m$ be two factorization into irreducibles. We will show by induction on n that $m = n$ and after a suitable reordering of factors p_i and q_i are associates. Let $n = 1$. Then $p_1 = q_1 \cdots q_m$. Since p_1 is prime and $p_1|q_1 \cdots q_m$, there is i such that p_1 and q_i are associates, i.e. $q_i = up_1$ for some unit u. W.l.o.g. we can assume that $i = 1$. Thus $p_1 = up_1q_2 \cdots q_m$. Consequently, $1 = uq_2 \cdots q_m$. Hence q_j, $j > 1$ are units and cannot be irreducibles.

Now assume that the claim is valid for $n - 1$. Since $p_1|q_1 \cdots q_m$, there is i such that $q_i = up_1$ for a unit u. Again w.l.o.g. we can assume that $i = 1$. Thus we have

$$p_2 \cdots p_{n-1} = uq_2 \cdots q_m \,.$$

By induction assumption $n - 1 = m - 1$ and after a suitable reordering $p_2 \sim uq_2$ and $p_j \sim q_j$ for $j > 2$. Thus $n = m$. Since $p_2 = vuq_2$ for a unit v, we get that $p_2 \sim q_2$. Consequently, p_i and q_i are associates for all i and the proof is done. □

1.4 Polynomials in one variable

Definition 1.4.1 Let R be a ring. Then the *polynomial ring* $R[X]$ is the collection of all formal sums of the form $a_0+a_1X+a_2X^2+\cdots+a_nX^n$ where $a_i \in R$. $R[X]$ forms a commutative ring under the usual addition and multiplication of polynomials.

The *degree* of a non-zero polynomial f is the largest n such that $a_n \neq 0$, and is denoted by $\deg(f)$.

Proposition 1.4.2 *If R is an integral domain, then $R[X]$ is an integral domain.*

PROOF: Suppose that $f(X) = a_0 + \cdots + a_nX^n$, $a_n \neq 0$ and $g(X) = b_0 + \cdots + b_mX^m$, $b_m \neq 0$ are non-zero polynomials. Then the $(n+m)$-th coefficient of fg is $a_n \cdot b_m$. Since R is an integral domain, we have $a_n \cdot b_m \neq 0$, i.e. fg is not the zero polynomial. □

Observe that in this case we have $\deg(fg) = \deg(f) + \deg(g)$ for non-zero polynomials f, g.

Proposition 1.4.3 *Let R be an integral domain. Then $R[X]^\times = R^\times$ (if we identify the elements of R with the constant polynomials in $R[X]$).*

PROOF: Clearly $R^\times \subseteq R[X]^\times$. Let $f \in R[X]$ be a non-constant polynomial (i.e. $\deg(f) \geq 1$). Consider fg for $g \in R[X]$. If $g = 0$ then $fg = 0$. If $g \neq 0$ then $\deg(fg) = \deg(f) + \deg(g) \geq \deg(f) \geq 1$. Thus in both cases $fg \neq 1$, i.e. $f \notin R[X]^\times$. □

Proposition 1.4.4 *Let k be a field and $f, g \in k[X]$, $g \neq 0$. Then there exists unique polynomials $q, r \in k[X]$ such that $f = gq + r$ and $\deg(r) < \deg(g)$.*

Theorem 1.4.5 *Let k be a field. Then $k[X]$ is a PID.*

PROOF: Let I be an ideal in $k[X]$. The case $I = \{0\}$ is trivial. Assume that $I \neq \{0\}$. Let $g \in I$ be an element of the smallest degree ≥ 0. Consider any $f \in I$. Then $f = gq + r$ and $\deg(r) < \deg(g)$. But $r = gq - f \in I$. Since g has the smallest degree, it follows that $r = 0$. Thus $f = gq$, i.e. $I = \langle g \rangle$. □

Corollary 1.4.6 *Let k be a field. Then $k[X]$ is a UFD.*

1.5 Polynomials in more variables

Let $X_1, \ldots, X_n$ be variables. A *monomial* in $X_1, \ldots, X_n$ is an expression $X_1^{\alpha_1} \cdot X_2^{\alpha_2} \cdots X_n^{\alpha_n}$, where $\alpha_1, \ldots, \alpha_n \in \mathbb{N}$. Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ then we simply write X^α instead of $X_1^{\alpha_1} \cdot X_2^{\alpha_2} \cdots X_n^{\alpha_n}$.

Definition 1.5.1 Let R be a ring. A *polynomial* f in $X_1, \ldots, X_n$ with coefficients in R is a finite linear combination of monomials, i.e.

$$f = \sum_\alpha a_\alpha X^\alpha\,, \quad a_\alpha \in R\,,$$

where the sum is over a finite number of n-tuples $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$. The set of all polynomials in $X_1, \ldots, X_n$ is denoted $R[X_1, \ldots, X_n]$.

An example of polynomial from $\mathbb{Z}[X_1, X_2, X_3]$ is for instance

$$f = 2X_1^3X_3 + 5X_1X_2X_3 - X_2^6X_3^2 + 13\,.$$

Observe that

$$f = (2X_1^3)X_3 + (5X_1X_2)X_3 + (-X_2^6)X_3^2 + (13)X_3^0 = (2X_1^3 + 5X_1X_2)X_3 + (-X_2^6)X_3^2 + (13)X_3^0\,,$$

and $2X_1^3 + 5X_1X_2$, $-X_2^6$, 13 are polynomials in $\mathbb{Z}[X_1, X_2]$.

Observation 1.5.2 *Let R be a ring. Then $R[X_1, \ldots, X_n] = R[X_1, \ldots, X_{n-1}][X_n]$, i.e. each element $f \in R[X_1, \ldots, X_n]$ can be expressed as follows:*

$$f = \sum_{j=0}^{d} f_j(X_1, \ldots, X_{n-1})X_n^j\,, \quad f_j \in R[X_1, \ldots, X_{n-1}]\,, \quad d \in \mathbb{N}\,.$$

Corollary 1.5.3 *Let R be a ring. Then $R[X_1, \ldots, X_n]$ is a ring as well. In addition, if R is an integral domain, then $R[X_1, \ldots, X_n]$ is an integral domain.*

PROOF: By induction on the number of variables. $\square$

Let k be a field. Then $k[X_1, \ldots, X_n]$ is an integral domain whence it has the field of fractions. We denote it by $k(X_1, \ldots, X_n)$.

Proposition 1.5.4 $R[X_1, \ldots, X_n]^\times = R^\times$.

PROOF: By induction and Proposition 1.4.3. $\square$

1.6 Unique factorization domain

In this we are going to prove that also $k[X_1, \ldots, X_n]$ is a UFD for a field k. Observe that $k[X_1, \ldots, X_n]$ is no more a PID. To see this, consider the polynomial ring $k[X, Y]$ and the ideal $\langle X, Y\rangle$. Assume that there is $f(X, Y)$ such that $\langle f\rangle = \langle X, Y\rangle$. Then $X = g(X, Y) \cdot f(X, Y)$ and $Y = h(X, Y) \cdot f(X, Y)$ for some $g, h \in k[X, Y]$. Let us see f, g as elements from $k[X][Y]$. Then

$$0 = \deg(X) = \deg(g \cdot f) = \deg(g) + \deg(f)\,.$$

Thus $\deg f = 0$ which implies that f is a constant polynomial, i.e. a member of $k[X]$. Similarly, $\deg(f) = 0$ for f seen as an element of $k[Y][X]$, i.e. $f \in k[Y]$. Consequently, $f \in k$. Thus $\langle f\rangle = k[X, Y]$. However, $\langle X, Y\rangle \neq k[X, Y]$. If they would be the same ideals, then $1 = f(X, Y) \cdot X + g(X, Y) \cdot Y$ for some $f, g \in k[X, Y]$ which is a contradiction.

Proposition 1.6.1 *Let R be a UFD and $a, b \in R$. Then $\gcd(a, b)$ exists.*

PROOF: Let $a = up_1^{r_1} \cdots p_n^{r_n}$ and $b = vp_1^{s_1} \cdots p_n^{s_n}$, $u, v \in R^\times$ (allow the exponents to be 0, to use a common set of irreducibles to express both a and b). We claim that $\gcd(a, b)$ is

$$g = p_1^{\min(r_1,s_1)} \cdots p_n^{\min(r_n,s_n)} .$$

Clearly $g|a$ and $g|b$. Let $d|a$ and $d|b$. Enlarge the collection of inequivalent irreducibles p_i if necessary such that d can be expressed as

$$d = wp_1^{h_1} \cdots p_n^{h_n} , \quad w \in R^\times .$$

From $d|a$ we have $a = dD$ for some $D \in R$. Let

$$D = Wp_1^{H_1} \cdots p_n^{H_n} , \quad W \in R^\times .$$

Then

$$wWp_1^{h_1+H_1} \cdots p_n^{h_n+H_n} = dD = a = up_1^{r_1} \cdots p_n^{r_n} .$$

Unique factorization and non-associateness of the p_i implies that the exponents are the same, i.e. for all i we have $h_i + H_i = r_i$. Thus $h_i \leq r_i$. Similarly $h_i \leq s_i$. Hence $h_i \leq \min(r_i, s_i)$, i.e. $d|g$. □

Observe that if any pair elements in a ring has a gcd, then each n-tuple of elements has it. In fact, we have

$$\gcd(a_1, a_2, a_3, \ldots, a_n) = \gcd(\gcd(a_1, a_2), a_3, \ldots, a_n) .$$

Proposition 1.6.2 *Let R be a UFD and $a \in R$. Then a is irreducible iff a is prime.*

PROOF: The right-to-left direction follows from Lemma 1.3.4. Suppose that a is irreducible and $a|bc$. If b or c is a unit, then a divides the other one. If b or c is 0, then $a|0$. Thus assume that b, c are non-unit non-zero elements. There is d such that $ad = bc$. Since R is a UFD, b and c have unique factorizations into irreducibles, i.e. $b = b_1 \cdots b_n$ and $c = c_1 \cdots c_m$. Then $b_1 \cdots b_n c_1 \cdots c_m$ is a factorization of bc. As a is irreducible, $a \sim b_i$ or $a \sim c_j$. Thus either $a|b$ or $a|c$. □

Proposition 1.6.3 *Let R be a UFD with field of fractions F. If $f(X) \in R[X]$ factors into the product of two non-constant polynomials in $F[X]$, then it factors into the product of two non-constant polynomials in $R[X]$.*

PROOF: Let $f = gh$ in $F[X]$. For suitable $c, d \in R$, $g_1 = cg$ and $h_1 = dh$ have coefficients in R. Thus $cdf = g_1 \cdot h_1$ in $R[X]$. Since R is a UFD, cd factors into the finite product of irreducibles. Let $p \in R$ be a irreducible element such that $p|cd$. Then $p|g_1h_1$. Since p is prime by Lemma 1.6.2, $p|g_1$ or $p|h_1$ (say $p|g_1$). Thus p divides all the coefficients of g_1 and $g_1 = pg_2$. Now we have a factorization $(cd/p)f = g_2 \cdot h_1$. Continuing in this fashion, we can remove all the irreducible factors of cd. □

It follows from the construction of the proof of the latter proposition that if $f = gh = g'h'$ with $g, h \in F[X]$ and $g', h' \in R[X]$, then $g' = ug$ and $h' = vh$ for some $u, v \in F^\times$, i.e. $g' \sim g$ and $h' \sim h$ in $F[X]$, i.e. $\deg(g) = \deg(g')$ and $\deg(h) = \deg(h')$.

Corollary 1.6.4 *Let R be a UFD with fraction field F and $f \in R[X]$. If $f = f_1 f_2 \cdots f_n$ for $f_i \in F[X]$ non-constant polynomials, then $f = f_1' f_2' \cdots f_n'$ with non-constant polynomials $f_i' \in R[X]$ and $f_i \sim f_i'$ in $F[X]$.*

PROOF: By induction on n. For $n = 2$ the claim follows from Proposition 1.6.3 and the above discussion. Assume that the claim is valid for $n-1$ and $f = f_1 \cdots f_n$. Then by Proposition 1.6.3 $f = f_1' g$ with $f_1', g \in R[X]$, $f_1 \sim f_1'$ and $g \sim f_2 \cdots f_n$ in $F[X]$. Thus there is $u \in F^\times$ such that $g = u f_2 \cdots f_n$. By induction assumption $g = f_2' \cdots f_n'$ with $f_i' \in R[X]$ non-constant, $f_2' \sim u f_2 \sim f_2$, and $f_i' \sim f_i$ for $i > 2$. Thus $f = f_1' f_2' \cdots f_n'$ and $f_i \sim f_i'$ in $F[X]$. □

Note that if f_i is irreducible in $F[X]$ then f_i' is irreducible in $F[X]$ by Lemma 1.3.4.

Definition 1.6.5 Let R be a UFD and $f \in R[X]$. The *content* of f (denoted $c(f)$) is the gcd of all coefficients of f, i.e. $c(f) = \gcd(a_0, \ldots, a_n)$ for $f = a_0 + \cdots + a_n X^n$. A polynomial f is said to be *primitive* if $c(f) = 1$.

Lemma 1.6.6 *Let R be a UFD and $f \in R[X]$. Then $f = c(f) \cdot f_1$ with f_1 primitive and this decomposition is unique up to units in R.*

PROOF: Clearly $f = c(f) \cdot f_1$ for a primitive polynomial f_1. Suppose that $f = c(f) \cdot f_1 = d \cdot g$ where $g \in R[X]$ is a primitive polynomial and $d \in R$. Then $d|f$ (i.e. $f = dh$ and $\deg(h) = \deg(f)$). Hence $d|c(f)$, i.e. $c(f) = du$ for some $u \in R$. Consequently, $uf_1 = g$. Since $u|g$ and g is primitive, we get $u \sim 1$. Thus $c(f) \sim d$ and $f_1 \sim g$. □

Lemma 1.6.7 (Gauss's Lemma) *The product of two primitive polynomials is primitive.*

PROOF: Let

$$f = a_0 + \cdots + a_m X^m, \qquad g = b_0 + \cdots + b_n X^n,$$

be primitive polynomials, and let p be an irreducible element of R. Let a_i be the first coefficient of f not divisible by p and b_j the first coefficient of g not divisible by p. Then $(i+j)$-th coefficient c_{i+j} of fg equals:

$$c_{i+j} = (a_0 b_{i+j} + a_1 b_{i+j-1} + \cdots + a_{i-1} b_{j+1}) + a_i b_j + (a_{i+1} b_{j-1} + \cdots + a_{i+j} b_0).$$

All the terms of c_{i+j} are divisible by p except $a_i b_j$. Therefore p does not divide the $(i+j)$-th coefficient of fg. We have shown that no irreducible element divides all the coefficients of fg. Thus fg must be primitive. □

Lemma 1.6.8 *Let R be a UFD and $f, g \in R[X]$. Then $c(fg) = c(f) \cdot c(g)$.*

PROOF: Let $f = c(f) \cdot f_1$ and $g = c(g) \cdot g_1$ with f_1 and g_1 primitive. Then $fg = c(f)c(g) f_1 g_1$ with $f_1 g_1$ primitive by Gauss's lemma. Since the decomposition $fg = c(f)c(g) f_1 g_1$ is unique, we have $c(fg) = c(f)c(g)$ (up to a unit). □

Lemma 1.6.9 *Let R be a UFD with field of fraction F. Then irreducible elements of $R[X]$ are exactly*

1. *the constant polynomials $f = c$ with c an irreducible element of R and*
2. *the primitive polynomials $f \in R[X]$ that are irreducible in $F[X]$.*

PROOF: Each constant polynomial $f = c$ with c an irreducible element of R is clearly irreducible in $R[X]$ and vice versa. Let $f \in R[X]$ such that f is primitive and irreducible in $F[X]$. Then the only possible factorization in $R[X]$ is $f = dg$ where $d \in R$ since f is irreducible in $F[X]$. Since f is primitive and $d|f$, $d \in R^\times$, i.e. f is irreducible in $R[X]$. Conversely, let f be an irreducible non-constant polynomial in $R[X]$. Then $f = c(f)f_1$. Thus $c(f)$ is a unit in $R[X]^\times = R^\times$, i.e. f is primitive. Moreover, f is irreducible in $F[X]$ by Proposition 1.6.3. □

Theorem 1.6.10 *Let R be a UFD with field of fractions F. Then $R[X]$ is a UFD.*

PROOF: First, we show that there is a factorization into irreducibles. Let $f \in R[X]$. Then $f = c(f)f_1$ with f_1 primitive. Since R is UFD, $c(f)$ factors into irreducibles of R which are irreducibles of $R[X]$ as well by Lemma 1.6.9. As $f_1 \in F[X]$ and $F[X]$ is a UFD, f_1 factors into irreducibles in $F[X]$, say $f_1 = g_1 \cdots g_n$. By Corollary 1.6.4 $f_1 = g_1' \cdots g_n'$ where g_i' are non-constant polynomials from $R[X]$ and each g_i' is irreducible in $F[X]$. It follows from Lemma 1.6.8 that each g_i' must be primitive since f_1 is primitive. Thus they are irreducible in $R[X]$ by Lemma 1.6.9.

Now let
$$f = c_1 \cdots c_m f_1 \cdots f_n = d_1 \cdots d_r g_1 \cdots g_s$$
be two factorizations of f into irreducibles with $c_i, d_j \in R$ and f_i, g_j primitive polynomials. By Lemma 1.6.6 we have
$$c_1 \cdots c_m \sim d_1 \cdots d_r\,, \qquad f_1 \cdots f_n \sim g_1 \cdots g_s\,.$$
Since R is a UFD, we see that $m = r$ and c_i's differ from d_i's only by units and ordering. Similarly since $F[X]$ is a UFD, we see that $n = s$ and f_i's differ from g_i's only by units in F and ordering. But if $f_i = ug_j$ with $u \in F^\times$, then $u \in R^\times$ because f_i and g_j are primitive. Indeed, $u = a/b$ for $a, b \in R$. Then $h = bf_i = ag_j$. Since f_i and g_i are primitive, we get $b \sim c(h) \sim a$ in R, i.e. $a/b \in R^\times$. □

Corollary 1.6.11 *Let k be a field. Then $k[X_1, \ldots, X_n]$ is a UFD.*

Example 1.6.12 Let $f, g \in k[X]$ such that $\gcd(f, g) = 1$ in $k[X]$. Prove that the following polynomial from $k[X, Y]$ is irreducible:
$$h(X, Y) = f(X) \cdot Y + g(X)\,.$$

Clearly h is irreducible in $k(X)[Y]$ (its degree in $k(X)[Y]$ is 1). Thus the only possible factorizations of h as a product pq are such that either $p \in k(X)$ or $q \in k(X)$, say $p \in k(X)$. Then $q = c \cdot Y + d$ for some $c, d \in k(X)$. Since we are interested in factorizations in $k[X, Y]$, assume that $p, q \in k[X, Y]$, i.e. $c, d \in k[X]$. We have
$$h = f \cdot Y + g = pq = p(c \cdot Y + d) = pc \cdot Y + pd\,.$$
Thus $f = pc$ and $g = pd$. As $\gcd(f, g) = 1$ in $k[X]$, we get $p \in k^\times$, i.e. h is irreducible in $k[X, Y]$.

Example 1.6.13 Prove that $Y + X^n \in k[X, Y]$ is irreducible for all $n \in \mathbb{N}$.

1.7 Affine varieties

Definition 1.7.1 Let k be a field. We define an *affine n-space* to be the set

$$k^n = \{(a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in k\}\,.$$

Let $f \in k[X_1, \ldots, X_n]$. Then f defines a function $f : k^n \to k$ in the obvious way. This correspondence need not be one-to-one. For instance, if k is a finite field, then there are only finitely many functions from k^n to k but countable many polynomials. However, as long as k is infinite, this assignment is injective.

Proposition 1.7.2 *Let k be an infinite field and $f \in k[X_1, \ldots, X_n]$. Then $f = 0$ iff $f : k^n \to k$ is the zero function.*

PROOF: The left-to-right direction is obvious. The other one can be proven by induction on the number of variables. When $n = 1$, we know that a non-zero polynomial in $k[X_1]$ can have only finitely many roots. Since $f(a) = 0$ for all $a \in k$ (and k is infinite), f must be the zero polynomial. Now assume that the claim is valid for $n-1$, and let $f \in k[X_1, \ldots, X_n]$. We can write $f(X_1, \ldots, X_n) = \sum_{i=0}^{d} g_i(X_1, \ldots, X_{n-1})X_n^i$. Fix $(a_1, \ldots, a_{n-1}) \in k^{n-1}$. Since $f(a_1, \ldots, a_{n-1}, x_n)$ is the zero function, $f(a_1, \ldots, a_{n-1}, X_n)$ must be the zero polynomial in $k[X_n]$, i.e. its coefficients $g_i(a_1, \ldots, a_{n-1})$ are zero. As $(a_1, \ldots, a_{n-1})$ was chosen arbitrarily, we get by the induction assumption that g_i are the zero polynomials. Thus f must be the zero polynomial. □

Corollary 1.7.3 *Let k be an infinite field and $f, g \in k[X_1, \ldots, X_n]$. Then $f = g$ iff $f : k^n \to k$ and $g : k_n \to k$ are the same functions.*

PROOF: Assume that $f : k^n \to k$ and $g : k_n \to k$ are the same functions. Then $f - g$ is the zero function, i.e. $f - g$ is the zero polynomial. Thus $f = g$ in $k[X_1, \ldots, X_n]$. The other direction is trivial. □

Definition 1.7.4 Let $S \subseteq k[X_1, \ldots, X_n]$. Then the *affine variety* defined by S is the set

$$\mathbf{V}(S) = \{a \in k^n \mid f(a) = 0 \text{ for all } f \in S\}\,.$$

By abuse of notation, we also write $\mathbf{V}(f_1, \ldots, f_k)$ for $\mathbf{V}(S)$ if $S = \{f_1, \ldots, f_n\}$.

Example 1.7.5 Here are some simple examples of affine varieties:

1. the affine n-space $k^n = \mathbf{V}(0)$,
2. the empty set $\emptyset = \mathbf{V}(1)$,
3. any single point $\{(a_1, \ldots, a_n)\} = \mathbf{V}(X_1 - a_1, \ldots, X_n - a_n)$,
4. a circle in $\mathbb{R}^2$ centered at the origin is the affine variety $\mathbf{V}(X^2 + Y^2 - r)$, where r is its radius,
5. any linear subspace of k^n.

Observation 1.7.6 *Let $S_1, S_2 \subseteq k[X_1, \ldots, X_n]$. If $S_1 \subseteq S_2$ then $\mathbf{V}(S_2) \subseteq \mathbf{V}(S_1)$.*

Note, that if $f, g \in S$ and $h \in k[X_1, \ldots, X_n]$, then

$$\mathbf{V}(S \cup \{0\}) = \mathbf{V}(S \cup \{f+g\}) = \mathbf{V}(S \cup \{f \cdot h\}) = \mathbf{V}(S)\,.$$

Thus $\mathbf{V}(\langle S \rangle) = \mathbf{V}(S)$. Thus there is no difference whether we consider S to be a subset of $k[X_1, \ldots, X_n]$ or an ideal in $k[X_1, \ldots, X_n]$.

Definition 1.7.7 Let $V \subseteq k^n$. Then the set

$$\mathbf{I}(V) = \{f \in k[X_1, \ldots, X_n] \mid f(a) = 0 \text{ for all } a \in V\}$$

is called *ideal of* V.

The set $\mathbf{I}(V)$ is really an ideal. Clearly, the zero polynomial $0 \in \mathbf{I}(V)$. If $f, g \in \mathbf{I}(V)$, then $(f+g)(a) = f(a) + g(a) = 0 + 0 = 0$ for all $a \in V$. Finally, for any $h \in k[X_1, \ldots, X_n]$ we have $(h \cdot f)(a) = h(a) \cdot f(a) = h(a) \cdot 0 = 0$ for all $a \in V$.

Observation 1.7.8 *Let $V_1, V_2 \subseteq k^n$. If $V_1 \subseteq V_2$ then $\mathbf{I}(V_2) \subseteq \mathbf{I}(V_1)$.*

Thus we have the following correspondence between affine varieties and ideals:

$$\left\{ \begin{array}{c} \text{affine varieties} \\ \text{in } k^n \end{array} \right\} \begin{array}{c} \xrightarrow{\mathbf{I}} \\ \xleftarrow{\mathbf{V}} \end{array} \left\{ \begin{array}{c} \text{ideals in} \\ k[X_1, \ldots, X_n] \end{array} \right\}.$$

The mappings $\mathbf{I}, \mathbf{V}$ are not inverses of each other in general. Consider e.g. $\langle X^2 \rangle$ in $k[X]$. Then $\mathbf{V}(X^2) = \{0\}$ and $\mathbf{I}(\mathbf{V}(X^2)) = \langle X \rangle \neq \langle X^2 \rangle$. However, we have $S \subseteq \mathbf{I}(\mathbf{V}(S))$ for S an ideal.

Lemma 1.7.9 *Affine varieties are closed under arbitrary intersections and finite unions, i.e.*

1. *if $\{S_i\}$ is a family of subsets of $k[X_1, \ldots, X_n]$, then $\bigcap_i \mathbf{V}(S_i) = \mathbf{V}(\bigcup_i S_i)$,*
2. *if $S_1, S_2 \subseteq k[X_1, \ldots, X_n]$, then $\mathbf{V}(S_1) \cup \mathbf{V}(S_2) = \mathbf{V}(S_1 S_2)$, where*

$$S_1 S_2 = \{f \cdot g \mid f \in S_1, g \in S_2\}\,.$$

PROOF: The first part is trivial. For the second consider $a \in \mathbf{V}(S_1) \cup \mathbf{V}(S_2)$. Thus either $f(a) = 0$ for all $f \in S_1$ or $g(a) = 0$ for all $g \in S_2$, say $f(a) = 0$ for all $f \in S_1$. Then $(f \cdot g)(a) = f(a) \cdot g(a) = 0$ for all $f \cdot g$ in $S_1 S_2$. Conversely, assume that $a \notin \mathbf{V}(S_1) \cup \mathbf{V}(S_2)$, i.e. $a \notin \mathbf{V}(S_1)$ and $a \notin \mathbf{V}(S_2)$. Thus there $f \in S_1$ and $g \in S_2$ such that $f(a) \neq 0$ and $g(a) \neq 0$. Hence $(f \cdot g)(a) \neq 0$, i.e. $f \cdot g \notin \mathbf{V}(S_1 S_2)$. □

Remark 1.7.10 Due to the previous lemma, it can be easily seen that affine varieties on k^n forms a topology whose closed sets are exactly affine varieties. This topology on k^n is called *Zariski topology.* Zariski topology e.g. on $\mathbb{R}^n$ is much more coarser than the usual one (closed set are in some sense "very small"). For instance the only closed proper subsets of k^1 w.r.t. this topology are just finite subsets.

Example 1.7.11 Let $f, g \in \mathbb{C}[X, Y]$. Show that $\mathbf{V}(f, g)$ is finite iff f and g have no common irreducible factor.

($\Rightarrow$): First, we prove that $\mathbf{V}(f)$ is infinite if f is non-constant. W.l.o.g. we can assume that $f = \sum_{i=0}^{N} a_i(X)Y^i$ and $N > 0$ (otherwise interchange the variables). Then $a_N \in \mathbb{C}[X]$ is the leading coefficient of f. Clearly, a_N can vanish only for finitely many values of X. This means that for infinitely many values of X, the leading coefficient a_N is non-zero. If we fix one of those values $x \in \mathbb{C}$, then $f(x, Y)$ is a polynomial from $\mathbb{C}[Y]$ of degree N. Since $\mathbb{C}$ is algebraically closed, $f(x, Y)$ has at least one root. Thus for each value of X where a_N does not vanish, we have an element of $\mathbf{V}(f)$. Moreover, for different such values, we get different elements of $\mathbf{V}(f)$.

Secondly, it is clear that if f and g have a common irreducible factor d, then $\mathbf{V}(d)$ is infinite and $\mathbf{V}(d) \subseteq \mathbf{V}(f, g)$ because $f = du$ and $g = dv$ for some $u, v \in \mathbb{C}[X, Y]$.

($\Leftarrow$): This implication holds for any field. So assume that $f, g \in k[X, Y]$. Recall that $k[X, Y] = k[X][Y]$. Consider factorizations of f and g into irreducibles:

$$f = c_1 \cdots c_n \cdot f_1 \cdots f_m\,, \quad g = d_1 \cdots d_k \cdot g_1 \cdots g_s\,,$$

where $c_i, d_j \in k[X]$ and $f_i, g_j \in k[X][Y]$ primitive. If f, g have no common irreducible factor in $k[X, Y]$, then $c_i \not\sim d_j$ and $f_i \not\sim g_j$. I claim that f, g have no common irreducible factor also in $k(X)[Y]$. Clearly, c_i, d_j are units of $k(X)$ and f_i, g_j are irreducibles also in $k(X)[Y]$. Assume that there is an irreducible element $e \in k(X)[Y]$ such that $e|f$ and $e|g$ in $k(X)[Y]$. Then $e \sim f_i$ for some i and $e \sim g_j$ for some j in $k(X)[Y]$. Thus $f_i = ug_j$ for some $u \in k(X)^\times$. Since f_i, g_j are primitive $u \in k[X]^\times = k^\times$, $f_i \sim g_j$ in $k[X][Y]$ (a contradiction). Consequently, $\gcd(f, g) = 1$ in $k(X)[Y]$.

Finally, since $\langle f, g\rangle = \langle 1\rangle$ in $k(X)[Y]$, there are $A, B \in k(X)[Y]$ such that $Af + Bg = 1$. If we multiply this equality by all denominators of all coefficients of A, B (which are from $k[X]$), we get $\tilde{A}f + \tilde{B}g = \tilde{C}$ for some $\tilde{A}, \tilde{B} \in k[X, Y]$ and $\tilde{C} \in k[X]$. Thus $\tilde{C} \in \langle f, g\rangle$ in $k[X, Y]$. Since $\tilde{C} \in k[X]$, it can have only finitely many roots. Let $x_1, \ldots, x_k$ be these roots. Then $(x, y) \in \mathbf{V}(f, g)$ only if $x = x_i$ for some i. Further, for all i we have that $f(x_i, Y), g(x_i, Y) \in k[Y]$ can also have only finitely many roots. Thus $\mathbf{V}(f, g)$ is finite.

1.8 Quotient rings

Definition 1.8.1 Let R be a ring. An equivalence relation $\sim$ on R is called a *congruence* if $a \sim a'$ and $b \sim b'$ implies $a + b \sim a' + b'$ and $ab \sim a'b'$.

Lemma 1.8.2 *Let R be a ring and I its ideal. Then the relation defined by $a \sim_I b$ iff $a - b \in I$, is a congruence.*

PROOF: First, $a - a = 0 \in I$, $b - a = -1 \cdot (a - b) \in I$, and $a - b, b - c \in I$ implies $a - c = a - b + b - c \in I$. Suppose that $a \sim a'$ and $b \sim b'$, i.e. $a - a', b - b' \in I$. Then $a + b - a' - b' = (a - a') + (b - b') \in I$. Further, $ab - a'b' = ab - a'b + a'b - a'b' = (a - a')b + a'(b - b') \in I$. □

Definition 1.8.3 Let R be a ring and I its ideal. Then the *quotient ring* R/I is the set of equivalence classes $\{[a] \mid a \in R\}$ where $[a] = \{b \in R \mid a \sim_I b\}$ endowed with operations: $[a] + [b] = [a + b]$ and $[a] \cdot [b] = [a \cdot b]$. The additive identity is $[0]$ and multiplicative is $[1]$.

It is easy to check that the latter algebra is really a ring. One has to only show that the operations are well-defined (i.e. they are independent of the choice of representatives of the equivalence classes). Suppose that $a \sim_I a'$ and $b \sim_I b'$. Then by Lemma 1.8.2 we have $a + b \sim_I a' + b'$ and $ab \sim_I a'b'$, i.e. $[a] + [b] = [a + b] = [a' + b'] = [a'] + [b']$ and $[a] \cdot [b] = [ab] = [a'b'] = [a'] \cdot [b']$. The ring axioms are trivially satisfied e.g.

$$[a]([b] + [c]) = [a(b + c)] = [ab + ac] = [a][b] + [a][c]\,, \quad [1] \cdot [a] = [1 \cdot a] = [a]\,.$$

Observe that $[0] = \{f \mid f - 0 \in I\} = I$.

Lemma 1.8.4 *Let R be a ring and I an ideal. Then R/I is an integral domain iff I is prime.*

PROOF: ($\Leftarrow$): Assume that $[a][b] = [0]$. Then $ab = ab - 0 \in I$. Since I is prime, we get $a \in I$ or $b \in I$. Thus $[a] = [0]$ or $[b] = [0]$.

($\Rightarrow$): Let $ab \in I$. Then $[0] = [ab] = [a][b]$. Since R/I is an integral domain either $[a] = [0]$ or $[b] = [0]$. Thus either $a \in I$ or $b \in I$. $\square$

Definition 1.8.5 Let R be a ring and I a proper ideal. The ideal I is called *maximal* if for all ideals $J \supseteq I$ we have either $J = R$ or $J = I$.

Observe that each maximal ideal I is prime. Indeed, assume that $ab \in I$. If $a \notin I$ and $b \notin I$, then $\langle I \cup \{a\} \rangle = R$, i.e. $1 = fa + g$ for some $f \in R$ and $g \in I$. Thus $b = fab + bg \in I$.

Lemma 1.8.6 *Let R be a ring and I a proper ideal. Then I is maximal iff R/I is a field.*

PROOF: ($\Rightarrow$): Since I is prime, R/I is an integral domain. We will prove that all non-zero elements of R/I have a multiplicative inverse. Let $[a] \neq [0]$, i.e. $a \notin I$. Since I is maximal, we have $\langle I \cup \{a\} \rangle = R$. Thus $1 = fa + g$ for some $f \in R$ and $g \in I$. Consequently, $fa - 1 = g \in I$, i.e. $[f][a] = [fa] = [1]$.

($\Leftarrow$): Assume that R/I is a field. Let $a \notin I$. Then there is $b \in R$ such that $[a][b] = [ab] = [1]$. Thus $1 - ab = g \in I$. Since $1 = g + ab \in \langle I \cup \{a\} \rangle$, we get $\langle I \cup \{a\} \rangle = R$. Hence we see that whenever we try to extend I by an element a not belonging to I, we obtain the whole ring R. This means that I is maximal. $\square$

Chapter 2

Gröbner bases

In this chapter we will develop the theory of Gröbner bases. The following problems can be considered as our motivation:

- **Ideal description:** Given an ideal I in $k[X_1, \ldots, X_n]$. Is there a finite generating set for I?
- **Ideal membership:** Given a polynomial $f \in k[X_1, \ldots, X_n]$ and an ideal $I = \langle f_1, \ldots, f_n \rangle \subseteq k[X_1, \ldots, X_n]$. Is there an algorithm how to decide whether $f \in I$ or not?
- **Solution of a system of polynomial equations:** Given an ideal $I = \langle f_1, \ldots, f_n \rangle \subseteq k[X_1, \ldots, X_n]$. Can we describe $\mathbf{V}(I)$ (at least if it is finite)?

In the case of polynomials in one variable we can answer all the questions immediately. Since $k[X]$ is a PID, the answer to the first question is trivially "yes". Moreover, if $I = \langle f_1, \ldots, f_n \rangle \subseteq k[X]$, then $I = \langle g \rangle$ where $g = \gcd(f_1, \ldots, f_n)$. Thus all polynomials in I are just multiples of g. Consequently, we have an algorithm for the second problem because $f \in I$ iff $g | f$ which can be easily determine by the division algorithm. The last problem is just the problem of computing the roots of g since $\mathbf{V}(I) = \mathbf{V}(g)$.

2.1 Term orders

We have seen that the division algorithm of polynomials in one variable was important for solving the first two above-mentioned problems. We would like to generalize it to the case of several variables. Note that the division in $k[X]$ uses the fact that we can order terms of a given polynomial w.r.t. the powers of X. We need something similar also for polynomials in $k[X_1, \ldots, X_n]$.

Definition 2.1.1 A relation $\preceq$ on a set S is a *partial order* if it is reflexive, transitive and antisymmetric. In addition, $\preceq$ is a *total order* if $x \preceq y$ or $y \preceq x$ for all $x, y \in S$. Finally, a total order on S is called a *well-ordering* if each non-empty subset of S has a minimum.

Let $M \subseteq S$. Recall that an element $y \in M$ is said to be *minimal element* of M w.r.t. a partial order $\preceq$ if $x \in M$ together with $x \preceq y$ implies $x = y$.

Observe that the relation $\leq_\ell$ on $\mathbb{N}^n$ defined as follows:

$$(a_1, \ldots, a_n) \leq_\ell (b_1, \ldots, b_n) \text{ if } a_i \leq b_i \text{ for all } i,$$

is a partial order.

Let $\alpha = (a_1, a_2, \dots, a_n) \in \mathbb{N}^n$ and $\beta = (b_1, b_2, \dots, b_n) \in \mathbb{N}^n$. Then we define the i-th projection $\pi_i(\alpha) = a_i$, the sum $\alpha + \beta = (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n)$ and the difference $\alpha - \beta = (a_1 - b_1, a_2 - b_2, \dots, a_n - b_n) \in \mathbb{Z}^n$.

Definition 2.1.2 A total order $\preceq$ on $\mathbb{N}^n$ is called a *term order (or monomial ordering)* if

1. $\alpha \preceq \beta$ implies $\alpha + \gamma \preceq \beta + \gamma$ for all $\gamma \in \mathbb{N}^n$,

2. $\bar{0} \preceq \alpha$ for all $\alpha \in \mathbb{N}^n$ (where $\bar{0}$ is the zero n-tuple).

Example 2.1.3 Let $\alpha = (a_1, \dots, a_n) \in \mathbb{N}^n$ and $\beta = (b_1, \dots, b_n) \in \mathbb{N}^n$. Then we define the following term orders:

- **Lexicographic Order:** $\alpha \preceq_{lex} \beta$ if either $\alpha = \beta$ or the left-most non-zero component of $\beta - \alpha$ is positive.

- **Graded Lex Order (grlex):** $\alpha \preceq_{grlex} \beta$ if either

$$|\alpha| = \sum_{i=1}^{n} a_i < |\beta| = \sum_{i=1}^{n} b_i \qquad \text{or} \qquad |\alpha| = |\beta| \text{ and } \alpha \preceq_{lex} \beta\,.$$

- **Graded Reverse Lex Order (grevlex):** $\alpha \preceq_{grevlex} \beta$ if either

$$|\alpha| = \sum_{i=1}^{n} a_i < |\beta| = \sum_{i=1}^{n} b_i \qquad \text{or} \qquad |\alpha| = |\beta|$$

  and the right-most non-zero component of $\beta - \alpha$ is negative.

- **Weighted Order:** Let $w \in \mathbb{N}^n$. Then $\alpha \preceq_w \beta$ if

$$\alpha \cdot w < \beta \cdot w \qquad \text{or} \qquad \alpha \cdot w = \beta \cdot w \text{ and } \alpha \preceq_{lex} \beta\,.$$

We have e.g.
$(0,3,4) \preceq_{lex} (1,2,0)$ since $(1,2,0) - (0,3,4) = (1,-1,-4)$,
$(3,2,1) \preceq_{lex} (3,2,4)$ since $(3,2,4) - (3,2,1) = (0,0,3)$,
$(0,0,1) \preceq_{lex} (0,1,0) \preceq_{lex} (1,0,0)$,

$(3,2,0) \preceq_{grlex} (1,2,3)$ since $|(3,2,0)| = 5 < 6 = |(1,2,3)|$,
$(1,1,5) \preceq_{grlex} (1,2,4)$ since $|(1,1,5)| = 7 = |(1,2,4)|$ and $(1,1,5) \preceq_{lex} (1,2,4)$,
$(0,0,1) \preceq_{grlex} (0,1,0) \preceq_{grlex} (1,0,0)$,

$(4,2,3) \preceq_{grevlex} (4,7,1)$ since $|(4,2,3)| = 9 < 12 = |(4,7,1)|$,
$(4,1,3) \preceq_{grevlex} (1,5,2)$ since $|(4,1,3)| = 8 = |(1,5,2)|$ and $(1,5,2) - (4,1,3) = (-3,4,-1)$,
$(0,0,1) \preceq_{grevlex} (0,1,0) \preceq_{grevlex} (1,0,0)$,

Lemma 2.1.4 *Let $\preceq$ be a term order on $\mathbb{N}^n$. Then $\leq_\ell \subseteq \preceq$, i.e. whenever $\alpha \leq_\ell \beta$ then $\alpha \preceq \beta$.*

PROOF: If $\alpha \leq_\ell \beta$ then $\pi_i(\alpha) \leq \pi_i(\beta)$ for all i. Thus $\beta - \alpha \in \mathbb{N}^n$. Consequently, $\bar{0} \preceq \beta - \alpha$. Finally,

$$\alpha = \bar{0} + \alpha \preceq \beta - \alpha + \alpha = \beta\,.$$

□

Theorem 2.1.5 (Dickson's Lemma) *Let $\emptyset \neq S \subseteq \mathbb{N}^n$. Then S has finitely many minimal elements w.r.t. $\leq_\ell$.*

PROOF: By induction on n. For $n = 1$ it is trivial since $\leq_\ell$ coincides with the usual order $\leq$ on $\mathbb{N}$ which is a well-ordering. Assume that the claim is valid for $n-1$. Let $S \subseteq \mathbb{N}^n$ and $\alpha_0 \in S$. Let us define for each $i \in \{1, \ldots, n\}$ and each $a \in \{0, 1, \ldots, \pi_i(\alpha_0) - 1\}$ the following set:

$$S_{i,a} = \{\alpha \in S \mid \pi_i(\alpha) = a\}\,.$$

Obviously every $S_{i,a}$ can be identify with a subset of $\mathbb{N}^{n-1}$. By induction assumption there is a finite set $M_{i,a}$ of minimal elements of $S_{i,a}$. Let

$$M = \{\alpha_0\} \cup \bigcup_{i,a} M_{i,a}\,.$$

The set M is obviously finite. I claim that each minimal element of S belongs to M. Let $\beta \in S$. We will show that $\alpha \leq_\ell \beta$ for some $\alpha \in M$. If β is not greater than or equal to α_0, then it has at least one component strictly smaller than the same component in α_0, i.e. there is i such that $\pi_i(\beta) \leq \pi_i(\alpha_0) - 1$. Thus $\beta \in S_{i,a}$ for some i and a. Consequently β must be greater than or equal to some $\alpha \in M_{i,a} \subseteq M$. □

Corollary 2.1.6 *Each term order $\preceq$ on $\mathbb{N}^n$ is a well-ordering.*

PROOF: Let $\emptyset \neq S \subseteq \mathbb{N}^n$. Then S has finitely many minimal elements $\{\alpha_1, \ldots, \alpha_k\}$ w.r.t. $\leq_\ell$. Let $\beta \in S$. Then $\alpha_i \leq_\ell \beta$ for some i which implies $\alpha_i \preceq \beta$. Since $\preceq$ is a total order, one of $\{\alpha_1, \ldots, \alpha_k\}$ must be the minimum of S w.r.t. $\preceq$. □

Note that since $\preceq$ is a well-ordering, every strictly increasing sequence in $\mathbb{N}^n$ eventually terminates.

2.2 Monomial ideals

Definition 2.2.1 An ideal $I \subseteq k[X_1, \ldots, X_n]$ is *monomial* if there is $S \subseteq \mathbb{N}^n$ (possibly infinite) such that I is generated by $\{X^\alpha \mid \alpha \in S\}$. We write $\langle X^\alpha \mid \alpha \in S\rangle$ for the monomial ideal generated by $S \subseteq \mathbb{N}^n$.

Theorem 2.2.2 *Each monomial ideal in $k[X_1, \ldots, X_n]$ is finitely generated.*

PROOF: Let I be a monomial ideal, and let $A = \{\alpha \mid X^\alpha \in I\}$. By Dickson's Lemma the set A has finitely many minimal elements $\{\alpha_1, \ldots, \alpha_k\}$. I claim that $I = \langle X^{\alpha_1}, \ldots, X^{\alpha_k}\rangle$. Clearly $I \supseteq \langle X^{\alpha_1}, \ldots, X^{\alpha_k}\rangle$. For the second inclusion it suffices to show that each generator of I lies in $\langle X^{\alpha_1}, \ldots, X^{\alpha_k}\rangle$. Let X^α be a generator of I, hence $\alpha \in A$. Then $\alpha_i \leq_\ell \alpha$ for some i, i.e.

$\alpha - \alpha_i \in \mathbb{N}^n$. Thus $X^\alpha = X^{\alpha_i} X^{\alpha - \alpha_i} \in \langle X^{\alpha_1}, \ldots, X^{\alpha_k} \rangle$. □

Lemma 2.2.3 *Let $A \subseteq \mathbb{N}^n$ satisfying the following condition:*

$$\alpha \in A\,, \quad \beta \in \mathbb{N}^n \quad \Longrightarrow \quad \alpha + \beta \in A\,. \tag{*}$$

Then the k-linear subspace J of $k[X_1, \ldots, X_n]$ generated by $\{X^\alpha \mid \alpha \in A\}$ is the monomial ideal $\langle X^\alpha \mid \alpha \in A \rangle$.

PROOF: We have to prove that J is an ideal. Clearly J is closed under addition and $0 \in J$. Let $f \in J$ and $g \in k[X_1, \ldots, X_n]$. Then

$$fg = \left(\sum_{\alpha \in A} c_\alpha X^\alpha \right) \cdot \left(\sum_{\beta \in \mathbb{N}^n} d_\beta X^\beta \right) = \sum_{\alpha, \beta} c_\alpha d_\beta X^{\alpha + \beta}\,,$$

where all the sums are finite. Since A satisfies (*), we get $X^{\alpha+\beta} \in J$. Thus $fg \in J$.

Clearly, $J \subseteq \langle X^\alpha \mid \alpha \in A \rangle$ because every k-linear combination of the monomials X^α must belong to $\langle X^\alpha \mid \alpha \in A \rangle$. On the other hand, since $\langle X^\alpha \mid \alpha \in A \rangle$ is the smallest ideal containing all X^α for $\alpha \in A$, we get $J \supseteq \langle X^\alpha \mid \alpha \in A \rangle$. □

From the previous lemma we obtain the following characterization of monomial ideals.

Theorem 2.2.4 *Let $I \subseteq k[X_1, \ldots, X_n]$ be a monomial ideal and $A = \{\alpha \mid X^\alpha \in I\}$. Then A satisfies (*) and I is generated as a k-linear subspace of $k[X_1, \ldots, X_n]$ by $\{X^\alpha \mid \alpha \in A\}$.*

Conversely, let $A \subseteq \mathbb{N}^n$ satisfying (*). Then the k-linear subspace of $k[X_1, \ldots, X_n]$ generated by $\{X^\alpha \mid \alpha \in A\}$ is a monomial ideal.

PROOF: ($\Rightarrow$): Let I be a monomial ideal. First, we will show that A satisfies (*). Let $\alpha \in A$ and $\beta \in \mathbb{N}^n$. Then $X^\alpha \in I$. Consequently, $X^\alpha X^\beta = X^{\alpha+\beta} \in I$. Thus $\alpha + \beta \in A$. The fact that I is generated as a k-linear subspace by A follows from Lemma 2.2.3. Indeed, since A satisfies (*), the k-linear subspace generated by $\{X^\alpha \mid \alpha \in A\}$ is the monomial ideal $\langle X^\alpha \mid \alpha \in A \rangle$ which is obviously equal to I.

($\Leftarrow$): It follows immediately from Lemma 2.2.3. □

Lemma 2.2.5 *Let $S \subseteq \mathbb{N}^n$ and $I = \langle X^\alpha \mid \alpha \in S \rangle$ be the corresponding monomial ideal. Then $I = \langle X^\alpha \mid \alpha \in A \rangle$ where*

$$A = \{\beta \in \mathbb{N}^n \mid (\exists \alpha \in S)(\alpha \leq_\ell \beta)\}\,.$$

Moreover, $X^\beta \in I$ iff $X^\alpha | X^\beta$ for some $\alpha \in S$, i.e. $A = \{\alpha \in \mathbb{N}^n \mid X^\alpha \in I\}$.

PROOF: Observe that $S \subseteq A$. Thus $I = \langle X^\alpha \mid \alpha \in S \rangle \subseteq \langle X^\alpha \mid \alpha \in A \rangle$. On the other hand, let $\beta \in A$, i.e. there is $\alpha \in S$ such that $\alpha \leq_\ell \beta$. Then $\beta - \alpha \in \mathbb{N}^n$ and $X^\beta = X^{\beta - \alpha} X^\alpha$, i.e. $X^\beta \in I$. Hence $\langle X^\alpha \mid \alpha \in A \rangle \subseteq I$.

The right-to-left direction of the second statement is straightforward. For the other one assume that $X^\beta \in I$. Observe that A satisfies (*). Thus by Lemma 2.2.3 I is generated as a k-linear space by $\{X^\alpha \mid \alpha \in A\}$. Consequently, $X^\beta = \sum_{\alpha \in A} c_\alpha X^\alpha$ where the sum is finite. Since two polynomials are equal iff they have the same coefficients, $\beta = \alpha$ for some $\alpha \in A$. As $\beta \in A$, there is $\alpha \in S$ such that $\alpha \leq_\ell \beta$, i.e. $X^\alpha | X^\beta$. □

Corollary 2.2.6 *Let $S \subseteq \mathbb{N}^n$ and $I = \langle X^\alpha \mid \alpha \in S\rangle$. Then the minimal elements of $A = \{\alpha \in \mathbb{N}^n \mid X^\alpha \in I\}$ belong to S, i.e. $I = \langle X^{\alpha_1},\ldots,X^{\alpha_s}\rangle$ for $\alpha_1,\ldots,\alpha_s \in S$.*

PROOF: By the previous lemma we have

$$A = \{\beta \in \mathbb{N}^n \mid (\exists \alpha \in S)(\alpha \leq_\ell \beta)\}\,.$$

Let α_0 be a minimal element of A. Then there exists $\alpha \in S$ such that $\alpha \leq_\ell \alpha_0$. Since $S \subseteq A$ and α_0 is minimal, we obtain $\alpha_0 = \alpha \in S$. □

2.3 Division in $k[X_1,\ldots,X_n]$

Definition 2.3.1 Let $f = \sum_\alpha c_\alpha X^\alpha$ be a non-zero polynomial in $k[X_1,\ldots,X_n]$ and $\preceq$ a term order.

1. The *multidegree* of f is
$$\mathrm{mdeg}(f) = \max\{\alpha \in \mathbb{N}^n \mid c_\alpha \neq 0\}\,,$$
(the maximum is taken w.r.t. $\preceq$).
2. The *leading coefficient* of f is
$$\mathrm{LC}(f) = c_{\mathrm{mdeg}(f)} \in k\,.$$
3. The *leading monomial* of f is
$$\mathrm{LM}(f) = X^{\mathrm{mdeg}(f)}\,.$$
4. The *leading term* of f is
$$\mathrm{LT}(f) = \mathrm{LC}(f)\cdot \mathrm{LM}(f)\,.$$

Let X^α and X^β be two monomials, and let $\preceq$ be a term order. Then we write $X^\alpha \preceq X^\beta$ if $\alpha \preceq \beta$.

Lemma 2.3.2 *Let $f, g \in k[X_1,\ldots,X_n]$ be non-zero polynomials. Then*

1. $\mathrm{mdeg}(fg) = \mathrm{mdeg}(f) + \mathrm{mdeg}(g)$*,*

2. if $f + g \neq 0$, then $\mathrm{mdeg}(f+g) \leq \max\{\mathrm{mdeg}(f), \mathrm{mdeg}(g)\}$*.*

PROOF: I claim that $\mathrm{LM}(fg) = \mathrm{LM}(f)\cdot\mathrm{LM}(g) = X^{\mathrm{mdeg}(f)+\mathrm{mdeg}(g)}$. For sure fg contains a term with $X^{\mathrm{mdeg}(f)+\mathrm{mdeg}(g)}$. Thus it suffices to show that all other monomials appearing in fg have smaller exponents. Let X^α (resp. X^β) be a monomial appearing in f (resp. in g). Then $\alpha \preceq \mathrm{mdeg}(f)$ and $\beta \preceq \mathrm{mdeg}(g)$. We have

$$\alpha + \beta \preceq \mathrm{mdeg}(f) + \beta \preceq \mathrm{mdeg}(f) + \mathrm{mdeg}(g)\,.$$

Hence $X^{\alpha+\beta}$ has a smaller exponent than $X^{\mathrm{mdeg}(f)+\mathrm{mdeg}(g)}$.

The second statement is obvious. □

Since $k[X]$ is a PID, it is possible to use the division algorithm in order to find out whether a given polynomial $f \in k[X]$ belongs to an ideal or not. This can be decided according to the remainder. However $k[X_1, \ldots, X_n]$ is not a PID. Thus we will need a more general division algorithm. More precisely, given a polynomial $f \in k[X_1, \ldots, X_n]$ and an ordered s-tuple $(f_1, \ldots, f_s)$, $f_i \in k[X_1, \ldots, X_n]$, we would like to express f as follows:

$$f = a_1 f_1 + a_2 f_2 + \ldots + a_s f_s + r\,,$$

because if $r = 0$ then clearly $f \in \langle f_1, \ldots, f_s \rangle$.

The division algorithm in $k[X_1, \ldots, X_n]$ is a quite straightforward generalization of the division algorithm in $k[X]$. We will illustrate it first on an example.

Example 2.3.3 Let $f = X^2Y + XY^2 + Y^2$ and $f_1 = XY - 1$, $f_2 = Y^2 - 1$. I will use the lex order such that $X \succeq Y$. Then the division goes as follows:

a_1:	$X + Y$	
a_2:	1	r
$XY - 1$	$X^2Y + XY^2 + Y^2$	
$Y^2 - 1$	$X^2Y - X$	
	$XY^2 + X + Y^2$	
	$XY^2 - Y$	
	$X + Y^2 + Y$	
	$Y^2 + Y$	X
	$Y^2 - 1$	
	$Y + 1$	
	1	$X + Y$
	0	$X + Y + 1$

$$f = (X + Y)(XY - 1) + 1 \cdot (Y^2 - 1) + X + Y + 1\,.$$

The division depends on the order of the divisors f_i. Let us divide f by $(Y^2 - 1, XY - 1)$.

a_1:	$X + 1$	
a_2:	X	r
$Y^2 - 1$	$X^2Y + XY^2 + Y^2$	
$XY - 1$	$X^2Y - X$	
	$XY^2 + X + Y^2$	
	$XY^2 - X$	
	$2X + Y^2$	
	Y^2	$2X$
	$Y^2 - 1$	
	1	
	0	$2X + 1$

$$f = (X+1)(Y^2-1) + X(XY-1) + 2X + 1\,.$$

Theorem 2.3.4 *Let $\preceq$ be a term order and $F = (f_1, \ldots, f_s)$ be an 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*

$$f = a_1 f_1 + a_2 f_2 + \ldots + a_s f_s + r\,,$$

where $a_i, r \in k[X_1, \ldots, X_n]$ and either $r = 0$ or r is a k-linear combination 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. Furthermore, if $a_i f_i \neq 0$, then we have $\mathrm{mdeg}(a_i f_i) \preceq \mathrm{mdeg}(f)$.*

PROOF: A precise description of the division algorithm is shown in Algorithm 1. We will

Algorithm 1 Division in $k[X_1, \ldots, X_n]$

```
Input: f, f_1, ..., f_s and a term order ⪯
Output: a_1, ..., a_s, r
  a_1 := 0, ..., a_s := 0; r := 0
  p := f
  while p ≠ 0 do
      i := 1
      divisionoccured := false
      while i ≤ s and divisionoccured = false do
          if LT(f_i)|LT(p) then
              a_i := a_i + LT(p)/LT(f_i)
              p := p − (LT(p)/LT(f_i))f_i
              divisionoccured := true
          else
              i := i + 1
          end if
      end while
      if divisionoccured = false then
          r := r + LT(p)
          p := p − LT(p)
      end if
  end while
```

prove that in each step of the algorithm we have

$$f = a_1 f_1 + a_2 f_2 + \cdots + a_s f_s + p + r\,. \tag{2.1}$$

This is obvious for the initial values. In case when $\mathrm{LT}(f_i)|\mathrm{LT}(p)$ we get

$$a_i f_i + p = \left(a_i + \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)}\right) f_i + \left(p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)}\, f_i\right)\,.$$

Since all remaining values are unaffected, (2.1) remains valid. In case when none of $\mathrm{LT}(f_i)$ divides $\mathrm{LT}(p)$, we have

$$p + r = (p - \mathrm{LT}(p)) + (r + \mathrm{LT}(p))$$

showing that (2.1) is still preserved.

Observe that mdeg(p) decreases in each step of the algorithm. Thus the algorithm must eventually terminate since $\preceq$ is a well-ordering. Moreover r has the desired properties since LT(p) is added to r only if LT(p) is not divisible by any of LT(f_i). Finally, if $a_i f_i \neq 0$, then each term of a_i is of the form LT(p)/LT(f_i) for some value of p. Observe that mdeg(p) $\preceq$ mdeg(f) at each step of the algorithm. Thus mdeg($a_i f_i$) $\preceq$ mdeg(f) because

$$\mathrm{LT}(a_i f_i) = \mathrm{LT}(a_i)\mathrm{LT}(f_i) = \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)}\mathrm{LT}(f_i) = \mathrm{LT}(p)\,.$$

□

Let $f \in k[X_1, \dots, X_n]$ and $F = (f_1, \dots, f_s)$ an ordered s-tuple of polynomials in $k[X_1, \dots, X_n]$. If the remainder r of f on the division by F is zero, then clearly $f \in \langle f_1, \dots, f_s\rangle$. However, this is only sufficient conditions and not necessary as it is show in the following example.

Example 2.3.5 Let $f_1 = XY + 1$, $f_2 = Y^2 - 1 \in k[X, Y]$ with the lex order. Dividing $f = XY^2 - X$ by $F = (f_1, f_2)$, we get

$$XY^2 - X = Y \cdot (XY + 1) + 0 \cdot (Y^2 - 1) + (-X - Y)\,.$$

Dividing $f = XY^2 - X$ by $F = (f_2, f_1)$, we get

$$XY^2 - X = X \cdot (Y^2 - 1) + 0 \cdot (XY + 1) + 0\,.$$

Thus $f \in \langle f_1, f_2\rangle$ but the remainder in the first case is $-X - Y$.

2.4 Hilbert Basis Theorem

Definition 2.4.1 Let $I \subseteq k[X_1, \dots, X_n]$ be an ideal and $\preceq$ a term order. We define

$$\mathrm{LT}(I) = \{\mathrm{LT}(f) \mid f \in I \setminus \{0\}\}\,, \quad \mathrm{LM}(I) = \{\mathrm{LM}(g) \mid g \in I \setminus \{0\}\}\,,$$

where LT(f) and LM(f) are taken w.r.t. $\preceq$. The ideal generated by LT(I) (resp. LM(I)) is denoted $\langle\mathrm{LT}(I)\rangle$ (resp. $\langle\mathrm{LM}(I)\rangle$).

Observation 2.4.2 *Let $I \subseteq k[X_1, \dots, X_n]$ be an ideal. Then $\langle\mathrm{LT}(I)\rangle$ is a monomial ideal.*

PROOF: It can be easily seen that $\langle\mathrm{LT}(I)\rangle = \langle\mathrm{LM}(I)\rangle$ since LT(g) is just a multiple of LM(g) by a non-zero constant. □

Lemma 2.4.3 *The ideal $\langle\mathrm{LT}(I)\rangle = \langle\mathrm{LT}(g_1), \dots, \mathrm{LT}(g_s)\rangle$ for some $g_1, \dots, g_s \in I$.*

PROOF: By Corollary 2.2.6 we get $\langle\mathrm{LT}(I)\rangle = \langle\mathrm{LM}(I)\rangle = \langle\mathrm{LM}(g_1), \dots, \mathrm{LM}(g_s)\rangle$ for some $g_i \in I$. Again by the previous observation we have

$$\langle\mathrm{LM}(g_1), \dots, \mathrm{LM}(g_s)\rangle = \langle\mathrm{LT}(g_1), \dots, \mathrm{LT}(g_s)\rangle\,.$$

□

Theorem 2.4.4 (Hilbert Basis Theorem) *Every ideal $I \subseteq k[X_1, \ldots, X_n]$ is finitely generated.*

PROOF: Clearly, $I = \{0\}$ is finitely generated. Thus assume that $I \neq \{0\}$. By previous lemma there are $g_1, \ldots, g_s \in I$ such that $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$. I claim that $I = \langle g_1, \ldots, g_s \rangle$.

Clearly $\langle g_1, \ldots, g_s \rangle \subseteq I$. Let $f \in I$. By the division algorithm there are polynomials $a_1, \ldots, a_s$ and r such that

$$f = a_1 g_1 + \cdots + a_s g_s + r \,,$$

where every term of r is divisible by none of $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)$. Then $r = f - (a_1 g_1 + \cdots + a_s g_s)$, i.e. $r \in I$. If $r \neq 0$ then $\mathrm{LT}(r) \in \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$. Thus by Lemma 2.2.5 we have $\mathrm{LT}(g_i) | \mathrm{LT}(r)$ for some i (a contradiction with the fact that r is the remainder of f on division by $(g_1, \ldots, g_s)$). Consequently, $r = 0$ which means that $f \in \langle g_1, \ldots, g_s \rangle$. □

Corollary 2.4.5 *The polynomial ring $k[X_1, \ldots, X_n]$ is Noetherian.*

Corollary 2.4.6 *Let $S \subseteq k[X_1, \ldots, X_n]$. Then $\mathbf{V}(S) = \mathbf{V}(f_1, \ldots, f_s)$ for some $f_1, \ldots, f_s \in \langle S \rangle$.*

PROOF: We have $\mathbf{V}(S) = \mathbf{V}(\langle S \rangle) = \mathbf{V}(f_1, \ldots, f_s)$ since $\langle S \rangle$ is finitely generated by Hilbert Basis Theorem. □

2.5 Gröbner Bases

Definition 2.5.1 Fix a term order. A finite subset $G = \{g_1, \ldots, g_s\}$ of an ideal I is called a *Gröbner basis* if

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

Observe that we have seen in the proof of Hilbert Basis Theorem that for every ideal $I \neq \{0\}$ a Gröbner basis exists and generates I.

Proposition 2.5.2 *Let $I \subseteq k[X_1, \ldots, X_n]$ be an ideal, $G = \{g_1, \ldots, g_s\}$ a Gröbner basis of I w.r.t. a term order, and $f \in k[X_1, \ldots, X_n]$. There there is a unique $r \in k[X_1, \ldots, X_n]$ with the following two properties:*

1. *No term of r is divisible by any of $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)$.*

2. *There is $g \in I$ such that $f = g + r$.*

PROOF: The division algorithm gives $f = \sum a_i g_i + r$, where r satisfies the first property and $\sum a_i g_i \in I$. Thus r with the required properties exists.

Now, assume that we can express f as follows:

$$f = g_1 + r_1 = g_2 + r_2 \,,$$

where $g_1, g_2 \in I$ and r_1, r_2 have the required properties. Then $r_1 - r_2 \in I$ and no term is divisible by any of $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)$. This means that $r_1 - r_2 = 0$ otherwise $\mathrm{LT}(r_1 - r_2) \in \langle \mathrm{LT}(I) \rangle$

would be divisible by some $\mathrm{LT}(g_i)$ by Lemma 2.2.5. □

Observe that the division by a Gröbner basis $G = \{g_1, \ldots, g_s\}$ does not depend on the order of g_i's.

Corollary 2.5.3 *Gröbner bases solve the ideal membership problem. More precisely, let $I \subseteq k[X_1, \ldots, X_n]$ be an ideal, G a Gröbner basis of I, and $f \in k[X_1, \ldots, X_n]$. Then $f \in I$ iff the remainder of f after division by G is zero.*

PROOF: Let r be the remainder. We saw already that $r = 0$ implies $f \in I$. Conversely, assume that $f \in I$. Then by the division algorithm we can write $f = \sum a_i g_i + r$ where r satisfies the conditions from the previous proposition. At the same time we can write $f = f + 0$ where 0 satisfies the same conditions as well. By uniqueness we get $r = 0$. □

Definition 2.5.4 We will write $\overline{f}^G$ for the remainder of f on division by $G = (g_1, \ldots, g_s)$.

If we have a basis $\{g_1, \ldots, g_s\}$ (i.e. a generating set) of an ideal I, then it may happen that

$$\mathrm{LT}(I) \neq \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle .$$

Thus not each generating set for I is necessarily a Gröbner basis. To see this consider for example the ideal $\langle f_1, f_2 \rangle$ where $f_1 = X^3 - 2XY$ and $f_2 = X^2Y + X - 2Y^2$. Let us use the lex term order. Then

$$X(X^2Y + X - 2Y^2) - Y(X^3 - 2XY) = X^2 .$$

Thus $X^2 \in \langle f_1, f_2 \rangle$ and $X^2 = \mathrm{LT}(X^2) \in \langle \mathrm{LT}(I) \rangle$. However,

$$X^2 \notin \langle \mathrm{LT}(f_1), \mathrm{LT}(f_2) \rangle = \langle X^3, X^2Y \rangle .$$

This is caused by the fact that the leading terms in the combination producing X^2 cancel.

Let $\alpha, \beta \in \mathbb{N}^n$, and let $\gamma = \sup\{\alpha, \beta\}$, i.e. for each i we have $\pi_i(\gamma) = \max\{\pi_i(\alpha), \pi_i(\beta)\}$. Then we call X^γ the *least common multiple* of X^α and X^β. It is denoted by $\mathrm{LCM}(X^\alpha, X^\beta)$. Fix a term order $\preceq$. The corresponding strict order will be denoted by $\prec$.

Definition 2.5.5 Let $f, g \in k[X_1, \ldots, X_n]$ be non-zero polynomials and $X^\gamma = \mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g))$. Then the *S-polynomial* of f and g is the combination

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

Observe that the leading terms of $\frac{X^\gamma}{\mathrm{LT}(f)} f$ and $\frac{X^\gamma}{\mathrm{LT}(g)} g$ cancel in $S(f,g)$. Indeed, as we can write $f = \mathrm{LT}(f) + f'$ and $g = \mathrm{LT}(g) + g'$ for some $f', g' \in k[X_1, \ldots, X_n]$ such that $\mathrm{mdeg}(f') \prec \mathrm{mdeg}(f)$ and $\mathrm{mdeg}(g') \prec \mathrm{mdeg}(g)$, we get

$$S(f,g) = \frac{X^\gamma}{\mathrm{LT}(f)}(\mathrm{LT}(f) + f') - \frac{X^\gamma}{\mathrm{LT}(g)}(\mathrm{LT}(g) + g') = \frac{X^\gamma}{\mathrm{LT}(f)}\, f' - \frac{X^\gamma}{\mathrm{LT}(g)}\, g' .$$

Moreover, since $\mathrm{mdeg}(f') \prec \mathrm{mdeg}(f)$ and $\mathrm{mdeg}(g') \prec \mathrm{mdeg}(g)$, we have

$$\mathrm{mdeg}(f') + \gamma - \mathrm{mdeg}(f) \prec \gamma , \quad \mathrm{mdeg}(g') + \gamma - \mathrm{mdeg}(g) \prec \gamma .$$

Thus $\mathrm{mdeg}(S(f,g)) \prec \gamma$ because

$$\mathrm{mdeg}(S(f,g)) \preceq \max\{\mathrm{mdeg}(f') + \gamma - \mathrm{mdeg}(f), \mathrm{mdeg}(g') + \gamma - \mathrm{mdeg}(g)\}\,.$$

Example 2.5.6 Let $f = X^3Y^2 - X^2Y^3 + X$ and $g = 3X^4Y + Y^2$, and let $\preceq$ be the lex order. Then $\mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g)) = X^4Y^2$. Thus

$$S(f,g) = \frac{X^4Y^2}{X^3Y^2}\,f - \frac{X^4Y^2}{3X^4Y}\,g = X \cdot f - Y \cdot g = -X^3Y^3 - X^2 - \frac{1}{3}\,Y^3\,.$$

Lemma 2.5.7 *Suppose that $f = \sum_{i=1}^{s} c_i X^{\alpha(i)} g_i$, where $g_i \in k[X_1,\ldots,X_n]$, $c_i \in k \setminus \{0\}$, $\alpha(i) \in \mathbb{N}^n$, and $\alpha(i) + \mathrm{mdeg}(g_i) = \delta$. If $\mathrm{mdeg}(f) \prec \delta$, then there are $c_{jk} \in k$ such that*

$$f = \sum_{j,k} c_{jk} X^{\delta - \gamma_{jk}} S(g_j, g_k)\,,$$

where $X^{\gamma_{jk}} = \mathrm{LCM}(\mathrm{LM}(g_j), \mathrm{LM}(g_k))$. Furthermore, $\mathrm{mdeg}(X^{\delta-\gamma_{jk}} S(g_j,g_k)) \prec \delta$ for each j,k.

PROOF: Let $d_i = \mathrm{LC}(g_i)$. Thus $c_i d_i = \mathrm{LC}(c_i X^{\alpha(i)} g_i)$. Since $\mathrm{mdeg}(c_i X^{\alpha(i)} g_i) = \delta$ for each i and $\mathrm{mdeg}(f) \prec \delta$, we have $\sum_{i=1}^{s} c_i d_i = 0$.

Define $p_i = X^{\alpha(i)} g_i / d_i$ and consider the following telescoping sum:

$$f = \sum_{i=1}^{s} c_i X^{\alpha(i)} g_i = \sum_{i=1}^{s} c_i d_i p_i = c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) +$$
$$(c_1d_1 + c_2d_2 + c_3d_3)(p_3 - p_4) + \cdots + (c_1d_1 + \cdots + c_{s-1}d_{s-1})(p_{s-1} - p_s) + (c_1d_1 + \cdots + c_sd_s)p_s\,.$$

Since $\alpha(i) + \mathrm{mdeg}(g_i) = \delta$ (i.e. $\mathrm{mdeg}(g_i) \leq_\ell \delta$) for each i, we have for each pair j,k:

$$\gamma_{jk} = \sup\{\mathrm{mdeg}(g_j), \mathrm{mdeg}(g_k)\} \leq_\ell \delta\,.$$

Thus $X^{\delta-\gamma_{jk}}$ is a monomial and we have

$$X^{\delta-\gamma_{jk}} S(g_j,g_k) = X^{\delta-\gamma_{jk}} \left(\frac{X^{\gamma_{jk}}}{\mathrm{LT}(g_j)}\, g_j - \frac{X^{\gamma_{jk}}}{\mathrm{LT}(g_k)}\, g_k \right) =$$
$$= \frac{X^{\delta}}{d_j \mathrm{LM}(g_j)}\, g_j - \frac{X^{\delta}}{d_k \mathrm{LM}(g_k)}\, g_k = \frac{X^{\alpha(j)} g_j}{d_j} - \frac{X^{\alpha(k)} g_k}{d_k} = p_j - p_k\,.$$

Using this and $\sum_{i=1}^{s} c_i d_i = 0$, the telescoping sum can be rewritten as follows:

$$f = c_1 d_1 X^{\delta-\gamma_{12}} S(g_1,g_2) + (c_1d_1 + c_2d_2) X^{\delta-\gamma_{23}} S(g_2,g_3) +$$
$$+ \cdots + (c_1d_1 + \cdots + c_{s-1}d_{s-1}) X^{\delta-\gamma_{s-1,s}} S(g_{s-1}, g_s)\,,$$

which is a sum of the desired form.

Finally, since $X^{\delta-\gamma_{jk}} S(g_j,g_k) = p_j - p_k$, it suffices to show that $\mathrm{mdeg}(p_j - p_k) \prec \delta$. But this is obvious because $\mathrm{mdeg}(p_j) = \mathrm{mdeg}(p_k) = \delta$ and $\mathrm{LC}(p_j) = \mathrm{LC}(p_k) = 1$. □

Theorem 2.5.8 *Let $I \subseteq k[X_1,\ldots,X_n]$ be an ideal. Then a basis $G = \{g_1,\ldots,g_s\}$ for I is a Gröbner basis for I iff for all pairs $i \neq j$, the remainder of $S(g_i,g_j)$ on division by G is zero.*

PROOF: ($\Rightarrow$): Since $S(g_i, g_j) \in I$, the remainder must be zero because G is a Gröbner basis. ($\Leftarrow$): Let $f \in I$ be a non-zero polynomial. We have to show that $\mathrm{LT}(f) \in \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)\rangle$. There are some $h_i \in k[X_1, \ldots, X_n]$ such that

$$f = \sum_{i=1}^{s} h_i g_i \,.$$

By Lemma 2.3.2 we have $\mathrm{mdeg}(f) \preceq \max\{\mathrm{mdeg}(h_i g_i) \mid 1 \le i \le s\}$. If we show that we can find the polynomials h_i in such a way that $\mathrm{mdeg}(f) = \mathrm{mdeg}(h_i g_i)$ for some i, then we are done since $\mathrm{LT}(g_i)|\mathrm{LT}(f)$ in that case.

Consider all possible ways that f can be expressed in the form $\sum_{i=1}^{s} h_i g_i$. Given such expression, let $m(i) = \mathrm{mdeg}(h_i g_i)$ and $\delta = \max\{m(1), \ldots, m(s)\}$. Thus $\mathrm{mdeg}(f) \preceq \delta$. For each such expression, we can get a possibly different δ. Since $\preceq$ is a well-ordering, we can choose such expression for which δ is minimal. For this expression we will prove that $\mathrm{mdeg}(f) = \delta$ which is what we want to show.

Suppose that $\mathrm{mdeg}(f) \prec \delta$. We can write f in the following form:

$$f = \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)\prec\delta} h_i g_i = \sum_{m(i)=\delta} \mathrm{LT}(h_i) g_i + \sum_{m(i)=\delta} (h_i - \mathrm{LT}(h_i)) g_i + \sum_{m(i)\prec\delta} h_i g_i \,.$$

Since monomials appearing in the second and the third summand have multidegree strictly less than δ, the first summand must also have multidegree strictly less than δ (we are assuming $\mathrm{mdeg}(f) \prec \delta$).

Let $\mathrm{LT}(h_i) = c_i X^{\alpha(i)}$. Then $\sum_{m(i)=\delta} \mathrm{LT}(h_i) g_i = \sum_{m(i)=\delta} c_i X^{\alpha(i)} g_i$. Thus we can use Lemma 2.5.7 and express it by means of S-polynomials:

$$\sum_{m(i)=\delta} \mathrm{LT}(h_i) g_i = \sum_{j,k} c_{jk} X^{\delta-\gamma_{jk}} S(g_j, g_k) \,.$$

Now we can use the assumption that the remainder of $S(g_j, g_k)$ after division by G is zero, i.e.

$$S(g_j, g_k) = \sum_{i=1}^{s} a_{ijk} g_i \,,$$

for some $a_{ijk} \in k[X_1, \ldots, X_n]$. Moreover, we know that $\mathrm{mdeg}(a_{ijk} g_i) \preceq \mathrm{mdeg}(S(g_j, g_k))$ (see Theorem 2.3.4). Then

$$X^{\delta-\gamma_{jk}} S(g_j, g_k) = \sum_{i=1}^{s} b_{ijk} g_i \,,$$

where $b_{ijk} = X^{\delta-\gamma_{jk}} a_{ijk}$ and by Lemma 2.5.7

$$\mathrm{mdeg}(b_{ijk} g_i) \preceq \mathrm{mdeg}(X^{\delta-\gamma_{jk}} S(g_j, g_k)) \prec \delta \,.$$

Thus we obtain

$$\sum_{m(i)=\delta} \mathrm{LT}(h_i) g_i = \sum_{j,k} c_{jk} X^{\delta-\gamma_{jk}} S(g_j, g_k) =$$

$$= \sum_{j,k} c_{jk} \left(\sum_{i=1}^{s} b_{ijk} g_i \right) = \sum_{i} \left(\sum_{j,k} c_{jk} b_{ijk} \right) g_i = \sum_{i=1}^{s} h'_i g_i \,,$$

and $\mathrm{mdeg}(h'_i g_i) \prec \delta$ since c_{jk} are constants. Finally,

$$f = \sum_{i=1}^{s} h'_i g_i + \sum_{m(i)=\delta} (h_i - \mathrm{LT}(h_i))g_i + \sum_{m(i)\prec\delta} h_i g_i \,.$$

Thus we have expressed f as a polynomial combination of g_i's where the multidegree of all summands is strictly less than δ. But this is a contradiction with the minimality of δ. Hence $\mathrm{mdeg}(f) = \delta$ and we are done. $\square$

Example 2.5.9 Prove that $G = \{Y - X^2, Z - X^3\}$ is a Gröbner basis for $I = \langle Y - X^2, Z - X^3\rangle$ w.r.t. the lex order given by $Y \succ Z \succ X$. We have

$$S(Y - X^2, Z - X^3) = \frac{YZ}{Y}(Y - X^2) - \frac{YZ}{Z}(Z - X^3) = YX^3 - ZX^2 \,.$$

By the division algorithm we get

$$YX^3 - ZX^2 = X^3(Y - X^2) + (-X^2)(Z - X^3) + 0 \,.$$

Thus $\overline{S(Y - X^2, Z - X^3)}^G = 0$ showing that G is a Gröbner basis.

Show that G is not Gröbner basis w.r.t. the lex order given by $X \succ Y \succ Z$. We have

$$S(-X^3 + Z, -X^2 + Y) = \frac{X^3}{X^3}(-X^3 + Z) - \frac{X^3}{X^2}(-X^2 + Y) = -XY + Z \,.$$

The division gets

$$-XY + Z = 0 \cdot (-X^3 + Z) + 0 \cdot (-X^2 + Y) - XY + Z \,.$$

Thus $\overline{S(-X^3 + Z, -X^2 + Y)}^G = -XY + Z$, i.e. G is not a Gröbner basis.

2.6 Buchberger's Algorithm

Now we will present how to construct a Gröbner basis from a generating set for an ideal.

Theorem 2.6.1 *Let $I = \langle f_1, \ldots, f_t\rangle \subseteq k[X_1, \ldots, X_n]$ be a non-zero ideal and $\preceq$ a term order. Then a Gröbner basis for I w.r.t. $\preceq$ can be constructed by Algorithm 2.*

PROOF: First, observe that $G \subseteq I$ in each step of the algorithm. This is clearly valid in the initial step. Then if $p, q \in I$, then $S(p, q) \in I$ and $\overline{S(p,q)}^G \in I$. The algorithm terminates when $\overline{S(p,q)}^G = 0$ for each pair p, q, i.e. G is a Gröbner basis.

Secondly, if the algorithm does not terminate, then G is expanded at least by one polynomial S, i.e. $G' \subsetneq G$. We will show that also $\langle \mathrm{LT}(G')\rangle \subsetneq \langle \mathrm{LT}(G)\rangle$. To see this consider $r \in G \setminus G'$. Since r is a remainder on division by G', $\mathrm{LT}(r)$ is not divisible by any of the leading terms of elements from G'. Thus $\mathrm{LT}(r) \notin \langle \mathrm{LT}(G')\rangle$ but $\mathrm{LT}(r) \in \langle \mathrm{LT}(G)\rangle$.

Finally, since the ideals $\langle \mathrm{LT}(G')\rangle$ form an ascending chain and $k[X_1, \ldots, X_n]$ is Noetherian, the chain must become constant, i.e. $G = G'$ at some step and the algorithm terminates. $\square$

Algorithm 2 Buchberger's Algorithm

Input: $F = \{f_1, \ldots, f_t\}$ and a term order $\preceq$

Output: a Gröbner basis $G = \{g_1, \ldots, g_s\}$ for $\langle F \rangle$ w.r.t. $\preceq$ such that $F \subseteq G$

```
G := F
repeat
    G' := G
    for each {p, q} ⊆ G', p ≠ q do
        S := \overline{S(p, q)}^{G'}
        if S ≠ 0 then
            G := G ∪ {S}
        end if
    end for
until G = G'
```

Example 2.6.2 Find a Gröbner basis of $\langle f_1, f_2 \rangle$ w.r.t. the lex order given by $X \succ Y$, where $f_1 = X^2$ and $f_2 = XY + Y^2$.

Let $F = (f_1, f_2)$. We have

$$S(f_1, f_2) = YX^2 - X(XY + Y^2) = -XY^2 = 0 \cdot X^2 + (-Y)(XY + Y^2) + Y^3\,,$$

$$\overline{S(f_1, f_2)}^F = Y^3\,.$$

Expand F by $f_3 = Y^3$. Then

$$S(f_1, f_2) = f_3\,, \qquad \overline{S(f_1, f_2)}^F = 0\,,$$
$$S(f_1, f_3) = Y^3X^2 - X^2Y^3 = 0\,, \qquad \overline{S(f_1, f_3)}^F = 0\,,$$
$$S(f_2, f_3) = Y^2(XY + Y^2) - XY^3 = Y^4 = Y \cdot f_3\,, \qquad \overline{S(f_2, f_3)}^F = 0\,.$$

Thus $G = \{X^2, XY + 2Y^2, Y^3\}$ is a Gröbner basis for $\langle f_1, f_2 \rangle$.

Lemma 2.6.3 *Let G be a Gröbner basis for a non-zero ideal I. If $p \in G$ satisfies $\mathrm{LT}(p) \in \langle \mathrm{LT}(G \setminus \{p\}) \rangle$, then $G \setminus \{p\}$ is a Gröbner basis for I as well.*

PROOF: We know that $\langle \mathrm{LT}(G) \rangle = \langle \mathrm{LT}(I) \rangle$. If $\mathrm{LT}(p) \in \langle \mathrm{LT}(G \setminus \{p\}) \rangle$, then $\langle \mathrm{LT}(G \setminus \{p\}) \rangle = \langle \mathrm{LT}(G) \rangle$. Thus by definition $G \setminus \{p\}$ is a Gröbner basis. □

Definition 2.6.4 A *minimal* Gröbner basis for a non-zero ideal I is a Gröbner basis G for I such that for all $p \in G$ we have

1. $\mathrm{LC}(p) = 1$,
2. $\mathrm{LT}(p) \notin \langle \mathrm{LT}(G \setminus \{p\}) \rangle$.

Lemma 2.6.5 *Let G, G' be two minimal Gröbner bases for an ideal $I \subseteq k[X_1, \ldots, X_n]$ w.r.t. a term order $\preceq$. Then $\mathrm{LT}(G) = \mathrm{LT}(G')$. Moreover, G and G' have the same number of elements.*

PROOF: Since G, G' are Gröbner basis for I, we have $\langle \mathrm{LT}(G)\rangle = \langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(G')\rangle$. If G is a minimal Gröbner basis for I, then $\mathrm{LT}(G)$ is a minimal basis for $\langle \mathrm{LT}(G)\rangle$ (i.e. it satisfies the conditions from Definition 2.6.4). Let $\mathrm{LT}(g) \in \mathrm{LT}(G)$ for some $g \in G$. Then $\mathrm{LT}(g')|\mathrm{LT}(g)$ for some $g' \in G'$. Further, $\mathrm{LT}(g'')|\mathrm{LT}(g')$ for some $g'' \in G$. Thus $\mathrm{LT}(g'')|\mathrm{LT}(g)$ showing that $\mathrm{LT}(g'') = \mathrm{LT}(g)$ since $\mathrm{LT}(G)$ is minimal. Consequently, $\mathrm{LT}(g)|\mathrm{LT}(g')$. But this means that $\mathrm{LT}(g)$ and $\mathrm{LT}(g')$ may differ only by a unit. Since $\mathrm{LC}(g) = \mathrm{LC}(g') = 1$, they must be equal. Thus $\mathrm{LT}(G) \subseteq \mathrm{LT}(G')$. The second inclusion is proved analogously.

I claim that $|G| = |\mathrm{LT}(G)|$. If there would be more elements in G, then there would have to be $g, g' \in G$ such that $\mathrm{LT}(g) = \mathrm{LT}(g')$ but this is not possible because G is minimal. Since $\mathrm{LT}(G)$ and $\mathrm{LT}(G')$ have the same number of elements, we are done. □

Example 2.6.6 Let $G(a) = \{g_1(a), g_2, g_3\}$ where $g_1(a) = X^2 + aXY$, $g_2 = XY$, and $g_3 = Y^2 - X$. Then for any $a \in k$, $G(a)$ is a minimal Gröbner basis for $\langle G(0)\rangle$ w.r.t. the grlex order.

First, observe that $g_1(a) = g_1(0) + a \cdot g_2 \in \langle G(0)\rangle$ for each $a \in k$. Conversely, $g_1(0) = g_1(a) - a \cdot g_2 \in \langle G(a)\rangle$ for each $a \in k$. Thus $\langle G(a)\rangle = \langle G(0)\rangle$. We have

$$S(g_1, g_2) = Y(X^2 + aXY) - X(XY) = aXY^2 = aY \cdot g_2\,, \qquad \overline{S(g_1, g_2)}^{G(0)} = 0\,,$$
$$S(g_1, g_3) = Y^2(X^2 + aXY) - X^2(Y^2 - X) = aXY^3 + X^3\,, \qquad \overline{S(g_1, g_3)}^{G(0)} = 0\,,$$
$$S(g_2, g_3) = Y(XY) - X(Y^2 - X) = X^2\,, \qquad \overline{S(g_2, g_3)}^{G(0)} = 0\,.$$

Thus $G(a)$ is a Gröbner basis for $\langle G(0)\rangle$. The minimality is obvious.

Definition 2.6.7 A *reduced* Gröbner basis for a non-zero ideal I is a Gröbner basis G for I such that for all $p \in G$ we have

1. $\mathrm{LC}(p) = 1$,
2. no monomial of p lies in $\langle \mathrm{LT}(G \setminus \{p\})\rangle$.

Observe that the Gröbner basis $G(a)$ from Example 2.6.6 is reduced iff $a = 0$.

Proposition 2.6.8 *Let I be a non-zero ideal. Then, for a given term order, I has a unique reduced Gröbner basis.*

PROOF: Let G be a minimal Gröbner basis for I. We say that g is reduced for G provided that no monomial of g is in $\langle \mathrm{LT}(G \setminus \{g\})\rangle$. Observe that if g is reduced for G, then g is reduced for any other minimal Gröbner basis G' for I such that $\mathrm{LT}(G') = \mathrm{LT}(G)$ since the definition of reduced involves only the leading terms.

If G is not reduced then there is $g \in G$ containing a monomial divisible by some element of $\mathrm{LT}(G \setminus \{g\})$. Let $g' = \overline{g}^{G\setminus\{g\}}$ and $G' = (G \setminus \{g\}) \cup \{g'\}$. I claim that G' is minimal Gröbner basis for I. Since G is minimal, $\mathrm{LT}(g)$ is not divisible by any of $\mathrm{LT}(G \setminus \{g\})$. Thus $\mathrm{LT}(g)$ must be the leading term of the remainder g', i.e. $\mathrm{LT}(g) = \mathrm{LT}(g')$. Thus $\mathrm{LT}(G') = \mathrm{LT}(G)$. Consequently, $\langle \mathrm{LT}(G')\rangle = \langle \mathrm{LT}(G)\rangle = \langle \mathrm{LT}(I)\rangle$ showing that G' is a Gröbner basis for I. Moreover, it is clearly minimal. In this way we can make all elements of G reduced without changing the set of leading terms $\mathrm{LT}(G)$.

Finally, we prove the uniqueness. Suppose that G, G' are reduced Gröbner basis for I. Since G and G' are minimal, we have $\mathrm{LT}(G) = \mathrm{LT}(G')$ by Lemma 2.6.5. Thus, given $g \in G$, there is $g' \in G'$ such that $\mathrm{LT}(g) = \mathrm{LT}(g')$. If we can show $g = g'$, then $G = G'$ and we are done.

Consider $g - g' \in I$. We have $\overline{g - g'}^{G} = 0$. Since $\mathrm{LT}(g) = \mathrm{LT}(g')$, the leading terms in $g - g'$ cancel and the remaining terms are divisible by none of $\mathrm{LT}(G) = \mathrm{LT}(G')$ since G and G' are reduced. This shows $\overline{g - g'}^{G} = g - g'$ and then $g - g' = 0$ follows. □

2.7 Elimination

Definition 2.7.1 Let $I \subseteq k[X_1, \ldots, X_n]$ be an ideal. The r-th *elimination ideal* $I_r \subseteq k[X_{r+1}, \ldots, X_n]$ is an ideal defined by $I_r = I \cap k[X_{r+1}, \ldots, X_n]$.

Observe that I_r is really an ideal of $k[X_{k+1}, \ldots, X_n]$.

Theorem 2.7.2 *Let $I \subseteq k[X_1, \ldots, X_n]$ be an ideal, and let G be a Gröbner basis for I w.r.t. the lex order given by $X_1 \succ \cdots \succ X_n$. Then for every $0 \le r \le n$ the set $G_r = G \cap k[X_{r+1}, \ldots, X_n]$ is a Gröbner basis for the r-th elimination ideal I_r w.r.t. the lex order given by $X_{r+1} \succ \cdots \succ X_n$.*

PROOF: Let $G = \{g_1, \ldots, g_s\}$. Relabeling, if necessary, we may assume that $G_r = \{g_1, \ldots, g_m\}$. We prove that G_r is a basis for I_r. Clearly $G_r \subseteq I_r$. Let $f \in I_r$. Since G is a Gröbner basis, we have $\overline{f}^{G} = 0$ and by the division algorithm

$$f = a_1 g_1 + \cdots + a_m g_m + a_{m+1} g_{m+1} + \cdots + a_s g_s \,,$$

where $\mathrm{mdeg}(a_i g_i) \preceq \mathrm{mdeg}(f)$. Thus $a_i g_i \in k[X_{r+1}, \ldots, X_n]$ because $\preceq$ is the lex order. Consequently, $a_{m+1} = \cdots = a_s = 0$, i.e. $f \in \langle G_r \rangle$.

Now we prove that G_r is a Gröbner basis for I_r. Clearly, $\langle \mathrm{LT}(G_r) \rangle \subseteq \langle \mathrm{LT}(I_r) \rangle$. Let $\mathrm{LT}(f) \in \mathrm{LT}(I_r) \subseteq k[X_{r+1}, \ldots, X_n]$. Then $\mathrm{LT}(g) | \mathrm{LT}(f)$ for some $g \in G$. This is equivalent to $\mathrm{mdeg}(g) \preceq \mathrm{mdeg}(f)$. Thus $g \in G_r = G \cap k[X_{r+1}, \ldots, X_n]$ showing that $\mathrm{LT}(f) \in \langle \mathrm{LT}(G_r) \rangle$. □

In fact if one wants to obtain a basis for I_r, it suffices to consider a so-called r-elimination term order, i.e. a term order where any monomial containing at least one of the first r variables is greater than all monomials in $k[X_{r+1}, \ldots, X_n]$. This is useful especially in application since the computation of Gröbner basis w.r.t. lex order might be more difficult. For instance one can consider the term order $\preceq_r$ defined as follows:

$$\alpha \preceq_r \beta \quad \text{if} \quad \sum_{i=1}^{r} \alpha_i < \sum_{i=1}^{r} \beta_i \qquad \text{or} \qquad \sum_{i=1}^{r} \alpha_i = \sum_{i=1}^{r} \beta_i \text{ and } \alpha \preceq_{grevlex} \beta \,.$$

This is in fact a weighted term order for $w = (1, \ldots, 1, 0, \ldots, 0)$, where the right-most 1 is at the r-th position, refined by the grevlex term order.

Example 2.7.3 Consider the following system of polynomial equations:

$$\begin{aligned} X^2 + Y + Z - 1 &= 0 \\ X + Y^2 + Z - 1 &= 0 \\ X + Y + Z^2 - 1 &= 0 \end{aligned}$$

and the ideal I generated by the left-hand sides. Then the reduced Gröbner basis for I w.r.t. the lex order given by $X \succ Y \succ Z$ contains the following polynomials:

$$\begin{aligned} g_1 &= Y^2 - Y - Z^2 + Z \\ g_2 &= YZ^2 + 1/2Z^4 - 1/2Z^2 \\ g_3 &= Z^6 - 4Z^4 + 4Z^3 - Z^2 \\ g_4 &= X + Y + Z^2 - 1 \end{aligned}$$

Then $I_2 = I \cap k[Z] = \langle g_3 \rangle$ and $I_1 = I \cap k[Y, Z] = \langle g_1, g_2, g_3 \rangle$.

We can even solve the system of equations since $g_3 = Z^2(Z-1)^2(Z^2+2Z-1)$. Thus the only possible values of Z's are $0, 1$ and $-1 \pm \sqrt{2}$. Substituting these values to g_1, g_2 we can determine possible values of Y's and finally we obtain the corresponding values for X's. In this way we can find the following five solutions:

$$\begin{aligned} &(1,0,0),\ (0,1,0),\ (0,0,1), \\ &(-1+\sqrt{2}, -1+\sqrt{2}, -1+\sqrt{2}), \\ &(-1-\sqrt{2}, -1-\sqrt{2}, -1-\sqrt{2}). \end{aligned}$$

Chapter 3

Affine varieties

3.1 Hilbert's Nullstellensatz

Theorem 3.1.1 (The Weak Nullstellensatz) *Let k be an algebraically closed field and $I \subseteq k[X_1, \dots, X_n]$ a proper ideal (i.e. $I \neq k[X_1, \dots, X_n]$). Then $\mathbf{V}(I) \neq \emptyset$.*

Corollary 3.1.2 *Let k be an algebraically closed field and $I \subseteq k[X_1, \dots, X_n]$ an ideal. Then $\mathbf{V}(I) = \emptyset$ iff $1 \in I$.*

PROOF: If $1 \in I$, then $\mathbf{V}(I) = \emptyset$ since 1 never vanish. Conversely, if $1 \notin I$, I is a proper ideal. Thus $\mathbf{V}(I) \neq \emptyset$ by the Weak Nullstellensatz. □

The assumption that k is algebraically closed is necessary. Consider for example an ideal $I = \langle X^2 + 1 \rangle \subseteq \mathbb{R}$. The ideal I is proper and $\mathbf{V}(I) = \emptyset$.

Definition 3.1.3 Let $I \subseteq k[X_1, \dots, X_n]$ be an ideal. The *radical* of I is the set

$$\sqrt{I} = \{f \mid (\exists m \in \mathbb{N})(f^m \in I)\}.$$

An ideal $I \subseteq k[X_1, \dots, X_n]$ is called *radical* if $I = \sqrt{I}$.

Lemma 3.1.4 *The radical $\sqrt{I}$ is a radical ideal containing I.*

PROOF: Clearly $0 \in \sqrt{I}$ because $0^1 = 0 \in I$. Let $f, g \in \sqrt{I}$ and $h \in k[X_1, \dots, X_n]$. Then there are $m, r \in \mathbb{N}$ such that $f^m \in I$ and $g^r \in I$. Thus $(fh)^m = f^m h^m \in I$, i.e. $fh \in \sqrt{I}$. In the binomial expansion of $(f+g)^{m+r-1}$ every term has a factor $f^i g^j$ with $i + j = m + r - 1$. Since either $i \geq m$ or $j \geq r$, either $f^i \in I$ or $g^j \in I$, whence $f^i g^j \in I$. Thus $(f+g)^{m+r-1} \in I$, i.e. $f + g \in \sqrt{I}$.

For each $f \in I$ we have $f^1 \in I$, hence $f \in \sqrt{I}$ (i.e. $I \subseteq \sqrt{I}$). Finally, we have to show that $\sqrt{\sqrt{I}} = \sqrt{I}$. Clearly, $\sqrt{I} \subseteq \sqrt{\sqrt{I}}$. Assume that $f \in \sqrt{\sqrt{I}}$, i.e. there is $m \in \mathbb{N}$ such that $f^m \in \sqrt{I}$. Thus there is $r \in \mathbb{N}$ such that $(f^m)^r \in I$. Consequently, $f^{mr} \in I$, i.e. $f \in \sqrt{I}$. □

Theorem 3.1.5 (The Strong Nullstellensatz) *Let k be an algebraically closed field. If I is an ideal in $k[X_1, \dots, X_n]$, then*

$$\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}.$$

PROOF: To show the inclusion $\sqrt{I} \subseteq \mathbf{I}(\mathbf{V}(I))$, assume that $f \in \sqrt{I}$ such that $f^m \in I$. Then $f^m(a_1, \dots, a_n) = 0$ for each $(a_1, \dots, a_n) \in \mathbf{V}(I)$. Thus we also have $f(a_1, \dots, a_n) = 0$ for each $(a_1, \dots, a_n) \in \mathbf{V}(I)$, i.e. $f \in \mathbf{I}(\mathbf{V}(I))$.

To prove the other inclusion, assume that $I \neq \langle 0 \rangle$ (for $I = \langle 0 \rangle$ the claim is trivial). Let $f \in \mathbf{I}(\mathbf{V}(I))$ and $f \neq 0$. We may suppose by Hilbert Basis Theorem that $I = \langle f_1, \dots, f_s \rangle$. Consider an ideal $I' \subseteq k[X_1, \dots, X_n, Y]$ defined by

$$I' = \langle f_1, \dots, f_s, 1 - Y \cdot f \rangle .$$

For every point $(a_1, \dots, a_{n+1}) \in \mathbf{V}(I')$ we have $a_{n+1} f(a_1, \dots, a_n) = 1$ and $f_i(a_1, \dots, a_n) = 0$ for $i = 1, \dots, s$. But then $(a_1, \dots, a_n) \in \mathbf{V}(I)$ and $f(a_1, \dots, a_n) \neq 0$ contradicting the choice of f. Consequently, $\mathbf{V}(I') = \emptyset$ and the Weak Nullstellensatz yields $1 \in I'$.

Hence there are polynomials $h, h_1, \dots, h_n \in k[X_1, \dots, X_n, Y]$ such that

$$1 = \sum_{i=1}^{s} h_i f_i + h(1 - Y \cdot f) .$$

In the fraction field $k(X_1, \dots, X_n, Y)$ we may substitute $1/f$ for Y and we get

$$1 = \sum_{i=1}^{s} h_i(X_1, \dots, X_n, 1/f) f_i .$$

Each $h_i(X_1, \dots, X_n, 1/f)$ is a fraction of polynomials where the denominator is f^m for some $m \in \mathbb{N}$. Then for suitably large $m \in \mathbb{N}$ all $h_i' = f^m h_i(X_1, \dots, X_n, 1/f) \in k[X_1, \dots, X_n]$. Thus multiplying both sides by f^m, we obtain $f^m = \sum_{i=1}^{s} h_i' f_i$, i.e. $f \in \sqrt{I}$. □

Now, let us discuss several consequences of the Strong Nullstellensatz. The first one tells us how to recognize whether a polynomial belong to a radical ideal.

Proposition 3.1.6 *Let k be an arbitrary field and $I = \langle f_1, \dots, f_s \rangle \subseteq k[X_1, \dots, X_n]$ be an ideal. Then $f \in \sqrt{I}$ iff $1 \in \langle f_1, \dots, f_s, 1 - Yf \rangle \subseteq k[X_1, \dots, X_n, Y]$.*

PROOF: We have seen in the proof of the Strong Nullstellensatz that $1 \in \langle f_1, \dots, f_s, 1 - Yf \rangle$ implies $f \in \sqrt{I}$. Conversely, let $f \in \sqrt{I}$, i.e. $f^m \in I \subseteq \langle f_1, \dots, f_s, 1 - Yf \rangle$ for some $m \in \mathbb{N}$. Thus

$$1 = Y^m f^m + (1 - Y^m f^m) = Y^m f^m + (1 - Yf)(1 + Yf + \dots + Y^{m-1} f^{m-1}) ,$$

showing that $1 \in \langle f_1, \dots, f_s, 1 - Yf \rangle$. □

The second consequence concerns the correspondence between affine varieties and ideals.

Theorem 3.1.7 *Let k be an arbitrary field. The maps*

$$\left\{ \begin{array}{c} \textit{affine varieties} \\ \textit{in } k^n \end{array} \right\} \begin{array}{c} \xrightarrow{\mathbf{I}} \\ \xleftarrow[\mathbf{V}]{} \end{array} \left\{ \begin{array}{c} \textit{ideals in} \\ k[X_1, \dots, X_n] \end{array} \right\} .$$

are inclusion-reversing and $\mathbf{V}(\mathbf{I}(V)) = V$ for any variety $V \subseteq k^n$ (i.e. $\mathbf{I}$ is always one-to-one).

In addition, if k is algebraically closed, and if we restrict to radical ideals, then the maps

$$\left\{\begin{array}{c}\textit{affine varieties}\\ \textit{in } k^n\end{array}\right\} \begin{array}{c}\xrightarrow{\mathbf{I}}\\ \xleftarrow{\mathbf{V}}\end{array} \left\{\begin{array}{c}\textit{radical ideals in}\\ k[X_1,\dots,X_n]\end{array}\right\}.$$

are inclusion-reversing bijections which are inverses of each other.

PROOF: We know already that $\mathbf{I}$ and $\mathbf{V}$ are inclusion-reversing (see Observation 1.7.6 and 1.7.8). We will show that $\mathbf{V}(\mathbf{I}(V)) = V$. By Hilbert Basis Theorem we may assume that $V = \mathbf{V}(f_1,\dots,f_s)$. Let $a \in V$. Then every $f \in \mathbf{I}(V)$ vanishes on a. Thus $a \in \mathbf{V}(\mathbf{I}(V))$. Conversely, $f_1,\dots,f_s \in \mathbf{I}(V)$, and thus $\langle f_1,\dots,f_s\rangle \subseteq \mathbf{I}(V)$. Since $\mathbf{V}$ is inclusion-reversing, we get $\mathbf{V}(\mathbf{I}(V)) \subseteq \mathbf{V}(\langle f_1,\dots,f_s\rangle) = V$.

In addition, if k is algebraically closed, then by the Strong Nullstellensatz we have $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$. Thus if we restrict the mappings only on radical ideals, then $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I} = I$ and we are done. □

It follows from the latter theorem that if we have a system of polynomial equations $f_1 = \cdots = f_s$ whose solution set is $\mathbf{V}(\langle f_1,\dots,f_s\rangle)$, then $\mathbf{V}(\langle f_1,\dots,f_s\rangle) = \mathbf{V}(\sqrt{\langle f_1,\dots,f_s\rangle})$. Indeed, we have

$$\mathbf{V}(\langle f_1,\dots,f_s\rangle) = \mathbf{V}(\mathbf{I}(\mathbf{V}(\langle f_1,\dots,f_s\rangle))) = \mathbf{V}(\sqrt{\langle f_1,\dots,f_s\rangle})\,.$$

Finally, we will prove that there is one-to-one correspondence between points of affine n-space and maximal ideals in $k[X_1,\dots,X_n]$.

Definition 3.1.8 Let R be a ring. A proper ideal $I \subseteq R$ is called *maximal* if for any ideal $J \supseteq I$ we have $J = I$ or $J = k[X_1,\dots,X_n]$.

Lemma 3.1.9 *Let R be a ring. Every maximal ideal $I \subseteq R$ is prime.*

PROOF: Assume that $I \subseteq R$ is a maximal ideal which is not prime. Then there are polynomials f, g such that $fg \in I$, $f \notin I$ and $g \notin I$. Since I is maximal, we have $\langle I \cup \{f\}\rangle = R$. Thus $1 = cf + h$ for some $c \in R$ and $h \in I$. If we multiply by g, we obtain $g = cfg + hg \in I$ which is a contradiction with the fact that $g \notin I$. □

Lemma 3.1.10 *Let $I \subseteq k[X_1,\dots,X_n]$ be a prime ideal. Then I is radical.*

PROOF: We have to show that if $f^m \in I$ for $m > 1$, then also $f \in I$. But it is easy to see since $f^m = f \cdot f^{m-1}$. □

Theorem 3.1.11 *If k is algebraically closed field, then every maximal ideal in $k[X_1,\dots,X_n]$ is of the form $\langle X_1 - a_1,\dots,X_n - a_n\rangle$ for some $a_1,\dots,a_n \in k$.*

PROOF: Let $I \subseteq k[X_1,\dots,X_n]$ be a maximal ideal. By the Weak Nullstellensatz we have $\mathbf{V}(I) \neq \emptyset$, i.e. there is a point $(a_1,\dots,a_n) \in \mathbf{V}(I)$. Since $\mathbf{I}$ is inclusion-reversing, we get $\mathbf{I}(\mathbf{V}(I)) \subseteq \mathbf{I}(\{(a_1,\dots,a_n)\})$. By the Strong Nullstellensatz $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$. As I is maximal, I is prime hence radical, i.e. $I = \sqrt{I}$. Thus we have $I \subseteq \mathbf{I}(\{(a_1,\dots,a_n)\})$. Since $\mathbf{I}(\{(a_1,\dots,a_n)\}) \neq k[X_1,\dots,X_n]$, we get $I = \mathbf{I}(\{(a_1,\dots,a_n)\})$ by maximality of I.

Thus it suffices to show that $\mathbf{I}(\{(a_1,\ldots,a_n)\}) = \langle X_1 - a_1, \ldots, X_n - a_n\rangle$. Clearly,

$$\langle X_1 - a_1, \ldots, X_n - a_n\rangle \subseteq \mathbf{I}(\{(a_1,\ldots,a_n)\}) .$$

Assume that there is $f \in \mathbf{I}(\{(a_1,\ldots,a_n)\})$ such that $f \notin \langle X_1 - a_1, \ldots, X_n - a_n\rangle$. Then by the division algorithm we have $f = g_1(X_1 - a_1) + \cdots + g_n(X_n - a_n) + r$ for some $r \in k$. Moreover $r \neq 0$ because $f \notin \langle X_1 - a_1, \ldots, X_n - a_n\rangle$. Since $r \in \mathbf{I}(\{(a_1,\ldots,a_n)\})$, we get $1 = (1/r)r \in \mathbf{I}(\{(a_1,\ldots,a_n)\})$ (a contradiction). □

3.2 Operations with ideals

Definition 3.2.1 Let I, J be ideals in $k[X_1,\ldots,X_n]$. Then we define the following operations:

1. The *sum* of I and J is the set

$$I + J = \{f + g \mid f \in I,\ g \in J\} .$$

2. The *product* of I and J is the ideal

$$IJ = \langle\{fg \mid f \in I,\ g \in J\}\rangle .$$

Observe that if $I = \langle f_1,\ldots,f_s\rangle$ and $J = \langle g_1,\ldots,g_r\rangle$, then $IJ = \langle\{f_ig_j \mid 1 \le i \le s,\ 1 \le j \le r\}\rangle$.

Lemma 3.2.2 *Let I, J be ideals in $k[X_1,\ldots,X_n]$. Then $I+J$ is the smallest ideal containing I and J. Moreover, if $I = \langle f_1,\ldots,f_s\rangle$ and $J = \langle g_1,\ldots,g_r\rangle$, then $I+J = \langle f_1,\ldots,f_s,g_1,\ldots,g_r\rangle$.*

PROOF: Clearly $0 = 0 + 0 \in I + J$. Let $f, g \in I + J$ and $h \in k[X_1,\ldots,X_n]$. Then there are $f_1, g_1 \in I$ and $f_2, g_2 \in J$ such that $f = f_1 + f_2$ and $g = g_1 + g_2$. Thus $f + g = (f_1 + g_1) + (f_2 + g_2) \in I + J$. Further, $hf = h(f_1 + f_2) = hf_1 + hf_2 \in I + J$.

The fact that $I + J$ is the smallest ideal containing I and J is evident since $I + J$ contains both and each ideal containing both must be closed under addition. Thus also the last statement is obvious. □

Theorem 3.2.3 *If I, J are ideals in $k[X_1,\ldots,X_n]$, then $\mathbf{V}(I + J) = \mathbf{V}(I) \cap \mathbf{V}(J)$ and $\mathbf{V}(IJ) = \mathbf{V}(I \cap J) = \mathbf{V}(I) \cup \mathbf{V}(J)$.*

PROOF: We saw in Lemma 1.7.9 that $\mathbf{V}(I) \cap \mathbf{V}(J) = \mathbf{V}(I \cup J)$. But $\mathbf{V}(I \cup J) = \mathbf{V}(\langle I \cup J\rangle) = \mathbf{V}(I + J)$ since $I + J$ is the smallest ideal containing I and J.

The fact that $\mathbf{V}(IJ) = \mathbf{V}(I) \cup \mathbf{V}(J)$ also follows from Lemma 1.7.9. Note that $IJ \subseteq I \cap J$. Thus $\mathbf{V}(I \cap J) \subseteq \mathbf{V}(IJ)$. Finally, let $x \in \mathbf{V}(I) \cup \mathbf{V}(J)$. Then $x \in \mathbf{V}(I)$ or $x \in \mathbf{V}(J)$, say that $x \in \mathbf{V}(I)$. Thus $f(x) = 0$ for all $f \in I \supseteq I \cap J$, i.e. $x \in \mathbf{V}(I \cap J)$ showing that $\mathbf{V}(I) \cup \mathbf{V}(J) \subseteq \mathbf{V}(I \cap J)$. Summing up, we have

$$\mathbf{V}(I) \cup \mathbf{V}(J) \subseteq \mathbf{V}(I \cap J) \subseteq \mathbf{V}(IJ) = \mathbf{V}(I) \cup \mathbf{V}(J) .$$

□

So far we have seen operations with ideals corresponding to the set-theoretic union and intersection. In the rest of the section we will concentrate on the set-theoretic difference. Of course affine varieties are not closed under this difference (consider e.g. a line and remove a single point). Thus we will try to find the smallest affine variety containing the difference.

Definition 3.2.4 The *Zariski closure* of $S \subseteq k^n$, denoted $\overline{S}$, is the smallest affine variety $\mathbf{V}(\mathbf{I}(S))$. It is in fact the closure in Zariski topology.

Proposition 3.2.5 *Let $S \subseteq k^n$. Then $\mathbf{V}(\mathbf{I}(S))$ is the smallest affine variety containing S.*

PROOF: If $W \supseteq S$ is an affine variety containing S, then $\mathbf{I}(W) \subseteq \mathbf{I}(S)$. Thus $W = \mathbf{V}(\mathbf{I}(W)) = \mathbf{V}(\mathbf{I}(S))$. □

Definition 3.2.6 Let I, J be ideals in $k[X_1, \ldots, X_n]$, then the *ideal quotient* (or *colon ideal*) of I and J is the set

$$I : J = \{f \in k[X_1, \ldots, X_n] \mid (\forall g \in J)(fg \in I)\}\,.$$

Proposition 3.2.7 *If I, J be ideals in $k[X_1, \ldots, X_n]$, then $I : J$ is an ideal containing I.*

PROOF: Note that $I : J \supseteq I$ because for each $f \in I$ we have $fg \in I$ for all $g \in J$. Thus $0 \in I : J$. Let $f_1, f_2 \in I : J$ and $h \in k[X_1, \ldots, X_n]$. Then for all $g \in J$ we have $f_1 g \in I$ and $f_2 g \in I$. Consequently, $(f_1 + f_2)g = f_1 g + f_2 g \in I$ for all $g \in J$. Finally, $f_1 hg \in I$ for all $g \in J$. Thus also $f_1 h \in I : J$. □

Theorem 3.2.8 *Let I, J be ideals in $k[X_1, \ldots, X_n]$. Then $\mathbf{V}(I : J) \supseteq \overline{\mathbf{V}(I) \setminus \mathbf{V}(J)}$. If, in addition, k is algebraically closed and I is radical, then*

$$\mathbf{V}(I : J) = \overline{\mathbf{V}(I) \setminus \mathbf{V}(J)}\,.$$

PROOF: First, we will show that $I : J \subseteq \mathbf{I}(\mathbf{V}(I) \setminus \mathbf{V}(J))$. Let $f \in I : J$ and $x \in \mathbf{V}(I) \setminus \mathbf{V}(J)$. Then $fg \in I$ for all $g \in J$. Since $x \in \mathbf{V}(I)$, we have $f(x)g(x) = 0$ for all $g \in J$. As $x \notin \mathbf{V}(J)$, there is $g \in J$ such that $g(x) \neq 0$. Hence $f(x) = 0$ showing that $I : J \subseteq \mathbf{I}(\mathbf{V}(I) \setminus \mathbf{V}(J))$. Thus $\mathbf{V}(I : J) \supseteq \mathbf{V}(\mathbf{I}(\mathbf{V}(I) \setminus \mathbf{V}(J))) = \overline{\mathbf{V}(I) \setminus \mathbf{V}(J)}$.

Now assume that k is algebraically closed and $I = \sqrt{I}$. Let $x \in \mathbf{V}(I : J)$, i.e. if $fg \in I$ for all $g \in J$, then $f(x) = 0$. Suppose that $f \in \mathbf{I}(\mathbf{V}(I) \setminus \mathbf{V}(J))$. Then for each $g \in J$ the polynomial fg vanishes on $\mathbf{V}(I)$ because f vanishes on $\mathbf{V}(I) \setminus \mathbf{V}(J)$ and g on $\mathbf{V}(J)$. Thus $fg \in \mathbf{I}(\mathbf{V}(I)) = \sqrt{I} = I$ for each $g \in J$. It follows that $f(x) = 0$, i.e. $x \in \mathbf{V}(\mathbf{I}(\mathbf{V}(I) \setminus \mathbf{V}(J)))$. □

Example 3.2.9

$$\begin{aligned}
\langle XZ, YZ\rangle : \langle Z\rangle &= \{f \in k[X,Y,Z] \mid (\forall h \in k[X,Y,Z])(hZ \cdot f \in \langle XZ, YZ\rangle)\} \\
&= \{f \in k[X,Y,Z] \mid Z \cdot f \in \langle XZ, YZ\rangle\} \\
&= \{f \in k[X,Y,Z] \mid Z \cdot f = aXZ + bYZ\} \\
&= \{f \in k[X,Y,Z] \mid f = aX + bY\} \\
&= \langle X, Y\rangle\,.
\end{aligned}$$

3.3 Irreducible varieties

Definition 3.3.1 An affine variety $V \subseteq k^n$ is *irreducible* if whenever $V = V_1 \cup V_2$ for some affine varieties V_1, V_2, then either $V_1 = V$ or $V_2 = V$.

Proposition 3.3.2 *Let $V \subseteq k^n$ be an affine variety. Then V is irreducible iff $\mathbf{I}(V)$ is a prime ideal.*

PROOF: ($\Rightarrow$): Let $fg \in \mathbf{I}(V)$. Set $V_1 = V \cap \mathbf{V}(f)$ and $V_2 = V \cap \mathbf{V}(g)$. The sets V_1, V_2 are affine varieties because affine varieties are closed under intersections. Then

$$V_1 \cup V_2 = (V \cap \mathbf{V}(f)) \cup (V \cap \mathbf{V}(g)) = V \cap (\mathbf{V}(f) \cup \mathbf{V}(g)) = V \cap \mathbf{V}(fg) = V\,.$$

The last equality follows from $\mathbf{V}(fg) \supseteq V$ because $\{fg\} \subseteq \mathbf{I}(V)$. Since V is irreducible, we have either $V = V_1$ or $V = V_2$, say the former holds. Then $V = V \cap \mathbf{V}(f) \subseteq \mathbf{V}(f)$. Thus f vanishes on V, i.e. $f \in \mathbf{I}(V)$ and $\mathbf{I}(V)$ is prime.

($\Leftarrow$): Let $V = V_1 \cup V_2$. Suppose that $V \neq V_1$. We have to show that $V_2 = V$. First, $V_2 \subseteq V$ and thus $\mathbf{I}(V) \subseteq \mathbf{I}(V_2)$. Second, since $V_1 \subsetneq V$, we have $\mathbf{I}(V) \subsetneq \mathbf{I}(V_1)$ (otherwise $V = \mathbf{V}(\mathbf{I}(V)) = \mathbf{V}(\mathbf{I}(V_1)) = V_1$). Take $f \in \mathbf{I}(V_1) \setminus \mathbf{I}(V)$ and any $g \in \mathbf{I}(V_2)$. Then fg vanishes on $V = V_1 \cup V_2$, i.e. $fg \in \mathbf{I}(V)$. Since $\mathbf{I}(V)$ is prime, g belongs to $\mathbf{I}(V)$ because $f \notin \mathbf{I}(V)$. Thus $\mathbf{I}(V) = \mathbf{I}(V_2)$. Since $\mathbf{I}$ is one-to-one, we get $V = V_2$. □

Proposition 3.3.3 *Let $V_1 \supseteq V_2 \supseteq V_3 \supseteq \cdots$ be a descending sequence of affine varieties. Then there is $n \in \mathbb{N}$ such that $V_n = V_{n+1} = \cdots$.*

PROOF: Applying the mapping $\mathbf{I}$, we get an ascending sequence of ideals:

$$\mathbf{I}(V_1) \subseteq \mathbf{I}(V_2) \subseteq \mathbf{I}(V_3) \subseteq \cdots\,.$$

Since $k[X_1, \ldots, X_n]$ is Noetherian, there is $n \in \mathbb{N}$ such that $\mathbf{I}(V_n) = \mathbf{I}(V_{n+1}) = \cdots$. But this means that $V_n = V_{n+1} = \cdots$ because $\mathbf{V}(\mathbf{I}(V_i)) = V_i$. □

Definition 3.3.4 Let $V \subseteq k^n$ be an affine variety. A decomposition $V = V_1 \cup \cdots \cup V_m$, where each V_i is irreducible, is called a *minimal decomposition* if $V_i \not\subseteq V_j$ for $i \neq j$.

Theorem 3.3.5 *Let $V \subseteq k^n$ be an affine variety. Then V has a minimal decomposition $V = V_1 \cup \cdots \cup V_m$ unique up to order of V_i's.*

PROOF: The existence of the minimal decomposition $V = V_1 \cup \cdots \cup V_m$ follows from Proposition 3.3.3.

To show that the decomposition is unique, assume that $V = V_1' \cup \cdots V_s'$ is another minimal decomposition. Then for each i we have

$$V_i = V_i \cap V = V_i \cap (V_1' \cup \cdots V_s') = (V_i \cap V_1') \cup \cdots \cup (V_i \cap V_s')\,.$$

Since V_i is irreducible, we have $V_i = V_i \cap V_j'$ for some j, i.e. $V_i \subseteq V_j'$. Applying the same argument also for V_j' (using V_i's to decompose V), there is k such that $V_j' \subseteq V_k$. Since the decomposition into V_i's is minimal, we get $V_i = V_j'$. Thus all V_i's must appear between $V_1', \ldots, V_s'$. A symmetric argument finishes the proof. □

Corollary 3.3.6 *Let k be an algebraically closed field. Then every radical ideal $I \subseteq k[X_1, \ldots, X_n]$ can be written uniquely as a finite intersection of prime ideals, $I = \bigcap_{i=1}^{s} P_i$, where $P_i \not\subseteq P_j$ for $i \neq j$.*

PROOF: First, observe that $\mathbf{I}(V_1 \cup V_2) = \mathbf{I}(V_1) \cap \mathbf{I}(V_2)$. Indeed, let $f \in k[X_1, \ldots, X_n]$. Then $f \in \mathbf{I}(V_1 \cup V_2)$ iff f vanishes on V_1 and V_2 iff $f \in \mathbf{I}(V_1)$ and $f \in \mathbf{I}(V_2)$. Thus we have

$$I = \sqrt{I} = \mathbf{I}(\mathbf{V}(I)) = \mathbf{I}(V_1 \cup \cdots \cup V_m) = \bigcap_{i=1}^{m} \mathbf{I}(V_i)\,,$$

where $\mathbf{V}(I) = V_1 \cup \cdots \cup V_m$ is the unique minimal decomposition. Since V_i's are irreducible, the ideals $\mathbf{I}(V_i)$ are prime. □

3.4 Varieties corresponding to principal ideals

Proposition 3.4.1 *Let $f \in k[X_1, \ldots, X_n]$ and $I = \langle f \rangle$. If $f = u f_1^{a_1} \cdots f_s^{a_s}$ is the unique factorization into irreducibles, then*

$$\sqrt{I} = \langle f_1 \cdots f_s \rangle\,.$$

PROOF: Let $N = \max\{a_1, \ldots, a_r\}$. Then

$$(f_1 \cdots f_s)^N = f_1^{N-a_1} \cdots f_s^{N-a_s} \cdot f\,.$$

Thus $(f_1 \cdots f_s)^N \in I$ and $f_1 \cdots f_s \in \sqrt{I}$.

Conversely, let $g \in \sqrt{I}$, i.e. $g^M \in I$ for some $M \in \mathbb{N}$. Thus there is a polynomial h such that $g^M = h \cdot f$. Consider the unique factorization of $g = v g_1^{b_1} \cdots g_r^{b_r}$ into irreducibles. Then

$$g^M = v^M g_1^{Mb_1} \cdots g_r^{Mb_r} = h \cdot u f_1^{a_1} \cdots f_s^{a_s}\,.$$

Since $k[X_1, \ldots, X_n]$ is a UFD, the irreducible polynomials on both sides must be the same up to units. Thus each f_i equals (up to a unit) to some g_j. Consequently, g is a polynomial multiple of $f_1 \cdots f_s$, i.e. $g \in \langle f_1 \cdots f_s \rangle$. □

Definition 3.4.2 Let $f \in k[X_1, \ldots, X_n]$. The *reduction* of f is the polynomial f_{red} such that $\langle f_{red} \rangle = \sqrt{\langle f \rangle}$. A polynomial f is called *reduced* (or *square-free*) if $f = f_{red}$.

Let $f = (X + Y^2)(X - Y)^2(Y - 3)^5$. Then $f_{red} = (X + Y^2)(X - Y)(Y - 3)$. Observe also that each irreducible polynomial is reduced.

Proposition 3.4.3 *Let $f \in \mathbb{C}[X_1, \ldots, X_n]$ and let $f = u f_1^{a_1} \cdots f_s^{a_s}$ be its decomposition into irreducible factors (u is a unit). Then*

$$\mathbf{V}(f) = \mathbf{V}(f_1) \cup \cdots \cup \mathbf{V}(f_s)$$

is the minimal decomposition into irreducible components.

PROOF: Let $a \in \mathbf{V}(f)$. Then $0 = f(a) = uf_1^{a_1}(a)\cdots f_s^{a_s}(a)$. Thus at least for one i we have $f_i(a) = 0$, i.e. $a \in \mathbf{V}(f_i)$. Consequently, $\mathbf{V}(f) \subseteq \mathbf{V}(f_1) \cup \cdots \cup \mathbf{V}(f_s)$. To see the second inclusion, note that $\langle f_1 \cdots f_s \rangle \subseteq \langle f_i \rangle$ for each i. Thus $\langle f_1 \cdots f_s \rangle \subseteq \bigcap_{i=1}^s \langle f_i \rangle$. Consequently,

$$\mathbf{I}(\mathbf{V}(f)) = \sqrt{\langle f \rangle} = \langle f_1 \cdots f_s \rangle \subseteq \bigcap_{i=1}^{s} \langle f_i \rangle = \bigcap_{i=1}^{s} \mathbf{I}(\mathbf{V}(f_i)) = \mathbf{I}(\bigcup_{i=1}^{s} \mathbf{V}(f_i)) .$$

Applying the mapping $\mathbf{V}$ to both sides, we get

$$\bigcup_{i=1}^{s} \mathbf{V}(f_i) \subseteq \mathbf{V}(f) ,$$

since $\mathbf{V}$ is inclusion-reversing and $\bigcup_{i=1}^s \mathbf{V}(f_i)$ is a variety because affine varieties are closed under finite unions.

Now we have to show that $\mathbf{V}(f_i)$ is irreducible, i.e. $\mathbf{I}(\mathbf{V}(f_i)) = \sqrt{\langle f_i \rangle} = \langle f_i \rangle$ is prime. Since f_i is irreducible, f_i is a prime element because $\mathbb{C}[X_1, \ldots, X_n]$ is a UFD. Thus $\langle f_i \rangle$ is a prime ideal. Finally, $\mathbf{V}(f_i) \not\subseteq \mathbf{V}(f_j)$ for $i \neq j$. Assume not. Then

$$\langle f_i \rangle = \mathbf{I}(\mathbf{V}(f_i)) \supseteq \mathbf{I}(\mathbf{V}(f_j)) = \langle f_j \rangle .$$

Thus $f_j | f_i$ which is not possible. □

3.5 Polynomial mapping on a variety

Definition 3.5.1 Let $V \subseteq k^m$ and $W \subseteq k^n$ be affine varieties. A function $\phi : V \to W$ is a *polynomial mapping* if there exist polynomials $f_1, \ldots, f_n \in k[X_1, \ldots, X_m]$ such that

$$\phi(a_1, \ldots, a_m) = (f_1(a_1, \ldots, a_m), \ldots, f_n(a_1, \ldots, a_m)) ,$$

for all $(a_1, \ldots, a_m) \in V$. We say that $(f_1, \ldots, f_n)$ *represents* ϕ.

Now we will be interested mainly in the case when $W = k$. Thus ϕ is represented by a single polynomial. Given a polynomial mapping $\phi : V \to k$, the polynomial which represents ϕ is usually not unique. Consider e.g. $V = \mathbf{V}(Y - X^2) \subseteq \mathbb{R}^2$. Then polynomial $f = X^3 + Y^3$ represents a polynomial mapping ϕ from V to $\mathbb{R}$. However, for any $h \in \mathbf{I}(V)$ the polynomial $g = X^3 + Y^3 + h(X, Y)$ represents the same polynomial mapping since for all $(a, b) \in V$ we have

$$\phi(a, b) = a^3 + b^3 = a^3 + b^3 + 0 = a^3 + b^3 + h(a, b) .$$

Proposition 3.5.2 *Let $V \subseteq k^m$ be an affine variety. Then $f, g \in k[X_1, \ldots, X_m]$ represent the same polynomial mapping $\phi : V \to k$ iff $f - g \in \mathbf{I}(V)$.*

PROOF: If $f - g \in \mathbf{I}(V)$, then for any point $a = (a_1, \ldots, a_m) \in V$, we have $f(a) - g(a) = 0$. Thus f, g represent the same polynomial mapping $\phi : V \to k$. Conversely, if f, g represent the same polynomial mapping $\phi : V \to k$, then at every point $a \in V$ we have $f(a) - g(a) = 0$. Thus $f - g \in \mathbf{I}(V)$. □

Definition 3.5.3 Let $V \subseteq k^n$ be an affine variety. We denote by $k[V]$ the set of all polynomial mappings from V to k.

The set $k[V]$ forms a ring under the point-wise operations, i.e. if $\phi, \psi \in k[V]$, then

$$\begin{aligned}(\phi + \psi)(a) &= \phi(a) + \psi(a)\\ (\phi \cdot \psi)(a) &= \phi(a) \cdot \psi(a)\,.\end{aligned}$$

Additive and multiplicative identity of $k[V]$ are represented respectively by constant polynomials 0 and 1.

Observe that if f represents $\phi \in k[V]$ and g represents $\psi \in k[V]$, then $f + g$ represents $\phi + \psi$. Indeed, for all $a \in V$ we have

$$(\phi + \psi)(a) = \phi(a) + \psi(a) = f(a) + g(a) = (f + g)(a)\,.$$

Similarly, $f \cdot g$ represents $\phi \cdot \psi$.

Theorem 3.5.4 *Let $V \subseteq k^n$ be an affine variety. Then the ring $k[V]$ is isomorphic to $k[X_1, \ldots, X_n]/\mathbf{I}(V)$.*

PROOF: Let us define a mapping $\Psi : k[X_1, \ldots, X_n]/\mathbf{I}(V)$ by $\Psi([f]) = \phi$ where $\phi : V \to k$ is the polynomial mapping represented by f. By Proposition 3.5.2 Ψ is a well-defined function since if $[f] = [f']$, then $f - f' \in \mathbf{I}(V)$, i.e. f, f' represent the same polynomial mapping. Since every polynomial mapping $\phi \in k[V]$ can be represented by a polynomial in $k[X_1, \ldots, X_n]$, Ψ is onto. To see that Ψ is injective, assume that $[f] \neq [g]$. Then $f - g \notin \mathbf{I}(V)$, i.e. they represent different polynomial mappings from $k[V]$. Thus $\Psi([f]) \neq \Psi([g])$.

Let $[f], [g] \in k[X_1, \ldots, X_n]/\mathbf{I}(V)$. Then $\Psi([f])$ and $\Psi([g])$ are represented by f and g respectively. Thus $\Psi([f]) + \Psi([g])$ is represented by $f + g$. Hence

$$\Psi([f] + [g]) = \Psi([f + g]) = \Psi([f]) + \Psi([g])\,.$$

Similarly, we have

$$\Psi([f] \cdot [g]) = \Psi([f \cdot g]) = \Psi([f]) \cdot \Psi([g])\,.$$

Finally, $\Psi([1])$ is the polynomial mapping in $k[V]$ which is represented by the constant polynomial 1, i.e. $\Psi([1])$ is the multiplicative identity in $k[V]$. □

Corollary 3.5.5 *Let $V \subseteq k^n$ be an affine variety. Then $k[V]$ is an integral domain iff V is irreducible. In addition, if k is algebraically closed, then $k[V]$ is a field iff $V = \{(a_1, \ldots, a_n)\}$. In fact, in this case $k[V]$ is isomorphic to k.*

PROOF: Since $k[X_1, \ldots, X_n]/\mathbf{I}(V)$ is an integral domain iff $\mathbf{I}(V)$ is a prime filter, the statement follows from the previous theorem. Assume that k is algebraically closed. Then $k[X_1, \ldots, X_n]/\mathbf{I}(V)$ is a field iff $\mathbf{I}(V)$ is a maximal filter iff $\mathbf{I}(V) = \langle X_1 - a_1, \ldots, X_n - a_n \rangle$ for some $(a_1, \ldots, a_n) \in k^n$. Concerning the last statement, it can be easily seen that $k[V]$, where $V = \{(a_1, \ldots, a_n)\}$, is isomorphic to k since each function in $k[V]$ can be represented by a constant polynomial. □

Observe that if $V = \mathbf{V}(I)$, then $k[V]$ need not be isomorphic to $k[X_1, \ldots, X_n]/I$. We proved this only for the case when $I = \mathbf{I}(V)$. To see this, consider an affine variety $V = \{(0,0)\} \subseteq \mathbb{C}^2$. Then $\mathbf{I}(V) = \langle X, Y \rangle$ and $\mathbb{C}[V] \cong \mathbb{C}[X,Y]/\mathbf{I}(V)$ is a field. However, if we take a different defining ideal for V, e.g. $I = \langle X^2, Y \rangle$, then $\mathbb{C}[X,Y]/I$ is not a field since $\langle X^2, Y \rangle$ is not a maximal ideal.

3.6 Zero-dimensional ideals

Lemma 3.6.1 *Fix a term order on $k[X_1, \ldots, X_n]$ and let $I \subseteq k[X_1, \ldots, X_n]$ be an ideal. Then every $f \in k[X_1, \ldots, X_n]$ is congruent w.r.t. I to a unique polynomial r which is a k-linear combination of the monomials in the complement of $\langle \mathrm{LT}(I) \rangle$.*

PROOF: Let G be a Gröbner basis for I w.r.t. the fixed term order and $f \in k[X_1, \ldots, X_n]$. Set $r = \overline{f}^G$. Then r is unique and it is a k-linear combination of monomials from the complement of $\langle \mathrm{LT}(I) \rangle$. Further, $f = q + r$ for some $q \in I$. Thus $f - r = q \in I$, i.e. $f \sim_I r$. □

Observe, that $k[X_1, \ldots, X_n]/I$ can be viewed also as a k-vector space since we can define the scalar multiplication by $c \cdot [f] = [c \cdot f]$ for $c \in k$. It can be easily checked that this definition satisfies all the axioms of a k-vector space. For instance

$$(c+d) \cdot [f] = [(c+d) \cdot f] = [cf + df] = [cf] + [df] = c \cdot [f] + d \cdot [f] \, .$$

Theorem 3.6.2 *Let $I \subseteq k[X_1, \ldots, X_n]$ be an ideal. Then $k[X_1, \ldots, X_n]/I$ is isomorphic as a k-vector space to $S = \mathrm{Span}(X^\alpha \mid X^\alpha \notin \langle \mathrm{LT}(I) \rangle)$.*

PROOF: By the previous lemma the mapping $\Phi([f]) = \overline{f}^G$ is a bijection. Indeed, let $[f], [g] \in k[X_1, \ldots, X_n]/I$. Then $r = \overline{f}^G \sim_I f$ and $r' = \overline{g}^G \sim_I g$. If $r = r'$, then $f \sim_I r = r' \sim_I g$, i.e. $[f] = [g]$. To see that Φ is onto, consider $r \in S$. Then $\overline{r}^G = r$ since any monomial in r is not divisible by any of $\mathrm{LT}(I)$. Thus $\Phi([r]) = r$.

Now, it suffices to check that Φ is a linear mapping. First, we will show that $\overline{f+g}^G = \overline{f}^G + \overline{g}^G$ and $\overline{c \cdot f}^G = c \cdot \overline{f}^G$. We have $f = q + \overline{f}^G$ and $g = h + \overline{g}^G$ for some $q, h \in I$. Thus $f + g = (q+h) + (\overline{f}^G + \overline{g}^G)$. Since none of the monomials in $\overline{f}^G + \overline{g}^G$ is divisible by any of $\mathrm{LT}(I)$, we get $\overline{f}^G + \overline{g}^G = \overline{f+g}^G$ by Proposition 2.5.2. Similarly, $c \cdot f = c \cdot q + c \cdot \overline{f}^G$, i.e. $\overline{c \cdot f}^G = c \cdot \overline{f}^G$. Hence we get

$$\Phi([f] + [g]) = \Phi([f+g]) = \overline{f+g}^G = \overline{f}^G + \overline{g}^G = \Phi([f]) + \Phi([g]) \, ,$$

$$\Phi(c \cdot [f]) = \Phi([c \cdot f]) = \overline{c \cdot f}^G = c \cdot \overline{f}^G = c \cdot \Phi([f]) \, .$$

□

Observe that $B = \{X^\alpha \mid X^\alpha \notin \langle \mathrm{LT}(I) \rangle\}$ is a basis for S. Thus, if B is finite, we have

$$\dim S = \dim k[X_1, \ldots, X_n]/I = |B| \, .$$

Theorem 3.6.3 *Let k be an algebraically closed field and $V = \mathbf{V}(I) \subseteq k^n$ an affine variety. Then V is finite iff $k[X_1, \ldots, X_n]/I$ is finite-dimensional.*

PROOF: ($\Leftarrow$): To show that V is finite, it suffices to prove that for each i there can be only finitely many distinct i-th components of the points of V. Fix i and consider the classes $[X_i^j] \in k[X_1, \ldots, X_n]/I$, where $j \in \mathbb{N}$. Since $k[X_1, \ldots, X_n]/I$ is finite-dimensional, $[X_i^j]$ must be linearly dependent. Thus for some $c_j \in k$ we have

$$[0] = \sum c_j [X_i^j] = \left[\sum c_j X_i^j\right] .$$

Thus $\sum c_j X_i^j \in I$. Since $\sum c_j X_i^j$ can have only finitely many roots in k, there are only finitely many distinct i-th components of the points of V.

($\Rightarrow$): For this it suffices to show that $\dim S$ is finite. If $V = \emptyset$, then by the Weak Nullstellensatz $I = k[X_1, \ldots, X_n]$. Thus $k[X_1, \ldots, X_n]/I$ is the trivial k-vector space. If V is nonempty, then for a fixed i, let a_j, $j = 1, \ldots, t$ be the distinct i-th components of the points of V. Let

$$f(X_i) = \prod_{j=1}^{t} (X_i - a_j) .$$

By construction f vanishes at every point of V, so $f \in \mathbf{I}(V) = \mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$. Thus there is $m \in \mathbb{N}$ such that $f^m \in I$. This means that $X_i^{tm} = \mathrm{LT}(f^m) \in \langle \mathrm{LT}(I) \rangle$.

Now we know that for each i there is $m_i \in \mathbb{N}$ such that $X_i^{m_i} \in \langle \mathrm{LT}(I) \rangle$. Thus any monomial $X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ such that $m_i \leq \alpha_i$ (for at least one i) must belong to $\langle \mathrm{LT}(I) \rangle$ as well. Consequently, the monomials in the complement of $\langle \mathrm{LT}(I) \rangle$ must have $\alpha_i \leq m_i - 1$ for all i. As a result, there can be at most $m_1 \cdots m_n$ many monomials in the complement showing that $\dim S$ is finite. □

Corollary 3.6.4 *Let k be an algebraically closed field and $V = \mathbf{V}(I) \subseteq k^n$ an affine variety. Then V is finite iff $I \cap k[X_i] \neq \langle 0 \rangle$ for each $i \in \{1, \ldots, n\}$.*

PROOF: The right-to-left direction is trivial. For the other observe that in the first part of previous proof we have constructed for arbitrary i a polynomial $\sum c_j X_i^j$ from $k[X_i]$ which belongs to I. □

Definition 3.6.5 Let $V_1, \ldots, V_t$ be k-vector spaces. The direct product $\prod_{i=1}^t V_i$ of $V_1, \ldots, V_t$ is the k-vector space defined on $V_1 \times \cdots \times V_t$ componentwise.

Lemma 3.6.6 (Chinese Remainder Theorem) *Let $I_1, \ldots, I_t \subseteq k[X_1, \ldots, X_n]$ be ideals. Set $I = \bigcap_{i=1}^t I_i$. Then we have the following:*

1. *The map $\Phi : k[X_1, \ldots, X_n]/I \to \prod_{i=1}^t k[X_1, \ldots, X_n]/I_i$ defined by*

$$\Phi([f]_I) = ([f]_{I_1}, \ldots, [f]_{I_t})$$

   is an injective linear mapping.

2. *If the ideals $I_1, \ldots, I_t$ are pairwise comaximal, i.e. $I_i + I_j = k[X_1, \ldots, X_n]$ for $i \neq j$, then Φ is an isomorphism of k-vector spaces.*

PROOF:

1. The mapping Φ is well-defined since if $[f]_I = [f']_I$, then $[f]_{I_i} = [f']_{I_i}$ for all i because $I \subseteq I_i$ for each i. Let $f, g \in k[X_1, \ldots, X_n]$ and $c \in k$. Then

$$\Phi([f]_I+[g]_I) = \Phi([f+g]_I) = ([f+g]_{I_1}, \ldots, [f+g]_{I_t}) = ([f]_{I_1}+[g]_{I_1}, \ldots, [f]_{I_t}+[g]_{I_t}) = \\ = ([f]_{I_1}, \ldots, [f]_{I_t}) + ([g]_{I_1}, \ldots, [g]_{I_t}) = \Phi([f]_I) + \Phi([g]_I)\,,$$

$$\Phi(c \cdot [f]_I) = \Phi([cf]_I) = ([cf]_{I_1}, \ldots, [cf]_{I_t}) = (c[f]_{I_1}, \ldots, c[f]_{I_t}) = \\ = c([f]_{I_1}, \ldots, [f]_{I_t}) = c \cdot \Phi([f]_I)\,.$$

Thus Φ is a linear mapping. To see that it is one-to-one, assume that $[f]_I \neq [g]_I$. Then $f - g \notin I = \bigcap_{i=1}^t I_i$, i.e. $f - g$ does not belong to at least one of I_i's, say to I_j. Hence $[f]_{I_j} \neq [g]_{I_j}$ showing that $\Phi([f]_I) \neq \Phi([g]_I)$.

2. Fix a number $i \in \{1, \ldots, t\}$ and let $J_i = \bigcap_{j \neq i} I_j$. Since I_i and I_j are comaximal for all $j \neq i$, there are elements $a_j \in I_i$ and $b_j \in I_j$ such that $a_j + b_j = 1$. Then $1 = \prod_{j \neq i}(a_j + b_j) \in I_i + \prod_{j \neq i} I_j \subseteq I_i + J_i$. Thus I_i and J_i are comaximal. Thus there are elements $p_i \in I_i$ and $q_i \in J_i$ such that $p_i + q_i = 1$. Let $([r_1]_{I_1}, \ldots, [r_t]_{I_t}) \in \prod_{i=1}^t k[X_1, \ldots, X_n]/I_i$. I claim that $\Phi([q_1 r_1 + \cdots + q_t r_t]_I) = ([r_1]_{I_1}, \ldots, [r_t]_{I_t})$. To prove this we have to show that for each i we have $[q_1 r_1 + \cdots + q_t r_t]_{I_i} = [r_i]_{I_i}$. Observe that for each $j \neq i$ we have $q_j \in J_j = \bigcap_{l \neq j} I_l \subseteq I_i$. Thus $\sum_{j \neq i} q_j r_j \in I_i$ showing that $[q_1 r_1 + \cdots + q_t r_t]_{I_i} = [q_i r_i]_{I_i}$. But $[q_i r_i]_{I_i} = [(1 - p_i) r_i]_{I_i} = [r_i]_{I_i}$.

$\square$

Theorem 3.6.7 *Let k be an algebraically closed field and $I = \langle f_1, \ldots, f_s \rangle \subseteq k[X_1, \ldots, X_n]$ such that $\mathbf{V}(I)$ is finite. Then*

$$|\mathbf{V}(I)| \leq \dim k[X_1, \ldots, X_n]/I\,.$$

If, in addition, I is radical, then

$$|\mathbf{V}(I)| = \dim k[X_1, \ldots, X_n]/I\,.$$

PROOF: Let $\mathbf{V}(I) = \{p_1, \ldots, p_t\}$. To each point $p_i = (a_1, \ldots, a_n) \in \mathbf{V}(I)$ we can assign the maximal ideal $M_i = \langle X_1 - a_1, \ldots, X_n - a_n \rangle$. Clearly, $I \subseteq M_i$ for each i. Indeed, let $f \in I$. Then $f(p_i) = 0$. Since M_i is maximal, hence radical, we have $M_i = \sqrt{M_i} = \mathbf{I}(\mathbf{V}(M_i)) = \mathbf{I}(\{p_i\})$, i.e. $f \in M_i$. Consequently, $I \subseteq \bigcap_{i=1}^t M_i$. Since $\langle \mathrm{LT}(I) \rangle \subseteq \langle \mathrm{LT}(\bigcap_{i=1}^t M_i) \rangle$, we get $\dim k[X_1, \ldots, X_n]/I \geq \dim k[X_1, \ldots, X_n]/\bigcap_{i=1}^t M_i$. It follows from Chinese Remainder Theorem that $k[X_1, \ldots, X_n]/\bigcap_{i=1}^t M_i \cong \prod_{i=1}^t k[X_1, \ldots, X_n]/M_i$. Further, $k[X_1, \ldots, X_n]/M_i$ is a field isomorphic to k (see Corollary 3.5.5), i.e. $\prod_{i=1}^t k[X_1, \ldots, X_n]/M_i \cong k^t$. Thus we have

$$t = \dim \prod_{i=1}^t k[X_1, \ldots, X_n]/M_i = \dim k[X_1, \ldots, X_n]/\bigcap_{i=1}^t M_i \leq \dim k[X_1, \ldots, X_n]/I\,.$$

Now assume that I is radical. We will prove that instead of inclusion $I \subseteq \bigcap_{i=1}^t M_i$ we have in fact equality $I = \bigcap_{i=1}^t M_i$. Let $f \in \bigcap_{i=1}^t M_i$. Then for each i we have $f(p_i) = 0$. Thus we get

$$f \in \mathbf{I}(p_1, \ldots, p_t) = \mathbf{I}(\mathbf{V}(I)) = \sqrt{I} = I\,.$$

The rest of the proof is a trivial modification of the previous method. □

Lemma 3.6.8 *Let k be a field containing $\mathbb{Q}$ and $f \in k[X]$ a non-constant polynomial. Then f is square-free iff $\gcd(f, f') = 1$. Moreover, $f_{red} = f/\gcd(f, f')$.*

PROOF: ($\Leftarrow$): We will prove it contra-positively. Assume that f is not square-free. Then we can write $f = f_1^2 f_2$ for some $f_1, f_2 \in k[X]$ such that f_1 is non-constant. The derivative of f is $f' = 2f_1 f_1' f_2 + f_1^2 f_2'$. Thus $f_1 | \gcd(f, f')$ showing that f_1 must be a constant polynomial (a contradiction).

($\Rightarrow$): Let $f = f_1 \cdots f_t$ be the decomposition into irreducible polynomials. Then

$$f' = \sum_{i=1}^{t} f_1 \cdots f_{i-1} \cdot f_i' \cdot f_{i+1} \cdots f_t = \sum_{i=1}^{t} g_i f_i' ,$$

where $g_i = f_1 \cdots f_{i-1} \cdot f_{i+1} \cdots f_t$. Since k contains $\mathbb{Q}$ and $f_i's$ are non-constant, we have $f_i' \neq 0$ for each i.[1]

Let $j \in \{1, \dots, t\}$. I claim that $\gcd(f_j, f') = 1$. We will prove that f_j cannot be the greatest common divisor of f_j and f'. Suppose that $f_j | f'$. Then we have

$$f' = a f_j = \sum_{i=1}^{t} g_i f_i' = \sum_{i \neq j} f_j h_i f_i' + g_j f_j' .$$

Thus

$$g_j f_j' = f_j \left(a - \sum_{i \neq j} h_i f_i' \right) .$$

Since g_j does not contain f_j, f_j' must be divisible by f_j but it is a contradiction with the fact that $f_j' \neq 0$ and $\deg f_j' < \deg f_j$.

Finally, we show that $\gcd(f, f') = 1$. Assume that some irreducible c divides f and f'. Since $f = f_1 \cdots f_t$, c is (up to units) either 1 or one of the irreducible factors. Suppose that $c = f_j$. Then $c | \gcd(f_j, f')$ but $\gcd(f_j, f') = 1$ which is a contradiction (i.e. c must be 1).

To prove the last statement observe that $\gcd(f, f') = f_1^{a_1 - 1} \cdots f_t^{a_t - 1}$ where $f = u f_1^{a_1} \cdots f_t^{a_t}$ is the factorization into irreducibles. Thus $f_{red} = f/\gcd(f, f') = u f_1 \cdots f_t$. □

Lemma 3.6.9 *Let I, J be ideals. Then $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.*

PROOF: Let $f \in \sqrt{I \cap J}$. Then $f^m \in I \cap J$ for some $m \in \mathbb{N}$. Thus $f \in \sqrt{I}$ and $f \in \sqrt{J}$. Conversely, let $f \in \sqrt{I} \cap \sqrt{J}$. Then there are $m, p \in \mathbb{N}$ such that $f^m \in I$ and $f^p \in J$. Thus $f^m f^p = f^{m+p} \in I \cap J$, i.e. $f \in \sqrt{I \cap J}$. □

Proposition 3.6.10 (Seidenberg's Lemma) *Let k be an algebraically closed field and let $I \subseteq k[X_1, \dots, X_n]$ be an ideal. If there exists a non-zero polynomials $g_i \in I \cap k[X_i]$ for each $i \in \{1, \dots, n\}$ such that $\gcd(g_i, g_i') = 1$, then I is radical.*

[1] If k is finite then this step does not work. Consider e.g. $f = X^3 - 2$ over the three-element field $\mathbb{Z}/\langle 3 \rangle$. Then $f' = 3X^2 = 0X^2 = 0$.

PROOF: By Lemma 3.6.8 the polynomials $g_1, \dots, g_n$ are square-free. We proceed by induction on n. For $n = 1$, the principal ideal $I \subseteq k[X_1]$ contains a square-free polynomial. Therefore it is generated by a square-free polynomial, i.e. it is a radical ideal.

Let $n > 1$. We write $g_1 = h_1 \cdots h_t$ with irreducible polynomials $h_1, \dots, h_t \in k[X_1]$. We claim that $I = \bigcap_{i=1}^t (I + \langle h_i \rangle)$. For every $f \in \bigcap_{i=1}^t (I + \langle h_i \rangle)$ there are $r_i \in I$ and $q_i \in k[X_1, \dots, X_n]$ such that $f = r_i + q_i h_i$, $i \in \{1, \dots, t\}$. Thus we have

$$f \cdot \prod_{j \neq i} h_j = (r_i + q_i h_i) \cdot \prod_{j \neq i} h_j = r_i \cdot \prod_{j \neq i} h_j + q_i g_1 \in I\,.$$

Since

$$\gcd(\prod_{j \neq 1} h_j, \prod_{j \neq 2} h_j, \dots, \prod_{j \neq t} h_j) = 1\,,$$

there are $p_1, \dots, p_t \in k[X_1]$ such that

$$p_1 \cdot \prod_{j \neq 1} h_j + p_2 \cdot \prod_{j \neq 2} h_j + \cdots + p_t \cdot \prod_{j \neq t} h_j = 1$$

(see Lemma 1.3.7 and note that $k[X_1]$ is a PID). Thus

$$f = p_1 \cdot f \cdot \prod_{j \neq 1} h_j + p_2 \cdot f \cdot \prod_{j \neq 2} h_j + \cdots + p_t \cdot f \cdot \prod_{j \neq t} h_j \in I\,,$$

which proves the claim.

Because of this claim and by Lemma 3.6.9 it is sufficient to show that $I + \langle h_i \rangle$ is radical for each $i = 1, \dots, t$. Thus we may assume that g_1 is irreducible. Then $g_1 = X_1 - a$ for some $a \in k$ since k is an algebraically closed field. Let us define the following ideal

$$J = \{f(a, X_2, \dots, X_n) \in k[X_2, \dots, X_n] \mid f \in I\}\,.$$

Observe that $f(X_1, X_2, \dots, X_n) \in I$ if, and only if, $f(a, X_2, \dots, X_n) \in J$. If f does not contain X_1 then it is clear. Assume that $f(a, X_2, \dots, X_n) \in J$ and f contains X_1. Then by division algorithm we can write $f = h_1(X_1 - a) + h_2$ where $h_2 \in k[X_2, \dots, X_n]$. If we substitute for X_1 the value a we get

$$f(a, X_2, \dots, X_n) = h_1(a - a) + h_2(X_2, \dots, X_n) = h_2(X_2, \dots, X_n)\,.$$

Hence $h_2 = f(a, X_2, \dots, X_n) \in J$. Since h_2 does not contain X_1, we have $h_2 \in I$. Thus $f \in I$.

Note that $g_2, \dots, g_n$ belongs to J and still satisfy $\gcd(g_i, g_i') = 1$ for $i \in \{2, \dots, n\}$. Thus by induction assumption $J \subseteq k[X_2, \dots, X_n]$ is a radical ideal. Let $f^m \in I$ for some $m \in \mathbb{N}$. Then $f(a, X_2, \dots, X_n)^m \in J$ and since J is radical we have $f(a, X_2, \dots, X_n) \in J$. Finally, by the above observation we get $f \in I$. □

Corollary 3.6.11 *Let k be an algebraically closed field. Then the following algorithm computes the radical of an ideal $I \subseteq k[X_1, \dots, X_n]$ such that $\mathbf{V}(I)$ is finite.*

1. *For $i = 1, \dots, n$ compute a generator $g_i \in k[X_i]$ of the elimination ideal $I \cap k[X_i]$.*
2. *Compute the reduction $(g_i)_{red}$ of g_i's and return the ideal $I + \langle (g_1)_{red}, \dots, (g_n)_{red} \rangle$.*

PROOF: By Corollary 3.6.4 the generators g_i exist. By Lemma 3.6.8 we can compute $(g_i)_{red}$ for each i. Since the ideal $J = I + \langle (g_1)_{red}, \ldots, (g_n)_{red} \rangle$ satisfies $I \subseteq J \subseteq \sqrt{I}$, we have $\sqrt{I} = \sqrt{J}$. Indeed, we have $\sqrt{I} \subseteq \sqrt{J}$ since the operation assigning to an ideal its radical is monotone w.r.t. inclusion and $\sqrt{I} \supseteq \sqrt{J}$ follows from $\sqrt{J} \subseteq \sqrt{\sqrt{I}} = \sqrt{I}$. Let $h_i = (g_i)_{red}$ for each i. By Lemma 3.6.8 the polynomials h_i satisfy $\gcd(h_i, h_i') = 1$. Thus by Seidenberg's Lemma yields the claim. □

3.7 Systems of polynomial equations

In this section, let k be an algebraically closed field.

Definition 3.7.1 Let $I \subseteq k[X_1, \ldots, X_n]$ be an ideal such that $\mathbf{V}(I)$ is finite and $i \in \{1, \ldots, n\}$. We say that I is *in normal X_i-position* if any two points $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in \mathbf{V}(I)$ satisfy $a_i \neq b_i$.

Lemma 3.7.2 *Let $I \subseteq k[X_1, \ldots, X_n]$ be an ideal such that $\mathbf{V}(I)$ is finite. Then there exists a tuple $(c_1, \ldots, c_{n-1}) \in k^{n-1}$ such that*

$$c_1 a_1 + \cdots + c_{n-1} a_{n-1} + a_n \neq c_1 b_1 + \cdots + c_{n-1} b_{n-1} + b_n$$

for all pairs of points $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in \mathbf{V}(I)$.

PROOF: Let $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in \mathbf{V}(I)$ be two distinct points in the variety given by I. In choosing the tuple $(c_1, \ldots, c_{n-1}) \in k^{n-1}$, we have to avoid the solutions of the linear equation

$$(a_1 - b_1)\xi_1 + \cdots + (a_{n-1} - b_{n-1})\xi_{n-1} = b_n - a_n \,.$$

Every such equation determines a hyperplane in k^{n-1}. Since there are only finitely many of them, we can choose a point $(c_1, \ldots, c_{n-1}) \in k^{n-1}$ which is not contained in any of these hyperplanes. □

Consequently, we can transform the ideal I into an ideal in normal X_n-position. More precisely, let

$$\mathbb{A} = \begin{pmatrix} 1 & 0 & \cdots & 0 & -c_1 \\ 0 & 1 & \cdots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -c_{n-1} \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

be the matrix of linear transformation assigning to an n-tuple $(X_1, \ldots, X_n)$ the n-tuple

$$(X_1, \ldots, X_n) \cdot \mathbb{A} = (X_1, \ldots, X_{n-1}, X_n - c_1 X_1 - \cdots - c_{n-1} X_{n-1}) \,.$$

The matrix $\mathbb{A}$ is clearly invertible and

$$\mathbb{A}^{-1} = \begin{pmatrix} 1 & 0 & \cdots & 0 & c_1 \\ 0 & 1 & \cdots & 0 & c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & c_{n-1} \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

We denote the n-tuple $(X_1, \ldots, X_n)$ by X. Let us define the set

$$J = \{f(X \cdot \mathbb{A}) \mid f \in I\}.$$

Observe that $f(X) \in J$ iff $f(X \cdot \mathbb{A}^{-1})$ is in I, Indeed, if $f(X) \in J$, then there is $g(X) \in I$ such that $g(X \cdot \mathbb{A}) = f(X)$. Thus $f(X \cdot \mathbb{A}^{-1}) = g((X \cdot \mathbb{A}^{-1}) \cdot \mathbb{A}) = g(X)$.

Now we can prove that J is an ideal. Zero polynomial is clearly in J. Let $f(X), g(X) \in J$ and $h(X) \in k[X_1, \ldots, X_n]$. Then $f(X \cdot \mathbb{A}^{-1}) \in I$ and $g(X \cdot \mathbb{A}^{-1}) \in I$. Thus

$$f(X \cdot \mathbb{A}^{-1}) + g(X \cdot \mathbb{A}^{-1}) \in I.$$

i.e.

$$f(X) + g(X) = f((X \cdot \mathbb{A}) \cdot \mathbb{A}^{-1}) + g((X \cdot \mathbb{A}) \cdot \mathbb{A}^{-1}) \in J$$

by definition of J. Similarly $f(X \cdot \mathbb{A}^{-1}) \cdot h(X \cdot \mathbb{A}^{-1}) \in I$. Thus

$$f(X) \cdot h(X) = f((X \cdot \mathbb{A}) \cdot \mathbb{A}^{-1}) \cdot h((X \cdot \mathbb{A}) \cdot \mathbb{A}^{-1}) \in J.$$

Moreover, there is a correspondence between points of $\mathbf{V}(I)$ and points of $\mathbf{V}(J)$. We have $(a_1, \ldots, a_n) \in \mathbf{V}(I)$ iff $(a_1, \ldots, a_n + c_1 a_1 + \cdots + c_{n-1} a_{n-1}) \in \mathbf{V}(J)$. Indeed, let $f(X) \in J$. Then $f(X \cdot \mathbb{A}^{-1}) \in I$, i.e.

$$f((a_1, \ldots, a_n) \cdot \mathbb{A}^{-1}) = f(a_1, \ldots, a_{n-1}, a_n + c_1 a_1 + \cdots + c_{n-1} a_{n-1}) = 0.$$

Since we chose f arbitrarily, $(a_1, \ldots, a_{n-1}, a_n + c_1 a_1 + \cdots + c_{n-1} a_{n-1}) \in \mathbf{V}(J)$. Conversely, if $f(X) \in I$, then $f(X \cdot \mathbb{A}) \in J$. Thus

$$0 = f((a_1, \ldots, a_{n-1}, a_n + c_1 a_1 + \cdots + c_{n-1} a_{n-1}) \cdot \mathbb{A}) = f(((a_1, \ldots, a_n) \cdot \mathbb{A}^{-1}) \cdot \mathbb{A}) = f(a_1, \ldots, a_n).$$

Finally, it can be easily seen that if $c_1, \ldots, c_{n-1}$ are chosen according to Lemma 3.7.2, then J is in normal X_n-position. Although Lemma 3.7.2 does not give us a deterministic algorithm how to find the numbers $c_1, \ldots, c_{n-1}$, we can still construct a probabilistic algorithm choosing $c_1, \ldots, c_{n-1}$ randomly and then checking whether J is in normal X_n-position. For that we need a criterion how to recognize whether an ideal in normal X_n-position. Before we formulate the promised criterion, we have to prove several technical statements.

Proposition 3.7.3 *Let R be a ring and $I \subseteq R$ an ideal. Then there is a one-to-one correspondence between set of ideals in R containing I and set of ideals in R/I. More precisely, let $J \supseteq I$ be an ideal in R and $\tilde{J}$ an ideal in R/I. Then the following mappings Φ and Ψ are inverses of each other:*

$$\begin{array}{rcl} J & \xrightarrow{\Phi} & \{[j]_I \in R/I \mid j \in J\} \\ \{j \in R \mid [j]_I \in \tilde{J}\} & \xleftarrow{\Psi} & \tilde{J} \end{array}$$

Moreover, Φ and Ψ preserve inclusions, i.e. $J_1 \subseteq J_2$ implies $\Phi(J_1) \subseteq \Phi(J_2)$ and similarly for Ψ. We also have $\Phi(R) = R/I$ and $\Psi(R/I) = R$.

PROOF: Let $J \supseteq I$ be an ideal in R. We have to check that $\Phi(J)$ is an ideal in R/I. Let $[a]_I, [b]_I \in \Phi(J)$ and $[c]_I \in R/I$. Then $a, b \in J$ and $[a]_I + [b]_I = [a+b]_I$. Since $a + b \in J$, we get $[a+b]_I \in \Phi(J)$. Analogously $[a]_I \cdot [c]_I = [a \cdot c]_I \in \Phi(J)$. Clearly, $[0]_I \in \Phi(J)$. Similarly, we can check for an ideal $\tilde{J}$ in R/I that $\Psi(\tilde{J})$ is an ideal in R containing I. Indeed, let $a \in I$. Then $a \in \Psi(\tilde{J})$ since $I = [0]_I \in \tilde{J}$.

Further, we have to show that $\Psi \circ \Phi$ is an identity on the set of ideals in R and $\Phi \circ \Psi$ an identity on the set of ideals in R/I. Let J be an ideal in R containing I. Then $j \in J$ iff $[j]_I \in \Phi(J)$ iff $j \in \Psi(\Phi(J))$. Similarly, let $\tilde{J}$ be an ideal in R/I. Then $[j]_I \in \tilde{J}$ iff $j \in \Psi(\tilde{J})$ iff $[j]_I \in \Phi(\Psi(\tilde{J}))$.

Finally, it can easily seen that Φ and Ψ are inclusion preserving and $\Phi(R) = R/I$, $\Psi(R/I) = R$. □

Observe that if J is a maximal ideal in R containing an ideal I, then $\Phi(J)$ is a maximal ideal in R/I. Similarly $\Psi(\tilde{J})$ is maximal for a maximal ideal $\tilde{J}$ in R/I.

Lemma 3.7.4 *Let R, S be rings and $\Phi : R \to S$ be a ring isomorphism and let $I \subseteq R$ be an ideal. Then $\Phi(I)$ is an ideal in S. Moreover, if I is maximal, then $\Phi(I)$ is maximal.*

PROOF: Recall that $\Phi(I) = \{b \in S \mid (\exists a \in R)(b = \Phi(a))\}$. Let $b_1, b_2 \in \Phi(I)$ and $c \in S$. Then there are $a_1, a_2 \in I$ such that $\Phi(a_1) = b_1$ and $\Phi(a_2) = b_2$. Thus

$$b_1 + b_2 = \Phi(a_1) + \Phi(a_2) = \Phi(a_1 + a_2)\,.$$

Since $a_1 + a_2 \in I$, we get $b_1 + b_2 \in \Phi(I)$. As Φ is an isomorphism, there is $c' \in R$ such that $\Phi(c') = c$. Consequently,

$$b_1 c = \Phi(a_1) \cdot \Phi(c') = \Phi(a_1 c')\,.$$

Thus $b_1 c \in \Phi(I)$. Finally, $0 \in \Phi(I)$ because $0 = \Phi(0)$.

Now assume that I is maximal. Let $J \supsetneq \Phi(I)$. Then using the inverse of Φ (which a ring isomorphism as well) we get $\Phi^{-1}(J) \supsetneq \Phi^{-1}(\Phi(I)) = I$. By maximality of I the ideal $\Phi^{-1}(J) = R$. But this means that $J = \Phi(R) = S$. □

Theorem 3.7.5 *Let $I \subseteq k[X_1, \ldots, X_n]$ be a radical ideal such that $\mathbf{V}(I)$ is finite and g_n the monic generator of $I \cap k[X_n]$. Then the following conditions are equivalent:*

1. *The ideal I is in normal X_n-position.*
2. $\deg(g_n) = \dim k[X_1, \ldots, X_n]/I$.
3. *The mapping $\Phi : k[X_n]/\langle g_n \rangle \to k[X_1, \ldots, X_n]/I$ defined by*

$$\Phi([f]_{\langle g_n \rangle}) = [f]_I\,,$$

is a ring isomorphism, i.e. the rings $k[X_n]/\langle g_n \rangle$ and $k[X_1, \ldots, X_n]/I$ are isomorphic.

PROOF: First, I claim that the mapping $\Phi : k[X_n]/\langle g_n \rangle \to k[X_1, \ldots, X_n]/I$ defined by

$$\Phi([f]_{\langle g_n \rangle}) = [f]_I\,,$$

is always an injective ring homomorphism. The mapping Φ is well-defined since $\langle g_n \rangle \subseteq I$. Thus whenever $[f]_{\langle g_n \rangle} = [f']_{\langle g_n \rangle}$, then $[f]_I = [f']_I$. The fact that Φ is a homomorphism can be easily checked. Finally, let $[f]_{\langle g_n\rangle} \neq [g]_{\langle g_n\rangle}$. Assume that $[f]_I = [g]_I$. Then $f-g \in I \cap k[X_n] = \langle g_n\rangle$ which is not possible. Thus $[f]_I \neq [g]_I$.

Second, note that $\langle g_n\rangle$ is radical. If $f^m \in \langle g_n\rangle \subseteq I$, then $f \in k[X_n] \cap I = \langle g_n\rangle$. Thus we have by Theorem 3.6.7

$$\deg(g_n) = \dim k[X_n]/\langle g_n\rangle \leq \dim k[X_1,\ldots,X_n]/I\,.$$

The inequality follows from the fact that Φ transforms a basis of $k[X_n]/\langle g_n\rangle$ into a linearly independent subset of $k[X_1,\ldots,X_n]/I$.

($1 \Rightarrow 2$): If I is in normal X_n-position, then g_n has at least $\dim k[X_1,\ldots,X_n]/I$ many roots, i.e. $\deg(g_n) \geq \dim k[X_1,\ldots,X_n]/I$.

($2 \Rightarrow 3$): If $\dim k[X_1,\ldots,X_n]/I = \deg(g_n) = \dim k[X_n]/\langle g_n\rangle$, then the rings $k[X_n]/\langle g_n\rangle$ and $k[X_1,\ldots,X_n]/I$ are isomorphic as k-vector spaces. Since Φ is also an injective linear mapping, it must be onto. Thus Φ is a ring isomorphism.

($3 \Rightarrow 1$): If the rings $k[X_n]/\langle g_n\rangle$ and $k[X_1,\ldots,X_n]/I$ are isomorphic, then $d = \deg(g_n)$ is exactly the number of points in $\mathbf{V}(I)$. Let $a_1,\ldots,a_d \in k$ be the roots of g_n (the roots are pairwise distinct because g_n is square-free). Then $g_n = \prod_{i=1}^d (X_n - a_i)$. Thus the maximal ideals in $k[X_n]$ containing $\langle g_n\rangle$ are of the form $\langle X_n - a_i\rangle$. Then $\langle [X_n - a_i]_{\langle g_n\rangle}\rangle$ is a maximal ideal in $k[X_n]/\langle g_n\rangle$. By Lemma 3.7.4 we have $\Phi(\langle [X_n - a_i]_{\langle g_n\rangle}\rangle)$ is a maximal ideal in $k[X_1,\ldots,X_n]/I$. Thus this ideal corresponds to a maximal ideal M_i in $k[X_1,\ldots,X_n]$ by Proposition 3.7.3. The ideal M_i has to be of this form $\langle X_1 - \alpha_{1i},\ldots,X_n - \alpha_{ni}\rangle$ for some $\alpha_{1i},\ldots,\alpha_{ni} \in k$ by Theorem 3.1.11. Observe that

$$\Phi(\langle [X_n - a_i]_{\langle g_n\rangle}\rangle) = \langle \Phi([X_n - a_i]_{\langle g_n\rangle})\rangle = \langle [X_n - a_i]_I\rangle\,.$$

Thus $X_n - a_i \in M_i$. Since $X_n - a_i \in M_i$, we get that $\alpha_{ni} = a_i$. Now for different roots $a_i \neq a_j$ we obtain different maximal ideals M_i and M_j, i.e. different points $(\alpha_{1i},\ldots,a_i)$ and $(\alpha_{1j},\ldots,a_j)$ in $\mathbf{V}(I)$. Since there are exactly d points in $\mathbf{V}(I)$, all of them have pairwise different the last component. □

Theorem 3.7.6 (The Shape Lemma) *Let $I \subseteq k[X_1,\ldots,X_n]$ be a radical ideal in normal X_n-position such that $\mathbf{V}(I)$ is finite, g_n the monic generator of $I \cap k[X_n]$, and $d = \deg(g_n)$.*

1. *The reduced Gröbner basis of I w.r.t. lex term order is of the form*

   $$\{X_1 - g_1,\ldots,X_{n-1} - g_{n-1}, g_n\}\,,$$

   where $g_1,\ldots,g_{n-1} \in k[X_n]$.

2. *The polynomial g_n has d distinct roots $a_1,\ldots,a_d \in k$, and*

   $$\mathbf{V}(I) = \{(g_1(a_i),\ldots,g_{n-1}(a_i),a_i) \mid i = 1,\ldots,d\}\,.$$

PROOF: By Theorem 3.7.5 using the isomorphism $\Phi : k[X_n]/\langle g_n\rangle \to k[X_1,\ldots,X_n]/I$, each polynomial $f \in k[X_1,\ldots,X_n]$ is congruent w.r.t. I to a polynomial $g \in k[X_n]$. Indeed, since Φ is onto there is $[g]_{\langle g_n\rangle} \in k[X_n]/\langle g_n\rangle$ such that

$$[f]_I = \Phi([g]_{\langle g_n\rangle}) = [g]_I\,.$$

Thus for each $X_i \in k[X_1, \ldots, X_n]$ there is a polynomial $g_i \in k[X_n]$ such that $X_i - g_i \in I$. We show that $G = \{X_1 - g_1, \ldots, X_{n-1} - g_{n-1}, g_n\}$ is a Gröbner basis w.r.t. the lex term order. Clearly $\mathrm{LT}(G) = \{X_1, \ldots, X_{n-1}, X_n^d\}$. Let $f \in I$. If $\mathrm{LT}(f)$ contains at least one of $X_1, \ldots, X_{n-1}$, then $\mathrm{LT}(f) \in \langle \mathrm{LT}(G) \rangle$. If $\mathrm{LT}(f)$ contains only X_n, then $f \in I \cap k[X_n]$, i.e. $\mathrm{LT}(g_n) | \mathrm{LT}(f)$. Thus G is a Gröbner basis. Moreover, it is obvious that G is a reduced Gröbner basis.

Finally, since g_n is square-free, it has d distinct roots. It is also clear that the solutions of a system of polynomial equations $X_1 - g_1 = \cdots = X_{n-1} - g_{n-1} = g_n = 0$ has solutions of the form $(g_1(a_i), \ldots, g_{n-1}(a_i), a_i)$ for a root a_i of g_n. □

Corollary 3.7.7 (Solving a system of polynomial equations) *Let k be an algebraically closed field, $f_1, \ldots, f_s \in k[X_1, \ldots, X_n]$, and $I = \langle f_1, \ldots, f_s \rangle$. Consider the following sequence of instructions:*

1. *For $i = 1, \ldots, n$ compute a generator g_i of $I \cap k[X_i]$. If $g_i = 0$ for some i, then return "Infinite number of solutions" and stop.*
2. *By Lemma 3.6.8 compute $h_i = (g_i)_{red}$ for each i. Then replace I by $I + \langle h_1, \ldots, h_n \rangle$.*
3. *Compute number d of monomials in the complement of $\langle \mathrm{LT}(I) \rangle$, i.e.*
$$d = |\{X^\alpha \mid X^\alpha \notin \langle \mathrm{LT}(I) \rangle\}| .$$
4. *Check if $\deg(h_n) = d$. In this case, let $(c_1, \ldots, c_{n-1}) = (0, \ldots, 0)$ and continue with step 7.*
5. *Choose randomly $(c_1, \ldots, c_{n-1}) \in k^{n-1}$. Apply the coordinate transformation*
$$X_1 \mapsto X_1, \ \ldots, \ X_{n-1} \mapsto X_{n-1}, \ X_n \mapsto X_n - c_1 X_1 - \cdots - c_{n-1} X_{n-1}$$
to I and get an ideal J.
6. *Compute a generator of $J \cap k[X_n]$ and check if it has degree d. If not, repeat steps 5 and 6 until this is the case. Then rename J and call it I.*
7. *Compute the reduced Gröbner basis of I w.r.t. the lex term order. It has shape*
$$\{X_1 - g_1, \ldots, X_{n-1} - g_{n-1}, g_n\}$$
with polynomials $g_1, \ldots, g_n \in k[X_n]$ and with $\deg g_n = d$. Return the tuples $(c_1, \ldots, c_{n-1})$ and $(g_1, \ldots, g_n)$ and stop.

This is an algorithm which decides whether the system of polynomial equations $f_1 = \cdots = f_s = 0$ has finitely many solutions. In that case, it returns tuples $(c_1, \ldots, c_{n-1}) \in k^{n-1}$ and $(g_1, \ldots, g_n) \in k[X_n]$ such that, after we perform the linear change of coordinates
$$X_1 \mapsto X_1, \ \ldots, \ X_{n-1} \mapsto X_{n-1}, \ X_n \mapsto X_n - c_1 X_1 - \cdots - c_{n-1} X_{n-1} ,$$
the transformed system of equations has the set of solutions
$$\{(g_1(a_i), \ldots, g_{n-1}(a_i), a_i) \mid i = 1, \ldots, d\} ,$$

where $a_1, \ldots, a_n \in k$ *are roots of* g_n.

In other words, the original system of equations has the set of solutions

$$\{(g_1(a_i), \ldots, g_{n-1}(a_i), a_i - c_1 g_1(a_i) - \cdots - c_{n-1} g_{n-1}(a_i)) \mid i = 1, \ldots, d\}.$$

PROOF: The correctness of the first step follows from Corollary 3.6.4. By Corollary 3.6.11 the ideal I is replaced by radical $\sqrt{I}$ in step 2. By Theorem 3.6.7 the number d computed in step 3 is exact number of solutions. If $\deg(g_n) = d$, then I is in normal X_n-position by Theorem 3.7.5. If not there is $(c_1, \ldots, c_{n-1}) \in k^{n-1}$ by Lemma 3.7.2 such that, after the linear change of coordinates, the transformed ideal J is in normal X_n-position. Thus by the Shape Lemma the transformed system of equations has the solution set

$$\{(g_1(a_i), \ldots, g_{n-1}(a_i), a_i) \mid i = 1, \ldots, d\}.$$

Let $\mathbb{A}$ be the matrix representing the linear change of coordinates. Since we proved that $(b_1, \ldots, b_n) \in \mathbf{V}(I)$ iff $(b_1, \ldots, b_n) \cdot \mathbb{A}^{-1} \in \mathbf{V}(J)$, we get $(g_1(a_i), \ldots, g_{n-1}(a_i), a_i) \cdot \mathbb{A} \in \mathbf{V}(I)$ because

$$(g_1(a_i), \ldots, g_{n-1}(a_i), a_i) = (g_1(a_i), \ldots, g_{n-1}(a_i), a_i) \cdot \mathbb{A} \cdot \mathbb{A}^{-1}.$$

$\square$