Algebraic Geometry
The Basics

In this introduction only the most important definitions and theorems are given. It is based on the book *"Ideals, Varieties, and Algorithms"* by *David Cox, John Little* and *Donal O'Shea*, which is an excellent introduction to algebraic geometry. More detailed descriptions and also the proofs for the theorems can be found there.

Examples were computed using *Maple 12* with its packages `Groebner` and `PolynomialIdeals`. The first package contains the low-level commands, the second package is newer and contains the more sophisticated ones. There are also other software packages like e.g. *Singular* and *Macaulay 2* for such computations [1].

A polynomial f in $x_1, \ldots, x_n$ with coefficients in $\mathbf{K}$ is a finite linear combination (with coefficients in $\mathbf{K}$) of monomials. We will write a polynomial f in the form

$$f = \sum_{\alpha} a_\alpha x^\alpha, \quad a^\alpha \in \mathbf{K}, \alpha \in \mathbb{N}$$

where the sum is over a finite number of n-tuples $\alpha = (\alpha_1, \ldots, \alpha_n)$. The set of all polynomials in $x_1, \ldots, x_n$ with coefficients in $\mathbf{K}$ is denoted $\mathbf{K}[x_1, ..., x_n]$. The sum and product of two polynomials is again a polynomial and one can show that under addition and multiplication, $\mathbf{K}[x_1, ..., x_n]$ satisfies all of the field axioms except for the existence of multiplicative inverses (because, for example, $\frac{1}{x_1}$ is not a polynomial). Such a mathematical structure is called a commutative ring. In the following all algebraic equations are polynomials in the ring $\mathbf{K}[\underline{x}] = \mathbf{K}[x_1, \ldots, x_n]$ where $\mathbf{K}$ is a field like $\mathbb{Q}$ or $\mathbb{C}$.

Ideals and Affine Varieties

At first polynomial ideals are defined which are the basic objects for everything else.

Definition 1. *A set $I \subseteq \mathbf{K}[\underline{x}]$ is called an **ideal** if the following conditions are fulfilled:*

- $\forall\, f, g \in I : f + g \in I$
- $\forall\, f \in I$ *and* $\forall\, h \in \mathbf{K}[\underline{x}] : hf \in I$

It follows that almost all ideals are infinite sets of polynomials and cannot be written down as a whole. The sole exception is the ideal $\{0\}$ which is also a proper subset resp. subideal of all other ideals because 0 is contained in every ideal. There is also an ideal which is a proper superset resp. superideal of them, namely the ideal which contains the constant polynomial 1 and with it all polynomials of

[1] see also the SAGE initiative on open-source mathematics software [http://www.sagemath.org/].

$\mathbf{K}[\underline{x}]$.
Using Definition 1 it is possible now to define the ideal generated by a set of given polynomials $f_1, \ldots, f_s$.

Definition 2. *Let* $f_1, \ldots, f_s$ *be polynomials in* $\mathbf{K}[\underline{x}]$. *Then the set*

$$\langle f_1, \ldots, f_s \rangle = \{ g \in \mathbf{K}[\underline{x}] : g = \sum_{i=1}^{s} h_i f_i \;\; and \;\; h_1, \ldots, h_s \in \mathbf{K}[\underline{x}] \}$$

is the ***ideal generated by*** $f_1, \ldots, f_s$.

The ideal generated by the given polynomials is the set of all combinations of these polynomials using coefficients from $\mathbf{K}[\underline{x}]$. The polynomials $f_1, \ldots, f_s$ form a so called *basis* of the ideal. Due to the fact that the same ideal can be generated by another set of polynomials, such a basis is not **unique**. Furthermore the ideal is obviously *finitely generated* and it can be shown that every ideal of $\mathbf{K}[\underline{x}]$ can be generated by a finite set of polynomials (Hilbert Basis Theorem).
So the two special ideals mentioned above can be written as $\langle 0 \rangle$ and $\langle 1 \rangle$.

Example 1. *A circle is to be intersected with an ellipse. The corresponding algebraic equations are* $f_1 = (x_1 - 1)^2 + (x_2 - 2)^2 - 4 = 0$ *and* $f_2 = x_1^2 + 3\,x_2^2 - 5 = 0$. *To define the corresponding ideal using Maple one has to type the following:*

```
with(PolynomialIdeals);

I1:=<(x[1]-1)^2+(x[2]-2)^2-4,x[1]^2+3*x[2]^2-5>;
```

All commands in the package `Groebner` *allow to use the notation* $[\ldots]$ *instead of* $< \ldots >$.

As it was mentioned above such a basis is not unique. For example the ideals $\langle f_1, f_2 \rangle$ and $\langle f_1 - f_2, f_2 \rangle$ are completely the same. But how can this be found out for two given ideals, if the are equal or not?
Two ideals I and J are equal if each element of I is contained in J and vice versa. It is sufficient to test if the basis of one ideal is contained in the other, and vice versa. To find out if a given polynomial is a member of an ideal it is necessary to test if the polynomial can be written as a combination of the ideal's basis. How this can be done in a systematic way will be explained later.
Before that affine varieties are introduced.

Definition 3. *For a given ideal* $I = \langle f_1, \ldots, f_s \rangle \subseteq \mathbf{K}[\underline{x}]$ *the set*

$$\mathbf{V}(I) = \{ (a_1, \ldots, a_n) \in \mathbf{K}^n : f_i(a_1, \ldots, a_n) = 0 \;\; for\ all \;\; 1 \le i \le s \} \subseteq \mathbf{K}^n$$

is called the ***affine variety*** *of the ideal I (an irreducible algebraic set).*

For each ideal $I = \langle f_1, \ldots, f_s \rangle$ there exist a unique variety $\mathbf{V}(I)$ which is the set of all solutions of the polynomials equations $f_1 = 0, \ldots, f_s = 0$, the so called *vanishing set.* It follows immediately that all bases of the ideal describe the same variety. In general the variety of an ideal is the more interesting thing, not the ideal itself, because the variety is exactly the set of solutions of the input equations $f_1, \ldots, f_s$. It has to be mentioned explicitly that the variety does not contain information about the multiplicity of solutions. It is just a set of points in $\mathbf{K}[\underline{x}]$, nothing more.
Two special varieties are $\emptyset$ and $\mathbf{K}^n$ which are the vanishing sets of the ideals $\langle 1 \rangle$ and $\langle 0 \rangle$ which appeared earlier.

Example 2. *A circle with center $(0,0)$ and a line are given by $x_1^2+x_2^2-1=0$ and $x_1+x_2-1=0$. Then the ideal generated by these two equations is given by $I=\langle x_1^2+x_2^2-1, x_1+x_2-1\rangle$ and the corresponding variety is $\{(1,0),(0,1)\}$.*

It is also possible that different ideals describe the same variety. This is related to the fact that solutions can appear with higher multiplicities.

Example 3. *The following polynomial ideals I and I' are given, each by two possible bases.*

$$\begin{aligned} I &= \langle x_1^2+x_2^2-1, x_1+x_2-1\rangle = \langle x_2^2-x_2, x_1+x_2-1\rangle \\ I' &= \langle (x_1^2+x_2^2-1)^2, x_1+x_2-1\rangle = \langle x_2^4-2\,x_2^3+x_2^2, x_1+x_2-1\rangle \end{aligned}$$

It can easily be seen that $\mathbf{V}(I)=\mathbf{V}(I')=\{(1,0),(0,1)\}$ but the ideals are not equal because $x_2^2-x_2$ cannot be written as a combination of $x_2^4-2\,x_2^3+x_2^2$ and x_1+x_2-1.

To test if two ideals describe the same variety *radicals* are introduced.

Definition 4. *Let $I \subseteq \mathbf{K}[\underline{x}]$ be an ideal. The set*

$$\sqrt{I} := \{f \in \mathbf{K}[\underline{x}] : \exists\; m \in \mathbb{N}, m \geq 1 \;\; with \;\; f^m \in I\}$$

*is called the **radical** of I.*

The computation of the radical of an ideal I can be seen as reducing I down to the most important things, relevant for its vanishing set. In the example above it is $\sqrt{I}=\sqrt{I'}=I$.

Example 4. *The ideal $I=\langle(2\,x_1-x_2-2)x_1, (2\,x_1-x_2-2)x_2^2\rangle$ is given, where its vanishing set $\mathbf{V}(I)$ is the line described by $2\,x_1-x_2-2$ and the isolated point $(0,0)$. To be exact, there are two copies of the point $(0,0)$ when multiplicities are taken into account.*
Computation of the radical using Maple leads to the slightly simpler ideal $\sqrt{I}=\langle-(2\,x_1+x_2)(2\,x_1-x_2-2), -(2\,x_1-x_2-2)x_1\rangle$ which has the same vanishing set, but now the point $(0,0)$ does not appear with higher multiplicity. The code for Maple is the following:

```
with(PolynomialIdeals);

I1:=<(2*x[1]-x[2]-2)*x[1], (2*x[1]-x[2]-2)*x[2]^2>;

rad:=Radical(I1);
```

Next some operations are given which can be applied to varieties.

Theorem 1. *Let $I=\langle f_1,\ldots,f_s\rangle$ and $J=\langle g_1,\ldots,g_t\rangle$ be ideals with corresponding varieties $V=\mathbf{V}(I)$ and $W=\mathbf{V}(J)$. Then the **union** and **intersection** of V and W can be described as follows:*

$$\begin{aligned} V \cap W &= \mathbf{V}(\langle f_1,\ldots,f_s,g_1,\ldots,g_t\rangle) \\ V \cup W &= \mathbf{V}(\langle f_i g_j : 1 \leq i \leq s, 1 \leq j \leq t\rangle) \end{aligned}$$

The first equality is quite clear, if one is searching for the solutions two systems have in common, the equations are combined and the resulting system is examined. The second equality can be used to construct varieties which are a composition of simpler varieties.

Example 5. *Three very simple varieties are given to show what happens, when varieties are intersected or joined.*

$$V_1 = \mathbf{V}(\langle x_1 \rangle) \quad V_2 = \mathbf{V}(\langle x_2 \rangle)$$

$$\begin{aligned} V_1 \cap V_2 &= \mathbf{V}(\langle x_1, x_2 \rangle) = \{(0,0)\} \\ V_1 \cup V_2 &= \mathbf{V}(\langle x_1 x_2 \rangle) \end{aligned}$$

What happens when two varieties are joined where one is a subset of the other variety?

$$V_1 \cup \mathbf{V}(\langle x_1, x_2 \rangle) = \mathbf{V}(\langle x_1^2, x_1 x_2 \rangle)$$

It can easily be seen that the vanishing set is the same, but when multiplicities are taken into account the point $(0,0)$ *appears twice.*
Again the code for maple and the corresponding commands:

```
with(PolynomialIdeals);

J1:=<x[1]>;  J2:=<x[2]>;

J_inters:=Add(J1,J2);

J_union:=Multiply(J1,J2);

Multiply(J1,J_union);
```

Now back to the different ways to generate an ideal. As already mentioned there are lots of different bases which describe all the same ideal, e.g. the ideals

$$\begin{aligned} I &= \langle f_1, f_2, f_3 \rangle \subseteq \mathbf{K}[x_1, x_2, x_3, x_4] \\ I' &= \langle f_1, x_2^2 f_1 - f_2, 2\, f_3 + (x_3 + 5) f_2 - f_1 \rangle \end{aligned}$$

It can easily be verified that each combination of the generators of I' can be written as a combination of generators of I and vice versa.
But what to do when the ideals are more complex? It is necessary to have a systematic way for testing if a polynomial is a combination of some other polynomials. Therefore the concept of *multivariate division with remainder* is introduced, which is similar to the well known *univariate division with remainder* which shall be introduced first.

Theorem 2. *Let* $f, g \in \mathbf{K}[x_1]$ *be univariate polynomials with* $g \neq 0$. *Then there exist unique polynomials* q *and* r *such that*

$$f = qg + r$$

with either $r = 0$ *or* $deg(r) < deg(g)$.

In the corresponding algorithm an appropriate multiple of g is subtracted from f such that the monomial with highest degree is cancelled from f. This procedure is repeated until the remainder is either 0 or has degree less than $deg(g)$.

Example 6. *Here an example with* $f = 2\,x^2 - 3\,x - 7$ *and* $g = x + 5$*:*

$$\begin{aligned} f - \boldsymbol{2x}\, g &= 2\,x^2 - 3\,x - 7 - 2\,x(x+5) = -13\,x - 7 \\ (-13\,x - 7) - \boldsymbol{(\text{-}13)} g &= -13\,x - 7 + 13\,x + 65 = \boldsymbol{58} \end{aligned}$$

It follows that $q = 2\,x - 13$ *and* 58. *To get these results with Maple the commands would be*

```
quo(f,g,x);  rem(f,g,x);
```

The process stops when the highest monomial of the remainder is not divisible by the highest monomial of g. So in the univariate case the degree of monomials can be seen as a natural *order* on the set of monomials, which guides the user trough the algorithm.
In the following *termorders* are introduced which allow ordering of a multivariate polynomial's monomials. With these termorders an analog algorithm can be defined for multivariate polynomials.

Definition 5. *Let $\underline{x}^\alpha = x_1^{\alpha_1} \dots x_n^{\alpha_n}$ and $\underline{x}^\beta = x_1^{\beta_1} \dots x_n^{\beta_n}$ be monomials in $\mathbf{K}[\underline{x}] = \mathbf{K}[x_1, \dots, x_n]$. To order these monomials a **monomial ordering** or **termorder** $>_{\underline{x}}$ on the set of monomials in $\mathbf{K}[\underline{x}]$ is defined by an ordering $>$ on the n-tuples $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$ which has to fulfill the following conditions:*

- *$>$ is a total ordering on $\mathbb{Z}^n_{\geq 0}$*
- *if $\alpha > \beta$ and $\gamma \in \mathbb{Z}^n_{\geq 0}$, then $\alpha + \gamma > \beta + \gamma$*
- *every nonempty subset of $\mathbb{Z}^n_{\geq 0}$ has a smallest element under $>$*

If such an ordering $>$ on $\mathbb{Z}_{\geq 0}$ is given the monomials are ordered using the following equivalence:

$$\underline{x}^\alpha >_{\underline{x}} \underline{x}^\beta \Longleftrightarrow \alpha > \beta$$

So monomials are ordered by comparing the ordered n-tuples constructed from the powers of each variable. Next the most important termorderings are given.

Definition 6. ***(Lexicographic Order)*** *Let $\alpha = (\alpha_1, \dots, \alpha_n)$ and $\beta = (\beta_1, \dots, \beta_n)$ be elements of $\mathbb{Z}^n_{\geq 0}$. We define $\alpha >_{lex} \beta$ if the leftmost nonzero entry of the vector-difference $\alpha - \beta \in \mathbb{Z}^n$ is positive.*

In Maple the keyword for this ordering is `plex`, e.g. a possible lexicographic termorder for polynomials containing the unknowns $\{x_1, x_2, x_3\}$ could be `plex(x[3],x[1],x[2])`.

Example 7. *How this ordering looks like for monomials in $\mathbf{K}[x_1, x_2]$ can be seen in the following. It is a sketch how the set of all monomials is ordered, first the 2-tuples are given, then the corresponding monomials starting with the smallest.*

$$(0,0) <_{lex} (0,1) <_{lex} (0,2) \dots <_{lex} (1,0) <_{lex} (1,1) <_{lex} (1,2) \dots$$

$$1 <_{lex} x_2 <_{lex} x_2^2 \dots <_{lex} x_1 <_{lex} x_1x_2 <_{lex} x_1x_2^2 \dots$$

Maple has the command `TestOrder` to test if a monomial is smaller than another one.

```
with(Groebner);

TestOrder(x[1]*x[2],x[2]^5,plex(x[1],x[2]));

TestOrder(x[2]^4,x[1]^2*x[2],plex(x[1],x[2]));
```

The result of the first test will be false*, the second result will be* true*.*

For the next termorderings the total degree of monomials is needed. For a monomial $\underline{x}^\alpha$ it is denoted with $|\alpha|$ where $|\alpha| = \alpha_1 + \dots + \alpha_n$.

Definition 7. ***(Graded Lex Order)*** *Let $\alpha = (\alpha_1, \dots, \alpha_n)$ and $\beta = (\beta_1, \dots, \beta_n)$ be elements of $\mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{grlex} \beta$ if $|\alpha| > |\beta|$ or, in case of $|\alpha| = |\beta|$, if $\alpha >_{lex} \beta$.*

In this termorder monomials are first ordered by the total degree and then ties are broken using $>_{lex}$. Here the keyword for Maple is `grlex` and a possible termorder could be `grlex(x[2],x[1],x[3])`.

Example 8. *Again a sketch how the monomials in* $\mathbf{K}[x_1, x_2]$ *are ordered.*

$$(0,0) <_{grlex} (0,1) <_{grlex} (1,0) <_{grlex} (0,2) <_{grlex} (1,1) <_{grlex} (2,0) \ldots$$

$$1 <_{grlex} x_2 <_{grlex} x_1 <_{grlex} x_2^2 <_{grlex} x_1x_2 <_{grlex} x_1^2 \ldots$$

The corresponding Maple command can be seen in Example 7, only `plex` *has to be replaced with* `grlex`.

And now the termorder which is commonly used. Computations using this order tend to be faster than computations wrt. other orders.

Definition 8. ***(Graded Reverse Lex Order)*** *Let* $\alpha = (\alpha_1, \ldots, \alpha_n)$ *and* $\beta = (\beta_1, \ldots, \beta_n)$ *be elements of* $\mathbb{Z}^n_{\geq 0}$. *We define* $\alpha >_{grevlex} \beta$ *if* $|\alpha| > |\beta|$ *or, in case of* $|\alpha| = |\beta|$, *if the rightmost nonzero entry of* $\alpha - \beta \in \mathbb{Z}^n$ *is negative.*

Again monomials are first ordered by the total degree. But ties are now broken using a different condition. In Maple this termorder is used with the keyword `tdeg`.

Example 9. *Here is a sketch how the monomials in* $\mathbf{K}[x_1, x_2]$ *are ordered when* $<_{grevlex}$ *is used.*

$$(0,0) <_{grevlex} (0,1) <_{grevlex} (1,0) <_{grevlex} (0,2) <_{grevlex} (1,1) <_{grevlex} (2,0) \ldots$$

$$1 <_{grevlex} x_2 <_{grevlex} x_1 <_{grevlex} x_2^2 <_{grevlex} x_1x_2 <_{grevlex} x_1^2 \ldots$$

As it can easily be seen monomials in this example are sorted the same way as with the previous order. This is a special property of $>_{grevlex}$, *if there are only two variables it leads to the same ordering as* $>_{grlex}$. *For three or more variables the ordering is really different, e.g.*

$$x_1^2x_3^2 >_{grlex} x_1x_2^2x_3 \quad \textit{but} \quad x_1^2x_3^2 <_{grevlex} x_1x_2^2x_3$$

All these orderings can also be combined which leads to the so called *Product Orders*. An example for a product order on $\mathbf{K}[x_1, x_2, x_3, x_4]$ in Maple would be `prod(plex(x[1], x[2]), tdeg(x[3], x[4]))`. This means that monomials are first compared using the `plex` order, ties are broken using the `tdeg` order. Even more than two partial orders are allowed.

It has to be noted explicitly that also the ordering of the variables can be varied, not only the type. All in all there are lots of different ways to define an order for ordering monomials.

Now is is possible to order the monomials of a polynomial. Before the multivariate polynomial division can be defined another definition is necessary.

Definition 9. *Let* $f \in \mathbf{K}[\underline{x}]$ *be a polynomial with* $f = \sum_\alpha a_\alpha x^\alpha$ *and let* $>_{\underline{x}}$ *be a monomial ordering on* $\mathbf{K}[\underline{x}]$. *We define the* ***leading monomial*** $LM(f)$ *as the highest monomial of* f *with respect to* $>_{\underline{x}}$, *the* ***leading coefficient*** $LC(f)$ *as the coefficient of the highest monomial, and the* ***leading term*** *as* $LT(f) = LC(f) \cdot LM(f)$.

The most important thing in this definition is the leading monomial. It will appear quite often in the following definitions and theorems.

Example 10. *Here is an example with $f = x_1^2x_2^3 - 5x_1x_2x_3 + 4\,x_1^3x_3^2$ where the termorder $>_{grlex}$ on $\mathbf{K}[\underline{x}]$ is used:*

$$deg(f) = 5 \quad LM(f) = x_1^3x_3^2 \quad LC(f) = 4 \quad LT(f) = 4\,x_1^3x_3^2$$

To get these results with Maple the following commands can be used:

```
with(Groebner);

f:=x[1]^2*x[2]^3-5*x[1]*x[2]*x[3]+4*x[1]^3*x[3]^2;

degree(f,[x[1],x[2],x[3]]);

LeadingMonomial(f,grlex(x[1],x[2],x[3]));

LeadingCoefficient(f,grlex(x[1],x[2],x[3]));

LeadingTerm(f,grlex(x[1],x[2],x[3]));
```

For the leading term Maple returns not the product but the pair $LC(f), LM(f)$.
If the termorder `plex(x[2],x[3],x[1])` *is used instead the results are as follows:*

$$deg(f) = 5 \quad LM(f) = x_1^2x_2^3 \quad LC(f) = 1 \quad LT(f) = x_1^2x_2^3$$

Now all ingredients are defined and it is possible to introduce the multivariate division.

Definition 10. *Let $F = [f_1, \ldots, f_s]$ be an ordered list of polynomials in $\mathbf{K}[\underline{x}]$ and $>_{\underline{x}}$ a monomial order. Then every polynomial $f \in \mathbf{K}[\underline{x}]$ can be written in the form*

$$f = a_1f_1 + \ldots + a_sf_s + r$$

*where all a_i and r are elements of $\mathbf{K}[\underline{x}]$ and r is either 0 or a polynomial where no monomial is divisible by any of $LM(f_1), \ldots, LM(f_s)$. r is called **a remainder** of f on division by F.*

The algorithm which produces the a_i and the remainder r acts in the following way: It is tested if $LM(f)$ is divisible by $LM(f_1)$, then by $LM(f_2)$ and so on. If the result of such a test is true for a leading monomial $LM(f_i)$, testing is stopped and an appropriate multiple of f_i is subtracted from f such that $LT(f)$ is cancelled. The result is again named f and the testing starts again. In the other case that $LM(f)$ is not divisible by $LM(f_1), \ldots, LM(f_s)$, the term $LT(f)$ is added to the remainder. It follows that in each step $LT(f)$ is removed, either by cancellation or by moving it to the remainder. The process is finished when f is 0.

Example 11. *As an example the polynomial $f = x_1^2x_2 + x_1x_2^2 + x_2^2$ is divided by the polynomials $f_1 = x_1x_2 - 1$ and $f_2 = x_2^2 - 1$, where the termorder $>_{lex}$ is used in $\mathbf{K}[x_1, x_2]$.*

$$\begin{aligned}
&f = x_1^2x_2 + x_1x_2^2 + x_2^2, \quad r = 0,\ a_1 = 0,\ a_2 = 0\\
&f \leftarrow x_1x_2^2 + x_1 + x_2^2, \quad r = 0,\ a_1 = x_1,\ a_2 = 0\\
&f \leftarrow x_1 + x_2^2 + x_2, \quad r = 0,\ a_1 = x_1 + x_2,\ a_2 = 0\\
&f \leftarrow x_2^2 + x_2, \quad r = x_1,\ a_1 = x_1 + x_2,\ a_2 = 0\\
&f \leftarrow x_2 + 1, \quad r = x_1,\ a_1 = x_1 + x_2,\ a_2 = 1\\
&f \leftarrow 1, \quad r = x_1 + x_2,\ a_1 = x_1 + x_2,\ a_2 = 1\\
&f \leftarrow 0, \quad r = x_1 + x_2 + 1,\ a_1 = x_1 + x_2,\ a_2 = 1
\end{aligned}$$

It follows that f can be written as

$$f = a_1f_1 + a_2f_2 + r = (x_1 + x_2)(x_1x_2 - 1) + (1)(x_2^2 - 1) + (x_1 + x_2 + 1)$$

where no monomial in the remainder $x_1 + x_2 + 1$ is divisible by $LM(f_1)$ or $LM(f_2)$.

It has to be said clearly that the result r is *a remainder* of f on division by the list F. If f_1 is exchanged with f_2 the following result is obtained:

$$f = a'_1 f_1 + a'_2 f_2 + r' = (x_1 + 1)(x_2^2 - 1) + (x_1)(x_1 x_2 - 1) + (2\,x_1 + 1)$$

So the remainder r depends on the order of the polynomials in the list F and of course, on the monomial order which has to be chosen first of all.

Using the multivariate division the notion of *reduction* can be defined.

Definition 11. *Let $F = [f_1, \dots, f_s]$ be an ordered list of polynomials in $\mathbf{K}[\underline{x}]$, $f \in \mathbf{K}[\underline{x}]$ and $>_{\underline{x}}$ a monomial order. Then we call the process of dividing f by F* ***reduction*** *and denote the remainder with $\overline{f}^F$. The choice of a monomial order is required to be able to compute the remainder.*

This reduction will be used quite often in the following definitions and theorems. But before that the corresponding Maple command is given.

Example 12. *The polynomial $f = x_1^2 x_2 + x_1 x_2^2 + x_2^2$ shall again be divided by the polynomials $f_1 = x_1 x_2 - 1$ and $f_2 = x_2^2 - 1$, where the termorder $>_{lex}$ is used in $\mathbf{K}[x_1, x_2]$.*

```
with(Groebner);

f:=x[1]^2*x[2]+x[1]*x[2]^2+x[2]^2;

f1:=x[1]*x[2]-1;

f2:=x[2]^2-1;

r:=Reduce(f,[f1,f2],plex(x[1],x[2]),’s’,’a’);

s;  a;
```

The result is a remainder r, a list of quotients a and a number s such that

$$f = \sum_{i=1}^{2} a_i f_i + \frac{r}{s}$$

For this example:

$$r = x_1 + x_2 + 1 \qquad a = [x_1 + x_2, 1] \qquad s = 1$$

The necessity of a monomial order will not be mentioned explicitly from now on. Next we define *interreduction.*

Definition 12. *Let $F = [f_1, \dots, f_s]$ be an ordered list of polynomials in $\mathbf{K}[\underline{x}]$. The process of replacing each polynomial f_i by $\overline{f_i}^{F\setminus\{f_i\}}$ is called* ***interreduction*** *of the list F.*

This means that every polynomial in F is reduced with respect to all the other elements of the list. An important property of an interreduction is that the original set of polynomials and the result of the interreduction generate the same ideal. Interreduction can sometimes be used to simplify generating sets (bases) of an ideal, to obtain shorter polynomials. The right choice of the monomial order is important.

Example 13. *The ideal $I = \langle (x_1-1)^2+(x_2+5)^2-6, 2\,x_1^2+2\,x_2^2-4\rangle$ is interreduced. The appropriate commands are the following:*

```
with(Groebner);

I1:=[(x[1]-1)^2+(x[2]+5)^2-6,2*x[1]^2+2*x[2]^2-20];

ir:=InterReduce(I1,plex(x[1],x[2]));
```

And the result is

$$ir = [215 - 150\,x_2 + 26\,{x_2}^2, x_1 - 15 + 5\,x_2]$$

Now back to ideals generated by a set of polynomials. There was already the question how one could decide if a given polynomial f is an element of $I = \langle f_1, \ldots, f_s\rangle$. The concept of reduction would be a good method to answer that question. First a result is given which is not the perfect solution.

Theorem 3. *Let $I = \langle f_1, \ldots, f_s\rangle \subseteq \mathbf{K}[\underline{x}]$ be an ideal and $f \in \mathbf{K}[\underline{x}]$. If $\overline{f}^F = 0$ then f is an element of I.*

The disadvantage of this result is that if $\overline{f}^F \neq 0$ the question is open as before. The crucial point is that the leading terms $LT(f_1), \ldots, LT(f_s)$ which are used in the division algorithm are in general "bad" representatives for the set of all leading terms which are possible in the ideal I.

Example 14. *Let $F = [f_1, f_2] = [x_1x_2+1, x_2^2-1]$ be an ordered list of polynomials in $\mathbf{K}[\underline{x}]$ and $p_1 = x_1f_1 + x_2f_2$ and $p_2 = x_2f_1 + x_1f_2$ be combinations of these polynomials.*
It is clear that $p_1, p_2 \in \langle f_1, f_2\rangle$. But if the reductions are computed wrt. `plex(x[1],x[2])`, *the following results are obtained:*

$$\overline{p_1}^F = 0 \qquad \overline{p_2}^F = -x_1 - x_2$$

In the first case Theorem 3 works quite fine, it does not in the second.

Now *standard bases* are defined which are "much better" representatives (generators) for an ideal. They are still dependent from a chosen monomial order but nevertheless very useful to deduce information about the ideal and the corresponding variety.

Standard Bases

Definition 13. *For a fixed monomial order and an ideal $I \in \mathbf{K}[\underline{x}]$ a finite subset $G = \{g_1, \ldots, g_t\}$ of I is called a **Groebner basis** or **standard basis** if*

$$\langle LM(g_1), \ldots, LM(g_t)\rangle = \langle LM(I)\rangle$$

where $LM(I)$ is the ideal generated by all the leading terms of the elements of I.

With other words a basis is also a Groebner basis if its leading monomials of the generators generate the same ideal as the leading monomials of all ideal elements.
A Groebner basis is a very special generating set of the ideal I with some nice properties. Such a basis is not unique due to the fact that adding another polynomial to the generators does not change this property. Another reason for non-uniqueness is the fact that a monomial order has to be chosen first.
In this introduction it will not be explained in detail how such a Groebner basis is computed explicitly, starting with a set of generators and a term order. Just a short appetizer: For all possible pairs of

generators the so called *S-polynomials* are computed and reduced with the list of generators. All remainders which are not 0 are added to the list and the procedure starts again. Such rounds are repeated until all remainders of the S-polynomials are all 0 after reduction. See the book “Ideals, Varieties, and Algorithms” by Cox, Little and O’Shea for a detailed description of the algorithm and enhancements of it.
With a Groebner basis we get a better result for the ideal-membership-question.

Theorem 4. *Let $G = \{g_1, \ldots, g_t\} \subseteq \mathbf{K}[\underline{x}]$ be a Groebner basis of an ideal I and $f \in \mathbf{K}[\underline{x}]$. The polynomial f is an element of I if and only if $\overline{f}^G = 0$.*

All in all the procedure for the ideal-membership-question is the following: first a termorder is fixed, then a Groebner basis of the ideal is computed and after that the polynomial f is reduced with respect to this basis. f is exactly only then an element of I if the result of the reduction is 0.
It has to be mentioned that the result of a reduction with respect to a Groebner basis is independent of the order of the basis elements, this was not the case when the reduction was done with respect to a normal basis.

Example 15. *As an example the polynomials from Example 14. Let $I = \langle f_1, f_2\rangle = \langle x_1x_2 + 1, x_2^2 - 1\rangle$ be an ideal in $\mathbf{K}[\underline{x}]$ and $p_1 = x_1f_1 + x_2f_2$ and $p_2 = x_2f_1 + x_1f_2$ polynomials which are definitely elements of I.*
Now a Groebner basis is computed wrt. `plex(x[1],x[2])` *and p_1, p_2 are reduced with that basis.*

```
with(Groebner);

with(PolynomialIdeals):

f1:=x[1]*x[2]+1;  f2:=x[2]^2-1;

G:=Basis(<f1,f2>,plex(x[1],x[2]));

p1:=x[1]*f1+x[2]*f2;

p2:=x[2]*f1+x[1]*f2;

Reduce(p1,G,plex(x[1],x[2]));

Reduce(p2,G,plex(x[1],x[2]));
```

The Groebner basis is

$$G = \langle x_2^2 - 1, x_1 + x_2\rangle$$

and now the expected results are obtained:

$$\overline{p_1}^F = 0 \qquad \overline{p_2}^F = 0$$

The package `PolynomialIdeals` *contains also two commands for testing if a polynomial or an ideal is contained in another ideal. They are used as follows:*

```
IdealMembership(p1,G);

IdealContainment(<p1,p2>,G);
```

The result of both commands will be true.

As mentioned above adding another polynomial of the ideal to the generators does not change the property of being a Groebner basis. To get a unique version of such a basis the so called *reduced Groebner bases* are defined.

Definition 14. *Let $G = \{g_1, \ldots, g_t\} \subseteq \mathbf{K}[\underline{x}]$ be a Groebner basis of a given ideal I. The generators G are a* ***reduced Groebner basis*** *if G is interreduced and all leading coefficients are 1.*

Fortunately all bases returned by Maple are interreduced. So at least the more important condition is fulfilled and the bases are quasi unique. This is not the case when *Singular* is used. But there exists a command to switch on basis-interreduction.
Now some remarks about Groebner bases:

- The number of polynomials in a Groebner basis can be very large, it depends on the complexity of the ideal and, of course, on the chosen monomial order. It is quite possible that only a part of the Groebner basis would be enough to generate the ideal I, but then the relevant condition $\langle LM(g_1), \ldots, LM(g_t)\rangle = \langle LM(I)\rangle$ is no more fulfilled.
- There are different methods to compute Groebner bases. The sketch of the algorithm above describes only the main concept. Lots of improvements were made to accelerate basis computations. Depending on the termorder the computations can be very expensive with respect to time and memory. Sometimes it is better to compute the basis for an "easy" termorder and then to convert it to the desired termorder using one of the conversion-algorithms.
- The monomial order $>_{lex}$ (in Maple `plex`) tends to be expensive in general, whereas the order $>_{grevlex}$ (in Maple `tdeg`) tends to be "relatively" cheap. If the type of order is chosen the computational costs can again be influenced by the order of unknowns.
- The typical way to order the polynomials in a basis is by sorting them wrt. the leading monomials, starting with the smallest one.

Example 16. *Now as an example reduced Groebner bases are computed for the ideal*

$$I = \langle x_1^2 x_2 + x_1 x_2^2 + x_2^2 x_3, x_1 x_2 - x_3, x_2^2 - 1\rangle$$

using different termorders:
$>_{lex}$ *in* $\mathbf{K}[x_1, x_2, x_3]$:

$$G = \{x_3^3 + 2\,x_3^2, x_2 x_3 + x_3^2 + x_3, x_2^2 - 1, x_1 + x_3^2 + x_3\}$$

$>_{lex}$ *in* $\mathbf{K}[x_3, x_1, x_2]$:

$$G = \{x_2^2 - 1, x_1^2 + x_1 x_2 + x_1, x_3 - x_1 x_2\}$$

$>_{grlex}$ *in* $\mathbf{K}[x_1, x_2, x_3]$:

$$G = \{x_3^2 + x_1 + x_3, x_2 x_3 - x_1, x_2^2 - 1, x_1 x_3 + x_1 + x_3, x_1 x_2 - x_3, x_1^2 + x_1 + x_3\}$$

The code for Maple looks as follows:

```
with(Groebner);

with(PolynomialIdeals):

f1:=x[1]^2*x[2]+x[1]*x[2]^2+x[2]^2*x[3];
```

```
f2:=x[1]*x[2]-x[3];  f3:=x[2]^2-1;

Basis(<f1,f2,f3>,plex(x[1],x[2],x[3]));

Basis(<f1,f2,f3>,plex(x[3],x[1],x[2]));

Basis(<f1,f2,f3>,grlex(x[1],x[2],x[3]));
```

It is no coincidence that in all the bases wrt. to $>_{lex}$ the first polynomial is univariate. This is because the lex-orders have the so called *elimination property*.
Now what is elimination resp. an elimination ideal?

Elimination

First of all the so called *elimination ideals* are defined.

Definition 15. *Let I be an ideal in $\mathbf{K}[\underline{x}] = \mathbf{K}[x_1, \ldots, x_n]$ and $1 \leq l < n$. Then the ideal $I_l = I \cap \mathbf{K}[x_{l+1}, \ldots, x_n]$ is called the **l-th elimination ideal** of I. I_l contains all elements of I which do not contain the variables $x_1, \ldots, x_l$.*

If a termorder has the elimination property, then a basis wrt. this order can be used to extract bases for the elimination ideals.

Theorem 5. *Let $G = \{g_1, \ldots, g_t\} \subseteq \mathbf{K}[x_1, \ldots, x_n]$ be a Groebner basis of an ideal I with respect to $>_{lex}$. Furthermore let $H = \{h_1, \ldots, h_k\}$ be the first k polynomials of G which do not contain the unknowns $x_1, \ldots, x_l$. Then H is a Groebner basis of the l-th elimination ideal I_l.*

It follows an example where it can be seen more clearly what this means.

Example 17. *The ideal $I = \langle x_1^2 x_2 + x_1 x_2^2 + x_2^2 x_3, x_1 x_2 - x_3, x_2^2 - 1\rangle$ is given with the Groebner basis wrt.* `plex(x[1],x[2],x[3])`

$$G = \langle x_3^3 + 2\,x_3^2, x_2 x_3 + x_3^2 + x_3, x_2^2 - 1, x_1 + x_3^2 + x_3\rangle$$

Then the following generators are all Groebner bases of the corresponding elimination ideal:

$$\begin{aligned} I_2 &= \langle x_3^3 + 2\,x_3^2\rangle \\ I_1 &= \langle x_3^3 + 2\,x_3^2, x_2 x_3 + x_3^2 + x_3, x_2^2 - 1\rangle \end{aligned}$$

There is also another command to do the elimination directly. It is contained in the package `PolynomialIdeals` *and to compute I_1 directly from the input polynomials it is used as follows:*

```
EliminationIdeal(<f1,f2,f3>,{x[2],x[3]});
```

The second argument gives the unknowns which shall not be eliminated. Furthermore no termorder has to be chosen, this is done by Maple internally. Unfortunately this choice is session-dependent.

It can easily be seen that with these elimination ideals it is quite easy to solve a system of equations with only finitely many solutions.

Example 18. *Here once again the Groebner basis G from above including I_2 and I_1.*

$$\begin{aligned} I_2 &= \langle x_3^3 + 2\,x_3^2 \rangle \\ I_1 &= \langle x_3^3 + 2\,x_3^2, x_2x_3 + x_3^2 + x_3, x_2^2 - 1 \rangle \\ G &= \langle x_3^3 + 2\,x_3^2, x_2x_3 + x_3^2 + x_3, x_2^2 - 1, x_1 + x_3^2 + x_3 \rangle \end{aligned}$$

Now the system can be solved step by step by solving the partial systems and extending the solutions.

```
with(Groebner);

with(PolynomialIdeals):

f1:=x[1]^2*x[2]+x[1]*x[2]^2+x[2]^2*x[3];

f2:=x[1]*x[2]-x[3];  f3:=x[2]^2-1;

I0:=<f1,f2,f3>;

G:=<op(Basis(I0,plex(x[1],x[2],x[3])))>;

NumberOfSolutions(I0);

I2:=EliminationIdeal(<f1,f2,f3>,{x[3]});

I1:=EliminationIdeal(<f1,f2,f3>,{x[2],x[3]});

L1:={solve(Generators(I2),{x[3]})};

L2:=map(y->op(map(z->z union y,{solve(eval(Generators(I1),y),
                                             {x[2]})})),L1);

L3:=map(y->op(map(z->z union y,{solve(eval(Generators(G),y),
                                             {x[1]})})),L2);
```

The result for the vanishing set is $\mathbf{V}(I) = \{(-2,1,-2),(0,-1,0),(0,1,0)\}$, *where the second solution has multiplicity 2.*

How does the the variety of the l-th elimination ideal $\mathbf{V}(I_l)$ correspond to the original variety $\mathbf{V}(I)$?

Theorem 6. *The variety* $\mathbf{V}(I_l) \in \mathbf{K}^{n-l}$ *is the smallest variety (wrt. inclusion) which contains* $\pi(\mathbf{V}(I))$, *where* $\pi(\mathbf{V}(I))$ *is the orthonormal projection of* $\mathbf{V}(I)$ *onto the subspace generated by equations* $x_1 = \ldots = x_l = 0$.

An important thing is that the equality $\mathbf{V}(I_l) = \pi(\mathbf{V}(I))$ only holds when I is a *projective variety* and I_l a *projective elimination ideal*. This means that here it can happen that a solution of I_l can not be extended to a solution of I_{l-1}.

Another application of elimination is implicitation. The following example shows how a variety can be deduced from a parametrisation.

Example 19. *A parametrisation of an ellipse is given.*

$$x[1] = \frac{5\,(1-t^2)}{1+t^2} \qquad x[2] = \frac{3\,(2\,t)}{1+t^2}$$

For all values of $t \in \mathbb{R}$ a point of the ellipse is obtained. The only point which cannot be reached is the left apex $(-5, 0)$. To compute the smallest variety which contains all these points (should be the ellipse), the following code could be used:

```
with(Groebner);

with(PolynomialIdeals):

par1:=x[1]-(5*(1-t^2))/(1+t^2);

par2:=x[2]-(3*(2*t))/(1+t^2);

J:=<numer(par1),numer(par2)>;

G:=Basis(J,plex(t,x[1],x[2]));

J1:=<G[1]>;
```

The first elimination ideal $J_1 = \langle 9\,x_1^2 + 25\,x_2^2 - 225\rangle$ has exactly the ellipse as vanishing set.

And now for something completely different.

Dimension, Primary Decomposition

It happens quite often that one is first of all interested in the *dimension* of a variety. Here is an example where the variety contains parts with different dimensions, and it is shown how the dimension is computed.

Example 20. *The ideal $I = \langle (2\,x_1 - x_2 - 2)x_1, (2\,x_1 - x_2 - 2)x_2^2\rangle$ is given. $\boldsymbol{V}(I)$ consists of a line and an isolated point. Using the Hilbert polynomial the dimension is computed (which should be 1).*

```
with(PolynomialIdeals):

I1:=<(2*x[1]-x[2]-2)*x[1], (2*x[1]-x[2]-2)*x[2]^2>;

HilbertDimension(I1,{x[1],x[2]});
```

If a variety contains parts with different dimensions, then the dimension of the whole variety is defined to be the largest of these numbers.

As already mentioned it is possible that an ideal describes a variety which is made up of some simpler varieties, e.g. the variety from the example above. It is the union of a line and an isolated point. The question is how such a decomposition can be found, if there is one.

Definition 16. *A* ***primary decomposition*** *of a given ideal I is an expression of I as an intersection of primary ideals, namely $I = \bigcap_{i=1}^{r} Q_i$. Such a decomposition is called* ***minimal*** *if the radicals $\sqrt{Q_i}$ are all different and $Q_i \not\supseteq \bigcap_{i \neq j} Q_j$. Furthermore if no radical $\sqrt{Q_i}$ is strictly contained in another radical $\sqrt{Q_j}$, then the primary components Q_i are uniquely determined.*
The radicals $\sqrt{Q_i} =: P_i$ are the corresponding prime ideals.

It follows an example where the variety can be decomposed into three different parts.

Example 21. *A rather large ideal J is given.*

$$\begin{aligned} J \;=\; & \langle 4\,{x_3}^2{x_1}^3 + 4\,{x_3}^2x_1{x_2}^2 + 4\,{x_3}^4x_1 - 16\,x_1{x_3}^2 + 5\,{x_3}^2x_2{x_1}^2 + 5\,{x_3}^2{x_2}^3 + \\ & +5\,{x_3}^4x_2 - 20\,x_2{x_3}^2 - 6\,{x_3}^2{x_1}^2 - 6\,{x_3}^2{x_2}^2 - 6\,{x_3}^4 + 24\,{x_3}^2, \\ & 4\,{x_1}^4 + 4\,{x_1}^2{x_2}^2 + 4\,{x_3}^2{x_1}^2 + 2\,{x_1}^2 + 5\,{x_1}^3x_2 + 5\,x_1{x_2}^3 + 5\,x_1x_2{x_3}^2 - \\ & -20\,x_1x_2 - 18\,{x_1}^3 - 18\,x_1{x_2}^2 - 18\,x_1{x_3}^2 + 72\,x_1 - 15\,x_2{x_1}^2 - 15\,{x_2}^3 - \\ & -15\,x_2{x_3}^2 + 60\,x_2 + 18\,{x_2}^2 + 18\,{x_3}^2 - 72\rangle \end{aligned}$$

Using the command

```
PrimaryDecomposition(J);
```

the primary decomposition is computed and the result is

$$Q_1 = \langle 4\,x_1 + 5\,x_2 - 6\rangle \qquad Q_2 = \langle {x_1}^2 + {x_2}^2 + {x_3}^2 - 4\rangle \qquad Q_3 = \langle {x_3}^2, x_1 - 3\rangle$$

which means that $\mathbf{V}(I)$ can be decomposed into a line, a sphere and an isolated point which appears with multiplicity 2.

Such decompositions are quite convenient if the variety has to be intersected with other varieties, because then each of the components can be treated separately. The worst case is that one has to deal with and ideal which is primary or even prime. In this case one has to take the ideal as a whole.

As a final comment is has to be mentioned that it is possible to extend the concept of ideals and varieties to projective spaces. Due to the fact that lots of subtleties appear there, here it is once more referred to the book *"Ideals, Varieties, and Algorithms"* by *David Cox, John Little* and *Donal O'Shea*.