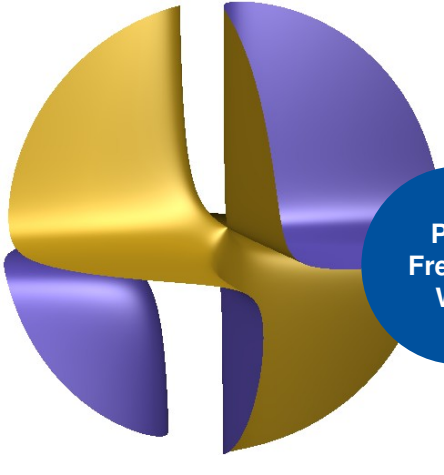
Universität Stuttgart
AG Algorithmik & Symbolisches Rechnen



Groups, Algorithms, Geometries & Applications A

Prof. Frederik Witt

Universität Stuttgart
SoSe 19

Table of contents

For concrete computations we use SINGULAR, a C-based programming language and computer algebra system which is freely available at

`https://www.singular.uni-kl.de/`

The website also provides further documentation and examples, see

`https://www.singular.uni-kl.de/index.php/singular-manual.html`

In these notes, input to SINGULAR will be preceeded by >; output of SINGULAR will be in red:

```
>5*4;
20
```

1. Rings, modules and morphisms

2. Gröbner bases

3. Affine and projective varieties

1. Definition.

(i) A **ring** $(A, +, \cdot)$ consists of an abelian group $(A, +)$ with neutral element 0, and an associative multiplication $\cdot : A \times A \to A$ such that for all $a, b, c \in A$,

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{and} \quad (b + c) \cdot a = b \cdot a + b \cdot c.$$

Furthermore, in this course a ring will always be **commutative and with identity**, i.e., multiplication $\cdot$ is commutative, and there is a neutral element 1 for $\cdot$. A subgroup of a ring A is a **subring** if it contains 1 and is closed under multiplication. A **unit** $u \in A \setminus \{0\}$ is an element such that there exists $u' \in A$ with $uu' = 1$. A ring whose nonzero elements are units is a **field**.

(ii) A **ring morphism** $\varphi : A \to B$ is a group morphism such that $\varphi(1_A) = 1_B$ and $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$. A **ring isomorphism** is a bijective ring morphism (its inverse is then also a ring morphism).

In the sequel, A and k will always denote a ring and a field respectively.

2. Examples. $\mathbb{Z}$, its quotients $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ or fields such as $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$. On the other hand, $\mathbb{N} = \{m \in \mathbb{Z} \mid m \geq 0\}$ is not a ring (it is not even a group).

3. Definition.

(i) Let A be a ring. A set M, together with two operations $+ : M \times M \to M$ (addition) and $\cdot : A \times M \to M$ (scalar multiplication) is called an A–module if $(M, +)$ is an abelian group, and for all $a, b \in A$, $m, n \in M$

- $(a+b) \cdot m = a \cdot m + b \cdot m, \quad a \cdot (m+n) = a \cdot m + a \cdot n$
- $(ab) \cdot m = a \cdot (b \cdot m)$
- $1 \cdot m = m$

(ii) Let M, N be A–modules. A map $\varphi : M \to N$ is called A–**module morphism** or A-**linear** if, for all $a \in A$ and $m, n \in M$

$$\varphi(am) = a\varphi(m), \quad \varphi(m+n) = \varphi(m) + \varphi(n).$$

If $N = M$, then φ is called an **endomorphism**.

(iii) $\mathrm{Hom}_A(M, N)$ denotes the set of all A–module morphisms $M \to N$.

(iv) A bijective A–linear map $\varphi : M \to N$ is called an **isomorphism** (φ^{-1} being automatically A-linear). In this case M and N are **isomorphic**.

4. Example. If A is a ring, then the direct sum (as abelian groups) $A^n = A \oplus \ldots \oplus A$ with the usual scalar action is an A-module.

5. Polynomials over A. A **monomial** in the variables $x_1, \ldots, x_n$ is a formal expression

$$x^\alpha := x_1^{\alpha_1} \ldots x_n^{\alpha_n}, \quad \alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n.$$

The set of monomials $\mathrm{Mon}(x_1, \ldots, x_n) = \{x^\alpha \mid \alpha \in \mathbb{N}^n\}$ forms a semi-group with neutral element $1 = x_1^0 \ldots x_n^0$ via

$$x_1^{\alpha_1} \ldots x_n^{\alpha_n} \cdot x_1^{\beta_1} \ldots x_n^{\beta_n} = x_1^{\alpha_1+\beta_1} \ldots x_n^{\alpha_n+\beta_n}.$$

The **degree** of x^α is the sum $|\alpha| = \alpha_1 + \ldots + \alpha_n$. A **polynomial over A in the variables** $x_1, \ldots, x_n$ is a finite linear combination of monomials x^α over A:

$$f = \sum_{\alpha=(\alpha_1,\ldots,\alpha_n)} a_\alpha x_1^{\alpha_1} \ldots x_n^{\alpha_n}, \quad a_\alpha \in A.$$

The **support** of f is the set $\operatorname{supp} f = \{x^\alpha \mid a_\alpha \neq 0\}$. For $f \neq 0$ the degree of f is the maximum $\deg(f)$ of all $|\alpha|$, $x_\alpha \in \operatorname{supp} f$; by convention, we put $\deg 0 = -1$.

$$A[x_1, \ldots, x_n] = \text{ set of } \textbf{polynomials in } n \textbf{ variables}.$$

6. Ring structure on the polynomials. A **term** is a polynomial of the form ax^α. The ring structure on $A[x_1, \ldots, x_n]$ is defined as follows:

$$\sum a_\alpha x^\alpha + \sum b_\alpha x^\alpha := \sum (a_\alpha + b_\alpha) x^\alpha$$
$$\Big(\sum a_\alpha x^\alpha\Big) \cdot \Big(\sum b_\alpha x^\alpha\Big) := \sum_\gamma \Big(\sum_{\alpha+\beta=\gamma} a_\alpha b_\beta \Big) x^\gamma.$$

If we identify $1 \in A$ with $1 = x^0$, then $A \subset A[x_1, \ldots, x_n]$ as a subring (with the obvious definitions). The elements of $A \subset A[x_1, \ldots, x_n]$ will be called **constant polynomials**, and A is the **base ring**. In particular, this gives $A[x_1, \ldots, x_n]$ the structure of an A-module for which $\mathrm{Mon}(x_1, \ldots, x_n)$ provides a basis.

7. Definition. Let A be a ring. An A-**algebra** is a ring B which contains A as a subring. Let B and C be two A-algebras. A ring morphism $\varphi : B \to C$ is called an A-**algebra morphism** if $\varphi(a) = a$ for all $a \in A$, i.e., $\varphi|_A = \mathrm{Id}_A$. More generally, if $\varphi : A \to B$ and $\psi : A \to C$ are two ring maps, then a ring map $\alpha : B \to C$ is an A–algebra morphism if $\alpha \circ \varphi = \psi$, that is, α is an A-algebra morphism with respect to the A-algebra structure on B and C induced by $\varphi(a) \cdot b$ and $\psi(a) \cdot b$.

8. Remark. In fact, if B is an A-algebra via the ring morphism $\varphi : A \to B$, $\varphi(a) \cdot b$ turns B into an A-module. Hence any A-algebra is also an A-module (the converse being false), for instance $A[x_1, \ldots, x_n]$. Similarly, any abelian group (which is a $\mathbb{Z}$-algebra) is a $\mathbb{Z}$-module. Moreover, an A-algebra morphism is an A-linear map.

9. Example. Let k be a field. Then we have a natural ring morphism $\varphi : \mathbb{Z} \to k$ defined by $1 \in \mathbb{Z} \mapsto 1 \in k$, i.e., k is a $\varphi(\mathbb{Z})$-algebra. Note that the kernel $\ker\varphi$ is either trivial, or there exists a unique positive prime $p \in \mathbb{Z}$ which divides any element in $\ker\varphi$ (cf. Remark 22). We call p the **characteristic of** k and write $p = \operatorname{char} k$. For instance, $\operatorname{char} \mathbb{Q} = 0$ while $\operatorname{char} \mathbb{Z}_p = p$.

10. Proposition [EH, Thm. 1.1]. *Let B be an A-algebra, and let $\alpha_1, \ldots, \alpha_n \in B$. Then there exists a unique A-algebra morphism $\varphi : A[x_1, \ldots, x_n] \to B$ determined by $\varphi(x_i) = \alpha_i$, the so-called* **substitution morphism**.

11. Proposition [EH, Thm. 1.3]. *There is a natural A-algebra isomorphism $A[x_1, \ldots, x_{n-1}, x_n] \cong A[x_1, \ldots, x_{n-1}][x_n]$.*

Definition of polynomial base rings 1 [GP, 1.1.9]

```
> ring A1=0,x,dp; //defines the ring ℚ[x]: characteristic 0, x the
variable, dp= degree reverse lexicographical ordering on Mon(x_1,...,x_n)
(see below)
> poly f=2/3x3+5x2+1/7x+2/5;
> poly g=1/3x4+2/9x+2/3;
> f*g;
2/9x7+5/3x6+1/21x5+38/135x4+14/9x3+212/63x2+58/315x+4/15
```

Definition of polynomial base rings 2 [GP, 1.1.9]

```
> ring A2=(7,a,b),(x,y,z),dp; //defines the ring ℤ_7(a,b)[x,y,z] with
degree reverse lexicographical ordering. It has characteristic 7,
invertible parameters a, b, and variables x, y, z
> poly f=2ax3y2z+(1/b)*x2z+xyz+2;
> poly g=3xy4z2+2xyz+3bx;
> f*g;
(-a)*x4y6z3+3/(b)*x3y4z3+3*x2y5z3+(-3a)*x4y3z2+(-ab)*x4y2z-
xy4z2+2/(b)*x3yz2+2*x2y2z2+3*x3z+(3b)*x2yz-3*xyz+(-b)*x
```

Definition of algebra morphisms [GP, 1.1.10]

```
> ring A=0,(a,b,c),dp; //defines the ring ℚ[a,b,c] with degree reverse lexicographical ordering
> poly f=a+b+ab+c3+5;
> ring B=0,(x,y,z),dp; //new basering B; if we do not specify otherwise, all computations now take place in B
> map F=A,x+y,x-y,z; //map F : A → B defined by a ↦ x + y, b ↦ x − y, c ↦ z
> poly g=F(f); //apply F to f
> g;
z3+x2-y2+2x+5
```

IMAP and FETCH [GP, 1.1.10]

```
> ring C=0,(x,y,c,b,a,z),dp; //defines the ring ℚ[x,y,z,a,b,c]
> imap(A,f); //"identity map" from A → C preserving the names of the variables, but displaying f with respect to the new ordering
c3+ba+b+a+5
> fetch(A,f); //fetch preserves order of variables
c3+xy+x+y+5
```

12. Definition.

(i) A subset $I \subset A$ is an **ideal** if it is an abelian subgroup and $a \in A$, $f \in I$ implies $a \cdot f \in I$, that is, I is an A-module. The ideal **generated** $I = (f_\lambda)_{\lambda \in \Lambda}$ by the subset $\{f_\lambda \mid \lambda \in \Lambda\}$ of A is the set of finite linear combinations of the f_λ, i.e.

$$I = (\{\sum_{\text{finite}} a_i f_i \mid i \in \Lambda,\ a_i \in A\}).$$

(this is indeed an ideal). If Λ is a finite set, then we call I **finitely generated**.

(ii) The **null ideal** is the ideal $(0) = \{0\}$ generated by 0. If an ideal is generated by one element it is called a **principal ideal**.

(iii) If I and J are two ideals of A, then $I + J$ and $I \cdot J$ are the ideals generated by $\{a + b \mid a \in I,\ b \in J\}$ and $\{a \cdot b \mid a \in I,\ b \in J\}$, respectively.

13. Example. Let $\varphi : A \to B$ be a ring morphism,and $J \subset B$ be an ideal. Then its preimage or **contraction** $\varphi^{-1}(J)$ is an ideal. In particular, $\ker\varphi = \varphi^{-1}((0))$ is an ideal. φ is **injective**, if $\ker\varphi = (0)$. On the other hand, if I is an ideal in A, then $\varphi(I)$ is merely a subring of B, but not an ideal in general. The **extension of I by** φ is the ideal generated by $\varphi(I)$. It is written $\varphi(I) \cdot B$.

Injectivity of ring morphisms [GP, 1.3.3]

```
> ring A=0,(a,b,c),dp; //defines A = Q[a,b,c]
> ring B=0,(x,y,z),dp; //defines B = Q[x,y,z] which is the base ring
> ideal I=x,y,x2-y3; //defines the ideal I = (x,y,x2 - y3) ⊂ B
> I;
I[1]=x
I[2]=y
I[3]=-y3+x2
> map phi=A,I; //defines φ : A → B, φ(a) = x; φ(b) = y, φ(c) = x^2 - y^2
> LIB "algebra.lib"; //loads additional library
// ** loaded /usr/bin/../share/singular/LIB/algebra.lib
⋮
> is_injective(phi,A);
0 //φ : A → B is not injective
> ideal J=x,x+y,z-x2+y3; //defines the ideal J ⊂ B
> map psi=A,J; //ψ : A → B
> is_injective(psi,A);
1 //ψ : A → B is injective
```

Computing the kernel of ring morphisms [GP, 1.3.3]

```
> alg_kernel(phi,A,"ker"); //defines the ideal ker ⊂ A and computes
generators
b3-a2+c
> setring A; //Since B is the basering we need first to set A as base
ring if we want to work with ideals in A
> ker; //print generators of the ideal ker ⊂ A
ker[1]=b3-a2+c
> setring B;
> alg_kernel(phi,A); //short version of alg_kernel
b3-a2+c
> alg_kernel(psi,A);
0
> ideal Z; //defines the zero ideal in B
> Z;
Z[1]=0
```

Surjectivity of ring morphisms [GP, 1.3.3]

```
> setring A; //we can now compute ideals in A
> preimage(B,phi,Z); //computes the preimage of φ, i.e., generators of
the ideal φ^{-1}(Z) = kerφ ⊂ A
_[1]=b3-a2+c
> ideal P=preimage(B,phi,Z); //defines the ideal P ⊂ A as the preimage
φ^{-1}(0)
> P;
P[1]=b3-a2+c
> setring B; //sets B as base ring, we can now deal with ψ : A → B
> psi;
psi[1]=x
psi[2]=x+y
psi[3]=y3-x2+z
> is_surjective(psi,A);
1 //ψ : A → B is surjective
> is_bijective(psi,A); //ψ : A → B is surjective
1 //ψ : A → B is injective
```

Remark on the base rings in SINGULAR

If we are working with several rings and work with an ideal I inside some ring A, the latter must be the base ring; if necessary, use the command

```
setring A.
```

The command `basering` prints the current base ring. If we are given generators of an ideal $I \subset B$ we can define a ring morphism $\phi : A \to B$ via the command

```
map phi=A,I
```

provided B is the base ring – morphisms are regarded as target space objects. This command maps the variables of the domain ring to the generators of the ideal. If there are less generators of the ideal than variables of the domain ring, then the remaining variables are mapped to 0. If there are more generators of the ideal than variables in the domain ring, the addtional generators are ignored. So we always specify the map and the domain ring, the target ring being the base ring. As another example in the code above,

```
is_bijective(phi,A)
```

tests if a given morphism ϕ from A to the base ring is bijective.

14. Remark [EH, Exercise 1.5]. If $I = (f_1, \ldots, f_r)$ and $J = (g_1, \ldots, g_s)$ are two finitely generated ideals, then so are $I + J$ and $I \cdot J$ with

$$I + J = (f_1, \ldots, f_r, g_1, \ldots, g_s), \quad I \cdot J = (f_i g_j \mid i = 1, \ldots, r, j = 1, \ldots, s).$$

15. Definition and Proposition. Let $I \subset A$ be an ideal. Then $a \sim b$ if and only if $a - b \in I$ defines an equivalence relation on A with equivalence class $\bar{a}$. The quotient ring A/I is the ring on the coset space $\{\bar{a} \mid a \in A\}$ with the following operations:

- $\bar{a} + \bar{b} := \overline{a + b}$
- $\bar{a} \cdot \bar{b} := \overline{a \cdot b}$

In particular, the **projection** or **quotient map** $\pi_I : A \to A/I$, $\pi_I(a) = \bar{a}$ becomes a surjective ring A-algebra morphism. Moreover, the scalar multiplication $a \cdot \bar{b} := \overline{a \cdot b}$ turns A/I into an A-module.

16. Example. In $\mathbb{Q}[x, y]/(x^2, xy)$ we have $\bar{x}^2 = 0$ and $\bar{x} \cdot \bar{y} = 0$. For instance, $\overline{5x^2y + 3x^4 + 1 + y} \cdot \overline{2x + xy + 7y^3} = \overline{1 + y} \cdot \overline{2x + 7y^3} = 2\bar{x} + 7\bar{y}^3 + 7\bar{y}^4$.

17. Comparison Lemma $A \leftrightarrow A/I$**.**

(i) *A ring morphism* $\varphi : A \to B$ *induces an isomorphism* $A/\ker\varphi \cong \operatorname{Im} B$*. In particular,* B *is a ring isomorphic to* A/I*,* I *ideal of* A*, if* φ *is surjective.*

(ii) *The map* $J \mapsto \pi_I(J)$ *induces a bijection*

$$\{\text{ideals in } A \text{ containing } I\} \longleftrightarrow \{\text{ideals in } A/I\}$$

whose inverse assigns to $J \subset A/I$ *the ideal* $\pi_I^{-1}(J)$ *in* A*.*

18. Definition.

(i) An element $a \in A$ is a **zero divisor** if there exists $b \in A \setminus \{0\}$ such that $ab = 0$.

(ii) A ring A which has only 0 as a zero divisor is called an **integral domain**.

(iii) A **principal ideal ring** is a ring for which any ideal is principal; it is a **principal ideal domain** if it is in addition an integral domain.

19. Example. $\mathbb{Z}$ is an integral domain. Further, it is easy to see that if A is an integral domain, then so is the polynomial ring $A[x]$. By recursion, any polynomial ring $A[x_1, \ldots, x_n]$ is integral. On the other hand, quotients of integral domains are usually not integral. Consider, for instance, the ideal $I = (f \cdot g)$. Then $\bar{f}, \bar{g} \neq 0$, but $\overline{fg} = 0$.

20. Definition. A proper ideal $I \subsetneq A$ is **prime** if $f \cdot g \in I$ implies $f \in I$ or $g \in I$, and **maximal**, if $I \subset I' \subsetneq A$ implies $I = I'$.

21. Lemma [GP, 1.3.11].

(i) *$I \subset A$ is prime if and only if A/I is an integral domain.*

(ii) *$I \subset A$ is maximal if and only if A/I is a field. In particular, a maximal ideal is prime.*

22. Remark.

(i) If $\varphi : A \to B$ is a ring morphism, and $J \subset B$ a prime ideal, then so is its contraction $\varphi^{-1}(J)$. On the other hand contractions of maximal ideals are not necessarily maximal (consider the inclusion $\mathbb{Z} \to \mathbb{Q}$ and $(0) \subset \mathbb{Q}$).

(ii) Consider the canonical $\mathbb{Z}$-algebra structure of a field k (cf. Example 9). The image of $\varphi : \mathbb{Z} \to k$ is an integral ring and is isomorphic with $\mathbb{Z}/\ker\varphi$, so that $\ker\varphi$ is a prime ideal. It is therefore equal to the trivial ideal or the principal ideal of a prime in $\mathbb{Z}$.

23. Lemma [GP, 1.3.12].

(i) *Let P, I, $J \subset A$ be ideals with P prime. If $I \not\subset P$, $I \cdot J \subset P$, then $J \subset P$.*

(ii) *Let P, $I_1, \ldots, I_n \subset A$ be ideals with P prime and $\bigcap_{i=1}^n I_i \subset P$ (resp. $=$). Then $I_j \subset P$ (resp. $=$) for some j.*

(iii) *(Prime avoidance) Let $P_1, \ldots, P_n$, $I \subset A$ be ideals with P_i prime and $I \subset \bigcup_{i=1}^n P_i$. Then $I \subset P_j$ for some j.*

Definition of quotient rings and testing for equality [GP, 1.3.13]

```
> ring A=0,(x,y,z),dp;
> ideal I=x2+y2-z5,z-x-y2;
> I;
I[1]=-z5+x2+y2
I[2]=-y2-x+z
> std(I); //computes a particularly nice generating system ("Gröbner"
or "standard base") of I - we will explain this in greater detail
later
_[1]=y2+x-z
_[2]=z5-x2+x-z
> qring Q=std(I); //defines the quotient ring Q = A/I where I must be
specified via a Gröbner base, and sets Q as current base ring again
whose variables are still denoted x, y and z
> poly f=z2+y2;
> poly g=z2+2x-2z-3z5+3x2+6y2; //elements of Q
> reduce(f-g,std(0)); //computes the remainder of the division of f − g
by the Gröbner base of (0̄); this is zero if and only if f̄ = ḡ
0
```

24. Definition. A **monomial ideal** of $k[x_1, \ldots, x_n]$ is an ideal generated by monomials.

25. Proposition [EH, 1.7]. *For an ideal $I \subset k[x_1, \ldots, x_n]$ are equivalent:*

(i) *I is monomial.*

(ii) *For any $f \in I$ one has $\operatorname{supp} f \subset I$.*

26. Corollary [EH, 1.8]. *Let $I \subset k[x_1, \ldots, x_n]$ be a monomial ideal, and G a set of monomials in I. Then G is a set of generators of I if and only if for each monomial $v \in I$ there exists $u \in G$ such that $u|v$.*

27. Remark. On the subset of monomials $\mathrm{Mon}(x_1, \ldots, x_n) \subset k[x_1, \ldots, x_n]$ we have the following **natural partial order**: $\alpha \leq_{nat} \beta$, $\alpha, \beta \in \mathbb{N}^n$, if and only if $\alpha_i \leq \beta_i$ for all $i = 1, \ldots, n$. Equivalently, $\alpha \leq_{nat} \beta$ if and only if $x^\alpha | x^\beta$, i.e., x^α divides x^β.

28. Theorem (Dickson's Lemma) [EH, 1.9], [GP, 1.2.6]. *Let $\emptyset \neq M \subset \mathrm{Mon}(x_1, \ldots, x_n)$. Then there is a finite subset $B \subset M$ such that for all $x^\alpha \in M$ there exists $x^\beta \in B$ with $x^\beta \leq_{nat} x^\alpha$.*

29. Corollary (Hilbert's Basissatz for monomial ideals) [EH, 1.10]. *Let $I \subset k[x_1, \ldots, x_n]$ be a monomial ideal. Then any subset of generators of I has a finite subset generating I.*

30. Definition. Let I be a monomial ideal. A subset G of monomial generators is **minimal** if any proper subset of G does not generate I any longer.

31. Proposition [EH, 1.11]. *Any monomial ideal I has a unique minimal set of monomial generators, the so-called* **minimal basis** *which is denoted by $G(I)$.*

32. Remark. If I and J are monomial ideals, then so are $I + J$ and $I \cdot J$. We have

$$G(I + J) \subset G(I) \cup G(J) \quad \text{and} \quad G(I \cdot J) \subset G(I)G(J)$$

for their minimal bases.

33. Corollary [EH, 1.12]. *Each ascending sequence of monomial ideals* $I_1 \subset I_2 \subset I_3 \subset \ldots$ *in* $k[x_1, \ldots, x_n]$ *eventually becomes stationary, that is, there exists a* $k \in \mathbb{N}$ *such that* $I_k = I_{k+1} = I_{k+2} = \ldots$.

34. Definition. A ring A is called **Noetherian** if any ascending sequence of ideals eventually becomes stationary.

35. Example.

(i) Every principal ideal ring such as $\mathbb{Z}$ or $k[x]$ is Noetherian.

(ii) Hilbert's celebrated basis theorem states that $k[x_1, \ldots, x_n]$ is Noetherian (see below). More generally, if A is Noetherian, then so is $A[x]$.

We pass to modules next and consider further examples of modules and morphisms between them.

36. Lemma and Definition [GP, 2.1.4]. *We can define an A-module structure on $\mathrm{Hom}_A(M,N)$ by*

$$(\varphi+\psi)(m) := \varphi(m)+\psi(m)$$
$$(a\varphi)(m) := a\cdot\varphi(m).$$

In particular, $M^\vee := \mathrm{Hom}_A(M,A)$ is an A-module, the so-called **dual module**.

37. Remark [GP, 2.1.5]. If M, N and L are A-modules, and $\varphi : M \to N$ is A-linear, then

$$\Phi : \mathrm{Hom}_A(N,L) \to \mathrm{Hom}_A(M,L), \quad \Phi(\lambda) := \lambda\circ\varphi$$

and

$$\Psi : \mathrm{Hom}_A(L,M) \to \mathrm{Hom}_A(L,N), \quad \Psi(\lambda) := \varphi\circ\lambda$$

are A-linear for the natural A-module structure on Hom.

Matrix operations 1 [GP, 2.1.6]

```
> ring A = 0,(x,y,z),dp;
> matrix M[2][3] = 1, x+y, z2, x, 0, xyz; //2x3 matrix. Note that for
SINGULAR matrices have polynomial entries, hence we need to specify
a base ring
> matrix N[3][3] = 1,2,3,4,5,6,7,8,9; //3x3 matrix
> M; //lists all entries of M
M[1,1]=1
M[1,2]=x+y
M[1,3]=z2
M[2,1]=x
M[2,2]=0
M[2,3]=xyz
> print(N); //displays N as usual if the entries are small
1,2,3,
4,5,6,
7,8,9
```

Matrix operations 2 [GP, 2.1.6]

```
> print(M+M); //addition of matrices
2, 2x+2y,2z2,
2x,0,2xyz
> print(x*N); //scalar multiplication
x, 2x,3x,
4x,5x,6x,
7x,8x,9x
> print(M*N); //multiplication of matrices
7z2+4x+4y+1,8z2+5x+5y+2,9z2+6x+6y+3,
7xyz+x, 8xyz+2x, 9xyz+3x
> M[2,3]; //access to single entry
xyz
> M[2,3]=37; //change single entry
> print(M);
1,x+y,z2,
x,0, 37
```

Matrix libraries 1 [GP, 2.1.6]

```
> LIB "matrix.lib"; LIB "inout.lib"; //libraries for matrix operations
> print(power(N,3)); //exponentiation of matrices
468, 576, 684,
1062,1305,1548
1656,2034,2412
> matrix K = concat(M,N); //concatenation of matrices; number of rows
of result matrix is max(nrows(A1),nrows(A2),...)
> print(K);
1,x+y,z2,1,2,3,
x,0, 37,4,5,6,
0,0, 0, 7,8,9
```

Matrix libraries 2 [GP, 2.1.6]

```
> ideal(M); //converts matrix to ideal by taking the entries as
generators
_[1]=1
_[2]=x+y
_[3]=z2
_[4]=x
_[5]=0
_[6]=37
> print(unitmat(5)); //5x5 unit matrix
1,0,0,0,0,
0,1,0,0,0,
0,0,1,0,0,
0,0,0,1,0,
0,0,0,0,1,
```

38. Definition.

(i) Let M be an A-module. An abelian subgroup N of M is an A-**submodule** of M if it is closed under scalar multiplication of A, i.e., for all $a \in A$, $n \in N$ we have $a \cdot n \in N$.

(ii) If $N \subset M$ is an A-submodule we define the quotient module M/N as the set of equivalence classes $\overline{m} = \overline{m+n}$ for $m \in M$, $n \in N$. This is again an A-module (cf. the case of A/I discussed above). Indeed, $\overline{m} + \overline{m'} = \overline{m+m'}$ and $a \cdot \overline{m} = \overline{a \cdot m}$ are well-defined operations on M/N turning it into an A-module.

39. Example. Let $\varphi : M \to N$ be an A-module morphism. The **kernel** $\ker\varphi := \{m \in M \mid \varphi(m) = 0\}$ and the **image** $\mathrm{im}\varphi := \{n \in N \mid n = \varphi(m) \text{ for some } m \in M\}$ are A-submodules of M and N respectively. The **cokernel** $\mathrm{coker}\varphi = N/\mathrm{im}\varphi$ is a quotient module.

Submodules of A^n [GP, 2.1.10]

```
> ring A=0,(x,y,z),dp;
> module M=[xy-1,z2+3,xyz],[y4,x3,z2]; //submodule in A^3
> M; //gives the generating vectors with respect to the canonical basis gen(i) = e_i of A^3
M[1]=xyz*gen(3)+xy*gen(1)+z2*gen(2)+3*gen(2)-gen(1)
M[2]=y4*gen(1)+x3*gen(2)+z2*gen(3)
> ideal I=x2+y2+z2;
> qring Q=std(I); //creates quotient ring A/I
> module M=fetch(A,M); //maps M from A-modules to Q = A/I-modules
> vector s1=[x2,y3,z];
> vector s2=[0,x2-y2,z];
> poly f=xyz;
> module N=s1,f*s2; //alternative definition of a module (over the current base ring Q)
> N;
N[1]=y3*gen(2)+x2*gen(1)+z*gen(3)
N[2]=x3yz*gen(2)-xy3z*gen(2)+xyz2*gen(3)
```

Kernel and image of module morphisms [GP, 2.1.13]

```
> ring A=0,(x,y,z),(c,dp); //(c, dp) specifies how to order monomials
of the module, see below. It also implies that vectors are represented
componentwise
> matrix M[2][3]=x,xy,z,x2,xyz,yz;
> module Ker=syz(M); //syz computes the kernel of M (in fact
the first syzygy, see below); it is a generalization of Gaussian
elimination from fields to rings
> Ker;
Ker[1]=[y2z-yz2,xz-yz,-x2y+xyz]
> vector k=[y2z-yz2,xz-yz,-x2y+xyz];
> M*k;
_[1,1]=0
_[2,1]=0
> module Im=M[1],M[2],M[3];
> Im;
Im[1]=[x,x2]
Im[2]=[xy,xyz]
Im[3]=[z,yz]
```

40. Proposition [GP, 2.1.16]. *Let $\varphi : M \to N$ be an A-module morphism. Then*

$$M/\ker\varphi \cong \operatorname{im}\varphi.$$

In analogy to the cokernel one also calls $M/\ker\varphi$ the **coimage** *of φ. The isomorphism then reads $\operatorname{coim}\varphi \cong \operatorname{im}\varphi$. In particular, given A-modules $N \subset M \subset L$, we have*

$$(L/N)/(M/N) \cong L/M.$$

41. Definition.

(i) Let M be an A-module with submodules M_λ. $\lambda \in \Lambda$. Then the **sum** of the M_λ is defined by

$$\sum_{\lambda\in\Lambda} M_\lambda := \{\sum_{\lambda\in\Lambda} m_\lambda \mid m_\lambda \in M_\lambda,\ m_\lambda \neq 0 \text{ only for finitely many } \lambda\} \subset M$$

and their **intersection** by $\bigcap_{\lambda\in\Lambda} M_\lambda \subset M$

(ii) Let $I \subset A$ be an ideal and M an A-module. We define IM by

$$IM := \{ \sum_{\text{finite}} a_i m_i \mid a_i \in I,\ m_i \in M \}.$$

(iii) The **direct sum** is the module (with the obvious operations)

$$\bigoplus_{\lambda \in \Lambda} M_\lambda = \{ (m_\lambda)_{\lambda \in \Lambda} \mid m_\lambda \in M_\lambda,\ m_\lambda \neq 0 \text{ for only finitely many } \lambda \}$$

The **direct product** is the module (with the obvious operations)

$$\prod_{\lambda \in \Lambda} M_\lambda = \{ (m_\lambda)_{\lambda \in \Lambda} \mid m_\lambda \in M_\lambda \}.$$

For a finite index set these notions coincide. We write $M_1 \oplus \ldots \oplus M_n$.

(iv) A module M which is isomorphic with the direct sum $\bigoplus_{\lambda \in \Lambda} A$ is called a **free** module (e.g., $A[x_1, \ldots, x_n]$). By convention, $M = (0)$ if $\Lambda = \emptyset$. The cardinality of Λ is the **rank** of M. A subset S of M is called a **basis**, if every $m \in M$ is a finite linear combination of elements in S in a unique way.

(v) An A-module M is **finitely generated** if there exists $m_1, \ldots, m_r \in M$ such that any $m \in M$ is a linear combination of the **generators** m_i. We write $M = \langle m_1, \ldots, m_r \rangle$. A module is **cyclic** if it is generated by one element (e.g., a principal ideal).

(vi) The **torsion submodule** of an A-module M is defined by

$$\mathrm{Tors}(M) := \{m \in M \mid am = 0 \text{ for some non zerodivisor } a \in A\}.$$

M is **torsionfree** if $\mathrm{Tors}(M) = 0$, and a **torsion module** if $\mathrm{Tors}(M) = M$.

(vii) Let N, $P \subset M$ be submodules. The **ideal quotient** $N : P$ is defined by

$$N : P := \{a \in A \mid aP \subset N\}.$$

If $N = 0$ then $\mathrm{Ann}(P) := (0 : P)$ is called the **annihilator** of P.

42. Remark. The ring of polynomials $A[x]$ is isomorphic to the direct sum $\bigoplus_{i=0}^{\infty} A$, where the sequence $(a_0, a_1, \ldots)$ is sent to the polynomial $\sum_{i=0}^{\infty} a_i x^i$. Since only finitely many a_i are different from zero we get a well-defined polynomial. On the other hand, the direct product $\prod_{i=0}^{\infty} A$ yields the ring $A[\![x]\!]$ of **formal power series**.

Operation on modules 1 [GP, 2.1.20]

```
> ring A=0,(x,y,z),(c,dp);
> module M=[xy,xz],[x,x];
> module N=[y2,z2],[x,x];
> M+N; //sum of two ideals
_[1]=[xy,xz]
_[2]=[x,x]
_[3]=[y2,z2]
> intersect(M,N); //intersection of two modules
_[1]=[x,x]
_[2]=[xy2,xz2]
> quotient(M,N); //quotient M:N as submodules of A^n
_[1]=x
> quotient(N,M); //quotient N:M as submodules of A^n
_[1]=y+z
```

Operation on modules 2 [GP, 2.1.20]

```
> qring Q=std(x5);
> module M=fetch(A,M);
> module Null; //the trivial module
> M;
M[1]=[xy,xz]
M[2]=[x,x]
> Null;
Null[1]=0
> quotient(Null,M); //the annihilator of M
_[1]=x4
```

43. Remark. The sum of submodules of an A–module, the product of an ideal with an A–module, the direct sum and the direct product of A–modules are again A–modules. The module quotient of two submodules of an A–module is an ideal in A. The quotient of a submodule by an ideal is a submodule of M. The torsion module $\mathrm{Tors}(M)$ is a submodule of M.

44. Proposition [GP, 2.1.21]. *Let M be an A-module and $N_1, N_2 \subset M$ be submodules, then*

$$(N_1 + N_2)/N_1 \cong N_2/(N_1 \cap N_2).$$

45. Lemma [GP, 2.1.22]. *Let M be an A-module. M is finitely generated if and only if $M \cong A^n/L$ for some $n \in \mathbb{N}$ and a submodule $L \subset A^n$. Equivalently, there exists a surjective homomorphism $\varphi : A^n \twoheadrightarrow M$.*

46. Definition. Let M be an A-module. Then M is called **Noetherian** if every A-submodule of M is finitely generated. In particular, A is a Noetherian ring if and only if it is Noetherian as an A-module over itself.

47. Lemma [GP, 2.1.28].

(i) *Submodules and quotient modules of Noetherian modules are Noetherian.*

(ii) *Let $N \subset M$ be A–modules, then M is Noetherian if and only if N and M/N are Noetherian.*

(iii) *Let M be an A–module, then the following properties are equivalent:*

- *M is Noetherian.*
- *Every ascending chain of submodules $M_1 \subset M_2 \subset \ldots \subset M_k \subset \ldots$ becomes stationary.*
- *Every non–empty set of submodules of M has a maximal element with respect to inclusion.*

The same holds for Noetherian rings and ideals instead of Noetherian modules and submodules.

48. Proposition [GP, 2.1.29]. *Let A be a Noetherian ring and M be a finitely generated A-module, then M is a Noetherian A-module.*

49. Lemma (Nakayama) [GP, 2.1.30]. *Let A be a ring and I be an ideal contained in the* **Jacobson ideal** *of A, i.e., the intersection of all maximal ideals of A. If M is a finitely generated A-module and N a submodule of M such that $M = IM + N$, then $M = N$. In particular, if $M = IM$, then $M = 0$.*

50. Corollary [GP, 2.1.31]. *Let $(A, \mathfrak{m})$ be a* **local ring**, *that is, $\mathfrak{m}$ is the only maximal ideal. Further, let M be a finitely generated A-module. If $m_1, \ldots, m_n \in M$ induce generators of the $A/\mathfrak{m}$-vector space $M/\mathfrak{m}M$, then they also generate M.*

1. Rings, modules and morphisms

2. Gröbner bases

3. Affine and projective varieties

The advantage of working with monomial ideals lied in the existence of a canonical generating set, namely the minimal basis $G(I)$. Formalising this idea gives rise to Gröbner bases.

51. Definition. A **monomial ordering** is a total ordering $<$ on $\mathrm{Mon}(x_1, \ldots, x_n)$ such that

$$x^\alpha < x^\beta \Longrightarrow x^\gamma x^\alpha < x^\gamma x^\beta$$

for all α, β and $\gamma \in \mathbb{N}^n$. A monomial ordering $<$ is called **global** resp. **local** if $x^\alpha > 1$ resp. $x^\alpha < 1$ for all $\alpha \in \mathbb{N}^n \setminus \{0\}$.

52. Remark.

(i) If we consider 0 as a monomial we set $0 < x^\alpha$ for all α.

(ii) All orderings we will consider in this course are global in view of the important characterisation below (Lemma 56). Still, local orderings have important applications in geometry. One should think of these as a device of implementing negative exponents, that is, of inverting monomials, leading to the *localisation* of a polynomial ring. This is an important idea in commutative algebra and algebraic geometry, whence the name of local ordering. See for instance [GP, Chapter 1.4] for an elementary introduction.

53. Examples of global orderings.

(i) **lexicographical ordering** $>_{lp}$:

$$x^\alpha >_{lp} x^\beta \Leftrightarrow \alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1}, \alpha_i > \beta_i$$

(ii) **Degree reverse lexicographical ordering** $>_{dp}$:

$$x^\alpha >_{dp} x^\beta \Leftrightarrow \deg x^\alpha > \deg x^\beta \text{ or if } \deg x^\alpha = \deg x^\beta$$
$$\text{then } \alpha_n = \beta_n, \ldots, \alpha_{i+1} = \beta_{i+1}, \alpha_i < \beta_i$$

(iii) **Degree lexicographical ordering** $>_{Dp}$:

$$x^\alpha >_{Dp} x^\beta \Leftrightarrow \deg x^\alpha > \deg x^\beta \text{ or if } \deg x^\alpha = \deg x^\beta$$
$$\text{then } \alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1}, \alpha_i > \beta_i$$

54. Remark. Let $>$ be a general ordering. Define $>'$ by $x^\alpha >' x^\beta$ if and only if $x^\alpha < x^\beta$. Then $>$ is global if and only if $>'$ is local.

Global monomial orderings

```
> ring A=0,(x,y,z),lp; //A = ℚ[x,y,z] with lexicographical ordering
> poly f=x3yz+y5+z4+x3+xy2;
> f;
x3yz+x3+xy2+y5+z4
> ring B=0,(x,y,z),dp; //B = ℚ[x,y,z] with degree reverse lexicographical ordering
> poly g=imap(A,f);
> g;
y5+x3yz+z4+x3+xy2
> ring C=0,(x,y,z),Dp; //C = ℚ[x,y,z] with degree lexicographical ordering
> poly h=imap(A,f);
> f;
x3yz+y5+z4+x3+xy2
```

Once we have fixed an ordering, we can give a definite representation of a polynomial $0 \neq f \in k[x_1, \ldots, x_n]$ as a sum of non-zero terms

$$f = a_{\alpha_1} x^{\alpha_1} + \ldots + a_{\alpha_r} x^{\alpha_r}, \quad x^{\alpha_1} > \ldots > x^{\alpha_r}.$$

55. Definition.

(i) The **leading monomial** of f is $\mathrm{LM}(f) = x^{\alpha_1}$.

(ii) The **leading exponent** of f is $\mathrm{LE}(f) = \alpha_1$.

(iii) The **leading term** of f is $\mathrm{LT}(f) = a_{\alpha_1} x^{\alpha_1}$.

(iv) The **leading coefficient** of f is $\mathrm{LC}(f) = a_{\alpha_1} \in k$.

(v) The **tail** of f is $\mathrm{tail}(f) = f - \mathrm{LT}(f) = a_{\alpha_2} x^{\alpha_2} + \ldots + a_{\alpha_r} x^{\alpha_r}$.

By convention we set $\mathrm{LM}(0) = 0$.

From now on we will fix some ordering $>$ on $\mathrm{Mon}(x_1, \ldots, x_n)$ **which will be global** unless mentioned otherwise (we shall write sometimes global ordering for emphasis).

Leading data of a polynomial

```
> ring A=0,(x,y,z),lp; //A = ℚ[x,y,z] with lexicographical ordering
> poly f=y4z3+2x2y2z2+3x5+4z4+5y2;
> f;
3x5+2x2y2z2+y4z3+5y2+4z4 //displays f according to the lexicographical
ordering
> leadmonom(f); //leading monomial
x5
> lead(f); //leading term
3x5
> leadexp(f); //leading exponent
5,0,0
> leadcoef(f); //leading coefficient
3
```

56. Lemma [GP, 1.2.5]. *Are equivalent:*

(i) $>$ *is a well ordering, i.e., every* $\emptyset \neq S \subset \mathrm{Mon}(x_1, \ldots, x_n)$ *has a least element* x^β *(this means that for all* $x^\alpha \in S$ *we have* $\alpha = \beta$ *or* $x^\alpha > x^\beta$*).*

(ii) $x_i > 1$ *for* $i = 1, \ldots, n$*.*

(iii) $x^\alpha > 1$ *for all* $\alpha \neq (0, \ldots, 0)$*, that is,* $>$ *is global.*

(iv) $x^\alpha \geq_{nat} x^\beta$ *and* $\alpha \neq \beta$ *implies* $x^\alpha > x^\beta$*.*

The well-ordering property immediately yields the

57. Corollary. *Let* $>$ *be an ordering on* $\mathrm{Mon}(x_1, \ldots, x_n)$*. If* u_1*,* $u_2, \ldots$ *is a sequence of monomials with* $u_1 \geq u_2 \geq \ldots$*, then there exists an integer* m *such that* $u_i = u_m$ *for all* $i \geq m$*.*

58. Lemma [Exercise]. *Let $f_1, \ldots, f_r \in k[x_1, \ldots, x_n]$ be nonzero polynomials. Then*

(i) $\mathrm{LM}(f_1 \cdot f_2 \cdot \ldots \cdot f_r) = \mathrm{LM}(f_1) \cdot \ldots \cdot \mathrm{LM}(f_r)$.

(ii) $\mathrm{LM}(f_1 + \ldots + f_r) \leq \max\big(\mathrm{LM}(f_1), \ldots, \mathrm{LM}(f_r)\big)$. *Equality holds if and only if* $\sum \mathrm{LC}(f_i) \neq 0$, *where the sum is taken over those i whose leading monomials* $\mathrm{LM}(f_i)$ *are maximal on the right hand side.*

59. Definition. Let $G \subset k[x_1, \ldots, x_n]$ be a nonempty subset. The **leading ideal of** G is the monomial ideal

$$\mathrm{LM}(G) := (\mathrm{LM}(f) \mid 0 \neq f \in G).$$

For $G = (0)$ we set $\mathrm{LM}((0)) = (0)$.

60. Remark. Let $I \subset k[x_1, \ldots, x_n]$ be an ideal with generating subset G. The monomial ideal $\mathrm{LM}(I)$ is generated by the leading monomials of all polynomials in I, and $\mathrm{LM}(G)$ is in general *properly contained* in $\mathrm{LM}(I)$. For instance, consider $I = (f, g)$ where $f = x_1x_2 - x_3x_4$, $g = -x_2^2 + x_1x_3$. For $>=>_{dp}$ we have $\mathrm{LM}(f) = x_1x_2$ and $\mathrm{LM}(g) = x_2^2$. Now $h = x_1^2x_3 - x_2x_3x_4 = x_2f + x_1g \in I$, but $\mathrm{LM}(I) \ni \mathrm{LM}(h) = x_1^2x_3 \notin (x_1x_2, x_2^2)$.

61. Definition. Let $I \subset k[x_1, \ldots, x_n]$ be a nontrivial ideal. A **Gröbner basis of** I is a finite subset $G = \{g_1, \ldots, g_m\}$ of I with $\mathrm{LM}(I) = \mathrm{LM}(G) = (\mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_m))$.

For instance, the generator g of a principal ideal $I = (g)$ provides a Gröbner basis, for $\mathrm{LM}(g) = (\mathrm{LM}(g))$ by (i) of Lemma 58. In general, we know that the monomial ideal $\mathrm{LM}(I)$ is finitely generated by Corollary 29 which yields existence of a Gröbner basis for any ideal.

62. Theorem [EH, 2.8]. *Let $I \subset k[x_1, \ldots, x_n]$ be a nontrivial ideal, and $\{g_1, \ldots, g_m\}$ be a Gröbner basis. Then $I = (g_1, \ldots, g_m)$.*

Theoretical application 1: Hilbert's basis theorem

63. Corollary (Hilbert's basis theorem) [EH, 2.9 & 10]. *$k[x_1, \ldots, x_n]$ is a Noetherian ring, that is, each ideal is finitely generated. Equivalently, every ascending chain of ideals $I_1 \subset I_2 \subset \ldots$ becomes stationary, i.e., there exists a k such that $I_j = I_k$ for all $j \geq k$.*

Next we address the question of **computing Gröbner bases explicitely**. This will be based on a general division algorithm for multivariate polynomials.

64. Definition. Let $G \subset k[x_1, \ldots, x_n]$ be any subset.

(i) G is called **interreduced** if $0 \notin G$ and if $\mathrm{LM}(g) \nmid \mathrm{LM}(f)$ for any two distinct elements $f, g \in G$. An interreduced Gröbner basis is also called **minimal**.

(ii) $f \in k[x_1, \ldots, x_n]$ is **reduced with respect to** G if for each $g \in G$, $g \neq f$, $\mathrm{LM}(g)$ does not divide any monomial in $\operatorname{supp} f$.

(iii) G is **reduced** if G is interreduced and if for each $g \in G$, $\mathrm{LC}(g) = 1$ and $\mathrm{tail}(g)$ is reduced with respect to G.

65. Remark. Any finite set G can be transformed to a minimal one G' with $(G) = (G')$, i.e., they generate the same ideal. Indeed, if f and $g \in G$ such that $\mathrm{LM}(g) = a\mathrm{LM}(f)$, then replace g by $g - af$.

66. Definition. Let

$$\mathcal{G} = \{G = (g_1, \ldots, g_s) \mid g_i \in k[x_1, \ldots, x_n],\ s \in \mathbb{N}\}$$

be the set of finite s-tuples of elements in $k[x_1, \ldots, x_n]$. A function

$$\mathrm{NF} : k[x_1, \ldots, x_n] \times \mathcal{G} \to k[x_1, \ldots, x_n], \quad (f, G) \mapsto \mathrm{NF}(f|G)$$

is called a **normal form** on $k[x_1, \ldots, x_n]$ if for all $G \in \mathcal{G}$ and $f \in k[x_1, \ldots, x_n]$ the following properties hold:

- $\mathrm{NF}(0|G) = 0$
- $\mathrm{NF}(f|G) \neq 0 \Rightarrow \mathrm{LM}(\mathrm{NF}(f|G)) \notin \mathrm{LM}(G)$
- If $G = (g_1, \ldots, g_s)$, then $f = \sum_{i=1}^{s} q_i g_i + \mathrm{NF}(f|G)$ for $q_i \in k[x_1, \ldots, x_n]$ with $\mathrm{LM}(\sum_{i=1}^{s} q_i g_i) \geq \mathrm{LM}(q_i g_i)$ for any i with $q_i g_i \neq 0$, that is, $\sum_{i=1}^{s} q_i g_i$ is a standard representation of $f - \mathrm{NF}(f|G)$. In particular, $\overline{f} = \overline{\mathrm{NF}(f|G)}$ in $k[x_1, \ldots, x_n]/(G)$.

Note that for a polynomial $p \in k[x_1, \ldots, x_n]$, $p = \sum_{i=1}^{s} q_i g_i$ is a **standard representation** if no cancellation of leading terms occurs on the right hand side, that is, $\mathrm{LM}(p) \geq \mathrm{LM}(q_i g_i)$ whenever $q_i g_i \neq 0$, and $\mathrm{LM}(p) = \mathrm{LM}(q_i g_i)$ for at least one i.

67. Remark. Put differently, the existence of a normal form is a *division theorem* where f is "divided" by an s-tuple $G = (g_1, \dots, g_s) \in \mathcal{G}$ with main part $\sum a_i g_i$ and remainder $\mathrm{NF}(f|G)$ such that $\mathrm{LM}(f) \geq \mathrm{LM}(\sum a_i g_i)$ and $\mathrm{LM}(f) \geq \mathrm{LM}(\mathrm{NF}(f|G))$ (exercise). Note, however, that the result may depend on the ordering of G!

68. Definition. We call NF a **reduced normal form** if for all f and G, $\mathrm{NF}(f|G)$ is reduced with respect to G.

The normal form has particularly nice properties if taken with respect to a Gröbner basis.

69. Lemma [GP, 1.6.7]. Let $I \subset k[x_1, \dots, x_n]$ be a nontrivial ideal, G be a Gröbner basis of I, and NF be a normal form on $k[x_1, \dots, x_n]$.

(i) For any $f \in k[x_1, \dots, x_n]$ we have $f \in I$ if and only if $\mathrm{NF}(f|G) = 0$.

(ii) If $\widetilde{\mathrm{NF}}$ is a further reduced normal form, then $\mathrm{NF}(f \mid G) = \widetilde{\mathrm{NG}}(f \mid G)$ for all f. In particular, since changing the order in G would produce a new normal form, $\mathrm{NF}(\cdot \mid G)$ does not depend on the ordering of G.

Normal form 1 [GP, 1.6.13]

```
> ring A=0,(x,y,z),dp;
> poly f=x2yz+xy2z+y2z+z3+xy;
> ideal I=xy+y2-1,xy;
> I;
I[1]=xy+y2-1
I[2]=xy
> reduce(f,I); //computes redNFB(f|(xy + y2 − 1, xy))
// ** I is no standard basis //Warning: result possibly depends on
ordering of the generators
y2z+z3
> I=xy,xy+y2-1; //Indeed...
> I;
I[1]=xy
I[2]=xy+y2-1
> reduce(f,I); //computes redNFB(f|(xy, xy + y2 − 1))
// ** I is no standard basis
y2z+z3-y2+1
```

Normal form 2 [GP, 1.6.13]

```
> ideal G=std(I); //computes a Gröbner basis of I
> G;
G[1]=x
G[2]=y2-1
> reduce(f,G);
z3+z
> G=y2-1,x;
> G;
G[1]=y2-1
G[2]=x
> reduce(f,G);
// ** G is no standard basis //For SINGULAR an ideal comes with an
ordered set of generators, so G is not considered as a Gröbner base
z3+z
> reduce(f,G,1); //optional value "1" suppresses tail reduction, hence
computes NFB(f|G)
z3+xy+z
```

70. Definition. Let $f, g \in k[x_1, \ldots, x_n]$ with $\mathrm{LM}(f) = x^\alpha$, $\mathrm{LM}(g) = x^\beta$ and $\mathrm{lcm}(x^\alpha, x^\beta) = x^\gamma$. Then the **s-polynomial** of f and g is defined as

$$\mathrm{spoly}(f, g) := x^{\gamma-\alpha} f - \frac{\mathrm{LC}(f)}{\mathrm{LC}(g)} \cdot x^{\gamma-\beta} g$$

If $\mathrm{LM}(g) | \mathrm{LM}(f)$, we can write more simply $\mathrm{spoly}(f, g) = f - \frac{\mathrm{LT}(f)}{\mathrm{LT}(g)} \cdot g$.

71. Division algorithm $\mathrm{NFB}(f|G)$ **[GP, Algorithm 1.6.10].**

input : $f \in k[x_1, \ldots, x_n]$, $G \in \mathcal{G}$
output: $\mathrm{NFB}(f|G) \in k[x_1, \ldots, x_n]$, a normal form of f with respect to G

```
1 h := f;
2 while (h ≠ 0) and (G_h := {g ∈ G | LM(g)|LM(h)} ≠ ∅) do
3 |   choose any g ∈ G_h;
4 |   h := spoly(h, g);
5 end
6 return h
```

(Note: B stands for Bruno Buchberger (austrian mathematician))

72. Remark. During the i-th while loop we compute an s-polynomial

$$h_i = h_{i-1} - m_i g_i, \quad \mathrm{LM}(h_{i-1}) > \mathrm{LM}(h_i),$$

where m_i is a term with $\mathrm{LT}(m_i g_i) = \mathrm{LT}(h_{i=1})$, $g_i \in G$. In particular, setting $h_0 := f$, we have $g_1 = f - m_1 g_1$, $h_2 = h_1 - m_2 g_2 = f - m_1 g_1 - m_2 g_2$ etc. This process ends after a finite number m of steps, and we finally get

$$h_m = f - \sum_{i=1}^{m} m_i g_i,$$

where $h_m = \mathrm{NF}(f|G)$. Thus, keeping track of the coefficients m_i, the Buchberger algorithm compute both the normal form and a standard representation of $f - \mathrm{NF}(f|G)$. In particular, we can write f as a linear combination $f = \sum m_i g_i$ if $f \in I = (G)$.

We can easily modify the division algorithm in order to get a reduced normal form:

73. Reduced normal form algorithm $\mathrm{redNFB}(f|G)$ **[GP, Algorithm 1.6.11].**

input : $f \in k[x_1, \ldots, x_n]$, $G \in \mathcal{G}$
output: $\mathrm{redNFB}(f|G) \in k[x_1, \ldots, x_n]$, a reduced normal form of f with respect to G

```
1  g := 0;
2  h := f;
3  while (h ≠ 0) do
4  |   h := NFB(h|G);
5  |   if (h ≠ 0) then
6  |   |   g := g + LT(h);
7  |   |   h := tail(h);
8  |   end
9  end
10 return g/LC(g)
```

74. Explicit computation of NFB and redNFB using the algorithm [GP, 1.6.12]. Consider $>_{dp}$ on $\mathrm{Mon}(x,y,z)$, and $f = x^3 + y^2 + 2z^2 + x + y + 1$, $G = \{x, y\}$.

(i) Computation of $\mathrm{NFB}(f|G) = 2z^2 + x + y + 1$. We initialise

$$h := f = x^3 + y^2 + 2z^2 + x + y + 1.$$

Then we have for the **while**-loops:

- $\mathrm{LM}(h) = x^3$, $G_h = \{x\}$
  $h_1 = \mathrm{spoly}(f, x) = y^2 + 2z^2 + x + y + 1$
- $\mathrm{LM}(h_1) = y^2$, $G_{h_1} = \{y\}$
  $h_2 = \mathrm{spoly}(h_1, y) = 2z^2 + x + y + 1$
- $\mathrm{LM}(h_2) = 2z^2$, $G_{h_2} = \emptyset$.

(ii) Computation of $\mathrm{redNFB}(f|G) = z^2 + 1/2$. We initialise

$$g := 0, \quad h := f = x^3 + y^2 + 2z^2 + x + y + 1.$$

Then we have for the **while**-loops:

- $h_1 = \mathrm{NFB}(h|G) = 2z^2 + x + y + 1$
  $g_1 = \mathrm{LT}(h_1) = 2z^2$, $h_2 = \mathrm{tail}(h_1) = x + y + 1$
- $h_3 = \mathrm{NFB}(h_2|G) = 1$
  $g_2 = g_1 + \mathrm{LT}(h_3) = 2z^2 + 1$, $h_4 = \mathrm{tail}(h_3) = 0$.

75. The Buchberger algorithm $\textsc{Std}(G)$ **[GP, Algorithm 1.7.1].** Next we want to compute Gröbner bases for a given ordering $>$ on $\mathrm{Mon}(x_1, \ldots, x_n)$ and normal form NF.

input : $G \in \mathcal{G}$
output: $S = \textsc{Std}(G)$ a Gröbner basis of $I = (G)$

```
1  S := G;
2  P := {(f, g) | f, g ∈ S, f ≠ g};
3  while (P ≠ ∅) do
4  |   choose (f, g) ∈ P;
5  |   P := P \ {(f, g)};
6  |   h := NF(spoly(f, g)|S);
7  |   if (h ≠ 0) then
8  |   |   P := P ∪ {(h, f) | f ∈ S};
9  |   |   S := S ∪ {h};
10 |   end
11 end
12 return S
```

76. Theorem (Buchberger's criterion) [GP, 1.7.3], [GP, 2.5.9], [CLS, 2.6.6]. *Let $I \subset k[x_1, \ldots, x_n]$ be an ideal, and let $G = \{g_1, \ldots, g_s\} \subset I$. Are equivalent:*

(i) *G is a Gröbner basis of I.*

(ii) $\mathrm{NF}(f \mid G) = 0$ *for all* $f \in I$.

(iii) $(G) = I$ *and* $\mathrm{NF}(\mathrm{spoly}(g_i, g_j) \mid G) = 0$ *for* $i, j = 1, \ldots, s$.

77. Remark. From a given Gröbner basis it is easy to construct a minimal and subsequently a reduced one (this is actually what SINGULAR does via the STD-command). Note that a reduced Gröbner basis of an ideal is unique (with respect to the given monomial ordering) [GP, Exercise 1.6.1].

78. Example [GP, 1.7.4]. We now compute $\textsc{Std}(G)$ explicitly using Buchberger's algorithm with NFB. Consider $>_{dp}$ on $\mathrm{Mon}(x,y)$ and $G = (x^2+y, xy+x)$. We initialise

$$S := S_0 = (x^2+y, xy+x), \quad P := P_0 = \{(x^2+y, xy+x)\}.$$

Then we have for the **while**-loops:

- $P_1 = \emptyset$
  $h_1 = \mathrm{NFB}(\mathrm{spoly}(x^2+y, xy+x) \mid S_0) = \mathrm{NFB}(-x^2+y^2 \mid S_0) = y^2+y \neq 0$
  $P_1 = \{(y^2+y, x^2+y), (y^2+y, xy+x)\}$, $S_1 = \{x^2+y, xy+x, y^2+y\}$
- $P_2 = \{(y^2+y, xy+x)\}$
  $h_2 = \mathrm{NFB}(\mathrm{spoly}(y^2+y, x^2+y) \mid S_1) = \mathrm{NFB}(-x^2y+y^3 \mid S_1) = 0$
- $P_2 = \emptyset$
  $h_3 = \mathrm{NFB}(-x^2y+y^3 \mid S_1) = 0$

The algorithm terminates and returns the Gröbner basis
$S = S_1 = \{x^2+y, xy+x, y^2+y\}$ for $I = (G)$.

Practical application 1: Ideal membership [GP, 1.8.1]

Problem: Determine for a given ideal I whether f is in I or not.

input : $I = (f_1, \ldots, f_r) \subset k[x_1, \ldots, x_n]$, $f \in k[x_1, \ldots, x_n]$
output: true or false according to whether or not $f \in I$

```
1 G := STD(I);
2 p := NF(f|G);
3 if p = 0 then
4 |   B := true;
5 else
6 |   B := false
7 end
8 return B
```

Ideal membership [GP, 1.8.1]

```
> ring A=0,(x,y),dp;
> ideal I=x10+x9y2,y8-x2y7;
> ideal G=std(I);
G[1]=x2y7-y8
G[2]=x9y2+x10
G[3]=x12y+xy11
G[4]=x13-xy12
G[5]=y14+xy12
G[6]=xy13+y12
> poly f=x2y7+y14;
> reduce(f,G);
-xy12+y8 // F is not in I
> f=xy13+y12;
> reduce(f,G);
0 // F is in I
```

Testing ideal equality [GP, 1.8.1]

```
> ring A=0,(x,y),dp;
> ideal I=x10+x9y2,y8-x2y7;
> ideal G=std(I);
> ideal K=x2y7+y14,y14+xy12;
> K;
K[1]=y14+x2y7
K[2]=y14+xy12
> reduce(K,G); //reduces the generators of K with respect to G
_[1]=-xy12+y8
_[2]=0 //K not contained in I
> poly f=(x10+x9y2)*(y8-x2y7);
> K=f;
> reduce(K,G);
_[1]=0 //K contained in I
```

Practical application 2: Solving polynomial equations [GP, 1.8.7], [CLS, Kap. 3.1]

Problem: $f_1, \ldots, f_\ell \in \mathbb{C}[x_1, \ldots, x_n]$ (or more generally, an algebraically closed field k, as for instance $\mathbb{C}$), determine the set of points $(a_1, \ldots, a_n) \in \mathbb{C}^n$ with

$$f_1(a_1, \ldots, a_n) = \ldots = f_\ell(a_1, \ldots, a_n) = 0.$$

This depends on the ideal $(f_1, \ldots, f_\ell)$ generated by the f_i and not on the generators! In general, if $I = (f_1, \ldots, f_\ell) \subset k[x_1, \ldots, x_n]$ is an ideal, we set

$$V(I) := \{(a_1, \ldots, a_n) \in k^n \mid f(a_1, \ldots, a_n) = 0 \text{ for all } f \in I\} = V(f_1, \ldots, f_\ell).$$

The problem is now to determine $V(I)$.

79. Remark. As for linear equations it is in general impossible to write down the solutions explicitly. The best we can do is to write down a basis of the solution space in the linear case, or a Gröbner base of I in the nonlinear case if we fix some monomial ordering. However, $V(I)$ will be a finite set of points if I is zero dimensional, see Remark 83 below. In this case we set on computing $V(I)$ explicitly. The reason to work over $\mathbb{C}$, or more generally, an algebraically closed field, is that $V(I)$ is not empty whenever $1 \notin I$, see Hilbert's Nullstellensatz below.

Solving equations 1 [GP, 1.8.7]

```
> ring A=0,(x,y,z),lp; //"solve"-command below uses Gröbner basis with
respect to LP-ordering
> ideal I=x2+y+z-1,x+y2+z-1,x+y+z2-1;
> ideal G=std(I);
> G;
G[1]=z6-4z4+4z3-z2
G[2]=2yz2+z4-z2
G[3]=y2-y-z2+z
G[4]=x+y+z2-1
> dim(G); //computes the dimension of the ideal (G) (see below); if
dim(G)=0, then the solution set is a finite collection of points
0
> LIB "solve.lib"; //library for solving polynomial equations
numerically
```

Solving equations 2 [GP, 1.8.7]

```
> def AC=solve(G,8,0,"nodisplay"); //solves the equations given by G numerically in the complex ring AC, "0": without multiplicities. SOLVE returns a ring with complex coefficients, DEF defines objects without a specific type: they inherit their type from the first assignment to them.
// 'solve' created a ring, in which a list SOL of numbers (the complex solutions)
// is stored.
// To access the list of complex solutions, type (if the name R was assigned
// to the return value):
setring R; SOL;
> setring AC;
> size(SOL); //gives the size of SOL, i.e., the number of elements in SOL, the solution set
5
```

Solving equations 3 [GP, 1.8.7]

```
> SOL; //displays the five solutions up to 8 digits
[1]:        [2]:          [3]:     [4]:     [5]:
 [1]:         [1]:          [1]:     [1]:     [1]: //values of X
-2.4142136   0.41421356   0        1        0
 [2]:         [2]:          [2]:     [2]:     [2]: //values of Y
-2.4142136   0.41421356   0        0        1
 [3]:         [3]:          [3]:     [3]:     [3]: //values of Z
-2.4142136   0.41421356   1        0        0
```

An example with complex solutions

```
> ring A=0,(x,y),lp;
> ideal I=(xy-4,y2-x3+1);
> ideal G=std(I);
> dim(G);
0
> LIB "solve.lib";
> def AC=solve(G,6,0,"nodisplay");
// 'solve' created a ring, in which a list SOL of numbers (the complex
solutions)
// is stored.
// To access the list of complex solutions, type (if the name R was
assigned
// to the return value):
setring R; SOL;
> setring AC;
> size(SOL);
5
```

```
> SOL;
[1]:        [2]:                    [3]:
 [1]:        [1]:                    [1]:
1.80699     (-1.38823-i*1.08623)  (-1.38823+i*1.08623)
 [2]:        [2]:                    [2]:
2.21363     (-1.78719+i*1.3984)  (-1.78719-i*1.3984)
[4]:                        [5]:
 [1]:                        [1]:
(0.484732-i*1.61705)      (0.484732+i*1.61705)
 [2]:                        [2]:
(0.680372+i*2.26969)      (0.680372-i*2.26969)
```

Theoretical application 2: Elimination and Extension

In the previous example, the generator $G[1] = z^6 - 4z^4 + 4z^3 - z^2$ was in $I \cap \mathbb{C}[z]$ and thus an univariate polynomial. We formalise this idea for general (not necessarily complete) fields as follows.

80. Definition. Given $I = (f_1, \ldots, f_s) \subset k[x_1, \ldots, x_n]$, the **$\ell$-th elimination ideal** I_ℓ is the ideal of $k[x_{\ell+1}, \ldots, x_n]$ defined by

$$I_\ell = I \cap k[x_{\ell+1}, \ldots, x_n].$$

In particular, $I_0 = I$.

The ℓ-th elimination ideal can be determined as follows.

81. The Elimination Theorem [CLS, 3.1.2]. *Let $I \subset k[x_1, \ldots, x_n]$ be an ideal and let G be a Gröbner basis of I with respect to $>_{lp}$ with $x_1 >_{lp} x_2 >_{lp} \ldots >_{lp} x_n$. Then, for every $0 \leq \ell \leq n-1$, the set*

$$G_\ell = G \cap k[x_{\ell+1}, \ldots, x_n]$$

is a Gröbner basis of the ℓ-th elimination ideal I_ℓ.

82. Example. In the previous example, where $I = (x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1) \subset \mathbb{C}[x, y, z]$, we find

$$I_0 = I \cap \mathbb{C}[x, y, z] = I$$
$$I_1 = I \cap \mathbb{C}[y, z] = (G_1) = (z^6 - 4z^4 + 4z^3 - z^2, 2yz^2 + z^4 - z^2, y^2 - y - z^2 + z)$$
$$I_2 = I \cap \mathbb{C}[z] = (G_2) = (z^6 - 4z^4 + 4z^3 - z^2).$$

83. Remark.

(i) By [CLS, Corollary 9.5.4], we can define $\dim I$, the **dimension of the ideal** I, to be the largest integer r such that there exist variables $x_{i_1}, \ldots, x_{i_r}$ with $I \cap \mathbb{C}[x_{i_1}, \ldots, x_{i_r}] = 0$. Then the condition $\dim I = \dim(G) = 0$ garantuees that I_{n-1} is not empty.

(ii) Instead of $>_{lp}$ (which is often inefficient) one can consider an **elimination ordering on** $x_1, \ldots, x_s$. This is a monomial ordering $>$ on $k[x_1, \ldots, x_n]$ such that $\mathrm{LM}(f) \in k[x_{s+1}, \ldots, x_n]$ implies $f \in k[x_{s+1}, \ldots, x_n]$ ($>_{lp}$ is actually an elimination ordering for any choice of variables). If G is a Gröbner basis for I with respect to $>$, then $G' = \{g \in G \mid \mathrm{LM}(g) \in k[x_{s+1}, \ldots, x_n]\}$ is a Gröbner basis for $I \cap k[x_{s+1}, \ldots, x_n]$, see for instance [CLS, 1.8.3].

Assume now that we have a partial solution $(a_{\ell+1}, \ldots, a_n) \in V(I_\ell)$. When does this extend to a solution $(a_\ell, \ldots, a_n) \in V(I_{\ell-1}) = V(G_{\ell-1})$?

84. Extension Theorem [CLS, 3.1.3]. *Let $I = (f_1, \ldots, f_s) \subset k[x_1, \ldots, x_n]$ be an ideal and let I_1 be the first elimination ideal of I (with respect to $>_{lp}$ or an elimination order). For each $1 \leq i \leq s$ we write f_i in the form*

$$f_i = c_i(x_2, \ldots, x_n)x_1^{N_i} + \text{ terms in which } x_1 \text{ has degree } < N_i,$$

with $N_i \geq 0$ and $c_i \in k[x_2, \ldots, x_n]$ nonzero. If we have a partial solution $(a_2, \ldots, a_n) \in V(I_1) \setminus V(c_1, \ldots, c_s)$, there exists $a_1 \in k$ with $(a_1, a_2, \ldots, a_n) \in V(I)$.

85. Corollary [CLS, 3.1.4]. *Let $I = (f_1, \ldots, f_s) \subset k[x_1, \ldots, x_n]$ be an ideal and assume that for some i, f_i is of the form*

$$f_i = c_i x_1^{N_i} + \text{ terms in which } x_1 \text{ has degree } < N_i,$$

with $c_i \in k$ nonzero and $N_i > 0$. If I_1 is the first elimination ideal of I and $(a_2, \ldots, a_n) \in V(I_1)$, there exists $a_1 \in k$ with $(a_1, a_2, \ldots, a_n) \in V(I)$.

This is based on the following

86. Proposition [CLS, 3.5.2]. *Let $G = \{g_1, \ldots, g_t\}$ be a Gröbner basis of $I \subset k[x_1, \ldots, x_n]$ for $>_{lp}$ with $x_1 > \ldots > x_n$. For each $1 \leq j \leq t$, let $c_j = c_{g_j}$, so that*

$$g_j = c_j(x_2, \ldots, x_n)x_1^{N_j} + \text{ terms in which } x_1 \text{ has degree} < N_j,$$

where $N_j \geq 0$ and $c_j \in k[x_2, \ldots, x_n]$ is nonzero. Assume $\mathbf{a} = (a_2, \ldots, a_n) \in V(I_1)$ is a partial solution with the property that $\mathbf{a} \notin V(c_1, \ldots, c_t)$. Then

$$\{f(x_1, \mathbf{a}) \mid f \in I\} = (g_o(x_1, \mathbf{a})) \subset k[x_1],$$

where $g_o \in G$ satisfies $c_o(\mathbf{a}) \neq 0$ and g_o has minimal x_1-degree among all elements $g_j \in G$ with $c_j(\mathbf{a}) \neq 0$ (the subscript letter "o" stands for "optimal"). Furthermore,

(i) $\deg(g_o(x_1, \mathbf{a})) > 0$.

(ii) *if $g_o(a_1, \mathbf{a}) = 0$ for $a_1 \in k$, then $(a_1, \mathbf{a}) \in V(I)$.*

Thus, if $\mathbf{a} \in V(I_1)$, the defining system $g_1 = \ldots = g_t = 0$ reduces to $g_o(x_1, \mathbf{a}) = 0$ when evaluated at $\mathbf{a}$.

87. Example. Consider the ideal $I = (x^2y + xz + 1, xy - xz^2 + z - 1)$ in $\mathbb{Q}[x, y, z]$. SINGULAR computes the Gröbner basis G of I with respect to $>_{lp}$, $x > y > z$:

$$\begin{aligned} g_1 &= y^2 - 2yz^2 - yz + y + 2z^4 - z^3, \\ g_2 &= xz^3 - xz^2 - y + z^2 + z - 1, \\ g_3 &= xy - xz^2 + z - 1, \\ g_4 &= x^2z^2 + x + 1. \end{aligned}$$

It follows that $I_1 = I \cap \mathbb{Q}[y, z] = (g_1)$ and

$$c_1 = g_1, \quad c_2 = z^2(z - 1), \quad c_3 = y - z^2, \quad c_4 = z^2.$$

Since $V(c_1, \ldots, c_4) = \{(0, 0)\}$, we have for any partial solution $(b, c) \neq (0, 0)$ that $\{f(x, b, c) \mid f \in I\} = (g_o(x, b, c)) \subset \mathbb{Q}[x]$. For instance we have $g_o = g_4$ for $(1, 1)$, and $\{f(x, 1, 1)\} = (x^2 + x + 1)$. For $(0, \frac{1}{2})$ we have $g_1(x, 0, \frac{1}{2}) = 0$, $g_2(x, 0, \frac{1}{2}) = -x/8 - \frac{1}{4}$, $g_3(x, 0, \frac{1}{2}) = -x/4 - \frac{1}{2}$ and $g_4(x, 0, \frac{1}{2}) = x^2/4 + x + 1$. For g_o we can take either g_2 or g_3. In particular, we can ignore the quadratic equation $g_4(x, 0, \frac{1}{2}) = 0$ when extending the partial solution $(0, \frac{1}{2})$.

Next we will generalise Gröbner bases to modules. For this, we let from now on $k[\mathbf{x}]$ be shorthand for $k[x_1, \ldots, x_n]$. We consider the free module

$$k[\mathbf{x}]^r = \bigoplus_{i=1}^{r} k[\mathbf{x}]e_i,$$

where $e_i = (0, \ldots, 1, \ldots, 0)$ denotes the i-th canonical basis vector of $k[\mathbf{x}]^r$.
Monomials are now given by

$$x^\alpha e_i = (0, \ldots, 0, x^\alpha, 0, \ldots, 0) \in k[\mathbf{x}]^r, \quad \alpha \in \mathbb{N}^n \setminus \{0\}, \quad i = 1, \ldots, n.$$

The support of $f = \sum_{i,\alpha \in \Lambda_i} a_{i,\alpha} x^\alpha e_i$ is $\operatorname{supp} f = \{x^\alpha e_i \mid a_{i,\alpha} \neq 0\}$.

88. Definition. Let $>$ be a monomial ordering on $k[\mathbf{x}]$. A **module monomial ordering** on $k[\mathbf{x}]^r$ or **module ordering** for short is a total ordering $>_m$ on the monomials $\{x^\alpha e_i \mid \alpha \in \mathbb{N}^n \setminus \{0\},\ i = 1, \ldots, r\}$ which satisfies

(i) $x^\alpha e_i >_m x^\beta e_j \Longrightarrow x^{\alpha+\gamma} e_i >_m x^{\beta+\gamma} e_j$

(ii) $x^\alpha > x^\beta \Rightarrow x^\alpha e_i >_m x^\beta e_i$

for all α, β and $\gamma \in \mathbb{N}^r$, $i, j = 1, \ldots, r$. In the sequel we often denote a module ordering $>_m$ simply by $>$ if there is no risk of confusion.

89. Remark. The second condition of Definition 88 implies that the module ordering is well-ordered and thus global if and only if the ordering on $k[\mathbf{x}]$ is well-ordered and thus global.

90. Example. If $>$ is an ordering on $k[\mathbf{x}]$, then one can define a module ordering $>_m$ by giving either **priority to the components**, that is,

$$x^\alpha e_i >_m x^\beta e_j \text{ if and only if } i < j \text{ or } (i = j \text{ and } x^\alpha > x^\beta).$$

This will be suggestively denoted by $>_m = (c, >)$. Or – this is SINGULAR'S default – we give **priority to the monomials** in $k[\mathbf{x}]$, that is,

$$x^\alpha e_i >_m x^\beta e_j \text{ if and only if } x^\alpha > x^\beta \text{ or } (x^\alpha = x^\beta \text{ and } i < j).$$

This will be therefore denoted by $>_m = (>, c)$. In both cases, the restriction to each component $>_m |_{k[\mathbf{x}]e_i \times k[\mathbf{x}]e_i}$ is just $>$.

91. Some definitions for module orderings. All the notions from the ring case carry over to the module case. We have, for instance, for any vector $f \in k[\mathbf{x}]^r \setminus \{0\}$ the notion of **leading monomial**, **coefficient** and **term**. Note that $\mathrm{LM}(f)$ and $\mathrm{LT}(f)$ are elements of $k[\mathbf{x}]^r$, while $\mathrm{LC}(f) \in k$. For a subset G of $k[\mathbf{x}]^r$ we call

$$\mathrm{LM}(G) := (\mathrm{LM}(g) \mid g \in G \setminus \{0\}) \subset k[\mathbf{x}]^r$$

the **leading submodule** of G. Since we can identify the monomials of $k[\mathbf{x}]^r$ with $\mathbb{N}^n \times E^r \subset \mathbb{N}^n \times \mathbb{N}^r = \mathbb{N}^{n+r}$, where $E^r = \{e_1, \ldots, e_r\}$, the natural partial ordering on $\mathbb{N}^{n+r}$ induces a natural partial ordering on the monomials of $k[\mathbf{x}]^r$, namely

$$x^\alpha e_i \leq_{nat} x^\beta e_j \text{ if and only if } i = j \text{ and } x^\alpha | x^\beta.$$

Equivalently, we say that $x^\alpha e_i$ divides $x^\beta e_j$ and write $x^\alpha e_i | x^\beta e_j$. Then for any set of monomials $G \subset k[\mathbf{x}]^r$ and any monomial $x^\alpha e_i$, we have

$$x^\alpha e_i \in (G) \quad \Leftrightarrow \quad x^\alpha e_i \text{ is divisible by some element of } G.$$

In particular, Dickson's Lemma for $\mathbb{N}^{n+r}$ is equivalent to the statement that any monomial submodule of $k[\mathbf{x}]^r$ is finitely generated – in strict analogy to the case of monomial ideals.

92. Definition.

(i) Let $M \subset k[\mathbf{x}]^r$ be a submodule. A **Gröbner basis of** M is a finite subset G of M with $\mathrm{LM}(M) = \mathrm{LM}(G)$, that is, for any $f \in M \setminus \{0\}$ there exists a $g \in G$ such that $\mathrm{LM}(g) | \mathrm{LM}(f)$. As for rings, a Gröbner basis generates the module.

(ii) $G \subset k[\mathbf{x}]^r$ is called **interreduced** if $0 \notin G$ and if $\mathrm{LM}(g) \nmid \mathrm{LM}(f)$ for any two distinct elements $f, g \in G$. An interreduced Gröbner basis is also called **minimal**.

(iii) $f \in k[\mathbf{x}]^r$ is **reduced with respect to** $G \subset k[\mathbf{x}]^r$ if no monomial of $\operatorname{supp} f$ is contained in $\mathrm{LM}(G)$.

(iv) $G \subset k[\mathbf{x}]^r$ is **reduced** if G is interreduced and if for each $g \in G$, $\mathrm{LC}(g) = 1$ and $\operatorname{tail}(g)$ is reduced with respect to G.

93. Definition. Let $\mathcal{G} = \{G = (g_1, \ldots, g_s) \mid g_i \in k[\mathbf{x}]^r,\ s \in \mathbb{N}\}$ be the set of finite s-tuples of elements in $k[\mathbf{x}]^r$. A function

$$\mathrm{NF} : k[\mathbf{x}]^r \times \mathcal{G} \to k[x_1, \ldots, x_n], \quad (f, G) \mapsto \mathrm{NF}(f|G)$$

is called a **normal form** on $k[\mathbf{x}]^r$ if for all $G \in \mathcal{G}$ and $f \in k[\mathbf{x}]^r$ the following properties hold:

- $\mathrm{NF}(0|G) = 0$
- $\mathrm{NF}(f|G) \neq 0 \Rightarrow \mathrm{LM}(\mathrm{NF}(f|G)) \notin \mathrm{LM}(G)$
- If $G = (g_1, \ldots, g_s)$, then there exists a standard representation

$$f - \mathrm{NF}(f|G) = \sum_{i=1}^{s} a_i g_i, \quad a_i \in k[\mathbf{x}], \quad s \geq 0.$$

In particular, $\bar{f} = \overline{\mathrm{NF}(f|G)}$ and $\overline{\mathrm{LM}(\mathrm{NF}(f|G))} \neq 0$ in $k[\mathbf{x}]^r/(G)$.

Lemma 69 holds mutatis mutandis also for modules.

94. Definition. Let $f, g \in k[\mathbf{x}]^r \setminus \{0\}$ with $\mathrm{LM}(f) = x^\alpha e_i$, $\mathrm{LM}(g) = x^\beta e_j$ and $\mathrm{lcm}(x^\alpha, x^\beta) = x^\gamma$. Then we define the **s-polynomial of f and g** by

$$\mathrm{spoly}(f,g) := \begin{cases} x^{\gamma-\alpha} f - \frac{\mathrm{LC}(f)}{\mathrm{LC}(g)} \cdot x^{\gamma-\beta} g, & i = j \\ 0, & i \neq j. \end{cases}$$

Then the Algorithms 71 (NFB) and 73 (redNFB) carry directly over to the module case.

95. Theorem [GP, 2.3.13]. *Let $M \subset k[\mathbf{x}]^r$ and $G = \{g_1, \ldots, g_s\} \subset M$. Are equivalent:*

(i) *G is a Gröbner basis of M.*

(ii) $\mathrm{NF}(f|G) = 0$ *for all $f \in M$.*

(iii) $M = (G)$ *and* $\mathrm{NF}(\mathrm{spoly}(g_i, g_j)|G) = 0$ *for $i, j = 1, \ldots, s$.*

Computing the Gröbner basis of modules 1 [GP, 2.3.12]

```
> ring A=0,(x,y,z),(c,dp); //monomial ordering DP on the module
monomials in Q[x,y,z] with priority given to components (priority to
monomials is SINGULAR's default)
> module M=[x+1,y,1],[xy,z,z2]; //defines the submodule M of Q[x,y,z]^3
> std(M);
_[1]=[0,xy2-xz-z,-xz2+xy-z2]
_[2]=[y,y2-z,-z2+y]
_[3]=[x+1,y,1]
> ring B=0,(x,y,z),dp; //switches to SINGULAR's default priority
(DP,C)
> module M=fetch(A,M); //Considers M now as a submodule of Q[x,y,z] with
respect to (DP,C)
> std(M);
_[1]=x*gen(1)+y*gen(2)+gen(3)+gen(1)
_[2]=y2*gen(2)-z2*gen(3)+y*gen(3)+y*gen(1)-z*gen(2)
```

Computing the Gröbner basis of modules 2 [GP, 2.3.12]

```
> ring C=0,(x,y,z),lp;
> module M=fetch(A,M);
> std(M);
_[1]=y2*gen(2)+y*gen(3)+y*gen(1)-z2*gen(3)-z*gen(2)
_[2]=x*gen(1)+y*gen(2)+gen(3)+gen(1)
> ring D=0,(x,y,z),(c,lp);
> module M=fetch(A,M);
> std(M);
_[1]=[0,xy2-xz-z,xy-xz2-z2]
_[2]=[y,y2-z,y-z2]
_[3]=[x+1,y,1]
```

Normal form for modules [GP, 2.3.10]

```
> ring A=0,(x,y,z),(c,dp);
> module M=[x,y,1],[xy,z,z2];
> vector f=[zx,y2+yz-z,y];
> reduce(f,M);
// ** M is no standard basis //warning that the reduction depends on
the given generators of M as we do not have a Gröbner basis
[0,y2-z,y-z]
> reduce(f,std(M));
[0,0,z2-z]
```

Practical application 3: Computing the intersection with free modules [GP, 2.8.2]

Problem: Given $f_1, \ldots, f_\ell \in k[\mathbf{x}]^r$ which define $M := (f_1, \ldots, f_\ell) \subset k[\mathbf{x}]^r$. Find generators of the submodule

$$M' := M \cap \bigoplus_{i=s+1}^{r} k[\mathbf{x}]e_i.$$

We say that M' is obtained from $f_1, \ldots, f_\ell$ by **eliminating** $e_1, \ldots, e_s$.

Solution: Compute a Gröbner basis G of M with respect to $>_m = (c, >)$. Then

$$G' := G \cap \bigoplus_{i=s+1}^{r} k[\mathbf{x}]e_i$$

is a Gröbner basis for M'.

Theoretical application 3: Computing syzygies

96. Definition. Let M be a $k[\mathbf{x}]$-module. A **syzygy** or **relation** between $f_1, \ldots, f_k \in M$ is a k-tuple $(q_1, \ldots, q_k) \in k[\mathbf{x}]^k$ satisfying

$$\sum_{i=1}^{k} q_i f_i = 0.$$

The set of all syzygies between $f_1, \ldots, f_k$ is the kernel of the module morphism

$$\varphi : F_1 := \bigoplus_{i=1}^{k} k[\mathbf{x}] e_i \to M, \quad e_i \mapsto f_i$$

and thus a submodule of $k[\mathbf{x}]^k$. It is called the **module of syzygies** and written $\mathrm{syz}(f_1, \ldots, f_k)$. We therefore have

$$\mathrm{syz}(f_1, \ldots, f_k) \subset k[\mathbf{x}]^k \overset{\varphi}{\twoheadrightarrow} (f_1, \ldots, f_k).$$

Since $k[\mathbf{x}]$ is Noetherian and $k[\mathbf{x}]^r$ is finitely generated, $k[\mathbf{x}]^r$ is Noetherian, thus $\mathrm{syz}(f_1, \ldots, f_k) \subset k[\mathbf{x}]^k$ is also finitely generated.

97. Lemma [GP, 2.5.3]. *Let $(f_1, \ldots, f_k) \subset k[\mathbf{x}]^r$ be a $M = k[\mathbf{x}]$-module. Consider the canonical embedding $k[\mathbf{x}]^r \subset k[\mathbf{x}]^{r+k}$ with projection $\pi : k[\mathbf{x}]^{r+k} \to k[\mathbf{x}]^k$ onto the last k components. Let $G = \{g_1, \ldots, g_s\}$ be a Gröbner basis of $F = (f_1 + e_{r+1}, \ldots, f_k + e_{r+k})$ with respect to a module ordering $(c, <)$ given by $x^\alpha e_i > x^\beta e_j$ if $i < j$ or $i = j$ and $x^\alpha > x^\beta$. If, possibly under relabeling, $\{g_1, \ldots, g_\ell\} = G \cap \bigoplus_{i=r+1}^{r+k} k[\mathbf{x}]e_i$ in $k[\mathbf{x}]^{r+k}$, then*

$$\operatorname{syz}(f_1, \ldots, f_k) = (\pi(g_1), \ldots, \pi(g_\ell)).$$

98. Computing generators for $\operatorname{syz}(f_1, \ldots, f_k)$ [GP, Algorithm 2.5.4].
input : $f_1, \ldots, f_k \in k[\mathbf{x}]^r$
output: $S = \{s_1, \ldots, s_\ell\} \subset k[\mathbf{x}]^k$ such that $(S) = \operatorname{syz}(f_1, \ldots, f_k) \subset k[\mathbf{x}]^k$

1 $F := \{f_1 + e_{r+1}, \ldots, f_k + e_{r+k}\} \subset k[\mathbf{x}]^{r+k}$;
2 compute $G = \mathrm{STD}(F)$ with respect to $(c, >)$;
3 $\{g_1, \ldots, g_\ell\} = G \cap \bigoplus_{i=r+1}^{r+k} k[\mathbf{x}]e_i$ with $g_i = \sum_{j=1}^{k} a_{ij} e_{r+j}$, $i = 1, \ldots, \ell$;
4 $s_i := (a_{i1}, \ldots, a_{ik}) = \pi(g_i)$, $i = 1, \ldots, \ell$;
5 **return** $S = \{s_1, \ldots, s_\ell\}$

Syzygies [GP, 2.5.5]

```
> ring A=0,(x,y,z),(c,dp);
> ideal M=xy,yz,xz;
> module S=syz(M); //computes the module of syzygies
> S; //syzygy module in Q[x,y,z]^3, k=3, given in terms of a Gröbner basis
S[1]=[0,x,-y]
S[2]=[z,0,-y]
> module F=[xy,1,0,0],[yz,0,1,0],[xz,0,0,1]; //computes the syzygy via
the algorithm; F⊂Q[x,y,z]^{1+3}
> module G=std(F);
> G; //the first two elements give the syzygies
G[1]=[0,0,x,-y] //s_1=π(G[1])=[0,x,−y]
G[2]=[0,z,0,-y] //s_2=π(G[2])=[z,0,−y]
G[3]=[yz,0,1] // G[3]=yze_1+1e_3 etc, but G[3]∉G∩⊕_{i=2}^4 k[x]e_i
G[4]=[xz,0,0,1] //G[4]∉G∩⊕_{i=2}^4 k[x]e_i
G[5]=[xy,1] //G[5]∉G∩⊕_{i=2}^4 k[x]e_i
```

99. Remark [GP, 2.5.6]. Let $I = (f_1, \ldots, f_s) \subset k[\mathbf{x}]$ be an ideal and let $\overline{\Sigma} = \{\overline{m}_1, \ldots, \overline{m}_k\}$, $\overline{m}_i \in (k[\mathbf{x}]/I)^r \cong k[\mathbf{x}]^r / I \cdot k[\mathbf{x}]^r$. We want to compute $\mathrm{syz}_{k[\mathbf{x}]/I}(\overline{\Sigma})$ where we consider $(\overline{\Sigma})$ and the resulting syzygy module as $k[\mathbf{x}]/I$-module. We can do this as follows. Let

$$\Sigma = \{m_1, \ldots, m_k, f_1 e_1, \ldots, f_1 e_r, \ldots, f_s e_1, \ldots, f_s e_r\} \subset k[\mathbf{x}]^r,$$

where $m_i \in k[\mathbf{x}]^r$ are representatives of $\overline{m}_i$. Note that $(f_1 e_1, \ldots, f_1 e_r, \ldots, f_s e_1, \ldots, f_s e_r) = I \cdot k[\mathbf{x}]^r$. We then compute a Gröbner basis $\{s_1, \ldots, s_\ell\}$ of $\mathrm{syz}(\Sigma)$ with $s_i = (s_{i1}, \ldots, s_{iN})$, $N = k + rs$. If $\overline{s}_i = (s_{i1}, \ldots, s_{ik}) \in k[\mathbf{x}]^k$, $i = 1, \ldots, \ell$, then

$$(\bar{s}_1, \ldots, \bar{s}_l) \subset k[\mathbf{x}]^k \overset{\pi_{I \cdot k[\mathbf{x}]^r}}{\twoheadrightarrow} (\overline{\Sigma}) \subset k[\mathbf{x}]^r / I \cdot k[\mathbf{x}]^r$$

that is, $\mathrm{syz}(\overline{\Sigma}) = (\bar{s}_1, \ldots, \bar{s}_l)$. Projecting this to $k[\mathbf{x}]^k / \left(I \cdot k[\mathbf{x}]^k\right)$ gives the desired syzygy module $\mathrm{syz}_{k[\mathbf{x}]/I}(\overline{\Sigma})$.

Practical application 4: Module membership [GP, 2.8.1]

Problem: Given $f, f_1, \ldots, f_k \in k[\mathbf{x}]^r$, decide whether or not $f \in M := (f_1, \ldots, f_k) \subset k[\mathbf{x}]^r$. If it is, find $q_i \in k[\mathbf{x}]$ such that $f = \sum q_i f_i$.

Solution: Compute a Gröbner basis $G = \{g_1, \ldots, g_s\}$ of M with respect to $>_m$ and choose any normal form NF on $k[\mathbf{x}]^r$. Then

$$f \in M \Longleftrightarrow \mathrm{NF}(f|G) = 0$$

since the proof of Lemma 69 applies here as well. Next choose a Gröbner basis $\{h_1, \ldots, h_\ell\}$ of $\mathrm{syz}(f, f_1, \ldots, f_k) \subset k[\mathbf{x}]^{k+1}$ with respect to the ordering $(c, >)$. Relative to the standard basis $(e_0, \ldots, e_k)$ of $k[\mathbf{x}]^{k+1}$ we write $h_i = (a_{i0}, \ldots, a_{ik})$. Since $h_i \in \mathrm{syz}(f, f_1, \ldots, f_k)$ we have $a_{i0} f + \sum_{j=1}^{k} a_{ij} f_j = 0$ for all j. On the other hand, $f = \sum b_i f_i$ for $f \in M$ so that $h = (1, -b_1, \ldots, -b_k) \in \mathrm{syz}(f, f_1, \ldots, f_k) = (G)$. Since $\mathrm{LM}(h_i)|\mathrm{LM}(h) = e_0$ for some i it follows that $\mathrm{LM}(h_i) = ce_0$ with $c \in k^*$, whence $f = -\sum_{j \geq 1} a_{ij} f_j / c$.

Module membership [GP, 2.8.1]

```
> ring A=0,(x,y,z),(c,dp);
> module M=[-z,-y,x+y,x],[yz+z2,yz+z2,-xy-y2-xz-z2,0];
> vector f=[-xz-z2,-xz+z2,x2+xy-yz+z2,0];
> reduce(f,std(M));
[0,xy-xz+yz+z2,-xz-2yz+z2,-x2-xz] //V is not in M
> vector w=[-x5yz-x5z2-z,-x5yz-x5z2-y,x6y+x5y2+x6z+x5z2+x+y,x];
> reduce(w,std(M));
0
> syz(w+M); //express W as a linear combination of m1 and m2 via
computing the syzygy module of the (w,m1,m2)
_[1]=[1,-1,x5] //Gröbner basis of syz(w,m1,m2)⊂ℚ[x,y,z]^3 is {e1−e2+x^5e3}
> lift(M,w); //the command LIFT(M,N) expresses the generators of the
submodule N⊂M in terms of the generators of M. Here, N=(w1) with
w1=w.
_[1,1]=1
_[2,1]=-x5 //w1=a11 m1+a21 m2
```

Practical application 5: Kernel of a module homomorphism [GP, Section 2.8.7]

Let $A = k[\mathbf{x}]/I$ for some ideal $I \subset k[\mathbf{x}]$, and let $M \subset A^m$ and $N = (n_1, \ldots, n_s) \subset A^n$ be submodules. We consider the A-module morphism $\varphi : A^m/M \to A^n/N$ induced by $\widehat{\varphi} : A^m \to A^n$ via $\pi_N \circ \widehat{\varphi} = \varphi \circ \pi_M$. If $\widehat{\varphi}(e_i) = b_i \in A^n$, then $\widehat{\varphi}$ is given by the matrix $B = (b_1, \ldots, b_m)$ considered as an A-linear operator $A^m \to A^n$.

Problem: Compute representatives in A^m of a system of generators of $\ker\varphi$.

Solution: $\varphi(\bar{a}) = 0$ if and only if $\widehat{\varphi}(a) \in N$ so we are looking for elements $(a_1, \ldots, a_n, a'_1, \ldots, a'_s)$ with $\sum a_i b_i = \sum a'_i n_i$. Therefore, we compute a system of generators $\{h_1, \ldots, h_\ell\}$ of $\mathrm{syz}(b_1, \ldots, b_m, n_1, \ldots, n_s) \subset A^{m+s}$. Then $\widetilde{h}_i \in A^m$ which is obtained by deleting the last s components of h_i is the desired system, and its projection down to A^m/M generates $\ker\varphi$.

Kernel of a module morphism 1 [GP, 2.8.9]

```
> ring K=0,(x,y,z),(c,dp);
> ideal I=x2y2-xyz2;
> qring A=std(I); //quotient ring A=ℚ[x,y,z]/I= current basering
> module N=[x2,xy,y2],[xy,xz,yz];
> matrix B[3][2]=x,y,zx,zy,y2,z2; //B is a 3x2-matrix, B:A^2→A^3
> module T=B[1],B[2],N[1],N[2]; //submodule T of A^(n+s)=A^(2+2)
> module S=syz(T); //syzygy module in A^4
> module Ker; //defines variable of type "module"
> int i;
> for(i=1;i<=size(S);i++){Ker=Ker+S[i][1..2];} //keeps only the first
two components
```

Kernel of a module morphism 2 [GP, 2.8.9]

```
>Ker;
Ker[1]=[xy2-yz2]
Ker[2]=[y3z-x2z2-xyz2+y2z2-xz3+yz3,xy3-x2yz]
Ker[3]=[x2yz-xz3]
Ker[4]=[x3z+x2z2-xyz2-y2z2+xz3-yz3,x3y-xy2z]
Ker[5]=[x3y-x2z2]
> reduce(B*Ker,std(N)); //We test by reducing the image of B(Ker)⊂A^m by
N
_[1]=0
_[2]=0
_[3]=0
_[4]=0
_[5]=0
```

100. Solving linear equations over a ring [GP, 2.8.8]. The solution of computing the kernel of module morphisms also enables us to compute solutions to linear equations in general. Let $I = (f_1, \ldots, f_k) \subset k[\mathbf{x}]$ be an ideal, and $A = k[\mathbf{x}]/I$. We consider the system of linear equations given by

$$\begin{array}{ccccccc} a_{11}Z_1 & + & \ldots & + & a_{1m}Z_m & = & b_1 \\ \vdots & & & & \vdots & & \vdots \\ a_{r1}Z_1 & + & \ldots & + & a_{rm}Z_m & = & b_r \end{array}$$

for a_{ij}, $b_i \in k[\mathbf{x}]$. Writing $T = (a_{ij})$, $Z = (Z_i)^\top$ and $b = (b_i)^\top$ we wish to solve the matrix equation $TZ = b$. Unlike the linear systems considered in linear algebra, the entries of the matrix T now belong to a ring and no longer to a field. However, considering T as a map $A^m \to A^r$, the solution set is of the form $z + \ker T$ as for vector spaces. To get a special solution z we first test whether b is a member of the submodule $\mathrm{Im}\,(T) \subset A^r$. If it is, we compute a representation $b = \sum r_i a_i$ with $r_i \in A$ and $a_i =$ the columns of T. This was done in the Practical application 4. The computation of the kernel is Practical application 5.

101. Definition. A sequence of A-modules with A-linear maps

$$L \xrightarrow{\alpha} M \xrightarrow{\beta} N$$

is called a **complex** if $\operatorname{im}\alpha \subset \ker\beta$, i.e., $\beta \circ \alpha = 0$, and **exact at** M if $\operatorname{im}\alpha = \ker\beta$. A sequence

$$\ldots M_{k-1} \xrightarrow{\alpha_{k-1}} M_k \xrightarrow{\alpha_k} M_{k+1} \ldots$$

is a **complex** respectively is **exact** if it is a complex respectively exact at every M_k, i.e., $\alpha_k \circ \alpha_{k-1} = 0$ respectively $\operatorname{im}\alpha_{k-1} = \ker\alpha_k$. A sequence of the form

$$0 \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0$$

is called a **short exact sequence** of A-modules.

102. Remark.

(i) $0 \longrightarrow M \xrightarrow{\varphi} N$ is exact $\Leftrightarrow \ker\varphi = \{0\} \Leftrightarrow \varphi$ is injective.

(ii) $M \xrightarrow{\varphi} N \longrightarrow 0$ is exact $\Leftrightarrow \mathrm{im}\varphi = N \Leftrightarrow \varphi$ is surjective.

(iii) $0 \longrightarrow M \xrightarrow{\varphi} N \longrightarrow 0$ is exact at M and N if and only if φ is an isomorphism.

103. Examples. If $\varphi : M \to N$ is an A-module morphism, then the natural inclusions $\ker \varphi \to M$, $\mathrm{im}\, \varphi \to N$ induce short exact sequences

$$0 \longrightarrow \ker \varphi \xrightarrow{\iota} M \xrightarrow{\varphi} \mathrm{im}\, \varphi \longrightarrow 0$$

and

$$0 \longrightarrow \mathrm{im}\, \varphi \xrightarrow{\iota} N \longrightarrow \mathrm{coker}\, \varphi \longrightarrow 0.$$

Here are two special instances of this:

- If $N_{1,2}$ are submodules of M, then the inclusion map $N_1 \cap N_2 \to N_1 \oplus N_2$, $n \mapsto n \oplus n$, and the difference map $N_1 \oplus N_2 \to N_1 + N_2$, $(n_1, n_2) \mapsto n_1 - n_2$ give the short exact sequence

$$0 \longrightarrow N_1 \cap N_2 \longrightarrow N_1 \oplus N_2 \longrightarrow N_1 + N_2 \longrightarrow 0.$$

- If $I \subset A$ is an ideal, and $a \in A$, then A/I maps onto $A/(I + (a))$. The kernel is generated by $\overline{a} \in A/I$. It follows that

$$0 \longrightarrow A/(I : (a)) \longrightarrow A/I \longrightarrow A/(I + (a)) \longrightarrow 0$$

  is exact. Here, the map $A/(I : (a)) \to A/I$ assigns to $\pi_{I:(a)}(b)$ the element $\pi_I(a \cdot b)$.

104. Remark.

(i) **Splitting of exact sequences:** An exact sequence
$M_1 \xrightarrow{\alpha_1} M_2 \xrightarrow{\alpha_2} M_3 \xrightarrow{\alpha_3} M_4$ gives rise to

$$M_1 \xrightarrow{\alpha_1} M_2 \longrightarrow \mathrm{im}\alpha_2 = \mathrm{ker}\alpha_3 \longrightarrow 0$$

and

$$0 \longrightarrow \mathrm{ker}\alpha_3 = \mathrm{im}\alpha_2 \longrightarrow M_3 \xrightarrow{\alpha_3} M_4 \ .$$

(ii) **Glueing of exact sequences:** The exact sequences
$M_1 \xrightarrow{\alpha_1} M_2 \xrightarrow{\alpha_2} \mathrm{im}\alpha_2 = \mathrm{ker}\alpha_3 \longrightarrow 0$ and
$0 \longrightarrow \mathrm{ker}\alpha_3 = \mathrm{im}\alpha_2 \longrightarrow M_3 \xrightarrow{\alpha_3} M_4$ give rise to the exact sequence

$$M_1 \xrightarrow{\alpha_1} M_2 \xrightarrow{\alpha_2} M_3 \xrightarrow{\alpha_3} M_4.$$

105. Example. If $\varphi : M \to N$ is an A-module morphism, then the exact sequence

$$0 \longrightarrow \ker \varphi \longrightarrow M \xrightarrow{\varphi} N \longrightarrow \operatorname{coker} \varphi \longrightarrow 0$$

can be split into

$$0 \longrightarrow \ker \varphi \longrightarrow M \xrightarrow{\varphi} \operatorname{im} \varphi \longrightarrow 0$$

and

$$0 \longrightarrow \operatorname{im} \varphi \longrightarrow N \longrightarrow \operatorname{coker} \varphi \longrightarrow 0.$$

In particular, any exact sequence

$$0 \longrightarrow M_1 \xrightarrow{\alpha_1} M_2 \xrightarrow{\alpha_2} \dots \xrightarrow{\alpha_{n-1}} M_n \xrightarrow{\alpha_n} 0$$

can be split up into short exact sequences

$$0 \longrightarrow \ker\alpha_i = \operatorname{im}\alpha_{i-1} \longrightarrow M_i \xrightarrow{\alpha_i} \operatorname{im}\alpha_i = \ker\alpha_{i+1} \longrightarrow 0$$

which can be glued back to the original exact sequence.

106. Definition. A finitely generated A-module M is said to have a **finite presentation** if there exists an A-linear map $\varphi : A^m \to A^n$ such that M is isomorphic to $\operatorname{coker}\varphi$, that is, we have an exact sequence

$$A^m \xrightarrow{\varphi} A^n \xrightarrow{\pi_{\operatorname{im}\varphi}} A^n/\operatorname{im}\varphi = \operatorname{coker}\varphi \cong M \longrightarrow 0.$$

φ is called the **presentation morphism** of M.

Presentation of submodules 1 [GP, 2.1.24]

```
> ring A=0,(x,y,z),dp;
> module N=[xy,0,yz],[0,xz,z2]; //defines the submodule N of A^3=Q[x,y,z]^3

> N;
//2 generators
N[1]=xy*gen(1)+yz*gen(3)
N[2]=xz*gen(2)+z2*gen(3)
> LIB "inout.lib"; //library for formatting output gives command SHOW
> show(N); //shows the generators as vectors
// module, 2 generator(s)
[xy,0,yz]
[0,xz,z2]
> print(N); //the matrix corresponding to A^2->N⊂A^3, e_i↦N[i]
xy,0,
0,xz,
yz,z2
```

Presentation of submodules 2 [GP, 2.1.24]

```
> show(N+x*N); //shows the generators of N+x*N
[xy,0,yz]
[0,xz,z2]
[x2y,0,xyz]
[0,x2z,xz2]
> print(N+x*N); //the matrix corresponding to A^4→N+x*N⊂A^3, e_i↦N[i]
xy,0, x2y,0,
0, xz,0, x2z,
yz,z2,xyz,xz2
> module K1=syz(N);
> K1;
K1[1]=0 //computes the kernel of A^2→N=(N[1],N[2]).
> print(K1) //gives the presentation matrix of N which is (0), i.e.,
N≅A^2
0,
0
```

Presentation of submodules 3 [GP, 2.1.24]

```
> module M=[xy,yz],[xz,z2]; //defines the submodule M⊂A^2
> print(M);
xy,xz,
yz,z2
> matrix p=M; //automatic type conversion module with corresponding
matrix A^2 --p--> M --> 0
> p;
p[1,1]=xy
p[1,2]=xz
p[2,1]=yz
p[2,2]=z2
> module K2=syz(M); //computes the kernel of A^2 --> M
> show(K2); //gives the generator of K2
K2[1]=[-z,y]
> print(K2); //presentation morphism
-z,
y
```

$$A^1 \xrightarrow{\varphi=\binom{-z}{y}} K2 \subset A^2 \xrightarrow{p=\pi_{K2}} M \cong \operatorname{coker}\varphi \longrightarrow 0$$

107. Definition.

(i) Let M be a finitely generated A-module. A **free resolution** of M is an exact sequence

$$\ldots \longrightarrow F_{k+1} \xrightarrow{\varphi_{k+1}} F_k \longrightarrow \ldots \longrightarrow F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \longrightarrow 0$$

with finitely generated, free A-modules $F_k \cong A^{r_k}$, $k \geq 0$. This free resolution has **length** $n \in \mathbb{N}$ if $F_k = 0$ for all $k > n$ and n is minimal with this property.

(ii) If $(A, \mathfrak{m})$ is a local ring, then a free resolution is **minimal** if $\varphi_k(F_k) \subset \mathfrak{m}F_{k-1}$ for $k \geq 1$. In this case we call $b_k(M) := \operatorname{rank}(F_k) = r_k$, $k \geq 0$, the **k-th Betti number** of M.

108. Computing free resolutions RES(I, m) **[GP, 2.5.7].** Since the sygyzy modules are finitely generated, we obtain a free resolution of given length m by successively computing syzygies.

input : $f_1, \ldots, f_k \in k[\mathbf{x}]^r$, $0 \neq m \in \mathbb{N}$
output: A list of matrices $A_1, \ldots, A_m$ with $A_i \in \mathrm{Mat}(r_{i-1} \times r_i, k[\mathbf{x}])$, $i = 1, \ldots, m$, $r_0 = r$ and $r_1 = k$, with free resolution of $M = k[\mathbf{x}]^r/(f_1, \ldots, f_k)$:

$$k[\mathbf{x}]^{r_m} \xrightarrow{A_m} k[\mathbf{x}]^{r_{m-1}} \longrightarrow \ldots \longrightarrow k[\mathbf{x}]^{r_1} \xrightarrow{A_1} k[\mathbf{x}]^r \xrightarrow{\pi(f_1,\ldots,f_k)} M \longrightarrow 0$$

$i := 1$;
$A_1 := \mathrm{matrix}(f_1, \ldots, f_k) \in \mathrm{Mat}(r \times k, k[\mathbf{x}])$;
while $(i < m)$ **do**
    $i := i + 1$;
    $A_i := \mathrm{syz}(A_{i-1})$;
end
return $A_1, \ldots, A_m$

109. Theorem [GP, 2.4.11]. *Let $(A, \mathfrak{m})$ be a local Noetherian ring and M be a finitely generated A-module. Then M has a minimal free resolution. Furthermore, the Betti numbers and the length (if defined) are independent of the minimal resolution and are thus invariants of M.*

110. Remark. The proof also shows that the length of a general free resolution is always equal or greater than the length of a minimal resolution.

111. Example. If $(A, \mathfrak{m}) = (K, 0)$ is a field and M thus a K-vector space, then a minimal resolution of M has length 0 and $b_0(M) = \dim_K M$.

112. Definition. Let $f_1, \ldots, f_k \in k[\mathbf{x}]^r =: F_0$ with module ordering $>_0$, and let $F_1 \cong k[\mathbf{x}]^k$ be the free $k[\mathbf{x}]$-module containing $\mathrm{syz}(f_1, \ldots, f_k)$. The **Schreyer ordering** is the module ordering $>_1$ on F_1 which is defined as follows:

$$\begin{aligned} x^\alpha \epsilon_i >_1 x^\beta \epsilon_j \quad \Longleftrightarrow \quad & \mathrm{LM}(x^\alpha f_i) >_0 \mathrm{LM}(x^\beta f_j) \text{ or} \\ & \mathrm{LM}(x^\alpha f_i) = \mathrm{LM}(x^\beta f_j) \text{ and } i < j, \end{aligned}$$

where ϵ_i, $i = 1, \ldots, k$, is the canonical basis of F_1. Of course, $>_1$ depends on $f_1, \ldots, f_k$.

113. Notation. Let $f_1, \ldots, f_k \in k[\mathbf{x}]^r$. For each $i \neq j$ such that f_i and f_j have their leading monomials in the same component, i.e., $\mathrm{LM}(f_i) = x^{\alpha_i} e_\nu$, $\mathrm{LM}(f_j) = x^{\alpha_j} e_\nu$ and $\gamma = \mathrm{lcm}(\alpha_i, \alpha_j)$ we define

$$m_{ji} := x^{\gamma - \alpha_i} \in k[\mathbf{x}].$$

In particular, $\mathrm{spoly}(f_i, f_j) = m_{ji} f_i - c_i m_{ij} f_j / c_j$ if $c_{i,j} = \mathrm{LC}(f_{i,j})$. Finally, assume that $\mathrm{spoly}(f_i, f_j) = \sum_{\nu=1}^{k} a_\nu^{(ij)} f_\nu$, $a_\nu^{(ij)} \in k[\mathbf{x}]$ is a standard representation (for instance, $\mathrm{NF}(\mathrm{spoly}(f_i, f_j) | (f_1, \ldots, f_k)) = 0$ for some normal form). Then for $i < j$ we set

$$s_{ij} := m_{ji} \epsilon_i - \frac{c_i}{c_j} m_{ij} \epsilon_j - \sum_{\nu} a_\nu^{(ij)} \epsilon_\nu.$$

114. Lemma [GP, 2.5.8]. *$s_{ij} \in \mathrm{syz}(\mathrm{f_1}, \ldots, \mathrm{f_k})$ and $\mathrm{LM}(s_{ij}) = m_{ji} \epsilon_i$.*

115. Theorem [GP, 2.5.9]. *Let $G = \{f_1, \ldots, f_k\}$ be a set of generators of $M \subset k[\mathbf{x}]^r$, and let NF be a given normal form. Let*

$$\Lambda := \{(i,j) \mid 1 \leq i < j \leq k,\ \mathrm{LM}(f_i) = x^\alpha e_\nu,\ \mathrm{LM}(f_j) = x^\beta e_\nu \text{ for some } \nu\}.$$

Assume that $\mathrm{NF}(\mathrm{spoly}(f_i, f_j) \mid (f_1, \ldots, f_k)) = 0$ for all $i, j = 1, \ldots k$. Then the following statements hold:

(i) *G is a Gröbner basis of M (Buchberger's criterion).*

(ii) *$S := \{s_{ij} \mid (i,j) \in \Lambda\}$ is a Gröbner basis of $\mathrm{syz}(f_1, \ldots, f_k)$ with respect to the Schreyer ordering.*

Theoretical application 4: Hilbert's syzygy theorem

116. Lemma [GP, 2.5.13]. *Let $G = \{g_1, \dots, g_s\}$ be a minimal Gröbner base of the submodule M of $k[\mathbf{x}]^r$ such that $\mathrm{LM}(g_i) \in \{e_1, \dots, e_r\}$ for all i. Let Λ denote the set of indices ℓ such that $e_\ell \notin \{\mathrm{LM}(g_1), \dots \mathrm{LM}(g_s)\}$. Then*

$$M = \bigoplus_{i=1}^{s} k[\mathbf{x}] g_i, \quad k[\mathbf{x}]^r / M \cong \bigoplus_{\ell \in \Lambda} k[\mathbf{x}] e_\ell.$$

117. Lemma [GP, 2.5.14]. *Let $G = \{g_1, \dots, g_s\}$ be a Gröbner basis of $M \subset k[\mathbf{x}]^r$ such that $(g_1, \dots, g_s)$ is ordered in the following way: if $i < j$ and $\mathrm{LM}(g_i) = x^{\alpha_i} e_\nu$, $\mathrm{LM}(g_j) = x^{\alpha_j} e_\nu$, then $\alpha_i \geq \alpha_j$ lexicographically. Let s_{ij} denote the syzygies defined above. Suppose that $\mathrm{LM}(g_1), \dots, \mathrm{LM}(g_s)$ do not depend on the variables $x_1, \dots, x_k$. Then the $\mathrm{LM}(s_{ij})$ taken with respect to the Schreyer ordering do not depend on $x_1, \dots, x_{k+1}$.*

118. Theorem (Hilbert's Syzygy Theorem) [GP, 2.5.15]. *Let $>$ be any monomial ordering on $k[\mathbf{x}]$. Then any finitely generated $k[\mathbf{x}]$-module M has a free resolution*

$$0 \longrightarrow F_m \longrightarrow F_{m-1} \longrightarrow \ldots \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

of length $m \leq n$, where the F_i are free $k[\mathbf{x}]$-modules.

Next we want to investigate Hilbert functions and polynomials.

119. Definition. A **graded ring** A is a ring with a decomposition $A = \bigoplus_{\nu \in \mathbb{N}} A_\nu$ as a direct sum of abelian groups such that $A_\nu A_\mu \subset A_{\nu+\mu}$ for all ν, $\mu \in \mathbb{N}$. The A_ν are called the **homogeneous components of degree** ν of A, and elements of A_ν are called **homogeneous**. A **graded k-algebra** is a k-algebra which is a graded ring for which A_ν is a k-vector space for all $\nu \in \mathbb{N}$ and $A_0 = k$.

120. Examples.

(i) Every ring A carries a trivial structure of a graded ring by setting $A_0 = A$ and $A_\nu = 0$ for $\nu \geq 1$.

(ii) If $I \subset A$ is an ideal, then

$$\mathrm{Gr}_I(A) = \bigoplus_{\nu \geq 0} \mathrm{Gr}_I(A)_\nu := \bigoplus_{\nu \geq 0} I^\nu / I^{\nu+1}$$

is a graded ring (where by convention, $I^0 = (1) = A$). Multiplication is given as follows: If $\overline{a} \in I^\nu / I^{\nu+1}$ and $\overline{b} \in I^\mu / I^{\mu+1}$, then $\overline{a} \cdot \overline{b} := \overline{a \cdot b} \in I^{\nu+\mu} / I^{\nu\mu+1}$ (this is indeed well-defined).

(iii) Let $A = k[x_1, \ldots, x_n]$ and $w = (w_1, \ldots, w_n)$ be an n-tuple of positive integers. We let $\mathrm{wdeg}(x^\alpha) = \sum w_i \alpha_i$ which is additive in the α_i. Then $A_\nu =$ the k-vector generated by monomials of $\mathrm{wdeg} = \nu$ is a graded k-algebra. The elements of A_ν are called **quasihomogeneous** or **weighted homogeneous of degree** ν.

121. Definition. Let $A = \bigoplus_{\nu \in \mathbb{N}} A_\nu$ be a graded ring. An A-module M is a **graded A-module** if there is a direct sum decomposition $M = \bigoplus_{\mu \in \mathbb{Z}} M_\mu$ into abelian groups with $A_\nu M_\mu \subset M_{\mu+\nu}$.

122. Examples.

(i) Let $A = \bigoplus_{\nu\in\mathbb{N}} A_\nu$ be a graded k-algebra, and consider the free A-module $A^m = \bigoplus_{i=1}^m Ae_i$. Let $\deg(e_i) := \nu_i \in \mathbb{Z}$, and M_ν be the k-vector space generated by fe_i with $f \in A_{\nu-\nu_i}$. Then $A^m = \bigoplus_{\nu\in\mathbb{Z}} M_\nu$ becomes a graded A-module.

(ii) If $M = \bigoplus_{\nu\in\mathbb{Z}} M_\nu$ is a graded A-module, we define for $d \in \mathbb{Z}$ the **d-th shift of** M by $M(d) := \bigoplus_{\nu\in\mathbb{Z}} M(d)_\nu$, where $M(d)_\nu := M_{\nu+d}$. Then $M(d)$ is a graded A-module. In particular, $A(d)$ is a graded A-module.

123. Lemma [Exercise]. *Let $M = \bigoplus_{\nu\in\mathbb{Z}} M_\nu$ be a graded A-module and $N \subset M$ be a submodule. Are equivalent:*

(i) *N is graded by the induced grading, i.e., $N = \bigoplus_{\nu\in\mathbb{Z}} N_\nu$ with $N_\nu = M_\nu \cap N$.*

(ii) *N is generated by homogeneous elements.*

(iii) *Let $m = \sum m_\nu$, $m_\nu \in M$. Then $m \in N$ if and only if $m_\nu \in N$ for all ν.*

A submodule satisfying one und thus all of these conditions is called a **graded** *or* **homogeneous** *submodule if M. If $M = A$, where A is a graded ring, we call N a* **graded** *or* **homogeneous** *ideal.*

124. Remark. Let $M = \bigoplus_{\nu\in\mathbb{Z}} M_\nu$ be a graded module and $N \subset M$ be a graded submodule. Then the quotient M/N is a graded module with $(M/N)_\nu = M_\nu/N_\nu \cong (M_\nu + N)/N$. If $M = A$ is a graded ring and $N = I$ is a homogeneous ideal, then A/I is a graded ring.

125. Definition. Let $A = \bigoplus_{\nu\geq 0} A_\nu$ be a graded ring, and $M = \bigoplus_{\nu\in\mathbb{Z}} M_\nu$ and $N = \bigoplus_{\nu\in\mathbb{Z}} N_\nu$ be two graded A-modules. An A-linear map $\varphi : M \to N$ is **graded** or **homogeneous of degree** d if $\varphi(M_\nu) \subset N_{\nu+d}$. We call φ simply **homogeneous** if it is homogeneous of degree 0.

126. Examples. Under the assumptions of the previous definition, multiplication with $f \in A_d$ defines a graded morphism $\varphi = f\cdot : M \to M$ of degree d.

127. Remark. If $\varphi : M \to N$ is a homogeneous morphism, then $\ker\varphi$, $\operatorname{im}\varphi$ and $\operatorname{coker}\varphi$ are graded A-submodules.

Graded rings and modules 1 [GP, 2.2.15]

```
> ring A=0,(x,y,z),dp;
> ideal I=y3-z2,x3-z;
> homog(I); //returns 1 or 0 depending on whether or not I is
homogeneous
0
> qhweight(I); //gives the weights of the variables x,y,z for which I
becomes quasihomogeneous (if they exist)
1,2,3
> ring B=0,(x,y,z),wp(1,2,3); //Let ν1,...,νn be positive integers.
Then wp(ν1,...,νn) is weighted reverse lexicographical ordering with
deg(x^α)=ν1α1+···+νnαn.
> ideal I=fetch(A,I); //redefines I as an ideal of B where the
variables x,y,z now have the weights 1,2,3 respectively
> homog(I);
1
```

Graded rings and modules 2 [GP, 2.2.15]

```
> module M=[y3-z2,x3-z],[x3,1];
> homog(M);
1
> attrib(M,"isHomog");
0,3 //M is a homogeneous submodule of Q[x,y,z]^2=Be_1⊕Be_2 if the grading is
induced by by the grading on B^2 given by deg e_1=0, deg e_2=3
```

//For more on the handling of graded modules see SINGULAR'S *library "gradedModules_lib"*

128. Lemma [GP, 2.2.14]. *Let $A = \bigoplus_{\nu \geq 0} A_\nu$ be a Noetherian graded k-algebra and let $M = \bigoplus_{\nu \in \mathbb{Z}} M_\nu$ be a finitely generated, graded A-module. Then*

(i) *there exists $m \in \mathbb{Z}$ such that $M_\nu = (0)$ for $\nu < m$;*

(ii) $\dim_k M_\nu < \infty$ *for all* ν.

129. Definition. Let $A = \bigoplus_{\nu \geq 0} A_\nu$ be a Noetherian graded k-algebra, and let $M = \bigoplus_{\nu \in \mathbb{Z}} M_\nu$ be a finitely generated, graded A-module. The **Hilbert function** $H_M : \mathbb{Z} \to \mathbb{Z}$ is defined by

$$\mathrm{H}_M(\nu) := \dim_k(M_\nu).$$

The **Hilbert-Poincaré series** on M is defined by

$$\mathrm{HP}_M(t) := \sum_{\nu \in \mathbb{Z}} \mathrm{H}_M(\nu) \cdot t^\nu \in \mathbb{Z}[\![t]\!][t^{-1}].$$

Both the Hilbert function and the Hilbert-Poincaré series depend only on the graded structure of M. In particular, we are free to consider M as an $A/\mathrm{Ann}(M)$-module and we shall usually do so when carrying out concrete computations.

130. Lemma [GP, 5.1.2]. *Let $A = \bigoplus_{\nu \geq 0} A_\nu$ be a Noetherian graded k-algebra, and let $M = \bigoplus_{\nu \in \mathbb{Z}} M_\nu$ be a finitely generated graded A-module.*

(i) *Let $N \subset M$ be a graded submodule, then*

$$\mathrm{H}_M(\nu) = \mathrm{H}_N(\nu) + \mathrm{H}_{M/N}(\nu)$$

for all ν. In particular, $\mathrm{HP}_M(t) = \mathrm{HP}_N(t) + \mathrm{HP}_{M/N}(t)$.

(ii) *Let d be an integer, then*

$$\mathrm{H}_{M(d)}(\nu) = \mathrm{H}_M(\nu + d)$$

for all ν. In particular, $\mathrm{HP}_{M(d)}(t) = t^{-d}\mathrm{HP}_M(t)$.

(iii) *Let d be a non-negative integer, let $f \in A_d$, and let $\varphi : M(-d) \to M$ be defined by $\varphi(m) := f \cdot m$. Then $\ker\varphi$ and $\mathrm{coker}\varphi$ are graded $A/(f)$-modules with respect to the induced gradings and*

$$\mathrm{H}_M(\nu) - \mathrm{H}_M(\nu - d) = \mathrm{H}_{\mathrm{coker}\varphi}(\nu) - \mathrm{H}_{\ker\varphi}(\nu - d).$$

In particular, $\mathrm{HP}_M(t) - t^d\mathrm{HP}_M(t) = \mathrm{HP}_{\mathrm{coker}\varphi}(t) - t^d\mathrm{HP}_{\ker\varphi}(t)$.

131. Definition. Let A be a graded k-algebra and M be a finitely generated, graded A-module. A **graded free resolution** of M is a resolution

$$\ldots \longrightarrow F_{k+1} \xrightarrow{\varphi_{k+1}} F_k \longrightarrow \ldots \longrightarrow F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \longrightarrow 0$$

such that every F_k is a finitely generated free A-module of the form $A(-d_1) \oplus \ldots \oplus A(-d_p)$, and the φ_k are homogeneous of degree 0.

132. Corollary [Exercise]. *Let $A = \bigoplus_{\nu \geq 0} A_\nu$ be a Noetherian graded k-algebra, and let $M = \bigoplus_{\nu \geq 0} M_\nu$ be a finitely generated and positively graded A-module. If*

$$0 \longrightarrow F_k \xrightarrow{\varphi_k} F_{k-1} \longrightarrow \ldots \longrightarrow F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \longrightarrow 0$$

is a graded free resolution of M, then we have

$$H_M(\nu) = \dim_k M_\nu = \sum_{j=0}^{k} (-1)^j \dim_k (F_j)_\nu = \sum_{j=0}^{k} (-1)^j H_{F_j}(\nu).$$

133. Theorem [GP, 5.1.3]. *Let A be a Noetherian graded k-algebra, and let M be a finitely generated and positively graded A-module. Furthermore, assume that A is generated by $x_1, \dots, x_n \in A_1$ as a k-algebra, that is, $A = k[x_1, \dots, x_n]/I$ for some ideal I of $k[x_1, \dots, x_n]$. Then*

$$\mathrm{HP}_M(t) = \frac{Q(t)}{(1-t)^n}$$

for some $Q(t) \in \mathbb{Z}[t]$.

Canceling all common factors of $\mathrm{HP}_M(t) = Q(t)/(1-t)^n$ yields a representation

$$\mathrm{HP}_M(t) = \frac{G(t)}{(1-t)^s}, \quad 0 \le s \le n, \quad G(t) = \sum_{k=0}^{d} g_k t^k \in \mathbb{Z}[t]$$

such that $g_d \neq 0$ and $G(1) \neq 0$. This leads to the

134. Definition. Let $A = \bigoplus_{\nu \geq 0} A_\nu$ be a Noetherian graded k-algebra, and let $M = \bigoplus_{\nu \geq 0} M_\nu$ be a finitely generated and positively graded A-module.

(i) $Q(t)$ and $G(t) \in \mathbb{Z}[t]$ are called the **first** and **second Hilbert series** of M.

(ii) Let $d = \deg G(t)$ be the **degree of** G, and let s be the **order of the pôle** of $\mathrm{HP}_M(t)$ at 1. For $\nu \geq d$, we let

$$\mathrm{P}_M(\nu) := \sum_{k=0}^{d} g_k \cdot \begin{pmatrix} s-1+\nu-k \\ s-1 \end{pmatrix}.$$

Then $\mathrm{P}_M(\nu)$ is a polynomial expression in ν and we can view P_M formally as a rational polynomial in ν (if treat ν as a variable, then the coefficients are no longer necessarily in $\mathbb{Z}$). $\mathrm{P}_M \in \mathbb{Q}[\nu]$ is called the **Hilbert polynomial** of M (by convention $\begin{pmatrix} n \\ -1 \end{pmatrix} = 0$ for $n \geq 0$ and $= 1$ for $n = -1$; the degree of the zero polynomial is -1).

135. Corollary (Hilbert) [GP, 5.1.5]. *We have* $\deg \mathrm{P}_M = s-1$ *and the polynomial expression in* ν *of* $\mathrm{P}_M(\nu)$ *equals* $\mathrm{H}_M(\nu)$ *for* $\nu \geq d$*. In particular, the Hilbert function is a polynomial in* ν *for* ν *big enough. Moreover, there exists* $a_k \in \mathbb{Z}$ *such that*

$$\mathrm{P}_M = \sum_{k=0}^{s-1} a_k \binom{\nu}{k} = \frac{a_{s-1}}{(s-1)!} \cdot \nu^{s-1} + \text{ lower terms in } \nu,$$

where $a_{s-1} = G(1) > 0$*.*

136. Example. Consider $k[x_1, \ldots, x_n]$ with its natural k-algebra grading. Then

$$\mathrm{H}_{k[\mathbf{x}]}(\nu) = \begin{cases} 0, & \nu < 0 \\ \binom{\nu+n-1}{n-1}, & \nu \geq 0 \end{cases}$$

and therefore

$$\mathrm{HP}_{k[\mathbf{x}]}(t) = \sum_{\nu=0}^{\infty} \binom{\nu+n-1}{n-1} t^\nu = \frac{1}{(1-t)^n}.$$

It follows that $G(t) = 1$ and $\mathrm{P}_{k[\mathbf{x}]}(\nu) = \mathrm{H}_{k[\mathbf{x}]}(\nu)$ for all $\nu \geq 0$.

Next we adress the question of computing the Hilbert-Poincaré series for modules of the form $k[\mathbf{x}]/I$. Again, we start with monomial ideals.

137. Lemma [GP, 5.2.2]. *Let $I \subset k[\mathbf{x}]$ be a homogeneous ideal, and let $f \in k[\mathbf{x}]$ be a homogeneous polynomial of degree d, then*

$$\mathrm{HP}_{k[\mathbf{x}]/I}(t) = \mathrm{HP}_{k[\mathbf{x}]/I+(f)}(t) + t^d \mathrm{HP}_{k[\mathbf{x}]/I:(f)}(t)$$

138. Example. Let $I = (xz, yz) \subset k[x, y, z]$. For $f = z$ we have $I + (f) = (z)$ and $I : (f) = k[x, y]$, whence

$$\mathrm{HP}_{k[x,y,z]/(xz,yz)}(t) = \mathrm{HP}_{k[x,y]}(t) + t\mathrm{HP}_{k[z]}(t) = \frac{-t^2 + t + 1}{(1-t)^2}$$

and thus

$$\mathrm{P}_{k[x,y,z]/(xz,yz)}(\nu) = \binom{\nu+1}{1} + \binom{\nu}{1} - \binom{\nu-1}{1} = \nu + 2$$

139. The algorithm MONOMIALHP(I) **[GP, 5.2.4].**
input : $I = (f_1, \ldots, f_r) \subset k[\mathbf{x}]$, $f_i \in \mathrm{Mon}(x_1, \ldots, x_n)$
output: $Q(t) \in \mathbb{Z}[t]$ such that $Q(t)/(1-t)^n$ is the Hilbert-Poincaré series of $k[\mathbf{x}]/I$

compute $G(I) = \{x^{\alpha_1}, \ldots, x^{\alpha_s}\}$ the minimal generating subset of monomials of I;
if $G(I) = \{0\}$ **then**
  return 1
end
if $G(I) = \{1\}$ **then**
  return 0
end
if *all elements of* $G(I)$ *have degree* 1 **then**
  return $(1-t)^s$
end
choose $1 \leq i \leq s$ such that $\deg(x^{\alpha_i}) > 1$ and $1 \leq k \leq n$ such that $x_k | x^{\alpha_i}$;
return MONOMIALHP$(I, x_k) + t\cdot$MONOMIALHP$(I : (x_k))$

Monomial Hilbert-Poincaré series [GP, 5.2.5]

```
> proc MonomialHP(ideal I)
.{
. I=interred(I); //computes the minimal basis of I
. int s=size(I);
. if(I[1]==0){return(1);} //I=0?
. if(I[1]==1){return(0);} //I=k[x]?
. if(deg(I[s])==1){return((1-var(1))^s);} //otherwise deg I[s]>1
. int j=1;
. while(leadexp(I[s])[j]==0){j++;} //find first x_j| deg I[s]
. return(MonomialHP(I+var(j))+var(1)*MonomialHP(quotient(I,var(j))));
.}
> ring A=0,(t,x,y,z),dp;
> ideal I=x5y2,x3,y3,xy4,xy7;
> MonomialHP(I);
t6-2t3+1 //=Q(t), divide by (1−t)^n, n=3, to obtain HP_{k[x,y,z]/I}
> intvec v=hilb(std(I),1); //alternatively, use the HILB(·,1)-command
> v; //This is Q(t) since we used 1 as option (use 2 for G(t))
1,0,0,-2,0,0,1,0 //interpretation: if v=(v_0,...,v_d,0), then Q(t)=∑_{i=0}^{d} v_i t^i
```

140. Theorem [GP, 5.2.6], [GP, 5.2.7]. *Let $>$ be any monomial ordering on $k[\mathbf{x}]$, and let $I \subset k[\mathbf{x}]$ be a homogeneous ideal. Then*

$$\mathrm{HP}_{k[\mathbf{x}]/I}(t) = \mathrm{HP}_{k[\mathbf{x}]/\mathrm{LM}(I)}(t),$$

where $\mathrm{LM}(I)$ is the leading ideal of I with respect to $>$. In particular, we have

$$\dim_k k[\mathbf{x}]/I = \dim_k k[\mathbf{x}]/\mathrm{LM}(I).$$

141. The Algorithm HILBERTPOINCARE(I) **[GP, 5.2.8].** We wish to compute the Hilbert-Poincaré series of $k[\mathbf{x}]/I$ for a homogeneous ideal I.

input : $I = (f_1, \ldots, f_k) \in k[\mathbf{x}]$ a homogeneous ideal, $\mathbf{x} = (x_1, \ldots, x_r)$
output: $Q(t) \in \mathbb{Z}[t]$ such that $Q(t)/(1-t)^r$ is the Hilbert-Poincaré series of $k[\mathbf{x}]/I$

```
1 compute STD(I);
2 return MONOMIALHILBERTPOINCARE(LM(g_1), ..., LM(g_s))
```

1. Rings, modules and morphisms

2. Gröbner bases

3. Affine and projective varieties

In the sequel we fix an **algebraically closed field** k subsequently referred to as the **ground field**. k is necessarily infinite; otherwise, $f(x) = 1 + \prod_{a \in k}(x - a)$ would be a nontrivial polynomial without zeroes. In particular, we can identify polynomials in $k[x_1, \ldots, x_n]$ with polynomial functions on k^n.

142. Definition. An **algebraic set of** k^n is the common zero locus of a finite number of polynomial equations, i.e., a set of the form

$$X = \mathcal{V}(f_1, \ldots, f_n) := \{(a_1, \ldots, a_n) \in k^n \mid f_1(a_1, \ldots, a_n) = \ldots = f_n(a_1, \ldots, a_n) = 0\}.$$

143. Remark. In fact, X only depends on the ideal generated by $f_1, \ldots, f_n$. Since $k[x_1, \ldots, x_n]$ is Noetherian, the algebraic sets are exactly the sets

$$\mathcal{V}(I) = \{x \in k^n \mid f(x) = 0 \text{ for all } f \in I\}$$

for an ideal $I \subset k[x_1, \ldots, x_n]$. Conversely, given an algebraic set X we define its **associated ideal** by

$$\mathcal{I}(X) = \{f \in k[x_1, \ldots, x_n] \mid f(x) = 0 \text{ for all } x \in X\}.$$

We obviously have

$$Y \subset X \Rightarrow \mathcal{I}(X) \subset \mathcal{I}(Y) \quad \text{and} \quad I \subset J \Rightarrow \mathcal{V}(J) \subset \mathcal{V}(I).$$

144. Example. First we recall that

$$1 \in I \iff I = k[x_1, \ldots, x_n],$$

an observation we will use quite often. Consider then, for instance, $\mathcal{I}(\{a\})$ for $a = (a_1, \ldots, a_n) \in k^n$. We claim that this is a maximal ideal equal to $(x_1 - a_1, \ldots, x_n - a_n)$. First, we note that $\mathcal{I}(\{a\})$ is the kernel of the evaluation map

$$\mathrm{ev}_a : k[x_1, \ldots, x_n] \to k, \quad f \mapsto f(a) = f(a_1, \ldots, a_n),$$

whence $\mathcal{I}(\{a\})$ is maximal. Moreover, the inclusion $(x_1 - a_1, \ldots, x_n - a_n) \subset \mathcal{I}(\{a\})$ is clear. Conversely, if f were in $\mathcal{I}(\{a\}) \setminus (x_1 - a_1, \ldots, x_n - a_n)$, then on degree grounds, $\mathrm{NF}(f | x_1 - a_1, \ldots, x_n - a_n) = b \in k$, whence we have a standard form $f - b = \sum q_i(x_i - a_i)$, $q_i \in k[x_1, \ldots, x_n]$. It follows that $b \in I$, whence $1 \in I$, a contradiction.

When is $\mathcal{V}(I)$ nonempty?

145. Theorem (Weak Nullstellensatz) [CLS, 4.1.1]. *$\mathcal{V}(I) \neq \emptyset$ if and only if I is a proper ideal of $k[x_1, \ldots, x_n]$.*

Clearly, we have $X = \mathcal{V}(\mathcal{I}(X))$ for any algebraic set X. What about $\mathcal{I}(\mathcal{V}(I))$?

146. Definition. The **radical of** I is the ideal $\sqrt{I}$ defined by

$$\sqrt{I} = \{a \in k[x_1, \ldots, a_n] \mid \text{there exists } n \in \mathbb{N} \text{ such that } a^n \in I\}.$$

Note that $I \subset \sqrt{I}$ and $\sqrt{\sqrt{I}} = \sqrt{I}$. I is called **reduced** or **radical** if $\sqrt{I} = I$.

147. Theorem (Hilbert's Nullstellensatz) [CLS, 4.2.6], [CLS, 4.5.11].

$$\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$$

In particular, $\mathcal{V}(\cdot)$ and $\mathcal{I}(\cdot)$ set up a bijection between algebraic subsets of k^n and the set of radical ideals in $k[x_1, \ldots, x_n]$. For instance, points $a = (a_1, \ldots, a_n) \in k^n$ correspond to maximal ideals $\mathfrak{m} \subset k[x_1, \ldots, x_n]$.

Computation of the radical

There are algorithms using Gröbner bases to compute the radical of an ideal. However, this requires some further technical tools so we content ourselves with an example using the built-in command RADICAL of SINGULAR.

```
> ring A=0,(x,y,z),dp;
> LIB "primdec.lib"; //loads library "primdec.lib" containing the
command RADICAL
// ** loaded /usr/bin/../share/singular/LIB/primdec.lib
⋮
> ideal I=xyz,x2,y4+y5;
> ideal RI=radical(I);
>RI;
RI[1]=x
RI[2]=y2+y
```

Practical application 6: Radical membership problem [GP, Section 1.8.6]

Problem: Let $I = (f_1, \ldots, f_k)$ be an ideal of $k[\mathbf{x}]$ and let $>$ be a monomial ordering on $\mathrm{Mon}(x_1, \ldots, x_n)$. Given $f \in k[\mathbf{x}]$ we want to determine whether or not $f \in \sqrt{I}$.

Solution: Recall Rabinovich's trick we used for the proof of Hilbert's Nullstellensatz 147. This is the statement that

$$f \in \sqrt{I} \iff 1 \in \widehat{I} := (f_1, \ldots, f_k, 1 - tf) \subset k[\mathbf{x}, t]$$

for some additional new variable t. But this is the membership problem 90 which we already solved.

Radical membership problem [GP, 1.8.9]

```
> ring A=0,(x,y,z),dp;
> ideal I=x5,xy3,y7,z3+xyz;
> poly f=x+y+z;
> ring B=0,(t,x,y,z),dp;
> ideal I=imap(A,I);
> poly f=imap(A,f);
> ideal II=I,1-t*f;
> std(II);
_[1]=1
> LIB"primdec.lib"; //for a cross check, compute √I directly
> setring A;
> radical(I);
_[1]=z
_[2]=y
_[3]=x
```

Practical application 7: Computing sodukos [DP, Section 3]

				5			8	
				6	2			5
6			4			7		
		7				9	6	
		5	2		6	1		
	3	6				4		
		3			7			4
1			5	8				
	6			1				

Source: W. Decker and G. Pfister, *A First Course in Computational Algebraic Geometry*, Lecture notes, p. 104

Problem: Suppose we are given a **well-posed** Sudoku, that is, we are given a collection of numbers in $\{1, \ldots, 9\}$ so that the Sudoku has a unique solution.

Solution: We represent the $9 \cdot 9 = 81$ cells by the variables $x_1, \ldots, x_{81}$. Then the entry a_i in the i-th cell of a completed Sudoku satisfies $a_i \in \{1, \ldots, 9\}$ if and only if a_i is a root of $F_i(x) = F_i(x_i) = \prod_{k=1}^{9}(x_i - k) \in \mathbb{Q}[x_i]$.

Let $1 \leq i < j \leq 81$. If $a = (a_1, \ldots, a_{81}) \in V(x_i - x_j)$, that is, $a_i = a_j$, then $F_i(a_i) = F_j(a_j)$, whence $F_i(x_i) - F_j(x_j)$ vanishes on $V(x_i - x_j)$ and is thus divisible by $x_i - x_j$. Consequently, the polynomials

$$G_{ij}(x) = G_{ij}(x_i, x_j) = \frac{F_i(x_i) - F_j(x_j)}{x_i - x_j} \in \mathbb{Q}[x_i, x_j],\ i < j.$$

are well-defined. The condition that neither a row, nor a column, nor a distinguished 3×3-block in a completed Sudoku has repeated entries can be implemented as follows. Set

$$\begin{aligned} E = \{&(i,j) \mid 1 \leq i < j \leq 81, \text{ and the } i\text{th and } j\text{th cell are in the same} \\ &\text{row, column, or distinguished } 3 \times 3\text{-block}\}. \end{aligned}$$

Let $I \subset \overline{\mathbb{Q}}[x_1, \ldots, x_{81}]$ ($\overline{\mathbb{Q}}$ = algebraic closure of $\mathbb{Q}$) be the ideal which is generated by the 891 polynomials F_i, $i = 1, \ldots, 81$, and G_{ij}, $(i,j) \in E$.

148. Proposition [DP, 3.1]. *Let $a = (a_1, \ldots, a_{81}) \in \overline{\mathbb{Q}}^{81}$. Then $a \in \mathcal{V}(I) \subset \overline{\mathbb{Q}}^{81}$ if and only if $a_i \in \{1, \ldots, 9\}$, for $i = 1, \ldots, 81$, and $a_i \neq a_j$, for $(i,j) \in E$.*

Put differently, a completed Sudoku is nothing but a point in $\mathcal{V}(I) \subset \overline{\mathbb{Q}}^{81} \cap \mathbb{Q}^{81}$, or equivalently, a maximal ideal in $\overline{\mathbb{Q}}[x_1, \ldots, x_{81}]$ containing $\sqrt{I}$.

149. Proposition [DP, 3.2]. *Let S be a well–posed Sudoku with preassigned numbers $\{a_i\}_{i \in L}$, for some subset $L \subset \{1, \ldots, 81\}$. We assign to S the ideal $I_S = I + (\{x_i - a_i\}_{i \in L})$. Then I_S is the maximal ideal corresponding to the completed sudoko $(a_1, \ldots, a_{81})$, that is, $I_S = \{x_1 - a_1, \ldots, x_{81} - a_{81}\}$. We can determine the a_i by computing the reduced Gröbner basis of I_S with respect to any monomial ordering.*

3	4	1	7	5	9	2	8	6
8	7	9	1	6	2	3	4	5
6	5	2	4	3	8	7	9	1
2	1	7	3	4	5	9	6	8
4	8	5	2	9	6	1	3	7
9	3	6	8	7	1	4	5	2
5	9	3	6	2	7	8	1	4
1	2	4	5	8	3	6	7	9
7	6	8	9	1	4	5	2	3

150. Definition.

(i) Let X be some set and $\mathcal{T}$ a subset of the power set of X. Then $\mathcal{T}$ is said to define a **topology on** X if the following conditions hold:

- $\emptyset, X \in \mathcal{T}$
- $F_1, \ldots, F_s \in \mathcal{T}$, then $\bigcup_{i=1}^{s} F_i \in \mathcal{T}$
- If $F_i \in \mathcal{T}$, I any indexing set, then $\bigcap_{i \in I} F_i \in \mathcal{T}$.

The elements of $\mathcal{T}$ are called **closed sets**; their complements $X \setminus F$, F closed, are called **open sets**. X together with the topology $\mathcal{T}$ is called a **topological space**. If $Y \subset X$, $\mathcal{T}_Y = \{F \cap Y \mid F \in \mathcal{T}\}$ defines a topology on Y, the so-called **subspace topology**.

(ii) A map $f : X \to Y$ between topological spaces is called **continuous**, if for each closed subset G of Y, $f^{-1}(G)$ is a closed subset of X.

151. Remark. The set theoretic de Morgan rules imply that one can equally well define a topology by its open sets, and a function $f : X \to Y$ is continuous if any preimage under f of an open set of Y is open in X. For instance, the usual Euclidean topology on $\mathbb{R}^n$ are the open sets which are arbitrary unions of open balls. Functions $f : \mathbb{R}^m \to \mathbb{R}^n$ which are continuous with respect to this topology are precisely the functions which satisfy $f(x_n) \to f(x)$ for any sequence $x_n \to x$.

152. Proposition [CLS, 4.3.4, 4.3.15]. *For ideals $\{I_\lambda\}_{\lambda\in\Lambda}$ and J in $k[x_1,\dots,]$, we have*

$$\mathcal{V}(\sum_\lambda I_\lambda) = \bigcap_\lambda \mathcal{V}(I_\lambda) \quad \text{and} \quad \mathcal{V}(I\cap J) = \mathcal{V}(I)\cup\mathcal{V}(J).$$

In particular, the set of algebraic sets defines a topology on k^n, the so-called **Zariski topology**. *We therefore get a correspondence compatible with the lattice structure between closed sets of k^n and radical ideals of $k[x_1,\dots,x_n]$.*

153. Example.

(i) For $X = k$ endowed with the Zariski topology the algebraic sets other than $\emptyset$ and k are the zeroes of a polynomial for $k[x]$ is principal. In particular, they are finite. It follows that proper nonempty subsets of k are Zariski open in if and only if their complement is finite. In particular, nonempty open subsets are dense, and the Zariski topology is not Hausdorff on k.

(ii) For any $f \in k[x_1,\dots,x_n]$ define the so-called **basic open set** by $k^n \setminus \mathcal{V}(f)$. It is easy to see that the basic open sets form a base for the Zariski topology, i.e., every open set is a union of basic open sets.

Operations on ideals [GP, Section 1.8.7]

It is easy to compute the intersection of two ideals I and J of $k[x_1, \ldots, x_n]$ via elimination orderings. SINGULAR has the built-in command INTERSECT:

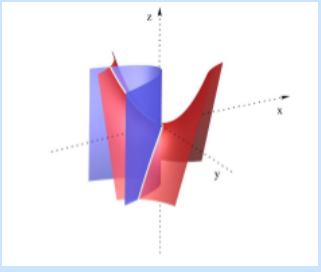
```
> ring A=0,(x,y,z),dp;
> ideal I=x,y;
> ideal J=y2,z;
> intersect(I,J);
_[1]=yz
_[2]=xz
_[3]=y2
```

154. Definition. A closed set is called **irreducible** if it is not the union of two strictly smaller closed subsets. An **affine variety** is an irreducible closed set.

155. Proposition [CLS, 4.5.3]. *An algebraic set X is an affine variety if and only if $\mathcal{I}(X)$ is prime. In particular, there is a one-to-one correspondence between affine varieties in k^n and prime ideals of $k[x_1, \ldots, x_n]$.*

156. Examples. Any point in k^n corresponds to a maximal ideal (weak Nullstellensatz). Hence they are irreducible; this, of course, can be checked directly. On the other hand, k^n with its Zariski topology is irreducible, but this is difficult to show by using the definition unless $n = 1$ (do you see why this case is special?). The **twisted cubic curve** $C = \{(t, t^2, t^3) \mid t \in k\} =$
$\mathcal{V}(y - x^2) \cap \mathcal{V}(z - x^3)$ in k^3 is irreducible as $\mathcal{I}(C) = (y - x^2, z - x^3)$ is prime.

157. Definition. The affine variety k^n is called **affine space** and written $\mathbb{A}^n_k$ or simply $\mathbb{A}^n$.



The intersection of $V(y - x^2)$ and $V(z - x^3)$

Source: W. Decker and G. Pfister, *A First Course in Computational Algebraic Geometry*, Lecture notes, p. 18

158. Proposition [CLS, 4.5.13]. *An algebraic set X is irreducible if and only if for every closed subset Y of X, the difference $X \setminus Y$ is Zariski dense in X. In particular, an open subset of an irreducible algebraic set is always dense.*

159. Definition. A topological space X is **Noetherian** if any descending chain of closed sets becomes stationary, that is, for $X \supset X_0 \supset X_1 \supset X_2 \supset \ldots$, X_i closed in X, there exists N such that $X_N = X_{N+1} = X_{N+2} = \ldots$.

160. Proposition [CLS, 4.6.1]. *Any algebraic set of $\mathbb{A}^n$ is Noetherian with respect to the induced subspace topology.*

161. Proposition [CLS, 4.6.4]. *Every algebraic set X can be written as a finite union*

$$X = X_1 \cup \ldots \cup X_k$$

of affine varieties X_i with $X_i \not\subseteq X_j$ if $i \neq j$. The set $\{X_1, \ldots, X_k\}$ is uniquely determined. Its elements X_i are called the **components** *of X.*

162. Remark.

(i) If $X = \mathcal{V}(I)$ is an algebraic set with irreducible components $X_i = \mathcal{V}(P_i)$, then the P_i are the **minimal** primes containing I, that is, there is no prime ideal Q containing I and strictly contained in one of the P_i. If $I = \sqrt{I}$ is a radical ideal, then the decomposition into irreducibles $\mathcal{V}(I) = \bigcup_i X_i$ corresponds to the decomposition $I = \sqrt{I} = \bigcap P$ where the union is taken over all prime ideals P with $I \subset P$ and P is prime and minimal, cf. the problem class.

(ii) Let X, $Y \subset \mathbb{A}^n_k$ be two closed subsets with $Y \subset X$. Then $X \setminus Y$ is Zariski dense in X if and only if Y contains no irreducible component of X.

Computing the decomposition 1

```
> LIB "primdec.lib";
> ring A=0,(x,y,z),dp;
> ideal I=xy; ideal J=y-x2,z-x3;
> radical(I);
_[1]=xy //The ideal I is radical
> primdecGTZ(I); //The ideals [i][1] are the prime ideals of the
irreducible components. The ideals [i][2] are only relevant if I is not
radical.
[1]:
 [1]:
_[1]=y
 [2]:
_[1]=y
[2]:
 [1]:
_[1]=x
 [2]:
_[1]=x
```

Computing the decomposition 2

```
> reduce(radical(J),std(J));
_[1]=0
_[2]=0 //The ideal J is radical.
> primdecGTZ(J);
[1]:
 [1]:
_[1]=y3-z2
_[2]=-y2+xz
_[3]=xy-z
_[4]=x2-y
 [2]:
_[1]=y3-z2
_[2]=-y2+xz
_[3]=xy-z
_[4]=x2-y
> reduce(-y2+xz,std(J));
0
> reduce(y3-z2,std(J));
0 //The ideal J is even prime.
```

163. Definition. Let $X \subset \mathbb{A}^{n_1}$ and $Y \subset \mathbb{A}^{n_2}$ be two algebraic sets. A map

$$F : X \to Y$$

will be called a **morphism** if there exists n_2 polynomials $f_1, \ldots, f_{n_2} \in k[x_1, \ldots, x_{n_1}]$ such that

$$F(p) = \big(f_1(p_1, \ldots, p_{n_1}), \ldots, f_{n_2}(p_1, \ldots, p_{n_1})\big)$$

for all points $p = (p_1, \ldots, p_{n_1}) \in X$. We denote by $\mathrm{Hom}(X, Y)$ the set of morphisms between X and Y. If $Y = \mathbb{A}^1 \cong k$ then we call F a **regular function**.

164. Proposition [CLS, 5.1.2]. *Two polynomials f and $g \in k[x_1, \ldots, x_n]$ define the same regular function on an algebraic set X if and only if $f - g \in \mathcal{I}(X)$.*

165. Definition. If $X \subset \mathbb{A}^n$ is an algebraic set, we call

$$A(X) := k[x_1, \ldots, x_n]/\mathcal{I}(X)$$

the **coordinate ring** of X.

166. Remark.

(i) The coordinate ring of an affine variety is a finitely generated k-algebra which is an integral domain if X is an affine variety. Such ring is also called an **affine ring** for every affine ring is isomorphic with the coordinate ring of an affine variety, cf. Proposition 170. In view of Proposition 164 we can regard $A(X)$ as the ring of regular functions on X.

(ii) Fix a monomial ordering on $k[x_1, \ldots, x_n]$. For an ideal I let the **complement of monomials** be the set $\mathcal{C}(I) := \{\alpha \in \mathbb{N}^n \mid x^\alpha \notin I\}$. Then the reduced normal form identifies the coordinate ring $A(X) = k[x_1, \ldots, x_n]/\mathcal{I}(X)$ as a *k-vector space* with $\bigoplus_{\alpha \notin \mathcal{C}(\mathcal{I}(X))} k \cdot x^\alpha$, cf. also [CLS, 5.3.1,4] and the problem class.

167. Definition. Let $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$ be affine varieties. We say that X and Y are isomorphic if there exist polynomial mappings $\alpha : X \to Y$ and $\beta : Y \to X$ such that $\alpha \circ \beta = \mathrm{Id}_Y$ and $\beta \circ \alpha = \mathrm{Id}_X$.

168. Theorem [CLS, 5.4.8, 5.4.9]. *If X and Y are affine varieties, then there is a natural isomorphism $\mathrm{Hom}(X, Y) \cong \mathrm{Hom}_k(A(Y), A(X))$ by assigning $F : X \to Y$ to the k-algebra morphism $F^* : A(Y) \to A(X)$, $F^*\bar{G} = \overline{G \circ F}$. In particular, two affine varieties are isomorphic if and only if their coordinate rings are isomorphic.*

169. Example. The map $F^* : k[x, y, z] \to k[t]$ induced by $F(x) = t$, $F(y) = t^2$ and $F(z) = t^3$ (cf. Proposition 10) induces actually an isomorphism $k[x, y, z]/(y - x^2, z - x^3)$ corresponding to the morphism $\mathbb{A}^1 \to C$, $t \mapsto (t, t^2, t^3)$. Therefore, the twisted cubic is isomorphic with $\mathbb{A}^1$. On the other hand, $t \mapsto (t^2, t^3)$ induces a morphism $\mathbb{A}^1 \to X = \{y^3 - x^2 = 0\} \subset \mathbb{A}^2$ which does *not* induce an isomorphism $k[x, y]/(y^3 - x^2) \to k[t]$ (can you see why? Algebraically/Geometrically?).

170. Corollary (category of affine varieties vs. category of finitely generated k-algebras which are integral domains). *The assignement $X \to A(X)$ extends to a contravariant functor between the category of affine k-varieties + morphisms and the category of finitely generated, integral k-algebras + k-algebra morphisms. In particular, this defines an equivalence of categories.*

171. The projective space. The second natural space for doing geometry is the projective space $\mathbb{P}^n_k$ (or simply $\mathbb{P}^n$ if we do not wish to emphasise the ground field). This is the set of lines in k^{n+1} through the origin (=one dimensional subspaces of k^{n+1}). A line $\ell \in \mathbb{P}^n_k$ is determined by any of its points $0 \neq (x_0, \ldots, x_n) \in \ell$. Two points $x, y \in k^{n+1} \setminus \{0\}$ determine the same line if they differ by a nonzero scalar, i.e., $x = \lambda y$ for $\lambda \in k^*$. Hence we get a map

$$\pi : k^{n+1} \setminus \{0\}, \quad (x_0, \ldots, x_n) \mapsto \operatorname{span}((x_0, \ldots, x_n))_k$$

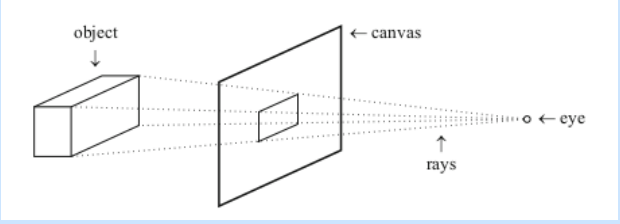
leading to the bijection $\mathbb{P}^n \cong k^{n+1} \setminus \{0\}/k^*$. Intuitively, it is clear that $\mathbb{P}^n_k$ should be an n-dimensional space. The line ℓ determined by the point $(x_0, \ldots, x_n)$ will be denoted by $[x_0 : \ldots : x_n]$ – these are the **homogeneous coordinates** of ℓ. These give rise to the subsets $U_i = \{[x_0 : \ldots : x_n] \mid (x_0, \ldots, x_n) \in k^{n+1} \setminus \{0\},\ x_i \neq 0\}$ which we identify with k^n via the bijections

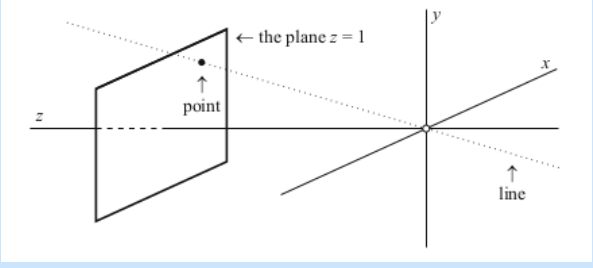
$$U_i \to k^n, \quad (x_0, x_1, \ldots, x_n) \mapsto \left(\frac{x_0}{x_i}, \frac{x_1}{x_i}, \ldots, \frac{x_n}{x_i}\right)$$

with x_i/x_i omitted. This yields two important ways of understanding $\mathbb{P}^n$:

- $\mathbb{P}^n_k = \bigcup_{i=0}^n U_i$, the **standard covering** of $\mathbb{P}^n$.
- $\mathbb{P}^n_k = k^n \cup \mathbb{P}^{n-1}_k$ with $k^n \cong U_i$, $\mathbb{P}^{n-1}_k = U_i^c$, the **cellular decomposition**.

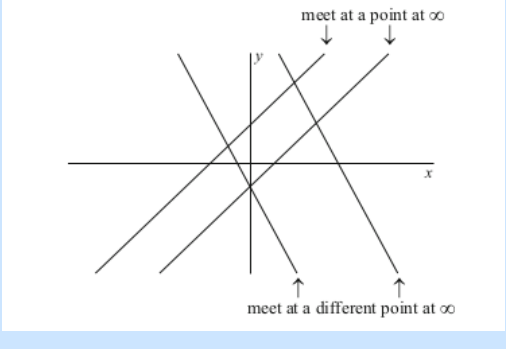
172. The cellular decomposition.

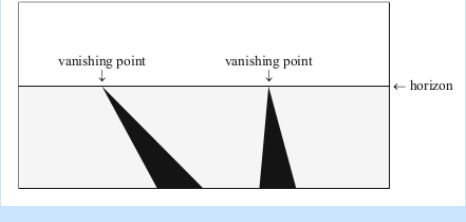




Source: D. Cox, J. Little and D. O'Shea, *Ideals, algorithms and varieties*, pp. 390 and 391

173. Geometrical motivation of projective space. We obtain projective spaces by adding the horizon at infinity to lines, planes etc.





Source: D. Cox, J. Little und D. O'Shea, *Ideals, algorithms and varieties*, S. 386

It is customary to denote by S the polynomial ring $k[x_0, \ldots, x_n]$ together with the standard grading $\bigoplus_{\nu \geq 0} S_\nu$, $S_\nu =$ the k-span of monomials of total degree ν.

174. Definition. An **algebraic set** in $\mathbb{P}^n_k$ is the common zero locus of a finite set of homogeneous polynomials in $S = k[x_0, \ldots, x_n]$.

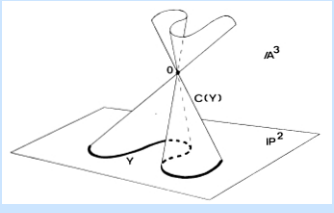
175. Algebraic sets and homogeneous ideals. For a homogeneous ideal I we define

$$\mathcal{V}_p(I) = \{[x_0 : \ldots : x_n] \in \mathbb{P}^n_k \mid f(x_0, \ldots, x_n) = 0 \text{ for all homogeneous } f \in I\}.$$

Conversely, for an algebraic set $X \subset \mathbb{P}^n$ we consider the homogeneous ideal

$$\mathcal{I}_p(X) = \text{ideal generated by all homogeneous polynomials in } S \text{ which vanish identically on } X.$$

176. Remark. A homogeneous ideal $I \subset S$ defining the projective algebraic set X also gives the affine algebraic set $C(X) := \{x \in k^{n+1} \mid f(x) = 0 \text{ for all } f \in I\}$, the so-called **cone of** X. Of course, this is just $\mathcal{V}(I) \subset \mathbb{A}^{n+1}$ if we consider I as an ideal of $k[x_0, \ldots, x_n]$.



The cone $C(X)$ over the curve $X = \mathcal{V}_p(I)$ in $\mathbb{P}^2_k$

Source: R. Hartshorne, *Algebraic Geometry*, Springer, 1977, p. 12

The following properties are also useful (cf. problem class or for instance Section VII.2 in P. Samuel and O. Zariski, *Commutative Algebra vol. 2*, Springer, 1960):

(i) The sum, product, intersection and radical of homogeneous ideals is also homogeneous.

(ii) Let I be a homogeneous ideal of $S = k[x_0, \ldots, x_n]$. Then I is prime if and only if for any pair of *homogeneous* elements f, g of S we have: $f \cdot g \in I \Leftrightarrow f \in I$ or $g \in I$.

It follows that if $\{I_\lambda\}_{\lambda\in\Lambda}$ is a family of homogeneous ideals, $\bigcap_\lambda \mathcal{V}_p(I_\lambda) = \mathcal{V}_p(\bigcup_\lambda I_\lambda)$; if $I_{1,2}$ are two homogeneous ideals, $\mathcal{V}_p(I_1) \cup \mathcal{V}_p(I_2) = \mathcal{V}_p(I_1 \cap I_2)$. In particular, projective algebraic sets define a topology which is again Noetherian.

177. Definition. The **Zariski topology on** $\mathbb{P}^n$ is defined by algebraic sets $\mathcal{V}_p(I)$ of $\mathbb{P}^n$, $I \subset S$ homogeneous, as closed sets. An irreducible algebraic set in $\mathbb{P}^n$ is called a **projective variety**.

178. Proposition [CLS, 8.3.6]. *Every projective algebraic set X can be decomposed into irreducible projective algebraic sets. Furthermore, a projective algebraic set X is a projective variety if and only if $\mathcal{I}(X)$ is prime.*

179. Examples.

(i) If X is a closed projective set, then $\pi^{-1}(X) = C(X) \cap \mathbb{A}^{n+1} \setminus \{0\}$ is closed in $\mathbb{A}^{n+1} \setminus \{0\}$. It follows that $\pi : \mathbb{A}^{n-1} \setminus \{0\} \to \mathbb{P}^n$ is continuous with respect to the (induced) Zariski topologies. Moreover, it is easy to see that the identification of U_i with k^n is actually a homeomorphism $U_i \cong \mathbb{A}^n$ between the (induced) Zariski topologies, that is, it is a bijective continuous map with continuous inverse (cf. Paragraph 171).

(ii) k-dimensional **Linear varieties** Λ^k of $\mathbb{P}^n$ are defined by linear homogeneous equations. Equivalently, they are of the form $\pi(V \setminus \{0\})$ for a $k+1$-dimensional linear subspace $V^{k+1} \subset k^{n+1}$. In particular, they given by the equations $x_0 = \ldots = x_{n-k} = 0$ for suitably chosen coordinates $x_0, \ldots, x_n$. In particular, $\mathcal{I}(\Lambda^k)$ is prime for $k[x_0, \ldots, x_n]/\mathcal{I}(\Lambda^k) \cong k[x_{n-k+1}, \ldots, x_n]$ is an integral domain, and $\Lambda^k \cong \mathbb{P}^k_n$. For instance, $U_i^c = V(x_i)$ is closed so that the standard covering is an *open* covering by the open subsets U_i; the cellular decomposition $\mathbb{P}^n = U_i \cup V(x_i)$ is a decomposition into an open subset U_i homeomorphic to the affine space $\mathbb{A}^n$ and a closed subset $V(x_i)$ which is the "horizon" at infinity of the affine space $U_i \cong \mathbb{A}^n$ (cf. Paragraph 173).

(ii) The **(projective) twisted cubic** is the projective algebraic set $X = \mathcal{V}_p(ty - x^2, t^2z - x^3, xz - y^2) \subset \mathbb{P}^3$. If $U_t = \{[t : x : y : z] \mid t \neq 0\} \subset \mathbb{P}^3$, then $U_t \cap X$ is mapped to (x', y', z') with $x' = x/t$, $y' = y/t$ and $z' = z/t$ with $y' - x'^2 = 0$, $z' - x'^3 = 0$ and $x'z' - y'^2 = 0$. The last equation is redundant so that we find the affine twisted cubic discussed in Example 156. If we intersect with the "hyperplane at infinity" given by $H = \mathcal{V}_p(t)$, then $H \cap X = V_p(t, ty - x^2, t^2z - x^3, xz - y^2) = \{[0 : 0 : 0 : 1]\}$ is the point "added at infinity". X is irreducible as the closure of the irreducible affine twisted cubic [CLS, 8.4.7].

180. Theorem (projective weak Nullstellensatz) [CLS, 8.3.9 and 8.3.10]. *If $I \subset S$ is a homogeneous ideal with $\mathcal{V}_p(I) \neq \emptyset$, then*

$$\mathcal{I}_p(\mathcal{V}_p(I)) = \sqrt{I}.$$

In particular, $\mathcal{I}_p$ and $\mathcal{V}_p$ set up inclusion-reversing bijections between nonempty projective varieties and radical homogeneous ideals properly contained in $(x_0, \ldots, x_n)$.

181. The algebra-geometry dictionary. ($A = k[x_1, \ldots, x_n]$, $S = k[x_0, x_1, \ldots, x_n]$)

algebraic sets in $\mathbb{A}^n$	$\longleftrightarrow$	radical ideals of A
affine varieties in $\mathbb{A}^n$	$\longleftrightarrow$	prime ideals of A
points in $\mathbb{A}^n$	$\longleftrightarrow$	maximal ideals of A
morphisms of affine varieties $X \to Y$	$\longleftrightarrow$	k-algebra morphisms $A(Y) \to A(X)$
algebraic sets in $\mathbb{P}^n$	$\longleftrightarrow$	radical ideals of S contained in $(x_0, \ldots, x_n)$
ascending chain condition	$\longleftrightarrow$	descending chain condition
$\sqrt{I} = \bigcap_{I \subset P} P$ minimal primes	$\longleftrightarrow$	$X = \bigcup X_i$ irreducibles

182. Remark. Note that unlike the (affine) coordinate ring $A(X)$, the graded **homogeneous coordinate ring** $S(X) := S/\mathcal{I}(X)$ is *not* a ring of functions. This will be remedied by introducing the *sheaf of regular functions*, see the course Algebraic Geometry 1.

Let $I \subset S$ be a homogeneous ideal so that the Hilbert function and thus the Hilbert polynomial of the graded ring S/I are defined.

183. Definition. The **dimension** of a nonempty projective algebraic set X is the degree of the Hilbert polynomial of $S(X)$.

184. Example. According to Example 136, $\dim \mathbb{P}^n = n$ which matches our geometric intuition.

185. The dimension of an algebraic set. We will now discuss the geometric meaning of this definition. Here, the idea is that dimension should be invariant under certain deformations or degenerations to a geometrically obvious case with a "natural" dimension. For instance, consider $I = (x^2y, x^3) \subset k[x, y]$. Then

$$\mathcal{V}(I) = \mathcal{V}(x^2y) \cap \mathcal{V}(x^3) = (\mathcal{V}(x) \cup \mathcal{V}(y)) \cap \mathcal{V}(x) = \mathcal{V}(x).$$

Regarded as an affine algebraic set in $\mathbb{A}^2$, $\mathcal{V}(x) \cong \mathbb{A}^1$, so its dimension should be 1. However, regarded as a projective algebraic set in $\mathbb{P}^1$, $\mathcal{V}(x) = \{[0 : 1]\}$, so its dimension should be 0.

To generalise the last example we call a projective algebraic set **monomial** if it is of the form $V_p(I)$ for some monomial ideal $I \subset S = k[x_0, \ldots, x_n]$.

186. Proposition [CLS, 9.1.1]. *If $I \subset S$ is a monomial ideal, then $V_p(I)$ is a finite union of linear varieties of $\mathbb{P}^n$.*

187. Definition. Let $I \subset S$ be a monomial ideal. Then the **dimension of** $\mathcal{V}_p(I)$ denoted by $\dim \mathcal{V}_p(I)$ is the maximal dimension of its linear varieties. Note that $\dim \mathcal{V}_p(I) = \mathcal{V}_p(\sqrt{I})$.

Assume we are given a monomial ideal I generated by monomials $m_1, \ldots, m_t \in k[x_0, \ldots, x_n]$. To compute the dimension we need to determine the component of $\bigcap V(m_i)$ of largest dimension. If $x_{i_0}, \ldots, x_{i_r}$ are variables such that at least one appears in each monomial m_j, then $x_{i_0} = \ldots = x_{i_r} = 0$ is contained in $\mathcal{V}(I)$. We therefore let

$$M_j = \{\ell \in \{0, \ldots, n\} \mid x_\ell \text{ divides the monomial } m_j\}$$

and

$$\mathcal{M} = \{J \subset \{0, \ldots, n\} \mid J \cap M_j \neq \emptyset \text{ for all } 0 \leq j \leq t\}.$$

188. Proposition [CLS, 9.1.3]. *We have*

$$\dim \mathcal{V}_p(I) = n - \min(|J| \mid J \in \mathcal{M}),$$

where $|J|$ is the number of elements of the set J.

189. Example. If $I = (x^2y, x^3)$ is as above, then $M_1 = \{0, 1\}$ and $M_2 = \{0\}$. It follows that $\mathcal{M} = \{\{0\}, \{0,\ 1\}\}$, whence $\dim \mathcal{V}_p(I) = 0$.

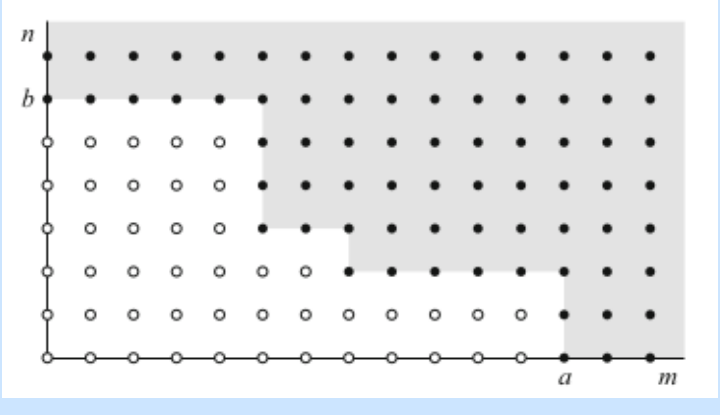
190. Coordinate subspaces. Consider a monomial ideal $I \subset k[x_0, \ldots, x_n]$. We consider again the complement of monomials $\mathcal{C}(I) := \{\alpha \in \mathbb{N}^n \mid x^\alpha \notin I\}$. Further, setting $e_i = (0, \ldots, 1, \ldots, 0)$ as usual, we define the **coordinate subspace** of $\mathbb{N}^n$ determined by $e_{i_1}, \ldots, e_{i_r}$ as follows:

$$[e_{i_1}, \ldots, e_{i_r}] = \{\sum_{j=1}^{r} a_j e_{i_j} \mid a_j \in \mathbb{N}\}$$

Its **dimension** is r by definition. Its **translate by** $\alpha \in \mathbb{N}^n$ is the set

$$\alpha + [e_{i_1}, \ldots, e_{i_r}] = \{\alpha + \beta \mid \beta \in [e_{i_1}, \ldots, e_{i_r}]\}.$$

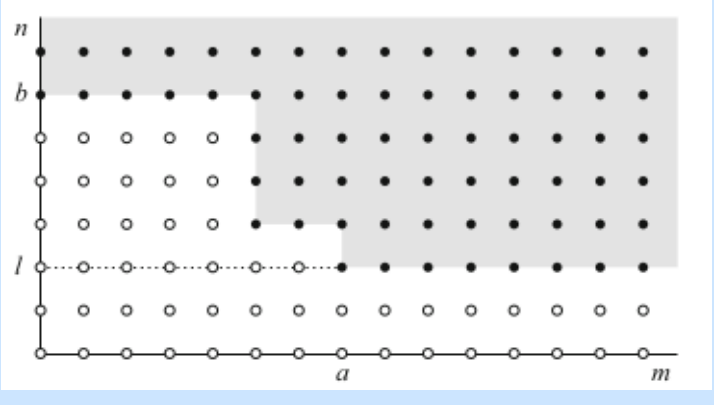
191. Example.



Let $I = (y^6, x^5y^3, x^7y^2, x^{12})$. The exponents in $\mathcal{C}(I)$ are given by open circles.

Source: D. Cox, J. Little and D. O'Shea, *Ideals, algorithms and varieties*, pp. 474

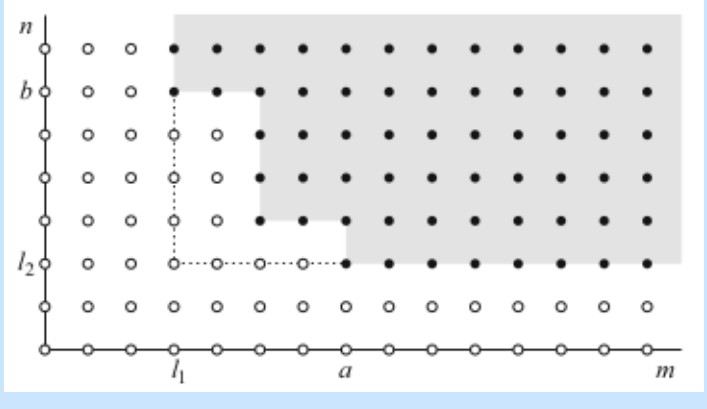
192. Example.



Let $I = (y^6, x^5y^3, x^7y^2)$. The exponents in $\mathcal{C}(I)$ are the open circles.

Source: D. Cox, J. Little and D. O'Shea, *Ideals, algorithms and varieties*, pp. 474

193. Example.



Let $I = (x^3y^6, x^5y^3, x^7y^2)$. The exponents in $\mathcal{C}(I)$ are the open circles.

Source: D. Cox, J. Little and D. O'Shea, *Ideals, algorithms and varieties*, pp. 475

194. Example. Consider a proper monomial ideal $I \subset k[x, y]$. Then $\mathcal{V}_p(I)$ is either

(i) empty, and x^a and $y^b \in I$ for some positive integers a and b. Further, $\mathcal{C}(I)$ consists of a finite number of points, cf. Example 191.

(ii) or the point $[x : y] = [1 : 0]$, and $x^a \notin I$ for all $a > 0$, but $y^b \in I$ for some b. Further, $\mathcal{C}(I)$ consists of a finite number of translates of $[e_1]$ and possibly of a finite number points not contained in these translates, cf. Example 192.

(iii) or the point $[x : y] = [0 : 1]$, and $y^b \notin I$ for all $b > 0$, but $x^a \in I$ for some a. Further, $\mathcal{C}(I)$ consists of a finite number of translates of $[e_2]$ and possibly of a finite number points not contained in these translates.

(iv) or the union of the points $[1 : 0]$ and $[0 : 1]$, and xy must divide every monomial in I. Further, $\mathcal{C}(I)$ consists of a finite number of translates of $[e_1]$, of $[e_2]$, and possibly of a finite number points not contained in these translates, cf. Example 193.

195. Proposition [CLS, 9.2.1]. *Let $I \subset S$ be a proper monomial ideal.*

(i) *The linear variety $\mathcal{V}_p(x_i \mid i \notin \{i_0, \ldots, i_r\})$ is contained in $\mathcal{V}_p(I)$ if and only if $[e_{i_0}, \ldots, e_{i_r}] \subset \mathcal{C}(I)$.*

(ii) $\dim \mathcal{V}_p(I) + 1 =$ *the maximal dimension of the coordinate subspaces in $\mathcal{C}(I)$.*

196. Theorem [CLS, 9.2.3]. *If $I \subset S$ is a proper monomial ideal, then the set $\mathcal{C}(I) \subset \mathbb{N}^{n+1}$ of exponents of monomials not lying in I can be written as a finite union of translates of (possibly 0-dimensional) coordinate subspaces of $\mathbb{N}^{n+1}$.*

197. Lemma [CLS, 9.2.5]. *The number of points in a coordinate translate $\alpha + [e_{i_0}, \ldots, e_{i_m}]$ of total degree s is equal to*

$$\binom{m+s-|\alpha|}{s-|\alpha|} - \binom{m+s-1-|\alpha|}{s-1-|\alpha|},$$

provided that $s > |\alpha| + 1$.

198. Proposition [CLS, 9.3.3]. *Let I be a proper monomial ideal in $S = k[x_0, \ldots, x_n]$. For $\nu \geq 0$, $H_{S/I}(\nu)$ is the number of monomials not in I and of total degree s. Furthermore,* $\deg P_{S/I} = \dim \mathcal{V}_p(I)$.

199. Corollary (Dimension theorem) [CLS, 9.3.8]. *Let $I \subset S = k[x_0, \ldots, x_n]$ be a homogeneous ideal. Then*

$$\dim \mathcal{V}_p(I) = \dim \mathcal{V}_p(\mathrm{LM}(I)).$$

200. Remark. In a similar way we can consider monomial algebraic subsets in $\mathbb{A}^n$ and "affine" Hilbert functions to define the dimension of affine varieties, see [CLS, Section 9.3].

References

[CLS] D. Cox, J. Little and D. O'Shea
Ideals, algorithms and varieties
Springer, 2007

[DP] W. Decker and G. Pfister
A First Course in Computational Algebraic Geometry
Lecture notes

[EH] V. Ene and J. Herzog
Gröbner Bases in Commutative Algebra
AMS, 2012

[GP] G.-M. Greuel and G. Pfister
A Singular *introduction to commutative algebra*
Springer, 2002.