COMPUTATIONS WITH SINGULAR AND MACAULAY2.

This is a mathematical introduction to the computer algebra systems `Macaulay2` and `Singular`.

To do computations we need to specify a ring. We work with the polynomial ring $S = k[x_1 \ldots, x_n]$. We use multi-index notation x^a for the monomial $x_1^{a_1} \cdots x_n^{a_n}$. We have to choose the field k, which most often will be $\mathbb{Q}$ or a finite field, preferably $\mathbb{Z}/32003$. Polynomials are written out in a definite order. Two of the most used orders are the *lexicographic* ordering (`Lex`), defined by $x^a > x^b$ if and only if the first non-zero entry in the vector $a - b$ is positive, and the *graded reverse lexicographic* order (`GRevLex`): $x^a > x^b$ if and only if $\deg x^a > \deg x^b$ or the last non-zero entry in $a-b$ is negative. Both orders are compatible with the semi-group structure on the set of monomials: $x^a > x^b$ if and only if $x^{a+c} > x^{b+c}$. For the variables (x, y, z) the order `GRevLex` gives

$$x^2 > xy > y^2 > xz > yz > z^2 > x > y > z > 1\ ,$$

while `Lex` gives

$$x^2 > xy > xz > x > y^2 > yz > y > z^2 > z > 1\ .$$

In `Macaulay2` the graded reverse lexicographic order is default. In `Singular` we have to write this order as `dp`.

The ring declaration for a ring in four variables over $\mathbb{Q}$ is in `Macaulay2`

```
R = QQ[x,y,z,t]
```

and in `Singular`

```
ring R = 0, (x,y,z,t), dp;
```

The algorithms in `Macaulay2` and `Singular` heavily depend on Gröbner bases. To use the programs you do not need to know what these are, but some idea about it helps, especially if things don't work the way you want.

Let $f = \sum_{a \in \mathbb{N}^n} c_a x^a$ be a polynomial. The *exponent* of f is the highest occurring power: $\exp(f) = \max\{\, a \in \mathbb{N}^n \mid c_a \neq 0 \,\}$, where the maximum is taken with the chosen monomial order. The *leading term* of f is $L(f) := c_{\exp(f)} x^{\exp(f)}$. For an ideal I all leading terms form an ideal

$$L(I) = \{\, L(f) \mid f \in I \,\} \cup \{0\}.$$

By definition $L(I)$ is an ideal, generated by monomials, and computing with such ideals is much easier. This can be used for I, because for

homogeneous ideals among others the degree and the codimension of I and $L(I)$ are equal.

In general the leading terms of a system of generators of I do not generate the ideal $L(I)$: take for instance $f = x^2 + y^2$ and $g = x^2 - y^2$ as generators of the ideal $I = (x^2, y^2)$, then $I = L(I)$, but $L(f) = L(g) = x^2$.

Definition 1. A *standard* or *Gröbner basis* of an ideal I is a system of generators $(f_1, \ldots, f_k)$ of I with the property that the leading terms $L(f_1), \ldots, L(f_k)$ generate the ideal $L(I)$ of leading terms.

We can decide whether or not a polynomial belongs to an ideal, once we have a Gröbner basis. Let $(f_1, \ldots, f_k)$ be a Gröbner basis of the ideal I and g a polynomial. If $L(g) \notin L(I)$, then $g \notin I$, by definition of $L(I)$; conversely, if $L(g) \in L(I)$, then there exists an f_i, a constant c and a monomial x^m such that $L(g) = cx^m L(f_i)$ (this is because $L(I)$ is a monomial ideal) and therefore $\exp(g - cx^m f_i) < \exp(g)$. Because $g \in I$ if and only if $g - cx^m f_i \in I$, we can replace g by $g - cx^m f_i$. This process terminates after finitely many steps: either we find a g' with $L(g') \notin L(I)$, or g is reduced completely to 0.

In fact, we have here adivision algorithm, for division with remainder with respect to a Gröbner basis. Such an algorithm exists for every list $F = [f_1, \ldots, f_k]$ of polynomials. Define the remainder $R_F(g)$ inductively by $R_F(g) = R_F(g - cx^a f_j)$, if j is the smallest index, such that $L(g)$ is divisible by $L(f_j)$, and $L(g) = cx^a L(f_j)$; if $L(g)$ is not divisible by any $L(f_j)$, then $R_F(g) = L(g) + R_F(g - L(g))$. In general the remainder depends on the order of the polynomials in the list, but that is not the case for a Gröbner basis.

Let f and g be two (monic) polynomials with leading terms $L(f) = x^a$ and $L(g) = x^b$. These both divide the least common multiple x^M, so $x^{M-a} \cdot L(f) - x^{M-b} \cdot L(g) = 0$ is a relation (also called *syzygy*). We define the *S-polynomial* of f and g as

$$S(f, g) = x^{M-a} f - x^{M-b} g \, .$$

Then we have $\exp(S(f, g)) < M$. The algorithm to find a Gröbner basis works as follows. We start with a list $F = [f_1, \ldots, f_k]$ of generators of the ideal. We choose two elements f and g from this list and compute the remainder $R_F(S(f, g))$ of the S-polynomial of f and g w.r.t. the list F. If $R_F(S(f, g)) = 0$, then we found a syzygy between the polynomials of the list. Otherwise $R_F(S(f, g))$ has a leading terms, not contained in the ideal generated by the leading terms of the polynomials in our list, and we add the polynomial $R_F(S(f, g))$to the list, which we again call F. Because the ring $S = k[x_1, \ldots, x_n]$ is Noetherian, this process terminates after a finite number of steps. Then all remainders $R_F(S(f, g))$ are zero.

Theorem 2 (Buchberger). *The list $F = [f_1, \ldots, f_k]$ is a Gröbner basis of the ideal $I = (f_1, \ldots, f_k)$, if $R_F(S(f_i, f_j)) = 0$ for all $i < j$.*

Proof. If $x^a \in L(I)$, then $x^a = L(g)$ with $g = \sum \lambda_i f_i$. Let $m = \max_i\{\exp(\lambda_i f_i)\}$, then $m \geq a$. If $m = a$ we are ready. Otherwise we decrease m without changing g by adding syzygies $\sum r_\alpha f_\alpha = 0$ to g. For this let j be the smallest index met $\exp(\lambda_j f_j) = m$; because the monomial x^m does not occur in g, the term $L(\lambda_j f_j)$ has to cancel, so there exists a $j' > j$ with $\exp(\lambda_{j'} f_{j'}) = m$. The S-polynomial $S(f_j, f_{j'})$ gives a syzygy $S_{jj'} = \sum r_\alpha f_\alpha$ with $\exp(r_\alpha f_\alpha) < \exp(r_j f_j)$ for $\alpha \neq j, j'$ and $\exp(f_j r_j) = \exp(f_{j'} r_{j'}) \leq m$, so there is a $l \in \mathbb{N}^n$ with $L(\lambda_j f_j) = cx^l L(f_j r_j)$. We continue with $g = \sum_i \lambda_i f_i - cx^l S_{jj'}$. If we did not decrease m, at least j increased. □

Now put

$$\Delta(I) = \{f = \sum f_a x^a \in S \mid f_a = 0 \text{ if } a \in \exp(I)\} .$$

The natural map $\Delta(I) \to S/L(I)$ is an isomorphism of vector-spaces. The quotient S/I and $\Delta(I)$ are isomorphic as vector spaces, the map being given by $g \mapsto R_F(g)$. A reduced Gröbner basis is a basis in which all elements are reduced as far as possible, that is $f_i - L(f_i) \in \Delta(I)$.

Example 3. Let us compute with the innocent looking ideal

$$(a^5 - b^5, b^5 - c^5, c^5 - d^5, d^5 - e^5, a^4b + b^4c + c^4d + d^4e + e^4a)$$

in five variables.

This can be done in `Singular` as follows

```
ring r = 0, (a,b,c,d,e),dp;
ideal i = a^5-b^5,b^5-c^5,c^5-d^5,d^5-e^5,
a^4*b+b^4*c+c^4*d+d^4*e+e^4*a;
ideal gbi = std(i); // std computes a Gröbner basis
gbi; // display the ideal
```

and in `Macaulay2`:

```
R = QQ[a..e]
I = ideal(a^5-b^5,b^5-c^5,c^5-d^5,d^5-e^5,
a^4*b+b^4*c+c^4*d+d^4*e+e^4*a)
J = gb(I); -- semicolon to suppress output
gens J -- displays the generators
```

The ideal has a Gröbner basis consisting of 149 elements, with maximal degree 16 and in total 3063 monomials. In one variable more and one degree higher the total number of monomials is of the Gröbner basis is 382928.

The output of a computation can easily be more than a printed page. If equations become too complicated we have to content ourselves with numerical information: the number of equations, but also their degree and the degree and codimension of the ideal.

We conclude with some applications of Gröbner bases.

- Elimination
  Suppose we have two groups of variables, x_i and y_i. We want to eliminate the x_i from an ideal I. We choose a monomial order with the property: $f \in k[y] \Leftrightarrow L(f) \in k[y]$. An example is s product order, where we first order after the x_i and then after the y_i. If $\{g_1, \ldots, g_r\}$ is a Gröbner basis of I, then $\{g_1, \ldots, g_r\} \cap k[y]$ is a Gröbner basis of $I \cap k[y]$.
- Saturation
  By homogenising with a variable h we sometimes introduce extra zeroes at infinity ($h = 0$). To cut away these we compute the saturation $\mathrm{Sat}(I, h) = \{f \in S \mid fh^n \in I \text{ for a } n \in \mathbb{N}\}$. If we choose h as last variable in the graded reverse lexicografic order, then a homogeneous polynomial f is divisible by h if and only if $L(f)$ is divisible by h. We only need to divide all elements of the Gröbner basis by suitable powers of h and these are seen from the leading terms.
- The intersection of two ideals
  Let $\{f_1, \ldots, f_m\}$ generate the ideal I and $\{g_1, \ldots, g_n\}$ the ideal J. We form the matrix
  $$M = \begin{pmatrix} -1 & f_1 & \ldots & f_m & 0 & \ldots & 0 \\ -1 & 0 & \ldots & 0 & g_1 & \ldots & g_n \end{pmatrix}$$
  and compute a Gröbner basis of the kernel. The concept of Gröbner basis can easily be extend from ideals in the polynomial ring to submodules of free modules. We search for vectors of polynomials $r = (r_0, r_1, \ldots, r_{m+n})$ with $Mr = 0$. Then $r_0 - \sum r_i f_i = 0$ and $r_0 - \sum r_{m+j} g_j = 0$ and all such r_0 generate the ideal $I \cap J$. The command `intersect` does this for you.

Exercise

Compute the discriminant of a polynomial in one variable with undetermined coefficients in some cases of low degree. For a quadratic polynomial $ax^2 + bx + c$ the discriminant is $b^2 - 4ac$. We will consider monic polynomials, so $x^2 + px + q$ with discriminant $p^2 - 4q$. The discriminant vanishes if the polynomial has multiple roots, and one way to compute it is by taking the resultant of the polynomial f and its derivative f'. A compact formula is given by the Sylvester determinant, in our example

$$\begin{vmatrix} 1 & p & q \\ 2 & p & 0 \\ 0 & 2 & p \end{vmatrix} = -p^2 + 4q \ .$$

Of course, it is not easy to compute big dete rminants. A quicker way to do it is by eliminating the variable x.

Here we show it for degree 4. In `Singular`:

```
ring s = 0, (a,b,c,d,x),dp;
poly f = x4+dx3+cx2+bx+a;
poly fx = diff(f,x);
poly dis = eliminate(ideal(f,fx),x)[1];
size(dis);
dis;
```

In `Macaulay2`:

```
QQ[a..d,x]
F = x^4+d*x^3+c*x^2+b*x+a
Fx = diff(x,F)
dis = eliminate(x,ideal(F,Fx));
size(dis_0)
```

Exercise. Extend this computation to higher degree, until the computation takes longer than a fraction of a second. How long did it take and what is the number of monomials in the discriminant in that degree? The time can be measured in `Singular` by giving the command `timer=1`, and in `Macaulay2` by writing `time` as first word on a command line. Show your program.