Applications of Groebner basis.

Testing if a polynomial g is in the ideal, or in the radical ideal generated by polynomials f1,..,fm.

This is the first application, it is the problem that Groebner basis was designed to solve.

```
> f1:=x^2+y^2+z^2-3;
```

$$f1 := x^2+y^2+z^2-3$$

```
> f2:=x*y+y*z+z*x-3;
```

$$f2 := x\,y+y\,z+z\,x-3$$

```
> f3:=x*y*z+x+y+z-4;
```

$$f3 := x\,y\,z+x+y+z-4$$

```
> g:=(z-1)*(z^2+4*z+7);
```

$$g := (z-1)\,(z^2+4\,z+7)$$

Is g in (f1,f2,f3)? **This can be answered with any admissible ordering**. Note: ***if any ordering will do, then take a total degree ordering*** because these tend to be faster.

```
> with(Groebner):
```

Type ?termorder to find out the syntax of the ordering, let's take tdeg:

```
> ord:=tdeg(x,y,z);
```

$$ord := \mathrm{tdeg}(x, y, z)$$

```
> F:={f1,f2,f3};
```

$$F := \{x^2+y^2+z^2-3,\ x\,y+y\,z+z\,x-3,\ x\,y\,z+x+y+z-4\}$$

```
> GB:=gbasis(F,ord);
```

$$GB := [x\,y+y\,z+z\,x-3,\ x^2+y^2+z^2-3,\ -x-y-4\,z+4+y\,z^2+z^2\,x,\ y^3+z\,y^2+y\,z^2+z^3+4\,x-2\,y-2\,z-4,\ z^4+4\,z\,x+4\,y\,z-2\,z^2-4\,x-4\,y-8\,z+9,\ y^2\,z^2-y^2-4\,y\,z-z^2+4\,y+4\,z-3]$$

```
> reduce(g,GB,ord);
```

$$z^3+3\,z^2+3\,z-7$$

Not zero, so g is not in the ideal (f1,f2,f3). So g can not be written as a R-linear combination of f1,f2,f3, where R=C[x,y,z].

Let's consider another question: Is it true or false, that g(alpha1,alpha2,alpha3) is always zero for all solutions (alpha1,alpha2,alpha3) of f1=0, f2=0, f3=0?
We know that this question is equivalent to: is g in the radical ideal of (f1,f2,f3) ?
We know that this is equivalent to: does there exist a positive integer n such that g^n in the ideal (f1,f2,f3)? And this is equivalent to:
does there exist a positive integer n, such that reduce(g^n,GB,ord)=0?

```
> reduce(g^1,GB,ord);
```

$$z^3+3\,z^2+3\,z-7$$

```
> reduce(g^2,GB,ord);
```

$$z^3+z^2-z-1-2\,z\,x-2\,y\,z+2\,x+2\,y$$

```
>  # g^3, g^4, ...
```

This is of course not a good method, how can we ever know up to which n to go with g^n? So it seems we can only do this with Groebner basis once we can bound the n. This, however, isn't so, we can do this problem with Groebner basis even if we don't have any bound for n.

Namely, as follows:
g in radical ideal of (f1,..,fm), if and only if:
for all solutions of f1,..,fm we have that g=0, if and only if

there are no solutions of f1=0, f2=0,..,fm=0 and g<>0, if and only if:
there are no solutions of f1=0,.,fm=0, and t*g-1 = 0 where t is a new variable. And this holds if and only if:
1 is an element of the ideal (f1,f2..,fm, t*g-1). And this holds if and only if:
reduce(1, gbasis(f1,..,fm,t*g-1), ..) =0, which holds if and only if the gbasis has a non-zero constant (this constant will then always be 1 because it will be reduced by primpart).

So we see that the inequality g<>0 is translated to an equality by introducing a new variable, and then we end up with only equalities, and we see now that g is in the radical, if and only if the new equations are inconsistent, which will hold if and only if 1 is in the ideal, but then it will also be in the Groebner basis.

```
> gbasis({f1,f2,f3, t*g-1}, tdeg(x,y,z,t));
```

$$[1]$$

So g^n must be in (f1,f2,f3) for some positive n:

```
> reduce(g^3,GB,ord);
```

$$0$$

So we see that we can not only check if g is in the ideal, we can also check if g is in the radical ideal. Note that it is not so easy to find a Groebner basis for the radical ideal.

Eliminating variables; Solving polynomial equations.

Take again the same polynomials f1,f2,f3 in x,y,z and think of them as equations. Suppose we want to **eliminate the variable x from the equations f1,f2,f3**, so we want to find all elements of the ideal that do not have the variable x, in other words we want to compute the **intersection of C[y,z] and the ideal (f1,f2,f3).**

If we take the following **elimination ordering:**

```
> ord:=lexdeg([x],[y,z]);
```

$$ord := \mathrm{lexdeg}([x], [y, z])$$

then x will be larger than any power product in [y,z], which means that in the reduction algorithm at first all the focus will be on the variable x. The reduction algorithm will do a maximal effort to eliminate the variable x. Now it is not hard to prove that if we take:

```
> F;
```

$$\{x^2+y^2+z^2-3,\ x\,y+y\,z+z\,x-3,\ x\,y\,z+x+y+z-4\}$$

```
> GB:=gbasis(F,ord);
```

$$GB := [y^2 z^2-y^2-4\,y\,z-z^2+4\,y+4\,z-3,\ -2+2\,y-2\,y\,z+2\,z+y^2+z^2-y\,z^2-z\,y^2-y^3-z^3+y^3 z+z^3 y,\ y^4+z^4+2\,y^3+2\,z\,y^2+2\,y\,z^2+2\,z^3-2\,y^2+4\,y\,z-2\,z^2-16\,y-16\,z+22,\ z^5+z^4-2\,z^3-10\,z^2+17\,z-7,\ z^4 y-z^4+4\,z\,y^2-2\,y\,z^2-4\,y^2-8\,y\,z+2\,z^2+9\,y+4\,z-5,\ y^3+z\,y^2+y\,z^2+z^3+4\,x-2\,y-2\,z-4]$$

and we take the intersection of this set GB with C[y,z] as follows:

```
> GB_yz:=[seq(`if`(has(i,x), NULL, i),i=GB)];
```

$$GB\_yz := [y^2 z^2-y^2-4\,y\,z-z^2+4\,y+4\,z-3,\ -2+2\,y+2\,z-2\,y\,z+y^2+z^2-y\,z^2-z\,y^2-y^3-z^3+y^3 z+z^3 y,\ y^4+z^4+2\,y^3+2\,z\,y^2+2\,y\,z^2+2\,z^3-2\,y^2+4\,y\,z-2\,z^2-16\,y-16\,z+22,\ z^5+z^4-2\,z^3-10\,z^2+17\,z-7,\ z^4 y-z^4+4\,z\,y^2-2\,y\,z^2-4\,y^2-8\,y\,z+2\,z^2+9\,y+4\,z-5]$$

or we can do this more easily with:

```
> GB_yz := remove(has,GB,x);
```

$$GB\_yz := [y^2 z^2-y^2-4\,y\,z-z^2+4\,y+4\,z-3,\ -2+2\,y-2\,y\,z+2\,z+y^2+z^2-y\,z^2-z\,y^2-y^3-z^3+y^3 z+z^3 y,\ y^4+z^4+2\,y^3+2\,z\,y^2+2\,y\,z^2+2\,z^3-2\,y^2+4\,y\,z-2\,z^2-16\,y-16\,z+22,\ z^5+z^4-2\,z^3-10\,z^2+17\,z-7,\ z^4 y-z^4+4\,z\,y^2-2\,y\,z^2-4\,y^2-8\,y\,z+2\,z^2+9\,y+4\,z-5]$$

then this GB_yz is in fact a Groebner basis for the C[y,z]-ideal:
I_yz = (f1,f2,f3) intersected with C[y,z].

Think of I_yz as all the things we get by eliminating x, and that explains why we call lexdeg([x],[y,z]) an elimination ordering.

Why is GB_yz a Groebner basis for the ideal I_yz? Well, take g in I_yz, since g in I we know that reduce(g,GB,ord)=0. But g has no x in it, so the leading monomial of g has no x in it. Now whenever i in GB, and when has(i,x)=true, then the leading monomial of i must also have the variable x because x is larger than any power product in [y,z]. Therefore, when i in GB and has(f,x)=true, we won't be able to reduce g (which had no x) or any partial reduction of g (which have smaller leading monomials) with i. So if we throw away the i that have x, and we form the set GB_yz like above, we see that if g has no x, then reduce(g,GB,ord)=0 if and only if reduce(g,GB_yz,ord)=0. So we see that every element g in I_yz can be reduced to zero with GB_yz, and hence GB_yz is a Groebner basis for I_yz.

The following are examples of elements of I_yz, and we see they all reduce to zero with the Groebner basis GB_yz of I_yz

```
> resultant(f1,f2,x); # Note: this is always in the ideal (f1,f2), hence in I, and hence in I_yz.
```

$$3\,y^2\,z^2-12\,y\,z+9+y^4+2\,y^3\,z+2\,z^3\,y+z^4-3\,y^2-3\,z^2$$

```
> reduce(%,GB_yz,ord);
```

$$0$$

```
> resultant(f1,f3,x); # This is in the ideal (f1,f3), hence in I, and hence in I_yz
```

$$13-8\,y-8\,z+2\,y^2-4\,y\,z+2\,z^2+y^4\,z^2+2\,y^3\,z+z^4\,y^2+2\,z^3\,y-3\,y^2\,z^2$$

```
> reduce(%,GB_yz,ord);
```

$$0$$

```
> resultant(f2,f3,x); # Also in I_yz.
```

$$3-4\,y+4\,y\,z-4\,z+y^2+z^2-y^2\,z^2$$

```
> reduce(%,GB_yz,ord);
```

$$0$$

Computing the image of a polynomial map.

A polynomial map is a map
F: C^n --> C^m
that is defined by polynomials. So if P is a vector in C^n then Psi(P) in C^m, so it has m entries. So the polynomial map must consist of m polynomials, and since these polynomials must be functions on C^n they must have n variables. So:

m polynomials in n variables define a polynomial map from C^n to C^m.
Example with n=2, m=3.

```
> restart; with(Groebner);
```

[*fglm*, *gbasis*, *gsolve*, *hilbertdim*, *hilbertpoly*, *hilbertseries*, *inter_reduce*, *is_finite*, *is_solvable*, *leadcoeff*, *leadmon*, *leadterm*, *normalf*, *pretend_gbasis*, *reduce*, *spoly*, *termorder*, *testorder*, *univpoly*]

```
> F:=[ x1^2+x1*x2, x1^2*x2+x2^2, x1*x2-x1^2 ];
```

$$F:=[x1^2+x1\,x2,\,x1^2\,x2+x2^2,\,x1\,x2-x1^2]$$

```
> P:=[5,6];
```

$$P:=[5,\,6]$$

Image of P under F is:

```
> Q:=subs(x1=P[1], x2=P[2], F);
```

$$Q := [55, 186, 5]$$

So the image of P under F is Q, and so P is one of the pre-images of Q under F. Are there any other pre-images? That is, compute all P such that F(P)=Q.

```
> F-Q;
```

$$[-55 + x1^2 + x1\,x2, -186 + x1^2\,x2 + x2^2, -5 + x1\,x2 - x1^2]$$

```
> gbasis(%, plex(x1,x2));
```

$$[-6 + x2, x1 - 5]$$

So in this example, P is the only pre-image of Q.

How can we compute the image of F, the set F(C^2) = {F(P) | P in C^2}?

That is in general not an easy question. What we compute is the **Zariski-closure** of this set. Recall that when V is a set, then I(V) is the ideal of V, the set of polynomials that vanish on V. And V(I(V)) is the solution set of I(V), which of course includes the set V. Now V(I(V)) is called the Zariski-closure of V.

What we will compute is the Zariski-closure of F(C^2), which in this example happens to be equal to F(C^2), but this need not always be the case (example: (x1,x2) -> (x1,x1*x2), the image is all points in C^2 except the ones of the form (0, not 0). The Zariski-closure of that is C^2).

Lets say that P=[x1,x2], so F(P) is just the list F above. What are the points Q=F(P) that can be obtained this way, the points Q=[y1, y2, y3] in C^3 that are an image of F? Well Q is in the image of F if and only if Q = F(P) has a solution x1=.., x2=..

So the equations we have are: F-Q = [0,0,0].

```
> Q:=[y1,y2,y3];
```

$$Q := [y1, y2, y3]$$

```
> F-Q;
```

$$[-y1 + x1^2 + x1\,x2, -y2 + x1^2\,x2 + x2^2, -y3 + x1\,x2 - x1^2]$$

Notice that this set F-Q is already a Groebner basis with respect to the ordering lexdeg([y1,y2,y3], [x1,x2]). We want to eliminate x1 and x2 to get equations in y1, y2, y3. For this we need an elimination ordering to eliminate x1 and x2, so we need lexdeg([x1,x2], [y1,y2,y3]). The set F-Q is not yet a Groebner basis w.r.t. that ordering, so computation is required.

```
> GB:=gbasis(%, lexdeg([x1,x2], [y1,y2,y3]));
```

$$\begin{aligned}GB := [&-8\,y3\,y1^3 - 8\,y1\,y3^3 - 12\,y1^2\,y3^2 - 2\,y3^4 - 2\,y1^4 + y1^5 + 16\,y1\,y2^2\,y3 + 2\,y3^3\,y1^2 - y3^5 - 8\,y1^2\,y2^2\\ &- 8\,y3^3\,y2 - 2\,y3^2\,y1^3 + y3^4\,y1 - 8\,y2^2\,y3^2 + 8\,y2\,y1^3 + 8\,y2\,y3\,y1^2 - 8\,y3^2\,y1\,y2 - y3\,y1^4,\\ &2\,x1\,y1 + 4\,x2\,y3 + 2\,x1\,y3 - 4\,x1\,y2 + y1^2 - y3^2, 4\,x2\,y1 - 4\,x1\,y2 - 2\,x1\,y1 - 2\,x1\,y3 + y1^2 - y3^2, -4\,y1\,x1\,y3\\ &+ 2\,y1^2 + 4\,y1\,y3 + 4\,y2\,y3 - 4\,y1\,y2 + 2\,y3^2 + 4\,y1\,x1\,y2 - y1^3 + y1\,y3^2 - 4\,y3^2\,x1 - 4\,y3\,x1\,y2 + y3\,y1^2 - y3^3\\ &, y1^2 + x1\,y1^2 - y3^2\,x1 + 2\,y1\,y3 + 2\,y2\,y3 - 2\,y1\,y2 + y3^2, 8\,y2^2\,y3 - 8\,y1\,y2^2 - 8\,y2\,y3^2 - 14\,y1\,y3^2 - 2\,y1^3\\ &- 2\,y1^2\,y3^2 - 10\,y3\,y1^2 + 16\,y1\,y2\,y3 - 6\,y3^3 + 8\,y1^2\,y2 + y3^4 + 8\,y3^3\,x1 + y1^4 + 8\,y1\,y3^2\,x1, 2\,y3\,y1^3\\ &+ 6\,y1\,y3^3 + 6\,y1^2\,y3^2 + 2\,y3^4 + 24\,y1\,y2^2\,y3 + y3^5 + y2\,y1^4 + 8\,y1^2\,y2^2 + y2\,y3^4 - 6\,y3^3\,y2 + 2\,y3^2\,y1^3\\ &- 2\,y3^4\,y1 + 8\,y2^3\,y3 - 8\,y1\,y2^3 - 16\,y2^2\,y3^2 - 2\,y2\,y1^3 - 18\,y2\,y3\,y1^2 - 2\,y2\,y1^2\,y3^2 + 16\,y3^3\,x1\,y2\\ &- 22\,y3^2\,y1\,y2 - y3\,y1^4, x1\,y3 - 2\,y2 + 2\,x2^2 + x1\,y1, 2\,x1\,x2 - y1 - y3, y3 + 2\,x1^2 - y1]\end{aligned}$$

```
> GB_Y := remove(has, GB, {x1,x2}); # Throw away things that have x1 or x2
```

$$\begin{aligned}GB\_Y := [&-8\,y3\,y1^3 - 8\,y1\,y3^3 - 12\,y1^2\,y3^2 - 2\,y3^4 - 2\,y1^4 + y1^5 + 16\,y1\,y2^2\,y3 + 2\,y3^3\,y1^2 - y3^5 - 8\,y1^2\,y2^2\\ &- 8\,y3^3\,y2 - 2\,y3^2\,y1^3 + y3^4\,y1 - 8\,y2^2\,y3^2 + 8\,y2\,y1^3 + 8\,y2\,y3\,y1^2 - 8\,y3^2\,y1\,y2 - y3\,y1^4]\end{aligned}$$

So we see that the image of F will be contained in the zero set of GB_Y. So:
F(C^2) subset V(GB_Y).
In fact, with such a computation we always find a set GB_Y such that V(GB_Y) is the Zariski-closure of F(C^2).

When Q is in V(GB_Y), how to compute a pre-image (if it exists) of Q?

```
> select(has,GB,x1);
```

$$[2\,x1\,y1+4\,x2\,y3+2\,x1\,y3-4\,x1\,y2+y1^2-y3^2,\ 4\,x2\,y1-4\,x1\,y2-2\,x1\,y1-2\,x1\,y3+y1^2-y3^2,\ -4\,y1\,x1\,y3$$
$$+2\,y1^2+4\,y1\,y3+4\,y2\,y3-4\,y1\,y2+2\,y3^2+4\,y1\,x1\,y2-y1^3+y1\,y3^2-4\,y3^2\,x1-4\,y3\,x1\,y2+y3\,y1^2-y3^3$$
$$,\ y1^2+x1\,y1^2-y3^2\,x1+2\,y1\,y3+2\,y2\,y3-2\,y1\,y2+y3^2,\ 8\,y2^2\,y3-8\,y1\,y2^2-8\,y2\,y3^2-14\,y1\,y3^2-2\,y1^3$$
$$-2\,y1^2\,y3^2-10\,y3\,y1^2+16\,y1\,y2\,y3-6\,y3^3+8\,y1^2\,y2+y3^4+8\,y3^3\,x1+y1^4+8\,y1\,y3^2\,x1,\ 2\,y3\,y1^3$$
$$+6\,y1\,y3^3+6\,y1^2\,y3^2+2\,y3^4+24\,y1\,y2^2\,y3+y3^5+y2\,y1^4+8\,y1^2\,y2^2+y2\,y3^4-6\,y3^3\,y2+2\,y3^2\,y1^3$$
$$-2\,y3^4\,y1+8\,y2^3\,y3-8\,y1\,y2^3-16\,y2^2\,y3^2-2\,y2\,y1^3-18\,y2\,y3\,y1^2-2\,y2\,y1^2\,y3^2+16\,y3^3\,x1\,y2$$
$$-22\,y3^2\,y1\,y2-y3\,y1^4,\ x1\,y3-2\,y2+2\,x2^2+x1\,y1,\ 2\,x1\,x2-y1-y3,\ y3+2\,x1^2-y1]$$

```
> remove(has,%,x2);
```

$$[-4\,y1\,x1\,y3+2\,y1^2+4\,y1\,y3+4\,y2\,y3-4\,y1\,y2+2\,y3^2+4\,y1\,x1\,y2-y1^3+y1\,y3^2-4\,y3^2\,x1-4\,y3\,x1\,y2$$
$$+y3\,y1^2-y3^3,\ y1^2+x1\,y1^2-y3^2\,x1+2\,y1\,y3+2\,y2\,y3-2\,y1\,y2+y3^2,\ 8\,y2^2\,y3-8\,y1\,y2^2-8\,y2\,y3^2$$
$$-14\,y1\,y3^2-2\,y1^3-2\,y1^2\,y3^2-10\,y3\,y1^2+16\,y1\,y2\,y3-6\,y3^3+8\,y1^2\,y2+y3^4+8\,y3^3\,x1+y1^4$$
$$+8\,y1\,y3^2\,x1,\ 2\,y3\,y1^3+6\,y1\,y3^3+6\,y1^2\,y3^2+2\,y3^4+24\,y1\,y2^2\,y3+y3^5+y2\,y1^4+8\,y1^2\,y2^2+y2\,y3^4$$
$$-6\,y3^3\,y2+2\,y3^2\,y1^3-2\,y3^4\,y1+8\,y2^3\,y3-8\,y1\,y2^3-16\,y2^2\,y3^2-2\,y2\,y1^3-18\,y2\,y3\,y1^2-2\,y2\,y1^2\,y3^2$$
$$+16\,y3^3\,x1\,y2-22\,y3^2\,y1\,y2-y3\,y1^4,\ y3+2\,x1^2-y1]$$

```
> remove(has,%,x1^2);
```

$$[-4\,y1\,x1\,y3+2\,y1^2+4\,y1\,y3+4\,y2\,y3-4\,y1\,y2+2\,y3^2+4\,y1\,x1\,y2-y1^3+y1\,y3^2-4\,y3^2\,x1-4\,y3\,x1\,y2$$
$$+y3\,y1^2-y3^3,\ y1^2+x1\,y1^2-y3^2\,x1+2\,y1\,y3+2\,y2\,y3-2\,y1\,y2+y3^2,\ 8\,y2^2\,y3-8\,y1\,y2^2-8\,y2\,y3^2$$
$$-14\,y1\,y3^2-2\,y1^3-2\,y1^2\,y3^2-10\,y3\,y1^2+16\,y1\,y2\,y3-6\,y3^3+8\,y1^2\,y2+y3^4+8\,y3^3\,x1+y1^4$$
$$+8\,y1\,y3^2\,x1,\ 2\,y3\,y1^3+6\,y1\,y3^3+6\,y1^2\,y3^2+2\,y3^4+24\,y1\,y2^2\,y3+y3^5+y2\,y1^4+8\,y1^2\,y2^2+y2\,y3^4$$
$$-6\,y3^3\,y2+2\,y3^2\,y1^3-2\,y3^4\,y1+8\,y2^3\,y3-8\,y1\,y2^3-16\,y2^2\,y3^2-2\,y2\,y1^3-18\,y2\,y3\,y1^2-2\,y2\,y1^2\,y3^2$$
$$+16\,y3^3\,x1\,y2-22\,y3^2\,y1\,y2-y3\,y1^4]$$

```
> sort(%,(i,j) -> evalb(length(i) < length(j)));
```

$$[y1^2+x1\,y1^2-y3^2\,x1+2\,y1\,y3+2\,y2\,y3-2\,y1\,y2+y3^2,\ -4\,y1\,x1\,y3+2\,y1^2+4\,y1\,y3+4\,y2\,y3-4\,y1\,y2$$
$$+2\,y3^2+4\,y1\,x1\,y2-y1^3+y1\,y3^2-4\,y3^2\,x1-4\,y3\,x1\,y2+y3\,y1^2-y3^3,\ 8\,y2^2\,y3-8\,y1\,y2^2-8\,y2\,y3^2$$
$$-14\,y1\,y3^2-2\,y1^3-2\,y1^2\,y3^2-10\,y3\,y1^2+16\,y1\,y2\,y3-6\,y3^3+8\,y1^2\,y2+y3^4+8\,y3^3\,x1+y1^4$$
$$+8\,y1\,y3^2\,x1,\ 2\,y3\,y1^3+6\,y1\,y3^3+6\,y1^2\,y3^2+2\,y3^4+24\,y1\,y2^2\,y3+y3^5+y2\,y1^4+8\,y1^2\,y2^2+y2\,y3^4$$
$$-6\,y3^3\,y2+2\,y3^2\,y1^3-2\,y3^4\,y1+8\,y2^3\,y3-8\,y1\,y2^3-16\,y2^2\,y3^2-2\,y2\,y1^3-18\,y2\,y3\,y1^2-2\,y2\,y1^2\,y3^2$$
$$+16\,y3^3\,x1\,y2-22\,y3^2\,y1\,y2-y3\,y1^4]$$

```
> %[1];
```

$$y1^2+x1\,y1^2-y3^2\,x1+2\,y1\,y3+2\,y2\,y3-2\,y1\,y2+y3^2$$

```
> P1:=solve(%,x1);
```

$$P1 := -\frac{y1^2+2\,y1\,y3+2\,y2\,y3-2\,y1\,y2+y3^2}{y1^2-y3^2}$$

```
> map(numer@normal,subs(x1=P1,remove(has,select(has,GB,x2),x2^2)));
```

$$[-2\,y1^3-6\,y3\,y1^2+8\,y1\,y2\,y3+8\,y1^2\,y2-6\,y1\,y3^2+4\,x2\,y3\,y1^2-4\,x2\,y3^3-2\,y3^3+8\,y2^2\,y3-8\,y1\,y2^2$$
$$+y1^4-2\,y1^2\,y3^2+y3^4,\ 4\,x2\,y1^3-4\,x2\,y1\,y3^2+8\,y1\,y2\,y3+8\,y2^2\,y3-8\,y1\,y2^2+8\,y2\,y3^2+2\,y1^3+6\,y3\,y1^2$$

$$+6\,y1\,y3^2+2\,y3^3+y1^4-2\,y1^2\,y3^2+y3^4,$$
$$-2\,x2\,y1^2-4\,x2\,y3\,y1-4\,x2\,y2\,y3+4\,x2\,y1\,y2-2\,x2\,y3^2-y1^3+y1\,y3^2-y3\,y1^2+y3^3]$$

```
> sort(%,(i,j) -> evalb(length(i) < length(j)));
```

$$[-2\,x2\,y1^2-4\,x2\,y3\,y1-4\,x2\,y2\,y3+4\,x2\,y1\,y2-2\,x2\,y3^2-y1^3+y1\,y3^2-y3\,y1^2+y3^3,\ 4\,x2\,y1^3-4\,x2\,y1\,y3^2+8\,y1\,y2\,y3+8\,y2^2\,y3-8\,y1\,y2^2+8\,y2\,y3^2+2\,y1^3+6\,y3\,y1^2+6\,y1\,y3^2+2\,y3^3+y1^4-2\,y1^2\,y3^2+y3^4,\ -2\,y1^3-6\,y3\,y1^2+8\,y1\,y2\,y3+8\,y1^2\,y2-6\,y1\,y3^2+4\,x2\,y3\,y1^2-4\,x2\,y3^3-2\,y3^3+8\,y2^2\,y3-8\,y1\,y2^2+y1^4-2\,y1^2\,y3^2+y3^4]$$

```
> P2:=solve(%[1],x2);
```

$$P2:=-\frac{1}{2}\,\frac{y1^3-y1\,y3^2+y3\,y1^2-y3^3}{y1^2+2\,y1\,y3+2\,y2\,y3-2\,y1\,y2+y3^2}$$

```
> P:=[P1,P2];
```

$$P:=\left[-\frac{y1^2+2\,y1\,y3+2\,y2\,y3-2\,y1\,y2+y3^2}{y1^2-y3^2},\ -\frac{1}{2}\,\frac{y1^3-y1\,y3^2+y3\,y1^2-y3^3}{y1^2+2\,y1\,y3+2\,y2\,y3-2\,y1\,y2+y3^2}\right]$$

So the image of P must be Q=[y1,y2,y3]. Let's check:

```
> image_P := subs(x1=P1, x2=P2 , F);
```

$$image\_P:=\left[\frac{(y1^2+2\,y1\,y3+2\,y2\,y3-2\,y1\,y2+y3^2)^2}{(y1^2-y3^2)^2}+\frac{1}{2}\,\frac{y1^3-y1\,y3^2+y3\,y1^2-y3^3}{y1^2-y3^2},\right.$$
$$-\frac{1}{2}\,\frac{(y1^2+2\,y1\,y3+2\,y2\,y3-2\,y1\,y2+y3^2)\,(y1^3-y1\,y3^2+y3\,y1^2-y3^3)}{(y1^2-y3^2)^2}$$
$$+\frac{1}{4}\,\frac{(y1^3-y1\,y3^2+y3\,y1^2-y3^3)^2}{(y1^2+2\,y1\,y3+2\,y2\,y3-2\,y1\,y2+y3^2)^2},$$
$$\left.\frac{1}{2}\,\frac{y1^3-y1\,y3^2+y3\,y1^2-y3^3}{y1^2-y3^2}-\frac{(y1^2+2\,y1\,y3+2\,y2\,y3-2\,y1\,y2+y3^2)^2}{(y1^2-y3^2)^2}\right]$$

```
> Q;
```

$$[y1,\,y2,\,y3]$$

This doesn't exactly look the same.

```
> should_be_zero:=map(numer, map(normal, image_P - Q ));
```

$$should\_be\_zero:=[8\,y3\,y1^3+8\,y1\,y3^3+12\,y1^2\,y3^2+2\,y3^4+2\,y1^4-y1^5-16\,y1\,y2^2\,y3-2\,y3^3\,y1^2+y3^5+8\,y1^2\,y2^2+8\,y3^3\,y2+2\,y3^2\,y1^3-y3^4\,y1+8\,y2^2\,y3^2-8\,y2\,y1^3-8\,y2\,y3\,y1^2+8\,y3^2\,y1\,y2+y3\,y1^4,\ y1^7+y1^6\,y3-2\,y1^6+8\,y2\,y1^5-3\,y1^5\,y3^2-12\,y3\,y1^5-30\,y1^4\,y3^2-8\,y1^4\,y2^2+24\,y3\,y2\,y1^4-3\,y1^4\,y3^3+16\,y2\,y1^3\,y3^2-40\,y3^3\,y1^3+3\,y1^3\,y3^4+16\,y1^2\,y2^2\,y3^2+3\,y1^2\,y3^5-30\,y1^2\,y3^4-16\,y3^3\,y2\,y1^2-y1\,y3^6-12\,y3^5\,y1-24\,y3^4\,y1\,y2-y3^7-8\,y2^2\,y3^4-8\,y3^5\,y2-2\,y3^6,\ -8\,y3\,y1^3-8\,y1\,y3^3-12\,y1^2\,y3^2-2\,y3^4-2\,y1^4+y1^5+16\,y1\,y2^2\,y3+2\,y3^3\,y1^2-y3^5-8\,y1^2\,y2^2-8\,y3^3\,y2-2\,y3^2\,y1^3+y3^4\,y1-8\,y2^2\,y3^2+8\,y2\,y1^3+8\,y2\,y3\,y1^2-8\,y3^2\,y1\,y2-y3\,y1^4]$$

This should be zero, and it isn't. However, note that when we computed the pre-image P of Q, that that was under an assumption, namely that Q was in V(GB_Y). Therefore, we shouldn't expect complete zeros here, but just things that become zero under our assumptions (the equations in GB_Y). So modulo GB_Y, these polynomials should become zero:

```
> map(normalf, should_be_zero, GB_Y, tdeg(y1,y2,y3));
```

$$[0, 0, 0]$$

Every element of F(C^2) is in V(GB_Y), but is every element of V(GB_Y) also in F(C^2)? We can find a pre-image P when the denominators in P don't vanish, so the corresponding points [y1,y2,y3] in V(GB_Y) are also in F(C^2), and furthermore they have precisely one pre-image, namely the P we just computed.

```
> map(denom,P);
```

$$[y1^2-y3^2, 2\,y1^2+4\,y1\,y3+4\,y2\,y3-4\,y1\,y2+2\,y3^2]$$

What if one of these two denominators is zero?

```
> gbasis({denom(P[1]), op(GB), x1*t1-1}, lexdeg([x1,x2,t1], [y1,y2,y3]));
```

$$[y2, y1+y3, t1\,y3+x1, x2, x1\,t1-1, x1^2+y3]$$

```
> gbasis({denom(P[2]), op(GB), x1*t1-1}, lexdeg([x1,x2,t1], [y1,y2,y3]));
```

$$[y2, y1+y3, t1\,y3+x1, x2, x1\,t1-1, x1^2+y3]$$

We see that if we add the extra assumption that x1<>0, then it follows that x2=0. So these denominators can only vanish when x1=0 or x2=0.

```
> subs(x1=0,F);
```

$$[0, x2^2, 0]$$

```
> subs(x2=0,F);
```

$$[x1^2, 0, -x1^2]$$

Now we see why we get a denominator. Because when x1=0 or x2=0, the corresponding images have not 1, but 2 pre-images.

So we see that all points in V(GB_y) that are not of the form [0, y2, 0] and not of the form [y1, 0, -y1] have precisely 1 pre-image, and the remaining points except [0,0,0] have two pre-images.

```
> gbasis(F - [0,0,0],plex(x1,x2,x3));
```

$$[x2^2, x1\,x2, x1^2]$$

```
> solve({op(%)});
```

$$\{x1=0, x2=0\}, \{x1=0, x2=0\}$$

So [0,0,0] has 1 pre-image.

Computing the inverse of a polynomial map.

Consider the following polynomial map from C^3 to C^3:

```
> restart; with(Groebner):
> F:=[x2+2*x3^2-x3*x1+x2*x3^2, x2+x3+2*x3^2-x3*x1+x2*x3^2, x1-x2*x3];
```

$$F := [x2+2\,x3^2-x3\,x1+x2\,x3^2, x2+x3+2\,x3^2-x3\,x1+x2\,x3^2, x1-x2\,x3]$$

```
> Q:=[y1,y2,y3];
```

$$Q := [y1, y2, y3]$$

Is F an invertible polynomial map? That means: is F onto and 1-1? If so, then the inverse is also a polynomial map. We can check if F is invertible, and if so, we can determine the inverse. Of course most maps are not invertible.

```
> F-Q;
```

$$[-y1+x2+2\,x3^2-x3\,x1+x2\,x3^2, -y2+x2+x3+2\,x3^2-x3\,x1+x2\,x3^2, -y3+x1-x2\,x3]$$

This set is already a Groebner basis in the lexdeg([y1,y2,y3],[x1,x2,x3]) ordering. Lets compute a pre-image of Q by eliminating x1,x2,x3.

```
> gbasis(%, lexdeg([x1,x2,x3], [y1,y2,y3]));
```

$$[y1-y2+x3, -y1+x2+2\,y1^2-4\,y1\,y2+2\,y2^2+y3\,y1-y3\,y2,$$
$$-y3+x1+y1^2-2\,y1^3+6\,y1^2\,y2-6\,y1\,y2^2-y3\,y1^2+2\,y1\,y3\,y2-y1\,y2+2\,y2^3-y3\,y2^2]$$

Note: the equations are of the form: x.i - something only consisting of y's, for i = 1, 2, 3.

```
> P := subs( solve({op(%)},{x1,x2,x3}), [x1,x2,x3]);
```

$$P := [y3 - y1^2 + 2\,y1^3 - 6\,y1^2\,y2 + 6\,y1\,y2^2 + y3\,y1^2 - 2\,y1\,y3\,y2 + y1\,y2 - 2\,y2^3 + y3\,y2^2,$$
$$y1 - 2\,y1^2 + 4\,y1\,y2 - 2\,y2^2 - y3\,y1 + y3\,y2, -y1 + y2]$$

```
> expand(subs(x1=P[1],x2=P[2],x3=P[3], F));
```

$$[y1, y2, y3]$$

So we see that this F is 1-1, and the unique pre-image of Q=[y1,y2,y3] is the point P.

Let F=[F[1], F[2], .., F[n]] with F[i] in C[x1,..,xn] be a polynomial map from C^n to C^n. Then F is invertible if and only if
gbasis(F - [y1,y2,..,yn] , lexdeg([x1,..,xn], [y1,..,yn]))
has n elements, each of which is of the form: x.i - element of C[y1,..,yn], where i=1..n.

Computing an algebraic relation between polynomials.

Transcendence degree.

```
> restart;
> u:=x^2+y^3; v:=x^3+y^2; w:=x*y;
```

$$u := x^2 + y^3$$
$$v := x^3 + y^2$$
$$w := x\,y$$

Now u, v and w are three polynomials in C[x,y], which has only transcendence degree two over C, and so they must be algebraically dependent, i.e. there must exist a polynomial P in three variables such that P(u,v,w)=0. How to find such P is the topic of this worksheet.

Let's use the names U,V,W for the variables of P. So we **want to find: P in C[U,V,W], such that: P(u,v,w) is zero**, where u,v,w are the polynomials in C[x,y] given above. When P is in C[U,V,W], then
P(u,v,w) is subs(U=u, V=v, W=w),
which is in C[x,y], and which should be zero.

Now we want to compute both with P in C[U,V,W], and also with u,v,w in C[x,y], so we are dealing with 5 variables. We can do this by computing in the ring R = C[x,y,U,V,W]. Consider the ideal (F) generated by the set F below. We have that:
u, v, and w are equivalent to U, V, and W modulo (F), hence:
P(U,V,W) is equivalent to P(u,v,w) modulo (F) for every P in C[U,V,W]. Since we want P(u,v,w) to be equal to 0, we want P(U,V,W) to be equivalent with 0 modulo (F), in other words, P must be in the ideal (F) in R. Furthermore P is in C[U,V,W] which is a subring of R. So P is in the ideal I_UVW of C[U,V,W] which is defined as I_UVW = the intersection of the ring C[U,V,W] with the ideal (F), which is a subset of a larger ring C[x,y,U,V,W].

```
> F:={U-u,V-v,W-w};
```

$$F := \{\mathrm{W} - x\,y, U - x^2 - y^3, V - x^3 - y^2\}$$

```
> with(Groebner):
```

Now we choose an elimination ordering, in such a way that x and y are > than any monomial in U,V,W. Then compute the Groebner basis.

Note that we may also take the ordering: plex(x,y,U,V,W), because under this ordering we also have that x,y are > anything in [U,V,W]. However, the elimination ordering lexdeg tends to be more efficient.

```
> ordering:=lexdeg([x,y],[U,V,W]); G:=gbasis(F,ordering);
```

$$ordering := \mathrm{lexdeg}([x, y], [U, V, \mathrm{W}])$$

$$
\begin{aligned}
G := [&-10\,W^6-3\,U\,V\,W^3+2\,W^2\,V\,U-W^4-3\,U\,V\,W^4-U^2\,V^2+10\,W^7+7\,U\,W^5\,V+U^5+V^5+5\,W^5\\
&+3\,W^3\,U^2\,V^2-3\,W^6\,V\,U-2\,W^2\,V^2\,U^2-V^3\,U^3-5\,W^8+W^9,\\
&-V\,x\,U+V^2+x\,W^3+W\,y\,U-2\,x\,W^2-y\,U+x\,W,\ x\,U^2-U\,V+y\,V^2+W^4-W\,U\,V-2\,W^3+W^2,\\
&-U\,y\,V+U^2+y\,W^3+W\,x\,V-2\,y\,W^2-x\,V+y\,W,\\
&U^2\,y\,V+W^5\,x-W^2\,V\,x\,U-3\,x\,W^4+3\,x\,W^3+V\,x\,U-x\,W^2+W^2\,V^2-U^3-V^2\,W,\\
&2\,U\,V\,W^3-U^2\,V^2-W^2\,V\,U+y\,U^3-W^6+3\,W^5-3\,W^4-W\,U\,V+W^3+V^3\,x,\ -V^3\,x\,U+V^4+V^2\,x\,W^3\\
&-2\,V^2\,x\,W^2+V^2\,x\,W-W\,U^3\,x-W^5\,U+W^2\,U^2\,V+3\,W^4\,U-3\,W^3\,U+x\,U^3-U^2\,V+W^2\,U,\ -W\,U\,V\\
&-4\,W^6+W^3+3\,U\,V\,W^3-4\,W^4+V^3\,x-2\,U\,V\,W^4-U^3\,V\,x+W^7+U^2\,x\,W^3-2\,U^2\,x\,W^2+U^2\,x\,W\\
&+W\,U^2\,V^2-W\,V^3\,x+6\,W^5,\ W^2\,U^3+V^3\,U\,W-V^2\,W^3+3\,V^2\,W^4+U^5\,x+U^3\,W^4+U^2\,V^4+W^6\,V^2-V^5\,x\\
&-U^4\,W\,V+U\,W^2\,V^3-3\,V^2\,W^5-2\,W^3\,U^3-V\,U^4-2\,V^3\,W^3\,U,\ U^2\,V^2\,x-V^3\,U-2\,U\,V\,x\,W^3+3\,W^2\,V\,x\,U\\
&+W^6\,x-4\,W^5\,x+6\,x\,W^4-4\,x\,W^3+V^2\,W^3-W\,U^3-2\,W^2\,V^2-V\,x\,U+x\,W^2+U^3+V^2\,W,\ -U^4\,x-U^2\,W^4\\
&+U^3\,W\,V+2\,W^3\,U^2-U^2\,W^2+V\,W^5\,x-W^2\,V^2\,x\,U-3\,V\,x\,W^4+3\,V\,x\,W^3+V^2\,x\,U-V\,x\,W^2+W^2\,V^3\\
&-V^3\,W,\ U\,W^5\,x-W^2\,V\,x\,U^2-3\,U\,x\,W^4+3\,U\,x\,W^3+U^2\,V\,x-U\,x\,W^2+2\,W^2\,V^2\,U-U^4-2\,V^2\,W^3\,U\\
&+U^2\,V^3+W^6\,V-3\,V\,W^5+3\,V\,W^4-V\,W^3-V^4\,x,\ y^2\,W-x\,U+V-y^2,\ -x\,W^2+y^2\,V-y\,U+x\,W,\\
&U\,y^2+V\,x^2+W^3-U\,V-W^2,\ -W+x\,y,\ W\,x^2-y\,V+U-x^2,\ -y\,W^2+x^2\,U-x\,V+y\,W,\\
&U\,x\,W^2+y\,U^2-W\,U\,x+V^2\,x^2+V\,W^3-V^2\,U-V\,W^2,\ -U+x^2+y^3,\ -V+x^3+y^2]
\end{aligned}
$$

Let H be the list of all polynomials in the list G, that do not contain x or y (that have degree 0 in {x,y}). It is clear that (H) will be contained in the ideal I_UVW, but in fact (H) equals I_UVW. The reason is as follows: Suppose Q in I_UVW, so Q in C[U,V,W] and Q in (F). Then Q can be reduced to 0 by G because G is a Groebner basis. However, Q only has monomials in U,V,W. Hence Q can only be reduced by polynomials g in which the leading power product is in [U,V,W]. Now the ordering was chosen in such a way that every monomial in which x or y occurs is bigger than any monomial in [U,V,W], so if the leading term of g only has the variables U,V,W then g must be in C[U,V,W].
So the conclusion is that if Q in I_UVW, so Q can be reduced to 0 by G and Q in C[U,V,W], then Q can also be reduced to 0 by those elements in G that are in C[U,V,W], i.e. Q can be reduced to 0 by the set H. Hence (H)=I_UVW, and in fact H is a Groebner basis for I_UVW with the same ordering as we had on R.

```
> H:=remove(has,G,{x,y});
```

$$
\begin{aligned}
H := [&-10\,W^6-3\,U\,V\,W^3+2\,W^2\,V\,U-W^4-3\,U\,V\,W^4-U^2\,V^2+10\,W^7+7\,U\,W^5\,V+U^5+V^5+5\,W^5\\
&+3\,W^3\,U^2\,V^2-3\,W^6\,V\,U-2\,W^2\,V^2\,U^2-V^3\,U^3-5\,W^8+W^9]
\end{aligned}
$$

```
> nops(H);
```

$$1$$

```
> P:=factor(H[1]);
```

$$
\begin{aligned}
P := &-10\,W^6-3\,U\,V\,W^3+2\,W^2\,V\,U-W^4-3\,U\,V\,W^4-U^2\,V^2+10\,W^7+7\,U\,W^5\,V+U^5+V^5+5\,W^5\\
&+3\,W^3\,U^2\,V^2-3\,W^6\,V\,U-2\,W^2\,V^2\,U^2-V^3\,U^3-5\,W^8+W^9
\end{aligned}
$$

```
> subs(U=u,V=v,W=w,P);
```

$$
\begin{aligned}
&-10\,x^6\,y^6-3\,(x^2+y^3)\,(x^3+y^2)\,x^3\,y^3+2\,x^2\,y^2\,(x^3+y^2)\,(x^2+y^3)-x^4\,y^4-3\,(x^2+y^3)\,(x^3+y^2)\,x^4\,y^4\\
&-(x^2+y^3)^2\,(x^3+y^2)^2+10\,x^7\,y^7+7\,(x^2+y^3)\,x^5\,y^5\,(x^3+y^2)+(x^2+y^3)^5+(x^3+y^2)^5+5\,x^5\,y^5\\
&+3\,x^3\,y^3\,(x^2+y^3)^2\,(x^3+y^2)^2-3\,x^6\,y^6\,(x^3+y^2)\,(x^2+y^3)-2\,x^2\,y^2\,(x^3+y^2)^2\,(x^2+y^3)^2-(x^3+y^2)^3\,(x^2+y^3)^3\\
&-5\,x^8\,y^8+x^9\,y^9
\end{aligned}
$$

```
> expand(%);
```

$$0$$

Let's look at some examples:

```
> normalf(x,G,ordering); # not in C[u,v,w] because not all x,y disappear:
```

$$x$$

```
> normalf(x^2,G,ordering); # not in C[u,v,w] because not all x,y disappear:
```

$$x^2$$

```
> normalf(x^3+y^2,G,ordering); # in C[u,v,w] because all x,y disappear:
```

$$V$$

```
> expand(u^2*v+w^3); # in C[u,v,w]
```

$$x^7+x^4y^2+2x^5y^3+2x^2y^5+x^3y^6+y^8+x^3y^3$$

```
> normalf(%,G,ordering); # hence all x,y must disappear:
```

$$\mathrm{W}^3+U^2V$$

```
> normalf(x^5+y^5,G,ordering);
```

All x,y disappear, so x^5+y^5 is an element of C[u,v,w]. If we substitute U=u, V=v, W=w in the following, we would get x^5+y^5 again.

$$-\mathrm{W}^3+UV-\mathrm{W}^2$$

```
> expand(subs(U=u, V=v, W=w, %));
```

$$x^5+y^5$$

```
> normalf(x^6+y^6,G,ordering);
```

This implies that x^6+y^6 is not an element of C[u,v,w].

$$-2x\mathrm{W}^2+V^2-yU+x\mathrm{W}+U^2-2y\mathrm{W}^2-xV+y\mathrm{W}$$

```
>
```

Testing if a polynomial g is an element of C[f1,f2..,fk]

Consider the polynomials
f1 = x^2+y
f2 = x^3 + y^2
f3 = x*y

Now R=C[f1,f2,f3] is a subring of C[x,y].
The ring R consists of all polynomials in x,y that can be expressed as a polynomial in f1,f2,f3, for example: f1^2*f2 +3*f3^4 is an element of R.

Note that f1, f2, f3 are algebraically dependent, because C[x,y] only has transcendence degree 2. If:
g = x^2*y^3
how can we find out if g is in R or not?

So we have to find out the following: does there exist a polynomial G in three variables, say G in C[z1,z2,z3], such that:
subs(z1=f1, z2=f2, z3=f3, G) = g?

If yes, then g in R, if no, then g not in R. Notice that: subs(z1=f1, z2=f2, z3=f3, G) is equivalent to G modulo I=(z1-f1, z2-f2, z3-f3).

So the question reduces to the following: In the ring C[x,y, z1,z2,z3], does there exist a polynomial G such that: not has(G,{x,y}), in other words: G in C[z1,z2,z3].
And: G is equivalent to g modulo I.

How to find such G, if it exists? Well, we can reduce g modulo I, and we want to do it in such a way that (if it is possible) the variables x,y completely disappear. So we have to use the lexdeg([x,y], [z1,z2,z3]) ordering, compute a Groebner basis of I, reduce g, and see if the result has an x or y in it. If there's no x,y then g in R, otherwise g is not in R.

Exercise: find out if g is in R.
Also find out if h=x^6*y+x^4*y^2+x*y^4 is in R.
Furthermore: determine an algebraic dependence between f1,f2,f3.

Checking if two rings are equal, or if one ring is a subring of another.

Let R1 = C[x1^2+x2, x2^2+x1, x1*x2]
and R2 = C[x1^3+x2^3, x2^3+3*x1^4*x2+x1^6, x1*x2]

Are R1 and R2 equal?

We split up this question into two questions:

1) Is R1 a subring of R2?
2) Is R2 a subring of R1?

Let f1:=x1^2+x2
f2:=x2^2+x1
f3:=x1*x2

g1:=x1^3+x2^3
g2:=x2^3+3*x1^4*x2+x1^6
g3:=x1*x2

So 1) is: are f1,f2,f3 elements of R2, so can f1,f2,f3 be written as polynomial functions in g1,g2,g3?
And 2) is the reverse. We have seen that we can answer these questions using the previous section.

```
> restart; f1:=x1^2+x2; f2:=x2^2+x1; f3:=x1*x2;
```

$$f1 := x1^2 + x2$$

$$f2 := x2^2 + x1$$

$$f3 := x1\ x2$$

```
> g1:=x1^3+x2^3; g2:= x2^3+3*x1^4*x2+x1^6; g3:=x1*x2;
```

$$g1 := x1^3 + x2^3$$

$$g2 := x2^3 + 3\ x1^4\ x2 + x1^6$$

$$g3 := x1\ x2$$

```
> ideal_for_ring_R2 := { G1-g1, G2-g2, G3-g3 }; # so the variables G1,G2,G3
  are equivalent to the polynomials g1,g2,g3 modulo this ideal.
```

$$ideal\_for\_ring\_R2 := \{G3 - x1\ x2, G1 - x1^3 - x2^3, G2 - x2^3 - 3\ x1^4\ x2 - x1^6\}$$

```
> with(Groebner):  ord:=lexdeg([x1,x2],[G1,G2,G3]);
```

$$ord := \mathrm{lexdeg}([x1, x2], [G1, G2, G3])$$

```
> GB_R2:=gbasis(ideal_for_ring_R2, ord):
> map(reduce, [f1,f2,f3], GB_R2, ord);
```

$$[x1^2 + x2, x2^2 + x1, G3]$$

So R1 is not a subring of R2, hence R1 is not equal to R2.

Is R2 a subring of R1?

```
> ideal_for_ring_R1 := { F1-f1, F2-f2, F3-f3 }; # so the variables F1,F2,F3
  are equivalent to the polynomials f1,f2,f3 modulo this ideal.
```

$$ideal\_for\_ring\_R1 := \{F1 - x1^2 - x2,\ F2 - x2^2 - x1,\ F3 - x1\,x2\}$$

```
> ord:=lexdeg([x1,x2],[F1,F2,F3]);
```

$$ord := \mathrm{lexdeg}([x1, x2], [F1, F2, F3])$$

```
> GB_R1:=gbasis(ideal_for_ring_R1, ord):
> map(reduce, [g1,g2,g3], GB_R1, ord);
```

$$[-F3 + F2\,F1 - F3^2,\ F1^3 - 3\,F3^2,\ F3]$$

So R2 is a subring of R1, and the above list tells you how you can express g1,g2,g3 as polynomials in f1,f2,f3.

```
> subs(F1=f1, F2=f2, F3=f3, %);
```

$$[-x1\,x2 + (x2^2 + x1)(x1^2 + x2) - x1^2\,x2^2,\ (x1^2 + x2)^3 - 3\,x1^2\,x2^2,\ x1\,x2]$$

```
> expand(%);
```

$$[x1^3 + x2^3,\ x2^3 + 3\,x1^4\,x2 + x1^6,\ x1\,x2]$$

```
> evalb( % = [g1,g2,g3] );
```

$$true$$

Is R1 equal to C[x1,x2]?

```
> reduce(x1, GB_R1, ord);
```

$$x1$$

No, R1 is a proper subring of C[x1,x2].

What is the algebraic relation between f1,f2,f3. We know that a relation must exist, because it's three polynomials in a ring with transcendence degree 2.

```
> remove(has, GB_R1, {x1,x2});
```

$$[-F2^3 + F2\,F1 + F2^2\,F1^2 - 2\,F1\,F3^2\,F2 - F1^3 + F3^4 - 3\,F3^3 + 3\,F3^2 + F2\,F1\,F3 - F3]$$

```
> nops(%);
```

$$1$$

```
> P:=%%[1];
```

$$P := -F2^3 + F2\,F1 + F2^2\,F1^2 - 2\,F1\,F3^2\,F2 - F1^3 + F3^4 - 3\,F3^3 + 3\,F3^2 + F2\,F1\,F3 - F3$$

```
> subs(F1=f1, F2=f2, F3=f3, %);
```

$$-(x2^2 + x1)^3 + (x2^2 + x1)(x1^2 + x2) + (x2^2 + x1)^2 (x1^2 + x2)^2 - 2\,(x1^2 + x2)\,x1^2\,x2^2\,(x2^2 + x1) - (x1^2 + x2)^3 + x1^4\,x2^4 - 3\,x1^3\,x2^3 + 3\,x1^2\,x2^2 + (x2^2 + x1)(x1^2 + x2)\,x1\,x2 - x1\,x2$$

```
> expand(%);
```

$$0$$

```
> factor(P);
```

$$-F2^3 + F2\,F1 + F2^2\,F1^2 - 2\,F1\,F3^2\,F2 - F1^3 + F3^4 - 3\,F3^3 + 3\,F3^2 + F2\,F1\,F3 - F3$$

Checking if R1 is a subring of R2 when there are side relations.

R = C[x,y,z]/(y^5-x^4, z*x-1). Choose the following elements of R:
u1:=x^2; u2:=y^2*z; u3:=y^4*z^3+y^3*z^2; v:=y^4*z^3;

Define the following two subrings of R
R1=C[u1,u2,u3] and R2=C[v].

Are they equal? Two subquestions:
1) are u1,u2,u3 in C[v]? What does it mean if u1 is in C[v]? Well, then we have to find a polynomial P, such that P(v)=u1. But this is an equality in the ring R, where we are working modulo (y^5-x^4, z*x-1).
Therefore, what we are searching is a polynomial P, such that P(v) is equivalent to u1 modulo (y^5-x^4, z*x-1).
If we use the variable V for the polynomial P, then we search for a P in C[V] such that P is equivalent to v modulo (V-v,y^5-x^4,z*x-1).

```
> restart; with(Groebner): u1:=x^2; u2:=y^2*z; u3:=y^4*z^3+y^3*z^2;
  v:=y^4*z^3;
```

$$u1 := x^2$$
$$u2 := y^2 z$$
$$u3 := y^4 z^3 + y^3 z^2$$
$$v := y^4 z^3$$

```
> ideal_R2 := {V-v,y^5-x^4,z*x-1};
```

$$ideal\_R2 := \{y^5 - x^4, z x - 1, V - y^4 z^3\}$$

```
> ord:=lexdeg([x,y,z],[V]);
```

$$ord := \mathrm{lexdeg}([x, y, z], [V])$$

```
> GB_R2:=gbasis(ideal_R2,ord):
> map(reduce, [u1,u2,u3], GB_R2, ord);
```

$$[V^{10}, V^3, V^2 + V]$$

So this means that in the ring R, where the following two equations hold: y^5-x^4=0 and z*x-1=0, we have that u1=v^10. So that means that in R we have u1-v^10=0. Now R is of the form C[x,y,z]/ideal_R, so u1-v^10 must be in ideal_R = (y^5-x^4, z*x-1). Let's check:

```
> ideal_R := {y^5-x^4,z*x-1};
```

$$ideal\_R := \{y^5 - x^4, z x - 1\}$$

```
> ord:=tdeg(x,y,z); GB_R:=gbasis(ideal_R, ord);
```

$$ord := \mathrm{tdeg}(x, y, z)$$
$$GB\_R := [z x - 1, y^5 - x^4]$$

```
> expand(u1-v^10);
```

$$x^2 - y^{40} z^{30}$$

```
> reduce(%, GB_R, ord);
```

$$0$$

Now lets check if R2 is a subring of R1. That means: is v equivalent to some polynomial in u1,u2,u3 modulo the side relations y^5-x^4=0 and z*x-1=0?

If we use the variables U1,U2,U3 for u1,u2,u3, then the question is:
is v equivalent to an element of C[U1,U2,U3] modulo (U1-u1, U2-u2, U3-u3, y^5-x^4, z*x-1)?
If it is, then we can find that element of C[U1,U2,U3] by reducing v modulo that ideal with an ordering that tries it's best to eliminate the variables x,y,z.

```
> ideal_R1 := {U1-u1, U2-u2, U3-u3,y^5-x^4,z*x-1};
```

$$ideal\_R1 := \{y^5 - x^4, z x - 1, U3 - y^4 z^3 - y^3 z^2, U1 - x^2, U2 - y^2 z\}$$

```
> ord:=lexdeg([x,y,z],[U1,U2,U3]);
```

$$ord := \mathrm{lexdeg}([x, y, z], [U1, U2, U3])$$

```
> GB_R1:=gbasis(ideal_R1,ord):
> v;
```

$$y^4 z^3$$

```
> reduce(v,GB_R1,ord);
```

$$U1 + 2\,U2 - U3^2 + U3 - U2^2\,U3^2 + 2\,U2^3 + U2^2\,U3 - U2\,U3^2 + 2\,U2^2 + U2\,U3$$

So R2 is also a subring of R1, therefore R1 equals R2. This may look strange, but keep in mind here that they are both subrings of R, and R has transcendence degree only 1 over C because there are 3 variables and 2 independent relations.

Let R=C[x,y,z]/(y^4+x^4+x^3*y^2+x^5*y,z*x-1).

Let N,M be positive integers, and let R_{N,M} be the subring of R generated by the equivalence classes of x, y^M and (z*y)^N in R.

Consider the following statement:
R_{N,M} = R_{1,1} if and only if N is odd and igcd(N,M)=1.
It's just a statement, I'm not claiming that it is true nor that it is false.

Test if the statement is true or false for small values for N,M. Note: you have to take N,M really small otherwise the computation will take too long.

Calculating the intersection of two ideals.

The sum of two ideals: Let I1 and I2 be ideals in the ring R=C[x1,..,xn]. Then the sum of I1 and I2 is:
I1 + I2 ={i1+i2 with i1 in I1 and i2 in I2}.
If I1 is generated by the set F1, and I2 is generated by the set F2, then F1 union F2 is a set of generators for I1+I2.

The intersection of two ideals: Let I be the intersection of I1 and I2. It is prove to see that I is also an ideal. How do we compute a Groebner basis for the ideal I?

How can we find any nonzero elements of I in the first place? Well, take the set I1*I2 which is the set of all products i1*i2 where i1 in I1, i2 in I2. This is an ideal, and it is a subset of both I1 and I2. Is it the intersection? Not always, take for example I1=(x1) and I2=(x1). So we will need to use a trick or something to find the intersection I.

Let f be an element of I. Introduce a new variable t, so we will be working in the ring R[t]=C[x1,..,xn,t]. The trick now is:
f = t*f + (1-t)*f
How does this do any good? Well, t*f is an element of the ideal (t)*I1 of R[t], and (1-t)*f is an element of the ideal (1-t)*I2. Therefore:
t*f+(1-t)*f is an element of the ideal (t)*I1+(1-t)*I2.
If I1 is generated by a set F1, and I2 is generated by a set F2, then t*F1 union (1-t)*F2 is a set of generators for the ideal (t)*I1+(1-t)*I2 in the ring R[t].
Now: f in R[t] is in the ideal I, the intersection of I1 and I2, if and only if:
f in R (so: degree(f,t)=0)
and f in (t)*I1+(1-t)*I2.

So I is the intersection of (t)*I1+(1-t)*I2 and R, and we can compute a Groebner basis for that by using an elimination ordering that eliminates t from (t)*I1+(1-t)*I2. So we have to use lexdeg([t],[x1,..,xn]), compute a Groebner basis, and throw away everything that has the variable t.

Time for an example:

```
> restart; with(Groebner):
> F1:={x1^2+x2*x3,x2^2+x3*x1}; # generates I1, not necessarily a Groebner basis
```

$$F1 := \{x2^2 + x3\,x1, x1^2 + x2\,x3\}$$

```
> F2:={x3^2+x1*x2,x1*x2*x3}; # generates I2, not necessarily a Groebner basis
```

$$F2 := \{x3^2 + x1\,x2, x1\,x2\,x3\}$$

```
> F:={seq(t*i1, i1=F1), seq( (1-t)*i2, i2=F2)};
```

$$F := \{(1-t)\,x1\,x2\,x3, t\,(x2^2 + x3\,x1), t\,(x1^2 + x2\,x3), (1-t)\,(x3^2 + x1\,x2)\}$$

Now F generates the ideal ideal (t)*I1+(1-t)*I2. This set F doesn't have to be a Groebner basis, even if F1 and F2 are Groebner basis. And with the ordering we need:

```
> ord:=lexdeg([t],[x1,x2,x3]);
```

$$ord := \text{lexdeg}([t], [x1, x2, x3])$$

with that ordering it is in fact very unlikely that F is a Groebner basis.

```
> GB:=gbasis(F,ord);
```

$$GB := [-x3^3\,x2 + x2^2\,x3\,x1, -x3^3\,x1 + x1^2\,x2\,x3, x2^2\,x3^2 + x1\,x2^3 + 2\,x3^3\,x1, -x2\,x3^2\,x1 + x2^2\,x1^2, x1^2\,x3^2 + x1^3\,x2 + 2\,x3^3\,x2, x3^3\,x2^2 + x3^4\,x1, x3^3\,x1^2 + x3^4\,x2, t\,x2^2 + t\,x3\,x1, -x3^2 - x1\,x2 + t\,x3^2 + t\,x1\,x2, t\,x1^2 + t\,x2\,x3, -x3^3 + t\,x3^3, -x2\,x3^2 - x1\,x2^2 + 2\,x2\,t\,x3^2, -x3^2\,x1 - x1^2\,x2 + 2\,x1\,t\,x3^2]$$

```
> GB:=remove(has,GB,t);
```

$$GB := [-x3^3\,x2 + x2^2\,x3\,x1, -x3^3\,x1 + x1^2\,x2\,x3, x2^2\,x3^2 + x1\,x2^3 + 2\,x3^3\,x1, -x2\,x3^2\,x1 + x2^2\,x1^2, x1^2\,x3^2 + x1^3\,x2 + 2\,x3^3\,x2, x3^3\,x2^2 + x3^4\,x1, x3^3\,x1^2 + x3^4\,x2]$$

Now GB is a Groebner basis for the intersection of I1 and I2, where I1=(F1) and I2=(F2).

So everything in GB is in I1 as well as in I2. That, of course, we can check with Groebner basis, because it is the central problem, the problem that Groebner basis was designed to solve.

```
> F1:=gbasis(F1,ord);
```

$$F1 := [x2^2 + x3\,x1, x1^2 + x2\,x3]$$

```
> F2:=gbasis(F2,ord);
```

$$F2 := [x3^2 + x1\,x2, x3^3]$$

```
> seq(reduce(i,F1,ord), i=GB ); # check if I=(GB) is subset of I1:
```

$$0, 0, 0, 0, 0, 0, 0$$

```
> seq(reduce(i,F2,ord), i=GB ); # check if I is a subset of I2:
```

$$0, 0, 0, 0, 0, 0, 0$$

OK, we verified it.

Primary decomposition of an ideal.

A subset V of C^n is called an algebraic set when V is the solution set of polynomial equations, so when there exists a set F of polynomials such that V=V(F). Recall that V(F) stands for the set of solutions of F.

Recall that if I is the ideal generated by F, I=(F), then V(F)=V(I). And if J is the radical ideal of I, then V(F) is also V(J).

Definition:
An algebraic set V is called reducible if there exist algebraic sets V1, V2 that are not equal to V, and such that V=V1 union V2.

Proposition 1:
Every algebraic set V is a union of finitely many irreducible algebraic sets.

Definition:
An ideal I in a ring R (we take R=C[x1,..,xn]) is called a prime ideal when R/I has no zero-divisors. An ideal I is called primary when the radical ideal of I is a prime ideal.

Proposition 2:
If I is an ideal then V(I) is irreducible if and only if I is a primary ideal.

Proposition 3: The primary decomposition of an ideal:
Every ideal I can be written as an intersection of finitely many primary ideals I1, I2,..,Ik.
Then the algebraic set V(I) equals the union of the irreducible algebraic sets V(I1), V(I2), ..., V(Ik).

Note: there exists an algorithm (which of course uses the Groebner basis algorithm) that calculates the primary decomposition of an ideal. So given an ideal I, it computes primary ideals I1,..,Ik such that I is the intersection of those. And it also calculates the corresponding prime ideals J1,..,Jk, which are the radical ideals of I1,..,Ik.

So if we have an algebraic set V, which we assume is given by an ideal I for which we have a set of generators, then we can split up V into irreducible parts, and we can write I as an intersection of primary ideals that correspond to those irreducible parts.

Example: I = (x1*x2^2). The solution set is the union of two lines: x1=0 and x2=0, and those are the irreducible components of V. The primary decomposition of I is I = intersection of (x1) and (x2^2), these are primary ideals, and the corresponding prime ideals (the radical ideals of these primary ideals) are: (x1) and (x2).

The coordinate ring of algebraic set.

Think of x1,x2,..,xn as functions on the set C^n, the so-called *coordinate functions.* So when P is the point (2,5,3) then x1 is a function that takes the value 2 at the point P, x2 takes value 5 at P, and x3 takes value 3. Given these coordinate functions x1,..,xn we can construct more functions on the set C^n as follows:
R = C[x1,..,xn], the set of all polynomials in x1,..,xn. This is called the *coordinate ring of the algebraic set C^n.* So we think of every element of R as some function on C^n.

Let V be an algebraic set, and V is a subset of C^n. Suppose that I = I(V), so I is the set of all elements of R (which we view as functions on C^n) that vanish on V. Since V is a subset of C^n, and x1,..,xn are functions from C^n to C, by restricting x1,..,xn to the set V we can think of x1,..,xn as functions from V to C. Of course, we can find more functions P: V -> C, namely every element P in R can be viewed as a polynomial function from V to C.
But then what is the set of all polynomial functions from V to C? Is it R? Not really, you see, the set R has different elements that, when restricted to V, take the same values and so restricted to V they really are the same functions. In particular, everything in the ideal I, when restricted to V, is the zero function. Therefore, the set of polynomial functions from V to C can not be identified with R, but it can be identified with R/I.

Definition:
If V is an algebraic set and I = I(V), then the ***coordinate ring*** of V is defined as R/I.

Definition:
The dimension of an algebraic set V is defined as the transcendence degree of its coordinate ring.

Note:
When V is reducible, so V is a union of irreducible sets V1,..,Vk, which are called the irreducible *components* of V, then these components V1,..,Vk can have different dimensions. As you would expect, the dimension of V in that case equals the highest dimension of the V1,..,Vk.

Note:
When I is an ideal, and J is its radical ideal, then the transcendence degree of R/I is the same as the transcendence degree of R/J.

Calculating the dimension of an algebraic set

To calculate the dimension of an algebraic set, we have to determine the transcendence degree of its coordinate ring. If the set is given by the ideal I, then the coordinate ring is R/J where J is the radical ideal of I. Now J can be determined, we can even determine much more namely a primary decomposition can be calculated. However, we don't need J to determine the dimension of the algebraic set, which equals transcendence degree of R/J, because this number is also equal to the transcendence degree of R/I.

How to determine the transcendence degree of R/I?

Well, R/I is generated by x1,..,xn. But there are relations between this generators. These relations are given by I. Consider the following subrings of R/I:

Let x_1 stand for the equivalence of x1 in the ring R/I. So x_1 = x1+I. And the same for x_2, .. , x_n. So R/I is a ring generated over C by x_1,..,x_n. Now we will construct a sequence of subrings as follows:
C subset C[x_1] subset C[x_1,x_2] ... subset R/I.

In this sequence of subrings, the transcendence degree goes up in every step by either 0 or 1. If it goes up by 0, then x_{i+1} is algebraically dependent on x_1,..,x_i, which means that there exists an algebraic relation between x_1,..,x_{i+1} in which x_{i+1} appears. We can determine such relations, when they exist.

```
> restart; with(Groebner):
> ord:=plex(x4,x3,x2,x1);
```

$$ord := \text{plex}(x4, x3, x2, x1)$$

Note that the pure lexicographic ordering is also an elimination ordering. Namely: x4 larger than everything in [x3,x2,x1], just like the ordering lexdeg([x4],[x3,x,x1]). But x3 is also larger than everything in [x2,x1], just like lexdeg([x4,x3],[x2,x1]). Etc.

```
> F:={x1^2+x2*x3, x2^2+x3*x4,x3^2+x4*x1,x4^2+x1*x2};
```

$$F := \{x1^2 + x2\,x3, x2^2 + x3\,x4, x3^2 + x4\,x1, x4^2 + x1\,x2\}$$

```
> F:=gbasis(F,ord);
```

$$F := [x1^5 + x2^5, x1^3\,x3 - x2^4, x1^2 + x2\,x3, x2^3 + x1\,x3^2, -x1\,x2^2 + x3^3, x3^2 + x4\,x1, x4\,x2^2 + x1^3, x2^2 + x3\,x4, x4^2 + x1\,x2]$$

```
> GB_x1:=remove(has,F,{x2,x3,x4});
```

$$GB\_x1 := [\,]$$

x_1 could be algebraically dependent over C, or could be independent. If it were dependent (which meant that there existed a relation involving just x_1), then the above calculation would have shown that. But it didn't so x_1 is algebraically independent over C, so going from C to C[x_1], the transcendence degree goes up by 1.

```
> GB_x1_x2:=remove(has,F,{x3,x4});
```

$$GB\_x1\_x2 := [x1^5 + x2^5]$$

So we see that x_2 is algebraically dependent over C[x_1]. So going from C[x_1] to C[x_1,x_2] the transcendence degree does not go up.

```
> GB_x1_x2_x3:=remove(has,F,{x4});
```

$$GB\_x1\_x2\_x3 := [x1^5 + x2^5, x1^3\,x3 - x2^4, x1^2 + x2\,x3, x2^3 + x1\,x3^2, -x1\,x2^2 + x3^3]$$

```
> map(normalf, GB_x1_x2_x3, GB_x1_x2, ord);
```

$$[0, x1^3\,x3 - x2^4, x1^2 + x2\,x3, x2^3 + x1\,x3^2, -x1\,x2^2 + x3^3]$$

The relations in GB_x1_x2_x3 have a non-zero coefficient for x3, because when we reduce modulo GB_x1_x2 the x3 still doesn't vanish (because note that to have a relation that involves x3, the coefficient should not just be zero in R, it should be zero in R/I).

So x_3 is dependent over C[x_1,x_2], and when we go to C[x_1,x_2,x_3] the transcendence degree does not go up.

```
> map(normalf,F,GB_x1_x2_x3,ord);
```

$$[0, 0, 0, 0, 0, x3^2 + x4\,x1, x4\,x2^2 + x1^3, x2^2 + x3\,x4, x4^2 + x1\,x2]$$

x_4 is also dependent over C[x_1,x_2,x_3], so when adding x_4, the transcendence degree does not go up. Therefore, the transcendence degree of R = C[x1,x2,x3,x4/I = C[x_1,x_2,x_3,x_4] equals 1.

So the solution set of I, which is V(I), is an algebraic set with dimension 1. Note that Maple has a different method of computing this dimension, based on the Hilbert series. See the help page for a definition. Such Hilbert series are very useful when studying polynomial ideals.

```
> hilbertdim(F, tdeg(x1,x2,x3,x4));
```

1

Note that hilbertdim works with any ordering. Therefore we take tdeg because in general that is the fastest.

Zero dimensional algebraic sets.

Let I be an ideal, and let V be its set of solutions, and I(V) is ideal of polynomials that vanish on V. We know that I(V) is the radical ideal of I, and that R/I(V) is the coordinate ring of the algebraic set V, where R=C[x1,..,xn].

When is the dimension of V equal to zero? It is zero when the transcendence degree of R/I(V) over C equals zero. Note that when V=V(I), then the transcendence degree of R/I equals the transcendence degree of R/I(V), even though I(V), which is the radical of I, can be a larger ideal than I.

1) So the dimension of V equals zero:
2) if and only if all elements of R/I(V) are algebraically dependent over C,
3) if and only if the equivalence classes of x.i in R/I(V) is algebraically dependent over C for every i=1..n,
4) if and only if for each x.i there exists a polynomial P.i(x.i) in C[x.i] such that P.i(x.i) in the ideal I(V),
5) if and only if for each x.i there exists a polynomial Q.i(x.i) in C[x.i] such that Q.i(x.i) in the ideal I (note that if P.i in I(V), then P.i to some power is in I, so we can take Q.i as some power of P.i),
6) if and only if R/I is finite dimensional as a C-vector space. Note: the set of monomials x1^e1*...*xn^en where e.i < degree(P.i) spans R/I as a C-vector space because whenever e.i >= degree(P.i) then we can reduce the monomial with P.i, and so 5) implies 6). Conversely, if R/I is finite dimensional, then the equivalence classes of x.i^0,x.i^1,x.i^2,...x.i^N in R/I must be linearly dependent over C whenever N is larger than the dimension of R/I as a C-vector space. Writing down such a linear dependence gives you a polynomial Q.i, so we see that 6) also implies 5).

Note: If G is a Groebner basis for an ideal I, then the set S of all power products in [x1,..,xn] that can not be reduced by G forms a basis of R/I as a C-vector space.
Why? Well, as long as a polynomial has power products that are not in S, we can reduce them with G. So we should not just reduce the leading monomial (which in Maple is done by the command reduce), but all monomials (which in Maple is called normalf). The normalf command will result in a polynomial in which all power products are in the set S, in other words, normalf reduces any polynomial to a linear combination of elements of S.

We see that this set S is finite if and only if the transcendence degree of R/I equals zero, if and only if the dimension of V is zero. Such an ideal I is called a *zero-dimensional ideal.*

We also see that if G is a Groebner basis for an ordering ord, then the set S is finite if and only if:
7) for each variable x.i there is an element g in G such that the leading power product of g is a power of x.i. Note that this is not the same statement as 5) because g is not necessarily an element of C[x.i], like P.i is. All of the above are also equivalent to the following statement:
8) V is a finite set. It is easy to see that 8) implies 4), if alpha1,..,alpha.n are the x.i-coordinates of the points of V, then we can take P.i(x.i) equal to (x.i-alpha1)*...*(x.i-alpha.n), this vanishes on V and hence it is in I(V). Conversely, 4) implies 8), because when P.i(x.i) is in I(V), then the x.i-coordinates of all elements of V are roots of P.i(x.i), so these points take at most degree(P.i) different x.i-coordinates. So the number of points in V is bounded by degree(P.1)*degree(P.2)*...*degree(P.n).
Note that in fact the number of elements of V equals the dimension (as C-vector space) of R/I(V), because if P1,..,Pk are the points in V, then for each i we can construct a polynomial function that takes value 1 on P.i, and value 0 on the other points of V, and it is not hard to see that this is a basis as vector space of R/I(V). The dimension of the vector space R/I is in general larger, but is always finite if and only if the dimension of R/I(V) is finite.

So we have 8 different statements, all of which are equivalent. The easiest way to check if they hold is by checking condition 7), because we can use any ordering with that condition, and so we can take a "fast" ordering (usually tdeg).

Checking if an ideal is zero-dimensional ideal is done as follows:

```
> restart; with(Groebner): ord:=tdeg(x1,x2,x3,x4);
```

$$ord := \mathrm{tdeg}(x1, x2, x3, x4)$$

```
> F:={x1^2+x2*x3,x2^2+x3*x4,x3^2+x4*x1,x4^2+x1*x2,x1^1+x2^2+x3^3+x4^4};
```

$$F := \{x1 + x2^2 + x3^3 + x4^4, x1^2 + x2\,x3, x2^2 + x3\,x4, x3^2 + x4\,x1, x4^2 + x1\,x2\}$$

```
> G:=gbasis(F,ord);
```

$$G := [x3^2 + x4\,x1, x2^2 + x3\,x4, x4^2 + x1\,x2, x1^2 + x2\,x3, x1\,x3\,x4 - x2\,x4^2, x4^4 - x2\,x4^2 - x3\,x4 + x1]$$

```
> v:=[seq(leadmon(i,ord)[2],i=G)];
```

$$v := [x3^2, x2^2, x1\,x2, x1^2, x1\,x3\,x4, x4^4]$$

```
> v:=remove(type,v,`*`);
```

$$v := [x3^2, x2^2, x1^2, x4^4]$$

```
> map(i->op(1,i),v);
```

$$[x3, x2, x1, x4]$$

So this set F corresponds to a zero-dimensional ideal, hence V(F) is a zero-dimensional algebraic set, in other words: it is a finite set.

```
> hilbertdim(F,ord);
```

$$0$$

```
> ord_lex:=plex(x1,x2,x3,x4);
```

$$ord\_lex := \mathrm{plex}(x1, x2, x3, x4)$$

```
> gbasis(F,ord_lex); # this will take a while.
Warning, computation interrupted
```

The easiest way to solve a zero-dimensional ideal is by using a pure lexicographic ordering. Because then we will find a polynomial consisting of only the variable x4. Such polynomial must be in the ideal because condition 5) for zero-dimensional ideals. But with the ordering we picked, it must then also be in the Groebner basis.

By calculating a root of that polynomial, and plugging in x4=that root in the Groebner basis, we only have the variables x1,x2,x3 remaining. But then again, because of the ordering, we will find a polynomial consisting only of the variable x3. We can continue this way, and find a solution of the ideal. We can find all solutions in this way.

But we may wonder now, is there no faster way to find a polynomial P4(x4) in C[x4] in the ideal? By faster we mean: using the faster ordering tdeg instead of plex? One would think so, because with tdeg we were able to decide if V is zero-dimensional or not. So why not compute the solutions with tdeg as well?

How to do that? Let's see, why again was it true that there is an element P4(x4) in the ideal? Well, we know that R/I is finite dimensional, and so if we take 1,x4,x4^2,.. and we normalf them,then at some point we should get a linearly dependent set. By calculating a linear dependence, we find an element P4(x4) in the ideal.

Here we take N=17. How do we know to take N=17? We don't, we simply keep on increasing N until the set of linear equations has a solution. This lead me to N=17. Of course that is something we can implement in a more clever way.

```
> N:=17;
```

$$N := 17$$

```
> expand(add(c[i]*normalf(x4^i,G,ord),i=0..N));
```

$$c_0 + c_2\,x4^2 + c_3\,x4^3 + c_7\,x4^3 - 2\,c_8\,x1 + c_{10}\,x4^2 + c_{11}\,x4^3 + c_{11}\,x4^2 + c_{12}\,x4^3 - 3\,c_{12}\,x1 - 3\,c_{13}\,x1 - 2\,c_{14}\,x4^2$$
$$+ c_{14}\,x1 - 2\,c_{15}\,x4^3 + 6\,c_{15}\,x4^2 + 6\,c_{16}\,x4^3 + c_{17}\,x4^2 - 18\,c_{17}\,x1 + c_6\,x3\,x4\,x2 + c_1\,x4 + c_5\,x2\,x4^3 + c_5\,x3\,x4^2$$
$$- c_5\,x4\,x1 - c_6\,x4^2\,x1 - c_7\,x4^3\,x1 + c_8\,x2\,x4^2 - c_8\,x2\,x3 + 2\,c_8\,x3\,x4 + c_9\,x2\,x4^3 + c_9\,x2\,x4^2 + 3\,c_9\,x3\,x4^2$$

$$
\begin{aligned}
&+c_9\, x2\, x3 - 2\, c_9\, x4\, x1 + 2\, c_{10}\, x3\, x4^3 + c_{10}\, x2\, x4^3 - 2\, c_{10}\, x4^2\, x1 - 2\, c_{11}\, x4^3\, x1 - c_{11}\, x3\, x4^3 - 2\, c_{11}\, x4^2\, x1 \\
&- 2\, c_{11}\, x1\, x3 - 2\, c_{12}\, x4^3\, x1 + c_{12}\, x4^2\, x1 - 2\, c_{12}\, x2\, x4^2 - c_{12}\, x3\, x4^2 + c_{12}\, x1\, x3 - 3\, c_{12}\, x2\, x3 + 3\, c_{12}\, x3\, x4 \\
&+ c_{13}\, x4^3\, x1 - 2\, c_{13}\, x2\, x4^3 - c_{13}\, x3\, x4^3 + 6\, c_{13}\, x2\, x4^2 + 7\, c_{13}\, x3\, x4^2 + 2\, c_{13}\, x2\, x3 - 3\, c_{13}\, x4\, x1 + 3\, c_{13}\, x3\, x4 \\
&+ 6\, c_{14}\, x2\, x4^3 + 9\, c_{14}\, x3\, x4^3 - 2\, c_{14}\, x4^2\, x1 + 3\, c_{14}\, x3\, x4^2 + c_{14}\, x1\, x3 + c_{14}\, x2\, x3 - 3\, c_{14}\, x4\, x1 - c_{14}\, x3\, x4 \\
&- 2\, c_{15}\, x4^3\, x1 - 3\, c_{15}\, x3\, x4^3 - 12\, c_{15}\, x4^2\, x1 + c_{15}\, x2\, x4^2 - c_{15}\, x3\, x4^2 - 9\, c_{15}\, x1\, x3 + c_{15}\, x4\, x1 - 12\, c_{16}\, x4^3\, x1 \\
&+ c_{16}\, x2\, x4^3 - c_{16}\, x3\, x4^3 + 4\, c_{16}\, x4^2\, x1 - 15\, c_{16}\, x2\, x4^2 - 4\, c_{16}\, x3\, x4^2 + 3\, c_{16}\, x1\, x3 - 6\, c_{16}\, x2\, x3 + 4\, c_{17}\, x4^3\, x1 \\
&- 15\, c_{17}\, x2\, x4^3 - 5\, c_{17}\, x3\, x4^3 + c_{17}\, x4^2\, x1 + 18\, c_{17}\, x2\, x4^2 + 9\, c_{17}\, x3\, x4^2 + c_{17}\, x1\, x3 - 3\, c_{17}\, x2\, x3 + 18\, c_{17}\, x3\, x4 \\
&+ c_7\, x2\, x4^2\, x3 + c_8\, x4^3\, x2\, x3 - c_9\, x3\, x4\, x2 - c_{10}\, x2\, x4^2\, x3 + 2\, c_{10}\, x3\, x4\, x2 - c_{11}\, x4^3\, x2\, x3 + 4\, c_{11}\, x2\, x4^2\, x3 \\
&+ c_{11}\, x3\, x4\, x2 + 4\, c_{12}\, x4^3\, x2\, x3 - 3\, c_{13}\, x3\, x4\, x2 - 4\, c_{14}\, x2\, x4^2\, x3 - 4\, c_{15}\, x4^3\, x2\, x3 + 9\, c_{15}\, x2\, x4^2\, x3 \\
&+ 7\, c_{15}\, x3\, x4\, x2 + 9\, c_{16}\, x4^3\, x2\, x3 + 4\, c_{16}\, x2\, x4^2\, x3 + 4\, c_{17}\, x4^3\, x2\, x3 - c_{17}\, x2\, x4^2\, x3 - 5\, c_{17}\, x3\, x4\, x2 - c_4\, x1 \\
&+ c_6\, x4^2 + c_4\, x2\, x4^2 + c_4\, x3\, x4
\end{aligned}
$$

```
> c[N]-1, coeffs(%,{x1,x2,x3,x4});
```

$$
\begin{aligned}
&c_{17}-1,\ c_{12}-9\,c_{15}+c_{17}+3\,c_{16}-2\,c_{11}+c_{14},\ -c_{11}-c_{16}+2\,c_{10}-c_{13}-3\,c_{15}-5\,c_{17}+9\,c_{14}, \\
&\quad c_7-2\,c_{15}+c_{11}+6\,c_{16}+c_3+c_{12},\ c_{17}-c_6+4\,c_{16}+c_{12}-2\,c_{11}-2\,c_{10}-12\,c_{15}-2\,c_{14}, \\
&\quad 9\,c_{17}-c_{15}+3\,c_{14}+3\,c_9+c_5-4\,c_{16}-c_{12}+7\,c_{13},\ c_{16}+6\,c_{14}+c_{10}-2\,c_{13}-15\,c_{17}+c_5+c_9, \\
&\quad -c_7+4\,c_{17}-2\,c_{12}-2\,c_{11}-2\,c_{15}+c_{13}-12\,c_{16},\ 9\,c_{16}+4\,c_{12}-c_{11}+4\,c_{17}-4\,c_{15}+c_8,\ c_0, \\
&\quad c_9-6\,c_{16}-3\,c_{12}+c_{14}+2\,c_{13}-3\,c_{17}-c_8,\ 2\,c_8+3\,c_{12}+3\,c_{13}+c_4+18\,c_{17}-c_{14},\ -2\,c_9-3\,c_{13}+c_{15}-c_5-3\,c_{14}, \\
&\quad -3\,c_{13}-18\,c_{17}-c_4+c_{14}-3\,c_{12}-2\,c_8,\ c_1,\ c_{17}+c_{10}-2\,c_{14}+c_{11}+6\,c_{15}+c_6+c_2, \\
&\quad 6\,c_{13}+c_{15}+18\,c_{17}+c_4-15\,c_{16}+c_9+c_8-2\,c_{12},\ c_7-c_{17}+9\,c_{15}-c_{10}+4\,c_{16}+4\,c_{11}-4\,c_{14}, \\
&\quad c_6+7\,c_{15}-5\,c_{17}+c_{11}+2\,c_{10}-3\,c_{13}-c_9
\end{aligned}
$$

```
> solve({%});
```

$$
\begin{aligned}
&\{c_{17}=1,\ c_0=0,\ c_1=0,\ c_4=0,\ c_{14}=0,\ c_{16}=0,\ c_3=0,\ c_{15}=0,\ c_{10}=0,\ c_8=0,\ c_{11}=0,\ c_2=-1,\ c_6=0,\ c_7=1, \\
&\quad c_{13}=-5,\ c_9=10,\ c_5=-5,\ c_{12}=-1\}
\end{aligned}
$$

```
> P4:=subs(%,add(c[i]*x4^i,i=0..N));
```

$$P4 := -x4^2 - 5\,x4^5 + x4^7 + 10\,x4^9 - x4^{12} - 5\,x4^{13} + x4^{17}$$

```
> normalf(P4,G,ord);
```

$$0$$

So P4 is in the ideal. Since N=17 is the smallest N for which we find a solution, we can conclude that the ideal I intersected with C[x4] is generated by this polynomial P4.

```
> factor(P4);
```

$$x4^2\,(x4-1)\,(x4^2+1)\,(x4^{12}+x4^{11}-4\,x4^8-5\,x4^7-x4^6+6\,x4^4+5\,x4^3+x4+1)$$

```
> {solve(%)};
```

$$\{0,\ 1,\ I,\ \mathrm{RootOf}(\_Z^{12}+\_Z^{11}-4\,\_Z^8-5\,\_Z^7-\_Z^6+6\,\_Z^4+5\,\_Z^3+\_Z+1),\ -I\}$$

We can plug in each of these values for x4, and then we only have the variables x1,x2,x3 remaining. We can find the values for those in a similar way. For example take x4=1.

```
> subs(x4=1,F);
```

$$\{x1^2+x2\,x3,\ 1+x1\,x2,\ x3^2+x1,\ x2^2+x3,\ x1+x2^2+x3^3+1\}$$

```
> gbasis(%,ord);
```

$$[1 + x3, x2 - 1, x1 + 1]$$

so for x4=1 it is easy to determine the values of the remaining variables. In general, however, we should expect that we need to do something similar as what we had to do to find those values for x4.

An assignment

```
> restart; with(Groebner):
```

Let F be a polynomial map from C^3 to C^5 given by:

```
> F:=[x1*x2+x3, x2*x3+x1, x3*x1+x2, x1*x2*x3, x1+2*x2+3*x3];
```

$$F := [x1\,x2 + x3, x2\,x3 + x1, x3\,x1 + x2, x1\,x2\,x3, x1 + 2\,x2 + 3\,x3]$$

Try to answer the following question:

Is F a 1-1 map?
If so, how do you show that?
If not, give to different points P1,P2 in C3 such that F(P1)=F(P2).

```
> eqn:=F-[y1,y2,y3,y4,y5];
```

$$eqn := [-y1 + x1\,x2 + x3, -y2 + x2\,x3 + x1, -y3 + x3\,x1 + x2, -y4 + x1\,x2\,x3, -y5 + x1 + 2\,x2 + 3\,x3]$$

```
> ord:=lexdeg([x1,x2,x3],[y1,y2,y3,y4,y5]);
```

$$ord := \mathrm{lexdeg}([x1, x2, x3], [y1, y2, y3, y4, y5])$$

```
> GB:=gbasis(eqn,ord):
> GB_Y:=remove(has,GB,[x1,x2,x3]):
> GB_Y:=gbasis(GB_Y,tdeg(y1,y2,y3,y4,y5)):
> hilbertdim(GB_Y,tdeg(y1,y2,y3,y4,y5));
```

$$3$$

So the image is 3-dimensional. This means that it could be 1-1, but doesn't have to be 1-1.

```
> reduce(x1,GB,ord);
```

$$x1$$

This means that we are not able to write x1 as a polynomial in y1..,y5.

```
> reduce(x2,GB,ord);
```

$$-3\,y4 + 2\,x1 + 9\,y3 - 3\,x1\,y5 + 3\,y2\,x1 + 6\,y1 - 2\,y5$$

```
> reduce(x3,GB,ord);
```

$$-2\,y2\,x1 + 2\,x1\,y5 - 3\,x1 - 4\,y1 - 6\,y3 + 2\,y4 + 3\,y5$$

We see that x2,x3 can be expressed as polynomials in x1,y1,y2,y3,y4,y5.

But still we do not know at this point if F is 1-1 or not. Try to find this out today in class.

If it's not 1-1, try to add one more coordinate to F (so making it a map from C^3 to C^6) in such a way that it becomes 1-1. Is that possible?

If it is 1-1, then try to remove one of the entries of F, making it a map from C^3 to C^5, in such a way that it still is 1-1. Is that possible?

Writing an ideal as an intersection of other ideals.

```
> F:=[-x3^3*x2+x2^2*x3*x1, -x3^3*x1+x1^2*x2*x3,
```

```
x2^2*x3^2+x1*x2^3+2*x3^3*x1, -x2*x3^2*x1+x2^2*x1^2,
x1^2*x3^2+x1^3*x2+2*x3^3*x2, x3^3*x2^2+x3^4*x1, x3^3*x1^2+x3^4*x2]
;
```

$F := [-x3^3\, x2 + x2^2\, x3\, x1, -x3^3\, x1 + x1^2\, x2\, x3, x2^2\, x3^2 + x1\, x2^3 + 2\, x3^3\, x1, -x2\, x3^2\, x1 + x2^2\, x1^2,$
$x1^2\, x3^2 + x1^3\, x2 + 2\, x3^3\, x2, x3^3\, x2^2 + x3^4\, x1, x3^3\, x1^2 + x3^4\, x2]$

```
> with(Groebner);
```

[*fglm*, *gbasis*, *gsolve*, *hilbertdim*, *hilbertpoly*, *hilbertseries*, *inter_reduce*, *is_finite*, *is_solvable*, *leadcoeff*, *leadmon*, *leadterm*, *normalf*, *pretend_gbasis*, *reduce*, *spoly*, *termorder*, *testorder*, *univpoly*]

The ideal I=(F) is not a primary ideal, which means that V(I) is a reducible algebraic set. How can we write V(I) as a union of irreducible components?

```
> gbasis(F,lexdeg([x1],[x2,x3]));
```

$[x3^6\, x2 + x2^4\, x3^3, -x3^3\, x2 + x2^2\, x3\, x1, x2^2\, x3^2 + x1\, x2^3 + 2\, x3^3\, x1, x3^3\, x2^2 + x3^4\, x1, -x3^3\, x1 + x1^2\, x2\, x3,$
$-x2\, x3^2\, x1 + x2^2\, x1^2, x3^3\, x1^2 + x3^4\, x2, x1^2\, x3^2 + x1^3\, x2 + 2\, x3^3\, x2]$

```
> remove(has,%,x1);
```

$$[x3^6\, x2 + x2^4\, x3^3]$$

```
> op(%);
```

$$x3^6\, x2 + x2^4\, x3^3$$

```
> factors(%);
```

$$[1, [[x3, 3], [x2, 1], [x3 + x2, 1], [x3^2 - x2\, x3 + x2^2, 1]]]$$

```
> v:=[seq(i[1],i=%[2])];
```

$$v := [x3, x2, x3 + x2, x3^2 - x2\, x3 + x2^2]$$

```
> seq(gbasis([op(F),i],tdeg(x1,x2,x3)),i=v);
```

$[x3, x1\, x2^3, x2^2\, x1^2, x1^3\, x2], [x2, x3^3\, x1, x1^2\, x3^2], [x3 + x2, x3^3\, x1 + x3^4, x1^2\, x3^2 - x3^4, x1^3\, x3 + x3^4], [$
$x3^2 - x2\, x3 + x2^2, x3^3\, x1 - x3^4 + x3^3\, x2, x2\, x3^2\, x1 - x3^4, x1^2\, x3^2 + x3^3\, x2, x1^2\, x2\, x3 + x3^3\, x2 - x3^4,$
$x1^3\, x2 + x3^3\, x2]$

```
>
```