Handouts

November 2, 2023 9:20 AM

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

[*Basis, FGLM, HilbertDimension, HilbertPolynomial, HilbertSeries, Homogenize, InitialForm, InterReduce, IsBasis, IsProper, IsZeroDimensional, LeadingCoefficient, LeadingMonomial, LeadingTerm, MatrixOrder, MaximalIndependentSet, MonomialOrder, MultiplicationMatrix, MultivariateCyclicVector, NormalForm, NormalSet, RationalUnivariateRepresentation, Reduce, RememberBasis, SPolynomial, Solve, SuggestVariableOrder, Support, TestOrder, ToricIdealBasis, TrailingTerm, UnivariatePolynomial, Walk, WeightedDegree*]

```
> f1,f2 := x*y+1, y+1;
```

$$f1, f2 := x\,y + 1, y + 1$$

```
> f := x*y^2-x;
```

$$f := x\,y^2 - x$$

```
> f1,f2 := x*y+1, y+1;
```

$$f1, f2 := x\,y + 1, y + 1$$

$$\overset{f_1}{\langle xy+1}, \overset{f_2}{y+1\rangle} = \langle \overset{f_3}{-x+1}, \overset{f_2}{y+1} \rangle$$

VUL

$$\downarrow$$

$$f_3 = f_1 - x f_2 = -x+1$$

Divide f by [f1,f2] using lexicographical ordering with x>y

```
> NormalForm( f, [f1,f2], plex(x,y) );
```

$$1 - x$$

```
> NormalForm( f, [f2,f1], plex(x,y) );
```

$$0$$

```
> NormalForm( f, [f1,f2], plex(x,y), 'a' );
```

$$1 - x$$

```
> a;
```

$$[y, -1]$$

$$I = \langle \overset{f_1}{xy+1}, \overset{f_2}{y+1} \rangle$$

$$\downarrow$$

$$I = \langle y+1, x-1 \rangle$$

```
> G := Basis( [f1,f2], plex(x,y) );
```

$$G := [y + 1, x - 1]$$

```
> NormalForm( f, G, plex(x,y) );
```

$$0$$

```
> NormalForm( f, [G[2],G[1]], plex(x,y) );
```

$$0$$

The Division Algorithm for $k[x_1, x_2, \ldots, x_n]$.

Input $\prec$ a monomial ordering on $\mathbb{Z}^n_{\geq 0}$
$f \in k[X]$, divisors $f_1, f_2, \ldots, f_s \in k[X]$
where $X = x_1, x_2, \ldots, x_s$, $f_i \neq 0$

Outputs quotients $a_1, a_2, \ldots, a_s \in k[X]$ and
remainder $r \in k[X]$ satisfying
(i) $f = a_1 f_1 + a_2 f_2 + \ldots a_s f_s + r$,
(ii) $LT(f_i)$ does not divide any term in r and
(iii) $LM(f) \geq LM(a_i f_i)$ for $1 \leq i \leq s$.

$(a_1, a_2, \ldots, a_s) \leftarrow (0, 0, \ldots, 0)$

$(r, p) \leftarrow (0, f)$

while $p \neq 0$ **do**

find the first i such that $LT(f_i) | LT(p)$.

if $\nexists i$ **then** $(r, p) \leftarrow (r + LT(p), p - LT(p))$ **CASE 1**

else $t \leftarrow LT(p)/LT(f_i)$

$(a_i, p) \leftarrow (a_i + t, p - t f_i)$ **CASE 2**

end if

end while

output $(a_1, a_2, \ldots, a_s, r)$

Proof of termination.
I claim each time round the loop either $p_{new} = 0$ or $LM(p_{new}) < LM(p_{old})$.

CASE 1. $LT(f_i) \nmid LT(p)$ $\quad p = LT(p) + \overbrace{(p - LT(p))}$

Is $LM(p - LT(p)) < LM(p)$ or $p - LT(p) = \underline{0}$.

CASE 2. Is $p - tf_i = 0$ or $LM(p - tf_i) < LM(p)$?

Letting $p_1, p_2, p_3, \ldots$ denote the values of p at the ith step in the division algorithm we have

$$LM(p_1 = f) > LM(p_2) > LM(p_3) > \ldots$$

Since $>$ is a well ordering Lemma 2 says such a sequence cannot continue indefinitely, hence eventually $p = 0$ and the $\div$ alg. stops.