35) Show that the *grlex* (degree, then lexicographic) ordering is a monomial ordering.

36) Rewrite the following polynomial, ordering its terms according to the *lex*, *grlex* and *grevlex* ordering and give $LM(f)$, $LT(f)$ and multideg(f) in each case.

$$f(x,y,z) = 2x^2y^8 - 3x^5yz^4 + xyz^3 - xy^4.$$

37) Let $B = (x^2y - z, xy - 1)$ and $f = x^3 - x^2y - x^2z + x$.
a) Compute the remainder of dividing f by B for both the *lex* and the *grlex* ordering.
b) Repeat part a) with the order of the pair B reversed.

38) Let $I = \langle x^3y^6, x^5y^4, x^6, x^4y^7\rangle$. Find a minimal generating set for I as a subset of the given generators.

39) Let $I = \langle xy^3 - x^2, x^3y^2 - y\rangle \lhd \mathbb{Q}[x,y] = R$.
a) Compute a (nonreduced to avoid messy coefficients) Gröbner basis for I with respect to *gradlex* ordering. Determine the possible form of canonical representatives for cosets in R/I. What is the dimension of R/I as a $\mathbb{Q}$ vector space.
b) The maps $\alpha: R/I \to R/I$, $I + p \mapsto I + x \cdot p$ and $\beta: R/I \to R/I$, $I + p \mapsto I + y \cdot p$ are $\mathbb{Q}$-vector-space homomorphisms of R/I. (Persuade yourself that they are, but you do not need to show this.) Compute matrices M_α and M_β for α, respectively β (with respect to the basis found in part a)).
c) Show that the map $\varphi: R \to \mathbb{Q}^{d\times d}$ (where d is the appropriate dimension), $f(x,y) \mapsto f(M_\alpha, M_\beta)$ is a ring homomorphism with kernel I. (In other words: we can compute in R/I by computing with these matrices instead.)

40) Let $f \in \mathbb{Z}[x]$ be monic (leading coefficient 1) and irreducible of degree n and $\mathbb{Q} < K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ be the splitting field of f where the α_i are the roots of f in K. Let $G = \mathrm{Gal}(K/\mathbb{Q})$
a) Show that the action of G on the roots of f gives a homomorphism $\varphi: G \S_n$.
b) Show that $\ker\varphi$ is trivial.
c) Show that $G^\varphi \le A_n$ if and only if $\mathrm{Disc}(f) = \mathrm{Res}(f, f')$ is a square in $\mathbb{Z}$.

Gröbner bases in GAP

To start using it, one has to define indeterminates and polynomials. Indeterminates are displayed either by their internal numbers or you can prescribe names. (Note however that the names hide the internal numbers and these numbers are basis for the monomial orderings. the best is to define a set of variables at the start and then not to redefine them afterwards.

```
gap> x:=X(Rationals,1); # number
x_1
gap> x:=X(Rationals,"x");
x
gap> y:=X(Rationals,"y");
y
gap> IndeterminateNumberOfUnivariateLaurentPolynomial(y);
2
```

The three orders from the lecture are defined as `MonomialLexOrdering()`, `MonomialGrlexOrdering()` and `MonomialGrevlexOrdering()`. `LeadingTerm` gives the leading term of a polynomial.

```
gap> LeadingTerm(x*y^2+2*x^2*y,MonomialGrlexOrdering());
2*x^2*y
```

`GrobnerBasis` computes a Gröbner basis. (You can set the info level as done here to get some information about the calculations.)

```
gap> B:=[x*y-y^2,y^2-x];
[ x*y-y^2, -x+y^2 ]
gap> GrobnerBasis(B,MonomialGrlexOrdering());
[ x*y-y^2, y^2-x, -x^2+x ]
gap> G:=ReducedGroebnerBasis(B,MonomialLexOrdering());
[ y^2-x, x*y-x, x^2-x ]
```

`PolynomialReduction` can be used to determine remainders. The first entry is the remainder, the second the coefficients with respect to the list of basis elements. (Note that the division algorithm works slightly different than the one in the book, thus if G is not a Gröbner basis you might get different remainders.)

```
gap> PolynomialReduction(x^5*y,G,MonomialGrlexOrdering());
[ x, [ x^4+x^3*y+x^2*y^2+x*y^3+y^4+y^3+y^2+y+1, y^4+y^3+y^2+y+1, 0 ] ]
```

If you want to change the variable ordering, you can give it as an argument to the ordering. For example to change to an order $y > x$ we could do:

```
gap> G:=ReducedGroebnerBasis(B,MonomialGrlexOrdering(y,x));
[ x^2-x, x*y-x, y^2-x ]
```