Homework 4

Algorithms for Elementary Algebraic Geometry

Math 191, Fall Quarter 2007

Solutions.

1. It is not true that there are only a finite number of vectors between any two vectors in a monomial ordering on $\mathbb{N}^n$ when $n > 1$. For instance, in the lexicographic order on $\mathbb{N}^2$,

$$(1, 0) > (0, a) > (0, 1),$$

for any $a > 2$. However, it is true for the grlex order, since there are only finitely many elements with a given total degree.

2. We know that I has a finite basis consisting of monomials; choose any such finite basis B of I consisting of monomials. If B is not minimal, one can remove any redundant element and form a new basis for the same ideal which has one fewer generator than the original one. We can keep repeating this process until the resulting basis is minimal. This process will terminate since B is finite. Now, suppose we are given two minimal bases $B = \{x^{\alpha(1)}, \ldots, x^{\alpha(s)}\}$ and $C = \{x^{\beta(1)}, \ldots, x^{\beta(t)}\}$ for I. Then $x^{\alpha(1)}$ is divisible by some $x^{\beta(i)}$, and $x^{\beta(i)}$ is also divisible by some $x^{\alpha(j)}$. Since $\{x^{\alpha(1)}, \cdots, x^{\alpha(s)}\}$ is minimal, one has $j = 1$ and hence $x^{\beta(i)} = x^{\alpha(1)}$. Continue this argument with $x^{\alpha(2)}, \ldots, x^{\alpha(s)}$, we will get $B = \{x^{\alpha(1)}, \ldots, x^{\alpha(s)}\} \subseteq \{x^{\beta(1)}, \ldots, x^{\beta(t)}\} = C$. Since C is a minimal basis, this yields $B = C$. The minimal basis of the monomial ideal

$$I = \langle x^2, x^5, xy^2, x^3y^3, y\rangle$$

of $k[x, y]$ is $B = \{x^2, y\}$.

3. (a) We need to show:
   i. for no α do we have $x^\alpha <_u x^\alpha$;
   ii. if $x^\alpha <_u x^\beta$ then $x^\alpha x^\gamma <_u x^\beta x^\gamma$;
   iii. for all α, β we have $x^\alpha \leq_u x^\beta$ or $x^\alpha \geq_u x^\beta$;
   iv. $x_i >_u 1$ for every i.

   Both $u \cdot \alpha$ and $u \cdot \beta$ are real numbers, so exactly one of the three cases

$$u \cdot \alpha > u \cdot \beta, \quad u \cdot \alpha = u \cdot \beta, \quad u \cdot \alpha < u \cdot \beta$$

must be true. For the cases $u \cdot \alpha > u \cdot \beta$ and $u \cdot \alpha < u \cdot \beta$, we have $x^\alpha >_u x^\beta$ and $x^\alpha <_u x^\beta$ respectively. If $u \cdot \alpha = u \cdot \beta$, we have $u \cdot (\alpha - \beta) = 0$. Since $u_1, \ldots, u_n$ are linearly independent over $\mathbb{Q}$, we must have $\alpha - \beta = 0$, so $x^\alpha = x^\beta$. This shows (i) and (iii). For (ii)

suppose $x^\alpha <_u x^\beta$, so $u \cdot \alpha < u \cdot \beta$. Then $u \cdot (\beta + \gamma - (\alpha + \gamma)) = u \cdot (\beta - \alpha) > 0$, hence $x^\alpha x^\gamma = x^{\alpha+\gamma} <_u x^{\beta+\gamma} = x^\beta x^\gamma$. Next we show $x^\alpha \geq_u 1$ for all α: this is equivalent to $u \cdot \alpha \geq 0$, which is true since u_i are all positive and $\alpha_i \geq 0$. This implies (iv).

(b) It is sufficient to show that $1, \sqrt{2}$ are linearly independent over $\mathbb{Q}$. This is true since $\sqrt{2}$ is irrational.

4. (a) The fact that $<_{\sigma,u}$ is a total ordering comes from the total ordering of $\mathbb{R}$ and of $<_\sigma$. For the multiplicative condition, if $x^\alpha <_{\sigma,u} x^\beta$, then either $u \cdot \alpha < u \cdot \beta$ or $u \cdot \alpha = u \cdot \beta$ and $x^\alpha <_\sigma x^\beta$. In the former case, $u \cdot (\alpha+\gamma) < u \cdot (\beta+\gamma)$, while in the latter case $u \cdot (\alpha+\gamma) = u \cdot (\beta+\gamma)$, and $x^{\alpha+\gamma} <_\sigma x^{\beta+\gamma}$. Thus in both cases $x^{\alpha+\gamma} <_{\sigma,u} x^{\beta+\gamma}$. Finally, for the third condition, note that $u \cdot \alpha \geq 0$ for all $\alpha \in \mathbb{N}^n$, since $u_1, \ldots, u_n \geq 0$. If $u \cdot \alpha = 0$, then we still have $1 \leq_{\sigma,u} x^\alpha$, since $1 \leq_\sigma x^\alpha$.

(b) Let $u = (1, 1, \ldots, 1)$. Then $u \cdot \alpha = |\alpha|$. So $<_{\text{lex},u}$ is the graded lexicographic order.