# MAS400: Solutions 1

Throughout this sheet $F$ will denote an arbitrary field unless otherwise stated.

1. For the following pairs of elements $f, g \in F[x]$ find the g.c.d. ($h$ say) of $f$ and $g$ and also find elements $a, b \in F[x]$ such that $af + bg = h$. (You should normalise $h$ so that its leading coefficient is 1.)

   (a) $f = x^2 - 2x + 1$ and $g = x^3 + 3x^2 - 7x + 3$.

   (b) $f = x^3 + 1$ and $g = x^4 + 5x^3 + 3x^2 - 2x - 1$.

   (c) $f = x^3 - 2$ and $g = 2x^2 + 3x - 1$.

   (d) $f = x^2 + 5x + 4$ and $g = 3x^2 - 2x + 1$.

   [You may assume that $F$ has characteristic 0, say $F = \mathbb{Q}$. It is also interesting to see what divergence we get from the general case when we set $F = \mathbb{F}_p$ for $p$ a prime.]

   The g.c.d. algorithm works with a particular field, not an arbitrary field. First, we will carry out the algorithm when $F = \mathbb{Q}$ (the workings will be identical over any field of characteristic 0). The answers are as follows.

   (a) $h = x - 1$, $a = (-x - 5)/2$, $b = 1/2$. Valid for all fields not of characteristic 2.

   (b) $h = x + 1$, $a = (x^2 + 6x + 8)/9$, $b = (-x - 1)/9$. Valid for all fields not of characteristic 3.

   (c) $h = 1$, $a = (-2x - 5)/11$, $b = (x^2 + x - 1)/11$. Valid for all fields not of characteristic 11.

   (d) $h = 1$, $a = (-51x + 67)/342$, $b = (17x + 74)/342$. Valid for all fields not of characteristics 2, 3, 19.

2. Show that the ideal of $I = \langle x, y \rangle$ of $F[x, y]$ cannot be generated by a single element.

   The ideal $I$ consists of all polynomials with zero constant term. We let $J = \langle x^2, xy, y^2 \rangle$. Thus $J$ consists of those polynomials that have zero coefficients for the monomials $1 = x^0y^0$, $x = x^1y^0$ and $y = x^0y^1$. Observe that whenever $q = q(x, y) \in I$ we have $xq, yq \in J$. Suppose that there is a $g \in F[x]$ such that $I = \langle g \rangle$. Then $g \in I$, so that $g = \alpha x + \beta y + j$ where $\alpha, \beta \in F$ and $j \in J$. Take $p \in F[x]$. Then $p = \gamma + q$ where $\gamma \in F$ and $q \in I$. So $gp = \alpha\gamma x + \beta\gamma y + h$ where $h = \alpha xq + \beta yq + jp \in J$. Since $x, y \in I$ there exist $p_1, p_2 \in R$ such that

$gp_1 = x$ and $gp_2 = y$. We can choose notation such that for $i = 1, 2$ we have $\gamma_i \in F$ and $p_i - \gamma_i \in I$, giving $gp_i = \alpha\gamma_i x + \beta\gamma_i y + h_i$ for some $h_i \in J$. But then $(\alpha\gamma_1, \beta\gamma_1) = (1, 0)$ and $(\alpha\gamma_2, \beta\gamma_2) = (0, 1)$. The former equation gives $\alpha \neq 0$, $\beta = 0$, while the latter gives $\alpha = 0$, $\beta \neq 0$, a contradiction. Thus $I$ cannot be singly generated.

3. For $n \geqslant 2$ show that the ideal of $I = \langle x_1, x_2, \ldots, x_n \rangle$ of $F[x_1, x_2, \ldots, x_n]$ cannot be generated by a single element. What is the minimum number of elements required to generate $I$? Justify your answer.

   We require a minimum of $n$ generators, for example $x_1, x_2, \ldots, x_n$; $n-1$ elements cannot generate $I$. The ideal $I$ consists of all polynomials with zero constant term. We let $J = \langle\, x_i^2, x_i x_j : 1 \leqslant i, j \leqslant n \,\rangle$. (In fact $J = I^2 = II$.) Thus $J$ consists of those polynomials that have zero coefficients for the monomials $1, x_1, x_2, \ldots, x_n$.

   Now the typical element of $I$ has the form $f = \lambda_1 x_1 + \cdots + \lambda_n x_n + g$ where $g \in J$ and $\lambda_i \in F$ for all $i$, and the typical element of $F[x_1, x_2, \ldots, x_n]$ is $p = \kappa + q$ where $q \in I$ and $\kappa \in F$. We have $qf \in J$, and thus $pf = \kappa(\lambda_1 x_1 + \cdots + \lambda_n x_n) + h$ where $h = qf + \kappa g \in J$. Let $f_i = \lambda_{i1} x_1 + \cdots + \lambda_{in} x_n + g_i$ where $g_i \in J$ and $\lambda_{ij} \in F$ for all $i$ and $j$. If $p_i \in F[x_1, x_2, \ldots, x_n]$ we shall define $\kappa_i$ and $q_i$ by $p_i = \kappa_i + q_i$ where $\kappa_i \in F$ and $q_i \in I$.

   If we identify $f = \lambda_1 x_1 + \cdots + \lambda_n x_n + g$ with the vector $v = (\lambda_1, \ldots, \lambda_n) \in F^n$ then this forces $f_i$ to be identified with $v_i = (\lambda_{i1}, \ldots, \lambda_{in})$. (The mapping from $I$ to $F^n$ is well-defined since $f \in I$ has a unique expression in the form $f = \lambda_1 x_1 + \cdots + \lambda_n x_n + g$ where $g \in J$ and $\lambda_i \in F$.) Anyway, the $p_1 f_1 + \cdots + p_m f_m$ gets mapped to $\kappa_1 v_1 + \cdots \kappa_m v_m \in F^n$. The $v_i$ are constant vectors (depending on $f_i$) in $F^n$, and since all spanning sets of $F^n$ require at least $n$ vectors it follows that $I$ also requires at least $n$ generators.

4. Let $n, m \in \mathbb{N}$, with $n \geqslant 1$. How many $n$-tuples $(a_1, \ldots, a_n) \in \mathbb{N}^n$ are there such that $\sum_{i=1}^{n} a_i = m$?
   This is a standard combinatorial trick. We make a one-to-one correspondence between such $n$-tuples and certain ways of placing $n + 1$ crosses into a line $m + n + 1$ boxes, with just one cross per box and the rest of the boxes being left blank. The crosses are labelled as the 0th cross up to the $n$th cross, with the 0th cross being placed in the leftmost box, the $n$th cross being placed in the rightmost box, and the $i$th cross being placed in a box strictly to the left of the $j$th cross whenever

$i < j$. The placement corresponding to the $n$-tuple $(a_1, \ldots, a_n)$ has $a_i$ blank boxes between the $i$th cross and the $(i+1)$th cross. Of course, it is also possible to determine the $n$-tuple $(a_1, \ldots, a_n)$ from the valid placement of $n+1$ crosses into a line of $m+n+1$ boxes. So we have a 1-to-1 correspondence between $n$-tuples and valid placements.

Now the first and last boxes contain crosses, but any distribution of the remaiming $n-1$ crosses among the remaining $m+n-1$ boxes is possible. There are $\binom{m+n-1}{n-1} = \binom{m+n-1}{m}$ such distributions, and therefore $\binom{m+n-1}{n-1} = \binom{m+n-1}{m}$ such $n$-tuples.