MAS400: Solutions 2

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

1. Show that $\mathbb{Z}[x]$ has ideals that are not generated by a single element. Thus $\mathbb{Z}[x]$ is not a principal ideal domain, even though it is a unique factorisation domain.

   An example of a non-principal ideal of $\mathbb{Z}[x]$ is $I = \langle 2, x\rangle$. More generally, the ideal $\langle n, x\rangle$ is non-principal for all $n \in \mathbb{Z} \setminus \{-1, 0, 1\}$. The ideal I consists of all polynomials $2p(x)+xq(x)$, where $p, q \in \mathbb{Z}[x]$. The polynomial $2p(x)$ has all of its coefficients being even integers, while $xq(x)$ has zero constant term. Therefore the typical element of I is a polynomial $f(x) = \sum_{i=1}^{n} a_i x^i$ where $a_i \in \mathbb{Z}$ for all i and a_0 is even. Suppose that I is principal, that is $I = \langle g\rangle$ for some polynomial g. Then the typical member of I is gh for some $h \in \mathbb{Z}[x]$. If $g = 0$ then $I = \{0\}$, a contradiction. If $\deg g \geqslant 1$ then $gh = 0$ (when $h = 0$) or $\deg(gh) \geqslant \deg g \geqslant 1$, so that $gh \neq 2$, also a contradiction. Therefore $\deg g = 0$ and $g = m \in \mathbb{Z} \setminus \{0\}$ is a non-zero constant, and so all coefficients of gh are integers divisible by m. Since $x \in I$, we need $m \mid 1$ (in $\mathbb{Z}$), forcing $m = 1$ or -1. But $1, -1 \notin I$, a contradiction that (finally) shows that I is non-principal. The non-principality of $\langle n, x\rangle$ for $n \notin \{-1, 0, 1\}$ is proved similarly.

2. Write, using pseudo-code, the univariate division algorithm (that is the algorithm that given $f, g \in F[x]$ with $g \neq 0$ will return $q, r \in F[x]$ such that $f = qg + r$ and $\deg r < \deg g$).

   See separate sheet of algorithms. Version II of `UnivariateDivision` is effectively a specialisation of `MultivariateDivision`, while Version I (probably 'better') is somewhat closer to one's idea of what long division does.

3. Rewrite the Euclidean Algorithm so that only a bounded number of variables is used. (These variables should be elements of $F[x]$, and not such things as an arbitrarily long sequence of elements of $F[x]$.)

   See separate sheet of algorithms. Version I is essentially as given in lectures. The crucial observation is that it is unnecessary to store $p_0, p_1, \ldots, p_{p-1}$ once we know p_j and p_{j+1}. Therefore we only need p_0, p_1,p_2, and we overwrite unneeded variables as appropriate. Similarly for the a_j and b_j. The q_j do not depend on their predecessors, and these can simply be replaced by q. See Version II of the algorithm.

4. Show that the only monomial order on $\mathbb{N}$ is $x^0 < x^1 < x^2 < \cdots < x^i < x^{i+1} < \cdots$.
Note the monomial x^i corresponds to $i \in \mathbb{N}$ and $(i) \in \mathbb{N}^1$. In lectures we showed that $0 < a$ for all non-zero $a \in \mathbb{N}^n$ whenever $<$ is a monomial order. So let $<$ be a monomial order on $\mathbb{N}$. We certainly have $0 < 1$, and thus also $m < m + 1$ for all $m \in \mathbb{N}$. So we have $0 < 1$, $1 < 2$, $2 < 3$, $3 < 4$, and so on. The transitivity of $<$ then ensures that $<$ is the usual order on $\mathbb{N}$.

5. Show that a totally ordered set is well ordered if and only if it has no infinite descending chains.
Let S be a totally ordered set. If S contains an infinite (strictly) descending chain, say

$$s_0 > s_1 > \cdots > s_i > s_{i+1} > \cdots$$

then $\{s_0, s_1, s_2, \ldots\}$ has no minimal element, and so S is not well-ordered. Conversely, suppose that S has no infinite descending chain. Let T be a subset of S with no minimal element, so that for all $t \in T$ there exists $u \in T$ such that $t > u$ (recall that S is totally ordered). But then we can form an infinite descending chain $t_0 > t_1 > t_2 > \cdots$ where for all i we have $t_i \in T$ and $t_{i+1} \in T$ is chosen to be strictly less than t_i. This contradiction establishes the result.

6. Any exercises that may be embedded in my lecture notes.
Exercise for the reader. This also applies to (most) future exercises I may set in this way.