Computer Algebra Exam (2001-2002): Sample Answers

1. (a) Bookwork.
   [2 marks for each part.] *[4 marks]*

   (b) Bookwork.
   [2 marks for each part.] *[6 marks]*

   (c) i. Just replace $x$ with $x$::name in the header. *[2 marks]*

   ii. If $p$ divides $g$ in $\mathbb{Q}[x]$ then $g = hp$ for some $h \in \mathbb{Q}[x]$ and so $g(a) = h(a)p(a) = 0$. Conversely if $g(a) = 0$ then $g$ has a non constant common factor with $p$ in $\mathbb{Q}[x]$. However $p$ is irreducible and so the only non-constant polynomial that divides it is $p$ (or any non-zero multiple). It follows that the common factor is $p$ and so $p$ divides $g$.
   [2 marks for the first part and 3 for the rest.] *[5 marks]*

   iii. The test is just $\texttt{gcdex}(g, p, x, u, v) \neq 1$ (assuming, as is the case for Maple, that leading coefficients are normalized to 1). This is justified by the preceding part.
   [1 mark for the test, 2 marks for the justification.] *[3 marks]*

   iv. The procedure `adiv` computes a canonical form for $f(a)/g(a)$. We prove this by showing that if $r_1$, $r_2$ are polynomials which are either 0 or of degree strictly less than that of $p$ then $r_1(a) = r_2(a)$ if and only if $r_1 = r_2$. The equality happens if and only if $(r_1 - r_2)(a) = 0$ and from part (i) this happens if and only if $p$ divides $r_1 - r_2$. If $r_1 \neq r_2$ we have contradiction since then $r_1 - r_2 \neq 0$ and has degree strictly smaller than that of $p$.
   [1 mark for saying that it computes a canonical form, 4 marks for the rest.] *[5 marks]*

2. (a) Essentially bookwork (in the course the result was proved for polynomials with coefficients from a field). The degree part was not covered in the course but it follows immediately by comparing degrees of the two sides and bearing in mind the either $R = 0$ or $\deg(R) < m$.

[6 marks for the proof, 2 marks for the degree part.] *[8 marks ]*

(b) We have $A = QB + R$ and hence

$$x^n A(1/x) = (x^{n-m} Q(1/x))(x^m B(1/x) + x^{n-m+1}(x^{m-1} R(1/x)),$$

i.e.,

$$\mathrm{rev}_n(A) = \mathrm{rev}_{n-m}(Q)\,\mathrm{rev}_m(B) + x^{n-m+1}\,\mathrm{rev}_{m-1}(R).$$

It follows that

$$\mathrm{rev}_n(A) \equiv \mathrm{rev}_{n-m}(Q)\,\mathrm{rev}_m(B) \pmod{x^{n-m+1}}$$

as required.

Now if $C$ is as given then we have

$$\begin{aligned} C\,\mathrm{rev}_n(A) &\equiv \mathrm{rev}_{n-m}(Q) C\,\mathrm{rev}_m(B) \pmod{x^{n-m+1}} \\ &\equiv \mathrm{rev}_{n-m}(Q) \pmod{x^{n-m+1}} \end{aligned}$$

as required.

[4 marks for the first bit, 3 marks for the rest.] *[7 marks ]*

(c) The complete algorithm (with the answers underlined) is:

$f := \underline{\mathrm{rev}_m(B)};$
$g := 1;$
**for** $i$ **from** 1 **to** $\lceil \lg(n-m+1) \rceil$ **do**
  $g := \underline{\texttt{rem}((2 - fg)g, x^{2^i})};$
**od;**
$Q := \mathrm{rev}_{n-m}(\texttt{rem}(g\,\mathrm{rev}_n(A), x^{n-m+1});$
**if** $\underline{A = QB}$ **then** TRUE **else** FALSE **fi;**

For $A = 2x^3 - x^2 + 2x - 1$ and $B = x^2 + 1$ we have $n = 3$, $m = 2$ and $\lceil \lg(n-m+1) \rceil = 1$. The trace of the algorithm is:

- $f := 1 + x^2;$
- $g := 1;$
- $g := \texttt{rem}(1 - x^2, x^2) = 1;$
- $Q := \mathrm{rev}_1(\texttt{rem}(2 - x + 2x^2 - x^3, x^2)) = \mathrm{rev}_1(2 - x) = 2x - 1;$
- $QB = (2x - 1)(x^2 + 1) = 2x^3 - x^2 + 2x + 1 = A$ so TRUE is returned.

[6 marks for completing the algorithm, 4 for the example.] *[10 marks ]*

3. (a) Bookwork. *[3 marks]*

(b) Bookwork. *[3 marks]*

(c) Take $g_1 = x^2 + y$, $g_2 = x^2$ and $f = y$ and use any total degree order. Then $f$ cannot be reduced w.r.t. $G$ but clearly $f \in (G)$ since $f = g_1 - g_2$. *[3 marks]*

(d) (Essentially bookwork.) It is a simple property of reduction w.r.t. $G$ that if $f \to_G h$ then $f \in (G)$ if and only if $h \in (G)$ and of course the same applies for $\to_G^*$. The 'only if' part follows immediately since $0 \in (G)$ (this is how part (b) is proved) . Suppose now that $f \in (G)$ and yet it does not reduce to 0. It is a fact that every reduction sequence terminates after finitely many steps (consequence of Hilbert's Basis Theorem) and so we have that $f \to_G^* h$ where $h \neq 0$ and $h$ cannot be further reduced. But $h \in (G)$ since $f \in (G)$. Thus there is a $g \in G$ such that $\mathrm{lpp}(g) | \mathrm{lpp}(h)$. But this means that $h$ can be reduced by using $g$ which is a contradiction.

[2 marks for 'only if' part, 3 marks for the rest.] *[5 marks]*

(e) Let $f \in (s_1, s_2, \ldots, s_m)$ be a non-zero polynomial. By definition there are polynomials $f_1, f_2, \ldots, f_m$ such that $f = \sum_{i=1}^m f_i s_i$. Thus every power product of $f$ is a multiple of some $s_i$, in particular this is so of $\mathrm{lpp}(f)$. Thus the condition given in part (d) of the question is satisfied and $\{ s_1, s_2, \ldots, s_m \}$ is a Gröbner basis of the ideal $(s_1, s_2, \ldots, s_m)$ no matter what order we use.

Now $s \in (s_1, s_2, \ldots, s_m)$ if and only if $s$ reduces to zero w.r.t. the given basis and for this to happen we must have $s_i \mid s$ for some $i$. The converse is immediate. (Of course we don't need Gröbner bases to prove this part.)

[Gröbner basis part: 1 mark for making use of the condition in some sensible way, 2 marks for the rest. Rider: 2 marks.] *[5 marks]*

(f) (The assumption that $k$ is algebraically closed is not necessary but it makes the argument a little shorter and should suggest the use of the Nullstellensatz.) For a subset $T$ of $\{ 1, 2, \ldots, n \}$ the variety $K_T$ is the set of zeros of the power product $\prod_{i \in T} x_i$. Let $s, s_1, s_2, \ldots, s_m$ be the power products corresponding to the varieties $K_S, K_{S_1}, K_{S_2}, \ldots, K_{S_m}$. Now $K_{S_1} \cap K_{S_2} \cap \cdots \cap K_{S_m} \subseteq K_S$ if and only if $s$ vanishes whenever $s_1, s_2, \ldots, s_m$ do. By Hilbert's Nullstellensatz this is so if and only if $s^r \in (s_1, s_2, \ldots, s_m)$ for some integer $r > 0$. From the preceding part, this is equivalent to $s_i \mid s^r$ for some $i$ and, since each $s_i$ is square free, this is equivalent to $s_i \mid s$. This is equivalent to the requirement that $S_i \subseteq S$ for some $i$.

[2 marks for converting the question to an algebraic one, 1 mark for making use of the Nullstellensatz, 3 marks for the rest.] *[6 marks]*