Solutions to Homework 2

Problem 1. (16 points) Cox, Section 2.2, Problem 2:
Let F be a field and $n \geq 1$ an integer. Consider the ring $F[x_1, \ldots, x_n]$. The leading term (with respect to the graded lexicographic ordering $>$) of $f \in F[x_1, \ldots, x_n]$ will be denoted by $\text{LT}(f)$. For an *exponent vector* $\alpha = (a_1, \ldots, a_n)$ of nonnegative integers a_i, let x^α denote the monomial

$$x^\alpha = x_1^{a_1} \cdots x_n^{a_n}.$$

Through the rest of this problem, $\alpha, \beta, \gamma, \delta$ will denote arbitrary exponent vectors. Clearly $x^\alpha x^\beta = x^{\alpha+\beta}$, a fact which you may use without proof.

(a): If $x^\alpha > x^\beta$, prove that $x^{\alpha+\gamma} > x^{\beta+\gamma}$.

(b): If $x^\alpha > x^\beta$ and $x^\gamma > x^\delta$, prove that $x^{\alpha+\gamma} > x^{\beta+\delta}$.

(c): For any nonzero $f, g \in F[x_1, \ldots, x_n]$, prove that $\text{LT}(fg) = \text{LT}(f)\text{LT}(g)$

Proof. Write $\beta = (b_1, \ldots, b_n)$, $\gamma = (c_1, \ldots, c_n)$, and $\delta = (d_1, \ldots, d_n)$.
(a): If $a_1 + \cdots + a_n > b_1 + \cdots + b_n$, then $(a_1 + c_1) + \cdots + (a_n + c_n) > (b_1 + c_1) + \cdots + (b_n + c_n)$, and hence $x^{\alpha+\gamma} > x^{\beta+\gamma}$.
Otherwise, we have $a_1 + \cdots + a_n = b_1 + \cdots + b_n$, but $a_j > b_j$ for some minimal $j \geq 1$.
Then $(a_1 + c_1) + \cdots + (a_n + c_n) = (b_1 + c_1) + \cdots + (b_n + c_n)$, and for each $1 \leq i \leq j-1$, we have $a_i + c_j = b_i + c_i$.
We further have $a_j + c_j > b_j + c_j$. Therefore, $x^{\alpha+\gamma} > x^{\beta+\gamma}$. QED (a)

(b): We have $a_1 + \cdots + a_n \geq b_1 + \cdots + b_n$ and $c_1 + \cdots + c_n \geq d_1 + \cdots + d_n$. If either of these $\geq$'s is $>$, then $(a_1 + c_1) + \cdots + (a_n + c_n) > (b_1 + d_1) + \cdots + (b_n + d_n)$, and hence $x^{\alpha+\gamma} > x^{\beta+\delta}$.
Thus, we may assume for the rest of the proof that both of the $\geq$'s above are $=$.
Then $(a_1 + c_1) + \cdots + (a_n + c_n) = (b_1 + d_1) + \cdots + (b_n + d_n)$, and in addition, there is some minimal $j \geq 1$ such that $a_j > b_j$, and there is some minimal $k \geq 1$ such that $c_k > d_k$.
Without loss of generality, we may assume that $j \leq k$. Then for all $1 \leq i \leq j-1$, we have $a_i = b_i$ and $c_i = d_i$, so that $a_i + c_i = b_i + d_i$.
We further have $a_j + c_j > b_j + d_j$. Therefore, $x^{\alpha+\gamma} > x^{\beta+\delta}$. QED (b)

(c): Let $A_\alpha x^\alpha = \text{LT}(f)$ and $C_\gamma x^\gamma = \text{LT}(g)$, where α and γ are exponent vectors, and where $A_\alpha, C_\gamma \in F^\times$.
Then $f = \sum_{\beta \leq \alpha} A_\beta x^\beta$, where the sum is over all exponent vectors β with $\beta \leq \alpha$, and each A_β is an element of F. Similarly, $g = \sum_{\delta \leq \gamma} C_\delta x^\delta$.
Then $fg = \sum_{\beta \leq \alpha} \sum_{\delta \leq \gamma} A_\beta C_\delta x^{\beta+\delta}$.
One of the terms in this sum is $A_\alpha C_\gamma x^{\alpha+\gamma}$, which is nonzero since $A_\alpha, C_\gamma \neq 0$ and F is a field. It suffices to show that all of the other terms in the sum have exponent strictly smaller than $\alpha + \gamma$.
To see this, an arbitrary such term is of the form $A_\beta C_\delta x^{\beta+\delta}$ where either

- $\alpha = \beta$ and $\gamma > \delta$, or
- $\alpha > \beta$ and $\gamma = \delta$, or
- $\alpha > \beta$ and $\gamma > \delta$.

In the first case, then $x^{\alpha+\gamma} > x^{\alpha+\delta} = x^{\beta+\delta}$, by part (a).
In the second case, then $x^{\alpha+\gamma} > x^{\beta+\gamma} = x^{\beta+\delta}$, by part (a).

In the third case, then $x^{\alpha+\gamma} > x^{\beta+\delta}$, by part (b).
In all cases, then, our desired claim holds. QED (c)

Problem 2. (8 points) Cox, Section 2.2, Problem 7:
Let F be a field, and let $f \in F[x_1, \dots, x_n]$. For any permutation $\sigma \in S_n$, denote by $\sigma \cdot f$ the polynomial obtained from f by permuting the variables according to σ.
Prove that both $\prod_{\sigma \in S_n} \sigma \cdot f$ and $\sum_{\sigma \in S_n} \sigma \cdot f$ are symmetric polynomials.

Proof. Given $\tau \in S_n$, then $\{\tau\sigma \,|\, \sigma \in S_n\} = S_n$. Therefore

$$\tau \cdot \left(\prod_{\sigma \in S_n} \sigma \cdot f \right) = \prod_{\sigma \in S_n} \tau \cdot \big(\sigma \cdot f\big) = \prod_{\sigma \in S_n} (\tau\sigma) \cdot f = \prod_{\sigma \in S_n} \sigma \cdot f,$$

where the first equality is because permuting the variables before or after multiplying out the product has the same effect; the second is because permuting the variables by σ and then by τ is the same as permuting them by $\tau\sigma$; and the third is by the set equality above.

Similarly,

$$\tau \cdot \left(\sum_{\sigma \in S_n} \sigma \cdot f \right) = \sum_{\sigma \in S_n} \tau \cdot \big(\sigma \cdot f\big) = \sum_{\sigma \in S_n} (\tau\sigma) \cdot f = \sum_{\sigma \in S_n} \sigma \cdot f,$$

as desired. QED

Problem 3. (8 points) Cox, Section 2.2, Problem 10:
Apply the proof method of Theorem 2.2.2 to express

$$\textstyle\sum_3 x_1^2 x_2 = x_1^2 x_2 + x_1^2 x_3 + x_2^2 x_3 + x_1 x_2^2 + x_1 x_3^2 + x_2 x_3^2$$

in terms of σ_1, σ_2, σ_3.

Solution. All six terms of $f = \sum_3 x_1^2 x_2$ have total degree 3, so the largest one (with respect to glex order) is $x_1^2 x_2$. So we define $h_1 = \sigma_1^{2-1} \sigma_2^{1-0} \sigma_3^0 = \sigma_1 \sigma_2$.

We expand $h_1 = (x_1 + x_2 + x_3)(x_1 x_2 + x_1 x_3 + x_2 x_3)$
$\quad = x_1^2 x_2 + x_1^2 x_3 + x_1 x_2 x_3 + x_1 x_2^2 + x_1 x_2 x_3 + x_2^2 x_3 + x_1 x_2 x_3 + x_1 x_3^2 + x_2 x_3^2,$
and hence $f - h_1 = -3x_1 x_2 x_3 = -3\sigma_3$.
Thus, $f = h_1 - 3\sigma_3 = \boxed{\sigma_1 \sigma_2 - 3\sigma_3}$

Note: To really do it strictly by the algorithm, upon computing $f - h_1 = -3x_1 x_2 x_3$, we should define $h_2 = -3\sigma_1^{1-1} \sigma_2^{1-1} \sigma_3^1 = -3\sigma_3$, and then observe $f - h_1 - h_2 = -3x_1 x_2 x_3 - (-3\sigma_3) = 0$, so that $f = h_1 + h_2 = \sigma_1 \sigma_2 - 3\sigma_3$.

Problem 4. (12 points) Cox, Section 2.2, Problem 11a,b:
Let $\alpha, \beta, \gamma \in \mathbb{C}$ be the roots of $y^3 + 2y^2 - 3y + 5$. Find the monic polynomials of degree three with integer coefficients that have the following roots:

(a): $\alpha\beta$, $\alpha\gamma$, $\beta\gamma$

(b): $\alpha + 1$, $\beta + 1$, $\gamma + 1$

Solution. Call the original polynomial $f(y)$. So reading off the coefficients, we have
$\alpha + \beta + \gamma = \sigma_1 = -2$, and $\alpha\beta + \alpha\gamma + \beta\gamma = \sigma_2 = -3$, and $\alpha\beta\gamma = \sigma_3 = -5$.

(a): Define $g(x) = (x - \alpha\beta)(x - \alpha\gamma)(x - \beta\gamma)$, so

$$\begin{aligned} g(x) &= x^3 - (\alpha\beta + \alpha\gamma + \beta\gamma)x^2 + (\alpha^2\beta\gamma + \alpha\beta^2\gamma + \alpha\beta\gamma^2)x - \alpha^2\beta^2\gamma^2 \\ &= x^3 - \sigma_2 x^2 + \sigma_1\sigma_3 x - \sigma_3^2 = x^3 + 3x^2 + 10x - 25. \end{aligned}$$

(b): Define $h(x) = (x - (\alpha + 1))(x - (\beta + 1))(x - (\gamma + 1))$, so

$$h(x) = f(x-1) = (x-1)^3 + 2(x-1)^2 - 3(x-1) + 5 = x^3 - x^2 - 4x + 9.$$

Problem 5. (10 points) Cox, Section 2.2, Problem 11c:
Let $\alpha, \beta, \gamma \in \mathbb{C}$ be the roots of $y^3 + 2y^2 - 3y + 5$. Find the monic polynomial of degree three with integer coefficients that has roots α^2, β^2, γ^2.

Solution. Define $k(x) = (x - \alpha^2)(x - \beta^2)(x - \gamma^2)$, so

$$k(x) = x^3 - (\alpha^2 + \beta^2 + \gamma^2)x^2 + (\alpha^2\beta^2 + \beta^2\gamma^2 + \alpha^2\gamma^2)x - \alpha^2\beta^2\gamma^2.$$

We compute

$$\alpha^2 + \beta^2 + \gamma^2 = (\alpha + \beta + \gamma)^2 - 2(\alpha\beta + \alpha\gamma + \beta\gamma) = \sigma_1^2 - 2\sigma_2 = (-2)^2 - 2(-3) = 10,$$

and

$$\begin{aligned} \alpha^2\beta^2 + \beta^2\gamma^2 + \alpha^2\gamma^2 &= (\alpha\beta + \alpha\gamma + \beta\gamma)^2 - 2(\alpha^2\beta\gamma + \alpha\beta^2\gamma + \alpha\beta\gamma^2) \\ &= \sigma_2^2 - 2\sigma_1\sigma_3 = (-3)^2 - 2(-2)(-5) = -11, \end{aligned}$$

and $\alpha^2\beta^2\gamma^2 = \sigma_3^2 = 25$. Thus, $k(x) = x^3 - 10x^2 - 11x - 25$.