SOLUTION TO PROBLEM 3B) ON HW 7

NATE BOTTMAN

Let $p_k(x_1, \ldots, x_n) = x_1^k + \ldots + x_n^k$. By the theorem on this worksheet, p_k can be expressed in terms of elementary symmetric polynomials. Explicit formulas can be obtained recursively from the **Newton Identities**:

$$ks_k = \sum_{i=1}^{k} (-1)^{i-1} s_{k-i} p_i$$

Problem 3(b). Let R be a field of characteristic 0. Show that $\{p_1, \ldots, p_n\}$ are algebraically independent generators of the ring of symmetric polynomials $R[x_1, \ldots, x_n]^{S_n}$.

Proof. First, I claim that $p_1, \ldots, p_n$ generate the ring of symmetric polynomials. Since the elementary symmetric polynomials generate the symmetric polynomials, it would suffice to show that the power sums generate the elementary symmetric polynomials. We prove this in a lemma.

Lemma 1.1. *Fix $n \geq 0$. For all $k \in [0, n]$, s_k can be expressed as a polynomial F_k in $p_1, \ldots, p_k$.*

Proof of lemma. The $k = 0$ case follows immediately, since $s_0 = 1$. Assume now that the result holds up to, but not including, some $k \in [0, n-1]$. By the Newton identity,

$$s_k = k^{-1} \sum_{i=1}^{k} (-1)^{i-1} s_{k-i} p_i = \sum_{i=1}^{k} (-1)^{i-1} k^{-1} F_{k-i} (p_1, \ldots, p_{k-i}) \, p_i.$$

This is a polynomial in the power sums $p_1, \ldots, p_k$. □

It remains to show that the power sums $p_1, \ldots, p_n$ are algebraically independent. I relegate this result, as well, to a lemma.

Lemma 1.2. *For $n \geq 0$ and $k \in [0, n]$, the power sums $p_1 (x_1, \ldots, x_n), \ldots, p_k (x_1, \ldots, x_n)$ are algebraically independent.*

Proof. Fix $n \geq 0$. For $k = 0$, the result is trivial, since a nontrivial element of R, without adjoining anything, is simply a nontrivial element of the ring. Next, assume that the result has been proven up to, but not including, some $k \in [1, n]$. Consider a nontrivial element F of $R[X_1, \ldots, X_k]$, which can be written as

$$F(X_1, \ldots, X_k) = f_0 (X_1, \ldots, X_{k-1}) + f_1 (X_1, \ldots, X_{k-1}) \, X_k + \cdots + f_m (X_1, \ldots, X_{k-1}) \, X_k^m.$$

There must be some nonzero f_l, since if every f_l is zero, F must be zero, a contradiction. Without loss of generality, assume that f_m is nonzero; if not, simply drop a sufficient number of identically-zero higher terms. By the inductive hypothesis, $f_m (p_1, \ldots, p_{k-1})$ must also be nonzero.

Now, a sublemma.

Sublemma 1.3. *For $n \geq 1$ and $k \in [1, n]$, p_k can be expressed as a polynomial in $s_1, \ldots, s_k$, and the coefficient of s_k in this representation is $(-1)^{k-1} k$.*

Date: Wednesday, Nov. 17.

Proof of sublemma. Fix $n \geq 1$. For $k = 1$, the result is immediate, since $p_1 = s_1$. Next, assume that the result holds up to, but not including, some $k \in [1, n]$. By the Newton identity,

$$p_k = (-1)^{k-1} k s_k - \sum_{i=1}^{k-1} (-1)^{i-1} s_{k-i} p_i,$$

so the claim follows for this particular k from the inductive hypothesis. By induction, the lemma is proven. $\square$

By this lemma, () yields

$$F(h_1(X_1), \ldots, h_k(X_1, \ldots, X_k)) = f_0(h_1(X_1), \ldots, h_{k-1}(X_1, \ldots, X_{k-1})) + \cdots +$$
$$+ f_m(h_1(X_1), \ldots, h_{k-1}(X_1, \ldots, X_{k-1})) \left(g(X_1, \ldots, X_{k-1}) + (-1)^{k-1} k X_k\right)^m.$$

Here we have denoted the polynomial expression for p_i in terms of the elementary symmetric polynomials by $h_i(s_1, \ldots, s_i)$; we have written h_k, somewhat more explicitly, as $g(s_1, \ldots, s_{k-1}) + (-1)^{k-1} k s_k$, where g is some polynomial. The right-hand side of this equation is a polynomial in $X_1, \ldots, X_k$. Furthermore, there is a nonzero monomial in this polynomial with an m-th power of X_k. To see this, first note that since we are working in a field of characteristic 0, the expression $\left(g(X_1, \ldots, X_{k-1}) + (-1)^{k-1} k X_k\right)^m$ contains the nonzero monomial $(-1)^{m(k-1)} k^m X_k^m$. Since $f_m(p_1, \ldots, p_{k-1})$ is not zero, $f_m(h_1(X_1), \ldots, h_{k-1}(X_1, \ldots, X_{k-1}))$ cannot be zero. It follows that the product

$$f_m(h_1(X_1), \ldots, h_{k-1}(X_1, \ldots, X_{k-1})) \left(g(X_1, \ldots, X_{k-1}) + (-1)^{k-1} k X_k\right)^m$$

contains a nonzero monomial with an m-th power of X_k. It is clear that the sum

$$f_0(h_1(X_1), \ldots, h_{k-1}(X_1, \ldots, X_{k-1})) + \cdots +$$
$$+ f_{m-1}(h_1(X_1), \ldots, h_{k-1}(X_1, \ldots, X_{k-1})) \left(g(X_1, \ldots, X_{k-1}) + (-1)^{k-1} k X_k\right)^{m-1}$$

cannot contain any m-th powers of X_k, so indeed, $F(h_1(X_1), \ldots, h_k(X_1, \ldots, X_k))$ contains a nonzero monomial with an m-th power of X_k. In particular, $F(h_1(X_1), \ldots, h_k(X_1, \ldots, X_k))$ is nonzero. By the algebraic independence of the elementary symmetric polynomials, it follows that $F(h_1(s_1), \ldots, h_k(s_1, \ldots, s_k))$ is nonzero; that is, $F(p_1, \ldots, p_k)$ is nonzero. This proves that $p_1, \ldots, p_k$ are algebraically independent. By the inductive hypothesis, we have now proven the lemma. $\square$

$\square$

2. Appendix (by Julia)

I shall sketch a somewhat different approach which uses the same idea. To prove that $p_1, \ldots, p_n$ are algebraically independent it is clearly enough to show that the monomials $\{p_n^{\alpha_n} \ldots p_1^{\alpha_1}\}_{\sum \alpha_i \leq N}$ are linearly independent over R for any N.

Introduce lexicographic order on monomials. Let $\underline{\alpha} = (\alpha_n, \ldots, \alpha_1), \underline{\beta} = (\beta_n, \ldots, \beta_1)$ be multiindeces. Then

$$\underline{\alpha} \geq \underline{\beta}$$

iff there exists $1 \leq i \leq n$ such that $\alpha_n \geq \beta_n, \ldots, \alpha_{i+1} \geq \beta_{i+1}$ and $\alpha_i > \beta_i$.

Lemma 2.1. *(A stronger version of Nate's Lemma 1.1).*

$$s_n^{\alpha_n} \ldots s_1^{\alpha_1} = \sum_{\underline{\alpha} \geq \underline{\beta}} c_{\underline{\beta}} p_n^{\beta_n} \ldots p_1^{\beta_1},$$

where $c_{\underline{\beta}} \in R$ and the coefficient by $s_n^{\alpha_n} \ldots s_1^{\alpha_1}$ is non-zero.

Proof. This is a direct consequence of Newton's identities. Note that it holds for s_k since

$$s_k = \frac{(-1)^{k-1}}{k} p_k + \text{ lower terms } .$$

Hence, the same is true for $s_k^{\alpha_k}$. Now take the product. □

Now let's do linear algebra. Consider a linear subspace in $k[x_1, \ldots, x_n]$ generated by all monomials on p_i of total degree $\leq N$. By the degree of $p_n^{\beta_n} \ldots p_1^{\beta_1}$ I mean $\sum i\beta_i$. Consider a linear transformation of this subspace onto the subspace generated by all monomials on s_i of total degree $\leq N$ GIVEN by the formulas in Lemma 2.1. If we order our monomials lexicographically from lowest to highest, then the statement of the lemma is equivalent to the following: the matrix of this linear transformation is lower triangular with non-zero elements on the diagonal. Hence, the transformation is invertible. Since the monomials on s_i are linearly independent by the algebraic independence of s_i, we conclude that the monomials on p_i are lineary independent.

Remark. We can also just count the dimension of the space generated by monomials on s_i of degree $\leq N$ (which is the same as the subspace generated by all monomials on x_i of total degree $\leq N$). Again, Newton identities imply that this subspace is generated by the monomials on p_i of degree $\leq N$. But we have the same number of them as for s_i. Hence they must be linearly independent.