WORKSHEET ON SYMMETRIC POLYNOMIALS

DUE TUESDAY, MARCH 2, 2021

1. Elementary symmetric polynomials

Definition 1.1. Let R be a ring (commutative, with unit). A polynomial $f \in R[x_1, \ldots, x_n]$ is symmetric if for any $\sigma \in S_n$, $f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = f(x_1, \ldots, x_n)$

Alternatively, define the action of S_n on $R[x_1, \ldots, x_n]$ via

$$\sigma \circ f(x_1, \ldots, x_n) = f(x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)}).$$

Symmetric polynomials are invariants of this action - they are polynomials for which the stabilizer is the entire group S_n.

Example 1.2. Let $n = 3$. Then $x_1^{17} + x_2^{17} + x_3^{17}$, $x_1x_2^{16} + x_2x_3^{16} + x_3x_1^{16}$ are symmetric whereas $x_1x_2^2x_3^3$ is not.

Consider the polynomial $\boxed{P(t) = (t - x_1)(t - x_2)\ldots(t - x_n)}$ in $R[x_1, \ldots, x_n][t]$. Let

$$P(t) = t^n - e_1(x_1, \ldots, x_n)t^{n-1} + e_2(x_1, \ldots, x_n)t^{n-2} - \ldots + (-1)^n e_n(x_1, \ldots, x_n)$$

Definition 1.3. Polynomials $e_i(x_1, \ldots, x_n)$, $1 \leq i \leq n$, are called the *elementary symmetric polynomials*.

Observe that $P(t)$ is clearly invariant under the action of S_n. Hence, the elementary symmetric polynomials are, in fact, symmetric. Of course, one can write them down explicitly:

$$\begin{aligned} e_1 &= x_1 + \ldots + x_n \\ e_2 &= x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n \\ &\ldots \\ e_{n-1} &= x_1x_2\cdots x_{n-1} + \ldots + x_2x_3\cdots x_n \\ e_n &= x_1 \ldots x_n \end{aligned}$$

Let $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$ and denote by $x^{\underline{\alpha}}$ the monomial $x_1^{\alpha_1} \ldots x_n^{\alpha_n}$. We'll say that $x^{\underline{\alpha}} > x^{\underline{\beta}}$ if $\underline{\alpha} > \underline{\beta}$ in lexicographical order (so $\underline{\alpha} < \underline{\beta} \iff$ leftmost non-zero entry of $\underline{\beta} - \underline{\alpha}$ is positive). If f is a polynomial in $R[x_1, \ldots, x_n]$ then the multidegree of f is the degree $\underline{\alpha}$ of the maximal monomial in f. The degree of a monomial $x^{\underline{\alpha}}$ is $\alpha_1 + \ldots + \alpha_n$. The degree of a polynomial f is the maximum among the degrees of its monomials.

Observe that any symmetric polynomial containing $x^{\underline{\alpha}}$ must contain $\sum_{\sigma \in S_n} x_1^{\sigma(\alpha_1)} \ldots x_n^{\sigma(\alpha_n)}$.

Definition 1.4. A polynomial f is called homogeneous if f is a sum of monomials of the same degree.

Note that elementary symmetric polynomials are homogeneous and determined by a multidegree $\underline{\alpha}$ which consists of only 0's and 1's.

Theorem 1.5. *(Problem 1). Let $p(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ be a symmetric polynomial. Then there exists a polynomial $F \in R[y_1, \ldots, y_n]$ such that $p(x_1, \ldots, x_n) = F(e_1, \ldots, e_n)$.*

In other words, any symmetric polynomial can be expressed in terms of elementary ones.

Example 1.6. $x_1^3 + x_2^3 + x_3^3 = e_1^3 - 3e_1e_2 + 3e_3$.

Proof. (Theorem 1.5): We proceed by double induction on number of variables n and the degree d of the monomials of p. Let us add one further piece to the result: defining the weight of a monomial $y^{\underline{\alpha}} = y_1^{\alpha_1} \cdots y_n^{\alpha_n}$ to be $\alpha_1 + 2\alpha_2 + \ldots + n\alpha_n$ and the weight of $F \in R[y_1, \ldots, y_n]$ to be the maximum of the weights over all monomials, we claim that the weight of F, $w(F)$, is $\leq d$.

The base cases, $n = 1$, $d \in \mathbb{Z}_{\geq 0}$ and $d = 1$, $n \in \mathbb{N}$, are obvious since $n = 1 \implies e_1 = x \implies p(x) = p(e_1)$, and since $d = 1 \implies p = e_1$ (if $d = 0$ then p is literally just a constant). Now suppose that we have some $n, d \in \mathbb{N}$ and that we've proven the result for all symmetric polynomials of $< n$ variables and any degree, and those of n variables and degree $< d$.

We now decompose p (a symmetric polynomial in $R[x_1, \ldots, x_n]$ with degree d) into $l + (x_1 \cdots x_n)q$, where l is the sum of all monomials of p where at least one variable is missing (i.e. we split the monomials of p into two types, the first being the monomials who are missing at least one variable, and the second being the monomials who are a multiple of $x_1 \cdots x_n$; we then let l be the sum of the monomials of the first type, and q being the sum of the monomials of the second type after factoring out $x_1 \cdots x_n$). BTW, "l" stands for "lacunary", which means "having gaps or missing portions".

But note that because p is symmetric, l is completely determined by what the monomials involving variables $x_1, \ldots, x_{n-1}$ are in p (since any monomial of l involves $\leq n-1$ variables, there is some $\sigma \in S_n$ that permutes the variables so that that monomial invovles the variables $x_1, \ldots, x_{n-1}$; conversely for any monomial involving the variables $x_1, \ldots, x_{n-1}$, every $\sigma \in S_n$ sends it to some monomial involving $\leq n-1$ variables, i.e. some monomial of l). But the monomials of p involving the variables $x_1, \ldots, x_{n-1}$ are exactly the ones of $p(x_1, \ldots, x_{n-1}, 0)$! Thinking of this as a polynomial of $n-1$ variables, we see that it is symmetric (w.r.t. S_{n-1}), since S_{n-1} embeds in S_n by sending $n \mapsto n$, and we know p is symmetric w.r.t./invariant under any $\sigma \in S_n$.

Thus, by the induction hypothesis, $p(x_1, \ldots, x_{n-1}, 0)$ is equal to some $r(e_1^{n-1}, \ldots, e_{n-1}^{n-1})$, where $r \in R[y_1, \ldots, y_{n-1}]$ with weight $\leq \deg(p(x_1, \ldots, x_{n-1}, 0)) = d$ and e_i^{n-1} is the ith elementary symmetric polynomial in $n-1$ variables. Now let us consider the polynomial $t(x_1, \ldots, x_n) := r(e_1^n, \ldots, e_{n-1}^n)$. Note that t is symmetric (it is a function of $e_1^n, \ldots, e_n^n$), and has degree equal to max over all monomials $y^{\underline{\alpha}}$ in r of $\alpha_1 + 2\alpha_2 + \ldots + (n-1)\alpha_{n-1}$, which is exactly weight$(r) \leq d$. Plugging in $x_n = 0$, we get back exactly $r(e_1^{n-1}, \ldots, e_{n-1}^{n-1}) = p(x_1, \ldots, x_{n-1}, 0)$. That is to say, the monomials of t involving the variables $x_1, \ldots, x_{n-1}$ are exactly the same as those of p. But since the lacunary part is completely determined by the monomials involving the variables $x_1, \ldots, x_{n-1}$, the lacunary parts of t and p are the same, implying that t and p differ by some multiple of $x_1 \cdots x_n = e_n^n$, say $e_n^n q$ (not necessarily the same q as above; I'm reusing the letter now since I never referred to that q).

We're in the final stretch: note that q (a polynomial in n variables) is symmetric (since for any $\sigma \in S_n$, $x_1 \cdots x_n \sigma(q) = \sigma(x_1 \cdots x_n q) = \sigma(p - t) = \sigma(p) - \sigma(t) = p - t = x_1 \cdots x_n q$) and has degree $\leq d - n$ (since t, p both are degree $\leq d$, and $x_1 \cdots x_n$ has degree n), we have by the induction hypothesis (see paragraph 2) that $q = s(e_1^n, \ldots, e_n^n)$ for some $s \in R[y_1, \ldots, y_n]$ of weight $\leq d - n$. Thus, we have that $p = (p - t) + t = r(e_1^n, \ldots, e_{n-1}^n) + e_n^n s(e_1^n, \ldots, e_n^n)$, i.e. $p(x_1, \ldots, x_n) = F(e_1^n, \ldots, e_n^n)$ for $F \in R[y_1, \ldots, y_n]$ defined as $F(y_1, \ldots, y_n) = r(y_1, \ldots, y_{n-1}) + y_n s(y_1, \ldots, y_n)$, where F has weight $\leq d$ because r has weight $\leq d$, and the weight of s is $\leq d - n$ meaning after multiplication by y_n the weight of $y_n s$ is $\leq d$. □

Definition 1.7. We say that $f_1, \ldots, f_m \in R[x_1, \ldots, x_n]$ are algebraically independent if there does not exist $0 \neq F \in R[x_1, \ldots, x_m]$ such that $F(f_1, \ldots, f_m) = 0$.

Theorem 1.8. *(Problem 2). Prove that elementary symmetric polynomials on n variables are algebraically independent.*

Proof. We again proceed by induction. For the base case $n = 1$, we see that $e_1^1 = x_1$ is indeed algebraically independent. We now fix $n \in \mathbb{N}$, and suppose we have proved that $\{e_1^m, \ldots, e_m^m\}$ is algebraically independent for all $m < n$.

Suppose on the contrary that $\{e_1^n, \ldots, e_n^n\}$ is not algebraically independent. Then, there is some non-zero $F \in R[y_1, \ldots, y_n]$ s.t. $F(e_1^n, \ldots, e_n^n) = 0$ — we furthermore request that F be the minimal degree such polynomial. Let us now group the terms of F by the exponent of y_n; i.e. $F(y_1, \ldots, y_n) = F_0(y_1, \ldots, y_{n-1}) + F_1(y_1, \ldots, y_{n-1})y_n^1 + \ldots + F_d(y_1, \ldots, y_{n-1})y_n^d$, where d is just some natural number, and the F_i are in $R[y_1, \ldots, y_{n-1}]$. Pluggin in $\{e_1^n, \ldots, e_n^n\}$, we see that $0 = F_0(e_1^n, \ldots, e_{n-1}^n) + \ldots + F_d(e_1^n, \ldots, e_{n-1}^n)(x_1 \cdots x_n)^d$. Since this is true for all particular $x_i \in R$, setting $x_n = 0$ gives us that $0 = F_0(e_1^{n-1}, \ldots, e_{n-1}^{n-1})$.

If F_0 is not identically 0, then we get that $\{e_1^{n-1}, \ldots, e_{n-1}^{n-1}\}$ is not algebraically independent, contradicting the induction hypothesis. If F_0 is identically 0, then we would be able to write $F = y_n F'$ for some $F' \in R[y_1, \ldots, y_n]$ of strictly lesser degree than F; but because $F(e_1^n, \ldots, e_n^n)$ (as a polynomial in $x_1, \ldots, x_n$) is identically 0, $F'(e_1^n, \ldots, e_n^n)$ must also be (since if it were not, multiplying by $y_n = x_1 \cdots x_n$ would not get to identically 0), contradicting that F is the/a minimal degree polynomial satisfying $F(e_1^n, \ldots, e_n^n) = 0$. Thus either way, our supposition results in a contradiction, so indeed $\{e_1^n, \ldots, e_n^n\}$ must be algebraically independent □

The combination of these two results is sometimes referred to as the "fundamental theorem of symmetric polynomials":

Theorem 1.9. *The ring of invariants of the polynomial ring on n variables under the action of the symmetric group is a polynomial ring on the elementary symmetric polynomials:*

$$R[x_1, \ldots, x_n]^{S_n} \simeq R[e_1, \ldots, e_n].$$

Hint: both statements can be proven by induction on n and then on the total degree of the polynomial. If you get stuck, check out Lang, IV.6. The proof in Lang is sketched on Wikipedia which also offers another, more elegant, alternative proof.

The ring $R[x_1, \ldots, x_n]^{S_n}$ is called the *ring of symmetric polynomials.*

2. Newton identities

This section is FYI although proving Newton identities is a very good exercise.

Let $p_k(x_1, \ldots, x_n) = x_1^k + \ldots + x_n^k$. Since p_k is symmetric, it can be expressed in terms of elementary symmetric polynomials. Explicit formulas can be obtained recursively via **Newton's Identities** (convention here is $e_0 = 1$):

$$ke_k = \sum_{i=1}^{k} (-1)^{i-1} e_{k-i} p_i$$

The following results are straightforward applications of the Newton identities.

Theorem 2.1. *Assume R is a field of characteristic 0. Then $\{p_1, \ldots, p_n\}$ are algebraically independent generators of the ring of symmetric polynomials $R[x_1, \ldots, x_n]^{S_n}$.*

Corollary 2.2. *Let $t_1, \ldots, t_n$ be all roots (counted with multiplicity and, possibly, complex) of a polynomial of degree n with real coefficients. Then $t_1^k + \ldots + t_n^k$ is a real number for any k.*

3. Application to Galois Theory

Problem 3 [Prelim 2009, 4] Let K be a field of characteristic zero and $f \in K[x]$ an irreducible polynomial of degree n. Let L be a splitting field for f. Let G be the group of automorphisms of L which act trivially on K.

(1) Show that G embeds in the symmetric group S_n.

Because K is characteristic 0 and f is irreducible over K, f is separable, so $\deg(f) = n \implies$ we have n distinct roots $\alpha_1, \ldots, \alpha_n$ in the splitting field L ($\alpha_i \notin K$, and moreover by definition of splitting field and adjoining elements $L = K(\alpha_1, \ldots, \alpha_n)$). By the properties of homomorphisms, any automorphism of L can only permute the roots $\alpha_1, \ldots, \alpha_n$, and because any automorphism of L is completely determined by its action on $\alpha_1, \ldots, \alpha_n$, every automorphism σ of L corresponds to a permutation of S_n; namely the one that sends $i \mapsto j$ if $\sigma(\alpha_i) = \alpha_j$. It is obvious that this correspondence is an injective homomorphism from $G \to S_n$, so indeed G embeds in S_n.

(2) For each n, give an example of a field K and polynomial f such that $G = S_n$.

Let us consider (for some field R of characteristic 0) $K := R(e_1^n, \ldots, e_n^n)$, i.e. the field of rational functions in $e_1^n, \ldots, e_n^n$ with coefficients in R, and $f := P(x) = (x - x_1)(x - x_2)\cdots(x - x_n) = x^n - e_1^n x^{n-1} + e_2^n t^{n-2} - \ldots + (-1)^n e_n^n \in K[x]$ (the P in the box from page 1, where $x_1, \ldots, x_n$ are just indeterminates). It is clear that K is characteristic 0. We now show that f is irreducible over K.

Looking at 505hw1 Theorem 5 (A UFD $\implies$ $A[x]$ UFD), we only used that x was algebraically independent of the elements of A in the proof, and so we can apply this in our situation to get that $R[e_1^n, \ldots, e_n^n]$ is a UFD. Then by Theorem 4 of 505hw1, f irreducible over $A := R[e_1^n, \ldots, e_n^n]$ implies f irreducible over $K = \mathrm{Frac}(A)$ (since f is non-constant). Finally, if we could factor f into say $g, h \in A[x]$ (a non-trivial factorization), then by matching powers of x, we get equations with e_i^n on the LHS and some polynomial expression on the RHS involving the elements of R and $e_1^n, \ldots, e_n^n$, contradicting again algebraic independence of the $e_1^n, \ldots, e_n^n$.

Thus, we have now irreducible f over K, with splitting field $L = K(x_1, \ldots, x_n)$ (since $x_1, \ldots, x_n$ are the roots of f). Note that L is also equal to $R(x_1, \ldots, x_n)$. The above part (1) tells us that $G := \mathrm{Aut}(L/K) \leq S_n$. But for any $\sigma \in S_n$ (thinking of S_n as the group permuting $x_1, \ldots, x_n$), we have that σ fixes $e_1^n, \ldots, e_n^n$ (since they are symmetric), so indeed σ fixes every element of K. Thus, $\sigma \in \mathrm{Aut}(L/K)$ (it is a isomorphism of L because for any element of L, say $\sum_{i \in I} p_i x^{\underline{\alpha_i}} / \sum_{j \in J} q_j x^{\underline{\beta_j}}$, σ acting on it yields $\sum_{i \in I} p_i \sigma(x^{\underline{\alpha_i}}) / \sum_{j \in J} q_j \sigma(x^{\underline{\beta_j}})$, and so with this it is easy to see injectivity and surjectivy as σ just permutes the indices of the x_i). This means that $S_n \leq G$, and so $G = S_n$ as desired.

(3) What are the possible groups G when $n = 3$. Justify your answer.

Like we noted in part (1), f has 3 distinct roots $\alpha_1, \alpha_2, \alpha_3 \in L \setminus K$, and $G := \mathrm{Aut}(L/K) \leq S_3$. Because L is the splitting field of a separable polynomial f, L/K is a Galois extension, so $|G| = [L : K] = [L : K(\alpha_1)][K(\alpha_1) : K]$. But $[K(\alpha_1) : K] = \deg(\mathrm{Irr}(\alpha_1, K)) = \deg(f) = 3$, so $|G|$ is a multiple of 3. So now we know either $|G| = 3$ or 6. The only order 3 group is $\mathbb{Z}/3\mathbb{Z}$, and the only order 6 group that is a subgroup of S_3 is S_3 itself, so those 2 are our only possibilities. Lastly, in the 505midterm, we saw cases where $\mathbb{Z}_3$ and S_3 were realized, so these are exactly the possible groups of G when $n = 3$.