## The fundamental theorem of alternating functions

## Matthieu Romagny

September 15th, 2005

Let A be a commutative ring with unit and  $n \ge 1$  be an integer. The symmetric group in n letters acts on the polynomial ring  $A[X_1, X_2, \ldots, X_n]$  by permutation of the variables. The most famous invariant polynomials are the elementary symmetric functions  $S_i$  determined by the expansion  $(T - X_1)(T - X_2) \ldots (T - X_n) = T^n - S_1 T^{n-1} + \cdots + (-1)^n S_n$ . The fundamental theorem of symmetric functions asserts that the invariant ring for this action is the subring  $A[S_1, S_2, \ldots, S_n]$ , and that the polynomials  $S_i$  are algebraically independent.

If one looks at the restricted action of the alternating group, there are more invariants. For example the Vandermonde polynomial  $V_n = \prod_{1 \le i < j \le n} (X_i - X_j)$  is multiplied by the signature  $\varepsilon(\sigma)$  under action of a permutation  $\sigma$ . When  $2 \in A^{\times}$ , it is known that the invariant ring is generated by the  $S_i$   $(1 \le i \le n)$  together with  $V_n$ . At the other extreme if 2 = 0 in A then  $V_n$  is symmetric, so the same result does not hold. In this note we provide the correct invariant ring for the action of the alternating group, for any A.

· · .

Keeping notations as above, consider the following four polynomials :

$$\Theta_n = \prod_{1 \le i < j \le n} (X_i + X_j) \quad ; \quad \Sigma_n = (V_n)^2 \quad ; \quad \Delta_n = \frac{1}{4} (\Sigma_n - \Theta_n^2) \quad ; \quad W_n = \frac{1}{2} (V_n + \Theta_n)$$

The first three are symmetric, while an odd permutation maps  $W_n$  to  $\Theta_n - W_n$ . Substituting  $2W_n - \Theta_n$  to  $V_n$  in the equation  $\Sigma_n = (V_n)^2$ , one finds the integrality equation  $(W_n)^2 - \Theta_n W_n - \Delta_n = 0$ . Finally, all four polynomials have coefficients in  $\mathbb{Z}$ : for  $W_n$  this is clear, and the above equation shows that this is true also for  $\Delta_n$ . As we now prove, for general A, the correct substitute for  $V_n$  is  $W_n$ :

**Theorem** Let  $n \ge 2$ . The ring of alternating polynomials in the variables  $X_1, \ldots, X_n$  is  $A[S_1, \ldots, S_n, W_n]$  with relation  $(W_n)^2 - \Theta_n W_n - \Delta_n = 0$ .

**Proof**: Let  $B = A[S_1, \ldots, S_n]$ , and denote by C the ring of alternating polynomials. We first prove that C is a free module over B with basis  $\{1, W_n\}$ . Let F be an alternating polynomial. It is clear that  $F^* = F - \tau F$  is independent of the choice of an odd permutation  $\tau$ . In particular for  $\sigma = (ij)$  this says that  $X_i - X_j$  divides  $F^*$ . In the sequel, we use repeatedly the fact that  $X_i - X_j$ is a nonzerodivisor in  $A[X_{i,j}]$ , for all (i, j). We will now prove that  $V_n$  divides  $F^*$ . We choose

Key words: Symmetric functions, alternating group, invariants

Mathematics Subject Classification: 05E05, 13A50, 14L30, 20B30

the lexicographic order on the pairs (i, j) with  $1 \le i < j \le n$ . Starting from  $F^* = (X_1 - X_2)Q_1$  we assume by induction on N that there exists  $Q_N$  such that

$$F^* = \left(\prod_{(i,j) \le N} (X_i - X_j)\right) Q_N$$

Let (u, v) be the N + 1-th pair. Then  $Q_N$  vanishes when we specialize to  $X_u = X_v$ , because  $X_u - X_v$  divides  $F^*$ . Hence  $X_u - X_v$  divides  $Q_N$ , by a direct computation. After n(n-1)/2 steps we have  $F^* = V_n Q$ . Clearly, Q is uniquely defined and invariant under the full symmetric group. Now we check that the polynomial  $P = F - W_n Q$  is also symmetric. If  $\sigma$  is odd we have  $F - \sigma F = F^* = V_n Q$  and  $\sigma W_n = \Theta_n - W_n = W_n - V_n$ . Hence,

$$\sigma P = \sigma F - \sigma W_n \cdot \sigma Q = \sigma F - (W_n - V_n)Q = F - W_n Q = P$$

This proves that 1 and  $W_n$  generate C as a B-module. Furthermore, if  $P = W_n Q$  with  $(P, Q) \in B^2$ , then after we apply an odd permutation we get  $P = (\Theta_n - W_n)Q = (W_n - V_n)Q$ . From this and  $P = W_n Q$  it follows that  $V_n Q = 0$  hence Q = 0. This shows that C is a free B-module. Therefore, the map  $B[T]/(T^2 - \Theta_n T - \Delta_n) \to C$  defined by  $T \mapsto W_n$  is a surjective map between free modules of the same rank, so it is an isomorphism.

Institut de Mathématiques Analyse Algébrique Université Pierre et Marie Curie Case 82 4, place Jussieu F-75252 Paris Cedex 05 romagny@math.jussieu.fr