# The fundamental theorem of alternating functions 

Matthieu Romagny

September 15th, 2005

Let $A$ be a commutative ring with unit and $n \geq 1$ be an integer. The symmetric group in $n$ letters acts on the polynomial ring $A\left[X_{1}, X_{2}, \ldots, X_{n}\right]$ by permutation of the variables. The most famous invariant polynomials are the elementary symmetric functions $S_{i}$ determined by the expansion $\left(T-X_{1}\right)\left(T-X_{2}\right) \ldots\left(T-X_{n}\right)=T^{n}-S_{1} T^{n-1}+\cdots+(-1)^{n} S_{n}$. The fundamental theorem of symmetric functions asserts that the invariant ring for this action is the subring $A\left[S_{1}, S_{2}, \ldots, S_{n}\right]$, 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 $V_{n}=\prod_{1 \leq i<j \leq n}\left(X_{i}-X_{j}\right)$ 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 $S_{i}(1 \leq i \leq n)$ 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 :

$$
\Theta_{n}=\prod_{1 \leq i<j \leq n}\left(X_{i}+X_{j}\right) \quad ; \quad \Sigma_{n}=\left(V_{n}\right)^{2} \quad ; \quad \Delta_{n}=\frac{1}{4}\left(\Sigma_{n}-\Theta_{n}^{2}\right) \quad ; \quad W_{n}=\frac{1}{2}\left(V_{n}+\Theta_{n}\right)
$$

The first three are symmetric, while an odd permutation maps $W_{n}$ to $\Theta_{n}-W_{n}$. Substituting $2 W_{n}-\Theta_{n}$ to $V_{n}$ in the equation $\Sigma_{n}=\left(V_{n}\right)^{2}$, one finds the integrality equation $\left(W_{n}\right)^{2}-\Theta_{n} W_{n}-$ $\Delta_{n}=0$. 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 $n \geq 2$. The ring of alternating polynomials in the variables $X_{1}, \ldots, X_{n}$ is $A\left[S_{1}, \ldots, S_{n}, W_{n}\right]$ with relation $\left(W_{n}\right)^{2}-\Theta_{n} W_{n}-\Delta_{n}=0$.

Proof : Let $B=A\left[S_{1}, \ldots, S_{n}\right]$, and denote by $C$ the ring of alternating polynomials. We first prove that $C$ is a free module over $B$ with basis $\left\{1, W_{n}\right\}$. 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 $\sigma=(i j)$ 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 $A\left[X_{i, j}\right]$, for all $(i, j)$. We will now prove that $V_{n}$ divides $F^{*}$. We choose
the lexicographic order on the pairs $(i, j)$ with $1 \leq i<j \leq n$. Starting from $F^{*}=\left(X_{1}-X_{2}\right) Q_{1}$ we assume by induction on $N$ that there exists $Q_{N}$ such that

$$
F^{*}=\left(\prod_{(i, j) \leq N}\left(X_{i}-X_{j}\right)\right) Q_{N}
$$

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,

$$
\sigma P=\sigma F-\sigma W_{n} \cdot \sigma Q=\sigma F-\left(W_{n}-V_{n}\right) Q=F-W_{n} Q=P
$$

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 $P=\left(\Theta_{n}-W_{n}\right) Q=\left(W_{n}-V_{n}\right) Q$. 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 $B[T] /\left(T^{2}-\Theta_{n} T-\Delta_{n}\right) \rightarrow C$ defined by $T \mapsto W_{n}$ is a surjective map between free modules of the same rank, so it is an isomorphism.

[^0]
[^0]:    Institut de Mathématiques
    Analyse Algébrique
    Université Pierre et Marie Curie
    Case 82
    4, place Jussieu
    F-75252 Paris Cedex 05
    romagny@math.jussieu.fr

