WORKSHEET ON SYMMETRIC POLYNOMIALS AND GAUSS LEMMA

DUE WEDNESDAY, NOVEMBER 28, 2018

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

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

The symmetric polynomials are invariants of this action - the 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:
$e_1 = x_1 + \ldots + x_n$
$e_2 = x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n$
$\ldots$
$e_n = x_1 \ldots x_n$

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. 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 $\sum\limits_{\sigma \in S_n} x_1^{\sigma(\alpha_1)} \ldots x_n^{\sigma(\alpha_n)}$.

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

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

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

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

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

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

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, VI.6. The proof in Lang is sketched on Wikipedia which also offers another, more elegant, alternative proof.
$R[x_1, \dots, x_n]^{S_n}$ is called the ring of symmetric polynomials.

2. Newton identities

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

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

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

(The convention here is $e_0 = 1$).

The following results are straightforward applications of the Newton identities.

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

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

3. Gauss Lemma

For this part let A be a unique factorization domain, and $K = \mathrm{Frac}(A)$ be its field of fractions. For any $s \in K$, we can write

$$s = p^r t$$

where p is an irreducible element in A, r is an integer, and $t \cong a/b \in K$ such that p does not divide a or b. Then the integer r is uniquely determined and is called the order of s at p:

$$r = \mathrm{ord}_p s.$$

For $f = a_nX^n + a_{n-1}X^{n-1} + \dots + a_0 \in K[X]$, we define *the order* of f at p to be ∞ if $f = 0$ and $\min_{0 \leq i \leq n} \mathrm{ord}_p a_i$ otherwise. Finally, we the define the *content* of f as follows:

$$\mathit{cont}(f) = \prod_{\mathrm{ord}_p f \neq 0} p^{\mathrm{ord}_p f}$$

OR any multiple of this product by an invertible element in A.
Caution: Content is defined UP TO a scalar multiplication by a unit element.

Definition 3.1. A polynomial $f(X) \in A[X]$ is primitive if $cont(f) = 1$.

Theorem 3.2. *(= Problem 3 a,b).*

1. *Let $f, g \in K[X]$. Then $cont(fg) = cont(f)cont(g)$*
2. *Let $f, g \in A[X]$. If f, g are both primitive, then fg is primitive.*

Corollary 3.3. *(= Problem 3 c) If a non constant polynomial with coefficients in A is irreducible over A, then it is irreducible over K.*

Remark 3.4. Any of the three statement above go under the name of "Gauss lemma", originally formulated for $A = \mathbb{Z}$. It says that if you could factor a non-constant polynomial with integer coefficients over the rationals (in a non-trivial way), then you could factor it over the integers.

Theorem 3.5. *(= Problem 4) Let A be a UFD. Then the polynomial ring $A[X_1, \ldots, X_n]$ is a UFD.*