September 5:

Math 432 Class Lecture Notes

- The Frobenius automorphism
- Roots of polynomials in a field
- Symmetric polynomials

0.1 Frobenius

An automorphism of a field F is a bijection that is a homomorphism for addition and multiplication.

In characteristic p, there is a canonical homomorphism of fundamental importance, useful both in a couple of the homework problems, and later on in this course.

Definition 1. If F has characteristic p, then the Frobenius map, sometimes written ϕ_p, is defined by

$$\phi_p(x) = x^p.$$

Theorem 2. ϕ_p is an automorphism.

Proof. The Frobenius map is obviously a homomorphism for multiplication. From the fact that the interior binomial coefficients are divisible by p, and hence zero since $p = 0$ in F, we see that ϕ_p is a homomorphism for addition:

$$\phi_p(x+y) = (x+y)^0 = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} = x^p + y^p = \phi_p(x) + \phi_p(y).$$

□

If F is a finite field with $q = p^n$ elements then any nonzero element x is an element of the multiplicative group F^* of order $q - 1$ and therefore satisfies $x^{q-1} = 1$. This means that any element of F satisfies

$$\phi_p^n(x) = x^{p^n} = x^q = x$$

and it follows that the Frobenius automorphism has order dividing n. Later we will see that it has order exactly equal to n, and that the only automorphisms of F are powers of ϕ_p.

0.2 Roots of a polynomial in a field

In the homework, and a later points in the course, we need to know that the number of roots of a polynomial in a field is at most the degree of the polynomial.

Theorem 3. If F is a field, f is an element of $F[x]$, and $\deg(f) = n$ then f has at most n roots in F.

The proof follows from the fact that $f(a) = 0$ is equivalent to $x - a$ dividing f, which in turn follows from the division algorithm for polynomials with coefficients in a field.

None of these results need hold over a ring. For instance, $x^2 - 1 \in \mathbf{Z}/8\mathbf{Z}[x]$ has 4 roots, and $x^3 - x \in \mathbf{Z}/6\mathbf{Z}[x]$ has 6 roots.

0.3 Symmetric polynomials

Let $x_1, \cdots, x_n$ be indeterminates (in specific situations these variables can be specialized to any needed values, e.g., to the roots of a polynomial of degree n).

The **elementary symmetric functions** of the x_i are defined by the equation

$$\prod_{i=1}^{n}(t + x_i) = \sum_{k=0}^{n} e_k t^{n-k} \quad .$$

Thus e_k is the product of all products of k distinct x_i, and $e_0 = 1$. For $n = 4$ the elementary symmetric functions are

$$\begin{aligned}
e_1 &= x_1 + x_2 + x_3 + x_4 \\
e_2 &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_3 + x_3x_4 \\
e_3 &= x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 \\
e_4 &= x_1x_2x_2x_4
\end{aligned}$$

Sometimes the defining equation is written

$$\prod_{i=1}^{n} t - x_i = \sum_{k=0}^{n} (-1)^k e_k t^{n-k}$$

to emphasize its applicability to roots of polynomials.

A polynomial in the x_i is said to be **symmetric** if it is unchanged when the variables are permuted. The elementary symmetric functions e_k are symmetric, as are the **power sums**

$$p_k := \sum_{i=1}^{n} x_i^k .$$

Theorem 4. Any symmetric polynomial is uniquely a polynomial in the e_k, $1 \leq k \leq n$.

Proof. A polynomial is a linear combination of **monomials**

$$x_1^{a_1} \cdots x_n^{a_n} .$$

The **degree** of a monomial is the sum $\sum a_i$ of the exponents.

Define a total order on monomials by saying that $m > m'$ if the degree of m is greater than the degree of m', and that, if the degrees are equal, then $m > m'$ if the first exponent where m and m' disagree has $a_i > a_i'$. More precisely,

$$x_1^{a_1} \cdots x_n^{a_n} > x_1^{a_1'} \cdots x_n^{a_n'}$$

if $\sum a_i > \sum a_i'$, or if $\sum a_i = \sum a_i'$ and there is a j such that $a_i = a_i'$ for $i < j$, and $a_j > a_j'$.

If $f \in F[x_1, \cdots, x_n]$ is a polynomial in the n variables x_i then define $\mathrm{init}(f)$ to be the largest monomial (with respect to the above order) that occurs in f. For instance,

$$\mathrm{init}(e_k) = x_1 x_2 \cdots x_k .$$

Now assume that f is symmetric, that $\operatorname{init}(f)$ is $x_1^{a_1} \cdots x_n^{a_n}$, and that the corresponding term in f is $cx_1^{a_1} \cdots x_n^{a_n}$ for some nonzero constant c.

A moment's reflection shows that the leading term can be cancelled by a symmetric function, i.e., that the leading term of

$$f - ce_1^{a_1-a_2} e_2^{a_2-a_3} \cdots e_{n-1}^{a_{n-1}-a_{n-1}} e_n^{a_n}$$

is strictly smaller than the leading term $\operatorname{init}(f)$ of f. This new function is symmetric, and after finitely many repetitions of this step we end up with 0, i.e., we express f as a polynomial in the elementary symmetric functions. This finishes the proof of existence.

If there are two different expressions for f as a polynomial in the e_k then there is a polynomial relation

$$g(e_1, \cdots, e_n) = 0$$

satisfied by the elementary symmetric functions. If the initial term of $g(y_1, \cdots, y_n)$, as a polynomial in indeterminates y_i, is $\prod y_i^{a_i}$ then the initial term of $g(e_1, \cdots, e_n)$, as a polynomial in the x_i, is easily checked to be

$$\prod x_i^{b_i}$$

where

$$b_i := \sum_{j \geq i} a_j.$$

However, the mapping from the n-tuple of a's to the n-tuple of $b's$ is bijective. (There is an inverse map: $a_i = b_i - b_{i+1}$.) Thus if g is a nonzero polynomial then its leading term, as a polynomial in the x_i, is not cancelled by any other term, and we see that a polynomial relation is impossible.

This finishes the proof of the theorem.

□

An important special case of this (that arises in diverse contexts, including statistics and group representations) is the find explicit polynomials expressing the power sums in terms of the elementary symmetric functions (see the homework).