September 10:

Math 432 Class Lecture Notes

- Power sums and elementary symmetric functions
- Cyclicity of finite subgroups of F^*

0.1 Power sums and elementary symmetric functions

The elementary symmetric functions of n indeterminates are defined by

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

and the power sums are defined by

$$p_k := \sum_{i=0}^{n} x_i^k$$

where k is any nonnegative integer.

A homework question asked for a proof of the identity

$$\sum_{j=0}^{k-1}(-1)^j p_{k-j} e_j + \quad (-1)^k k e_k = 0.$$

One approach is to find a relationship between the generating functions of the e's and p's, since the only way that an identity of the above shape can hold is if there is such a relationship.

The generating function for the e's can be written

$$\sum_j (-1)^j e_j t^j = \prod_i (1 - t x_i).$$

The generating function for the p's can be found by summing a geometric series:

$$\sum p_k t^k = \sum_{i,k} x_i^k t^k = \sum_i \frac{x_i t}{1 - x_i t}.$$

With some work one finds a relationship between these generating functions (roughly, the second is the logarithmic derivative of the first) from which the identity follows.

Another approach is to first handle the case $k \geq n$. Substitute $t = x_i$ in the defining identities for the e's and multiply by x_i^{k-n} to get

$$\sum_{j=0}^{n} (-1)^j e_j x_i^{k-j} = 0.$$

Summing over i gives the desired identity (with a little careful thought as to how to reconciel the two statements).

If $k < n$ then the following curious argument works. Evaluate the LHS of the identity (i.e., the function presumed to be 0). In this symmetric function $g(x_1, \cdots, x_n)$ all monomials involve at most k different terms. If this symmetric function is nonzero, then some monomial involving at most the first k variables is nonzero, i.e.,

$$g(x_1, \cdots, x_k, 0, \cdots, 0) \neq 0.$$

However, this reduces to the case $n = k$ of the identity, which we already know to be true.

0.2 Cyclicity of finite subgroups of F^*

Theorem 1. If G is a finite subgroup of the multiplicative group F^* of a field then G is cyclic.

Corollary 2. If F is finite then F^* is cyclic, i.e., "primitive roots exist."

As we discovered in class, the proof is simplified by using the following result.

Lemma 3. If x and y are elements of an abelian group and have relatively prime orders, then the order of xy is the product of the orders of x and y.

Proof. Suppose x has order m, y has order n, and xy has order r. Since the group is abelian

$$(xy)^{mn} = x^{mn}y^{mn} = 1$$

so the order of r divides mn. Also

$$1 = (xy)^{ra} = y^{ra}$$

and the b divides ra. Since a and b are relatively prime, a divides r. Similarly, b divides r.

Therefore ab divides r and r divides ab so $r = ab$ as claimed. □

Remark 4. We have used two facts from elementary number theory: Suppose that u and v are relatively prime; then if u divides vw then u divides w; if both u and v divides w then uv divides w.

Now we prove the theorem. Let G be a finite subgroup of the multiplicative group F^* of a field F. Assume that the prime factorization of the order of G is

$$\#G := n = \prod_{p_i^{a_i}}.$$

For each i, the polynomial $x^{n/p_i} - 1$ can have at most n/p_i roots. Since G has n elements we can find an element u_i such that $u_i^{n/p_i} \neq 1$. The element $v_i := u_i^{n/p_i^{a_i}}$ has order $p_i^{a_i}$. Indeed, it's clear that v_i raised to the $p_i^{a_i}$ is equal to 1, so the order is a power of p_i. But

$$v_i^{p_i^{a_i-1}} = u_i^{n/p_i} \neq 1$$

so the order is exactly equal to $p_i^{a_i}$.

By successive applications of the Lemma we see that the product of the v_i has order $n = \prod p_i^{a_i}$, and the group is cyclic as claimed.