Section 33: Finite Fields

Def: A field is a *finite field* if it has finite order.

Thm. Let E be a finite extension of degree n over a finite field F. If F has q elements, then E has q^n elements.

Corollary: If E is a finite field of characteristic p, then E contains exactly p^n elements for some positive integer n.

Thm. Let E be a field of p^n elements contained in an algebraic closure $\bar{\mathbb{Z}}_p$ of $\mathbb{Z}_p$. The elements of E are precisely the zeros in $\bar{\mathbb{Z}}_p$ of the polynomial $x^{p^n} - x \in \mathbb{Z}_p[x]$.

Def: An element α of a field is an *nth root of unity* if $\alpha^n = 1$. It is a *primitive nth root of unity* if $\alpha^n = 1$ and $\alpha^m \neq 1$ for $0 < m < n$.

Note: The nonzero elements of a finite field with p^n elements are all $(p^n - 1)$th roots of unity.

Thm. The multiplicative group $\langle F^*, \cdot \rangle$ of nonzero elements of a finite field F is cyclic.

Corollary: A finite extension E of a finite field F is a simple extension of F.

Lemma: If F is a prime of characteristic p with algebraic closure $\bar{F}$, then $x^{p^n} - x$ has p^n distinct zeros in $\bar{F}$.

Freshman's Dream: If F is a field of prime characteristic p, then $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n}$ for all $\alpha, \beta \in F$ and all positive integers n.

Thm. A finite field $GF(p^n)$ of p^n elements exists for every prime power p^n.

Proof Sketch: We can construct a field by looking for all the zeros of $x^{p^n} - x$ and showing that they form a field of p^n elements.

Corollary: If F is any finite field, then for every positive integer n, there is an irreducible polynomial in $F[x]$ of degree n.

Thm. Let p be a prime and let $n \in \mathbb{Z}^+$. If E and E' are fields of order p^n, then $E \simeq E'$.

Note: This theorem basically says that there is only one finite field of order p^n, up to isomorphism.

Selected Exercises

10. Show that every irreducible polynomial in $\mathbb{Z}_p[x]$ is a divisor of $x^{p^n} - x$ for some n.

12. Show that a finite field of p^n elements has exactly one subfield of p^m elements for each divisor m of n.

13. Show that $x^{p^n} - x$ is the product of all monic irreducible polynomails in $\mathbb{Z}_p[x]$ of degree d dividing n.