Galois Theory and Finite Fields

Kevin James

Proposition

Any finite field is isomorphic to $\mathbb{F}_{p^n}$ for some prime p and $n \in \mathbb{N}$, where $\mathbb{F}_{p^n}$ is the splitting field for $x^{p^n} - 1$ over $\mathbb{F}_p$. The extension $\mathbb{F}_{p^n}/F_p$ is Galois with $\mathrm{Gal}(\mathbb{F}_{p^n}/F_p) =< \sigma_p >\cong \mathbb{Z}/n\mathbb{Z}$, where σ_p denotes the Frobenius map. The subfields of $\mathbb{F}_{p^n}$ are all Galois over $\mathbb{F}_p$ and are in 1-1 correspondence with the divisors d of n. More precisely they are the subfields $\mathbb{F}_{p^d}$, the fixed fields of σ_p^d.

Corollary

The irreducible polynomial $x^4 + 1 \in \mathbb{Z}[x]$ is reducible modulo every prime p.

Proposition

The finite field $\mathbb{F}_{p^n}$ is simple. In particular, there exists an irreducible polynomial of degree n over $\mathbb{F}_p$ for every $n \in \mathbb{N}$.

Proposition

The polynomial $x^{p^n} - x$ is precisely the product of all the distince irreducible polynomials in $\mathbb{F}_p[x]$ of degree d where $d|n$.