Title: Finite groups induced by groups of polynomial automorphisms, and an application.

Abstract:

In this talk I will point out a for many people new and interesting link between finite groups and nonlinear maps in Affine Algebraic Geometry. This link is useful in both fields, as I will try to point out.

In the field of Affine Algebraic Geometry, the polynomial automorphism group $\mathrm{GA}_n(k)$ of a field k is the set of polynomial maps $F : k^n \longrightarrow k^n$ for which there exists a polynomial inverse. Where this group is usually studied over $\mathbb{C}$, or other fields of characteristic zero, I will discuss this group for finite fields $k = \mathbb{F}_q$. This induces a natural quotient map

$$\pi : \mathrm{GA}_n(\mathbb{F}_q) \longrightarrow \mathrm{Sym}(\mathbb{F}_q^n)$$

by sending a polynomial map to the bijection it generates on $\mathbb{F}_q^n$. ($\mathrm{GA}_n(\mathbb{F}_q)$ is infinite, the kernel contains $(x_1 + x_2^q - x_2, x_2, \ldots, x_n)$ for one.)

Now this makes it possible to go back and forth: pick a finite group and study its preimage, or pick a subgroup of $\mathrm{GA}_n(\mathbb{F}_q)$ and study its image. As an example, I will show how the p-sylow group of $\mathrm{Sym}(\mathbb{F}_p^n)$ can be studied by understanding a well-known subgroup $\mathrm{BA}_n(\mathbb{F}_p)$ of $\mathrm{GA}_n(\mathbb{F}_p)$. As an application, I will show how iteratively applying elements in $\mathrm{BA}_n(\mathbb{F}_p)$ to an element of $\mathbb{F}_p^n$ can be efficiently computed. Given time, I will show how to apply this to session-key establishment by a Diffie-Hellman protocol in symmetric key cryptography.