24 mars 2009

Cours de Théorie des Nombres MM020

Une application de la théorie des corps finis d'après Jean-Pierre Serre

Michel Waldschmidt

Institut de Mathématiques de Jussieu

http ://www.math.jussieu.fr/~miw/

As the title indicates, the purpose of the present lecture is to show how to use finite fields for solving problems on infinite fields. This can be done on two different levels: the elementary one uses only the fact that most algebraic geometry statements involve only finitely many data, hence come from geometry over a finitely generated ring, and the residue fields of such a ring are finite; the examples we give in §§1-4 are of that type. A different level consists in using Chebotarev's density theorem and its variants, in order to obtain results over non-algebraically closed fields; we give such examples in §§5-6. The last two sections were only briefly mentioned in the actual lecture; they explain how cohomology (especially the étale one) can be used instead of finite fields; the proofs are more sophisticated[1], but the results have a wider range.

How to use finite fields for problems concerning infinite fields

http ://arxiv.org/abs/0903.0517

Author : Jean-Pierre Serre (Submitted on 3 Mar 2009)

Abstract : The first part is expository : it explains how finite fields may be used to prove theorems on infinite fields by a reduction mod p process.
The second part gives a variant of P.Smith's fixed point theorem which applies in any characteristic.

1. Automorphisms of the affine n-space

Let us start with the following simple example:

Theorem 1.1. *Let σ be an automorphism of the complex affine n-space $\mathbf{C}^n$, viewed as an algebraic variety. Assume that $\sigma^2 = 1$. Then σ has a fixed point.*

Surprisingly enough this theorem can be proved by "replacing $\mathbf{C}$ by a finite field".

More generally:

Theorem 1.2. *Let G be a finite p-group acting algebraically on the affine space $\mathbf{A}^n$ over an algebraically closed field k with $\operatorname{char} k \neq p$. Then the action of G has a fixed point.*

Action algébrique d'un groupe fini sur l'espace affine

Soient k un corps algébriquement clos, n un entier positif et G un groupe. Le groupe G *agit algébriquement sur l'espace affine* $\mathbf{A}^n$ si, pour tout $g \in G$, il existe des polynômes $P_{g,1}, \dots, P_{g,n}$ dans $k[X_1, \dots, X_n]$, tels que l'application

$$\sigma_g : (x_1, \dots, x_n) \longmapsto \big(P_{g,1}(x_1, \dots, x_n), \dots, P_{g,n}(x_1, \dots, x_n)\big)$$

soit une bijection de $\mathbf{A}^n$ sur $\mathbf{A}^n$, et que l'application $g \mapsto \sigma_g$ soit un homomorphisme de G dans le *groupe symétrique* $\mathfrak{S}_{\mathbf{A}^n}$ de $\mathbf{A}^n$ (groupe des bijection de $\mathbf{A}^n$ sur $\mathbf{A}^n$).

Action d'un groupe fini sur un ensemble

Quand un groupe G *agit sur un ensemble* E (c'est-à-dire quand on se donne une injection de G dans le groupe symétrique $\mathfrak{S}_E$ de E), *l'orbite* d'un élément x de E est

$$Gx = \{gx \ ; \ g \in G\} \subset E,$$

le stabilisateur de x est le sous-groupe G_x de G qui fixe x

$$G_x = \{g \in G \ ; \ gx = x\} \subset G,$$

et la surjection naturelle $G \mapsto Gx$ qui envoie g sur gx induit une bijection de G/G_x sur Gx. Ainsi quand G ou E est fini, le stabilisateur G_x de x est d'indice fini dans G, et cet indice est le nombre d'éléments de l'orbite de x.

Exemples

1. Prenons une matrice $n \times n$ à coefficients complexes A et une matrice $1 \times n$ à coefficients complexes B. Alors $\underline{x} \to A\underline{x} + B$ est un endomorphisme algébrique de $\mathbf{A}^n$. C'est un automorphisme si et seulement si A est inversible.
2. Soit $P \in \mathbf{C}[X]$. Alors $(x_1, x_2) \mapsto \big(x_1, x_2 + P(x_1)\big)$ est un automorphisme de $\mathbf{A}^2$.

Exercice. Donner un exemple d'un système de polynômes $(P_1, \dots, P_n)$ dans $\mathbf{C}[X_1, \dots, X_n]$, qui ne sont pas tous de degré 1, tels que l'application

$$(x_1, \dots, x_n) \mapsto (P_1(x_1, \dots, x_n), \dots, P_n(x_1, \dots, x_n))$$

soit une bijection σ de $\mathbf{C}^n$ sur $\mathbf{C}^n$ telle que σ^2 soit l'identité.

Formule des classes

Quand un groupe fini G agit sur un ensemble E, l'ensemble E est réunion disjointe des orbites (*être sur la même orbite est une relation d'équivalence sur* E).

Si E est fini, le nombre d'éléments de E est la somme des indices des stabilisateurs, qui sont des diviseurs de l'ordre de G.

Par conséquent si G est un p-groupe et que le nombre d'éléments de E est fini non multiple de p, alors il existe une orbite à un élément : G a un point fixe.

Anneaux de type fini comme groupe additif

Soit k un corps. Supposons que le groupe additif de k soit un $\mathbf{Z}$–module de type fini. Alors k est un corps fini.

Tout sous–$\mathbf{Z}$–module d'un $\mathbf{Z}$–module de type fini est un $\mathbf{Z}$–module de type fini. Donc k est de caractéristique p finie. Soit $\{x_1, \ldots, x_m\}$ un système de générateurs de k comme $\mathbf{Z}$–module. L'application $\mathbf{Z}^m \to k$ qui envoie $(a_1, \ldots, a_m)$ sur $a_1x_1 + \cdots + a_mx_m$ est un homomorphisme surjectif de groupes additifs qui donne par passage au quotient une surjection de $(\mathbf{Z}/p\mathbf{Z})^m$ sur k. Donc k est un corps fini.

Il en résulte que *si A est un anneau qui est de type fini comme $\mathbf{Z}$–module et si $\mathfrak{M}$ est un idéal maximal de A, alors $A/\mathfrak{M}$ est un corps fini.*

Théorème des zéros de Hilbert

(Hilbert Nullstellensatz)

Soient k un corps algébriquement clos, n un entier positif, A l'anneau $k[X_1, \ldots, X_n]$.
Pour chaque $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in k^n$, l'idéal $\mathfrak{M}_{\underline{\alpha}}$ de A engendré par les n éléments $(X_1 - \alpha_1, \ldots, X_n - \alpha_n)$ est maximal : c'est l'ensemble des polynômes qui s'annulent au point $\underline{\alpha}$.
Le Théorème des zéros de Hilbert affirme qu'*on obtient ainsi tous les idéaux maximaux de A.*
Par conséquent dire qu'une famille de polynômes $(P_i)_{i\in I}$ de $k[X_1, \ldots, X_n]$ n'a pas de zéros commun dans k^n équivaut à dire qu'elle engendre l'idéal (1), donc qu'il existe une famille $(Q_i)_{i\in I}$ de polynômes de $k[X_1, \ldots, X_n]$, de support fini, telle que

$$\sum_{i\in I} P_iQ_i = 1.$$

Anneaux de type fini comme $\mathbf{Z}$–algèbre

Dans son texte Serre utilise un énoncé plus puissant :
Si A est un anneau qui est une $\mathbf{Z}$–algèbre de type fini, alors pour tout idéal maximal $\mathfrak{M}$ de A le quotient $A/\mathfrak{M}$ est un corps fini.
La référence est Bourbaki Algèbre commutative Chapitre V § 3 n° 4. Cette section concerne les *anneaux de Jacobson* qui sont les anneaux pour lesquels tout idéal premier est intersection d'idéaux maximaux.
Un exemple est $\mathbf{Z}$. Plus généralement, *si A est un anneau de Jacobson et B un anneau qui est une A–algèbre de type fini, alors B est un anneau de Jacobson.*
De plus, si $\mathfrak{M}'$ est un idéal maximal de B, alors l'image inverse $\mathfrak{M}$ de $\mathfrak{M}'$ par le morphisme $A \to B$ (qui fait de B une A–algèbre) est un idéal maximal de A, et *le corps $B/\mathfrak{M}'$ est une extension finie de $A/\mathfrak{M}$.*

Proof of Theorem 1.2

a) The case $k = \mathbf{F}_\ell$, where ℓ is a prime number $\neq p$

We may assume that the action of G is defined over some finite extension $\mathbf{F}_{\ell^m}$ of $\mathbf{F}_\ell$. Then the group G acts on the product $\mathbf{F}_{\ell^m} \times \cdots \times \mathbf{F}_{\ell^m}$. However, G is a p-group and the number of elements of $\mathbf{F}_{\ell^m} \times \cdots \times \mathbf{F}_{\ell^m}$ is not divisible by p. Hence there is an orbit consisting of one element, i.e. there is a fixed point for the action of G.

b) Reduction to the case $k = \overline{\mathbf{F}}_\ell$

Since G is finite, we can find a ring $\Lambda \subset \mathbf{C}$ finitely generated over $\mathbf{Z}$, over which the action of G can be defined. This means that the action of G is given by

$$g(x_1, \ldots, x_n) = (P_{g,1}(x_1, \ldots, x_n), \ldots, P_{g,n}(x_1, \ldots, x_n)),$$

where the coefficients of the polynomials $P_{g,i}(x_1, \ldots, x_n)$ belong to Λ. Assume that there is no fixed point. The system of equations

$$x_i - P_{g,i}(x_1, \ldots, x_n) = 0$$

has no solution in $\mathbf{C}$. Thus, by Hilbert's Nullstellensatz, there exist polynomials $Q_{g,i}(x_1, \ldots, x_n)$ such that

$$\sum_{g,i} (x_i - P_{g,i}(x_1, \ldots, x_n)) Q_{g,i}(x_1, \ldots, x_n) = 1. \tag{1}$$

$$\sum_{g,i} (x_i - P_{g,i}(x_1, \ldots, x_n)) Q_{g,i}(x_1, \ldots, x_n) = 1. \tag{1}$$

By enlarging Λ if necessary, we may assume that it contains $1/p$ and the coefficients of the $Q_{g,i}$'s. Let $\mathfrak{m}$ be a maximal ideal of Λ. Then the field $\Lambda/\mathfrak{m}$ is finite (see e.g. [5], p.68, cor.1), we have char $\Lambda/\mathfrak{m} \neq p$ (since p is invertible in Λ) and by (1) the conditions of the theorem hold for the algebraic closure of $\Lambda/\mathfrak{m}$. So we can apply part a) of the proof to get a contradiction.

Remark. The technique of replacing a scheme X of finite type over k by a scheme over Λ is sometimes called "spreading out X"; its properties are described in [10], §10.4.11 and §17.9.7.