Ho Chi Minh University of Science HCMUS

Update: April 18, 2009

Finite fields: some applications

Michel Waldschmidt [5]

Fifth course

April 18, 2009

6 An application of the theory of finite fields, following Jean-Pierre Serre

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.

6.1 Algebraic action of a finite group on the affine space

Let Ω be an algebraically closed field, n a positive integer and G a group. An *algebraic action of G on the affine space* $\mathbf{A}^n$ is given by polynomials $P_{g,1},\dots,P_{g,n}$ in $\Omega[X_1,\dots,X_n]$, such that the mapping

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

is a bijective from $\mathbf{A}^n$ onto $\mathbf{A}^n$, and that the map $g\mapsto\sigma_g$ is a homomorphism from G into the *symmetric group* $\mathfrak{S}_{\mathbf{A}^n}$ of $\mathbf{A}^n$ (group of bijective maps from $\mathbf{A}^n$ onto $\mathbf{A}^n$.

Examples.
1. Let A be a $n\times n$ matrix with complex coefficients and B a $1\times n$ matrix with complex coefficients. Then $\underline{x}\rightarrow A\underline{x}+B$ is an algebraic endomorphism of $\mathbf{A}^n$.

It is an automorphism if and only if A is a regular matrix.
2. Let $P\in\mathbf{C}[X]$. Then $(x_1,x_2)\mapsto\bigl(x_1,x_2+P(x_1)\bigr)$ is an automophism of

[5] This text is accessible on the author's web site
http://www.math.jussieu.fr/~miw/coursVietnam2009.html

$\mathbf{A}^2$.
3. Let $P \in \mathbf{C}[X]$ be an *odd* polynomial : $P(-X) = -P(X)$. An automorphism σ of the affine space $\mathbf{A}^3$ over $\mathbf{C}$ such that $\sigma^2 = 1$ is given by

$$(x_1, x_2, x_3) \longmapsto \bigl(x_2, x_1, x_3 + P(x_1 - x_2)\bigr).$$

The elements (a, a, b) in the plane $x_1 = x_2$ are fixed under σ.
4. Let $P \in \mathbf{C}[X]$. The automorphism

$$\sigma : (x_1, x_2) \longmapsto \bigl(x_1, -x_2 + P(x_1)\bigr).$$

of $\mathbf{A}^2$ satisfies $\sigma^2 = 1$. If the polynomial P is odd, an other example is

$$\sigma : (x_1, x_2) \longmapsto \bigl(-x_1, x_2 + P(x_1)\bigr).$$

If P is *even* : $P(-X) = P(X)$, one can take

$$\sigma : (x_1, x_2) \longmapsto \bigl(-x_1, -x_2 + P(x_1)\bigr).$$

5. Let τ be an automorphism of $\mathbf{A}^n$ such that $\tau^2 = 1$ and let φ be an automorphism of $\mathbf{A}^n$. Then $\sigma = \varphi \circ \tau \circ \varphi^{-1}$ satisfies $\sigma^2 = 1$.

6.2 Action of a finite group on a set

When a group G *acts on a set* E (which means that we are given a morphism of the group G into the symmetric group $\mathfrak{S}_E$ of E), the *orbit* of an element x of E is

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

the stabilizer of x is the subgroup G_x of G which fixes x

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

and the natural surjective mapping $G \mapsto Gx$ which maps g to gx induces a bijective map from G/G_x onto Gx.

Therefore, when either G or E is finite, the stabilizer G_x of x has finite index in G, and this index is the number of elements in the orbit of x.

When a group G acts on a set E, the set E is the disjoint union of the orbits. This partition of E defines an equivalence relation, the classes of which are the orbits. Denote by E/G the set of classes. The stabilizers of two equivalent elements are conjugate: for $y = gx$ we have $G_y = g^{-1}G_x g$. If G_x is finite, then G_y also and they have the same number of elements.

Proposition 47 (Class formula). *When E is finite, the number of elements in E is the sum over E/G of the indices of the stabilizers.*

These indices are divisors of G. As a consequence, if p is a prime and if G is a p–group (which means that its order is a power of p), and if the number of elements in E is finite and not a multiple of p, then there exists at least one orbit with one element: G has a fixed point.

6.3 Rings of finite type as Z–algebras

Chapter V § 3 n° 4 of Bourbaki *Commutative Algebra* deals with *Jacobson Rings*, which are the rings in which any prime ideal is an intersection of maximal ideals. An example is $\mathbf{Z}$. Other examples are the fields and the quotients $A/\mathfrak{A}$ of a Jacobson ring A by an ideal $\mathfrak{A} \neq A$

Theorem 48. *Let A is a Jacobson ring and $\varrho : A \rightarrow B$ a morphism which gives to B a structure of A–algebra of finite type. Then B is a Jacobson ring. Moreover, if $\mathfrak{M}'$ is a maximal ideal of B, then the inverse image $\mathfrak{M} = \varrho^{-1}(\mathfrak{M}')$ is a maximal ideal of A, and the field $B/\mathfrak{M}'$ is a finite extension of $A/\mathfrak{M}$.*

Corollary 49. *Let A be a ring. Assume A is a $\mathbf{Z}$–algebra of finite type. Then for any maximal ideal $\mathfrak{M}$ of A the quotient $A/\mathfrak{M}$ is a finite field.*

6.4 Hilbert Nullstellensatz

Let k be a field, n a positive integer and A the ring $k[X_1, \ldots, X_n]$.

For each $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in k^n$, the ideal $\mathfrak{M}_{\underline{\alpha}}$ of A generated by the n elements $(X_1 - \alpha_1, \ldots, X_n - \alpha_n)$ is maximal: this is the set of polynomials which vanish at the point $\underline{\alpha}$, the quotient $A/\mathfrak{M}$ is k.

Theorem 50 (Hilbert Nullstellensatz). *If k is algebraically closed, then any ideal of A is of this form.*

Corollary 51. *Let Ω be an algebraically closed field and $(P_i)_{i \in I}$ a family of polynomials in $\Omega[X_1, \ldots, X_n]$. If these polynomials have no common zero in Ω^n, then there exists a family of polynomials $(Q_i)_{i \in I}$ in $\Omega[X_1, \ldots, X_n]$, such that*

$$\{i \in I \; ; \; Q_i \neq 0\} \quad \textit{is finite and} \quad \sum_{i \in I} P_i Q_i = 1.$$

HOW TO USE FINITE FIELDS FOR PROBLEMS CONCERNING INFINITE FIELDS

JEAN-PIERRE SERRE

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.

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.*

Proof of Theorem 1.2

a) The case $k = \overline{\mathbf{F}}_\ell$, 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 $k = \overline{\mathbf{F}}_\ell$

Date: March 4, 2009.

I want to thank A.Zykin who wrote a preliminary version of this lecture.

[1] Indeed, I would not have been able to give them without the help of Luc Illusie and of his two reports [12] and [13].

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

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

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 $\operatorname{char} \Lambda/\mathfrak{m} \neq p$ (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.

Question. Assume the hypotheses of Theorem 1.2. Let k_o be a subfield of k such that the action of G is defined over k_o. Does there exist a fixed point of G which is rational over k_o ? Even the case $k = \mathbf{C}$, $k_o = \mathbf{Q}$, $|G| = 2$, $n = 3$ does not seem to be known.

Exercises

1. Let L be an infinite set of prime numbers. For every $p \in L$, let $k(p)$ be a denumerable field of characteristic p. Let $A = \prod k(p)$ be the product of the $k(p)$'s. Show that there exists a quotient of A which is isomorphic to a subfield of $\mathbf{C}$.(*Hint.* Use an ultrafilter on L.)

2. Let $P_i(X_1, ..., X_n)$ be a family of polynomials with coefficients in $\mathbf{Z}$. Show that the following properties are equivalent:

a) The P_i's have a common zero in $\mathbf{C}$.

b) There exists an infinite set of primes p such that the P_i's have a common zero in $\mathbf{F}_p$.

c) For every prime p, except a finite number, there exists a field of characteristic p in which the P_i's have a common zero.

3. Assume the hypotheses of Theorem 1.2. Show that the number of fixed points of G is either infinite or $\equiv 1 \bmod p$. (*Hint.* Suppose the set S of fixed points is finite. Using the same argument as in the proof of Theorem 1.2, we may assume that the action of G is defined over a finite field k_1 with q elements, with $(q, p) = 1$, that the points of S are rational over k_1, and that k_1 contains the p-th roots of unity. We then get $|S| \equiv q^n \bmod p$, hence $|S| \equiv 1 \bmod p$ since $q \equiv 1 \bmod p$.) [Smith's theory gives more: if S is finite, it has one element only, see §7.4.]