Proc. Conf. Marseille-Luminy, 2007; Contemp. Math. Series, AMS, 2009.

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: April 13, 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 [**?**] and [**?**].

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. [**?**], p.68, cor.1), we have $\operatorname{char} \Lambda/\mathfrak{m} \neq p$ (since p is invertible in Λ) and by (**??**) 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 [**?**], §10.4.11 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.]

2. Fixed points for finite group actions

Consider a finite group G of order m acting on a k-variety X, where k is an algebraically closed field[2]. Let us assume that there are a finite number of fixed points in $X(k)$ and that G acts freely outside these points.

Theorem 2.1. *Suppose we have two actions of G on X satisfying the above properties, the number of fixed points being a and a' respectively. Then $a \equiv a' \pmod{m}$.*

Sketch of proof

Assume first that X, the two actions of G, and the fixed points, are defined over a finite field $\mathbf{F}_q$. We then have

$$|X(\mathbf{F}_q)| \equiv a \pmod{m} \quad \text{and} \quad |X(\mathbf{F}_q)| \equiv a' \pmod{m},$$

hence $a \equiv a' \pmod{m}$.

The general case is reduced to this case by an argument similar to (but less obvious than) the one given in §1. [One replaces X by a separated scheme of finite type X_0 over a ring Λ which is finitely generated over $\mathbf{Z}$, in such a way that the the two actions of G extend to X_0; one also needs that the corresponding fixed points Y and Y' are finite and étale over $\mathrm{Spec}(\Lambda)$, and that the two actions of G on $X_0 - Y$ and on $X_0 - Y'$ are free. That all these conditions can be met is a consequence of [**?**], *loc.cit.*] One can then reduce modulo a maximal ideal of Λ.

Remarks

1) Theorem 1.1 is a corollary of Theorem 2.1. Indeed the involution $z \mapsto -z$ of $\mathbf{C}^n$ has only one fixed point, hence the number of fixed points of any other involution is either odd or infinite; it cannot be 0.

2) The results of §§1, 2 can also be proved by topological arguments, see §7.4 below.

3. Injectivity and surjectivity of maps between algebraic varieties

The following theorem was proved independently by J.Ax and A.Grothendieck in the 60's (see [**?**], [**?**], p.184, and [**?**], §10.4.11), and has been rediscovered several times since.

Theorem 3.1. *Let X be an algebraic variety over an algebraically closed field k. If a morphism $f : X \to X$ is injective then it is bijective.*

Sketch of proof

Assume first that k is an algebraic closure of a finite field k_1, and that f is defined over k_1. Then $X(k_1)$ is finite; since

$$f : X(k_1) \to X(k_1)$$

is injective, it is bijective. The same argument, applied to the finite extensions of k_1, shows that $f : X(k) \to X(k)$ is bijective. The case of an arbitrary algebraically closed field is reduced to the one above as in §§1-2, by

[2]The reader may interpret the word "k-variety" in the sense of FAC, i.e. as meaning a separated and reduced scheme of finite type over $\mathrm{Spec}(k)$, cf. [**?**], §10.10. Since we are only interested in the k-points, the "reduced" assumption has no importance.

choosing a ring Λ of finite type over $\mathbf{Z}$ over which X and f are defined, and reducing modulo a maximal ideal of Λ; for more details, see Grothendieck, [**?**], *loc.cit.*

Remark. When $k = \mathbf{C}$ a topological proof of this theorem was given by Borel in 1969 (see [**?**]).

4. Nilpotent groups

In 1955 M.Lazard ([**?**]) proved the following theorem:

Theorem 4.1. *Let G be an algebraic group over an algebraically closed field k. If the underlying variety of G is isomorphic to the affine space $\mathbf{A}^n$, for some $n \geqslant 0$, then G is nilpotent.*

Sketch of proof

Lazard proves even more: he shows that G is *nilpotent of class* $\leqslant n$, i.e. that every iterated commutator of length $> n$ is equal to 1. As in §1, we may assume that k is an algebraic closure of a finite field k_1 and that G is defined over k_1. If $p = \operatorname{char} k$, the group $G(k_1)$ is a finite p-group, hence is nilpotent. By applying this to the finite extensions of k_1 one sees that $G(k)$ is a locally nilpotent group, i.e. is an increasing union of nilpotent groups. A further argument is needed to show that $G(k)$ is indeed nilpotent of class $\leqslant n$, see [**?**][3].

Note that we may deduce Theorem **??** from Theorem **??** together with the following standard result:

Theorem 4.2. *Let G be a connected linear algebraic group. Then either G is nilpotent or it contains a one dimensional torus $\mathbf{G}_m$ as a subgroup.*

Proof of Theorem **??** *from Theorem* **??** *and Theorem* **??**

Assume that the underlying variety of G is isomorphic to $\mathbf{A}^n$. In particular, G is an affine variety; this is known to imply that the group G can be embedded in some $\mathbf{GL}_N$, i.e. that G is a linear group. Assume further that G is not nilpotent; then $\mathbf{G}_m \subset G$ by Theorem **??**. Choose an element σ of $\mathbf{G}_m$ of prime order $\ell \neq \operatorname{char} k$. The element σ acts on $G \simeq \mathbf{A}^n$ by left translation and thus by Theorem **??** has a fixed point: contradiction!

Exercise. Give a topological proof of Theorem **??** when $k = \mathbf{C}$ by using the fact that, for a non nilpotent connected group, either H^1 or H^3 is non zero. Extend this proof to arbitrary fields using ℓ-adic cohomology.

5. Finite subgroups of $\mathbf{GL}_n(\mathbf{Q})$

The following theorem is a well-known result of Minkowski (see [**?**], [**?**], [**?**]); it gives a multiplicative upper bound for the order of a finite subgroup of $\mathbf{GL}_n(\mathbf{Q})$.

Theorem 5.1. *Let ℓ be a prime number. If A is a subgroup of $\mathbf{GL}_n(\mathbf{Q})$ of order ℓ^a then*

$$a \leqslant M(n,\ell) = \left[\frac{n}{\ell-1}\right] + \left[\frac{n}{\ell(\ell-1)}\right] + \left[\frac{n}{\ell^2(\ell-1)}\right] + \dots . \tag{2}$$

[3]Note the following misprints in [**?**]: in the last part of the proof of Lemma 1, "$s \geqslant t$" should be "s divisible by t" and "$W = C_2(X, W)$" should be "$W = C_2(X, V)$".

Proof for $\ell \neq 2$

The idea is to reduce mod p for an appropriate choice of $p \neq \ell$. First, we have $A \subset \mathbf{GL}_n(\mathbf{Z}[1/N])$ for a suitable $N \geqslant 1$. If p is sufficiently large ($p > 2$ is enough) and does not divide N, then the reduction mod p gives a subgroup A' of $\mathbf{GL}_n(\mathbf{F}_p)$ such that $|A| = |A'|$. Hence $|A|$ divides $|\mathbf{GL}_n(\mathbf{F}_p)|$, which is equal to $p^{n(n-1)/2}\prod_{i=1}^{n}(p^i - 1)$. Let us choose p such that its image in $(\mathbf{Z}/\ell^2\mathbf{Z})^*$ is a generator of this group. This is always possible by Dirichlet's theorem on primes in arithmetic progressions since $(\mathbf{Z}/\ell^2\mathbf{Z})^*$ is cyclic. Once p is chosen in this way, $p^i - 1$ is divisible by ℓ only if i is divisible by $\ell - 1$ and in this case the ℓ-adic valuation $v_\ell(p^i - 1)$ of $p^i - 1$ is equal to $1 + v_\ell(i)$. Hence $v_\ell(|A|) \leqslant \sum(1 + v_\ell(i))$, where the sum is over the integers i with $1 \leqslant i \leqslant n$ which are divisible by $\ell - 1$; a simple computation shows that this sum is equal to $M(n, \ell)$ if $\ell \neq 2$, cf. [**?**], §1.3.

Remark 5.2. In the case $\ell = 2$ one has to replace the group $\mathbf{GL}_n$ by an orthogonal group $\mathbf{O}_n$ in order to get the desired bound.

Remark 5.3. The result is optimal in the sense that, for every prime number ℓ, there exist subgroups of $\mathbf{GL}_n(\mathbf{Q})$ of order $\ell^{M(n,\ell)}$, see [**?**] and [**?**]. These subgroups have the following Sylow-type property:

Theorem 5.4. *Let A, P be two finite ℓ-subgroups of $\mathbf{GL}_n(\mathbf{Q})$. Suppose that $|P| = \ell^{M(n,\ell)}$. Then A is $\mathbf{GL}_n(\mathbf{Q})$-conjugate to a subgroup of P.*

[In particular, if $|A| = |P|$, then A and P are conjugate.]

Sketch of proof

We only give the proof when $\ell \neq 2$ (otherwise we have to consider orthogonal groups). Let us reduce mod p for a prime p chosen as above. We get two ℓ-subgroups A and P of $\mathbf{GL}_n(\mathbf{F}_p)$; by construction, P is a Sylow subgroup of $\mathbf{GL}_n(\mathbf{F}_p)$. By Sylow's theorem, A is conjugate to a subgroup of P, i.e. there exists an embedding $i : A \to B$ which is the restriction of an inner automorphism of $\mathbf{GL}_n(\mathbf{F}_p)$. The linear representations $A \to \mathbf{GL}_n(\mathbf{Q})$ and $A \xrightarrow{i} P \to \mathbf{GL}_n(\mathbf{Q})$ become isomorphic after reduction mod p. Since $p \neq \ell$, a standard argument shows that they are isomorphic over $\mathbf{Q}_p$, hence also over $\mathbf{Q}$, and this completes the proof.

Remark 5.5. In [**?**], Schur gave another proof of Minkowski's Theorem using an interesting lemma on characters of finite groups ([**?**], §2.1, prop.1). He also extended the theorem (by a different method) to arbitrary number fields (see [**?**], §2.2).

6. Generalizations to other algebraic groups and fields

A natural question is: what happens in Theorem **??** if $\mathbf{Q}$ is replaced by an arbitrary field k and $\mathbf{GL}_n$ by an arbitrary reductive group G ? This is answered in [**?**]: roughly speaking, one can give a sharp bound for the order of a finite ℓ-subgroup of $G(k)$ when one knows the root system of G and the Galois group of the ℓ-cyclotomic tower of k (one needs also to assume that G is "of inner type", but this is automatic for the most interesting examples, such as G_2, F_4, E_7 or E_8). The proof follows Minkowski's method; the main difference is that Dirichlet's theorem on arithmetic progressions is replaced

by a variant of the Chebotarev's density theorem which applies to every normal domain which is finitely generated over $\mathbf{Z}$ (see [**?**], §2.7 and [**?**], §6.4). As a sample, here is the case where $k = \mathbf{Q}$ and G is of type E_8:

Theorem 6.1. *Let G be a group of type E_8 over $\mathbf{Q}$ and let A be a finite subgroup of $G(\mathbf{Q})$. Then $|A|$ divides the number*

$$M(\mathbf{Q}, E_8) = 2^{30} \cdot 3^{13} \cdot 5^5 \cdot 7^4 \cdot 11^2 \cdot 13^2 \cdot 19 \cdot 31.$$

Sketch of proof

We may assume that G is defined over $\mathbf{Z}[1/N]$ for some $N \geqslant 1$ and that A is an ℓ-subgroup of $G(\mathbf{Z}[1/N])$ for some prime ℓ (the general bound is then obtained by multiplicativity). By reducing mod p for p large enough, we see that $|A|$ divides $|E_8(\mathbf{F}_p)|$. One knows (see e.g. [**?**], Theorem 9.4.10) that

$$|E_8(\mathbf{F}_p)| = p^{120}(p^2-1)(p^8-1)(p^{12}-1)(p^{14}-1)(p^{18}-1)(p^{20}-1)(p^{24}-1)(p^{30}-1).$$

By choosing p as in Minkowski's proof, one gets the desired bound. As an example, let us do the computation when ℓ is equal to 3:

Choose $p \equiv 2, 4, 5$ or $7 \pmod 9$. Then $p^2 - 1$ is divisible by 3 but not by 9. This implies that the 3-adic valuations of the eight factors $p^2 - 1$, $p^8 - 1$, ..., $p^{30} - 1$ are respectively: 1, 1, 2, 1, 3, 1, 2, 2. Their sum is 13, as claimed.

Remark 6.2. The bound in Theorem **??** is optimal in the following sense: for every $\ell = 2, 3, ..., 31$, there exists a group G of type E_8 over $\mathbf{Q}$ such that $G(\mathbf{Q})$ contains a subgroup of order 2^{30}, 3^{13}, ..., 31, cf. [**?**], §13.5. [Recall that there are three different groups of type E_8 over $\mathbf{Q}$, up to isomorphism; they are characterized by the structure of their $\mathbf{R}$-points. For most values of ℓ, one can choose G such that $G(\mathbf{R})$ is compact.]

Exercise. Let K be a quadratic number field with discriminant d. Show that Theorem **??** is valid with $\mathbf{Q}$ replaced by K and $M(\mathbf{Q}, E_8)$ replaced by $c(d)M(\mathbf{Q}, E_8)$, where $c(d)$ is defined by:

$c(8) = 2^8$, $c(5) = 5^5$, $c(13) = 13^2$, $c(17) = 17^2$, $c(29) = 29$, $c(37) = 37$,

$c(41) = 41$, $c(61) = 61$ and $c(d) = 1$ for the other values of d (in particular those which are negative).

7. Proofs via Topology

As indicated at the end of §2, the results of §§1,2 can also be obtained - and sometimes improved - by using topological methods, based on cohomology (either standard, if the ground field is $\mathbf{C}$, or étale). There are several ways to do so; we shall summarize a few of them below.

The notation will be the following: X is an algebraic variety over an algebraically closed field k and G is a finite group which acts on X; the fixed point set of G is denoted by X^G. We assume that X is quasi-projective (in most applications, X is affine), so that the quotient variety X/G is well defined. The cohomology groups $H^i(X)$ will be understood as the étale ones, with arbitrary support; in case we need cohomology with proper support, we shall write $H^j_c(X)$, with a c in index position. The letter ℓ will denote a prime number distinct from char k.

7.1. *Using Cartan-Leray's spectral sequence*

Suppose that G acts freely on X. There is a Cartan-Leray spectral sequence (first defined in [**?**] in the context of standard sheaf cohomomology - for the case of étale cohomology, see [**?**], §8.5)

$$H^i(G, H^j(X, C)) \Longrightarrow H^{i+j}(X/G, C),$$

where C is any finite abelian group. If X is the affine n-space $\mathbf{A}^n$ and $|C|$ is prime to char k, then $H^j(X, C) = 0$ for $j > 0$ and $H^0(X, C) = C$. In that case the spectral sequence degenerates and gives $H^i(G, C) = H^i(X/G, C)$ for every i, i.e. X/G has the same cohomology as the classifying space of G. Take now $C = \mathbf{Z}/\ell\mathbf{Z}$ and suppose that ℓ divides $|G|$. It is well known that $H^j(G, C)$ is non zero for infinitely many j's, and that $H^j(X/G, C)$ is zero for $j > 2.\dim X$: contradiction!

Conclusion: *the only finite groups which can act freely on* $\mathbf{A}^n$ *are the* p*-groups, with* $p = \text{char } k$. This gives another proof of Theorem 1.1.

Exercise. Let G be a finite p-group, with $p = \text{char } k$. Show that there exists a free action of G on $\mathbf{A}^n$, provided that n is large enough. (*Hint*: embed G in a connected unipotent group.)

7.2. *Using Euler-Poincaré characteristics*

Let $\chi(X)$ be the Euler-Poincaré characteristic of X, relative to the ℓ-adic cohomology. It is known (see [**?**], [**?**]) that $\chi(X)$ does not depend on the choice of ℓ, and that it coincides with the Euler-Poincaré characteristic of X with proper support (Grothendieck-Laumon's theorem, cf. [**?**] - in case $k = \mathbf{C}$, see the Appendix of [**?**]). In other words, we have

$$\chi(X) = \sum(-1)^j \dim H^j(X, \mathbf{Q}_\ell) = \sum(-1)^j \dim H^j_c(X, \mathbf{Q}_\ell).$$

A useful property of χ is its *additivity* : if X is the disjoint union of locally closed subvarieties X_λ, then $\chi(X) = \sum \chi(X_\lambda)$; this follows from the definition of $\chi(X)$ via cohomology with proper support.

If $|G|$ is prime to char k, and G acts freely on X, one has $\chi(X) = |G|.\chi(X/G)$, cf. [**?**]. (In particular $\chi(X) = 1$ implies $|G| = 1$; since $\chi(\mathbf{A}^n) = 1$, we recover the statement given at the end of §7.1.)

Assume now that G is an ℓ-group. We have:

$$\chi(X^G) \equiv \chi(X) \pmod{\ell}.$$

Indeed, using induction on $|G|$, one may assume that G is cyclic of order ℓ; in that case, G acts freely on $Y = X - X^G$ and we have

$$\chi(X) = \chi(X^G) + \chi(Y) = \chi(X^G) + \ell.\chi(Y/G) \equiv \chi(X^G) \pmod{\ell}.$$

In particular, *if* $\chi(X)$ *is not divisible by* ℓ*, then* X^G *is non empty.* This gives another proof of Theorem 1.2 (with the letter p replaced by ℓ). A similar argument applies to Theorem 2.1: with the notation of that theorem, one has $a \equiv \chi(X) \pmod{m}$ and $a' \equiv \chi(X) \pmod{m}$, hence $a \equiv a' \pmod{m}$.

7.3. *Using Lefschetz numbers*

If s is an element of G, of order prime to char k, let $t(s)$ be its Lefschetz number:

$$t(s) = \sum(-1)^j.\text{Tr}(s, H^j(X, \mathbf{Q}_\ell)) = \sum(-1)^j.\text{Tr}(s, H^j_c(X, \mathbf{Q}_\ell)), \quad \text{cf. [?]}.$$

It is known (*loc.cit.*) that $t(s) = 0$ if s has no fixed point. If $X = \mathbf{A}^n$, one has obviously $t(s) = 1$. Hence *every automorphism of* $\mathbf{A}^n$*, whose order is finite and prime to* $\text{char}(k)$*, has a fixed point.* In the special case where $k =$

C, this was proved by D.Petrie and J.D.Randall [**?**] by a similar argument, based on standard cohomology.

Remark. For a general report on the possible actions of algebraic groups (not necessarily finite) on $\mathbf{A}^n$, see H.Kraft [**?**].

7.4. *Using Smith theory*

In the situation of Theorem 1.2, for $k = \mathbf{C}$, Smith theory (cf. P.A.Smith [**?**] and A.Borel [**?**]) gives more than the mere existence of a fixed point: it gives non trivial information on the cohomology of X^G. For instance, it shows that, if $\dim X^G = 0$, then X^G is reduced to one point. Similar results hold in any characteristic. More precisely, suppose that G is a finite p-group and let us write $H^j(X)$ instead of $H^j(X, \mathbf{Z}/p\mathbf{Z})$.

Theorem 7.5. *Let N be an integer such that $H^j(X) = 0$ for all $j \geqslant N$. Then* :

a) *$H^j(X^G) = 0$ for all $j \geqslant N$.*

b) If $N = 1$ and $\dim H^0(X) = 1$, *then* $\dim H^0(X^G) = 1$.

The proof when $|G| = p$ will be given in §8 below. The general case follows by induction on $|G|$: if $|G| > p$, one chooses a central subgroup H of G of order p and one applies the induction hypothesis to the action of G/H on X^H.

Corollary. *If X is p-acyclic, so is X^G.*

This is obvious, since " p-acyclic " means that $\dim H^j$ is equal to 0 for $j > 0$ and to 1 for $j = 0$. Note that this implies that, if X^G is finite, it has only one element.

Remark. The prime number p is allowed to be equal to char k. This case is of interest mainly when X is a projective variety. For instance, if X is a smooth projective surface in characteristic p and if X is rational, then X is p-acyclic [use the Artin-Schreier exact sequence] and the corollary above shows that the same is true for X^G; in particular, X^G is not empty.

8. Smith Theory: Proof of Theorem 7.5

Let G be a cyclic group of prime order p. The group algebra $\mathbf{F}_p[G]$ is isomorphic to the truncated polynomial ring $\mathbf{F}_p[t]/(t^p)$. This very simple fact is basic in Smith's proofs. It explains the rather artificial-looking definitions given below.

8.1. *R-abelian categories. Definitions*

Let F be a field and let n be an integer > 1. Let R be the F-algebra generated by an element t with the relation $t^n = 0$; it has for basis $1, ..., t^{n-1}$. Let C be an *R-abelian category*, i.e. an abelian category such that, for every pair of objects A, B of C, $\mathrm{Hom}_C(A, B)$ has an R-module structure, and the composition of maps is R-bilinear. In particular, t defines an endomorphism t_A of every object A of C, and we have $t_A^n = 0$. If i is a positive integer, the image of the endomorphism t_A^i of A will be denoted by t^iA, and its kernel will be written A_{t^i}.

We have $A \supset tA \supset t^2A \supset ... \supset t^nA = 0$, and $A/A_{t^i} = t^iA$.

We shall say that A is *constant* if $tA = 0$, and that A is *free* if the morphism $A/tA \to t^{n-1}A$ given by t_A^{n-1} is an isomorphism, i.e. if $A_{t^{n-1}} =$

tA; this implies that all the quotients $t^iA/t^{i+1}A$ are isomorphic to A/tA for $i = 1, ..., n-1$.

Example. If C is the category Mod_R of all R-modules, the notion of freeness just defined coincides with the usual one. As for the "constant" R-modules, they are the F-vector spaces with zero t-action.)

8.2. *The (I,A,B) setting*

We now choose an exact sequence in C:

(8.2.1) $0 \to I \to A \to B \to 0$

such that I is free and B is constant.

Lemma 8.2.2. *For every i with $1 \leqslant i \leqslant n-1$ we have :*

(8.2.3) *The natural map $A_{t^i}/t^{n-i}A \to B$ is an isomorphism.*

(8.2.4) *The natural map $A/t^iA \to B \oplus t^{n-i}A$ is an isomorphism.*

(In (8.2.4), the map $A/t^iA \to t^{n-i}A$ is induced by t_A^{n-i}.)

Proof. For every object Y of C, let us put $h_i(Y) = Y_{t^i}/t^{n-i}Y$. If

$$0 \to Y' \to Y \to Y'' \to 0$$

is an exact sequence in C, we have an hexagonal exact sequence

$$\begin{array}{ccccc} & & h_i(Y') & \to & h_i(Y) & & \\ & \nearrow & & & & \searrow & \\ h_{n-i}(Y'') & & & & & & h_i(Y'') \\ & \nwarrow & & & & \swarrow & \\ & & h_{n-i}(Y) & \leftarrow & h_{n-i}(Y') & & \end{array}$$

Apply this to (8.2.1). Since B is constant, we have $h_i(B) = B$, and since I is free, we have $h_i(I) = 0$ for every i. We thus get the exact sequence

$$0 = h_i(I) \longrightarrow h_i(A) \longrightarrow h_i(B) = B \longrightarrow h_{n-i}(I) = 0,$$

which proves (8.2.3). As for (8.2.4), it follows from the fact that $A/t^iA \to t^{n-i}A$ is surjective and that its kernel, by (8.2.3), is $h_i(A) = B$.

Remark. When $C = Mod_R$, (8.2.1) implies that the R-module A is a direct sum[4] of indecomposable modules which are isomorphic to either F or R : in other words, the only "Jordan blocks" which can occur are of rank either 1 or n.

8.3. *The main statements*

We now consider another R-abelian category C' and a cohomological functor (H, δ) on C with values in C' (cf. [**?**], §2.1); we assume that this functor is compatible with the R-structures of C and C'. For every $j \in \mathbf{Z}$, and every object E of C, $H^j(E)$ is an object of C'; every exact sequence $0 \to E \to E' \to E'' \to 0$ in the category C gives rise to an infinite exact sequence in C':

$$... \longrightarrow H^j(E) \longrightarrow H^j(E') \longrightarrow H^j(E'') \xrightarrow{\delta_j} H^{j+1}(E) \longrightarrow ...$$

We make the following assumptions:

(8.3.1) $H^j(E) = 0$ for every $j < 0$ and every $E \in Ob(C)$. This implies that the functor H^0 is left exact.

(8.3.2) For every $E \in Ob(C)$, one has $H^j(E) = 0$ for j large enough (which may depend on E).

[4]possibly infinite : Smith theory does not require any finiteness assumption.

We are now going to apply the cohomological functor (H, δ) to the C-objects I, A, B of the exact sequence (8.2.1). The first result is:

Proposition 8.3.3. *Let N be a positive integer. Assume that $H^j(A) = 0$ for all $j \geqslant N$. Then the same is true for B, i.e. $H^j(B) = 0$ for all $j \geqslant N$.*

In the special case $N = 1$ one can say more:

Proposition 8.3.4. *Assume that $H^j(A) = 0$ for all $j > 0$, and that $H^0(A)$ is constant, i.e. $t.H^0(A) = 0$. Then the same is true for B and the natural map $H^0(A) \to H^0(B)$ is an isomorphism.*

8.4. *Proof of Proposition 8.3.3*

We prove first:

Lemma 8.4.1. *Let m be a positive integer. Suppose that $H^j(A)$, $H^j(B)$, $H^j(t^iA)$ and $H^j(A_{t^i})$ are 0 for $j = m + 1$ and all $i = 1, ..., n - 1$. Suppose also that $H^m(A) = 0$. Then $H^m(B), H^m(t^iA)$ and $H^m(A_{t^i})$ are 0.*

Proof. Since $H^{m+1}(t^iA) = 0$ the map $H^m(A) \to H^m(A/t^iA)$ is surjective, and this shows that $H^m(A/t^iA) = 0$. By (8.2.4) this implies that $H^m(B)$ and $H^m(t^{n-i}A)$ are 0, and since $n - i$ takes all values between 1 and $n - 1$ we also have $H^m(t^iA) = 0$. By (8.2.3), A_{t^i} is an extension of B by $t^{n-i}A$; hence $H^m(A_{t^i})$ is also 0.

We can now prove Proposition 8.3.3. Indeed, by (8.3.2), we may choose an $m > N$ such that the hypotheses of Lemma 8.4.1 are satisfied. One then uses descending induction on m. By Lemma 8.4.1, this is possible until we reach $m = N$; the proposition follows.

Note that we obtain at the same time the vanishing of $H^j(t^iA)$ and $H^j(A_{t^i})$ for all $j \geqslant N$ and all $i = 1, ..., n - 1$.

8.5. *Proof of Proposition 8.3.4*

We apply Proposition 8.3.3 with $N = 1$. As mentioned above, we obtain the vanishing, not only of $H^1(B)$, but also of $H^1(tA)$ and $H^1(A_t)$. Since H^0 is left exact, the sequence

$$0 \longrightarrow H^0(A_t) \longrightarrow H^0(A) \xrightarrow{t} H^0(A)$$

is exact, and since $t.H^0(A) = 0$ we see that $H^0(A_t) \to H^0(A)$ is an isomorphism. Using the exact sequence

$$H^0(A_t) \longrightarrow H^0(A) \longrightarrow H^0(tA) \longrightarrow H^1(A_t),$$

we deduce that $H^0(tA) = 0$. By (8.2.4) this implies that the natural map $H^0(A/t) \to H^0(B)$ is an isomorphism. But the map $H^0(A) \to H^0(A/tA)$ is also an isomorphism, since $H^0(tA)$ and $H^1(tA)$ are both 0. Hence $H^0(A) \to H^0(B)$ is an isomorphism.

8.6. *Proof of Theorem 7.5*

We can now prove Theorem 7.5 by applying what we have done to the case where $R = \mathbf{F}_p[G] = \mathbf{F}_p[t]/(t^p)$ and C is the category of the $\mathbf{F}_p[G]$-étale sheaves over X/G, i.e. the sheaves which are killed by p, and are endowed with an action of G.

We take for C' the categorie Mod_R of all R-modules, and for cohomological functor the functor "étale cohomology over X/G "; hence, if Y is a sheaf belonging to C, $H^j(Y)$ is nothing else than $H^j(X/G, Y)$; condition

(8.3.1) is obviously satisfied and condition (8.3.2) is a well known theorem of M.Artin, cf. [**?**], §5.

We take for sheaf A the direct image by the map $\pi : X \to X/G$ of the constant sheaf $\mathbf{Z}/p\mathbf{Z}$, i.e. $A = \pi_*(\mathbf{Z}/p\mathbf{Z})$; we have $H^j(A) = H^j(X, \mathbf{Z}/p\mathbf{Z}) = H^j(X)$, cf. [11, §5]. There is a natural action of G on A, coming from the action of G on the variety X.

We take for sheaf B the constant sheaf $\mathbf{Z}/p\mathbf{Z}$ on X^G "extended by zero on $X/G - X^G$ " (direct image by the inclusion[5] $X^G \to X/G$); we have $H^j(B) = H^j(X^G)$. The sheaf B is constant (in the sense of 8.1) : the group G acts trivially on it.

There is a natural surjection $A \to B$. Its kernel I is free in the sense of §8.1. This is checked "fiber by fiber"; if x is a geometric point of X/G, and x belongs to X^G, the fiber of I at x is 0; if x belongs to $X - X^G$, the fiber of I at x is a free R-module of rank 1.

We can now apply Proposition 8.3.3 and Proposition 8.3.4. They give the two parts of Theorem 7.5.

Remark. The same proof applies in the usual context of sheaf theory, provided that the space X/G has finite cohomogical dimension (so that (8.3.2) holds). It also applies in a combinatorial context, with cohomology replaced by homology; this was already mentioned in [**?**], proof of Prop.2.10.

References

[1] Artin, M. Dimension cohomologique: premiers résultats. In SGA 4, vol.3, Lect. Notes in Math. **305** (1973), pp. 43-63.

[2] Ax, J. The elementary theory of finite fields. Ann. Math. **88** (1968), 239-271.

[3] Borel, A. Nouvelle démonstration d'un théorème de P.A.Smith. Comment. Math. Helv. **29** (1955), 27-39 (= Oe., vol.I, n°34).

[4] Borel, A. Injective endomorphisms of algebraic varieties. Arch. Math. **20** (1969), 531–537 (= Oe., vol.III, n°83).

[5] Bourbaki, N. Algèbre Commutative. Chapitre V. Entiers, Hermann, Paris, 1964.

[6] Cartan, H. and Leray, J. Relations entre anneaux de cohomologie et groupe de Poincaré. Colloque de Topologie Algébrique, Paris, CNRS (1947), pp. 83-85; see also H.Cartan's Oeuvres, vol.III, pp. 1226-1231.

[7] Carter, R.W. Simple Groups of Lie Type. John Wiley & Sons, London-New York-Sydney, 1972, Pure and Applied Mathematics, vol. **28**.

[8] Colmez, P. and Serre, J-P. Grothendieck-Serre Correspondence. A.M.S. - S.M.F., 2004.

[9] Grothendieck, A. Sur quelques points d'algèbre homologique. Tôhoku Math.J. **9** (1957), 119-121.

[10] Grothendieck, A. Eléments de Géométrie Algébrique (rédigés avec la collaboration de J.Dieudonné). IV. Etude Locale des Schémas et des Morphismes de Schémas (Troisième Partie), Publ. Math. I.H.E.S. **28** (1966), 5-255.

[11] Grothendieck, A. Foncteurs fibres, supports, étude cohomologique des morphismes finis. In SGA 4, vol.2, Lect. in Math. **272** (1972), pp. 366-412.

[12] Illusie, L. Miscellany on traces in l-adic cohomology: a survey. Japanese J. Math. **1** (2006), 107-136.

[13] Illusie, L. and Zheng, W. Odds and ends on finite group actions and traces. Preprint, 2009.

[5] The natural map $X^G \to \pi(X^G)$ is a homeomorphism for the étale topology (it is even an isomorphism of schemes if p is distinct from char k); hence we may identify X^G with its image in X/G.

[14] Kraft, H. Challenging problems on affine n-space. Sém. Bourbaki **802** (1994-1995), Astérisque **237** (1996), pp. 295-317.
[15] Kraft, H. and Popov, V.L. Semisimple actions on the three-dimensional affine space are linear. Comment. Math. Helv. **60** (1985), 466-479.
[16] Laumon, G. Comparaison de caractéristiques d'Euler-Poincaré en cohomologie ℓ-adique, C. R. Acad. Sci. Paris **292** (1981), 209-212.
[17] Lazard, M. Sur la nilpotence de certains groupes algébriques. C. R. Acad. Sci. Paris **241** (1955), 1687–1689.
[18] Minkowski, H. Zur Theorie der positiven quadratischen Formen, J. Crelle **101** (1887), 196–202 (= Ges. Abh., Band I, n°VI).
[19] Petrie, D. and Randall, J.D. Finite order automorphisms of affine varieties, Comment. Math. Helv. **61** (1986), 203-221.
[20] Schur, I. Über eine Klasse von endlichen Gruppen linearer Substitutionen, Sitz. Preuss. Akad. Wiss. Berlin (1905), 77–91 (= Ges. Abh., Band I, n°6).
[21] Serre, J-P. Zeta and L-functions, in "Arithmetical Algebraic Geometry" (Proc. Conf. Purdue Univ. 1963), pp. 82–92, Harper and Row, New York, 1965 (= Oe., vol.II, n°64).
[22] Serre, J-P. Complète Réductibilité, Sém. Bourbaki **932** (2003-2004) (= Exposés de Séminaires 1950-1999, 2ème édition, S.M.F., Doc. Math. **1** , 2008, pp. 265-289).
[23] Serre, J-P. Bounds for the orders of the finite subgroups of $G(k)$, in "Group Representation Theory" (edit. M.Geck, D.Testerman & J.Thévenaz), E.P.F.L. Press, 2007, pp. 405–450 [available on http://www.college-de-france.fr].
[24] Smith, P.A. A theorem on fixed points for periodic transformations, Ann. Math. **35** (1934), 572–578.

Jean-Pierre Serre
Collège de France
3, rue d'Ulm, F-75005 Paris