JEAN-PIERE SERRE LECTURES

GABRIEL C. DRUMMOND-COLE

1. March 4: A lecture on finite group theory I and II

[Welcome to POSTECH. It's my great honour and pleasure to introduce Prof. Jean-Pierre Serre. He'll stay here until next Friday. He'll deliver six hours of lecture. Today the topic chapters in finite groups. Let's welcome him.]

Thank you very much for the invitation. I've selected my favorite chapter in finite group theory. It will take some time. I don't want to make an interruption after one hour.

We start with Jordan, around 1870, who said, you have G a finite group with a subgroup H in G, and you call n the index of H in G which is at least 2. Then you have an action of G on $X = G/H$ transitively. Now if you have an element $g \in G$, you can look on its action on X, and the theorem of Jordan is

Theorem 1.1. *(Jordan) There exists at least one element $g \in G$ which has no fixed point on X, it moves everything.*

The typical example of that, take G the symmetric group S_3, for H the symmetric group S_2. The quotient has three points. You can fix everything, you can swap two, but you have the cyclic permutation.

It's good to rewrite this theorem in terms of H. If you let $x \in X$, the subgroup of G fixing x is a conjugate of H. That is, it is a group of the form gHg^{-1}. Why? It's true for the unit element of g.

So then we can rewrite:

Theorem 1.2. *(Jordan) There exists $g \in G$ which is not conjugate with any element of H.*

In formulae, you could say, take the union over all $g \in G$ of gHg^{-1}, that's a union of subgroups of G, and the theorem is that this is not G. If you had it in this way, the proof is practically in the picture. Look at the situation. If you modify g on the right, writing it gh, you find that $ghHh^{-1}g = gHg^{-1}$. So these conjugates are parameterized by G/H. You have n such subgroups, each of which has the same number of elements $|H|$. So you can count the union, very roughly, by saying, I have n things with that many elements, so the total number is at most $n|G/H| = G$, but these have one point in common, namely 1, and you should say the following. Inside the set $G - 1$ you have the union $gHg^{-1} - 1$,a nd now if you count them, you find $n(|H| - 1) = |G| - n$. But the union was contained in $G - 1$ which has order $|G| - 1$. So you win, because you find that $|G - \cup_{g \in G} gHg^{-1}| \geq n - 1$.

That is the proof. Now a comment, this has a good point and a bad point. What is the good aspect of Jordan's theorem? It is very useful when you do Galois theory. You have equations, geometric problems and you're interested in knowing what the Galois group H is. There are usually obvious possibilities. Maybe you have an irreducible polynomial of degree n. So then the group is contained in S_n. You have some idea that it is in fact equal. If you could construct elements in the Galois group, then you could do it. Usually the information you have is that some conjugacy classes are in H.

Suppose you work over $\mathbb{Q}$, you can go to a finite field and the Galois group is simpler. The Galois group in characteristic p embeds in the Galois group of characteristic zero. So you just need to see that H contains an element of each conjugacy class. For example in elliptic curves, you look at Galois groups of division points.

What's the negative aspect? In character theory of finite groups, you want to make a list of finite characters. If you were working with Lie groups, the situation would be much easier. If you were working with the unitary group over $\mathbb{C}$, in that case, the maximal torus, every conjugacy class intersects T^n. So the character theory of Lie groups is easier because you can study it on Abelian subgroups. The Jordan theorem tells you that for finite groups you need at least two.

As an exercise, for GL_2 of a finite field, construct two subgroups, proper, which together intersect every conjugacy class. That is the Jordan theorem.

Now we are going to make it slightly more complicated, more precise. Let G, H, X, and n be as before. For the more refined form we will ask more of G, that the order of G is a power of a prime number. If you look at the action of G on X, we want that each orbit has order a power of p not equal to 1. That looks rather, I'll explain what is the reason to ask that.

Theorem 1.3. *(Fein, [illegible]) Refined form*

This is a result of 1981, and relies on the classification of finite simple groups, a list of all simple finite groups, namely $A_n, n \geq 5$, the algebraic groups $PSL_2(\mathcal{F}_p), p \geq 5$ (and some similar things) and 26 sporadic groups. The proof was announced in 1980. People are still working on writing a connected linear proof.

Any proof in mathematics should be written linearly so that any piece relies on any previous piece. It's not written like that yet. It's several thousand pages. For instance, it was discovered that there was a gap, and people fixed the gap but they did it by writing a book of length 1600 pages. They told me when I was giving them trouble [unintelligible]. But it's worse than that.

So you reduce to the case where G is simple. You may assume H is a maximal subgroup. If you really knew the simple groups one by one and their maximal subgroups, you'd win by checking. They do the checking for algebraic groups, but for the sporadic groups they say it depends on published and unpublished properties af the sporadic groups. I suppose most of those unpublished properties have been published.

In certain situations it's usual to say that it depends on the classification. But experts believe that the classification is correct.

What are the consequences of the refined form of Jordan's theorem?

There are consequences related to number theory. Number fields are finite extensions of $\mathbb{Q}$. Let L/K be a finite extension of degree at least 2 of algebraic number fields. Then there is a norm map $L^\times \to K^\times$. We're interested in the cokernel. $K^\times/NL^\times$. The theorem is that this cokernel is infinite. I'm not going to give the proof. In fact this is equivalent to the refined form.

You have K and L and L is not Galois, so you take a Galois extension E, and so you have the Galois group G and the group H. Then you get that a group must be infinite because otherwise they would coincide.

Another theorem has to do with $Br(K) \to Br(L)$ and the kernel is infinite, and this is also infinite. This is also equivalent.

So these for now rely on the classification of finite simple groups.

Now, are there questions? I would be happy to answer questions during the lecture.

This story was based on some inequality, which I'm going to write,

$$|G| - |\cup g \in GgHg^{-1}| \geq n - 1$$

where $n = (G : H)$.

2. Frobenius groups

The next question is when you have equality? Certainly $H \neq G$, but I also don't want $H = 1$. So the proof was by looking at the conjugates, and you see that if the subgroups intersect more than at 1 you get a strict equality. So equality in the formula is equivalent to $H \cap gHg^{-1} = 1$ if $g \notin H$. Again let X be G/H. On X this condition is equivalent to the only element of G which fixes two points is the identity. Then we will have the division of G in three pieces. There is 1, which fixes everything, the elements conjugate to H, which fix one point, and the rest, which fix zero points.

We need to see examples. The smallest example is $G = S_3$, $H = S_2$, and X three points. The unit element fixes three points. Transposition fixes one point, and the cyclic permutation, two of them, and they fix no points. There is another easy-to-visualize example, which is the following. Take k a finite field, and for X take k itself. For G take bijections $X \to X$ of the form $x \to ax + b$ where $a \neq 0$ and $b \in k^+$. What is H? It's the ones that fix zero, its $x \mapsto ax$. If $|k|$ has q elements, then $k^\times$ has $q-1$ elements and k^+ has q elements, so G has order $q(q-1)$ and H has order $q - 1$. The conditions are fulfilled. If $a \neq 1$ then you have $x = ax + b, x = \frac{b}{1-a}$. If $x = 1$ then you have no solutions unless $b = 0$.

In this example there is another subgroup which is important. This is the subgroup A made up of $x \mapsto x + b$. This is a *normal* subgroup in G. If you look at the way the group acts, you see that every element of G can be written in AH in a unique way, it's a semidirect product. The intrinsic definition of A is that A is the set of $g \in G$ which have no fixed point and of course you have to add the element 1.

So that brings us to the next theorem.

3. Frobenius theorem

This tells you that the example I gave to you is essentially the only one.

More precisely, suppose $H \subset G$ and assume $H \cap gHg^{-1} = 1$ for all $g \notin H$. Some people call this the trivial intersection property, which is reasonable because it is as small as can be. Then we can try to mimic the construction by defining A. We want this to be a subgroup, so we define $A = 1 \cup \{\text{all elements not conjugate to} h \in H\}$.

As a formula it looks a bit bad but it's like

$$A = 1 \cup (G - \bigcup_{g \in G} gHg^{-1}).$$

It's a little strange, you're picking those elements that fix everything or nothing.

The beautiful theorem of Frobenius is that A is a subgroup of G. I don't remember the date exactly but it must be around 1905 or 1906. Once you know it is a subgroup it's obvious that it is a normal subgroup. It's stable by conjugation. It's easy to compute the order, and then you check that G is a semi-direct product of A and H.

The proof uses character theory. Frobenius had invented character theory around 1900 and he realized consequences purely in terms of the group structure. This was the most remarkable application.

Let me tell you the idea. I'm assuming you know a little about characters of finite groups. The main step is the following. Construct a homomorphism $G \to GL_n(\mathbb{C})$ with the property that its kernel is A. If you do that you win because the kernel is a normal subgroup. You start from a homomorphism $H \to GL_n(\mathbb{C})$ which is faithful, the kernel is trivial, and show that it can be extended to G in such a way that it is trivial on A. A faithful representation is easy to give, the regular representation is faithful. It's a reasonable theorem. If you believe in the theorem, then G/A is H so any representation of H should give you one trivial on A. You don't construct the representation because that is something that no one knows how to do. You can construct the character, which is the trace function, and the trace is a function on H, the trace of $\rho(h)$ is $f(h)$ where $f : H \to \mathbb{C}$ is the so-called character of ρ. We have no problem to extend it to G. You extend it to G. You have to define $F : G \to \mathbb{C}$ which has to be a class function. W want $F|_H = f$ and $F(a) = n$ if $a \in A$. For $g = 1$ you have to put $F(1) = n$. If g is conjugate to h, you put $F(g) = f(h)$. If g is not conjugate, then $F(g) = n$. You have to prove that this is not ambiguous. This makes sense for any class function.

So next we introduce the scalar product of characters. If you have f_1 and f_2, then the scalar product is

$$\langle f_1, f_2 \rangle_G = \frac{1}{|G|} \sum_{g \in G} f_1(g) f_2(g^{-1})$$

If we have $f \mapsto F$, then it's easy to check that

$$\langle f_1, f_2 \rangle_H = \langle F_1, F_2 \rangle_G.$$

It's a little computation. Next step, you show that, you want to see that $\langle F, \chi \rangle_G \in \mathbb{Z}$. You do this by showing this is related to $\langle f, \chi|_H \rangle$. This means that F is a linear combination with integer coefficients η_i of characters.

Now the next step is that if you start with an f which is a character of an irreducible character of H, then F is the character of an irreducible character of G.

We know that F is a linear combination of characters with linear coefficients. You compute $\langle F, F \rangle = \sum \eta_i^2$. On the other hand this is $\langle f, f \rangle = 1$. This implies that all η_i are zero except one which is ± 1.

It cannot be minus because it is positive on 1. So it is +1. Then by linearity you get it for every reducible representation.

So we proved that the extension is really a character. So you have $\rho_G : G \to GL_n(\mathbb{C})$. We know that the trace of $\rho_G(a)$ is n. But this is the sum of the eigenvalues λ_i. This is only possible, with these roots of unity, for the sum to be n, if they are all 1. Then we are finished. We have constructed the representation we wanted.

So that is the proof.

I will speak more on the representations of finite groups for my last lecture here.

4. The structure of Frobenius groups

We have $G = A.H$, and A is called the Frobenius kernel, it's the one that is invariant, and H is the Frobenius cokernel. You have to remember the example where $G = ax + b$ and A was the additive group and H was the multiplicative group. Now the first thing to do is to look at the Frobenius kernel A. I told you that G is a semi-direct product. If you start with a group A and a group H acting by automorphisms on A, then you can always make a semidirect product $G = A.H$. When is it true that $A = 1 \cup (G - \bigcup_{g \in G} gHg^{-1})$. The answer is an exercise in group theory. It's true when H acts freely on $A - \{1\}$. That means that if you write this action in exponential form $a \mapsto {}^{h}a$. Then ${}^{h}a = a$ implies $A = 1$ or h is 1. So this is what happens in the $ax + b$ group.

This will give us a property of A. We assume always that H is not 1. Then select $h \in H$ of order a prime power. We can always do that because H is not 1. Then we will find an automorphism σ of A with the property that it fixes essentially nothing. We know that $\sigma(a) \neq a$ for all $a \neq 1$. This is called a fixed-point free action sometimes, I don't use that because it's wrong.

So we get a property of the Frobenius kernel, which is, there exists an automorphism σ of A of prime order p with no fixed point except the identity. Conversely, that characterizes Frobenius kernels, because if you have such an A you can take the semi-direct product with a cyclic group.

People looked at examples and [unintelligible].

So people looked at, well, for $p = 2$ you have A is Abelian of odd order and $\sigma(a) = a^{-1}$. So for $p = 3$ the group A is a central extension of two Abelian groups. This was Burnside.

For $p = 5$, if I remember correctly the nilpotence class is 6. All this suggests a theorem that was not proved until much later.

Theorem 4.1. *(J. G. Thompson's thesis) A Frobenius kernel A is a nilpotent group.*

At the time it was enough to prove that it is solvable. This thesis was, I'm not sure, 1960? A few years later he found a proof in four pages. He was disappointed.

This is all I want to say about Frobenius kernels.

There are many interesting things to say about Frobenius cokernels.

5. Frobenius complements H

There is in fact a complete classification. The main theorem is

Theorem 5.1. *For a group H, the following properties are equivalent:*

1 *H is a Frobenius cokernel,*

2 *there exists a linear representation over $\mathbb{C}$, $H \mapsto GL_N(\mathbb{C})$ for $N \geq 1$, such that the action of H on $\mathbb{C}^n - \{0\}$ is free (we call such a thing an almost free action),*

2' *there exists a linear representation that is irreducible and almost free,* *2" there exists an irreducible linear representation valued in k where the characteristic of k does not divide $|H|$ (independent of k),*

3 H can act on a sphere S_{N-1} freely, by orthogonal transformations, and

3' H is the fundamental group of a compact Riemannian manifold of constant positive curvature.

This is the reason these groups are studied, Riemannian geometers like these spaces. Constant curvature that is zero is flat.

If you take for k the real numbers, you'll find something basically in the orthogonal group, so $3''$ is the same as $2''$ with $k = \mathbb{R}$. If you take them simply connected it's a sphere and so if you mod out by a group action you get one of these groups.

Some of the arguments are quite amusing, so let me talk about them. As your questions show, the main thing is to show independence of k.

6. Independence of k

First, we should show that it depends only on the characteristic of k. Suppose that you know it for $\mathbb{Q}$ then you know it for an arbitrary field of characteristic zero, because you extend your scalars, $GL_N(\mathbb{Q}) \subset GL_n(k)$. Not having 1 an eigenvalue is stable under extension.

For the reverse, you have a vector space over k of finite dimension and an almost free action on V. You want to find one over $\mathbb{Q}$. You take a nonzero vector in V, it has only finitely many transforms, and take the sum $\mathbb{Q}hv$. Then this is finite dimensional over $\mathbb{Q}$. You have an obvious action. The dimension will increase. The dimension is not fixed. That argument shows that for every characteristic, it's enough that you prove it for $\mathbb{Q}$ and $\mathbb{F}_p$.

So now I have to show that $\mathbb{Q}$ implies $\mathbb{F}_p$ and vice versa.

If you have it over $\mathbb{Q}$, you take $e \in V$ nonzero, then make the lattice generated over $\mathbb{Z}$ by the transforms He. This is a free Abelian group which is stable under H. So you replaced $GL_n(\mathbb{Q})$ by $GL_n(\mathbb{Z})$. Now that gives you, for $H \mapsto GL_n(\mathbb{Z})$, that maps to $GL_n(\mathbb{F}_p)$. Because the condition that p does not divide the characteristic, the eigenvalues reduce faithfully in characteristic p. So you win. That gives you $\mathbb{Q}$ to $\mathbb{F}_p$. The other direction is much more amusing. There is no chance you can prove it directly. You know very well you cannot lift from characteristic p to characteristic 0. So you use the p-adic integers. These are the limit of $\mathbb{Z}/p^n\mathbb{Z}$. So a p-adic integer is a family $x_n \in \mathbb{Z}/p^n\mathbb{Z}$ which play nicely by modding out by $p^{n-1}\mathbb{Z}$.

So first write it on a smaller field than the complex numbers.

We have $\rho : H \to GL_n(\mathbb{Z}/n\mathbb{Z})$. Can we lift this to $GL_N(\mathbb{Z}/p^2\mathbb{Z})$? Well, cohomology tells us that there is an obstruction, there is an element of a cohomology group that is against you. It lies in $H^2(H)$ with coefficients in the kernel of the map $GL_N(\mathbb{Z}/p^2) \to GL_N(\mathbb{Z}/p)$. These are matrices, $N \times N$ with coefficients in $\mathbb{F}_p$. This is an Abelian group of order p^{N^2}. The main thing is that it is prime to $|H|$. Now it's a basic fact in group cohomology that if the group of coefficients and the order of the group are relatively prime, the cohomology is zero. So you can lift.

And now of course you can lift to $\mathbb{Z}/p^q$. So you lift inside and get a lift $\rho_\infty : H \to GL_N(\mathbb{Z}_p) \subset GL_N(\mathbb{Q}_p)$, the field of fractions where you add $\frac{1}{p}$. The initial action was almost free, and so then you are almost free in characteristic of zero, so we know it's true over $\mathbb{Q}$. So you get the p-adic and then down to $\mathbb{Q}$. That is essentially the proof.

I don't want to give you the classification, but it's mainly based on the proof, the properties of the characters of the group. I can telly ou immediately from a character table if it's there or not by seeing the eigenvalues.

The end result is, there are several properties of H which are necessary, not necessarily sufficient.

7. Properties of H

- There should be at most 1 element of order 2.
- Abelian subgroups are cyclic. It's easy to see. An Abelian group, you can just look at the representations, they're order one.
- Subgroups of order pq for p, q, prime, are cyclic. This also implies that p-Sylow subgroups are cyclic.

At the end he shows that these groups are almost solvable, but not quite.

Theorem 7.1. *(Wolf) Either H is solvable or it has a subgroup H' of index* 1 *or* 2 *which is isomorphic to the direct product of a solvable group with $SL_2(\mathbb{F}_5)$ (the so-called binary icosahedral group).*

The icosahedron has symmetries $A_5 = PSL_2(\mathbb{F}_5)$, and if you lift that to SL_2, that acts on a space of dimension three, almost freely.

Let me come back to the point of view of Riemannian geometry. People were interested in S_{N-1} and you wanted to have H acting freely by orthogonal transformations, the same as keeping the metric fixed.

Now the topologists want more groups than that. They would like like it to be an action by homeomorphisms of S_{n-1}. That means the fundamental group of a manifold (a topological manifold) with universal cover a sphere. It's not at all obvious that you get more groups. When I was a beginner you didn't have counterexamples. Then it turned out that, it was a very difficult piece of work, Madson, Thomas, [illegible], they characterized those H which satisfy the toplogists' conditions. Here H should satisfy:

1. Abelian subgroups are cyclic, and
2. either 0 or 1 elements of order 2.

Take the group, take $21 = 3 \times 7$, and $3 | (7 - 1 = 6)$. So you can make a Frobenius group of order 21 by taking a cyclic group of order 7 semidirect product with a cyclic group of order 3. So there is no element of order 2 and all Abelian subgroups are cyclic. There is a p, q condition for the geometers and that was not satisfied.

You are probably tired.

8. March 10: Cohomological invariants and trace forms (I)

Thank you, good evening, and I will start by recalling things from toplogy, because it is first in topology that cohomological invariants appear.

Suppose you have a topological space X and a vetor bundle (for example the tangent bundle if X is a manifold). Let V be an n-dimensional (to make things precise, complex) vector bundle over the base X.

Then you have the so-called Chern classes, I will assume you know cohomology, in $H^{2i}(X, \mathbb{Z})$, they are called $c_i(V)$. What are the properties they have?

They are discrete invariants; if you deform V continuously they don't change. I should also say that $c_i = 0$ if $i > n$.

They are functorial in the following sense. Suppose you map $X \to Y$ and you have a vector bundle V_Y over Y, then you can pull it back to define one (V_X) over X. If you look at the Chern classes $c_i(V_X)$ and $c_i(V_Y)$, if I call the map φ, then

$$c_i(V_X) = \varphi^* c_i(V_Y).$$

As you know, these are used in differential geometry to describe invariants. When you find an invariant that is an integer, you think that they can be described in terms of Chern classes.

I should take a good category of spaces, like finite complexes. I will call this category $\mathcal{T}op$, which is a category of topological spaces (which are finite complexes) with morphisms continuous maps up to homotopy.

On the other hand, we have, if you take an X, we can define $Vect(X)$ to be the isomorphism classes of vector bundles (of dimension n). I can view that as a functor $Vect_n$ from the category $\mathcal{T}op$ to the category $\mathcal{S}et$. On the other hand I have cohomology, which goes from $\mathcal{T}op$ to Abelian groups.

What do the Chern classes do? They go from the first functor to the second functor. Maybe Chern proved this, I'm not sure.

Theorem 8.1. *The only morphisms of functors between $Vect_*$ and Coh are the polynomials in the Chern classes with coefficients in $\mathbb{Z}$.*

It is in that sense that the Chern classes give you everything. Now you think, maybe you can change this and take different morphisms.

Vector bundles can be viewed in a different way, you can think of fiber spaces, and also principal fiber spaces. When you have a vector bundle of dimension n over X, you can make a new bundle in the following way. For every point $p \in X$, you choose a basis of the fiber of V_p and look at all possible bases. So call this P, for principal. This is again a bundle over X. Now it has an action of $GL_n(\mathbb{C})$. That action is such that the group acts transitively and freely on the fibers. If you change the basis, there is only one element that takes you from one to the other.

So that is a principal bundle, you have an action of a group which acts freely with fibers as orbits. Such things can be described in general by what is called non-Abelian cohomology, $H^1(X, G)$. Roughly you do this by taking a covering of X on which the bundle is trivial, you look at a change of basis which depends on two parameters, and so on.

A general problem you can ask is to choose any group now, any topological group G and you'll have a functor just like $Vect_n$, but you'll have a functor from $\mathcal{T}op$ to $\mathcal{S}et$ which attaches to X to the set $H^1(X, G)$. You can ask for a functor into cohomology, making invariants for a principal bundle. If you take G to be the orthogonal group $O_n(\mathbb{R})$ or $O_n(\mathbb{C})$, you get orthogonal bundles. In the first case if you take cohomology modulo 2, you get invariants like the Chern classes, called the Stiefel–Whitney class, where $w_1 = 1, \ldots, w_i \in H^i(X, \mathbb{Z}/2\mathbb{Z})$ with $w_i = 0$ for $i > n$, and it's a theorem (probably of Whitney)

Theorem 8.2. *Every morphism from $H^1(\quad , G) \to H(\quad , \mathbb{Z}/2\mathbb{Z})$ are the polynomials in the Stiefel–Whitney classes.*

Now I want to go to algebra and algebraic geometry. I'm going to put the corresponding functor, well, due to Hilbert–Hurwitz, we'll get a correspondence between a lot of different [unintelligible]. I'll start with a field of characteristic other than 2. We'll relate about 6 different objects.

(1) a curve in $\mathbf{k}$, projective, connected, smooth, of genus 0.
(2) A quadratic form $q$in three variables, coefficients in $\mathbf{k}$, non-degenerate, of discriminant 1 (that is if you write it $(ax^2 + by^2 + cz^2$ then $abc = 1)$.
(3) A quaternion algebra with center $\mathbf{k}$. (This has i, j with $i^2 = \alpha$, $j^2 = \beta$ and $(ij)(ij) = -\alpha\beta)$, with $\alpha, \beta \in \mathbf{k}^\times$
(4) An element of $H^1(\mathbf{k}, PGL(2))$
(5) An element of $H^1(\mathbf{k}, SO_3(q))$
(6) An element of $Bra(\mathbf{k})$

How do these look? If you have a quadratic form in three variables, you write $F(x, y, z) = 0$ and this defines a conic in the plane. This is certainly a curve of genus zero, smooth and so on.

An element can be written $q = x_0 + x_1 i + x_2 j + x_3 ij$. Then the norm of q is $x^2 - \alpha x_1^2 - \beta x_2^2 + \alpha\beta x_3^2$. You set $x_0 = 0$ and that gives you something of discriminant one.

If you know about sheaves and cohomology, you take the sheaf called the invertible sheaf L. From L you take the tangent bundle, of degree 2. When I have a sheaf, I can take the sections of the sheaf, $H^0(X, \underline{L})$, and the dimension of the space has dimension 3 Whenever you take a basis, you get a map from X to the space $\mathbb{P}_2$.

Now I have to explain a little more about these things.

What about the Brauer group? Take all algebras over $\mathbf{k}$ of finite dimension and with center $\mathbf{k}$, that are simple. The tensor product has this property. You can say that A and A' are equivalent if $A \otimes M_n \cong A' \otimes M'_n$. If you do that, you get a group, the algebars with respect to, the zero element, do you write it additively or multaplicitivity. So let 0 be the class of matrix algebras. Then the Brauer group of $\mathbf{k}$ consists of $\mathbb{H}^2(\mathbf{k}, \mathbb{G}_*)$. What is Br_2? It's the subgroup killed by unintelligible.

Let's explain what it means in general, $H^i(\mathbf{k}, G)$ with G Abelian and G being an algebraic group.

Here $\mathbb{G}_m$ is the multiplicative group.

Choose a separable closure. Then that Galois group which is a profinite group, a limit of finite groups, you take the cohomology (in dimension i), and you get $H^i(Gal(H/K), G(K))$. Take the direct limit and you get the cohomology. So what about $H^0(\mathbf{k}, F)$? This is $G(k)$. It's not obvious that you are in this same world, but it turns out that $H^1(\mathbf{k}, G_*) = 0P$. Then $H^2(\mathbf{k}, b_n)$ is isomorphic to $Br(2)$

There are a couple of ways of attacking $H^1(\mathbf{k}, PGL_2)$. Let me start with the one that gives the answer but not the explanation. Look at the maps from Γ to $G(\mathbf{k})$. Call this map a so that $\gamma \mapsto a_\gamma$. You want these to be cocycles. So $a_{\gamma\gamma'} = a_\gamma(a'_\gamma)$. Now if you have two cocycles a and b, you have to say when a is equal to the degree and that happens when there exists $g \in \mathbf{k}$ such that $b_\Gamma = g^{-1} a_\Gamma \gamma(g)$.

Let me give an alternate way, more geometrically. You consider P a principal homogeneous space over $G(K)$. So P is a set on which $G(K)$ acts. It's convenient to make it act on the right, but it's just a matter of convenience, so if I have an element $g \in G(K)$ and $p \in P$, then I move to pg. So it acts freely and transitively.

Also I want an action (on the left) on P of $\Gamma_{K/k}$. So I think I have not forgotten any, no, I think there no condition, I may have forgotten one thing. This is called a torsor, a twisted thing. I told you for the vector bundle sometimes it's better to [unintelligible]. So then $H^1(K/k, G)$ is the set of equivalence classes of such torsors.

The proof that it is the same as the one with cocycles is extremely easy. You take a point, and transform it by Galois. You get another point, and there's a g that [too fast].

There is a case where this doesn't say anything at all, if $\mathbf{k} = \mathbb{C}$ then all of these are 0, or if $\mathbf{k} = \mathbf{k}_s$. It's more amusing to look at $\mathbf{k} = \mathbb{R}$. Now the quadratic forms, there are two possibilities, I could have $x^2 + y^2 + z^2$ or I could have $x^2 - y^2 - z^2$. I get two conics, one with no points and one which is standard. You get two possibilities for the quaternions, similarly. For the twisted cohomology, there $K = \mathbb{C}$ and $\mathbf{k} = \mathbb{R}$. Then you want to solve these equations over here [indicating].

So let me go back and get two functors and get the morphisms between the two functors.

Let $\mathbf{k}_0$ be the ground field. I'll assume the characteristic is not 2. The category is field extensions of $\mathbf{k}_0$. The functor, the most general case is the following. Choose an algebraic group G and consider the functor $H^1(\quad, G)$ which maps $\mathbf{k} \mapsto H^1(\mathbf{k}, G)$. I'll be happy to explain the case where G is a finite group, and even more specially $\mathbb{S}_n$. That will be the first functor. The second functor will be $H : \mathbf{k} \to H^i(\mathbf{k}, K)$ for an Abelian group C, which for me today will be $\mathbb{Z}/2\mathbb{Z}$.

I'll take the case S_n. I want to explain first what is exactly the functor $H^1(\quad, S_n)$. The nice thing about S_n is that this is a 0-dimensional space. Then $S_n(K)$ is just a set. Then the equality we have is a homomorphism because there is no action of γ on $a_{\gamma'}$. So a cocycle is a map $a : \Gamma \to S_n$. Two cocycles are homologous if they are conjugate. So you are looking at the conjugacy classes of maps to S_n.

I need the notion of an Etale algebra of degree n. This will be a commutative algebra $E/\mathbf{k}$ of degree n (its dimension as a vector space) and I want it as nice as possible. Assume that after field extension, it becomes split, $\mathbf{kk}$.

It is well-known in Galois theory that if $K/\mathbf{k}$ is a separable extension of degree d^3m, then it is an algebra of rank m. One proves that every étale is a product where each factor is a field.

Now extend E, one can prove that $E \otimes_{\mathbf{k}} \mathbf{k}_s$ is $\mathbf{k}_s \times \mathbf{k}_s$. In this way you receive a homomorphism $\Gamma_k \to S_n$, φ_E, defined up to conjugation. This is not stated this way but this is Galois theory. An etale algebra of rank n is the same as a homomorphism $\varphi_E : \Gamma_k \to S_n$. If E is a field then $\varphi_E(\Gamma_{\mathbf{k}})$ acts transitively on [illegible].

Okay, so now what will be the next [unintelligible]? It will be to consider the category $Field/\mathbf{k}_0$, the two functors $H^1(\quad, S^n)$, that is, etale algebras of rank n, and the other will be $H^*(\quad, \mathbb{Z}/2\mathbb{Z})$. The morphisms between these two will be the invariants.

Theorem 8.3. *These invariants are a free module over the $H^*(\mathbf{k}, \mathbb{Z}/2\mathbb{Z})$ with basis Stiefel–Whitney classes $w_0, \ldots, w_m$ where m is the integral part of $n/2$.*

Explaining this will be what we do next time. It's rather remarkable that they only go halfway.

9. March 13: Linear representations of finite groups (colloquium)

Welcome to the first colloquium of the spring semester. It's my great honor and pleasure to introduce Jean-Pierre Serre.

I plan to do

(1) the standard things, starting over $\mathbb{C}$, and then

(2) over characteristic p, where it becomes a little different, you have the so-called Brauer characters, and then
(3) characteristic p from the point of view of homotopy theory, and finally
(4) in characteristic "1".

9.1. So let G be finite and consider $\rho : G \to GL_n(\mathbb{C})$. Then the character of ρ is the trace of $\rho(g)$, this is denoted χ. It's better to think that $G \to GL_n(V)$ where V is a finite dimensional space.

If you know χ_V you know ρ. That is, $\rho_1 \cong \rho_2$ if and only if $\chi_1 = \chi_2$. You'll have the same thing for infinite groups provided the representations are semisimple, which means the direct sum of irreducible representations.

The normal tools that you use to prove this does not apply to infinite groups so it's a bit surprising, but the true form of this has to do with algebras. If you have A a **k**-algebra (in characteristic 0), and V is an A-module, finite dimensional over **k**, then V_1 and V_2 are isomorphic if and only if they have the same trace.

After that the next step is to give:

9.2. properties of these characters.

(a) There is an orthogonality formula

$$\frac{1}{|G|}\sum_{g\in G}\chi_1(G)\chi_2(g^{-1})$$

for χ_i irreducible, is 0 for $\chi_1 \neq \chi_2$ and 1 if they coincide.

(b) A character is a class function:

$$\chi(x) = \chi(gxg^{-1})$$

b_1 The irreducible characters form a $\mathbb{C}$-basis of class functions (valued in $\mathbb{C}$).

Let $R(G)$ be the $\mathbb{Z}$-linear combinations of characters. If χ is a character then $n\chi$ is a character, $\chi_1 + \chi_2$ is a character. An element of $R(G)$ is sometimes called a *virtual character*. If you take the point of view Grothiendieck style, then $R(G)$ is the Grothiendieck group of the category of representations of G.

This means that the Grothiendieck group, to every V you attach $[V] \in R(G)$, and to every exact sequence $0 \to V_1 \to V_2 \to V_3 \to 0$ you get the equality $[V_2] = [V_1]+[V_3]$.

This is not just a group, it is also an algebra, because if V_1 and V_2 are representations, so is their tensor product, and its character is the product of their characters.

But $R(G)$ has more structure than that.

c There are λ^i operations. If V is a representation of G, you can use the exterior powers $\bigwedge^i V$. So you get operations $\lambda^i : R(G) \to R(G)$ which cannot be reduced to the tensor product.

These operations are related to the so-called Adams operations Ψ. These are defined $\Psi^n f(g) = f(g^n) - f(g)^n$.

Let me take the example of $\lambda^2\chi$. Then $\chi(g)$ is the sum of eigenvalues of g in the corresponding space V. Then

$$\lambda^2\chi(g) = \sum_{i<j}\lambda_i\lambda_j.$$

You can also compute $\chi^2(g)$,

$$\chi^2(g) = \lambda_1^2 + \cdots + \lambda_n^2 + 2\sum_{i<j}\lambda_i\lambda_j$$

So we've proved

$$\chi^2 = \psi^2\chi + 2\lambda^2\chi.$$

So these are especially useful when n is prime to the order of G because then $\Psi^n(g) = \sigma_m\chi(g)$. Let's choose N to be the order of G and call A_n the ring over $\mathbb{Z}$ generated by Nth roots of unity.

This is free over $\mathbb{Z}$ of rank $\psi(N)$. You have the action of the Galois group which is well-known to be $(\mathbb{Z}/n\mathbb{Z})^\times$. So σ_t of a root of unity z is z^t. Then the formal is the sum of λ_i^m.

So let me put $R(G)$ inside $R'(G)$, the ring of all class functions $G \to A_N$ with the property $\psi^m(f) = \sigma_m(f)$ for all m prime to N. You can easily prove that $R(G)$ contains $NR'(G)$.

You can prove also, you can write $\Psi^p\chi(g) \cong \chi(g)^p \mod pA_N$. The smaller thing is inside that ring, do that for every prime p. Then it becomes really close.

For those of you who do algebraic geometry, if you are interested in such questions, it's interesting to write *Spec* $R(G)$. I cannot resist describing, for $G = S_3$, we have three classes. It turns out that if you write $R'(G)$ that will be rather large, it will be $\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$. I want to write the spectrum of $\mathbb{Z}$ as a line with points the primes. So for $\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$ the spectrum is three lines. You should map to this from *Spec* $R(G)$. The three lines will correspond to the elements of order 1, order 2 and order 3. From this [picture] you see that the spectrum is connected and that reducing modulo anything other than two or three you'll get three irreducible representations.

9.3. characteristic p. If we have $G \to GL_n(V)$, it is not true that it is semisimple. We cannot expect the trace will characterize the modules. more precisely, if you have a module that is not semisimple, you can force it to be by taking the direct sum of the Holder quotients, writing it as $V \supset V_1 \subset \cdots$ and taking the sum of V_i/V_{i+1}.

If I take $V \oplus \cdots \oplus V$ p times, the character is 0, it's multiplied by p. So you need something better than the trace. There are two ways to do it.

The first method (due to Brauer) is to take the characteristic polynomial instead of the trace. Then it is a theorem that two semisimple representations such that the characteristic polynomials of g are the same for all g are isomorphic.

It's a bit disagreeable to calculate the full characteristic polynomial. Brauer lifted not the trace but the eigenvalues. So $\rho(g)$ has eigenvalues $\lambda_1, \ldots, \lambda_n$. In characteristic p there are no roots of unity of order p. So these are roots of unity of order prime to p. They lie in some finite field in fact, in some $\mathbb{F}_q$ for q large. So choose a ring in which [unintelligible] in such a way that you have a cross sectino from $\mathbb{F}_q$, a lifting. You can do that.

So you can lift λ_i^W in W. Then you define the Brauer character by the formula $\sum\lambda_i^W$. You multiply by p but you don't lose information because you're in characteristic 0.

The proof also shows that you need to know $\rho(g)$ only for g of order prime to p. The Brauer character depends only on that. That's very useful.

9.4. Homotopy point of view in characteristic p. The objection to the Brauer method is that you assume the objects are semisimple. Say you have G a p-group. This has only one irreducible representation in characteristic p. The semisimple representations are copies of the one dimensional trivial one, so that doesn't give you very much.

But for G the cyclic group of order p you have a two dimensional representation, and for order three, the Jordan blocks. You'd like to not lose these.

The homotopy method is that you want to neglect something, you want to neglect projective modules (finite dimensional).

Let me remind you that P is projective when it is a direct factor of a free module. In the example, the only projective one is the longest one, the regular one, of dimension p.

I will say that M is homotopic to M' if $M \oplus P \cong M' \oplus P'$ for some projective modules P and P'. This is a general method in a category, you can introduce an equivalence relation like that. The interest in these projective modules here lies in the fact that we switch operations.

Suppose that M is a quotient of a projective. Then the kernel ΩM is interesting. Then it's not difficult to show that if $M_1 \cong M_2$ then $\Omega M_1 \cong \Omega M_2$. Its analog in topology is the loop space construction. If I start with X. I can define P, the paths in X, choosing first an x_0, starting with x_0. This is a contractible space, you deform it along itself to x_0. It plays the role of P. The fiber of x_0 is the space of loops. It's extremely useful to have a situation like that where one of the objects is trivial and you get an interesting comparison between the two.

You can also switch things, putting any M into a P, and then you call it $\Omega^{-1}M$, the cokernel. If you think of the cyclic group, you keep the different Jordan things, they're distinct. You can try to compute Ω with them, it's not very difficult.

Then there is a theorem which I would call Theorem 23 if I were numbering things,

Theorem 9.1. *Suppose M_1 and M_2 are isomorphic in the homotopy category of modules over G. Suppose too that their semisimplifications are isomorphic. Then $M_1 \cong M_2$, so that resolves two different opposite points of view. It's not easy to check in practice that the two things are the same in the homotopy category. In practice you can do it*

I call this Theorem 23 because it combines the Brauer construction (2) with the characteristic p homotopy theory (3).

Let me speak about

9.5. The strange characteristic 1. If you have a vector space of dimension n, it comes with a basis $e_1, \dots, e_n$. In characteristic 1, these are still there, it's a set with n elements. You cannot add. 0 does not exist. From that point of view, so $GL_n(\mathbf{k})$ is S_n, the symmetric group of n elements. This started with Tits, who saw that theorems about semisimple groups had an analogue when you replaced the group by the Weyl group. The Weyl group of S_n is $GL_n(V)$.

The analogy becomes stronger with Tits buildings. The number of complexes depends on the cardinal of the field, but the buildinngs become the Coxeter complex when you write $q = 1$.

This tells me that I can look at representations of G in characteristic 1, take them to be $G \to S_n$, make the Grothiendieck group of that.

What are the irreducible objects? They correspond to transitive actions. Then $V \cong G/H$ for some $H \subset G$. If you take any V, it's a direct sum of its orbits.

You can make a Grothiendieck ring, which in that case was introduced by Burnside, he didn't use the ring language. The Burnside ring, call it $Burn(G)$, this shows a basis. Take the irreducibles, the basis is $[G/H_i]$, where H_i are representatives of the conjugacy classes of subgroups. It's a ring because the analogue of the tensor product is the direct product.

This is simpler than the character group. It has a natural map $Burn(G) \to R(G)$ because when you have a G-set V, you can take V as a basis and that gives a linear representation over $\mathbb{Z}$.

Take the symmetric group with three elements and see what we get. We have subgroups of orders 1, 2, 3, and 6. So $Burn(S^3)$ is order 4. We get a larger spectrum than for the characters.

The spectrum will have four components. You have the one of order 1, two that cross for orders 2 and 3, and I forget about the one of order 6 [picture].

Dress gave a lot of theorems about this, and he described the spectrum. One consequence of the theory is that the spectrum of the Burnside ring is connected if and only if G is solveable. Maybe I should recall that for a commutative ring, the spectrum being connected, that's the same as saying there is no idempotent.

So I have one minute left which I am not going to use.

[Do you have any advice?]

I get asked this all the time. I don't believe that old implies wise. To be fair I also don't believe that young implies wise.

You have to have some feeling for the thing you're studying, like it's a family you're entering or a country you're discovering, you should feel at ease, if you don't like the feeling then don't work on that, you won't discover anything, not even a counterexample.