Notes for 'Finite Groups in Number Theory'
J. P. Serre.

Contents

Introduction to these Lectures

I will discuss theorems which you will not find in the literature, either because they are too easy or too hard. This will include:

- Jordan.
- Frobenius, Cheb. density theorem for arbitrary fields.
- Sylow and fusion groups.
- Finite groups $\leftrightarrow$ Lie groups. For example $GL_n(\mathbb{F}_p) \leftrightarrow$ Alg groups.
- Representation theroy $\leftrightarrow$ Reduction mod p.

1 Jordan's Theorems.

See the article in Bulletin AMS 2003, for the following theorem dating from 1872:

Theorem 1.1 (Jordan)**.** *Let G be finite, $H \subset G$, $n = (G : H)$, $n \geq 2$. Then there exists $g \in G$ which is not conjugate to any element of H:*

$$\bigcup gHg^{-1} \neq G.$$

Theorem 1.2. *Assume G acts transitively on a finite set X, with $|X| \geq 2$. Then there exists $g \in G$ which has no fixed point on X*

Proof. $\bigcup gHg^{-1} = \{1\} \cup \bigcup_{g \in G/H} g\left(H - \{1\}\right)g^{-1}$. This has at most $1 + n\left(|H| - 1\right)$ $= |G| - (n-1)$ many elements. Thus the number of elements of G which are not conjugate to H is at least $n - 1$. □

In a moment we look at the case where we have equality. We will apply this to Chebatorev density.

Definition 1.3. Denote by G_0 the elements not conjugate to any element of H, and by G_n the set of all $g \in G$ such that $|X^g| = n$. ◇

Theorem 1.4 (Cameron-Cohen)**.**

$$\frac{|G_0|}{|G_n|} \geq \frac{1}{n}.$$

Proof. Let $X(g) = |X^g|$ = number of fixed points. Looking at the trace χ of the map

$$G \to S_n \to GL_n(\mathbb{C}),$$

we have

$$G_n = \{g | g \in G, \chi(g) = n\}.$$

Now we use Fourier analysis.:

$$\int_G \left(\chi(g) - 1\right)\left(\chi(g) - n\right) \leq n\frac{|G_0|}{|G_n|}$$

If $\chi(g) \in [0, n]$ then this integral is n, otherwise it is 0. (I don't understand this part). Now expand the integral:

$$\int_G \left(\chi(g) - 1\right)\left(\chi(g) - n\right) = \int_G \left(\chi^2 - (n+1)\chi + n\right),$$

and

$$\int \chi = 1, \int \chi^2 \geq 2$$

and so $\int \left(\chi(g) - 1\right)\left(\chi(g) - n\right) \geq 2 - (n+1) + n = 2$. □

Remark 1.5. We will not use this but I couldn't resist. ◇

In the theory of compact Lie groups, to characterize G you take a maximal torus $T \subset G$, and do something.

Example 1.6. Best case: take $GL_2(\mathbb{F}_p)$, and let B be a Borel subgroup; these are the elements whose eigenvalues are not rational, and is isomorhic to a non-split torus $\mathbb{F}_{p^2}$. Borel subgroups are OK. ◇

Example 1.7. Let G be a reductive group over $\mathbb{Q}_p$. ◇

Positive Results

Theorem 1.8. *A finite skew field D is commutative.*

Proof. Take $D \supset K \supset F$, where F is the center and K is the maximal commutative subfield. Then K is uniquely determined, since it is a finite extension of a finite field. Now use Skolem Noether and Jordan's theorem. □

Question 1.9. Let $H \subset G$. When can we use these ideas to show $G = H$. ◇

Example 1.10. Elliptic curves: when is the map $G_{\mathbb{Q}} \to GL_2(\mathbb{F}_l)$ surjective? In practice you can only construct conjugacy classes of elements in the image. By Jordan's theorem you only need to hit every conjugacy class. ◇

Definition 1.11. An S-character χ of a finite group is an element of the character ring such that

(1) Values of χ are real and positive.

(2) $\langle 1, \chi \rangle = 1$.

(3) $\chi(1) > 1$.

◇

Example 1.12. (1) Let G act on X with $|X| > 1$ and set $\chi(g) = |X^g|$.

(2) Let ψ be an irreducible character of G of degree at least 2 and set $\chi = \psi\bar{\psi}$

◇

Theorem 1.13. *If χ is an S-character then there exists a $g \in G$ with $\chi(g) = 0$.*

Corollary 1.14 (Burnside)**.** *If χ is an irreducible S-character of dimension ≥ 2 then there exists a g such that $\chi(g) = 0$.*

Proof. This time we write integration as sum

$$\sum_{g\in G}\chi(g) = |G|,$$

and

$$\int \chi(g) = 1.$$

As $\chi(g) \in \mathbb{Z}$ and $\chi(1) \geq 2$, one character value must be negative, hence 0 by the positivity assumption. □

Proof of corollary. $\chi(g) \in \mathbb{Z}(\zeta_n)$ for some n, and

$$\chi(g) = \sum z_\lambda, z_\lambda \in \mu_n.$$

Set $\sigma_i(z) = z^i$. Then

$$\sigma_i(\chi(g)) = \sum z_\lambda^i = \chi(g^i).$$

Now it is clear what to do: collect things by character (i.e. sum over irreducible representaitons of $(\mathbb{Z}/n\mathbb{Z})^\times$)

$$\sum \chi(g) \in \mathbb{Z}.$$

Define

$$Sp(\alpha) = \frac{1}{[\mathbb{Q}(\alpha):\mathbb{Q}]}\operatorname{tr}(\alpha).$$

Then

$$\int \chi(g) = \sum Sp(\chi(g^i)) = |G|.$$

$Sp(\chi(g^i))$ is a positive integer, unless $\chi(g^i) = 0$.

□

Theorem 1.15. *Let α be an algebraic integer, totally real. Then*

(1) $Sp(\alpha) \geq 1$.

(2) (Siegel) $Sp(\alpha) \geq \frac{3}{2}$ if $\alpha \neq 1$.

(3) (Smyth) $Sp(\alpha) \geq \frac{5}{3}$ if $\alpha \neq 1$, $\frac{3\pm\sqrt{5}}{2}$ (with some other slight hypothesis).

Proof. For part (1), note that $Sp(\alpha)$ is a sum of conjugates of α and use the arithmetic geometric mean inequality. The others are harder. □

Frobenius

Let G act on X transitively with $|X| \geq 2$, and let H be the stabilizer of a point and $n = |H|$. From above the number of fixed points is at least $n - 1$. We want to understand when we get equality.

So suppose we get equality: $|G_0| = n - 1$. This happens iff H does not intersect any of its conjugates. In terms of the action of G on X this means the following:

- $|X^g| = n$ if $g = 1$
- $|X^g| = 1$ if g is conjugate to a non-trivial element of H.
- $|X^g| = 0$ otherwise.

Example 1.16. Let F be a finite group with n elements, G acting as $x \mapsto ax + b$. Then G is a semi-direct product. If $a = 1$ there is 1 fixed point, if $a = 1, b \neq 0$ there are 0 fixed points. ◇

Theorem 1.17 (Frobenius)**.** *If H does not meet its conjugates then G is a semidirect product $G = H \cdot N$, where N is normal and $N = \{1\} \cup G^0$.*

Theorem 1.18 (Real content)**.** *N is a subgroup.*

Let $H \subset G$. Look at $R(H) \to R(G)$. If χ is a character of H, we define $\widetilde{\chi}$ by $\widetilde{\chi}(g)$ is $\chi(h)$ if g is conjugate to h and $\chi(1)$ otherwise. We can write this in a non-obvious way. For V an H-module, we can write

$$\widetilde{V} := \operatorname{Ind}_H^G V - \operatorname{rk}(V) \cdot \{\operatorname{Ind}_H^G 1 - 1\}.$$

Proposition 1.19. *The following are true.*

(1) *$R(H) \to R(G)$ is a ring homomorphism.*

(2) $\operatorname{rk} \widetilde{V} = \operatorname{rk} V$.

(3) $< \widetilde{V}, 1 >=< V, 1 >$.

Remark 1.20. This implies that $R(H) \to R(G)$ is an isometry:

$$\left\langle \widetilde{\chi}, \widetilde{\chi'} \right\rangle = \left\langle 1, \widetilde{\chi}, \widetilde{\chi'} \right\rangle = \left\langle 1, \widetilde{\chi\chi'} \right\rangle = \langle 1, \chi\chi' \rangle .$$

◇

Take V irreducible. Then $< \widetilde{V}, \widetilde{V} >= 1$, so V has dimension one.

Take C to be a *faithful* representation of H (e.g. the regular representation). Then $\widetilde{V}|_H = V$. If V is an H-representation then there is an action G on V which extends the H-action, and furthermore $\widetilde{\chi}(g) = \operatorname{rk}(V)$. For $g \in G_0$, if $\operatorname{tr}(g) = \operatorname{rk}(V)$, then $g = 1$ (as $\sum \lambda_i =$ something we are sure that the kernel of the action of G is N).

2 Frobenius's theorem

When one uses the classification of finite simple groups, no one really uses that there are 26 sporadic groups, we use their properties.

I start by correcting a little bit of what I did last time.

Theorem 2.1 (Frobenius)**.** *Let $H \subset G$ such that H does not intersect its conjugates, and set $N = \{1\} \cup \left(G - \bigcup_{g \in G} gHg^{-1}\right)$. Then N is a subgroup.*

Proof. Look at the map on modules

$$R(H) \to R(G).$$

and use the facts

(1) Then the map $V \mapsto \tilde{V}$ is compatible with multiplication, addition, and duality.

(2) The composition
$$R(H) \to R(G) \to R(H)$$
is the identity.

□

Now suppose let $G = H.N$ (N is normal, . means semidirect product). H acts freely on $N = \{1\}$.

Definition 2.2. We say that G is a **Frobenius** group if it can be obtained as a non-trivial semi-direct product in this way. ◇

Remark 2.3. A Frobenius group has a unique decomposition of this form; N is then called the *Frobenius kernel* and H the *Frobenius complement.* ◇

It is thus natural to ask when a subgroup occurs as a Frobenius kernel.

Lemma 2.4. *A given group N is a Frobenius kernel iff there is an automorphism σ of N, of prime order, which is 'fixed point free', i.e. fixes no element of $N - \{1\}$.*

Proof. If you have such a σ you get a decompositoin, and the other direction is clear. Also, you take H to be the group generated by σ. □

Theorem 2.5 (Thompson's thesis)**.** *A Frobenius kernel is a* nilpotent group.

Proof. Order $\sigma = 2, 3$ are easy. 5 was hard. Not every nilpotent group can be obtained. □

Question 2.6. When is a group H a Frobenius complement? ◇

Theorem 2.7. *The following are equivalent:*

(a) *H is a Frobenius complement.*

(b) *There is a free action of H on some sphere S by orthogonal trnsformations.*

(c) *There is a homomorphism of H into some linear group over some field $H \to GL_n(k)$ such that the action is free outside 0, and* $\operatorname{char} k \nmid \#H$

(c') *(c), but we can take $k = \mathbb{Z}/p\mathbb{Z}$ for some p.*

Proof. (a) $\leftrightarrow$ (c') are clearly equivalent. Serre spoke the proof of the rest. much too quickly without writing anything. The point is that the obstruction to lifting the H action on $\mathbb{F}_p$ to $\mathbb{Z}/p^2\mathbb{Z}$ is an element of $H^2(H, M_N(\mathbb{Z}/p\mathbb{Z}))$, and by the hypothesis $p \nmid \#H$ this is 0. So you can reduce to the characteric zero case. □

Remark 2.8. Topologists and differential geometers are interested in this result. ◇

This concludes what Serre wanted to add to the previous lecture.

Remark 2.9. Most H's are solvable, but there are a few exceptions (Poncairé has one). ◇

In the spirit of Jordan

I don't know whether this is a theorem, so we will call it a fact:

Theorem 2.10. *Let $H \subset G$, $H \neq G$, finite. Then there exists $g \in G$ which is not conjugate to an element of H. Furthermore we can choose g to have order a power of a prime.*

Remark 2.11. You could hope for prime order, but this fails: take $C_2 \subset C_4$. However, for many groups you can make g have prime order. ◇

Just after the announcement of the Classification of Finite Simple Groups, the following theorem was announced:

Theorem 2.12 (Fem, Kautn, Schacher (1981))**.** *It is enough to prove the previous theorem when G is a simple abelian group and H a maximal subgroup.*

The reduction to the simple case is not difficult at all. You can do it even if you are not fully awake.

Proof. Choose a minimal non-trivial normal subgroup G_1 of G. If $H \supset G_1$, then apply induction (and check that you can line up the order correctly). If not $H \cdot G_1$ is strictly larger than H so is equal to G (else the intersection would be a non-trivial normal subgroup), and so by induction $G_1 = G$, and in that case G is simple. □

Theorem 2.13 (Malle, Navarro, Olsson (2000))**.** *If χ is an irreducible character of a finite group G of degree > 1, then there exists $g \in G$ of prime power order with $\chi(g) = 0$.*

Last lecture we defined S-characters.

Question 2.14. If ψ is an S-character with $\psi(1) > 1$, is there a $g \in G$ of prime power order with $\psi(g) = 0$? ◇

Remark 2.15. If you replace *finite group* in the above theorem with *compact Lie group*, then the question has an affirmitive answer. ◇

To go any further we need the Chebatorev density theorem.

The Chebatorev Density Theorem

This theorem is quite recent, it is exactly my age.

Theorem 2.16 (1926)**.** Classical statement*: Let $K \subset L$ be a finite extension of number fields with Galois grop G, and rings of integers $\mathcal{O}_K \subset \mathcal{O}_L$. Let S be the set of ramified primes.; denote by $\mathfrak{p}$ primes of $\mathcal{O}_K$, and $\mathfrak{P}$ primes of $\mathcal{O}_L$. Let $G_{\mathfrak{P}}$ be the stabilizer of $\mathfrak{P}$. Then $G_{\mathfrak{P}}$ acts on the residue field $k(\mathfrak{P})$. Let $I_{\mathfrak{P}}$ be the Inertia group at $\mathfrak{P}$, i.e. the kernel of this action. Then $G_{\mathfrak{P}}/I_{\mathfrak{P}}$ is the automorphism group of $k(\mathfrak{p}) \subset k(\mathfrak{P})$, with canonical Frobenius generator $\sigma_{\mathfrak{P}}$. Then the following are true.*

(1) For every $g \in G$, there exists infinitely many $\mathfrak{P}$ at which $\sigma_{\mathfrak{P}} = g$.

(2) Alternatively, the conjugacy class $c(g)$ is equal to $\sigma_{\mathfrak{p}}$ for infinitely many $\mathfrak{p}$.

We really want a theorem more like Dirichlet's theorem. With the above notation, and let

$$\pi_K(x) = \sum_{N\mathfrak{p} \leq x} 1.$$

The *shape* of the theorem should be

$$\pi(x) \sim \frac{x}{\log x},$$

or better

$$\pi(x) = \frac{x}{\log x} + O\left(\frac{x}{(\log x)^2}\right)$$

or better

$$\pi(x) = Li(x) + O\left(e^{-c\sqrt{\log x}}\right)$$

where

$$Li(x) = \int_2^x \frac{dt}{\log t}.$$

For the Prime Number Theorem, $c = \frac{1}{20}$ is possible for the Prime Number Theorem. With the Riemann Hypothesis the error term should be $O(x^{1/2} \log x)$.

Remark 2.17. It is unfortunate that there exists another logarithmic integral

$$li(x) = \int_0^x \frac{dt}{\log t}.$$

The difference between the two is $li(x) - Li(x) = li(2)$, where $li(2) = 1.045\ldots$. Note that $li(x)$ is improper and you need to take the principal value. ◇

Definition 2.18. We define a modified prime counting function by

$$\pi_{K,c}(x) = \sum_{N\mathfrak{p} \leq x, \sigma_{\mathfrak{p}} = c} 1.$$

◇

Theorem 2.19. *The above counting function has the following asymptotics:*

$$\pi_{K,c}(x) = \frac{|C|}{|G|} Li(x) + O(\ldots).$$

The crucial work is of course done via L-functions, and so characters come in. Let χ be a character. Then define

$$\pi_{K,\chi}(x) = \sum_{N\mathfrak{p} \leq x} \chi(\sigma_{\mathfrak{p}}),$$

where $\chi(\sigma_{\mathfrak{p}})$ is the mean value of χ on the class of $\sigma_{\mathfrak{p}}$. There is a theorem we can prove next lecture.

3 Applications of Chebotarev for number fields.

Theorem 3.1. *Suppose $K \subset L \subset \tilde{L}$ is a finite extension of number fields, with Galois groups G, H and $X = G/H$. Then for every conjugacy class $c \subset G$, the set of (unramified) primes $\mathfrak{p}$ of K such that $\sigma_{\mathfrak{p}} \in c$ has density $\frac{|c|}{|G|}$.*

The orbits of $\sigma_{\mathfrak{p}}$ on X; each one corresponds to a prime $\mathfrak{P}$ of L over $\mathfrak{p}$, and the size of the orbit $|orbit|$ is the degree of $\mathfrak{P}$ = the degree of the residue field.

Theorem 3.2 (Jordan)**.** *Let $n = [L : K]$ such that $n \geq 2$. then the set of primes $\mathfrak{p}$ such that there is no prime of degree 1 above $\mathfrak{p}$ has density $\frac{1}{n}$.*

Proof. Let $L = K[x]/(f)$ for f irreducible. Then the set of $\mathfrak{p}$ for which $f(x) = 0$ mod $\mathfrak{p}$ has no solutions in $K(\mathfrak{p})$ has density at least $\frac{1}{n} > 0$. □

Lets translate this into number theory. We are going to look at something a b'it strange, but not too strange. To this extension we associate the following objects:

(1) $M_1 := K^*/NL^*$.

(2) $M_2 := I_K/NI_L$.

(3) $M_3 := \ker\left(Br(K) \to Br(L)\right)$.

These are all killed by n.

Definition 3.3. Let $A \to B$ be a homomorphism of abelian groups. We say it is *almost injective* if the kernel and cokernel are finite. ◇

In the above case everything is a countable $\mathbb{Z}/N\mathbb{Z}$-module, and these have a structure theorem: any such module M is a direct sum

$$M := \bigoplus \mathbb{Z}/l^{\alpha}\mathbb{Z},\ l^{\alpha}|N.$$

We can thus speak of the multiplicity of the l^{α} piece in M (and it may be infinite).

Theorem 3.4. *The modules M_i are pairwise isomorphic modulo a finite $\mathbb{Z}/N\mathbb{Z}$-module.*

In fact we are going to find essentially explicit isomorphisms.

Proof. We have a natural map $M_1 \to M_2$, $a \mapsto (a)$. We only need to see that the kernel and cokernel are finite. If we write it additively, introducing the module $M := \tilde{L}^*$, then $M_1 = M^G/N_{G/H}M^H =: h(M)$. From an exact sequence of G-modules

$$0 \to A \to B \to C \to 0$$

we get an exact sequence

$$0 \to \text{subobject} \to h(A) \to h(B) \to h(C) \to \text{quotient} \to 0$$

where the middle three terms are exact. Thus we get

$$0 \to E_{\tilde{L}}^* \to \tilde{L}^* \to I_L \to cl_L \to 0,$$

proving the first part.

For the second part, we have (up to a finite part coming from the real places)

$$Br_n(K) - \bigoplus \mathbb{Z}/N\mathbb{Z} = \mathbb{Z}/N\mathbb{Z} \otimes I_K.$$

Furthermore

$$\begin{array}{ccc} Br_n(K) & \longrightarrow & Br_n(L) \\ \downarrow & & \downarrow \\ \mathbb{Z}/n\mathbb{Z} \otimes I_K & \longrightarrow & \mathbb{Z}/N\mathbb{Z} \otimes I_L \\ \downarrow & & \downarrow \\ \mathfrak{p} & \longrightarrow & \sum \deg(\mathfrak{P}/\mathfrak{p})\mathfrak{P} \end{array} .$$

We set

$$c(\mathfrak{p}) := \gcd \deg(\mathfrak{P}/\mathfrak{p}).$$

Also, we have

$$\sum \deg = n,$$

and

$$\ker = \mathbb{Z}/c(\mathfrak{p})\mathbb{Z}$$

which is exactly what you would have gotten by (2). □

So not only are the M_i isomorphic mod finite groups, we find that they are

$$\bigoplus_{\mathfrak{p}} \mathbb{Z}/c(\mathfrak{p})\mathbb{Z}.$$

Definition 3.5. Define $c(g) = gcd\,(\text{orbits of } g)$. ◇

Theorem 3.6. *With M_i as above,*

$$M_i \cong \left(\bigoplus_{g \in G} \mathbb{Z}/c(g)\mathbb{Z} \right)_{\aleph_0}.$$

Corollary 3.7. *M_i is (are) infinite iff there exists a $g \in G$ of prime power order with no fixed points.*

Corollary 3.8. *For $n \geq 2$, the M_i are infinite.*

Remark 3.9. This is really equivalent, because you can construc S_n extensions of any number field. ◇

Remark 3.10. The following can be made into coherent statements about something.

(a) g of order l^α, l prime, size of orders divisible by l.

(b) Choose a g, a prime l such that $l \| |\text{orbits of } g|$.

◇

Frobenian Sets and Frobenian Functions

We state everything for ordinary primes, but everything will be true in general.

Definition 3.11. Let $\mathscr{P}$ be the set of all primes, $S \subset \mathscr{P}$ a finite subset, and $\Sigma \subset \mathscr{P} - S$. We then say that Σ is if there exists a Galois extension $L/\mathbb{Q}$ with Galois group G, unramified outside S, and a subset Σ_G of G (stable by conjugation), such that for $p \notin S$, $p \in \Sigma$ iff $\sigma_p \in \Sigma_G$. ◇

Fire alarm

Back to Frobenian Sets

Definition 3.12. We say that $\Sigma \subset \mathscr{P}$ is *Frobenian* if there exists a set S such that $\Sigma \cap (\mathscr{P} - S)$ is S-Frobenian. ◇

Definition 3.13. A **Frobenian function** is a function

$$a : \mathscr{P} - S \to \Omega$$

where Ω is a finite set and such that there exists an extension $L \supset \mathbb{Q}$ as before and a function

$$A : \operatorname{conj} \operatorname{Gal}(L/\mathbb{Q}) \to \Omega$$

satisfies $a(p) = A(\sigma_p)$. ◇

Example 3.14 (Cyclotomic fields)**.** Let p map to the residue class mod m. This comes from $L = \mathbb{Q}(\zeta_m)$. ◇

Definition 3.15. Let $A : G \to \Omega$ be a Frobenian function. We set $a_{id} := A(1)$ and $a_c := A(c)$, where c is a complex conjugation.

◇

Theorem 3.16. *Let f_α be a family of polynomials over $\mathbb{Z}$, and set*

$$N_f(p) = \textit{number of solutions mod } p.$$

Then the following are true.

(a) N_f *is a Frobenian function.*

(b) a_{id} *is the residue class mod* m *of the Euler characteristic of complex conjugation.*

(c) a_{id} *is a residue class mod* m *of the trace of complex conjugation acting on the cohomology with compact support*

4 More on Frobenian Sets and Functions

Let K be a number field and V_K be the set of maximal ideals of $\mathcal{O}_K$.

Definition 4.1. A subset $\Sigma \subset V_K - S$ (for some set of bad primes $S \subset V_K$) is S-**Frobenian** if there exists a finite Galois extension $L \supset K$ with $G = \mathrm{Gal}(L/K)$ and a subset σ of G such that

(1) L/K is unramified outside of S;

(2) σ is stable under conjugation;

(3) $\mathfrak{p} \in \Sigma$ iff $\mathrm{Frob}_\mathfrak{p} \in \sigma$.

More generally we say that Σ is Frobenian if there exists an S such that Σ is S-**Frobenian**. ◇

Let K^S be the maximal extension of K unramified outsied of S, and set $G_{K,S} := \mathrm{Gal}(K^S/K)$ (which is a profinite group). The following correspondence is rather clear.

Lemma 4.2. *There is a one-to-one correspondence between clopen subsets of $G_{K,S}$ which are stable under conjugation and S-Frobenian sets.*

Let $G_K = \mathrm{Gal}(\bar{K}/K)$. Then clopen subsets of G_K correspond to Frobenius sets modulo finite sets. $G_\mathbb{Q}$ is a mysterious object, but we get some control. There are some obvious constructions one one side where the corresponding thing on the other side isn't obvious.

Example 4.3. Let k be an integer, and consider the map $G_{K,S} \to G_{K,S}$ given by $g \mapsto g^k$. Given $U \subset G_{K,S}$, we can consider its inverse image, which is clopen is U is. This is not an obvious construction from the point of view of primes.

Take for example as your Frobenius set all $p = 2 \mod 7$. Under this construction you get $p = 3 \mod 7$. ◇

Example 4.4. Let $f : \mathscr{P}_K - S \to \Omega$, where Ω is a finite set. Then the set of $\mathfrak{p}$ with $f(\mathfrak{p}) = \omega$ for a fixed $\omega \in \Omega$ is an S-Frobenian function. ◇

We now see an easy classification: an S-Frobenian function corresponds to class functions, i.e. functions $f : G_{K,S} \to \Omega$ which are continuous and invariant under conjugation. So we consider functions of this type. For an extension $K' \supset K$, you get a map from Frobenian functions on $G_{K'}$ to Frobenian functions on G_K. In terms of primes this map is not obvious.

Remark 4.5. Frobenian functions have nice invariants. For example, one should naturally consider $f(1)$, and if K is totally real one should look at $f(c)$, where c is a representative of complex conjugation. ◇

Example 4.6. Take $K = \mathbb{Q}$, and let $\Sigma = \{p : p \text{ can be written in the form } 2x^2 + xy + 9y^2\}$. Exercise: this is Frobenian, with $S = 71$ and density $1/7$. Transform this by exponentian by k as above. The discriminant is $1 - 8 \cdot 9 = -71$. You are using that the class number is 7. ◇

Example 4.7. Here is a non-example. Let Σ be the set of primes which in base ten begin with one. Then this has no density (exercise; the lower and upper bounds don't coincide). ◇

Example 4.8. Take a prime p which can be written as $1+x^2$. This might be Frobenian. However, conjecturally this set is infinite, and if so it has zero density and is not Frobenian. ◇

Lemma 4.9. *A Frobenian set with zero density is finite. An S-Frobenian set of zero density is empty.*

Question 4.10 (Tate)**.** What is a non-Frobenian set with positive density?

Serre: Just take a Frobenius set and remove a zero density set of primes. ◇

Example 4.11. Let $K = \mathbb{Q}$ and $N(p) = 1 + p - a_p$. Then the set $\{p : a_p = 0\}$ has density $1/2$ in the CM case and density zero otherwise. ◇

Let $f \in \mathcal{O}_K[\bar{x}]$, and $N(\mathfrak{p})$ be the number of solutions mod $\mathfrak{p}$ (you can think of this as counting the rational points on the fibers of a scheme over $\mathcal{O}_K$).

Theorem 4.12. *Let M be a non-zero integer. Then the function $p \mapsto N(\mathfrak{p}) \mod m$ is Frobenius.*

Remark 4.13. It is a pity that the seminars of Grothendieck did not have exercises. I should have insisted. This theorem is a missing exercise from SGA 4.5. ◇

By additivity this theorem is also true for a projective scheme.

Proof. We may assume m is a prime power l^α.

Lets take our scheme V to be projective instead, and let V_K be the generic fiber. Lets do the special case where V_K is a smooth projective variety. If you remove (invert) a finite set of primes and call the resulting scheme V_S, then V_S is smooth, and doesn't change whether f is Frobenian.

Now the way Grothendieck computes $N(\mathfrak{p})$ is via the trace formula:

$$N(\mathfrak{p}) = \sum_{i=0}^{2\dim V_K} (-1)^i \operatorname{tr}\left(\mathrm{Frob}_{\mathfrak{p}}\right) H_c^i\left(V_{\bar{K}}, \mathbb{Q}_l\right)^*$$

for some prime l. Now the H^i are finite dimensional vector spaces. Enlarge our S by the set L of primes dividing l and call this S'. Now there is a $\mathbb{Z}_l$-lattice which is $G_{K,S'}$ stable, and the formula becomes

$$N(\mathfrak{p}) = \sum_{i=0}^{2\dim V_K} (-1)^i \operatorname{tr}(\operatorname{Frob}_{\mathfrak{p}}) V_i.$$

where V is a $\mathbb{Z}/l^\alpha\mathbb{Z}$ module. Also, now it is clear that $f(1) =$ the Euler characteristic of V_K.

General Case: Use resolution of singularities and constructible sheaves. □

Remark 4.14. We can enlarge the class of Frobenian functions by enlarging Ω to pro-finite sets such that each finite reduction is Frobenian. Then the above function is *pro-Frobenian.* ◇

Remark 4.15. Now consider $f(g^k)$ and the function $\mathfrak{p} \mapsto N(p^k)$. What about $k = -1$? When V is smooth and projective of dimension d. Then the function we want is the *Tate twist*, given by $N(p)p^{-k}$.

We may also consider the case of changing K. ◇

Corollary 4.16. *Let V and f as above, and suppose $\chi(V(\mathbb{C}))$ is 3. Then one concludes that there are infinitely many p such that $N(p) = 3 \mod 10$.*

This would be a hard theorem otherwise.

Modular forms

It doesn't really matter what congruence subgroup we take, so take $\Gamma_0(N)$. Take some space $M_k(N)$ of modular forms of weight k and level N for $\Gamma_0(N)$, and $\phi = a_0 + a_1 q + \ldots$ such that the a_i are algebraic integers (whence $a_i \in K$ for some finite K).

Theorem 4.17. *The map $p \mapsto a_p \mod m$ is Frobenian, and furthermore S can be taken to be the divisors of Nm.*

This is an exercise on Deligne's paper about constructing Galois representations.

Proof. The proof is similar, we want to write this as a linear combination of traces.

Step 1: ϕ is a normalized eigenfunction of the Hecke operators, $m = l^\alpha$. In that case we know that

$$a_p = \operatorname{tr}(\operatorname{Frob}_{\mathfrak{p}}(V))$$

for V some vector space of dimension 2 over an extension of $\mathbb{Q}_l$.

Step 2: ϕ is a linear combination with coefficients in $\mathcal{O}_K$ of eigenforms.

Step 3: Step 2 with denominators (i.e. the linear combination is over K not $\mathcal{O}_K$). Then $n\phi$ is of type 2 for some n. So we apply step 2. □

Question 4.18. What are the invariants? We have $f(1) = 2a_1$ and $f(c) = 0$. This is because the Galois representations are 2-dimensional. ◇

Choose a lattice L of modular forms with coefficients in $\mathcal{O}_K$ which is stable under T_p.

Theorem 4.19. *The function $p \mapsto T_p \in \mathrm{End}\,(L/mL)$ is Frobenian, and its value at 1 is 2 and at c is 0.*

Proof. The proof is the same. □

Next time we speak on schemes over $\mathbb{Z}$.

5 Chevatorev Density for Arbitrary Schemes

Before I started with Jordan's theorems and then went out of bounds. Today I will do worse. Next week we will return to more elementary things, such as the Sylow theorems. After that I don't know, maybe study reductions mod p and things which aren't in the literature. After that we will talk about GL_2 over a small base, if we have enough time. These very small groups occur all the time in number theory, so there is a good excuse to study these.

But today I said it will be worse, because we will speak on the Chebatorev density theorem for arbitrary schemes. To this end, let $V \to \operatorname{Spec} \mathbb{Z}$ be a scheme of finite type. If you do not like schemes, then just think of a ring A which is finitely generated over $\mathbb{Z}$. If you have such an object, from the algebra point of view, you are interested in the maximal ideals. Then $\kappa(\mathfrak{p}) \in A/\mathfrak{p}$ is a finite field, and we set $N(\mathfrak{p}) = \#\kappa(\mathfrak{p})$. Call also $\bar{V}$ the set of closed points (or the *atomization* of V).

As in prime number theory, we define a counting function.

Definition 5.1. We define the *counting function* of V to be

$$\pi(X)_V = \sum_{\mathfrak{p} \in \bar{V},\, N(\mathfrak{p}) \leq X} 1.$$

(Here N means norm.) ◇

We are interested in how this function grows. Consider the case wehre V is reduced and irreducible. Let K be the function field, and assume that $\operatorname{char} K = 0 \geq 0$. When $p = 0$ we also want V *flat* over $\mathbb{Z}$ (so no torsion) and $V \to \operatorname{Spec}(V)$ is a dominant map. Also let $d = \operatorname{tr\,deg} K/\mathbb{Q} = \dim V - 1$. So the standard case is $d = 0, d + 1 = 1$. We may now state a theorem.

Theorem 5.2 (Prime Number Theorem)**.** *If $d + 1 = \dim V$, then*

$$\pi_V(X) = \frac{1}{d+1} X^{d+1} / \log(X) + o\left(X^{d+1}/\log X\right).$$

We get a refined form.

Theorem 5.3. *We can refine the above theorem as,*

$$\pi_V(X) = Li\left(X^{d+1}\right) + O\left(X^{d+1} \exp\left(-c\sqrt{(}\log X)\right)\right),$$

and we can take the same c that we do for the classical prime number theorem.

Remark 5.4. Recall that

$$Li(X) - \left(X^{d+1}\right) \sim \frac{X^{d+1}}{(d+1)\log X},$$

so the second theorem implies the first. ◇

Proof. Inducting on the dimension, we may change V by adding or removing a subscheme of smaller dimension (absorb the extra into the error term). We change the problem slightly. Set instead

$$\pi'_V = \sum_{N\mathfrak{p}\leq X, \deg \mathfrak{p}=1} 1$$

where here $\deg \mathfrak{p}$ means the degree of the residue field. Then

$$\pi(X) = \pi'(X) = O\left(X^{d+\frac{1}{2}} \log X\right).$$

(With the Riemann Hypothesis the log gives the correct error term.)

Now K contains a field K_0 which is a finite extension of $\mathbb{Q}$, and $K \supset K_0$ is a regular extension. Geometrically we have $V \to \operatorname{Spec} \mathcal{O}_{K_0} \to \operatorname{Spec} K$ where now the first map has an absolutely irreducible generic fiber (this is just the Stein Factorizaiton).

Remark 5.5. If you prove the Riemann Hypothesis for K_0 (by accident) it will imply something for V. ◇

Now we count using the primes of $\mathcal{O}_{K_0}$ (assume now $V = \operatorname{Spec} A$). Let v be a prime of $\mathcal{O}_{K_0}$. Then V_v is a variety over $\kappa(v)$, of dimension d, and outside a finite number of v (which we do not count at all) is absolutely irreducible. We now look at the points such that v has degree one. Then

$$\pi'(X) = \sum_{\deg v=1, N(v)\leq X} N(V_v),$$

and this is easy to count.

Let Y be a variety over $\mathbb{F}_p$, absolutely irreducible of dimension d, and $N(Y) = |Y(\mathbb{F}_p)|$. Then we know

$$|N(Y) - N(v)^d| \leq BN(v)^{d-\frac{1}{2}}$$

where B is the sum of $\dim H^i_c\left(Y_{\bar{\mathbb{F}}_p}, \mathbb{Q}_l\right)$ This is an easy consequence of the Weil conjectures. Probably the B are independent of l, but we don't need that. We need something stronger than just the Weil bounds. B is at least uniformly bounded because the comology varies in a constructible way.

Thus

$$\pi'(X) = \sum_{\deg v=1, N(v)\leq X} N(v)^d + O(X^{d+\frac{1}{2}})$$

and we are left with estimating this sum. Now this is a problem about number fields. We know that

$$\pi_{K_0}(X) = \sum_{\deg v=1, N(v)\leq X} 1 = Li(X) + O\left(X \exp\left(-c\sqrt{\log X}\right)\right)$$

i.e. we use the $d = 0$ case of the theorem we want to prove. This is typical: we use algebraic geometry to reduce to a classical analytic number theory problem. Estimating this sum is essentially partial summation; we can write it as

$$\pi'(X) = \sum_{\alpha \leq t \leq X} \{\pi_{K_0}[t] - \pi_{K_0}(t-1)\}\, t^d = \int_2^X d\pi_{K_0}(t) \cdot t^d\, dt.$$

Using integration by parts, we find that

$$\pi'(X) = \pi_{K_0}(X) \cdot X^d - \int_2^X dt^{d-1} \pi_{K_0}(t)\, dt.$$

(Sorry about the two d's.) Thus we have

$$\pi_{K_0}(X) = Li(X) + \text{ error } =$$

$$Li(X)X^d - d\int_2^X Li\,(t)\, t^{d-1}\, dt$$

and we need the estimate

$$\int_2^X t^\lambda \exp\left(-c\sqrt{\log t}\right)\, dt << X^{\lambda+1} \exp\left(-c\sqrt{\log X}\right)$$

for $\lambda \geq 0$ an integer. We differentiate and get

$$\frac{1}{\log X} X^d + Li\,(X)\, dX^{d-1} - dLi(X)X^{d-1} =$$

$$\frac{(d+1)X^d}{\log X^{d+1}} = \frac{X^d}{\log X}.$$

And we have a proof. You can also make the following line of thought

$$\int \frac{t^d}{\log t}\, dt = \int \frac{t^{d+1}}{\log t^d}\, dt$$

into a correct proof. □

Without Grothendieck's theory you can do this for curves. For higher dimension you really need cohomology.

Now we turn to density.

Definition 5.6. We say that a subset $\Omega \subset \bar{V}$ has density λ if

$$\sum_{\omega \in \Omega, N(\omega) \leq X} 1 = \lambda \frac{X^{d+1}}{\log\left(X^{d+1}\right)} + o(-).$$

◇

Let $W \to V$ be a finite map and W flat over $\mathbb{Z}$ and G a finite group acting faithfully on W so that $V = W/G$. We may assume that the covering is étale by throwing away a subset of V. As before, for $\mathfrak{p} \in \bar{V}$, we have $\sigma_\mathfrak{p} =$ Frobenius at $\mathfrak{p}$ (as a conjugacy class in G): we can choose $\mathfrak{P} \in \bar{W}$ above $\mathfrak{p}$, and as usual set $D_\mathfrak{P} =$ the stabilizer of $\mathfrak{P}$ in G. $D_\mathfrak{P} \cong$ the Galois group of the residue field. This is cyclic, and generated by Frobenius, which we lift to a conjugacy class.

Theorem 5.7 (Chebatorev)**.** *If c is a conjugacy class in G, then the set of $\mathfrak{p}$ for which $\sigma_\mathfrak{p}$ is in c has density $\frac{|C|}{|G|}$.*

Alternatively, we have the following stronger theorem.

Theorem 5.8. *The number of such $\mathfrak{p}$'s with $N(\mathfrak{p}) \leq X$ is*

$$\frac{|C|}{|G|} Li(X^{d+1}) + O\left(X^{d+1} \exp\left(-c\sqrt{\log X}\right)\right).$$

We regret that we haven't yet defined a zeta function.

Definition 5.9. We define the *zeta function* of V to be

$$\zeta_V(s) = \prod_{\mathfrak{p} \in \bar{V}} \left(\frac{1}{1 - N(\mathfrak{p})^s}\right).$$

◇

Then we get the following further refined theorem.

Theorem 5.10.

$$\zeta_V(X) = \zeta_{K_0}(s - d) \cdot E,$$

where

$$E = \prod_{v \in K_0} \left(1 - \alpha_{i,\mathfrak{p}}^s\right)^{\beta_{i,\mathfrak{p}}}$$

for some α and β which you have control over.

Corollary 5.11. *We have that $\zeta_V(s)$ has a simple pole at $s = d + 1$ and is non-zero for $\Re(s) > d + 1$. Furthermore,*

$$L_V(s, \chi) = L_{K_0}(s - d, \chi_*).$$

Recall that if you have a map of groups $\phi : G_1 \to G_0$, then a character of G_0 induces a character on G_1, and if ϕ is injective then you get the induced character. If ϕ is surjective then you can push forward a character too. So in the above forumla, χ^* is an induced character under some map.

Proof of Chebatorev. Very similar. The main variant is that instead of computing

$$\sum 1$$

we compute

$$\sum \chi$$

for a character χ. Then we have

$$\pi_{W/V,\chi}(X) = \sum_{\deg \mathfrak{p}=1, N(\mathfrak{p})\leq X} \chi\left(\sigma_{\mathfrak{p}}\right).$$

Now the *main point* is to fix v of degree 1 in K_0 and compute the sum

$$\sum(\sigma_{\mathfrak{p}}) = \chi^*(\mathrm{Frob}_v)N(v)^d + O\left(N(v)^{d-\frac{1}{2}}\log N(v)\right).$$

So this is the main term. You can compute this using cohomology, or by the following trick, which I explain because it can save your life in case of danger. We work now over $\mathbb{F}_p$. We want to compute a sum like

$$\sum \chi(\sigma_p), \mathfrak{p} \in V(\mathbb{F}_p).$$

Work instead with $W(\bar{\mathbb{F}}_p)$; this has both a G and a Frobenius action. We then get

$$\sum_{\mathfrak{p}\in V(\mathbb{F}_p)} \chi(\sigma_p), = \frac{1}{|G|}\chi(g)\cdot\Lambda(g^{-1}F)$$

where $\Lambda(g^{-1}F)$ is the number of points of W twisted by g. We lose irreducibility of W so we have to work a little harder than before and find something more complicated, but still get a nice formula. □

6 small (Finite) GROUPS

Today we will look at groups of small order (say less than 8) such as $A_n, S_n, SL_2, PGL_2, PSL_2$.

n = 2: Let I have two elements. Then it is a torson for $\mathbb{Z}/2\mathbb{Z}$.

n = 3: Let I be a set with three elements. What canonical things can we do with it? We get a map

$$I \mapsto \text{ group of type (2,2)}, 0 = \{\emptyset\},$$

with such things as $x, y \in I, x + y = 0$ and so on. For example, we could take $H \subset \mathbb{F}_2^I$ such that $\sum x_i = 0$. We see that $S_3 \cong Sym(I) \to GL_2(\mathbb{F}_2) = \mathrm{SL}_2(\mathbb{F}_2)$ which is of course an isomorphism.

Remark 6.1. We are not so interested in particular automorphisms, only canonical ones. ◇

n = 4: Suppose we have a set I with 4 elements. We can attatch to it an affine space over a 2^2-group. What is a 2^2 group? We have $H \subset V := \mathbb{F}_2^I$ defined by $\sum x_i = 0$, and furthermore we have $L \subset H$ generated by $(1, 1, 1, 1)$. So we look at the quotient H/L. We see already from this that we get a map

$$S_4 = Sym(I) \to GL_{H/L} \cong S_3.$$

The three non-trivial images of elements of H/L correspond to the partitions of I of type $2, 2$. More carefully, we get a map

$$V/L \xrightarrow{\phi} V/H = \mathbb{F}_2$$

and we get a torsor $X := \phi^{-1}\{0\}$ over H/L. Thus we have

$$S_4 \to \text{Affine tr of } \mathbb{F}_2^2 = \mathbb{F}_2^2 \cdot S_3.$$

Characteristic 3: We know that $\mathbb{P}^1(\mathbb{F}_3)$ has 4 elements, and thus get a map

$$PGL_2(\mathbb{F}_3) \to S_3$$

which is an isomorphism by counting elements. This is unsatisfactory, we want a more functorial construction.

Instead let I be a set with 4 elements, and take $H \subset \mathbb{F}_3^4$ such that $\sum x_i = 0$. We can equip this with a non-degenerate quadratic form $q(x) = \sum x_i^2$ which defines a conic $C \subset \mathbb{P}^2_{\mathbb{F}_3}$ with a canonical isomorphism $C(\mathbb{F}_3) \cong I$, so we have, canonically,

$$Sym(I) \cong \mathrm{Aut}(C)(\mathbb{F}_3).$$

We also have

$$\begin{array}{ccc} \widehat{A_4} & \longrightarrow & \widehat{S_4} = GL_2(\mathbb{F}_3) \\ \downarrow & & \downarrow \\ A_4 & \longrightarrow & S_4 = PGL_2(\mathbb{F}_3) \end{array} .$$

Remark 6.2 (Wiles)**.** We have $\mathbb{Z}_3 \to \mathbb{F}_3 \to 0$, giving

$$GL_2(\mathbb{Z}_3) \to GL_2(\mathbb{F}_3) \to 0$$

and a section. It is a nice exercise to prove this using cohomology. In fact you can do a little better, we looking at a character table we get a section

$$\begin{array}{ccc} GL_2(\mathbb{Z}_3) & \longrightarrow & GL_2(\mathbb{F}_3)\ . \\ \uparrow & \swarrow & \\ GL_2(\mathbb{Z}[\sqrt{-2}]) & & \end{array}$$

◇

More is true, for example you get

$$\begin{array}{ccc} & & E_8(\mathbb{Z}_{31}) \\ & \nearrow & \downarrow \\ PGL_2(\mathbb{F}_{31}) & \longrightarrow & E_8(\mathbb{F}_{31}) \end{array}$$

but there are not yet so nice applications as in the $p = 3$ case.

Draw the picture of a 3-regular graph G truncated at radius 2. Then

$$\mathrm{Aut}(G) \cong \{\pm 1\} \times S_4 = GL_2(\mathbb{Z}/4\mathbb{Z})/(\pm 1).$$

Indeed, let L be a free $\mathbb{Z}/4\mathbb{Z}$-module of rank 2. You can count the subgroups of $\mathrm{Aut}(G)$ which are cyclic of order 4; these correspond to fixing an outer point. The ± 1 corresponds to switching every pair. Maybe this part is wrong.

If you look at the extremal points of the graph you get 6 points which are related. You get partitions A and B with $|A| = |B| = 3$ and A intersects each partition in one element. There are 4 possible such partitions.

For the people who work with elliptic curves (I am sure there are a few in the audience). You know this situation quite well. You look at the points of order 2, these are given by $x_1, x_2, x_3 = \mathfrak{p}\left(\frac{\omega_i}{2}\right), \ldots$, and we have $2\omega_i = \sum \omega_i = 0$. Look at the 4 division points and you get 6 values.

Quartic fields with Galois group S_4 or A_4

This has little to do with Galois theory. Take

$$\Gamma \to S_4, A_4 \to S_3, A_3.$$

Give yourself inside Γ a subgroup Γ_1 of index 3, and also inside Γ_1 a subgroup Γ_2 of index 2 (up to conjugacy). It is convienient to use cohomological language (or at least transfer); you have a map $\Gamma_1 \xrightarrow{\phi} \mathbb{Z}/2\mathbb{Z}$ and a transfer map $\Gamma \xrightarrow{tr\phi} \mathbb{Z}/2\mathbb{Z}$. You can thus find $F_2 \supset F_1 \supset \mathbb{Q}$ where F_1 is cubic and F_2 is quadratic, generated by $\alpha \in F_1$.

Now you look in the tables of quartic fields, courtesy of Godwih.

I think I have said probably enough on this part.

n = 5

Now I will write you a list of the isomorphisms that I want to tell you about and discuss only some of them.

- $A_5 \cong SL_2(\mathbb{F}_4)$.
- $A_5 \cong \mathrm{PSL}_2(\mathbb{F}_5)$,
- $S_5 \cong PGL_2(\mathbb{F}_5)$.
- $2 \cdot A_5 \cong SL_2(\mathbb{F}_5)$.

n ≥ 6

- $S_6 \cong Sp_4(\mathbb{F}_2)$.
- $A_6 \cong PSL_2(\mathbb{F}_g)$ (but $S_6 \ncong PGL_2(\mathbb{F}_g)$).
- $3 \cdot A_7$.
- $A_8 = \mathrm{SL}_4(\mathbb{F}_2)$.
- $S_8 = A_8 +$ something.

A_6

We do the most interesting case. There is a correspondence between curves of genus 2 ramified at 6 poits and a 2^4-smyplectic form.

Let $|I| = 6$. As usual we get $0 \subset L \subset H \subset \mathbb{F}_3^I$, so we get H/L of dimension 4. Also as before we get a non-degenerate quadratic form $q(x) = \sum x_i^2$.

Thus in the geometric language we get a degree 2 hypersurface $Q \subset \mathbb{P}^3_{\mathbb{F}_3}$. We can classify such things and recognize that Q is not $\mathbb{P}^1 \times \mathbb{P}^1$ (since S_6 acts on Q, but not on $\mathbb{P}^1 \times \mathbb{P}^1$ In fact we get $\mathrm{Res}^{\mathbb{F}_9}_{\mathbb{F}_3} \mathbb{P}^1$, giving an automorphism

$$A_6 \cong \mathrm{PGL}_2(\mathbb{F}_9).$$

Remark 6.3. Recall that

$$S_n \to \mathrm{Aut}\, S_n$$

is surjective for all $n \neq 6$. ◇

A_8

This one is rather suprising. Let $|I| = 8$ and $0 \subset L \subset H \subset \mathbb{F}_2^I$ as before, getting a quadratic form $q(x) = \sum_{i<j} x_i x_j$. This is non-degenerate. H/L has dimension 6. We thus get a map

$$S_8 = Sym(I) \to O_6(\mathbb{F}_2, q)$$

where q is split (i.e. isomorphic to a standard form $x_1x_2 + \ldots$. If you know anything about Lie theory you find that $D_3 \cong A_3$, and the automorphism group is SL_4. We want to exploit this.

It turns out that $\mathrm{SL}_4(\mathbb{F}_2) \subset O_6(\mathbb{F}_2, q)$ of index 2. More generally let W be of dimension 4 over $\mathbb{F}_2$. Then $\Lambda^2 W$ has dimension 6, and we get

$$\Lambda^2 W \times \Lambda^2 W \to \Lambda^4 W = \mathbb{F}_2,$$

inducing a map

$$SL(W) \to O(\Lambda^2 W) = O(6).$$

Finally, the last isomorphism below comes from $X(7)$.

List of isomorphisms

- $S_3 = SL_2(\mathbb{F}_2)$.
- $S_4 = 2^2 S_3 = \mathbb{F}_2^2 \cdot S_3$.
- $A_4 = \mathbb{F}_2^2 \cdot C_3$.
- $S_4 \cong PGL_2(\mathbb{F}_3)$.
- $A_4 = PSL_2(\mathbb{F}_3)$.
- $PSL_2(\mathbb{F}_7) \cong SL_3(\mathbb{F}_2)$.

7 Sylow, Fusion, and Local Conjugation.

Sylow

Sylow's original proof more or less looks at conjugacy classes.

There is another proof by Miller where you write $|G| = p^n m, (m, p) = 1$, and look at certain subsets. This is the proof that is very common at the moment.

Remark 7.1. Sylow is Norwegian, the theorem is around 1860. ◇

Here is another good proof. Suppose you have a group $G \subset G_1$ and G_1 has a p-Sylow, say S_1. Then you deduce that G has a p-Sylow, by making G act on G_1/S_1, which has order prime to p. Thus you get $S \subset G$ of index prime to p. By induction you win.

Nonetheless it is a mess to describe the Sylow subgroups of a group. One example is

$$G \subset S_N \subset GL_N(\mathbb{Z}/p\mathbb{Z})$$

and the Sylow group of GL_N is clear (upper triangular).

Now we want to study *Sylow type situations*. Let $\mathcal{G}$ be a category (or even just set) of groups and $\mathcal{S}$ be a subcategory satisfying the following axioms.

- If $A, B \subset G \in \mathcal{G}$, then all associated groups (automorphisms, normalizer, etc) are also in $\mathcal{G}$.
- $s \in G$, $aAs^{-1} \subset A \Rightarrow sAs^{-1} = A$. (This excludes things like $SL_2(\mathbb{Q})$).
- (Sylow axiom) if $G \in \mathcal{G}$ and $S \subset G$ then there is an $S \in \mathcal{S}$ such that for all $S' \subset \mathcal{G}$, S' is conjugate to a subgroup of S.

Example 7.2. Here are some

(1) Sylow groups.

(2) (P. Hall) LEt Σ be set of primes; $\mathcal{G}$ finite solvable groups and $\mathcal{S}$ finite groups with index a product of elements of σ.

(3) (Borel) $\mathcal{G}$ is the category of smooth linear algebraic groups, say over an algebraically closed field k, $\mathcal{S}$ is the category of smooth connected solvable subgroups.

(3') $\mathcal{G}$ reductive groups, $\mathcal{S}$ tori (over an algebraically closed field).

(3") $\mathcal{S}$ split tori.

(4) (Cartan, Weyl) $\mathcal{G}$ compact lie groups, $\mathcal{S}$ tori (in the topological sense).

(5) (Iwasawa, Cartan) $\mathcal{G}$ real Lie groups with finitely many connected components and $\mathcal{S}$ is compact real Lie groups.

$\diamond$

So that is a good looking list.

Applications of Sylow theory

Many of the main applications of the Sylow theorems apply here.

Fratinni argument: Suppose you have a normal subgroup $H \subset G$. Now take S_H to be a p-Sylow subgroup of H and take the normalizer $N_G(S_H)$. Then the Fratinni argument says the following.

Proposition 7.3. *The natural action*

$$N_G(S_H) \to G/H$$

is surective.

Proof. Let $g \in G$. Then

$$gS_Hg^{-1} = hS_Hh^{-1}$$

and $hg^{-1} \in$ something Serre immediately erased. $\square$

Here is an application.

Definition 7.4. A projection $G \to G/H$ is an **essential extension** if no proper subgroup of G maps onto G/H $\diamond$

Theorem 7.5. *If $G \to G/H$ is essential, then H is a direct product of p-groups (p may vary; i.e. H is a nilpotent group).*

Proof. Frattini argument: S_H is normal in G, hence contained in H. $\square$

Example 7.6. Let F be a profinite group. We are interested in lifting properties.

Definition 7.7. We say a map $G \to G/H$ has the **abeilan lifting property** if every hom $F \to G/H$ lifts to $F \to G$ (iff $H^2(F, module)) = 0$). We define just the **lifting** property to be the same without the abelian restricion on H. $\diamond$

Lemma 7.8. *The abelian lifting property implies the lifting property.*

Proof. It is enough to prove it when $G \to G/H$ is essential. But then H is nilpotent. But then H has a non-trivial normal abelian subgroup. Call this H'. Now argue by induction. $\diamond$

$\diamond$

Remark 7.9. No finite group has these lifting properties. It is remarkable that this holds for pro-finite groups. ◇

Remark 7.10. You can try the same for **discrete groups**. Then it is non-trivial that the abelian lifting property is equivalent to the cohomology property. This is due to Stallings and Swan.

If $cd(F) \leq 1$ then F is free. This implies that you have the lifting property. ◇

Remark 7.11. It is irresistible the temptation to call something elementary... ◇

Fusion

We begin with old results of Burnside.

Definition 7.12. Let $H \subset G$. We have the conjugacy classes of elements of H in H G. Some of them get *fused* by G. ◇

Let $S \subset G$ be p-Sylow and let $N = N_G S$ be its normalizer. Then N *strongly controls* the fusion of S in G if S is abelian.

Theorem 7.13 (Burnside)**.** *Let A, B be subsets of the center of S and let $g \in G$ be such that $gAg^{-1} = B$. Then there exists $n \in N_G S$ with $nan^{-1} = gag^{-1}$ for all $a \in A$. In particular we have that $nAn^{-1} = B$*

Sometimes people don't use the word strongly here.

Corollary 7.14. *Write out what happens when S is abelian.*

Proof. Frattini argument. Take the centralizer of $C_G A$. Then $S \subset C$. Then S is in the centralizer of $B = gAg^{-1}$, which is gCg^{-1}. Thus

$$g^{-1}Sg \subset C$$

and as both are Sylows of C there exists a $c \in C$ with

$$cSc^{-1} = g^{-1}Sg.$$

This shows that $gc \in N$ and c commutes with A. Hence we choose $n = gc$ □

Remark 7.15. This proof works also for compact Lie groups. Then $\mathcal{S}$ of course is tori (which are abelian). Then $N/T = W$ is a Weyl group. ◇

Example 7.16. $\mathcal{G}$ is smooth linear algebraic groups, $\mathcal{S}$ is unipotent, smooth and connected. (Think of GL_3, this is highly non-abelian.) When S is non-abelian, N is not enough to describe the Fusion.

Take $G = GL_3(\mathbb{F}_p)$ and take A the element

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

and for B

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Then they are not conugate (via a normal subgroup). One way to see this is the following. We can conjugate them via the parabolic subgroup in two steps.

In the general situation we should instead work with the parabolic subgroups. ◇

The loose form of the following theorem is that fusion in S is controlled by 'local fusion'.

Theorem 7.17 (Alpevin's theorem)**.** *Suppose $A, B \subset S$. We say that they are **locally fused** if there is a subgroup $T \subset S$ containing them and an element x of $N_G T$ with $xAx^{-1} = B$.*

The really interesting case is the following.

Example 7.18. Let $\mathcal{G}$ be algebraic reductive groups over an algebraically closed field and $\mathscr{S}$ be the unipotent subgroups. Then $B = TU$ and U is 'the Sylow'. $U = R^l B$ is normal in B.

Look at the minimal parabolic groups contined in B and different from B of course (these are called rank one parabolics). You get r of them, and thus you also get r unipotent radicals. Then the fusion holds in the following form.

Let $A, B \subset U$ and let $g \in G$ conjugate them. Then you can split g as $s_1 \dots s_n$ such that $s_i \in$ either $N_G U_i$ or Then you can conjugate A and B by a series of moves using the s_i, beginning with s_N, and each group belongs to the unipotent radical. ◇

8 Fusion and Self Control

Suppose you have a Sylow subgroup $S \subset G$ and a G-module M. On cohomology you get an inclusion

$$H^i(G,M)_p \subset H^i(S,M), i \geq 1.$$

Cantan-Eilenberg and Tate discovered that the image are the 'stable' elements.

For each p-group $P \subset G$, we get an element

$$\alpha_P \in H^i(P,M).$$

Theorem 8.1. *The following are true.*

(a) For $P' \subset P$, $\alpha_P \mapsto \alpha_{P'}$.

(b) For $g \in G$, g conj. $P \to P'$, $P' = gPg^{-1}$ and

$$H^i(P,M) \to H^i(P',M).$$

(c) α_P comes from $\alpha \in H^i(G,M)$.

(d) By b it is enough to have α_P for $P \subset S$.

Last time we had exceptional isomorphisms A_6 and A_7, $3A_6, 3A_7$. The 3-Sylow is $C_3 \times C_3$, and $H^i(C_3 \times C_3, \mathbb{Z}/3\mathbb{Z})$... you find a cohomology class and the 3-Sylow group of $3A_6$ is a p^{2+1}-group (an Eisenberg group). You get $S_6 \to A_8$.

Remark 8.2. You get the Valentine group $\subset GL_3(\mathbb{C})$, which has some amazing representations. ◇

Similarly, if you look in PGL_3 you find A_6.

Remark 8.3. The TeXer came in late so the preceding may be non-sensical. ◇

Self Control

This is Serre's terminology. Let $H \subset G$ be groups.

Definition 8.4. We say that there is *self-control* of $H \subset G$ if H controls its fusion in G. Recall that this means that for every subgroup $A \subset H$, $g \in G$ such that $gAg^{-1} \subset A$, then there exists $h \in G$ such that $gag^{-1} = hah^{-1}$. (Tate: this should be *strongly self controlled*). ◇

We will speak a lot about this.

Example 8.5. Trivial example: Supose that H is a retract of G, i.e. there is a projection of G onto H, or equivalently there is a normal complement N of H in G such that G is a semi-direct product of H by N. In this case there is no problem. ◇

Theorem 8.6 (Frobenius)**.** *Let G be finite and S p-Sylow. Then the following are equivalent.*

(a) S has self control in G.

(b) S has a normal complement in G.

(c) For every p-subgroup P of G and $g \in N_G P$ such that g has p'-order, g centralizes P iff $N_G P / C_G P$ is a p-group.

What Frobenius did is prove the difficult part (c) $\Rightarrow$ (b). I have already told you that $(b) \Rightarrow (a)$, and $(a) \Rightarrow (c)$ is easy (but I don't want to do it).

The starting point of the proof is finding a non-trivial normal subgroup by the following idea. If $S \neq 1$ is a p-group, then there is a map $\alpha : S \to \mathbb{Z}/p\mathbb{Z}$ which we can think of as $\alpha \in H^1(S, \mathbb{Z}/p\mathbb{Z})$. We need to show that this is compatible with fusion, but that is clear. Now you lift to G and let G_1 be the kernel of α and S_1 be the kernel of α on S. It is not clear that if you continue this you get your N, but this is true.

Theorem 8.7 (Criterion for self-control)**.** *Let $H \subset G$. Let $X = G/H$ (a homogeneous space). Then self control is equivalent to the following property (called SC): for every pair P, Q of elements of X there exists a $g \in G$ such that*

(1) $gP = Q$.

(2) g commutes with the subgroup G_{PQ} of elements of G fixing P and Q.

Proof. Assume self control. Set $H = G_P$. Then $G_{PQ} \subset G_P$. Choose g such that $gP = Q$; we want to modify this to get condition (2). We have $G_{PQ} \subset G_Q = gG_Pg^{-1}$. Thus $g^{-1}G_Qg \subset G_P$. By self-control there is an element $h \in H$ such that $g^{-1}xg = h^{-1}xh$ for all $x \in G_{PQ}$. But then hg^{-1} commutes with G_{PQ}.

The converse is just as trivial. □

Example 8.8. Consider $S_{n-1} \subset S_n$ and $X = \{1, \ldots, n\}$. You are given $P, Q \in X$. If $P = Q$ then $g = 1$. If $P \neq Q$ then let g translate P to Q. Thus $S_i \subset S_n$ has self-control. ◇

Example 8.9. Consider $GL_n \subset GL_{n+m}$. This also has self control. To do this with the criterion is a big mess. Suppose we have a subgroup $A \subset GL_n$. We need to prove that if there exists $g \in GL_{n+m}$ such that $gAg^{-1} \subset GL_n$, then we can replace g by an element of GL_n.

But then we have $M = k^n$ viewed as a $k[A]$-module of rank n. We need another module M' such that $M \oplus 1 \cong M' \oplus 1$ (this is exactly equivalent to Fusion). By the Krull Schmitz theorem we know that $M \cap M'$. ◇

Remark 8.10. People like to joke that there is a field k with one element. Then $GL_n(k) = S_n$, and so we can deduce the previous theorem from the latter one. ◇

Example 8.11. Let $GL_n(k) \subset GL_n(k')$ for **any** extension k' of k. In terms of modules you have some module Λ which is a k-algebra. For two Λ-modules M_1 and M_2 of rank n, if $M_1 \otimes k' \cong M_2 \otimes k'$ then $M_1 \cong M_2$. $\diamond$

Proof. **Case 1**: k is infinite. Look at $\phi \in \mathrm{Hom}_k(M_1, M_2)$. Then the determinant is non-zero and we get a k-rational point.

Case 2: For a finite extension take the restriction of scalars. $\square$

Let me give for relaxiation a completely different style of example. Let G be a real Lie group with finitely many connected components. Let K be a maximal compact subgroup. We will be interested in the quotient G/K. We will assume that this is a Riemannian symmetric space of hyperbolic (i.e. non-positive curvature) type. A symmetric space means that for every point there is a symmetry about that point, i.e. an automorphism which fixes a point and reverses a tangent vector.

Theorem 8.12. *In this case $K \subset G$ has self control.*

Proof. There is a unique geodesic joining any two points. Take the symmetry with respect to the midpoint. This does the trick. $\square$

Example 8.13. Take a linear algebraic group G whose connected component is a reductive group. Then there is an $\mathbb{R}$-structure on G such that $G(\mathbb{R}) \subset G(\mathbb{C})$ has self control (Borel). For instance $G(\mathbb{C})/G(\mathbb{R}) \cong \mathbb{R}^n$. $\diamond$

Remark 8.14. I don't believe that the symmetric part is necessary, but I haven't checked it. $\diamond$

This next one is used quite often in the literature.

Example 8.15. Let V/k, char $k \neq 2$. Assume that on V we have a non-degenerate symmetric or alternating form q. Look at $O_q(V) \subset GL(V)$ (resp. $Sp(V, q) \subset GL(V)$). Then there is self-control. $\diamond$

In another language, if you have two orthogonal representations which are isomorphic (i.e. conjugate) in GL then they are in O.

Proof. It is convenient to give a unified proof. Let A be a finite dimensional algebra over k with an involution $a \mapsto a^*$. Let $U_A := \{a | a \in A : aa^* = 1\}$. Then $U_A \subset A^\times$.

Theorem 8.16. *This pair has self control.*

This implies the theorem we wanted, taking $A = \mathrm{End}(V)$. The proof uses the following lemma.

Lemma 8.17. *Let A be a finite dimensional k-algebra and $x \in A$. Then there exists $y \in A$ with $y^2 = x$ and $y \in k[x]$.*

Proof. *Proof of Lemma A plays no role in this lemma. You can replace A by $k[x]$ and reduce to the case when A is a local Artin algebra with residue field k and use Hensel (char $\neq 2$) to lift. □

Now let $A, *$ be an algebra with an involution. Then $x^* = *$ implies that there exists a y fixed by $*$ with $y^2 = x$ and $y \in k[x]$.

You can finishe the proof yourself. □

9 More on Fusion Control and Element-Conugate Homomorphisms.

We begin with some additions and corrections to last week. The first addition is the following. We said that a subgroup $H \subset G$ has **self-control** if for any $A \subset H$ and g such that $gAg^{-1} \subset H$, then we can find an h that does the same.

Lemma 9.1. *Take X a homogeneous space G/H. Suppose that for any two points $P, Q \in X$ and suppose that there exists a $g \in G$ such transforms P into Q and which commutes with the stabliizer of the pair (P, Q).*

This is equivalent to the following.

Lemma 9.2. *There exists a set S of representatives of G/H (i.e. we can write $G = S \cdot H$) which is stable under H conjugation.*

Proposition 9.3 (Mastow)**.** *If G is a real Lie group over $\mathbb{R}$ such that the index of the connected component is finite, then we get an S as in the last lemma. In fact one can take $S = \exp(L_1) \cdots \exp(L_i)$, $L_i \subset \mathrm{Lie}(G)$.*

Let G be a reductive group over $\mathbb{C}$ and consider $G(\mathbb{C}) = K \exp(P)$ for $P \subset \mathrm{Lie}(G)$, $K = G(\mathbb{R})$ and $P = i \,\mathrm{Lie}\, K$. Now we make a correction.

Remark 9.4. Last time we said that if you have a symmetric space X, one should take an involution with respect to the midpoint, but this involution is not in the connected component. We fix this by taking a product of involutions $i_R i_P$. ◇

Examples of Self control

I still have a few to give you.

Example 9.5. Let k be algebraically closed of char $\neq 2$. We have

$$O_n(k) \to GL_n(k)$$

$$Sp_n() \to GL_n(k).$$

Let A be an algebra with an involution and let $U \subset A^\times$. We were proving that U has self control. If you have $x \in A^\times$ such that $x^* = x$ then there is a $y \in A$ with $y^* = y$ and $y^2 = x, y \in k[x]$.

We need that there exists a $g' \in A^\times$ such that $g' = gU$ with g' commuting to $U \cap gUg^{-1}$. Now I need to copy a formula because this is the kind of thing that you mix up. We get $x = gg^*$. Then $y^2 = gg^*$. Then $y^{-1}g \in U$ (easy computation). Then $g = yy^{-1}g \in U$. I don't want to do the computation on the board, but it is trivial. ◇

Example 9.6. $SO_n \to GL_n$ has self control for n odd. Basically you do it in O_n and project onto SO_n. This does *not* have self control for n even and ≥ 2. You have to go to the normalizer. ◇

Theorem 9.7 (Griess). *(1)* $G_2(\mathbb{C}) \subset SO_7(\mathbb{C}) \subset O_7(\mathbb{C}) \subset GL_7(\mathbb{C})$ *and*

$$G_2(\mathbb{C}) \to GL_7(\mathbb{C})$$

has self control.

(2) $F_4(\mathbb{C}) \to E_6(\mathbb{C})$ *has self control.*

The proof consists in looking at the double cosets. More interesting is whether this is true over k algebraically closed of characteristic > 3.

Question 9.8. Are there other embeddings with a similar property? ◇

Another case is $G_2 \subset Spin_8$ by 'triality'. When n is odd you get $SO_n \to GL_n$ and $Sp_n \to GL_n$.

This concludes what I wanted to tell you about self control.

Element Conjugate Homomorphisms.

Let Γ be a group and let G be another group. Consider

$$\rho_1, \rho_2 : \Gamma \to G.$$

Definition 9.9. We say that ρ_1 and ρ_2 are element conjugate if for every $\gamma \in \Gamma$, $\rho_1(\gamma)$ is G-conjugate to $\rho_2(\gamma)$. ◇

We are going to give a few cases where locally implies global, i.e. if ρ_1 and ρ_2 are locally conjugate then they are conjugate.

Example 9.10. Here is a small counterexample. Let Γ be the group

$$\Gamma = \left\{ \begin{pmatrix} 1 & n \\ 0 & \epsilon \end{pmatrix} : n \in \mathbb{Z}, \epsilon = \pm 1 \right\}.$$

Let G be the dihedral group, and let $\epsilon : \Gamma \to \pm 1$. Then $\rho_1 : \gamma \mapsto \gamma$ and $\rho_2 : \gamma \mapsto \epsilon\gamma$. These are locally conugate but not conjugate. This is a minimal, but not semisimple counterexample. ◇

We conclude that we need a semistable semisimplicty hypothesis.

Example 9.11. If $G = GL_n(k)$, k a field and ρ_1, ρ_2 are semisimple then local to global holds. ◇

Theorem 9.12 (Brauer)**.** *Let k be a field and let A be an algebra over k with unit. We are interested in $\rho_1, \rho_2 : A \to M_n(k)$, and let E_1, E_2 be A-modules, n-dimensional over k. Let $X \subset A$ such that A is the smallest k-vector space containing X. An xample would be $A - k[\Gamma], X = \Gamma$.*

Suppose

(1) For every $x \in X$, $\rho_1(x), \rho_2(x)$ have the same characteristic polynomial. and that

(2) ρ_i are semi-simple

Then E_1 and E_2 are isomorphic.

If you supress (2) then they are just isomorphic in the K_0 group of A.

Remark 9.13. The trace does not work well in characteristic p for stupid reasons $(\oplus_1^p E)$. ◇

Proof. The proofs in the books are not good. The point is that under the hypothesis, the traces are the same. Then the multiplicity of the irreducible components are the same. Then you can write your two modules (after base change) as

$$E_1 = F \oplus pE_1^1$$

$$E_2 = F \oplus E_2^1$$

and you find that

$$(ch.E_1^1)^p \cong (ch.E_2^1)^p.$$

You then induct to remove the p. □

Now take k algebraically closed of characteristic not 2, and take G either $O_n(k)$ or $Sp_n(k)$.

Theorem 9.14. *Local to global holds for G.*

Proof. Look at $\Gamma \to \emptyset_n(k) \subset GL_n(k)$ and use the previous theorem and fusion. □

Now you ask, 'for what Lie group does this kind of thing hold?'

Theorem 9.15 (Griess, Larsen)**.** *Local to global is not true (for suitable finite Γ and ground field $\mathbb{C}$) for SO_n, n even and ≥ 6, or when G is an exceptional Lie group (other than G_2).*

SO_4 is okay.

This is too bad. One wants to understand for instance maps $A_5 \to E_8(\mathbb{C})$ up to conjugation.

Remark 9.16. Local to global is also not true for PGL_n, $n \geq 3$. People working in Langlands care about this. For instance, consider $\Gamma = C_3 \times C_3$ and map this to PGL_3. For an embedding ρ, you recieve an invariant third root of unity. That invariant you cannot tell from the local conjugation. Now you write down ρ_1, ρ_2 which are locally conjugate but with different invariants. $\diamond$

Example 9.17. Let Γ finite and let L/K have Galois group Γ and be unramified (to make things easier). Given an irreducible $\Gamma \to PGL_3$. If you have two locally conjugate ρ, then they are locally conjugate from the point of view of local fields. So they have the same L-function. But in principal they should still give different global representaitons. $\diamond$

From my point of view the locally conjugate stuff is just an excuse to think about Fusion.

The beginning of Friday's lecture.

What we want to speak about is representations of a finite group G in characteristic p and the relation with characteristic 0. In general they are not semi-simple.

Remark 9.18. There are two points of view.

(1) Replace a representation with its semi-simplification, i.e. $\oplus M_i$, summing over its Jordan-Holder decomposition. Let K_0 be a group of $k[G]$-modules of finite type and look at $M \mapsto [M] \in K_0(G)$. Then $[M] = [M']$ iff their semi-simplifications are the same. You can describe the elements of $K_0(G)$ via

   (a) Char. poly.

   (b) Brauer trace.

(2) *Homotopy category.* Define a new category by taking M to be $k[G]$-modules. Define a new hom

$$\mathrm{Hom}_{mod}(M_1, M_2) = \mathrm{Hom}(M_1, M_2)/\sim$$

   where two are equivalent if the map factors through a projective module. If G is a p-group. If $G = C_p$, $M = \oplus Jordan$.

$\diamond$

Theorem 9.19. *Two modules are isomorphic iff they are the same from the two above points of view.*

References

Mastow. Annals. 1956ish.

Griess - Invent. Math. 121 (1995) 25-277.

Larsen - Israel J. - 8 (1994) 253 - 277 .

– Ofnart. Oxford 47 (1996) 73-83

10 Representations in Characteristic p

When you study representations of a group G in characteristic p, we have two techniques: taking semisimplifications and studying Grothendieck groups.

Brauer Characters

Let G be a group and let V,V' be two semi-simple $k[G]$-modules of finite dimension.

Theorem 10.1. *V is isomorphic to V' if and only if for every $g \in G$, the characteristic polynomial of g_V is the same as for $g_{V'}$.*

I.e g_V and $g_{V'}$ have the same multisets of eigenvalues.

We have instead the following lazy way (lazy for the speaker and the listener). Now let G be finite of order $n \cdot p^\alpha$, $(n,p) = 1$, and suppose $k \supset \mu_n$. Then the set of eigenvalues is in k.

Then the lazy way is to identify $\mu_n(k) \cong \mu_n(\mathbb{C})$ via ϕ. We can then embed the eigenvalues in $\mathbb{C}$.

Definition 10.2. The Brauer character is

$$\chi_{Br}(g) = \sum \phi(z_i)$$

where z_i are the eigenvalues of g_V. ◇

Theorem 10.3 (Brauer, Nesbilt)**.** *If V, V' are semisimple, then $V \cong V'$ iff $\chi_{Br,V} = \chi_{Br,V'}$.*

Proof. In the case of a finite group we can decompose g into its Jordan decomposition su where s has order prime to p, u has order a power of p and they commute. Then the eigenvalues of g are the same as of s.

If you have two semisimple modules V, V', then if for every cyclic subgroup $C \subset G$ of order prime to p, $V|_C \cong V'|_C$, then $V \cong V$. □

This was the lazy way. Still with the same notation we can define in $\mathbb{C}$ the subfield $\mathbb{Q}(\zeta_n)$ and even $\mathbb{Z}(\zeta_n)$. We can look at the prime ideals lying above p. Choose one of them. Then the residue field can be imbedded in k. Now the lifting is more natural.

Usually one then completes at $\mathfrak{p}$, getting the standart setting for Brauer characters, which is a local field K of characteristic 0 with residue field k.

Now this has nothing to do with finite groups. It works even for algebras. Let K have discrete valuation v with integers $\mathcal{O}_K$ and uniformizer π, $k = \mathcal{O}_K/\pi\mathcal{O}_K$ the residue field, K char. 0 and k char. $p > 0$. Let G be a group (not necessairly finite).

We could instead consider an $\mathcal{O}_K$-algebra A and look at $A \otimes K$, $A \otimes k$.

(1) Begin with V a finite dimensional K-vector space with G action. Does there exist an $\mathcal{O}_K$-lattice L which is G-stable.

This is not true in general, but there is a simple, perhaps not so useful, criterion. Look at the image of $\mathcal{O}_K[G]$ in the endomorphisms $\mathrm{End}_K V$. This is an $\mathcal{O}_K$-module, and it is finitely generated over $\mathcal{O}_K$ iff there exists a stable lattice L as above. In particular this is OK if G is finite.

(2) Assume this condition is fulfulled and choose such an L. We reduce it, forming L/piL which is a vector space over k with a G action. This is not in general semisimple, but we can define $\tilde{L}^{ss}$ to be its semisimplificaiton $\oplus V_i$, V_i its Jordan quotients.

Theorem 10.4 (Brauer)**.** *$\tilde{L}^{ss}$ is independent of the choice of L.*

Remark 10.5. You have the same proof for algebras. ◇

You can also prove this using characteristic polynomials. Just restrict the Brauer characters.

Theorem 10.6 (Ribet-Thompson)**.** *Let k be finite, K local, complete with respect to a discrete valuation with residue field k. Let G be a group (pro-finite is ok) and let V be a representationa and assume that there is a stable lattice, and assume that V is irreducible. Choose L and look at $\tilde{L}$ as a $k[G]$-module. Then there is a choice of L such that $\tilde{L}$ is indecomposable.*

Ribet used this to manufacture non-trivial extension of some modules. For the proof you in general have to use the Bruhah-Tits building.

Remark 10.7. The theorem would look better if one could replace irreducible by indecomposible. You can do the same thing for algebras. This is not too necessary though. ◇

Example 10.8. Let A be finite dimensional algebra over a field k as above. Then A is generated additively (i.e. as a module) by its invertible elements except when $|k| = 2$ and A has a quotient isomorhic to $F_2 \times \mathbb{F}_2$. I.e. let $G = A^\times$, then we get a quotient $k[G] \to A$. ◇

Homotopy and Loops

Assume that G is finite. One defines a category of $k[G]$-modules and declares that projective modules are 0, and quotient the hom sets by maps which can be factored through a projective module.

Definition 10.9. We define the **loop functor** of Hilton, for a finitely generated M to be ΩM in the following

$$0 \to \Omega M \to P \to M \to 0$$

where P is any projective module. You let $\Omega^{-1}M = SM$ to be the **suspension** functor

$$0 \to M \to P \to \Omega^{-1}M \to 0.$$

$\diamond$

Example 10.10. Let $G = C_p$ cyclic of order p. Then we have a classification of indecomposible modules via Jordan matricies $J_1, \ldots, J_p$; J_1 is trivial, J_p is free of rank p, and every module is $M = \oplus n_i J_i$. Then $M \sim M'$ in the homotopy category iff $n_i = n_i'$ ofr $i \neq p$.

So you lose very little information. $\diamond$

Now an application to algebraic geometry. This is From Nakaima, Inv. math $\sim$ 1985. Let k be a field (algebraically closed) of characteristic p. Let X be a projective (because I am chicken) algebraic variety. We have G finite acting on X, so we can speak of X/G. Suppose we are given $\mathscr{F}$ a coherent sheaf on X/G. We are interested in $H^i(X, \pi^*\mathscr{F})$. This is a G-module.

We need a tameness assumption. Here this takes the following form: for every point $x \in X$, the stabilizer G_x of x has order prime to p.

Assume that $H^i = 0$ except for $i = n$

Theorem 10.11. $H^i(X, \pi^*\mathscr{F}) \cong \Omega^{m+1} H^{n+m}(X)$

Corollary 10.12. *If $H^i(X) = 0$ for $i \neq n+m, m > 0$ then H^n is a projective module. Also, if G acts freely then $H^n(X)$ is a free $k[G]$-module.*

The proof is that if you know a module from the Brauer and homotopy point of view, then you know it. If the group is cyclic of order p, then you get $\Omega_i = J_{p-i}$, $\omega^2 J_i = J_i$.

Nakaima was interested in the case of an algebraic curve. Then

$$H^0 \cong \Omega^2 H^2.$$

Of course in the proof one proves something more.

Remark 10.13. General fact: there is a complex C of $k[G]$-modules with $C^i = 0$ for $i < 0$ adn $i > \dim X$ (i.e. bounded, call this a 'perfect complex'; see SGA 6 or in Mumford's book on Abelian varieties) such that

$$H^i(X) \cong H^i(C).$$

$\diamond$

Proof. *[Proof of the theorem] We will show how this remark implies the above theorem for a curve. Then we have

$$0 \to C^0 \xrightarrow{\delta} C^1 \to 0$$

$$0 \to H^0(X) \to C^0 to \delta C^0 \to 0$$

and

$$0 \to \delta C^0 \to C^1 \to H^1 \to 0.$$

These imply that

$$\Omega^1 \delta C^0 = H^0(X), \Omega H^1 = \delta C^0.$$

The bigger proof is not different. □

Now take G finite and $k = \mathbb{F}_p$. Let 1 be k with the trivial action. What is $\Omega^2 1$? Recall that

$$0 \to I \to \mathbb{F}_p[G] \to 1 \to 0,$$

so $\Omega^1 1 = I$.

There is a canonical extension

$$1 \to \Omega^2 1 \to E \to G \to 1$$

which is universal. There is $\alpha \in H^2(G, \Omega^2 1) \sim H^1(G, \Omega 1) \sim H^0(G, 1) = 1$. This is an essential extension, i.e. this α does not belong to the image of $H^2(G, M) \to H^2(G, \Omega^2 1)$. One can also show that this is the largest one with kernel abelian and killed by p. For A_5 and $p = 2$ you can calculate this. This is of interest to people who play the inverse Galois game.